

Elementary Abstract Algebra: Examples and Applications

Supervising editors:

Justin Hill, Chris Thron

St. Philip's College / Texas A&M University-Central Texas

Incorporating source materials by

Thomas Judson (Stephen F. Austin State University)

Dave Witte Morris and Joy Morris (University of Lethbridge)

A. J. Hildebrand (University of Illinois Urbana-Champaign)

With chapters by

Christy Douglass, Jennifer Lazarus, Mark Leech, Moses Marmolejo, Adam McDonald, Katrina Smith, Johnny Watts, David Weathers, Holly Webb (TAMU-CT)

and additional contributions by

Semi Harrison, Rachel McCoy, Khoi Tran (TAMU-CT)

May 12, 2023

This book is offered under the GNU Free Documentation License, Version 1.2, or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the appendix, entitled “GNU Free Documentation License”. The Set Theory and Functions chapters are licensed under Creative Commons license (Attribution-NonCommercial-ShareAlike 2.0).

Material from the 2012 version of "Abstract Algebra, Theory and Applications" by Thomas Judson may be found throughout much of the book. Attributions are found at the beginning of each chapter. Judson's book is covered by the GFDL license, and all chapters of the current book containing his work are covered by the same license. A current version of "Abstract Algebra, Theory and Applications" may be found at:

abstract.ups.edu.

The Set Theory and Functions chapters are largely based on material from "Proofs and Concepts" (version 0.78, May 2009) by Dave Witte Morris and Joy Morris, which may be found online at:

<https://archive.org/details/flooved3499>, or
<http://people.uleth.ca/~dave.morris/books/proofs+concepts.html>

Their book is covered by the Creative Commons license (Attribution-NonCommercial-ShareAlike 2.0), and the two chapters containing their work are covered by the same license.

The material on induction was modified from \LaTeX code originally obtained from A. J. Hildebrand, whose course web page is at:

<http://www.math.uiuc.edu/~hildebr/>

Justin and Chris would like to express their deepest gratitude to Tom, Dave and Joy, and A. J. for generously sharing their original material. They were not involved in the preparation of this manuscript, and are not responsible for any errors or other shortcomings.

Please send comments and corrections to: thron@tamuct.edu. You may also request the solutions manual and \LaTeX source code from this same email address.

Course web page: <http://abstractalgebra.altervista.org/>

Online book: <http://s12x.aimath.org/book/aafmt/>

©2013,2014, 2015, 2018, 2020, 2022 by Justin Hill and Chris Thron.
Some rights reserved.




Portions ©1997 by Thomas Judson. Some rights reserved.









Portions ©2006-2009 by Dave Witte Morris and Joy Morris. Some rights reserved.




Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. The license may be found at: <https://www.gnu.org/licenses/fdl-1.3.en.html>









ISBN: 978-0-359-04211-1









Contents




| | | |
|----------|--|-----------|
| 1 | Forward | 1 |
| 2 | Glossary of symbols | 8 |
| 3 | Preliminaries | 10 |
| 3.1 | In the Beginning  | 10 |
| 3.2 | Integers, rational numbers, real numbers | 11 |
| 3.2.1 | Properties of arithmetic operations | 12 |
| 3.2.2 | Order relations | 15 |
| 3.2.3 | Manipulating equations and inequalities | 16 |
| 3.2.4 | Exponentiation (VERY important) | 20 |
| 3.3 | Test yourself | 21 |
| 4 | Complex Numbers | 25 |
| 4.1 | The origin of complex numbers  | 25 |
| 4.1.1 | A number that can't be real (and we can prove it!) | 25 |
| 4.1.2 | Unreal, but unavoidable | 29 |
| 4.1.3 | A mathematical revolution | 30 |
| 4.2 | Arithmetic with complex numbers  | 35 |
| 4.2.1 | Complex arithmetic | 35 |








| | | |
|----------|--|-----------|
| 4.2.2 | Comparison of integer, rational, real and complex addition properties | 40 |
| 4.2.3 | Comparison of integer, rational, real and complex multiplication properties | 41 |
| 4.2.4 | Modulus and complex conjugate | 42 |
| 4.3 | Alternative representations of complex numbers  | 46 |
| 4.3.1 | Cartesian representation of complex numbers | 46 |
| 4.3.2 | Vector representation of complex numbers | 47 |
| 4.3.3 | Polar representation of complex numbers | 48 |
| 4.3.4 | Converting between rectangular and polar form | 48 |
| 4.3.5 | Multiplication and powers in complex polar form | 52 |
| 4.3.6 | A Remark on representations of complex numbers | 59 |
| 4.4 | Complex numbers and roots of algebraic equations | 60 |
| 4.4.1 | Roots of unity and regular polygons  | 60 |
| 4.4.2 | Complex n th roots in general  | 70 |
| 4.4.3 | Complex roots of polynomial equations  | 73 |
| 4.5 | Applications of complex numbers  | 76 |
| 4.5.1 | General remarks on the usefulness of complex numbers | 76 |
| 4.5.2 | Complex numbers in electrical engineering: phasors | 77 |
| 4.5.3 | Complex numbers and fractals: the Mandelbrot set | 83 |
| 4.6 | Hints for “Complex Numbers” exercises | 86 |
| 4.7 | Study guide for “Complex Numbers” chapter | 88 |
| 5 | Modular Arithmetic | 92 |
| 5.1 | Introductory examples  | 92 |
| 5.2 | Modular equivalence and modular arithmetic | 94 |
| 5.3 | Modular equations  | 103 |
| 5.3.1 | More uses of modular arithmetic | 103 |
| 5.3.2 | Solving modular equations | 106 |
| 5.4 | The integers mod n (a.k.a. \mathbb{Z}_n)  | 113 |
| 5.4.1 | Remainder arithmetic | 113 |




| | | |
|----------|--|------------|
| 5.4.2 | Cayley tables for \mathbb{Z}_n | 119 |
| 5.4.3 | Closure properties of \mathbb{Z}_n | 121 |
| 5.4.4 | Identities and inverses in \mathbb{Z}_n | 123 |
| 5.4.5 | Inverses in \mathbb{Z}_n | 123 |
| 5.4.6 | Other arithmetic properties of \oplus and \odot | 125 |
| 5.4.7 | Group: a central concept in abstract algebra | 126 |
| 5.5 | Modular division  | 128 |
| 5.5.1 | A sticky problem | 128 |
| 5.5.2 | Greatest common divisors | 133 |
| 5.5.3 | Computer stuff | 137 |
| 5.5.4 | Diophantine equations | 138 |
| 5.5.5 | Multiplicative inverse for modular arithmetic | 146 |
| 5.5.6 | Chinese remainder theorem | 149 |
| 5.6 | Hints for “Modular Arithmetic” exercises | 152 |
| 5.7 | Study guide for “Modular Arithmetic” chapter | 154 |
| 6 | Modular Arithmetic, Decimals, and Divisibility | 158 |
| 6.1 | Decimal representations | 158 |
| 6.1.1 | Decimal representation formula | 158 |
| 6.1.2 | Formulas for decimal digits of integers | 159 |
| 6.1.3 | Formulas for decimal digits of nonintegers | 161 |
| 6.1.4 | Repeating decimals | 164 |
| 6.1.5 | Divisibility rules | 166 |
| 6.2 | Decimal representations in other bases | 170 |
| 7 | Set Theory | 177 |
| 7.1 | Set Basics  | 177 |
| 7.1.1 | Definition and examples | 178 |
| 7.1.2 | Important sets of numbers | 181 |
| 7.1.3 | Operations on sets | 183 |
| 7.2 | Properties of set operations  | 189 |







| | | |
|----------|--|------------|
| 7.3 | Do the subsets of a set form a group?  | 195 |
| 7.4 | Hints for “Set Theory” exercises | 198 |
| 7.5 | Study guide for “Set Theory” chapter | 199 |
| 8 | Functions: Basic Concepts | 201 |
| 8.1 | The Cartesian product: a different type of set operation  | 201 |
| 8.2 | Introduction to functions  | 204 |
| 8.2.1 | Informal look at functions | 204 |
| 8.2.2 | Official definition of functions | 211 |
| 8.3 | One-to-one functions  | 215 |
| 8.3.1 | Concept and definition | 215 |
| 8.3.2 | Proving that a function is one-to-one | 218 |
| 8.4 | Onto functions  | 227 |
| 8.4.1 | Concept and definition | 227 |
| 8.4.2 | Proving that a function is onto | 229 |
| 8.5 | Bijections  | 235 |
| 8.5.1 | Concept and definition | 235 |
| 8.5.2 | Proving that a function is a bijection | 236 |
| 8.6 | Composition of functions  | 242 |
| 8.6.1 | Concept and definition | 242 |
| 8.6.2 | Proofs involving function composition | 247 |
| 8.7 | Inverse functions  | 252 |
| 8.7.1 | Concept and definition | 252 |
| 8.7.2 | Which functions have inverses? | 255 |
| 8.8 | Do functions from A to B form a group? | 258 |
| 8.9 | Hints for “Functions: basic concepts” exercises | 261 |
| 8.10 | Study guide for “Functions: Basic Concepts” chapter | 262 |







| | | |
|-----------|--|------------|
| 9 | Introduction to Cryptography  | 267 |
| 9.1 | Overview and basic terminology | 267 |
| 9.2 | Private key cryptography | 269 |
| 9.2.1 | Shift codes | 269 |
| 9.2.2 | Affine codes | 272 |
| 9.2.3 | Monoalphabetic codes | 275 |
| 9.2.4 | Polyalphabetic codes | 276 |
| 9.2.5 | Spreadsheet exercises | 279 |
| 9.3 | Public key cryptography | 283 |
| 9.3.1 | The RSA cryptosystem  | 285 |
| 9.3.2 | Message verification | 287 |
| 9.3.3 | RSA exercises  | 288 |
| 9.3.4 | Additional exercises: identifying prime numbers  | 291 |
| 9.4 | References and suggested readings | 298 |
| 9.5 | Hints for “Applications (I): Introduction to Cryptography” exercises | 299 |
| 9.6 | Study guide for “Applications (I): Introduction to Cryptog- raphy” chapter | 300 |
| 10 | Sigma Notation | 302 |
| 10.1 | Lots of examples  | 302 |
| 10.2 | Algebraic rules for Sigmas | 305 |
| 10.2.1 | Constant multiples, sums, and products of sums | 305 |
| 10.3 | Change of variable and rearrangement of sums  | 307 |
| 10.4 | Common Sums  | 316 |
| 10.5 | Summation by parts | 320 |
| 11 | Application: Sigma Notation in Linear Algebra | 326 |
| 11.1 | Introduction to sigma notation in linear algebra  | 326 |
| 11.2 | Matrix multiplication | 327 |
| 11.3 | The identity matrix and the Kronecker delta | 330 |


| | | |
|-----------|--|------------|
| 11.4 | Abbreviated matrix notations | 335 |
| 11.5 | Matrix transpose and matrix inverse | 337 |
| 11.5.1 | Matrix transpose | 337 |
| 11.5.2 | Matrix inverse | 339 |
| 11.6 | Rotation matrices in 3 dimensions | 339 |
| 11.7 | Matrix traces | 343 |
| 11.8 | Levi-Civita symbols and applications | 346 |
| 11.8.1 | Levi-Civita symbols: definitions and examples | 346 |
| 11.8.2 | Levi-Civita symbols and determinants | 349 |
| 11.8.3 | Levi-Civita symbols and cross products | 354 |
| 11.8.4 | Proof of the vector BAC-CAB Rule | 357 |
| 11.8.5 | Proof of Euler's Rotation Theorem | 361 |
| 11.9 | Hints for "Sigma Notation" and "Applications of Sigma Notation" exercises | 367 |
| 11.10 | Study guide for "Sigma Notation" chapter | 369 |
| 12 | Polynomials | 373 |
| 12.1 | Why study polynomials? | 373 |
| 12.2 | Review of polynomial arithmetic  | 376 |
| 12.3 | Polynomial operations in summation notation | 378 |
| 12.4 | More exotic polynomials | 385 |
| 12.5 | Polynomial properties and summation notation | 391 |
| 12.6 | Polynomials and division | 399 |
| 12.6.1 | The Division Algorithm for polynomials over fields  | 399 |
| 12.6.2 | Greatest common divisors of polynomials | 403 |
| 12.6.3 | Polynomial roots and the FTOA (easy part)  | 406 |
| 12.6.4 | Algebraic closure and the FTOA (hard part) | 414 |
| 12.7 | Hints for "Polynomial Rings" exercises | 418 |



| | |
|---|------------|
| 13 Symmetries of Plane Figures  | 419 |
| 13.1 Definition and examples | 420 |
| 13.2 Composition of symmetries | 425 |
| 13.3 Do the symmetries of an object form a group?  | 429 |
| 13.4 The dihedral groups | 435 |
| 13.5 For further investigation | 445 |
| 13.6 An unexplained miracle | 446 |
| 13.7 Hints for “Symmetries of Plane Figures” exercises | 449 |
| 14 Permutations  | 450 |
| 14.1 Introduction to permutations | 450 |
| 14.2 Permutation groups and other generalizations | 452 |
| 14.2.1 The symmetric group on n numbers | 453 |
| 14.2.2 Isomorphic groups | 455 |
| 14.2.3 Subgroups and permutation groups | 456 |
| 14.3 Cycle notation  | 458 |
| 14.3.1 Tableaus and cycles | 458 |
| 14.3.2 Composition (a.k.a. product) of cycles | 461 |
| 14.3.3 Product of disjoint cycles | 464 |
| 14.3.4 Products of permutations using cycle notation | 468 |
| 14.3.5 Cycle structure of permutations | 470 |
| 14.4 Algebraic properties of cycles  | 473 |
| 14.4.1 Powers of cycles: definition of order | 473 |
| 14.4.2 Powers and orders of permutations in general | 477 |
| 14.4.3 Transpositions and inverses | 482 |
| 14.5 “Switchyard” and generators of the permutation group  | 485 |
| 14.6 Other groups of permutations  | 492 |
| 14.6.1 Even and odd permutations | 492 |
| 14.6.2 The alternating group | 498 |
| 14.7 Additional exercises | 500 |

| | |
|--|------------|
| 14.8 Hints for “Permutations” exercises | 502 |
| 14.8.1 Hints for additional exercises (Section 14.7) | 502 |
| 15 Introduction to Groups  | 503 |
| 15.1 Formal definition of a group | 504 |
| 15.2 Examples | 507 |
| 15.2.1 The group of units of \mathbb{Z}_n | 514 |
| 15.2.2 Groups of matrices | 516 |
| 15.3 Basic properties of groups | 519 |
| 15.4 Subgroups  | 528 |
| 15.5 Cyclic groups  | 535 |
| 15.5.1 Definitions | 535 |
| 15.5.2 Orbits (cyclic subgroups) | 539 |
| 15.5.3 Subgroups of cyclic groups | 545 |
| 15.6 Additional group and subgroup exercises | 547 |
| 15.7 Hints for “Abstract Groups: Definitions and Basic Properties” exercises | 550 |
| 16 Further Topics in Cryptography | 551 |
| 16.1 Diffie-Hellman key exchange | 551 |
| 16.1.1 Man in the middle attack | 559 |
| 16.2 Elliptic curve cryptography | 560 |
| 16.2.1 Definition of elliptic curves | 562 |
| 16.2.2 Elliptic curve arithmetic | 563 |
| 16.2.3 Elliptic curve groups | 568 |
| 16.2.4 Elliptic curves over \mathbb{Z}_p | 570 |
| 16.2.5 An encryption system using elliptic curves | 572 |
| 16.2.6 Next steps | 576 |
| 16.3 References and suggested reading | 576 |
| 16.4 Hints for “Further Topics in Cryptography” exercises | 579 |

| | |
|---|------------|
| 17 Equivalence Relations and Equivalence Classes | 580 |
| 17.1 Binary relations  | 580 |
| 17.2 Partitions and properties of binary relations  | 588 |
| 17.3 Examples of equivalence relations  | 600 |
| 17.4 Obtaining partitions from equivalence relations  | 606 |
| 17.4.1 From equivalence relations to equivalence classes | 606 |
| 17.4.2 From equivalence classes to partitions | 609 |
| 17.5 Modular arithmetic redux  | 612 |
| 17.5.1 The integers modulo 3 | 613 |
| 17.5.2 The integers modulo n | 615 |
| 17.5.3 What do we mean by “the same thing”? | 617 |
| 17.5.4 Something we have swept under the rug | 617 |
| 17.6 Hints for “Equivalence Relations and Equivalence Classes” exercises | 621 |
| 18 Cosets and Quotient Groups (a.k.a. Factor Groups)  | 622 |
| 18.1 Definition of cosets | 623 |
| 18.2 Cosets and partitions of groups | 627 |
| 18.3 Lagrange’s theorem, and some consequences | 631 |
| 18.3.1 Lagrange’s theorem | 631 |
| 18.3.2 Orders of elements, Euler’s theorem, Fermat’s little theorem, and prime order | 634 |
| 18.4 Normal subgroups and factor groups | 637 |
| 18.4.1 Normal subgroups | 637 |
| 18.4.2 Factor groups | 640 |
| 18.5 Factoring of groups and simple groups | 645 |
| 18.5.1 Concepts, definitions, and examples | 645 |
| 18.5.2 Simplicity of the alternating groups A_n for $n \geq 5$ | 647 |
| 18.5.3 The simplicity of A_n and the impossibility of poly- nomial root formulas | 651 |
| 18.6 Hints for “Cosets” exercises | 657 |

| | | |
|---|---|------------|
| 19 Error-Detecting and Correcting Codes |  | 659 |
| 19.1 Definitions and basic properties | | 659 |
| 19.2 Block Codes | | 663 |
| 19.3 Group codes |  | 671 |
| 19.4 Linear Block Codes | | 674 |
| 19.5 Code words and encoding in block linear codes | | 681 |
| 19.5.1 Canonical Parity-check matrices |  | 681 |
| 19.5.2 Standard Generator Matrices | | 684 |
| 19.5.3 Error detection and correction | | 688 |
| 19.6 Efficient Decoding | | 692 |
| 19.6.1 Decoding using syndromes | | 692 |
| 19.6.2 Coset Decoding | | 695 |
| 19.7 Additional algebraic coding exercises | | 698 |
| 19.8 References and Suggested Readings | | 700 |
| 19.9 Hints for “Error Detecting and Correcting Codes” exercises | | 701 |
| 20 Isomorphisms of Groups |  | 702 |
| 20.1 Preliminary examples | | 702 |
| 20.2 Formal definition and basic properties of isomorphisms | | 707 |
| 20.3 Examples and generalizations | | 710 |
| 20.3.1 Examples of isomorphisms | | 710 |
| 20.3.2 General properties of isomorphisms |  | 721 |
| 20.4 Classification up to isomorphism | | 723 |
| 20.4.1 Classifying cyclic groups | | 723 |
| 20.4.2 Characterizing all groups: Cayley’s theorem | | 725 |
| 20.5 Direct products and classification of abelian groups |  | 730 |
| 20.5.1 Direct Products | | 731 |
| 20.5.2 Classifying finite abelian groups by factorization | | 736 |
| 20.6 Proof that $U(p)$ is cyclic | | 743 |
| 20.6.1 Internal direct products | | 746 |
| 20.7 Hints for “Isomorphisms” exercises | | 751 |

| | |
|---|------------|
| 21 Exploration: Relating polynomials and matrices | 752 |
| 21.1 Definition of vector space | 753 |
| 21.2 Polynomials are also vectors | 755 |
| 21.3 Identifying polynomials with matrices | 756 |
| 21.4 Hints for “Polynomials and Matrices” exercises | 769 |
| 22 Homomorphisms of Groups | 770 |
| 22.1 Preliminary examples | 770 |
| 22.2 Definition and several more examples | 776 |
| 22.3 Proofs of homomorphism properties | 782 |
| 22.4 The First Isomorphism Theorem | 786 |
| 22.5 Hints for “Homomorphism” exercises | 789 |
| 23 Group Actions | 790 |
| 23.1 Basic definitions  | 790 |
| 23.2 Symmetries of regular polyhedra | 797 |
| 23.2.1 G -equivalence and orbits | 797 |
| 23.2.2 Stabilizers, stabilizer subgroups, and fixed point sets | 801 |
| 23.2.3 Counting formula for the order of polyhedral rotational symmetry groups | 804 |
| 23.2.4 Representing a symmetry group in terms of stabilizer subgroups | 807 |
| 23.2.5 Examples of other regular polyhedral rotation groups | 809 |
| 23.2.6 Euler’s formula for regular polyhedra | 823 |
| 23.2.7 Are there other regular polyhedra? | 827 |
| 23.2.8 Reflection symmetries of polyhedra | 828 |
| 23.2.9 Finite subgroups of the group of rotations in 3 dimensions | 829 |
| 23.3 Group actions associated with subgroups and cosets | 830 |
| 23.3.1 The integer lattice | 832 |
| 23.4 Conjugation | 841 |

| | | |
|-----------|---|------------|
| 23.4.1 | Commutative diagrams and the definition of conjugation | 841 |
| 23.4.2 | Conjugacy and group action | 846 |
| 23.4.3 | Order of conjugate elements | 847 |
| 23.4.4 | Conjugacy classes and the class equation | 850 |
| 23.5 | Hints for “Group Actions, with Applications” exercises | 854 |
| 24 | Introduction to Rings and Fields | 855 |
| 24.1 | Definitions and Examples  | 855 |
| 24.1.1 | Polynomial rings | 862 |
| 24.1.2 | Some Ring Proofs | 863 |
| 24.2 | Subrings | 865 |
| 24.3 | Extension Rings | 869 |
| 24.4 | Product Rings | 874 |
| 24.5 | Isomorphic rings | 877 |
| 24.6 | Ring homomorphisms: kernels, and ideals | 881 |
| 24.6.1 | Homomorphism kernels and ideals | 885 |
| 24.7 | Further properties of ideals and principal ideals | 891 |
| 24.8 | Quotient Rings | 893 |
| 24.9 | Integral domains, Principal ideal domains and fields | 896 |
| 24.9.1 | Division rings and fields  | 901 |
| 24.9.2 | Further properties of fields | 906 |
| 24.10 | Polynomials over fields | 908 |
| 24.10.1 | Algebraic closure of fields | 914 |
| 24.10.2 | Field extensions and algebraic elements | 916 |
| 24.10.3 | Applications of algebraic field extensions | 920 |
| 24.11 | References | 921 |
| 24.12 | Hints for “Introduction to Rings” exercises | 922 |
| 25 | Polynomial Codes | 923 |
| 25.1 | Polynomials with coefficients in \mathbb{Z}_2 | 923 |
| 25.2 | Cyclic Binary Codes | 925 |
| 25.3 | Polynomial Codes: definition and basic properties | 929 |

| | |
|---|------------|
| 26 Appendix: Induction proofs–patterns and examples | 938 |
| 26.1 Basic examples of induction proofs | 938 |
| 26.2 Advice on writing up induction proofs | 939 |
| 26.3 Induction proof patterns & practice problems | 940 |
| 26.4 Strong Induction, with applications | 946 |
| 26.5 More advice on induction and strong induction proofs | 950 |
| 26.6 Common mistakes | 951 |
| 26.7 Strong induction practice problems | 952 |
| 26.8 Non-formula induction proofs | 954 |
| 26.9 Practice problems for non-formula induction | 955 |
| 26.10 Fallacies and pitfalls | 956 |
| | |
| GNU Free Documentation License | 961 |
| | |
| GNU Free Documentation License | 961 |
| | |
| Index | 970 |

Forward

All truths are easy to understand once they are discovered; the point is to discover them. (*Source: Galileo Galilei, "Dialogue on the Two Chief World Systems"*)

To the student:

Many students start out liking math. Some like it well enough that they even want to teach it. However, when they reach advanced math classes (such as abstract algebra), they become bewildered and frustrated. Their textbooks talk about strange mathematical thingamabobs they've never heard of, which have nonsensical properties that come from who knows where. In lectures, the professor/oracle makes pronouncements (a.k.a "theorems") and utters long incantations (a.k.a "proofs"), but it's hard to see the point of either.

If the above paragraph describes you, then this book is meant for you!

There's a good reason why higher math classes are bewildering for most students. I believe that we math instructors tend to take too much for granted.¹ It's easy to forget that we're only able to understand abstractions because we have concrete examples that we keep referring back to, consciously or subconsciously. These examples enable us to fit new abstract ideas in with specific behaviors and patterns that we're very familiar with.

¹My father always says that trying to understand math is frustrating, but once you've got it it's even more frustrating to try to explain it to others.

But students who don't have a firm hold on the examples have nothing to hold on to, and are left grasping (and gasping) for air.

To be sure, most students have previously been exposed to various important examples that historically gave rise to abstract algebra. These examples include the complex numbers, integers mod n , symmetries, and so on. They can give definitions and do some basic computations according to the rules. But they haven't been given a chance to internalize these examples. They can kind of follow along, but they aren't "fluent".

Our hope is that after reading this book students will be able to say, "I've seen complex numbers, integers mod n and permutations before, but now I understand what makes them tick. I can see they have deep underlying similarities, which they share with other mathematical structures."

This is actually a very good time to be learning abstract algebra. Abstract algebra has moved from the outer boondocks inhabited by specialists and puzzle enthusiasts out into the center stage of modern science and technology. Two areas where abstract algebra has made strong contributions stand out particularly: information processing and physics. Coding of information is at the heart of information technology, and abstract algebra provides all of the methods of choice for information coding that is both reliable (impervious to errors) and private. On the other hand, many if not most of the great advances in physics in the past 100 years are due to deeper understanding of physical symmetries and the groups that produce them (the Lorentz group in special relativity is just one example). We try as much as possible to make connections with these two areas, and hope to do so increasingly in future editions.

We hope you enjoy the book. Send us your comments!

To the instructor

This book is not intended for budding mathematicians. It was created for a math program in which most of the students in upper-level math classes are planning to become secondary school teachers. For such students, conventional abstract algebra texts are practically incomprehensible, both in style and in content. Faced with this situation, we decided to create a book that our students could actually read for themselves. In this way we have been able to dedicate class time to problem-solving and personal interaction rather than rehashing the same material in lecture format.

Admittedly it falls short of the typical syllabus for an upper-level abstract algebra class. But what's the point of covering the syllabus, if the students don't retain anything? The unhappy fact is that many students at this level haven't yet mastered the important basic examples (complex numbers, etc.) that provide motivation, so it's unrealistic to expect them to grasp abstractions if they don't even understand what's being abstractified. So instead we have dived deeply into basic examples—and these are the just the basic examples that will be most useful to those who go on to a career in high school teaching.

The book is highly modular, and chapters may be readily omitted if students are already familiar with the material. Some chapters (“Preliminaries” and “Sigma Notation”) are remedial. Other chapters cover topics that are often covered in courses in discrete mathematics, such as sets, functions, and equivalence classes. (Much of this material is taken from the Morris' book, with some amplifications.) We have found from experience that students need this re-exposure in order to gain the necessary facility with these concepts, on which so much of the rest of the book is based.

Whenever possible we have introduced applications, which may be omitted at the instructor's discretion. However, we feel that it is critically important for preparing secondary teachers to be familiar with these applications. They will remember these long after they have forgotten proofs they have learned, and they may even be able to convey some of these ideas to their own students.

Additional resources

This is the Information Age, and a mere textbook is somewhat limited in its ability to convey information. Accordingly, as we continue to use the book in our classes, we are continuing to build an ecosystem to support the book's use:

- The book's web site is <http://abstractalgebra.altervista.org/>.
- An electronic version of the book is available at <https://sl2x.aimath.org/book/aafmt/>.
- For a print copy, we recommend an on-demand print service such as <https://www.printme1.com/>.

- A comprehensive set of short video presentations of the book’s content may be found on the EAAEA YouTube channel: <https://www.youtube.com/playlist?list=PL2uooHqQ6T7PW5na4EX8rQX2WvBBdM8Qo>. A second YouTube channel with worked exercises may be found at: <https://www.youtube.com/playlist?list=PL2uooHqQ6T7NMO1Lk5lX3tDyQF8URCwwK>.
- An “Instructor’s Supplement” is available upon request: email the editor thron@tamuct.edu from a verifiable faculty email address.
- Any instructor wishing to customize the material or extract certain portions may email the editor thron@tamuct.edu to request the L^AT_EX source code.

Acknowledgements

In our preparation of this text, we were fortunate to find via the web some extraordinarily generous authors (Tom Judson, Dave Witte Morris and Joy Morris, A. J. Hildebrand) who freely shared their material with us. Thanks to them, we were able to put the first version of this textbook together within the span of a single semester (not that we’re finished – this is a living book, not a dead volume). We hope that other instructors will similarly benefit from the material offered here.

Several Master’s students at Texas A&M-Central Texas have made contributions to the book as part of a projects course or thesis. Their names are listed in the title, and their contributions are acknowledged at the beginning of each chapter.

Our very special thanks to Meghan DeWitt for her thorough critical reading of the book and her incisive comments. The book has greatly benefited from her numerous suggestions.

Unless the LORD builds the house, the builders labor in vain.
Unless the LORD keeps the city, the watchman is wakeful in vain. It is vanity to rise up early, stay up late, and eat the bread of sorrows, for He gives sleep to those He loves.” (Psalm 127:1-2)

Organization plan of the book

A chapter organization diagram is given in Figure 1.0.1. Brief descriptions of the chapters and their dependencies are as follows:

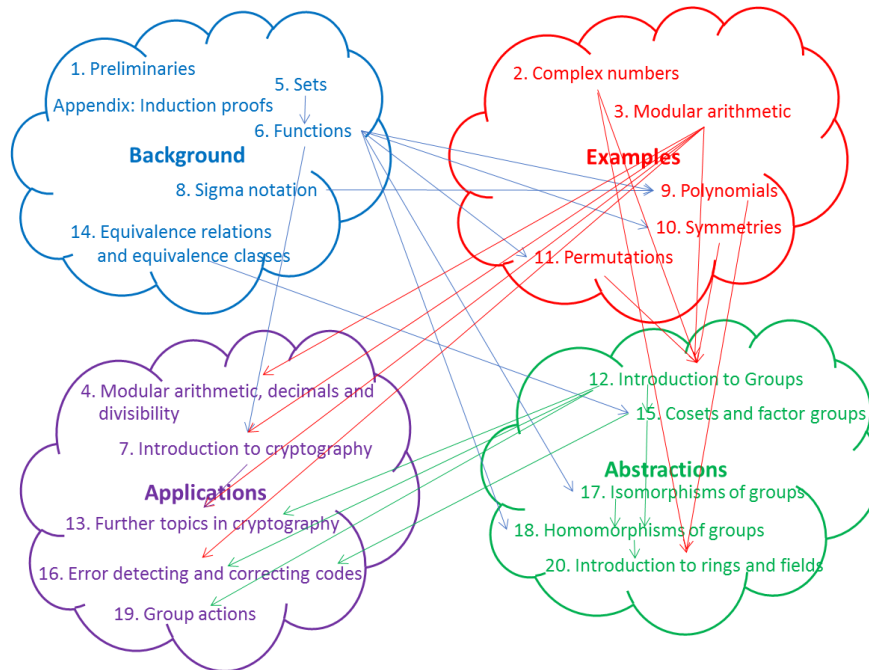


Figure 1.0.1. Interdependence of chapters

1. Preliminaries: A review of properties of integers, rationals, and reals, at the high school level. We only review the properties – we do not formally construct these number systems. Some remedial exercises are included. Used in: All other chapters.
2. Complex numbers: Basic properties of complex arithmetic, polar form, exponentiation and roots. Some exercises require proofs of complex number properties. The last section presents applications to signal processing and fractals. Used in: Symmetries (10); all theory chapters (
3. Modular arithmetic: The gold-standard example of finite groups and rings. Arithmetic properties, Euclidean algorithm, Diophantine equations; We bring out homomorphism properties (without the terminology). Used in: all subsequent chapters

4. Modular arithmetic, decimals, and divisibility: application of modular arithmetic to decimal representation of real numbers (in arbitrary bases) and divisibility rules.
5. Sets. Basic set properties. Can be skipped if students have an adequate background in discrete math. Used in: functions
6. Functions. Basic ideas of domain, range, into, onto, bijection. This chapter can be skipped if students have an adequate background. Used in: all subsequent chapters
7. Introduction to cryptography: Explains the concepts of public and private key cryptography, and describes some classic cyphers as well as RSA. Used in: Further topics in Cryptography (13)
8. Sigma notation: This chapter prepares for the “polynomials” chapter. Sigma notation is useful in linear algebra as well. Can be skipped if students are already familiar with this notation. Used in: Polynomials (9)
9. Polynomials: fundamental example of rings. Euclidean algorithm for polynomials over fields. FTOA, prove easy part and discuss the hard part. Will cover this again more rigorously in later chapter. Used in: Introduction to Groups (12), Introduction to Rings (20)
10. Symmetries: Symmetries are a special case of permutations. They are treated first because they are easily visualizable, and because they connect algebraic aspects to geometry as well as complex numbers. Used in: Permutations (11)
11. Permutations: In light of Cayley’s theorem, this example is key to the understanding of finite groups. Students are introduced to the mechanics of working with permutations, including cycle multiplication. Cycle structure is explored, as are even and odd permutations. Used in: Introduction to Groups (12)
12. Introduction to Groups: This chapter introduced basic properties of groups, subgroups, and cyclic groups, drawing heavily on the examples presented in previous chapters. Used in: all subsequent chapters
13. Further topics in cryptography. Diffie-Hellman key exchange, elliptic curve cryptography over \mathbb{R} and over \mathbb{Z}_p

14. Equivalence relations and equivalence classes. This is necessary for understanding cosets. This chapter may be skipped if students have seen them before. Used in: Cosets and Factor Groups (15)
15. Cosets and Factor Groups: Introductory properties, Lagrange's theorem, Fermat's Theorem, simple groups. Used in: all subsequent chapters.
16. Error Detecting and Correcting Codes. A discussion of block codes. Some knowledge of linear algebra is required.
17. Isomorphisms of Groups: Examples and basic properties; direct products (internal and external); classification of abelian groups up to isomorphism. Used in: all subsequent chapters
18. Homomorphisms of Groups: Kernel of homomorphism; properties; first isomorphism theorem. Used in: all subsequent chapters
19. Group Actions: Besides basic definitions, this chapter contains a long discussion of group actions applied to regular polyhedral, as well as the universal covering space of the torus.
20. Introduction to Rings: Includes definitions and examples; subrings and product rings; extending polynomial rings to fields; isomorphisms and homomorphisms; ideals; principal ideal domains; prime ideals and unique factorization domains; division rings; fields; algebraic extensions.
21. Appendix: Induction Proofs – patterns and examples. Some proofs in the book require induction. This section gives the background needed for students to write formal induction proofs.

Glossary of symbols

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$: natural numbers (positive integers), integers, rationals, real numbers, complex numbers

$\mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$: rationals, real numbers, complex numbers without 0

\mathbb{Z}_n : Integers mod n

Q_8 : Quaternion group ($\{\pm 1, \pm i, \pm j, \pm k\}$)

\oplus, \odot : Modular addition and multiplication

$M_n(\mathbb{Z}, \mathbb{R}, \mathbb{C} \dots)$: $n \times n$ matrices with entries in $\mathbb{Z}, \mathbb{R}, \mathbb{C} \dots$

$\exists; \forall$: There exists; for all

$\text{cis } \theta$: $\cos \theta + i \sin \theta$

$|x|, |z|, |S|, |G|, |g|$: Absolute value of the real number x ; modulus of the complex number z ; number of elements in the set S or the group G ; order of the group element g .

$a \div b$: a divides b .

$GL_n(\mathbb{R})$: General linear group of invertible $n \times n$ matrices with coefficients in \mathbb{R} .

$\text{mod}(m, n)$: Remainder of m when divided by n

$a \equiv b \pmod{n}$: a is equivalent to $b \pmod{n}$

$a \in S$: a is an element of the set S

$:=$: Defined as

$U(n)$: Group of units (elements with multiplicative inverses) mod n .

$, \cup, \cap, \setminus$: Empty set, union, intersection, set difference

\times : Cartesian product or vector cross product (depending on context)

iff: If and only if

$f \circ g$: Composition of f and g (apply g first, then f)

ϵ_{ijk} : Levi-Civita (totally antisymmetric tensor) symbol

Id: Identity function

id, e : Identity element of a group

gcd, lcm: Greatest common divisor, least common multiple

$\begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$: Permutation in tableau format

$(a_1 \cdots a_{n_1})(b_1 \cdots b_{n_2}) \dots$: Permutation in cycle notation

Preliminaries

3.1 In the Beginning

Let's start at the very beginning
A very good place to start
When you read you begin with A B C
When you sing you begin with Do Re Me

(Oscar Hammerstein, *The Sound of Music*)

God made the integers; all else is the work of man. (Leopold Kronecker, German mathematician, 1886)

If Maria had been more mathematically inclined, she might have continued: “When you count, you begin with 1 2 3”. Ordinarily we think of the “counting numbers” (which mathematicians call the *natural numbers* or *positive integers*) as the “very beginning” of math.

It's true that when we learn math in school, we begin with the counting numbers. But do we really start at the “very beginning”? How do we know that $1 + 1 = 2$? How do we know that the methods we learned to add, multiply, divide, and subtract will always work? We've been taught how to factor integers into prime factors. But how do we know this always works?

Mathematicians are the ultimate skeptics: they won't take “Everyone knows” or “It's obvious” as valid reasons. They keep asking “why”, breaking things down into the most basic assumptions possible. The very basic

assumptions they end up with are called *axioms*. They then take these axioms and play with them like building blocks. The arguments that they build with these axioms are called *proofs*, and the conclusions of these proofs are called *propositions* or *theorems*.

The mathematician's path is not an easy one. It is exceedingly difficult to push things back to their foundations. For example, arithmetic was used for thousands of years before a set of simple axioms was finally developed (you may look up "Peano axioms" on the web).¹ Since this is an elementary book, we are not going to try to meet rigorous mathematical standards. Instead, we'll lean heavily on examples, including the integers, rationals, and real numbers. Once you are really proficient with different examples, then it will be easier to follow more advanced ideas.²

This text is loaded with proofs, which are as unavoidable in abstract mathematics as they are intimidating to many students. We try to "tone things down" as much as possible. For example, we will take as "fact" many of the things that you learned in high school and college algebra—even though you've never seen proofs of these "facts". In the next section we remind you of some of these "facts". When writing proofs or doing exercise feel free to use any of these facts. If you have to give a reason, you can just say "basic algebra".

We close this prologue with the assurance that abstract algebra is a beautiful subject that brings amazing insights into the nature of numbers, and the nature of Nature itself. Furthermore, engineers and technologists are finding more and more practical applications, as we shall see in some of the later chapters.

The original version of this chapter was written by David Weathers.

3.2 Integers, rational numbers, real numbers

We assume that you have already been introduced to the following number systems: integers, rational numbers, and real numbers. These number systems possess the well-known arithmetic operations of addition, subtraction, multiplication, and division. The following statements hold for all of these number systems.

¹The same is true for calculus. Newton and Leibniz first developed calculus around 1670, but it wasn't made rigorous until 150 years later.

²Historically, mathematics has usually progressed this way: examples first, and axioms later after the examples are well-understood.

Warning 3.2.1. There are number systems for which the following properties do NOT hold (as we shall see later). So they may be safely assumed ONLY for integers, rational numbers, and real numbers. \diamond

3.2.1 Properties of arithmetic operations

We assume the following properties of arithmetic operations on the integers, rational numbers, and real numbers. In the following list of properties, a, b, c are arbitrary numbers (integers, rational, or real), unless otherwise specified. We use the notation $a \cdot b$ to denote the product of a and b (i.e. a multiplied by b).

- (A) **Additive identity:** $0 + a = a, a + 0 = a$.
- (B) **Multiplicative identity:** $1 \cdot a = a, a \cdot 1 = a$.
- (C) **Additive inverse.** For every number a there is a unique number denoted $-a$ such that $a + -a = 0$ and $-a + a = 0$. Note that $a + -b$ is usually written as $a - b$.
- (D) **Multiplicative inverse** (**real and rational numbers only**) For every nonzero real or rational number a there is a unique number $1/a$ such that $a \cdot 1/a = 1$ and $1/a \cdot a = 1$.
- (E) **Addition is associative:** $(a + b) + c = a + (b + c)$. (Note that the parentheses indicate which operation is performed first: for example, in $(a + b) + c$ the $a + b$ is done first, and then c is added to the result.)
- (F) **Multiplication is associative** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Same comment applies as in previous property.)
- (G) **Addition is commutative :** $a + b = b + a$ (Be careful about this one! It's easy to take for granted. We will see that in some number systems, it's not true.)
- (H) **Multiplication is commutative :** $a \cdot b = b \cdot a$ (Same comment applies as in previous property.)
- (I) **Multiplication distributes over addition:** $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$. (Technically, these are called the *left distributive* and *right distributive* properties respectively.)

(J) **Zero divisor property** $a \cdot 0 = 0$ and $0 \cdot a = 0$.

Exercise 3.2.2.

- (a) For each of the properties (D,E,F,G,H) above, give a specific equation (with actual numbers) that illustrates the property. For example, for property (E) a specific example would be $(3 + 5) + 4 = 8 + 4 = 12$ is equal to $3+(5+4) = 3 + 9 = 12$.
- (b) Give a specific example that shows that subtraction is *not* commutative.
- (c) Give a specific example that shows that division is *not* associative.

◇

Exercise 3.2.3. Which of the above properties must be used to prove each of the following statements? (Note each statement may require more than one property)

- (a) $(x + y) + (z + w) = (z + w) + (x + y)$
- (b) $(x \cdot y) \cdot z = (z \cdot x) \cdot y$
- (c) $(a \cdot x + a \cdot y) + a \cdot z = a \cdot ((x + y) + z)$
- (d) $((a \cdot b) \cdot c + b \cdot c) + c \cdot a = c \cdot ((a + b) + a \cdot b)$

◇

Note that the associative property allows us to write expressions without putting in so many parentheses. So instead of writing $(a + b) + c$, we may simply write $a + b + c$. By the same reasoning, we can remove parentheses from any expression that involves only addition, or any expression that involves only multiplication: so for instance, $(a \cdot (b \cdot c) \cdot d) \cdot e = a \cdot b \cdot c \cdot d \cdot e$. Using the associative and distributive property, it is possible to write any arithmetic expression without parentheses. So for example, $(a \cdot b) \cdot (c + d)$ can be written as $a \cdot b \cdot c + a \cdot b \cdot d$. (Remember that according to operator precedence rules, multiplication is always performed before addition: thus $3 \cdot 4 + 2$ is evaluated by first taking $3 \cdot 4$ and then adding 2.)

These properties can be used to prove arithmetic statements that ordinarily we take for granted. For example, we automatically replace $-1 \cdot a$ with $-a$, but this really needs to be justified. In fact, this requires one of the other properties in the above list:

Exercise 3.2.4. Show that $a + (-1 \cdot a) = 0$ and $(-1 \cdot a) = 0$ (this is the same thing as showing that $-1 \cdot a$ is the additive inverse of a , or $-1 \cdot a = -a$). Which of the above properties did you use? \diamond

Exercise 3.2.5. Rewrite the following expressions without any parentheses and simplify as much as possible, but *without using the commutative property*.

- (a) $((x + y) + (y + z)) \cdot w - 2y \cdot w$
- (b) $0.5 \cdot ((x + y) + (y + z) + (z + x))$
- (c) $(((((a + b) + c) \cdot d) + e) \cdot f) + g + h$

\diamond

Exercise 3.2.6. For parts (a–c) of the preceding exercise, now apply the commutative property to the results to simplify the expressions as much as possible. \diamond

Exercise 3.2.7. Given the expression: $((a - b) + b)(a - b) + b^2$

- (a) Simplify the expression *without using distributive or commutative property*.
- (b) Simplify the expression *without using the commutative property*.
- (c) Simplify the expression using all laws.

\diamond

Exercise 3.2.8. Given the expression: $(r + p)(s + q) - (p + s)(q + r)$

- (a) Simplify the expression *without using distributive or commutative property*.
- (b) Simplify the expression *without using the commutative property*.
- (c) Simplify the expression using all laws.

◇

3.2.2 Order relations

We also have *order relations* on the real, rational, and integer number systems, which are expressed by the terms ‘greater than’ and ‘less than’ with corresponding symbols $>$ and $<$. If a and b are numbers, then the mathematical statement ‘ $a > b$ ’ is logically identical to the statement ‘ $b < a$ ’ (another way of saying this is: $a > b$ if and only if $b < a$). **Positive numbers** are defined to be those numbers greater than the additive identity 0, and **negative numbers** are defined to be those that are less than 0. We assume the following properties of the order relation on the integers, rational numbers, and real numbers:

- (A) The multiplicative identity 1 is positive.
- (B) Given two numbers, exactly one of these three are true: either the first number is greater than the second, or the second number is greater than the first, or the two numbers are equal.
- (C) The sum of two positive numbers is positive. The sum of two negative numbers is negative.
- (D) The product of two positive or two negative numbers is positive. The product of a positive and negative number is negative.

Exercise 3.2.9. Using the above properties, show that $1 + 1$, $1 + 1 + 1$, and $1 + 1 + 1 + 1$ are all positive. (It can be shown by induction that the sum of any number of copies of 1 must be positive. The set $\{1, 1 + 1, 1 + 1 + 1, \dots\}$ is called the *set of positive integers*.) ◇

Exercise 3.2.10. Suppose $a > b$, $b \geq 0$ and $ab = 0$ (note that ‘ $b \geq 0$ ’ means that either $b > 0$ or $b = 0$). What can you conclude about the values of a

and b ? Use one (or more) of the properties we have mentioned to justify your answer. \diamond

Exercise 3.2.11. Suppose $ab > cb$, $b < 0$, and $c < 0$. For each of the following statements, either prove that it is always true, or give an example to show that it is not always true:

- (a) $a > b$
- (b) $a < 0$.
- (c) $b < c$
- (d) $a < c$

\diamond

Besides these order properties, there is a special order property that applies only to integers. This property is called the *principle of well-ordering*, and may be stated as a proposition as follows:

Proposition 3.2.12. (*Well-ordering principle*) Any set of positive integers has a smallest element.

This may seem obvious, but in mathematics we have to do our best not to take anything for granted. Sometimes the most “obvious” statements are the most difficult to prove. In this case, the well-ordering principle can be proved from the principle of mathematical induction (see Chapter 26). The proof is beyond the scope of this course.³

3.2.3 Manipulating equations and inequalities

Following are some common rules for manipulating equations and inequalities. Notice there are two types of inequalities: *strict inequalities* (that use the $>$ or $<$ symbols) and *nonstrict inequalities* (that use the \geq or \leq symbols).

³It is also possible to prove the principle of mathematical induction from well-ordering principle—it’s a matter of personal preference which is taken as an axiom, and which is taken as a consequence.

- (A) **Substitution:** If two quantities are equal then one can be substituted for the other in any true equation or inequality and the result will still be true.
- (B) **Balanced operations:** Given an equation, one can perform the same operation to both sides of the equation and maintain equality. The same is true for inequalities for the operation of addition, and for multiplication or division by a *positive* number.
- (C) **Inequality reversal:** Multiplying or dividing an inequality by a negative value will reverse the inequality symbol.
- (D) **Fractions in lowest terms:** The ratio of two integers can always be reduced to lowest terms, so that the numerator and denominator have no common factors.

Exercise 3.2.13. Give specific examples for statements (A–D) given above. You may use either numbers or variables (or both) in your examples. For (A) and (B), give one example for each of the following cases: (i) equality, (ii) strict inequality, (iii) nonstrict inequality. \diamond

Exercise 3.2.14. Parts (a–f) of this exercise give a sequence of successive steps in a proof of an important arithmetic fact. For each of the steps, give either an arithmetic operation property (from Section 3.2.1) or an equation manipulation rule (from Section 3.2.3) which justifies the step.

- (a) $1 - 1 = 0$
- (b) $(1 - 1) \cdot a = 0 \cdot a$
- (c) $(1 - 1) \cdot a = 0$
- (d) $1 \cdot a + (-1) \cdot a = 0$
- (e) $a + (-1) \cdot a = 0$
- (f) $(-1) \cdot a$ is the additive inverse of a .

\diamond

As a result of the previous exercise, we have a proof of the following proposition:

Proposition 3.2.15. For any integer, rational, or real number a the following equation holds: $-a = (-1) \cdot a$.

This proposition may seem way too obvious to you, but it's actually saying something very significant. “ $-a$ ” denotes the additive inverse of a , while “ $(-1) \cdot a$ ” denotes the additive inverse of 1 times the number a . There is no a priori reason why these two things should be the same. Try to think back to when you first learned this arithmetic stuff—at that time, it probably wasn't as obvious as it seems now. The exercise shows that it actually follows from even more basic facts about arithmetic.

The following exercise walks you through a proof of another important fact.

Exercise 3.2.16. For each step in the following argument, give either an arithmetic operation property (from Section 3.2.1) or an equation manipulation rule (from Section 3.2.3) which justifies the step.

We first suppose that $a > b$ and $c > d$.

- (a) $a - b > 0$ and $c - d > 0$
- (b) $(a - b) + (c - d) > 0$
- (c) $a + (-b + c) - d > 0$
- (d) $a + (c - b) - d > 0$
- (e) $(a + c) + (-b + -d) > 0$
- (f) $((a + c) + (-b + -d)) + (b + d) > b + d$
- (g) $(a + c) + ((-b + -d) + (b + d)) > b + d$
- (h) $(a + c) + ((-b + -d) + (d + b)) > b + d$
- (i) $(a + c) + (-b + ((-d + d) + b)) > b + d$
- (j) $(a + c) + (-b + (0 + b)) > b + d$
- (k) $(a + c) + (-b + b) > b + d$
- (l) $(a + c) + 0 > b + d$
- (m) $a + c > b + d$

◇

The preceding exercise gives us a proof of the following proposition, which we will need later in the book.

Proposition 3.2.17. Let a, b, c, d be integer, rational, or real numbers such that $a > b$ and $c > d$. It follows that $a + c > b + d$.

Finally, we're going to prove is that -1 is negative. At this point you may be thinking, "Duh, it's got a minus sign, so of course it's negative!" But if you look back in Section 3.2.1 property (B), you'll see that the minus sign on -1 just means that it's the additive inverse of the multiplicative identity 1. On the other hand, negative numbers were defined in Section 3.2.2 as numbers that are less than the additive identity 0. Just because we've decided to write the additive inverse of 1 as -1 , doesn't mean that we can automatically assume that $-1 < 0$. Remember, be skeptical!

Proposition 3.2.18. $-1 < 0$

PROOF. This will be our first exposure to a proof technique called *proof by contradiction*. We'll make use of this technique throughout the book. In this case, the idea goes as follows. There's no way that -1 could be positive, because if it were then $1 + (-1)$ would also have to be positive, which it isn't because we know it's 0. There's also no way that -1 could be 0, because if it were we'd have $-1 = 0$, and adding 1 to both sides gives $0 = 1$, which is false because 1 is positive and 0 isn't. Since -1 isn't positive and it isn't equal to 0, the only option left is that it's negative. This is the gist of the argument, but we have to write it out more carefully to satisfy those nit-picking mathematicians. Every step in our argument must have a solid reason.

So here goes the formal proof. We'll give a logical sequence of mathematical statements, followed by a reason that justifies each statement—this is called *statement-reason format*.

First we show that $-1 > 0$ is false:

| Statement | Reason |
|---------------------------|--|
| Suppose $-1 > 0$. | Proof by contradiction: supposing the opposite |
| $1 > 0$ | Prop. (A) in Section 3.2.2 |
| $1 + (-1) > 0$. | Prop. (C) in Section 3.2.2 |
| $1 + (-1) = 0$ | Prop. (B) in Section 3.2.1 |
| Contradiction is achieved | The last 2 statements contradict |
| $-1 > 0$ is false | The supposition must be false |

Next, we show that $-1 = 0$ is false:

| Statement | Reason |
|---------------------------|---|
| Suppose $-1 = 0$ | Proof by contradiction: supposing the opposite |
| $1 + (-1) = 1 + 0$ | Follows from previous statement by substitution |
| $0 = 1$ | Props. (A) and (B) in Section 3.2.1 |
| $0 > 0$ | Prop. (A) in Section 3.2.2 |
| Contradiction is achieved | $0 > 0$ contradicts Prop. (B) in Section 3.2.2 |
| $-1 = 0$ is false | The supposition must be false |

According to Property (B) in Section 3.2.2, there are three possibilities: either $-1 > 0$, $-1 = 0$, or $-1 < 0$. We have eliminated the first two possibilities. So the third possibility must be true: $-1 < 0$. This completes the proof.

□⁴

Exercise 3.2.19. Using Proposition 3.2.15 Proposition 3.2.18, and one of the order relation properties, show that the additive inverse of any positive number is negative. ◇

3.2.4 Exponentiation (VERY important)

Exponentiation is one of the key tools of abstract algebra. It is *essential* that you know your exponent rules inside and out!

- (I) Any nonzero number raised to the power of 0 is equal to 1.⁵
- (II) A number raised to the sum of two exponents is the product of the same number raised to each individual exponent.

⁴The '□' symbol will be used to indicate the end of a proof. In other words: Ta-daa!

⁵Technically 0^0 is undefined, although often it is taken to be 1. Try it on your calculator!

- (III) A number raised to the power which is then raised to another power is equal to the same number raised to the product of the two powers.
- (IV) The reciprocal of a number raised to a positive power is the same number raised to the negative of that power.
- (V) Taking the product of two numbers and raising to a given power is the same as taking the powers of the two numbers separately, then multiplying the results.

Exercise 3.2.20. For each of the above items (I–V), give a general equation (using variables) that expresses the rule. For example one possible answer to (II) is: $x^{y+z} = x^y \cdot x^z$. \diamond

Exercise 3.2.21. Write an equation that shows another way to express a number raised to a power that is the difference of two numbers. \diamond

3.3 Test yourself

Test yourself with the following exercises. If you feel totally lost, I strongly recommend that you improve your basic algebra skills before continuing with this course. Trying to do higher math without a confident mastery of basic algebra is like trying to play baseball without knowing how to throw and catch.

Exercise 3.3.1. Simplify the following expressions. Factor whenever possible

(a) $2^4 4^2$

(d) $\frac{a^5}{a^7} \cdot \frac{a^3}{a}$

(b) $\frac{3^9}{9^3}$

(e) $x(y-1) - y(x-1)$

(c) $\left(\frac{5}{9}\right)^7 \left(\frac{9}{5}\right)^6$

\diamond

Exercise 3.3.2. Same instructions as the previous exercise. These examples are harder. (*Hint:* It's usually best to make the base of an exponent as simple as possible. Notice for instance that $4^7 = (2^2)^7 = 2^{14}$.)

(a) $6^{1/2} \cdot 2^{1/6} \cdot 3^{3/2} \cdot 2^{1/3}$

(d) $2^3 \cdot 3^4 \cdot 4^5 \cdot 2^{-5} \cdot 3^{-4} \cdot 4^{-3}$

(b) $(9^3)(4^7) \left(\frac{1}{2}\right)^8 \left(\frac{1}{12}\right)^6$

(c) $4^5 \cdot 2^3 \cdot \left(\frac{1}{2}\right)^5 \cdot \left(\frac{1}{4}\right)^3$

(e) $\frac{x(x-3) + 3(3-x)}{(x-3)^2}$

◇

Exercise 3.3.3. Same instructions as the previous exercise. These examples are even harder. (*Hint:* Each answer is a single term, there are no sums or differences of terms.)

(a) $\frac{a^5 + a^3 - 2a^4}{(a-1)^2}$

(f) $\left(\frac{(x+y)^{x+y}(x-y)^{x-y}}{(x^2-y^2)^x}\right)$

(b) $a^x b^{3x} (ab)^{-2x} (a^2 b)^{x/2}$

(c) $(x+y^{-1})^{-2} (xy+1)^2$

(g) $\left(\frac{6^6}{2^2 3^3} + \frac{2^8 3^6}{6^3}\right)^{1/2}$

(d) $\frac{(3^x + 9^x)(1 - 3^x)}{1 - 9^x}$

(e) $\frac{3x^2 - x}{x-1} + \frac{2x}{1-x}$

(h) $\frac{(a+b)(b+c) + (a-b)(b-c)}{a+c}$

◇

Exercise 3.3.4. Find ALL real solutions to the following equations.

(a) $x^2 = 5x$

(d) $3^{-x} = 3(3^{2x})$

(b) $(x - \sqrt{7})(x + \sqrt{7}) = 2$

(e) $16^5 = x^4$

(c) $2^{4+x} = 4(2^{2x})$

(f) $\frac{1}{1+1/x} - 1 = -1/10$

◇

Exercise 3.3.5. (*Challenge problems*) These problems come from Chinese high school math web sites (thanks to J. L. Thron)

- (a) Simplify: $\frac{2^{n+4}-2(2^n)}{2(2^{n+3})}$
- (b) Given $m = 7^9$ and $n = 9^7$, express 63^{63} in terms of m and n .
- (c) Given $2^x 3^y = 10$ and $2^y 3^x = 15$, find x and y .
- (d) Show that the following expression always has real roots: $(x-3)(x-2) = a(a+1)$, where a is any real number.
- (e) If $3x - 5y + 3 = 0$, find $\frac{8^{x+2}}{32^y}$.
- (f) Solve for x : $(6x+7)^2(3x+4)(x+1) = 6$ (multiply to obtain two quadratic terms, then substitute)
- (g) Solve for x : $9^x + 12^x = 16^x$. (divide the equation by one of the terms)
- (h) Solve for x : $\frac{x+1}{x+2} + \frac{x+8}{x+9} = \frac{x+2}{x+3} + \frac{x+7}{x+8}$. (Simplify the numerators in each fraction)
- (i) Given that $m = 2019^2 + 2020^2$, evaluate $\sqrt{2m-1}$. (use the fact that $2020 = 2019+1$)
- (j) Solve for x : $\sqrt{x^2+9} + \sqrt{x^2-9} = 5 + \sqrt{7}$. (To avoid squaring twice, use difference of squares to obtain a second equation, then use the two equations together to eliminate one of the square roots.)
- (k) Given $a = 4^{1/3} + 2^{1/3} + 1$, evaluate $\frac{3}{a} + \frac{3}{a^2} + \frac{1}{a^3}$. (Write out the expressions for $\frac{1-x^3}{1-x}$ and $(1+y)^3$, and see if you can relate them to the given expressions)
- (l) Solve for x : $x = \sqrt{x - \frac{1}{x}} + \sqrt{1 - \frac{1}{x}}$. (To avoid squaring twice, use difference of squares to obtain a second equation, then use the two equations together to eliminate one of the square roots.)
- (m) Suppose that $a+b+c = 0$ and $a^3+b^3+c^3 = 0$. Show that $a^n+b^n+c^n = 0$ for all odd values of n . (Look at two cases: (a) at least one of a, b, c is equal to 0; (b) exactly two of the numbers have the same sign (without loss of generality, you may assume that $a, b > 0$ and $c < 0$)).
- (n) Given $a^2 - 9a + 1 = 0$, find $a^2 - 7a + \frac{18}{a^2 + 1}$. (solve the first equation for a^2 and for $a^2 + 1$, and use substitutions.)

- (o) Given that x_1 and x_2 are both solutions to the equation $x^2 + 1 = 1/x$, find $2021^{x_1 - x_2}$ (graph the functions $y = x^2 + 1$ and $y = 1/x$).
- (p) Given that $x + y = 3$ and $xy = 1$, evaluate $x^5 + y^5$ (use the first two expressions to find quadratic equations for x and y , then substitute repeatedly for x^2 and y^2 in $x^5 + y^5$).
- (q) Given that $\frac{a+b}{c} = \frac{a+c}{b} = \frac{b+c}{a}$, find the value of $\frac{abc}{(a+b)(b+c)(c+a)}$ (Be careful! There may be more than one answer. Take two of the equations and clear the denominators. Both sides will have a common factor, which may or may not be zero.)
- (r) Given $x = 2 + \sqrt{2}$, find $x^4 - 4x^3 + 7x^2 - 20x + 16$. (Find a quadratic equation satisfied by $2 + \sqrt{2}$.)
- (s) Given $4x^{-4} - 2x^{-2} = 3$ and $x^4 + y^2 = 3$, find $4x^{-4} + y^4$.
- (t) Given $30^x = 2010$ and $67^y = 2010$, find $x^{-1} + y^{-1}$.
- (u) Given $a + b = 6$ and $ab + (c - a)^2 + 9 = 0$, find $a + b + c$ (Try to find a particular solution for a, b, c . Look at the signs of the terms.)
- (v) Simplify $\frac{1234^2}{2469^2 + 2467^2 - 2}$ (no calculator required!)
- (w) Given $2^a = 10$, $2^b = 5$, $2^c = 200$, compute $a - 4041b + 2020c - 6060$. (Exponent rules!)
- (x) Given $\frac{xy}{x+y} = 1$, $\frac{yz}{y+z} = 2$, $\frac{xz}{x+z} = 3$, find x . (Take reciprocals and break the fractions apart. Then add together the equations.)
- (y) Given that $a_1, a_2, \dots, a_{1000}$ are the first 1000 terms of a geometric series with $a_1 = 1/5$ and $a_{1000} = 20$. The product $a_1 \cdot a_2 \cdot \dots \cdot a_{1000}$ can be expressed as 2^x . Find x . (Recall that the n th term of a geometric series has the form ar^n . Group terms in the geometric series in pairs.)
- (z) Without using a calculator, determine which is larger: 9^{12} or 15^9 .

◇

Complex Numbers

HORATIO: O day and night, but this is wondrous strange!

HAMLET: And therefore as a stranger give it welcome. There are more things in heaven and earth, Horatio, Than are dreamt of in your philosophy.

(Source: Shakespeare, *Hamlet*, Act 1 Scene 5.)

Although complex numbers are defined to include “imaginary” numbers, the practical applications of complex numbers are far from “imaginary”. We shall touch on some of the applications in this chapter: but there are many many more in engineering, in physics, and in other sciences as well.

Thanks to Tom Judson for material used in this chapter.

4.1 The origin of complex numbers

4.1.1 A number that can't be real (and we can prove it!)

Way back in your first algebra class, you saw equations like:

- $x^2 = 4$
- $x^2 = 36$
- $x^2 = 7$

You also learned how to solve them either by hand, or using the `SQRT` button on a simple calculator. The solutions to these equations are

- $x = \pm 2$
- $x = \pm 6$
- $x = \pm 2.64575131106459\dots$

But what about equations like:

$$x^2 = -1$$

Your simple calculator can't help you with that one!¹ If you try to take the square root of -1, the calculator will choke out `ERR` OR or some similar message of distress. But why does it do this? Doesn't -1 have a square root?

In fact, we can prove mathematically that -1 does not have a *real* square root. As proofs will play a very important part in this course, we'll spend some extra time and care explaining this first proof.

Proposition 4.1.1. -1 has no real square root.

PROOF. We give two proofs of this proposition. The first one explains all the details, while the second proof is more streamlined. It is the streamlined proof that you should try to imitate when you write up proofs for homework exercises.

Long drawn-out proof of Proposition 4.1.1 with all the gory details:

We will use a common proof technique called *proof by contradiction*. Here's how it goes:

First we *suppose* that there exists a real number a such that $a^2 = -1$. Now we know that any real number is either positive, or zero, or negative—there are no other possibilities. So we consider each of these three cases: $a > 0$, or $a = 0$, or $a < 0$.

- In the case that $a > 0$ then $a^2 = a \cdot a = (\textit{positive}) \cdot (\textit{positive}) =$ a positive number (that is, $a^2 > 0$). But this couldn't possibly be true, because we have already supposed that $a^2 = -1$: there's no way that $a^2 > 0$ and $a^2 = -1$ can both be true at the same time!

¹It's true that the fancier graphing calculators can handle it, but that's beside the point.

- In the case that $a = 0$, then $a^2 = a \cdot a = (0) \cdot (0) = 0$. But $a^2 = 0$ also contradicts our *supposition* that $a^2 = -1$.
- In the case that $a < 0$, then $a^2 = a \cdot a = (\text{negative}) \cdot (\text{negative}) =$ a positive number, so $a^2 > 0$. As in the first case, this contradicts our *supposition* that $a^2 = -1$.

So no matter which of the three possible cases is true, we're still screwed: in every case, we always have a contradiction. We seem to have reached a dead end – a logically impossible conclusion. So what's wrong?

What's wrong is the *supposition*. It must be the case that the supposition is not true. Consequently, the statement “there exists a real number a such that $a^2 = -1$ ” must be false. In other words, -1 has no real square root. This completes the proof. \square ²

The above proof is pretty wordy. Often the first draft of a proof can be pretty messy. So it's usually good to go back and rewrite the proof in such a way as to bring out the essential details. Here's our second crack at the above proof:

Streamlined proof of Proposition 4.1.1 (suitable for writing up homework exercises)

The proof is by contradiction. Suppose $\exists a \in \mathbb{R}$ such that $a^2 = -1$ (note the symbol “ \exists ” means “there exists,” the symbol \mathbb{R} denotes the real numbers, and the expression “ $a \in \mathbb{R}$ ” means that a is contained in \mathbb{R} , that is, a is a real number).

There are two cases: either (i) $a \geq 0$ or (ii) $a < 0$.

In Case (i), then $a^2 = a \cdot a = (\text{nonnegative}) \cdot (\text{nonnegative}) \geq 0$, which contradicts the supposition.

In Case (ii), then $a^2 = a \cdot a = (\text{negative}) \cdot (\text{negative}) > 0$, which contradicts the supposition.

By contradiction, it follows that -1 has no real square root. \square

You may note that in the streamlined case, we reduced the number of cases from three to two. That's because we noticed that we really could combine the “positive” and the “zero” case into a single case.

So far we've only considered square roots, but naturally we may ask the same questions about cube roots, fourth roots, and so on:

²The ' \square ' symbol will be used to indicate the end of a proof. In other words: Ta-da!

Exercise 4.1.2. Imitate the proof of Proposition 4.1.1 to prove that -2 has no real fourth root. \diamond

Exercise 4.1.3. Try to use the method of Proposition 4.1.1 to prove that -4 has no real cube root. At what step does the method fail? \diamond

Notice that the n th root of a is a solution of the equation $x^n - a = 0$ (and conversely—any solution of $x^n - a = 0$ is an n th root of a). Based on this observation, we may generalize the notion of “root”:

Definition 4.1.4. Given a function $f(x)$ which is defined on the real numbers and takes real values, then a **root** of $f(x)$ is any solution of the equation $f(x) = 0$. \triangle

Exercise 4.1.5.

- Sketch the function $f(x) = x^2 + 9$. Does the function have any real roots? Explain how you can use the graph to answer this question.
- Prove that the function $f(x) = x^2 + 9$ has no real roots. (You may prove by contradiction, as before).
- Graph the function $f(x) = x^6 + 7x^2 + 5$ (you may use a graphing calculator). Determine whether $f(x)$ has any real roots. *Prove* your answer (note: a picture is not a proof!).

\diamond

Exercise 4.1.5 underscores an important point. A graph can be a good visual aid, but it’s not a mathematical proof. We will often use pictures and graphs to clarify things, but in the end we’re only certain of what we can prove. After all, pictures can be misleading.

Exercise 4.1.6. ^{*3} Suppose that $a \cdot x^{2n} + b \cdot x^{2m} + a = 0$ has a real root, where a, b, m, n are nonzero integers. What can you conclude about the signs of a and b ? *Prove* your answer. \diamond

³Asterisks (*) indicate problems that are more difficult. Take the challenge!

4.1.2 Unreal, but unavoidable

Mathematicians have known Proposition 4.1.1 for thousands of years, and for a long time that settled the question. Unfortunately, that nasty $\sqrt{-1}$ kept popping up in all sorts of inconvenient places. For example, about 400 years ago, it was very fashionable to study the roots of cubic polynomials such as $x^3 - 15x - 4 = 0$. A mathematician named Bombelli came up with a formula for a solution that eventually simplified to: $x = (2 + \sqrt{-1}) + (2 - \sqrt{-1})$. By canceling out the $\sqrt{-1}$ terms, he got the correct solution $x = 4$. But how can you cancel something that doesn't exist?

Since mathematicians couldn't completely avoid those embarrassing $\sqrt{-1}$'s, they decided to put up with them as best they could. They called $\sqrt{-1}$ an *imaginary* number, just to emphasize that it wasn't up to par with the *real* numbers. They also used the symbol i to represent $\sqrt{-1}$, to make it less conspicuous (and easier to write). Finally, they created a larger set of numbers that included both real and imaginary numbers, called the *complex numbers*.⁴

Definition 4.1.7. The *complex numbers* are defined as

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\},$$

where $i^2 = -1$. If $z = a + bi$, then a is the **real part** of z and b is the **imaginary part** of z . (Note that the imaginary part of a complex number is a *real number*. It is the coefficient of i in the expression $z = a + bi$.) \triangle

Examples of complex numbers include

- $1 + i$
- $5.387 - 6.432i$
- $\frac{1}{2} - \frac{\sqrt{3}}{2}i$
- $3i$ (equal to $0 + 3i$)
- 7.42 (equal to $7.42 + 0i$).
- 0 (equal to $0 + 0i$).

⁴The web site <http://math.fullerton.edu/mathews/n2003/ComplexNumberOrigin.html> gives more information about the origin of complex numbers.

Exercise 4.1.8.

- (a) Write down the complex number with real part 0 and imaginary part 7.
- (b) Write down a complex number whose real part is the negative of its imaginary part.
- (c) Write down a complex number that is also a real number.

◇

4.1.3 A mathematical revolution

The creation of complex numbers was a revolutionary event in the history of mathematics. Mathematicians were forced to recognize that their beloved “real” numbers just weren’t good enough to deal with the mathematical problems they were encountering. So they had to create a *new number system* (the complex numbers) with *new* symbols (i) and *new* arithmetic rules (like $i \cdot i = -1$).

In fact, this was not the first time that a controversial new number system was founded. The ancient Greeks thought that all numbers could be expressed as a ratio of integers $\frac{m}{n}$ — in other words, the Greeks thought all numbers were rational. It came as a huge shock when someone proved that some real numbers are *not* rational. We will presently give the original proof, but first we will need some properties of odd and even integers:

Exercise 4.1.9.

- (a) Fill in the blanks: The product of two odd integers is < 1 > , and the product of two even integers is < 2 > .
- (b) Use proof by contradiction to prove the following statement: If m is an integer and m^2 is even, then m is also even. (*Hint*)⁵
- (c) It is possible to make a more general statement than part (b). Use proof by contradiction to prove the following statement: If m is an integer d is a positive integer, and m^d is even, then m is also even. (*Hint*)

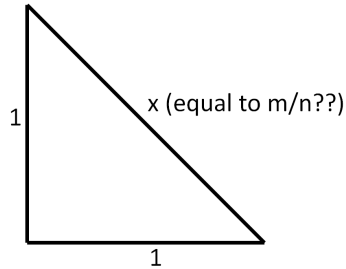


Figure 4.1.1. Isosceles right triangle

◇

Proposition 4.1.10. Given a right isosceles triangle where both legs have length 1 (see Figure 4.1.1). Let x be the length of the hypotenuse. Then x is irrational—that is, it cannot be expressed as a ratio of integers.

PROOF. The proof is by contradiction. *Suppose* that x is rational: that is, $x = \frac{m}{n}$ for some integers m and n . We can always reduce a fraction to lowest terms (as noted in Section 3.2.3), so we can assume m and n have no common factors.

Since x is the hypotenuse of a right triangle, the Pythagorean Theorem gives us $x^2 = 1^2 + 1^2 = 2$. We can plug $x = \frac{m}{n}$ into $x^2 = 2$ to get $(\frac{m}{n})^2 = 2$, which can be rearranged to give

$$m^2 = 2n^2.$$

From this we see that m^2 is divisible by 2, which means that m^2 is even. Exercise 4.1.9 part (b) then tells us that m is even, so there must be an integer j such that $m = 2j$. Plugging $m = 2j$ into $m^2 = 2n^2$ gives $4j^2 = 2n^2$, which simplifies to $2j^2 = n^2$. Hence n^2 is even, and as before we conclude that n is even. So $n = 2k$ for some integer k .

At this point, we have $m = 2j$ and $n = 2k$, which means that m and n have a common factor of 2. But at the beginning of the proof, we said that m and n were reduced to lowest terms, so they have no common factor. This is a contradiction. Therefore our *supposition* must be false, so x cannot be rational. □

⁵All *Hints* can be found at the end of the book (or by clicking on the *Hints* link.)

We have seen in our proofs that whenever we make a statement, we also need to give a reason that justifies the statement. In many cases, it's possible to state a proof very succinctly in “statement–reason” format. For instance, here is a “statement–reason” proof of Proposition 4.1.10:

| Statement | Reason |
|---|---|
| x is the hypotenuse of the right triangle in Figure 4.1.1 | Given |
| x is rational | <i>supposition</i> (will be contradicted) |
| $x^2 = 2$ | Pythagorean Theorem |
| $x = m/n$ where m, n are integers | Definition of rational |
| m, n have no common factors | Fraction can always be reduced |
| $(m/n)^2 = 2$ | Substitution |
| $m^2 = 2n^2$ | Rearrangement |
| $m = 2k$ where k is an integer | Exercise 4.1.9 part (b) |
| $(2k/n)^2 = 2$ | Substitution |
| $n^2 = 2k^2$ | Rearrangement |
| $n = 2j$ where j is an integer | Exercise 4.1.9 part (b) |
| m and n have a common factor | 2 is a factor of both |
| <i>supposition</i> is false | Contradictory statements |
| x cannot be rational | Negation of <i>supposition</i> |

Note that the preceding proof amounts to a proof that $\sqrt{2}$ is irrational, since we know that $\sqrt{2}$ is the length of the hypotenuse in question. Given the results of Exercise 4.1.9, we can use a similar proof to find more irrational numbers.

Exercise 4.1.11.

- (a) Prove that the cube root of 2 is irrational. (*Hint*)
- (b) Prove that the n th root of 2 is irrational, if n is a positive integer greater than 1.
- (c) Prove that $2^{1/n}$ is irrational, if n is a negative integer less than -1.

◇

In the proof of Proposition 4.1.10, we “plugged in” or substituted one expression for another. For example, when we discovered that m was divisible by 2 we substituted $2j$ for m , which was useful for the algebra that

followed. *Substitution* is a key technique used throughout all of abstract algebra.

Exercise 4.1.12. Use substitution to prove the following statement: if $3|n$ and $4|m$, then $12|mn$ (the notation “ $3|n$ ” means that 3 divides n). (*Hint*)
◇

Exercise 4.1.13. Use substitution to prove the following statement: if $12|n$ and $n|4m$, where n and m are integers, then $3|m$. (*Hint*) ◇

We should also come clean and admit that our proof of Proposition 4.1.10 falls short of true mathematical rigor. The reason is that we made use of Exercise 4.1.9, and we never actually proved part (a) of the exercise. Even though it’s something that “everybody knows”, mathematicians still want a proof! Now, part (a) is a consequence of a more general proposition known as *Euclid’s Lemma*:. Before giving this lemma, let’s be precise about what we mean by “prime number”:

Definition 4.1.14. A *prime number* is a natural number (i.e. positive integer) bigger than 1 that only has one factor bigger than 1, namely itself.
△

Now we are ready to state Euclid’s lemma:

Proposition 4.1.15. Let a and b be integers, and let p be a prime number. If p divides ab , then either p divides a , or p divides b .

Remark 4.1.16. In mathematics, when we say “either X is true or Y is true”, we also include the possibility that both X and Y are true. So in this case, when we say “ p divides a , or p divides b ”, it’s possible that p divides both a and b . △

PROOF. We’re not ready to give a proof yet, but we’ll give one later (see Exercise 5.5.23 in Section 5.5.4). □

Exercise 4.1.17. Modify the proof of Proposition 4.1.10 to prove that $\sqrt{3}$ is irrational. (You will find Proposition 4.1.15 to be useful in the proof.) ◇

Exercise 4.1.18. Prove that $\sqrt{6}$ is irrational. ◇

Exercise 4.1.19. Prove that $p^{1/n}$ is irrational, if p is a prime and n is any integer with $|n| > 1$. \diamond

Exercise 4.1.20.

- (a) Suppose that a, b, c are integers and $(a/b)^2 = c$. Suppose further that a and b have no common factors except 1: that is, any integer $x > 1$ which divides b doesn't divide a . Prove by contradiction that $b = 1$.
- (b) Generalize part (a): Suppose that a, b, c are integers and $(a/b)^n = c$, where n is a positive integer. If a and b have no common factors, prove by contradiction that $b = 1$.
- (c) Use part (b) to prove the following: Let a and n be integers, both greater than 1. Let x be a real n th root of a . If x is not an integer, then x is irrational.

\diamond

The inconvenient truth expressed in Proposition 4.1.10 forced mathematicians to extend the 'real' numbers to include *irrational* as well as *rational* numbers. But complex numbers opened the floodgates by setting a precedent. New generations of mathematicians became so used to working with "unreal" numbers that they became accustomed to making up other number systems whenever it suited their purpose. Within a few centuries after the complex numbers, several new number systems were created. This eventually prompted mathematicians to study the properties of general numbers systems. The outcome of this is what is known today as abstract algebra!

To close this section, here's another exercise to practice using substitution:

Exercise 4.1.21.

- (a) Suppose that:
- a is a negative number;
 - n is a positive integer;
 - the equation $x^n = a$ has a real solution for the unknown x .

What can you conclude about n ? Make a clear statement and *prove* your statement. (**Hint**)

- (b) Replace the condition “ n is a positive integer” in part (a) with “ n is a negative integer.” Now what can you conclude about n ? Make a clear statement and *prove* your statement.

◇

Exercise 4.1.22. Do imaginary numbers “really” exist? Write two or three sentences to express your opinion.⁶ ◇

4.2 Arithmetic with complex numbers

4.2.1 Complex arithmetic

To add two complex numbers $z = a + bi$ and $w = c + di$, we just add the corresponding real and imaginary parts:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

Using this definition, we may prove directly that complex addition (like regular addition) is commutative.⁷

Proposition 4.2.1. Addition on complex numbers is commutative.

PROOF. We just need to show that for any two complex numbers z and w , it’s always true that $z + w = w + z$. Writing $z = a + bi$ and $w = c + di$ as above, the proof using statement-reason format runs as follows:

| Statement | Reason |
|-------------------------------|--------------------------------|
| $z + w = (a + bi) + (c + di)$ | substitution |
| $= (a + c) + (b + d)i$ | definition of complex addition |
| $= (c + a) + (d + b)i$ | real addition is commutative |
| $= (c + di) + (a + bi)$ | def. of complex addition |
| $= w + z.$ | substitution |

⁶There is no “right” answer to this question.

⁷It is important to realize that this *must* be proved and *can’t* just be assumed. Later on we will define operations that are *not* commutative.

□

Notice how we started in this proof with one side of the equality, and through a series of steps ended up with the other side. This is a good method to follow, when you're trying to prove two things are equal.

Exercise 4.2.2. Prove that addition on complex numbers is associative. ◇

Now that we have addition worked out, let's do multiplication. We observe that the complex number $a + bi$ looks just like the polynomial $a + bx$, except the imaginary i replaces the unknown x . So we'll take a cue from polynomial multiplication, and multiply complex numbers just like polynomial factors, using the FOIL (first, outside, inside, last) method. Better yet, with complex numbers it's more convenient to use FLOI (first, last, outside, inside) instead. The product of z and w is

$$(a + bi)(c + di) = ac + bdi^2 + adi + bci = (ac - bd) + (ad + bc)i.$$

Question: How did we get rid of the i^2 in the final equality? Answer: Remember, we defined $i^2 = -1$, and we just made the substitution.

A bevy of nice properties follow from this definition:

Example 4.2.3. Complex multiplication is commutative. This may be proved as follows. (Note that here we are combining statement-reason and paragraph proof formats. It's OK to mix and match formats, as long as you get the job done!)

$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i \quad (\text{FLOI})$$

On the other hand:

$$\begin{aligned} (c + di)(a + bi) &= (ca - db) + (cb + da)i && (\text{FLOI}) \\ &= (ac - bd) + (bc + ad)i && (\text{commutativity of real multiplication}) \end{aligned}$$

Since we obtain the same expression for $(a + bi)(c + di)$ and $(c + di)(a + bi)$, it follows that $(a + bi)(c + di) = (c + di)(a + bi)$. ◆

Similar proofs can be given for other multiplicative properties:

Exercise 4.2.4. Prove the associative law for multiplication of 'complex numbers. (Follow the style of Example 4.2.3). ◇

Exercise 4.2.5. Prove the distributive law for complex arithmetic: that is, if u, w , and z are complex numbers, then $(u)(w + z) = uw + uz$. \diamond

Two arithmetic operations down, two to go! Let's consider subtraction of complex numbers. We may define $z - w$ using complex addition and multiplication as: $z - w = z + (-1) \cdot w$.

Exercise 4.2.6. Given that $z = a + bi$ and $w = c + di$ use the above definition of subtraction to derive an expression for $z - w$ in terms of a, b, c, d . Express your answer as (Real part) + (Imaginary part) i . \diamond

Division is a little more complicated. First we consider division of a complex number by a real number. In this case we can define division as multiplication by the reciprocal, just as with real numbers:

$$\frac{a + bi}{c} = (a + bi) \cdot \frac{1}{c} = a \cdot \frac{1}{c} + (bi) \cdot \frac{1}{c} = \frac{a}{c} + \frac{b}{c}i,$$

where we have used the distributive, associative, and commutative properties of complex multiplication.

Now let's try to make sense of the ratio of two complex numbers:

$$\frac{w}{z} = \frac{c + di}{a + bi}.$$

This notation suggests that it should be true that

$$\frac{w}{z} = (c + di) \cdot \frac{1}{a + bi}.$$

But what is $1/(a + bi)$? To understand this, let's go back to arithmetic with real numbers. If we have an ordinary real number r , then $1/r$ is the *multiplicative inverse* of r : that is, $r \cdot 1/r = 1/r \cdot r = 1$. We also write $1/r$ as r^{-1} . By analogy, to make sense of $1/z = 1/(a + bi)$, we need to find a complex number z^{-1} such that $z^{-1} \cdot z = z \cdot z^{-1} = 1$.

Exercise 4.2.7. Given that $z = a + bi$ is a complex number and $z \neq 0$ (recall that 0 is the same as $0 + 0i$). Show that the complex number

$$w = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i.$$

satisfies $zw = wz = 1$, where $z = a + bi$. (***Hint***) \diamond

Based on the previous exercise, we are able to define z^{-1} for the complex number $z = a + bi$:

$$z^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i = \frac{a - bi}{a^2 + b^2},$$

where the second equality follows from the distributive law. We finally arrive at the formula for dividing two complex numbers:

$$\frac{c + di}{a + bi} = (c + di) \cdot \frac{a - bi}{a^2 + b^2},$$

or alternatively

$$\frac{c + di}{a + bi} = \frac{a - bi}{a^2 + b^2} \cdot (c + di).$$

(These formulas hold as long as $a + bi \neq 0$).

It seems obvious that we should be able to write this formula more compactly as

$$\frac{c + di}{a + bi} = \frac{(c + di)(a - bi)}{a^2 + b^2},$$

and in fact we can. This is because the distributive and associative laws once again come to our rescue. Starting with the first expression above for $(c + di)/(a + bi)$ we have:

$$\begin{aligned} \frac{c + di}{a + bi} &= (c + di) \cdot \frac{a - bi}{a^2 + b^2} && \text{(from above)} \\ &= (c + di) \cdot \left((a - bi) \cdot \frac{1}{a^2 + b^2} \right) && \text{(distributive law)} \\ &= ((c + di) \cdot (a - bi)) \cdot \frac{1}{a^2 + b^2} && \text{(associative law)} \\ &= \frac{(c + di) \cdot (a - bi)}{a^2 + b^2} && \text{(definition of division).} \end{aligned}$$

We summarize the formulas for complex addition, multiplication, and division below:

- Addition: $(a + bi) + (c + di) = (a + c) + (b + d)i$
- Multiplication: $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
- Division: $\frac{c + di}{a + bi} = \frac{(c + di)(a - bi)}{a^2 + b^2}$

Exercise 4.2.8. Evaluate each of the following.

- (a) $(3 - 2i) + (5i - 6)$ (k) $\frac{a + bi}{b - ai}$
- (b) $(5 - 4i)(7 + 2i)$ (l) $\frac{1 + i}{1 - i} + \frac{1 - i}{1 + i}$
- (c) $(\sqrt{7} + \sqrt{6}i)(\sqrt{7} - \sqrt{6}i)$ (m) $\frac{\sqrt{3} - \sqrt{5}i}{\sqrt{5} + \sqrt{3}i}$
- (d) $(a - bi)(a + bi)$ (n) i^{45} (*Hint*)
- (e) $(a + bi)(b + ai)$ (o) $(1 + i)^4$ (*Hint*)
- (f) $(2 + \sqrt{3}i)^2$ (p) $(1 + i)^{41}$
- (g) $(1 + i)(-1 + i)(-1 - i)(1 - i)$ (q) $(1 + \sqrt{3}i)^{11}$
- (h) $(\sqrt{3} + i)(-1 + \sqrt{3}i)(-\sqrt{3} - i)(1 - \sqrt{3}i)$ (r) $i^{1001} + i^{1003}$
- (i) $\left(\sqrt{5 + \sqrt{5}} + i\sqrt{5 - \sqrt{5}}\right)^4$ (*Hint*) (s) $\left(\frac{i}{3+4i}\right) + \left(\frac{2}{4+3i}\right)$
- (j) $\frac{1 + 2i}{2 - 3i}$

◇

Exercise 4.2.9. If the nonzero complex number z has equal real and imaginary parts, then what can you conclude about z^2 ? What can you conclude about z^4 ? (*Hint*) ◇

Exercise 4.2.10. $z = 3 + i$ is a solution to $z^2 - 6z + k = 0$. What is the value of k ? ◇

You are probably familiar with the fact that the product of two nonzero real numbers is also nonzero. Is the same true for complex numbers? The answer is yes.

Proposition 4.2.11. Given that $z = a + bi$, $w = c + di$, and $z \cdot w = 0$. Then it must be true that either $z = 0$ or $w = 0$.

The proof of Proposition 4.2.11 is outlined in the following exercise.

Exercise 4.2.12. Complete the proof of Proposition 4.2.11 by filling in the blanks. Note that some blanks may require an expression, and not just a single number or variable.

- (a) The proof is by contradiction. So we begin by *supposing* that $z \neq \underline{\langle 1 \rangle}$ and $w \neq \underline{\langle 2 \rangle}$ (which is the negation of what we're trying to prove).
- (b) Since $z \neq \underline{\langle 3 \rangle}$, it follows that z has an inverse z^{-1} such that $z^{-1} \cdot z = \underline{\langle 4 \rangle}$.
- (c) Since $z \cdot w = 0$, we can multiply both sides of this equation by $\underline{\langle 5 \rangle}$ and obtain the equation $w = \underline{\langle 6 \rangle}$. This equation contradicts the *supposition* that $\underline{\langle 7 \rangle}$.
- (d) Since our supposition has led to a false conclusion, it follows that our supposition must be $\underline{\langle 8 \rangle}$. Therefore it cannot be true that $\underline{\langle 9 \rangle}$, so it must be true that $\underline{\langle 10 \rangle}$.

◇

4.2.2 Comparison of integer, rational, real and complex addition properties

It is obvious that addition with integers, rational numbers, and real numbers have very similar properties. In this section, we explore some of these properties.

For instance, integers have an ***additive identity***, that is, one special unique integer that can be added to any integer without changing that integer. The additive identity of the integers is 0, because for instance $5 + 0 = 5$ and $0 + 5 = 5$. In general, if we let n be an arbitrary integer, then $n + 0 = 0 + n = n$. It's pretty easy to see that 0 is also the additive identity of the rationals, and the additive identity of the reals.

Every integer also has an ***additive inverse***, that is a corresponding number that can be added to the integer such that the sum is the additive identity (that is, 0). For example, the additive inverse of the number 5 is -5 , because $5 + (-5) = 0$ and $(-5) + 5 = 0$. In general, if we let n be an arbitrary integer, then $n + (-n) = (-n) + n = 0$.

Notice an *important difference* between additive identity and additive inverse: the number 0 is the identity for all integers, but each integer has a *different* inverse.

| | Integers (n, m, k) | Rationals ($\frac{n}{m}, \frac{p}{q}, \frac{j}{k}$) | Reals (x, y, z) | Complex ($a + bi, c + di, e + fi$) |
|-------------------|-----------------------------|--|------------------------|--------------------------------------|
| Additive identity | $n + 0 = 0 + n = n$ | $\frac{n}{m} + 0 = 0 + \frac{n}{m} = \frac{n}{m}$ | $x + 0 = 0 + x = x$ | $(a + bi) + \dots = \dots$ |
| Additive inverse | $n + (-n) = (-n) + n = 0$ | $\frac{n}{m} + \dots = \dots$ | \dots | \dots |
| Associative law | $n + (m + k) = (n + m) + k$ | $\frac{n}{m} + (\frac{p}{q} + \frac{j}{k}) = \dots$ | \dots | \dots |
| Commutative law | $n + m = m + n$ | \dots | \dots | \dots |

Table 4.1: Additive properties of different number systems

Exercise 4.2.13. Complete all entries of Table 4.1, which shows the additive properties of integers, rationals, reals, and complex numbers.

◇

4.2.3 Comparison of integer, rational, real and complex multiplication properties

Just as we've talked about the *additive* identity and inverse for different number systems, in the same way we can talk about the *multiplicative* identity and inverse for different number systems.

The integers have multiplicative identity 1 because $n \cdot 1 = 1 \cdot n = n$. However, most integers do *not* have a multiplicative inverse. Take the number 5, for example. There is no *integer* that can be multiplied by 5 to give 1 (of course, $5 \cdot \frac{1}{5} = \frac{1}{5} \cdot 5 = 1$, but $\frac{1}{5}$ is not an integer, so it doesn't count).

On the other hand, the real numbers do have multiplicative inverses, with just one exception.

Exercise 4.2.14. Which real number does not have a multiplicative inverse? *Explain* your answer. ◇

Exercise 4.2.15. Complete all entries of Table 4.2, which shows the multiplicative properties of *nonzero* rationals, reals, and complex numbers.

| | Rationals $(\frac{n}{m}, \frac{p}{q}, \frac{j}{k})$ | Reals (x, y, z) | Complex $(a + bi,$ $c + di, e + fi)$ |
|-------------------------|--|---|---|
| Multiplicative identity | ... | $x \cdot 1 = 1 \cdot x = x$ | $(a + bi) \cdot \dots = \dots$ |
| Multiplicative inverse | ... | $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$ if $x \neq 0$ | ... |
| Associative law | ... | $x(yz) = (xy)z$ | ... |
| Commutative law | ... | $xy = yx$ | ... |

Table 4.2: Multiplicative properties of different number systems

◇

Exercise 4.2.16. Prove FOIL for complex numbers: that is, if $u, v, w,$ and z are complex numbers, then $(u + v)(w + z) = uw + uz + vw + vz.$ ◇

Tables 4.1-4.2 show that complex numbers also follow the same fundamental algebraic rules that real numbers do. This makes life a lot simpler! From now on, in our proofs we may freely apply these properties to complex numbers, just like with real numbers. But it's important to realize that we had to go through the process first of establishing the properties specifically for complex numbers, because there are number systems in which these basic properties do not hold—be forewarned!

4.2.4 Modulus and complex conjugate

We are familiar with the absolute value of a real number: for instance, $|\sqrt{7}| = \sqrt{7}.$ In general, for a real number x the absolute value can be defined as $|x| \equiv \sqrt{x^2}.$ (Here and elsewhere, the square root symbol is used to denote the *positive* square root.)

Definition 4.2.17. For a complex number $z,$ the *absolute value* or *modulus* of $z = a + bi$ is $|z| = \sqrt{a^2 + b^2}.$ △

Complex numbers have an additional operation that real numbers do not have.

Definition 4.2.18. The *complex conjugate* of a complex number $z = a + bi$ is defined to be $\bar{z} = a - bi$. \triangle

Example 4.2.19. Let $z = 2 + 3i$ and $w = 1 - 2i$. Then

$$\bar{z} = \overline{2 + 3i} = 2 - 3i \text{ and } \bar{w} = \overline{1 - 2i} = 1 + 2i.$$

Notice also that

$$z + w = (2 + 3i) + (1 - 2i) = 3 + i \text{ and } zw = (2 + 3i)(1 - 2i) = 8 - i,$$

so that

$$\overline{z + w} = 3 - i \text{ and } \overline{zw} = 8 + i.$$

On the other hand, you may check that

$$\bar{z} + \bar{w} = (2 - 3i) + (1 + 2i) = 3 - i \text{ and } \bar{z}\bar{w} = (2 - 3i)(1 + 2i) = 8 + i.$$

What a “coincidence”!

Another remarkable “coincidence” occurs when we multiply complex numbers by their complex conjugates:

$$z \cdot \bar{z} = (2 + 3i)(2 - 3i) = 13 \text{ and } w \cdot \bar{w} = (1 - 2i)(1 + 2i) = 5,$$

while on the other hand, we may compute the moduli of z and w as

$$|z| = \sqrt{2^2 + 3^2} = \sqrt{13} \text{ and } |w| = \sqrt{1^2 + 2^2} = \sqrt{5}.$$

◆

Exercise 4.2.20. Evaluate each of the following.

(a) \bar{i}

(f) $(\overline{\sqrt{3} - i})^{-1}$

(b) $(4 - 5i) - \overline{(4i - 4)}$

(g) $\overline{(\sqrt{3} - i)^{-1}}$

(c) $(9 - i)\overline{(9 - i)}$

(h) $\overline{\left(\overline{(4 - 9i)^{-1}}\right)^{-1}}$

(d) $(3 + 4i) + \overline{(3 + 4i)}$

(e) $(\sqrt{7} + 8i) - \overline{(\sqrt{7} + 8i)}$

(i) $(a + bi)\overline{(a + bi)}$

- (j) $(a + bi) + \overline{(a + bi)}$ (l) $(4 - 7i) \cdot (\overline{3 + 3i})^{-1}$
 (k) $\frac{\overline{3+8i}}{7+6i}$.

◇

In order to use the complex conjugate and modulus operations effectively, we need to know how they interact with the arithmetic operations of addition, multiplication, subtraction, and division. In the following, we prove several propositions that establish important properties of these two operations.

Proposition 4.2.21. Given z and w are complex numbers, then $\overline{z + w} = \overline{z} + \overline{w}$.

PROOF. We may write z as $a + bi$ and w as $c + di$. Then

$$\begin{aligned} \overline{z + w} &= \overline{a + bi + c + di} \\ &= (a - bi) + (c - di) && \text{by definition of conjugate} \\ &= (a + c) - (b + d)i && \text{commutative, associative} \\ &= \overline{(a + c) + (b + d)i} && \text{by definition of conjugate} \\ &= \overline{z + w} && \text{by definition of complex addition} \end{aligned}$$

□

Exercise 4.2.22. Prove each of the following propositions (follow the style of Proposition 4.2.21).

- (a) $\overline{\overline{z}} = z$ (g) $|z|^3 = |z^3|$ (*Hint*)
 (b) $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$ (h) $z^{-1} = \frac{\overline{z}}{|z|^2}$ (*Hint*)
 (c) If a is real, then $a\overline{z} = \overline{az}$ (i) $|z^{-1}| = \frac{1}{|z|}$ (*Hint*)
 (d) $|z| = |\overline{z}|$ (j) $(\overline{z})^{-1} = \overline{z^{-1}}$
 (e) $z\overline{z} = |z|^2$ (k) $(zw)^{-1} = w^{-1}z^{-1}$
 (f) $|zw| = |z||w|$

◇

Exercise 4.2.23. Simplify the following expression: $(z + i\bar{z})(z - i\bar{z}) + (z + \bar{z})(z - \bar{z})$. \diamond

Exercise 4.2.24. Suppose that z is a complex number such that $z^{-1} = \bar{z}$.

- (a) Find the modulus of z .
- (b) How many solutions does this equation have?

\diamond

Exercise 4.2.25.

- (a) Show that the complex number $z = a + bi$ is a pure real number if and only if $\bar{z} = z$. (Note that you actually need to prove two things here: (i) If z is real, then $\bar{z} = z$; (ii) If $\bar{z} = z$, then z is real).
- (b) Prove that $i(z + \bar{z})(z - \bar{z})$ is real for any complex number z .
- (c) In view of part (a), complete the following statement: “The complex number $z = a + bi$ is a pure imaginary number if and only if $\bar{z} = \dots\dots$ ” Prove your statement.

\diamond

Now that we have proved properties of complex numbers in the previous two exercises, we may make use of these properties to prove facts about complex numbers without having to write everything out as $a + bi$.

Exercise 4.2.26.

- (a) Prove that If $|z| = 1$ and z is not a real number, then $\frac{z-1}{z+1}$ is a pure imaginary number. (***Hint***)
- (b) Prove that If $|z| = 1$ and z is not a pure imaginary number (i.e. z is not of the form $0 = bi$), then $\frac{z-i}{z+i}$ is a pure imaginary number.

\diamond

Exercise 4.2.27.

- (a) *Use appropriate properties from Exercise 4.2.22 to prove the following: for any nonzero complex number z , the absolute value of $z + \bar{z}^{-1}$ is greater than $\sqrt{3}$. (*Hint*)
- (b) Give an example of z such that $|z + \bar{z}^{-1}| = 2$.
- (c) Give four additional examples of z such that $|z + \bar{z}^{-1}| = 2$.
- (d) **Show that for any nonzero complex number z , $|z + \bar{z}^{-1}| \geq 2$. (*Hint*)
- (e) Show by example that part (d) is *not* true if $z + \bar{z}^{-1}$ is replaced with $z + z^{-1}$. Find the smallest possible value for $|z + z^{-1}|$.

◇

4.3 Alternative representations of complex numbers

4.3.1 Cartesian representation of complex numbers

There are several ways to represent complex numbers, that have different conceptual advantages. For instance, a complex number $z = a + bi$ can be considered simply as a pair of real numbers (a, b) , where the first number is the real part and the second number is the imaginary part. We are used to plotting ordered pairs (a, b) on an xy plane, where a is the x coordinate and b is the y coordinate. Representing a complex number in this way as an ordered pair (a, b) is called the *rectangular* or *Cartesian* representation. The rectangular representations of $z_1 = 2 + 3i$, $z_2 = 1 - 2i$, and $z_3 = -3 + 2i$ are depicted in Figure 4.3.1.

Often the notation $a + bi$ is also referred to as “rectangular representation”, since it’s so similar to (a, b) . In the following, we will refer to $a + bi$ as the “rectangular form” of the complex number z .

Mathematicians naturally think of complex numbers as points on a plane – in fact, the complex numbers are often referred to as the “complex plane”.

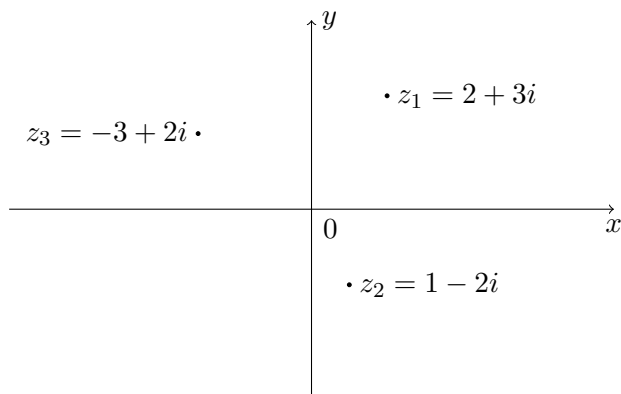


Figure 4.3.1. Rectangular coordinates of a complex number

4.3.2 Vector representation of complex numbers

You should already know that a point in a plane can also be considered as a *vector*: in other words, the ordered pair (a, b) can be identified with the vector $a\mathbf{i} + b\mathbf{j}$, where \mathbf{i} and \mathbf{j} are the unit vectors in the $x+$ and $y+$ directions, respectively. So complex numbers can also be considered as two-dimensional vectors.

Exercise 4.3.1.

- Write the numbers $3 + 7i$ and $-5 + 9i$ as vectors.
- Find the sum of the two vectors that you found in (a).
- Find the sum $(3 + 7i) + (-5 + 9i)$
- What is the relation between your answers to (b) and (c)? Explain.

◇

Although the preceding exercise may seem sort of pointless, in fact it is extremely significant. This is our first example of an *isomorphism*: a correspondence between mathematical systems that are essentially identical. At this point we will not give a formal definition of isomorphism, but to get the gist of the idea consider two mathematicians (Stan and Ollie) with very different tastes. Stan thinks geometrically, so he always thinks of complex

numbers as vectors in a plane; while Ollie thinks algebraically, so he writes complex numbers as $a + bi$. If Stan and Ollie work on the same problem involving complex addition, even though Stan's answer will be a vector and Ollie's will look like $a + bi$, their answers will always agree (that is, if they both do the problem right).

Of course this correspondence between complex numbers and vectors breaks down when we consider multiplication, because we have never seen multiplication of 2-D vectors before. But it works perfectly well if we stick with addition.

4.3.3 Polar representation of complex numbers

Nonzero complex numbers can also be represented using *polar coordinates*. To specify any nonzero point on the plane, it suffices to give an angle θ from the positive x axis in the counterclockwise direction and a distance r from the origin, as in Figure 4.3.2. The distance r is the absolute value or modulus defined previously, while the angle θ is called the *argument* of the complex number z .

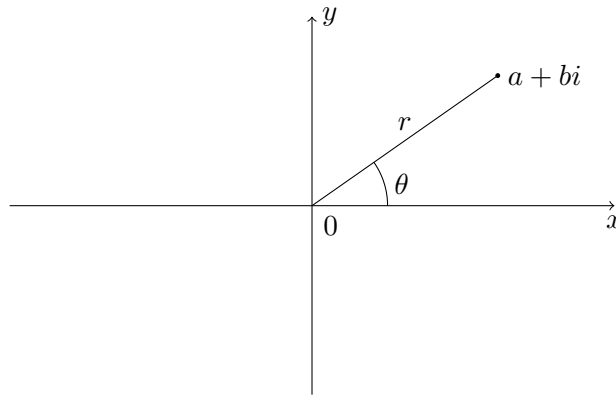


Figure 4.3.2. Polar coordinates of a complex number

4.3.4 Converting between rectangular and polar form

We can see from the Figure 4.3.2 that

$$z = a + bi = r \cos \theta + (r \sin \theta)i,$$

where

$$\begin{aligned} r &= |z| = \sqrt{a^2 + b^2} \\ a &= r \cos \theta \\ b &= r \sin \theta. \end{aligned}$$

We will frequently use the abbreviation ‘cis’, which stands for “cosine plus i sine”:

$$\text{cis } \theta := \cos \theta + i \sin \theta.$$

(In this expression, the notation “:=” means “is defined as”. Note that we’re writing ‘ $i \sin \theta$ ’ instead of $(\sin \theta)i$, because then we don’t need a parenthesis.) Multiplying both sides by r gives

$$r \text{cis } \theta = r(\cos \theta + i \sin \theta)$$

We know from trigonometry that adding 2π to θ does not change $\cos \theta$ or $\sin \theta$. This means for example that the following complex numbers are equal: $2.6 \text{cis } (\frac{\pi}{9})$, $2.6 \text{cis } (2\pi + \frac{\pi}{9})$, $2.6 \text{cis } (-2\pi + \frac{\pi}{9})$, \dots . However, we can always find a θ between 0 and 2π such that $z = r \text{cis } \theta$; so the standard representation of $z = r \text{cis } \theta$ has $0 \leq \theta < 2\pi$.

Example 4.3.2. Let $z = 2 \text{cis } \frac{\pi}{3}$. Then

$$a = 2 \cos \frac{\pi}{3} = 1$$

and

$$b = 2 \sin \frac{\pi}{3} = \sqrt{3}.$$

Hence, the rectangular representation is $z = 1 + \sqrt{3}i$. 

Conversely, if we are given a rectangular representation of a complex number, it is often useful to know the number’s polar representation.

Example 4.3.3. Let $z = 3\sqrt{2} - 3\sqrt{2}i$ (see Figure 4.3.3). Then the modulus of z is

$$r = \sqrt{a^2 + b^2} = \sqrt{36} = 6.$$

We can find the argument θ by noticing that the tangent is equal to $\frac{-3\sqrt{2}}{3\sqrt{2}}$ or -1 . This means that $\theta = \arctan(-1)$. Since the angle is in the fourth quadrant, this means that $\theta = \frac{7\pi}{4}$.

In general, for the complex number $a + bi$ we have

$$\theta = \arctan\left(\frac{b}{a}\right),$$

where we must be careful to choose the value of θ corresponding to the quadrant where $a + bi$ is located. The best way to make sure you've chosen the right θ is to *draw a picture* (like Figure 4.3.3). \blacklozenge

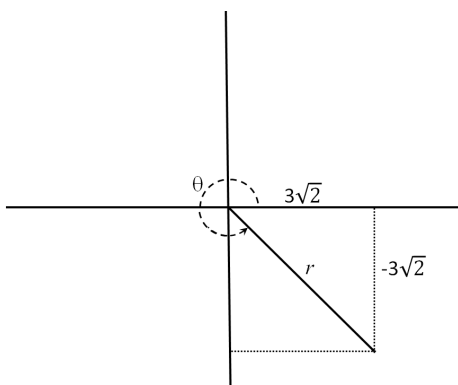


Figure 4.3.3. Modulus and argument of $z = 3\sqrt{2} - 3\sqrt{2}i$

Exercise 4.3.4. Convert the following complex numbers to rectangular form (that is, write as $a + bi$). Give *exact* answers and not decimals (use square roots if necessary).

- | | |
|--|--|
| (a) $2 \operatorname{cis}(\pi/6)$ | (e) $\sqrt{2} \operatorname{cis}(5\pi/3)$ |
| (b) $5 \operatorname{cis}(9\pi/4)$ | (f) $\frac{1}{\sqrt{7}} \operatorname{cis}(-7\pi/6)$ |
| (c) $3 \operatorname{cis}(\pi)$ | (g) $14 \operatorname{cis}(30\pi/12)$ |
| (d) $\frac{\operatorname{cis}(7\pi/4)}{2}$ | |

\blacklozenge

Exercise 4.3.5. Convert the following complex numbers to polar representation (Give exact answers, no decimal approximations).

- | | | |
|--------------|----------------------|-------------------------------|
| (a) $1 - i$ | (e) $-2 - 2i$ | (i) $\sqrt{6} - \sqrt{6}i$ |
| (b) $-1 + i$ | (f) $\sqrt{3} + i$ | (j) $-3\sqrt{2} - \sqrt{6}i$ |
| (c) -5 | (g) $-3i$ | |
| (d) $2 + 2i$ | (h) $2i + 2\sqrt{3}$ | (k) $-\sqrt{50} - \sqrt{50}i$ |

◇

Pictures are essential for gaining an intuitive grasp of how complex numbers work. They're also a lot more fun to draw than mathematical symbols.

Exercise 4.3.6.

- (a) Figure 4.3.2 shows polar and Cartesian representations of a complex number z in the complex plane. Redraw the figure, and put \bar{z} in the picture as well. Show the Cartesian coordinates of \bar{z} , as well as the modulus and the complex argument (angle).
- (b) Use your picture to obtain the polar representation of \bar{z} in terms of the modulus and complex argument of z .

◇

The close interrelationship between plane geometry and complex numbers is a rich source of mathematical insight. The following exercise explores some aspects of this relationship.

Exercise 4.3.7.

- (a) Consider the following set of complex numbers:

$$\{z \text{ such that } |z| < 2.\}$$

In the complex plane, what does this set look like? Draw a picture, and describe verbally.

- (b) Use complex numbers to specify the set of all points on a circle of radius 5 with center at the origin (your answer should look like the set specification given in part (a)).

(c) Consider the following set of complex numbers:

$$\{z \text{ such that } |z - i| = 2.\}$$

In the complex plane, what does this set look like? Draw a picture, and describe verbally.

(d) Describe the following as a set of complex numbers: the set of all points on a circle of radius 3 that passes through the origin and has center on the positive x -axis.

◇

4.3.5 Multiplication and powers in complex polar form

The polar representation of a complex number makes it easy to find products, quotients, and powers of complex numbers.

Proposition 4.3.8. Let $z = r \operatorname{cis} \theta$ and $w = s \operatorname{cis} \phi$ be two nonzero complex numbers. Then

$$z \cdot w = rs \operatorname{cis}(\theta + \phi).$$

Alternatively, we may write

$$r \operatorname{cis} \theta \cdot s \operatorname{cis} \phi = rs \operatorname{cis}(\theta + \phi).$$

PROOF. The proof uses the following trigonometric formulas (surely you remember them!):

$$\begin{aligned} \cos(\theta + \phi) &= \cos \theta \cos \phi - \sin \theta \sin \phi \\ \sin(\theta + \phi) &= \cos \theta \cdot \sin \phi + \sin \theta \cdot \cos \phi \end{aligned}$$

Exercise 4.3.9. Fill in the blanks to complete the proof:

$$\begin{aligned}
z \cdot w &= r \operatorname{cis} \theta \cdot \underline{\langle 1 \rangle} \\
&= r (\cos \theta + i \sin(\underline{\langle 2 \rangle})) \cdot s(\underline{\langle 3 \rangle}) \\
&= rs \cdot (\cos \theta + i \sin(\underline{\langle 4 \rangle})) \cdot (\underline{\langle 5 \rangle}) \\
&= rs ((\cos \theta \cos \phi - \sin \theta \sin \phi) + i(\underline{\langle 6 \rangle})) \\
&= rs (\cos(\theta + \phi) + i \sin(\underline{\langle 7 \rangle})) \\
&= rs \operatorname{cis}(\underline{\langle 8 \rangle})
\end{aligned}$$

◇

□

Exercise 4.3.10. Use Proposition 4.3.8 and the polar expression for \bar{z} that was given in Section 4.3.4 to give a simple proof of the following identity:

$$z\bar{z} = |z|^2.$$

◇

We will also want to divide complex numbers in polar form. But first, we need to characterize multiplicative inverses. Note for example that $[2 \operatorname{cis}(3\pi/4)]^{-1} = (1/2) \operatorname{cis}(-3\pi/4)$ since

$$2 \operatorname{cis}(3\pi/4) \cdot (1/2) \operatorname{cis}(-3\pi/4) = 2 \cdot (1/2) \cdot \operatorname{cis}(3\pi/4 - 3\pi/4) = \operatorname{cis}(0) = 1,$$

and similarly

$$(1/2) \operatorname{cis}(-3\pi/4) \cdot 2 \operatorname{cis}(3\pi/4) = \operatorname{cis}(0) = 1.$$

Exercise 4.3.11.

- (a) Let $z = 13 \operatorname{cis}(\frac{5\pi}{7})$. Find a complex number w (in complex polar form) such that $zw = wz = 1$. Write w so that its argument is between 0 and 2π . What is the sum of the arguments of z and w ?
- (b) Let $z = \frac{3}{8} \operatorname{cis}(0.39\pi)$. Find a complex number w (in complex polar form) such that $zw = wz = 1$. Write w so that its argument is between 0 and 2π . What is the sum of the arguments of z and w ?

- (c) Given that $z = r \operatorname{cis} \theta$ and $w = s \operatorname{cis} \phi$. Determine what s and ϕ must be so that $w = z^{-1}$. That is, find values for s and ϕ (in terms of r and θ) so that

$$z \cdot s \operatorname{cis} \phi = s \operatorname{cis} \phi \cdot z = 1.$$

Specify ϕ in such a way that it lies in the interval $[0, 2\pi]$.

◇

From Exercise 4.3.11 we may deduce that the inverse of a complex number $w = s \operatorname{cis} \phi$ is

$$w^{-1} = \frac{1}{s} \operatorname{cis}(2\pi - \phi),$$

which we could also write as

$$w^{-1} = \frac{1}{s} \operatorname{cis}(-\phi)$$

since changing the argument by 2π does not change the value of the number.

Now recall that to divide two complex numbers z and w , we rewrite $\frac{z}{w}$ as $z \cdot w^{-1}$. So with $z = r \operatorname{cis} \theta$ and $w = s \operatorname{cis} \phi$ we may divide as follows:

$$\frac{z}{w} = (r \operatorname{cis} \theta) \cdot \left(\frac{1}{s} \operatorname{cis}(-\phi)\right) = \frac{r}{s} \operatorname{cis}(\theta - \phi).$$

The previous discussion proves the following proposition.

Proposition 4.3.12. Let $z = r \operatorname{cis} \theta$ and $w = s \operatorname{cis} \phi$ be two nonzero complex numbers. Then

$$\frac{z}{w} = \frac{r}{s} \operatorname{cis}(\theta - \phi).$$

Alternatively, we may write

$$\frac{r \operatorname{cis} \theta}{s \operatorname{cis} \phi} = \frac{r}{s} \operatorname{cis}(\theta - \phi).$$

In summary, multiplication and division of complex numbers in polar form proceeds as follows:

Multiplication:

- Multiply the two moduli together to get the modulus of the product.

- Add the two arguments together to get the argument of the product.

Division:

- Divide the modulus of the numerator by the modulus of the denominator to get the modulus of the quotient.
- Subtract the argument of the denominator from the argument of the numerator to get the argument of the quotient.

Example 4.3.13. If $z = 3 \operatorname{cis}(\pi/3)$ and $w = 2 \operatorname{cis}(\pi/6)$, then

$$zw = (2 \cdot 3) \operatorname{cis}(\pi/3 + \pi/6) = 6 \operatorname{cis}(\pi/2) = 6i.$$



Exercise 4.3.14. Calculate each of the following products using complex polar arithmetic. Give the answer in rectangular form if you can do so without using roots or decimals. Otherwise, leave the answer in polar form.

- (a) $2 \operatorname{cis}\left(\frac{\pi}{4}\right) \cdot \frac{1}{2} \operatorname{cis}\left(\frac{3\pi}{4}\right)$
 (b) $14 \operatorname{cis}\left(\frac{6\pi}{5}\right) \cdot \frac{1}{7} \operatorname{cis}\left(\frac{4\pi}{5}\right)$
 (c) $\operatorname{cis}\left(\frac{9\pi}{7}\right) \cdot 2 \operatorname{cis}\left(\frac{8\pi}{7}\right) \cdot 3 \operatorname{cis}\left(\frac{4\pi}{7}\right)$
 (d) $\sqrt{3} \operatorname{cis}\left(\frac{\pi}{12}\right) \cdot \sqrt{56} \operatorname{cis}\left(\frac{\pi}{15}\right) \cdot \sqrt{21} \operatorname{cis}\left(\frac{\pi}{15}\right)$
 (e) $\sqrt{5} \operatorname{cis}\left(\frac{\pi}{19}\right) \cdot 3^{1/3} \operatorname{cis}\left(\frac{\pi}{3}\right) \cdot 45^{1/3} \operatorname{cis}\left(\frac{-10\pi}{57}\right)$



Exercise 4.3.15. Calculate each of the following quotients using complex polar arithmetic. Give the answers in polar form.

- (a) $\frac{5 \operatorname{cis}\left(\frac{5\pi}{6}\right)}{2 \operatorname{cis}\left(\frac{\pi}{2}\right)}$ (b) $\frac{27 \operatorname{cis}\left(\frac{7\pi}{12}\right)}{6 \operatorname{cis}\left(\frac{5\pi}{3}\right)}$

$$(c) \frac{2\sqrt{2} + 2\sqrt{2}i}{\frac{\sqrt{3}}{4} + \frac{1}{4}i}$$

$$(e) \frac{\sqrt{27}i}{\sqrt{3} - 3i}$$

$$(d) \frac{3 - 3i}{2 - \sqrt{12}i}$$

$$(f) \frac{\sqrt{17} - \sqrt{51}i}{-17 - 17i}$$

◇

Proposition 4.3.8 is the key fact used in finding the following formula for powers of complex numbers in polar form:

Proposition 4.3.16. (*de Moivre's Theorem*)

Let $z = r \operatorname{cis} \theta$ be a nonzero complex number. Then for $n = 1, 2, \dots$ we have

$$(r \operatorname{cis} \theta)^n = r^n \operatorname{cis}(n\theta). \quad (P(n))$$

(We identify this statement as “ $P(n)$ ” for later convenience.)

Before giving the proof, we first give some general explanation of the ideas behind the proof.

Ideas Behind the Proof: We will use a very common proof technique called *induction*.⁸ Induction is commonly used to prove statements of the form “ $P(n)$ is true for $n = 1, 2, 3, \dots$ ”, where n is some equation or statement involving the quantity n .

Notice that we actually want to prove an *infinite* number of statements: that is, we want to prove:

- $(r \operatorname{cis} \theta)^1 = r^1 \operatorname{cis} \theta$
- $(r \operatorname{cis} \theta)^2 = r^2 \operatorname{cis}(2\theta)$
- $(r \operatorname{cis} \theta)^3 = r^3 \operatorname{cis}(3\theta) \dots$

The first statement is obviously true. The second statement (for $n = 2$) can be proved using Proposition 4.3.8:

Exercise 4.3.17. Prove $(r \operatorname{cis} \theta)^2 = r^2 \operatorname{cis}(2\theta)$ using Proposition 4.3.8. ◇

⁸In the Appendix we give a more thorough treatment of the topic of induction. Here we give only a brief presentation.

The third statement (for $n = 3$) can be proved using the statement for $n = 2$:

Exercise 4.3.18. Fill in the blanks to complete the proof:

$$\begin{aligned}
 (r \operatorname{cis} \theta)^3 &= r \operatorname{cis} \theta \cdot (\underline{\langle 1 \rangle})^2 && \text{(associative)} \\
 &= r \operatorname{cis} \theta \cdot (r^2 \cdot \underline{\langle 2 \rangle}) && \text{(by the previous exercise)} \\
 &= r^3 \cdot \operatorname{cis}(\theta + \underline{\langle 3 \rangle}) && \text{(by Proposition 4.3.8)} \\
 &= \underline{\langle 4 \rangle} && \text{(by basic algebra)}
 \end{aligned}$$

◇

So we have actually used the statement for $n = 2$ to prove the statement for $n = 3$. We could continue in this fashion to prove $n = 4$ from $n = 3$:

Exercise 4.3.19. Prove $(r \operatorname{cis} \theta)^4 = r^4 \operatorname{cis}(4\theta)$, using Proposition 4.3.8 and the result of the previous exercise (*Hint*) ◇

Obviously it would take a long time to prove $n = 5$ from $n = 4$, $n = 6$ from $n = 5$, and so on. So instead, we will prove the following statement that covers all these cases:

If $(r \operatorname{cis} \theta)^k = r^k \operatorname{cis}(k\theta)$ is true, then $(r \operatorname{cis} \theta)^{k+1} = r^{k+1} \operatorname{cis}((k+1)\theta)$ is also true.

This allows us to “ladder up”: if the statement is true for some integer, then it’s also true for the *next* integer.

In summary, the induction proof has two basic elements:

- Prove the statement $P(n)$ for $n = 1$ (this is called the “base case”);
- Assuming that $P(n)$ is true for $n = k$, it follows that $P(n)$ is also true for $n = k + 1$ (this is called the “induction step”).

Now that we’ve given the ideas, here is the actual proof of Proposition 4.3.16:

PROOF. We will use induction on n . First, for $n = 1$ the proposition is trivial. This establishes the “base case”.

Next, assume that $P(n)$ is true for $n = k$: that is, $z^k = r^k \operatorname{cis}(k\theta)$. Then using this fact and exponent rules, we may rewrite z^{k+1} as

$$\begin{aligned} z^{k+1} &= z^k z \\ &= r^k \operatorname{cis}(k\theta) r(\operatorname{cis} \theta) \\ &= r^{k+1} [\operatorname{cis}(k\theta + \theta)] \\ &= r^{k+1} \operatorname{cis}[(k+1)\theta]. \end{aligned}$$

This establishes the “induction step”, which completes the proof. \square

Example 4.3.20. We will compute z^{10} where $z = 1 + i$. Rather than computing $(1 + i)^{10}$ directly, it is much easier to switch to polar coordinates and calculate z^{10} using de Moivre’s Theorem:

$$\begin{aligned} z^{10} &= (1 + i)^{10} \\ &= \left(\sqrt{2} \operatorname{cis}\left(\frac{\pi}{4}\right)\right)^{10} \\ &= (\sqrt{2})^{10} \operatorname{cis}\left(\frac{5\pi}{2}\right) \\ &= 32 \operatorname{cis}\left(\frac{\pi}{2}\right) \\ &= 32i. \end{aligned}$$

◆

Notice that de Moivre’s Theorem says nothing about a complex number raised to negative powers. For any real number x , we know x^{-n} means $(x^n)^{-1}$. Complex numbers happen to work the same way.

Definition 4.3.21. Given a complex number $z = r \operatorname{cis} \theta$,

$$z^{-n} = (z^n)^{-1}.$$

△

Example 4.3.22. Let $z = 2 \operatorname{cis}(\pi/4)$. What is z^{-3} ?

$$\begin{aligned} z^{-3} &= (z^3)^{-1} \\ &= ([2 \operatorname{cis}(\pi/4)]^3)^{-1} \\ &= (8 \operatorname{cis}(3\pi/4))^{-1} \quad (\text{by de Moivre’s Theorem}) \\ &= \frac{1}{8} \operatorname{cis}(5\pi/4) \quad (\text{by Exercise 4.3.11}) \end{aligned}$$



Exercise 4.3.23. Calculate each of the following expressions. Write the answer as $a + bi$ if you can do so without using roots or decimals. Otherwise, you may leave the answer in polar form.

(a) $(1 + i)^{-3}$

(f) $(-\sqrt{2} - \sqrt{2}i)^{12}$

(b) $(1 - i)^6$

(g) $(-2 + 2i)^{-5}$

(c) $(\sqrt{3} + i)^5$

(h) $(\sqrt{2 + \sqrt{2}} - i\sqrt{2 - \sqrt{2}})^{16}$

(d) $(-i)^{10}$

(i) $\frac{(\sqrt{15} - 3\sqrt{5}i)^5}{60^2}$

(e) $((1 - i)/2)^4$

(j) $\frac{(1 - i)^{10}}{(-\sqrt{3} + i)^6}$



4.3.6 A Remark on representations of complex numbers

We have seen that a complex number z can be expressed in a number of different ways:

- As $a + bi$, where a and b are real numbers;
- As a point in the Cartesian (two-dimensional) plane;
- As a pair of real numbers (a, b) that give the rectangular coordinates of the point in the plane;
- As a pair of numbers (r, θ) where $r \geq 0$ and $0 \leq \theta < 2\pi$, that give the polar coordinates of the point in the plane;
- As $r \cdot (\cos \theta + i \cdot \sin \theta)$, or the equivalent form $r \cdot \text{cis}(\theta)$.

In abstract mathematics, it is very common to represent the “same” entity in a number of different ways. One of the main goals of abstract algebra is to identify mathematical structures that are the “same” algebraically even though they appear to be different. Mathematical structures that are the “same” algebraically are said to be *isomorphic*. We will be seeing isomorphic structures throughout this course.

The importance of isomorphism in mathematics cannot be overstated.⁹ Realizing that the same thing can be represented in two different ways is often the key to mathematical progress, and can lead to enormous simplifications. For instance, we have seen that it's easier to add complex numbers in Cartesian form, while it's much simpler to multiply complex numbers in polar form. Since Cartesian and polar forms are simply two different ways of representing the same thing, we can freely switch back and forth between the two forms, using whichever is most convenient at the moment.

Exercise 4.3.24.

- (a) Using de Moivre's formula for z^3 where $z = \text{cis } \theta$, find formulas for $\cos 3\theta$ and $\sin 3\theta$ in terms of $\cos \theta$ and $\sin \theta$. (*Hint*)
- (b) Using part (a), find a formula for $\cos 3\theta$ in terms of $\cos \theta$. (*Hint*)
- (c) Show that for any n , it is always possible to find a formula for $\cos n\theta$ in terms of $\cos \theta$.
- (d) * Show that for any *even* n , it is always possible to find a formula for $\cos n\theta$ in terms of *even* powers of $\cos \theta$.

◇

4.4 Complex numbers and roots of algebraic equations

4.4.1 Roots of unity and regular polygons

As we mentioned before, complex numbers got their start when mathematicians started considering the solutions to algebraic equations. One particularly important equation is

$$z^n = 1, \quad \text{where } n \in \mathbb{N}.$$

For example, when $n = 4$ the complex numbers which solve $z^4 = 1$ are $z = 1, -1, i,$ and $-i$. In general, the complex numbers that satisfy the equation

⁹There are other types of “morphisms” as well, such as homeomorphism (in topology), diffeomorphism (in differential topology), and just plain morphism (in category theory).

$z^n = 1$ are called the *n th roots of unity*. (In other words, “ n th root of unity” means the same thing as “ n th root of 1”.)

Exercise 4.4.1.

- (a) Give two distinct square roots of unity (that is, $z^n = 1$ for $n = 2$).
 (b) For what integers n is -1 an n th root of unity?

◇

It turns out that in general we can find n different n th roots of unity, as per the following proposition:

Proposition 4.4.2. The complex number z is an n th root of unity if and only if z satisfies the following condition:

$$z = \operatorname{cis}\left(\frac{2k\pi}{n}\right), \text{ where } k \text{ is an integer between } 0 \text{ and } n - 1.$$

To illustrate this proposition, consider the case $n = 4$. Then the equation gives: $z = \operatorname{cis}(2k\pi/4)$ where $k = 0, 1, 2, 3$, which works out to $\operatorname{cis}(0)$, $\operatorname{cis}(\pi/2)$, $\operatorname{cis}(\pi)$, and $\operatorname{cis}(3\pi/2)$. Converting to Cartesian form we get $1, i, -1, -i$ as our four roots, in perfect agreement with what we found in the first paragraph of this section.

So, let’s give a proof!

PROOF. The proposition is an “if and only if” assertion, meaning that we’ll have to prove it both ways. We’ll start with the “only if” part. To this end, we suppose z is a complex n th root of unity. Our goal is to show that z must satisfy the given formula. Any complex number may be written in polar form, so we may write $z = r \operatorname{cis}(\theta)$ where r is the modulus and θ is the complex argument of z . So we may deduce:

$$\begin{aligned} z^n &= 1 && (z \text{ is a } n\text{th root of unity}) \\ \Rightarrow (r \operatorname{cis}(\theta))^n &= 1 && (\text{polar form of } z) \\ \Rightarrow r^n \operatorname{cis}(n\theta) &= 1 && (\text{de Moivre's theorem}) \\ \Rightarrow |r^n \operatorname{cis}(n\theta)| &= |1| && (\text{take modulus of both sides}) \\ \Rightarrow |r|^n &= 1 && (\text{properties of modulus}) \\ \Rightarrow r &= 1. && (\text{Since } r \text{ is a nonnegative number}) \end{aligned}$$

Now substituting $r = 1$ back into the third line in this series of implications, we get:

$$\begin{aligned}
 \operatorname{cis}(n\theta) &= 1 && \text{(substitution)} \\
 \Rightarrow \cos(n\theta) + i \sin(n\theta) &= 1 && \text{(definition of cis)} \\
 \Rightarrow \cos(n\theta) = 1 \text{ and } \sin(n\theta) &= 0 && \text{(equality of complex numbers)} \\
 \Rightarrow n\theta = m \cdot 2\pi &&& \text{(periodicity of sin and cosine, from trig)} \\
 \Rightarrow \theta = m \cdot 2\pi/n. &&& \text{(basic algebra)}
 \end{aligned}$$

To recap, we have:

$$z = r \operatorname{cis}(\theta) \text{ where } r = 1 \text{ and } \theta = 2\pi m/n, \text{ where } m \text{ is an integer.}$$

Now, any fraction of the form m/n can be written as an integer plus a fractional part between 0 and 1. Furthermore, the fractional part always has the form k/n where k is an integer between 0 and $n - 1$. In other words:

$$m/n = \ell + k/n \quad \text{where } \ell \text{ and } k \text{ are integers and } 0 \leq k < n.$$

It follows by substitution that

$$\begin{aligned}
 z &= \operatorname{cis}(2\pi m/n) && \text{(from last equality in previous series)} \\
 \Rightarrow z &= \operatorname{cis}(2\pi(\ell + k/n)) && \text{(substitution)} \\
 \Rightarrow z &= \operatorname{cis}(2\pi\ell) \operatorname{cis}(2\pi k/n) && \text{(algebraic properties of cis)} \\
 \Rightarrow z &= \operatorname{cis}(2\pi k/n). && \text{(def. of cis and trig)}
 \end{aligned}$$

Our goal has been achieved: z must definitely have the form $\operatorname{cis}(2\pi k/n)$ where $0 \leq k < n$.

Now for the “if” part; we must show that complex numbers which satisfy the formula as also n th roots of unity. By de Moivre’s Theorem,

$$z^n = \operatorname{cis}\left(n \frac{2k\pi}{n}\right) = \operatorname{cis}(2k\pi) = 1.$$

Finished!

□

Remark 4.4.3. Note that the condition

$$z = \operatorname{cis} \left(\frac{2k\pi}{n} \right), \text{ where } k \text{ is an integer between } 0 \text{ and } n - 1.$$

does indeed specify n distinct values for z . This is because k/n produces n different fractions between 0 and 1, so $\frac{2k\pi}{n}$ gives n different angles between 0 and 2π . Our vector representation of complex numbers tells us that different angles must produce different complex numbers. \triangle

Exercise 4.4.4.

- (a) Using Proposition 4.4.2, write three cube roots of unity in polar form. Convert to the form $a + bi$.
- (b) Using Proposition 4.4.2, write six 6th roots of unity in polar form. Convert to the form $a + bi$.

◇

Exercise 4.4.5. In this exercise you will give a different proof that there are exactly 4 4th roots of unity, by showing that any complex apart from 1, -1 , i , or $-i$ cannot possibly be a 4th root of unity. First we suppose that w is a complex number such that $w \notin \{1, -1, i, -i\}$.

- (a) Show that $(w - 1)(w + 1)(w - i)(w + i) \neq 0$. (*Hint*)
- (b) Show that this implies that w is not a 4th root of unity. (*Hint*)

◇

Exercise 4.4.6.

- (a) Multiply out the product $(z - 1)(z - \operatorname{cis}(\frac{2\pi}{3}))(z - \operatorname{cis}(\frac{4\pi}{3}))$ and simplify. (*Hint*)
- (b) Use your result in (a) to show that there are exactly 3 cube root of unity.

◇

When represented in the complex plane, the roots of unity have some very interesting geometric properties:

Example 4.4.7. The 8th roots of unity can be represented as eight equally spaced points on the unit circle (Figure 4.4.1). For example, some 8th roots of unity are

$$\begin{aligned}\omega &= \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ \omega^3 &= -\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i \\ \omega^5 &= -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i \\ \omega^7 &= \frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.\end{aligned}$$

In fact, the 8th roots of unity form a *regular octagon*. ◆

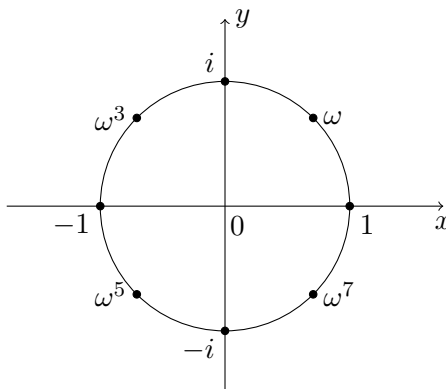


Figure 4.4.1. 8th roots of unity

Exercise 4.4.8. Sketch the cube roots of unity in the complex plane. Use the distance formula (from geometry) to show that the three points are all the same distance from one another. Connect the three points to form a triangle. What kind of triangle is it? ◇

4.4 COMPLEX NUMBERS AND ROOTS OF ALGEBRAIC EQUATIONS 65

Exercise 4.4.9. Prove (using geometry) that the 4th roots of unity form a square. (*Hint:* Besides showing that all sides are equal, you also have to show that they are perpendicular.) \diamond

Exercise 4.4.10. *Prove (using geometry) that the 6th roots of unity form a regular hexagon. (*Hint:* Draw lines from each point to the origin, forming 6 triangles. What can you say about these triangles?) \diamond

Once again, we see an interesting relationship between complex numbers and plane geometry. Let us explore this relationship a little further.

Exercise 4.4.11.

(a) Draw a picture of the 6th roots of unity in the complex plane. Label them A, B, C, D, E, F with $A = 1, B = \text{cis}\left(\frac{2\pi}{6}\right)$, and C, D, E, F going counterclockwise around the circle.

(b) Fill in each of the following blanks with the letter corresponding to the product of the two complex numbers. For example, $B \cdot B = \text{cis}\left(\frac{2\pi}{6}\right) \cdot \text{cis}\left(\frac{2\pi}{6}\right) = \text{cis}\left(\frac{4\pi}{6}\right) = C$.

$$\begin{array}{lll} B \cdot A = \underline{\langle 1 \rangle} & B \cdot C = \underline{\langle 3 \rangle} & B \cdot E = \underline{\langle 5 \rangle} \\ B \cdot B = \underline{\langle 2 \rangle} & B \cdot D = \underline{\langle 4 \rangle} & B \cdot F = \underline{\langle 6 \rangle} \end{array}$$

(c) Using your answers from part (b), on your picture draw an arrow from A to $B \cdot A$; similarly draw arrows from B to $B \cdot B$, C to $B \cdot C$, and so on. What do you observe about the arrows?

(d) It appears that multiplying all of the corners of the hexagon $ABCDEF$ by B produces a *rotation* of the hexagon. What is the angle of rotation?

(e) Fill in the blanks:

$$\begin{array}{lll} E \cdot A = \underline{\langle 1 \rangle} & E \cdot C = \underline{\langle 3 \rangle} & E \cdot E = \underline{\langle 5 \rangle} \\ E \cdot B = \underline{\langle 2 \rangle} & E \cdot D = \underline{\langle 4 \rangle} & E \cdot F = \underline{\langle 6 \rangle}. \end{array}$$

(f) Just as in part (c), use your answers from part (d) to draw arrows from A to $E \cdot A$, B to $E \cdot B$, etc. What do you observe about the arrows?

- (g) Fill in the blanks: If you choose one particular 6th root of unity and multiply it with all the other 6th roots, the new values correspond to different < 1 > of the original hexagon. The angle of < 2 > is equal to the complex argument of the < 3 >.

◇

Exercise 4.4.12.

- (a) Just as in part (b) of Exercise 4.4.11 fill in the blanks with the correct letter A, B, C, D, E or F (recall that \bar{A} denotes the complex conjugate of A).

$$\begin{array}{lll} \bar{A} = \underline{\text{< 1 >}} & \bar{C} = \underline{\text{< 3 >}} & \bar{E} = \underline{\text{< 5 >}} \\ \bar{B} = \underline{\text{< 2 >}} & \bar{D} = \underline{\text{< 4 >}} & \bar{F} = \underline{\text{< 6 >}}. \end{array}$$

- (b) Just as in part (c) of Exercise 4.4.11, draw arrows from A to \bar{A} , B to \bar{B} , etc. What do you observe about the arrows?
- (c) We refer to the geometrical motion produced by complex conjugation as “flipping”. What is the axis of the “flip” that is produced by taking the complex conjugates of the sixth roots of unity?

◇

The previous exercises (when suitably generalized) lead to the following stupendous conclusion:

- Every *rigid* motion of a regular n -gon is equivalent to some combination of complex conjugation and multiplication by one of the n th roots of unity. (By “rigid motion” we mean any motion that a rigid object could undergo, without stretching or bending or distorting it in any way. We’ll have more to say about rigid motions in Chapter 13.)

Exercise 4.4.13.

- (a) What geometrical motion corresponds to the following algebraic operation: Multiply all 6th roots by D , then take the complex conjugates.

- (b) What geometrical motion corresponds to the following algebraic operation: “Take the complex conjugates of all 6th roots, then multiply by D .”
- (c) What geometrical motion corresponds to the following algebraic operation: “Multiply all 6th roots by C , then take the complex conjugates.”
- (d) What geometrical motion corresponds to the following algebraic operation: “Take the complex conjugates of all 6th roots, then multiply by C .”

◇

Exercise 4.4.13 also gives us our first exposure to a phenomenon that is quite common in abstract algebra, namely the existence of non-commutative operations (also known as *non-abelian* operations). We saw that both multiplication by a n th root of unity and complex conjugation corresponded to motions of a regular n -gon. However, the *order* of the motions matters: rotating first and then conjugating (i.e. “flipping”) gives a *different* result than conjugating first, then performing the rotation afterwards.

Exercise 4.4.14. If you’ve studied matrix multiplication, then you may have seen non-commutative operations before:

- (a) Give an example of two 2×2 matrices that do *not* commute: that is $AB \neq BA$.
- (b) Give an example of two 2×2 matrices that *do* commute.

◇

The previous exercises give a small hint as to the extensive and beautiful relationship between the complex numbers and plane geometry. The following exercises further explore this relationship.

Exercise 4.4.15. Consider a plane with Cartesian coordinates. Let O be the point $(0, 0)$, let A be the point (a, b) , and let C be the point (c, d) . Also, let $w = a + bi$ and $z = c + di$. We may consider the three complex numbers $0, w, z$ as representing the vertices of triangle OAC .

(A word to the wise: drawing a picture can be extremely helpful.)

- (a) Express the lengths of the three sides of the triangle in terms of w and z . For example, the length of side OA is $|w|$.
- (b) Show that multiplying $0, w$, and z by $\frac{\bar{w}}{|w|}$ rotates the triangle so that side OA lies along the real axis (you may use polar coordinates).
- (c) Let $0, w'$, and z' be the three vertices of the rotated triangle. Show that $\operatorname{Re}[z'] = \frac{z\bar{w} + \bar{z}w}{2|w|}$ and $\operatorname{Im}[z'] = \frac{z\bar{w} - \bar{z}w}{2|w|}$.
- (d) Show that the area of the rotated triangle is $\left| \frac{z\bar{w} - \bar{z}w}{4} \right|$. (Since rotation doesn't change the area, your formula also gives the area of triangle OAC .)
- (e) Let $OA'C'$ denote the rotated triangle. Express the cosine of angle $\angle A'OC'$ in terms of w and z .
- (f) Let $|OA'|, |OC'|$, and $|A'C'|$ denote the lengths of the three sides of the rotated triangle. Use complex arithmetic with w and z to prove the *law of cosines*:

$$|A'C'|^2 = |OA'|^2 + |OC'|^2 - 2|OA'||OC'| \cos(\angle A'OC').$$

(Since rotation does not change lengths or angles, you have also proved the law of cosines for the original triangle OAC .)

◇

Exercise 4.4.16. As in the previous problem, consider points O, A, C in the Cartesian plan represented by complex numbers $0, w$, and z respectively.

- (a) The segments OA and OC are two sides of a parallelogram P , where O, A, C are three of the four vertices of P . Let D be the fourth vertex of P . Let v be the complex number that represents D . Express v in terms of w and z .
- (b) We have seen that points in the plane are associated with vectors, which in turn may be represented by complex numbers. For example, the vector \vec{AC} is represented by the complex number $z - w$. Find the complex number that represents the vector \vec{OD} .
- (c) Let F and G be any two points in the plane, represented by the complex numbers q and r respectively. Show that OF is perpendicular to OG if and only if q/r is imaginary (you may use polar coordinates).

- (d) Show that the two diagonals of the parallelogram P are perpendicular if and only if the parallelogram is a *rhombus*, i.e. all sides of the parallelogram are equal.

◇

Exercise 4.4.17. As in the previous problems, consider points O, A, C in the Cartesian plane represented by complex numbers $0, w, z$ respectively.

- (a) The perpendicular bisector of side OA corresponds to the set of complex numbers $\{w/2 + itw, t \in \mathbb{R}\}$. Similarly, the perpendicular bisector of OC corresponds to the set of complex numbers $\{z/2 + isz, s \in \mathbb{R}\}$. Express the perpendicular bisector AC as sets of complex numbers.
- (b) The perpendicular bisectors of OA and OC intersect at a point B in the Cartesian plane, which corresponds to a complex number v . Since v is on both perpendicular bisectors, we may write $v = w/2 + it'w$ and $v = z/2 + is'z$. By setting these expressions, we may solve for s' in terms of t, w, z . Since s' is real we have $s' = \bar{s}'$, so that we may obtain another equation for s' in terms of t', \bar{w}, \bar{z} . Solve for t' by setting these two equations equal. Then solve for s' using your solution for t' .
- (c) Since we have $v = w/2 + it'w$ and $v = z/2 + is'z$, we may also write v as the average of these two expressions: $v = 1/2(w/2 + it'w) + 1/2(z/2 + is'z)$. By plugging in the values of t' and s' and rearranging, show that we may write $v = (w + v)/2 + ir'(w - v)$, where r' is real.
- (d) Conclude that the perpendicular bisectors of triangle OAC all meet at a single point.
- segments OA and OC are two sides of a parallelogram P , where O, A, C are three of the four vertices of P . Let D be the fourth vertex of P . Let v be the complex number that represents D . Express v in terms of w and z .
- (e) We have seen that points in the plane are associated with vectors, which in turn may be represented by complex numbers. For example, the vector \vec{AC} is represented by the complex number $z - w$. Find the complex number that represents the vector \vec{OD} .
- (f) Let F and G be any two points in the plane, represented by the complex numbers q and r respectively. Show that OF is perpendicular to OG if and only if q/r is imaginary (you may use polar coordinates).

- (g) Show that the two diagonals of the parallelogram P are perpendicular if and only if the parallelogram is a *rhombus*, i.e. all sides of the parallelogram are equal.

◇

In fact, many intricate theorems in plane geometry that require long proofs using conventional methods can be proven much more easily using complex numbers. We will not be exploring this further; but we hope these examples will stimulate your imagination!

4.4.2 Complex n th roots in general

In the previous section, we characterized all complex solutions of the equation $z^n = 1$; we called these solutions the n th roots of unity. A natural question to ask then is, What about the n th roots of any complex number? That is, given a complex number $a + bi$, can we find all solutions to the equation $z^n = a + bi$? Let's explore some simple cases first.

Exercise 4.4.18.

- (a) Find all square roots of 1.
- (b) Find all square roots of 4.
- (c) Find all square roots of -1.
- (d) Find all square roots of -2.
- (e) In each of the above cases, given one of the square roots, you can find a second square root by multiplying by ____ (fill in the blank).

◇

We may use the observation from part (e) of the previous exercise to find alternative square roots of other complex numbers.

Exercise 4.4.19.

- (a) The complex number $1 + i$ is one square root of $2i$. Can you find another one?

4.4 COMPLEX NUMBERS AND ROOTS OF ALGEBRAIC EQUATIONS 71

(b) Find two square roots of $8i$. (*Hint*)

(c) Find two square roots of $-8i$.

◇

Next, let us consider the case of cube roots. Consider for example the cube roots of $1 + i$, which are the solutions to

$$z^3 = 1 + i.$$

We may rewrite this in polar form as

$$(r \operatorname{cis} \theta)^3 = \sqrt{2} \operatorname{cis} \left(\frac{\pi}{4} \right),$$

where $r \operatorname{cis} \theta$ is z in polar form. De Moivre's theorem then gives us:

$$r^3 \operatorname{cis} 3\theta = \sqrt{2} \operatorname{cis} \left(\frac{\pi}{4} \right).$$

One solution for r and θ which satisfies this equation is:

$$r^3 = \sqrt{2} \Rightarrow r = 2^{1/6} \quad \text{and} \quad 3\theta = \pi/4 \Rightarrow \theta = \pi/12,$$

so that

$$z = 2^{1/6} \operatorname{cis}(\pi/12).$$

We may use deMoivre's theorem to verify that this z is indeed a cube root of $1 + i$. But is it the only one? In fact, if we multiply this z by $\operatorname{cis}(2\pi/3)$ and cube the result, we find:

$$\begin{aligned} \left(2^{1/6} \operatorname{cis}(\pi/12) \cdot \operatorname{cis}(2\pi/3) \right)^3 &= \left(2^{1/6} \operatorname{cis}(\pi/12) \right)^3 \cdot (\operatorname{cis}(2\pi/3))^3 \\ &= (1 + i) \cdot 1 \\ &= 1 + i, \end{aligned}$$

so that $z \cdot \operatorname{cis}(2\pi/3)$ is also a cube root of $1 + i$. Why does this work? Notice that $\operatorname{cis}(2\pi/3)$ is a *cube root of unity*, so it turns into 1 when cubed. The same thing happens with $\operatorname{cis}(4\pi/3)$, which is the other cube root of unity—you may check that $z \cdot \operatorname{cis}(4\pi/3)$ is an additional cube root of $1 + i$. This example suggests a general procedure for finding 3 distinct cube roots of complex numbers:

- Find a single cube root using de Moivre's Theorem;
- Multiply your result by $\text{cis}(2\pi/3)$ and $\text{cis}(4\pi/3)$ to obtain 3 distinct cube roots.

This takes care of cube roots. But let's not stop there! We can use a similar procedure to find n distinct n th roots of any complex number:

- Find a single root using de Moivre's Theorem;
- Multiply your result by all n roots of unity to obtain n distinct roots.

Exercise 4.4.20. Show that the 2-step procedure above gives *all* n th roots of a given complex number. That is, show that any complex n th root of z can be obtained as an n th root of unity times any other complex n th root of z . You may proceed as follows. Suppose z is a complex number, and w_1 and w_2 are n th roots of z . Show that there exists an n th root of unity u such that w_1 is the product of u and w_2 , i.e. $w_1 = u \cdot w_2$. \diamond

Exercise 4.4.21. (In this exercise, you may leave your answers in polar form)

- Find all fifth roots of $-i$.
- Find all fourth roots of $-1 + \sqrt{3}i$.
- Find all fourth roots of $\sqrt{1/2 + \sqrt{2}/4} + i\sqrt{1/2 - \sqrt{2}/4}$. (**Hint**)
- Find all sixth roots of $-16i$.
- Find all seventh roots of $5 - 5i$.

\diamond

Exercise 4.4.22. In previous exercises, we have considered n th roots where n is a *positive* integer. But what about *negative* roots?

- For parts (a-e) in Exercise 4.4.21, find the corresponding *negative* roots (i.e., in part (a) find the negative 5th roots, etc).

- (b) Explain the relationship between the moduli of the roots you found in Exercise 4.4.21, and the roots you found in part (a).
- (c) Explain the relationship between the complex arguments of the roots you found in Exercise 4.4.21, and the complex arguments you found in part (a).

◇

4.4.3 Complex roots of polynomial equations

Next we consider more general algebraic equations than the basic n th root equations we've been looking at so far. As a first example, consider the equation $z^2 + pz = q$, where p and q are real numbers. Using the quadratic formula, it is not too hard to show that if $a+bi$ is a solution of $z^2 + pz = q$ then the complex conjugate $a - bi$ is also a solution. This is because $z^2 + pz = q$ can also be written as $z^2 + pz - q = 0$, and the quadratic formula tells us that there are two solutions, given by:

$$z = \frac{-p \pm \sqrt{p^2 - (4)(1)(-q)}}{2} = \frac{-p}{2} \pm \frac{\sqrt{p^2 + 4q}}{2}.$$

The $-p/2$ term is always real, but the square root term is either real or imaginary depending on the sign of $p^2 + 4q$ (since q could be negative). If the square root term is real, then both roots are real, and each root is its own complex conjugate. If the square root term is imaginary, then the \pm means that the imaginary parts of the two roots are negatives of each other, so that the two roots are complex conjugates.

Exercise 4.4.23. Consider the cubic equation $z^3 + pz^2 + qz = r$, where p, q and r are all real numbers.

- (a) Using an appropriate identity from Exercise 4.2.22, show that $\overline{z^3} = \bar{z}^3$.
- (b) Similarly, show $\overline{pz^2} = p\bar{z}^2$ and $\overline{qz} = q\bar{z}$, and $\bar{r} = r$.
- (c) Use (a) and (b) to show that $\overline{z^3 + pz^2 + qz - r} = \bar{z}^3 + p\bar{z}^2 + q\bar{z} - r$.
- (d) Using (c), show that $z^3 + pz^2 + qz - r = 0$ implies that $\bar{z}^3 + p\bar{z}^2 + q\bar{z} - r = 0$.
- (e) Using (d), show that if z is a solution to $z^3 + pz^2 + qz = r$ then \bar{z} is also a solution.

◇

Exercise 4.4.24. Suppose the cubic equation $z^3 + pz^2 + qz = r$ has an odd number of solutions. Show that at least one of the solutions must be real.
◇

The proof in Exercise 4.4.23 can be straightforwardly generalized to quartic, quintic, and higher-degree polynomials as well. The result is:

Proposition 4.4.25. Given that the complex number z is a solution of $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \dots + a_1z = a_0$, where a_0, a_1, \dots, a_{n-1} are real numbers. Then \bar{z} is also a solution to the same equation.

Exercise 4.4.26. Given that $3 - 7i$ and $-2 + i$ are solutions to an equation of the form $z^4 + a_3z^3 + a_2z^2 + a_1z + a_0 = 0$ where a_0, a_1, a_2, a_3 are real.

- (a) Find two other solutions to the same equation.
- (b) *Find a_0, a_1, a_2, a_3 . (*Hint*)

◇

Exercise 4.4.27. Given that $p(z) = z^3 + a_2z^2 + a_1z + a_0 = 0$, where a_0, a_1, a_2 are real numbers. Suppose $p(1) = 16$, and suppose that $1 + 2i$ is a root of $p(z)$.

- (a) Find two other solutions to the same equation.
- (b) Find a_0, a_1, a_2 .

◇

Exercise 4.4.28. Given the equation $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \dots + a_1z = a_0$, where a_0, a_1, \dots, a_{n-1} are real numbers. Let N be the number of solutions of the equation that are *not* real. Prove that either $N = 0$ or N is divisible by 2. (*Hint*) ◇

Exercise 4.4.29. Suppose that $p(z)$ is a fourth degree polynomial with real coefficients. Suppose that $p(z) = p(-z)$. Suppose also that $3 + 4i$ is a root of $p(z)$ and that $p(0) = 1$.

- (a) Find three other roots of $p(z)$.
- (b) Find $p(z)$.

◇

The most famous result concerning complex roots of polynomials is known as the **Fundamental Theorem of Algebra**:

Proposition 4.4.30. Given any equation of the form $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \dots + a_1z = a_0$, where $n > 0$ and a_0, a_1, \dots, a_{n-1} are real numbers. Then there exists at least one and at most n distinct complex numbers which solve the given equation.

The Fundamental Theorem of Algebra actually has two parts. The easy part is the “at most n distinct complex roots” part, and the hard part is the “at least one complex root” part. We will eventually prove the easy part in Chapter 12, but sadly the hard part is beyond our scope. For more information on this see the Remark at the end of the chapter.

Exercise 4.4.31.

- (a) Give an example of an equation of the form $z^2 + a_1z = a_0$ that has only one solution.
- (b) Give an example of an equation of the form $z^3 + a_2z^2 + a_1z = a_0$ that has only one solution.
- (c) Can you give an example of an equation of the form $z^3 + a_2z^2 + a_1z = a_0$ that has exactly two solutions?

◇

Exercise 4.4.32. Using the Fundamental Theorem of Algebra and Exercise 4.4.28, prove the following proposition: Given an equation of the form $z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \dots + a_1z = a_0$, where $n > 0$ and a_0, a_1, \dots, a_{n-1} are real numbers. Suppose the equation has no real solutions. Then the equation has at least two distinct solutions. ◇

Exercise 4.4.33. Using the Fundamental Theorem of Algebra and Exercise 4.4.28, prove the following proposition: Given an equation of the form

$z^n + a_{n-1}z^{n-1} + a_{n-2}z^{n-2} + \dots + a_1z = a_0$, where n is a positive odd number and a_0, a_1, \dots, a_{n-1} are real numbers. Then the equation has at least one real solution. \diamond

Exercise 4.4.34. Give an example of a polynomial of the form $z^6 + a_5z^5 + a_4z^4 + \dots + a_1z = a_0$, that has no real solutions, and exactly two distinct complex solutions. \diamond

Remark 4.4.35. (*historical background*) The Fundamental Theorem of Algebra is a famous “hard problem” in the history of mathematics. Some of the greatest mathematicians in history (including Euler, Lagrange, Laplace, and Gauss) thought they had proofs, only to have later mathematicians point out flaws or gaps in the arguments. See http://www-history.mcs.st-and.ac.uk/HistTopics/Fund_theorem_of_algebra.html for more details. In the modern mathematics curriculum, the proof is usually given in courses on complex analysis as an easy consequence of “Liouville’s theorem”, which was first proved in 1847. Modern college students who learn basic concepts from the theory of complex variables can readily grasp the theorem which stymied the greatest mathematical minds of history. \triangle

4.5 Applications of complex numbers

4.5.1 General remarks on the usefulness of complex numbers

We have already discussed that it took some time for complex numbers to be generally accepted by mathematicians, who tended to have a preference for “pure” numbers such as the integers. But complex numbers have had their revenge. Today the “purest” form of mathematics, namely number theory, is heavily dependent on complex numbers. The famous Fermat’s Last Theorem was proved using techniques that involved complex numbers.¹⁰

But quite apart from pure mathematics, complex numbers have proved to be extremely practical. Complex numbers are indispensable tools for scientists and engineers. Virtually all of modern physics is based on complex numbers. Engineers build bridges using complex numbers. Without complex numbers, there would probably be no computers, cell phones or most other

¹⁰See http://www-history.mcs.st-and.ac.uk/HistTopics/Fermat's_last_theorem.html for some of the long and sordid history of Fermat’s Last Theorem.

electronics. A strong argument could be made that complex numbers are even more useful than “real” numbers.

Much of the practical usefulness of complex numbers comes from their close relationship with the trigonometric functions cosine and sine. We have seen a little bit of this already in the representation $z = r \operatorname{cis} \theta$. Complex numbers give a powerful way to express complicated functions of sine and cosine in a very simple way. We will give an introduction of this in the next section—you may see it again, or have already seen it, in your differential equations course.

4.5.2 Complex numbers in electrical engineering: phasors

We have already seen there is a close relationship between complex numbers and the trigonometric functions sine and cosine. This relationship is the basis for much of the usefulness of complex numbers – as we shall explain in this section.

Figure 4.5.1 shows the graphs of the cosine and sine functions. They look like waves: for instance, the graph of $y = \cos(t)$ is a wave that includes the point $(0, 1)$. The *amplitude* of this wave is 1. The *period* of this wave is 2π radians.

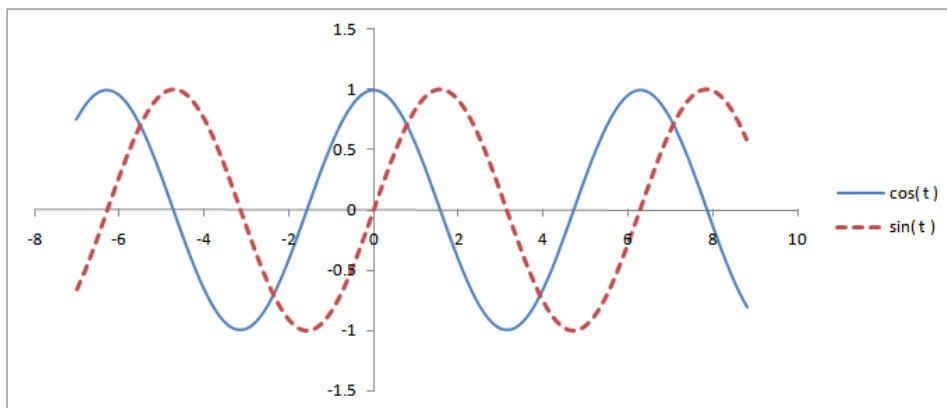


Figure 4.5.1. Graphs of cosine and sine

Note that some references use the word “wavelength” instead of “period”. This is because they are considering equations like $y = \cos(x)$ where the independent variable x represents distance. We are considering the in-

dependent variable to be time: so it is appropriate to use the word “period” instead.

Of course, there are cosine and sine waves with different periods. However, in this section we will *only* be looking at cosine and sine waves with period 2π . We re-emphasize: all the cosine and sine waves in this chapter (and any that you use in the homework problems) have period 2π .

Now we can create other waves by using the cosine as a “parent function”. For instance, the graph of $y = A \cos(t + \theta)$ where $A > 0$ is similar to the graph of $y = \cos(t)$, with the following differences:

- The amplitude is A
- The *phase shift* (relative to the cosine curve) is θ .

Remark 4.5.1.

- You may have studied “parent functions” in high school, and if so you may remember that the graph of $y = f(t + c)$ is shifted to the *left* compared to the graph of $y = f(t)$. It follows that a positive phase shift will shift the graph to the *left*, while a negative phase shift will shift it to the *right* (see Figure 4.5.2).¹¹
- If the variable t is considered as time, then $y = A \cos(t + \theta)$ is *advanced* by θ (corresponding to a left shift of the graph), while $y = A \cos(t - \theta)$ is *delayed* by θ (corresponding to a right shift of the graph).

△

Exercise 4.5.2. Sketch the function $y = 1.5 \cos(t + \pi/3)$. Label the amplitude and phase shift on your graph. ◇

Exercise 4.5.3. Give the equation of a cosine wave with amplitude 7 and phase shift $-\pi/2$. Graph the function. How is this function related to a sine wave? ◇

¹¹You should be careful when you encounter the term “phase shift” in other books, because some books define a positive phase shift as moving the graph to the *right*. This is not wrong: it’s just different terminology.

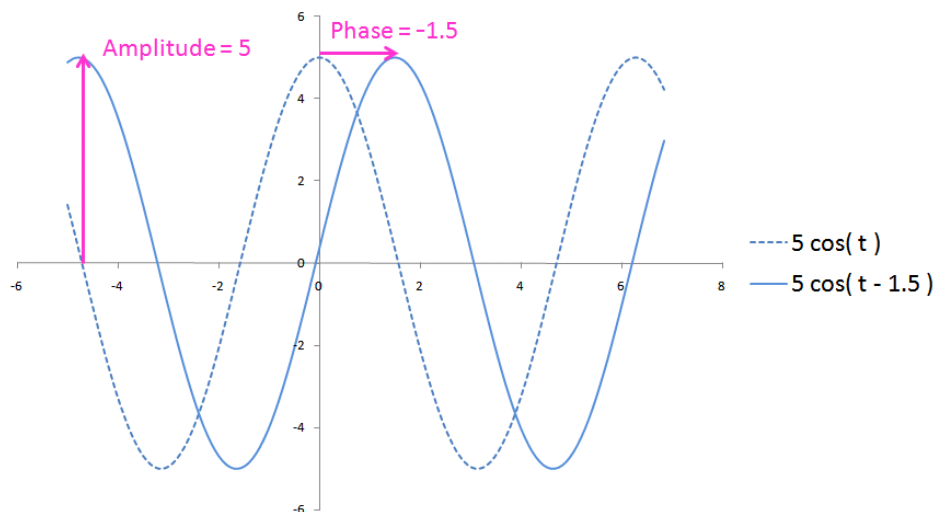


Figure 4.5.2. Cosine wave with amplitude and phase shift

Exercise 4.5.4. Give the equation of a cosine wave with amplitude $1/2$ and phase shift 2π . Graph the function. How is this wave related to the original cosine wave with phase shift 0 ? \diamond

Exercise 4.5.5.

- (a) Sketch the function $y = \sin(t)$.
- (b) Find three different choices of A, θ such that $\sin(t) = A \cos(t + \theta)$. What are the possible values of A ? (*Hint*)

\diamond

In summary, amplitude and phase are two important properties of cosine and sine waves; and in fact the amplitude and phase uniquely determine the actual wave, as you saw in Exercises 4.5.3 and 4.5.4. Now earlier in this chapter, we saw a different mathematical object that was characterized by amplitude and phase. Naturally, we're referring to the complex numbers. We will now make a deep connection between these two types of mathematical objects that, on the surface, are very different.

Recall that the *real part* of the complex number $z = a + bi$ is a , and the *imaginary part* is b . We also use the notation $\operatorname{Re}[z]$ to denote the real part

of the complex number z , and the notation $\text{Im}[z]$ to denote the imaginary part.

Exercise 4.5.6. Show that $\text{Re}[A \text{cis } \theta \cdot \text{cis}(t)] = A \cos(t + \theta)$. (*Hint*) \diamond

Exercise 4.5.7. Show that $\text{Im}[A \text{cis } \theta \cdot \text{cis}(t)] = A \sin(t + \theta)$. \diamond

The previous two exercises show that:

- A cosine wave with amplitude A and phase shift θ can be represented as the real part of the complex number $A \text{cis } \theta$ times the complex function $\text{cis}(t)$.
- A sine wave with amplitude A and phase shift θ can be represented as the imaginary part of the complex number $A \text{cis } \theta$ times the complex function $\text{cis}(t)$.

We may also understand this situation in terms of two-dimensional vectors with the help of Figure 4.5.3. We've already shown how complex numbers can be seen as two-dimensional vectors: in particular, the complex number $\text{cis } \theta$ is identified with $\cos \theta \mathbf{i} + \sin \theta \mathbf{j}$. As t varies, the point $\text{cis}(t + \theta)$ moves around the unit circle, and the real part of $\text{cis}(t + \theta)$ is the projection of the moving point onto the x -axis. In other words, the cosine wave on the right side of Figure 4.5.3 tells us the vector's horizontal distance to the y -axis as a function of time t .

Now when two waves cross each other they produce a wave of a different shape—we may see this in water waves at the beach or pool (or physics class). This is called *wave superposition*. We will now see how complex numbers make it easy to compute the shape of this new wave.

Exercise 4.5.8.

- (a) Using $\text{cis } \theta = \cos \theta + i \sin \theta$, complete the following argument by filling in the blanks:

$$\begin{aligned} 2 \cos(t + \pi/2) + 2 \cos(t - 5\pi/6) &= \text{Re}[2 \text{cis}(t + \pi/2)] + \text{Re}[\underline{\langle 1 \rangle}] \\ &= \text{Re}[2 \text{cis}(t) \cdot \text{cis}(\pi/2)] + \text{Re}[\underline{\langle 2 \rangle}] \\ &= \text{Re}[(2 \text{cis}(\pi/2) + 2 \text{cis}(-5\pi/6)) \cdot \underline{\langle 3 \rangle}] \end{aligned}$$

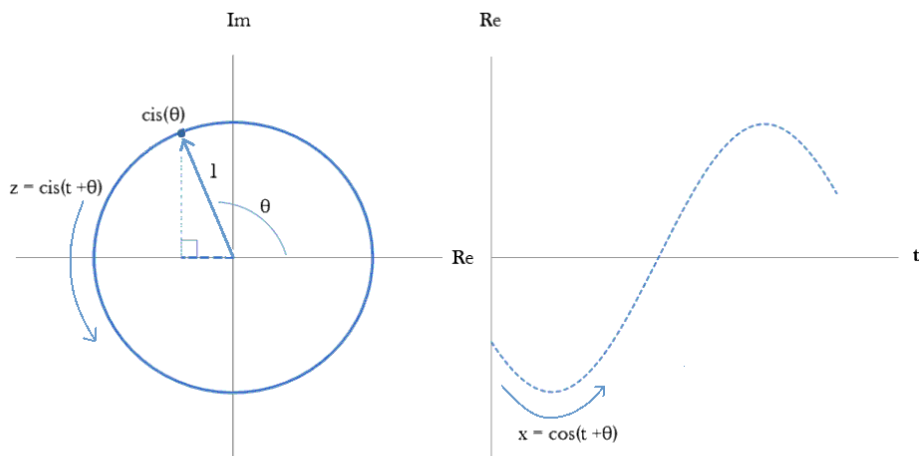


Figure 4.5.3. Graphs of the vector representation and the wave representation of cosine

- (b) Convert $2 \operatorname{cis}(\pi/2)$ and $2 \operatorname{cis}(-5\pi/6)$ to cartesian form, and find the sum. Then convert back to polar form.
- (c) Use your result in (b) to simplify the right-hand side of (a).
- (d) Your result in (c) shows that the sum of the two cosine waves $2 \cos(t + \pi/2)$ and $2 \cos(t - 5\pi/6)$ is also equal to a cosine wave. Find the amplitude and phase shift of the sum. Is the amplitude equal to the sum of the amplitudes? Explain.

◇

Let us summarize our findings:

- Associated with each sine or cosine wave is a complex number $A \operatorname{cis}(\theta)$ such that A is the amplitude and θ is the phase shift of the wave. This complex number is called the **phasor** associated with the wave.

- The sum of two sine or cosine waves is also equal to a cosine wave
- The amplitude and phase shift of the sum of two cosine waves may be obtained by adding the phasors of the two constituent cosine waves.

Exercise 4.5.9. A radio antenna receives three cosine-wave signals. The first signal has an amplitude of 4 and a phase shift of 0. The second has an amplitude of 3 and a phase shift of $\pi/2$. The third signal has an amplitude of 2 and a phase shift of $-\pi/3$.

- On graph paper, plot the three phasors corresponding to the three signals. (The three phasors are $4 \operatorname{cis}(0)$, $3 \operatorname{cis}(\pi/2)$, and $2 \operatorname{cis}(-\pi/3)$)
- Use your picture in (a) to graphically add the three phasors. (Remember how to add vectors: add the x -components, and add the y -components.)
- Convert the three phasors to rectangular form, and add them together algebraically.
- Use your result from (c) to find the amplitude and phase shift of the sum of the three signals.

◇

Exercise 4.5.10. As in the previous problem, a radio antenna receives three cosine-wave signals. The three signals have equal amplitude. The first signal have a phase shift of 0. The second has a phase shift of $2\pi/3$. The third signal has a phase shift of $4\pi/3$.

- What is the amplitude of the sum of the three signals?
- What is the phase shift of the sum of the three signals?

◇

We hope that from the examples in this section, you may get some idea of how important complex numbers are in the study of signals. In fact, for many electrical engineers complex numbers are their “bread and butter”.

4.5.3 Complex numbers and fractals: the Mandelbrot set

The intricate *Mandelbrot set* (see Figure 4.5.4) is a beautiful application of complex numbers. The Mandelbrot set is defined by means of *iteration* of the function $f(z) = z^2 + c$. The definition is a little complicated: we show how it works using a couple of examples.

First consider $c = 1$, so $f(z) = z^2 + 1$. We start with $z = 0$, which gives $f(0) = 1$; and we iterate by evaluating the function on the result of the previous evaluation. So we compute $f(1) = 2, f(2) = 5, f(5) = 26, \dots$. It is clear that $|f(z)|$ is getting larger and larger after repeated iterations.

On the other hand, if we use $c = i$ and start with $z = 0$, we get $f(0) = i$ at first, and repeated iteration gives $f(i) = -1 + i, f(-1 + i) = -i, f(-i) = -1 + i, \dots$ so that this time $|f(z)|$ doesn't continue to grow indefinitely after repeated iterations.

The Mandelbrot set is defined to be the set of values c for which the iterations of $f(z) = z^2 + c$ starting from $z = 0$ do *not* grow indefinitely upon iteration. Thus i is in the Mandelbrot set, while 1 is not.

Exercise 4.5.11. Which of the following numbers is in the Mandelbrot set? *Demonstrate* your answers.

- | | |
|--------------|-----------------|
| (a) $c = 0$ | (c) $c = -i$ |
| (b) $c = -1$ | (d) $c = 1 + i$ |

◇

Exercise 4.5.12. In the definition of the Mandelbrot set, we mentioned that you have to check whether the iterations “grow indefinitely”. The question, is, How far do you have to check? We can actually give an answer:

- (a) Given any two complex numbers z, w , show that:

$$|z + w| \leq |z| + |w|.$$

This is called the *triangle inequality* for complex numbers (it is closely related to the ‘triangle inequality’ for vectors). (**Hint**)

- (b) Prove the following variation of the triangle inequality: Given two complex numbers z, w then $|z| \geq |z - w| - |w|$.

- (c) Suppose that $|c| < 2$, and suppose that $z \geq 2$. Use (b) to show that $|z^2 + c| > |z|$.
- (d) In order to guarantee that a number c is in the Mandelbrot set, all we have to do is show that one of the iterates of the function $f(z) = z^2 + c$ is larger than a given positive number r . What is the value of r ?

◇

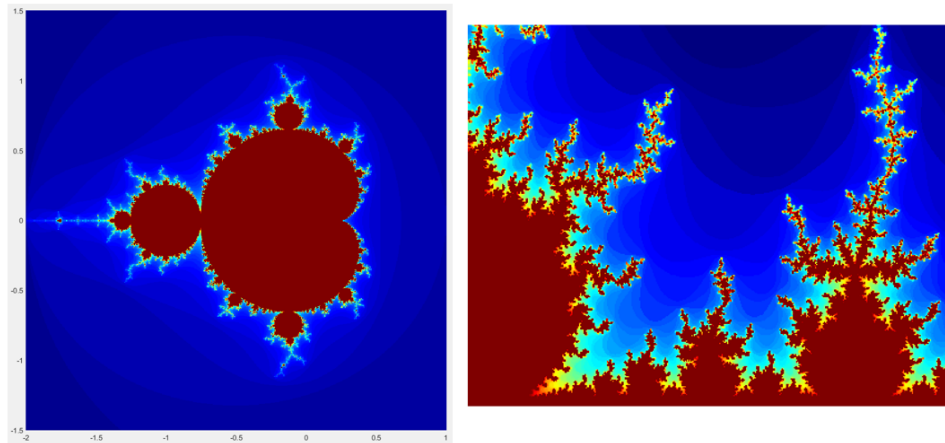


Figure 4.5.4. (*Left*) The Mandelbrot set: the set itself is colored in maroon. The set has delicate filaments that extend from the different bulb-shaped areas, which are outlined in lighter color. (*Right*) Detail of the Mandelbrot set, along the top edge of the heart-shaped region shown in the figure at left.

Exercise 4.5.13. (*Programming exercise*)

- (a) Write an Excel spreadsheet that can multiply two complex numbers. Put the real and imaginary parts of the first number in cells A1 and B1; Put the real and imaginary parts of the second number in cells C1 and D1; Put the real and imaginary parts of the result in cells E1 and F1. Use your sheet to compute $(3 + 4i)(7 - 8i)$.
- (b) Copy your Excel sheet, and modify it to compute the square of a complex number. Put the real and imaginary parts of the first number in cells A1 and B1; Put the real and imaginary parts of the result in cells C1 and D1. Use your sheet to compute $(12 - 5i)^2$.

- (c) Copy and modify your Excel sheet to compute $z^2, (z^2)^2, ((z^2)^2)^2, \dots$ (20 number altogether) for a given complex number z . Put the real and imaginary parts of z in cells A1 and B1; Put the real and imaginary parts of the results in columns C and D. Use your sheet with $z = 0.8 + 0.6i$. Plot the results as 20 points in the plane (use Scatter Plot). What do you notice about your numbers?
- (d) Modify your Excel sheet to compute the first 100 iterates of the function $f(z) = z^2 + c$ for given complex numbers z, c (see Exercise 4.5.11). Put the real and imaginary parts of z in cells A1 and B1; Put the real and imaginary parts of c in cells A2 and B2; put the results in columns C and D. Using your sheet, determine which of the following numbers is in the Mandelbrot set: (i) $z = -1.04039 + 0.2509294i$; (ii) $c = -0.1155989 + 0.7639405i$.

◇

Exercise 4.5.14. sing $c = -3/4 + 0.01$ compute the sequence for 100 iterations, and note the iteration at which the value exceeds 2. Do the same thing for $c = -3/4 + 0.001$, but for 1000 iterations. Do you see any relationship between your results and the value of π ? ◇

4.6 Hints for “Complex Numbers” exercises

Exercise 4.1.9(b) Start your proof this way: “Given that m is an integer and m^2 is even. Suppose that m is odd. Then . . .” (complete the proof by obtaining a contradiction. You should make use of part (a) in your proof.

Exercise 4.1.9(c) The proof is similar to that in (b). What modifications do you need to make?

Exercise 4.1.11(a) Start out your proof this way: “Let x be the cube root of 2. Then x satisfies the equation $x^3 = 2$.” For the rest of the proof, follow closely the proof of Proposition 4.1.10. (Or use the statement–reason format, if you prefer.

Exercise 4.1.12 Since $3|n$, it follows that $n = 3j$ for some integer j . Obtain a similar equation from $4|m$, and multiply your equations together.

Exercise 4.1.13 Since $n|4m$, it follows that $4m = n \cdot j$ for some integer j . Since $12|n$, then what can you substitute for n ?

Exercise 4.1.21 Try using contradiction. Suppose n is even, so that $n = 2k$ for some integer k .

Exercise 4.2.7 To show $zz^{-1} = 1$, rewrite z^{-1} as $(a - bi) \cdot \frac{1}{a^2 + b^2}$. This is justified by the distributive law. Remember also that showing $z^{-1}z = 1$ requires its own proof.

Exercise 4.2.8(i) In the answer $x + yi$, x and y both turn out to be integers!

Exercise 4.2.8(n) Yes, you can do it! Find the first few powers of i , and see the pattern.

Exercise 4.2.8(o) It’s easiest to compute $(1 + i)^2 \cdot (1 + i)^2$.

Exercise 4.2.9 If you have trouble with this one, do some examples.

Exercise 4.2.22(f) Use part (e).

Exercise 4.2.22(g) and (h) See Exercise 4.2.7.

Exercise 4.2.26 Use part (b) of the previous exercise, plus some of the results from Exercise 4.2.22.

Exercise 4.2.27(a) Use the formula $|w|^2 = w \cdot \bar{w}$. (d) This one requires calculus.

Exercise 4.3.19 Just make minor changes to the previous exercise.

Exercise 4.3.24(a) Replace $\text{cis} \dots$ with $\cos \dots + i \sin \dots$ on both sides of the de Moivre equation. Then do the algebra on the right-hand side, and separate

the real and imaginary parts. Recall that two complex numbers are equal iff their real parts and imaginary parts are equal separately. (b) Use a basic identity involving cosine and sine.

Exercise 4.5.5(b) What left shifts will change a cosine curve into a sine curve?

Exercise 4.5.6 Use Proposition 4.3.8 to evaluate $\text{cis } \theta \cdot \text{cis}(t)$, and recall that $\text{cis}(\alpha)$ means the same as $\cos(\alpha) + i \sin(\alpha)$.

Exercise 4.4.5(a) We have already shown in Proposition 4.2.11 that the product of two nonzero complex numbers is never equal to 0. Use this to show that the product of four nonzero complex numbers is never equal to 0.

Exercise 4.4.5(b) Multiply out the inequality that you proved in (a).

Exercise 4.4.6(a) It's easier to multiply the numbers in polar form, you don't have to convert to Cartesian. Note that $\text{cis}\left(\frac{4\pi}{3}\right)$ is the complex conjugate of $\text{cis}\left(\frac{2\pi}{3}\right)$.

Exercise 4.4.9 Besides showing that all sides are equal, you also have to show that they are perpendicular.

Exercise 4.4.10 Draw lines from each point to the origin, forming 6 triangles. What can you say about these triangles?

Exercise 4.4.15(c) Note that $OA = |z|$, $OC = |w|$, and $AC = |z - w|$.

Exercise 4.4.18(c) Use your answer to part (b).

Exercise 4.4.21(c) To find the polar form of this number, try squaring it.

Exercise 4.4.26(b) If r is a solution to the above equation, then $z - r$ divides $z^4 + a_3z^3 + a_2z^2 + a_1z + a_0$.

Exercise 4.4.28 Let M be the number of distinct solutions with positive imaginary part. Then how many distinct solutions are there with negative imaginary part? And how many non-real solutions are there altogether?

Exercise 4.5.12 You may show that $(|z + w|)^2 \leq (|z| + |w|)^2$. When you take the square, use the identity that expresses $|z|^2$ in terms of z and its complex conjugate. After simplification, use polar form.

4.7 Study guide for “Complex Numbers” chapter

Note: all study guides were written by Katrina Smith.

Section 4.1, The origin of complex numbers

Concepts

1. n th roots of a real number
2. Roots of a real function
3. Proof by contradiction
4. Irrational number: cannot be written as a quotient of integers
5. Definition of i (square root of -1)
6. Definition of complex numbers: $\mathbb{C} = \{a + bi, \quad a, b \in \mathbb{R}\}$

Notation

1. Symbols for number systems: \mathbb{R} =real numbers, \mathbb{Z} =integers, \mathbb{N} =natural numbers (positive integers), \mathbb{Q} =rational numbers, \mathbb{C} =complex numbers
2. \exists means “there exists”, and \in means “element of”. So $\exists x \in \mathbb{C}, x^3 = -1$ means “there exists a complex number x such that $x^3 = -1$.”

Competencies

1. Given a real number, prove whether it has any real n th roots. (4.1.2, 4.1.3)
2. Use proof by contradiction to prove a value or function has no real roots. (4.1.2, 4.1.3)
3. Given an n th root which is not an integer, prove that it is irrational. (4.1.11, 4.1.17)

Section 4.2, Arithmetic with complex numbers**Concepts:**

1. Complex arithmetic
2. Identity & inverse (additive & multiplicative)
3. Associative law
4. Commutative law
5. Absolute value or modulus of complex number
6. Complex conjugate

Key Formulas

1. Complex addition: $(a + bi) + (c + di) = (a + c) + (b + d)i$
2. Complex multiplication (FLOI): $(a + bi)(c + di) = (ac - bd) + (ad + bc)i$
3. Complex division: $\frac{c + di}{a + bi} = \frac{(c + di)(a - bi)}{(a^2 + b^2)}$, when $(a + bi) \neq 0$
4. Modulus of complex number: $|z| = \sqrt{a^2 + b^2}$
5. Complex conjugate of a complex number: $\bar{z} = a - bi$

Competencies

1. Simplify expressions involving complex numbers in $a + bi$ form, including inverse and complex conjugation. (4.2.8, 4.2.20)
2. Simplify algebraic expressions with variables in $a + bi$ form, including inverse and complex conjugation. (4.2.8d, e, k, 4.2.20i, j)
3. Be able to state the associative, inverse, identity, commutative, and distributive properties for different number systems. (4.2.15)
4. Prove identities for a complex number z involving algebraic expressions, modulus, complex conjugate *without* converting back to Cartesian form. (4.2.22a-i)

Section 4.3, Alternative representations of complex numbers**Concepts:**

1. Forms of complex number: rectangular and polar form
2. Converting from rectangular form to polar form and vice versa
3. Complex multiplication and division using polar form
4. De Moivre's Theorem (raising complex numbers to integer powers)

Key Formulas

1. Converting from polar form to rectangular: $a = r \cos \theta; b = r \sin \theta$
2. Converting from rectangular form to polar: $r = |z| = \sqrt{a^2 + b^2};$
 $\theta = \tan^{-1} \left(\frac{b}{a} \right)$ (** be careful about \tan^{-1} – make sure it's in the right quadrant **)
3. Multiplication of complex numbers: $r \operatorname{cis} \theta \cdot s \operatorname{cis} \phi = r s \operatorname{cis}(\theta + \phi)$
4. Division of complex numbers: $\frac{r \operatorname{cis} \theta}{s \operatorname{cis} \phi} = \left(\frac{r}{s} \right) \operatorname{cis}(\theta - \phi)$
5. De Moivre's Theorem: $(r \operatorname{cis} \theta)^n = r^n \operatorname{cis}(n\theta)$

Notes

(a) $r \operatorname{cis} \theta := r(\cos \theta + i \sin \theta)$; “:=” means “is defines as”

Competencies

1. Be able to convert back and forth between rectangular form and polar form. (4.3.4, 4.3.5)
2. Perform complex multiplications and divisions using polar form (if the problem is stated in terms of rectangular form, convert to polar form first). (4.3.14, 4.3.15)
3. Raise complex numbers to positive and negative integer powers using de Moivre's theorem. (4.3.23)
4. Prove trigonometric formulas for $\cos(n\theta)$ and $\sin(n\theta)$ using de Moivre's theorem. (4.3.24)

Section 4.4, Complex numbers and roots of algebraic equations**Concepts:**

1. n^{th} roots of unity
2. n^{th} roots of arbitrary complex numbers
3. The Fundamental Theorem of Algebra
4. Complex roots of polynomials with real coefficients come in conjugate pairs.

Key Formulas

1. Roots of unity: $z = \text{cis} \left(\frac{2k\pi}{n} \right)$, where $k = 0, 1, \dots, n - 1$

Competencies

1. Know how to find n^{th} roots of unity for any $n \in \mathbb{N}$. (4.4.4)
2. Relate complex conjugation and multiplication by n^{th} roots of unity to rigid motions of a regular n -gon. (4.4.11 - 4.4.13)
3. Find all n^{th} roots of a given complex number by (1) Finding a single root using de Moivre's theorem: (2) Multiplying that single root by all n^{th} roots of unity. (Note: there are always n n^{th} roots for any complex number.) (4.4.19, 4.4.21).
4. Be able to prove complex conjugation properties of roots of polynomial equations with real coefficients. (4.4.23)
5. Use complex conjugate properties of roots to reconstruct polynomials. (4.4.26)

Modular Arithmetic

What goes up, must come down
Spinnin' wheel, got ta go round
Talkin' 'bout your troubles it's a cryin' sin
Ride a painted pony, Let the spinnin' wheel spin
(Source: "Spinnin' Wheel", *Blood, Sweat, and Tears*)


Cycles are everywhere. So are integers. Modular arithmetic combines the two by wrapping the integers around a circle.


Thanks to Tom Judson for material used in this chapter. David Weathers also contributed a section.


5.1 Introductory examples


Modular arithmetic was originally motivated by common, real-life situations. So we begin our introduction by describing several problems based on practical situations for you to think about. We don't ask you to find the solutions just yet – instead, focus on the similarities between the different problems.


Example 5.1.1. Don has whipped up some stew that he wants to slow-cook in his crockpot. The stew is supposed to cook for exactly 40 hours. The crockpot is not automatic, so Don has to turn it on and off by hand. When would be a good time for Don to turn on the crockpot? (Additional information: Don is away at work from 8 a.m. to 5 p.m. every day. Also,


Don would like to avoid waking up in the middle of the night to turn the crockpot on or off.) 


Example 5.1.2. Jennifer owns a vintage 1957 Thunderbird which has had two previous owners. She claims that the car's first owner drove it 129,000 miles, the second owner drove it 77,000 miles, and she's driven 92,500 miles. If her claim is true, then what should the odometer read? Note that on old cars the odometer only goes up to 99,999. 


Example 5.1.3. April 15, 2012 was on a Friday. What day of the week was December 24 of 2011? (Note 2012 is a leap year!) 

Example 5.1.4. A lunar year is 354 days. If Chinese New Year is determined according to the lunar year, and Chinese New Year is February 14 in 2010, then when is Chinese New Year in 2011? In 2012? In 2009? ¹ 

Example 5.1.5. The hour hand on Tad's old watch is broken and does not move. Currently the watch shows a time of 3:46. Tad has just begun a 3-part test, where each part takes 75 minutes (plus a 10-minute break between parts). What time will the watch read when the first part is over? The second part? The entire test? 

Example 5.1.6. A racing car starts at the 3 mile mark of a 5-mile circuit. It goes another 122 miles. Then, it turns around and drives 444 miles in the reverse direction. Where does the car end up? 

Example 5.1.7. Suppose our race car is driving around the 5-mile track again. If it starts at the 3 mile mark and makes 17 consecutive runs of 24 miles each, what mile marker does it end up at? 

Exercise 5.1.8. Try to describe what all of the preceding problems have in common. Describe some differences. 

¹Note that the Chinese calendar actually adds extra months in some years, so not every Chinese year is 354 days. So this example is not 100% accurate

Notice that in each example the set of possible answers is restricted to a finite set of integers. For instance, in the odometer example (Example 5.1.2) we know even before working the problem that the answer must be an integer between 0 and 99,999 (inclusive). In other words, there are 100,000 possible answers to the question, regardless of the particular mileages involved.

Exercise 5.1.9. Give the number of possible answers for Examples 5.1.1 and 5.1.3. \diamond

Each example above requires arithmetic to solve, but it's arithmetic with a twist. For example, in Example 5.1.6 if the car is at the 3-mile mark and travels another 3 miles, then it arrives at the 1-mile marker. This is a strange equation: $3 + 3 = 1$. The reason of course is that the location "cycles" back to 0 instead of increasing to 5, 6, 7, \dots . This "arithmetic with cycles" is actually called *modular arithmetic*. The size of one cycle (which is equal to the number of possible answers described in Exercise 5.1.9 is called the *modulus*.

Exercise 5.1.10. Give the modulus for the seven examples at the beginning of this chapter. \diamond

In summary, modular arithmetic refers to arithmetic done according to a modulus, so that the numbers reset (or cycle around) every time you reach the modulus.

5.2 Modular equivalence and modular arithmetic

In order to understand the situation more thoroughly, let us focus on the 5-mile racetrack example used in Examples 5.1.6 and 5.1.7. The racetrack (with mile markers) is shown in Figure 5.2.1.

Let's say the car starts at mile marker 0. The car may then travel forward (counterclockwise) or backwards (clockwise) any number of miles; we may define the car's *net displacement* as the the total number of forward miles traveled minus the the total number of backward miles. Net displacement is a very useful concept if you are a race car driver. For example, the winner of the Indianapolis 500 is the the first driver to achieve a net displacement of 500 miles (in this case, only forward motion is allowed!)

We may characterize the displacement of the car using a conventional number line, as shown in Figure 5.2. Moving forward around the racetrack

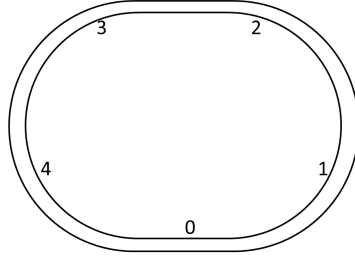


Figure 5.2.1. 5-mile racetrack

corresponds to moving right (positive direction) on the number line; while moving backward around the racetrack corresponds to moving left (negative direction).

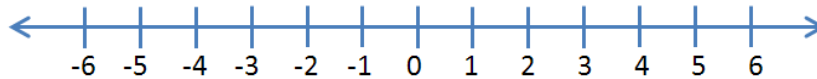


Figure 5.2.2. Displacements on a 5-mile racetrack

Exercise 5.2.1. Compute the net displacement for the following multi-stage trips:

- (a) 346 miles in the forward direction, then 432 miles in the backward direction, then 99 miles in the forward direction.
- (b) A forward displacements of 44 miles, followed by 13 additional forward displacements of 53 miles (one after the other).
- (c) Repeat the following sequence 25 times: a forward displacement of 17 miles, followed by a backward displacement of 9 miles, followed by a forward displacement of 22 miles.

◇

From the preceding exercise, it appears that we may use ordinary addition, subtraction and/or multiplication to compute the car's net displacement after a trip involving several stages.

On the other hand, if we want to represent the *position* of the car on the track as it relates to net displacement, we would have to relabel the number line as shown in Figure 5.2.3, using only the integers 0, 1, 2, 3, 4.

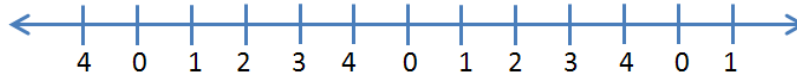


Figure 5.2.3. Positions on the 5-mile racetrack

Exercise 5.2.2.

- (a) Compute the positions on the racetrack corresponding to each of the net displacements that you computed in Exercise 5.2.1.
- (b) How are your answers in (a) related to the corresponding answers in Exercise 5.2.1?

◇

You may have noticed that different displacements may correspond to the same position. For example, displacements of 8, 23, and -17 all correspond to the same position (namely 3). We say that two displacements that correspond to the same position are *equivalent*. The fact that displacements 8 and 23 are equivalent on a 5-mile racetrack may be expressed mathematically as: $8 \equiv 23 \pmod{5}$ (in words, we say ‘8 is equivalent to 23 mod 5’).

How can you tell when two displacements correspond to the same position? In our racetrack example we may notice that 8, 23, and -17 all have remainder 3 when divided by 5. So in this example at least, we can see that the position on the racetrack corresponds to the remainder when the displacement is divided by the length of the racetrack (which serves as the modulus). You may verify that this is true for any displacement: the position is what’s left after all whole multiples of 5 are taken out.

This seems to indicate that we can define a notion of equivalence in terms of remainders. But let’s be careful here. You’ve probably been finding remainders since elementary school—but have you really thought about what you’re doing? How do you know there will always be a remainder? And

how do you know there's only one? Why couldn't some numbers have two different remainders, and some have none at all? It appears that before we can define modular equivalence in terms of remainders, first we're going to have to establish some solid facts about remainders:

Proposition 5.2.3. (*The division algorithm*) Given any integer a and any positive integer m , then there exists a unique number r between 0 and $m - 1$ such that $a = q \cdot m + r$ for some integer q . In this expression, q is called the *quotient*, and r is called the *remainder*.

PROOF. It turns out that proving this “simple” fact is not so simple! Although this fact has been used for millennia (it's sometimes called *Euclidean division*, because Euclid used it ca. 300 B.C.), the first rigorous proof was found relatively recently. There are actually two things to prove: first, that the remainder r exists, and second, that it's unique. We're going to punt on the ‘existence’ part: you can find the proof in a book on number theory.² The ‘unique’ part is proved by the following fill-in-the-blanks exercise:

Exercise 5.2.4. Fill in the blanks in the following proof that the remainder is always unique.

We'll give a proof by contradiction. Suppose that a has two different remainders when divided by m . Let's call these two different remainders r and s , where $0 \leq r, s \leq \underline{\langle 1 \rangle}$ and $r \neq s$.

It follows that $a = q \cdot m + r$ and $a = p \cdot m + \underline{\langle 2 \rangle}$, where q and p are $\underline{\langle 3 \rangle}$. Setting these two expressions equal and rearranging enables us to obtain an expression for $r - s$, namely: $r - s = (\underline{\langle 4 \rangle}) \cdot m$. Thus $r - s$ is an integer multiple of $\underline{\langle 5 \rangle}$.

On the other hand, we know that $r \geq 0$ and $s \leq \underline{\langle 6 \rangle}$, so by arithmetic we obtain $r - s \geq \underline{\langle 7 \rangle}$. Furthermore, $r \leq \underline{\langle 8 \rangle}$ and $s \geq \underline{\langle 9 \rangle}$, so $r - s \leq \underline{\langle 10 \rangle}$. Combining these two results, we find that $r - s$ is an integer between $\underline{\langle 11 \rangle}$ and $\underline{\langle 12 \rangle}$.

Now, the only integer multiple of m between $\underline{\langle 13 \rangle}$ and $\underline{\langle 14 \rangle}$ is $\underline{\langle 15 \rangle}$. It follows that $r - s = \underline{\langle 16 \rangle}$, or $r = \underline{\langle 17 \rangle}$. But this contradicts our supposition that $\underline{\langle 18 \rangle}$. So our supposition cannot be true: and a cannot have $\underline{\langle 19 \rangle}$. Thus the remainder when a is divided by m is unique, and the proof is complete. \diamond

²Or check the internet, e.g.: <http://www.oxfordmathcenter.com/drupal7/node/479>.

□

We'll use the notation “ $\text{mod}(a, m)$ ” to indicate the remainder of a when divided by m . This notation is used in most mathematical software (such as Excel, Matlab, and so on), and it reflects the fact that the remainder is a function of a and m .

Remark 5.2.5. Unlike many references, we do *not* use the expressions “ $a \text{ mod } m$ ” or “ $a \pmod{m}$ ” to denote the remainder when a is divided by m . In this book we *never* write “ $a \text{ mod } m$ ” or “ $a \pmod{m}$ ” as stand-alone expressions. Here's the reason why. Suppose for the moment that we do use $17 \pmod{5}$ to denote the remainder of $17 \text{ mod } 5$. Then we could write $2 = 17 \pmod{5}$, but it would be *false* to write $17 = 2 \pmod{5}$, since 17 is not the remainder of $2 \text{ mod } 5$. In this book the \pmod{n} refers to the relation ‘ \equiv ’ and not to the b . Thus for us, $2 \equiv 17 \pmod{5}$, and $17 \equiv 2 \pmod{5}$ are both correct. \triangle

Now that we know that unique remainders really do always exist, we're in a position to use them in our definition of modular equivalence:

Definition 5.2.6. Two integers a and b are *equivalent* mod m if both a and b have the same remainder when divided by m . To denote that a and b are *equivalent* mod m , we write: $a \equiv b \pmod{m}$. \triangle

Remark 5.2.7. Notice that Definition 5.2.6 uses the 3-lined “ \equiv ” here instead of the usual $=$ sign. This notation is used to emphasize the fact that modular equivalence resembles equality, but is not quite the same thing. For example, we have already seen that 8 and 23 are equivalent mod 5, even though they are not equal. In a later chapter we'll discuss equivalence relations, and we'll see that equivalence is in some sense a generalization of equality. For now, be alerted to the fact that “ \equiv ” and “ $=$ ” do not necessarily have the same properties. It's tempting for instance to make statements such as, “ $a \equiv b \pmod{m}$ implies $a - b \equiv 0 \pmod{m}$ ”. But just because this is true for $=$ doesn't mean it's also true for \equiv ! In this case the statement turns out to be true, but it requires proof – and in this class you are not allowed to make assertions that have not been proven.³ \triangle

The following result enables us to verify when we've indeed found a remainder.

³This may be one reason why not many mathematicians are politicians, and vice-versa.

Proposition 5.2.8. If $a \equiv r \pmod{m}$ and $0 \leq r \leq m - 1$, then $r = \text{mod}(a, m)$.

PROOF. Given that $a \equiv r \pmod{m}$, by the definition of modular equivalence it follows that a and r have the same remainder mod m . But since $0 \leq r \leq m - 1$, the remainder of r is r itself. It follows that the remainder of a is also r : so $r = \text{mod}(a, m)$. \square

There is an alternative (and very useful) way to determine modular equivalence. Suppose that $a \equiv b \pmod{m}$, so that a and b have the same remainder when divided by m . Let's call this remainder r . Then we can write $a = p \cdot m + r$ and $b = q \cdot m + r$ for some integers p, q . It follows from basic algebra that $a - p \cdot m = b - q \cdot m$. We then proceed step-by-step using basic algebra as follows:

$$\begin{aligned} a - p \cdot m &= b - q \cdot m \\ \Rightarrow a - b &= p \cdot m - q \cdot m \\ \Rightarrow a - b &= (p - q) \cdot m. \\ \Rightarrow a - b &\text{ is divisible by } m. \end{aligned}$$

In summary, we have shown that

$$\text{If } a \equiv b \pmod{m} \text{ then } a - b \text{ is divisible by } m.$$

which we can also write as

$$a \equiv b \pmod{m} \Rightarrow a - b \text{ is divisible by } m.$$

It turns out that the *converse* statement is also true.⁴ The converse statement is:

$$\text{If } a - b \text{ is divisible by } m \text{ then } a \equiv b \pmod{m}.$$

One way to prove this is to prove the *contrapositive*, which is logically equivalent.⁵ In this case, the contrapositive statement is, “If $a \not\equiv b \pmod{m}$, then $a - b$ is not divisible by m ”.

⁴In general, if you have a statement of the form “If A then B”, then the converse is “If B then A”. Similarly, the converse of “A \Rightarrow B” is, “B \Rightarrow A”.

⁵In general, the contrapositive of “If A as true then B is also true”, is “If B is not true then A is not true”. Alternatively: if you have a statement “A \Rightarrow B”, then the contrapositive is “not B \Rightarrow not A”. Unlike the converse, the contrapositive is *always* true if the original statement is true

Exercise 5.2.9. Finish the proof of the contrapositive by filling in the blanks:

Suppose $a \not\equiv b \pmod{m}$. Let r be the remainder of a when divided by $\underline{\langle 1 \rangle}$, and let s be the remainder of $\underline{\langle 2 \rangle}$ when divided by $\underline{\langle 3 \rangle}$. Since the remainders are unequal, it follows that one must be bigger than the other: let us choose a to be the number with the larger remainder, so that $r > \underline{\langle 4 \rangle}$. By the definition of remainder, we may write $a = p \cdot m + \underline{\langle 5 \rangle}$, and we may also write $b = q \cdot \underline{\langle 6 \rangle} + \underline{\langle 7 \rangle}$. Then by basic algebra, $a - b = (p - q) \cdot \underline{\langle 8 \rangle} + (r - \underline{\langle 9 \rangle})$.

We want to show that $r - s$ is the remainder of $a - b$ when divided by m . To do this, we need to show that $r - s$ is between 0 and $\underline{\langle 10 \rangle}$. Since $r > s$ it follows that $r - s > \underline{\langle 11 \rangle}$. Furthermore, Since $r < m$ and $s \geq 0$, it follows that $r - s < \underline{\langle 12 \rangle}$. So we have shown that $r - s$ is between $\underline{\langle 13 \rangle}$ and $\underline{\langle 14 \rangle}$, so by Proposition $\underline{\langle 15 \rangle}$ it follows that $r - s$ is the remainder of $a - b$ when divided by m . However, $r - s > 0$, which means that $a - b$ is not divisible by $\underline{\langle 16 \rangle}$. This is exactly what we needed to prove, so the proof is complete. \diamond

We summarize Exercise 5.2.9 and the preceding discussion together in the following proposition.

Proposition 5.2.10. Given any two integers a and b , and a modulus m (m is a positive integer). Then

$$a \equiv b \pmod{m} \text{ if and only if } a - b = k \cdot m,$$

where k is an integer.

We may rewrite Proposition 5.2.10 more elegantly using mathematical shorthand as follows: Given $a, b, m \in \mathbb{Z}$, then

$$a \equiv b \pmod{m} \text{ iff } m|(a - b).$$

Note the two shorthand expressions we have used here: the symbol ‘ \in ’ means ‘contained in’ or ‘elements of’, while the single vertical line ‘|’ means ‘divides’.

The following proposition establishes important facts about modular equivalence that we’ll need later.

Proposition 5.2.11. Given any integers a, b, c and a positive integer n such that $a \equiv b \pmod{n}$ and $c \equiv b \pmod{n}$. Then it is also true that $a \equiv c, c \equiv a, b \equiv a$, and $b \equiv c$ (all these equivalences are \pmod{n}).

Remark 5.2.12. This proposition actually establishes that modular equivalence is both *transitive* and *symmetric*. If you haven't seen this terminology before don't worry—we'll talk about transitive and symmetric relations in the Equivalence Relations chapter. \triangle

Exercise 5.2.13. Prove Proposition 5.2.11. (*Hint*)⁶ \diamond

Exercise 5.2.14. Suppose January 25 is a Thursday.

- (a) Use Definition 5.2.6 to determine whether January 3 is a Thursday. Show your reasoning.
- (b) Use Proposition 5.2.10 to determine whether January 31 is a Thursday. Show your reasoning.
- (c) Find the nearest Thursday to January 15. Show your reasoning.
- (d) Find the nearest Thursday to April 18. Show your reasoning. (Note: the year is not a leap year.)

\diamond

Exercise 5.2.15. Determine whether or not the following equivalences are true. Explain your reasoning. If the equivalence is not true, change one of the numbers to make it true.

- (a) $71 \equiv 13 \pmod{4}$
- (b) $-23 \equiv 13 \pmod{6}$
- (c) $101 \equiv 29 \pmod{6}$
- (d) $50 \equiv 13 \pmod{7}$
- (e) $654321 \equiv 123456 \pmod{5}$
- (f) $1476532 \equiv -71832778 \pmod{10}$

\diamond

Let us now return to the problem of finding the position corresponding to the net displacement following a multi-stage trip. When you computed racetrack positions in Exercise 5.2.2, most likely you simply took the net displacements you computed in Exercise 5.2.1, divided by 5 and took remainder. However, our new concept of modular equivalence gives us another

⁶All *Hints* can be found at the end of the book (or by clicking on the *Hints* link.)

way of solving this problem – one that can be much, much easier if we're dealing with large displacements.

Example 5.2.16. Suppose Dusty drives around the 5-mile track 112 miles in a positive direction, then 49 miles in a negative direction, then 322 miles in a positive direction. To find Dusty's net displacement we may take $112 - 49 + 322 = 385$ and then take the remainder mod 5 (which turns out to be 0). But notice that:

$$\begin{aligned}\text{mod}(112, 5) &= 2, \\ \text{mod}(-49, 5) &= 1, \\ \text{mod}(322, 5) &= 2,\end{aligned}$$

and we compute

$$2 + 1 + 2 = 5 \equiv 0 \pmod{5}.$$

We have obtained the same answer with much less work. How did we do it? By *replacing each number with its remainder*. ♦

Can we do the same thing with multiplication?

Example 5.2.17. Suppose I travel on my racetrack at a 113 miles per hour in the positive direction for 17 hours. We may compute:

$$\text{Net displacement : } 113 \cdot 17 = 1921 \text{ miles}$$

$$\text{Final position : } 1921 = 384 \cdot 5 + 1 \Rightarrow \text{final position} = 1.$$

On the other hand, we may reach the same conclusion by a somewhat easier route:

$$\begin{aligned}\text{mod}(113, 5) &= 3, \\ \text{mod}(17, 5) &= 2,\end{aligned}$$

and we compute

$$3 \cdot 2 = 6 \equiv 1 \pmod{5}.$$

Again, we have obtained the correct answer by *replacing each number with its remainder*. ♦

Does this work in general? In fact it does! However, this requires a mathematical proof. We will discuss the proof in a later section – but at

least our discussion shows that *arithmetic with remainders* is meaningful and useful.

If we're doing arithmetic $(\text{mod } n)$, then the remainders will necessarily be between 0 and $n - 1$ (inclusive). This set of remainders has a special name, which later on we'll use extensively:

Definition 5.2.18. The set of integers $\{0, 1, \dots, n - 1\}$ is called the set of *integers mod n* , and is denoted by the symbol \mathbb{Z}_n . \triangle

Remark 5.2.19. In this chapter, we are considering \mathbb{Z}_n as a subset of \mathbb{Z} . Later on in Chapter 17 we will view \mathbb{Z}_n from an entirely different perspective. (You don't really need to know this now—just file it away for future reference.) \triangle

Exercise 5.2.20. Now you're ready! Give answers for the seven examples at the beginning of this chapter. \diamond

5.3 Modular equations

5.3.1 More uses of modular arithmetic

Supermarkets and retail stores have a nasty little secret. Every time you scan your purchases, they're using modular arithmetic on you! In fact, modular arithmetic is the basis for bar codes you see in stores. We will use these practical examples to introduce *modular equations*.

Exercise 5.3.1. Universal Product Code (UPC) symbols are now found on most products in grocery and retail stores. The UPC symbol (see Figure 5.3.1) is a 12-digit code which identifies the manufacturer of a product and the product itself. The first 11 digits contain the information, while the twelfth digit is used to check for errors that may occur while scanning. If $d_1d_2 \cdots d_{12}$ is a valid UPC code, then

$$3 \cdot d_1 + 1 \cdot d_2 + 3 \cdot d_3 + \cdots + 3 \cdot d_{11} + 1 \cdot d_{12} \equiv 0 \pmod{10}.$$

So the scanning device that cashiers use reads the code and adds up the numbers mod 10. If they don't add to zero, then the device knows it hasn't scanned properly. (Smart little bugger, that scanner is!)

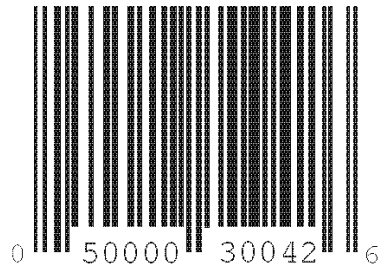


Figure 5.3.1. A UPC code

- (a) Show that the UPC number 0-50000-30042-6, which appears in Figure 5.3.1, is a valid UPC number.
- (b) Show that the number 0-50000-30043-6 is not a valid UPC number.
- (c) (*for geeks*) Write a program or Excel spreadsheet that will determine whether or not a UPC number is valid.
- (d) One common scanning error occurs when two consecutive digits are accidentally interchanged. This is called a **transposition error**. The UPC error detection scheme can catch most transposition errors. Using the UPC in (a) as the correct UPC, show that the transposition error 0-50003-00042-6 is detected. Find a transposition error that is not detected.
- (e) Using the UPC in (a) as the correct UPC, show that the single-digit error 0-50003-30042-6 is detected.
- (f) ****Prove that the UPC error detection scheme detects all single digit errors. (*Hint*)**

◇

It is often useful to use an **inner product** notation for these types of error detection schemes.⁷ In the following text, the notation

$$(d_1, d_2, \dots, d_k) \cdot (w_1, w_2, \dots, w_k) \equiv 0 \pmod{n}$$

⁷You may have seen inner products (a.k.a. “dot products”) in one of your math classes talking about vectors.

will be used to mean

$$d_1w_1 + d_2w_2 + \cdots + d_kw_k \equiv 0 \pmod{n}.$$

Exercise 5.3.2. Every book has an *International Standard Book Number* (ISBN-10) code. This is a 10-digit code indicating the book's language, publisher and title. The first digit indicates the language of the book; the next three identify the publisher; the next five denote the title; and the tenth digit is a check digit satisfying

$$(d_1, d_2, \dots, d_{10}) \cdot (1, 2, \dots, 10) \equiv 0 \pmod{11}.$$

ISBN-10 codes are nice in that all single-digit errors and most transposition errors can be detected. One complication is that d_{10} might have to be a 10 to make the inner product zero; in this case, the character 'X' is used in the last place to represent 10.

- (a) Show that 3-540-96035-X is a valid ISBN-10 code.
- (b) Is 0-534-91500-0 a valid ISBN-10 code? What about 0-534-91700-0 and 0-534-19500-0?
- (c) How many different possible valid ISBN-10 codes are there?
- (d) Write a formula of the form $d_{10} \equiv \dots \pmod{\dots}$ to calculate the check digit in an ISBN-10 code. (*Hint*)
- (e) *Prove that any valid ISBN-10 code also satisfies:

$$(d_1, d_2, \dots, d_{10}) \cdot (10, 9, \dots, 1) \equiv 0 \pmod{11}.$$

- (f) * Prove that if $(d_1, d_2, \dots, d_9, d_{10})$ is a valid ISBN-10 code, then $(d_{10}, d_9, \dots, d_2, d_1)$ is also a valid ISBN-10 code (as long as d_{10} is not equal to X).
- (g) (*for geeks*) Write a computer program or Excel spreadsheet that calculates the check digit for the first nine digits of an ISBN code.
- (h) A publisher has houses in Germany and the United States. Its German prefix is 3-540. Its United States prefix will be 0-*abc*. Find four possibilities for *abc* such that the rest of the ISBN code will be the same for a book printed in Germany and in the United States.

- (i) **Prove that the ISBN-10 code detects all single digit errors. (*Hint*)
- (j) **Prove that the ISBN-10 code detects all transposition errors. (*Hint*)

◇

5.3.2 Solving modular equations

In Exercise 5.3.2 part (h) you solved a modular equation with three variables by trial and error: you couldn't solve for one variable at a time, so you had to test out sets of values for a , b , c together and see if the the ISBN equation held. The UPC and ISBN error detection schemes themselves, given again below, are examples of modular equations with 12 and 10 variables, respectively:

$$(3 \cdot d_1) + (1 \cdot d_2) + (3 \cdot d_3) + \cdots + (3 \cdot d_{11}) + (1 \cdot d_{12}) \equiv 0 \pmod{10}.$$

$$(d_1, d_2, \dots, d_{10}) \cdot (10, 9, \dots, 1) \equiv 0 \pmod{11}.$$

Can the above equations be solved? You may remember from college algebra that a single equation with several variables usually has several solutions. If we want to narrow it down to a single solution we have to supply additional information, as in the following exercise.

Exercise 5.3.3. Suppose you're given the following UPC: 1-54637-28190-?. Write a modular equation to solve for the missing check digit, then solve it. ◇

In the preceding exercise you should have come up with an equation that looks like:

$$(3 \cdot 1) + \dots + (3 \cdot 0) + (1 \cdot x) \equiv 0 \pmod{10}.$$

How did you solve this? One possible method is to add up all the terms the left side of the equation short of the variable, and then figure out how much you need to add to that sum to get a number divisible by 10. Keep this method and your own method (if different) in mind, as they are good intuition on how to solve these problems in general.

Is there a *unique* answer for x ? Practically, for a UPC code x must be between 0 and 9 (that is, $x \in \mathbb{Z}_{10}$: with this restriction, there is indeed only

one solution. But if we remove that restriction, then there are many solutions. For instance $x = 12$ and $x = 22$ both work (check this for yourself). Can you think of any other integers that work?

In fact any integer equivalent to $2 \pmod{10}$ also works. But from our intuitive methods, would we have come up with these other possible solutions? In most cases not. Therefore we need to come up with a general method that will give us all possible integer solutions of a modular equation. Just as in basic algebra, we'll start with simpler equations and move to more complicated ones.

Example 5.3.4. Let's start with a basic modular equation involving addition:

$$8 + x \equiv 6 \pmod{11}$$

From algebra we understand how to solve an equation with an $=$ sign, but what do we do with this \equiv sign? In fact, we can turn it in to an $=$ sign by using Proposition 5.2.10, which says that $8 + x \equiv 6 \pmod{11}$ means the same as:

$$8 + x = k \cdot 11 + 6$$

And then we can solve for x like any other equation. The result is

$$x = k \cdot 11 - 2$$

So we solved for x , but what numbers does x actually equal? What does $k \cdot 11 - 2$ mean? k is an integer, therefore x can equal -2 (if $k = 0$), or -13 (if $k = -1$), or 9 (if $k = 1$), and so on. In other words x equals -2 plus any integer multiple of 11 , which, by the definition of modular equivalence, means

$$x \equiv -2 \pmod{11}$$

This is a correct solution: but it's not the only way to write it. It would be just as valid to write

- $x \equiv -13 \pmod{11}$
- $x \equiv 20 \pmod{11}$
- $x \equiv 130 \pmod{11}$
- ...

Notice however that there is only one way to write the solution in terms of a number in \mathbb{Z}_{11} , namely:

$$\text{mod}(x, 11) = 9$$

In order to avoid ambiguity, mathematicians and textbooks always write solutions mod n in terms of numbers in \mathbb{Z}_n . In our current example, it's easy enough to obtain the standard solution ($x \equiv 9 \pmod{11}$) directly from the equation $x = k \cdot 11 - 2$? by taking one of the 11's and adding it to the -2 to get

$$x = (k - 1) \cdot 11 + 11 - 2 = (k - 1) \cdot 11 + 9.$$

Since k is an arbitrary integer, $k - 1$ is also an arbitrary integer. So we get $x \equiv 9 \pmod{11}$.



To summarize our general method for solving modular equations so far:

1. Turn the \equiv sign into an $=$ sign using the definition of modular equivalence. This introduces an additional variable k .
2. Find (by trial and error if necessary) the value of k that puts x in the appropriate range.
3. Change the equation back into an equivalence.

Exercise 5.3.5. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

(a) $5 + x \equiv 1 \pmod{3}$

(b) $25 + x \equiv 6 \pmod{12}$



Now let's spice things up with some multiplication:

Example 5.3.6. Given the equation

$$5x + 3 \equiv 9 \pmod{11}.$$

Using the definition of modular equivalence, this becomes

$$5x + 3 = 11k + 9.$$

Solving this equality using basic algebra gives us

$$x = \frac{11k + 6}{5}.$$

Now remember that x must be an *integer*. In order for the right side to be an integer, we need to find a k that makes $\frac{11k+6}{5}$ an integer. At this point we may use trial and error to find a k in \mathbb{Z}_5 such that $11 \cdot k + 6$ is a multiple of 5. We get $k = 4$; and in fact adding $5 \cdot n$ to 4 also works for any $n \in \mathbb{Z}$, since $5n$ is always divisible by 5. Now we can solve for x by substituting $k = 4 + 5n$ back in to the previous equation:

$$\begin{aligned} x &= \frac{11(4 + 5 \cdot n) + 6}{5} \\ &= \frac{11 \cdot 4 + 6}{5} + \frac{11 \cdot (5n)}{5} \\ &= 10 + 11n \end{aligned}$$

Therefore $x \equiv 10 \pmod{11}$ is the general solution. You may check (which is always a good idea!) by plugging $10 + 11n$ for a couple values of n back into the original equation, and you'll see these numbers work. \blacklozenge

Just to make sure you've mastered the process, we'll give another example:

Example 5.3.7. To solve the equation $4x + 5 \equiv 7 \pmod{11}$ we proceed step by step (note that the symbol \Rightarrow is mathematicians' shorthand for "implies"):

$$\begin{aligned} 4x + 5 &\equiv 7 \pmod{11} \\ \Rightarrow 4x + 5 &= 11k + 7 && \text{(by modular equivalence)} \\ \Rightarrow x &= \frac{11k + 2}{4} && \text{(basic algebra)} \end{aligned}$$

Now, $11k + 2$ is a multiple of 4 when $k = 2$, as well as when k equals 2 plus any multiple of 4. Therefore $k = 2 + 4n$, hence we may continue from the previous equation:

$$\begin{aligned}
 x &= \frac{2 + 11k}{4} \\
 \Rightarrow x &= \frac{2 + 11 \cdot (2 + 4n)}{4} && \text{(substitution)} \\
 \Rightarrow x &= 6 + 11n. && \text{(simplification)}
 \end{aligned}$$

Therefore $x \equiv 6 \pmod{11}$ is the general solution. \blacklozenge

Remark 5.3.8. Example 5.3.7 demonstrates some good practices that you can make use of when you write up your own proofs:

- Instead of using a sentence to explain your reasoning for each step, place the reason to the right in parentheses. This shrinks down the size of the proof.
- Another way to shrink the proof is to use mathematical equations, expressions, and symbols (such as \Rightarrow , \forall) whenever you can to accurately communicate your steps in the proof.

\triangle

In summary, a general method for solving modular equations is:

1. Turn the \equiv sign into an $=$ sign using the definition of modular equivalence (just as with modular addition). This introduces another constant k .
2. Solve the resulting equation for your variable x . If the expression is not a fraction, then go to step 5. Otherwise, go to step 3.
3. By trial and error, find a value k_0 for k which makes the fraction into an integer.
4. Substitute $k_0 + n \cdot (\text{denominator})$ in for k , and simplify.
5. Change the equation back into an equivalence.

Exercise 5.3.9. Find all $x \in \mathbb{Z}$ satisfying each of the following equations. (If there's no solution, then you can say "no solution"—but show why!)

- (a) $9x \equiv 3 \pmod{5}$ (f) $27x \equiv 2 \pmod{9}$
(b) $5x \equiv 1 \pmod{6}$ (g) $3 + x \equiv 2 \pmod{7}$
(c) $7x \equiv 9 \pmod{13}$ (h) $5x + 1 \equiv 13 \pmod{23}$
(d) $8x \equiv 4 \pmod{12}$ (i) $5x + 1 \equiv 13 \pmod{26}$
(e) $11x \equiv 2 \pmod{6}$ (j) $3x + 2 \equiv 1 \pmod{6}$

◇

One major disadvantage of our solution method is the use of trial and error in step 3. If large numbers are involved, then this step can take a long time. However, there are techniques to speed things up:

Example 5.3.10. Consider the equation $79x \equiv 9 \pmod{15}$. In Section 5.2 we mentioned that when we're doing arithmetic mod n , we can replace any number with its remainder mod n without changing the answer. In this example then, we can replace the 79 with its remainder mod 15, which is 4. Thus we have

$$4x \equiv 9 \pmod{15},$$

which leads to

$$x = \frac{15k + 9}{4}.$$

By rewriting the numerator, we can simplify the right-hand side:

$$x = \frac{(12k + 3k) + (8 + 1)}{4} = 3k + 2 + \frac{3k + 1}{4}.$$

and we readily discover that $k = 1 + 4n$ makes the right-hand side an integer, so that

$$x = \frac{15 \cdot (1 + 4n) + 9}{4} = 6 + 15n, \text{ or } x \equiv 6 \pmod{15}.$$

◆

Here's another example, which is just a little more complicated.

Example 5.3.11. To solve the equation $447x + 53 \equiv 712 \pmod{111}$ we proceed as follows:

$$\begin{aligned}
 447x + 53 &\equiv 712 \pmod{111} \\
 \Rightarrow 447x &\equiv 659 \pmod{111} && \text{(subtract 53 from both sides)} \\
 \Rightarrow 3x &\equiv 104 \pmod{111} && \text{(modular equivalence)} \\
 \Rightarrow 3x &= 104 + 111k && \text{(basic algebra)} \\
 \Rightarrow x &= \frac{104 + 111k}{3} && \text{(basic algebra)} \\
 \Rightarrow x &= 34 + \frac{2}{3} + 37k && \text{(basic algebra)}
 \end{aligned}$$

It should be clear that no value of k makes the right side an integer. Hence x has no solution. You may have run into a similar situation in a previous exercise. \blacklozenge

Exercise 5.3.12. Find all $x \in \mathbb{Z}$ satisfying each of the following equations.

- | | |
|---|---|
| (a) $112x \equiv 2 \pmod{6}$ | (f) $469x + 122 \equiv 1321 \pmod{231}$ |
| (b) $74x \equiv 9 \pmod{13}$ | (g) $246x + 200 \equiv 401 \pmod{81}$ |
| (c) $856x \equiv 4 \pmod{123}$ (*Hint*) | (h) $339 + 411x \equiv 2 \pmod{297}$ |
| (d) $272x \equiv 24 \pmod{9}$ | (i) $530x - 183 \equiv 215 \pmod{128}$ |
| (e) $242x + 39 \equiv 489 \pmod{236}$ | |

\blacklozenge

From parts (h) and (i) of Exercise 5.3.12 we see that even our trick with modular equivalences doesn't make all modular equations easy to solve. When the coefficient of x and the modulus are both large, you may end up needing *lots* of trial and error. Such "brute force" methods are rather distasteful to snobby mathematicians, who prefer "elegant" solutions. Later we'll talk about an "elegant" method (the Euclidean algorithm) that solves modular equations without any trial and error whatsoever.

5.4 The integers mod n (a.k.a. \mathbb{Z}_n)

5.4.1 Remainder arithmetic

Several times now in this chapter we've simplified our modular calculations by replacing numbers with their remainders mod n (remember, we have defined these remainders as the set \mathbb{Z}_n). We will now fulfill the promise we made at the end of the first section by proving that if you replace numbers with their remainders, we don't change the result of our modular calculations. That is, we'll show that modular arithmetic can be thought of as arithmetic on the remainders, or "remainder arithmetic" (as opposed to "integer arithmetic" or "complex arithmetic" which we're already familiar with).

Before we do this, we need to address an important issue. Consider the case of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, so 3 and 4 are in \mathbb{Z}_5 . However the sum $3 + 4$ is 7, which is not in \mathbb{Z}_5 . If we're going to do arithmetic with the remainders, we should define a "sum" on \mathbb{Z}_n such that the result is also in \mathbb{Z}_n . This motivates the following two definitions:

Definition 5.4.1. Modular Addition

The sum mod n of two remainders mod n is the remainder left after dividing their regular sum by n ; that is, if $a, b \in \mathbb{Z}_n$ then

$$a \oplus b = r \text{ iff } a + b = r + sn \text{ and } r \in \mathbb{Z}_n.$$

△

Note that in Definition 5.4.1 we write $a \oplus b = r$ rather than $a \oplus b \equiv r \pmod{n}$, since $a \oplus b$ is defined to be *equal* to the remainder. The same holds for the following definition:

Definition 5.4.2. Modular Multiplication

The product mod n of two remainders mod n is the remainder left after dividing their regular product by n ; that is, if $a, b \in \mathbb{Z}_n$ then

$$a \odot b = r \text{ iff } a \cdot b = r + sn \text{ and } r \in \mathbb{Z}_n.$$

△

Before we continue, we should take special note of the following important points.

Remark 5.4.3.

- It is important to note that the operations \oplus and \odot *depend on the modulus involved*. We must always make sure that the modulus is clearly specified before talking about \oplus and \odot .
- Although technically we could define $\ell \oplus m$ and $\ell \odot m$ for *any* two integers $\ell, m \in \mathbb{Z}$, in the following we will restrict the operations to elements of \mathbb{Z}_n . So for example if we are working in \mathbb{Z}_7 , we may write $3 \oplus 4 = 0$ and $5 \odot 6 = 2$, but we won't write expressions like $7 \oplus 6$ or $13 \odot 22$.

△

Our first step towards showing that ordinary arithmetic can be replaced with arithmetic with remainders is the following proposition:

Proposition 5.4.4. Given $\ell, m \in \mathbb{Z}$.

- (a) $\text{mod}(\ell + m, n) = \text{mod}(\ell, n) \oplus \text{mod}(m, n)$,
 (b) $\text{mod}(\ell \cdot m, n) = \text{mod}(\ell, n) \odot \text{mod}(m, n)$.

Before we prove Proposition 5.4.4, let's give an example of how it can be applied. Suppose we want to compute the following remainders:

$$\text{mod}(8640 + 1059895, 7) \quad \text{and} \quad \text{mod}(8640 \cdot 1059895, 7).$$

OK, let's apply the proposition. If we let $\ell = 8640$, $m = 1059895$ and $n = 7$, then we have the following correspondence

$$\text{mod}(\ell + m, n) \rightarrow \text{mod}(8640 + 1059895, 7)$$

By division we may compute $\text{mod}(8640, 7) = 2$ and $\text{mod}(1059895, 7) = 4$. This gives us the correspondence:

$$\text{mod}(\ell, n) \rightarrow 2; \quad \text{mod}(m, n) \rightarrow 4.$$

Using these correspondences, Proposition 5.4.4 gives us immediately that

$$\text{mod}(8640 + 1059895, 7) = 2 \oplus 4, \quad \text{and} \quad \text{mod}(8640 \cdot 1059895, 7) = 2 \odot 4,$$

which gives us 6 and 1 for the sum and product, respectively. Isn't this an awful lot simpler than adding and multiplying those two large numbers?

So let's get back to the proof. We'll do (a) here: part (b) is left as an exercise.

PROOF. For simplicity we let $a := \text{mod}(\ell, n)$ and $b := \text{mod}(m, n)$. Then according to the definition of remainder mod n we have

$$\ell = a + sn \quad \text{and} \quad m = b + tn.$$

Adding these two equations (which is basically substitution) and basic algebra we find

$$\ell + m = a + b + (s + t)n$$

Now by the definition of \oplus , there is some $p \in \mathbb{Z}$ such that $a + b = (a \oplus b) + pn$; therefore

$$\ell + m = (a \oplus b) + pn + (s + t)n = (a \oplus b) + (p + s + t)n. \quad (\text{subs. and basic algebra})$$

Hence by the definition of modular equivalence,

$$\ell + m \equiv a \oplus b \pmod{n}.$$

Now since $a \oplus b$ is between 0 and $n - 1$ by definition, it follows from Proposition 5.2.8 that

$$\text{mod}(\ell + m, n) = a \oplus b.$$

Recalling the definitions of a and b above we get finally:

$$\text{mod}(\ell + m, n) = \text{mod}(\ell, n) \oplus \text{mod}(m, n),$$

and we're finished! □

Exercise 5.4.5.

(a) Prove part (b) of Proposition 5.4.4.

(b) Come up with a definition for modular subtraction (use the symbol \ominus).

(c) Using your definition, prove the following:

Given $\ell, m \in \mathbb{Z}$. If $a = \text{mod}(\ell, n)$ and $b = \text{mod}(m, n)$, then $\text{mod}(\ell + m, n) = a \oplus b$.

◇

The diagram in Figure 5.4.1 gives a way to visualize Proposition 5.4.4. In the diagram we only show the relation between $+$ and \oplus ; the situation with \cdot and \odot is similar. On the left side of the diagram, we show two numbers ℓ and m being added to give $\ell + m$. The arrows from left to right show that the numbers ℓ, m , and $\ell + m$ can all be “translated” by taking remainders. If we “translate” ℓ and m first and then take the modular sum; or we can take $\ell + m$ first and then “translate” the result. In either case, we end up with the same answer.

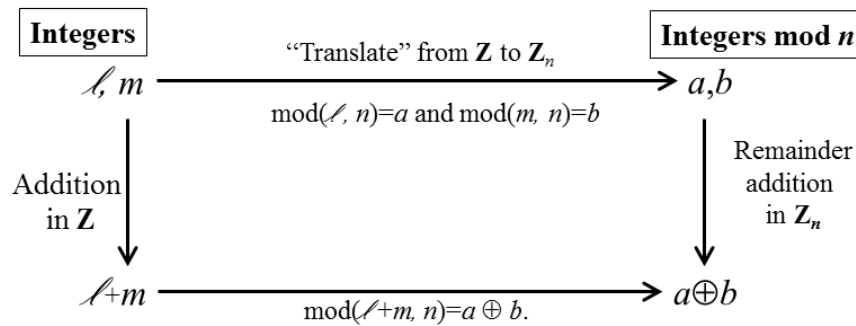


Figure 5.4.1. Visualization of Proposition 5.4.4.

Exercise 5.4.6. Make a diagram similar to Figure 5.4.1 for modular multiplication instead of modular addition. ◇

Now that we’ve proven Proposition 5.4.4, we can combine operations into more complicated expressions and show equivalence.

Exercise 5.4.7.

(a) Using part (b) of Proposition 5.4.4 above, show that if $\ell \in \mathbb{Z}$ and $a = \text{mod}(\ell, n)$ then $\text{mod}(\ell^2, n) = a \odot a$. (*Hint*)

- (b) Using part (a) prove a similar relation involving ℓ^3 .
- (c) Using part (b) prove a similar relation involving ℓ^4 .
- (d) From parts (a),(b) and (c), what do you infer about ℓ^k where k is any natural number? (Note that to actually *prove* this fact requires the use of induction.)

◇

Exercise 5.4.8. Given $\ell, m, p \in \mathbb{Z}$ and $a = \text{mod}(\ell, n)$, $b = \text{mod}(m, n)$, and $c = \text{mod}(p, n)$. Show the following equivalences using Proposition 5.4.4.

- (a) $\text{mod}((\ell + m) + p, n) = (a \oplus b) \oplus c.$ (*Hint*)
- (b) $\text{mod}((\ell + (m + p)), n) = a \oplus (b \oplus c).$
- (c) $\text{mod}((\ell \cdot m) \cdot p, n) = (a \odot b) \odot c.$
- (d) $\text{mod}((\ell \cdot m) + p, n) = (a \odot b) \oplus c.$
- (e) $\text{mod}((\ell + m) \cdot p, n) = (a \oplus b) \odot c.$

◇

We can use similar methods as in Exercise 5.4.8, to show that *any* arithmetical expression involving integers with no matter how many additions, multiplications, and subtractions, can be shown to be equivalent mod n to the corresponding arithmetical expression in \mathbb{Z}_n using the modular operations \oplus, \odot, \ominus .

This completes our discussion showing that arithmetic mod n can be reduced to arithmetic in \mathbb{Z}_n . What we've shown can simplify other modular arithmetic arguments as well:

Exercise 5.4.9. Use Proposition 5.4.4 twice and the first definition of modular equivalence (Definition 5.2.6) to prove the following propositions. (It is also possible to prove these propositions directly from the definitions, but the point of this exercise is to look at the proof from a different perspective.)

Proposition: Given $\ell, m, x, y \in \mathbb{Z}$ where $\ell \equiv x \pmod{n}$ and $m \equiv y \pmod{n}$, then

- (a) $\ell + m \equiv x + y \pmod{n}$,
 (b) $\ell \cdot m \equiv x \cdot y \pmod{n}$.

◇

This proposition shows that we can freely replace numbers in arithmetic expressions involving $+$ and \cdot with other numbers that are equivalent mod n , as long as we're only interested in the result mod n . For example, suppose we want to find the following remainder:

$$\text{mod}(80056 \cdot 69944, 56).$$

We may notice that $80056 \equiv 80000 \pmod{56}$ and $69944 \equiv 70000 \pmod{56}$. So we can replace 80056 with 80000 and 69944 with 70000 in the computation:

$$\text{mod}(80000 \cdot 70000, 56) = \text{mod}(5600000000, 56) = 0.$$

By noticing some patterns we were able to save ourselves quite a bit of work.

Note that we were careful to specify that replacement with modular equivalents works in modular equations that involve addition and/or multiplication. It does *not* work for integer exponents. For example, it is not true that $2^1 \equiv 2^4 \pmod{3}$, even though $1 \equiv 4 \pmod{3}$. It turns out that exponents can be replaced with simpler exponents in modular equivalences, but we won't find out how this works until Section 18.3.2 (if you want to look ahead!)

Exercise 5.4.10. Prove or disprove, using the proposition in Exercise 5.4.9:

- (a) $7787 \cdot 21005 \cdot 495 \equiv 56002 \cdot 492 \cdot 213 \pmod{7}$
 (b) $(12345 \cdot 6789) + 1357 \equiv (98765 \cdot 13579) + 9876 \pmod{10}$
 (c) $(4545 \cdot 5239) + 1314 \equiv (7878 \cdot 3614) + 4647 \pmod{101}$
 (d) $765432121234567 \cdot 234567878765432 \equiv 456456456456456456 \cdot 789789789789789789789 \pmod{10}$
 (e) $543254325432543254325432^3 \equiv 12121212121212121212^7 \pmod{10}$
 (f) $786786786786786786786^3 \equiv 456456456456456456456^4 \pmod{10}$
 (g) $654321^{87654321} \equiv 123456^{12345678} \pmod{5}$

◇

5.4.2 Cayley tables for \mathbb{Z}_n

The fact that we can replace integers with their remainders mod n leads us to a simpler way of thinking about modular arithmetic. First, recall the integer number line, pictured (again) in Figure 5.4.2: We may relabel

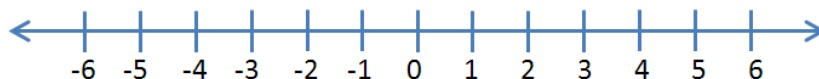


Figure 5.4.2. The usual number line

the integers with their remainders mod 5, pictured in Figure 5.4.3: All the

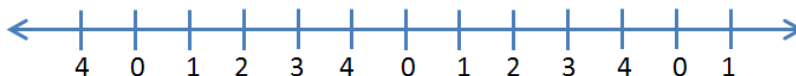


Figure 5.4.3. The number line mod 5

numbers equivalent to 0 mod 5 are labeled 0; all the numbers equivalent to 1 mod 5 are labeled 1; and so on. The whole infinite set of integers then is reduced to repetitive cycles of the integers 0 through 4. In other words, all the integers are equivalent to either 0, 1, 2, 3, or 4, mod 5.

Furthermore, as we just discussed, the sum and product mod 5 of any two numbers is exactly equivalent to the sum and product mod 5 of their corresponding remainders. Therefore, the sum or product of *any* two numbers mod 5 can be determined by the sum or product of the integers 0 – 4. So we only have to focus on the sums and products of these five numbers to get the result of any modular calculation mod 5.

So let's calculate these sums and products. We are only using the remainders for mod 5 (recall we have already defined this set as \mathbb{Z}_5). The following table then gives the results of addition mod 5 for \mathbb{Z}_5 :

As an example of how to read this table, the entry in the “2” row and the “3” column is 0, which tells us that $2 \oplus 3 = 0$ (remember, this result depends on fact that we're working in mod 5).

The following table gives the results of multiplication mod 5 for \mathbb{Z}_5 :

| \oplus | 0 | 1 | 2 | 3 | 4 |
|----------|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

Table 5.1: Addition table for \mathbb{Z}_5

| \odot | 0 | 1 | 2 | 3 | 4 |
|---------|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 |
| 2 | 0 | 2 | 4 | 1 | 3 |
| 3 | 0 | 3 | 1 | 4 | 2 |
| 4 | 0 | 4 | 3 | 2 | 1 |

Table 5.2: Multiplication table for \mathbb{Z}_5

Again, looking at the entry in the "2" row and the "3" column we see 1, which tells us that $2 \odot 3 = 1$.

Similarly, for each set of numbers \mathbb{Z}_n we can construct a table to determine the result of any possible calculation mod n . Tables like these are known as **Cayley tables**.⁸ We will see them often throughout the course.

Exercise 5.4.11. Use the above Cayley tables for \oplus and \odot in \mathbb{Z}_5 to calculate each of the following. (Remember, compute the remainders *before* doing the arithmetic.)

- (a) $\text{mod}(456 \cdot (252 + 54), 5)$
- (b) $\text{mod}(523 + (4568 \cdot (43 + 20525)), 5)$
- (c) $\text{mod}((456 \cdot 252) + (456 \cdot 54), 5)$
- (d) $\text{mod}(523 + ((4568 \cdot 43) + (4568 \cdot 20525)), 5)$

◇

Later on (in the chapter on Equivalence Relations) we'll show another way of looking at the integers mod n .

⁸Technically, this kind of operation table is only called a "Cayley table" if the operation satisfies the "group properties" (see Section 5.4.7).

5.4.3 Closure properties of \mathbb{Z}_n

Let's look a little further into the arithmetic properties of the numbers \mathbb{Z}_n that we've just defined.

Example 5.4.12. To start exploring, first consider \mathbb{Z}_8 . Tables 5.3 and 5.4 are the addition and multiplication tables for \mathbb{Z}_8 , respectively.

| \oplus | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|----------|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

Table 5.3: Addition table for \mathbb{Z}_8

| \odot | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---------|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Table 5.4: Multiplication table for \mathbb{Z}_8



There is an important feature exhibited in both Table 5.3 and Table 5.4 that is easy to overlook. Notice that every entry in the table is also an element of \mathbb{Z}_8 . You can think of the set $\{0, \dots, 7\}$ as a closed box, and when you add or multiply any two numbers in that box mod 8, you always get another number in that box, never outside of it (indeed because addition and multiplication mod 8 return a remainder that is some number 0-7). We express this mathematically by saying that \mathbb{Z}_8 is **closed** under addition and

multiplication mod 8. (Alternatively we may say: addition and multiplication mod 8 have the property of *closure*.) It seems reasonable that the same should be true for any \mathbb{Z}_n , and we state this formally as a proposition (as mathematicians are wont to do):

Proposition 5.4.13. \mathbb{Z}_n is closed under modular addition and multiplication, for all positive integers n .

Exercise 5.4.14. Prove Proposition 5.4.13. That is, show that the modular sum and modular product of two elements of \mathbb{Z}_n are also in \mathbb{Z}_n . (*Hint*) \diamond

In general closure is not hard to prove (when it's true), but it should not be taken for granted. There are many examples of number systems that are not closed under various operations. For instance, the positive integers are not closed under the operation of subtraction, because (for example) $5 - 7$ is not a positive integer. Similarly, the positive integers are not closed under the operation of square root, because the square root of 2 is not an integer.

Exercise 5.4.15. For each of the following number systems, state whether or not they are closed under (i) addition (ii) subtraction (iii) multiplication (iv) division (v) square root. In cases where closure holds you can simply state the fact (no proof is necessary). In cases where closure doesn't hold, give a counterexample. For example, we know that the negative real numbers are not closed under square root because $\sqrt{-1}$ is not a negative real number. (*Hint*)

- | | |
|--------------------------|-----------------------------------|
| (a) The integers | (d) The positive rational numbers |
| (b) The rational numbers | (e) The positive real numbers |
| (c) The real numbers | (f) The nonzero real numbers |

\diamond

Exercise 5.4.16. Prove that the complex numbers are closed under complex addition and multiplication. \diamond

5.4.4 Identities and inverses in \mathbb{Z}_n

Next, we want to look at some additional properties that were introduced in Chapter 4, namely identities and inverses (both additive and multiplicative). This time we'll go through these properties more quickly.

Consider first the additive identity. Remember that an additive identity is an element which, when added to any other element a , gives a result of a . For the specific case of \mathbb{Z}_8 , we can see from the first row of Table 5.3 that $0 \oplus a = a$ for any $a \in \mathbb{Z}_8$. Similarly, the first column of Table 5.3 show that $a \oplus 0 = a$ for any $a \in \mathbb{Z}_8$.

Is 0 an additive identity for *any* \mathbb{Z}_n ? Not surprisingly, the answer is Yes:

Proposition 5.4.17. $0 \in \mathbb{Z}_n$ is the additive identity of \mathbb{Z}_n .

PROOF. Given any $a \in \mathbb{Z}_n$, then $a \oplus 0$ is computed by taking the remainder of $a+0 \bmod n$. Since $a+0 = a$, and $0 \leq a < n$, it follows that the remainder of a is still a . Hence $a \oplus 0 = a$. Similarly we can show $0 \oplus a = a$. Thus 0 satisfies the definition of identity for \mathbb{Z}_n . \square

Exercise 5.4.18. Give a similar proof that 1 is the multiplicative identity for \mathbb{Z}_n when $n > 1$. What is the multiplicative identity for \mathbb{Z}_n when $n = 1$? \diamond

5.4.5 Inverses in \mathbb{Z}_n

Now let's find out whether the integers mod n have additive and multiplicative inverses. Additive inverse first: for each element of \mathbb{Z}_n is there a corresponding element of \mathbb{Z}_8 such that their modular sum is the additive identity (that is, 0)? You may see in Table 5.3 that each row of the addition table contains a 0 (e.g. $1 \oplus 7 = 0$). It follows that each element of \mathbb{Z}_8 has an additive inverse. But will the same be true for \mathbb{Z}_{27} , or \mathbb{Z}_{341} , or \mathbb{Z}_{5280} ? We can't just take this for granted—we need to give a proof:

Proposition 5.4.19. Let \mathbb{Z}_n be the integers mod n and $a \in \mathbb{Z}_n$. Then for every a there is an additive inverse $a' \in \mathbb{Z}_n$.

In other words: for any $a \in \mathbb{Z}_n$ in we can find an a' such that:

$$a \oplus a' = a' \oplus a = 0.$$

We structure the proof of Proposition 5.4.19 as an exercise. We prove the two cases $a = 0$ and $a \neq 0$ separately.

Exercise 5.4.20.

- (a) Show that $0 \in \mathbb{Z}_n$ has an additive inverse in \mathbb{Z}_n .
- (b) Suppose a is a nonzero element of \mathbb{Z}_n (in mathematical shorthand, we write this as: $a \in \mathbb{Z}_n \setminus \{0\}$), and let $a' = n - a$.
- (i) Show that a' is in \mathbb{Z}_n . (*Hint*)
 - (ii) Show that $a \oplus a' = a' \oplus a = 0 \pmod{n}$: that is, a' is the additive inverse of a .

◇

That takes care of additive inverse. What about multiplication? That is, no matter what n is, given $a \in \mathbb{Z}_n$ is there always another element of \mathbb{Z}_n which multiplies to give the multiplicative identity?

Before attempting to prove this, first let's see if it's true in \mathbb{Z}_8 . Consider the multiplication table for \mathbb{Z}_8 in Table 5.4. We find that rows 0, 2, 4, and 6 do not contain a 1. This means that for $a = 0, 2, 4,$ or 6 , there's no $b \in \mathbb{Z}_8$ such that $a \odot b \equiv 1 \pmod{8}$. So 0, 2, 4, and 6 have no multiplicative inverses in \mathbb{Z}_8 .

Actually, it's not too hard to see that 0 *never* has a multiplicative inverse for any \mathbb{Z}_n (why?). This means that it's impossible to prove a multiplicative version of Proposition 5.4.19, since we have a **counterexample** that shows that not every element of \mathbb{Z}_n has an inverse, no matter what n is.

Remark 5.4.21. This example shows that it's often easier to *disprove* something than to prove it! To disprove a general statement, you only need to find *just one* counterexample, whereas an unlimited number of examples can never prove a general statement. △

But all is not lost as far as multiplicative inverses are concerned. We'll see later that they play a very important role when we consider arithmetic with the *nonzero* elements of \mathbb{Z}_n :

Exercise 5.4.22.

- (a) Find an integer $n > 2$ such that all *nonzero* elements of \mathbb{Z}_n have multiplicative inverses.
- (b) Find two additional values of $n > 5$ such that all nonzero elements of \mathbb{Z}_n have multiplicative inverses.
- (c) What do the three numbers you found in (a) and (b) have in common?

◇

5.4.6 Other arithmetic properties of \oplus and \odot

In many respects, \oplus and \odot are very similar to the ordinary arithmetic operations $+$ and \cdot . It makes sense that they too should be associative, distributive, and commutative (recall these properties were defined in Section 3.2.1). But as mathematicians, it's not enough for something to "make sense"—we need solid proof. So let's buckle down and crank out some proofs.

Proposition 5.4.23. In the following n is an arbitrary positive integer and a, b, c denote arbitrary elements of \mathbb{Z}_n .

- (a) Modular addition and multiplication are commutative:

$$\begin{aligned}a \oplus b &= b \oplus a \\ a \odot b &= b \odot a.\end{aligned}$$

- (b) Modular addition and multiplication are associative:

$$\begin{aligned}(a \oplus b) \oplus c &= a \oplus (b \oplus c) \\ (a \odot b) \odot c &= a \odot (b \odot c).\end{aligned}$$

- (c) Modular multiplication distributes over modular addition:

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c).$$

PROOF. We'll prove associativity, and you'll prove the other parts as exercises (the proofs are pretty similar). The proof strategy is familiar: we'll prove modular arithmetic properties by making use of the corresponding properties of ordinary arithmetic.

Modular addition is associative: Given a, b, c are elements of \mathbb{Z}_n , we may apply part (a) of Exercise 5.4.8 and get

$$\text{mod}((a + b) + c, n) = (a \oplus b) \oplus c.$$

Similarly, we may apply part (b) of Exercise 5.4.8 to get

$$\text{mod}(a + (b + c), n) = a \oplus (b \oplus c).$$

Now here's where we use regular arithmetic. The associative property of integer addition tells us that $(a + b) + c = a + (b + c)$, so the left-hand sides are equal. So $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, and the proof is complete. \square

Exercise 5.4.24. Explain the step in the above proof where we used part (a) of Exercise 5.4.8 to conclude that $\text{mod}((a+b)+c, n) = (a \oplus b) \oplus c$. What values are we using for ℓ, m, p , and why is it OK to use these values? \diamond

Exercise 5.4.25.

- (a) Prove that addition mod n is commutative.
- (b) Prove that multiplication mod n is commutative.
- (c) Prove that multiplication mod n is associative.
- (d) Prove part (c) of Proposition 5.4.23.

\diamond

5.4.7 Group: a central concept in abstract algebra

It's time for us to make a confession. We have an ulterior motive. We've been spending lots of time and effort discussing modular arithmetic because it provides good examples of one of the central concepts in abstract algebra, namely the notion of a *group*.

Notice that the set \mathbb{Z}_n with the operation of \oplus has an identity, and inverses, and the property of closure. Furthermore, \mathbb{Z}_n is associative under \oplus , as we just showed. Any combination of a set and an operation that has those three properties, as well as the associative property, is called a *group*. Here's the formal definition:

Definition 5.4.26. A *group* is a set combined with an operation that has the following properties:

- *Closure*: the set is closed under the operation;
- *Identity*: the set has an identity element for the operation;
- *Inverse*: every element of the set has an inverse under the operation;
- *Associative*: the operation is associative.

△

Notice that we do *not* include the commutative property in this list. Later on we'll see examples of groups that are *not* commutative. Groups that do have the commutative property are called ***abelian groups***.

Now that we've defined groups, in retrospect we may look back and see that we've encountered groups before. In fact, we've been working with groups since the very beginning of the book!

Exercise 5.4.27. For each of the following sets of numbers, determine which of the four group properties holds, using the operation of addition. If a property does *not* hold, give a specific counterexample which shows that the property is false. State also whether or not each set is a group.

- (a) Integers; (b) Positive integers; (c) Rational numbers; (d) Real numbers; (e) Complex numbers. ◇

We've shown several examples of group under the operation of addition ($+$ or \oplus). But what about multiplication? With multiplication, things turn out quite differently.

Exercise 5.4.28. For each of the following sets of numbers, determine which of the four group properties holds, using the operation of multiplication. If a property does *not* hold, give a specific counterexample which shows that the property is false. State also whether or not each set is a group.

- (a) Integers; (b) Positive integers; (c) Rational numbers; (d) Real numbers; (e) Complex numbers. ◇

Based on our experience with the previous exercise, we may generalize:

Exercise 5.4.29.

- (a) Explain why it is *impossible* for any set of (real or complex) numbers which contains both 0 and 1 to be a group under the operation of multiplication.
- (b) Explain why \mathbb{Z}_n is *not* a group under \odot for any $n > 1$.

◇

We've seen in Exercise 5.4.29 that 0 causes a problem for multiplication, as far as making groups is concerned. But what if we remove 0 from the set? We may have better luck:

Exercise 5.4.30.

- (a) Show that the nonzero elements of \mathbb{Z}_3 is a group under \odot .
- (b) Can you find an $n > 3$ such that the nonzero elements of \mathbb{Z}_n do *not* form a group under \odot ? If so, tell which n , and explain why \mathbb{Z}_n fails to be a group in this case.

◇

Now that you know what a group is, we'll be referring back to this definition fairly frequently throughout the rest of the book. In particular, we'll be saying a lot more about multiplicative groups, which turn out to be somewhat more intricate (and more interesting) than additive groups.

5.5 Modular division

Before getting to modular division, we'll look at something else first. This all may seem irrelevant, but please be patient: we'll get to the point soon enough.

5.5.1 A sticky problem

The following problem may not seem to have anything to do with modular arithmetic, but it's an interesting problem and fun to think about. (And it turns out to be relevant after all!)⁹

Example 5.5.1. Someone gives us a pencil and two unmarked sticks of lengths 52 cm and 20 cm respectively (see Figure 5.5.1). We are told to

⁹This section is by David Weathers, edited by C.T.

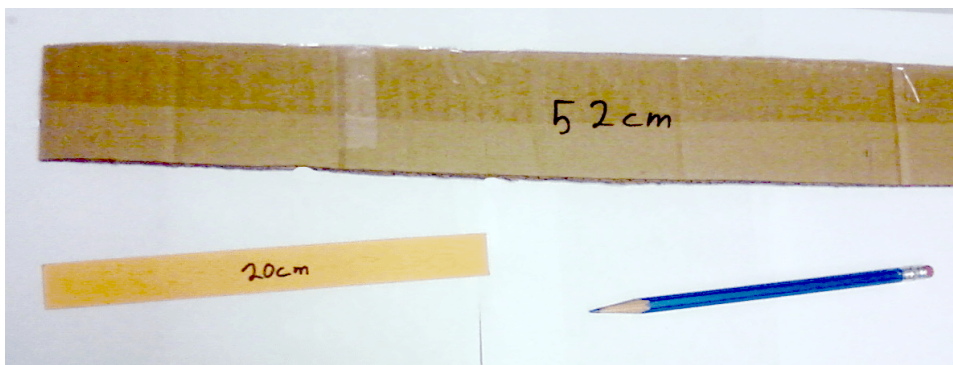


Figure 5.5.1. Two sticks



Figure 5.5.2. First mark

make measuring sticks by using the pencil to make markings on the sticks. Question: what is the smallest length that we can accurately measure? Clearly we can measure 20 cm lengths with the shorter rod, but is it possible to make smaller measurements?

Here's one way to look at the situation. Imagine for a moment that we lay the 20 cm measuring stick next to the 52 cm stick such that the ends line up. At that point we could make a 20 cm mark on the 52 cm stick (see Figure 5.5.2).

At this point we move the 20 cm stick further down the the 52 cm stick such that one end is on the pencil mark, and and make another mark. Now there are two 20 cm sections marked on the 52 cm stick, as shown in Figure 5.5.3.

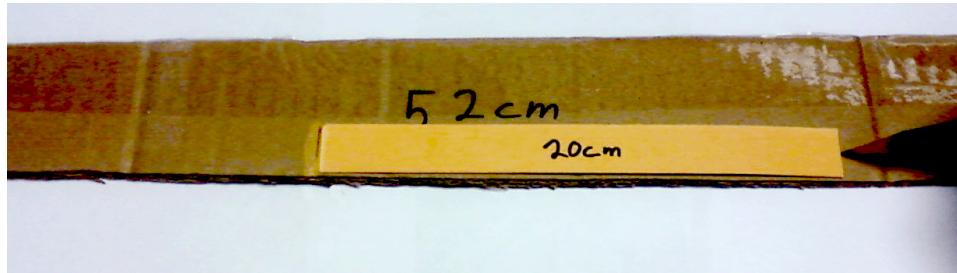


Figure 5.5.3. Second mark

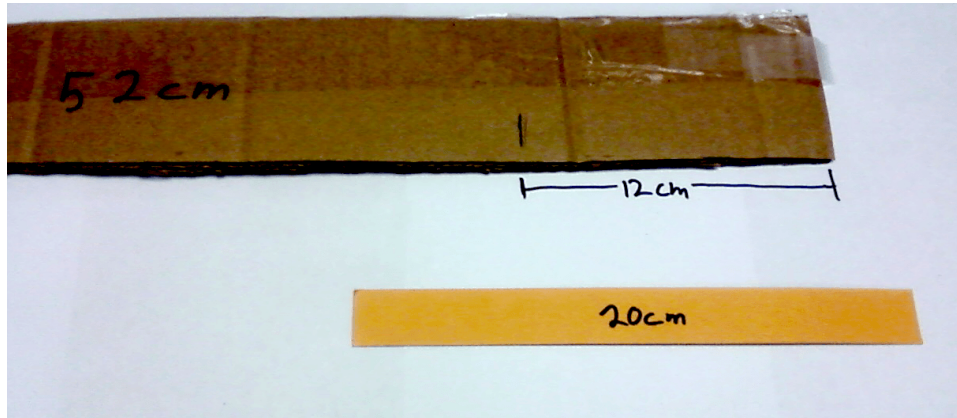
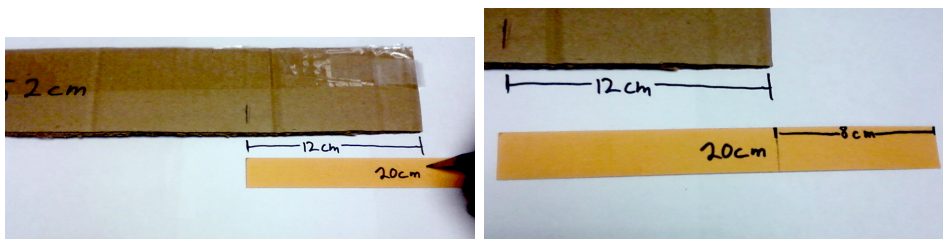


Figure 5.5.4. Remaining distance

Since we know the sum of the marked sections is 40 cm, and the length of the large stick is 52 cm, the remainder of the distance must be 12 cm, as shown in Figure 5.5.4. So we've actually made progress. At the beginning we were only able to measure lengths larger than 20 cm: but now we can measure 12 cm with the latest mark we've made.

But let's not stop there. We can use the 12 cm section to divide up the 20 cm stick. This will subdivide the 20 cm stick into a 12 cm section and a 8 cm section, as shown in Figure 5.5.5.

Now we're rolling! Let's subdivide the 12 cm section using the 8 cm section. This will produce an 8 cm section and a 4 cm section (see Figure 5.5.6). Now if we try to use the 4 cm section to subdivide any of the other sections,

**Figure 5.5.5.** More subdivision**Figure 5.5.6.** More subdivision

we will no longer have a remainder. This is because 4 cm evenly divides all the other lengths we have created, as shown in Figure 5.5.7.



Exercise 5.5.2. Using the method above, find the smallest measure given sticks of length:

- (a) 30 cm and 77 cm.
- (b) 7 feet and 41 feet (Pretty long sticks!).
- (c) 33 in and 72 in.



While working on the exercises, you may have noticed that the units of measure used do not matter. The only thing that matters is the actual count of those units of measure.

Exercise 5.5.3. Using the method above:

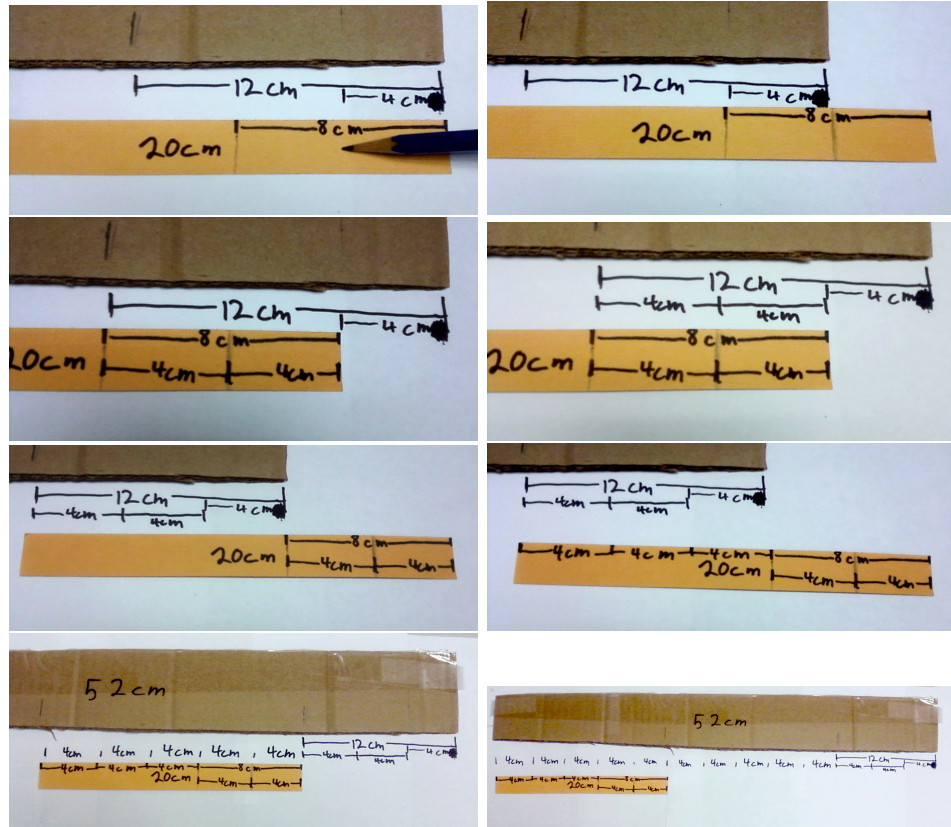


Figure 5.5.7. More subdivision

- Convert the measurements in Exercise 5.5.2 part (a) into millimeters, and solve the problem again. How is your result using millimeters related to your answer to part (a) in the previous exercise?
- Convert the measurements in Exercise 5.5.2 part (b) into inches, and solve the problem again. How is your result using inches related to your answer to part (a) in the previous exercise?
- Use what you've discovered in part (b) to quickly find a solution to the two-sticks problem when one stick is 720 inches and the other is 600 inches.

◇

5.5.2 Greatest common divisors

You may be familiar with the notion of greatest common divisor (gcd) of two numbers. The gcd is defined as the greatest number that divides the two given numbers. gcd's play a key role in modular arithmetic, as we shall see.

The general question we now consider is: What's a good way to find the gcd of two integer numbers? It may be easy to find the gcd of small numbers like 12 and 20, but what if you have to find the gcd of 583768 and 260568447?

At this point, let's think back to our two-sticks problem. We saw that when we began with sticks of length 52 and 20 we ended up with a minimum measurable distance of 4, which just so happens to be the gcd of 52 and 20. Was this a coincidence? Not at all! The minimum measurable distance has to evenly divide the two sticks' lengths, otherwise we could find a smaller measurable distance using the marking-off procedure described in the previous section. This implies that the minimum measurable distance must be a common divisor. To show that it's the *greatest* common divisor takes a little more work—we'll give the proof below. For now, we'll assume that the minimum measurable distance is in fact the gcd.

So to get the gcd of 583768 and 260568447, in theory we could try creating one stick of length 583768 and another of length 260568447 and follow the same procedure. Of course this isn't practical. So instead, we'll try to duplicate the same procedure mathematically, without resorting to actual sticks. Notice that when we subdivided a larger stick of length a into sections of the length of b , the result was essentially the same as dividing a by b while leaving a remainder r . See if you can complete the connection in the following example.

Example 5.5.4. Let's use algebraic language to express the two-sticks algorithm applied to 52 and 20. Let's start by setting this up as a division problem with a remainder (recall Proposition 5.2.3), since this is effectively what is being done in the stick example above.

$$52 = 20 \cdot q_1 + r_1,$$

where q_1 and r_1 are integers (we put the subscript '1' on the variables q_1 and r_1 because we're going to repeat the process). By division with remainder we find $q_1 = 2$ and $r_1 = 12$. Now we repeat the process, but this time dividing the remainder 12 into the smaller stick length 20:

$$20 = 12 \cdot q_2 + r_2,$$

which yields $q_2 = 1, r_2 = 8$. Here we go again, this time dividing the second remainder 8 into the first remainder 12:

$$12 = 8 \cdot q_3 + r_3$$

This yields $q_3 = 1, r_3 = 4$. One more time, this time dividing the new remainder 4 into the previous remainder 8:

$$8 = 4 \cdot q_4 + r_4$$

This yields $q_4 = 2, r_4 = 0$.

Now notice that 8 is divisible by 4. In the equation before that, we have $12 = 4 \cdot 2 + 4$. Since the right hand side is a sum of multiples of 4, the left hand side must also be a multiple of 4. In the next equation up $20 = 12 \cdot x + 8$ again, the right hand side is a sum of multiples of 4, so the left hand side must also be a multiple of 4. Continuing this logic upward shows that all intervals created along the way are divisible by 4. Hence the algorithm has generated a divisor of the original lengths 52 and 20. In summary, the *last nonzero remainder* gave us the gcd.

The procedure we have just described is called the ***Euclidean algorithm***. (An *algorithm* is a mathematical procedure designed to compute a specific result). The Euclidean algorithm is very powerful, and in fact can be used to calculate gcd's of large numbers as we'll see below.



As noted above, the divisor produced by the Euclidean algorithm turned out to be the greatest common divisor. Let's prove this in general.

Proposition 5.5.5. The Euclidean algorithm applied to two integers will give the gcd of those two integers.

PROOF. This proof is broken up into two parts, (A) and (B). Part (A) shows that the algorithm always produces a divisor of the two given integers. Part (B) shows that the produced divisor is indeed the gcd.

- (A) Given integers a and b and $a > b$ if we were to plug them into the Euclidean Algorithm we get:

$$a = b \cdot q_1 + r_1$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

$$\vdots$$

until there is an equation with no remainder left.

$$r_{k-2} = r_{k-1} \cdot q_{k-1} + r_k$$

$$r_{k-1} = r_k \cdot q_k + 0$$

It is clear that r_k divides r_{k-1} . Consider the next equation up.

$$r_{k-2} = r_{k-1} \cdot q_{k-1} + r_k = r_k \cdot q_{k-1} \cdot q_k + r_k$$

This shows that r_k divides the right hand side, so r_k must divide r_{k-2} . In the next equation up, the right can be set up as multiples of r_k which means the next r term is divisible by r_k . Continue all the way to the top and it must be that r_k divides both a and b .

- (B) Now suppose there is another number c that divides a and b such that $a_1 \cdot c = a$ and $b_1 \cdot c = b$. We can rewrite the initial equation of the algorithm as follows.

$$a_1 \cdot c = (b_1 \cdot c) \cdot q_1 + r_1 \Rightarrow a_1 \cdot c - (b_1 \cdot c) \cdot q_1 = r_1$$

This shows that c must divide r_1 . Consider the next equation.

$$b_1 \cdot c = (r_1) \cdot q_2 + r_2 \Rightarrow b_1 \cdot c - (r_1) \cdot q_2 = r_2$$

Since c divides both r_1 and b_1 then c must divide r_2 also. Repeat all the way to the bottom and c will have to divide r_k .

Since c divides r_k , c is no larger than r_k . So all divisors of a and b must be no larger than r_k . From part (A) we know that r_k divides both a and b . Therefore r_k must be the gcd of a and b .

□

The Euclidean algorithm may be summarized as follows.

- 1: Start with two integers a and b where $a > b$
- 2: Divide b into a and find the remainder r
- 3: If $r = 0$, b is the greatest common divisor.
- 4: If the remainder is not 0, then replace a with b and b with r and return to step 1.

Exercise 5.5.6. What is the greatest common divisor of:

- (a) 1168 and 2338?
- (b) 2343 and 4697?
- (c) 1006 and 13581?

◇

Let's analyze this algorithm just a little further. In the first step when we divide a by b , the remainder satisfies the equation, $r_1 = a - q_1 \cdot b$, where q is an integer. In other words, r_1 can be written in the general form: $r_1 = n \cdot a + m \cdot b$, where n and m are integers.

Exercise 5.5.7.

- (a) Show that r_2 can also be written in the form: $r_2 = n \cdot a + m \cdot b$, where n and m are integers.
- (b) Show that for $k > 2$, if r_{k-2} and r_{k-1} can both be written in the form $n \cdot a + m \cdot b$ where n and m are integers, then r_k can also be written in the same form.
- (c) Show that the gcd of two numbers a and b can always be written in the form $n \cdot a + m \cdot b$ where n and m are integers.

◇

The above exercise amounts to an inductive proof of the following proposition.

Proposition 5.5.8. The gcd of two numbers a and b can be written in the form $n \cdot a + m \cdot b$ where n and m are integers.

This proposition will be useful in the next section.

5.5.3 Computer stuff

For the computationally inclined reader here are two examples, in C++ syntax, of functions that calculate the greatest common divisor.

```
int gcdLoop (int a, int b){
    int divisee=a;
    int divisor=b;
    int remainder;
    //if they are the same, then either is the greatest divisor
    if (a == b)
        return a;
    //If a < b, then switch, otherwise the algorithm will not work.
    if (a < b){
divisee=b;
divisor=a;
    }
    // At this point, a is the larger of the two numbers
    do{
    // '%' returns the remainder of the integer division.
        remainder = divisee % divisor;
    //Set up the next iteration if the remainder is not 0 --
    // if the remainder is 0, then we're done
        if (remainder !=0){
divisee = divisor;
divisor = remainder;}
        else
            {break;}
    }while (1);
    return divisor;
}
```

This second example is also in C++, but uses recursion.

```
int gcdRecurse (int a, int b){
    int remainder;
    if (a == b)
        return a;
    if (a <$ b)
```

```

    {
        //'%' returns the remainder of the integer division
        remainder = b % a;
        if (remainder == 0)
            return a;
        else
            return gcdRecurse(a, remainder);
    }
else
{
    remainder = a % b;
    if (remainder == 0)
        return b;
    else
        return gcdRecurse(b, remainder);
}
//By calling itself, it will repeat the process until the remainder is 0
}

```

Exercise 5.5.9. Create a spreadsheet (with Excel, LibreOffice, or OpenOffice) that calculates the gcd of two integers that uses the procedure above. Excel has a built-in gcd function, but you're not allowed to use it for this exercise. But you may use the MOD function: “=MOD(A2,B2)” will compute the remainder when A2 is divided by B2. You may refer to the spreadsheet in Figure 5.5.8 for ideas. \diamond

5.5.4 Diophantine equations

Let's look now at another type of problem, which has played a key role in the history of mathematics.

Definition 5.5.10. A *Diophantine equation* in the variables m, n is an equation of the form

$$a \cdot m + b \cdot n = c$$

where a, b, c are integers, and m and n are assumed to have integer values.

\triangle

| | A | B | C |
|---|----------|-----------|-----------|
| 1 | Larger # | Smaller # | Remainder |
| 2 | 1053 | 863 | 190 |
| 3 | 863 | 190 | 103 |
| 4 | 190 | 103 | 87 |
| 5 | 103 | 87 | 16 |
| 6 | 87 | 16 | 7 |
| 7 | 16 | 7 | 2 |
| 8 | 7 | 2 | 1 |
| 9 | 2 | 1 | 0 |

Figure 5.5.8. Spreadsheet for computing gcd

Example 5.5.11. Find all integers m and n such that $16m + 42n = 8$.

To solve this, let us list each of the steps in finding the gcd of 42 and 16, as we explained in the previous section:

$$42 = (16) \cdot 2 + 10$$

$$16 = (10) \cdot 1 + 6$$

$$10 = (6) \cdot 1 + 4$$

$$6 = (4) \cdot 1 + 2$$

$$4 = (2) \cdot 2 + 0$$

Now let's start over again, but this time we'll keep track of what we're doing. If we start at the top of the list, but move the $16 \cdot 2$ to the other side of the equation, this yields:

$$42 \cdot 1 + 16 \cdot (-2) = 10.$$

Let's define a shorthand "pair notation" for the left-hand side. Let's represent any expression of the form $42 \cdot x + 16 \cdot y$ as (x, y) . Using this rule, we denote $42 \cdot 1 + 16 \cdot (-2)$ by the pair $(1, -2)$. Then our previous equation can be represented in "pair notation" as:

$$(1, -2) = 10.$$

This “vector notation” can save a lot of writing over the course of a long computation.

Now consider the next equation down the list, which is $16 = (10) \cdot 1 + 6$. Using pair notation, we can write 16 with $(0,1)$ (since $16 = 42 \cdot 0 + 16 \cdot 1$). We’ve already seen that $10 = (1, -2)$, so we get:

$$(0, 1) = (1, -2) + 6.$$

Now we can move the $(1, -2)$ to the left-hand side and subtract it from $(0, 1)$ to get:

$$(-1, 3) = 6.$$

Now the next equation down the list is $10 = (6) \cdot 1 + 4$. Making similar replacements, we find:

$$(1, -2) = (-1, 3) + 4 \quad \Rightarrow \quad (2, -5) = 4.$$

Repeat again for the next equation down the list: $6 = (4) \cdot 1 + 2$, which gives:

$$(-1, 3) = (2, -5) + 2 \quad \Rightarrow \quad (-3, 8) = 2.$$

At this point, we’ve gone as far as we can go. (Verify this: what happens if you try to continue?) Now if we replace the pair notation $(-3, 8)$ with what it originally represents, we get:

$$42 \cdot (-3) + 16 \cdot 8 = 2.$$

If we multiply this equation by 4, we have

$$42 \cdot (-12) + 16 \cdot 32 = 8.$$

It follows that $m = 32, n = -12$ is an integer solution to our original equation, $16m + 42n = 8$.

Unfortunately we’re not quite done yet, because we’re supposed to find *all* integer solutions. But we do have a particular solution, and we can leverage this information as follows.¹⁰ Suppose that m, n is an arbitrary

¹⁰What we’re doing here is a common ploy in mathematics. We’re using a *particular* solution to reduce the problem to a *homogeneous* equation (if you’re not familiar with this terminology, then don’t worry about it). Exactly the same method is used in differential equations, and in linear algebra.

solution, so that $42n + 16m = 8$. We may subtract from this equality the equation for the particular solution $m = -12, n = 32$:

$$\begin{array}{r} 42n + 16m = 8 \\ - (42(-12) + 16(32) = 8) \\ \hline 42(n + 12) + 16(m - 32) = 0 \end{array}$$

Rearranging and dividing by common factors, we obtain:

$$21(n + 12) = -8(m - 32).$$

Now since the right-hand side is divisible by 8, then the left-hand side must also be divisible by 8. This implies that $n + 12$ must be divisible by 8, or

$$n + 12 = 8k \quad (\text{for some integer } k).$$

If we plug this in to the equation just above, we get:

$$21(8k) = -8(m - 32), \quad \text{or} \quad m - 32 = -21k.$$

We may rearrange to obtain finally:

$$m = 32 - 21k \quad \text{and} \quad n = -12 + 8k \quad (\text{where } k \text{ is an arbitrary integer})$$

as the most general solution to $16m + 42n = 8$. ◆

Example 5.5.12. We'll give another example, giving just the computations and no other words. We find integer solutions to $1053x + 863y = 245$ as follows:

$$\begin{aligned} 1053 &= 863 + 190 \Rightarrow 190 = (1, -1) \\ 863 &= 4 \cdot 190 + 103 \Rightarrow 103 = (0, 1) - 4 \cdot (1, -1) = (-4, 5) \\ 190 &= 103 + 87 \Rightarrow 87 = (1, -1) - (-4, 5) = (5, -6) \\ 103 &= 87 + 16 \Rightarrow 16 = (-4, 5) - (5, -6) = (-9, 11) \\ 87 &= 5 \cdot 16 + 7 \Rightarrow 7 = (5, -6) - 5 \cdot (-9, 11) = (50, -61) \\ 16 &= 2 \cdot 7 + 2 \Rightarrow 2 = (-9, 11) - 2 \cdot (50, -61) = (-109, 133) \\ 7 &= 3 \cdot 2 + 1 \Rightarrow 1 = (50, -61) - 3 \cdot (-109, 133) = (377 - 460). \end{aligned}$$

This means that: $377 \cdot 1053 - 460 \cdot 863 = 1$ (You may check this on a calculator.)

Now we may multiply both sides by 245, which gives:

$$(245 \cdot 377) \cdot 1053 - (245 \cdot 460) \cdot 863 = 245.$$

Thus $x = (245 \cdot 377) = 92365$ and $y = -(245 \cdot 460) = -112700$, so that

$$1053 \cdot 92365 - 863 \cdot 112700 = 245$$

is an integer solution.

To find *all* integer solutions, we suppose that (x, y) is an arbitrary solution to $1053x + 863y = 245$. We can subtract our computed solution to give:

$$1053(x - 92365) + 863(y + 112700) = 0,$$

or

$$1053(x - 92365) = -863(y + 112700).$$

The left-hand side is divisible by 1053, and our computation shows that $\gcd(1053, 863) = 1$, so by *Euclid's Lemma* (Proposition 4.1.15 in Chapter 4) it must be the case that $y + 112700$ is also divisible by 1053. If we write $y + 112700 = 1053k$, it follows by algebra that $x - 92365 = -863k$. This means that

$$x = 92365 - 863k, \quad y = -112700 + 1053k$$

is the most general solution.

This solution is correct, but we can simplify it by shifting the value of k . Note that $92365 = 107 \cdot 863 + 24$ and $112700 = 107 \cdot 1053 + 29$. So we may replace k with $(\ell + 107)$ to obtain:

$$x = 92365 - 863(\ell + 107), \quad y = -112700 + 1053(\ell + 107),$$

which after working out the algebra gives us:

$$x = 24 - 863\ell, \quad y = 29 + 1053\ell.$$

◆

Exercise 5.5.13. Using the process above, find all integer solutions to the following equations.

(a) $45m + 16n = 27$

(b) $360m + 14n = 32$

(c) $389m + 50n = 270$

(d) $4801m + 500n = 1337$

(e) $3524m + 7421n = 333$

(f) $20m + 17n = 12$

◇

Exercise 5.5.14. Modify the spreadsheet from Exercise 5.5.9 to find the coefficients n and m such that $na + mb = \gcd(a, b)$ for given integers a, b . Refer to Figure 5.5.9 for ideas. ◇

| | A | B | C | D | E | F |
|----|----------|-----------|-----------|----------|------------|-------------|
| 1 | Larger # | Smaller # | Remainder | Quotient | First coef | Second coef |
| 2 | | | 1053 | | 1 | 0 |
| 3 | | | 863 | | 0 | 1 |
| 4 | 1053 | 863 | 190 | 1 | 1 | -1 |
| 5 | 863 | 190 | 103 | 4 | -4 | 5 |
| 6 | 190 | 103 | 87 | 1 | 5 | -6 |
| 7 | 103 | 87 | 16 | 1 | -9 | 11 |
| 8 | 87 | 16 | 7 | 5 | 50 | -61 |
| 9 | 16 | 7 | 2 | 2 | -109 | 133 |
| 10 | 7 | 2 | 1 | 3 | 377 | -460 |
| 11 | 2 | 1 | 0 | 2 | -863 | 1053 |

Figure 5.5.9. Spreadsheet for computing gcd

Do all Diophantine equation have solutions? Let's investigate.

Exercise 5.5.15. Explain why the following Diophantine equations have no integer solutions.

(a) $2m + 4n = 1$ (*Hint*)

(b) $3m + 27n = 2$

◇

The previous exercise shows that not all Diophantine equations can be solved. The following proposition shows which can and cannot be solved.

Proposition 5.5.16. Given the Diophantine equation $an + bm = c$, where a, b, c are integers. Then the equation has integer solutions for n and m if and only if c is a multiple of the gcd of a and b .

PROOF. Since this is an “if and only if” proof, we need to prove it both ways. We’ll do “only if” here, and leave the other way as an exercise.

Since we’re doing the “only if” part, we assume that $an + bm = c$ is solvable. We’ll represent the gcd of a and b by the letter d . Since $\gcd(a, b)$ divides both a and b , we may write $a = da'$ and $b = db'$ for some integers a', b' . By basic algebra, we have $an + bm = d(a'n + b'm)$. If we substitute this back in the original Diophantine equation, we get:

$$d(a'n + b'm) = c$$

It follows that c is a multiple of d , which is the gcd of a and b . □

Exercise 5.5.17. Prove the “if” part of Proposition 5.5.16. (*Hint*) ◇

At the beginning of this section, we “introduced” Diophantine equations. But we have seen them before:

Exercise 5.5.18.

- (a) Find the general integer solution to: $242m + 119n = 53$.
- (b) Use your solution to solve the modular equation: $242x \equiv 53 \pmod{119}$.
- (c) Use your solution to solve the modular equation: $119y \equiv 53 \pmod{242}$.

◇

This example shows that Diophantine equations are just modular equations in a disguised form! Furthermore, each Diophantine equation is associated with *two* modular equations:

Exercise 5.5.19. Given that (m, n) is a solution to $a \cdot m + b \cdot n = c$, give (a) a modular equation with base b involving the constants a and c which

has m as a solution; and (b) a modular equation with base a involving the constants b and c which has n as a solution. \diamond

In Example 5.3.11, we saw that not all equations of the form $ax \equiv c \pmod{b}$ have an answer. We now have the means to determine which modular arithmetic equations have an answer:

Proposition 5.5.20. Given a modular equation $ax \equiv c \pmod{b}$, where a, b, c are integers. Then the equation has an integer solution for x if and only if c is an integer multiple of the greatest common divisor of a and b .

Exercise 5.5.21. Prove both the “if” and the “only if” parts of Proposition 5.5.20. (*Hint*) \diamond

Exercise 5.5.22. Which of the following equations have integer solutions? If solutions exist, find them all. If no solutions exist, prove it!

- (a) $15x \equiv 3 \pmod{12}$
- (b) $4x \equiv 17 \pmod{23}$
- (c) $503x \equiv 919 \pmod{1002}$
- (d) $504x \equiv 919 \pmod{1002}$
- (e) $423x + 60 \equiv 720 \pmod{101}$

\diamond

To close off this section, we take care of some unfinished business. Way back when we were showing the existence of irrational numbers, we made use of *Euclid’s lemma* (Proposition 4.1.15 in Chapter 4). We weren’t able to give a real proof then—but now we can, thanks to Proposition 5.5.16. In the proof, we use the terms “prime” and “relatively prime”: recall that a prime number is a natural number > 1 whose only factor > 1 is itself (Definition 4.1.14); and two numbers are *relatively prime* if they have no common factors > 1 .

Exercise 5.5.23.

- (a) Let p be a prime, and let a be an integer. Show that a is relatively prime to p if and only if there exist integers m and n such that $pm + an = 1$. (*Hint*)
- (b) Suppose p is prime, and suppose a is relatively prime to p . Suppose also that p divides ab . By multiplying the equation in part (a) by b , show that p must divide b . (*Hint*)
- (c) Prove **Euclid's Lemma**: Let p be a prime number, and let a and b be integers. If p divides ab , then either p divides a or p divides b . (*Hint*)

◇

Euclid's lemma can be used to prove another "obvious" fact about natural numbers that "everybody knows" (but few people can prove): namely, that all natural numbers greater than 1 can be factored as a product of primes in exactly one way. This fact is known as the **Fundamental Theorem of Arithmetic**. There are two parts to the proof: first, showing that such a factorization always exists; and second, that there is only one way to do it (up to rearrangement of the factors). Both parts may be proved by induction, and a proof of the first part is given in Section 26.4.

5.5.5 Multiplicative inverse for modular arithmetic

This section is supposed to be about modular division, but so far we've been talking about all kinds of other stuff. You may be wondering, So where's the modular division? You're about to find out!

Recall that the set \mathbb{Z}_n under the operation \oplus forms a group: it has closure, it's associative, it has an additive identity, and all elements have inverses. On the other hand \mathbb{Z}_n does not form a group under \odot for any $n \geq 2$.

Why is this? Because the inverse property fails for the element 0. The multiplicative identity must be 1, yet $0 \cdot m \neq 1$ for all $m \in \mathbb{Z}_n$.

But let's not give up so easily in our quest to form multiplicative groups. Since it appears that 0 is a problem, suppose we take all the elements of \mathbb{Z}_n *except* 0? We write the set of nonzero elements of \mathbb{Z}_n as $\mathbb{Z}_n \setminus \{0\}$. Let's see whether this a group under \odot . We remind you that $a \odot b$ is defined by: $a \odot b = r$ where $a, b, r \in \mathbb{Z}_n$ and $a \cdot b = kn + r$ where k an integer.)

Example 5.5.24. The Cayley table for $\mathbb{Z}_3 \setminus \{0\}$ is:

| | | |
|---------|---|---|
| \odot | 1 | 2 |
| 1 | 1 | 2 |
| 2 | 2 | 1 |

Notice that each column has 1, meaning that each element has an inverse. It is also closed, associative and has an identity. Thus $\mathbb{Z}_3 \setminus \{0\}$ is a group under \odot . ♦

Example 5.5.25. The Cayley table for $\mathbb{Z}_4 \setminus \{0\}$ is

| | | | |
|---------|---|---|---|
| \odot | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 |
| 2 | 2 | 0 | 2 |
| 3 | 3 | 2 | 1 |

Notice that the 2 column does not have a 1 in it, meaning that 2 does not have an inverse in \mathbb{Z}_4 . Thus, $\mathbb{Z}_4 \setminus \{0\}$ is not a group under \odot . ♦

The fact that 2 has no inverse is due to 2 being a divisor of 4. This makes all integer multiples of 2 to cycle between the values 0 and 2 (mod 4).

Example 5.5.26.

Finding the multiplicative inverse in $\mathbb{Z}_n \setminus \{0\}$ for small values of n is not difficult. But what about finding the multiplicative inverse of 3 in $\mathbb{Z}_{31} \setminus \{0\}$?

Really all we're looking for is a number k such that $3k \equiv 1 \pmod{31}$. Since 31 is prime, it must be relatively prime to 3, meaning the gcd of 31 and 3 must be 1. 1 is a multiple of 1, so there is a solution and in fact this is just a special case of an earlier proposition. We convert it to a Diophantine equation:

$$3k + 31j = 1$$

Using the gcd algorithm, we find:

$$31 + 3 \cdot (-10) = 1,$$

and applying (mod 31) gives

$$3 \cdot (-10) \equiv 1 \pmod{31}.$$

Finally, we use the definition of modular arithmetic to convert -10 into a member in \mathbb{Z}_{31} :

$$3 \cdot (21) \equiv 1 \pmod{31}.$$



Exercise 5.5.27. Prove or disprove that the following sets form a group by either finding a multiplicative inverse for all members, or by finding a member that does not have a multiplicative inverse.

- (a) $\mathbb{Z}_5 \setminus \{0\}$
- (b) $\mathbb{Z}_7 \setminus \{0\}$
- (c) $\mathbb{Z}_9 \setminus \{0\}$
- (d) Make a conjecture for which sets $\mathbb{Z}_n \setminus \{0\}$ form a group under multiplication.



Proposition 5.5.28. If p is a prime number, then all elements in $\mathbb{Z}_p \setminus \{0\}$ have an inverse under multiplication mod p .

PROOF. Let a, p be known integers where $a < p$ and p is prime. There exists an inverse to a under multiplication (mod p) when there is a solution k to the equation $ak = 1 \pmod{p}$ where k is an integer. By Proposition 5.5.20, this equation can be solved if and only if the gcd of a and p is equal to 1. Since p is prime and $a < p$ then the gcd of a and p must be 1. \square

The previous proposition is actually a special case of the following:

Proposition 5.5.29. Let $n > 1$ be an integer, and let a be an element of $\mathbb{Z}_n \setminus \{0\}$. Then a has a multiplicative inverse in \mathbb{Z}_n if and only if $\gcd(a, n) = 1$ (that is, a is relatively prime to n).

The proof of this proposition is up to you:

Exercise 5.5.30. Let $n > 1$ be an integer, and let a be an element of $\mathbb{Z}_n \setminus \{0\}$.

- (a) Prove the “only if” part of Proposition 5.5.29. That is, prove that if a has an inverse in $\mathbb{Z}_n \setminus \{0\}$ then $\gcd(a, n) = 1$. (*Hint*)

- (b) Prove the “if” part of Proposition 5.5.29. That is, prove that if $\gcd(a, n)=1$ then a has an inverse in $\mathbb{Z}_n \setminus \{0\}$. (*Hint*)

◇

Exercise 5.5.31. Show that if n is not prime, then $\mathbb{Z}_n \setminus \{0\}$ is not a group under multiplication. (*Hint*) ◇

5.5.6 Chinese remainder theorem

We now are experts at finding solutions to congruences of the form $ax \equiv c \pmod{b}$. But what about multiple congruences? Take for example:

$$x \equiv 4 \pmod{7}; \quad x \equiv 5 \pmod{9}.$$

Can we find an x that solves both at the same time?

The first-century Chinese mathematician Sun Zi considered problems like this, and was able to come up with a general method of solution. His result is now known as the *Chinese Remainder Theorem*.

We may apply Sun Zi’s solution (expressed in modern algebraic language) to our particular case as follows. For the first congruence we have the general solution $x = 4 + 7k$, where k is any integer in \mathbb{Z} . If we substitute $4 + 7k$ for x in the second congruence, we get:

$$4 + 7k \equiv 5 \pmod{9} \Rightarrow 7k \equiv 1 \pmod{9}.$$

At this point we could use the Euclidean algorithm to find k . But it’s often easier to use the trial-and-error methods that we developed earlier. In this case, the method amounts to adding multiples of 9 to the right-hand side until you get something that is divisible by 7. In this case, we find:

$$7k \equiv 1 + 3 \cdot 9 \pmod{9} \Rightarrow 7k \equiv 28 \pmod{9} \Rightarrow k \equiv 4 \pmod{9}.$$

This means $k = 9j + 4$ for some integer j . We substitute $9j + 4$ for k back into $x = 4 + 7k$ to get:

$$x = 4 + 7(9j + 4) = 4 + 63j + 28 = 32 + 63j.$$

So the answer must be $x \equiv 32 \pmod{63}$. When we check, $32 = 9 \cdot 3 + 5 = 7 \cdot 4 + 4$ and $95 = 9 \cdot 10 + 5 = 7 \cdot 13 + 4$ and indeed that is the case. Notice

the ending modulus was the least common multiple of the first and second modulus (7 and 9, respectively) in the original set of modular equations.

Now, not all multiple congruences have an answer. Take the following pair of congruences:

$$x \equiv 3 \pmod{4}; \quad x \equiv 4 \pmod{6}.$$

We follow the same pattern. There is a solution for the first congruence $x = 4k + 3$ where k is any integer. Plug this into the second congruence to yield:

$$4k + 3 \equiv 4 \pmod{6} \Rightarrow 4k \equiv 1 \pmod{6}.$$

From the Euclidean algorithm, we know there is a solution to this congruence if and only if $\gcd(4, 6) = 1$, but we know $\gcd(4, 6) = 2$. Therefore there is no solution.

Exercise 5.5.32. Solve the following pairs of congruences or show that they have no common solution:

- (a) $x \equiv 2 \pmod{3}; \quad x \equiv 3 \pmod{4}$.
- (b) $x \equiv 12 \pmod{23}; \quad x \equiv 7 \pmod{11}$.
- (c) $x \equiv 3 \pmod{13}; \quad x \equiv 20 \pmod{31}$.
- (d) $x \equiv 2 \pmod{6}; \quad x \equiv 56 \pmod{72}$.

◇

Exercise 5.5.33.

- (a) Find a pair of congruences of the form: $x \equiv a \pmod{9}; \quad x \equiv b \pmod{15}$ that have no common solution.
- (b) Given congruences of the form

$$ax \equiv b \pmod{3}; \quad cx \equiv d \pmod{7}$$

which both have solutions. Show that common solutions also exist.
 (*Hint*)

(c) *Prove the following: Given a pair of congruences

$$ax \equiv b \pmod{m}; \quad cx \equiv d \pmod{n}$$

which both have solutions, such that $\gcd(m, n) = 1$. Then the congruences also have a common solution. (*Hint*)

(d) *Prove the following: Given a pair of congruences

$$x \equiv b \pmod{m}; \quad x \equiv d \pmod{n}.$$

such that $\gcd(m, n) = 1$. Then there exist common solutions to both congruences; and all common solutions are congruent mod mn . (*Hint*)

◇

We can use the same method to solve any number of simultaneous congruences. Take for example:

$$x \equiv 4 \pmod{7}; \quad x \equiv 5 \pmod{9}; \quad x \equiv 1 \pmod{2}.$$

From the above example we know the general solution for the first two congruences is $x \equiv 32 \pmod{63}$. So we need to solve:

$$x \equiv 32 \pmod{63}; \quad x \equiv 1 \pmod{2}$$

We solve this by the same process as before:

$$\begin{aligned} x = 1 + 2k &\Rightarrow 1 + 2k \equiv 32 \pmod{63} \Rightarrow 2k \equiv 31 \pmod{63} \\ &\Rightarrow 2k \equiv 31 + 63 \pmod{63} \Rightarrow 2k \equiv 94 \pmod{63} \\ &\Rightarrow k \equiv 47 \pmod{63}. \end{aligned}$$

Substitute to obtain $x = 1 + 2(47 + 63j) = 95 + 126j \equiv 95 \pmod{126}$.

Exercise 5.5.34. Solve the following sets of congruences or show that they do not have a solution:

(a) $x \equiv 2 \pmod{3}; \quad x \equiv 3 \pmod{4}; \quad x \equiv 4 \pmod{5}$.

(b) $x \equiv 12 \pmod{23}; \quad x \equiv 7 \pmod{11}; \quad x \equiv 3 \pmod{4}$.

◇

5.6 Hints for “Modular Arithmetic” exercises

Exercise 5.2.13: Use the alternative definition of modular equivalence in Proposition 5.2.10.

Exercise 5.3.1(f): Prove by contradiction: suppose the codes d_1, d_2, \dots, d_{10} and e_1, e_2, \dots, e_{10} are both valid, and suppose that all digits are equal except for the n 'th digit (so $d_n \neq e_n$). There are two cases: (a) n is even; (b) n is odd. In case (a), show that this implies $e_n - d_n \equiv 0 \pmod{10}$, and derive a contradiction. Prove case (b) similarly.

Exercise 5.3.2(d): Use the fact that $10 \equiv -1 \pmod{11}$.

Exercise 5.3.2(i): Prove by contradiction: Suppose the codes d_1, d_2, \dots, d_{10} and e_1, e_2, \dots, e_{10} are both valid, and suppose that all digits are equal except for the n 'th digit (so $d_n \neq e_n$). Show that $d_n - e_n$ satisfies $(d_n - e_n)n \equiv 0 \pmod{11}$, and show that the only solution is $d_n - e_n = 0$.

Exercise 5.3.2(j): Suppose the code d_1, d_2, \dots, d_{10} is valid, and suppose the code is still valid when the digits d_n and d_{n+1} are exchanged. Write down two modular equations, and take the difference between the two modular equations. Use this to find an equation involving d_n and d_{n+1} .

Exercise 5.3.12(c): Find a *negative* number that is equivalent to 856 (mod 123).

Exercise 5.4.7(a): Let $m = \ell$ and $b = a$. Check the conditions of the proposition still hold, and apply the proposition.

Exercise 5.4.8(a): You will need to use Proposition 5.4.4 twice.

Exercise 5.4.14: Use the definitions of \oplus and \odot .

Exercise 5.4.15: Be careful about 0!

Exercise 5.4.20(b)(i): Use the fact that $0 < a < n$.

Exercise 5.5.15(a): The left-hand side is always even, no matter what m and n are.

Exercise 5.5.17: Use Proposition 5.5.8.

Exercise 5.5.21: Use Proposition 5.5.16.

Exercise 5.5.23(a): Use Proposition 5.5.16. (b): p must divide the left-hand side of the multiplied equation (explain why). (c): Consider two cases (I) a is relatively prime to p ; (II) a is not relatively prime to p .

Exercise 5.5.30: Use Proposition 5.5.20.

Exercise 5.5.31: Use the previous exercise.

Exercise 5.5.33(b): If y is a particular solution to $ax \equiv b \pmod{3}$, then $x = y + 3k$ is also a solution. Similarly, if z is a particular solution to $cx \equiv d \pmod{7}$, then $x = z + 7\ell$ is also a solution. Set the two expressions equal, and show there is always a solution for k, ℓ regardless of the values of y, z .

Exercise 5.5.33 (c): Follow the method used in the Chinese Remainder Theorem, and for each modular equivalence obtained show that a solution exists.

Exercise 5.5.33 (d): Suppose that x and y are both solutions to the given pair of congruences. Show that $x - y \equiv 0 \pmod{m}$ and $x - y \equiv 0 \pmod{n}$. This implies that both m and n divide $x - y$ (explain why).

5.7 Study guide for “Modular Arithmetic” chapter

Section 5.1, Introductory examples

Concepts:

1. Modular arithmetic
2. Modulus

Competencies

1. Be able to give the modulus involved in a practical problem involving “cycles”. (5.1.10)

Section 5.2, Modular equivalence and modular arithmetic

Concepts:

1. Net displacement
2. Modular equivalence: two numbers are equivalent mod m if they have the same remainder under division by m .
3. Modular equivalence (alternative formulation): Given $a, b, m \in \mathbb{Z}$, then $a \equiv b \pmod{m}$ iff $m \mid (a - b)$
4. Integers modulo m (these are the possible remainders of integers under division by m)

Notation

1. \in means ‘contained in’ or ‘elements of’
2. \equiv means modular equivalence, similar to equality, but not quite the same
3. \mid means ‘divides’

Competencies

1. Determine whether or not two integers are equivalent modulo a given base. (5.2.15)

Section 5.3, Modular equations

Concepts:

1. Application of modular arithmetic to UPC and ISBN codes
2. Transposition errors in scanning codes
3. Solving modular equations

Key Formulas

1. Inner product of two tuples: $(d_1, d_2, \dots, d_k) \cdot (w_1, w_2, \dots, w_k) = d_1w_1 + d_2w_2 + \dots + d_kw_k$
2. UPC check formula: $(d_1, d_2, d_3, d_4, \dots, d_{12}) \cdot (3, 1, 3, 1, \dots, 1) \equiv 0 \pmod{10}$
3. ISBN formula: $(d_1, d_2, \dots, d_{10}) \cdot (1, 2, \dots, 10) \equiv 0 \pmod{11}$
(note d_{10} might have to be a 10 to make the inner product 0, ‘X’ is used to represent 10).

Competencies

1. Be able to validate UPC codes and find errors. (5.3.1)
2. Be able to validate ISBN codes and find errors. (5.3.2)
3. Be able to solve modular equations with small coefficients using trial and error. (5.3.5, 5.3.9)
4. In modular equations, replace coefficients with their remainders before solving. (Example 5.3.10, 5.3.12)

Section 5.4, The integers mod n (also known as \mathbb{Z}_n)**Concepts:**

1. Modular addition and multiplication
2. Cayley tables for addition and multiplication in \mathbb{Z}_n
3. Closure properties of \mathbb{Z}_n
4. Additive & multiplicative identities and inverses in \mathbb{Z}_n
5. Commutative, associative, & distributive properties in \mathbb{Z}_n
6. Definition of a group (a set with an operation that is closed, associative, has an identity, and all set elements have inverses)

Key Formulas

1. Modular addition: $a, b \in \mathbb{Z}_n$ then $a \oplus b = r$ iff $a + b = r + sn$ and $r \in \mathbb{Z}_n$
2. Modular multiplication: $a \odot b = r$ iff $a \cdot b = r + sn$ and $r \in \mathbb{Z}_n$
(note that $=$ is used rather than \equiv in modular addition and multiplication equations, since $a \oplus b$ is defined as equal to the remainder for modular addition and modular multiplication.)

Competencies

1. Be able to draw “commutative diagrams” that relate arithmetic in \mathbb{Z} to arithmetic in \mathbb{Z}_n . (5.4.6)
2. Prove modular equivalence between arithmetic expressions involving integers and modular arithmetic expressions involving the integers’ remainders. (5.4.7, 5.4.8)
3. Simplify expressions mod n by replacing terms in the expression with their remainders. (5.4.10)
4. Know how to tell whether a set is closed under a certain arithmetic operation. (5.4.15)
5. Create tables for addition and multiplication mod n .

5.7 STUDY GUIDE FOR “MODULAR ARITHMETIC” CHAPTER 157

6. Be able to find multiplicative inverses of elements in \mathbb{Z}_n , or prove they have none. (5.4.22)
7. Know the group properties by memory. (Definition 5.4.26)
8. Be able to show if elements of a given \mathbb{Z}_n are a group or not. (5.4.30)

Section 5.5, Modular division

Concepts:

1. Greatest common divisors (gcd)
2. Euclidean algorithm for finding gcd
3. Computing gcd using spreadsheets
4. Diophantine equations: $a \cdot m + b \cdot n = c$, where a, b, c are integers, and m and n are assumed to have integer values.
5. Multiplicative inverse for modular arithmetic: If $a \in \mathbb{Z}_n$, then $x \in \mathbb{Z}_n$ is the multiplicative inverse of a in \mathbb{Z}_n if $a \odot x = 1$.
6. Chinese remainder theorem

Key Formulas

1. Euclidean algorithm formulas: $a = b \cdot q_1 + r_1, b = r_1 \cdot q_2 + r_2,$
 $r_1 = r_2 \cdot q_3 + r_3, \dots$

Competencies

1. Be able to find the greatest common divisor using the Euclidean algorithm. (5.5.6)
2. Be able to find all integer solutions to a Diophantine equation. (5.5.13)
3. Know the four group properties by heart (closure, identity, inverse, associative) and be able to tell from a Cayley table whether or not a certain set with a given operation is a group. (5.5.27)
4. Solve pairs of congruences or show they have no common solution. (5.5.32)

Modular Arithmetic, Decimals, and Divisibility

"I'm all about that, all about that bass I'm all about that, all about that bass I'm all about that bass, no treble We gon' take it to a whole another level" (Source: "All About That Bass", Meghan Trainor)

We grew up working with numbers in base 10. so let's explore the how we represent numbers, find the k 'th decimal of integer and non-integer numbers, and deriving divisibility rules of integers all in base 10. The problem is that bases come in all different sizes, so we will also delve into converting integers and non-integers from base 10 to other bases and vice versa!

This chapter is by Adam McDonald and Chris Thron.

6.1 Decimal representations

6.1.1 Decimal representation formula

We are so used to writing decimal numbers, that we take for granted what we're doing. Let's think a little more carefully about what's really going on when we write a decimal number. Let's start with integers. Essentially, representing an integer as a decimal means writing the integer in terms of powers of 10. For example, the number 72483 means:

$$72483 = 7 \cdot 10^4 + 2 \cdot 10^3 + 4 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0. \quad (6.1.1)$$

In general, a $m + 1$ -digit decimal number n which has digits $d_m, d_{m-1} \dots d_0$ (from largest to smallest) has the value:

$$n = d_m 10^m + d_{m-1} 10^{m-1} + \dots + d_0. \quad (6.1.2)$$

Note that each digit d_j must be in \mathbb{Z}_{10} .

6.1.2 Formulas for decimal digits of integers

It is easy for a human being to identify the digits of a decimal number, because we're used to decimal arithmetic. But we want a way of *mathematically* defining the digits. This is useful when we need to have a computer recognize the decimal digits of a number (computers use *binary* rather than decimal numbers, so it takes some doing to get them to produce decimal digits).

Let's do this first with a simple example. We'll take our favorite number $n = 72483$, and see if we can develop a mathematical process to read off the digits. The lowest digit (i.e. the number in the one's place) is found by taking the mod base 10: $3 = \text{mod}(n, 10)$. Then if we subtract this digit from n , we get 72480, which is divisible by 10. When we divide by 10, we obtain 7248. Notice that the one's digit of this new number is equal to the 10's digit of n . So we can repeat the same process and take the modulus base 10 to obtain $8 = \text{mod}(7248, 10)$. We then take $7248 - 8 = 7240$, divide by 10, and repeat the process until we get all the digits (from lowest to highest).

Let's generalize this to an arbitrary integer, n expressed in base 10. The lowest digit (i.e. the number in the one's place) is found by calculating $\text{mod}(n, 10)$. Let's call this d_0 . We compute $(n - d_0)/10$ which we will call a_1 . The second digit d_1 is equal to $\text{mod}(a_1, 10)$. To obtain the third digit d_2 , we first compute $a_2 = (a_1 - d_1)/10$ and then $d_2 = \text{mod}(a_2, 10)$. From here, we will repeat the same steps to get the rest of the digits. We may summarize the entire process in the following series of equations:

$$\begin{aligned}
a_0 &= n; & d_0 &= \text{mod}(n, 10) \\
a_1 &= \frac{a_0 - d_0}{10}; & d_1 &= \text{mod}(a_1, 10) \\
a_2 &= \frac{a_1 - d_1}{10}; & d_2 &= \text{mod}(a_2, 10) \\
& & & \vdots \\
a_m &= \frac{a_{m-1} - d_{m-1}}{10}; & d_m &= \text{mod}(a_m, 10),
\end{aligned}$$

This sequence of $m + 1$ equations can be summarized as follows:

$$\begin{aligned}
a_0 &= n; & d_0 &= \text{mod}(n, 10) \\
a_k &= \frac{a_{k-1} - d_{k-1}}{10}; & d_k &= \text{mod}(a_k, 10), & k &= 1, \dots, m
\end{aligned}$$

These equations specify a *recursive process* or *recursive method*, so called because we're repeating the same calculation again and again with the results of previous calculations. The neat thing is that we can use a similar process to find digits of numbers in other bases as well. We'll explain how this works in the next section.

Exercise 6.1.3. Apply the above recursive method to obtain the sequences $\{a_k\}$ and $\{d_k\}$ for the following cases:

- (a) The 100's digit of $n = 238$.
- (b) The 1000's digit of $n = 52812$.
- (c) The 10000's digit of $n = 27819$.

◇

The above procedure can be long, particularly if we're trying to find d_m for a large value of m . Fortunately, there's a way to shortcut the process:

Example 6.1.4. Let's find the digit d_6 for the number $n = 1928307465$ (we may note in this case $d_6 = 8$). First, we can remove the digits above d_6 digit taking n modulo 10^7 :

$$\text{mod}(n, 10^7) = 8307465.$$

On the other hand, we can obtain all digits below d_6 by taking n modulo 10^7 :

$$\text{mod}(n, 10^7) = 307465$$

Now subtracting the two we get:

$$\text{mod}(n, 10^7) - \text{mod}(n, 10^6) = 8000000$$

From this point, we easily obtain d_6 by dividing by 10^6 . So in summary, we have:

$$d_6 = \frac{\text{mod}(n, 10^7) - \text{mod}(n, 10^6)}{10^6}$$

◆

This formula can be generalized to find the digit d_k for any positive integer n :

$$d_k = \frac{\text{mod}(n, 10^{k+1}) - \text{mod}(n, 10^k)}{10^k} \quad (6.1.5)$$

Exercise 6.1.6. Show how the formula in (6.1.5) can be used to find the following digits.

- (a) The 2nd digit of $n=238$ base 10
- (b) The 4th digit of $n=21657$ base 10
- (c) The 3rd digit of $n=4356$ base 10

◇

6.1.3 Formulas for decimal digits of nonintegers

So far we've been talking about finding decimal digits of integers. What about other real numbers? Happily, it turns out there are similar formulas that work for any real number, as we will now show. To make things simple, in this section we will consider numbers between 0 and 1. Then for a general real number, we can separate it into its integer part and fractional part, and use our previous formulas for the integer part and the formulas in this section for the rest.

Numbers between 0 and 1 have a decimal expansion like integers do:

$$x = d_{-1}10^{-1} + d_{-2}10^{-2} + \cdots + d_{-k}10^{-k} + \cdots, \text{ where } d_{-j} \in \mathbb{Z}_{10} \quad (6.1.7)$$

Fractional numbers differ from integer in that the decimal expansion may be *infinite*, that is to say it may go on forever.¹

Let's see if we can compute the d_{-k} digit of a decimal number less than 1. But first, let's recall some useful notation:

Definition 6.1.8. The *floor* is the highest integer less than or equal to the given decimal number, x , and is represented as $\lfloor x \rfloor$. \triangle

Earlier, we used two methods, recursive method and a generalized formula, to find d_k of a decimal integer. We can do the same to find d_{-k} of the fractional part of a decimal number. We will take the fraction representation of $x = 0.17428$ and find its third decimal digit, d_{-3} . This will be done using two different methods (just like we did with integers). First, we will use a recursive method, then we will find a direct formula. Let's begin with the recursive method, which gives us the digits one by one. We may notice that the first decimal digit of x is actually the integer part of $10x$: in other words, $d_{-1} = \lfloor 10x \rfloor$. We may subtract this from $10x$ to obtain $b_{-1} = 0.7428$. Notice that b_{-1} contains all the digits of x except d_{-1} . So let's do it again. Multiplying b_{-1} by 10 and taking the floor, we obtain d_{-2} . Subtracting this from $10b_{-1}$ gives us $b_{-2} = 0.428$. Once more should do it! Multiply b_{-2} by 10 and taking the floor gives $d_{-3} = 4$. Done!

In general, the recursive process for finding d_{-k} is as follows:

$$\begin{aligned} d_{-1} &= \lfloor 10x \rfloor; & b_{-1} &= 10x - d_{-1} \\ d_{-2} &= \lfloor 10b_{-1} \rfloor; & b_{-2} &= 10b_{-1} - d_{-2} \\ & & \vdots & \\ d_{-k} &= \lfloor 10b_{-k+1} \rfloor; & b_{-k} &= 10b_{-k+1} - d_{-k} \\ & & \vdots & \end{aligned} \quad (6.1.9)$$

This process can take a very long time if we're trying to find d_{-k} for large values of k . Recall that formula (6.1.5) gives an easy way of finding

¹In fact it is true that "almost all" numbers between 0 and 1 have infinite decimal expansions—and yes, "almost all" has a mathematically precise definition!

individual decimal digits of integers. Can we do the same thing for fractions? Yes we can!

Example 6.1.10. Find d_{-3} of the decimal number $x = 0.17428$ Since we're looking for d_{-3} , Let's multiply x by 10^3 .

$$0.17428 \cdot 10^3 = 174.28$$

Then take the floor:

$$\lfloor 174.28 \rfloor = 174$$

Finally, take the modulus base 10 (which is the 1's place of the number, as we've seen before):

$$\text{mod}(174, 10) = 4$$

This gives us the correct value of d_{-3} . ♦

Let's recap the steps in Example 6.1.10s:

- (i) multiply the given x by 10^k ,
- (ii) take the floor of the number found in step (i),
- (iii) find the modulus of number in step (ii) base 10.

This procedure can be generalized to the following formula:

$$d_{-k} = \text{mod}(\lfloor x \cdot 10^k \rfloor, 10) \tag{6.1.11}$$

Exercise 6.1.12. Complete the following exercises using the recursive method from Equation (6.1.9) and re-do them by using Equation (6.1.11):

- (a) Find the 2nd decimal digit of 0.238 base 10
- (b) Find the 4th decimal digit of 0.54289 base 10
- (c) Find the 3rd decimal digit of 0.7129 base 10

♦

6.1.4 Repeating decimals

You have probably encountered fractions with infinite decimal expansions, such as $1/9 = 0.11111\dots$, $1/11 = 0.09090909\dots$, and $1/7 = 0.142857142857\dots$. It is a strange and wonderful fact that these infinite decimal expansions always *repeat*: for example, the decimal expansion for $1/7$ has the sequence 142857 that keeps on repeating. This observation suggests two questions:

1. Why do decimal fractions repeat?
2. What is the period of repetition?

In this section we'll answer these two questions. But first we need to prove a preliminary proposition.

Proposition 6.1.13. Let $n > 2$ be an integer such that $\gcd(n, 10) = 1$. Then there exist a positive integer m such that $\text{mod}(10^m, n) = 1$.

PROOF. Consider the infinite sequence: $\text{mod}(10, n)$, $\text{mod}(10^2, n)$, $\text{mod}(10^3, n)$, \dots . All of these numbers are between 1 and $n - 1$. Since the sequence is infinite and only can take at most $n - 1$ values, it follows there must be at least two values that are equal, so $\text{mod}(10^k, n) = \text{mod}(10^j, n)$, where $k > j$. But,

$$\begin{aligned} \text{mod}(10^k, n) &= \text{mod}(10^j \cdot 10^{k-j}, n) && \text{[exponent rules]} \\ &= \text{mod}(10^j, n) \odot \text{mod}(10^{k-j}, n) && \text{[Proposition 5.4.4].} \end{aligned}$$

Since $\text{mod}(10^k, n) = \text{mod}(10^j, n)$, it follows by substitution that

$$\text{mod}(10^j, n) = \text{mod}(10^j, n) \odot \text{mod}(10^{k-j}, n),$$

which “implies” $\text{mod}(10^{k-j}, n) = 1$ (*but see Exercise 6.1.14!*) So if we set $m = k - j$, we have $\text{mod}(10^m, n) = 1$, and the proof is finished. \square

Exercise 6.1.14.

1. What is wrong with the following argument?

$$\begin{aligned} 16 &= 4 \cdot 4 \\ \text{mod}(16, 6) &= \text{mod}(4 \cdot 4, 6) \\ 4 &= \text{mod}(4, 6) \odot \text{mod}(4, 6) \\ 4 \odot 1 &= 4 \odot 4 \quad (\text{in mod } 6) \\ 1 &= 4 \quad (\text{in mod } 6). \end{aligned}$$

2. Explain why the condition $\gcd(n, 10) = 1$ is required in Proposition 6.1.13.

◇

Proposition 6.1.13 leads to the following definition:

Definition 6.1.15. Given a positive integer n with $\gcd(10, n) = 1$. The smallest positive integer m such that $\text{mod}(10^m, n) = 1$ is called the *multiplicative order* of $n \pmod{10}$.

(Note that the order of n is guaranteed to exist because of Proposition 6.1.13). △

We can now prove that a large class of fractions repeat, as follows:

Proposition 6.1.16. Let $n > 1$ be a positive integer with $\gcd(10, n) = 1$, and let m be the multiplicative order of $n \pmod{10}$. Then the decimal expansion of $\frac{1}{n}$ repeats every m digits.

PROOF. Given that m is the multiplicative order of $n \pmod{10}$, from Definition 6.1.15, we get $\text{mod}((10^m - 1), n) = 0$. In other words, $10^m - 1$ is divisible by n , so that $\frac{10^m - 1}{n}$ is an integer. Letting $k = \frac{10^m - 1}{n}$, it follows that:

$$\begin{aligned} \frac{1}{n} &= \frac{k}{10^m - 1} && \text{substitution} \\ &= \frac{k}{10^m} \left(\frac{1}{1 - 10^{-m}} \right) && \text{factor} \\ &= \frac{k}{10^m} (1 + 10^{-m} + \dots) && \text{geometric series} \\ &= k \cdot 10^{-m} + k \cdot 10^{-2m} + \dots && \text{distributive law and algebra} \end{aligned}$$

Next from the definition of k , we may conclude that $k < 10^m$ (verify this). So $k \cdot 10^{-m} < 1$, and the nonzero decimal digits of $k \cdot 10^{-m}$ are all contained in the first m decimal places to the right of the decimal point. Similarly, the nonzero decimal digits of $k \cdot 10^{-2m}$ all lie within the second m decimal places (between the 10^{-m-1} place and the 10^{-2m} place), the nonzero decimal digits of $k \cdot 10^{-3m}$ are all in the following m decimal places, and so on. In other

words, the terms $k \cdot 10^{-m}, k \cdot 10^{-2m}, \dots$ are all within successive blocks of m digits. Thus k is the repeating sequence in the repeating decimal (possibly padded by some zeros, in case k has less than m nonzero digits), and that the fraction repeats every m digits. \square

Exercise 6.1.17. Given that the fraction $j/n < 1$ and $\gcd(10, n) = 1$, show that j/n is still a repeating fraction with the same period as $1/n$. \diamond

Exercise 6.1.18. In Proposition 6.1.16 we proved that the decimal expansion of $\frac{1}{n}$ repeats every m digits for a positive integer $n > 1$ with $\gcd(10, n) = 1$. Does the proposition still hold if $\gcd(10, n) \neq 1$? If yes then prove it, and if no then give a counterexample. \diamond

6.1.5 Divisibility rules

How do we know if a decimal integer, m , is divisible by an decimal integer, n ? In this section we will be discovering the divisibility rules for different integers, n . We will start with finding the divisibility rule for $n = 3$.

Example 6.1.19. Is 234 divisible by 3? Answering this question is equivalent to showing whether or not $\text{mod}(234, 3) = 0$. Let's first write the decimal representation of 234:

$$234 = 200 + 30 + 4 = 2 \cdot 10^2 + 3 \cdot 10 + 4$$

Since $\text{mod}(10, 3) = 1$, we get

$$\begin{aligned} \text{mod}(234, 3) &= \text{mod}(2 \cdot 10^2 + 3 \cdot 10 + 4, 3) && \text{[substitution]} \\ &= \text{mod}(2 \cdot (1)^2 + 3 \cdot (1) + 4, 3) && \text{[Props. 5.2.8 and 5.4.4]} \\ &= \text{mod}(9, 3) = 0 && \text{[arithmetic]} \end{aligned}$$

\blacklozenge

Let's generalize Example 6.1.19. Suppose we have a decimal number, n , with digits $d_0 \dots d_m$ so that the number can be written as $d_m d_{m-1} \dots d_0$. Then we can write

$$n = d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \dots + d_0 \cdot 10^0$$

It follows that

$$\begin{aligned}\text{mod}(n, 3) &= \text{mod}(d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \cdots + d_0 \cdot 10^0, 3) \\ &= \text{mod}(d_m + d_{m-1} + \cdots + d_0, 3) = 0.\end{aligned}$$

This observation leads to the following proposition.

Proposition 6.1.20. An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Example 6.1.21. Is 6472 divisible by 11? In the following argument we use the fact that $10 \equiv -1 \pmod{11}$, which means that we can replace 10 with -1 whenever we are taking mod's base 10.

$$\begin{aligned}\text{mod}(6472, 11) &= \text{mod}(6 \cdot 10^3 + 4 \cdot 10^2 + 7 \cdot 10 + 2 \cdot 1, 11) \\ &= \text{mod}(6 \cdot (-1)^3 + 4 \cdot (-1)^2 + 7 \cdot (-1) + 2, 11) \\ &= \text{mod}(-6 + 4 - 7 + 2, 11) = \text{mod}(-7, 11) = 4\end{aligned}$$

Since $\text{mod}(6472, 11) \neq 0$, 6472 is not divisible by 11. \blacklozenge

Proposition 6.1.22. A number is divisible by 11 if and only if the *alternating sums* of the digits is divisible by 11. (Note: alternating sums is where the signs of the number alternate when summing.)

PROOF. Given an integer with digits $d_0 \dots d_n$ where the number is written as $d_n d_{n-1} \dots d_1 d_0$ we can write

$$n = d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \cdots + d_0 \cdot 10^0$$

it follows that:

$$\begin{aligned}\text{mod}(n, 11) &= \text{mod}(d_m \cdot 10^m + d_{m-1} \cdot 10^{m-1} + \cdots + d_0 \cdot 10^0, 11) && \text{[substitution]} \\ &= \text{mod}(d_m \cdot (-1)^m + d_{m-1} \cdot (-1)^{m-1} + \cdots + d_0 \cdot (-1)^0, 11) && \text{[mod}(10, 11) = -1] \\ &= \text{mod}((-1)^m(d_m - d_{m-1} + \cdots + d_0 \cdot 1), 11) && \text{[factor out } (-1)^m]\end{aligned}$$

Therefore, $\text{mod}(n, 11) = 0$ if and only if the alternating sums of the digits of the number $d_n \dots d_0$ is divisible by 11. \square

Exercise 6.1.23.

| | A | B | C |
|----|--------------------|-----------------------|---|
| 1 | base | 37 | |
| 2 | | | |
| 3 | $10^{n(n \geq 0)}$ | $\text{Mod}(A_n, 37)$ | |
| 4 | 1 | 1 | |
| 5 | 10 | 10 | |
| 6 | 100 | 26 | |
| 7 | 1000 | 1 | |
| 8 | 10000 | 10 | |
| 9 | 100000 | 26 | |
| 10 | 1000000 | 1 | |
| 11 | 10000000 | 10 | |
| 12 | 100000000 | 26 | |
| 13 | | | |

Figure 6.1.1. Spreadsheet to compute the powers of 10 mod 37

- (a) In Proposition 6.1.20 we showed that a number is divisible by 3 if and only if the sum of its digits is divisible by 3. Write a similar argument and state a proposition for a number that is divisible by 9.
- (b) Figure 6.1.1 shows a table giving the different powers of 10 mod base 37.

Based on the results shown in Figure 6.1.1, propose a divisibility rule to check whether numbers are divisible by 37. Apply your rule to the following numbers: 17094, 411108, 365412

- (c) Create a spreadsheet similar to the the spreadsheet in Figure 6.1.1. Use your spreadsheet to find $\text{mod}(10^n, 111)$ for $0 \leq n \leq 8$. Come up with a proposition for numbers in base 11 and prove it similarly the divisibility rule for numbers in base 11 was proved in Proposition 6.1.22.

◇

Here's a number-magic trick involving divisibility that you can try on your friends. This example is thanks to Mr. Ogungbesan Adedoyinsola, a student at the University of Lagos.

Example 6.1.24. Let $n=321$. The digits in reverse order give $m = 123$. Now subtract $n - m = 321 - 123 = 198$. We can add the digits of 198 to get $1 + 9 + 8 = 18$. Since the sum of the digits of 198 is divisible by 9, 198 is divisible by 9. ♦

Exercise 6.1.25. Repeat Example 6.1.24 with the numbers: 4567, 314142, 583651. ♦

Amazing! But we have the mathematical tools to see why it works:

Exercise 6.1.26.

- (a) Take any decimal integer, write the digits in reverse order, and subtract the reversed number from the original number. Show that the result is always divisible by 9.
- (b) If the decimal integer has an odd number of digits, show that the result obtained in (a) will always be divisible by 99.
- (c) Show that if you take any decimal integer n , rearrange the digits, multiply by any power of 10, and subtract n from the resulting number, then your final result will always be divisible by 9.

♦

There are many variations on this theme—maybe you can come up with one yourself.

Exercise 6.1.27. Take any number with an even number of digits, reverse the number, and add the two together. Show that the result is always divisible by 11. ♦

Exercise 6.1.28. Take any number with any number of digits. Write the digits in reverse order and append them to the end of the original number (for example, if the original number is 2834, the end result is the number 28344382). Show that the result is always divisible by 11. (Hint: Think about Exercise 6.1.27). ♦

Exercise 6.1.29.**

- Factor the number 1001, and use your result to design a procedure that does the following. Given a number n with m digits, using a single subtraction (and no multiplication) construct a number n' with $m - 3$ digits such that $\text{mod}(n, 7) = \text{mod}(n', 7)$, $\text{mod}(n, 11) = \text{mod}(n', 11)$, and $\text{mod}(n, 13) = \text{mod}(n', 13)$.
- Explain how it is possible to use your procedure to take an arbitrarily large number n and obtain a number with three or fewer digits which has the same divisibility with respect to 7, 11, and 13 as n does.
- Use your procedure to test (by hand) the numbers 14142131356237 and 314159653589 for divisibility by 7, 11, and 13, using only subtraction and 3 final divisions of a 3-digit number.

◇

Exercise 6.1.30.**

- Prove that the following rule works for divisibility by 7. Given a m -digit number, remove the last digit d_0 to obtain a $m - 1$ -digit number, then subtract $2d_0$ from the $m - 1$ -digit number. Then the new number has the same divisibility by 7 as the original number.
- Use the result in (a) to test the number 27182818284590 for divisibility by 7.
- Obtain similar rules for divisibility by 13 and 19.
- Use your rules from (c) to test 27182818284590 for divisibility by 13 and 19.

◇

6.2 Decimal representations in other bases

We've mentioned above that we can express numbers in other bases besides base 10. First we should explain what it means to represent a number in base b , where $b > 2$ is a positive integer. Recall that the base 10 number $d_n d_{n-1} \dots d_1 d_0$ represents the integer:

$$d_n d_{n-1} \dots d_1 d_0 = d_n \cdot 10^n + d_{n-1} \cdot 10^{n-1} + \dots + d_1 \cdot 10 + d_0.$$

For a number expressed in base b , we simply replace the 10's with b 's:

$$(d_n d_{n-1} \dots d_1 d_0)_b = d_n \cdot b^n + d_{n-1} \cdot b^{n-1} + \dots + d_1 \cdot b + d_0.$$

For example, $(6342)_8$ represents the number:

$$(6342)_8 = 6 \cdot 8^3 + 3 \cdot 8^2 + 4 \cdot 8^1 + 2 \cdot 8^0.$$

Note that if $(d_n d_{n-1} \dots d_1 d_0)_b$ is a base b representation, then all of the digits d_0, \dots, d_n must be between 0 and $b - 1$.

In order to be able to use other base representations effectively, we'll need to know how to convert numbers back and forth between other bases and base 10. Let's see how this is done.

Example 6.2.1. Find 137 in base 6. I will solve this following the recursive method described in Section 6.2, but using base 6 instead of base 10.

$$\begin{aligned} a_0 &= 137; d_0 = \text{mod}(137, 6) = 5 \\ a_1 &= \frac{137 - 5}{6} = 22; d_1 = \text{mod}(22, 6) = 4 \\ a_2 &= \frac{22 - 4}{6} = 3; d_2 = \text{mod}(3, 6) = 3 \\ a_3 &= \frac{3 - 3}{6} = 0 \end{aligned}$$

Since $a_3 = 0$ we can stop. To write the solution take the moduli in reverse order. Therefore, 137 in base 6 is 345. \blacklozenge

Example 6.2.2. Find 121 in base 3. Once again using the recursive method

$$\begin{aligned}
a_0 &= 121; & d_0 &= \text{mod}(121, 3) = 1 \\
a_1 &= \frac{121 - 1}{3} = 40; & d_1 &= \text{mod}(40, 3) = 1 \\
a_2 &= \frac{40 - 1}{3} = 13; & d_2 &= \text{mod}(13, 3) = 1 \\
a_3 &= \frac{13 - 1}{3} = 4; & d_3 &= \text{mod}(4, 3) = 1 \\
a_4 &= \frac{4 - 1}{3} = 1; & d_4 &= \text{mod}(1, 3) = 1 \\
a_5 &= \frac{1 - 1}{3} = 0
\end{aligned}$$

Since $a_5 = 0$ we do not have to continue. To write the solution take the moduli in reverse order. Therefore, 121 in base 3 is 11111. \blacklozenge

Example 6.2.3. Find the 5th digit of 65432 in base 3. (This is the coefficient of 3^4 in the base 3 representation). We may use Eq. 6.1.5, just replacing base 10 with base 3:

$$d_4 = \frac{\text{mod}(65432, 3^5) - \text{mod}(65432, 3^4)}{3^4}$$

\blacklozenge

You might be thinking that this is very similar to how we found the k 'th digit of a decimal integer in Section 6.1.2 and you would be correct! The main difference is that the base in the modulus is not a base of 10 but the base of the number we are finding (in the above example base 3). Also, instead of finding only one of the digits of a number in base 10, we are finding *all* the digits of a number in another base (in the above example it is base 3). We know we are done finding the entire number when $a_n = 0$ and we write the final number in the reverse order of how we found the modulus'.

Exercise 6.2.4.

- (a) Find 1567 in base 5.
- (b) Find 344 in base 3.

- (c) Find 7281 in base 7.
 (d) Find 3491 base 4.
 (e) Find 65432 in base 3.

◇

Being able to represent numbers in base 2 is important in computer science because this is how computers do arithmetic. In base 2 the digits are called *bits*. All information that is stored in the computer is stored in the form of bits. A block of 8 bits is called a *byte*: computer memory is measured in terms of kilobytes, megabytes, or gigabytes. Integers are commonly stored as either 2 or 4 bytes.

Example 6.2.5. Find 31 in base 2.

$$\begin{array}{ll}
 a_0 = 31; d_0 = \text{mod}(31, 2) = 1; & a_1 = \frac{31-1}{2} = 15; b_1 = \text{mod}(15, 2) = 1 \\
 a_2 = \frac{15-1}{2} = 15; b_2 = \text{mod}(14, 2) = 0; & a_3 = \frac{14-0}{2} = 15; b_3 = \text{mod}(7, 2) = 1 \\
 a_4 = \frac{7-1}{2} = 15; b_4 = \text{mod}(6, 2) = 0; & a_5 = \frac{6-0}{2} = 15; b_5 = \text{mod}(3, 2) = 1 \\
 a_6 = \frac{3-1}{2} = 15; b_6 = \text{mod}(1, 2) = 1; & a_7 = \frac{1-1}{2} = 0; b_7 = \text{mod}(0, 2) = 0
 \end{array}$$

Therefore $N = 31$ written in base 2 is 0110101. If stored as a 2-byte integer, N would be represented as 0b000000000110101 (the '0b' prefix indicates that the number is a binary number). ◆

Exercise 6.2.6. Express the following as 2-byte binary integers

- (a) 73
 (b) 235
 (c) 1940
 (d) 67037

◇

Base 16 is also often used: numbers in base 16 are called *hexadecimal* numbers. In hexadecimal (or ‘hex’) representation, the letters A, B, C, D, E, F are used to represent 10, 11, 12, 13, 14, 15 respectively. In many computer languages (like Java, C++, and Python), a hexadecimal number is indicated by the prefix ‘0x’. So for example, the hex number $0xABCD$ signifies $10 \cdot 16^3 + 11 \cdot 16^2 + 12 \cdot 16^1 + 13$.

Exercise 6.2.7. Find the hex representations of the following decimal numbers

- (a) 4095
- (b) 10000.
- (c) 123456

◇

Converting numbers from base 10 to another base is fun! But how about converting numbers from another base to base 10? Piece of cake:

Example 6.2.8. Convert 121 in base 3 to a number in base 10.

$$(121)_3 = 1 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0 = 1 \cdot 9 + 2 \cdot 3 + 1 \cdot 1 = (16)_{10} \quad \blacklozenge$$

Example 6.2.9. Convert 4752 in base 8 to a number in base 10

$$(4752)_8 = 4 \cdot 8^3 + 7 \cdot 8^2 + 5 \cdot 8^1 + 2 \cdot 8^0 = 4 \cdot 512 + 7 \cdot 64 + 5 \cdot 8 + 2 \cdot 1 = (2538)_{10} \quad \blacklozenge$$

Do you recognize this from before? All that we’re doing is using the defining equation for base b representation:

$$(n)_b = d_m \cdot (b)^m + d_{m-1} \cdot (b)^{m-1} + \dots + d_0 \quad (6.2.10)$$

Exercise 6.2.11. Convert the given numbers with their bases to a number in base 10:

1. 456 base 7
2. 32102 base 4
3. 8714 base 9

◇

Earlier we mentioned the importance of converting numbers in base 10 to base 2. It is just as important to convert numbers in base 2 to base 10.

Example 6.2.12. Convert 1011 in base 2 to a number in base 10.

$$(1011)_2 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 \cdot 1 = (11)_{10}$$

◆

Exercise 6.2.13. Convert the given numbers in base 2 to a number in base 10:

- (a) 10101
- (b) 11011001
- (c) 100111011

◇

Exercise 6.2.14. In computer graphics, colors are often represented using *RGB notation*. Colors have red, green, and blue components; and each component has an intensity level from 0 to 255, which can be stored as a single byte. Each byte is represented as two hex digits, so colors are represented as a six-digit hex number. For example, 0xFFFFFF represents intensities of 255 for red, green and blue, corresponding to the color white, while 0x000000 represents black. 0xFF0000, 0x00FF00, 0x0000FF represent pure red, pure green, and pure blue respectively.

Find the red, green, and blue intensities for the following colors in hex representation:

- (a) 0xAA45E2

(b) $0x29A4F3$

(c) $0x774422$

◇

Set Theory

“A set is a Many that allows itself to be thought of as a One.”
(Georg Cantor)

“(Set theory is) the finest product of mathematical genius and one of the supreme achievements of purely intellectual human activity.” (David Hilbert)

“Set” is one of the most fundamental concepts in mathematics, and sets have been a part of mathematics since ancient times. However, a truly rigorous theory of sets was only developed about a hundred years ago. We won’t get into the difficulties involved in coming up with a rigorous theory (we’ll just mention “Russell’s paradox” in passing). Instead, we’ll focus on the algebraic properties of sets: in particular the operations of intersection, union, and complement, and proving identities involving these operations.

7.1 Set Basics

You’ve probably seen sets, set relations, and set operations in previous classes. In fact, in the previous two chapters of this book you’ve already been working with sets. So we’ll review them quickly before moving on to further properties and proofs concerning sets and their accessories.

This chapter is an adapted and expanded version of a chapter by D. and J. Morris.

7.1.1 Definition and examples

First of all, let's give a precise mathematical definition for "set":

Definition 7.1.1. A *set* is a well-defined collection of objects: that is, it is defined in such a manner that we can determine for any given object x whether or not x belongs to the set. The objects that belong to a set are called its *elements* or *members*. We will denote sets by capital letters, such as A or X ; if a is an element of the set A , we write $a \in A$. \triangle

Two common ways of specifying sets are:

- by listing all of its elements inside a pair of braces; or
- by stating the property that determines whether or not an object x belongs to the set.

For example, we could define a particular set E by listing its elements:

$$E = \{2, 4, 6, \dots\},$$

or by specifying properties which characterize its elements:

$$E = \{x : x > 0 \text{ and } x \text{ is divisible by } 2\}.$$

(here the ":" signifies "such that"). We can also describe E in a less mathy way by simply calling it "the set of positive even numbers".

We write $2 \in E$ when we want to say that 2 is in the set E , and $-3 \notin E$ to say that -3 is not in the set E .

Sets don't have to involve numbers. For example, we could define a certain set X by listing:

$$X = \{\text{Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday}\},$$

or by property:

$$X = \{x : x \text{ is the name of a weekday (in English)}\}.$$

For the purposes of this book, it would be good enough to say, " X is the set of weekday names (in English)" (we're not so snobby about set brackets).

Exercise 7.1.2.

(a) What elements are in the following set:

$$S = \{x : x \text{ is the name of a U.S. state and } x \text{ begins with 'W'}\}$$

Write the set as a list of objects.

(b) Rewrite the following as a list $= \{x : x \text{ is a type of regular polygon with less than 6 sides}\}$.

(c) Rewrite the following set of dates by using a property:

$$T = \{\text{Jan. 4th 2011, Jan. 11th 2011, Jan. 18 2011, Jan. 25 2011, \dots, Dec. 27 2011}\}$$

(Note: January 1 2011 was on a Saturday).

(d) Write the set of odd integers O : (i) as a list, and (ii) by using a property.

◇

It is possible for the elements of a set to be sets in their own right. For instance, we could define

$$T = \{x : x \text{ is a National League baseball team}\}.$$

A more mathematical (but less interesting) example would be

$$S = \{x : x \text{ is a set of integers}\}.$$

Then elements of S would include the sets $\{1, 2, 3, 4\}$, $\{\text{the set of odd integers}\}$, $\{0\}$, and so on.

We can even go farther, and define sets of sets of sets. For instance, the set L of major baseball leagues in the U.S. has two elements:

$$L = \{\text{American League, National League}\}.$$

However, the American League A consists of a set of teams:

$$A = \{\text{Yankees, Red Sox, \dots}\},$$

while the National League N also consists of a set of teams:

$$N = \{\text{Cubs, Phillies, \dots}\}.$$

Each of these teams consists of a set of players: so altogether the set L is a set of sets of sets!

Exercise 7.1.3.

- (a) Describe the 21st century as a set of sets of sets of sets of sets of sets of sets. (*Hint*)
- (b) (For you biologists out there) Describe the animal kingdom as a set of sets of sets of sets of sets of sets of sets of sets (*Hint*)

◇

This notion of “sets of sets” can bring us into dangerous territory. For example, consider the set

$$S = \{x : x \text{ is a set which is not an element of itself}\}.$$

We may then pose the question: is S an element of itself?¹

Let us consider the possibilities:

- Suppose first that S is an element of itself. Then S must satisfy the defining property of elements of S – that is, S must be an example of a set x for which “ x is not an element of itself.” It follows that S is not an element of itself. This contradicts our supposition – so apparently our supposition is wrong, and S must not be an element of itself.
- On the other hand, suppose that S is not an element of itself. Then S satisfies the defining property of elements of S – that is, S is an example of a set x for which “ x is not an element of itself.” It follows that S is an element of S . Once again this contradicts our supposition – so apparently S must be an element of itself!

How do we get out of this mess? No matter what we assume, we end up with a contradiction! The problem, as is often the case, lies in *hidden assumptions* that we have made. Our definition of S makes reference to the unknown x , where x is an “arbitrary” set. Herein lies the rub: the notion of “arbitrary” set is *not well-defined*. Put another way: the set of “all possible sets” is NOT a set!

In the following discussion we will avoid this problem by always starting out with a well-defined set that contains all the sets and elements of interest in a particular example or problem. Such an all-encompassing set is referred to as a *universal set*. Note each particular problem will have its

¹This question is called *Russell’s paradox*, and plays an important role in the history of set theory.

own universal set. For instance, if we are talking about public opinion polls in the United States, an appropriate universal set might be the set of American citizens. If we're talking about sets of prime and composite numbers, our universal set could be either the set of integers, or the set of natural numbers. If we are talking about roots of algebraic equations, depending on our particular interest we might choose the universal set to be the set of real numbers, or the set of complex numbers. When we talk about sets in a general way, we often denote sets by capital letters A, B, C, \dots , and it's assumed that all these sets are subsets of some universal set U .

7.1.2 Important sets of numbers

We will refer often to the following sets of numbers. Although we are presuming that these sets are “given”, the reader should be aware that it's not at all easy to formally define them in a mathematically precise way. (Although we won't give any definitions here, you may encounter them in other mathematics courses, such as logic or analysis.)

- $\mathbb{N} = \{n : n \text{ is a natural number}\} = \{1, 2, 3, \dots\}$; (Note that according to our definition the natural numbers do not include 0. Some books include 0 as a natural number.)
- $\mathbb{Z} = \{n : n \text{ is an integer}\} = \{\dots, -1, 0, 1, 2, \dots\}$;
- $\mathbb{Q} = \{r : r \text{ is a rational number}\}$;
- $\mathbb{R} = \{x : x \text{ is a real number}\}$;

You may recall that in Chapter 4, we defined the set of complex numbers \mathbb{C} as

$$\mathbb{C} := \{x + iy, \text{ such that } x, y \in \mathbb{R}\}.$$

This is just one example of a favorite gambit of mathematicians, namely creating new sets from existing sets in various imaginative ways. You'll be seeing many more examples of this as we go along.

Subsets and proper subsets

Definition 7.1.4. A set A is a **subset** of B , written $A \subset B$ or $B \supset A$, if every element of A is also an element of B . \triangle

For example, using this notation we may write:

$$\{\text{sons of John and Jane Doe}\} \subset \{\text{children of John and Jane Doe}\}$$

and

$$\{4, 5, 8\} \subset \{2, 3, 4, 5, 6, 7, 8, 9\}$$

and

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

According to Definition 7.1.4, every set is a subset of itself. That is, for any set A , $A \subset A$, since every element in A is (of course) in A . Sometimes though we may want to take about subsets of A that really are strictly contained in A , without being all of A . Such subsets are called **proper subsets**. Formally, a set B is a **proper subset** of a set A if $B \subset A$ and $B \neq A$. For instance, if John and Jane Doe had only sons, then $\{\text{sons of John and Jane Doe}\}$ is not a proper subset of $\{\text{children of John and Jane Doe}\}$.

Remark 7.1.5. In this book, we use ‘ \subset ’ for subset, and we have no special symbol to distinguish “proper subset” from “subset”. Some authors use ‘ \subseteq ’ to denote subset, and ‘ \subset ’ to denote proper subset. This has the advantage that then ‘ \subseteq ’ and ‘ \supseteq ’ are similar to ‘ \leq ’ and ‘ \geq ’, while ‘ \subset ’ and ‘ \supset ’ are like ‘ $<$ ’ and ‘ $>$ ’. But we rarely have to distinguish the case of proper subsets, so it’s not worth defining a special symbol for them. \triangle

If A is not a subset of B , we write $A \not\subset B$; for example, $\{4, 7, 9\} \not\subset \{2, 4, 5, 8, 9\}$. Two sets are **equal**, written $A = B$, if we can show that $A \subset B$ and $B \subset A$.

It is convenient to have a set with no elements in it. This set is called the **empty set** and is denoted by \emptyset . For instance, if John and Jane Doe had only daughters, then

$$\{\text{sons of John and Jane Doe}\} = \emptyset$$

Note that the empty set is a subset of every set.

Exercise 7.1.6. Let S be a set with a single element.

- (a) How many subsets does it have?
- (b) How many proper subsets does it have?

- (c) How many nonempty subsets does it have?
- (d) How many nonempty proper subsets does it have?

◇

Exercise 7.1.7.

- (a) Can you give an example of a set with exactly three subsets? How about exactly three proper subsets?
- (b) What is the smallest number of elements a set must have in order to have at least eight proper subsets?

◇

7.1.3 Operations on sets

In our days of carefree innocence, we were introduced to *operations* on integers, rational numbers, etc.. An operation on the integers takes two integers and always comes up with another integer. For instance, the '+' operation gives $2 + 3 = 5$ (of course, we know now that this means that + has the property of *closure*).

Exercise 7.1.8. What's wrong with the following statement: "Subtraction is an operation on the natural numbers." ◇

In a similar way, we can construct new sets out of old sets using *set operations*. The mathematical definitions of the basic set operations are as follows:

Definition 7.1.9. The *union* $A \cup B$ of two sets A and B is defined as

$$A \cup B = \{x : x \in A \text{ or } x \in B\};$$

△

Definition 7.1.10. the *intersection* of A and B is defined by

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

△

For example: if $A = \{1, 3, 5\}$ and $B = \{1, 2, 3, 9\}$, then

$$A \cup B = \{1, 2, 3, 5, 9\} \quad \text{and} \quad A \cap B = \{1, 3\}.$$

We may also consider the union and the intersection of more than two sets. For instance, the union of three sets A_1, A_2 , and A_3 can be written $A_1 \cup A_2 \cup A_3$ or $\bigcup_{i=1}^3 A_i$.

Similarly, the intersection of the same three sets can be written as $A_1 \cap A_2 \cap A_3$ or $\bigcap_{i=1}^3 A_i$.

Remark 7.1.11. There's actually a technical difficulty with our notations for $A_1 \cup A_2 \cup A_3$ and $A_1 \cap A_2 \cap A_3$. The problem is that the notation is ambiguous: does $A_1 \cup A_2 \cup A_3$ mean $(A_1 \cup A_2) \cup A_3$ or $A_1 \cup (A_2 \cup A_3)$? As it turns out, it doesn't make any difference (we'll show this in the next section). Since it doesn't matter which order we do the \cup , we just leave off the parentheses (and the same for \cap). This is really nothing new: you're used to writing $3 + 4 + 7 + 9$ instead of $((3 + 4) + 7) + 9$, because it doesn't matter what order you add the numbers. △

Exercise 7.1.12.

- (a) Find three sets A_1, A_2, A_3 such that $A_1 \cup A_2 \cup A_3 = \mathbb{Z}$ and $A_1 \cap A_2 \cap A_3 = \emptyset$
- (b) Find three sets A_1, A_2, A_3 such that (i) $A_1, A_2, A_3 \subset \mathbb{C}$; (ii) $A_1 \cap A_2 \neq \emptyset, A_2 \cap A_3 \neq \emptyset, A_1 \cap A_3 \neq \emptyset$; and (iii) $A_1 \cap A_2 \cap A_3 = \emptyset$
- (c) Find three sets that satisfy all conditions of part (b) and in addition satisfy $A_1 \cup A_2 \cup A_3 = \mathbb{C}$.

◇

We may generalize to intersections and unions of collections of n sets by writing:

$$\bigcup_{i=1}^n A_i = A_1 \cup \dots \cup A_n$$

and

$$\bigcap_{i=1}^n A_i = A_1 \cap \dots \cap A_n$$

for the union and intersection, respectively, of the collection of sets A_1, \dots, A_n .

Example 7.1.13. Specify the following sets, either by:

- listing the elements;
- describing with a property; or
- giving another set that we've already defined that has the same elements.

(a) $\bigcup_{i=1}^n \{i\}$

(b) $\bigcup_{i=1}^n \{1, \dots, i\}$

(c) $\bigcup_{i=1}^{\infty} \{1, \dots, i\}$

Solutions:

(a) $\bigcup_{i=1}^n \{i\} = \{1\} \cup \{2\} \cup \{3\} \cup \dots \cup \{n\}$
 $= \{1, \dots, n\}$ [list of elements]
 $=$ all integers from 1 to n . [property]

(b) $\bigcup_{i=1}^n \{1, \dots, i\} = \{1\} \cup \{1, 2\} \cup \{1, 2, 3\} \cup \dots \cup \{1, \dots, n\}$
 $= \{1, \dots, n\}$ [list of elements]
 $=$ all integers from 1 to n . [property]

(c) $\bigcup_{i=1}^{\infty} \{1, \dots, i\} =$ [by part (b)] $\{1, \dots, \infty\} = \mathbb{N}$



Exercise 7.1.14. Specify the following sets, either by:

- listing the elements;
- describing with a property; or
- giving another set that we've already defined that has the same elements.

- (a) $\bigcap_{i=1}^n \{i\}$
- (b) $\bigcap_{i=1}^n \{1, \dots, i\}$
- (c) $\bigcap_{i=1}^{\infty} \{1, \dots, i\}$
- (d) $\bigcup_{r=0}^{n-1} \{\text{Integers that have remainder } r \text{ when divided by } n\}$
- (e) $\bigcap_{r=0}^{n-1} \{\text{Integers that have remainder } r \text{ when divided by } n\}$

◇

Exercise 7.1.15.

- (a) Find an infinite collection of sets $\{A_i\}, i = 1, 2, 3, \dots$ such that (i) $A_i \subset \mathbb{R}, i = 1, 2, 3, \dots$; (ii) each A_i is a closed interval of length 1 (that is, $A_i = [a_i, a_i + 1]$ for some a_i ; and (iii) $\bigcup_{i=1}^{\infty} A_i = [0, \infty)$. (That is, the union of all the A_i 's is the set of all nonnegative real numbers.)
- (b) Find an infinite collection of sets $\{A_i\}, i = 1, 2, 3, \dots$ such that (i) $A_i \subset \mathbb{R}, i = 1, 2, 3, \dots$; (ii) each A_i is an open interval of length 1 (that is, $A_i = (a_i, a_i + 1)$ for some a_i ; and (iii) $\bigcup_{i=1}^{\infty} A_i = (0, \infty)$. (That is, the union of all the A_i 's is the set of all positive real numbers.)
- (c) Find an infinite collection of sets $\{A_n\}, n = 1, 2, 3, \dots$ such that (i) $A_n \subset [-1/2, 1/2], n = 1, 2, 3, \dots$; (ii) each A_n is an open interval of length $1/n$; and (iii) $\bigcap_{n=1}^{\infty} A_n = \{0\}$.
- (d) **Find an infinite collection of sets $\{A_n\}, n = 1, 2, 3, \dots$ such that (i) $A_n \subset [0, 1], n = 1, 2, 3, \dots$; (ii) each A_n is an open interval of length $1/n$; (iii) $A_{n+1} \subset A_n, n = 1, 2, 3, \dots$; and (iv) $\bigcap_{n=1}^{\infty} A_n = \emptyset$.

◇

When two sets have no elements in common, they are said to be **disjoint**; for example, if E is the set of even integers and O is the set of odd integers, then E and O are disjoint. Two sets A and B are disjoint exactly when $A \cap B = \emptyset$.

Exercise 7.1.16.

- (a) Find disjoint nonempty sets A_1, A_2, A_3, A_4 such that $\bigcup_{i=1}^4 A_i = \mathbb{Z}$.

- (b) Find disjoint nonempty sets A_1, A_2, A_3, A_4 such that $\bigcup_{i=1}^4 A_i = \mathbb{R}$.
- (c) Find disjoint nonempty sets A_1, A_2, A_3, A_4 such that $\bigcup_{i=1}^4 A_i = \mathbb{C}$.

◇

If we are working within the universal set U and $A \subset U$, we define the **complement**² of A (denoted by A'), to be the set

$$A' = \{x : x \in U \text{ and } x \notin A\}.$$

Definition 7.1.17. The **difference** of two sets A and B is defined as

$$A \setminus B = A \cap B' = \{x : x \in A \text{ and } x \notin B\}.$$

△

Note that it's not necessary for B to be inside A to define $A \setminus B$. In fact, $A \setminus (A \cap B)$ is exactly the same thing as $A \setminus B$ (you may draw a picture to see why this is true).

Exercise 7.1.18. Suppose that $A \subset B$. What is the largest subset of B that is disjoint from A ? ◇

The set difference concludes our set operations for now. The following example and exercises will give you an opportunity to sharpen your set operation skills.

Example 7.1.19. Let \mathbb{N} be the universal set, and suppose that

$$A = \{x \in \mathbb{N} : x \text{ is divisible by } 2\}$$

$$B = \{x \in \mathbb{N} : x \text{ is divisible by } 3\}$$

$$C = \{x \in \mathbb{N} : x \text{ is divisible by } 6\}$$

$$D = \{\text{the odd natural numbers}\}$$

Then specify the following sets:

- (a) $A \cap B$

²Please note the spelling: 'complement', not 'compliment', thank you!

(b) $C \cup A$ (c) $D \setminus B$ (d) B'

Solutions:

(a)

$$\begin{aligned} A \cap B &= \{x \in \mathbb{N} : x \text{ is divisible by 2 and } x \text{ is divisible by 3}\} \\ &= \{x \in \mathbb{N} : x \text{ is divisible by 6}\} \\ &= C \end{aligned}$$

(b)

$$\begin{aligned} C \cup A &= \{x \in \mathbb{N} : x \text{ is divisible by 6 or } x \text{ is divisible by 2}\} \\ &= \{2, 4, 6, 8, 10, 12, \dots\} \\ &= A \end{aligned}$$

(c)

$$\begin{aligned} D \setminus B &= \{x \in \mathbb{N} : x \in D \text{ and } x \notin B\} \\ &= \{x \in \mathbb{N} : x \text{ is an odd natural number and } x \text{ is not divisible by 3}\} \\ &= \{x \in \mathbb{N} : x \text{ is an odd natural number that is not divisible by 3}\} \end{aligned}$$

(d)

$$\begin{aligned} B' &= \{x \in \mathbb{N} : x \text{ is divisible by 3}\}' \\ &= \{x \in \mathbb{N} : x \text{ is not divisible by 3}\} \end{aligned}$$

**Exercise 7.1.20.** Let \mathbb{N} be the universal set and suppose that

$$\begin{aligned} A &= \{x \in \mathbb{N} : x \text{ is divisible by 2}\} \\ B &= \{x \in \mathbb{N} : x \text{ is divisible by 3}\} \\ C &= \{x \in \mathbb{N} : x \text{ is divisible by 6}\} \\ D &= \{\text{the odd natural numbers}\} \end{aligned}$$

Specify each of the following sets. You may specify a set either by describing a property, by enumerating the elements, or as one of the four sets A, B, C, D :

- (a) $(A \cap B) \setminus C$ (c) $A \cup B \cup C \cup D$
(b) $A \cap B \cap C \cap D$

◇

Exercise 7.1.21. Let \mathbb{N} be the universal set and suppose that

$$\begin{aligned}A &= \{x : x \in \mathbb{N} \text{ and } x \text{ is even}\}, \\B &= \{x : x \in \mathbb{N} \text{ and } x \text{ is prime}\}, \\C &= \{x : x \in \mathbb{N} \text{ and } x \text{ is a multiple of 5}\}.\end{aligned}$$

Describe each of the following sets. Make your description as concise as possible.

- (a) $A \cap B$ (e) $(A \cup B)'$
(b) $(A \cap B)'$ (f) $A' \cup B'$
(c) $A' \cap B'$ (g) $B \cap C$
(d) $A \cup B$ (h) $A \cap (B \cup C)'$

◇

7.2 Properties of set operations

Now that we have the basics out of the way, let's look at some of the properties of set operations. The individual steps of the following proofs depend on *logic*; and a rigorous treatment of these proofs would require that we introduce formal logic and its rules. However, many of these logical rules are intuitive, and it should be possible for you to follow the proofs even if you haven't studied mathematical logic.

First, we give two rather obvious (but very useful) properties of \cup and \cap :

Proposition 7.2.1. Given any sets A, B , It is always true that

$$A \cap B \subset A \quad \text{and} \quad A \subset A \cup B.$$

PROOF. The style of proof we'll use here is often described as *element by element*, because the proofs make use of the definitions of $A \cap B$ and $A \cup B$ in terms of their elements.

First, suppose that x is an element of $A \cap B$. we then have:

$$\begin{array}{ll} x \in A \cap B & \text{[supposition]} \\ \Rightarrow x \in A \text{ and } x \in B & \text{[def. of } \cap \text{]} \\ \Rightarrow x \in A. & \text{[logic]} \end{array}$$

Since every element of $A \cap B$ is an element of A , it follows by the definition of \subset that $A \cap B \subset A$.

Exercise 7.2.2. Give a similar proof of the second part of Proposition 7.2.1.
 \diamond

□

Many useful properties of set operations are summarized in the following multi-part proposition:

Proposition 7.2.3. Let A , B , and C be subsets of a universal set U . Then

1. $A \cup A' = U$ and $A \cap A' = \emptyset$
2. $A \cup A = A$, $A \cap A = A$, and $A \setminus A = \emptyset$;
3. $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$;
4. $A \cup U = U$ and $A \cap U = A$;
5. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
6. $A \cup B = B \cup A$ and $A \cap B = B \cap A$;
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $(B \cap C) \cup A = (B \cup A) \cap (C \cup A)$;
8. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and $(B \cup C) \cap A = (B \cap A) \cup (C \cap A)$.

PROOF. We'll prove parts (1), (2), (5), and (7), and leave the rest to you!

(1) From our definitions we have:

$$\begin{aligned} A \cup A' &= \{x : x \in A \text{ or } x \in A'\} && \text{[def. of } \cup \text{]} \\ &= \{x : x \in A \text{ or } x \notin A\} && \text{[def. of complement]} \end{aligned}$$

But every $x \in U$ must satisfy either $x \in A$ or $x \notin A$. It follows that $A \cup A'$ includes all elements of U ; so $A \cup A' = U$.

We also have

$$\begin{aligned} A \cap A' &= \{x : x \in A \text{ and } x \in A'\} && \text{[def. of } \cap \text{]} \\ &= \{x : x \in A \text{ and } x \notin A\} && \text{[def. of complement]} \end{aligned}$$

But there is no element x that is both in A and not in A , it follows that there are no elements in $A \cap A'$; so $A \cap A' = \emptyset$.

(2) Observe that

$$\begin{aligned} A \cup A &= \{x : x \in A \text{ or } x \in A\} && \text{[def. of } \cup \text{]} \\ &= \{x : x \in A\} \\ &= A \end{aligned}$$

and

$$\begin{aligned} A \cap A &= \{x : x \in A \text{ and } x \in A\} && \text{[def. of } \cap \text{]} \\ &= \{x : x \in A\} \\ &= A. \end{aligned}$$

Also,

$$\begin{aligned} A \setminus A &= A \cap A' && \text{[def. of } \setminus \text{]} \\ &= \emptyset. && \text{[by part 1]} \end{aligned}$$

(5) For sets A , B , and C ,

$$\begin{aligned} A \cup (B \cup C) &= A \cup \{x : x \in B \text{ or } x \in C\} && \text{[def. of } \cup \text{]} \\ &= \{x : x \in A \text{ or } x \in B \text{ or } x \in C\} && \text{[def. of } \cup \text{]} \\ &= \{x : x \in A \text{ or } x \in B\} \cup C && \text{[def. of } \cup \text{]} \\ &= (A \cup B) \cup C. && \text{[def. of } \cup \text{]} \end{aligned}$$

A similar argument proves that $A \cap (B \cap C) = (A \cap B) \cap C$.

(7) We show that these two sets are equal by showing that:

- (I) Every element x in $A \cup (B \cap C)$ is also an element of $(A \cup B) \cap (A \cup C)$;
 (II) Every element x in $(A \cup B) \cap (A \cup C)$ is also an element of $A \cup (B \cap C)$.

(It's actually a rather common strategy to prove that two sets are equal by showing that every element of one set is an element of the other set, and vice versa.)

Let's begin by proving (I). Take any element $x \in A \cup (B \cap C)$. Then $x \in A$ or $(x \in B \cap C)$, by the definition of \cup . We may therefore consider two cases: (i) $x \in A$, or (ii) $x \in B \cap C$. (Actually some x 's are included in both cases, but that's not a problem.)

Case i: If $x \in A$, then by Proposition 7.2.1 we know $x \in A \cup B$ and $x \in A \cup C$. By the definition of \cap , we then have $x \in (A \cup B) \cap (A \cup C)$.

Case ii: If $x \in B \cap C$, then by Proposition 7.2.1 we know $x \in B$ and $x \in C$. By Proposition 7.2.1, then $x \in A \cup B$ and $x \in A \cup C$. By the definition of \cap , this means that $x \in (A \cup B) \cap (A \cup C)$.

This completes the proof of (I). Now we'll prove (II). Take any element $x \in (A \cup B) \cap (A \cup C)$. Then we may consider two cases: (i) $x \in A$, or (ii) $x \notin A$.

Case i: If $x \in A$, then by Proposition 7.2.1 it's also true that $x \in A \cup (B \cap C)$.

Case ii: Suppose $x \notin A$. Now, since $x \in (A \cup B) \cap (A \cup C)$, by the definitions of \cap and \cup we know that $(x \in A \text{ or } x \in B)$ and $(x \in A \text{ or } x \in C)$. But since $x \notin A$, it must be true that $x \in B$, and also $x \in C$. By the definition of \cap , this means that $x \in B \cap C$. by Proposition 7.2.1, we have that $x \in A \cup (B \cap C)$. This completes the proof of (II), which completes the proof of (7). \square

Exercise 7.2.4. Fill in the blanks in the following proof of Proposition 7.2.3 part (3):

Observe that

$$\begin{aligned} A \cup \emptyset &= \{x : x \in A \text{ or } x \in \emptyset\} && \text{[Def. of } \cup \text{]} \\ &= \{x : x \in \text{-----}\} && \text{[}\emptyset \text{ has no elements]} \\ &= A && \text{Def. of set } A \end{aligned}$$

and

$$\begin{aligned} A \cap \emptyset &= \{x : x \in \text{-----} \text{ and } x \in \text{-----}\} && \text{-----} \\ &= \emptyset && \text{-----} \end{aligned}$$

◇

Exercise 7.2.5. Prove parts 4,6,8 of Proposition 7.2.3 using element-by-element proofs. ◇

The following rules that govern the operations \cap, \cup and $'$ follow from the definitions of these operations:

Proposition 7.2.6. (*De Morgan's Laws*) Let A and B be sets. Then

- (1) $(A \cup B)' = A' \cap B'$;
- (2) $(A \cap B)' = A' \cup B'$.

We will use the same strategy we used to prove Proposition 7.2.3 part (7)-that is, we show that sets are equal by showing they are subsets of each other.

PROOF.

We'll prove (1), and leave (2) as an exercise. The proof will show that the sets on the left and right sides of the equality in (1) are both subsets of each other.

First we show that $(A \cup B)' \subset A' \cap B'$. Let $x \in (A \cup B)'$. Then $x \notin A \cup B$. So x is neither in A nor in B , by the definition of \cup . By the definition of $'$, $x \in A'$ and $x \in B'$. Therefore, $x \in A' \cap B'$ and we have $(A \cup B)' \subset A' \cap B'$.

To show the reverse inclusion, suppose that $x \in A' \cap B'$. Then $x \in A'$ and $x \in B'$, and so $x \notin A$ and $x \notin B$. Thus $x \notin A \cup B$ and so $x \in (A \cup B)'$. □

Exercise 7.2.7. Prove Proposition 7.2.6 part (2). ◇

Proposition 7.2.3 and Proposition 7.2.6 provide us with an arsenal of rules for set operations. You should consider these as your “rules of arithmetic” for sets: just as you used arithmetic rules in high school to solve algebraic equations, so now you can use these rules for set operations to solve set equations. Here is an example of how to do this:

Example 7.2.8. Prove that

$$(A \setminus B) \cap (B \setminus A) = \emptyset.$$

PROOF. To see that this is true, observe that

$$\begin{aligned} (A \setminus B) \cap (B \setminus A) &= (A \cap B') \cap (B \cap A') && \text{[definition of } \setminus \text{]} \\ &= A \cap A' \cap B \cap B' && \text{[by Proposition 7.2.3 parts 5 and 6]} \\ &= \emptyset \cap \emptyset && \text{[by Proposition 7.2.3 part 1]} \\ &= \emptyset. \end{aligned}$$

□

◆

Exercise 7.2.9. Prove the following statements by mimicking the style of proof in Example 7.2.8; that is use the definitions of \cap , \cup , \setminus , and $'$ as well as their properties listed in Proposition 7.2.3 and Proposition 7.2.6. This type of proof is called an “algebraic” proof. Every time you use a property, remember to give a reference!

(You may find it easiest to begin with the more complicated side of the equality, and simplify until it agrees with the other side. If you make that work, then start with the other side and simplify until the simplified versions of both sides finally agree.)

- (a) $(A \cap B) \setminus B = \emptyset.$
- (b) $(A \cup B) \setminus B = A \setminus B.$
- (c) $A \setminus (B \cup C) = (A \setminus B) \setminus C.$
- (d) $(A \cap B) \setminus (B \cap C) = A \cap B \cap C.$
- (e) $A \cup (B \setminus C)' = (A \cup C) \cup (B \cup C)'.$
- (f) $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$
- (g) $(A \cup B \cup C) \cap D = (A \cap D) \cup (B \cap D) \cup (C \cap D).$
- (h) $(A \cap B \cap C) \cup D = (A \cup D) \cap (B \cup D) \cap (C \cup D).$

◆

7.3 Do the subsets of a set form a group?

Some of the properties in Proposition 7.2.3 may ring a bell. Recall that in the Section 5.4.7 of the Modular Arithmetic chapter we defined a *group* to be a set combined with an operation that has the following properties:

1. The set is *closed* under the operation (in other words, the operation has the property of *closure*);
2. The set has a unique *identity*;
3. Every element of the set has its own *inverse*;
4. The set elements satisfy the *associative property* under the group operation;
5. *Some* groups satisfy the *commutative property* under the group operation.

If you forgot what these properties mean, look back at Section 5.4.3 and the following subsections, where we discuss these properties as applied to the integers mod n .

What we're going to do now is a first taste of a magic recipe that you're going to see again and again in Abstract Algebra. We're going to turn *sets* into *elements*. Abracadabra!

What do we mean by this? Let's take an example. Take the 3-element set $S = \{a, b, c\}$.

Exercise 7.3.1.

- (a) List the *subsets* of $S = \{a, b, c\}$. Include the empty set and non-proper subsets of S . How many subsets are in your list?
- (b) If you listed the subsets of $\{a, b\}$, how many subsets would be in your list?
- (c) If you listed the subsets of $\{a, b, c, d\}$, how many subsets would be in your list?
- (d) **If you listed the subsets of $\{a, b, c, \dots, x, y, z\}$, how many subsets would be in your list? (*Hint*)



Let's take the list of subsets of $\{a, b, c\}$ that you came up with in part (a) of the previous exercise. We can consider this list as a set of 8 elements, where each element is a subset of the original set $S = \{a, b, c\}$. Let's call this 8-element set G . Remember, the elements of G are *subsets* of the original set S .

So now let's face the question: Is G a group?

Recall that a group has a single *operation*: that is, a way of combining two elements to obtain a third element. We actually have two candidates for an operation for G : either intersection or union. So we actually have two questions:

- Is G with the operation \cup a group?
- Is G with the operation \cap a group?

We'll take these questions one at a time. First we investigate group properties for the set G with the operation \cup :

Exercise 7.3.2. Let G be the set of subsets of the set $\{a, b, c\}$.

- (a) Does the set G with the operation \cup have the closure property? *Justify* your answer.
- (b) Does the set G with the operation \cup have an identity? If so, what is it? Which part of Proposition 7.2.3 enabled you to draw this conclusion?
- (c) Is the operation \cup defined on the set G associative? Which part of Proposition 7.2.3 enabled you to draw this conclusion?
- (d) Is the operation \cup defined on the set G commutative? Which part of Proposition 7.2.3 enabled you to draw this conclusion?
- (e) Does each element of G have a unique inverse under the operation \cup ? If so, which part of Proposition 7.2.3 enabled you to draw this conclusion? If not, provide a counterexample.
- (f) Is the set G a group under the \cup operation? *Justify* your answer.

◇

Although Exercise 7.3.2 deals with a particular set of subsets, the results of the exercise are completely general and apply to the set of any subsets of *any* set (and not just $\{a, b, c\}$).

Now we'll consider \cap :

Exercise 7.3.3. Given a set A , let G be the set of all subsets of A .

- (a) Does the set G with the operation \cap have the closure property? *Justify* your answer.
- (b) Does the set G with the operation \cap have an identity? If so, what is it? Which part of Proposition 7.2.3 enabled you to draw this conclusion?
- (c) Is the operation \cap defined on the set G associative? Which part of Proposition 7.2.3 enabled you to draw this conclusion?
- (d) Is the operation \cap defined on the set G commutative? Which part of Proposition 7.2.3 enabled you to draw this conclusion?
- (e) Does each element of G have a unique inverse under the operation \cap ? If so, which part of Proposition 7.2.3 enabled you to draw this conclusion? If not, provide a counterexample.
- (f) Is the set G a group under the \cap operation? *Justify* your answer.

◇

No doubt you're bitterly disappointed that neither \cap nor \cup can be used to define a group. However, take heart! Mathematicians use these operations to define a different sort of algebraic structure called (appropriately enough) a *Boolean algebra*. We won't deal further with Boolean algebras in this course: suffice it to say that mathematicians have defined a large variety of abstract algebraic structures for different purposes.

Although \cap and \cup didn't work, there is a consolation prize:

Exercise 7.3.4. Besides \cup and \cap , there is another set operation called *symmetric difference*, which is sometimes denoted by the symbol Δ and is defined as:

$$A\Delta B = (A \setminus B) \cup (B \setminus A).$$

Given a set U , let G be the set of all subsets of U . Repeat parts (a)–(f) of Exercise 7.3.3, but this time for the set operation Δ instead of \cap . ◇

7.4 Hints for “Set Theory” exercises

Exercise 7.1.3(a): A century is a collection of years,

Exercise 7.3.1(d): Guess the pattern from the previous parts of this exercise.

7.5 Study guide for “Set Theory” chapter

Section 7.1, Set Theory

Concepts:

1. Definition of a set
2. Sets of sets
3. Universal set
4. Subsets and proper subsets
5. Empty set
6. Union and intersection of sets
7. Disjoint sets
8. Complement set
9. Difference of sets

Competencies

1. Given a description of the elements of a set, list the elements (and vice versa). (7.1.2)
2. Be able to describe sets of sets. (7.1.3)
3. Be able to specify sets given operations on the sets. (7.1.14, 7.1.20)

Section 7.2, Properties of set operations

Concepts:

1. Properties of set operations
2. De Morgan’s Laws

Key Formulas

1. Given any sets A, B , it is always true that $A \cap B \subset A$ and $A \subset A \cup B$.
2. Properties of set operations: Let A, B , and C be subsets of a universal set U . Then
 - (a) $A \cup A' = U$ and $A \cap A' = \emptyset$
 - (b) $A \cup A = A$, $A \cap A = A$, and $A \setminus A = \emptyset$;
 - (c) $A \cup \emptyset = A$ and $A \cap \emptyset = \emptyset$;
 - (d) $A \cup U = U$ and $A \cap U = A$;
 - (e) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ and $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$;
 - (f) $A \cup B = B \cup A$ and $A \cap B = B \cap A$;
 - (g) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$;
 - (h) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.
3. De Morgan's Laws: Let A and B be sets. Then
 - (a) $(A \cup B)' = A' \cap B'$;
 - (b) $(A \cap B)' = A' \cup B'$.

Competencies

1. Prove set identities algebraically, making use of the above properties of set operations. (7.2.9)

Section 7.3, Do the subsets of a set form a group?**Concepts:**

1. Group properties (Definition 5.4.26)

Competencies

1. Be able to prove or disprove group properties of set operations. (7.3.2)

Functions: Basic Concepts

The idea of a function should be familiar to you from previous math classes. Your calculus class no doubt was all about functions defined on real numbers. In this book, we will be more interested in functions on *finite* sets. Rather than “doing things” to these functions (such as integrating and differentiating), instead we will dig more deeply into the basic nature of functions themselves. This will eventually lead us to discover profound connections between groups and functions (see the Permutations chapter).

This chapter is an adapted and expanded version of a chapter by D. and J. Morris.

8.1 The Cartesian product: a different type of set operation

In the previous chapter, we introduced set operations such as \cup and \cap . In this chapter we are going to need yet another set operation. This operation is called the “Cartesian product”, and is denoted by the symbol \times . In order to define the Cartesian product, we will first need a preliminary definition:

Definition 8.1.1. For any objects x and y , mathematicians use (x, y) to denote the *ordered pair* whose first coordinate is x and whose second coordinate is y . Two ordered pairs are equal if and only if both coordinates are equal:

$$(x_1, y_1) = (x_2, y_2) \text{ iff } x_1 = x_2 \text{ and } y_1 = y_2.$$

△

Example 8.1.2. The “coordinate plane” (or “ xy -plane”) that is used for graphing functions is one example of a set of ordered pairs. The xy -plane corresponds to $\mathbb{R} \times \mathbb{R}$ (sometimes written as \mathbb{R}^2), and is the set of ordered pairs of real numbers:

$$\mathbb{R} \times \mathbb{R} = \{(x, y) | x \in \mathbb{R}, y \in \mathbb{R}\}$$

Notice that the elements of \mathbb{R}^2 are *not* real numbers, but rather ordered pairs of real numbers. In other words,

$$x \in \mathbb{R} \text{ and } y \in \mathbb{R}, \text{ but } (x, y) \notin \mathbb{R}.$$



We arrive at our general definition of Cartesian product by replacing \mathbb{R} and \mathbb{R} in our previous example with arbitrary sets A and B :

Definition 8.1.3. For any sets A and B , we define the *Cartesian product* of A and B (denoted $A \times B$ as:

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

In other words, x is an element of $A \times B$ if and only if x is an ordered pair of the form (a, b) , where a is an element of A and b is an element of B .



Example 8.1.4.

1. $\{2, 3, 4, 5, 6, 7, 8, 9, 10, J, Q, K, A\} \times \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\} = \{\text{a standard deck of cards}\}$
2. $\{1, 2, 3\} \times \{a, b\} = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}$.
3. $\{a, b\} \times \{1, 2, 3\} = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$.



Exercise 8.1.5. In view of the previous example, is \times commutative? *Explain* your answer. ◇

Exercise 8.1.6. Specify each set by listing its elements.

- (a) $\{a, i\} \times \{n, t\}$ (c) $\{1, 2, 3\} \times \{3, 4, 5\}$
(b) $\{Q, K\} \times \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$ (d) $\{y, g, Y, G\} \times \{y, g, Y, G\}$

◇

Now $A \times B$ can be considered an operation on the sets A and B , just like $A \cup B$ and $A \cap B$. But there is a very significant difference. Recall that if A and B are both subsets of the same universal set U , then so are $A \cup B$ and $A \cap B$. This is *not* the case for $A \times B$! The operation $A \times B$ takes the sets A and B and creates another set with a *completely new* type of element!

Exercise 8.1.7. Let $A = \{a, b\}$ and let $B = \{b, c\}$.

- (a) Write the elements of $A \times B$ (there are four).
(b) What is $A \cap (A \times B)$? (Another way of thinking about this is: what elements of A are also elements of $A \times B$?)
(c) What is $B \cap (A \times B)$? (Another way of thinking about this is: what elements of B are also elements of $A \times B$?)
(d) We have shown in the previous chapter that the subsets of $\{a, b, c\}$ are closed under \cup and \cap . Are the subsets of $\{a, b, c\}$ also closed under \times ? *Explain* your answer.

◇

We have been trying to emphasize that $A \times B$ is a very different set from the sets A and B . One question we could ask is: how does the number of elements in $A \times B$ compare with the numbers of elements in the sets A and B ? By considering the above examples, you may be able to figure out a formula for yourself. Go ahead and try, before reading the answer below.

Proposition 8.1.8. Given any sets A and B , then:

$$|A \times B| = |A| \cdot |B|.$$

Here the notation " $|S|$ " means the number of elements in S .

PROOF. We can prove this formula by some creative arranging. Suppose the sets A and B have m and n elements, respectively. We may list these elements as follows:

$$A = \{a_1, a_2, a_3, \dots, a_m\} \text{ and } B = \{b_1, b_2, b_3, \dots, b_n\}.$$

It follows that the elements of $A \times B$ are:

$$\begin{array}{cccccc} (a_1, b_1), & (a_1, b_2), & (a_1, b_3), & \cdots & (a_1, b_n), \\ (a_2, b_1), & (a_2, b_2), & (a_2, b_3), & \cdots & (a_2, b_n), \\ (a_3, b_1), & (a_3, b_2), & (a_3, b_3), & \cdots & (a_3, b_n), \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ (a_m, b_1), & (a_m, b_2), & (a_m, b_3), & \cdots & (a_m, b_n). \end{array}$$

In the above table that represents the elements of $A \times B$:

- each row has exactly n elements, and
- there are m rows,

It follows that the number of entries in the table is $m \cdot n$. □

Exercise 8.1.9.

- (a) If $B = \{\text{vanilla, chocolate, strawberry}\}$, then what is $B \times \emptyset$?
- (b) Using the definition of Cartesian product, show that for any set A , $A \times \emptyset = \emptyset$.


◇

8.2 Introduction to functions

8.2.1 Informal look at functions

You have seen many examples of functions in your previous math classes. Most of these were probably given by formulas, for example $f(x) = x^3$. But


functions can also be given in other ways. The key property of a function is that it accepts inputs, and provides a corresponding output value for each possible input.


Example 8.2.1. For the function $f(x) = x^3$, the input x can be any real number. Plugging a value for x into the formula yields an output value, which is also a real number. For example, using $x = 2$ as the input yields the output value $f(2) = 2^3 = 8$. 

The following properties are true of any function f :

1. Any function has a set of allowable inputs, which we call the *domain* of the function.
2. Any function also has a set that contains all of the possible outputs, which we call the *codomain* of the function.

In Example 8.2.1, any real number can be used as the input x , so the domain is \mathbb{R} , the set of all real numbers. Similarly, any output is a real number, so the codomain can also be taken as \mathbb{R} .

Example 8.2.2. For the function $f(x) = x^2$, the input x can be any real number. The output is always a real number, so we can use \mathbb{R} as the codomain. So we can take the domain and the codomain as the same set – but we don't have to. You may have already noticed that the output of f is never a negative number, so we could have used the interval $[0, \infty) = \{x \in \mathbb{R} \mid x \geq 0\}$ as the codomain. This shows that *the codomain of a function is not unique* – you can choose a different codomain and not change the function. However, *the domain of a function is unique*. If the set of allowable inputs is changed, then the function is changed in an essential fashion. 

Example 8.2.3. $g(x) = 1/x$ is *not* a function from \mathbb{R} to \mathbb{R} . This is because 0 is an element of \mathbb{R} , but the formula does not define a value for $g(0)$. Thus, 0 cannot be in the domain of g . To correct this problem, one could say that g is a function from the set $\{x \in \mathbb{R} \mid x \neq 0\}$ of *nonzero* real numbers, to \mathbb{R} . 

Intuitively, a function from A to B can be thought of being any process that accepts inputs from the set A , and assigns an element of the set B to

each of these inputs. The process need not be given by a formula. Indeed, most of the functions that arise in science or in everyday life are not given by exact formulas, as illustrated in the following exercise.

Example 8.2.4.

1. Each point on the surface of the earth has a particular temperature right now, and the temperature (in degrees centigrade) is a real number. Thus, temperature defines a function **temp** from the surface of the earth to \mathbb{R} : $\text{temp}(x)$ is the temperature at the point x .
2. The items in a grocery store each have a particular price, which is a certain number of cents, so **price** can be thought of as a function from the set of items for sale to the set \mathbb{N} of all natural numbers: $\text{price}(x)$ is the price of item x (in cents).
3. If we let **People** be the set of all people (alive or dead), then **mother** (i.e. biological mother) is a function from **People** to **People**. For example,

$$\text{mother}(\text{Prince Charles}) = \text{Queen Elizabeth}.$$

(To avoid ambiguity, we need to say that, by “mother,” we mean “biological mother.”)

4. In contrast, **grandmother** is *not* a function from **People** to **People**. This is because people have not just one grandmother, but two (a maternal grandmother and a paternal grandmother). For example, if we say that Prince Charles wrote a poem for his grandmother, we do not know whether he wrote the poem for the Queen Mother, or for his other grandmother. A function is not ever allowed to have such an ambiguity. (In technical terms, **grandmother** is a “relation,” not a function. This will be explained in a later section)



Functions are often represented as a *table* of values.

Example 8.2.5. The following table represents the prices of items in a grocery store:

| item | price (in cents) |
|--------|------------------|
| apple | 65 |
| banana | 83 |
| cherry | 7 |
| donut | 99 |
| eggs | 155 |

This table represents a function price with the following properties:

- The domain of price is $\{\text{apple}, \text{banana}, \text{cherry}, \text{donut}, \text{eggs}\}$.
- $\text{price}(\text{banana}) = 83$.
- $\text{price}(\text{guava})$ does not exist, because guava is not in the domain of the function.
- The codomain of price can be taken as \mathbb{N} , since all our prices are natural numbers. Now of course we don't really need all of \mathbb{N} : we can kick some numbers out of \mathbb{N} that aren't actual prices, and the resulting set would still be a codomain. In fact, we could keep kicking numbers out until we get the set ...
- $\{65, 83, 7, 99, 155\}$. This “smallest possible codomain” is what we call the *range* of price . The range is the set of *actual* outputs of a function. No matter what codomain we choose, it is always true that the range is a subset of the codomain.



It is also possible to represent each row of the table by an ordered pair. For example, the first row of the table is $\text{apple} \mid 65$. This has apple on the left and 65 on the right, so we represent it by the ordered pair $(\text{apple}, 65)$, which has apple on the left and 65 on the right. The second row is represented by $(\text{banana}, 83)$. Continuing in this way yields a total of 5 ordered pairs (one for each row). To keep them gathered together, we can put the 5 ordered pairs into a single set:

$$\{ (\text{apple}, 65), (\text{banana}, 83), (\text{cherry}, 7), (\text{donut}, 99), (\text{eggs}, 155) \}.$$

This set of ordered pairs contains exactly the same information as a table of values, but the set is a more convenient form for mathematical manipulations.

Exercise 8.2.6. Here is a function f given by a table of values.

| x | $f(x)$ |
|-----|--------|
| 1 | 7 |
| 2 | 3 |
| 3 | 2 |
| 4 | 4 |
| 5 | 9 |

- (a) What is the domain of f ?
- (b) What is the range of f ?
- (c) What is $f(3)$?
- (d) Represent f as a set of ordered pairs.
- (e) Find a formula to represent f . (*Hint*)

◇

Example 8.2.7. Not every table of values represents a function. For example, suppose we have the following price list, which is a slight change from Example 8.2.5:

| item | price (in cents) |
|--------|------------------|
| apple | 65 |
| banana | 83 |
| cherry | 7 |
| donut | 99 |
| banana | 155 |

There's a problem here. Lines 2 and 5 of the table list two different prices for a banana. So you might pick up a banana, expecting to pay 83 cents, and end up having the cashier charge you \$1.55. This is not allowed in a function: each input must have exactly one output. So if a table represents a function, and an item appears in the left side of more than one row, then all of those rows must have the same output listed on the right side. (In such a case, the duplicate rows are unnecessary because they add no new information.) ◇

The following remark summarizes the characteristics that a 2-column table must possess if it does indeed correspond to a function.

Remark 8.2.8. A 2-column table represents a function from A to B if and only if:

1. every value that appears in the left column of the table is an element of A ,
2. every value that appears in the right column of the table is an element of B ,
3. every element of A appears in the left side of the table, and
4. no two rows of the table have the same left side, but different right sides.

△

Just as with tables, not all sets of ordered pairs represent functions. For instance, if we convert the table in Example 8.2.7 into a set of ordered pairs, we get:

$$\{ (\text{apple}, 65), (\text{banana}, 83), (\text{cherry}, 7), (\text{donut}, 99), (\text{banana}, 155) \}.$$

Do you see why this set of ordered pairs doesn't represent a function? It's because the input "banana" has two different outputs: 83 and 155 cents.

Suppose on the other hand we start with the set of ordered pairs from Example 8.2.5 and delete the ordered pair containing "donut". Our set of ordered pairs then becomes

$$C := \{ (\text{apple}, 65), (\text{banana}, 83), (\text{cherry}, 7), (\text{eggs}, 155) \}.$$

In Example 8.2.5 the domain was $A := \{\text{apple}, \text{banana}, \text{cherry}, \text{donut}, \text{eggs}\}$. However, the set C no longer tells us the price of a donut, which is one of the items in A . Therefore C doesn't specify a function on the domain A because it doesn't define an output for all possible inputs in A . This is similar to the case of $g(x) = 1/x$, which we previously saw was not a function from \mathbb{R} to \mathbb{R} because the input 0 had no output in \mathbb{R} . (However, you should note that $g(x)$ is a function if we change the domain to $\mathbb{R} \setminus \{0\}$.)

Exercise 8.2.9. Let $A = \{a, b, c, d\}$ and $B = \{1, 3, 5, 7, 9\}$. Which of the following sets of ordered pairs represent functions from A to B ?

- | | |
|---|---|
| a. $\{(a, 1), (b, 3), (c, 5), (d, 7)\}$ | g. $\{(a, a), (b, a), (c, a), (d, a)\}$ |
| b. $\{(a, 1), (b, 2), (c, 3), (d, 4)\}$ | h. $\{(a, 1), (b, 3), (c, 5), (d, 5), (e, 3)\}$ |
| c. $\{(a, 1), (b, 3), (c, 5), (d, 3)\}$ | i. $\{(1, a), (3, a), (5, a), (7, a), (9, a)\}$ |
| d. $\{(a, 1), (b, 3), (c, 5), (d, 7), (a, 9)\}$ | j. $\{(c, 1), (b, 3), (a, 7), (d, 9)\}$ |
| e. $\{(a, 1), (b, 3), (c, 5)\}$ | k. $A \times B$ |
| f. $\{(a, 1), (b, 1), (c, 1), (d, 1)\}$ | |

◇

Exercise 8.2.10. In Exercise 8.2.9, those sets that correspond to functions from A to B are subsets of $A \times B$. Explain why the set of ordered pairs describing a function from A to B must necessarily be a subset of $A \times B$. ◇

In summary, a set of ordered pairs C is a function from A to B if and only if :

- $C \subset A \times B$
- each input $a \in A$ is part of an ordered pair in C
- and each input $a \in A$ is paired with only one output $b \in B$.

It is sometimes helpful to represent a function $f: A \rightarrow B$ by drawing an *arrow diagram*:

- a dot is drawn for each element of A and each element of B , and
- an arrow is drawn from a to $f(a)$, for each $a \in A$.

For example, suppose

- $A = \{a, b, c, d, e\}$,
- $B = \{1, 2, 3, 4\}$, and
- $f = \{(a, 1), (b, 3), (c, 4), (d, 4), (e, 3)\}$.

An arrow diagram of f is shown in Figure 8.2.1 Notice that:

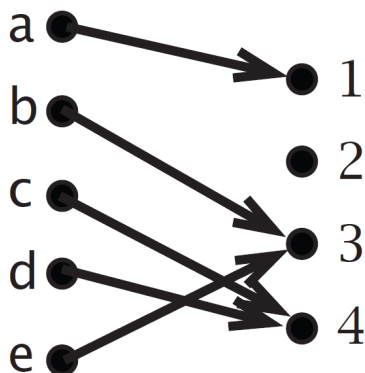


Figure 8.2.1. Arrow diagram for function f .

1. There is exactly one arrow coming out of each element of A . This is true for the arrow diagram of any function.
2. There can be any number of arrows coming into each element of B (perhaps none, perhaps one, or perhaps many). The elements of B that do have arrows into them are precisely the elements of the range of f . In this example, the range of f is $\{1, 3, 4\}$.

8.2.2 Official definition of functions

The preceding section provided some intuition about how and why functions are represented as sets of ordered pairs, and since ordered pairs are elements created by a Cartesian product, we learned how to view a function from A to B as a particular subset of $A \times B$. This view leads to our official definition of a function:

Definition 8.2.11. Suppose A and B are sets.

A set f is a **function from A to B** if

- (a) $f \subset A \times B$
- (b) $\forall a \in A, \exists$ a unique $b \in B$ s.t. $(a, b) \in f$

(Condition (b) can also be stated as follows: every $a \in A$ is in one and only one ordered pair in f).

We write “ $f: A \rightarrow B$ ” to denote that f is a function from A to B . We also call A the **domain** of f , and B the **codomain** of f .

If the pair $(a, b) \in f$, then we say that b is the **image** of a under the function f .

△

Notation 8.2.12. Suppose $f: A \rightarrow B$.

1. For $a \in A$, it is convenient to have a name for the element b of B , such that $(a, b) \in f$. The name we use is $f(a)$:

$$f(a) = b \text{ if and only if } (a, b) \in f.$$

2. Each element a of A provides us with an element $f(a)$ of B . The **range** of f is the set that includes all of these elements $f(a)$. That is,

$$\text{Range of } f = \{b \in B : \exists a \in A \text{ with } f(a) = b\}.$$

The range is always a subset of the codomain. The range can be denoted $\{f(a) \mid a \in A\}$.

△

Example 8.2.13. Suppose that the function f is defined by $f(x) = x^2$, on the domain $\{0, 1, 2, 4\}$. Then

1. to represent f as a set of ordered pairs, each element of the domain must appear exactly once as a first coordinate, with the corresponding output given in the second coordinate. Since there are four elements in the domain, there will be four ordered pairs: $\{(0, 0), (1, 1), (2, 4), (4, 16)\}$;
2. to give a table for f , we include one row for every element of the domain. The table will be:

| n | $f(n)$ |
|-----|--------|
| 0 | 0 |
| 1 | 1 |
| 2 | 4 |
| 4 | 16 |



3. if we are asked what is $f(3)$, the answer is that $f(3)$ is *undefined*, because 3 is not in the domain of f . Even though we know that $3^2 = 9$, the formula we gave for f only applies to elements that are in the domain of f ! It is not true that $f(3) = 9$;
4. the range of f is the set of possible outputs: in this case, $\{0, 1, 4, 16\}$;
5. if we are asked what is $f(2)$, the answer is $f(2) = 4$;
6. is f a function from $\{n \in \mathbb{N} \mid n \leq 4\}$ to $\{0, 1, 4, 16\}$? The answer is no, because the first set is $\{0, 1, 2, 3, 4\}$, which includes the value 3, but 3 is not in the domain of f .
7. is f a function from $\{0, 1, 2, 4\}$ to $\{n \in \mathbb{N} \mid n \leq 16\}$? The answer is yes; even though the second set has many values that are not in the range, it is a possible codomain for f . A codomain can be any set that contains all of the elements of the range.



Exercise 8.2.14. The following table describes a certain function g .

| n | $g(n)$ |
|-----|--------|
| 2 | 7 |
| 4 | 9 |
| 6 | 11 |
| 8 | 13 |
| 10 | 15 |

- (a) What is the domain of g ?
- (b) What is the range of g ?
- (c) What is $g(6)$?
- (d) What is $g(7)$?
- (e) Represent g as a set of ordered pairs.
- (f) Draw an arrow diagram to represent g .
- (g) Write down a formula that describes g .
(Express $g(n)$ in terms of n .)



Exercise 8.2.15. Suppose

- f is a function whose domain is $\{0, 2, 4, 6\}$, and
- $f(x) = 4x - 5$, for every x in the domain.

Describe the function in each of the following ways:

- (a) Make a table.
- (b) Use ordered pairs.
- (c) Draw an arrow diagram involving two sets.



Exercise 8.2.16. Which of the following sets of ordered pairs are functions from $\{x, y, z\}$ to $\{a, b, c, d, e\}$?

- If it is such a function, then what is its range?
- If it is not such a function, then explain why not.

- (a) $\{(y, a), (x, b), (y, c)\}$
- (b) $\{(y, a), (x, b), (z, c)\}$
- (c) $\{(y, a), (x, c), (z, a)\}$



Exercise 8.2.17. Which of the following are functions from $\{1, 2, 3\}$ to $\{w, h, o\}$? (If it is not such a function, then explain why not.)

- | | |
|----------------------------------|----------------------------------|
| (a) $\{(1, w), (1, h), (1, o)\}$ | (c) $\{(1, h), (2, o), (3, w)\}$ |
| (b) $\{(1, h), (2, h), (3, h)\}$ | (d) $\{(w, 1), (h, 2), (o, 3)\}$ |

◇

Exercise 8.2.18. For the given sets A and B , write each function from A to B as a set of ordered pairs. (It turns out that if $|A| = m$ and $|B| = n$, then the number of functions from A to B is n^m . Do you see why?)

1. $A = \{a, b, c\}$, $B = \{d\}$
2. $A = \{a, b\}$, $B = \{c, d\}$
3. $A = \{a\}$, $B = \{b, c, d\}$
4. $A = \{a, b\}$, $B = \{c, d, e\}$
5. $A = \{a, b, c\}$, $B = \{d, e\}$

◇

8.3 One-to-one functions

8.3.1 Concept and definition

We begin this section with an example.

Example 8.3.1.

- Suppose Inspector Gadget knows two facts:
 1. Alice is the thief's wife, and
 2. Alice is Bob's wife.

Then the inspector can arrest Bob for theft, because a person cannot (legally) be the wife of more than one husband.¹

- On the other hand, suppose the inspector knows:
 1. Alice is the forger's mother, and
 2. Alice is Charlie's mother.

Then the inspector does not know enough to be sure who the forger is, because it could be some other child of Alice.

¹According to U.S. law as of 2017.

This example illustrates a fundamental difference between the *wife* function and the *mother* function: two different people can have the same mother, but only one person can have any particular person as their legal wife. In mathematical terms, this important property of the *wife* function is expressed by saying that the *wife* function is *one-to-one*. ♦

Example 8.3.2. Now let's revisit the function we saw in Example 8.2.4 part (1). *Temp* is the function from the set of points on the earth to the set of measured temperatures at those points. Is *Temp* a one-to-one function? Not at all: it's very likely that at any given time, at least two points on the equator have exactly the same temperature (to arbitrary precision). ²

Another way to say this is that at any given time,

there exists a temperature b for which we can find two points on earth x
and y such that $\text{Temp}(x) = \text{Temp}(y) = b$.

♦

Exercise 8.3.3. Is the function *AtomicNumber* from the set of chemical elements to the set of natural numbers a one-to-one function? Explain why or why not. ♦

Remark 8.3.4. If you have an arrow diagram of a function, then it is easy to tell whether or not the function is one-to-one. For example:

1. The function f in Figure 8.3.1(a) is *not* one-to-one. This is because the arrow from b and the arrow from c go to the same place, so $f(b) = f(c)$. In general, if arrows from two different elements of the domain go to the same element of the range, then the function is not one-to-one.
2. The function g of Figure 8.3.1(b) is one-to-one. This is because the arrows from two different elements of the domain never go to the same element of the range. In short, there is only *one* element of the domain that goes *to* any *one* element of the range.

△

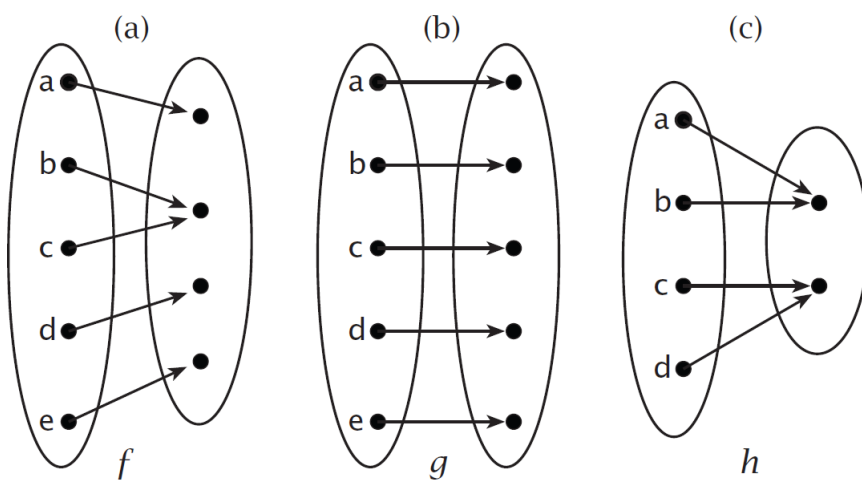


Figure 8.3.1. Arrow diagrams of three functions f , g , and h .

Exercise 8.3.5. Is function h of Figure 8.3.1 one-to-one? Explain why or why not. \diamond

This concept of one-to-one is very useful. If we know A is a function, we know that every input of A has exactly one output. But if we know that A is a one-to-one function, then we also know that every output in the range of A is caused by *exactly* one input. Alternatively, we can say that every potential output in the codomain has *at most one* input.

We have given an informal idea of the meaning of one-to-one—now it's time for a formal definition.

Definition 8.3.6. Suppose f is a function with domain A and codomain B . We say f is **one-to-one** iff for all $a_1, a_2 \in A$ such that $f(a_1) = f(a_2)$, we have $a_1 = a_2$. \triangle

Some higher math books use the fancy term **injective** instead of one-to-one. It means the same thing.

Exercise 8.3.7.

²It's not only likely: it's a sure thing. This can be proven mathematically, given that Temp is a continuous function. Can you prove it?

Each of the following sets of ordered pairs is a function from $\{1, 2, 3, 4\}$ to $\{a, b, c, d, e\}$. Either prove that the function is one-to-one, or prove that it is not.

- (a) $f = \{(1, a), (2, b), (3, d), (4, e)\}$ (d) $i = \{(1, e), (2, e), (3, e), (4, e)\}$
 (b) $g = \{(1, c), (2, d), (3, d), (4, e)\}$ (e) $j = \{(1, a), (2, c), (3, e), (4, c)\}$
 (c) $h = \{(1, e), (2, d), (3, c), (4, b)\}$ (f) $k = \{(1, a), (2, c), (3, e), (4, d)\}$

◇

Exercise 8.3.8. Notice that in part (a) of the previous problem, it's not true that every element in the codomain is the image of an element of the domain. Explain why this doesn't prevent the function f from being one-to-one. ◇

8.3.2 Proving that a function is one-to-one

The concept of one-to-one will be very important in this course, and one of the tools we will need is the ability to prove that a function is one-to-one. Though many of the functions we will encounter throughout this book are not algebraic, we will learn this style of proof using algebraic functions, as they are a bit easier to deal with. Here are some examples of this type of proof.

Example 8.3.9. Determine which of the following functions are one-to-one. If so, give a proof. If not, give a counterexample.

- (a) $f: \mathbb{R} \rightarrow \mathbb{R}$, defined by $f(x) = x + 1$.

Let's go back to the definition of one-to-one. Suppose we know that $f(x) = f(y)$, where x, y are real numbers. Can we conclude that $x = y$? If so, then that means that f is one-to-one.

So let's follow through on this. $f(x) = f(y)$ means that $x + 1 = y + 1$. Subtracting 1 from both sides of the equation, we find that indeed, $x = y$. Hence, f is one-to-one, according to the definition.

(b) $f: \mathbb{C} \rightarrow \mathbb{R}$ by $f(z) = \operatorname{Re}[z]$.

Let's start the same way as the previous example. Suppose we know that $f(z) = f(w)$, where w, z are complex numbers. Can we conclude that $w = z$? In this case, $f(z) = f(w)$ simply means that the real parts of z and w are equal. But there are many complex numbers in \mathbb{C} which have the same real part: for example, $2 + i$ and $2 + 2i$. Since $f(2 + i) = f(2 + 2i)$, it's not always true that $f(z) = f(w)$ implies $z = w$. This single counterexample is enough to prove that f is not one-to-one.

(c) $f: A \rightarrow \mathbb{R}$, where $f(z) = \operatorname{Re}[z]$ and $A = \{z \in \mathbb{C} : \operatorname{Im}[z] = 4\}$.

Notice that the function is the same as in the previous example, but the domain is different. This makes a big difference, and we don't get the same answer with this new domain. How can that be? Well, let's try to do the same as before, and see what goes haywire. Once again, suppose we know that $f(z) = f(w)$, where $w, z \in A$. As before, this means that $\operatorname{Re}[z] = \operatorname{Re}[w]$. But since $z, w \in A$, we also know that $\operatorname{Im}[z] = \operatorname{Im}[w] = 4$. Since z and w have the same real and imaginary parts, they are equal. So f is one-to-one.

(d) $g: \mathbb{R} \rightarrow \mathbb{R}$, defined by $g(x) = |x|$.

We demonstrate this by finding two distinct real numbers whose image is the same:

$$g(1) = |1| = 1 = |-1| = g(-1),$$

but $1 \neq -1$. This shows that g is *not* one-to-one.

(e) $h: \mathbb{N} \rightarrow \mathbb{N}$, defined by $h(x) = |x|$.

Since all natural numbers are nonnegative, we have $|x| = x$ for every natural number x . So given that $h(x) = h(y)$, we can argue as follows:

$$h(x) = h(y) \Rightarrow |x| = |y| \Rightarrow x = y.$$

Hence h is one-to-one. (Note that the function h agrees with g in the previous example, but the result is different because the domains are different.)

(f) $h: \mathbb{R} \rightarrow \mathbb{R}$, defined by $h(x) = -x^2 + 7x - 4$.

If we try to apply the definition directly as above, we run into complications. So we try an indirect approach. We know how to solve $h(x) = y$ using the quadratic formula:

$$h(x) = y \Rightarrow -x^2 + 7x - 4 = y \Rightarrow x = \frac{7 \pm \sqrt{33 - 4y}}{2}.$$

The \pm is a tipoff that in some cases there may be two values of x that give the same y . We're free to choose y , so let's choose a value that gives a simple result. Take $y = 8$ for instance, which gives us:

$$x = \frac{7 \pm 1}{2} \text{ or } x = 3, 4.$$

We can verify that in fact $h(3) = 8$ and $h(4) = 8$. Since in this case two different x 's give the same y , it follows that h is not one-to-one.

This example gives us a chance to point out a common mistake. Suppose we chose $y = 33/4$ instead of $y = 8$. Then we would get $x = 7/2$ as the unique value x such that $f(x) = 33/4$. But this is *not* enough to prove that h is one-to-one. In order to be one-to-one, each y be the image of at most one x for *all* possible values of y in the codomain.



Remark 8.3.10. In previous classes you may have seen the *horizontal line test* to show whether or not a function $f : \mathbb{R} \rightarrow \mathbb{R}$ was one-to-one. We may show how this works using the function $f(x) = x + 1$ (which we already know is one-to-one from Example 8.3.9 above). Figure 8.3.2 is the graph of f , together with the graph of a horizontal line (dotted line).

Now, the the horizontal line has an equation of the form $y = c$ (Why is this?). Any solution of the equation $f(x) = c$ corresponds to a point of intersection between the graphs of $y = c$ and $y = f(x)$. Now here's the key point. If for *every* horizontal line there's at most one intersection for *every* horizontal line, then for *every* real number c , the equation $f(x) = c$ has at most one solution—which is the same thing as saying that $f(x)$ is one-to-one. We may state this result in general as follows:

(*Horizontal line test for one-to-oneness*) The function $f : \mathbb{R} \rightarrow \mathbb{R}$ is one-to-one if and only if the graph of $f(x)$ intersects every horizontal line *at most once*.

So the horizontal line test proves that f is a one-to-one function, right? Alas, pictures are not proofs—although they can be pretty convincing. Typically, a mathematician will use pictures to convince herself of what's true

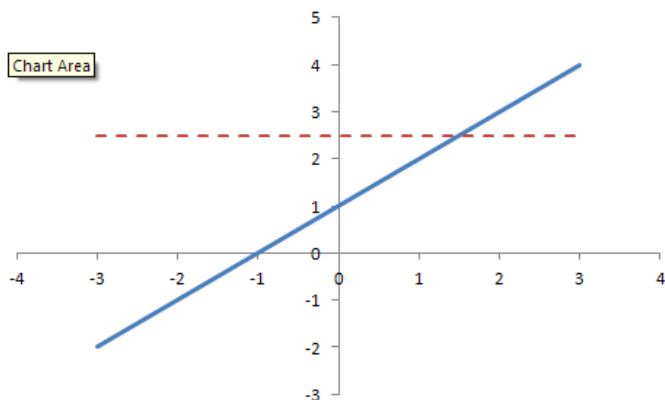


Figure 8.3.2. Graph of function $f(x) = x + 1$ (with horizontal line used for horizontal line test).

before attempting a real proof. (It's a lot easier to prove something when you're confident that it must be true.)

On the other hand, to disprove a function is one-to-one, you only need a single counterexample. Consider the function $g(x) = |x|$ from Part 2 of Example 8.3.9, which is graphed in Figure 8.3.3. Using the graph we can easily identify two values in the domain that produce the same value in the codomain. However, while the horizontal line test here suggests our counterexample, we still need to verify that the counterexample works. So again we need the disproof in Part 2 of Example 8.3.9, not just a picture.

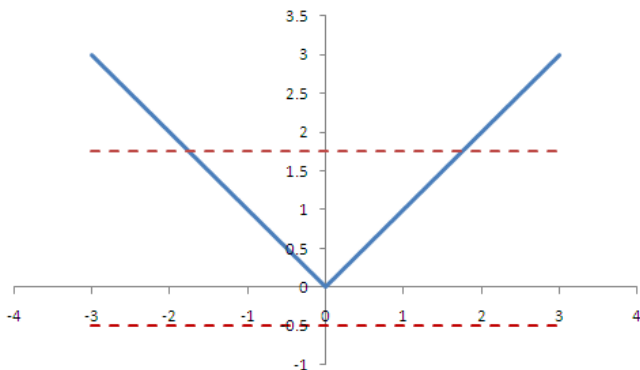


Figure 8.3.3. Graph of function $f(x) = |x|$ (with horizontal lines used for horizontal line test).

In summary, the horizontal line test can only *suggest* whether or not a function is one-to-one. In the end, you still need to prove or disprove. Furthermore, the horizontal line test is usually only a good tool for functions whose domain and codomain are \mathbb{R} (or subsets of \mathbb{R}). \triangle

Exercise 8.3.11. Suppose that the function f has domain $[a, b]$ and codomain $[c, d]$ (where for example $[a, b]$ signifies the interval $\{a \leq x \leq b, x \in \mathbb{R}\}$). State the horizontal line test for one-to-one functions in this case. What changes, if any, need to be made in the horizontal line test for $f : \mathbb{R} \rightarrow \mathbb{R}$? \diamond

Exercise 8.3.12. Graph each function and use the horizontal line test to determine whether or not the following functions are one-to-one.

- (a) $f : [0, \pi] \rightarrow \mathbb{R}, f(x) = \cos(x)$.
- (b) $f : [0, \pi] \rightarrow [-1, 1], f(x) = \sin(x)$.
- (c) $f : [-\pi, \pi] \rightarrow [-1, 1], f(x) = \cos(x/2)$.
- (d) $f : [-\pi, \pi] \rightarrow [-10, 10], f(x) = \sin(x/2)$.
- (e) $f : [1, 3] \rightarrow [0, 5], f(x) = 6 - 2x$.

\diamond

Exercise 8.3.13.

- (a) Sketch the function $f : \mathbb{R} \rightarrow \mathbb{R}$, where $f(x) = x(x - 2)(x + 2)$.
- (b) Using the horizontal line test, determine whether f is a one-to-one function.
- (c) Now consider the same function f , but restricted to the domain $[-1, 1]$ (that is, the interval $-1 \leq x \leq 1$). Is the function still one-to-one? *Explain* your answer.

\diamond

When you don't know whether or not a particular function is one-to-one, a good strategy is to try to prove that it's one-to-one. If the proof works,

then great you're done. If the proof fails, the manner in which it fails may indicate an example to show that the function is not one-to-one. Here's an example of this technique.

Example 8.3.14. Let $f: \mathbb{N} \rightarrow \mathbb{N}$ be defined by $f(n) = (n - 2)^2 + 1$. Is f one-to-one?

(Aside: Please take note of the domain in this problem. As we've noted previously, a function may be one-to-one on one domain, and not on a different domain.)


First let's try to prove that f is one-to-one. Start with arbitrary elements $m, n \in \mathbb{N}$, and suppose that $f(m) = f(n)$. By the definition of f , this means that $(m - 2)^2 + 1 = (n - 2)^2 + 1$, or $(m - 2)^2 = (n - 2)^2$. Two numbers have the same square, if and only if they are equal in absolute value, so it follows that $m - 2 = \pm(n - 2)$. There are now two cases:

- If $m - 2 = +(n - 2)$ then adding 2 to each side, we get $m = n$.
- If $m - 2 = -(n - 2) = -n + 2$, then adding 2 to each side, we get $m = -n + 4$.

Since $m, n \in \mathbb{N}$, it's not hard to see that if $n \geq 4$, then $-n + 4$ is not a natural number. But if n is 1,2,3 then $-n + 4 \in \mathbb{N}$. For example $n = 1$ gives $m = 3$, which suggests that $f(1) = f(3)$. We may indeed check that $f(1) = f(3)$.

Now the great thing about cases where f is not one-to-one is that the writeup of the solution is very simple. All you have to do is give one example of two different values that return the same function value. In the current example we have:

Solution: f is *not* one-to-one because $f(1) = 2$ and $f(3) = 2$.

So the writeup is easy: two values is all it takes. The hard thing is finding the two values! 

There is an equivalent way to show functions are one-to-one that is also useful. To see it, recall the wife function from the beginning of the section. The wife function is one-to-one because one woman can't be (legally) married to two different husbands. We can express the same thing in a different way by saying that two different husbands must be married to two different wives. These two statements are *contrapositives* of each other, and are in fact

equivalent. (“contrapositive” is a logical term—you may have run across it before in other math classes.)

If we generalize this reasoning to arbitrary one-to-one functions, we have the following two equivalent statements:

- A function is one-to-one iff any element of the range is mapped from only one element of the domain;
- A function is one-to-one iff two different elements of the domain always map to two different elements of the range.

We formalize this equivalence in the following alternative definition of one-to-one:

Definition 8.3.15. (*Alternate*) Suppose $f: A \rightarrow B$. We say f is a **one-to-one function** iff for all $a_1, a_2 \in A$ such that $a_1 \neq a_2$, we have $f(a_1) \neq f(a_2)$. \triangle

Here is an example of how to use this definition in a proof:

Example 8.3.16.

Let $g: \mathbb{Z}_{23} \rightarrow \mathbb{Z}_{23}$ be defined by $g(n) = 5 \odot n$. Is $g(n)$ one-to-one?

Solution:

Suppose $n_1, n_2 \in \mathbb{Z}_{23}$, and $g(n_1) = g(n_2)$.

Then,

$$\begin{aligned} 5 \odot n_1 &= 5 \odot n_2 && \text{[given]} \\ 5 \text{ has a multiplicative inverse, } m, \text{ in } \mathbb{Z}_{23} &&& \text{[Prop. 5.5.28]} \\ m \odot (5 \odot n_1) &= m \odot (5 \odot n_2) && \text{[substitution]} \\ n_1 &= n_2 && \text{[associativity and inverse property]} \end{aligned}$$

◆

Example 8.3.17. We know from calculus that the function $e^x: \mathbb{R} \rightarrow \mathbb{R}$ is a **strictly increasing** function since its derivative is always positive. In mathematical terms, we can say

$$x > y \text{ implies } e^x > e^y.$$

We can use this fact and Definition 8.3.15 to prove that e^x is a one-to-one function as follows:

Take any two real numbers x_1 and x_2 where $x_1 \neq x_2$. If $x_1 > x_2$, then by the above equation it follows that $e^{x_1} > e^{x_2}$. On the other hand, if $x_1 < x_2$, then by the above equation it follows that $e^{x_1} < e^{x_2}$. In either case, we have $e^{x_1} \neq e^{x_2}$. By Definition 8.3.15, it follows that e^x must be one-to-one. \blacklozenge

Exercise 8.3.18.

- (a) Show that any strictly increasing function from \mathbb{R} to \mathbb{R} is one-to-one.
- (b) Show that any strictly decreasing function from \mathbb{R} to \mathbb{R} is one-to-one.
- (c) Does the answer to (a) or (b) change if we change the domain and codomain to $[0, 1]$? *Explain* your answer.

\blacklozenge

Exercise 8.3.19. Suppose $f : \mathbb{Q} \rightarrow \mathbb{R}$ is a function such that $f(q_1) - f(q_2)$ is irrational whenever $q_1 \neq q_2$. Show that this implies that f is one-to-one. (Recall that \mathbb{Q} is the set of rational numbers.) \blacklozenge

We close this section with a bevy of exercises. Use whatever method you like, but make sure they're solid proofs.

Exercise 8.3.20.

For each of the following functions, either prove the function is one-to-one, or prove that it is not.

- (a) $f : [0, 1] \rightarrow [0, 1], f(x) = 1$.
- (b) $g : \mathbb{R}^+ \rightarrow \mathbb{R}, g(x) = x$.
- (c) $h : \mathbb{R} \rightarrow \mathbb{R}, h(x) = x^2$.
- (d) $h : \mathbb{R}^+ \rightarrow \mathbb{R}, h(x) = x^2$.
- (e) $p : [a, b] \rightarrow [3a, 3b + 10], p(x) = 3x + 2$.
- (f) $q : \mathbb{R} \rightarrow \mathbb{R}, q(x) = \frac{1}{|x+1|+1}$.

- (g) $r : [-1, 1] \rightarrow [0, 1], r(x) = \frac{1}{|x+1|+1}$.
- (h) $s : \mathbb{R} \rightarrow \mathbb{R}, s(x) = (x+1)(x+2)(x+3)$.
- (i) $t : \mathbb{R}^+ \rightarrow \mathbb{R}^+, t(x) = (x+1)(x+2)(x+3)$.

◇

Exercise 8.3.21. For each function, either prove that it is one-to-one, or prove that it is not.

- (a) $f : \mathbb{Q} \rightarrow \mathbb{Q}$ defined by $f(r) = \frac{3}{5}r - 2$.
- (b) $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = (x+2)^2$.
- (c) $f : \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(n) = (n+2)^2$.
- (d) $f : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $f(n) = (n-1)n(n+1) + 1$.
- (e) $f : \mathbb{N} \rightarrow \mathbb{N}$ defined by $f(n) = (n-1)n(n+1) + 1$.
- (f) $f : A \rightarrow A$ defined by $f(x) = (x-1)x(x+1)$, where $A = \{x \in \mathbb{R} \text{ and } x > 1\}$ (requires calculus).
- (g) $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = \left\lfloor \frac{x+1}{2} \right\rfloor$.

◇

Exercise 8.3.22. For each function, either prove that it is one-to-one, or prove that it is not.

- (a) $g : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$ defined by $g(n) = n \oplus 2$.
- (b) $g : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$ defined by $g(x) = x \oplus x$.
- (c) $g : \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$ defined by $g(n) = n \odot 2$.
- (d) $g : \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$ defined by $g(n) = n \odot 2$.
- (e) $g_a : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g_a(n) = n \odot a$, where a can be any fixed element of \mathbb{Z}_7 .
- (f) $f_b : \mathbb{Z}_{32} \rightarrow \mathbb{Z}_{32}$ defined by $f_b(n) = n \odot b$, $b \in \mathbb{Z}_{32}$, and b is odd.



- (g) $f_b: \mathbb{Z}_{188} \rightarrow \mathbb{Z}_{188}$ defined by $f_b(n) = n \odot b$, $b \in \mathbb{Z}_{188}$, and b is even.
- (h) $g: \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$ defined by $g(n) = n \odot n \odot n$.
- (i) $g: \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g(n) = n \odot n \odot n$.

◇

Exercise 8.3.23. For each function, either prove that it is one-to-one, or prove that it is not.

- (a) $g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C} \setminus \{0\}$ defined by $g(z) = z^{-1}$.
- (b) $r: A \rightarrow \mathbb{R}$ defined by $r(z) = \operatorname{Re}[z] + \operatorname{Im}[z]$, where $A = \{z \in \mathbb{C} : \operatorname{Im}[z] > 0\}$.
- (c) $g: \mathbb{C} \rightarrow \mathbb{C}$ defined by $g(z) = az + b$ where a and b are fixed complex numbers and $a \neq 0$.
- (d) $g: \mathbb{C} \rightarrow \mathbb{C}$ defined by $g(z) = z^3$.
- (e) Let $n \in \mathbb{Z}$ and let $h_n: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C} \setminus \{0\}$ be defined by $h_n(z) = z^n$. For which values of n is the function $h(z)$ a one-to-one function? *Prove* your answer.

◇

8.4 Onto functions



8.4.1 Concept and definition

In an arrow diagram of a function $f: A \rightarrow B$, the definition of a function requires that there is exactly one arrow out of each element of A , but it says nothing about the number of arrows into each element of B . There may be elements of B with lots of arrows into them (unless the function is one-to-one), and there may be other elements of B that have no arrows into them. The function is called *onto* if all of the elements of B are hit by arrows; none are missed.

Example 8.4.1. Figure 8.4.1 shows arrow diagrams of various functions, some onto and some not. In Figure 8.4.1,

- f is onto, but not one-to-one.
- g is both one-to-one and onto.
- h is neither one-to-one nor onto.
- i is one-to-one, but not onto.

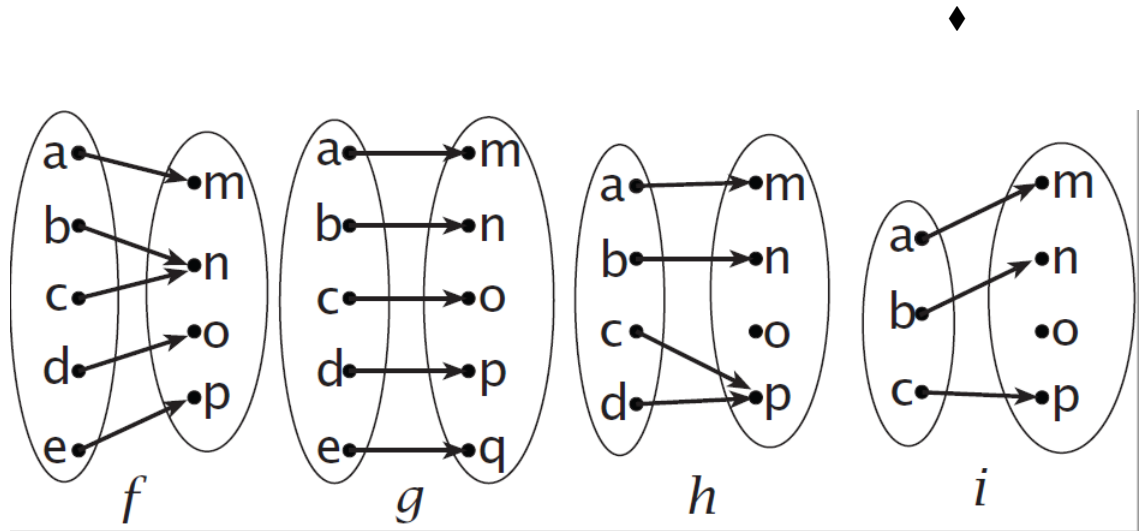


Figure 8.4.1. Arrow diagrams for various functions

Example 8.4.2. Not every woman is a mother. This means that if you draw an arrow from each person to his or her mother, there will be some women who have no arrows into them. So the function

$$\text{mother: People} \rightarrow \text{Women}$$

is *not* onto. ◆

Exercise 8.4.3. Is the function $\text{AtomicNumber: } \{ \text{Chemical Elements} \} \rightarrow \mathbb{N}$ onto? Explain why or why not. ◇

The following is the "official" definition of onto.

Definition 8.4.4. Suppose $f: A \rightarrow B$. We say f is *onto* if for all $b \in B$, there is some $a \in A$ such that $f(a) = b$. \triangle

Some higher math books use the fancy term *surjective*, which means exactly the same as onto.

You may think of onto functions as follows. If a function is onto, then no matter what element I pick in the codomain, there is always some value in the domain that produces it. Alternatively, I could say that every possible output in the codomain has *at least one* input. (Contrast this to the definition of one-to-one, which says that every possible output has *at most one* input.)

Exercise 8.4.5. If the function f is onto, then what is the relation between the range of f and the codomain of f ? (*Hint*) \diamond

Exercise 8.4.6. Each of the following sets of ordered pairs is a function from $\{1, 2, 3, 4, 5\}$ to $\{\clubsuit, \diamond, \heartsuit, \spadesuit\}$. Either prove that the function is onto, or prove that it is not.

(a) $a = \{(1, \clubsuit), (2, \diamond), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

(b) $b = \{(1, \clubsuit), (2, \heartsuit), (3, \clubsuit), (4, \heartsuit), (5, \clubsuit)\}$

(c) $c = \{(1, \heartsuit), (2, \heartsuit), (3, \heartsuit), (4, \heartsuit), (5, \heartsuit)\}$

(d) $d = \{(1, \diamond), (2, \spadesuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

(e) $e = \{(1, \clubsuit), (2, \spadesuit), (3, \heartsuit), (4, \spadesuit), (5, \clubsuit)\}$

\diamond

8.4.2 Proving that a function is onto

First we give some simple examples of onto proofs. Later we will show a more systematic approach.

Example 8.4.7.

- Consider the function: $f: \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x + 1$.

Let y be an arbitrary value in the codomain \mathbb{R} . To show that f is onto, we just need to show that for any such y , there is an x in the domain such that $f(x) = y$. Now if we set $x = y - 1$, then $f(x) = (y - 1) + 1 = y$. It's also true that x is in the domain of f , since x is a real number. This completes the proof that f is onto.

- Consider the function $h: \mathbb{N} \rightarrow \mathbb{N}$, defined by $h(x) = |x|$.

Let y be an arbitrary value in the codomain \mathbb{N} . Since all natural numbers are nonnegative, we have $|y| = y$. So we may take $x = y$, and obtain $h(x) = y$ (note x is also in the domain of h). Therefore h is onto.



Just as with one-to-one, it is typically easier to prove that a function is *not* onto. All you have to do is provide a counterexample, as the following examples show.

Example 8.4.8.

- Consider the function $f: \{1, 2, 3\} \rightarrow \{a, b, c\}$ defined by $f = \{(1, b), (2, a), (3, a)\}$. Notice that c never appears as an output in this function. This shows that f is not onto.
- Consider the function $g: \mathbb{R} \rightarrow \mathbb{R}$ defined by $g(x) = |x|$. To show that g is not onto, we only need to find a single number y in the codomain that is not mapped onto. $y = -1$ is one example, since we can never have $|x| = -1$ for any real number x . This shows that g is not onto.
- Consider the function $h: [0, 5] \rightarrow [0, 12]$ defined by $h(x) = 2x + 2$. Notice that $h(0) = 2$ and $h(x) \geq 2$ as long as $x > 0$. It follows that there is no x in the domain which is mapped to 0, which is in the codomain. This shows that h is not onto.
- Consider the function $q: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ defined by $q(x) = x \odot x$. We may list the values of $q(x)$ for $x = 0, 1, 2, 3, 4$: they are 0, 1, 4, 4, 1 respectively. There is no x such that $q(x) = 3$, so q is not onto.



Remark 8.4.9. We may use a variant of the horizontal line test to indicate whether a function $f : \mathbb{R} \rightarrow \mathbb{R}$ is onto. For instance, recall the function $f(x) = x + 1$ shown in Figure 8.3.2. In the case of an onto function, the equation $f(x) = c$ has *at least one* solution for any real value $c \in \mathbb{R}$. (Recall that for one-to-one it was *at most one*, so there's a slight difference here.) By tweaking the argument we used for the original horizontal line test, we arrive at the following general rule:

(*Horizontal line test for onto-ness*) The function $f : \mathbb{R} \rightarrow \mathbb{R}$ is onto if and only if the graph of $f(x)$ intersects every horizontal line at least once.

From Figure 8.3.2, it *appears* that $f(x) = x + 1$ is onto. Just as before, this observation doesn't qualify as a mathematical proof. Nonetheless, it strongly hints that we should try to prove onto-ness rather than looking for a counterexample.

On the other hand, the line $y = -1$ in Figure 8.3.3 does not intersect the graph of $f(x) = |x|$ defined on the set of all real numbers. This indicates that -1 is not in the range of the function. Once we've verified this mathematically, we have sufficient proof that $f(x)$ is not onto. \triangle

Exercise 8.4.10. Suppose that the function f has domain $[a, b]$ and codomain $[c, d]$, where $[a, b]$ and $[c, d]$ are intervals of real numbers. Restate the horizontal line test for onto functions in this case. What changes need to be made in the statement? \diamond

Exercise 8.4.11. Use the horizontal line test to determine whether the following functions are onto. For those functions that are not onto, give a y in the codomain which is not in the range of the function.

- | | |
|--|---|
| (a) $g : \mathbb{R} \rightarrow \mathbb{R}, g(x) = 5x - 2$ | (d) $f : [0, \pi/6] \rightarrow [0, 1/2], f(x) = \sin(x).$ |
| (b) $f : [0, \pi] \rightarrow [-1, 1], f(x) = \cos(x).$ | (e) $f : [0, \pi/4] \rightarrow [0, \sqrt{2}/2], f(x) = 1 - \cos(x).$ |
| (c) $f : [0, \pi] \rightarrow [-1, 1], f(x) = \sin(x).$ | (f) $f : [1, 3] \rightarrow [0, 5], f(x) = 6 - 2x.$ |

\diamond

We now give some examples of rigorous “onto” proofs. These proofs typically require working backwards, so some preliminary scratchwork may be helpful before writing out the actual proof.

Example 8.4.12. Define $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(x) = 5x - 2$. Determine whether g is onto.

Scratchwork 8.4.13. Just as in the previous examples, given any $y \in \mathbb{R}$ we need to find a value of x that makes $g(x) = y$. So we start with the equation $g(x) = y$ and solve for x :

$$\begin{aligned} g(x) = y &\Rightarrow 5x - 2 = y && \text{[by substitution]} \\ \Rightarrow x = \frac{y+2}{5} &&& \text{[solve for } x \text{ using basic algebra]} \end{aligned}$$

△

Now that we have a formula for x , let’s do our proof. (Although you need the scratchwork to come up with the formula for x , you don’t actually need to include the scratchwork in your proof.)

PROOF. Given $y \in \mathbb{R}$, let $x = (y + 2)/5$. Since the reals are closed under addition and non-zero division, it follows that $x \in \mathbb{R}$. Then

$$g(x) = 5x - 2 = 5 \left(\frac{y+2}{5} \right) - 2 = (y+2) - 2 = y.$$

Therefore g is onto. □

◆

Example 8.4.14. Define $h: [0, 2] \rightarrow [-7, -1]$ by $h(x) = -3x - 1$. Determine whether h is onto.

Scratchwork 8.4.15. Starting with the equation $h(x) = y$ and solving for x , we find $x = (y + 1)/(-3)$. We need to verify that x is in the domain of h whenever y is in the codomain. Notice that

$$\begin{aligned} y \geq -7 &\Rightarrow y + 1 \geq -6 && \text{[basic algebra]} \\ \Rightarrow \frac{y+1}{-3} &\leq 2 && \text{[basic algebra]} \end{aligned}$$

We also have

$$\begin{aligned} y \leq -1 &\Rightarrow y + 1 \leq 0 && \text{[basic algebra]} \\ &\Rightarrow \frac{y+1}{-3} \geq 0 && \text{[basic algebra]} \end{aligned}$$

We conclude that $0 \leq x \leq 2$, so x is in the domain of h . Thus h is onto. \triangle

Now that we have a formula for x , let's do our proof. (Although you need the scratchwork to come up with the formula for x , you don't actually need to include the scratchwork in your proof.)

PROOF. Given $y \in \mathbb{R}$, let $x = \frac{y+1}{-3}$. By basic algebra, $-7 \leq y \leq -1 \Rightarrow 0 \leq \frac{y+1}{-3} \leq 2$, so x is in the domain of h . Also,

$$h(x) = -3 \left(\frac{y+1}{-3} \right) - 1 = y.$$

Therefore h is onto. \square

\square

\blacklozenge

Example 8.4.16. Define $f: \mathbb{C} \rightarrow \mathbb{C}$ by $f(z) = z^2$. Determine whether f is onto.

Scratchwork 8.4.17. As in the previous examples, given any $z \in \mathbb{C}$ we need to find a value of w that makes $f(w) = z$. So as before we solve for w . This time it's helpful to use polar form, so we write $z = r \operatorname{cis} \theta$ and $w = s \operatorname{cis} \phi$:

$$\begin{aligned} f(w) = z &\Rightarrow (s \operatorname{cis} \phi)^2 = r \operatorname{cis} \theta && \text{[by substitution]} \\ &\Rightarrow s^2 \operatorname{cis} 2\phi = r \operatorname{cis} \theta && \text{[De Moivre's Theorem]} \\ &\Rightarrow s = \sqrt{r} \text{ and } \phi = \theta/2 \text{ is a solution} && \text{[substitution]} \end{aligned}$$

\triangle

Now that we have z , we can proceed as before.

PROOF. Given $z = r \operatorname{cis} \theta \in \mathbb{C}$, let $w = \sqrt{r} \operatorname{cis}(\theta/2)$. By the definition of polar form, $w \in \mathbb{C}$ and we have

$$f(w) = (\sqrt{r} \operatorname{cis}(\theta/2))^2 = (\sqrt{r})^2 \operatorname{cis}(2\theta/2) = r \operatorname{cis} \theta = z,$$

where we have used De Moivre's Theorem. It follows that f is onto. \square \blacklozenge

Exercise 8.4.18. For each function, either prove that it is onto, or prove that it is not.

- (a) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 1.$ (g) $q : \mathbb{R} \rightarrow (0, 1], q(x) = \frac{1}{|x|+1}.$
 (b) $g : \mathbb{R} \rightarrow \mathbb{R}, g(x) = x.$ (h) $q : \mathbb{R}^+ \rightarrow [0, 1], q(x) = \frac{1}{|x|+1}.$
 (c) $g : [-1, 1] \rightarrow [-2, 2], g(x) = x.$ (i) $[2, 4] \rightarrow [2, 10], r(x) = 4x - 6.$
 (d) $h : \mathbb{R} \rightarrow \mathbb{R}, h(x) = x^2.$ (j) $[3, 4] \rightarrow [3, 10], r(x) = 4x - 6.$
 (e) $h : [-2, 2] \rightarrow [0, 4], h(x) = x^2.$ (k) $s : \mathbb{R} \rightarrow \mathbb{R}, s(x) = \sqrt[3]{x+5} - 5.$
 (f) $p : \mathbb{R} \rightarrow \mathbb{R}, p(x) = 3x + 2.$

◇

Exercise 8.4.19. For each of the following functions, either prove that it is onto, or prove that it is not.

- (a) $g : \mathbb{C} \rightarrow \mathbb{C}$ defined by $g(z) = z^2 + 1.$
 (b) $g : \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$ defined by $g(z) = z^{-1}.$
 (c) $g : \mathbb{C} \setminus \{1\} \rightarrow \mathbb{C} \setminus \{0\}$ defined by $g(z) = (z - 1)^{-1}.$
 (d) $g : \mathbb{R} \times [0, 1] \rightarrow \mathbb{C}$ defined by $g((x, y)) = |x| \operatorname{cis}(2\pi y).$
 (e) $g : \mathbb{C} \rightarrow \mathbb{R}$ defined by $g(z) = |z|.$

◇

Exercise 8.4.20. For each of the following functions, either prove that it is onto, or prove that it is not.

- (a) $g : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$ defined by $g(x) = x \oplus x.$
 (b) $g : \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ defined by $g(x) = (x \odot 2) \oplus 3.$
 (c) $g : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g(x) = (x \odot x) \oplus 1.$
 (d) $g : \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ defined by $g(x) = x \odot x \odot x.$
 (e) $g : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g(x) = x \odot x \odot x.$
 (f) $g : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g(n) = n \odot x$, where x can be any fixed element of \mathbb{Z}_7 .

(g) $f: \mathbb{Z}_{32} \rightarrow \mathbb{Z}_{32}$ defined by $f(n) = n \odot b$, $b \in \mathbb{Z}_{32}$, and b is odd.

(h) $f: \mathbb{Z}_{188} \rightarrow \mathbb{Z}_{188}$ defined by $f(n) = n \odot b$, $b \in \mathbb{Z}_{188}$, and b is even.

◇

8.5 Bijections

8.5.1 Concept and definition

Some “especially nice” functions are both one-to-one and onto.

Definition 8.5.1. A function is a *bijection* if and only if it is both one-to-one and onto. △

In words, a bijection has the following properties:

- All inputs have only one output (function)
- All outputs are paired with only one input (one-to-one)
- And all possible outputs of the codomain are paired (onto)

Example 8.5.2. Consider a hypothetical country Z , in which

- every person is married to at least one other person (no singles),
- everyone is married to at most one other person (no polygamists or polyandrists), and
- every marriage is between a man and a woman (no same-sex marriages).

Let $\text{Men} = \{\text{male inhabitants of } Z\}$, and $\text{Women} = \{\text{female inhabitants of } Z\}$. Then the function $\text{wife}: \text{Men} \rightarrow \text{Women}$ is a bijection, since:

- Two different men cannot have the same wife, so we know that wife is one-to-one.

- Every woman is the wife of some man (because everyone is married), so *wife* is also onto.

Similarly, the function $\text{husband}: \text{Women} \rightarrow \text{Men}$ is also a bijection. \blacklozenge

Remark 8.5.3. In the country Z described above, it is clear that the number of men is exactly equal to the number of women. (If there were more men than women, then not every man could have a wife; if there were more women than men, then not every women could have a husband.) This is an example of the following important principle:

If A and B are finite sets, and there exists a bijection from A to B , then A and B have the same number of elements.

Finding a bijection is one way to show two sets have the same number of elements. \triangle

Exercise 8.5.4. Draw an arrow diagram of a bijection. \diamond

Exercise 8.5.5. Is the function $\text{AtomicNumber}: \{ \text{Chemical elements} \} \rightarrow \mathbb{N}$ a bijection? Justify your answer. \diamond

8.5.2 Proving that a function is a bijection

Since a bijection is both one-to-one and onto, a proof that a function is a bijection (usually) has two parts:

1. Show that the function is one-to-one.
2. Show that the function is onto.

The two parts can come in either order: it is perfectly acceptable to first prove that the function is onto, and then prove that it is one-to-one.

How would you show that function is not a bijection? You guessed it, by counterexample. You only need a counterexample that shows either the function is not onto, or is not one-to-one, because a bijection requires both.

Example 8.5.6. Define $f: [1, 3] \rightarrow [-2, 8]$ by $f(x) = 5x - 7$. Then f is a bijection.

PROOF. It suffices to show that f is both one-to-one and onto:

- (*one-to-one*) Given $x_1, x_2 \in \mathbb{R}$, such that $f(x_1) = f(x_2)$, we have

$$5x_1 - 7 = 5x_2 - 7.$$

Adding 7 to both sides and dividing by 5, we have

$$\frac{(5x_1 - 7) + 7}{5} = \frac{(5x_2 - 7) + 7}{5},$$

Which implies $x_1 = x_2$. So f is one-to-one.

- (*onto*) Given $y \in \mathbb{R}$, let $x = (y + 7)/5$. Then

$$f(x) = 5x - 7 = 5\left(\frac{y + 7}{5}\right) - 7 = (y + 7) - 7 = y.$$

We need to verify that x is in the domain of f for every y is in the codomain:

$$-2 \leq y \leq 8 \Rightarrow 5 \leq y + 7 \leq 15 \quad [\text{basic algebra}]$$

$$\Rightarrow 1 \leq \frac{y + 7}{5} \leq 3 \quad [\text{basic algebra}]$$

$$\Rightarrow x \in [1, 3] \quad [\text{substitution}]$$

So f is onto.

Since f is both one-to-one and onto, we conclude that f is a bijection.

□

◆

Exercise 8.5.7. For each function below, either prove that it's a bijection, or prove that it is not.

(a) $a : [-3, 3] \rightarrow [-20, 20], a(x) = 5x + 2$

(b) $b : [3, 5] \rightarrow [1, 5], b(x) = 2x - 5$

(c) $c : [0, 1] \rightarrow [-30, -15], c(x) = -12x - 15$

(d) $d : [-1, 1] \rightarrow [-27, 3], d(x) = -15x - 12$

(e) $e : [-1, 1] \rightarrow [-1, 1], e(x) = x^3$

(f) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = \sqrt[3]{x - 4}$

- (g) $e : \mathbb{R}^+ \rightarrow (0, 1), e(x) = \frac{1}{|x|+1}$.
- (h) $e : \mathbb{R}^+ \rightarrow [0, 1], e(x) = \frac{1}{|x|+1}$.
- (i) $f : \mathbb{R} \rightarrow \mathbb{R}, f(x) = 4x - 6$.
- (j) $g : [0, 27] \rightarrow [-5, -2], g(x) = \sqrt[3]{x} - 5$.
- (k) $h : [-1, 2] \rightarrow [0, 10], h(x) = \sqrt{(x+1)^2 + 1}$

◇

Exercise 8.5.8. Let $a, b \in \mathbb{R}$, and define $f : \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = ax + b$.

- (a) Show that if $a \neq 0$, then f is a bijection.
- (b) Show that if $a = 0$, then f is *not* a bijection.

◇

Exercise 8.5.9. Let $a, b \in \mathbb{R}$, and define $f : [1, 2] \rightarrow [4, 7]$ by $f(x) = ax + b$. Find all values of a and b such that f is a bijection. ◇

When a function is defined *piecewise*, the one-to-one and onto proofs are a little harder:

Example 8.5.10.

For instance, consider the function f from \mathbb{R} to \mathbb{R} defined by:

$$f(x) = \begin{cases} e^x & \text{if } x > 0 \\ 1 - x^2 & \text{if } x \leq 0 \end{cases}$$

By graphing this function you can see that the horizontal line tests suggest that $f(x)$ is indeed one-to-one and onto. To complete the actual proof, we may prove onto and one-to-one separately. We may prove the function is onto by proving:

- (a) If $y > 1$, there exists an $x > 0$ such that $f(x) = y$.
- (b) If $y \leq 1$, there exists an $x \leq 0$ such that $f(x) = y$.

From these two facts, it follows that $f(x)$ is onto, because no matter whether $y > 1$ or $y \leq 1$) there exists an x such that $f(x) = y$.

To show that $f(x)$ is one-to-one, we will need to show:

(c) If $x_1 > 0$ and $x_2 > 0$, then $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

(d) If $x_1 > 0$ and $x_2 \leq 0$, then $f(x_1) \neq f(x_2)$.

(e) If $x_1 \leq 0$ and $x_2 \leq 0$, then $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

From these facts it follows that $f(x)$ is one-to-one, because no matter whether $x > 0$ or $x \leq 0$) it is always true that $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. \blacklozenge

Exercise 8.5.11. Prove statements (a)–(e) in Example 8.5.10. For example, you can prove (a) as follows. Given $y > 1$, setting $x = \ln(y)$ gives $f(x) = y$ since $f(x) = e^x$ in this case. \blacklozenge

Exercise 8.5.12. Define a function f from \mathbb{R} to \mathbb{R} by:

$$f(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x + 1 & \text{if } x \leq 0. \end{cases}$$

Prove or disprove:

(a) f is onto;

(b) f is one-to-one;

\blacklozenge

Exercise 8.5.13. Define function g from \mathbb{R} to \mathbb{R} by:

$$g(x) = \begin{cases} 1/x & \text{if } x > 0 \\ x - 1 & \text{if } x \leq 0. \end{cases}$$

Prove or disprove:

- (a) g is onto; (b) g is one-to-one.

◇

Exercise 8.5.14. Define function h from \mathbb{R} to \mathbb{R} by:

$$h(x) = \begin{cases} x^3 & \text{if } |x| > 1 \\ x^{1/3} & \text{if } |x| \leq 1. \end{cases}$$

Prove or disprove:

- (a) h is onto; (b) h is one-to-one.

◇

So far we have only looked at functions from \mathbb{R} to \mathbb{R} . Of course, bijections can have different domains and ranges. We close this section with several exercises which examine bijections on various domains and codomains.

Exercise 8.5.15. For each function, either prove that it is a bijection, or prove that it is not.

- (a) $h: \mathbb{C} \setminus \{-3\} \rightarrow \mathbb{C} \setminus \{0\}$ defined by $h(z) = \frac{1}{z+3}$.
- (b) $g: A \rightarrow B$ defined by $g(z) = \frac{1}{z}$, where $A = \{z \in \mathbb{C} : 0 < |z| < 1\}$ and $B = \{z \in \mathbb{C} : |z| > 1\}$.
- (c) $f: A \rightarrow B$ defined by $f(z) = z^2$, where $A = \{r \operatorname{cis} \theta \in \mathbb{C} : r \geq 0 \text{ and } 0 \leq \theta \leq \pi/2\}$ and $B = \{r \operatorname{cis} \theta \in \mathbb{C} : r \geq 0 \text{ and } 0 \leq \theta \leq \pi\}$.
- (d) $f: A \rightarrow \mathbb{C}$ defined by $f(z) = z^4$, where $A = \{r \operatorname{cis} \theta \in \mathbb{C} : r \geq 0 \text{ and } 0 \leq \theta < \pi/2\}$.
- (e) $f: A \rightarrow \mathbb{C}$ defined by $f(z) = z^k$, where $A = \{r \operatorname{cis} \theta \in \mathbb{C} : r \geq 0 \text{ and } 0 \leq \theta < 2\pi/k\}$, where $k > 1$ is an integer. (Is it a bijection for all possible values of k ? If so then prove it, and if not find a counterexample.)
- (f) $f: [0, 1) \rightarrow \mathbb{T}$ defined by $f(\theta) = \operatorname{cis} 2\pi\theta$, where $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.

◇

Exercise 8.5.16. For each function, either prove that it is a bijection, or prove that it is not.

- (a) $g: \mathbb{Z}_9 \rightarrow \mathbb{Z}_9$ defined by $g(x) = (x \odot 3) \oplus 3$.
- (b) $g: \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g(x) = (x \odot 4) \oplus 4$.
- (c) $g: \mathbb{Z}_{11} \rightarrow \mathbb{Z}_{11}$ defined by $g(x) = x \odot 2$.
- (d) $g: \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$ defined by $g(x) = x \odot x$.
- (e) $g: \mathbb{Z}_8 \rightarrow \mathbb{Z}_8$ defined by $g(x) = x \odot x \odot x$.
- (f) $h: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ defined by $h(x) = (3 \odot x \odot x \odot x) \oplus 2$.
- (g) $h: \mathbb{Z}_4 \rightarrow \mathbb{Z}_4$ defined by $h(x) = x \odot x \odot x \odot x$.

◇

Exercise 8.5.17. Define $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ by $f(m, n) = m^2 + n - 1$.

- (a) Prove or disprove: f is onto. (*Hint*)
- (b) Prove or disprove: f is one-to-one. (*Hint*)
- (c) Prove or disprove: f is a bijection.

◇

Exercise 8.5.18. Define $g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ by $g(m, n) = (m + n, m + 2n)$.

- (a) Prove or disprove: g is onto. (*Hint*)
- (b) Prove or disprove: g is one-to-one. (*Hint*)
- (c) Prove or disprove: g is a bijection.

◇

Exercise 8.5.19. Define $g: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ by $g(m, n) = (m + n, m - n)$.

- (a) *Prove or disprove: g is onto.
- (b) Prove or disprove: g is one-to-one.
- (c) Prove or disprove: g is a bijection.

◇

Exercise 8.5.20. Suppose A , B , and C are sets. Define

$$f: (A \times B) \times C \rightarrow A \times (B \times C) \text{ by } f((a, b), c) = (a, (b, c)).$$

Show that f is a bijection.

◇

8.6 Composition of functions

8.6.1 Concept and definition

The term “composition” is a name that mathematicians use for applying one function to the result of another. Actually, this comes up fairly often in everyday life.

Example 8.6.1.

1. The father of the mother of a person is a grandfather of the person. (To be precise, it is the *maternal* grandfather of the person — and his or her other grandfather is *paternal*.) To express the relationship in a mathematical formula, we can write:

$$\forall x, (\text{grandfather}(x) = \text{father}(\text{mother}(x))).$$

A mathematician abbreviates this formula by writing

$$\text{grandfather} = \text{father} \circ \text{mother}$$

and says that the (maternal) grandfather function is the *composition* of father and mother.

2. The brother of the mother of a person is an uncle of the person, so uncle is the composition of brother and mother:

$$\forall x, (\text{uncle}(x) = \text{brother}(\text{mother}(x))),$$

or, more briefly,

$$\text{uncle} = \text{brother} \circ \text{mother}.$$

(For the sake of this example, let us ignore the issue that uncle and brother are not functions in general.)

3. The daughter of a child is a granddaughter, so granddaughter is a composition of daughter and child:

$$\text{granddaughter} = \text{daughter} \circ \text{child}.$$



Exercise 8.6.2. State the usual name for each composition. (Ignore the fact that sister, daughter, and many of the other relations are not functions in general.)

- (a) husband \circ sister
- (b) husband \circ mother
- (c) husband \circ wife
- (d) husband \circ daughter
- (e) mother \circ sister
- (f) daughter \circ sister
- (g) parent \circ parent
- (h) child \circ child
- (i) parent \circ parent \circ parent
- (j) child \circ brother \circ parent



Definition 8.6.3. Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. The *composition* of g and f (denoted $g \circ f$) is the function from A to C defined by

$$g \circ f(a) = g(f(a)) \text{ for all } a \in A.$$



The notation $g \circ f$ is read as “ g compose f ” or “ g composed with f .” Since $g \circ f(a) = g(f(a))$, the notation $g \circ f(a)$ is sometimes read as “ g of f of a .”

Example 8.6.4. Define $f: \mathbb{R} \rightarrow \mathbb{R}$ and $g: \mathbb{R} \rightarrow \mathbb{R}$ by $f(x) = 3x$ and $g(x) = x^2$. Then $g \circ f$ and $f \circ g$ are functions from \mathbb{R} to \mathbb{R} . For all $x \in \mathbb{R}$, we have

$$g \circ f(x) = g(f(x)) = g(3x) = (3x)^2 = 9x^2$$

and

$$f \circ g(x) = f(g(x)) = f(x^2) = 3(x^2) = 3x^2.$$

Notice that (in this example) $f \circ g \neq g \circ f$, so *composition is not commutative*.

◆

Warning 8.6.5. To calculate the value of the function $g \circ f$ at the point a , do *not* begin by calculating $g(a)$. Instead, you need to calculate $f(a)$. Then plug that value into the function g . This may seem strange, but it follows from the fact that $g \circ f(a)$ means the same thing as $g(f(a))$, and you're always supposed to evaluate what's inside the parentheses first and work your way outward. ◇

Exercise 8.6.6. Fill in the blanks of the following proof to show that function composition is associative.

PROOF. Suppose $f: X \rightarrow Y$, $g: Y \rightarrow W$, and $h: W \rightarrow Z$. Then

$$h \circ (g \circ f)(x) = h((g \circ f)(x)) = \underline{\langle 1 \rangle},$$

and

$$(h \circ g) \circ f(x) = (h \circ g)(\underline{\langle 2 \rangle}) = \underline{\langle 3 \rangle}.$$

Since the two right-hand sides are equal, it follows that $h \circ (g \circ f)(x) = (h \circ g) \circ f(x)$; in other words function composition is associative. □ ◇

Example 8.6.7. Figure 8.6.1 provides an arrow diagram to illustrate the composition $g \circ f$.

- Starting from any point of A , follow the arrow (for the function f that starts there to arrive at some point of B .
- Then follow the arrow (for the function g) that starts there to arrive at a point of C .

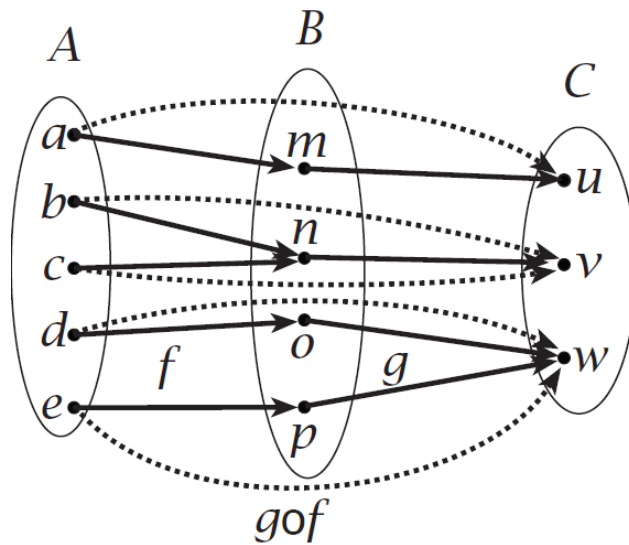


Figure 8.6.1. Arrows for the composition $g \circ f$ are dotted.

For example, the f -arrow from a leads to m and the g -arrow from m leads to u . So $g \circ f(a) = u$. Notice how we write the result as $g \circ f$ with g on the left and f on the right even though f appears on the left in Figure 8.6.1. This is an unfortunate consequence of the fact that when we calculate $g(f(x))$ we work right to left, computing $f(x)$ first and applying g to the result. ♦

Note that in the definition of $g \circ f$ (Definition 8.6.3), the domain of $g : B \rightarrow C$ is required to be equal to the codomain of $f : A \rightarrow B$. Actually $g \circ f$ can be defined as long as the domain of g contains the specified codomain of f . This is true because the codomain of a function is not unique: if $f : A \rightarrow D$ and $D \subset B$, then B is also a valid codomain of f . The reason for the requirement on the domain of g is further explored in the following exercise.

Exercise 8.6.8. Let $f : \mathbb{N} \rightarrow \mathbb{Z}_5$ defined by $f(n) \equiv n \pmod{5}$. Let $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by:

$$g(x) = x^2.$$

- Is it possible to define $f \circ g$? Explain your answer.
- Is it possible to define $g \circ f$? Explain your answer.

◇

Exercise 8.6.9. The following formulas define functions f and g from \mathbb{R} to \mathbb{R} . Find formulas for $f \circ g(x)$ and $g \circ f(x)$.

- (a) $f(x) = 3x + 1$ and $g(x) = x^2 + 2$
- (b) $f(x) = 3x + 1$ and $g(x) = (x - 1)/3$
- (c) $f(x) = ax + b$ and $g(x) = cx + d$ (where $a, b, c, d \in \mathbb{R}$)
- (d) $f(x) = |x|$ and $g(x) = x^2$
- (e) $f(x) = |x|$ and $g(x) = -x$

◇

Exercise 8.6.10. Let $A = \{1, 2, 3, 4\}$, $B = \{a, b, c, d\}$, and $C = \{\clubsuit, \diamond, \heartsuit, \spadesuit\}$. The sets of ordered pairs in each part are functions $f: A \rightarrow B$ and $g: B \rightarrow C$. Represent $g \circ f$ as a set of ordered pairs.

- (a) $f = \{(1, a), (2, b), (3, c), (4, d)\}$,
 $g = \{(a, \clubsuit), (b, \diamond), (c, \heartsuit), (d, \spadesuit)\}$
- (b) $f = \{(1, a), (2, b), (3, c), (4, d)\}$,
 $g = \{(a, \clubsuit), (b, \clubsuit), (c, \clubsuit), (d, \clubsuit)\}$
- (c) $f = \{(1, b), (2, c), (3, d), (4, a)\}$,
 $g = \{(a, \clubsuit), (b, \spadesuit), (c, \heartsuit), (d, \diamond)\}$
- (d) $f = \{(1, a), (2, b), (3, c), (4, d)\}$,
 $g = \{(a, \clubsuit), (b, \clubsuit), (c, \heartsuit), (d, \spadesuit)\}$
- (e) $f = \{(1, a), (2, b), (3, a), (4, b)\}$,
 $g = \{(a, \clubsuit), (b, \clubsuit), (c, \heartsuit), (d, \spadesuit)\}$

◇

Exercise 8.6.11. The following formulas define functions f and g from \mathbb{C} to \mathbb{C} . Find formulas for $f \circ g(x)$ and $g \circ f(x)$.

- (a) $f(r \operatorname{cis} \theta) = (r + 3) \operatorname{cis}(\theta - \pi/6)$ and $g(r \operatorname{cis} \theta) = (r \operatorname{cis} \theta)^2$
- (b) $f(a + bi) = 3a + 4bi$ and $g(a + bi) = (a + bi)^2$
- (c) $f(r \operatorname{cis} \theta) = \log r + i\theta$ and $g(a + bi) = e^a \operatorname{cis} b$ (Note the domain of f is $\mathbb{C} \setminus \{0\}$).
- (d) $f(r \operatorname{cis} \theta) = r^3 \operatorname{cis}(\theta + 2)$ and $g(r \operatorname{cis} \theta) = 2r \operatorname{cis}(\theta + 4)$
- (e) $f(z) = |z|$ and $g(z) = -z$

◇

Exercise 8.6.12. The following formulas define functions f and g from \mathbb{Z}_k to \mathbb{Z}_k for different values of k . Find formulas for $f \circ g(x)$ and $g \circ f(x)$.

- (a) $f, g : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{15}$, where $f(n) = (7 \odot n) \oplus 6$ and $g(m) = (6 \odot m) \oplus 2$
- (b) $f, g : \mathbb{Z}_{25} \rightarrow \mathbb{Z}_{25}$, where $f(n) = n \odot n$ and $g(m) = m \oplus 3$
- (c) $f, g : \mathbb{Z}_7 \rightarrow \mathbb{Z}_7$, where $f(n) = (3 \odot n) \oplus 5$ and $g(m) = (4 \odot m) \oplus 6$
- (d) $f, g : \mathbb{Z}_{20} \rightarrow \mathbb{Z}_{20}$, where $f(n) = (4 \odot n) \oplus 19$ and $g(m) = (5 \odot m) \oplus 9$
- (e) $f, g : \mathbb{Z}_q \rightarrow \mathbb{Z}_q$, where $f(n) = (a \odot n) \oplus b$ and $g(m) = (c \odot m) \oplus d$

◇

8.6.2 Proofs involving function composition

The properties of $f \circ g$ depend on the properties of f and g , and vice versa. Usually these properties are proven by using the definition of composition, along with the definitions of other functional properties. Here is one example.

Example 8.6.13. Suppose $f : A \rightarrow B$ and $g : B \rightarrow C$, where $A \subset C$. Show that if

$$g \circ f(a) = a, \text{ for every } a \in A,$$

then f is one-to-one.

Scratchwork 8.6.14. In proving such statements, it is often helpful to draw a picture (see Figure 8.6.2) showing the sets involved, and arrows joining the the different values. To show that f is one-to-one; we may show that $f(a_1) = f(a_2)$ implies $a_1 = a_2$. In the picture, we have drawn $f(a_1) = f(a_2)$. Now we are also given that $g \circ f(a) = a$, for every $a \in A$. So as the picture shows, $g(f(a_1)) = a_1$. But what about $g(f(a_2))$? On the one hand, we know $g \circ f(a_2) = a_2$ from the problem's givens. But on the other hand, since $f(a_2) = f(a_1)$ we have $g(f(a_2)) = g(f(a_1))$, or $g(f(a_2)) = a_1$. By substitution, it follows that $a_1 = a_2$. \triangle

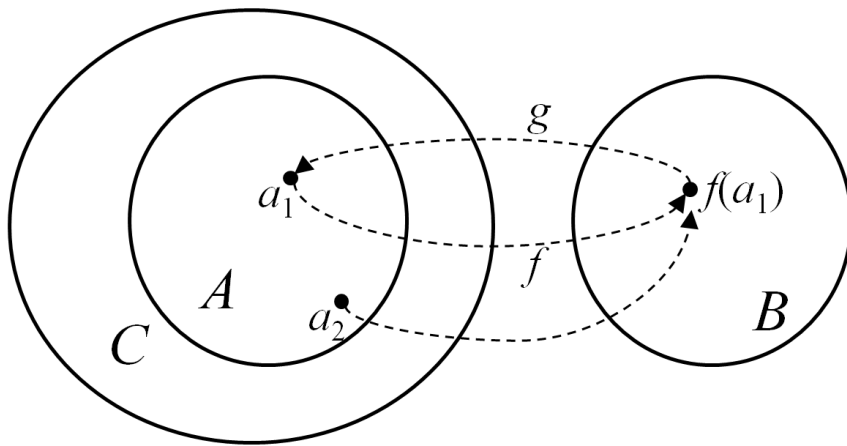


Figure 8.6.2. Scratchwork picture for Example 8.6.13.

PROOF. Given that $g \circ f(a) = a$, for every $a \in A$, by the definition of composition, this means that, for any $a_1, a_2 \in A$ we have

$$g(f(a_1)) = a_1 \text{ and } g(f(a_2)) = a_2.$$

Now suppose $f(a_1) = f(a_2)$. Then by the definition of a function,

$$g(f(a_1)) = g(f(a_2))$$

By our original hypothesis we then get $a_1 = a_2$, and thus f is one-to-one. \square \blacklozenge

Example 8.6.15. Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if f and g are onto, then $g \circ f$ is onto.

Scratchwork 8.6.16. To show that $g \circ f$ is onto, we need to show that for any $c \in C$, there exists a $a \in A$ such that $g \circ f(a) = c$. As Figure 8.6.3 shows, we can work our way backwards. Given any c , since g is onto we can find a b such that $g(b) = c$. Furthermore, since f is onto we can find a a such that $f(a) = b$. By substitution, this gives $g(f(a)) = c$, or $g \circ f(a) = c$. \triangle

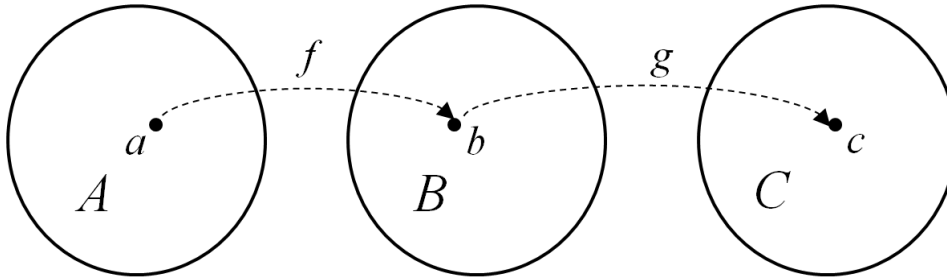


Figure 8.6.3. Scratchwork picture for Example 8.6.15.

PROOF. Let c be an arbitrary element of C . Since g is onto, there exists a b in B such that $g(b) = c$. Since f is onto, there exists a a in A such that $f(a) = b$. It follows that $g \circ f(a) = g(f(a)) = g(b) = c$. Since c is an arbitrary element of C , this implies that $g \circ f$ is onto. \square \blacklozenge

Example 8.6.17. Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if $g \circ f$ is one-to-one, and the range of f is B , then g is one-to-one.

PROOF. Suppose b_1 and b_2 are distinct elements of B . Since the range of f is B , it follows that there exist $a_1 \neq a_2$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Since $g \circ f$ is one-to-one, it follows that $g \circ f(a_1) \neq g \circ f(a_2)$. But by definition of \circ , $g \circ f(a_1) = g(f(a_1)) = g(b_1)$; and similarly $g \circ f(a_2) = g(b_2)$. By substitution, it follows that $g(b_1) \neq g(b_2)$. Thus distinct elements of B always map to distinct elements of C under the function g : which is the same as saying that g is one-to-one.

An alternative proof runs as follows. Let $c \in C$ be such that $c = g(b_1)$ and $c = g(b_2)$. Then since the range of f is B , there exist a_1 and a_2 such that $f(a_1) = b_1$ and $f(a_2) = b_2$. It follows by substitution that $g(f(a_1)) = g(f(a_2))$. But this is the same as saying that $g \circ f(a_1) = g \circ f(a_2)$. Since $g \circ f$ is one-to-one, it follows that $a_1 = a_2$. Applying f to both sides of this equation gives $f(a_1) = f(a_2)$, or $b_1 = b_2$. We have shown that for any

$c \in C$, there is at most one $b \in B$ such that $g(b) = c$. This means that g is one-to-one. \square \blacklozenge

Exercise 8.6.18.

- (a) Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if f and g are one-to-one, then $g \circ f$ is one-to-one.
- (b) Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if $g \circ f$ is one-to-one, then f is one-to-one.
- (c) Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if $g \circ f$ is onto, then g is onto.
- (d) Give an example of functions $f: A \rightarrow B$ and $g: B \rightarrow C$, such that $g \circ f$ is onto, but f is not onto.
- (e) Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if $g \circ f$ is onto, and g is one-to-one, then f is onto.
- (f) Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Show that if f is onto and $g \circ f$ is 1-1, then g is 1-1.
- (g) Define $f: [0, \infty) \rightarrow \mathbb{R}$ by $f(x) = x$. Find a function $g: \mathbb{R} \rightarrow \mathbb{R}$ such that $g \circ f$ is one-to-one, but g is *not* one-to-one.
- (h) Suppose f and g are functions from A to A . If $f(a) = a$ for every $a \in A$, then what are $f \circ g$ and $g \circ f$?

\diamond


Exercise 8.6.19. Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$. Use properties from the different examples and exercises earlier in this chapter to prove the following. In your solutions, refer to the the specific examples or exercises you are using to draw your conclusions.

- (a) Show that if f and g are bijections, then $g \circ f$ is a bijection.
- (b) Show that if f and $g \circ f$ are bijections, then g is a bijection.
- (c) Show that if g and $g \circ f$ are bijections, then f is a bijection.

◇

We have shown that various properties of $f \circ g$ follow based on properties of f and g . We can also show corresponding “negative” properties as the contrapositives of these properties.

Example 8.6.20. Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$ and g is *not* onto. Then $g \circ f$ is *not* onto.

PROOF. This is just the contrapositive of Exercise 8.6.18(c), which says that $g \circ f$ is onto implies that g is onto. \square 

Exercise 8.6.21. Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$.

- (a) Show that if f is not one-to-one, then $g \circ f$ is not one-to-one.
- (b) Prove or disprove: $g \circ f$ is a bijection if and only if both g and f are bijections.

◇

Exercise 8.6.22. Using properties from Exercises 8.6.18 and 8.6.19 (or their contrapositives), determine which of the following are bijections.

- (a) $f \circ g$ in Exercise 8.6.9 parts (a)-(e).
- (b) $f \circ g$ in Exercise 8.6.11 parts (a)-(e).
- (c) $f \circ g$ in Exercise 8.6.12 parts (a)-(e).

◇

Exercise 8.6.23. Suppose $f: A \rightarrow B$, $g: B \rightarrow A$ and $f \circ g$ is a bijection.

- (a) Give an example to show that $g \circ f$ is not necessarily a bijection.
- (b) Add the condition that g is onto. Show that in this case, $g \circ f$ must be a bijection.

◇

The following exercise leads into the next section:

Exercise 8.6.24. Suppose

- $f: A \rightarrow B$,
- $g: B \rightarrow A$,
- $g \circ f(a) = a$, for every $a \in A$, and
- $f \circ g(b) = b$, for every $b \in B$.

Show that f is a bijection.

◇

8.7 Inverse functions

8.7.1 Concept and definition

The word "inverse" commonly means something that is "backwards" or "opposite" to something else. So an inverse of a function should be a function that is somehow backwards or opposite to the original function. You have actually seen inverse functions many times before, perhaps without realizing it.

Example 8.7.1. In Example 8.5.6, we showed that $f(x) = 5x - 7$ is a bijection. A quick look at the proof reveals that the formula

$$x = \frac{y + 7}{5}$$

plays a key role. This formula is obtained by replacing $f(x)$ in $f(x) = 5x - 7$ with y , and solving for x .

In order to see $x = \frac{y+7}{5}$ as an "inverse function," we translate into the language of functions, by defining $g: \mathbb{R} \rightarrow \mathbb{R}$ by $g(y) = (y + 7)/5$. Then the above assertion can be restated as:

$$y = f(x) \Leftrightarrow x = g(y).$$

This tells us that g does exactly the opposite of what f does: if f takes x to y , then g takes y to x . We will say that g is an “inverse” of f . \blacklozenge

Example 8.7.2. Let $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ be defined by: $f(x) = x^2$. We may define $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ by: $g(y) = \sqrt{y}$. Note that in this case the domains and ranges are restricted to *positive* real numbers. Given this restriction, by the definition of square root we have

$$y = x^2 \Leftrightarrow x = \sqrt{y}.$$

In view of the definitions of f and g , we may see that this is the same formula as in the previous example: $y = f(x) \Leftrightarrow x = g(y)$. \blacklozenge

Example 8.7.3. In the previous examples, the domain and codomain were the same—but this doesn’t always have to be the case. Let $f: \mathbb{R} \rightarrow \mathbb{R}^+$ be defined by $f(x) = e^x$. We may define $g: \mathbb{R}^+ \rightarrow \mathbb{R}$ by $g(y) = \ln(y)$, where ‘ln’ denotes the natural logarithm function. Here we also obtain $y = f(x) \Leftrightarrow x = g(y)$ as before, as long as x is in the domain of f and y is in the domain of g . \blacklozenge

The \Leftrightarrow statement which has popped up in the last three examples can be re-expressed as a pair of equations involving f and g , as the following proposition shows:

Proposition 8.7.4. Suppose that $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are functions such that

$$\forall x \in X, \forall y \in Y, (y = f(x) \Leftrightarrow x = g(y)).$$

Then the following statements are also true:

- (a) $g(f(x)) = x$ for all $x \in X$. and
- (b) $f(g(y)) = y$ for all $y \in Y$,

We will furnish the proof of (a), while the proof of (b) is left as an exercise.

PROOF. The proof of (a) runs as follows. Suppose that $y = f(x) \Leftrightarrow x = g(y)$ for all x, y in the respective domains of f and g . Then for any $x \in X$, we may define z as $z = f(x)$. By the \Leftrightarrow statement it follows that $x = g(z)$. But then

we may substitute the first equation into the second and obtain $g(f(x)) = x$. Since x was an arbitrary element of X , it follows that $g(f(x)) = x$ for all $x \in X$. \square

Exercise 8.7.5. Prove part (b) of Proposition 8.7.4. \diamond

Exercise 8.7.6. Prove the converse of Proposition 8.7.4. That is, given that

$$g(f(x)) = x \text{ for all } x \in X \quad \text{and} \quad f(g(y)) = y \text{ for all } y \in Y,$$

it follows that

$$\forall x \in X, \forall y \in Y, (y = f(x) \Leftrightarrow x = g(y)).$$

\diamond

Finally, we can give the definition of an inverse function:

Definition 8.7.7. Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are functions. We say that g is an *inverse function* for the function f if and only if:

- (a) $f(g(y)) = y$ (in other words, $f \circ g(y) = y$) for all $y \in Y$, and
- (b) $g(f(x)) = x$ (in other words, $g \circ f(x) = x$) for all $x \in X$.

\triangle

Example 8.7.8. The husband of the wife of any married man is the man himself – in other words,

$$\text{husband}(\text{wife}(y)) = y.$$

Also, the wife of the husband of any married woman is the woman herself, so that

$$\text{wife}(\text{husband}(x)) = x.$$

It follows that the wife function is an inverse of the husband function. In fact, it's pretty clear that husband is the *only* inverse of wife. \blacklozenge

Exercise 8.7.9. In each case, use Definition 8.7.7 to determine whether g is an inverse of f .

- (a) $f: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f(x) = 9x - 6$ and
 $g: \mathbb{R} \rightarrow \mathbb{R}$ is defined by $g(y) = (y + 6)/9$.
- (b) $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is defined by $f(x) = 2x^2$ and
 $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is defined by $g(y) = \sqrt{y}/2$.
- (c) $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is defined by $f(x) = 2/x$ and
 $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is defined by $g(y) = 2/y$.
- (d) $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is defined by $f(x) = \sqrt{x+1} - 1$ and
 $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ is defined by $g(y) = y^2 + 2y$.

◇

8.7.2 Which functions have inverses?

It turns out that most functions do *not* have inverses.

Exercise 8.7.10. Which of the functions depicted in Figure 8.4.1 have inverses? ◇

From the previous exercise, you may have guessed the following rule:

Proposition 8.7.11. Suppose $f: X \rightarrow Y$. Then f has an inverse $g: Y \rightarrow X$ if and only if f is a bijection.

This is another “if and only if” proof, so it must be proved in both directions. We will prove the forward direction of this proposition. You will prove the reverse direction. The forward direction says that if $f: X \rightarrow Y$ has an inverse $g: Y \rightarrow X$, then f is a bijection. In other words we must assume the first statement, and from that prove that f is one-to-one and onto.

PROOF. (*forward direction*) Assume there is a function $g: Y \rightarrow X$ that is an inverse of f . Then by the definition of an inverse function,

- (a) $f(g(y)) = y$ for all $y \in Y$, and
(b) $g(f(x)) = x$ for all $x \in X$.

Suppose then that $f(x_1) = f(x_2)$ for some $x_1, x_2 \in X$. Then since g is a function we have

$$g(f(x_1)) = g(f(x_2))$$

Therefore by (b), $x_1 = x_2$. Hence f is one-to-one.

Now suppose $y \in Y$. Then since g is a function, there exists a unique $x \in X$ such that $g(y) = x$. Substituting into (a) we get

$$f(x) = y.$$

Therefore $\forall y \in Y, \exists x \in X$ s.t. $f(x) = y$. Hence f is onto. So f is both one-to-one and onto: thus f is a bijection. \square

Exercise 8.7.12. Prove the reverse direction of Proposition 8.7.11. (*Hint*)
 \diamond

A function that has an inverse is said to be *invertible*. The following exercise deals with a very important class of invertible functions/bijections.

Exercise 8.7.13. Given a number $a \in \mathbb{Z}_n$, consider the function $f_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ given by $f_a(m) = a \odot m$.

- (a) Show that the function f_6 defined on \mathbb{Z}_7 is a bijection by finding an inverse of f_6 .
- (b) For the six numbers $a = 0, 1, 2, 3, 4, 5$ in \mathbb{Z}_6 , which of these give bijections for f_a ? *Explain* your answer. Suppose that $a \in \mathbb{Z}_n$ is relatively prime to n . Show that in this case, $f_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is a bijection (you may want to refer to Section 5.5.4). (*Hint*)
- (c) Suppose that $a \in \mathbb{Z}_n$ such that $ax \equiv 1 \pmod{n}$ does *not* have an integer solution x . Show that in this case, $f_a : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ is *not* a bijection. (*Hint*)

\diamond

We close out this section with several exercises that prove various properties of inverses.

Exercise 8.7.14.

- (a) Prove that any inverse of a bijection is a bijection.

- (b) Show that the inverse of a function is *unique*: if g_1 and g_2 are inverses of f , then $g_1 = g_2$. (*Hint*)

◇

Remark 8.7.15.

- (a) Exercise 8.7.14 is key because it enables us to talk about *the* inverse of a function, since there is never more than one inverse. We will use the special notation f^{-1} to denote the inverse of the function f .
- (b) According to Definition 8.2.11, any function can be specified by a set of ordered pairs. That is, if $f : X \rightarrow Y$, we can also write $f \subset X \times Y$, where for all $x \in X$ there is a unique $y \in Y$ such that $(x, y) \in f$. If f is a function that has an inverse, f^{-1} can also be expressed as a subset of $Y \times X$:

$$f^{-1} = \{ (y, x) \mid (x, y) \in f \}.$$

This is simply a restatement of the fact that

$$y = f(x) \text{ iff } x = f^{-1}(y).$$

△

In Definition 8.7.7 we defined the inverse of a function f by specifying how it acted on single points: that is, for a function $f : A \rightarrow B$ we require f^{-1} to satisfy $f^{-1} \circ f(a) = a$ and $f \circ f^{-1}(b) = b$ for all $a \in A$ and $B \in B$. But we can look at this situation in a different way. In fact $f \circ f^{-1}$ and $f^{-1} \circ f$ are functions in their own right. What kind of functions are they? Let's see:

Definition 8.7.16. For any set A , define the *identity map* $\text{Id}_A : A \rightarrow A$ by $\text{Id}_A(a) = a$ for every $a \in A$. △

Exercise 8.7.17.

- (a) Show that Id_A is invertible. (*Hint*)
- (b) Find the inverse of Id_A . (*Hint*)

- (c) Suppose $f: X \rightarrow Y$ and $g: Y \rightarrow X$. Show that g is the inverse of f if and only if

$$f \circ g = \text{Id}_Y \text{ and } g \circ f = \text{Id}_X.$$

(*Hint*)

◇

We close this section with an exercise that shows two very important properties of inverses.

Exercise 8.7.18.

- (a) Suppose $f: A \rightarrow B$ and $g: B \rightarrow C$ are bijections. Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. (*Hint*)
- (b) Suppose $f: X \rightarrow Y$ is a bijection. Show that the inverse of f^{-1} is f . That is, $(f^{-1})^{-1} = f$.

◇

8.8 Do functions from A to B form a group?

At the end of the Sets chapter in Section 7.3 we considered the question, Do the subsets of a set form a group? Let's consider a similar question, but this time with functions.

Recall (once again) from Section 5.4.7 that a group is a set together with an operation defined on that set such that:

1. The set is *closed* under the operation (in other words, the operation has the property of *closure*);
2. The set has a unique *identity*;
3. Every element of the set has its own *inverse*;
4. The set elements satisfy the *associative property* under the group operation;

If we're going to make a group out of the set of functions from A to B , the first thing we need to do is define an operation. So far, the only operation we have on functions is composition. But this gives us a problem, because the composition of two functions that have the same domain and the same codomain isn't always well-defined:

Exercise 8.8.1. Give an example of sets A and B and two functions $f : A \rightarrow B$ and $g : A \rightarrow B$ such that the composition $f \circ g$ is *not* well-defined. \diamond

For $f \circ g$ to be well-defined, the domain of f must contain the range of g . We can guarantee this by taking $B = A$, so we consider only functions from a set A to itself:

Exercise 8.8.2. Given that $f : A \rightarrow A$ and $g : A \rightarrow A$, show that $f \circ g$ and $g \circ f$ are both well-defined functions from A to A . \diamond

Exercise 8.8.2 confirms that the set of functions from A to A is closed under the operation of composition. So far, so good—but we still have more fish to fry. We still need to find an identity for our set. This one's not hard: Definition 8.7.16 gives us the identity map Id_A .

That takes care of two group properties—we have two more to go. Let's look at inverses. We've seen that not all functions have inverses under composition. So to make this part work, we'll have to further restrict ourselves to the set of *invertible* functions from A to A .

The last thing we need to verify is the associative property. Fortunately, you already showed that function composition is associative in Exercise 8.6.6.

The foregoing discussion amounts to a proof of the following proposition.

Proposition 8.8.3. Let A be a set, and let G be the set of all invertible functions from A to A . Then G is a group under composition.

In the following exercise we look at some particular sets of functions, and investigate whether or not these sets form groups under composition. Recall that to show whether or not a set with binary operation is a group, you just need to show the properties: closure, identity, inverse, and associative. We're lucky in this case that we don't have to prove associative in every single case, because the operation of function composition is always associative, as we've proven before. So it's enough just to prove closure, identity, and inverse.

Exercise 8.8.4.

- (a) Let G_1 be the set of all nonzero functions from \mathbb{R} to \mathbb{R} of the form $f(x) = ax$, where a is a nonzero real number. (For example, the functions $g(x) = -7x$ and $h(x) = \sqrt{2}x$ are both elements of G_1 .) Prove or disprove: G_1 is a group under composition. (Note: G_1 is the set of nonzero **linear functions** from \mathbb{R} to \mathbb{R} .)
- (b) Let G_2 be the set of all nonzero functions from \mathbb{R} to \mathbb{R} of the form $f(x) = ax + b$ where a and b are real numbers which are not both zero. (For example, the functions $p(x) = 29.4x + 42.3$, $q(x) = 15$ and $r(x) = -\pi x$ are all elements of G_2 .) Prove or disprove: G_2 is a group under composition. (Note: G_2 is called the set of all nonzero **affine functions** from \mathbb{R} to \mathbb{R} .)
- (c) Let G_3 be the set of all nonconstant functions from \mathbb{R} to \mathbb{R} of the form $f(x) = ax + b$ where a is a nonzero real number and b can be any real number. Prove or disprove: G_3 is a group under composition.
- (d) Let G_4 be the set of all functions from \mathbb{R} to \mathbb{R} of the form $f(x) = ax^3$, where a is a nonzero real number. Prove or disprove: G_4 is a group under composition.
- (e) *Let G_5 be the set of all functions from \mathbb{R} to \mathbb{R} of the form

$$f(x) = \begin{cases} ax, & \text{for } x \text{ rational} \\ bx, & \text{for } x \text{ irrational} \end{cases}$$

where a and b are nonzero *rational* numbers. Prove or disprove: G_5 is a group under composition.

◇

Finally, recall that some groups are commutative (commutative groups are also called **abelian** groups). Are groups under composition always abelian? Let's find out:

Exercise 8.8.5. For each of the examples in Exercise 8.8.4 which are groups, prove or disprove that the group is abelian. To check this, you just need to check whether or not the formula $f \circ g = g \circ f$ for all f, g in the set. What this means is that if the group is not abelian, all you need to do is provide a single counterexample. ◇

8.9 Hints for “Functions: basic concepts” exercises

Exercise 8.2.6(e): There is a formula of the form $f(x) = ax^2 + bx + c$

Exercise 8.4.5: Can there be any elements in the codomain that are not in the range?.

Exercise 8.5.17(a): Consider the values $f(1, i)$ for $i = 1, 2, 3, \dots$ (b): Consider the values $f(2, j)$ and $f(1, i)$.

Exercise 8.5.18(a): Given any element (i, j) of $\mathbb{Z} \times \mathbb{Z}$, set $i = m + n$ and $j = m + 2n$ and solve for m and n in terms of i and j .

Exercise 8.5.18(b): Suppose that $g(m, n) = g(p, q)$. It follows that $(m + n, m + 2n) = (p + q, p + 2q)$.

Exercise 8.7.13: (c) Use Proposition 5.5.20, and recall that $ax \equiv 1 \pmod{n}$ means the same thing as $a \odot x = 1$ for $a, x \in \mathbb{Z}_n$. You may use this fact to find an inverse for f_a . (d) Use the fact that $a \odot x = 1$ has no solution to show that f_a is not onto, which implies that f_a has no inverse.

Exercise 8.7.17: (a) Notice that $f(x) = x$ is the identity function when the set A is equal to \mathbb{R} . Think about how you would show that $f(x)$ is invertible in this case. Then apply the same proof, replacing x with a and f with Id_A . (b) Again, think of the case $f(x) = x$. What is the inverse of this function?

Exercise 8.7.12: Given that f is a bijection from X to Y . We may define a function g from Y to X as follows. Given any $y \in Y$, since f is onto there is at least one x such that $f(x) = y$. Furthermore, since f is one-to-one there is at most one x such that $f(x) = y$. Putting these two facts together gives us that there is *exactly* one x such that $f(x) = y$. We may define $g(y)$ as this unique x . It remains to show that for any $y \in Y$, $f(g(y)) = y$; and for any $x \in X$, $g(f(x)) = x$.

Exercise 8.7.18: (a) Apply Definition 8.7.7 directly, replacing f with $g \circ f$ and g with $g^{-1} \circ f^{-1}$. (b) Apply Definition 8.7.7 again, this time replacing f with f^{-1} . What should g be replaced with?

8.10 Study guide for “Functions: Basic Concepts” chapter

Section 8.1, The Cartesian product: a different type of set operation

Concepts:

1. Ordered pairs (x, y)
2. Cartesian product of sets: the set of all ordered pairs
3. Order of a set S (i.e. number elements), denoted by $|S|$.

Key Formulas

1. Equality of ordered pairs: $(x_1, y_1) = (x_2, y_2)$ iff $x_1 = x_2$ and $y_1 = y_2$.
2. Cartesian product: $A \times B = \{(a, b) \mid a \in A, b \in B\}$ (Definition 8.1.3)
3. Order of a Cartesian product: Given any sets A and B , then:
 $|A \times B| = |A| \cdot |B|$. (Proposition 8.1.8)

Competencies

1. Given a pair of finite sets, list the elements of the Cartesian product. (Example 8.1.4, 8.1.6, 8.1.7)
2. Determine the number of elements in a Cartesian product. (8.1.9)

Section 8.2, Introduction to functions

Concepts:

1. A function accepts inputs, and provides a single output for each input.
2. Domain & codomain of functions (“inputs” and “possible outputs” of the function).
3. Range of a function (range are the “actual outputs”; range is contained in any possible codomain)

8.10 STUDY GUIDE FOR “FUNCTIONS: BASIC CONCEPTS” CHAPTER 263

4. Image of an element of the codomain: $f(a)$ is the image of a under the function f .
5. Arrow diagrams representing functions
6. “Official” definition of a function as a subset of the Cartesian product of domain and codomain (Definition 8.2.11)

Competencies

1. Be able to give the domain, range, $f(x)$, the set of ordered pairs, and write a formula to represent a function. (8.2.6, 8.2.14)
2. Be able to represent a function using: a formula; a set of ordered pairs; a 2-column table; an arrow diagram.
3. Know if a set of ordered pairs represents a function. (8.2.9, 8.2.16)

Section 8.3, One-to-one functions

Concepts:

1. One-to-one functions (injective): each element of the range is the image of a *unique* element of the domain.
2. Contrapositive of a statement: the contrapositive of a statement of the form “If A then B ” is, “If not B then not A ”. The contrapositive is logically equivalent to the original statement.

Competencies

1. Be able to identify one-to-one functions. (8.3.3, 8.3.5)
2. Be able to use the horizontal line test on real-valued functions to determine one-to-oneness. (8.3.12, 8.3.13)
3. Prove whether functions are one-to-one or not. (8.3.20, 8.3.21)

Section 8.4, Onto functions**Concepts:**

1. Onto functions (surjective): each element of the codomain is the image of *at least* one element of the domain.
2. Onto proofs
3. Horizontal line test to show onto-ness (applies only to real-valued functions)

Competencies

1. Be able to identify onto functions. (8.4.3)
2. Be able to use the horizontal line test for real-valued onto functions. (8.4.11)
3. Prove whether a function is onto or not. (8.4.18, 8.4.19, 8.4.20)

Section 8.6, Composition of functions**Concepts:**

1. Composition of two functions: apply the second function to the output of the first function. *Note:* functions are applied *right to left*.
2. Proofs involving function composition

Competencies

1. Be able to draw arrow diagrams of function compositions (Figure 8.6.1)
2. Be able to compute the composition of two functions. (8.6.2, 8.6.9)
3. 1-1 and onto proofs of compositions of functions, based on the 1-1 and onto properties of the functions being composed. (8.6.18-8.6.24)

Section 8.7, Inverse functions**Concepts:**

1. Inverse functions: the functions $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are inverses of each other iff $g(f(x)) = x$ for all $x \in X$, and $f(g(y)) = y$ for all $y \in Y$. (Definition 8.7.7)
2. A function has an inverse iff it is a bijection (both 1-1 and onto). (Theorem 8.7.11)
3. Identity map: $\text{Id}_A: A \rightarrow A$ by $\text{Id}_A(a) = a$ for every $a \in A$. (Definition 8.7.16)
4. $f: X \rightarrow Y$ and $g: Y \rightarrow X$ are inverses of each other iff $f \circ g = \text{Id}_Y$ and $g \circ f = \text{Id}_X$. (8.7.18)
5. Inverse of compositions: if $f: X \rightarrow Y$ and $g: Y \rightarrow Z$ both have inverses, then so does $g \circ f$ and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. (8.7.18)

Competencies

1. Determine whether or not g is an inverse of f . (8.7.9)
2. Prove that the invertible functions must be bijections. (Theorem 8.7.11, Exercises 8.7.12, 8.7.14)
3. Show that Id_A is invertible and find the inverse. (8.7.17)
4. Prove facts about inverse of compositions and inverse of inverse functions (8.7.18a, b, c)

Section 8.8, Do functions from A to B form a group?**Concepts:**

1. Abelian group (same as commutative group)

Competencies

1. Be able to determine whether particular sets of functions form groups under composition. (8.8.4)
2. Be able to prove whether or not a particular group of functions is abelian or not. (8.8.5)

Introduction to Cryptography

Cryptography is the study of sending and receiving secret messages. The aim of cryptography is to send messages across a channel so only the intended recipient of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic; that is, that it has not been sent by someone who is trying to deceive the recipient. Modern cryptography is heavily dependent on abstract algebra and number theory.

Prerequisites: The cryptographic systems we'll be looking at are all based on modular arithmetic. To understand this chapter, the reader should be familiar with the material in Chapters 5 and 8. Section 25.2 also uses some simple matrix multiplication.

Thanks to Tom Judson for material used in this chapter.

9.1 Overview and basic terminology

The message to be sent is called the *plaintext* message. The disguised message is called the *ciphertext*. The plaintext and the ciphertext are both written in an *alphabet*, consisting of *letters* or *characters*. Characters can include not only the familiar alphabetic characters A, ..., Z and a, ..., z but also digits, punctuation marks, and blanks. A *cryptosystem*, or *cipher*, has two parts: *encryption*, the process of transforming a

plaintext message to a ciphertext message, and **decryption**, the reverse transformation of changing a ciphertext message into a plaintext message.

There are many different families of cryptosystems, each distinguished by a particular encryption algorithm. Cryptosystems in a specified cryptographic family are distinguished from one another by a variable parameter called a **key**. A classical cryptosystem has a single key, which must be kept secret, known only to the sender and the receiver of the message. If person A wishes to send secret messages to two different people B and C , and does not wish to have B understand C 's messages or vice versa, A must use two separate keys, so one cryptosystem is used for exchanging messages with B , and another is used for exchanging messages with C .

Some systems use two separate keys, one for encoding and another for decoding. These are called **public key cryptosystems**, because typically the encoding key is made public while the decoding key is kept secret. A public key cryptosystem allows A and B to send messages to C using the same encoding key. Anyone is capable of encoding a message to be sent to C , but only C knows how to decode such a message.

On the other hand, in **single** or **private key cryptosystems** the same key is used for both encrypting and decrypting messages. To encrypt a plaintext message, we apply to the message procedure which transforms a plaintext message into an encrypted message. We will call this procedure an **encryption function**, and denote it by the letter f . Given the encrypted form of the message, we can recover the original message by applying the **decryption function** f^{-1} , which basically undoes the transformation performed by the encryption function.¹ Both the encryption function f and the decryption function f^{-1} must be relatively easy to compute; however, they must be virtually impossible to guess if only examples of coded messages are available.

In Section 9.2 we will look at private key cryptography, beginning with a classic example from antiquity. In Section 9.3 we will look at a famous example of a public key cryptosystem, which was only discovered in the last century and has had an enormous impact on information security in the digital age.

¹In fact, f^{-1} is the *inverse* of f —we will study inverse functions in general in Chapter 8.

9.2 Private key cryptography

9.2.1 Shift codes

Example 9.2.1. One of the first and most famous private key cryptosystems was the shift code used by Julius Caesar. We first represent the alphabet numerically by letting $A = 0, B = 1, \dots, Y = 24, Z = 25$. This means for example that the word BAY would be represented numerically as:

$$1, 0, 24.$$

An example of a shift encoding function is

$$f(n) = \text{mod}(n + 3, 26).$$

which can also be written as

$$f(n) = n \oplus 3,$$

with the understanding that n refers to the numerical value assigned to each letter, and \oplus refers to addition in \mathbb{Z}_{26} . This encoding function takes

$$0 \rightarrow 3, 1 \rightarrow 4, \dots, 24 \rightarrow 1, 25 \rightarrow 2,$$

so that our numerical representation of BAY is changed to: 4, 3, 1, which is the numerical representation of EDB.

The decoding function is the inverse of the function f , which we can find in the usual way by solving the equation $m = n \oplus 3$ for n . The result is $n = m \ominus 3$, so that

$$f^{-1}(m) = m \ominus 3 \quad \text{or} \quad f^{-1}(m) = m \oplus 23.$$

Suppose we receive the encoded message DOJHEUD. To decode this message, we first represent it numerically:

$$3, 14, 9, 7, 4, 20, 3.$$

Next we apply the decryption function to get

$$0, 11, 6, 4, 1, 17, 0,$$

which is the numerical representation of ALGEBRA. Notice here that there is nothing special about either of the numbers 3 or 26. We could have used a larger alphabet or a different shift. \blacklozenge

Exercise 9.2.2.

- (a) Encode IXLOVEXMATH using the cryptosystem in Example 9.2.1.
- (b) Encode the same message using the encoding function $f(n) = n \oplus 10$.

◇

Exercise 9.2.3.

- (a) Decode ZLOOA WKLVA EHARQ WKHA ILQDO, which was encoded using the cryptosystem in Example 9.2.1.
- (b) Decode: OFOBIDRSXQIYENYPVYGCPBYWDROROKBD, which was encoded using a shift code with a shift of 10.

◇

Exercise 9.2.4.

- (a) The following is a ciphertext that was encoded using a shift code with a shift of 9.
FWHKYVOGVFGCVQWFIHOKYVQG VFGCVHSPOKYVQGVFGCV
Find the plaintext.
- (b) A plaintext is encoded using a shift code with a shift of 14. The resulting ciphertext is shift-encoded again, using a shift of 14. The result is:
VJGOQTGAQWMPQYVJGNGUUUWTGAQWCTGXQN VCKTG
Find the plaintext.

◇

Cryptanalysis is concerned with deciphering a received or intercepted message. Methods from probability and statistics are great aids in deciphering an intercepted message; for example, the frequency analysis of the characters appearing in the intercepted message often makes its decryption possible.

Example 9.2.5. Suppose we receive a message that we know was encrypted by using a shift transformation on single letters of the 26-letter alphabet. To

find out exactly what the shift transformation was, we must compute b in the equation $f(n) = n + b \pmod{26}$. We can do this using *frequency analysis*. The letter E = 04 is the most commonly occurring letter in the English language. Suppose that S = 18 is the most commonly occurring letter in the ciphertext. Then we have good reason to suspect that $18 = 4 \oplus b$, or $b = 14$. Therefore, the most likely encoding function is

$$f(n) = n \oplus 14.$$

The corresponding decoding function is

$$f^{-1}(m) = m \oplus 12.$$

It is now easy to determine whether or not our guess is correct. \blacklozenge

Exercise 9.2.6. The following ciphertext was encoded using a shift code. Both the letters E and I are encoded as vowels.

IWPDAIWPEYOEOPDAMQAAJKBPDAOYEAJYAOYWNBHCWQOO

Find the plaintext. \blacklozenge

Exercise 9.2.7. In the following shift-coded ciphertext, one of the double-letter patterns represents 'ss'.

SGDDRRDMBDNELZSGDLZSHBRHRHMHSREQDDCNLFDNQFBZMSNQ

Find the plaintext. \blacklozenge

Exercise 9.2.8.

- (a) For the English alphabet, how many different shift codes are there?
- (b) Thai script has 44 letters. How many different shift codes are there for the Thai language?

\blacklozenge

9.2.2 Affine codes

Let us investigate a slightly more sophisticated cryptosystem. Suppose that the encoding function is given by

$$f(n) = \text{mod}(an + b, 26),$$

which can also be written as

$$f(n) = (a \odot n) \oplus b.$$

We first need to find out when a decoding function f^{-1} exists. Such a decoding function exists when we can solve the equation

$$m \equiv an + b \pmod{26} \quad \text{or} \quad a \odot n = m \ominus b$$

for n in \mathbb{Z}_{26} . By Proposition 5.5.20 in Chapter 5, this is possible exactly when a has an inverse in \mathbb{Z}_{26} , which means that $\text{gcd}(a, 26) = 1$. Such a cryptosystem is called an *affine cryptosystem*.

Exercise 9.2.9.

- (a) Which of the numbers 0, 1, 2, ..., 10 have inverses mod 26?
- (b) For the numbers in (a) which have inverses mod 26, compute the inverses.

◇

Exercise 9.2.10. Find the decoding function for the following affine encoding functions (used on the English alphabet).

- (a) $f(n) = (3 \odot n) \oplus 14$
- (b) $f(n) = (5 \odot n) \oplus 15$
- (c) $f(n) = (7 \odot n) \oplus 23$

◇

Exercise 9.2.11. Show that the general formula for the decoding function for $f(n) = (a \odot n) \oplus b$ is

$$f^{-1}(m) = (a^{-1} \odot m) \ominus (a^{-1} \odot b).$$

(That is, show that $f \circ f^{-1}(m) = m$, and $f^{-1} \circ f(n) = n$. Note that n and m are *variables*, while a and b are *constants* which characterize the encoding function.) \diamond

Example 9.2.12. Let's consider the affine cryptosystem encoding function $f(n) = (a \odot n) \oplus b$, where \odot and \oplus are multiplication and addition mod 26 respectively. For this cryptosystem to work we must choose an $a \in \mathbb{Z}_{26}$ that is invertible. This is only possible if $\gcd(a, 26) = 1$. Recognizing this fact, we will let $a = 5$ since $\gcd(5, 26) = 1$. The reader may check that $a^{-1} = 21$. Therefore, we can take our encryption function to be $f(n) = (5 \odot n) \oplus 3$. Thus, ALGEBRA is encoded as 3, 6, 7, 23, 8, 10, 3, or DGHXIKD. The decryption function will be

$$f^{-1}(n) = (21 \odot n) \ominus (21 \odot 3) = (21 \odot n) \oplus 15.$$

\blacklozenge

Exercise 9.2.13. For each of the following functions, (i) determine whether the function is a valid encoding function; (ii) if the function is valid, find the decoding function. (Assume the function is working on an alphabet with 26 letters.)

- (a) $f(n) = (4 \odot n) \oplus 7$
- (b) $f(n) = (5 \odot n) \oplus 13$
- (c) $f(n) = (11 \odot n) \oplus 14$
- (d) $f(n) = (13 \odot n) \oplus 22$

\diamond

Exercise 9.2.14.

- (a) The general form for an affine cryptosystem encoding function is $f(n) = (a \odot n) \oplus b$. How many different possible values of a are there, for an affine cryptosystem that works on the English alphabet of 26 letters?
- (b) For the same situation as (a), how many different possible values are there for b ?

- (c) What is the total number of affine cryptosystems that work on an alphabet of 26 letters?

◇

Exercise 9.2.15. The Spanish alphabet has 29 letters. Give answers to parts (a), (b), and (c) of Exercise 9.2.14, but with the Spanish alphabet instead of the English alphabet. ◇

Exercise 9.2.16. The Hebrew alphabet has 22 letters. Give answers to parts (a), (b), and (c) of Exercise 9.2.14, but with the Hebrew alphabet instead of the English alphabet. ◇

Exercise 9.2.17. Suppose that the encoding function for an affine cryptosystem is $f(n) = (a \odot n) \oplus b$, and the decoding function is $f^{-1}(m) = (a' \odot m) \oplus b'$. Suppose that a different cryptosystem uses the encoding function $g(n) = (a' \odot n) \oplus b'$. What is the decoding function for this second cryptosystem? ◇

Exercise 9.2.18.

- (a) The following message was encoded using an affine cryptosystem that encodes A as M and B as B.

CKMYCZMLCOZCWKOHUCKDOHLMZLLNMZGZOEUVFYU

Find the plaintext.

- (b) The following message was encoded using an affine cryptosystem that encodes A as G and C as C.

MQTNOELNWNTEHCEWHISCFKYHHFYKGCCEIPXQWFISCF

Find the plaintext.

- (c) The following message was encoded using an affine cryptosystem that encodes R as S and S as D.

OMFMFNSOMNDSFNDLADOMNOSFNDLAJNAALOZAUFSDONAU

Find the plaintext.

- (d) The following message was encoded using an affine cryptosystem that encodes M as N and O as D.

NVEMBNVEHLJHJEMBNZJHLDWOBVJDI

Find the plaintext.

◇

9.2.3 Monoalphabetic codes

In both shift codes and affine codes, one character in the encoded message represents exactly one character in the original message. Cryptosystems that employ such a one-to-one substitution are called *monoalphabetic cryptosystems*. The “cryptoquips” that appear regularly in many newspapers make use of this type of cryptosystem (see Figure 9.2.1).

CRYPTOQUIP

XKFB ZKQZ ENG XQL SFQYYG
 TQCTIIMYFH TG Q PIB QSZDLZ,
 D’C LNSF KF LNOOFSFH ZKF
 QEIBG IO HFPPDZ.

Yesterday’s Cryptoquip: MONTH IN WHICH
 MANY LOUD, POWER-PACKED MUSIC
 CONCERTS TAKE PLACE ON A DAILY BASIS:
 ROCKTOBER.

Today’s Cryptoquip Clue: Z equals T

CRYPTOQUIP BOOK 1! Send \$4.50 (check/m.o.) to
 CryptoClassics Book 1, P.O. Box 536475, Orlando, FL 32853-6475

The Cryptoquip is a substitution cipher in which one letter stands for another. If you think that X equals O, it will equal O throughout the puzzle. Single letters, short words and words using an apostrophe give you clues to locating vowels. Solution is by trial and error.

© 2002 by King Features Syndicate, Inc.

Figure 9.2.1. Example of cryptoquip (source: “Cecil Whig”, <http://www.cecildaily.com/diversions/cryptoquip/>).

Exercise 9.2.19. What is the total number of monoalphabetic cryptosystems? ◇

Although there are many different possible monoalphabetic cryptosystems, they are relatively easy to break using frequency analysis. (You may even find web sites that can automatically decode cryptoquips.)

9.2.4 Polyalphabetic codes

A cryptosystem would be more secure if a ciphertext letter could represent more than one plaintext letter. To give an example of this type of cryptosystem, called a *polyalphabetic cryptosystem*, we will generalize affine codes by using matrices. The idea works roughly the same as before; however, instead of encrypting one letter at a time we will encrypt pairs of letters (as before, letters are represented by elements of \mathbb{Z}_{26}). We can store a pair of letters n_1 and n_2 in a vector

$$\mathbf{n} = \begin{pmatrix} n_1 \\ n_2 \end{pmatrix}.$$

Let A be a 2×2 invertible matrix with entries in \mathbb{Z}_{26} . We can define an encoding function by

$$f(\mathbf{n}) = (A \odot \mathbf{n}) \oplus \mathbf{b},$$

where \mathbf{b} is a fixed column vector and matrix operations are performed in \mathbb{Z}_{26} . The formula for the decoding function (which is the inverse of the encoding function) is very similar to the decoding function formula that we found for affine encoding:

$$f^{-1}(\mathbf{m}) = (A^{-1} \odot \mathbf{m}) \ominus (A^{-1} \odot \mathbf{b}),$$

where A^{-1} is the *matrix inverse* of A : that is, $A^{-1}A = AA^{-1} = I$, where I is the 2×2 identity matrix. *Note* that in these formulas, we are using *modular* matrix multiplication instead of *regular* matrix multiplication: that is, the regular \cdot and $+$ operations are replaced by \odot and \oplus :

Exercise 9.2.20. Perform the following operations using modular matrix multiplication (mod 26):

(a) $\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} \begin{pmatrix} 4 \\ 4 \end{pmatrix}$

(c) $\begin{pmatrix} 12 & 4 \\ 13 & 5 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 20 & 20 \end{pmatrix}$

(b) $\begin{pmatrix} 1 & 13 \\ 16 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \end{pmatrix}$

(d) $\begin{pmatrix} 13 & 2 \\ 2 & 13 \end{pmatrix} \begin{pmatrix} 2 & 13 \\ 13 & 2 \end{pmatrix}$

◇

Example 9.2.21. Suppose that we wish to encode the word HELP. The corresponding digit string is 7, 4, 11, 15. If

$$A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix},$$

then

$$A^{-1} = \begin{pmatrix} 2 & 21 \\ 25 & 3 \end{pmatrix}.$$

(You may check that $\text{mod}(AA^{-1}, 26) = \text{mod}(A^{-1}A, 26) = I$.) If $\mathbf{b} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$, then our message is encrypted as RRGR, where HE encrypts as RR and LP encrypts as GR. ◆

In order to make use of polyalphabetic cryptosystems, we need to be able to find the inverse of a 2×2 matrix with entries in \mathbb{Z}_{26} . As we *noted* above, this inverse is under matrix multiplication mod 26, rather than regular matrix multiplication. Still, we can try to make use of the matrix inverse formula from regular matrix multiplication:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} kd & -kb \\ -kc & ka \end{pmatrix},$$

where

$$k = \frac{1}{ad - bc}.$$

This suggests that the following formula may be valid mod 26:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} k \odot d & -k \odot b \\ -k \odot c & k \odot a \end{pmatrix},$$

where

$$k = ((a \odot d) \ominus (b \odot c))^{-1},$$

and $(\dots)^{-1}$ means inverse under multiplication in \mathbb{Z}_{26} . We will see in the following exercise that this works as long as $(a \odot d) \ominus (b \odot c)$ has a multiplicative inverse in \mathbb{Z}_{26} .

Exercise 9.2.22. Suppose that $(a \odot d) \ominus (b \odot c)$ has an inverse in \mathbb{Z}_{26} : that is to say, suppose there is a $k \in \mathbb{Z}_{26}$ such that $k \odot ((a \odot d) \ominus (b \odot c)) = 1$. Show that the matrices:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} k \odot d & -k \odot b \\ -k \odot c & k \odot a \end{pmatrix}$$

are inverses of each other in \mathbb{Z}_{26} . That is, show that $AB = BA = I$ under matrix multiplication mod 26.

◇

The previous exercise leaves open the question of whether $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has an inverse when $(a \odot d) \ominus (b \odot c)$ has no inverse in \mathbb{Z}_{26} . Once again, we can reach back to our previous matrix knowledge to resolve this issue. Recall that the quantity $ad - bc$ is called the **determinant** of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. There is also a famous formula for the determinant of the product of matrices:

$$\det(A)\det(B) = \det(AB).$$

This same formula carries over to matrix multiplication mod 26, because (as we've seen) in any equation using only the operations of multiplication, addition, and subtraction, we can replace these operations with their modular versions and still have a true equation. We can use this to show that $(a \odot d) \ominus (b \odot c)$ *must* have an inverse in \mathbb{Z}_{26} in order for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to have an inverse:

Exercise 9.2.23. Suppose that $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix with entries in \mathbb{Z}_{26} , such that $(a \odot d) \ominus (b \odot c)$ has no inverse in \mathbb{Z}_{26} . Show that A has no inverse in \mathbb{Z}_{26} . (*Hint*) ◇

Exercise 9.2.24. Find matrix inverses in \mathbb{Z}_{26} for the following matrices. If no inverse exists, then prove there is no inverse.

(a) $\begin{pmatrix} 9 & 2 \\ 20 & 5 \end{pmatrix}$

(b) $\begin{pmatrix} 2 & 3 \\ 23 & 2 \end{pmatrix}$

(c) $\begin{pmatrix} 4 & 11 \\ 3 & 2 \end{pmatrix}$

(d) $\begin{pmatrix} 2 & 2 \\ 3 & 4 \end{pmatrix}$

◇

Exercise 9.2.25. For the same matrices as in Exercise 9.2.24, find the matrix inverses in \mathbb{Z}_{29} . ◇

Exercise 9.2.26. Given that

$$A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}, \text{ and } \mathbf{b} = \begin{pmatrix} 2 \\ 5 \end{pmatrix}.$$

- (a) Use the encryption function $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ to encode the message CRYPTOLOGY.
- (b) What is the decoding function?

◇

Frequency analysis can still be performed on a polyalphabetic cryptosystem, because we have a good understanding of how pairs of letters appear in the English language. The pair *th* appears quite often; the pair *qz* never appears. To avoid decryption by a third party, we must use a larger matrix than the one we used in Example 9.2.21.

9.2.5 Spreadsheet exercises

Spreadsheets can be used to automate many of the calculations that we have looked at in the previous sections.

Shift encoding and decoding spreadsheet

Exercise 9.2.27. In this exercise, you will use a spreadsheet to create an automated shift encoder for English. Please refer to Figure 9.2.2 for guidance:

- (i) Put the Shift value in cell C2.

| | A | B | C | D | E | F | G | H | I | J |
|----|---|---|---|---|-------------|----|----|----|----|----|
| 1 | AUTOMATED SHIFT ENCODING FOR ENGLISH | | | | | | | | | |
| 2 | Shift: 15 | | | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | Tables: | | | | | | | | | |
| 5 | A | 0 | A | | Plaintext: | H | E | L | L | O |
| 6 | B | 1 | B | | Numerical: | 7 | 4 | 11 | 11 | 14 |
| 7 | C | 2 | C | | Shifted: | 22 | 19 | 0 | 0 | 3 |
| 8 | D | 3 | D | | Ciphertext: | W | T | A | A | D |
| 9 | E | 4 | E | | Numerical: | 22 | 19 | 0 | 0 | 3 |
| 10 | F | 5 | F | | Unshifted: | 7 | 4 | 11 | 11 | 14 |
| 11 | G | 6 | G | | Recovered: | H | E | L | L | O |
| 12 | H | 7 | H | | | | | | | |

Figure 9.2.2. Automatic shift encoder for English.

- (ii) Put the alphabet (starting with A), numerical values for the letters (starting with 0), and the alphabet again in columns A, B, C starting on line 5.
- (iii) Type your plaintext in row 5, starting in column F.
- (iv) Row 6 beginning in column F contains the numerical values for the plaintext. The formula in cell F6 is: “=VLOOKUP(F5, \$A\$5:\$B\$30,2)”. The significance of this formula is as follows:
 - The function VLOOKUP means that the program will look up a given value in a given table;
 - The F5 is the first argument of VLOOKUP, which means that the value being looked up is in cell F5;
 - The \$A\$5:\$B\$30 is the second argument of VLOOKUP, which means that it represents the cells containing the table that the value will be looked up in. The dollar signs are used to guarantee that the table will remain fixed when the formula is copied and pasted into another cell; The 2 which is the third lookup of VLOOKUP indicates that the value in the second column in the same row as the looked-up value is placed in the cell where the formula is located.
- (v) Row 7 beginning in column F gives the encoded numerical values. The formula in cell F7 is “=MOD(F6+\$C\$2,26)”. The dollar signs on C2

guarantee that when the formula is copied, the shift still refers to the value in C2.

- (vi) Row 8 beginning in column F gives the ciphertext. The formula in cell F8 is: “=VLOOKUP(F7,\$B\$5:\$C\$30,2)”.
- (vii) Rows 9,10, and 11 are similar to rows 6,7,8 respectively. Try to do this yourself.

Once you have completed the formulas, select cells F6 through J11, and use the spreadsheet’s “Fill Right” capability to carry the formulas to the other columns. (If your plaintext is longer, you can select more columns and fill right. \diamond)

Exercise 9.2.28. The Spanish alphabet has 3 more letters than English: ‘Ch’ (comes after C in the alphabet), ‘Ll’ (comes after L in the alphabet), and ‘Nn’ (comes after N). Modify the sheet you created in Exercise 9.2.27 to make a Spanish language shift encoder. Use your sheet to decode the following message:

MS KIUPVX UIB NIKPS VX MB BPMUYAM MS UMQXA

(Note that ‘Ch’ counts as a single letter.) \diamond

Affine encoding and decoding spreadsheet

Exercise 9.2.29. Create a spreadsheet that can perform any affine encoding on English plaintext. You may model your spreadsheet on the sheet in Figure 9.2.3. Use your spreadsheet to decode the following message:

EMBNDODFDZXIDPEMBSBJJZOBFDZVOBUDSEVHOB

which was encoded using an affine encoding function with $b = 21$. \diamond

Exercise 9.2.30. In order to decode an affine cryptosystem on English letters with encoding function $f(p) = (a \odot p) \oplus b$, it is necessary to find the inverse of a under multiplication mod 26. We have ways of finding inverses of individual numbers. But we can also use spreadsheet software to find all inverses in one fell swoop as described below.

| | A | B | C | D | E | F | G | H | I | J |
|----|--------------------------------------|---|---|---|-----------------|---|----|----|----|----|
| 1 | Spreadsheet for affine encode/decode | | | | | | | | | |
| 2 | a: | | 3 | | | | | | | |
| 3 | b: | | 8 | | | | | | | |
| 4 | a^{-1} | | 9 | | | | | | | |
| 5 | | | | | | | | | | |
| 6 | A | 0 | A | | Plaintext: | H | E | L | L | O |
| 7 | B | 1 | B | | Numerical: | 7 | 4 | 11 | 11 | 14 |
| 8 | C | 2 | C | | Affine: | 3 | 20 | 15 | 15 | 24 |
| 9 | D | 3 | D | | Ciphertext | D | U | P | P | Y |
| 10 | E | 4 | E | | Numerical: | 3 | 20 | 15 | 15 | 24 |
| 11 | F | 5 | F | | Affine inverse: | 7 | 4 | 11 | 11 | 14 |
| 12 | G | 6 | G | | Plaintext: | H | E | L | L | O |
| 13 | H | 7 | H | | | | | | | |

Figure 9.2.3. Automatic affine encoder for English.

Open a sheet in your favorite spreadsheet software (Excel, LibreOffice, or OpenOffice). Put the numbers 0 through 25 in column A, starting at row 3, and also in row 2 starting in column B. To fill up the table, put the formula “=MOD(\$A3*B\$2,26)” in cell B3, as shown in Figure 9.2.4. This formula causes the software to take the product of the contents of cells A3 and B2, and put the result mod 26 into cell B3. The dollar signs are important: these indicate “fixed reference”. For example, the ‘\$A3’ means that when this formula is copied to other cells, the reference to column A remains unchanged while the column may change. On the other hand, the ‘B\$2’ means that when the formula is copied to other cells, the reference to column 2 remains unchanged.

At this point, select the range of cells from B3 to AA28 (this will be a square region of 26×26 cells. Use your spreadsheet’s “Fill down” and “Fill right” feature to fill all the cells in this region. The location of all of the ‘1’s in this table shows all of the inverses. For example, there is a ‘1’ in the row labeled 9 and column labeled 3. This means that 9 and 3 are inverses of each other mod 26.

Use this spreadsheet table to create a 2-column table: in the first column, put the numbers 0 through 26, and in the second column, put the inverses (if the number has no inverse, just put a ‘-’). \diamond

| | A | B | C | D | E | F | G | H | I |
|---|-------------------------------------|--------------------|----------|----------|----------|----------|----------|----------|----------|
| 1 | Multiplication table mod 26. | | | | | | | | |
| 2 | | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 3 | 0 | =MOD(\$A3*B\$2,26) | | | | | | | |
| 4 | 1 | | | | | | | | |
| 5 | 2 | | | | | | | | |
| 6 | 3 | | | | | | | | |

Figure 9.2.4. Mod 26 multiplication table.

Exercise 9.2.31. Following the previous exercise, find all inverses of the numbers mod 29 (this can be used in affine encoding of Spanish, which has 29 letters). \diamond

Exercise 9.2.32. Make a spreadsheet that can do polyalphabetic coding. you may base your sheet’s design on Figure 9.2.5. The figure shows the encoding of the word CRYPTOLOGY using $A = \begin{pmatrix} 3 & 5 \\ 1 & 2 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$.

Use your spreadsheet to decode the following words that were encoded using $f(\mathbf{p}) = A\mathbf{p} + \mathbf{b}$ with the given A and \mathbf{b} .

(a) VVDGOFOKLY, $A = \begin{pmatrix} 13 & 5 \\ 9 & 2 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 7 \\ 13 \end{pmatrix}$.

(b) VWFGTWQKTA, $A = \begin{pmatrix} 17 & 13 \\ 6 & 3 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 14 \\ 18 \end{pmatrix}$.

(c) EXUFQPRRGA, $A = \begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix}$, and $\mathbf{b} = \begin{pmatrix} 4 \\ 8 \end{pmatrix}$.

\diamond

9.3 Public key cryptography

If traditional cryptosystems are used, anyone who knows enough to encode a message will also know enough to decode an intercepted message. In 1976, W. Diffie and M. Hellman proposed public key cryptography, which is based

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
|----|------------------|----|---|--------------------|------------------|--------------------------------|---|----|----|----|----|----|-------------------------------------|---|---------------------------------|---|---|---|---|---|---|---|
| 1 | Matrix A: | | | | Vector b: | | | | | | | | $A^{-1} \bmod 26$ | | $-A^{-1} * b$ | | | | | | | |
| 2 | 3 | 5 | | | 2 | $\text{mod}(ad - bc, 26)$ | | | | 1 | 2 | 21 | | | 6 | | | | | | | |
| 3 | 1 | 2 | | | 2 | <i>inverse mode 26 by hand</i> | | | | 1 | 25 | 3 | | | 22 | | | | | | | |
| 4 | Tables: | | | | | | | | | | | | | | | | | | | | | |
| 5 | A | 0 | A | Plaintext: | | | | C | Y | T | L | G | | | | | | | | | | |
| 6 | B | 1 | B | | | | | R | P | O | O | Y | | | | | | | | | | |
| 7 | C | 2 | C | | | | | | | | | | | | | | | | | | | |
| 8 | D | 3 | D | Numerical: | | | | 2 | 24 | 19 | 11 | 6 | | | | | | | | | | |
| 9 | E | 4 | E | | | | | 17 | 15 | 14 | 14 | 24 | | | | | | | | | | |
| 10 | F | 5 | F | | | | | | | | | | | | | | | | | | | |
| 11 | G | 6 | G | Encoded | | | | 15 | 19 | 25 | 1 | 10 | | | | | | | | | | |
| 12 | H | 7 | H | numerical: | | | | 12 | 4 | 23 | 15 | 4 | | | | | | | | | | |
| 13 | I | 8 | I | | | | | | | | | | | | | | | | | | | |
| 14 | J | 9 | J | Ciphertext: | | | | P | T | Z | B | K | | | | | | | | | | |
| 15 | K | 10 | K | | | | | M | E | X | P | E | | | | | | | | | | |
| 16 | L | 11 | L | | | | | | | | | | | | | | | | | | | |
| 17 | M | 12 | M | Numerical: | | | | 15 | 19 | 25 | 1 | 10 | | | | | | | | | | |
| 18 | N | 13 | N | ciphertext | | | | 12 | 4 | 23 | 15 | 4 | | | | | | | | | | |
| 19 | O | 14 | O | | | | | | | | | | | | | | | | | | | |
| 20 | P | 15 | P | Decoded | | | | 2 | 24 | 19 | 11 | 6 | | | | | | | | | | |
| 21 | Q | 16 | Q | numerical: | | | | 17 | 15 | 14 | 14 | 24 | | | | | | | | | | |
| 22 | R | 17 | R | | | | | | | | | | | | | | | | | | | |
| 23 | S | 18 | S | Decoded | | | | C | Y | T | L | G | | | | | | | | | | |
| 24 | T | 19 | T | plaintext: | | | | R | P | O | O | Y | | | | | | | | | | |

Figure 9.2.5. (Semi-)automatic polyalphabetic encoder/decoder for English. Note that cell N3 is entered by hand, based on the value in N2.

on the observation that the encryption and decryption procedures need not have the same key. This removes the requirement that the encoding key be kept secret. The encoding function f must be relatively easy to compute, but f^{-1} must be extremely difficult to compute without some additional information, so that someone who knows only the encrypting key cannot find the decrypting key without prohibitive computation. It is interesting to note that to date, no system has been proposed that has been proven to be “one-way;” that is, for any existing public key cryptosystem, it has never been shown to be computationally prohibitive to decode messages with only knowledge of the encoding key.

9.3.1 The RSA cryptosystem

The RSA cryptosystem introduced by R. Rivest, A. Shamir, and L. Adleman in 1978, is based on the difficulty of factoring large numbers. Though it is not a difficult task to find two large random primes and multiply them together, factoring a 150-digit number that is the product of two large primes would take 100 million computers operating at 10 billion instructions per second about 50,000 years under the fastest algorithms currently known.

Let us look at how RSA works in a practical context. Suppose that Jennifer is running an online boutique, and wants to receive credit card information from customers over the internet. Unfortunately it's all too easy to snoop the internet, and it certainly wouldn't be good for Jennifer's customers if their credit card numbers were stolen. So she needs a suitable code for the credit card information in order to protect her customer's privacy. The code may be constructed as follows:

- (a) Choose two random 150-digit prime numbers p and q . (This is easier said than done! We will consider some possible ways of doing this in Section 9.3.4.)
- (b) Compute the product $n = pq$ as well as $m = (p - 1)(q - 1)$. (It can be shown that m is actually the number of positive integers in \mathbb{Z}_n that are relatively prime to n .)
- (c) Find a large random integer E that is relatively prime to m . This is done by making a guess for E , then using the Euclidean algorithm to check whether $\gcd(E, m) = 1$. If not, then keep guessing until you find an E that works. In general relatively prime numbers are not uncommon, and the Euclidean algorithm is pretty quick (especially for a computer), so E is not too difficult to find.
- (d) Using the Euclidean algorithm, find D such that $DE \equiv 1 \pmod{m}$.

Now, let's say that Jennifer has a customer whose credit card number is x . Before requesting the credit card information, Jennifer's computer sends the numbers E and n to the customer's computer, which then calculates $y = x^E \pmod{n}$ and sends y to Jennifer's computer. Jennifer recovers x by computing $y^D \pmod{n}$, which (as we shall show in a minute) turns out to be x , as long as x is less than n .

Notice some amazing things here. First, E and n are sent out *openly* over the internet. Jennifer doesn't care if snoopers find out this information.

In fact, she sends the *same* E and n to each customer! But this does not compromise her customers' security, because only Jennifer knows m , and it takes both E and m to find D . As long as no one can figure out m , the credit card numbers are safe!

To summarize: once the public key (E, n) and the private key D have been constructed, the process of encoding and decoding is simple:

- To encode a numerical plaintext x : compute $x^E \pmod{n}$.
- To decode a numerical ciphertext y : compute $y^D \pmod{n}$.

Example 9.3.1. Before exploring the theory behind the RSA cryptosystem or attempting to use large integers, we will use some small integers just to see that the system does indeed work. Suppose that we wish to send some message, which when digitized is 395. Let $p = 23$ and $q = 29$. Then

$$n = pq = 667 \quad \text{and} \quad m = (p - 1)(q - 1) = 616.$$

We can let $E = 487$, since $\gcd(616, 487) = 1$. The encoded message is computed to be

$$\text{mod}(395^{487}, 667) = 570.$$

(This may seem like a very long computation, but there are fast ways of doing this: see Exercise 9.3.3 below.) Using the Euclidean algorithm, we determine that $191E = 1 + 151m$; therefore, the decrypting key is $(n, D) = (667, 191)$. We can recover the original message by calculating

$$\text{mod}(570^{191}, 667) = 395.$$



This really seems like magic. How in the world does it work? First of all, we know that $DE \equiv 1 \pmod{m}$; so there exists a k such that

$$DE = km + 1.$$

This means that

$$y^D = (x^E)^D = x^{DE} = x^{km+1} = (x^m)^k x.$$

At this point we need *Euler's theorem* from Chapter 18, which states the following. Suppose m is the number of positive integers less than n that are relatively prime to n . Then it is true that:

$$x^m \equiv 1 \pmod{n}.$$

for *any* x that is relatively prime to n .

We can use this to simplify our previous expression for y^D :

$$y^D = (x^m)^k x \equiv (1)^k x \equiv x \pmod{n},$$

and presto! We have our result.

We can now ask how one would go about breaking the RSA cryptosystem. To find D given n and E , we simply need to factor n and solve for D by using the Euclidean algorithm. If we had known that $667 = 23 \cdot 29$ in Example 5, we could have recovered D .

Exercise 9.3.2. Show that if p and q are primes, then the number of positive integers less than pq which are relatively prime to pq is $(p-1)(q-1)$. (*Hint*) \diamond

9.3.2 Message verification


There is a problem of message verification in public key cryptosystems. Since the encoding key is public knowledge, anyone has the ability to send an encoded message. If Alice receives a message from Bob, she would like to be able to verify that it was Bob who actually sent the message. Suppose that Bob's encrypting key is (n', E') and his decrypting key is (n', D') . Also, suppose that Alice's encrypting key is (n, E) and her decrypting key is (n, D) . Since encryption keys are public information, they can exchange coded messages at their convenience. Bob wishes to assure Alice that the message he is sending is authentic. Before Bob sends the message x to Alice, he decrypts x with his own key:

$$x' = \text{mod}(x^{D'}, n').$$

Anyone can change x' back to x just by encryption, but only Bob has the ability to form x' . Now Bob encrypts x' with Alice's encryption key to form

$$y' = \text{mod}(x'^E, n),$$

a message that only Alice can decode. Alice decodes the message and then encodes the result with Bob's key to read the original message, a message that could have only been sent by Bob.

9.3.3 RSA exercises 

Exercise 9.3.3. This problem demonstrates a fast method for computing very large powers of numbers in modular arithmetic using a spreadsheet. You will need this method in order to do the subsequent problems. We will demonstrate the method by computing $\text{mod}(23^{485}, 617)$.

(a) Use a spreadsheet to compute the following sequence of numbers:

$$23, \text{mod}(23^2, 617), \text{mod}(23^4, 617), \dots, \text{mod}(23^{256}, 617)$$

Note that each power of 23 in this series is the *square* of the previous power. So to compute any number in this series, square the previous number and reduce mod 617. You may use the MOD spreadsheet function. It is easiest to put all the numbers in a single column. (This way, you can use the spreadsheet's "Fill down" feature.)

- (b) Write 485 as a sum of powers of 2. (This is the same thing as finding the *binary expansion* of 485.)
- (c) Using the results of (b), identify a set of entries from the table you found in part (a), such that the product of these entries is equivalent to $23^{485} \pmod{617}$. (**Hint**)
- (d) Use your result from (c) to compute $\text{mod}(23^{485}, 617)$.

◇

Exercise 9.3.4. Building off the previous exercise, create a spreadsheet that can compute $\text{mod}(x^q, n)$ for general x, q, n . You may follow the pattern of the spreadsheet in Figure 9.3.1. Some of the formulas in the spreadsheet are:

- Cell A8: =B3
- Cell B8: =MOD(A8,2)
- Cell A9: =(A8 - B8)/2
- Cell D9: = D8*2
- Cell E9: = MOD(E8*E8, \$B\$4)

- Cell F8: = B8
- Cell G8: = E8^F8
- Cell H8: = G8
- Cell H9: = MOD(G9*H8,\$B\$4)

You may obtain the rest of the formulas using the spreadsheet’s “fill down” capability.

| | A | B | C | D | E | F | G | H |
|----|--------------------------------------|-------------------------|---|------------------------------|-----------------------------|---------------------------|-------------------------|---------------------------------|
| 1 | COMPUTING LARGE POWERS MODULO A BASE | | | | | | | |
| 2 | <i>number</i> | 222 | | | | | | |
| 3 | <i>power</i> | 3894 | | | | | | |
| 4 | <i>base</i> | 617 | | | | | | |
| 5 | | | | | | | | |
| 6 | Binary expansion of power | | | | | | | |
| 7 | <i>Reduced power</i> | <i>Binary expansion</i> | | <i>Exponent (power of 2)</i> | <i>mod(num.^exp., base)</i> | <i>Bin. Exp. Of power</i> | <i>Factors of power</i> | <i>Running product mod base</i> |
| 8 | 3894 | 0 | | 1 | 222 | 0 | 1 | 1 |
| 9 | 1947 | 1 | | 2 | 541 | 1 | 541 | 541 |
| 10 | 973 | 1 | | 4 | 223 | 1 | 223 | 328 |
| 11 | 486 | 0 | | 8 | 369 | 0 | 1 | 328 |
| 12 | 243 | 1 | | 16 | 421 | 1 | 421 | 497 |
| 13 | 121 | 1 | | 32 | 162 | 1 | 162 | 304 |
| 14 | 60 | 0 | | 64 | 330 | 0 | 1 | 304 |
| 15 | 30 | 0 | | 128 | 308 | 0 | 1 | 304 |
| 16 | 15 | 1 | | 256 | 463 | 1 | 463 | 76 |
| 17 | 7 | 1 | | 512 | 270 | 1 | 270 | 159 |
| 18 | 3 | 1 | | 1024 | 94 | 1 | 94 | 138 |
| 19 | 1 | 1 | | 2048 | 198 | 1 | 198 | 176 |
| 20 | 0 | 0 | | 4096 | 222 | 0 | 1 | 176 |

Figure 9.3.1. Spreadsheet for taking large powers modulo a given base.



Exercise 9.3.5. Using your spreadsheet from the previous exercise, encrypt each of the following plaintexts using RSA. Before encoding, divide the plaintext into blocks of integers of length 2; that is, if the plaintext is 142528, encode 14, 25, and 28 separately.

- (a) $n = 3551, E = 629$, plaintext = 31
- (b) $n = 2257, E = 47$, plaintext = 23

- (c) $n = 120979, E = 13251, \text{plaintext} = 142371$
- (d) $n = 45629, E = 781, \text{plaintext} = 231561$

◇

Exercise 9.3.6. Decrypt each of the following RSA messages y . (In this case, do not break y into blocks—decode the entire number.)

- (a) $n = 3551, D = 1997, y = 2791$
- (b) $n = 5893, D = 81, y = 34$
- (c) $n = 120979, D = 27331, y = 112135$
- (d) $n = 79403, D = 671, y = 129381$

◇

Exercise 9.3.7. Encrypted messages are often divided into blocks of n letters. A message such as THE WORLD WONDERS WHY might be encrypted as JIW OCFRJ LPOEVYQ IOC but sent as JIW OCF RJL POE VYQ IOC. What are the advantages of using blocks of n letters? ◇

Exercise 9.3.8. Construct an RSA cryptosystem as follows:

- (a) On the web, find two four-digit primes
- (b) Use these primes to compute n and m .
- (c) Choose a value of E which is less than m , and use your Diophantine Equation spreadsheet (Exercise 5.5.14 in the Modular Arithmetic chapter) to find the inverse D under multiplication mod m . If it turns out that E is not relatively prime to m , try again.
- (d) Test your cryptosystem by encoding ‘123’, and then decoding it. To encode, use the spreadsheet that you created in Exercise 9.3.4 earlier in this chapter. To decode, make another copy of the same sheet.

◇

9.3.4 Additional exercises: identifying prime numbers

We saw in Section 9.3.1 that the RSA algorithm depends on finding very large primes. In practice, large primes are found using trial and error. That is, we choose a large random number and test to see whether it's prime. If the test fails, then try, try again.

So it all comes down to figuring out how to test whether a number is prime. In this section, we consider some possible ways of doing this.

“Brute force” method, and sieve of Eratosthenes

One way to do this is sheer brute force: try dividing by 2,3,4, ..., and if nothing divides then the number is prime. There are various ways to make this process more efficient, as we will see in the following exercises.

Exercise 9.3.9. To test whether the number n is a prime, you divide n all the integers 1,2,3,... up to a , and see if any of them divides evenly. How large does a have to be in order to guarantee that n really is a prime? (*Hint*) \diamond

When testing whether n is prime, by the “brute force” method, as long as n is odd we don't need to divide by even numbers (Why?). This means that you only need to test about half of the numbers up to a —more precisely, we only need to test $\lceil a/2 \rceil$ numbers, where $\lceil x \rceil$ means “the next integer larger than x ”. ($\lceil x \rceil$ is called the *ceiling* of x .)

We can pull the same trick with factors that are divisible by 3. Once we've tested 3 as a factor, we don't need to check 9,15,21,... or any other number that is divisible by 3. (Why?) So it seems that this reduces the number of factors that we need to check by about a third, since every third integers are divisible by 3. However, we need to be careful here. We've already ruled out the numbers that are divisible by 2, so the numbers that are divisible by both 2 and 3 have already been ruled out. In other words (using m to denote a positive integer, and using the notation $|\{\dots\}|$ to denote the size of sets):

$$\begin{aligned} |\{m \leq a \text{ and } (2 \mid m \text{ or } 3 \mid m)\}| = \\ |\{m \leq a \text{ and } 2 \mid m\}| + |\{m \leq a \text{ and } 3 \mid m\}| - |\{m \leq a \text{ and } 6 \mid m\}|. \end{aligned}$$

If we are not so careful with the “ceiling function” (which changes the result by at most 1 anyway), this tells us:

$$|\{m \leq a \text{ and } 2 \mid m \text{ or } 3 \mid m\}| \approx \frac{a}{2} + \frac{a}{3} - \frac{a}{6}.$$

We can turn this around and find the number of integers which are *not* divisible by 2 or 3:

$$\begin{aligned} |\{m \leq a \text{ and } 2 \nmid m \text{ and } 3 \nmid m\}| &\approx a - \frac{a}{2} - \frac{a}{3} + \frac{a}{6} \\ &\approx a \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \\ &\approx \frac{a}{3}. \end{aligned}$$

This gives the number of trial divisions required to test whether n is prime. (Of course we also need to test divisibility by 2 and 3, which are 2 additional divisions.)

The same reasoning can be extended to take into account divisibility by 5, 7, 11, and so on:

Exercise 9.3.10. Using the same reasoning as above, show that after dividing by 2, 3, 5 the number of additional divisions required to test for primality is approximately:

$$a \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right).$$

◇

The technique of eliminating numbers to check based on previous divisibility is called the *sieve of Eratosthenes*.

Fermat's test for primality

Even using various tricks to reduce the number of computations, the brute force method requires far too many calculations to be useful for RSA encoding. A different algorithm for testing primality is *Fermat's factorization algorithm*, which depends on the following fact:

Exercise 9.3.11. Let $n = ab$ be an odd composite number where $a, b \in \mathbb{N}$. Prove that n can be written as the difference of two perfect squares :

$$n = x^2 - y^2 = (x - y)(x + y),$$

where both x and y are greater than 1. Consequently, a positive odd integer can be factored exactly when we can find integers x and y such that $n = x^2 - y^2$. (*Hint*) \diamond

We can use this fact to factor n by trying different pairs of squares in order to get n as the difference of the two. Of course, we want to do this systematically. So we want to see what values of x and y we actually need to check:

Exercise 9.3.12. In the formula $n = x^2 - y^2 = (x - y)(x + y)$, what is the smallest possible value for x that needs to be tested? (*Hint*) \diamond

There are other special conditions that x and y must satisfy:

Exercise 9.3.13. For the purposes of this exercise, assume that n is an odd number and that $n = x^2 - y^2$.

- (a) Show that if x is odd then y is even, and if x is even then y is odd. (*Hint*)
- (b) Show that for any odd number m , then $m^2 \pmod{4} = 1$. (*Hint*)
- (c) Let $m = x + y$. Show that m is odd, and that we can rewrite $n = (x - y)(x + y)$ as: $n = m(m - 2y)$.
- (d) Show that if $n \pmod{4} = 1$, then y must be even. (*Hint*)
- (e) Show that if $n \pmod{4} = 3$, then y must be odd. (*Hint*)

\diamond

The Fermat primality testing scheme is better for finding factors that are nearly equal. The brute force method of Exercise 9.3.14 is much better when one factor is much bigger than the other one.

Exercise 9.3.14.

- (a) Create a spreadsheet that factors large numbers using the brute force scheme. You may use the spreadsheet in Figure 9.3.2 for inspiration. Some of the formulas in the spreadsheet are:
 - Cell A7: `=A6+2`

- Cell B6: $=B\$2/A6$
- Cell C6: $=IF(B6=FLOOR(B6,1),A6,0)$
- Cell E2: $=MAX(C6:C99999)$

You may obtain the rest of the formulas using the spreadsheet's “fill down” capability.

- Use this spreadsheet to factor $n = 3551$. Then, use your result to find the decoding key D for Exercise 9.3.5 part (a).
- Use this spreadsheet to find the decoding key D for Exercise 9.3.5 part (b).
- Use this spreadsheet to find the decoding key D for Exercise 9.3.5 part (c).
- Use this spreadsheet to find the decoding key D for Exercise 9.3.5 part (d).
- Use this spreadsheet to find the decoding key D for Exercise 9.3.5 part (e).
- Given the encryption key $(n, E) = (451, 231)$, find D .
- Given the encryption key $(n, E) = (3053, 1921)$, find D .

◇

| | A | B | C | D | E |
|---|------------------------------|-----------|--------------------|--------------------|-----|
| 1 | BRUTE FORCE FACTORING | | | | |
| 2 | Number n: | 45629 | | Max. factor | 443 |
| 3 | sqrt(n) | 213.609 | | | |
| 4 | | | | | |
| 5 | Trial factors | Quotient | Which are factors? | | |
| 6 | | 3 15209.7 | | 0 | |
| 7 | | 5 9125.8 | | 0 | |
| 8 | | 7 6518.43 | | 0 | |
| 9 | | a 5069.89 | | n | |

Figure 9.3.2. Spreadsheet for brute force factoring method

Exercise 9.3.15.

- Make a spreadsheet for Fermat's factoring method. You may use the spreadsheet in Figure 9.3.3 for inspiration. Some of the formulas in the spreadsheet are:

- Cell A7: =A6+1
- Cell B6: =SQRT(A6*A6 - \$B\$2)
- Cell C6: =IF(B6=FLOOR(B6,1),A6-B6,0)
- Cell D6: =IF(B6=FLOOR(B6,1),A6+B6,0)
- Cell E2: =MAX(C6:C99999)
- Cell E3: =MAX(D6:D99999)

You may obtain the rest of the formulas using the spreadsheet’s “fill down” capability.

- (b) Use this spreadsheet to factor $n = 7433551$. Then, use your result to find the decoding key D for $(n, E) = (7433551, 12345)$.
- (c) Use this spreadsheet to factor $n = 16394854313$. Then, use your result to find the decoding key D for $(n, E) = (16394854313, 34578451)$.

◇

| | A | B | C | D | E |
|---|-------------------------|--------------------|---------------------|-------------------|-----|
| 1 | FERMAT FACTORING | | | | |
| 2 | Number n: | 45629 | | Small factor: | 103 |
| 3 | sqrt(n) | 213.609457 | | Big factor: | 443 |
| 4 | | | | | |
| 5 | Trial x | sqrt(x^2-n) | Small factor | Big factor | |
| 6 | 214 | 12.922848 | 0 | 0 | |
| 7 | 215 | 24.4131112 | 0 | 0 | |
| 8 | 216 | 32.0468407 | 0 | 0 | |
| 9 | 217 | 38.2099463 | 0 | 0 | |

Figure 9.3.3. Spreadsheet for Fermat difference-of-squares factoring method

Exercise 9.3.16. * Using the results from Exercise 9.3.13 parts (d) and (e), modify the spreadsheet that you created in Exercise 9.3.15 to make it twice as efficient. In other words, modify the formula in cell A6 so that you can replace the formula in A7 with the formula: ‘=A6+2’. ◇

Probabilistic methods using the “little Fermat theorem”

In practice, neither the brute force nor the Fermat method is used to verify large prime numbers. Instead, *probabilistic methods* are used: these methods can show that it’s very, very likely that n is a prime, but they don’t prove for certain. The principal test of this type is the ***Miller-Rabin test*** for primality. This test uses some of the principles described below.

In Exercise 18.3.15 in Section 18.3.2, we will prove the following fact (which is widely known as *Fermat’s little theorem*):

If p is any prime number and a is any nonzero integer, then $a^{p-1} \equiv 1 \pmod{p}$.

We can use Fermat’s little theorem as a screening test for primes. For example, 15 cannot be prime since

$$2^{15-1} \equiv 2^{14} \equiv 4 \pmod{15}.$$

However, 17 is a potential prime since

$$2^{17-1} \equiv 2^{16} \equiv 1 \pmod{17}.$$

We say that an odd composite number n is a ***pseudoprime*** if

$$2^{n-1} \equiv 1 \pmod{n}.$$

Exercise 9.3.17. Which of the following numbers are primes and which are pseudoprimes?

- | | |
|---------|---------|
| (a) 341 | (b) 811 |
| (c) 601 | (d) 561 |
| (e) 771 | (f) 631 |

◇

Let n be an odd composite number and b be a positive integer such that $\gcd(b, n) = 1$. If $b^{n-1} \equiv 1 \pmod{n}$, then n is a ***pseudoprime base b***. We can get a more accurate test for the primality of n if we test n versus a number of prime bases. If n is a pseudoprime for several prime bases, then we can say with high confidence that n is most probably a prime.

Exercise 9.3.18. Show that 341 is a pseudoprime base 2 but not a pseudoprime base 3. \diamond

There exist composite numbers that are pseudoprimes for all bases to which they are relatively prime. These numbers are called *Carmichael numbers*. The first Carmichael number is $561 = 3 \cdot 11 \cdot 17$. In 1992, Alford, Granville, and Pomerance proved that there are an infinite number of Carmichael numbers [4]. However, Carmichael numbers are very rare. There are only 2163 Carmichael numbers less than 25×10^9 . For more sophisticated primality tests, see [1], [6], or [7].

Remark 9.3.19. (*historical background*) Encrypting secret messages goes as far back as ancient Greece and Rome. As we know, Julius Caesar used a simple shift code to send and receive messages. However, the formal study of encoding and decoding messages probably began with the Arabs in the 1400s. In the fifteenth and sixteenth centuries mathematicians such as Alberti and Viete discovered that monoalphabetic cryptosystems offered no real security. In the 1800s, F. W. Kasiski established methods for breaking ciphers in which a ciphertext letter can represent more than one plaintext letter, if the same key was used several times. This discovery led to the use of cryptosystems with keys that were used only a single time. Cryptography was placed on firm mathematical foundations by such people as W. Friedman and L. Hill in the early part of the twentieth century.

During World War II mathematicians were very active in cryptography. Efforts to penetrate the cryptosystems of the Axis nations were organized in England and in the United States by such notable mathematicians as Alan Turing and A. A. Albert. The period after World War I saw the development of special-purpose machines for encrypting and decrypting messages. The Allies gained a tremendous advantage in World War II by breaking the ciphers produced by the German Enigma machine and the Japanese Purple ciphers.

By the 1970s, interest in commercial cryptography had begun to take hold. There was a growing need to protect banking transactions, computer data, and electronic mail. In the early 1970s, IBM developed and implemented LUZIFER, the forerunner of the National Bureau of Standards' Data Encryption Standard (DES).

The concept of a public key cryptosystem, due to Diffie and Hellman, is very recent (1976). It was further developed by Rivest, Shamir, and Adleman with the RSA cryptosystem (1978). It is not known how secure

any of these systems are. The trapdoor knapsack cryptosystem, developed by Merkle and Hellman, has been broken. It is still an open question whether or not the RSA system can be broken. As of 2014, 360-digit numbers have been factored—in practice, RSA keys of more than 1000 digits may be used.

There's been a great deal of controversy about research in cryptography in recent times: the National Security Agency would like to keep information about cryptography secret, whereas the academic community has fought for the right to publish basic research. What's not controversial is that cryptography has come a long way since 1929, when Henry Stimson, Secretary of State under Herbert Hoover, dismissed the Black Chamber (the State Department's cryptography division) in 1929 on the ethical grounds that “gentlemen do not read each other's mail.” △

9.4 References and suggested readings

- [1] Bressoud, D. M. *Factorization and Primality Testing*. Springer-Verlag, New York, 1989.
- [2] Diffie, W. and Hellman, M. E. “New Directions in Cryptography,” *IEEE Trans. Inform. Theory* **22** (1976), 644–54.
- [3] Gardner, M. “A New Kind of Cipher that Would Take a Million Years to Break,” *Scientific American* **237** (1977), 120–24.
- [4] Granville, A. “Primality Testing and Carmichael Numbers,” *Notices of the American Mathematical Society* **39**(1992), 696–700.
- [5] Hellman, M. E. “The Mathematics of Public Key Cryptography,” *Scientific American* **241** (1979), 130–39.
- [6] Koblitz, N. *A Course in Number Theory and Cryptography*. Springer-Verlag, New York, 1987.
- [7] Pomerance, C., ed. *Cryptology and Computational Number Theory*. Proceedings of Symposia in Applied Mathematics, vol. 42. American Mathematical Society, Providence, RI, 1990.
- [8] Rivest, R. L., Shamir, A., and Adleman, L., “A Method for Obtaining Signatures and Public-key Cryptosystems,” *Comm. ACM* **21**(1978), 120–26.

9.5 Hints for “Applications (I): Introduction to Cryptography” exercises

Exercise 9.2.23: Prove by contradiction. If A has an inverse, then there exists a matrix B such that $AB = I$. Take the determinant of this equation, and show that it produces a contradiction to the fact that $(a \odot d) \ominus (b \odot c)$ has no inverse.

Exercise 9.3.2: It is possible to list all of the numbers between 1 and pq which are *not* relatively prime to pq .

Exercise 9.3.3(c): Remember your exponent rules!

Exercise 9.3.9: Consider the case where n is the product of two *equal* factors: $n = a \cdot a$. Then how large must a be? Compare this with the general case where n is the product of two unequal factors: $n = xy$. Show that the *smaller* of these two factors must be smaller than a .

Exercise 9.3.11: Suppose $n = ab$. Choose a to be the smaller factor. Write $a = x - y$ and $b = x + y$, and solve for x and y . To finish the proof, you need to prove that x and y must both be integers.

Exercise 9.3.12: Solve for x . What value of y makes x as small as possible?

Exercise 9.3.13(a): Prove by contradiction. (b): Write $m = 2k + 1$. (d): Use part (c), part (b), and the distributive law. (e): This is similar to part(b).

9.6 Study guide for “Applications (I): Introduction to Cryptography” chapter

Section 9.2, Private key cryptography

Concepts:

1. Shift codes (monoalphabetic cryptosystem – one-to-one substitution)
2. Affine codes (monoalphabetic cryptosystem – one-to-one substitution)
3. Affine codes (polyalphabetic cryptosystem – ciphertext represents more than one letter)
4. Modular matrix multiplication
5. Matrix inverses in \mathbb{Z}_n

Competencies

1. Know how to encode and decode using the shift code method. (9.2.2, 9.2.3, 9.2.6, 9.2.7)
2. Be able to find the decoding function when given a valid encoding affine function. (9.2.10, 9.2.13)
3. Be able to solve modular matrix multiplication. (9.2.20)
4. Be able to find matrix inverses in \mathbb{Z}_n , when they exist. (9.2.24)

Section 9.3, Public key cryptography

Concepts:

1. RSA cryptosystem (more advanced encryption system: uses modular exponentiation to encrypt and decrypt messages)
2. Binary expansion (like decimal expansion, except it uses base 2 instead of base 10)
3. Identifying prime numbers by brute force (Euler totient function and sieve of Eratosthenes)

4. Identifying prime numbers by Fermat’s test for primality (Fermat’s factorization algorithm)
5. Pseudoprime numbers

Key formulas

1. Fermat’s factorization algorithm: If n is an odd composite number, then $n = x^2 - y^2 = (x - y)(x + y)$ for some x and y
2. Pseudoprime formula: the odd number n is a pseudoprime base b if $\text{mod}(b^{n-1}, n) = 1$

Competencies

1. Compute binary expansion of exponent, either by hand (9.3.3) or by spreadsheet (9.3.4).
2. Using binary expansion of exponent to rapidly compute modular exponentials by spreadsheet. (9.3.3, 9.3.4)
3. Given a base, encoding (decoding) key, and message, encrypt (decrypt) RSA messages. (9.3.5, 9.3.6)
4. Given a base and encoding (or decoding) key, use brute force method by spreadsheet to find the corresponding decoding (or encoding) key. (9.3.9)
5. Use Fermat’s factoring method by spreadsheet to factor large numbers. (9.3.15)
6. Determine if a number is pseudoprime relative to a given base. (9.3.17)

Sigma Notation

We're about to start looking at polynomials, which means we'll be working with sums of terms—sometimes many terms. Such sums are often written using a special notation known as “sigma notation”. It's possible that you are already a master of sigma notation. If not, you can brush up with the material in this section. (At very least, you should try some of the exercises to make sure that you haven't gotten rusty.)

David Weathers wrote the original version of Sections 10.1-10.4. Johnny Watts started Sections 11.1-10.5, while Rachel McCoy made significant improvements to Section 10.5.

10.1 Lots of examples

In mathematics one often encounters sums everywhere. Sometimes these sums have very few terms, but occasionally the sums can reach hundreds, thousands or even an infinite number of terms. In these cases, rather than listing each and every term or listing the first several terms and assuming the pattern is obvious, one can represent a sum using *summation notation*, often referred to as *sigma notation*.

Sigma notation has four main parts: the *index variable*, the *starting value*, the *final value* and the *formula*. These parts are illustrated in the following example.

Example 10.1.1. Consider:

$$\sum_{i=1}^{10} (i + 2)$$

In this case, the Σ symbol lets us know that this is a sum. The $i = 1$ serves two functions. It tells us that the index variable is i , and that i has a starting value of 1. The 10 is the final value, and the $(i + 2)$ to the right of the Σ is the formula. The i in the formula, takes each integer value from the starting value (1) to the final value (10). Therefore we have:

$$\sum_{i=1}^{10} (i + 2) = 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12 = 75.$$



This notation has a lot of flexibility. For example, the sum's formula can be a constant value:

$$\sum_{i=1}^{10} 5 = 5 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 5 + 5 = 50.$$

Or we could have the index as an exponent:

$$\sum_{i=1}^{10} (2^i) = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{10}$$

Now all the examples so far have a numerical value that can be calculated. However, summation notation can also be used to express functions of variables such as:

$$\sum_{i=1}^{10} (x^i) = x^1 + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9 + x^{10}$$

Note that any variables in the formula that do not match the index are left as variables (such as x in the previous example). While we do not know what the sum value is other than in terms of x , we can much more concisely state the sum in sigma notation.

Another typical use for the index in the formula is to denote an index in a coefficient. Consider the polynomial:

$$ax^2 + bx + c.$$

Instead of using a different letter, we can use a subscript to denote a different value but use the same letter:

$$a_2x^2 + a_1x + a_0.$$

And when we use subscripts, we can use the index in the formula to denote that subscript.

$$\sum_{i=0}^2 a_i x^i$$

Changing the starting and/or final values does not affect the pattern of the formula, but it does change the number of terms and any index values used in that formula. Take one of the previous examples:

$$\sum_{i=1}^{10} i = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10$$

If we were to change the $i = 1$ to $i = 4$ then the sum would lose terms 1,2,3:

$$\sum_{i=4}^{10} i = 4 + 5 + 6 + 7 + 8 + 9 + 10$$

Likewise, if we were to also change the 10 to 6, it would lose the terms 10,9,8 and 7;

$$\sum_{i=4}^6 i = 4 + 5 + 6.$$

Exercise 10.1.2. Evaluate the following:

(a) $\sum_{i=0}^{400} 2$

(b) $\sum_{j=17}^{20} 2j^2 - j$

(c) $\sum_{k=0}^4 (x^{2k} - k)$ (Your answer should be in terms of x).

(d) $\sum_{k=0}^{100} \left(\frac{1}{k+2} - \frac{1}{k+1} \right)$

◇

10.2 Algebraic rules for Sigmas

As with any algebraic notation, there are rules that allow us to do algebraic manipulations with expressions that involve sigmas. In this section, we explore some of these rules.

10.2.1 Constant multiples, sums, and products of sums

Many of the rules for manipulating sigmas follow from the commutative law of addition and the associative and distributive laws for addition and multiplication. To motivate these rules, we will look at simple examples and then generalize.

Let's first consider the example:

$$\sum_{i=0}^5 2i$$

We know this is the sigma notation for $2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 + 2 \cdot 4 + 2 \cdot 5$. Using the distributive property of addition and multiplication of integers, we know this sum is the same as $2 \cdot (1 + 2 + 3 + 4 + 5)$. Now we convert the sum in the parenthesis to sigma notation to yield

$$2 \cdot \sum_{i=0}^5 i.$$

The same argument could be used for any sum multiplied by any constant. We can write this rule as:

$$\sum_{i=a}^b c \cdot d_i = c \cdot \sum_{i=a}^b d_i, \quad (10.2.1)$$

where c denotes an arbitrary constant and d_i represents the term of the sum corresponding to index i . Suppose next we take the sum of two sums and combine them into a single sum using the commutative law:

$$\begin{aligned} \sum_{i=0}^4 i + \sum_{j=0}^4 2^j &= (0 + 1 + 2 + 3 + 4) + (2^0 + 2^1 + 2^2 + 2^3 + 2^4) \\ &= (0 + 2^0) + (1 + 2^1) + (2 + 2^2) + (3 + 2^3) + (4 + 2^4) \\ &= \sum_{i=0}^4 (i + 2^i). \end{aligned}$$

Applying the same process to an arbitrary sum of two sums gives:

$$\sum_{i=0}^n x_i + \sum_{j=0}^n y_j = \sum_{i=0}^n (x_i + y_i) \quad (10.2.2)$$

Now let's look at an example of a product of two sums. Using the commutative law of addition and the distributive law repeatedly, we have:

$$\begin{aligned} \left(\sum_{i=1}^4 i \right) \left(\sum_{j=1}^3 \frac{1}{j} \right) &= (1 + 2 + 3 + 4)(1 + 1/2 + 1/3) \\ &= 1(1 + 1/2 + 1/3) + 2(1 + 1/2 + 1/3) + 3(1 + 1/2 + 1/3) + 4(1 + 1/2 + 1/3) \\ &= 1 \cdot 1 + 1 \cdot (1/2) + 1 \cdot (1/3) + 2 \cdot 1 + 2 \cdot (1/2) + 2 \cdot (1/3) + 3 \cdot 1 + 3 \cdot (1/2) + 3 \cdot (1/3) \\ &\quad + 4 \cdot 1 + 4 \cdot (1/2) + 4 \cdot (1/3). \end{aligned}$$

We see that the product of a sum of 4 terms with a sum of 3 terms gives a sum of $4 \cdot 3 = 12$ terms. Furthermore, the 12 terms consist of all possible products of (a term from the first sum) times (a term from the second sum). We introduce the following notation to describe this:

$$\left(\sum_{i=1}^4 i \right) \left(\sum_{j=1}^3 \frac{1}{j} \right) = \sum_{i=1}^4 \sum_{j=1}^3 \frac{i}{j}.$$

We may generalize the above example to the product of two arbitrary sums as follows:

$$\begin{aligned} \left(\sum_{i=1}^n x_i \right) \left(\sum_{j=1}^m y_j \right) &= \sum_{i=1}^n \left(x_i \left(\sum_{j=1}^m y_j \right) \right) \\ &= \sum_{i=1}^n \sum_{j=1}^m x_i y_j \end{aligned} \quad (10.2.3)$$

Exercise 10.2.4. In view of Equation (10.2.2), one might suppose that the following is true:

$$\left(\sum_{i=0}^n x_i \right) \cdot \left(\sum_{i=0}^n y_i \right) \stackrel{?}{=} \sum_{i=0}^n x_i y_i$$

- (a) Is this statement always true? If not, give an example of sequences $\{x_i\}$ and $\{y_i\}$ such that the equality does not hold.

- (b) Is this statement *ever* true? If possible, give an example of sequences $\{x_i\}$ and $\{y_i\}$ such that the equality *does* hold.

◇

We may now use Equations (10.2.2) and (10.2.3) to break down complicated multiple sums into simpler parts which may be evaluated more easily:

Exercise 10.2.5. Given that $\sum_{i=1}^{20} i = 210$ and $\sum_{i=1}^{20} i^2 = 2870$, Evaluate the following double sums:

- (a)

$$\sum_{i=1}^{20} \sum_{j=1}^{20} (i+j)^2$$

- (b)

$$\sum_{i=1}^{20} \sum_{j=1}^{20} (i-j)^2$$

- (c)

$$\sum_{i=1}^{20} \sum_{j=1}^{20} (3i-4j)^2$$

◇

10.3 Change of variable and rearrangement of sums



Change of variable (a.k.a. substitution) is an extremely powerful technique in mathematics. We've used change of variable in previous chapters, and most likely you've seen change of variable when doing integrals in calculus. Change of variable can also be used to simplify sums (in fact, there is a very close relationship between integrals and sums, so it's no surprise that the same techniques are useful in both regimes).

Consider for example the following sum:

$$\sum_{i=2}^7 (i-1)$$

If we write this out term by term, we get $1 + 2 + 3 + 4 + 5 + 6$ which has a very easy representation as a sigma, namely $\sum_{j=1}^6 j$. It follows that

$$\sum_{i=2}^7 (i-1) = \sum_{j=1}^6 j.$$

Writing it this way, we can see how we got from one sum to the other by making the replacement $j = i - 1$. We also had to change the limits of the sum accordingly (just like you have to change integral limits when you change variable).

A similar example is:

$$\begin{aligned} \frac{1}{8} \sum_{j=5}^9 2^{j-2} &= \sum_{j=5}^9 2^{j-2} \cdot 2^{-3} \\ &= \sum_{j=5}^9 2^{j-5}. \end{aligned}$$

We may substitute $i = j - 5$. Noticing that $j = 5 \Rightarrow i = 0$ and $j = 9 \Rightarrow i = 4$, we obtain

$$\frac{1}{8} \sum_{j=5}^9 2^{j-2} = \sum_{i=0}^4 2^i.$$

Exercise 10.3.1. Take the following sigma notation examples and change the formula and final value so that the starting value becomes 0 and the sum maintains the same value. Calculate the value of both the listed sum and the resulting sum to show that the value is the same.

(a) $\sum_{i=3}^7 2i$

(b) $\sum_{j=7}^{21} \cos(j\pi)$

(c) $\sum_{j=20}^{24} (j - 20)$

◇

Breaking up sums and re-indexing can sometimes make things a lot simpler. Consider the following example:

$$S = \sum_{k=1}^{21} \operatorname{cis} \left(\frac{2\pi k}{20} \right).$$

Let's break this up into two sums, from $k = 1$ to 10 and from $k = 11$ to 21:

$$S = \sum_{k=1}^{10} \operatorname{cis} \left(\frac{2\pi k}{20} \right) + \sum_{k=11}^{21} \operatorname{cis} \left(\frac{2\pi k}{20} \right).$$

It would be nice to combine these two sums into one. But to do this, we need to make the summation limits the same. So we'll change variable: $j = k - 10$ in the second sum. Then the sum from $k = 11$ to 21 becomes a sum from $j = 1$ to 11:

$$S = \sum_{k=1}^{10} \operatorname{cis} \left(\frac{2\pi k}{20} \right) + \sum_{j=1}^{11} \operatorname{cis} \left(\frac{2\pi(j+10)}{20} \right).$$

Now let's massage the sum over j a little bit. Using the properties of cis , the summand can be rewritten:

$$\begin{aligned} \operatorname{cis} \left(\frac{2\pi(j+10)}{20} \right) &= \operatorname{cis} \left(\frac{2\pi j}{20} + \pi \right) \\ &= \operatorname{cis} \left(\frac{2\pi j}{20} + \pi \right) \\ &= \operatorname{cis} \left(\frac{2\pi j}{20} \right) \operatorname{cis}(\pi) \\ &= -\operatorname{cis} \left(\frac{2\pi j}{20} \right). \end{aligned}$$

Furthermore, we don't change anything if we replace the j with k , since it's just a sum index anyway. Making these substitutions, we have:

$$S = \sum_{k=1}^{10} \operatorname{cis} \left(\frac{2\pi k}{20} \right) + \sum_{k=1}^{11} -\operatorname{cis} \left(\frac{2\pi k}{20} \right).$$

Now we can split the 11'th term off from the second sum, and combine the two sums from 1 to 10:

$$\begin{aligned}
 S &= \sum_{k=1}^{10} \operatorname{cis} \left(\frac{2\pi k}{20} \right) + \sum_{k=1}^{10} -\operatorname{cis} \left(\frac{2\pi k}{20} \right) - \operatorname{cis} \left(\frac{2\pi \cdot 11}{20} \right) \\
 &= \sum_{k=1}^{10} \left(\operatorname{cis} \left(\frac{2\pi k}{20} \right) - \operatorname{cis} \left(\frac{2\pi k}{20} \right) \right) - \operatorname{cis} \left(\frac{2\pi \cdot 11}{20} \right) \\
 &= \sum_{k=1}^{10} (0) - \operatorname{cis} \left(\frac{2\pi \cdot 11}{20} \right) \\
 &= -\operatorname{cis} \left(\frac{2\pi \cdot 11}{20} \right). \\
 &= \operatorname{cis} \left(\frac{\pi}{10} \right).
 \end{aligned}$$

Exercise 10.3.2. By splitting up the sums and rearranging, evaluate the following sums:

(a) $\sum_{k=1}^{15} \operatorname{cis} \left(\frac{\pi k}{7} \right)$

(b) $\sum_{k=1}^{35} \operatorname{cis} \left(\frac{\pi k}{9} \right)$

◇

We've already seen cases where one sigma is inside another, when taking the product of two sums. Nested sums like this can often be rearranged to obtain useful formulas.

Example 10.3.3. Consider the product of the sums $\sum_{i=0}^2 3^i$ and $\sum_{j=0}^2 3^{-j}$. By the distributive law and additive commutivity we have:

$$\begin{aligned}
\left(\sum_{i=0}^2 3^i\right) \left(\sum_{j=0}^2 3^{-j}\right) &= \sum_{i=0}^2 \left(3^i \left(\sum_{j=0}^2 3^{-j}\right)\right) \\
&= \sum_{i=0}^2 \left(\sum_{j=0}^2 3^{i-j}\right) \\
&= \sum_{i=0}^2 \sum_{j=0}^2 3^{i-j}.
\end{aligned}$$

This sum has 9 terms, where each term corresponds to a pair (i, j) as shown in Figure 10.3.1. These terms can be arranged along diagonal lines (as shown in the figure) so that all terms on each diagonal have the same value. So we can add the terms diagonal-by-diagonal as follows:

$$\begin{aligned}
\sum_{i=0}^2 \sum_{j=0}^2 3^{i-j} &= 3^{-2} + 2 \cdot 3^{-1} + 3 \cdot 3^0 + 2 \cdot 3^1 + 3^2 \\
&= 1/9 + 2/3 + 3 + 6 + 9 \\
&= 18 \frac{7}{9}.
\end{aligned}$$

We may rewrite the five terms on the right in summation notation to obtain the following equalities:

$$\begin{aligned}
\sum_{i=0}^2 \sum_{j=0}^2 3^{i-j} &= \sum_{n=1}^3 n 3^{3-n} + \sum_{n=1}^2 n 3^{n-3} \\
&= 3 + \sum_{n=1}^2 n(3^{n-3} + 3^{3-n}) \\
&= 3 + \sum_{m=1}^2 (3-m)(3^m + 3^m)
\end{aligned}$$



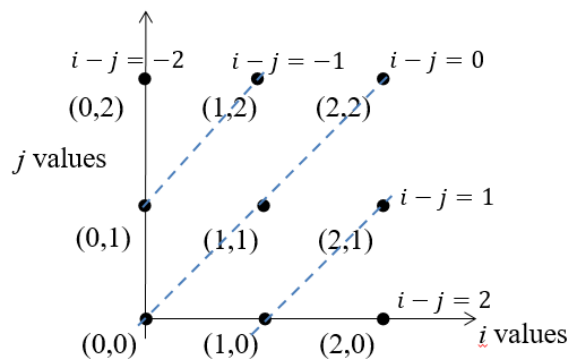


Figure 10.3.1. Grid points corresponding to the terms in the sum: $\sum_{i=0}^2 \sum_{j=0}^2 3^{i-j}$.

Exercise 10.3.4. Show that the sum on the right-hand side of the preceding equation can be written alternatively as:

$$\begin{aligned} \sum_{n=1}^3 n3^{3-n} + \sum_{n=1}^2 n3^{n-3} &= 3 + \sum_{n=1}^2 n(3^{n-3} + 3^{3-n}) \\ &= 3 + \sum_{m=1}^2 (3-m)(3^m + 3^m). \end{aligned}$$

◇

Exercise 10.3.5. By generalizing the above example, rewrite each of the following expressions as a product of sums:

(a)

$$\sum_{n=1}^4 n4^{4-n} + \sum_{n=1}^3 n4^{n-4}$$

(b)

$$11 + \sum_{n=1}^{10} (11-n)(5^n + 5^{-n})$$

◇

The situation becomes interesting when the sum inside depends on the the index variable of the outside sigma:

$$\sum_{i=0}^3 \sum_{j=0}^i 1$$

Unlike previous double sums, the inside sum will change depending on what i is. When $i = 0$ then $\sum_{j=0}^i 1 = \sum_{j=0}^0 1 = 1$ so 1 would be the first term in the outside sum. When $i = 1$ then $\sum_{j=0}^i 1 = \sum_{j=0}^1 1 = 1 + 1 = 2$ so 2 would be the next term. With each successive term, the inside sum increases by 1, so the result is $1 + 2 + 3 + 4 = 10$.

Note that the index of the outer sum may appear in any or all parts of the inner sum. Here are some examples:

$$\sum_{i=0}^3 \sum_{j=i}^{10} 1; \quad \sum_{i=0}^3 \sum_{j=1}^{10i} i; \quad \sum_{i=0}^3 \sum_{j=i}^{2i} (3i + x^j).$$

In some cases, nested sums may be simplified by exchanging the order of summation. Take for example:

$$\sum_{i=0}^2 \sum_{j=0}^i 1$$

The first term has $i = 0$ and $j = 0$: we write this as $(i, j) = (0, 0)$. When $i = 1$, then we have two terms: $j = 0$ and $j = 1$. Finally, when $i = 2$, we have $j = 0, 1$, or 2 . Altogether we have the index pairs: $(0, 0), (1, 0), (1, 1), (2, 0), (2, 1), (2, 2)$. These index pairs may be displayed on a grid, as shown in Figure 10.3.2.

Alternatively, we can arrange these index pairs by j coordinate. When j is 0, i takes the values $(0,1,2)$; when j is 1, i takes the values of $(1,2)$; and when j is 2, i takes the value 2. This can be expressed as the sum:

$$\sum_{j=0}^2 \sum_{i=j}^2 1$$

So far our examples have only two sigmas, but it's quite possible to have an unlimited number of nested sigmas. For example, with three nested sigmas we would have grid points in three dimensions. It doesn't matter what order you sum the terms in—as long as you include them all!

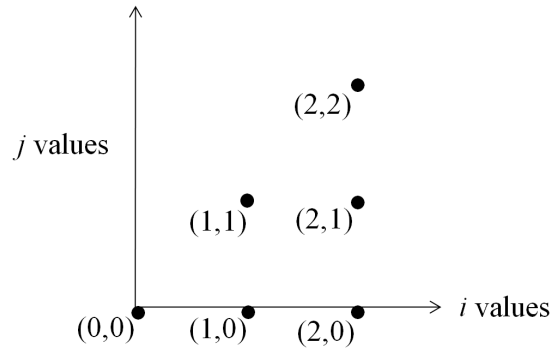


Figure 10.3.2. Grid points corresponding to the terms in the sum: $\sum_{i=0}^2 \sum_{j=0}^i 1$.

Exercise 10.3.6. Draw a grid point diagram (similar to Figure 10.3.2) for each of the following sums. Then use the grid point diagram as a guide to exchanging the order of summation.

(a) $\sum_{i=0}^4 \sum_{j=0}^8 i$

(b) $\sum_{j=0}^3 \sum_{i=j}^{j+3} (i + j)$ (Write as the sum of two summations.)

(c) $\sum_{k=0}^7 \sum_{i=0}^k (2i + 1)$

(d) $\sum_{i=1}^6 \sum_{j=i}^{i+1} (i - j)$ (Write as a nested sum plus two additional terms.)

(e) $\sum_{i=1}^5 \sum_{j=i}^{10} ij$

(f) $\sum_{i=m}^n \sum_{j=i}^{2n} jx^i$ (Write as the sum of two summations.)

- (g) $\sum_{i=m}^n \sum_{j=0}^i (i-j)^2$ (You may assume $m > 0$. Write as the sum of two summations.)

◇

Exercise 10.3.7.

- (a) Using a grid point diagram, interchange the order of summation in the following nested sum:

$$\sum_{k=1}^5 \sum_{\ell=1}^k (\ell + k)$$

- (b) Using a grid point diagram, interchange the order of summation in the following nested sum:

$$\sum_{i=1}^7 \sum_{j=1}^i ij$$

- (c) Using what you've from (a) and (b) above, give a general formula for interchanging sums of the form:

$$\sum_{m=1}^M \sum_{n=1}^m f(m, n),$$

where $f(m, n)$ is an arbitrary expression involving the variables m and n .

◇

Exercise 10.3.8.

- (a) In Exercise 10.3.7, all sums had 1 as lower limit. Repeat the exercise (parts a,b,c) but use 0 as the lower limit on all sums.
- (b) Repeat Exercise 10.3.7 again, but use 2 as the lower limit on all sums.

- (c) Based on what you have learned from (a) and (b), give a general formula for interchanging the order of summation in the following expression:

$$\sum_{m=a}^b \sum_{n=a}^m f(m, n),$$

◇

Exercise 10.3.9. Using exchange of summation and other sum manipulation techniques, find the exact values of the following sums:

(a) $\sum_{i=1}^9 \sum_{j=1}^7 i(8-j)$

(d) $\sum_{i=1}^{10} \sum_{j=i}^{10} \frac{i}{j(j+1)}$

(b) $\sum_{i=1}^{10} \sum_{j=1}^{10} (j-i)$

(e) $\sum_{i=1}^{20} \sum_{j=1}^i \frac{i}{(400-j^2)+j+20}$
(*Hint*)

(c) $\sum_{i=1}^{10} \sum_{j=1}^i \frac{1}{11-j}$

(f) $\sum_{i=1}^{10} \sum_{j=1}^i (j+i)$

◇

10.4 Common Sums

There are several sums, even a few infinite sums, for which the total value is known. One very basic example is:

$$\sum_{i=1}^k 1.$$

Exercise 10.4.1. Evaluate the preceding sum. Be careful—the answer is NOT 1. ◇

Another very useful example is:

$$\sum_{i=1}^k i = 1 + 2 + 3 \cdots + (k-1) + k$$

If one were to take the first term 1 and add it to the last term k , we get $k+1$. If we take the second term 2 and add to the second-to-last term $k-1$ again we get $k+1$. This is true for all terms in between. In the case of an even number of terms (such as $1+2+3+4$), the terms split evenly. In the case of an odd number of terms (such as $1+2+3+4+5+6+7$) we have 3 pairs that add to 8 but an additional term in the middle. In either case, we take the first term add to the last term and multiply that quantity by $1/2$ the number of terms. The formula is thus:

$$\sum_{i=1}^k i = \frac{k(k+1)}{2}.$$

We can use the same reasoning to arrive at the following formula.

$$\sum_{i=a}^k i = a + (a+1) + (a+2) \cdots + (k-1) + k = (k+a)(k-a+1)/2,$$

where a and k are integers and $a < k$.

Exercise 10.4.2.

- Write the sum of odd integers from $2a+1$ to $2k+1$ in sigma notation. (Note that every odd number can be expressed as $2n+1$, where n is an integer.)
- Give a formula for the sum that you wrote in (a). (Use the same reasoning that we used to find sums of consecutive integers.)
- Write the sum of even integers from $2a$ to $2k$ in sigma notation.
- Give a formula for the sum that you wrote in (c).
- Write the sum of every 5th integer from a to $a+5k$ in sigma notation.
- Give a formula for the sum that you wrote in (e).

◇

All of the sums in Exercise 10.4.2 have a constant difference between consecutive terms (this constant difference is also called the *step size*). The step sizes for parts (a), (c), and (e) are 2, 2, and 5 respectively. Any sum with a constant step size is called an *arithmetic sum*: and all arithmetic sums can be evaluated using the same technique that was used in parts (b), (d), and (f) of the exercise.

Geometric sums are defined as the sum of non-negative integer powers of a common base. For example, here is a geometric sum with base $1/2$:

$$\sum_{i=0}^n \left(\frac{1}{2}\right)^i = \left(\frac{1}{2}\right)^0 + \left(\frac{1}{2}\right)^1 + \left(\frac{1}{2}\right)^2 \cdots + \left(\frac{1}{2}\right)^n = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} \cdots + \left(\frac{1}{2}\right)^n$$

We can evaluate this sum using an algebraic trick. Let S be the value of this sum. We can solve for S by multiplying S term-by-term by $1/2$ and subtracting:

$$S = 1 + \frac{1}{2} + \cdots + \frac{1}{2^n} \quad \text{and} \quad \frac{1}{2}S = \frac{1}{2} + \cdots + \frac{1}{2^{n+1}},$$

so that

$$\left(S - \frac{1}{2}S\right) = 1 - \frac{1}{2^{n+1}}.$$

Solving this last equation for S gives:

$$S = \frac{1 - \frac{1}{2^{n+1}}}{1 - \frac{1}{2}}.$$

This same technique can be used to prove the formula for a great variety of geometric sums, as we show in the following exercise.

Exercise 10.4.3.

(a) Let

$$S = \sum_{i=0}^n ar^i,$$

where both a and r are complex numbers, and n is a positive integer. Use the “sum subtraction” technique (used above for the geometric sum with base $1/2$) to derive the the following general formula:

$$\sum_{i=0}^n ar^i = a \frac{1 - r^{n+1}}{1 - r}$$

(Note the formula can also be written: $\sum_{i=0}^n ar^i = a \frac{r^{n+1} - 1}{r - 1}$.)

- (b) Unfortunately, there is one value of r where the above formula doesn't work. What is this uncooperative value of r , and what is the correct formula in this case?

◇

Exercise 10.4.4.

- (a) Evaluate $\sum_{n=0}^{10} \left(\frac{4}{5}\right)^n$.
- (b) Evaluate $\sum_{n=0}^{100} \left(\frac{4}{5}\right)^n$.
- (c) Evaluate $\sum_{n=0}^{1000} \left(\frac{4}{5}\right)^n$.
- (d) What do you think happen when the upper limit of the sum gets arbitrarily large?

◇

Exercise 10.4.5. Use “sum subtraction” to obtain a general formula for the following sum:

$$S = \sum_{k=m}^n w \cdot z^k,$$

Where m, n are arbitrary integers ($m < n$) and w, z are arbitrary complex numbers.

◇

Exercise 10.4.6.

- (a) Let $z = \text{cis}(2\pi/3)$. Evaluate $\sum_{n=1}^3 z^n$.
- (b) Let $z = \text{cis}(2\pi/10)$. Evaluate $\sum_{n=-4}^5 z^n$.
- (c) Let $z = \text{cis}(2\pi/13)$. Evaluate $\sum_{n=2}^{14} z^n$.
- (d) Write down an equation that generalizes the results of parts (a),(b),(c). Prove your equation.

◇

Some sums can be evaluated by grouping terms together to partially cancel out. Two examples are:

$$1-2+3-4+\dots-1000 = (1-2)+(3-4)+\dots+(999-1000) = (-1)+(-1)+\dots+(-1) = -500.$$

$$\begin{aligned} 1-4+9-16+25-36+\dots+49^2 &= 1+(-4+9)+(-16+25)+\dots+(-48^2+49^2) \\ &= 1+5+9+\dots+97 \\ &= (1+4\cdot 0)+(1+4\cdot 1)+\dots+(1+4\cdot 24) \\ &= (1+\dots+1)+4\cdot(0+1+\dots+24) \\ &= 24+4\cdot(24+1)\frac{24}{2} \\ &= 24+1200=1224. \end{aligned}$$

In calculus you saw (or will see) sums that have an infinite number of terms, otherwise known as *infinite series*. Some examples include:

$$\begin{aligned} e^x &= \sum_{i=0}^{\infty} \frac{x^i}{i!} = 1 + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} \dots \\ \sin(x) &= \sum_{i=0}^{\infty} \frac{(-1)^i x^{2i+1}}{(2i+1)!} = \frac{x^1}{1!} - \frac{x^3}{3!} + \frac{x^5}{5!} \dots \end{aligned}$$

Although we won't be talking about infinite series, the same summation notation that we've been using also applies to sums with an infinite number of terms.

10.5 Summation by parts

Those who have studied integrals in calculus may be familiar with the process of integration by parts. This is used when you need to find the integral of the product of two terms. While this process is used for continuous situations, there is a version of this process for discrete situations called *summation by parts*.

To show how summation by parts works, we'll look at a particular case. Consider the following product of sums:

$$\left(\sum_{n=1}^5 a_n \right) \left(\sum_{n=1}^5 b_n \right).$$

If we broke this up into individual terms, we'd obtain $n \cdot n = n^2$ terms of the form $a_j b_k$. Figure 10.5.1 shows the terms arranged on a grid. We've separated these terms into two parts using a diagonal line, and we've further grouped terms either by row (above the line) or by column (below the line). You'll see in a minute why we've arranged things like this.

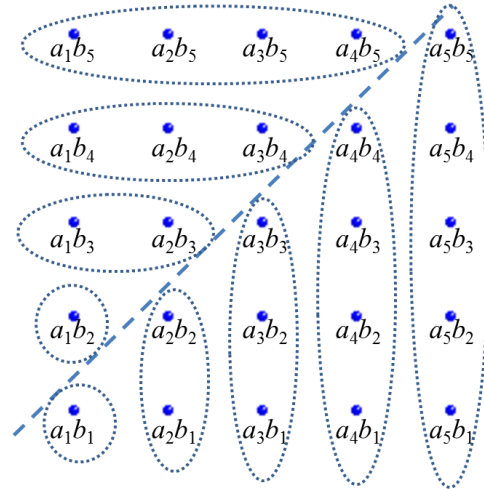


Figure 10.5.1. Arrangements of terms in the product of sums $\left(\sum_{n=1}^5 a_n\right) \left(\sum_{n=1}^5 b_n\right)$.

Now let's go back and express the sum of all these terms a different way. We'll introduce the notation:

$$A_k = \sum_{j=1}^k a_j \text{ and } B_k = \sum_{j=1}^k b_j.$$

A_k and B_k are the k th **partial sums** for the series $\sum a_j$ and $\sum b_j$, respectively. The product of sums that we started with can be written succinctly as $A_5 B_5$.

We may use this new notation to re-express the grouped terms in the figure. Consider first the terms below the diagonal line. These terms are grouped by column, and each group is encircled by an oval:

- The sum of the first oval(column on far left) is: $a_1 b_1 = a_1 B_1$;

- The sum of the second oval(column second from the left) is: $a_2(b_1 + b_2) = a_2B_2$;
- The sum the third oval(column third from the left) is: $a_3(b_1 + b_2 + b_3) = a_3B_3$;
- The sum of the fourth oval(column fourth from left) is: $a_4(b_1 + b_2 + b_3 + b_4) = a_4B_4$;
- The sum of the fifth oval(column on the far right) is: $a_5(b_1 + b_2 + b_3 + b_4 + b_5) = a_5B_5$.

Adding these five sums together accounts for all the terms below the diagonal line:

$$a_1B_1 + a_2B_2 + \dots + a_5B_5 = \sum_{k=1}^5 a_kB_k,$$

where we've used summation notation to make the expression more compact.

Now let's repeat this process for the horizontal ovals above the diagonal line:

- The sum for the first oval(bottom row above line) is: $a_1b_2 = A_1b_2$;
- The sum for the second oval(second row from bottom) is: $(a_1 + a_2)b_3 = A_2b_3$;
- The sum for the third oval(second row from the top) is: $(a_1 + a_2 + a_3)b_4 = A_3b_4$;
- The sum for the fourth oval(top row) is: $(a_1 + a_2 + a_3 + a_4)b_5 = A_4b_5$.

Adding these five sums together accounts for all the terms below the diagonal line:

$$A_1b_2 + \dots + A_4b_5 = \sum_{k=1}^{5-1} A_kb_{k+1}.$$

Since we've now accounted for terms both above and below the line, we obtain the sum of all terms by adding together:

$$A_5B_5 = \sum_{k=1}^5 a_kB_k + \sum_{k=1}^{5-1} A_kb_{k+1}.$$

By rearranging this equation, we find:

$$\sum_{k=1}^5 a_k B_k = A_5 B_5 - \sum_{k=1}^{5-1} A_k b_{k+1}.$$

There's really nothing special about the number '5' in our above expression—we just chose it because this was a relatively simple case that we could illustrate. To get the general formula, we simply replace '5' with 'n':

$$\sum_{k=1}^n a_k B_k = A_n B_n - \sum_{k=1}^{n-1} A_k b_{k+1}.$$

Notice the striking similarity between this formula and the formula for integration by parts:

$$\int_a^b u dv = uv|_a^b - \int_a^b v du.$$

The resemblance makes a lot of sense, since integration is essentially a kind of summation (more precisely, a summation taken to a limit.)

Now let's look at some examples to see how we can make use of this formula.

Example 10.5.1. Evaluate $\sum_{k=1}^n 2^{k-1} k$.

In order to use the summation by parts formula, we need to define a_k and B_k so that the summand $2^{k-1} k$ is the product of a_k and B_k . Just as in integration by parts, we want to make our choice based on what makes the calculations easiest. Note that B_k is a partial sum of k terms, and that $k = 1 + \dots + 1$. So it's natural to choose $B_k = k$, which means that $a_k = 2^{k-1}$.

Based on our choice of B_k and a_k , we can now figure out b_k and A_k . As we noted above, B_k is the sum of k 1's, so that $b_k = 1$. This leaves us with $a_k = 2^{k-1}$, so that

$$A_k = \sum_{j=1}^k a_j.$$

As we've seen before, we may rewrite this by shifting the starting value of the index, so that

$$A_k = \sum_{j'=0}^{k-1} 2^{j'} = \frac{2^k - 1}{2 - 1} = 2^k - 1,$$

where we've used our standard formula for the sum of geometric series.

Summarizing our progress so far, we have:

$$a_k = 2^{k-1}; \quad B_k = k; \quad b_k = 1; \quad A_k = 2^k - 1.$$

Plugging the above values into the summation by parts formula, we find:

$$\sum_{k=1}^n 2^{k-1}k = (2^n - 1)n - \sum_{k=1}^{n-1} (2^k - 1).$$

The summation on the far right can be evaluated by breaking it into two separate parts:

$$\sum_{k=1}^{n-1} (2^k - 1) = \sum_{k=1}^{n-1} 2^k - \sum_{k=1}^{n-1} 1 = (2^n - 1) - (n - 1).$$

◆

We can put this into our equality and do some further algebraic puttering to obtain the final result:

$$\begin{aligned} \sum_{k=1}^n 2^{k-1}k &= (2^n - 1)n - (2^n - 1) + (n - 1) \\ &= 2^n n - n - (2^n - 1) + (n - 1) \\ &= 2^n n - 2^n \\ &= 2^n(n - 1). \end{aligned}$$

Exercise 10.5.2. Evaluate $\sum_{k=1}^n k^2$ by taking $B_k = k$ and $a_k = k$. You will need the expression for the sum $1 + 2 + \dots + m$ that we derived previously.
◆

From the preceding examples we may see that $B_k = k$ is a frequent choice. This is closely related to the fact that $u = x$ is a frequent choice when applying the integration by parts formula.

Exercise 10.5.3. Prove the following equation using summation by parts:

$$\sum_{k=1}^n k^3 = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}$$

◇

Exercise 10.5.4.(a) Evaluate $\sum_{k=1}^n 3^k k$.(b) Evaluate $\sum_{k=1}^n 3^k k^2$.(c) Evaluate $\sum_{k=1}^{7n} \operatorname{cis}(2\pi k/7) \cdot k$.

◇

Application: Sigma Notation in Linear Algebra

11.1 Introduction to sigma notation in linear algebra

Linear algebra is the algebra of real space: not just 3-dimensional space, but n -dimensional generalizations. The important mathematical objects in linear algebra are vectors and matrices: You may remember that matrices represent functions (transformations) that act on vectors. Although linear algebra is a relatively recent field of mathematics (which got its start in the mid-1800's), since the advent of computers it has risen to the 'top of the heap' so to speak, so that most modern applications of mathematics to real-world problems are built on linear algebra.

Sigma notation is a powerful notational tool for expressing relations and proving identities in linear algebra. In this chapter, we will look at some of the ways that sigma notation can be used to prove properties of vectors and matrices in three-dimensional space. These properties are basic to in the physics of moving objects and fields.

This chapter ties together material from several chapters in the book. Besides sigma notation, we need concepts from sets, functions, and just a little bit from permutations (we'll give the background you need in this chapter). To understand the chapter, the reader should already have seen vectors and matrices (up to size 3×3) and know a little bit about how they work.

In the following discussions, we will assume that all matrices have real entries. However, all of the results that we will prove also apply (in some cases, with slight modifications) for matrices with *complex* entries, or matrices with entries in \mathbb{Z}_p .

11.2 Matrix multiplication

It should come as no surprise that summation notation commonly shows up when working with matrices. In the following discussion, we will follow the common practice of denoting a matrix with a capital letter in italics, and the entries of the matrix with the same letter in lowercase. Thus for example, $a_{2,4}$ denotes the entry of matrix A in row 2, column 4.

Consider the example of multiplying the 3×3 matrix A and the 3×2 matrix B .

$$AB = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix} \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \\ b_{3,1} & b_{3,2} \end{pmatrix}$$

$$= \begin{pmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} + a_{1,3}b_{3,1} & a_{1,1}b_{1,2} + a_{1,2}b_{2,2} + a_{1,3}b_{3,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{2,1} + a_{2,3}b_{3,1} & a_{2,1}b_{1,2} + a_{2,2}b_{2,2} + a_{2,3}b_{3,2} \\ a_{3,1}b_{1,1} + a_{3,2}b_{2,1} + a_{3,3}b_{3,1} & a_{3,1}b_{1,2} + a_{3,2}b_{2,2} + a_{3,3}b_{3,2} \end{pmatrix}$$

Wouldn't it be nice if we could shorten that mess? Fortunately we can! Let the matrix C be the product AB , where A is an $m \times n$ matrix and B is an $n \times p$ matrix, which implies that the dimensions of C will be $m \times p$.¹ If the row number is given by the first index (in this case i), and the column number is given by the second index (in this case j), we can write the entries of C as:

$$c_{i,j} = \sum_{k=1}^n a_{i,k}b_{k,j}$$

Exercise 11.2.1. In the above formula, both i and j are restricted to a particular range of values. What are the possible values of i and j ? \diamond

¹Remember the requirement for multiplying any two matrices is that the number of columns of the first must match the number of rows of the second.

Let's show how this formula works in a specific case. Suppose A is a 3×3 matrix and B is a 3×2 matrix as in our previous example, then the result of the product AB is a 3×2 matrix that we can call C . Now suppose we want to find the entry on the third row in the second column of C , then we would compute:

$$\begin{aligned} c_{3,2} &= \sum_{k=1}^3 a_{3,k}b_{k,2} \\ &= a_{3,1}b_{1,2} + a_{3,2}b_{2,2} + a_{3,3}b_{3,2}. \end{aligned}$$

Sure enough, when we look at the long version we wrote earlier for the product AB our result matches the entry on the second row, third column.

The above formula makes it possible to calculate individual matrix elements, without having to compute the entire matrix.

Exercise 11.2.2.

- Let the entries of A be given by $a_{i,j} = \sqrt{i+j}$ for $1 \leq i, j \leq 100$. Let $C = A \cdot A$ (we can also write $C = A^2$). Compute $c_{10,10}$.
- Let the entries of A and B be given by $a_{i,j} = (i+j)^2$ and $b_{i,j} = \frac{1}{i+j}$ for $1 \leq i, j \leq 27$. Let $C = A \cdot B$. Compute $c_{8,8}$.
- For the matrices A and B in part (b), give a general formula for $c_{k,k}$, $1 \leq k \leq 27$ where $C = AB$.

◇

Exercise 11.2.3.

- Let the entries of A and B be given by $a_{i,j} = 2^{i+j}$ and $b_{i,j} = 2^{-(i+j)}$ for $1 \leq i, j \leq 50$. Let $C = AB$. Compute $c_{7,11}$.
- Let the entries of A and B be given by $a_{i,j} = 3^{i+j}$ and $b_{i,j} = 4^{-(i+j)}$ for $1 \leq i, j \leq 22$. Let $C = AB$. Compute $c_{5,4}$.
- Let the entries of A and B be given by $a_{i,j} = r^{i+j}$ and $b_{i,j} = s^{-(i+j)}$ for $1 \leq i, j \leq N$, where r and s are arbitrary real numbers. Let $C = AB$. Give a general formula for $c_{i,j}$, $1 \leq i, j \leq N$. (Note the same formula works if r and s are taken as complex numbers.)

◇

Exercise 11.2.4.

- (a) Let the entries of A and B be given by $a_{i,j} = 2^{ij}$ and $b_{i,j} = 2^{-ij}$ for $1 \leq i, j \leq 20$. Let $C = AB$. Compute $c_{11,11}$.
- (b) For A, B, C as in part (a), compute $c_{9,6}$.
- (c) Let the entries of A and B be given by $a_{i,j} = 2^{ij}$ and $b_{i,j} = 2^{-ij}$ for $1 \leq i, j \leq N$. Let $C = AB$. Give a general formula for $c_{i,j}$ that is valid for any (i, j) with $1 \leq i, j \leq N$.
- (d) Let the entries of A and B be given by $a_{i,j} = w^{ij}$ and $b_{i,j} = w^{-ij}$ for $1 \leq i, j \leq N$, where w is a fixed complex number. Let $C = AB$. Give a general formula for $c_{i,j}$ that is valid for any (i, j) with $1 \leq i, j \leq N$.

◇

Exercise 11.2.5.

- (a) Let $z = \text{cis}(\pi/4)$, and let the entries of A and B be given by $a_{i,j} = z^{ij}$ and $b_{i,j} = z^{-ij}$ for $1 \leq i, j \leq 8$. Let $C = AB$. Compute $c_{4,4}$ and $c_{3,5}$.
- (b) Let $z = \text{cis}(2\pi/N)$, and let the entries of A and B be given by $a_{i,j} = z^{ij}$ and $b_{i,j} = z^{-ij}$ for $1 \leq i, j \leq N$. Let $C = AB$. Give a general formula for $c_{k,k}$ which is valid for all k with $1 \leq k \leq N$.
- (c) Let $z = \text{cis}(2\pi/N)$, and let the entries of A and B be given by $a_{i,j} = z^{ij}$ and $b_{i,j} = z^{-ij}$ for $1 \leq i, j \leq N$. Let $C = AB$. Give a general formula for $c_{k+1,k}$ which is valid for all k with $1 \leq k \leq N - 1$.

◇

Exercise 11.2.6. Given three matrices A, B, C with sizes $m \times n, n \times p, p \times q$ respectively.

- (a) Let $D = BC$. Write a formula for the entries $d_{i,j}$ of D in terms of the entries of B and C ($b_{i,k}$ and $c_{k,j}$, respectively).

- (b) Let $G = AD$. Write a formula for the entries $g_{\ell,j}$ of G in terms of the entries of A , B and C .
- (c) Let $H = (AB)$, and let $M = HC$. Write a formula for the entries $m_{\ell,j}$ of M in terms of the entries of A , B and C .
- (d) Using parts (b) and (c), show that matrix multiplication is *associative*.
(*Hint*)

◇

11.3 The identity matrix and the Kronecker delta

The identity matrix I often comes up when working with matrices. You may remember that an identity matrix has 1's on its diagonal and 0's everywhere else:

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{bmatrix}.$$

Notice that the (i, j) entry lies on the diagonal if and only if its row index (i) is equal to its column index (j). This pattern is expressed in summation notation by the so-called **Kronecker delta**.² The Kronecker delta is written as $\delta_{i,j}$ and takes the following values:

$$\delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

By comparison with our description of the identity matrix, we may see that the i, j entry of the identity matrix is equal to $\delta_{i,j}$. We may denote the

²After Leopold Kronecker (1823-1891), a prominent German mathematician who made many contributions to abstract algebra and number theory. Outside of those areas, he is most famous for his strong opposition to the theory of transfinite numbers first proposed by Georg Cantor (1845-1918). Most (but not all) mathematicians today would say that Cantor was right and Kronecker was wrong. This is a fascinating research topic if you're interested in the history of mathematics.

(i, j) entry of I as $[I]_{i,j}$), so that:

$$[I]_{i,j} = \delta_{ij}.$$

Exercise 11.3.1.

(a) We know that if a matrix B is the inverse of the $n \times n$ matrix A then we have the equations: $BA = I$ and $AB = I$. Rewrite these matrix equations in summation notation, making use of the Kronecker delta δ_{ij} (As above, denote the (i, j) entries of A and B as $a_{i,j}$ and $b_{i,j}$ respectively. You will need to choose your indices in order to make the product work out correctly.)

(b) What matrix equation corresponds to the following system of equations in summation notation: $\sum_{k=1}^n \delta_{ik} \delta_{kj} = \delta_{ij}$.

◇

It is possible to use the Kronecker delta to define matrices besides the identity matrix. For example, consider the 4×4 matrix A with entries $a_{i,j}$ defined by:

$$a_{i,j} := \delta_{i+1,j}, \quad 1 \leq i, j \leq 4.$$

In this case, the entry is 1 if the column index is one greater than the row index, and 0 otherwise:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}.$$

Exercise 11.3.2. Write out the following matrices:

(a) The matrix C defined by $c_{i,j} := \frac{1}{2}(-\delta_{i,j+1} + \delta_{i,j-1})$ $1 \leq i, j \leq 6$.

(b) The matrix D defined by $d_{i,j} := -2\delta_{i,j} + \delta_{i+1,j} + \delta_{i-1,j}$, $1 \leq i, j \leq 5$.

(c) The matrix U defined by $u_{i,j} := \delta_{i,j-1} + 2\delta_{i,j-2} + 3\delta_{i,j-3}$, $1 \leq i, j \leq 4$.

(d) The matrix X defined by $x_{i,j} := -2\delta_{i,j} + 2\delta_{i,4-j}$ $1 \leq i, j \leq 5$.

◇

For matrices that are expressible in terms of Kronecker deltas, it is possible to find matrix products using summation notation.

Example 11.3.3. Let \mathbf{v} be the 10×1 matrix given by

$$v_{j,1} = j, j = 1 \dots 10.$$

(Note that \mathbf{v} is essentially a column vector.) Let us compute $C\mathbf{v}$, where the matrix C defined by

$$c_{i,j} := \frac{1}{2}(-\delta_{i-1,j} + \delta_{i+1,j}), \quad 1 \leq i, j \leq 10.$$

The summation notation expression for the product is:

$$[C\mathbf{v}]_{ij} = \sum_{k=1}^{10} c_{i,k} v_{k,j}.$$

The first thing to notice is that the second index j must be 1 since \mathbf{v} is a 10×1 matrix. We may also substitute the expressions for $d_{i,k}$ and $v_{k,j}$ and simplify:

$$\begin{aligned} [C\mathbf{v}]_{i1} &= \sum_{k=1}^{10} \frac{1}{2}(-\delta_{i-1,j} + \delta_{i+1,j})k && \text{[Definitions of } c_{i,k} \text{ and } v_{k,1}] \\ &= -\frac{1}{2} \sum_{k=1}^{10} \delta_{i-1,k}k + \frac{1}{2} \sum_{k=1}^{10} \delta_{i+1,k}k && \text{[Summation rules]} \end{aligned}$$

At this point, we need to think about how the δ 's function within these two sums. Consider the first sum, namely:

$$\sum_{k=1}^{10} \delta_{i-1,k}k.$$

For each value of $i = 1, \dots, 10$, this sum will give a different result:

- When $i = 1$, all terms in the sum are 0, so the result is zero.

- When $i = 2$, the only term that contributes is the $k = 1$ term, since $\delta_{1,k} = 0$ unless $k = 1$. So for $i = 2$, the sum gives 1.
- Similarly when $i = 3, \dots, 10$, the only term that contributes is the $k = i - 1$ term, since $\delta_{3,k} = 0$ unless $k = i - 1$. So the sum gives $i - 1$ for $2 \leq i \leq 10$.

We may summarize these findings as follows:

$$\sum_{k=1}^{10} \delta_{i-1,k} k = \begin{cases} 0 & \text{if } i = 1 \\ i - 1 & \text{if } 2 \leq i \leq 10. \end{cases}$$

The second sum may be evaluated similarly: this time, $i = 10$ is the exceptional case:

$$\sum_{k=1}^{10} \delta_{i+1,k} k = \begin{cases} i + 1 & \text{if } 1 \leq i \leq 9 \\ 0 & \text{if } i = 10. \end{cases}$$

Substituting these expressions into our matrix product formula gives:

$$[C\mathbf{v}]_{i1} = \begin{cases} -\frac{0}{2} + \frac{2}{2} = 1 & \text{if } i = 1 \\ -\frac{i-1}{2} + \frac{i+1}{2} = 1 & \text{if } 2 \leq i \leq 9 \\ -\frac{9}{2} + \frac{0}{2} = -4.5 & \text{if } i = 10. \end{cases}$$

The result is a 10×1 column vector with entries all 1, except for a -4.5 in the 10^{th} entry. \blacklozenge

Let's try another example, this time with two square matrices.

Example 11.3.4. This time we'll compute the entries of the matrix product FV , where the entries f_{ij} of F and v_{ij} of V are given by:

$$f_{ij} := \delta_{i+1,j} - \delta_{i,j}; \quad v_{i,j} := 2^{i+j}, \quad 1 \leq i, j \leq 20.$$

We may begin once again with the matrix product formula:

$$\begin{aligned}
 [FV]_{ij} &= \sum_{k=1}^{20} f_{ik}v_{kj} && \text{[Matrix multiplication formula]} \\
 &= \sum_{k=1}^{20} (\delta_{i+1,k} - \delta_{i,k})2^{k+j} && \text{[Substitution]} \\
 &= \sum_{k=1}^{20} \delta_{i+1,k}2^{k+j} - \delta_{i,k}2^{k+j} && \text{[Substitution]} \\
 &= 2^{i+1+j} - 2^{i+j} && \text{[Select nonzero term in each summation]} \\
 &= 2^{i+j}(2 - 1) && \text{[Exponent rules \& common factor]} \\
 &= 2^{i+j}.
 \end{aligned}$$

The shakiest step in this computation is the one labeled “Select nonzero term in each summation”, and we should double-check to make sure we did it right. When $i = 1, 2, \dots, 19$, then it is always true that $\delta_{i+1,k}$ will be nonzero for a single value of k between 1 and 20, so the sum over k of $\delta_{i+1,k}$ will reduce to a single term. But the case $i = 20$ is different. In this case, $\delta_{20+1,k}$ is equal to 0 for *all* values of k between 1 and 20. So we’ll have to redo the calculation in this case:

$$\begin{aligned}
 \sum_{k=1}^{20} \delta_{20+1,k}2^{k+j} - \delta_{20,k}2^{k+j} &= 0 - 2^{20+j} \\
 &= -2^{20+j}.
 \end{aligned}$$

This brings us to the final result:

$$[FV]_{ij} = \begin{cases} 2^{i+j} & \text{if } 1 \leq i \leq 19 \text{ and } 1 \leq j \leq 20 \\ -2^{20+j} & \text{if } i = 20 \text{ and } 1 \leq j \leq 20. \end{cases}$$

◆

Exercise 11.3.5. Let \mathbf{v} be the 10×1 matrix (a.k.a column vector) given by: $v_{j,1} = j^2$, $j = 1 \dots 10$. Compute $D\mathbf{v}$, where the entries of D are given by $d_{i,j} := -2\delta_{i,j} + \delta_{i+1,j} + \delta_{i-1,j}$, $1 \leq i, j \leq 10$ (The matrix D is an example of a *discrete second derivative matrix*.) ◇

Exercise 11.3.6. Let F and B be the 50×50 matrices defined by $f_{i,j} = \delta_{i+1,j} - \delta_{i,j}$, and $b_{i,j} = \delta_{i,j} - \delta_{i-1,j}$, respectively. (F and B are examples of **forward difference matrix** and **backward difference matrix**, respectively.)

(a) Compute FB . Compute BF .

◇

It turns out that matrices defined using Kronecker deltas play a prominent role in numerical analysis, and in particular the numerical solution of ordinary and partial differential equations.

11.4 Abbreviated matrix notations

In the following discussion, we will be seeing lots of sums involving matrices. This being the case, it's worth our while to try to simplify our notation. In our expression for $C = AB$, we had:

$$c_{i,j} = \sum_{k=1}^n a_{i,k} b_{k,j}$$

Now, notice that the index k runs over all columns of A and all rows of B (recall that matrix multiplication is only defined if the number of columns of A is equal to the number of rows of B). This being the case, we don't really need to mention that k runs from 1 to n —we should simply understand that the index k runs over all possible values. We can therefore convey the same information by simply writing:

$$c_{i,j} = \sum_k a_{i,k} b_{k,j}.$$

This makes more complicated matrix multiplications much simpler. For example, if $D = (AB)C$ where A is $n \times p$, B is $p \times q$, and C is $q \times r$ instead of

$$d_{i,m} = \sum_{j=1}^q \left(\sum_{k=1}^p a_{i,k} b_{k,j} \right) c_{j,m},$$

we may write

$$d_{i,m} = \sum_j \left(\sum_k a_{i,k} b_{k,j} \right) c_{j,m},$$

which further simplifies to

$$d_{i,m} = \sum_{j,k} a_{i,k} b_{k,j} c_{j,m}.$$

We could write either $\sum_{j,k}$ or $\sum_{k,j}$: all possible values of k and j are summed over, so it doesn't matter which order we mention the indices.

There is an even more abbreviated notation that is commonly used in physics, called **Einstein notation** (yes, it's that Einstein!) Notice that in our expression for $c_{i,j}$, the subscript k is *repeated*: that is, it appears as a subscript on $a_{i,k}$ and on $b_{k,j}$. Similarly, in our expression for $d_{i,m}$ the summed subscripts (j and k) are also repeated: both appear as subscripts in two terms. The Einstein rule may be summarized as:

Repeated indices are assumed to be summed.

So for example, the expression

$$d_{i,m} = \sum_j \left(\sum_k a_{i,k} b_{k,j} \right) c_{j,m}$$

in Einstein notation simplifies to:

$$d_{i,m} = a_{i,k} b_{k,j} c_{j,m}.$$

Exercise 11.4.1. Write the following expressions in both abbreviated notations. Note that all indices are summed over the full range of possible values.

- (a) $\sum_{i=1}^m \left(\sum_{j=1}^n \left(\sum_{k=1}^p a_{i,j} b_{j,i} \right) c_{k,k} \right)$
- (b) $\sum_{\ell=1}^L \left(\sum_{m=1}^M \left(\sum_{n=1}^N a_{\ell,m} b_{n,\ell} \right) c_{m,n} \right)$

◇

Exercise 11.4.2. Suppose A, B, C, D are $n \times n$ matrices. Write the complete (unabbreviated) expression corresponding to the following sums in Einstein notation:

(a) $a_{i,j}a_{k,\ell}b_{p,k}b_{i,\ell}$

(b) $d_{i,j}a_{k,\ell}b_{j,k}b_{i,\ell}$

◇

In the following sections we will use the first type of abbreviated notation (not Einstein notation).

11.5 Matrix transpose and matrix inverse

11.5.1 Matrix transpose

Transpose is another operation on matrices that lends itself to summation notation. Recall that the transpose of a matrix changes the rows to columns, so that the first row becomes the first column, the second row becomes the second column, and so on. The transpose of matrix A is denoted as A^T . Using indices and recalling that first index is the row and the second is the column, we can express this as:

$$[A^T]_{i,j} = [A]_{j,i},$$

that is, the (i, j) entry of A^T is equal to the (j, i) entry of A . Since we typically write the (j, i) entry of A as $a_{j,i}$, we may also write:

$$[A^T]_{i,j} = a_{j,i}.$$

Don't get caught up with the particular indices i and j —the important thing is that the indices are switched when you take the transpose. For example, we can also write $[A^T]_{j,i} = a_{i,j}$ or $[A^T]_{k,m} = a_{m,k}$.

Now let's demonstrate the power of our new notation to prove an important property of transpose:

Proposition 11.5.1. If A and B are matrices such that the matrix product is defined, then

$$(AB)^T = B^T A^T.$$

PROOF. We'll prove this by expressing the (i, j) entry of the left-hand side in summation notation, doing some algebraic hocus-pocus, and showing that

it agrees with the (i, j) entry of the right side. First we make things clear by specifying that A has n columns and B has n rows (these dimensions have to agree, or the product is not defined). This gives us

$$[AB]_{i,j} = \sum_k a_{i,k} b_{k,j}.$$

(remember that we decided to use abbreviated notation, so we leave off the summation limits) so the (i, j) entry of the left-hand side is:

$$[(AB)^T]_{i,j} = [AB]_{j,i} = \sum_k a_{j,k} b_{k,i}.$$

At this point we can introduce A and B transpose because the j, k entry of any matrix is the k, j entry of its transpose:

$$\sum_k a_{j,k} b_{k,i} = \sum_k [A^T]_{k,j} [B^T]_{i,k}.$$

Since the terms of A and B are being expressed as a summation, they commute (i.e. order doesn't matter), which allows us to say (using our definition of matrix product):

$$\sum_k [A^T]_{k,j} [B^T]_{i,k} = \sum_k [B^T]_{i,k} [A^T]_{k,j} = [B^T A^T]_{i,j},$$

Voilà, we have the (i, j) entry of the right-hand side, and the proof is complete. \square

Exercise 11.5.2. Give a formula for $(ABC)^T$, and prove your formula using summation notation. \diamond

Exercise 11.5.3. We know that the transpose of a $n \times n$ matrix is a $n \times n$ matrix. So we can consider transpose as a function from $M_n(\mathbb{R})$ to $M_n(\mathbb{R})$, where $M_n(\mathbb{R})$ is the set of $n \times n$ matrices with real-number entries. Prove or disprove the following:

- (a) Transpose defines an invertible function from $M_n(\mathbb{R})$ to $M_n(\mathbb{R})$.
- (b) Transpose preserves addition, i.e. $A^T + B^T = (A+B)^T$ for any matrices $A, B \in M_n(\mathbb{R})$.

- (c) Transpose preserves multiplication, i.e. $A^T \cdot B^T = (A \cdot B)^T$ for any matrices $A, B \in M_n(\mathbb{R})$.

◇

11.5.2 Matrix inverse

We can also express matrix inverse equations in summation notation. Recall that the inverse of a matrix A is a matrix A^{-1} such that $AA^{-1} = I$ and $A^{-1}A = I$.

Exercise 11.5.4.

- (a) Express the equations $AA^{-1} = I$ and $A^{-1}A = I$ using summation notation. You may use the notation $[A]_{i,j}$ and $[A^{-1}]_{i,j}$ to express the entries of the two matrices.
- (b) Suppose that A and B are invertible square matrices of the same size (so that A^{-1} and B^{-1} exist and are also of the same size). Prove that $(AB)^{-1} = B^{-1}A^{-1}$.

◇

11.6 Rotation matrices in 3 dimensions

In three-dimensional space, the *dot product* (or *scalar product*) of two vectors $v := [v_1, v_2, v_3]^T$ and $w := [w_1, w_2, w_3]^T$ is defined as

$$v \cdot w := v_1w_1 + v_2w_2 + v_3w_3 = \sum_j v_jw_j,$$

where we have made use of summation notation to shorten the expression. If we also define the *length* of the vector v (denoted by $\|v\|$) as

$$\|v\| := (v \cdot v)^{1/2},$$

then we may then write the *cosine formula* as

$$\cos(\theta) = \frac{v \cdot w}{\|v\|\|w\|},$$

where θ is the angle between the two vectors v and w . (You may have encountered this formula in physics class or precalculus.)

Any 3×3 matrix A produces a function from three-dimensional space to itself as follows: given any vector $v := [v_1, v_2, v_3]^T$, then the image vector is Av . Using summation notation, we may write:

$$[Av]_i = \sum_j A_{ij}v_j.$$

Now whenever we move an object in space, to get the new locations of various points on the object we have to define a function whose domain and codomain are subsets of \mathbb{R}^3 . If that object is a rigid sphere (like the earth), and the motion is such that the center of the sphere does not change, the motion is called a **rotation**. The function that describes a rotation in \mathbb{R}^3 can actually be expressed as a matrix as described above. But not all 3×3 matrices are rotation matrices. They must have some particular mathematical properties, as described in the next two paragraphs.

First, a rotation matrix R must *preserve lengths and angles*. In other words, if v and w are any two 3-d vectors, then $\|Rv\| = \|v\|$, $\|Rw\| = \|w\|$, and furthermore the angle between Rv and Rw must be the same as the angle between v and w . In view of the cosine formula, this means that the dot product must be preserved: $Rv \cdot Rw = v \cdot w$. In fact, since vector length is the square root of a dot product, all of these conditions will be satisfied as long as

$$Rv \cdot Rw = v \cdot w$$

for any two 3-d vectors v and w .

Another important property of rotation matrices is that they *preserve handedness*. Handedness in three dimensions is defined as follows. Suppose you have three mutually perpendicular unit vectors (u, v, w) in \mathbb{R}^3 (note the order of the three vectors is important). Point your index finger in the direction of u , and simultaneously point your thumb in the direction of w (make sure you're using your right hand!). Now without moving your thumb or index finger try to line up your middle finger with the direction of v . If you are able to do so, then (u, v, w) determines a right-handed coordinate system. If on the other hand your middle finger can only point in the $-v$ direction, then u, v, w determines a left-handed coordinate system. Note that the handedness of a set of vectors depends on how you represent them in space.

Exercise 11.6.1.

- (a) Draw a set of x , y , and z axes so that the vectors $([1, 0, 0]^T, [0, 1, 0]^T, [0, 0, 1]^T)$ form a right-handed system.
- (b) Draw a set of x , y , and z axes so that the vectors $([1, 0, 0]^T, [0, 1, 0]^T, [0, 0, 1]^T)$ form a left-handed system.

◇

When we say that any rotation matrix R preserves handedness, we mean that the handedness of three vectors (u, v, w) is the same as the handedness of the three vectors (Ru, Rv, Rw) . So for example, if you draw your coordinate system so that the unit x , y , and z ($[1, 0, 0]^T, [0, 1, 0]^T, [0, 0, 1]^T$) form a right-handed coordinate system, then the image vectors $\{R[1, 0, 0]^T, R[0, 1, 0]^T, R[0, 0, 1]^T\}$ must also form a right-handed coordinate system.

It turns out that this second condition is mathematically equivalent to the condition that the determinant of R is positive, i.e. $\det(R) \geq 0$. We won't prove this, but we can give a few examples to show that it is reasonable. Consider the 3×3 matrix $-I$, which has determinant equal to -1 . This matrix will map the x , y , and z axes to the $-x$, $-y$, and $-z$ axes respectively. By using the right-hand rule, you may verify that if the x , y , and z axes form a right-handed coordinate system, then the $-x$, $-y$, and $-z$ axes form a left-handed coordinate system.

The following exercise gives some other examples of matrices R with $\det(R) < 0$ which do not preserve handedness.

Exercise 11.6.2.

- (a) Find a matrix R which maps the unit vectors along the x , y , and z axes to the unit vectors along the $-x$, y , and z axes respectively. What's its determinant?
- (b) Show that the function defined in (a) maps a right-handed coordinate system to a left-handed coordinate system.
- (c) Repeat parts (a) and (b) for the case where the x , y , and z axes to the y , x , and z axes respectively.

◇

So let's go back to the first condition for rotation matrices, namely that they preserve inner products: $Rv \cdot Rw = v \cdot w$. Let's rewrite this in coordinate notation. First, note that $[Rv]_k$ and $[Rw]_k$ can be written as $\sum_i r_{ki}v_i$ and $\sum_j r_{kj}w_j$ respectively, where r_{kj} is the (k, j) entry of R . Therefore we have:

$$\begin{aligned} Rv \cdot Rw &= \sum_k [Rv]_k [Rw]_k \\ &= \sum_k \left(\sum_i r_{ki}v_i \right) \left(\sum_j r_{kj}w_j \right) \\ &= \sum_{i,j,k} (r_{ki}v_i)(r_{kj}w_j) \\ &= \sum_{i,j,k} r_{ki}r_{kj}v_iw_j. \end{aligned}$$

Recall our rotation condition: $Rv \cdot Rw = v \cdot w$, which must be true for any two vectors v and w . In summation notation, this becomes:

$$\sum_{i,j,k} r_{ki}r_{kj}v_iw_j = \sum_m v_mw_m$$

Now let's consider different possibilities for v and w . For example we may let $v = w = [1, 0, 0]^T$. This means that $v_i = \delta_{i1}$ and $w_j = \delta_{j1}$, where δ is our old friend the Kronecker delta. Plugging this into our summation notation expression gives:

$$\sum_{i,j,k} r_{ki}r_{kj}\delta_{i1}\delta_{j1} = \sum_m \delta_{m1}\delta_{m1}.$$

Because of the δ 's, when we sum over i, j , and m the only terms that contribute will be $i = j = m = 1$. In summary, we obtain:

$$\sum_k r_{k1}r_{k1} = 1.$$

Using this strategy, we can obtain a whole bunch of identities:

Exercise 11.6.3.

- (a) Repeat the foregoing argument with $v = [1, 0, 0]$ and $w = [0, 1, 0]$ (i.e. plug these two vectors into the rotation condition). Show how this gives you the value of $\sum_{i,j,k} r_{k1}r_{k2}$.

- (b) We may generalize the argument in (a) by choosing v and w to be all different possible combinations of the different coordinate vectors $\{[1, 0, 0], [0, 1, 0], [0, 0, 1]\}$. To do this, you may express v as $v_k = \delta_{ki}$ and w as $w_k = \delta_{kj}$, where i and j are both from the set $\{1, 2, 3\}$. By using these replacements into the rotation condition, show that if R is a rotation matrix then

$$\sum_k r_{ki} r_{kj} = \delta_{ij}.$$

- (c) Show the converse of (a), namely: given that

$$\sum_k r_{ki} r_{kj} = \delta_{ij},$$

show that

$$\sum_{i,j,k} r_{ki} r_{kj} v_i w_j = \sum_m v_m w_m$$

for all v, w .

- (d) Show that the expression $\sum_k r_{ki} r_{kj} = \delta_{ij}$ can be rewritten in matrix form as:

$$R^T R = I.$$

◇

We summarize these results in a proposition:

Proposition 11.6.4. A 3×3 matrix R is a rotation matrix if and only if $\det(R) > 0$ and $R^T R = I$.

We will pick up on rotation matrices in Section 11.8.2 when we talk about determinants, and again in Section 11.8.5 when we prove Euler's rotation theorem.

11.7 Matrix traces

Another cool application of summation notation with matrices is to prove things about the *trace* of a matrix. The trace only applies to square matrices (equal number of rows and columns) and is the sum of all the entries on the diagonal—that is, the sum of all entries with the same column and row number. In summation notation, the trace of an $n \times n$ matrix as:

$$\operatorname{Tr}(A) = a_{1,1} + a_{2,2} + \dots + a_{n,n} = \sum_i a_{i,i}$$

This time we are using the index i for both the row position and the column position, so its the position of the index that denotes row and column. The formula for the product used two different letters for the indices because they were not always equal, but for trace the row and column number will always be equal, so we only need one letter.

The next exercise covers some basic properties of traces:

Exercise 11.7.1.

- (a) Prove that if A and B are square matrices of the same size, then $\operatorname{Tr}(A + B) = \operatorname{Tr}(A) + \operatorname{Tr}(B)$.
- (b) Prove that if A is a square matrix with real entries and k is a real number, then $\operatorname{Tr}(kA) = k\operatorname{Tr}(A)$.

◇

In the above exercise, we have considered the trace of the sum of two matrices. Now we consider the trace of the *product* of two matrices. To this end, let A and B be a $n \times n$ matrices. So first we have:

$$\operatorname{Tr}(AB) = \sum_i [AB]_{i,i} = \sum_i \left(\sum_k a_{i,k} b_{k,i} \right) = \sum_{i,k} a_{i,k} b_{k,i}.$$

All we've done here is take the matrix product formula, and set the second index of the second matrix entry equal to first index of the first matrix entry. Now to make things interesting, let's find the trace for the reverse order:

$$\operatorname{Tr}(BA) = \sum_i [BA]_{i,i} = \sum_i \left(\sum_k b_{i,k} a_{k,i} \right) = \sum_{i,k} a_{k,i} b_{i,k}.$$

Let's play with this last equation a bit. As we mentioned before, we can change the sum over i, k to a sum over i, k without changing anything. Furthermore, since $b_{i,k}$ and $a_{k,i}$ are numbers, they commute under multiplication:

$$\operatorname{Tr}(BA) = \sum_{i,k} b_{i,k} a_{k,i} = \sum_{k,i} a_{k,i} b_{i,k}.$$

Finally, we rename the indices by changing k to i and i to k . (Remember, it's the positions of the indices that are important, not the letters we call them by!) After renaming, we get:

$$\operatorname{Tr}(BA) = \sum_{i,k} a_{i,k} b_{k,i},$$

which agrees with our original expression for $\operatorname{Tr}(AB)$.

Exercise 11.7.2. In the above proof that $\operatorname{Tr}(AB) = \operatorname{Tr}(BA)$, we assumed that both A and B were square matrices. Show that the formula is still true when A is a $m \times n$ matrix and B is a $n \times m$ matrix. (Notice that AB and BA are both square matrices, so that $\operatorname{Tr}(AB)$ and $\operatorname{Tr}(BA)$ are both well-defined.) \diamond

Exercise 11.7.3. Show that $\operatorname{Tr}(ABC) = \operatorname{Tr}(CAB)$, as long as the dimensions of A, B, C are such that the products are well-defined. (*Hint*) \diamond

Exercise 11.7.4. Show that

$$\operatorname{Tr}(ABCD) = \operatorname{Tr}(DABC) = \operatorname{Tr}(CDAB) = \operatorname{Tr}(BCDA),$$

as long as the matrices have dimensions so that all of these products are defined. Notice that all of these arrangements of the matrices A, B, C, D are *cyclic* rearrangements of each other (i.e. it's as if the A, B, C, D are written on a clock face, and are always read around clockwise) (we will have a lot more to say about cyclic rearrangements (a.k.a cyclic permutations) in Chapter 14.) \diamond

Exercise 11.7.5. In linear algebra, given two $n \times n$ matrices A and B we say that A is *similar* to B if there exists an invertible matrix S such that $B = S^{-1}AS$.

(a) Prove that if A is similar to B , then B is similar to A . (*Hint*)

(b) Prove that if A is similar to B , then $\text{Tr}(A) = \text{Tr}(B)$. (*Hint*)

◇

Exercise 11.7.6. Let A be a $n \times n$ diagonal matrix with positive entries, so that the entries of A are given by: $[A]_{i,j} = a_i \delta_{ij}$ where $a_i > 0, i = 1, \dots, n$. Define the matrix $\log A$ as follows: $[\log A]_{i,j} = \log(a_i) \delta_{ij}$, where \log refers to natural logarithm. Show that:

$$\text{Tr}(\log A) = \log(\det A).$$

(Remember that the determinant of a diagonal matrix is the product of the entries on the diagonal.) This formula is actually quite general, and applies to many non-diagonal matrices as well, as long as $\log A$ is properly defined.

³

◇

11.8 Levi-Civita symbols and applications

11.8.1 Levi-Civita symbols: definitions and examples

When dealing with vectors and matrices in physics, one often finds lurking the Levi-Civita symbol,⁴ which is written as an epsilon (the Greek letter ϵ) with various numbers of subscripts. The possible values it can take are 1, -1, or 0, depending on the values of the subscripts (we refer to these subscripts as “indices”). This might not seem too useful since it can only take three different values, but you will see that it does a great job of simplifying expressions that ordinarily would be much more complicated.

For an epsilon with two indices (written as ϵ_{ij}), each index can be either 1 or 2. The different values that ϵ_{ij} can take are:

$$\epsilon_{ij} = \begin{cases} 1 & \text{if } i = 1, j = 2, \\ -1 & \text{if } i = 2, j = 1, \\ 0 & \text{if } i = j. \end{cases}$$

³In some cases, the formula can be used to estimate the determinants of very large matrices: see <http://arxiv.org/pdf/hep-lat/9707001>.

⁴Levi-Civita actually refers to one person, not two: the Italian mathematician Tullio Levi-Civita, (1873-1941), who worked on mathematical physics (including relativity).

For an epsilon with three indices, each index can be either 1, 2, or 3. The values of ϵ_{ijk} are:

$$\epsilon_{ijk} = \begin{cases} 1 & \text{where } (i, j, k) = (1, 2, 3), (2, 3, 1), \text{ or } (3, 1, 2), \\ -1 & \text{where } (i, j, k) = (2, 1, 3), (1, 3, 2), \text{ or } (3, 2, 1), \\ 0 & \text{where } i = j, i = k, \text{ or } j = k, \text{ i.e., if any index is repeated.} \end{cases}$$

What's the rule behind this definition? The six possible rearrangements of $(1, 2, 3)$ in the definition of ϵ_{ijk} are called *permutations*. We will be studying permutations in detail in Chapter 14—but for now, we may simply think of them as rearrangements of the integers $1, 2, \dots, n$ (in this particular case, we have $n = 3$). The three arrangements $(2, 1, 3)$, $(1, 3, 2)$, and $(3, 2, 1)$ can all be obtained from $(1, 2, 3)$ by a single exchange of two numbers. For example, $(2, 1, 3)$ is obtained from $(1, 2, 3)$ by exchanging $1 \leftrightarrow 2$; and the other two rearrangements exchange $2 \leftrightarrow 3$ and $1 \leftrightarrow 3$ respectively. On the other hand, to get $(2, 3, 1)$ or $(3, 1, 2)$ from $(1, 2, 3)$ requires *two* exchanges. Since the number of exchanges for $(2, 1, 3)$, $(1, 3, 2)$, and $(3, 2, 1)$ is odd, these are called *odd permutations*, while the others (including $(1, 2, 3)$) are called *even permutations*. So the definition of ϵ_{ijk} may be summarized as follows: it's equal to 1 if (i, j, k) is an even permutation, -1 if (i, j, k) is an odd permutation, and 0 if (i, j, k) is not a permutation (i.e. there are repeated indices).

You may wonder, Why this strange definition? We'll see more reasons later, but for now we can relate the definition of ϵ_{ijk} to rotations of the x, y, z axes in 3-dimensional space. Let's call these axes 1, 2, 3 instead of x, y, z . Now, if it is possible to rotate the axes so that 1 moves to 2, 2 moves to 3, and 3 moves to 1: in other words $(1, 2, 3)$ has moved to $(2, 3, 1)$. It's also possible to move $(1, 2, 3)$ to $(3, 1, 2)$. Notice that these two are exactly the even permutations! On the other hand, it is not possible to move $(1, 2, 3)$ to $(1, 3, 2)$: To do so would require turning one of the axes around (this is called a *reflection*). So the sign of ϵ_{ijk} distinguishes rotations from reflections. Besides this geometrical interpretation, we'll have a lot more to say about even and odd permutations in Section 14.6.)

We may simplify the notation somewhat if we define the *sign* of a permutation as follows:

$$\text{sign}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is an even permutation,} \\ -1 & \text{if } \sigma \text{ is an odd permutation.} \end{cases}$$

We may then concisely express the general definition of the *Levi-Civita symbol* with n indices as:

$$\epsilon_{i_1 i_2 i_3 \dots i_n} = \begin{cases} \text{sign}(i_1, i_2, \dots, i_n) & \text{if no indices are repeated,} \\ 0 & \text{if any index is repeated.} \end{cases}$$

The symbol with n indices is sometimes called an n -dimensional Levi-Civita symbol: for instance, ϵ_{ijk} is a 3-dimensional Levi-Civita symbol. The reason for this is that most often they are used with vector spaces that have the same dimension as the number of indices in the symbol. So the Levi-Civita symbol with three indices, ϵ_{ijk} is most useful in three dimensions, as we'll see shortly.

Exercise 11.8.1. Using the general definition of the Levi-Civita symbol, show that:

- (a) $\sum_{i,j} \epsilon_{ij} \delta_{ij} = 0$
- (b) $\epsilon_{i_1 i_2 \dots i_n} \delta_{i_j i_k} = 0$ for any j, k such that $1 \leq j < k \leq n$,
- (c) $\epsilon_{ijk} = \epsilon_{jki} = \epsilon_{kij}$.

◇

In the Set Theory chapter you saw the formula:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

This means that you may count all the elements contained in set A or set B by counting the elements in A and B separately, then subtracting their intersection. You have to subtract the intersection because the overlap between A and B gets counted twice in the separate counts of A and B . (Think of a set diagram, where A and B are represented by intersecting circles.) When we split up summations depending on whether indices are equal or unequal, we have to add and subtract in a similar way. We can prove this using Levi-Civita symbols.

Exercise 11.8.2.

(a) Show that for any values $i, j, k \in \{1, 2, 3\}$, it is always true that

$$1 = |\epsilon_{ijk}| + \delta_{ij} + \delta_{jk} + \delta_{ik} - 2\delta_{ij}\delta_{ik}$$

(*Hint*).

(b) Show that

$$\sum_{i,j,k} a_{i,j,k} = \sum_{i,j,k \text{ all unequal}} a_{i,j,k} + \sum_{i,k} a_{i,i,k} + \sum_{i,j} a_{i,j,j} + \sum_{j,k} a_{k,j,k} - 2 \sum_i a_{i,i,i}.$$

(*Hint*).

◇

11.8.2 Levi-Civita symbols and determinants

Now that we've defined Levi-Civita symbols, we can actually use them for something! The first application we'll look at is determinants. Suppose you have a 2×2 matrix A :

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

(Note that previously we separated multiple subscripts with a comma, e.g. $a_{i,j}$: but from now on we'll leave out the comma (e.g. a_{ij}), which is the way most math books do it.)

Then the determinant is:

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

We can write this using the Levi-Civita symbol as:

$$\det A = \sum_{i,j} \epsilon_{ij} a_{1i} a_{2j}$$

Let's check this by evaluating the double sum. Remember that in this case, both i and j run from 1 to 2

$$\begin{aligned} \det A &= \sum_{i,j} \epsilon_{ij} a_{1i} a_{2j} \\ &= \sum_i \left(\sum_j \epsilon_{ij} a_{1i} a_{2j} \right) \\ &= \sum_i (\epsilon_{i1} a_{1i} a_{21} + \epsilon_{i2} a_{1i} a_{22}) \\ &= \epsilon_{11} a_{11} a_{21} + \epsilon_{12} a_{11} a_{22} + \epsilon_{21} a_{12} a_{21} + \epsilon_{22} a_{12} a_{22} \end{aligned}$$

Looking at the definition, we know that ϵ_{11} and ϵ_{22} equals zero, so the leftmost and rightmost terms go to zero. For the remaining terms we have ϵ_{12} which equals 1, and ϵ_{21} which equals -1. So we're left with:

$$\det A = a_{11} a_{22} - a_{12} a_{21},$$

which is exactly the definition you learned in linear algebra.

The natural generalization to a 3×3 matrix as:

$$\det A = \sum_{i,j,k} \epsilon_{ijk} a_{1i} a_{2j} a_{3k}.$$

Exercise 11.8.3. Show that the above formula using ϵ_{ijk} does agree with the determinant that you obtain from row (or column) expansion. \diamond

Exercise 11.8.4. There is a formula for the determinant of a $n \times n$ matrix in terms of an n -index Levi-Civita symbol. Guess what the formula should be (you don't need to prove it). \diamond

Based on our definition of the Levi-Civita symbol ϵ_{ijk} in terms of the sign of the permutation (i, j, k) , we can also write the formula for a 3×3 determinant as:

$$\det A = \sum_{\text{permutations } \phi} \text{sign}(\phi) \cdot a_{1\phi(1)} a_{2\phi(2)} a_{3\phi(3)}.$$

Exercise 11.8.5. Use this formula to prove that the determinant of any 3×3 square matrix A is equal to the determinant of its transpose. That is,

$$\det A = \det A^T$$

(*Hint*)

◇

An important concept to keep in mind when dealing with these Levi-Civita symbols is what they mean based on when indices are equal or unequal, and how that relates to permutations. To see how this works, let's look at a proof to show that if any two rows in a 3×3 matrix are equal, the determinant is 0. Based on our definition we start out with:

$$\det A = \sum_{i,j,k} \epsilon_{ijk} a_{1i} a_{2j} a_{3k}$$

We want to show what happens when any two rows are equal, so let's do one case where row 1 equals row 2. In that case $a_{2j} = a_{1j}$. That means we can rewrite our determinant as:

$$\det A = \sum_{i,j,k} \epsilon_{ijk} a_{1i} a_{1j} a_{3k}$$

Now the letters i, j, k are just "dummy indices" or placeholders, so we can replace them with any letters we want. So we can replace i with j and vice-versa without changing the value:

$$\det A = \sum_{j,i,k} \epsilon_{jik} a_{1j} a_{1i} a_{3k}$$

Now remember what we discussed earlier, if you interchange two indices (that is, an odd permutation) of ϵ_{ijk} , you get its negative, so $\epsilon_{jik} = -\epsilon_{ijk}$. Furthermore, We can replace $\sum_{j,i,k}$ with $\sum_{i,j,k}$ because the order of summation doesn't matter. This gives us

$$\det A = \sum_{i,j,k} -\epsilon_{ijk} a_{1j} a_{1i} a_{3k},$$

Hey, whaddya know: this is exactly equal to the negative of our original expression for $\det A$! There's only one way that a number can be its own negative—the number *must* be zero. We conclude that if the first row is the same as the second row in a 3×3 matrix, the determinant is always zero.

Exercise 11.8.6.

- (a) We showed that if the first and second row of a 3×3 matrix is the same, the determinant is zero. Now finish the proof that the determinant of a 3×3 matrix is always zero if *any* two rows are the same; that is, prove it for the remaining cases.
- (b) Show that any 3×3 matrix which has two columns equal also has determinant equal to 0.

◇

We can take the notion of equal and unequal indices as step farther by proving that the determinant of a product of two matrices is equal to the product of their determinants. Let's start with a simple 2×2 matrix. If matrices A and B are both 2×2 , we want to prove that $\det(AB) = \det A \det B$. We can write $\det(AB)$ as:

$$\det(AB) = \sum_{x,y} \epsilon_{xy} [AB]_{1x} [AB]_{2y}$$

Based on what we learned on how to represent products in terms of summation symbols, we can expand this as:

$$\begin{aligned} \det(AB) &= \sum_{x,y} \epsilon_{xy} \left[\sum_i a_{1i} b_{ix} \sum_j a_{2j} b_{jy} \right] \\ &= \sum_{x,y} \epsilon_{xy} \left[\sum_{i,j} a_{1i} a_{2j} b_{ix} b_{jy} \right] \\ &= \sum_{i,j} a_{1i} a_{2j} \left[\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy} \right], \end{aligned}$$

where in the last equality we have exchanged the order of summation.

At this point we can now consider the product of two possibilities for our indices, one where $i = j$ and another where $i \neq j$:

$$\det(AB) = \sum_{i=j} (\dots) + \sum_{i \neq j} (\dots).$$

Of the two sums on the right-hand side, the first makes zero contribution:

Exercise 11.8.7. Given that $i = j$, show that $\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy}$ is equal to 0. Use this to show that the first summation in the square brackets makes zero contribution. (**Hint**) ◇

Since we can ignore the case where $i = j$, let us look at the case where $i \neq j$. There are actually two cases: $i = 1, j = 2$ and $i = 2, j = 1$. Notice that:

$$\begin{aligned}\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy} &= \sum_{x,y} \epsilon_{xy} b_{1x} b_{2y} \text{ when } i = 1, j = 2; \\ \sum_{x,y} \epsilon_{xy} b_{ix} b_{jy} &= - \sum_{x,y} \epsilon_{xy} b_{1x} b_{2y} \text{ when } i = 2, j = 1.\end{aligned}$$

These two cases can be summarized as:

$$\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy} = \sum_{x,y} \epsilon_{xy} \epsilon_{ij} b_{1x} b_{2y}.$$

This gives us:

$$\begin{aligned}\sum_{i,j} a_{1i} a_{2j} \left[\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy} \right] &= \sum_{i,j} a_{1i} a_{2j} \left[\sum_{x,y} \epsilon_{xy} \epsilon_{ij} b_{1x} b_{2y} \right] \\ &= \left(\sum_{i,j} \epsilon_{ij} a_{1i} a_{2j} \right) \left(\sum_{x,y} \epsilon_{xy} b_{1x} b_{2y} \right),\end{aligned}$$

where in the second line we have noticed that the terms with x, y in the RHS of the first line can be separated from the terms with i, j . At this point we are just about done, since we may recognize the two terms in this final expression as $\det A$ and $\det B$, respectively. Since the original expression we started with was $\det(AB)$, we have:

$$\det(AB) = \det A \det B.$$

This proof as it stands only works for 2×2 matrices, but it turns out that a similar proof works for $n \times n$ matrices. A key step in the proof was the identity:

$$\sum_{x,y} \epsilon_{xy} b_{ix} b_{jy} = \sum_{x,y} \epsilon_{xy} \epsilon_{ij} b_{1x} b_{2y},$$

which held whenever $i, j \in \{1, 2\}$ and $i \neq j$. A similar equality holds in the 3×3 case (and indeed in the $n \times n$ case).

Exercise 11.8.8.

(a) Show that

$$\sum_{x,y,z} \epsilon_{xyz} b_{ix} b_{jy} b_{kz} = \sum_{x,y,z} \epsilon_{xyz} \epsilon_{ijk} b_{1x} b_{2y} b_{3z},$$

whenever $i, j, k \in \{1, 2, 3\}$. (*Hint*)

(b) Give a complete proof of $\det(AB) = \det A \det B$ for the case where A and B are 3×3 matrices.

◇

We may use some of the facts which we've established in this section to prove some important properties of rotation matrices.

Exercise 11.8.9. Recall from Section 11.6 that a rotation matrix R must satisfy $R^T R = I$ and $\det R \geq 0$.

- (a) Using Exercise 11.8.5 and the determinant product formula $\det A \det B = \det(AB)$, show that $\det R = 1$ and $\det R^T = 1$.
- (b) Since $\det R = 1$ it follows that $R \in SL_3(\mathbb{R})$ and hence R is invertible. Use this fact to show that $R^T = R^{-1}$.

◇

The results of the previous exercise are important, so we'll restate them as a proposition.

Proposition 11.8.10. For any rotation matrix R , $\det R = 1$ and $R^T = R^{-1}$.

11.8.3 Levi-Civita symbols and cross products

You may have seen the formula for the cross product of two vectors in vector calculus, or college physics. Given two three-dimensional vectors $\mathbf{a} = (a_1, a_2, a_3)$ and $\mathbf{b} = (b_1, b_2, b_3)$, the **cross product** of \mathbf{a} and \mathbf{b} can be expressed as (note that the absolute value brackets in the formula indicate that it's a determinant and not a matrix.)

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix},$$

where $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ are the vectors along the $x, y,$ and z directions in \mathbb{R}^3 (sometimes they're written as $\mathbf{i}, \mathbf{j}, \mathbf{k}$ instead).

It may seem strange that the matrix we're taking the determinant of has some entries that are vectors, and some entries that are numbers. But since we can still do addition and scalar multiplication with vectors, we can plug the vectors into the determinant formula and still get a result—which happens to be a vector. (Hey, if it works, don't knock it!)

For example, suppose we have the vectors:

$$\mathbf{a} = [2 \ 2 \ 4] \quad \text{and} \quad \mathbf{b} = [-1 \ 2 \ -3].$$

Then the cross product $\mathbf{a} \times \mathbf{b}$ is given by the determinant:

$$\mathbf{a} \times \mathbf{b} = \begin{vmatrix} \mathbf{e}_1 & \mathbf{e}_2 & \mathbf{e}_3 \\ 2 & 2 & 4 \\ -1 & 2 & -3 \end{vmatrix}.$$

Therefore:

$$\begin{aligned} \mathbf{a} \times \mathbf{b} &= \mathbf{e}_1 \begin{vmatrix} 2 & 4 \\ 2 & -3 \end{vmatrix} - \mathbf{e}_2 \begin{vmatrix} 2 & 4 \\ -1 & -3 \end{vmatrix} + \mathbf{e}_3 \begin{vmatrix} 2 & 2 \\ 1 & 2 \end{vmatrix} \\ &= -14\mathbf{e}_1 + 2\mathbf{e}_2 + 6\mathbf{e}_3. \end{aligned}$$

Or we can write the last line in a more familiar fashion:

$$[-14, 2, 6].$$

So all we have to do to define a cross product using the Levi-Civita symbol is to simply plug these terms into the formula for the 3×3 determinant from earlier:

$$\mathbf{a} \times \mathbf{b} = \det A = \sum_{i=1}^3 \sum_{j=1}^3 \sum_{k=1}^3 \epsilon_{ijk} \mathbf{e}_i a_j b_k.$$

If you compare this formula with our original definition of 3×3 determinant (just before Exercise 11.8.3), you'll see that we have dropped the first index on each term. The reason is that the \mathbf{e} terms will always be on the first row, a on the second, and b on the third.

We can actually shorten this up a little bit more, by rewriting the formula to find the i^{th} component of $\mathbf{a} \times \mathbf{b}$. In other words, we don't want the summation of all three \mathbf{e}_i terms, just one particular \mathbf{e}_i term. That means we remove the summation over i , which leaves us with:

$$(\mathbf{a} \times \mathbf{b})_i = \sum_{j=1}^3 \sum_{k=1}^3 \epsilon_{ijk} a_j b_k.$$

So for example, the first component (intuitively the x component, or as we would say, the \mathbf{e}_1 component) is:

$$(\mathbf{a} \times \mathbf{b})_1 = a_2 b_3 - a_3 b_2.$$

Exercise 11.8.11. Find the formulas for $(\mathbf{a} \times \mathbf{b})_2$ and $(\mathbf{a} \times \mathbf{b})_3$. (There's an easy solution if you apply cyclic permutations to the indices in the formula for $(\mathbf{a} \times \mathbf{b})_1$. \diamond)

Exercise 11.8.12. Use the Levi-Civita symbol to find the cross product of the vectors $\mathbf{a} = [2, -3, 2]$ and $\mathbf{b} = [1, 4, -3]$. \diamond

Exercise 11.8.13. Use the Levi-Civita symbol-based equation for the cross product to show $\mathbf{a} \times \mathbf{b} = -\mathbf{b} \times \mathbf{a}$. \diamond

In the following discussion, we will be writing many multiple sums involving the indices i, j and k , where each of these indices runs from 1 to 3. It is convenient to simplify the notation by representing the multiple sum as a single sum over multiple indices. For instance, with this simplified notation we may rewrite our expression for $\mathbf{a} \times \mathbf{b}$ as

$$\mathbf{a} \times \mathbf{b} = \sum_{i,j,k} \epsilon_{ijk} \mathbf{e}_i a_j b_k,$$

and we may rewrite the expression for $(\mathbf{a} \times \mathbf{b})_i$ as

$$(\mathbf{a} \times \mathbf{b})_i = \sum_{j,k} \epsilon_{ijk} a_j b_k.$$

Note that we do not bother to indicate that the indices i, j, k run from 1 to 3: this is understood by the nature of ϵ_{ijk} .

11.8.4 Proof of the vector BAC-CAB Rule

As another example, suppose we want to prove what is known as the *BAC*–*CAB* rule, which states:

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = \mathbf{b}(\mathbf{a} \cdot \mathbf{c}) - \mathbf{c}(\mathbf{a} \cdot \mathbf{b}).$$

We'll arrive at this formula this by two different routes: the brute-force method or the symmetry method. Let's start with the brute force method.

PROOF.(1) (brute force method) We can rewrite this using Levi-Civita symbols by using our definition of cross product. First we find the cross product of \mathbf{b} and \mathbf{c} :

$$(\mathbf{b} \times \mathbf{c})_i = \sum_{j,k} \epsilon_{ijk} b_j c_k.$$

The tricky part is taking the cross product of that result with \mathbf{a} . Let's use \mathbf{d} to represent $\mathbf{b} \times \mathbf{c}$. Then the first component of \mathbf{d} is:

$$d_1 = (\mathbf{b} \times \mathbf{c})_1 = b_2 c_3 - b_3 c_2.$$

We can find the other components by noting that the indices are cyclic permutations. Recall that ϵ_{123} is equivalent to ϵ_{231} because the cycles (123) and (231) are equivalent. So to go from d_1 to d_2 , we need an equivalent cycle that replaces the 1 in the i position (the first position) with a 2. Now the j position, the second position, would have to be 3, because in this cycle 2 goes to 3, and similarly for the last position it will become a 1. So 1 becomes 2, 2 becomes 3, and 3 becomes 1. Using this replacement we get d_2 :

$$d_2 = (\mathbf{b} \times \mathbf{c})_2 = b_3 c_1 - b_1 c_3.$$

The same strategy gives us d_3 :

$$d_3 = (\mathbf{b} \times \mathbf{c})_3 = b_1 c_2 - b_2 c_1.$$

By substitution (and some algebraic rearranging) we can find $\mathbf{a} \times \mathbf{d}$, which is the same as $\mathbf{a} \times (\mathbf{b} \times \mathbf{c})$:

$$\begin{aligned} (\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_1 &= (\mathbf{a} \times \mathbf{d})_1 = a_2 d_3 - a_3 d_2 = a_2 (b_1 c_2 - b_2 c_1) - a_3 (b_3 c_1 - b_1 c_3) \\ &= b_1 (a_2 c_2 + a_3 c_3) - c_1 (a_2 b_2 + a_3 b_3). \end{aligned}$$

Again, we can use the strategy of cyclically permuting the indices to easily find b_2 and b_3 :

$$\begin{aligned} (\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_2 &= (\mathbf{a} \times \mathbf{d})_2 = a_3 d_1 - a_1 d_3 = a_3 (b_2 c_3 - b_3 c_2) - a_1 (b_1 c_2 - b_2 c_1) \\ &= b_2 (a_3 c_3 + a_1 c_1) - c_2 (a_1 b_1 + a_3 b_3), \end{aligned}$$

$$\begin{aligned}(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_3 &= (\mathbf{a} \times \mathbf{d})_3 = a_1 d_2 - a_2 d_1 = a_1 (b_3 c_1 - b_1 c_3) - a_2 (b_2 c_3 - b_3 c_2) \\ &= b_3 (a_1 c_1 + a_2 c_2) - c_3 (a_1 b_1 + a_2 b_2).\end{aligned}$$

Recall the definition of dot product in three dimensions:

$$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + a_2 b_2 + a_3 b_3.$$

Look closely at the first component of our resulting vector:

$$(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_1 = b_1 (a_2 c_2 + a_3 c_3) - c_1 (a_2 b_2 + a_3 b_3).$$

The right hand side is the difference of two terms: $b_1 (a_2 c_2 + a_3 c_3)$ and $c_1 (a_2 b_2 + a_3 b_3)$. The first term can be seen as b_1 times something that is “almost” a dot product: it’s just missing the term $a_1 c_1$. Similarly, the second term is c_1 times an “almost” dot product that’s just missing a $a_1 b_1$. What are we going to do about the missing terms? Why, just add them in! In fact, we can simply add and subtract $a_1 b_1 c_1$ and rearrange to get:

$$\begin{aligned}b_1 (a_2 c_2 + a_3 c_3) - c_1 (a_2 b_2 + a_3 b_3) &= b_1 (a_2 c_2 + a_3 c_3) - c_1 (a_2 b_2 + a_3 b_3) + a_1 b_1 c_1 - a_1 b_1 c_1 \\ &= (b_1 (a_2 c_2 + a_3 c_3) + a_1 b_1 c_1) - (c_1 (a_2 b_2 + a_3 b_3) + a_1 b_1 c_1) \\ &= b_1 (a_2 c_2 + a_3 c_3 + a_1 c_1) - c_1 (a_2 b_2 + a_3 b_3 + a_1 b_1) \\ &= b_1 (\mathbf{a} \cdot \mathbf{c}) - c_1 (\mathbf{a} \cdot \mathbf{b}).\end{aligned}$$

It’s magic! So we have shown

$$(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_1 = b_1 (\mathbf{a} \cdot \mathbf{c}) - c_1 (\mathbf{a} \cdot \mathbf{b})$$

The same steps can be used to justify adding missing terms in the other two components as well:

$$(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_2 = b_2 (\mathbf{a} \cdot \mathbf{c}) - c_2 (\mathbf{a} \cdot \mathbf{b}).$$

$$(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_3 = b_3 (\mathbf{a} \cdot \mathbf{c}) - c_3 (\mathbf{a} \cdot \mathbf{b}).$$

Since we have all three components of the vectors represented and multiplied by the same thing we can shorten this to:

$$\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = \mathbf{b} (\mathbf{a} \cdot \mathbf{c}) - \mathbf{c} (\mathbf{a} \cdot \mathbf{b}).$$

Done! □

The other way of proving the BAC-CAB rule requires a bit more finesse than our previous brute force approach. This time around we are going

make more use of the symmetries of ϵ , so that we do not have to write out every single term.

PROOF.(2) (*Symmetry method*) First let us write the BAC-CAB rule in a way that allows us to more easily ask what happens for every possible value our indices can take, so that we may organize them and get rid of any zero terms.

We begin by writing the i th component of $\mathbf{a} \times (\mathbf{b} \times \mathbf{c})$ using Levi-Civita symbols as

$$\begin{aligned} (\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_i &= \sum_{j,k} \left[\epsilon_{ijk} a_j \left(\sum_{m,n} \epsilon_{kmn} b_m c_n \right) \right] \\ &= \sum_{j,k,m,n} [\epsilon_{ijk} a_j (\epsilon_{kmn} b_m c_n)]. \end{aligned}$$

By separating out the sum over k , we can rewrite this as:

$$(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_i = \sum_{j,m,n} \left[\sum_k \epsilon_{ijk} \epsilon_{kmn} \right] a_j b_m c_n.$$

Let's define the quantity inside the [...] as S_{ijmn} :

$$S_{ijmn} := \sum_k \epsilon_{ijk} \epsilon_{kmn}.$$

Then we will be able to simplify our expression for $(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_i$ if we can find a simpler expression for S_{ijmn} . This quantity will have a different value for each choice of i, j, m, n .

Let's focus on the indices i and j . First, if $i = j$ then $\epsilon_{ijk} = \epsilon_{iik} = 0$, so $S_{iimn} = 0$. On the other hand, if $i \neq j$, there is only one value of k that makes ϵ_{ijk} nonzero (because we must have $k \neq i, j$). We must also have $m, n \neq k$ in order for $\epsilon_{kmn} \neq 0$. It follows that there are two possibilities for which $S_{ijmn} \neq 0$:

(A) $i \neq j$, $m = i$ and $n = j$;

(B) $i \neq j$, $m = j$ and $n = i$.

In case (A) we have:

$$S_{ijjj} = \left[\sum_k \epsilon_{ijk} \epsilon_{kij} \right] = \left[\sum_k \epsilon_{ijk}^2 \right] = 1.$$

In case (B) we have:

$$S_{ijji} = \left[\sum_k \epsilon_{ijk} \epsilon_{kji} \right] = \left[\sum_k -[\epsilon_{ijk}^2] \right] = -1.$$

In summary we have:

$$\begin{aligned} S_{ijmn} &= 1 \text{ if } m = i, n = j, \text{ and } i \neq j; \\ S_{ijmn} &= -1 \text{ if } n = i, m = j, \text{ and } i \neq j; \\ S_{ijmn} &= 0 \text{ otherwise.} \end{aligned}$$

Let's plug this back into our expression for $(\mathbf{a} \times (\mathbf{b} \times \mathbf{c}))_i$. We can then separate the terms where $m = i, n = j$ from the terms where $n = i, m = j$. Notice that there is no longer a sum over 3 indices but only one index, since m and n are determined by i and j :

$$\underbrace{\sum_{j, j \neq i} a_j b_i c_j}_{\text{(terms for } m = i, n = j)}} - \underbrace{\sum_{j, j \neq i} a_j b_j c_i}_{\text{(terms for } m = j, n = i)}}$$

Now if we add $a_i b_i c_i$ to the first set of terms, and add $-a_i b_i c_i$ to the second set of terms, then the overall sum doesn't change but the two expressions simplify:

$$\sum_j a_j b_i c_j - \sum_j a_j b_j c_i$$

This is the same as:

$$b_i(\mathbf{a} \cdot \mathbf{c}) - c_i(\mathbf{a} \cdot \mathbf{b}),$$

which is the $BAC - CAB$ rule. \square

In this case the brute force method wasn't much harder than the symmetry method, but for more complicated expressions it is far easier to use the symmetries of ϵ to prove a statement rather than do it term by term.

The symmetry method gives an added windfall, namely a general identity that will prove useful later:

Exercise 11.8.14. Using some facts from the discussion above, show that $S_{ijmn} := \sum_k \epsilon_{ijk} \epsilon_{kmn}$ can also be written in terms of Kronecker deltas as follows:

$$S_{ijmn} = \delta_{im} \delta_{jn} - \delta_{in} \delta_{jm}.$$

◇

11.8.5 Proof of Euler's Rotation Theorem

In Section 23.2.6 we prove Euler's formula for regular polyhedra. Our proof depends on the following proposition:

Proposition 11.8.15. (*Euler's Rotation Theorem*): Any rotation (besides the identity) in three dimensions has exactly one axis which is fixed by the rotation.

In this section, we'll prove this beautiful theorem! (*Note* the proof requires familiarity with properties of eigenvalues and determinants, which is a topic that is covered in most undergraduate Linear Algebra classes.)

First, we need to establish a general identity involving three-dimensional Levi-Civita symbols.

Proposition 11.8.16. Given any 3×3 matrix A , then

$$\sum_{j,k,\ell} \epsilon_{jkl} a_{ij} a_{k\ell} = \sum_{j,k,\ell} \epsilon_{jkl} a_{ji} a_{k\ell}.$$

(Observe the minute difference between the two sides: there's an a_{ij} on the left-hand side which becomes an a_{ji} on the right. Minute differences matter!)

PROOF. Let us consider the case $i = 1$:

$$\sum_{j,k,\ell} \epsilon_{jkl} a_{1j} a_{k\ell} = \sum_{j,k,\ell} \epsilon_{jkl} a_{j1} a_{k\ell}.$$

and we'll leave the cases $i = 2, 3$ as exercises.

On both right and left sides there are terms with $j = 1$, $j = 2$, and $j = 3$. We'll consider these cases one by one.

- $j = 1$: these terms are equal on both sides, since in this case $a_{1j} = a_{j1} = a_{11}$.
- $j = 2$: in view of the ϵ_{jkl} on both sides, since $j = 2$ the only nonzero terms are $k = 3, \ell = 1$ or $k = 1, \ell = 3$. On the left-hand side this gives $a_{12}a_{31} - a_{12}a_{13}$, while on the right-hand side we get $a_{21}a_{31} - a_{21}a_{13}$.
- $j = 3$: once again, in view of the ϵ_{jkl} on both sides, since $j = 3$ the only nonzero terms are $k = 1, \ell = 2$ or $k = 2, \ell = 1$. On the left-hand side this gives $a_{13}a_{12} - a_{13}a_{21}$, while on the right-hand side we get $a_{31}a_{12} - a_{31}a_{21}$.

Adding all left-hand side terms gives

$$a_{12}a_{31} - a_{12}a_{13} + a_{13}a_{12} - a_{13}a_{21} = a_{12}a_{31} - a_{13}a_{21},$$

while adding all right-hand side terms gives

$$a_{21}a_{31} - a_{21}a_{13} + a_{31}a_{12} - a_{31}a_{21} = -a_{21}a_{13} + a_{31}a_{12}.$$

Miraculously, these turn out to be equal.

Exercise 11.8.17. Complete the proof of Proposition 11.8.16 by showing equality for the cases $i = 2, 3$. \diamond

□

No doubt this formula seems entirely unmotivated and somewhat useless (although you have to admit it's kind of cute.) However, it becomes incredibly useful when we apply it to rotation matrices. To this end, suppose R is a rotation matrix whose (j, k) entry is denoted by r_{jk} . Then the equality in Proposition 11.8.16 applied to matrix R becomes:

$$\sum_{j,k,\ell} \epsilon_{jkl} r_{ij} r_{k\ell} = \sum_{j,k,\ell} \epsilon_{jkl} r_{ji} r_{k\ell},$$

which implies (by rearranging terms)

$$\sum_j r_{ij} \left(\sum_{k,\ell} \epsilon_{jkl} r_{k\ell} \right) = \sum_j r_{ji} \left(\sum_{k,\ell} \epsilon_{jkl} r_{k\ell} \right).$$

The expressions in parentheses on the left and right are identical. So let's define:

$$z_j := \sum_{k,\ell} \epsilon_{jkl} r_{k\ell},$$

and we can replace the parenthetical expressions in our equality by z_j :

$$\sum_j r_{ij}z_j = \sum_j r_{ji}z_j.$$

Rewriting this in matrix notation gives $Rz = R^T z$. Using the fact that $R^T = R^{-1}$ (see Proposition 11.8.10) and a series of algebraic manipulations, we find:

$$\begin{aligned} Rz = R^{-1}z &\Rightarrow Rz - R^{-1}z = 0 \\ &\Rightarrow R^2z - Iz = 0 \\ &\Rightarrow (R + I)(R - I)z = 0. \end{aligned}$$

Now, there are two cases to consider:

- In the case where $(R - I)z \neq 0$, then it must be true that $y := (R - I)z$ is a nonzero vector which satisfies $(R + I)y = 0$. This implies that y is an eigenvector of R with eigenvalue -1 . Now since R is 3×3 , it must have 3 eigenvalues in total. Let λ_1 and λ_2 be the 2 remaining eigenvalues. We know from linear algebra that the product of the eigenvalues is equal to the determinant of R , which is equal to 1 by Proposition 11.8.10. This implies that $-1 \cdot \lambda_1 \cdot \lambda_2 = 1$ or $\lambda_1 \cdot \lambda_2 = -1$. Now, the λ 's could be complex, or they could be real. If complex, then they must be complex conjugates of each other (since R is a real matrix), but then their product would be positive (why is this?). Since their product is negative, this is not possible.

We may conclude that the λ 's are real. Now let w be an eigenvector for the eigenvalue λ_1 . Then $Rw = \lambda_1 w$, so that $\|Rw\| = |\lambda_1| \|w\|$. But we know from the properties of rotations (see Section 11.6 that $\|Rw\| = \|w\|$). This implies $|\lambda_1| = 1$. The same argument shows $|\lambda_2| = 1$.

So what've we got? We know that λ_1 and λ_2 are real. We also know that $|\lambda_1| = |\lambda_2| = 1$, so each λ is either $+1$ or -1 . Finally, we know that $\lambda_1 \cdot \lambda_2 = -1$. This means that one of the λ 's must be -1 , and one must be 1 . Since the remaining eigenvalue is -1 , It follows that there is a unique eigenvector with eigenvalue 1 , which is the unique fixed axis of the rotation.

- In the case where $(R - I)z = 0$, then the vector z is fixed by the rotation R . But is it the only fixed vector? We'll show that if there

is another fixed vector, then R must be the identity. Suppose that there's another vector y which is not parallel to z and is also fixed by the rotation, so that $Ry = y$. Since $R^T = R^{-1}$, we may multiply both sides by R^T and obtain $y = R^T y$, or

$$y_j = \sum_m r_{mj} y_m.$$

By the same token, we have $z = R^T z$, or

$$z_k = \sum_n r_{nk} z_n.$$

Consider now the vector w defined by:

$$w_i := \sum_{j,k} \epsilon_{ijk} y_j z_k.$$

Since y and z are both fixed under the rotation R we may replace y_m and z_k with $\sum_m r_{mj} y_m$ and $\sum_n r_{nk} z_n$ respectively, so that:

$$w_i := \sum_{j,k,m,n} \epsilon_{ijk} (r_{mj} y_m) (r_{nk} z_n) = \sum_{j,k,m,n} \epsilon_{ijk} r_{mj} r_{nk} y_m z_n.$$

Now we may compute Rw using summation notation as:

$$\begin{aligned} [Rw]_\ell &= \sum_i r_{\ell i} w_i \\ &= \sum_{i,j,k,m,n} \epsilon_{ijk} r_{\ell i} r_{mj} r_{nk} y_m z_n \\ &= \sum_{m,n} \left(\sum_{i,j,k} \epsilon_{ijk} r_{\ell i} r_{mj} r_{nk} \right) y_m z_n. \end{aligned}$$

It looks like we're venturing deeper and deeper into mathematical muck. But lo! The expression in parentheses is something that we've seen before, in Exercise 11.8.8:

$$\sum_{i,j,k} \epsilon_{ijk} r_{\ell i} r_{mj} r_{nk} = \sum_{i,j,k} \epsilon_{lmn} \epsilon_{ijk} r_{1i} r_{2j} r_{3k},$$

and we may further simplify using other facts we've picked up here and there:

$$\begin{aligned}\sum_{i,j,k} \epsilon_{lmn} \epsilon_{ijk} r_{1i} r_{2j} r_{3k} &= \epsilon_{lmn} \sum_{i,j,k} \epsilon_{ijk} r_{1i} r_{2j} r_{3k} \\ &= \epsilon_{lmn} \det R \\ &= \epsilon_{lmn}.\end{aligned}$$

So, breathing a huge sigh of relief, we may replace what's in the parentheses with ϵ_{lmn} and obtain

$$[Rw]_\ell = \sum_{m,n} \epsilon_{lmn} y_m z_n = w_\ell.$$

So we have three vectors fixed by R : z , y , and w . If we can show that these are linearly independent, then *all* vectors must be fixed by R , and R must be the identity.

To show that the vectors are linearly independent, it's enough to show that $\det[w \ y \ z] \neq 0$, where $[w \ y \ z]$ is the 3×3 matrix with columns w, y, z . We know that the transpose has the same determinant, so we may find the determinant using the Levi-Civita formula as:

$$\begin{aligned}\det[w \ y \ z] &= \det[w \ y \ z]^T \\ &= \sum_{i,j,k} \epsilon_{ijk} w_i y_j z_k \\ &= \sum_{i,j,k} \epsilon_{ijk} \left(\sum_{m,n} \epsilon_{imn} y_m z_n \right) y_j z_k \\ &= \sum_{i,j,k,m,n} \epsilon_{ijk} \epsilon_{imn} y_j z_k y_m z_n \\ &= \sum_{j,k,m,n} \left(\sum_i \epsilon_{ijk} \epsilon_{imn} \right) y_j y_m z_k z_n\end{aligned}$$

(note that in the third line when we substituted in the expression for w_i , we had to change the summation indices from j, k to m, n to avoid conflict with the j, k indices that we were already using for a different summation.) In the final line, we've separated out the summation over i for a reason. Exercise 11.8.14 tells us that:

$$\sum_k \epsilon_{ijk} \epsilon_{kmn} = \delta_{im} \delta_{jn} - \delta_{in} \delta_{jm}.$$

Assuming this is true (you really should try to prove it, if you haven't already), this enables us to evaluate our expression quite nicely.

Exercise 11.8.18. Using the previous identity, show that

$$\begin{aligned} \sum_{j,k,m,n} \left(\sum_i \epsilon_{ijk} \epsilon_{imn} \right) y_j y_m z_k z_n &= (y \cdot y)(z \cdot z) - (y \cdot z)^2 \\ &= \|y\|^2 \|z\|^2 \sin(\theta), \end{aligned}$$

where θ is the angle between the vectors y and z . (Recall the inner product of two vectors $a \cdot b$ is given by $\sum_i a_i b_i$, while $\|a\|^2 = a \cdot a$.) \diamond

On the basis of the previous exercise, we may conclude that w, y, z are linearly independent vectors (and thus a basis of \mathbb{R}^3), so long as y and z are nonzero, nonparallel vectors.

Now let's recap. We showed that in the case where $(R - I)z = 0$, then z gives the direction of a fixed axis. We also showed, that if there is a different fixed axis, then the rotation must be the identity. So as long as R is not the identity, then R must have a unique fixed axis. We're done ... almost.

Exercise 11.8.19. Actually we're not *quite* done. We never showed that the vector z defined by $z_i := \sum_{j,k} \epsilon_{ijk} r_{jk}$ is a nonzero vector. We'll take care of this case in this exercise.

- (a) Show that if $z = 0$, then it must be true that $r_{ij} = r_{ji}$ for all $i, j \in \{1, 2, 3\}$: in other words, R is symmetric.
- (b) Show that if R is a symmetric rotation matrix, then $(R^2 - I)v = 0$ for *any* vector v .

Once we've shown (b), we have that $(R + I)(R - I)v = 0$ and we're back to the two cases that we've proved already. \diamond

Now we're *really* done!

11.9 Hints for “Sigma Notation” and “Applications of Sigma Notation” exercises

Exercise 10.3.9(e): This is a more difficult one. Exchange order of summation. You will need to use a summation formula from the next section. The denominator factors as the difference of squares. Part of the final answer will look like $1 + 1/2 + 1/3 + \dots + 1/19$, which you can evaluate using a spreadsheet or some other method.

Exercise 11.8.8: Both sides are 0 if any of the two indices i, j, k are equal (show this). Then you only need to consider the three possible cases where i, j, k are all unequal.

Exercise 11.8.18(a): You will need to change around the indices in the formula from Exercise 11.8.14. Make the following replacements: $k \rightarrow i, i \rightarrow j, j \rightarrow k$. Then use the fact that $\epsilon_{ijk} = \epsilon_{jki}$ (see Exercise 11.8.1. to obtain

$$\sum_i \epsilon_{ijk} \epsilon_{imn} = \delta_{jm} \delta_{kn} - \delta_{jn} \delta_{km}.$$

You may plug this form into the expression on the left-hand side. You then obtain 2 terms, which you can evaluate separately. Summing over a delta eliminates one of its two indices: for example:

$$\sum_{j,k,m,n} \delta_{jm} \delta_{kn} y_j y_m z_k z_n = \sum_{j,k} y_j y_j z_k z_k,$$

since the only m term that contributes is $m = j$, and the only n term that contributes is $n = k$. From there, it’s a short hop to the expression with inner products.

In order to get the expression with $\sin \theta$, you will need the cosine formula for inner products (see Section 11.6).

Exercise 11.2.6: Write matrices G and H from parts (b) and (c) in terms of A, B , and C .

Exercise 11.7.3: Notice that the product AB is in both terms. So for simplicity you can define $M := AB$, and use a previous result.

Exercise 11.7.5(a) You don’t need summation notation here, just use basic properties of inverses. (b): Use one of the previous exercises.

Exercise 11.8.1: There are two possibilities to consider, $i = j$ and $i \neq j$.

Exercise 11.8.2(a): Hint: Make a table for all possible values of i, j, k .

Exercise 11.8.2(b): Multiply the equation you found in (a) by a_{ijk} and sum over all i, j, k .

Exercise 11.8.5: Notice that $a_{1,\phi(1)}a_{2,\phi(2)}a_{3,\phi(3)}$ is equal to $a_{\phi^{-1}(1),1}a_{\phi^{-1}(2),2}a_{\phi^{-1}(3),3}$, and that $\text{sign}(\phi)$ is equal to $\text{sign}(\phi^{-1})$.

Exercise 11.8.7: Replace ϵ_{xy} with $-\epsilon_{yx}$, and show that the expression is equal to the negative of itself. (Alternatively, you can just verify the two cases: $i = j = 1$ and $i = j = 2$.)

11.10 Study guide for “Sigma Notation” chapter

Section 10.1, Lots of examples

Concepts:

1. Summation notion (sigma notation) – Σ is the symbol used to denote summation it is called sigma
 - (a) Index variable – variable used in the equation that will change and is located beneath the Σ symbol
 - (b) Starting value – located below the Σ and is the value that begins the summation
 - (c) Final value – located above the Σ and is the last value in the summation
 - (d) Formula – located to the right of Σ , which includes the variable, used to calculate the result

Competencies

1. Evaluate expressions given in summation notation. (10.1.2)

Section 10.2, Sigma notation properties

Concepts:

1. Addition and scalar multiplication of sums
2. Changing the summation index without changing the sum (10.3.1)

Key formulas

1. Formulas for addition and scalar multiplication of sums:

$$(a) \sum_{i=a}^b c \cdot d_i = c \cdot \sum_{i=a}^b d_i$$

$$(b) \sum_{i=0}^n (x_i + y_i) = \sum_{i=0}^n x_i + \sum_{i=0}^n y_i$$

$$(c) \sum_{i=0}^n (c \cdot x_i + d \cdot y_i) = c \cdot \sum_{i=0}^n x_i + d \cdot \sum_{i=0}^n y_i$$

Competencies

1. Be able to change the starting value and formula of sigma notations and maintain the same results. (10.3.1)

Section 10.3, Nested sigmas**Concepts:**

1. Nested sigmas – The entire sum of the inside sigma must be calculated for each value of the index of the outside sigma. *Note* that the index of the outer sum may appear in any or all parts of the inner sum.
2. Rearranging the order of summation – exchange the order of the summations and adjust the limits.

Competencies

1. Be able to exchange the order of sums and use other sum manipulation techniques to calculate values of summations. (10.3.6, 10.3.9)

Section 10.4, Common Sums**Concepts:**

1. Common summation formulas
2. Geometric series – sum of non-negative integer powers of a common base

Key formulas

$$1. \sum_{i=1}^k i = \frac{k(k+1)}{2}$$

$$2. \sum_{i=a}^k i = a + (a + 1) + (a + 2) + \cdots + (k - 1) + k = (k + a) * \frac{k - a + 1}{2}$$

where a and k are integers and $a < k$.

3.

$$\sum_{i=0}^{n-1} ar^i = a \frac{1 - r^n}{1 - r}$$

Competencies

1. Be able to write the sum of given integers in sigma notation and give the formula for that sum. (10.4.2)

Section 11.1, Sigma notation in linear algebra

Concepts:

1. Matrix multiplication with sigma notation
2. Kronecker delta
3. Abbreviated matrix notations
4. Matrix transpose
5. Matrix inverse
6. Rotation matrices
7. Matrix traces – the sum of all the entries on the diagonal

Competencies

1. Be able to write the formula for a given entry of a matrix in terms of other matrices. (11.2.6)
2. Understand the relationship between the Kronecker delta and the identity matrix. Also, how to use it to write matrix equations in summation notation. (11.3.1)
3. Be able to write sigma notations in both forms of abbreviated notations. (11.4.1)

4. Be able to expand abbreviated notations into unabbreviated expressions. (11.4.2)
5. Be able to express the equations for an identity matrix using summation notation. (11.5.4)
6. Understand the basic properties of traces. (11.7.1)

Polynomials

In this chapter we'll be looking at polynomials from an algebraic point of view. First we'll review basic polynomial arithmetic that you've seen in high school; then we'll jump off from there and see how far we can generalize. We'll look at polynomial long division, and show that there are many striking resemblances with integer division. Finally, we'll say something about factoring of polynomials.

This chapter is by Jennifer Lazarus, based on preliminary work by David Weathers, Johnny Watts, and Semi Harrison (edited by C.T.). Thanks to Tom Judson for the original chapter source.

12.1 Why study polynomials?

Undoubtedly you've seen polynomials quite a bit in high school math. You've added and multiplied them; you've graphed them; you've factored them; you've found roots. Let's take a moment to remind ourselves why polynomials and their operations are important.

Polynomials are used to express relationships between variables. For example, we may consider the situation of a vehicle that is moving on a straight road. We'll use x to denote the position, and t to denote time. If (for example) the vehicle has an initial displacement of 100 meters, initial velocity equal to 40 m/sec, and constant acceleration -5 m/sec², then we may write the following relationship between position (x) and time (t):

$$x = -\frac{5}{2}t^2 + 40t + 100$$

(the factor of $-\frac{5}{2}$ in the t^2 term comes from calculus). In this equation, we have expressed x as a function of t : in other words, t is the *independent variable*, and x is the *dependent variable*.

Now suppose a second vehicle is moving along the same road in the opposite direction. We'll represent this vehicle's position as y , and suppose that y depends on t as follows:

$$y = t^2 - 30t + 600.$$

If we're interested in the position of the second vehicle relative to the first, then we should take $y - x$, which we can also write as $y + (-1)x$:

$$y + (-1)x = (t^2 - 30t + 600) + (-1)\left(-\frac{5}{2}t^2 + 40t + 100\right).$$

This equation illustrates two operations with polynomials, namely *scalar multiplication* and *polynomial addition*. Naturally we may perform the operations and obtain:

$$y - x = \frac{7}{2}t^2 - 70t + 500.$$

If we are interested in the time(s) at which the two vehicles meet (hopefully without colliding!), then we need to find the solution(s) (also known as the *roots* of $y - x = 0$, or

$$\frac{7}{2}t^2 - 70t + 500 = 0.$$

It is interesting to note that even though the coefficients of this polynomial are rational numbers, in general the solution(s) will not be rational numbers. (In fact, we know from the quadratic formula that in some cases the solutions are not even real numbers!)

Now suppose instead that the two vehicles are moving on two perpendicular roads which cross at $(0, 0)$. In this case, the square of the distance between the two vehicles is given by (using the Pythagorean theorem)

$$\begin{aligned} (\text{Distance between vehicles})^2 &= x^2 + y^2 \\ &= \left(-\frac{5}{2}t^2 + 40t + 100\right)^2 + (t^2 - 30t + 600)^2. \end{aligned}$$

Here we see both polynomial addition and *polynomial multiplication*. Using polynomial arithmetic (which we explain in detail in the next section),

we find:

$$(\text{Distance between vehicles})^2 = \frac{29}{4}t^4 - 260t^3 + 3200t^2 - 28,000t + 370000.$$

If we would like to find the time(s) at which the relative distance is equal to 500, we should solve

$$500^2 = \frac{29}{4}t^4 - 260t^3 + 3200t^2 - 28,000t + 370000,$$

which can be rearranged to give

$$\frac{29}{4}t^4 - 260t^3 + 3200t^2 - 28,000t + 120000 = 0.$$

This equation has two real solutions and two complex solutions. (In Section 12.6.3 we will see that a polynomial of degree four always has at least 1 and at most 4 distinct complex roots.) The real solutions correspond to the two times that the cars are 500 meters apart.

Exercise 12.1.1. Suppose vehicle 1 has an initial position of $x_0 = 150$ m, an initial velocity of $v_0 = 60$ m/sec, and a constant acceleration of $a = -8$ m/sec². Additionally, suppose vehicle 2 has an initial position of $y_0 = 80$ m, an initial velocity of $v_0 = -50$ m/s, and a constant acceleration of $a = 2$ m/sec².

- Express the position of the second vehicle relative to the first, assuming they are moving on the same road in opposite directions. Determine the time(s) at which the vehicles meet.
- Determine the time, $t > 0$, at which the distance between the vehicles is equal to 400 m, if the vehicles are moving on two perpendicular roads which cross at $(0, 0)$. Give an answer that is correct to three decimal places.

◇

The above discussion gives just one example of an application of polynomials to a practical situation. There are myriads of other examples where polynomials describe the behavior of real-world systems, and polynomial operations and equations are used to make useful predictions and estimations.

12.2 Review of polynomial arithmetic

Let's briefly review what you've previously learned about polynomial arithmetic in earlier algebra classes. In this section we'll cover polynomial addition, subtraction, and multiplication. Polynomial division is a bit more complicated, so we'll talk about that later.

In your earlier classes, most likely you considered polynomials with integer, rational, or real coefficients. But everything we do in this chapter also applies to polynomials with complex coefficients. And in fact, there are even more exotic types of polynomials to which the same formulas and results apply. We'll consider these later in the chapter.

We'll begin with an example. Let

$$p(x) = x^3 - 3x + 2 \quad \text{and} \quad q(x) = 5x^3 + 3x^2 - 6x + 5.$$

Then we can add $p(x)$ and $q(x)$ as follows:

$$\begin{aligned} p(x) + q(x) &= (x^3 - 3x + 2) + (5x^3 + 3x^2 - 6x + 5) \\ &= (1 + 5)x^3 + 3x^2 + (-3 - 6)x + (2 + 5) \\ &= 6x^3 + 3x^2 - 9x + 7 \end{aligned}$$

Notice, we first grouped together terms with the same power of x , and then we added the coefficients.

Multiplication of polynomials is a bit more involved, so we'll start with polynomials of single terms (monomials) and work our way up from there. Suppose we have:

$$p(x) = 5x^3 \quad \text{and} \quad q(x) = 3x^2.$$

Then their product is

$$\begin{aligned} p(x)q(x) &= 5x^3 3x^2 \\ &= (5 \cdot 3)x^{(3+2)}, \\ &= 15x^5, \end{aligned}$$

where we combined the coefficients and the exponents (remember your exponent rules!).

Let's extend ourselves a bit and multiply a polynomial of two terms by a monomial:

$$p(x) = 5x^3 + 2x \quad \text{and} \quad q(x) = 3x^2.$$

According to the distributive law, we multiply each term in the first polynomial with the second polynomial:

$$\begin{aligned} p(x)q(x) &= (5x^3 + 2x)3x^2 \\ &= 5x^3 3x^2 + 2x 3x^2 \\ &= (5 \cdot 3)x^{(3+2)} + (2 \cdot 3)x^{(1+2)} \\ &= 15x^5 + 6x^3. \end{aligned}$$

In order to multiply a two term polynomial by another two term polynomial, e.g.

$$p(x) = 5x^3 + 2x \text{ and } q(x) = 3x^2 - 6x,$$

we extend the distributive law even further. Like before, each term in the first polynomial is being multiplied by the second polynomial. Then the product is

$$\begin{aligned} p(x)q(x) &= (5x^3 + 2x)(3x^2 - 6x) \\ &= 5x^3(3x^2 - 6x) + 2x(3x^2 - 6x) \end{aligned}$$

At this point we just have the sum of two terms, each involving a monomials times a two-term polynomial, which we now know can be calculated using the distributive property,

$$\begin{aligned} &= 5x^3(3x^2 - 6x) + 2x(3x^2 - 6x) \\ &= (15x^5 - 30x^4) + (6x^3 - 12x^2) \\ &= 15x^5 - 30x^4 + 6x^3 - 12x^2 \end{aligned}$$

This is just the same result as the FOIL method you learned in high school, but thinking in terms of the distributive property has the advantage of being applicable to polynomials that have more than just two terms each. For instance, with

$$p(x) = 5x^3 + 4x^2 - 2x \text{ and } q(x) = 3x^2 - 6x,$$

we obtain

$$\begin{aligned} p(x)q(x) &= 5x^3(3x^2 - 6x) + 4x^2(3x^2 - 6x) - 2x(3x^2 - 6x) \\ &= (15x^5 - 30x^4) + (12x^4 - 24x^3) + (-6x^3 + 12x^2) \\ &= 15x^5 - 30x^4 + 12x^4 - 24x^3 - 6x^3 + 12x^2 \\ &= 15x^5 + (-30 + 12)x^4 + (-24 - 6)x^3 + 12x^2 \\ &= 15x^5 - 18x^4 - 30x^3 + 12x^2. \end{aligned}$$

Again notice that we are grouping like terms by exponent. Later, when we give a more general way of multiplying polynomials, this method of distribution is what you need to have in mind.

Exercise 12.2.1.

- (a) Let $p(x) = 4x^2 + 7x$ and $q(x) = -2x^2 - 3x + 2$. Using polynomial arithmetic, compute both the sum and the product of $p(x)$ and $q(x)$.
- (b) Let $p(x) = 3x^2 + 8x - 2$ and $q(x) = 2x^2 - 5x + 9$. Using polynomial arithmetic, compute both the sum and the product of $p(x)$ and $q(x)$.

◇

12.3 Polynomial operations in summation notation

In the preceding section, we discussed familiar polynomial operations. In this section we give general formulas for these operations in terms of summation notation. These formulas are important both theoretically and practically: theoretically, because they give us a way to express general polynomial operations in proofs; and practically, because they provide instructions for programming polynomial operations on computers.

So far we have been using polynomials with real (and occasionally complex) coefficients—but keep in mind that the formulas that we obtain will also apply to other types of polynomials as well, as we shall see in Section 12.4.

First we give the summation representation for an arbitrary polynomial:

Definition 12.3.1. A polynomial may be written as

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_Nx^N = \sum_{n=0}^N a_nx^n,$$

Where a_n is the *coefficient* of x^n , $n = 1, 2, \dots, N$. It is possible for $a_n = 0$, in which case we usually omit the corresponding x^n term (for instance, we write $-7 + x^2$ rather than $-7 + 0x + x^2$). When we write a polynomial as a sum in this way we will *assume* that $a_N \neq 0$ (here a_N is called the *leading*

coefficient. Thus the largest power of x that appears in the polynomial is x^N : this largest power is called the **degree** of the polynomial. \triangle

Remark 12.3.2. According to Definition 12.3.1, we write polynomials in ascending order. This differs from Section 12.2, where we wrote polynomials in descending order as is customary in secondary school. Since the operation ‘+’ is commutative, the two ways are equivalent: but we will increasingly use this new way, which turns out to be useful for a number of reasons. \triangle

Example 12.3.3. Express the following polynomials in summation notation:

(a) $p_1(x) = 1 + x + x^2 + x^3$

(b) $p_2(x) = 0 + x + 2x^2 + 3x^3 + 4x^4 + 5x^5 + 6x^6 + 7x^7$

(c) $p_3(x) = 5x + 4x^2 + 3x^3 + 2x^4$

(d) $p_4(x) = x + 4x^2 + 9x^3 + 16x^4 + 25x^5$

(e) $p_5(x) = -3ix^3 + 4x^4 + 5i^5x^5$ (note that here i denotes $\sqrt{-1}$)

(f) $p_6(x) = \sqrt{2} \operatorname{cis}(\pi/3)x^3 + \sqrt{3} \operatorname{cis}(2\pi/3)x^6 - x^9 + 2 \operatorname{cis}(4\pi/3)x^{12} + \sqrt{5} \operatorname{cis}(5\pi/3)x^{15} + \sqrt{6}x^{18}$

(g) $p_7(x) = 0 + \frac{1}{2}x + \frac{2}{3}x^2 + \frac{3}{4}x^3 + \frac{4}{5}x^4$

(h) $p_8(x) = i + (1 + 2i)x + (2 + 3i)x^2 + (3 + 4i)x^3 + (4 + 5i)x^4 + (5 + 6i)x^5 + (6 + 7i)x^6$

Answers:

(a) $p_1(x) = \sum_{j=0}^3 x^j$

(b) $p_2(x) = \sum_{m=0}^7 mx^m$

(c) $p_3(x) = \sum_{k=1}^4 (6 - k)x^k$

(d) $p_4(x) = \sum_{\ell=0}^5 \ell^2 x^\ell$

(e) $p_5(x) = \sum_{n=3}^5 ni^n x^n$

(f) $p_6(x) = \sum_{q=1}^6 \sqrt{q+1} \operatorname{cis}(q\pi/3)x^{3q}$

$$(g) p_7(x) = \sum_{i=0}^5 \frac{ix^i}{i+1}$$

$$(h) p_8(x) = \sum_{a=0}^6 (a + (a+1)i)x^a$$

Note that we don't always begin the sum at 0, depending on the polynomial. Also, the power of x may be a function of the index, as in p_6 .



Exercise 12.3.4. Write down the polynomial that each summation represents.

$$(a) p(x) = \sum_{j=0}^6 (j^2 + 2)x^{3j}$$

$$(b) p(x) = \sum_{r=2}^5 (r+1)i^r x^r$$

$$(c) p(x) = \sum_{s=0}^8 (-1)^s x^{2s}$$



Exercise 12.3.5. Re-express the following polynomials in summation notation, and give the degree of each polynomial.

$$(a) 2 + 0x + 6x^2 + 0x^3 + 10x^4 + 0x^5 + 14x^6 + 0x^7 + 18x^8$$

$$(b) \operatorname{cis}\left(\frac{\pi}{2}\right)x^2 + 0x^3 + \operatorname{cis}(\pi)x^4 + 0x^5 + \operatorname{cis}\left(\frac{3\pi}{2}\right)x^6$$

$$(c) 1 + 2x + 4x^2 + 8x^3 + 16x^4 + 32x^5$$

$$(d) 1 + 4x + 11x^2 + 30x^3 + 85x^4 \text{ (*Hint*)}$$

$$(e) 1 - \frac{1}{3}x + \frac{1}{5}x^2 - \frac{1}{7}x^3 + \frac{1}{9}x^4 - \frac{1}{11}x^5$$



Remark 12.3.6. In cases where there is no apparent pattern in the coefficients, then summation notation may not be beneficial. For example, suppose:

$$p(x) = 7 + 22x^2 + x^3 - 6x^6 + 4x^8 - x^9.$$

Since there's no clear pattern in the coefficients, there's no advantage in writing $p(x)$ in summation notation. \triangle

Although the following definition may seem rather obvious, nonetheless we should state it to be precise.

Definition 12.3.7. Two polynomials are said to be *equal* if and only if their corresponding coefficients are equal. That is, if we let

$$p(x) = \sum_{m=0}^M a_m x^m; \quad q(x) = \sum_{n=0}^N b_n x^n,$$

then $p(x) = q(x)$ if and only if $M = N$ and $a_m = b_m$ for all $0 \leq m \leq M$. \triangle

Now we're ready to express our arithmetical rules in summation notation.

Definition 12.3.8. We define the *sum of two polynomials* as follows. Let

$$p(x) = \sum_{m=0}^M a_m x^m; \quad q(x) = \sum_{n=0}^N b_n x^n,$$

Then the sum of $p(x)$ and $q(x)$ is

$$p(x) + q(x) = \sum_{k=0}^{\max(M,N)} (a_k + b_k) x^k.$$

In this formula, if $M > N$ then it's understood that $b_k = 0$ when $k > N$; and if $N > M$ then it's understood that $a_k = 0$ when $k > M$. \triangle

Notice that we have taken the upper limit of the sum to $\max(M, N)$ in order to make sure to include all nonzero terms from both polynomials.

Now that we have a formula for adding polynomials, the next step is to obtain a formula for multiplying polynomials, using summation notation. To do this, let's repeat the polynomial multiplication procedure we used in Section 12.2, only this time we'll use two general polynomials instead of specific examples. As with addition, we use

$$p(x) = \sum_{m=0}^M a_m x^m; \quad q(x) = \sum_{n=0}^N b_n x^n.$$

In the multiplication example in Section 12.2, we split up the first polynomial, and multiplied each term of the first polynomial by the second polynomial. When applied to $p(x)$ and $q(x)$, this becomes:

$$\begin{aligned} p(x)q(x) &= a_0x^0 \cdot q(x) + a_1x^1 \cdot q(x) + \dots + a_Nx^N \cdot q(x) \\ &= \sum_{m=0}^M a_mx^m \cdot q(x) \\ &= \sum_{m=0}^M a_mx^m \cdot \left(\sum_{n=0}^N b_nx^n \right), \end{aligned}$$

where in the last equation we have replaced $q(x)$ with its expression in summation notation. Now since a_mx^m is constant with respect to n , we may pull a_mx^m inside the sum over n , which gives:

$$p(x)q(x) = \sum_{m=0}^M \sum_{n=0}^N (a_mx^m)b_nx^n = \sum_{m=0}^M \sum_{n=0}^N a_mb_nx^{m+n},$$

where we have used our multiplication rule for monomials: $(a_mx^m)b_nx^n = a_mb_nx^{m+n}$.

Although this expression is correct, it's kind of a hodgepodge. The reason is that not all the terms with the same power of x are grouped together. So let's try to collect terms according to like power of x .

We'll start with x^0 . Since terms have the form $a_mb_nx^{m+n}$, this means we need to find all values of m and n such that $m+n=0$. Since both m and n are nonnegative, the only possibility is $m=0, n=0$, which gives the term $a_0b_0x^0$.

Next let's look at x^1 . In this case we want terms $a_mb_nx^{m+n}$ which have $m+n=1$. There are two: $a_1b_0x^1$ and $a_0b_1x^1$.

If we treat x^2 similarly, we have three terms: $a_2b_0x^2$, $a_1b_1x^2$, and $a_0b_2x^2$. Then x^3 has four terms: $a_3b_0x^3$, $a_2b_1x^3$, $a_1b_2x^3$, and $a_0b_3x^3$. Do you see the pattern? For x^k we will get $k+1$ terms: $a_kb_0x^k$, $a_{k-1}b_1x^k$, \dots , $a_1b_{k-1}x^k$, and $a_0b_kx^k$. Since $+$ is commutative, we may sum these terms together to obtain the coefficient of x^k , which we will denote as c_k :

$$c_k = a_0b_k + a_1b_{k-1} + \dots + a_{k-1}b_1 + a_kb_0 = \sum_{j=0}^k a_jb_{k-j},$$

This is the coefficient of x^k in the summation notation expression for the product. At last we have our general formula:

Definition 12.3.9. The *product of two polynomials* $p(x) = \sum_{m=0}^M a_m x^m$ and $q(x) = \sum_{n=0}^N b_n x^n$ is given by:

$$p(x)q(x) = \sum_{k=0}^{M+N} c_k x^k,$$

where

$$c_k = \sum_{j=0}^k a_j b_{k-j}$$

for each k . △

Let's verify the formula by computing $f(x)$, where:

$$f(x) = (1 + x^2 - 2x^3)(x + 4x^3).$$

$f(x)$ is the product of $p(x)$ and $q(x)$, where:

$$p(x) = 1x^0 + 0x^1 + 1x^2 + (-2)x^3 \quad \text{and} \quad q(x) = 0x^0 + 1x^1 + 0x^2 + 4x^3$$

Both polynomials have degree 3, so the degree of the product is $3+3=6$:

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k x^k = \sum_{k=0}^6 c_k x^k.$$

Now all we have to do is find the values of the seven coefficients c_0, \dots, c_6 , some of which may be zero. Let us start with c_0 :

$$c_0 = \sum_{i=0}^0 a_i b_{0-i} = a_0 b_0 = 0 \cdot 1 = 0.$$

Already we've found a term that is zero. We still need to find six more coefficients—how about we look at the fifth coefficient:

$$c_4 = \sum_{i=0}^4 a_i b_{4-i} = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0.$$

Notice that $a_4 = b_4 = 0$ since $p(x)$ and $q(x)$ both have degree 3, so the first and last terms are both 0. Altogether we have

$$c_4 = 0 + 0 \cdot 4 + 1 \cdot 0 + (-2) \cdot 1 + 0 = -2.$$

Doing the same for the other coefficients gives us:

$$f(x) = 0x^0 + 1x^1 + 0x^2 + 5x^3 + (-2)x^4 + 4x^5 + (-8)x^6$$

Getting rid of the zero terms and dealing with the negatives gives us the simplified version:

$$f(x) = x + 5x^3 - 2x^4 + 4x^5 - 8x^6.$$

Exercise 12.3.10.

Perform the following polynomial multiplications in two ways: first, by following the procedure described in Section 12.2; and second, by using the coefficient formula in Definition 12.3.9 directly. Verify that the two methods agree.

- (a) $(-5 + x)(3x + x^2)$
- (b) $(-\sqrt{3} + x)(2\sqrt{3} + 5x^3)$
- (c) $(7/2 - 3x + 4x^2)(2 + x^3)$
- (d) $(-7x^2 + 4x^3 + 8x^5)(3 - 5x + 10x^2)$

◇

The coefficient formula enables us to compute a single coefficient for a product of polynomials without having to compute the rest of the product. Here are some exercises for practice:

Exercise 12.3.11.

- (a) Give the coefficient of x^{100} in the polynomial $p(x)^2$, where $p(x) = \sum_{n=0}^{100} x^n$.
- (b) Give the coefficient of x^{25} in the polynomial $p(x) \cdot q(x)$, where $p(x) = \sum_{n=0}^{25} nx^n$ and $q(x) = \sum_{m=0}^{25} x^m$.
- (c) Give the coefficient of x^{33} in the polynomial $p(x) \cdot q(x)$, where $p(x) = \sum_{n=1}^{33} \frac{x^n}{n}$ and $q(x) = \sum_{n=0}^{32} (33 - n)x^n$.

◇

12.4 More exotic polynomials

So far we've performed algebraic operations on polynomials with integer, rational, real, or complex coefficients. We may identify different sets of polynomials according to the type of coefficient used. For instance we may define:

- $\mathbb{Z}[x]$ is the set of polynomials in the variable x with integer coefficients;
- $\mathbb{Q}[x]$ is the set of polynomials in the variable x with rational coefficients;
- $\mathbb{R}[x]$ is the set of polynomials in the variable x with real coefficients;
- $\mathbb{C}[x]$ is the set of polynomials in the variable x with complex coefficients.

We refer to $\mathbb{Z}[x]$ as “the set of polynomials over \mathbb{Z} ”, $\mathbb{Q}[x]$ as “the set of polynomials over \mathbb{Q} ”, and so on.

However, we can generalize polynomials far beyond these cases. In this section, we introduce several new types of polynomials and define arithmetic operations (addition and multiplication) on these new types. In order to do this, we'll make use of the summation notation formulas in the last section (reproduced here for convenience):

$$p(x) = \sum_{m=0}^M a_m x^m; \quad q(x) = \sum_{n=0}^N b_n x^n,$$

$$p(x) + q(x) = \sum_{k=0}^{\max(M,N)} (a_k + b_k) x^k,$$

$$p(x)q(x) = \sum_{k=0}^{M+N} c_k x^k, \text{ where } c_k = \sum_{j=0}^k a_j b_{k-j}.$$

We'll just need to replace conventional addition and multiplication (using real or complex numbers) with other addition and multiplication operations that are appropriate to the coefficients that we are working with.

Polynomials over \mathbb{Z}_n

Consider first $\mathbb{Z}_n[x]$, where \mathbb{Z}_n denotes the integers mod n . For example, two polynomials $p(x)$ and $q(x)$ in $\mathbb{Z}_4[x]$ are

$$\begin{aligned} p(x) &= 1 + 3x + x^3 \\ q(x) &= 2 + 2x + 3x^2 + 3x^3. \end{aligned}$$

In this case, we should consider the variable x as representing an unknown element in \mathbb{Z}_4 , so the '+' operation in these expressions should be interpreted as addition in \mathbb{Z}_4 . All operations on coefficients will also make use of addition mod \mathbb{Z}_4 . So for polynomial addition we may use the above formulas for polynomial addition only use + in \mathbb{Z}_4 instead of ordinary +. For example, using $p(x)$ and $q(x)$ defined above we have:

$$\begin{aligned} p(x) + q(x) &= (1 + 2) + (3 + 2)x + (0 + 3)x^2 + (1 + 3)x^3 \\ &= 3 + x + 3x^2. \end{aligned}$$

To multiply, we can use the same strategy, namely, use the previous formula for polynomial multiplication, but replace both + and \cdot with their counterparts in \mathbb{Z}_4 . Alternatively, we may use the distributive law as in Section 12.2, with the understanding that we are distributing modular multiplication over modular addition. As before, we group together all terms with like powers of x and use modular arithmetic to combine these terms into a single term. The result is:

$$\begin{aligned} p(x)q(x) &= 1 \cdot 2 + (3 \cdot 2 + 1 \cdot 2)x + (3 \cdot 2 + 1 \cdot 3)x^2 + \\ &\quad (1 \cdot 2 + 3 \cdot 3 + 1 \cdot 3)x^3 + (1 \cdot 2 + 3 \cdot 3)x^4 + \\ &\quad (1 \cdot 3)x^5 + (1 \cdot 3)x^6 \\ &= 2 + 1x^2 + 2x^3 + 3x^4 + 3x^5 + 3x^6. \end{aligned}$$

Exercise 12.4.1. Compute the sum and product of $p(x)$ and $q(x)$.

- (a) $p(x) = 1 + x + 2x^2$, $q(x) = 3x^2 + x^3$, where both polynomials are in $\mathbb{Z}_5[x]$.
 (b) $p(x) = 1 + 4x^2 + 3x^3 + 2x^4$, $q(x) = 5 + 2x^2 + x^3$, where both polynomials are in $\mathbb{Z}_6[x]$.

◇

It turns out that $\mathbb{Z}_2[x]$ in particular is of great practical use (in polynomial codes), so we include some exercises to get you warmed up for what's coming.

Exercise 12.4.2. Compute the sum and product of $p(x)$ and $q(x)$, where both polynomials are in $\mathbb{Z}_2[x]$.

(a) $p(x) = 1 + x + x^2$, $q(x) = 1 + x + x^2 + x^3$

(b) $p(x) = 1 + x^2 + x^4$, $q(x) = x^2 + x^3 + x^4$.

(c) $p(x) = 1 + x + x^2 + x^3 + x^4$, $q(x) = p(x)$.

◇

Polynomials over $n\mathbb{Z}$

Recall that $n\mathbb{Z}$ consists of all integer multiples of n : for example, $5\mathbb{Z} = \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}$. We may consider the set $n\mathbb{Z}[x]$, the set of all polynomials whose coefficients are all multiples of n . Certainly it is possible to add and multiply these polynomials, because any such polynomial is also in $\mathbb{Z}[x]$. But it is important to note that any sum or product of polynomials in $n\mathbb{Z}[x]$ is also in $n\mathbb{Z}[x]$: in other words, $n\mathbb{Z}[x]$ is *closed* under addition and multiplication.

Exercise 12.4.3.

(a) Suppose that $p(x) = a_2x^2 + a_1x + a_0$ and $q(x) = b_1x + b_0$, and both $p(x)$ and $q(x)$ are elements of $5\mathbb{Z}[x]$. Prove that $p(x) + q(x)$ and $p(x)q(x)$ are also elements of $5\mathbb{Z}[x]$. (**Hint**)

(b) Repeat the proof of (a), except replace $5\mathbb{Z}[x]$ with $n\mathbb{Z}[x]$, where n is an arbitrary positive integer.

(c) Repeat the proof of (b), except use general polynomials $p(x) = \sum_{j=1}^n a_j x^j$ and $q(x) = \sum_{k=1}^m b_k x^k$.

◇

Polynomials over $\mathbb{R}[x]$

Our next example is $\mathbb{R}[x][y]$, which represents polynomials in the variable y whose coefficients are polynomials in a different variable x . For example, the following two polynomials are elements of $\mathbb{R}[x][y]$:

$$\begin{aligned} p(x, y) &= (1 + 3x) + (1 + x^2)y + (5x)y^2 \\ q(x, y) &= (3x) + (2 + 2x)y + (4x^2)y^2. \end{aligned}$$

We may add them as follows:

$$\begin{aligned} p(x, y) + q(x, y) &= ((1 + 3x) + 3x) + ((1 + x^2) + (2 + 2x))y + (5x + 4x^2)y^2 \\ &= (1 + 6x) + (3 + 2x + x^2)y + (5x + 4x^2)y^2. \end{aligned}$$

We will multiply $p(x, y)$ and $q(x, y)$ using the summation formula for coefficients found in Definition 12.3.9.

$$c_0 = \sum_{i=0}^0 a_i b_{0-i} = a_0 b_0 = (1 + 3x) \cdot (3x) = 3x + 9x^2.$$

$$\begin{aligned} c_1 &= \sum_{i=0}^1 a_i b_{0-i} = a_0 b_1 + a_1 b_0 = ((1 + 3x) \cdot (2 + 2x)) + ((1 + x^2) \cdot (3x)) \\ &= (1 + 8x + 6x^2) + (2 + 2x + 2x^2 + 2x^3) \\ &= 3 + 10x + 8x^2 + 2x^3. \end{aligned}$$

$$\begin{aligned} c_2 &= \sum_{i=0}^2 a_i b_{0-i} = a_0 b_2 + a_1 b_1 + a_2 b_0 = ((1 + 3x) \cdot (4x^2)) + (1 + x^2) \cdot (2 + 2x) + ((5x) \cdot (3x)) \\ &= (4x^2 + 12x^3) + (2 + 2x + 2x^2 + 2x^3) + 15x^2 \\ &= 2 + 2x + 21x^2 + 14x^3. \end{aligned}$$

$$\begin{aligned} c_3 &= \sum_{i=0}^3 a_i b_{0-i} = a_1 b_2 + a_2 b_1 = ((1 + x^2) \cdot (4x^2)) + ((5x) \cdot (2 + 2x)) \\ &= (4x^2 + 4x^4) + (10x + 10x^2) \\ &= 10x + 14x^2 + 4x^4. \end{aligned}$$

$$c_4 = \sum_{i=0}^4 a_i b_{0-i} = a_2 b_2 = 5x \cdot 4x^2 = 20x^3.$$

Therefore, we have the following:

$$\begin{aligned} p(x, y)q(x, y) &= c_0 + c_1 y + c_2 y^2 + c_3 y^3 + c_4 y^4 \\ &= (3x + 9x^2) + (3 + 10x + 8x^2 + 2x^3)y + (2 + 2x + 21x^2 + 14x^3)y^2 \\ &\quad + (10x + 14x^2 + 4x^4)y^3 + (20x^3)y^4. \end{aligned}$$

Exercise 12.4.4. Compute the sum and product of $p(x, y)$ and $q(x, y)$ where:

$$\begin{aligned} p(x, y) &= (1 + 8x) + (3 - 2x)y^2 \text{ and} \\ q(x, y) &= (5x + 6x^2)y - (2 + 6x)y^2 \end{aligned}$$

◇

Polynomials over \mathbb{M}_n

Next we consider $\mathbb{M}_n[x]$, the set of polynomials in the variable x with coefficients that are $n \times n$ matrices with real entries. Consider the two polynomials $p(x), q(x) \in \mathbb{M}_2[x]$ given by:

$$\begin{aligned} p(x) &= \begin{bmatrix} -1 & 5 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 4 & 3 \\ 2 & -4 \end{bmatrix} x + \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} x^2 \\ q(x) &= \begin{bmatrix} 4 & 2 \\ -3 & 6 \end{bmatrix} + \begin{bmatrix} 2 & -1 \\ 0 & 9 \end{bmatrix} x + \begin{bmatrix} 9 & -1 \\ 8 & 1 \end{bmatrix} x^2 \end{aligned}$$

We add $p(x)$ and $q(x)$ as follows:

$$\begin{aligned}
 p(x) + q(x) &= \left(\begin{bmatrix} -1 & 5 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 4 & 3 \\ 2 & -4 \end{bmatrix} x + \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} x^2 \right) \\
 &\quad + \left(\begin{bmatrix} 4 & 2 \\ -3 & 6 \end{bmatrix} + \begin{bmatrix} 2 & -1 \\ 0 & 9 \end{bmatrix} x + \begin{bmatrix} 9 & -1 \\ 8 & 1 \end{bmatrix} x^2 \right) \\
 &= \left(\begin{bmatrix} -1 & 5 \\ -2 & 4 \end{bmatrix} + \begin{bmatrix} 4 & 2 \\ -3 & 6 \end{bmatrix} \right) + \left(\begin{bmatrix} 4 & 3 \\ 2 & -4 \end{bmatrix} + \begin{bmatrix} 2 & -1 \\ 0 & 9 \end{bmatrix} \right) x \\
 &\quad + \left(\begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} + \begin{bmatrix} 9 & -1 \\ 8 & 1 \end{bmatrix} \right) x^2 \\
 &= \begin{bmatrix} 3 & 7 \\ -5 & 10 \end{bmatrix} + \begin{bmatrix} 6 & 2 \\ 2 & 5 \end{bmatrix} x + \begin{bmatrix} 8 & -1 \\ 10 & 2 \end{bmatrix} x^2.
 \end{aligned}$$

Again, we will use the summation formula for the coefficients to compute the product of $p(x)$ and $q(x)$.

$$c_0 = \sum_{i=0}^0 a_i b_{0-i} = a_0 b_0 = \begin{bmatrix} -1 & 5 \\ -2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 4 & 2 \\ -3 & 6 \end{bmatrix} = \begin{bmatrix} -19 & 28 \\ -20 & 20 \end{bmatrix}.$$

$$\begin{aligned}
 c_1 &= \sum_{i=0}^1 a_i b_{1-i} = a_0 b_1 + a_1 b_0 = \begin{bmatrix} -1 & 5 \\ -2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ 0 & 9 \end{bmatrix} + \begin{bmatrix} 4 & 3 \\ 2 & -4 \end{bmatrix} \cdot \begin{bmatrix} 4 & 2 \\ -3 & 6 \end{bmatrix} \\
 &= \begin{bmatrix} -2 & 46 \\ -4 & 38 \end{bmatrix} + \begin{bmatrix} 7 & 26 \\ 20 & -20 \end{bmatrix} = \begin{bmatrix} 5 & 72 \\ 16 & 18 \end{bmatrix}.
 \end{aligned}$$

$$\begin{aligned}
 c_2 &= \sum_{i=0}^2 a_i b_{2-i} = a_0 b_2 + a_1 b_1 + a_2 b_0 = \begin{bmatrix} -1 & 5 \\ -2 & 4 \end{bmatrix} \cdot \begin{bmatrix} 9 & -1 \\ 8 & 1 \end{bmatrix} + \begin{bmatrix} 4 & 3 \\ 2 & -4 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ 0 & 9 \end{bmatrix} \\
 &\quad + \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 4 & 2 \\ -3 & 6 \end{bmatrix} \\
 &= \begin{bmatrix} 31 & 6 \\ 14 & 6 \end{bmatrix} + \begin{bmatrix} 8 & 23 \\ 4 & -38 \end{bmatrix} + \begin{bmatrix} -4 & -2 \\ 5 & 10 \end{bmatrix} = \begin{bmatrix} 35 & 27 \\ 23 & -22 \end{bmatrix}.
 \end{aligned}$$

$$\begin{aligned}
 c_3 &= \sum_{i=0}^3 a_i b_{3-i} = a_1 b_2 + a_2 b_1 = \begin{bmatrix} 4 & 3 \\ 2 & -4 \end{bmatrix} \cdot \begin{bmatrix} 9 & -1 \\ 8 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 2 & -1 \\ 0 & 9 \end{bmatrix} \\
 &= \begin{bmatrix} 60 & -1 \\ -14 & -6 \end{bmatrix} + \begin{bmatrix} -2 & 1 \\ 4 & 7 \end{bmatrix} = \begin{bmatrix} 58 & 0 \\ -10 & 1 \end{bmatrix}.
 \end{aligned}$$

$$c_4 = \sum_{i=0}^4 a_i b_{4-i} = a_2 b_2 = \begin{bmatrix} -1 & 0 \\ 2 & 1 \end{bmatrix} \cdot \begin{bmatrix} 9 & -1 \\ 8 & 1 \end{bmatrix} = \begin{bmatrix} -9 & 1 \\ 26 & -1 \end{bmatrix}.$$

Therefore, we have the following:

$$\begin{aligned} p(x)q(x) &= c_0 + c_1x + c_2x^2 + c_3x^3 + c_4x^4 \\ &= \begin{bmatrix} -19 & 28 \\ -20 & 20 \end{bmatrix} + \begin{bmatrix} 5 & 72 \\ 16 & 18 \end{bmatrix}x + \begin{bmatrix} 35 & 27 \\ 23 & -22 \end{bmatrix}x^2 + \begin{bmatrix} 58 & 0 \\ -10 & 1 \end{bmatrix}x^3 + \begin{bmatrix} -9 & 1 \\ 26 & -1 \end{bmatrix}x^4 \end{aligned}$$

Exercise 12.4.5. Compute the sum and product of $p(x)$ and $q(x)$, where:

$$p(x) = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 2 & 4 \end{bmatrix}x + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}x^2$$

$$q(x) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}x^2$$

◇

12.5 Polynomial properties and summation notation

In the past several sections, we have looked at polynomials with different types of coefficients. These different types of polynomials have a lot in common. In this section, we will look more deeply into just what it is that is common to all.

Since we want our discussion to be general, we don't want to restrict ourselves to any particular set of coefficients. Instead, we will denote our polynomials by $R[x]$, where the set of coefficients R can represent \mathbb{R} , \mathbb{C} , \mathbb{Q} , \mathbb{Z} , \mathbb{Z}_n , or \mathbb{M}_n (i.e. $n \times n$ matrices). This means that the results of this section will be valid for many different types of polynomials. The only properties that we require of the set R are the following:

- (I) R has two binary operations, denoted as $+$ and \cdot (i.e. addition and multiplication);

- (II) R is closed under both addition and multiplication;
- (III) Addition in R is commutative;
- (IV) Addition and multiplication are both associative;
- (V) Multiplication distributes over addition: e.g. $a \cdot (b + c) = a \cdot b + a \cdot c$
and $(a + b) \cdot c = a \cdot c + b \cdot c$.

(We will see somewhat later that all of these properties are characteristic of a type of mathematical structure called a “ring”. But for the time being, we may simply recognize them as properties that are common to the number systems that we have been using so far.)

Given that R has addition and multiplication operations, we may define addition and multiplication in $R[x]$ using Definitions 12.3.8 and 12.3.9. Let’s first make sure that the definitions give well-behaved, closed operations in $R[x]$.

Proposition 12.5.1. Given that R satisfies conditions (I)-(V) listed above. Then Definitions 12.3.8 and 12.3.9 produce closed addition and multiplication operations in $R[x]$.

You will prove Proposition 12.5.1 in the following exercise.

Exercise 12.5.2.

- (a) Prove that Definition 12.3.8 gives a closed operation in $R[x]$ by showing that whenever $p(x)$ and $q(x)$ are polynomials in $R[x]$, then $p(x) + q(x)$ is also a polynomial in $R[x]$.
- (b) Prove that Definition 12.3.9 gives a closed multiplication operation in $R[x]$ by showing that whenever $p(x)$ and $q(x)$ are polynomials in $R[x]$, then $p(x)q(x)$ is also in $R[x]$.

◇

Now that we’ve shown that the operations of addition and multiplication in $R[x]$ are properly defined, we may verify that these operations have workable properties.

Proposition 12.5.3. Given that R satisfies conditions (I)-(V) listed above, then addition in $R[x]$ is both commutative:

$$p(x) + q(x) = q(x) + p(x),$$

and associative:

$$(p(x) + q(x)) + r(x) = p(x) + (q(x) + r(x)).$$

PROOF. First, we show commutativity: Given two polynomials $p(x)$ and $q(x)$ where

$$p(x) = \sum_{i=0}^m a_i x^i; \quad q(x) = \sum_{i=0}^n b_i x^i,$$

then

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i,$$

and

$$p(x) + q(x) = \sum_{i=0}^{\max(m,n)} (b_i + a_i) x^i.$$

Since the addition is commutative, we have $a_i + b_i = b_i + a_i$ for all i . It follows that all coefficients of $p(x) + q(x)$ are equal to the corresponding coefficients of $q(x) + p(x)$. By the definition of polynomial equality, this means that $p(x) + q(x) = q(x) + p(x)$. \square

PROOF. Next we'll prove additive associativity. To do this, we must introduce a third polynomial, $r(x)$, with degree ℓ and coefficients $c_i, i = 0 \dots \ell$.

$$r(x) = \sum_{i=0}^{\ell} c_i x^i.$$

We have,

$$\begin{aligned}
 (p(x) + q(x)) + r(x) &= \left(\sum_{i=0}^m a_i x^i + \sum_{i=0}^n b_i x^i \right) + \sum_{i=0}^{\ell} c_i x^i \\
 &= \left(\sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i \right) + \sum_{i=0}^{\ell} c_i x^i \\
 &= \sum_{i=0}^{\max((m,n),\ell)} (a_i + b_i + c_i) x^i \\
 &= \sum_{i=0}^{\max(m,(n,\ell))} (a_i + b_i + c_i) x^i \\
 &= \sum_{i=0}^m a_i x^i + \sum_{i=0}^{\max(n,\ell)} (b_i + c_i) x^i \\
 &= \sum_{i=0}^m a_i x^i + \left(\sum_{i=0}^n b_i x^i + \sum_{i=0}^{\ell} c_i x^i \right) \\
 &= p(x) + (q(x) + r(x)).
 \end{aligned}$$

Therefore, by the definition of polynomial equality and polynomial addition, $(p(x) + q(x)) + r(x) = p(x) + (q(x) + r(x))$. Note that we have used additive associativity of the coefficients (i. e. $(a_i + b_i) + c_i = a_i + (b_i + c_i)$ for all i).

□

It's also true that the set $R[x]$ has an additive identity and additive inverses. We'll look first at identity.

Proposition 12.5.4. Given that R satisfies properties (I)-(V), then the additive identity of $R[x]$ is $0x^0$, where 0 denotes the additive identity of R .

PROOF. The proof has two parts: (i) $p(x) + 0x^0 = p(x)$ and (ii) $0x^0 + p(x) = p(x)$, $\forall p(x) \in R[x]$. We'll prove (i) and leave (ii) as an exercise.

(i) Given an arbitrary polynomial $p(x) = \sum_{i=0}^m a_i x^i \in R[x]$. Then,

$$\begin{aligned}
p(x) + 0x^0 &= \left(\sum_{i=0}^m a_i x^i \right) + 0x^0 \\
&= \sum_{i=0}^m (a_i + 0) x^i \\
&= \sum_{i=0}^m a_i x^i \\
&= p(x)
\end{aligned}$$

So part (i) of the proof is finished.

Exercise 12.5.5. Complete part (ii) of the proof of Proposition 1.6.6. \diamond

\square

In the following we'll write the additive identity of $R[x]$ as 0 instead of $0x^0$, but don't forget that the additive identity of $R[x]$ is also a polynomial in $R[x]$.

Before we prove additive inverse, we should first clarify some notation. If a is an element of a ring R , then we'll write the additive inverse of a as $-a$. (This is obvious if R is \mathbb{R} , \mathbb{Z} , or some other familiar set of numbers—but we also need to think about the general case where R is some other set such as \mathbb{Z}_n , and the $+$ operation is not regular addition.) Using this notation, we may now characterize the additive inverse of a polynomial.

Exercise 12.5.6. Determine the additive inverse of each element in Z_5 and explain your answer. \diamond

Proposition 12.5.7. Let $p(x) = \sum_{i=0}^n a_i x^i$ be a polynomial in $R[x]$, where R satisfies properties (I)-(V). Then the additive inverse of $p(x)$ is $q(x) = \sum_{i=0}^n (-a_i) x^i$, where $-a_i$ is the additive inverse of a_i in R .

Exercise 12.5.8. Prove Proposition 12.5.7 by showing that $p(x) + q(x)$ and $q(x) + p(x)$ both sum to the additive identity of $R[x]$. \diamond

If we compare our results with the definition of group (Definition 5.4.26), we make an important discovery:

Proposition 12.5.9. Let $R[x]$ be the set of polynomials over a set R that satisfies properties (I)-(V). Then $R[x]$ is an abelian group under addition (recall that “abelian” means that the group’s operation is commutative).

Exercise 12.5.10. Prove Proposition 12.5.9. You may use the propositions that we already proved in this section. \diamond

Next, we consider the proof for multiplicative associativity in general, but before giving a proof, let’s do an example to see how this works.

Exercise 12.5.11. Show that the multiplication of two linear polynomials and one quadratic polynomial is associative. (use $a_0 + a_1x$, $b_0 + b_1x$, and $c_0 + c_1x + c_2x^2$ as your polynomials.) \diamond

We’ve been talking about polynomial addition—now it’s multiplication’s turn. First we prove multiplicative associativity in $R[x]$:

Proposition 12.5.12. Multiplication in $R[x]$ is associative:

$$(p(x)q(x))r(x) = p(x)(q(x)r(x)).$$

PROOF. We’ve seen that the product of two polynomials $p(x)$ and $q(x)$ may be written in summation notation as:

$$p(x)q(x) = \sum_{i=0}^m \sum_{j=0}^n a_i b_j x^{i+j}$$

Now we multiply a third polynomial, $r(x)$, to calculate its product with $(p(x)q(x))$:

$$\begin{aligned} (p(x)q(x))r(x) &= \left(\sum_{i=0}^m \sum_{j=0}^n a_i b_j x^{i+j} \right) \left(\sum_{k=0}^{\ell} c_k x^k \right) \\ &= \sum_{i=0}^m \sum_{j=0}^n \left(a_i b_j x^{i+j} \left(\sum_{k=0}^{\ell} c_k x^k \right) \right) \\ &= \sum_{i=0}^m \sum_{j=0}^n \sum_{k=0}^{\ell} a_i b_j x^{i+j} \cdot c_k x^k \\ &= \sum_{i=0}^m \sum_{j=0}^n \sum_{k=0}^{\ell} a_i b_j c_k x^{i+j+k}. \end{aligned}$$

In the above calculation we have twice brought multiplicative terms inside of summations, using the distributive law. The last step uses a familiar exponent rule.

To complete the proof of associativity, we need to show that the summation expression for $p(x)(q(x)r(x))$ may be simplified into the same expression. The calculation is very similar, and we leave it as an exercise:

Exercise 12.5.13. Show $p(x)(q(x)r(x))$ also simplifies to $\sum_{i=0}^m \sum_{j=0}^n \sum_{k=0}^{\ell} a_i b_j c_k x^{i+j+k}$.

Give a justification for each step of your calculation. \diamond

The exercise shows that $(p(x)q(x))r(x)$ and $p(x)(q(x)r(x))$ both simplify to the same expression, so they are equal. This completes the proof. \square

Next we consider the distributive property for polynomials.

Proposition 12.5.14. Polynomials in $R[x]$ have both right distributivity across addition:

$$(q(x) + r(x))p(x) = q(x)p(x) + r(x)p(x),$$

and left distributivity across addition:

$$p(x)(q(x) + r(x)) = p(x)q(x) + p(x)r(x).$$

PROOF. To show right distributivity, we have:

$$\begin{aligned}
 (q(x) + r(x))p(x) &= \left(\sum_{j=0}^n b_j x^j + \sum_{j=0}^{\ell} c_j x^j \right) \sum_{i=0}^m a_i x^i \\
 &= \left(\sum_{j=0}^{\max(n,\ell)} (b_j + c_j) x^j \right) \sum_{i=0}^m a_i x^i \\
 &= \left(\sum_{j=0}^{\max(n,\ell)} (b_j x^j + c_j x^j) \right) \sum_{i=0}^m a_i x^i \\
 &= \sum_{j=0}^{\max(n,\ell)} \left((b_j x^j + c_j x^j) \sum_{i=0}^m a_i x^i \right) \\
 &= \sum_{j=0}^{\max(n,\ell)} \sum_{i=0}^m (b_j x^j + c_j x^j) a_i x^i \\
 &= \sum_{j=0}^{\max(n,\ell)} \sum_{i=0}^m (b_j x^j a_i x^i + c_j x^j a_i x^i) \\
 &= \sum_{j=0}^{\max(n,\ell)} \sum_{i=0}^m b_j x^j a_i x^i + \sum_{j=0}^{\max(n,\ell)} \sum_{i=0}^m c_j x^j a_i x^i \\
 &= \sum_{j=0}^n \sum_{i=0}^m b_j x^j a_i x^i + \sum_{j=0}^{\ell} \sum_{i=0}^m c_j x^j a_i x^i \\
 &= \sum_{j=0}^n b_j x^j \sum_{i=0}^m a_i x^i + \sum_{j=0}^{\ell} c_j x^j \sum_{i=0}^m a_i x^i \\
 &= q(x)p(x) + r(x)p(x),
 \end{aligned}$$

which gives us right distributivity. We'll leave left distributivity up to you:

Exercise 12.5.15. Provide justification for each of the steps in the calculation in Proposition 12.5.14 \diamond

Exercise 12.5.16. Prove that polynomials in $R[x]$ have left distributivity across addition. \diamond

\square

12.6 Polynomials and division

So far, we have looked at addition and multiplication of polynomials. We've also dealt with subtraction, because subtraction is simply addition of additive inverses. So it's only natural to consider the question of polynomial division.

We've just mentioned that subtraction is the same as addition of additive inverses. Similarly, division is multiplication by multiplicative inverses.

Do polynomials have multiplicative inverses? Be careful here. In high-school algebra or in calculus, the polynomial $p(x)$ has a perfectly good multiplicative inverse, namely $1/p(x)$. But $1/p(x)$ is not a polynomial, so for us it doesn't count!

Exercise 12.6.1.

- (a) Which elements of $\mathbb{R}[x]$ have multiplicative inverses that are also elements of $\mathbb{R}[x]$?
- (b) Which elements of $\mathbb{R}[x]$ have multiplicative inverses that are also elements of $\mathbb{R}[x]$?

◇

12.6.1 The Division Algorithm for polynomials over fields

In Chapter 5, we used the following fact about integers: for any two integers a and b with $b > 0$, then there exist unique integers q and r such that $a = bq + r$, where $0 \leq r < b$. This fact was known to the ancient Greeks, who proved it using what's known as the *division algorithm*.¹ It turns out that a similar division algorithm exists for many types of polynomials. In this section we'll give the proof. But first, as usual, we look at some examples.

Example 12.6.2. Dividing polynomials in $\mathbb{R}[x]$ is very similar to long division of real numbers. For example, suppose that we divide $x^3 - x^2 + 2x - 3$ by $x - 2$.

¹As we said before, you may find a proof in any book on number theory. Or, take a look at: <http://2000clicks.com/mathhelp/NumberTh09EuclidsAlgorithm.aspx>.

$$\begin{array}{r}
 x - 2 \overline{) \begin{array}{r} x^2 + x + 4 \\ x^3 - x^2 + 2x - 3 \\ \hline x^3 - 2x^2 \\ \hline x^2 + 2x - 3 \\ x^2 - 2x \\ \hline 4x - 3 \\ 4x - 8 \\ \hline 5 \end{array} }
 \end{array}$$

In the example, we need to take the leading power term of x in the divisor and multiply by something that will make it equal to the the leading power term in the dividend. In this case it's x^2 . This gives $x^2 \cdot (x - 2) = x^3 - 2x^2$. Subtract from the dividend to yield a remainder of $x^2 + 2x - 3$ and repeat until the remainder is of a degree less than the divisor.

Hence, $x^3 - x^2 + 2x - 3 = (x - 2)(x^2 + x + 4) + 5$, which you may check by multiplying out the right-hand side. \blacklozenge

In $\mathbb{Z}_p[x]$ the process of division is very similar. You may want to use a Cayley table for multiplication, to determine what terms go in the quotient. Additionally, when subtracting the product of the quotient and divisor from the dividend, each negative term must be replaced with its equivalent in \mathbb{Z}_p , which is the remainder mod p .

Example 12.6.3. Divide $(2x^3 + 3x^2 + x + 4)$ by $(x + 2)$ where both polynomials are in $\mathbb{Z}_5[x]$.

$$\begin{array}{r}
 x + 2 \overline{) \begin{array}{r} 2x^2 + 4x + 3 \\ 2x^3 + 3x^2 + x + 4 \\ \hline 2x^3 + 4x^2 \\ \hline 4x^2 + x + 4 \\ 4x^2 + 3x \\ \hline 3x + 4 \\ 3x + 1 \\ \hline 3 \end{array} }
 \end{array}$$

\blacklozenge

Exercise 12.6.4. Find $q(x)$ and $r(x)$ in the following equations. All polynomials are in $\mathbb{R}[x]$.

- (a) $x^2 + 3x + 27 = (x - 2)q(x) + r(x)$
 (b) $15x^3 + 13x - 27 = (x - 5)q(x) + r(x)$
 (c) $10x^3 - x^2 + 3x + 27 = (2x^2 - 4)q(x) + r(x)$

◇

Exercise 12.6.5.

- (a) Divide $3x^6 + x^5 + 4x^4 + 2$ by $x + 3$ where both polynomials are in $\mathbb{Z}_5[x]$.
 (b) Divide $x^7 + x^5 + x^3 + x$ by $x + 1$ where both polynomials are in $\mathbb{Z}_2[x]$.
 (c) Divide $4x^5 + 2x^4 + 3x^3 + 5x^2 + x + 6$ by $x + 6$ where both polynomials are in $\mathbb{Z}_7[x]$.
 (d) Divide $x^5 + 9x^4 + 6x^3 + 2x^2 + 7x + 3$ by $x^2 + 7x + 9$ where both polynomials are in $\mathbb{Z}_{11}[x]$.
 (e) Divide $7x^3 + 2x^2 + 4x + 8$ by $5x + 6$, where both polynomials are in $\mathbb{Z}_{13}[x]$.

◇

We are now ready to prove the division algorithm for polynomials. In order to make our results as general as possible, we won't be too specific about the coefficients. In Section 12.5 we gave five properties that our set of coefficients R should satisfy (including associativity, distributivity, and commutativity of addition). In this section we will refer to our set of coefficients as F , and we require that F have the same properties as R plus two more:

- (VI) F has a multiplicative identity (which we will denote as 1)
 (VII) The nonzero elements of F have multiplicative inverses: that is, if $a \in F$ and $a \neq 0$, then there exists an element $a^{-1} \in F$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

These properties are characteristic of a type of mathematical structure called a **field**. We'll study fields more extensively in Chapter 24: but for now, we simply recognize Properties (I)-(VII) as common properties of many (but not all) of the number systems we've seen so far.

Exercise 12.6.6. Of the number systems $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}, \mathbb{Z}_n, \mathbb{M}_n$, which all satisfy (I)-(V), which do not satisfy (VI) and (VII)? \diamond

Proposition 12.6.7. (*Division algorithm for polynomials*) Suppose that the set F has addition and multiplication operations that satisfy (I)-(VII). Let $f(x)$ and $g(x)$ be nonzero polynomials in $F[x]$, where the degree of $g(x)$ is greater than 0. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$f(x) = g(x)q(x) + r(x),$$

where the degree of $r(x)$ is less than the degree of $g(x)$.

PROOF. We will first prove the existence of $q(x)$ and $r(x)$. We define a set S as follows:

$$S = \{f(x) - g(x)h(x), \text{ for all } h(x) \in F[x]\}.$$

This set is nonempty since $f(x) \in S$. Let $r(x)$ be a polynomial of smallest degree in S .² This means that there must exist a $q(x)$ such that

$$r(x) = f(x) - g(x)q(x).$$

We need to show that the degree of $r(x)$ is less than the degree of $g(x)$. Let's prove this by contradiction. So we assume the contrary, namely that $\deg g(x) \leq \deg r(x)$. Let n, m be the degree of $g(x), r(x)$ respectively, where $n \leq m$. Then we may write

$$g(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$r(x) = b_0 + b_1x + \cdots + b_mx^m,$$

where $a_n \neq 0$ and $b_m \neq 0$. Taking a cue from the process of long division, we define a new polynomial $r'(x)$ by

$$r'(x) := r(x) - b_m a_n^{-1} x^{m-n} g(x)$$

²At this point we can't assume that there's only one such polynomial, so we have to say "a polynomial" rather than "the polynomial".

It's tedious to write out all the terms of $r'(x)$. Fortunately, it's not really necessary. We only need to remark that the degree of $r'(x)$ is less than the degree of $r(x)$, since the leading-order terms of $r(x)$ and $b_m(a_n^{-1})x^{m-n}g(x)$ are both b_mx^m , so they cancel. We may plug in $r(x) = f(x) - g(x)q(x)$ to obtain

$$\begin{aligned} r'(x) &:= f(x) - g(x)q(x) - b_m a_n^{-1} x^{m-n} g(x) \\ &= f(x) - g(x) (q(x) - b_m a_n^{-1} x^{m-n}). \end{aligned}$$

This shows that $r'(x)$ is also in S (look back at the definition and see!). But $\deg r'(x) < \deg r(x)$, which contradicts our condition that $r(x)$ is an element of S with smallest degree. The rules of proof by contradiction allow us to conclude that our assumption is false: namely, it must be true that $\deg g(x) > \deg r(x)$. This finishes the proof of existence.

To show that $q(x)$ and $r(x)$ are unique, suppose that polynomials $q'(x)$ and $r'(x)$ satisfy $f(x) = g(x)q'(x) + r'(x)$, so that

$$f(x) = g(x)q(x) + r(x) = g(x)q'(x) + r'(x).$$

This implies

$$g(x)[q(x) - q'(x)] = r'(x) - r(x).$$

If $q(x) - q'(x)$ is not the zero polynomial, then since the field F has no zero divisors it follows that $\deg(g(x)) \leq \deg(g(x)[q(x) - q'(x)])$. This in turn implies

$$\deg g(x) \leq \deg(g(x)[q(x) - q'(x)]) = \deg(r'(x) - r(x)).$$

However, the degrees of both $r(x)$ and $r'(x)$ are strictly less than the degree of $g(x)$, so their difference can't have such a large degree. It follows that $q(x) - q'(x) = 0$, which implies that $q(x) = q'(x)$ and $r(x) = r'(x)$. \square

12.6.2 Greatest common divisors of polynomials

In the Modular Arithmetic chapter, we used the Euclidean algorithm to find the gcd's of sets of integers. Now that we have a division algorithm for polynomials, we can find gcd's of polynomials in the same way.

To illustrate this, we begin with an example in $\mathbb{R}[x]$.

Example 12.6.8.

Suppose that we would like to find the gcd of $a(x) = x^4 - 5x^3 + 5x^2 + 5x - 6$ and $b(x) = x^4 + 5x^3 + 5x^2 - 5x - 6$. We first divide $a(x)$ by $b(x)$ to determine the remainder, r_1 .

$$x^4 + 5x^3 + 5x^2 - 5x - 6 \overline{) \begin{array}{r} 1 \\ x^4 - 5x^3 + 5x^2 + 5x - 6 \\ -x^4 - 5x^3 - 5x^2 + 5x + 6 \\ \hline -10x^3 + 10x \end{array}}$$

So $r_1 = -10x^3 + 10x$. We then divide $b(x)$ by r_1 to determine the second remainder, r_2 .

$$-10x^3 + 10x \overline{) \begin{array}{r} -\frac{1}{10}x - \frac{1}{2} \\ x^4 + 5x^3 + 5x^2 - 5x - 6 \\ -x^4 + x^2 - 6 \\ \hline 5x^3 + 6x^2 - 5x - 6 \\ -5x^3 + 5x \\ \hline 6x^2 - 6 \end{array}}$$

So $r_2 = 6x^2 - 6$. We then divide r_1 by r_2 to determine the third remainder, r_3 .

$$6x^2 - 6 \overline{) \begin{array}{r} -\frac{5}{3}x \\ -10x^3 + 10x \\ 10x^3 - 10x \\ \hline 0 \end{array}}$$

Notice that $r_3 = 0$. This means that $6x^2 - 6$ divides both $a(x)$ and $b(x)$. Furthermore, any real, nonzero multiple of $6x^2 - 6$ will divide both $a(x)$ and $b(x)$. For convenience, we choose the multiple with a leading coefficient of 1. This means that $x^2 - 1$ is the gcd of $a(x)$ and $b(x)$. You should check that $x^2 - 1$ divides both $a(x)$ and $b(x)$. \blacklozenge

Exercise 12.6.9.

- (a) Use the Euclidean algorithm to compute the gcd of $a(x) = 5x^3 - 2x^2 - 22x + 21$ and $b(x) = 5x^4 - 7x^3 + 15x^2 - 21x$ in $\mathbb{R}[x]$.

- (b) Use the Euclidean algorithm to compute the gcd of $a(x) = 4x^4 - 4x^3 - 4x^2 + 12x - 8$ and $b(x) = 8x^4 - 8x^3 + 8x^2 - 12x + 4$ in $\mathbb{R}[x]$.

◇

Now that we've seen some examples with coefficients in $\mathbb{R}[x]$, let's see how the Euclidean algorithm can be applied to determine the gcd of polynomials in $\mathbb{Z}_p[x]$, where p is prime.

Example 12.6.10. Suppose that we would like to find the gcd of $a(x) = x^4 + 2x^3 + 5x^2 + 5x + 1$ and $b(x) = x^4 + 5x^3 + 5x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$. We first divide $a(x)$ by $b(x)$ to determine the remainder, r_1 .

$$x^4 + 5x^3 + 5x^2 + 2x + 1 \begin{array}{r} 1 \\ \hline x^4 + 2x^3 + 5x^2 + 5x + 1 \\ \hline 6x^4 + 2x^3 + 2x^2 + 5x + 6 \\ \hline 4x^3 + 3x \end{array}$$

So $r_1 = 4x^3 + 3x$. We then divide $b(x)$ by r_1 to determine the second remainder, r_2 .

$$4x^3 + 3x \begin{array}{r} 2x + 3 \\ \hline x^4 + 5x^3 + 5x^2 + 2x + 1 \\ \hline 6x^4 + x^2 \\ \hline 5x^3 + 6x^2 + 2x + 1 \\ \hline 2x^3 + 5x \\ \hline 6x^2 + 1 \end{array}$$

So $r_2 = 6x^2 + 1$. We then divide r_1 by r_2 to determine the third remainder, r_3 .

$$6x^2 + 1 \begin{array}{r} 3x \\ \hline 4x^3 + 3x \\ \hline 3x^3 + 4x \\ \hline 0 \end{array}$$


Notice that $r_3 = 0$. Therefore, $6x^2 + 1$ divides both $a(x)$ and $b(x)$. We multiply $6x^2 + 1$ by the inverse of 6 to obtain the gcd for $a(x)$ and $b(x)$. The

result is $x^2 + 6$. We leave it to the reader to check that $x^2 + 6$ divides both $a(x)$ and $b(x)$. \blacklozenge

Exercise 12.6.11.

- (a) Use the Euclidean algorithm to compute the gcd of $a(x) = x^3 + x^2 + 3x$ and $b(x) = 3x^3 + 2x^2 + x + 4$ in $\mathbb{Z}_5[x]$.
- (b) Use the Euclidean algorithm to compute the gcd of $a(x) = x^3 + 2x^2 + 2$ and $b(x) = 2x^2 - x + 1$ in $\mathbb{Z}_3[x]$.

\diamond

12.6.3 Polynomial roots and the FTOA (easy part) 

When you first learned about factoring polynomials with integer or real coefficients, you may have been told (or noticed on your own) that a polynomial of degree n has at most n roots. This result is important enough that it has a name: it's part of the *Fundamental Theorem of Algebra*, or *FTOA* for short (sadly, it's only the easy part of FTOA—we'll discuss the hard part later).

Most likely though you've never seen a proof of the FTOA. No worries—the proof is at hand! In keeping with our previous discussion, we will state our results in terms of $F[x]$, where the set of coefficients F satisfies properties (I)-(VII).

The following preliminary proposition gives us a way to relate polynomial values to polynomial remainders.

Proposition 12.6.12. Let F satisfy properties (I)-(VII), $f(x) \in F[x]$, and $a \in F$. When $f(x)$ is divided by $x - a$, the remainder is $f(a)$.

PROOF. According to Proposition 12.6.7, if we divide $f(x)$ by $x - a$, it will produce two unique polynomials $q(x)$ and $r(x)$ such that $f(x) = (x - a)q(x) + r(x)$. Since the degree of $x - a$ is 1, then according to the division algorithm, the degree of $r(x)$ must be less than 1. Therefore $r(x)$ must be a constant r , and we may write:

$$f(x) = (x - a)q(x) + r.$$

If we set $x = a$ then we get:

$$\begin{aligned} f(a) &= (a - a)q(x) + r \\ &= 0 \cdot q(x) + r \\ &= r. \end{aligned}$$

□

This proposition can save lots of time when finding remainders under division by monomials.

Exercise 12.6.13.

- (a) Find the remainders when $\sum_{k=1}^{100} kx^{k-1}$ is divided by $x - 1$ and $x + 1$, respectively.
- (b) Find the remainders when $\sum_{k=0}^{100} \left(\frac{1}{2}\right)^k x^k$ is divided by $x - 1/2$ and $x + 1/2$, respectively.
- (c) Find the remainders when $\sum_{k=0}^{100} 3^k x^k$ is divided by $x + 1/9$ and $x - 1/9$, respectively.

◇

The following proposition is an important special case of Proposition 12.6.12.

Proposition 12.6.14. Let F satisfy properties (I)-(VII), $f(x) \in F[x]$, and $a \in F$. Then $x - a$ divides $f(x)$ if and only if $f(a) = 0$.

PROOF. From Proposition 12.6.12 $f(x) = (x - a) \cdot q(x) + f(a)$. Therefore $f(a) = 0$ if and only if $f(x) = (x - a) \cdot q(x)$, which is true if and only if $x - a$ divides $f(x)$. □

We may also restate Proposition 12.6.14 as: a is a root of the polynomial $f(x)$ if and only if $x - a$ divides $f(x)$.

We will need to take care of some preliminaries in order to prove (the easy part of) the Fundamental Theorem of Algebra. From basic algebra with real numbers, we know that if $ab = 0$ then either $a = 0$ or $b = 0$ (see also Proposition 4.2.11 of Chapter 4). Actually, this **zero-divisor property** hold for any set R that satisfies (I)-(VII):

Proposition 12.6.15. Suppose that F satisfies properties (I)-(VII). Given $a, b \in F$ and $ab = 0$, then either $a = 0$ or $b = 0$.

Exercise 12.6.16. Prove Proposition 12.6.15. (*Hint:* you may follow the steps given in Exercise 4.2.12 \diamond)

It turns out that if F satisfies the zero-divisor property, then $F[x]$ satisfies the same property:

Proposition 12.6.17. Suppose F satisfies Properties (I)-(VII), and suppose $p(x), q(x) \in F[x]$. Then $p(x)q(x) = 0$ iff either $p(x) = 0$ or $q(x) = 0$.

PROOF. Since this is a “iff” proof, we must actually prove both the “if” statement and the “only if” statement.

First we prove the “if” part. It follows from the formula for multiplication of polynomials that if either $p(x) = 0$ or $q(x) = 0$, then the product $p(x)q(x)$ must also be 0. That was easy!

The “only if” part is harder. We will prove the contrapositive, namely that $p(x) \neq 0$ and $q(x) \neq 0$ implies that $p(x)q(x) \neq 0$. Let

$$p(x) = \sum_{i=0}^m a_i x^i \text{ and } q(x) = \sum_{j=0}^n b_j x^j,$$

where $a_m \neq 0$ and $b_n \neq 0$. We can then write

$$p(x)q(x) = \sum_{k=0}^{m+n} c_k, \text{ where } c_k = \sum_{i=0}^k a_i b_{k-i}.$$

Consider the coefficient c_{m+n} , which may be expanded out as

$$c_{m+n} = a_0 b_{m+n} + a_1 b_{m+n-1} + \dots + a_m b_n + \dots + a_{n+m-1} b_1 + a_{n+m} b_0.$$

Take a look at these terms for a moment. Which of them are nonzero? Notice how we’ve separated out the term $a_m b_n$ in the middle of the expansion. Since $a_m \neq 0$ and $b_n \neq 0$, this term is nonzero. Now, are there any other nonzero terms? All terms have the form $a_i b_j$, and for every other term in the series (besides $a_m b_n$) we have either $i > m$ or $j > n$. If $i > m$ then $a_i = 0$, since the degree of $p(x)$ is m and all coefficients of terms of higher degree are 0. For the same reason, if $j > n$ then $b_j = 0$. It follows that except for the

term $a_m b_n$, all other terms $a_i b_j$ are 0, which implies that $c_{m+n} = a_m b_n \neq 0$. But this means that $p(x)q(x)$ has a nonzero term, namely $c_{m+n}x^{m+n}$, so $p(x)q(x) \neq 0$. The proof is completed. \square

And here's the result we've been waiting for. Now that we've prepared the ground, it's not so difficult to prove.

Proposition 12.6.18. (*Fundamental Theorem of Algebra: easy part*) Suppose F satisfies properties (I)-(VII), and let $f(x)$ be a polynomial in $F[x]$ of degree n . Then the equation $f(x) = 0$ has at most n solutions: that is, there are at most n distinct elements $\{x_1, \dots, x_n\}$ of F such that $f(x_m) = 0$ for $1 \leq m \leq n$.

PROOF. Suppose a_1 is a solution to $f(x) = 0$. Then by Proposition 12.6.14 it follows that $x - a_1$ divides $f(x)$. Therefore $f(x) = (x - a_1)g_{n-1}(x)$ where the degree of $g_{n-1}(x) = n - 1$.

Now if $a_2 \neq a_1$ is another solution then using our above result we have

$$f(a_2) = (a_2 - a_1)g_{n-1}(a_2) = 0.$$

Since $a_2 - a_1 \neq 0$, it follows that $g_{n-1}(a_2) = 0$. So we can write $g_{n-1}(x) = (x - a_2)g_{n-2}(x)$ where the degree of $g_2(x) = n - 2$.

Continuing in the same way, if there are distinct roots a_1, a_2, \dots, a_n then

$$f(x) = (x - a_1)(x - a_2)\dots(x - a_n)g_0,$$

where the degree of g_0 is 0 (in other words, g_0 is a constant.). So there can't be any more solutions, a_{n+1} , because $(x - a_{n+1})$ doesn't divide g_0 . \square

The previous theorem immediately gives us an extremely important general property of roots of polynomials:

Proposition 12.6.19. Suppose F satisfies properties (I)-(VII), and let c be any element F . Then c has at most n n^{th} roots.

PROOF. Given $C \in F$, then the polynomial $x^n - c$ is an element of $F[x]$. By Proposition 12.6.18, the equation $x^n - c = 0$ has at most n solutions. This is exactly the same thing as saying that c has at most n n^{th} roots. \square

Exercise 12.6.20.

(a) Find all fourth roots of 5625 in $\mathbb{R}[x]$. Give exact solutions.

- (b) Find all fifth roots of $3125i$ in $\mathbb{C}[x]$. Give exact solutions.
- (c) Find all fifth roots of 5 in \mathbb{Z}_7 .
- (d) Find all sixth roots of 1 in \mathbb{Z}_7 .

◇

Take note of the “at most” qualification in Proposition 12.6.18. There are cases of polynomials in $F[x]$ which do not have *any* roots in F . For example, there are polynomials in $\mathbb{R}[x]$ that have no roots at all in $\mathbb{R}[x]$, as the next examples illustrate.

Example 12.6.21. Find the roots of $p(x) = 2x^2 + 2x + 5$.

Since this is a quadratic polynomial we can use the famous quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

In $p(x)$, $a = 2$, $b = 2$, and $c = 5$. We substitute those values into the formula and obtain the following:

$$\begin{aligned} x &= \frac{-2 \pm \sqrt{2^2 - 4 \cdot 2 \cdot 5}}{2 \cdot 2} = \frac{-2 \pm \sqrt{-36}}{4} = \frac{-2 \pm 6i}{4} \\ &= \frac{-1 \pm 3i}{2}. \end{aligned}$$

So the roots of $p(x)$ are $x = -\frac{1}{2} + \frac{3}{2}i$, $-\frac{1}{2} - \frac{3}{2}i$. Neither of these roots are elements of \mathbb{R} . As noted above this does not contradict FTOA, which only guarantees there won't be more than 2 roots. ◇

The next example is a cubic polynomial in $\mathbb{Z}[x]$. To find the rational roots, we will make use of the following proposition.

Proposition 12.6.22. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ be a polynomial in $\mathbb{Z}[x]$. Any rational roots of $f(x)$ expressed in lowest terms have numerators, p , which are factors of a_0 and denominators, q , which are factors of a_n .

PROOF. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ be a polynomial in $\mathbb{Z}[x]$ and suppose that p/q is a root of $f(x)$, where the fraction p/q is in lowest terms (so p and q are relatively prime).

First we will show that p is a factor of a_0 . Since p/q is a root of $f(x)$ we have $f\left(\frac{p}{q}\right) = 0$, which implies

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_0 = 0.$$

Multiplying both sides by q^n , we have,

$$\left(a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_0\right) q^n = 0,$$

which simplifies to

$$a_n p^n + a_{n-1} (p^{n-1} q) + \dots + a_0 q^n = 0.$$

This expression can be rearranged to obtain:

$$p(-a_n p^{n-1} - a_{n-1} (p^{n-2} q) - \dots - a_1 q^{n-1}) = a_0 q^n.$$

Since $f(x) \in \mathbb{Z}[x]$, all the coefficients a_i are also integers. p and q are also integers. Since integers are closed under addition and multiplication, it follows that both sides of the above equation are integers. Since p divides the left-hand side, it must also divide the right-hand side. Therefore p divides $a_0 q^n$. Now p and q are relatively prime: so in order for p to divide $a_0 q^n$, it must divide a_0 . In other words, p is a factor of a_0 —which is just what we wanted to prove.

It turns out the proof that q is a factor of a_n is basically the same, if we use a little trick. The first equation that we wrote down above was:

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_0 = 0.$$

Let's multiply both sides by $(q/p)^n$. After simplifying, and rearranging we get:

$$a_0 \left(\frac{q}{p}\right)^n + a_1 \left(\frac{q}{p}\right)^{n-1} + \dots + a_n = 0.$$

Now, this new equation corresponds exactly to the first equation with the following replacements:

$$a_n \rightarrow a_0; a_{n-1} \rightarrow a_1; \dots; a_0 \rightarrow a_n; p \leftrightarrow q.$$

We can then go through the entire previous argument, making these replacements. We concluded previously that p is a factor of a_0 —so if we apply the identical argument to the equation with replacements, we obtain that q is a factor of a_n . You may fill in the details in the following exercise.

Exercise 12.6.23. Starting with the equation $a_0 (q/p)^n + a_1 (q/p)^{n-1} + \dots + a_n = 0$, give the complete argument which shows that q is a factor of a_n . \diamond

□

Now let's get some practice using Proposition 12.6.22.

Example 12.6.24. Find the roots of $f(x) = 3x^3 + 10x^2 + 11x + 6$.

Since this is a cubic polynomial, we can't use the quadratic formula, at least not to begin with. The coefficients are integers, so we may use Proposition 12.6.22, which says that *any* rational roots of $p(x)$ have numerators that are factors of a_0 and denominators that are factors of a_n . This does not guarantee that there are rational roots: sometimes polynomials are irreducible, but we still try every method possible to find those roots unless we know that we can't reduce the polynomial. So we will proceed with trying to find the roots of $f(x)$ using Proposition 12.6.22.

In $f(x)$, possible numerators of any rational roots are: $p = \pm 1, \pm 2, \pm 3, \pm 6$. The possible denominators are: $q = \pm 1, \pm 3$. So we have as possible rational roots the following: $p/q = \pm 1, \pm \frac{1}{3}, \pm 2, \pm \frac{2}{3}, \pm 3, \pm 6$. By Proposition 12.6.14, if $f(p/q) = 0$ then $(x - p/q)$ is a factor of $f(x)$; which would make p/q a root of $f(x)$. After testing all possibilities we find the following rational root: $f(-2) = 3(-2)^3 + 10(-2)^2 + 11(-2) + 6 = 0$. Therefore, $x = -2$ is a root of $f(x)$ and $(x + 2)$ is a factor of $f(x)$. We then use long division to factor $f(x)$.

$$\begin{array}{r}
 \quad 3x^2 + 4x + 3 \\
 x+2 \overline{) 3x^3 + 10x^2 + 11x + 6} \\
 \underline{3x^3 + 6x^2} \\
 4x^2 + 11x + 6 \\
 \underline{4x^2 + 8x} \\
 3x + 6 \\
 \underline{3x + 6} \\
 0
 \end{array}$$

So now we have $f(x) = (x+2)(3x^2 + 4x + 3)$. We use the quadratic formula to find the following roots for $3x^2 + 4x + 3$. $x = \frac{-2 \pm \sqrt{5}i}{3}$. So there are two complex roots and one real root. They are $x = \frac{-2 - \sqrt{5}i}{3}, -2, \frac{-2 + \sqrt{5}i}{3}$. \blacklozenge

Exercise 12.6.25.

- (a) Find the roots of $f(x) = 2x^2 + x + 1$. Give exact solutions.
 (b) Find the roots of $f(x) = 5x^3 + 17x^2 + 7x + 3$. Give exact solutions.

\diamond

In the exercises above, the leading coefficient is not 1. The situation is especially simple if the leading coefficient is 1. In such a case, the rational roots are integers:

Exercise 12.6.26.

- (a) Given that $p(x) \in \mathbb{Z}[x]$, and $p(x)$ has leading coefficient 1, show that all rational roots of $p(x)$ are integers.
 (b) Find the roots of $f(x) = x^3 - 13x + 12$.

\diamond

12.6.4 Algebraic closure and the FTOA (hard part)

We've been referring to the “easy” part of the Fundamental Theorem of Algebra. It's time now to consider the “hard” part.

Proposition 12.6.18 says that any polynomial in $F[x]$ of degree n has at most n roots that are elements of F , as long as F satisfies properties (I)-(VII). But the proposition can't guarantee the existence of even one root—and we've shown in Example 12.6.21 that there may be no roots at all!

Exercise 12.6.27. Give an example of a polynomial in $\mathbb{Q}[x]$ which has roots in \mathbb{R} but no roots in \mathbb{Q} . \diamond

For some special cases of F however, a nonconstant polynomial in $F[x]$ (i.e. a polynomial with degree 1 or more) always has roots in F . As a lead-in, we may notice that for every nonconstant polynomial in $\mathbb{R}[x]$ that we looked at we were always able to find complex roots, even when weren't able to find real roots. This might lead us to conjecture that every nonconstant polynomial in $\mathbb{R}[x]$ has at least one root in \mathbb{C} . The hard part of the Fundamental Theorem of Algebra affirms that this is true. What's more, not just nonconstant polynomials in $\mathbb{R}[x]$, but also those in $\mathbb{C}[x]$ all have at least one in \mathbb{C} . Here's the statement of the theorem:

Proposition 12.6.28. (*Fundamental Theorem of Algebra: hard part*) Any nonconstant polynomial in $\mathbb{C}[x]$ has at least one complex root.

There are several proofs of this theorem. The most elegant involves the field of mathematics known as “complex analysis”, and specifically the theory of integrals of functions whose domain and codomain are \mathbb{C} . This proof is one of the highlights in most undergraduate complex analysis classes.³

Here are some examples that illustrate Proposition 12.6.28.

Example 12.6.29. We begin with an example of a linear binomial in $\mathbb{C}[x]$. Let $p(x) = (3 + 2i)x + (2 - i)$. Find the root of $p(x)$ (since $p(x)$ is linear, it will only have one root).

³For a visualizable, constructive proof that uses basic calculus, see <https://arxiv.org/abs/2002.04418>.

First we set $p(x)$ equal to zero and then proceed to find the root as follows. Beginning with $(3 + 2i)x + (2 - i) = 0$, we may rearrange to obtain

$$x = \frac{-2 + i}{3 + 2i},$$

and multiplying numerator and denominator by $3 - 2i$ and simplifying gives

$$x = \frac{4 + 7i}{13} \in \mathbb{C}[x].$$

◆

Example 12.6.30. Let's do another example, but this time with a quadratic trinomial in $\mathbb{C}[x]$. Let $p(x) = (1 + i)x^2 + (2 - i)x + (3 + 3i)$. Find the roots of $p(x)$.

Since this is a quadratic polynomial we can use the quadratic formula and obtain the following:

$$\begin{aligned} x &= \frac{-(2 - i) \pm \sqrt{(2 - i)^2 - 4(1 + i)(3 + 3i)}}{2(1 + i)} = \frac{(-2 + i) \pm \sqrt{3 - 4i - 24i}}{(2 + 2i)} \\ &= \frac{(-2 + i) \pm \sqrt{3 - 28i}}{(2 + 2i)} = \frac{(-2 + i) \pm \sqrt{3 - 28i}}{(2 + 2i)} \cdot \frac{2 - 2i}{2 - 2i} \\ &= \frac{6 + 6i \pm (2 - 2i)\sqrt{3 - 28i}}{8} = \frac{3 + 3i \pm (1 - i)\sqrt{3 - 28i}}{4}. \end{aligned}$$

So the two roots are $x = \left\{ \frac{3+3i-(1-i)\sqrt{3-28i}}{4}, \frac{3+3i+(1-i)\sqrt{3-28i}}{4} \right\}$.

◆

Exercise 12.6.31.

- (a) Find the root of $p(x) = (4 - 3i)x + (2 + 6i)$. Give an exact solution.
- (b) Find the roots of $p(x) = (2 + i)x^2 + (2 - 3i)x + (7 + 3i)$. Give exact solutions.

◇

Proposition 12.6.32. Any polynomial $p(x)$ of degree n in $\mathbb{C}[x]$ can be completely factored as a constant times a product of n linear terms, as follows:

$$p(x) = b(x - a_1)(x - a_2) \dots (x - a_n). \quad (12.6.33)$$

where $b, a_1, \dots, a_n \in \mathbb{C}$.

PROOF. Let $p(x)$ be an arbitrary polynomial of degree n in $\mathbb{C}[x]$. By Proposition 12.6.28, $p(x)$ has at least one complex root a . So $(x - a)$ is a factor of $p(x)$ and we can write $p(x) = (x - a_1)p_1(x)$; where the degree of $p_1(x)$ is $n - 1$. If $p_1(x)$ is linear, then we are done, but if $p_1(x)$ is not linear, then by Proposition 12.6.28 it also has a complex root a_2 . So $(x - a_2)$ is a factor of $p_2(x)$ and we can write $p(x) = (x - a_1)(x - a_2)p_2(x)$; where the degree of $p_2(x)$ is $n - 2$. The same argument continues until we reach $p_{n-2}(x)$, which has degree 1. But this means that $p_{n-2}(x)$ can be written as $bx - c$, which we may rewrite as $b(x - a_n)$, where $a_n = c/b$. It follows finally that $p(x) = b(x - a_1)(x - a_2) \dots (x - a_n)$. \square

Exercise 12.6.34. Suppose $p(x)$ is a polynomial of degree n such that the coefficient of x^n is 1 (such a polynomial is called a *monic polynomial*). Show that for a monic polynomial, the coefficient b in Proposition 12.6.32 is equal to 1. \diamond

Now let's apply Proposition 12.6.32 to an example.

Example 12.6.35. Let $f(x) = x^4 - 4x^3 + 10x^2 - 24x + 24$ be a polynomial in $\mathbb{C}[x]$. Notice that the coefficients of $f(x)$ are integers, so $f(x)$ is also in $\mathbb{Z}[x]$. Therefore we can use Proposition 12.6.22 to factor out our first linear term. Since $a_0 = 24$ and $a_n = 1$, possible rational roots are

$$\frac{p}{q} = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12.$$

By Proposition 12.6.14, if $f(p/q) = 0$ then $(x - p/q)$ is a factor of $f(x)$ i.e. p/q a root of $f(x)$. After testing all possibilities we find the following rational root: $f(2) = 2^4 - 4(2)^3 + 10(2)^2 - 24(2) + 24 = 0$. Therefore, $x = 2$ is a root of $f(x)$ and $(x - 2)$ is a factor of $f(x)$. After dividing $f(x)$ by $(x - 2)$ we have the following:

$$\begin{aligned} f(x) &= (x - 2)(x^3 - 2x^2 + 6x - 12) = (x - 2)(x^2(x - 2) + 6(x - 2)) \\ &= (x - 2)(x - 2)(x^2 + 6) = (x - 2)^2(x^2 + 6). \end{aligned}$$

Solving $x^2 + 6 = 0$ for x gives us additional roots: $x = -\sqrt{6}i, 2, \sqrt{6}i$. In summary, we have

$$f(x) = (x - 2)(x - 2)(x + \sqrt{6}i)(x - \sqrt{6}i).$$

So as Proposition 12.6.32 states, $f(x)$ factors completely into a product of linear terms. \blacklozenge

Remark 12.6.36. Although $f(x)$ is a fourth degree polynomial, and factors into the product of 4 linear terms, yet it only has 3 *distinct* roots because of the repeated factor $(x - 2)$. This agrees with Proposition 12.6.18, which implies that a polynomial of degree 4 has *at most* n distinct solutions. \triangle

Take a moment to savor the full generality of Proposition 12.6.28. We don't have to restrict ourselves to polynomials with real coefficients: even if the polynomial's coefficients are imaginary or complex, the proposition still guarantees that the polynomial has a root. Further, Proposition 12.6.32 then guarantees that it can be factored into a product of linear factors.

Exercise 12.6.37. Factor each of the following polynomials into a product of linear terms.

(a) $p(x) = x^3 + (-6 + i)x^2 + (13 - 6i)x + 13i = 0$ (*hint*: evaluate $p(-i)$).

(b) $f(x) = x^3 - 6ix^2 - 11x + 6i = 0$ (*hint*: evaluate $f(i)$).

\diamond

Exercise 12.6.38.

(a) Suppose that $p(x) \in \mathbb{C}[x]$ and $p(x) = p(-x)$. Show that $p(x)$ is actually a polynomial in x^2 , so that $p(x)$ can be written as $q(x^2)$ where $q(x) \in \mathbb{C}[x]$. (*Hint*: If $p(a) = 0$, then what about $p(-a)$? Use this fact to get two linear factors of $p(x)$, and multiply them together. The case where $p(0) = 0$ should be treated separately.)

(b) Suppose that $p(x) \in \mathbb{C}[x]$ and $p(x) = -p(-x)$. Show that $p(x)$ can be written as $xq(x^2)$ where $q(x) \in \mathbb{C}[x]$.

\diamond

12.7 Hints for “Polynomial Rings” exercises

Exercise 12.3.5(d): Note $4 = 3 + 1$ and $11 = 3^2 + 2$.

Exercise 12.3.11(d): Are there any common factors you can take outside the summations before multiplying?

Exercise 12.4.3: Note that if a_2 is in $5\mathbb{Z}$, then $a_2 = 5a'_2$ where a'_2 is also an integer. The same thing holds for all the other coefficients in $p(x)$ and $q(x)$.

Exercise 12.6.20(b): Use the method in Section 4.4.2.

Symmetries of Plane Figures



“In all the arts it is symmetry that gives pleasure, preserving unity, and making the whole beautiful.” (Augustine, *Of True Religion*, xxx.55 (Tr. J. H. S. Burleigh))

“It is only slightly overstating the case to say that physics is the study of symmetry.” (Philip W. Anderson, 1977 Nobel laureate in physics)

“So our problem is to explain where symmetry comes from. Why is nature so nearly symmetrical? No one has any idea why.” (Richard Feynman, 1965 Nobel laureate in physics)

The above quotes give some flavor of the importance and the mystery of symmetry, in both art and science. In keeping with our practice throughout this book, we will introduce this general topic by means of a basic example, namely symmetries of plane figures. Many of the concepts that you will learn in this chapter are applicable to symmetries in general. In particular: wherever you find a symmetry, you will always find a *group* lurking behind it (see Section 5.4.7 for the mathematical definition of a group).

Thanks to Tom Judson for material used in this chapter.

13.1 Definition and examples

In plane geometry we talk about various shapes: triangles, rectangles, pentagons, and so on. Shapes are important because real objects have shapes (duh), and objects are important. What would life be without triangles?

Now suppose you and your friend cut an equilateral triangle out of a piece of plain white paper and put it on the table. Then you tell your friend to go out of the room. While she's gone, you take the triangle and move it, but in such a way that it looks exactly the same. You can do this by rotating the triangle, or flipping it over, or by some combination of these two actions. When your friend comes back into the room, although the triangle has been moved there's no way for her to tell. This type of motion is called a *symmetry operation*. Clearly we may perform symmetry operations on other objects besides equilateral triangles, but only if the shape of the object has some kind of regularity. In the following discussion, we will explore the relationship between shapes and symmetry operations.

We've given an intuitive picture of what symmetry means—now let's try to translate that into mathematics. We start with a definition:

Definition 13.1.1. A *symmetry* of a geometrical figure is a rearrangement of the figure that (i) preserves distances and angles between points of the figure, and (ii) leaves the appearance and location of the figure unchanged.

△

Remark 13.1.2. The meaning of “preserves distances” can be expressed more precisely as follows. Take any two points A and B of the original figure. The figure is then rearranged so that A and B are sent to points A' and B' respectively. Then in order for the rearrangement to be a symmetry, the distance between A and B must always be equal to the distance between A' and B' .

Similarly, the meaning of “preserves angles” can be expressed more precisely as follows. Take any three points A, B, C of the original figure. The figure is then rearranged so that A, B, C are sent to A', B', C' respectively. In order for the rearrangement to be a symmetry, $\angle ABC$ must always be equal to $\angle A'B'C'$ regardless of the choice of A, B, C .¹ △

¹It can be shown mathematically that a rearrangement that preserves distances must necessarily preserve angles as well. So strictly speaking, the additional angle preservation requirement is not necessary.

A motion that preserves distances and angles between parts of a figure is also called a *rigid motion*. Intuitively, you may think of the figure as a rigid object, and the “rearrangement” is effected by moving the rigid object in some fashion. For example, any *rotation* that does not change the shape of the object is a rigid motion.



Figure 13.1.1. Mercedes Logo

Example 13.1.3. Consider the Mercedes logo shown in Figure 13.1.1.

- Imagine pinning the center of the logo to the page and spinning the logo 120° counterclockwise about its center. The resulting image looks exactly like the original, because each of the three points on the circumference moves to the location of the next point over. So a 120° counterclockwise rotation is a symmetry of the logo.
- If you rotate the image 180° counterclockwise about the center, the resulting image is no longer identical to the original (try it!). So a 180° counterclockwise rotation is not a symmetry of the logo.
- We could also “flip over” the logo (like flipping a pancake) in such a way that the left half moves to the right, and vice versa. Then the vertical point stays in the same place while the left and right point exchange positions, leaving the appearance of the logo unchanged. The motion has the same effect as if the logo were *reflected* across the vertical axis. After the motion, the logo looks the same.
- Shifting the original image (shifts are also called *translations* in any direction is a rigid motion, and the resulting image looks the same as the original, but the location is different. Hence this shift is *not* a symmetry of the Mercedes logo.



Exercise 13.1.4. List six different symmetries of the Mercedes logo. (*Hint*)
 ◇

This is not the first time we've played with symmetries of a figure. At the end of Chapter 1, we saw that the complex sixth roots of unity determined a regular hexagon in the complex plane, and that complex multiplication and complex conjugation could be used to rotate or reflect the hexagon. Let us investigate the hexagon a bit further.

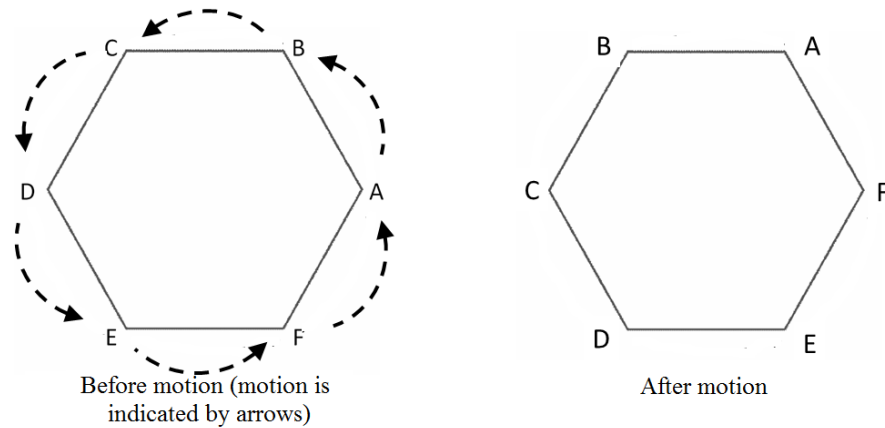


Figure 13.1.2. Hexagon and 60° rotation

Example 13.1.5. Figure 13.1.2 shows a 60° counterclockwise rotation of a regular hexagon where the vertices of the hexagon are labeled A, B, C, D, E, F . (Notice how the letters run *counterclockwise* around the hexagon. We will consistently follow this pattern. The reason is that in mathematical convention, a counterclockwise rotation is considered as *positive*, while a clockwise rotation is considered as *negative*.)

The rotation moves A to B , B to C , and so on. Now of course there are other points on our figure, namely all the points on the line segments between the vertices. But notice that if we account for where the vertices are moved to, then the movement of the line segments is automatically accounted for. If we know where A and B are moved to, we know exactly where \overline{AB} is. Therefore, our 60 degree rotation can be defined by the movement of the vertices $\{A, B, C, D, E, F\}$.

Now if we input a point from $\{A, B, C, D, E, F\}$, our rotation outputs a point from $\{A, B, C, D, E, F\}$. We have used this “input-output” language before, namely in the Functions chapter.

In fact, we can think of the 60 degree rotation as a function r_{60} from $\{A, B, C, D, E, F\} \rightarrow \{A, B, C, D, E, F\}$, where (using ordered pair notation)

$$r_{60} = \{(A, B), (B, C), (C, D), (D, E), (E, F), (F, A)\}.$$

Before leaving this example, we make note of a peculiarity that has tripped up many a student. If you compare the ‘before’ hexagon (shown at left in Figure 13.1.2) with the ‘after’ hexagon (shown at right), it appears that the original vertex B has been relabeled as A , C has been relabeled as B , and so on. However, according to our function we say that A goes to B , not B goes to A . This is because we’re thinking of symmetry as a *motion* rather than a relabeling. The fact that original vertex B is relabeled as A means that A moved to B , and not vice versa. So you should take care in future examples—whenever you see a vertex X being relabeled as Y this means that $Y \rightarrow X$, and not vice versa.²



Exercise 13.1.6.

- (a) Is r_{60} one-to-one? Explain why or why not.
- (b) Is r_{60} onto? Explain why or why not.
- (c) Is r_{60} a bijection? Explain why or why not.



Exercise 13.1.6 exemplifies a general property of symmetries:

Proposition 13.1.7. If S is the set of points that represent a figure, all symmetries of the figure are bijections from $S \rightarrow S$.

PROOF. Since the result of any symmetry acting on S must be all of S , then every point of S must be in the range of S . Thus any symmetry is onto.

²Actually, we could have defined symmetries as relabelings rather than motions, and all of the conclusions of this chapter would still hold. We’d just have to rewrite all of our tableaux to reflect this different convention.

Furthermore, the symmetry must map two different points to two different points, since the distance between points must be left unchanged by the symmetry. Hence any symmetry is one-to-one. So since any symmetry is both onto and one-to-one, it follows that any symmetry is a bijection. \square

Proposition 13.1.7 says that all symmetries are bijections, but the *converse* is not true: not all bijections are symmetries.

Exercise 13.1.8. Create a bijection from $\{A, B, C, D, E, F\} \rightarrow \{A, B, C, D, E, F\}$ that does not correspond to a symmetry of the regular hexagon in Figure 13.1.2. *Explain* why it is not a symmetry. \diamond

Example 13.1.9.

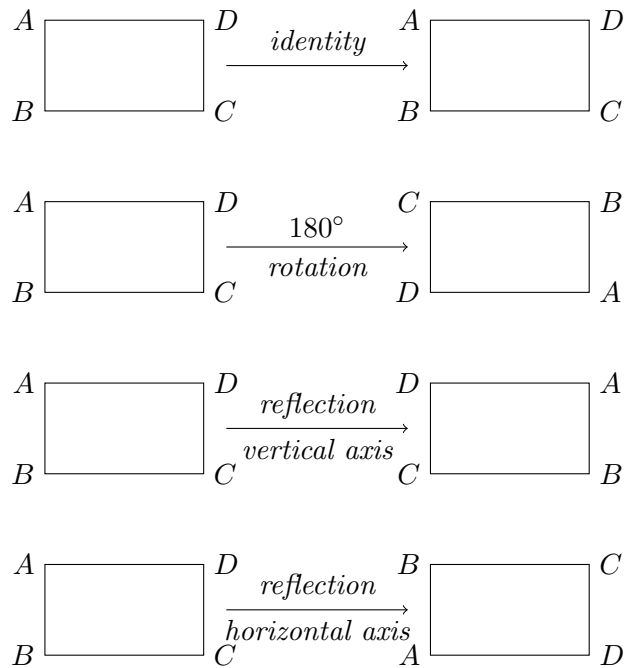


Figure 13.1.3. Symmetries of a rectangle



Figure 13.1.3 shows all symmetries of a rectangle.

Exercise 13.1.10.

- (a) Explain why a 90° rotation, a 270° rotation, or reflection across a diagonal are not symmetries of the rectangle $ABCD$.
- (b) What subcategory of rectangle would have a 90° rotation, 270° rotation, and a reflection across a diagonal as symmetries?
- (c) What rotation angle does the identity symmetry correspond to? (Give the easiest answer.)
- (d) Write each of the symmetries of a rectangle as a function (use either a table, ordered pairs, arrow diagram, etc.)

◇

13.2 Composition of symmetries

Since the symmetries of a figure are functions, we can do anything with symmetries that we can do with functions—including composition. That is, we can perform two symmetries on a figure back-to-back, and since they are both functions, by definition of function composition the result is a function. In fact, we saw in the Functions chapter that the composition of two bijections is a bijection. So the composition (or net motion) resulting from two symmetries is a bijection. But a bijection of a figure is not necessarily a symmetry, as we showed in Exercise 13.1.8 above. This raises the question: is the composition of two symmetries a symmetry? That is: if one symmetry is followed by another on a figure, is the net motion a symmetry? You will investigate this question in the following exercise.

Exercise 13.2.1. With reference to the symmetries of a rectangle in Example 13.1.9, let r_{180} be the 180° counterclockwise rotation and let s_v be the reflection across the vertical axis. (Note that reflection across the vertical axis is sometimes called “horizontal reflection,” since the figure “flips” from left to right. Admittedly this is confusing, but that’s what people call it so what can you do?)

- (a) Write the function r_{180} in ordered pair notation.
- (b) Write the function s_v in ordered pair notation.

- (c) Write the function $r_{180} \circ s_v$ in ordered pair notation. Is it a symmetry of the rectangle? If so, then which one?
- (d) Write the function $s_v \circ r_{180}$ in ordered pair notation. Is it a symmetry of the rectangle? If so, then which one?

◇

At this point let us introduce an alternative notation for symmetries that's easier to write. This notation is called **tableau form**, and for r_{180} it looks like the following:

$$r_{180} = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

To form these, we simply put the inputs of our function on the top row and their corresponding outputs on the bottom row.

Example 13.2.2. For example, since

$$s_v = \{(A, D), (B, C), (C, B), (D, A)\},$$

then the top row of the tableau for s_v would read, “ $ABCD$ ”, and the bottom row of the tableau would read, “ $DCBA$ ”. Hence

$$s_v = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}.$$

◆

Example 13.2.3. Suppose we wanted to find $r_{180} \circ s_v$ using the tableau forms for r_{180} and s_v above. That is

$$r_{180} \circ s_v = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} \circ \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = ?$$

To see how this works, let's “follow” each possible input (A, B, C, D) as we put it into the composition. Remember that the composition of functions works right to left; we are first reflecting the rectangle and then rotating it. So starting from the right,

- s_v takes $A \rightarrow D$, and r_{180} takes $D \rightarrow B$. Therefore $r_{180} \circ s_v$ takes $A \rightarrow B$; i.e. $(r_{180} \circ s_v)(A) = B$.
- s_v takes $B \rightarrow C$, and r_{180} takes $C \rightarrow A$; therefore $r_{180} \circ s_v$ takes $B \rightarrow A$
- s_v takes $C \rightarrow B$, and r_{180} takes $B \rightarrow D$; therefore $r_{180} \circ s_v$ takes $C \rightarrow D$
- s_v takes $D \rightarrow A$, and r_{180} takes $A \rightarrow C$; therefore $r_{180} \circ s_v$ takes $D \rightarrow C$

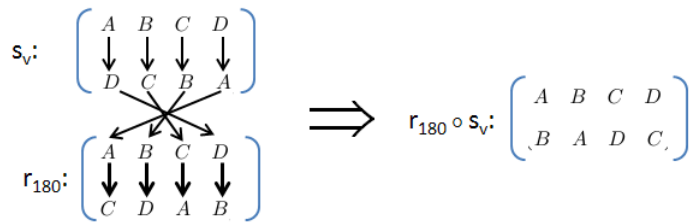


Figure 13.2.1. Composition of symmetries using tableaux.

Figure 13.2.1 shows this process using tableaux. If you think about it, it’s really just a variation on an arrow diagram.

In summary we have

$$r_{180} \circ s_v = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} \circ \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}$$



Exercise 13.2.4.

- Write s_h in tableau form, where s_h is reflection across the horizontal axis. (Note s_h is sometimes referred to as “vertical reflection,” since the two reflected halves are stacked on top of each other.)
- Does $r_{180} \circ s_v = s_h$?

- (c) Compute $s_h \circ s_v$. Is this a symmetry? If so, which one?
 (d) Compute $s_v \circ r_{180}$. Is this a symmetry? If so, which one?

◇

Exercises 13.2.4 and 13.2.1 seem to indicate that the composition of two symmetries of a figure is a symmetry of the figure. We can actually prove that this is always true.

Proposition 13.2.5. Suppose f and g are both symmetries of a figure. Then $f \circ g$ is itself a symmetry of the same figure.

PROOF. Recall that composition works from right to left. Since g is a symmetry, g takes the points of the figure and rearranges them so that the angles and distances of points in the figure are preserved. The symmetry f then takes the points of this preserved figure and moves them in such a way that the angles, and distances of points in the figure are preserved. Hence the net result of $f \circ g$ preserves angles and distances between points in the figure. Therefore by definition, $f \circ g$ is a symmetry of the figure. \square

Exercise 13.2.6. With reference to the hexagon in Figure 13.1.2, for the symmetries f and g in parts (a)-(d) below:

- (i) Write the symmetries f and g in tableau form.
 (ii) Compute $f \circ g$ and $g \circ f$, expressing your answers in tableau form.
 (iii) Describe the symmetries that correspond to $f \circ g$ and $g \circ f$, respectively.

Note id denotes the identity symmetry, that is the symmetry that leaves all points unchanged. Also, all rotations are counterclockwise.

- (a) $f = \text{rotation by } 240^\circ, g = \text{rotation by } 120^\circ$
 (b) $f = \text{id}, g = \text{rotation by } 120^\circ$
 (c) $f = \text{rotation by } 240^\circ, g = \text{reflection across the line } BE$
 (d) $f = \text{rotation by } 180^\circ, g = \text{reflection across the line } CF$

◇

| \circ | id | ρ_1 | ρ_2 | μ_1 | μ_2 | μ_3 |
|----------|----------|----------|----------|----------|----------|----------|
| id | id | ρ_1 | ρ_2 | μ_1 | μ_2 | μ_3 |
| ρ_1 | ρ_1 | ρ_2 | id | μ_3 | μ_1 | μ_2 |
| ρ_2 | ρ_2 | id | ρ_1 | μ_2 | μ_3 | μ_1 |
| μ_1 | μ_1 | μ_2 | μ_3 | id | ρ_1 | ρ_2 |
| μ_2 | μ_2 | μ_3 | μ_1 | ρ_2 | id | ρ_1 |
| μ_3 | μ_3 | μ_1 | μ_2 | ρ_1 | ρ_2 | id |

Table 13.1: Composition of the symmetries of an equilateral triangle

13.3 Do the symmetries of an object form a group?



With reference to the set of symmetries of a particular figure, Proposition 13.2.5 tells us that this set is closed under the operation of composition. Given this fact, the next natural inquiry is to see if this set of symmetries forms a group under composition. Let's look first at a particular example to see if it works.

Example 13.3.1. Figure 13.3.1 shows all the symmetries of an equilateral triangle: id is the identity ; ρ_1 is the 120° counterclockwise rotation; ρ_2 is the 240° counterclockwise rotation; μ_1 is the reflection across the median through A ; μ_2 is the reflection across the median through B ; and μ_3 is the reflection across the median through C . We remind the reader once again of the comment we made in Example 13.1.5: for example, in the symmetry ρ_1 the triangle's vertices A, B, C before the motion appear to be relabeled as C, A, B respectively, which means that $C \rightarrow A$, $A \rightarrow B$, and $B \rightarrow C$ rather than vice-versa.



Table 13.1 displays all possible compositions of the symmetries shown in Figure 13.3.1. The table is arranged like a multiplication table: for example, the table entry in the row marked " ρ_1 " and the column marked " μ_1 " corresponds to the composition $\rho_1 \circ \mu_1$. From now on we will refer to all such tables as **Cayley tables**, regardless of the operation being represented (addition, multiplication, composition, ...)

Remark 13.3.2. NOTE it is very easy to get mixed up with Cayley tables for the composition operation. When *looking up* the value of $f \circ g$, you use

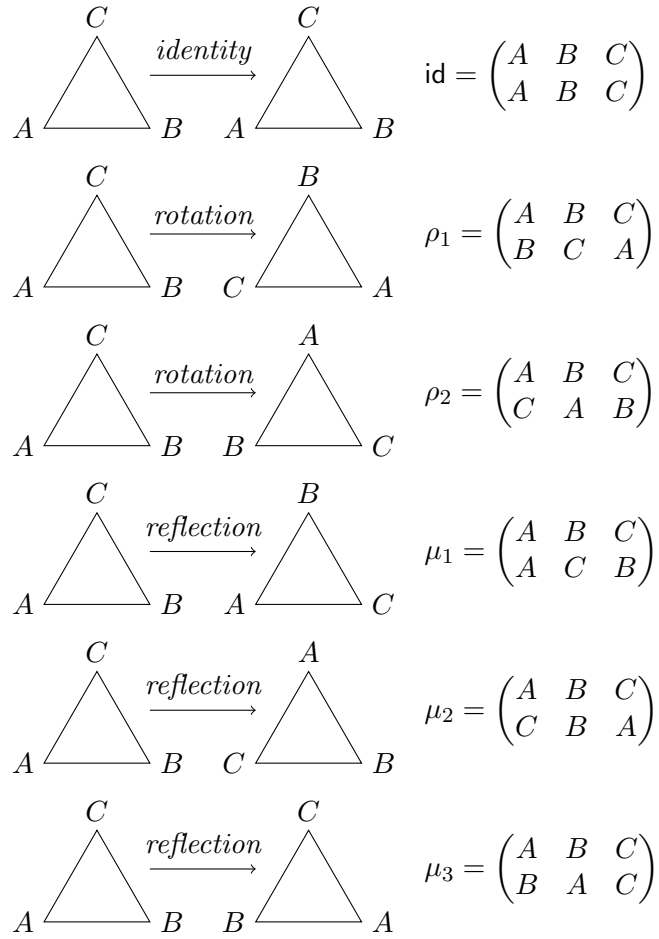


Figure 13.3.1. Symmetries of an Equilateral Triangle

the row headings for f and the column headings for g , but when *computing* $f \circ g$, it is g that is applied first and then f . \triangle

Exercise 13.3.3. Verify the following entries in Table 13.1 by (i) writing the symmetries in tableau form and (ii) computing the composition directly.

- (a) Row 2, column 4
- (b) Row 4, column 2
- (c) Row 3, column 6
- (d) Row 6, column 3

\diamond

Exercise 13.3.4. Use Table 13.1 to answer the following questions.

- (a) Explain why Table 13.1 shows that id satisfies the definition of an identity element.
- (b) Does every element in S have an inverse? List the inverses for each symmetry that has an inverse.
- (c) Explain why Table 13.1 shows that composition is *not* commutative.

\diamond

So far so good. The composition operation on S has closure, an identity, and inverses for each element. There is one more group property left to check – the associative property. It is difficult to check this property on the Cayley table of S ; we would have to prove it for all 3-symmetry combinations in S , which would be a bit exhausting.³ However, luckily we can prove the symmetries of any figure are associative in general.

Proposition 13.3.5. The set of symmetries S of any figure under composition is associative.

³In mathematics, there is a type of proof called “proof by exhaustion,” but this is typically a last resort. One famous mathematician (George Polya) once said, “Mathematics is being lazy. Mathematics is letting the principles do the work for you so that you do not have to do the work for yourself.”

PROOF. By definition, we know any symmetry of a figure is a function. From the Functions chapter, we know that composition of functions is associative. Therefore for any three symmetries $s_1, s_2, s_3 \in S$, by the associative property of functions,

$$(s_1 \circ s_2) \circ s_3 = s_1 \circ (s_2 \circ s_3).$$

Therefore S is associative under composition. □

Tada! The set of symmetries of an equilateral triangle are indeed a group under function composition.

We've managed to prove this for one example; what about for the set of symmetries of any figure? Could we prove the set of symmetries of any figure are a group under composition? We've already proved the closure and associative properties hold for any figure (Propositions 13.3.5 and 13.2.5). Now what about the identity and existence of inverses? We could create Cayley tables for the infinite number of figures, but we have better things to do. So let's prove these properties generally.

Proposition 13.3.6. The set of symmetries S of any figure has an identity.

PROOF. By the definition of a symmetry, the "non-movement" of a figure is a symmetry: it corresponds to the identity function id . Then for any symmetry $s \in S$, using results from the Functions chapter we have

$$\text{id} \circ s = s \circ \text{id} = s$$

So by the definition of identity, id is the identity of S . □

Proposition 13.3.7. All elements of the set S of symmetries of any figure have inverses.

PROOF. Given a symmetry $s \in S$, by definition s is a bijection. In the Functions chapter, we showed that every bijection has an inverse s^{-1} . It remains to show that s^{-1} is itself a symmetry. This means that we have to show:

- (i) s^{-1} leaves distances unchanged between points in the figure;
- (ii) s^{-1} leaves angles unchanged between points in the figure;

(iii) s^{-1} leaves the appearance of the figure unchanged.

These three items are proved as follows:

(i) This proof is similar to (ii), and we leave it as an exercise.

(ii) We show that s^{-1} leaves angles between points unchanged as follows:

- Choose any three points A, B, C in the figure, and let $A' = s^{-1}(A), B' = s^{-1}(B), C' = s^{-1}(C)$.
- By the definition of inverse, it follows that $s(A') = A, s(B') = B, s(C') = C$.
- Since s is a symmetry, it follows that $\angle A'B'C' = \angle ABC$.
- Since A, B, C were arbitrary points in the figure, we have shown that s^{-1} leaves angles between points unchanged.

(iii) In the Functions chapter, we showed that s^{-1} is also a bijection. Hence it leaves the appearance of the figure unchanged.

□

Exercise 13.3.8. Write out the proof of Proposition 13.3.7 part (i). (*Hint*)

◇

And finally, as the grand finale for this series of propositions, we have:

Proposition 13.3.9. The set S of symmetries of any figure forms a group.

Exercise 13.3.10. Prove Proposition 13.3.9 (make use of the propositions that we've proved previously.) ◇

Exercise 13.3.11.

(a) Write the Cayley table for the symmetries of a rectangle.

(b) List the inverses of each symmetry of the symmetries of a rectangle.

**Exercise 13.3.12.**

- (a) Describe all symmetries of a square (For example, “reflection about the vertical axis ” describes one symmetry: give similar descriptions of all symmetries of the square. For rotations, use counterclockwise rotations rather than clockwise: it’s the mathy way of doing rotations.)
- (b) Label the square’s vertices as A, B, C, D , and write down each symmetry in tableau form. As in Figure 13.3.1, denote each symmetry by a variable (you may use ρ_1, ρ_2, \dots for the rotations and μ_1, μ_2, \dots for the reflections).
- (c) Write the Cayley table for the symmetries of a square.
- (d) For each symmetry of a square, list its inverse.

**Exercise 13.3.13.** With reference to the logos in Figure 13.3.2:

- (a) For which logos do the set of symmetries include all symmetries of the equilateral triangle? (Note: there are at least two!)
- (b) For which logos do the set of symmetries include all symmetries of the rectangle?
- (c) For which logos do the set of symmetries include all symmetries of the hexagon?
- (d) Which logos have set of symmetries which are proper subsets of the set of all symmetries as the rectangle?
- (e) Give two logos such that all symmetries of the first logo are also symmetries of the second logo.
- (f) Which logos have no symmetries except for the identity?



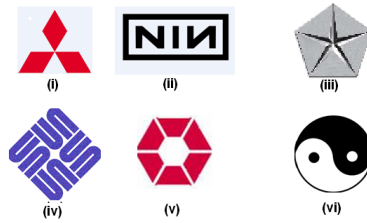


Figure 13.3.2. Logos for Exercise 13.3.13

13.4 The dihedral groups

We have investigated the symmetries of equilateral triangle, square, and regular hexagon. But what about other regular polygons: heptagon, octagon, nonagon, decagon, and so on? (Recall from geometry that a *regular polygon* has all sides equal and all angles equal.) In this section, we will take a general look at the symmetries of n -sided regular polygons.

We already know from Exercise 13.3.10 that the symmetries of any n -sided regular polygon form a group. We define the *n th dihedral group* to be the group of symmetries of a regular n -gon. We will denote this group by D_n .

Let us try to count the number of elements of D_n . We can number the vertices of a regular n -gon by $1, 2, \dots, n$ (Figure 13.4.1). Any symmetry will move the n -gon so that each vertex is replaced by another vertex. Notice that any vertex can replace the first vertex: so there are exactly n choices to replace the first vertex. Suppose we replace vertex 1 by vertex k : then vertex 2 must be replaced either by vertex $k + 1$ or by vertex $k - 1$, because these are the only vertices next to vertex k . So for each of the n choices for replacing vertex 1, there are two choices for replacing vertex 2: which makes $2n$ possible choices altogether. If you think about it, you'll see that once the replacements for vertices 1 and 2 are determined, the entire symmetry is fixed (again, because vertices must remain next to each other). We summarize our conclusion in the following proposition.

Proposition 13.4.1. The dihedral group, D_n , is a group of order $2n$.

Let us try to characterize these $2n$ elements of the dihedral group D_n .

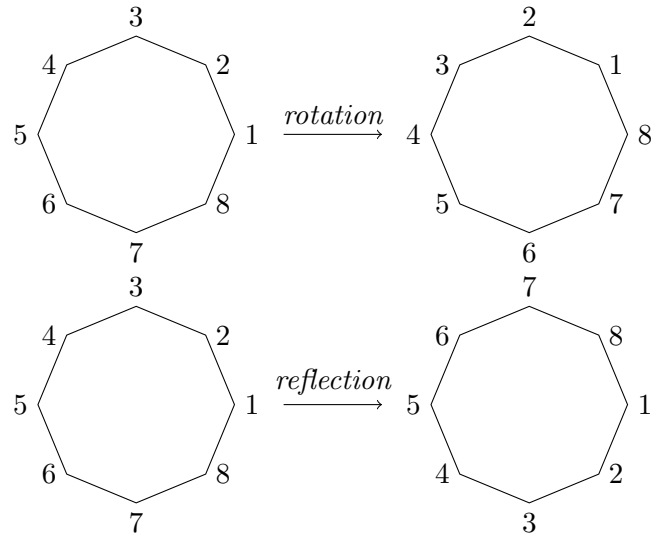


Figure 13.4.1. Rotations and reflections of a regular n -gon

First, we know that the elements of the dihedral group includes n rotations:

$$\text{id}, \frac{360^\circ}{n}, 2 \cdot \frac{360^\circ}{n}, \dots, (n-1) \cdot \frac{360^\circ}{n}.$$

We will denote the rotation $360^\circ/n$ by r . Notice that:

- $r \circ r = \text{rotation by } 2 \cdot \frac{360^\circ}{n}$
- $r \circ r \circ r = \text{rotation by } 3 \cdot \frac{360^\circ}{n}$

We can generalize this pattern by writing:

$$r^k = \text{rotation by } k \cdot \frac{360^\circ}{n} \quad (k = 1, 2, 3, \dots),$$

where the notation r^k means that we compose r with itself k times: $r \circ r \dots \circ r$. We can also continue this pattern with $k = 0$ and write:

$$r^0 = \text{rotation by } 0 \cdot \frac{360^\circ}{n} = \text{id}.$$

We also have

$$r^n = \text{rotation by } n \cdot \frac{360^\circ}{n} = \text{rotation by } 360^\circ = \text{id},$$

since rotation by 360 degrees is tantamount to not moving the figure at all.

Exercise 13.4.2.

- (a) Using the above definition of r^k , show that $r^k \circ r^m = r^{m+k}$ for any natural numbers k, m .
- (b) Show that $r^k \circ r^{n-k} = r^{n-k} \circ r^k = \text{id}$ for $1 < k < n$.
- (c) What does (b) tell us about the inverse of r^k ?

◇

From the above discussion, it should be clear that the n rotations in D_n can be expressed as:

$$\text{id}, r, r^2, \dots, r^{n-1},$$

where we have included id since it is “rotation by 0 degrees” (as mentioned above, we could also write id as r^0). This gives us a nice way of characterizing the rotations in D_n . But until now we don’t have a nice way of writing the reflections. We’ll take care of that now!

We have labeled the vertices of the n -gon as $1, 2, \dots, n$. In the following discussion, we will use the letter s to denote the reflection that leaves the vertex labeled 1 *fixed*, that is, $s(1) = 1$.⁴ Another way of saying the same thing is: the vertex labeled 1 is “fixed by” s .

Exercise 13.4.3.

- (a) Write the reflection s for the pentagon in tableau form.
- (b) How many vertices are fixed by s ? What are they?
- (c) What is s^2 ? (Recall that s^2 means the same as $s \circ s$.)

◇

Exercise 13.4.4.

- (a) Write the reflection s for the octagon in tableau form.

⁴In math books you may also find the term “invariant” instead of “fixed”.

- (b) How many vertices are fixed by s ? What are they?
 (c) What is s^2 ?

◇

By generalizing the arguments used in the preceding exercises, it is possible to prove for any n that:

$$s^2 = \text{id}.$$

Now we have already shown there are n distinct rotations. Suppose we follow each of these rotations by the reflection s : that is, consider the set

$$S \equiv \{s \circ \text{id}, s \circ r, s \circ r^2, \dots, s \circ r^{n-1}\}$$

It appears that S has n elements: but are these elements distinct? The following exercise provides an answer:

Exercise 13.4.5. Prove the following proposition by filling in the blanks:

Proposition. If $0 < p, q < n$ and $p \neq q$, then $s \circ r^p$ and $s \circ r^q$ are distinct elements of D_n : that is, $s \circ r^p \neq s \circ r^q$.

PROOF.

- The proof is by contradiction. Given $0 < p, q < n$ and $p \neq q$, and suppose that $s \circ r^p \underline{< 1 >} s \circ r^q$
- Compose both sides of the equation with s , and obtain the equation: $s \circ (s \circ r^p) = \underline{< 2 >}$.
- By the associative property of composition, this can be rewritten: $(s \circ s) \circ \underline{< 3 >} = \underline{< 4 >}$
- Since $s \circ s = \underline{< 5 >}$, this can be rewritten: $\text{id} \circ \underline{< 6 >} = \underline{< 7 >}$.
- Since id is a group identity, we have: $r^p = \underline{< 8 >}$.
- But we have already shown that r^p and r^q are distinct symmetries if $0 < p, q < n$ and $p \neq q$. This is a contradiction.

- Therefore we conclude that our supposition was incorrect, and $s \circ r^p \underline{< 9 >} s \circ r^q$. This completes the proof.

□

◇

Exercise 13.4.6. Prove the following proposition:

Proposition If $0 < q < n$ then s and $s \circ r^q$ are distinct elements of D_n : that is, $s \neq s \circ r^q$. (*Hint*) ◇

Exercise 13.4.7. Fill in the blanks to prove that given any integers p, q with $0 < p, q < n$, $s \circ r^p \neq r^q$:

- The proof is by contradiction: so given integers p, q with $0 < p, q < n$, we suppose < 1 >.
- By multiplying both sides on the *right* by r^{n-p} , we obtain $s \circ r^p \circ$
< 2 > = $r^q \circ$ < 3 >
- By associativity, we have $s \circ$ < 4 > = < 5 >
- Using the fact that < 6 > = id, we obtain $s =$ < 7 >
- The left side of this equation is a reflection, and the right side is a < 8 >, which is a contradiction.
- This contradiction implies that our supposition is incorrect, so given integers p, q with $0 < p, q < n$, we conclude < 9 >.

◇

The preceding exercises have shown that the rotations and $\{s, s \circ r, s \circ r^2, \dots, s \circ r^{n-1}\}$ are all distinct elements of D_n . Since there are $2n$ of these symmetries altogether, and since D_n has $2n$ elements, we have proved the following:

Proposition 13.4.8. The $2n$ elements of D_n may be listed as:

$$\{\text{id}, r, r^2, \dots, r^{n-1}, s, s \circ r, s \circ r^2, \dots, s \circ r^{n-1}\},$$

or alternatively as

$$\{s^j \circ r^k, (j = 0, 1; k = 0, 1, \dots, n - 1)\},$$

where we are using the notation: $s^0 = r^0 = \text{id}$.

There is actually another way to characterize the elements of D_n , as we shall see in the following exercises:

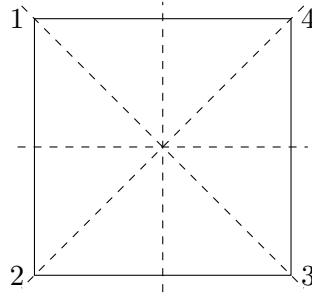


Figure 13.4.2. Lines of reflection for a square (D_4)

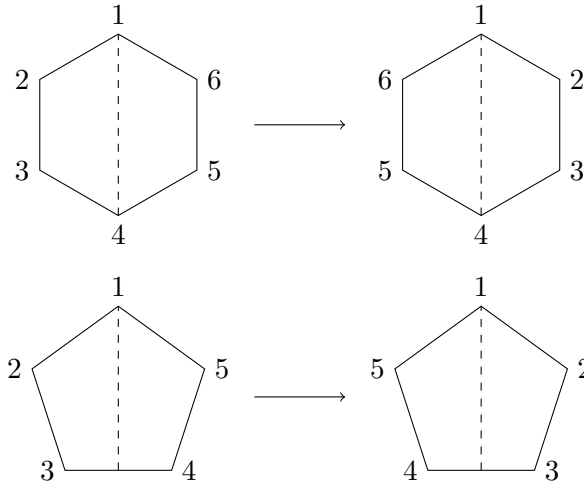


Figure 13.4.3. Types of reflections of a regular n -gon

Exercise 13.4.9.

- (a) List four reflections of the square in tableau form. (**Hint**)
- (b) Let μ be any of the reflections in part (a). What is $\mu \circ \mu$?
- (c) How many reflections have no fixed vertices?
- (d) How many reflections fix exactly one vertex?
- (e) How many reflections fix exactly two vertices?

◇

Exercise 13.4.10.

- (a) List five reflections of the pentagon in tableau form. (**Hint**)
- (b) Let μ be any of the reflections in part (a). What is $\mu \circ \mu$?
- (c) How many reflections have no fixed vertices?
- (d) How many reflections fix exactly one vertex?
- (e) How many reflections fix exactly two vertices?

◇

Exercise 13.4.11.

- (a) List six reflections of the hexagon in tableau form. (**Hint**)
- (b) Let μ be any of the reflections in part (a). What is $\mu \circ \mu$?
- (c) How many reflections have no fixed vertices?
- (d) How many reflections fix exactly one vertex?
- (e) How many reflections fix exactly two vertices?

◇

Exercise 13.4.12.

- (a) Complete the second row of the following tableau that represents the reflection of the nonagon that fixes vertex 4:

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ -- & -- & -- & 4 & -- & -- & -- & -- & -- \end{pmatrix}$$

- (b) Complete the second row of the following tableau that represents the reflection of the 10-gon that fixes vertex 4:

$$\mu_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ -- & -- & -- & 4 & -- & -- & -- & -- & -- & -- \end{pmatrix}$$

- (c) Complete the second row of the following tableau that represents the reflection of the 10-gon that exchanges vertices 6 and 7:

$$\mu_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ -- & -- & -- & -- & -- & 7 & 6 & -- & -- & -- \end{pmatrix}$$

- (d) What is $\mu_1 \circ \mu_1$? What is $\mu_2 \circ \mu_2$? What is $\mu_3 \circ \mu_3$?

◇

The preceding exercises are generalized to arbitrary n in the following proposition. Although we do not give a complete proof, it is reasonable that we can generalize Exercise 13.4.10 to all *odd* n -gons, and we can generalize Exercise 13.4.11 to all *even* n -gons:

Proposition 13.4.13.

- The dihedral group D_n contains n distinct reflections (in addition to n distinct rotations);
- For any reflection $\mu \in D_n$, we have $\mu \circ \mu = \text{id}$.

Exercise 13.4.14.

- (a) Based on results we've shown, prove that $s \circ r^p$ must be a reflection, for $0 < p < n$.

- (b) Using part (a) and other results we've shown, show that $(s \circ r^p) \circ (s \circ r^p) = \text{id}$. (*Hint*)
- (c) Using part (b) and composing on the left by $r^{n-p} \circ s$, show that $r^{n-p} \circ s = s \circ r^p$ for $0 < p < n$.

◇

All of our results on dihedral groups can now be summarized in the following proposition:

Proposition 13.4.15. Every element of the group D_n , $n \geq 3$, consists of all compositions of the two elements r and s , satisfying the relations:

- (a) $r^n = \text{id}$
- (b) $s^2 = \text{id}$
- (c) $r^p \circ s = s \circ r^{n-p}$ for $0 < p < n$.

Proposition 13.4.15 enables us to compute any composition of elements of D_n directly, without the need of tableau form:

Example 13.4.16. In D_5 , to compute $(s \circ r^3) \circ (s \circ r^4)$ we have (using Proposition 13.4.15 and associativity):

$$\begin{aligned}
 (s \circ r^3) \circ (s \circ r^4) &= s \circ (r^3 \circ s) \circ r^4 \text{ by associativity} \\
 &= s \circ (s \circ r^2) \circ r^4 \text{ by Prop. 13.4.15(c)} \\
 &= (s \circ s) \circ r \circ r^5 \text{ by associativity} \\
 &= \text{id} \circ r \circ \text{id} \text{ by Prop. 13.4.15(a) and (b)} \\
 &= r
 \end{aligned}$$

◆

In fact, following the method of Example 13.4.16 it is possible to derive a general formula for the composition of two reflections. Such a formula may be very useful in certain situations: for instance, in the following exercises.

Exercise 13.4.17. Using only associativity and Proposition 13.4.15, complete the entire Cayley table for D_4 . Remember, there is a row and a column for each element of D_4 . List the elements as indicated in Proposition 13.4.8. You don't need to show all your computations. (*But don't use tableau form—no cheating!*) \diamond

Exercise 13.4.18. Using only associativity and Proposition 13.4.15, complete the entire Cayley table for D_5 . You don't need to show all your computations. (*But don't use tableau form—no cheating!*) \diamond

Exercise 13.4.19. Consider an 8-gon with vertices labeled counterclockwise as $1, 2, \dots, 8$. Let s be the reflection that leaves vertex 1 fixed, and let r be counterclockwise rotation by $2\pi/8$. Using only associativity and Proposition 13.4.15, compute the following. Express your answers in the form $s^m r^n$, where m, n are positive integers.

- (a) $r^3 s r^3$
- (b) $s r^3 s$
- (c) $r^m s r^m$, where $0 \leq m < 8$.
- (d) $s r^m s$, where $0 \leq m < 8$.
- (e) $r s r^2 s r^3 s r^4$
- (f) $s r^4 s r^4$

 \diamond

Exercise 13.4.20. For each of the computations in Exercise 13.4.19, determine whether the result is a rotation or reflection. If the result is a rotation, give the angle of rotation; and if it's a reflection, give the line of reflection. For example, the symmetry sr is a reflection about the line which passes through the midpoints of segments $\overline{12}$ and $\overline{56}$. \diamond

Exercise 13.4.21.

- (a) In the group D_n , let r be counterclockwise rotation by $2\pi/n$ and let s be the reflection that leaves vertex 1 fixed. We have shown that $r^k s = s r^{n-k}$. Let μ be an arbitrary reflection in D_n . Show that a similar equation holds for r and μ : namely, $r^k \mu = \mu r^{n-k}$. (*Hint*: we've shown that μ can be written as $s r^m$ for some integer m .)
- (b) Let ρ be an arbitrary rotation in D_n , and let μ be an arbitrary reflection in D_n . Show that $\rho \mu = \mu \rho^{-1}$. (*Hint*: Look at the hint for (a), and consider that ρ can be written in terms of r .)

◇

Exercise 13.4.22.

- (a) In the group D_n , let r be counterclockwise rotation by $2\pi/n$ and let s be the reflection that leaves vertex 1 fixed. Is $r^4 s^3 r^2 s$ a reflection or rotation? *Prove* your answer.
- (b) Let ρ be an arbitrary rotation in D_n , and let μ be an arbitrary reflection in D_n . Is $\rho^4 \mu^3 \rho^2 \mu$ a reflection or rotation? *Prove* your answer.
- (c) Let k, ℓ, m, n be integers. Given the symmetry $\rho^k s^\ell \rho^m s^n$, under what conditions is this symmetry a reflection? Under what conditions is this symmetry a rotation? *Prove* your answers.

◇

13.5 For further investigation

In this chapter, we have looked at the groups involved with symmetries of plane figures. But really, there is no need to restrict ourselves to two dimensions. Three-dimensional regular figures (such as the tetrahedron, cube, icosahedron, and dodecahedron) also have symmetry groups associated with them. We will say more about the symmetries of regular polyhedra in Chapter 23.

Neither do we need to restrict ourselves to symmetries of objects. The symmetries of *patterns* also play an important role in art and architecture. For instance, every possible regular repeating pattern that can be put on

wallpaper (or used as floor tiling) is associated with a symmetry group. It turns out that there are exactly 17 of these symmetry groups: they are called the *wallpaper groups*. For an excellent elementary reference on this subject, I highly recommend “17 Plane Symmetry Groups” by Anna Nelson, Holli Newman, and Molly Shipley, available on the web (as of January 2014) at <http://caicedoteaching.files.wordpress.com/2012/05/nelson-newman-shipley.pdf>.

In physics, symmetry groups are used to describe the regular three-dimensional patterns associated with crystals. Many references for the crystallographic groups can also be found on the web: one I recommend is “Crystallographic Point Groups (short review)” by Mois I. Aroyo, available on the web at: http://www.crystallography.fr/mathcryst/pdf/uberlandia/Aroyo_Point.pdf.

13.6 An unexplained miracle

It’s good for us to step back for a moment and take stock of what we’ve accomplished so far. We’ll begin with some exercises.

Exercise 13.6.1.

- (a) Give the Cayley table for the integers mod 4 under addition.
- (b) Give the Cayley table for the four rotations of the square (4-sided polygon). You may use r to denote rotation by 90 degrees, so that the rotations will be $\{\text{id}, r, r^2, r^3\}$.
- (c) Give the Cayley table for the four complex 4th roots of unity. You may use z to denote $\text{cis}(\pi/2)$ so that the roots will be $\{1, z, z^2, z^3\}$.
- (d) Do you see any connection between your answers to (a), (b), and (c) above?

◇

Exercise 13.6.1 show a deep connection between three extremely diverse concepts that arose from three totally different fields of study:

- Arithmetic mod n , which first arose from the study of the natural numbers and their divisibility properties;

- The n 'th complex roots of unity, a concept that arose from the study of roots of polynomials.
- The rotations of a regular n -gon, which is a purely geometrical phenomenon.

We express the amazing similarity between these three diverse concepts by saying that they are all described by the “same” group. (The technical term for this is “isomorphism”: we will study this concept in detail in Chapter 20.)

Take a moment to appreciate how incredible this is. How is it that three concepts with totally different backgrounds and completely different applications end up being described in exactly the same way?

But the wonders do not stop there. It turns out that an infinite version of this same group is an important part of the so-called Standard Model of quantum physics, that is used to explain the existence of particles such as electrons, protons, and neutrons. How is it that a mathematical structure introduced by an 18th century mathematician ⁵ to study integer division could end up influencing the theory of elementary particles that were not even dreamed of in the 18th century?

This mystical unity of description across widely different phenomena says something very profound about the universe. Galileo ⁶ expressed it this way: “Mathematics is the language with which God has written the universe.” When Galileo said this, his mathematics consisted of little more than what today we would call “high school algebra” – he had not an inkling of abstract algebra. But what Galileo expressed based on his limited mathematics has turned been fulfilled with a vengeance by abstract algebra.

Physicist Eugene Paul Wigner⁷ won the 1963 Nobel Prize in Physics, in part because of his application of the theory of groups to quantum physics. In 1960 Wigner wrote a famous paper called “the Unreasonable Effectiveness of Mathematics in the Natural Sciences,” ⁸ in which he states: “The miracle of the appropriateness of the language of mathematics for the formulation of the laws of physics is a wonderful gift which we neither understand nor

⁵This mathematician was Leonhard Euler (1707-1783). The integers mod n were further developed by Carl Friedrich Gauss (1777-1855).

⁶Galileo Galilei, Italian physicist (1564-1642), whose work on the motion of objects was foundational to the later work of Isaac Newton.

⁷1902-1995

⁸The paper can be found at: <http://www.dartmouth.edu/~matc/MathDrama/reading/Wigner.html>

deserve.” To this day, apparently no physicist or mathematician has yet offered a satisfactory explanation for Wigner’s “miracle”.

13.7 Hints for “Symmetries of Plane Figures” exercises

Exercise 13.1.4: The rearrangement that doesn't move anything is still considered to be a symmetry: for obvious reasons, it is called the *identity*.

Exercise 13.3.8: The proof is very similar to part (ii) of the same proposition.

Exercise 13.4.6: The proof is very similar to the previous proof.

Exercise 13.4.9: Look at Figure 13.4.2 for some ideas.

Exercise 13.4.10(a): Look at Figure 13.4.3 for some ideas.

Exercise 13.4.11(a): Look at Figure 13.4.3 for some ideas.

Exercise 13.4.14(b): If μ is a reflection, then what is $\mu \circ \mu$?

Permutations

”For the real environment is altogether too big, too complex, and too fleeting for direct acquaintance. We are not equipped to deal with so much subtlety, so much variety, so many permutations and combinations. And although we have to act in that environment, we have to reconstruct it on a simpler model before we can manage it.”

(Source: Walter Lippmann, Pulitzer prize-winning journalist)

We mentioned at the beginning of the “Functions” chapter that we would be interested in functions on finite sets. In this chapter we will investigate the gory details of bijections (functions that are one-to-one and onto) whose domain and range are the same finite set. Until now we have looked at functions as a process, a machine; mappings that take set elements to other set elements. In this chapter, we will begin to consider functions as things, objects; as set elements *in their own right*. This new point of view will culminate in the realization that *all* finite groups are in some sense just groups of functions. You may not understand this yet, but don’t worry—you will by the end of the chapter!

Thanks to Tom Judson for material used in this chapter.

14.1 Introduction to permutations

In Chapter 13 we saw that all symmetries are bijections whose domain and codomain were the same. Thus symmetries are special cases of *permutations*, which are defined mathematically as follows.

Definition 14.1.1. A bijection whose domain and codomain are equal is called a *permutation*. The set of all bijections from a finite set X to itself is called the *set of permutations on X* and is denoted as S_X . \triangle

Example 14.1.2. Let us recall for a moment the equilateral triangle $\triangle ABC$ from the Symmetries chapter. Let T be the set of vertices of $\triangle ABC$; i.e. $T = \{A, B, C\}$. We may list the permutations of T as follows. For input A , we have 3 possible outputs; then for B we would have two possible outputs (to keep the one-to-one property of each combination); and finally for C only one possible output. Therefore there are $3 \cdot 2 \cdot 1 = 6$ permutations of T . Below are the six permutations in S_T :

$$\begin{array}{ccc} \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} & \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} & \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \\ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} & \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} & \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} \end{array}$$

◆

Which of these permutations are symmetries of the equilateral triangle? In the Symmetries chapter we saw that they all are: so in this case the set of symmetries on T is equal to S_T .

Now suppose instead we label the vertices of an *isosceles* triangle as A, B, C , and let T represent these vertices. In this case, S_T is the same as before: it doesn't matter what arrangement or position the vertices are in, or even if A, B , and C are vertices at all. The permutations depend only on the set T , and are oblivious to whether or not they correspond to the vertices of some figure.

But what about the symmetries of an isosceles triangle? It turns out that an isosceles triangle has only two symmetries (see exercise below). So the set of symmetries on T is a subset of S_T , but not the whole set.

Exercise 14.1.3. Suppose that the two congruent sides of triangle ABC are \overline{AB} and \overline{BC} . Give the two symmetries, in tableau form. \diamond

Exercise 14.1.4. Suppose T is used to represent any three-sided figure. Which permutation(s) do(es) the set of symmetries of T always contain? \diamond

Exercise 14.1.5. Suppose $X = \{A, B, C, D\}$.

- (a) How many permutations are there on X ?
- (b) List S_X .
- (c) List the elements in S_X that are not symmetries of the square.
- (d) What additional elements in S_X are not symmetries of the rectangle?

◇

Actually, *any* symmetry is a permutation, since a symmetry is by definition a bijection from a finite set of points to itself. But as we've seen in Exercises 14.1.3, 14.1.4, 14.1.5 (as well as Exercise 13.1.8 from the Symmetries chapter), *not* all permutations (bijections) are symmetries. Given a set X that represents a figure, the set of symmetries from $X \rightarrow X$ is therefore a subset of S_X .

14.2 Permutation groups and other generalizations

We saw in the Symmetries chapter that the set of symmetries of any figure form a group under the operation of function composition. Since we've already seen that permutations are closely related to symmetries, this naturally leads to the question: is S_X a group under function composition? Fortunately, this time the answer is easier to prove.

Proposition 14.2.1. Given any set X , S_X is a group under function composition.

PROOF.

- First then, if $f, g \in S_X$, then $f \circ g$ would be, by definition of composition, a function from $X \rightarrow X$. Further, since it is a composition of two bijections, $f \circ g$ would be a bijection (proved in Functions chapter). Therefore by definition $f \circ g$ is permutation from $X \rightarrow X$. In other words $f \circ g \in S_X$. So S_X is closed under function composition.
- Second, the identity of S_X is just the permutation that sends every element of X to itself (We will call this permutation id , just like we did with symmetries.).

- Third, if $f \in S_X$, then by definition f is a bijection; hence from the Inverse section of the Functions chapter we know f has an inverse f^{-1} from $X \rightarrow X$ that is also a bijection. Hence $f^{-1} \in S_X$. Therefore every permutation in S_X has an inverse.
- Finally, composition of functions is associative, which makes the group operation associative.

Hence S_X is a group under function composition. □

14.2.1 The symmetric group on n numbers

We can label the vertices of a triangle as A, B, C or $1, 2, 3$ or *apple, pear, cherry* or whatever, without changing the triangle. No matter how we label the triangle, the symmetries of the triangle will be the "same" in some sense (although we write them down differently).

Since symmetries are special cases of permutations, this motivates us to investigate the effect of relabeling on permutations in general.

For starters, we'll look at a simple example. Let $X = \{A, B, C, D\}$ and $Y = \{1, 2, 3, 4\}$. Suppose

$$\mu = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}; \quad \sigma = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}$$

and

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}; \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Is $\mu = \tau$? Technically no, because their domain/codomains are different, yet we can clearly see that they are somehow equivalent. But how do we express this equivalence?

Suppose we start with the tableau for μ . We cross out every 'A' in the tableau and replace with '1'. Similarly, we replace B, C, D with $2, 3, 4$ respectively. Then what we end up with is exactly τ . In other words, performing a "face-lift" on μ gives τ . Therefore μ and τ are equivalent, as are σ and ρ .

Exercise 14.2.2.

- (a) Write $\mu \circ \sigma$ in tableau form.
- (b) Write $\tau \circ \rho$ in tableau form.
- (c) Is $\mu \circ \sigma$ equivalent to $\tau \circ \rho$? *Explain* your answer.
- (d) Is $\sigma \circ \mu$ equivalent to $\rho \circ \tau$? *Explain* your answer.

◇

Let's summarize our findings so far:

- The sets S_X and S_Y are equivalent in the following sense: for each element of S_X we can find an equivalent element of S_Y by replacing A, B, C, D with $1, 2, 3, 4$.
- Further, in the exercises we saw that the composition of two particular elements in S_X is equivalent to the composition of the two equivalent elements in S_Y . Although we've only shown this for two particular examples, it makes sense that the same thing would work no matter which two elements in S_X that we choose (after all, all we're doing is replacing letters with numbers—and we're always replacing the same letter with the same number). So we can say that composition acts the “same” on both sets.

So far we have only looked at sets with four elements. Now it's time to generalize these results to sets of any size. First, some notation:

Notation 14.2.3. The *order of a set* Y is the number of elements of Y , and is written as $|Y|$.¹ △

Now let $X = \{1, 2, \dots, n\}$, and consider any set Y with $|Y| = n$. We could do a similar “face-lifting” as above to show that S_X is equivalent to S_Y . So the group S_X is equivalent to the permutations of *any* set of n elements.

Notation 14.2.4. Let $X = \{1, 2, \dots, n\}$. Instead of writing S_X , we write S_n . S_n is called the *symmetric group* on n numbers. △

¹You're probably used to seeing $|\dots|$ as representing absolute value. Of course a set is not a number, so it has no absolute value. We use $|Y|$ to denote order because it's a measure of the *size* of set Y , just as the absolute value of a number is the “size” of the number.

14.2.2 Isomorphic groups

In Section 13.6 we compared the groups \mathbb{Z}_n , the n rotations of a regular n -gon, and the n^{th} roots of unity. We saw that, as long as you made a suitable pairing (bijection) between the elements of any two of these sets, then their Cayley tables were exactly the same.

We've just seen the very same thing for S_n . If $|X| = |Y| = n$ and we replace each of the elements in X with a corresponding element in Y , we concluded that the composition of *any* two elements in S_X is equivalent to the composition of the two equivalent elements in S_Y . That's exactly the same thing as saying that the Cayley table entries are equivalent between the two groups.

This "equivalence of groups" is one of the premier concepts in abstract algebra, almost as important as the concept of a group itself. When two groups are equivalent like this, we say that they are *isomorphic groups*; we also say that the bijection that causes the groups to be equivalent is an *isomorphism*. We will see in a later chapter how to show in general that two groups are isomorphic; but for now, forming the groups' Cayley Tables and seeing if you can match elements to make the tables the same is a very good strategy.

Exercise 14.2.5. Let $W = \{G, H\}$ and $Z = \{J, K\}$.

- (a) Write the Cayley Tables for S_W and S_Z . It would be helpful to write the entries of S_W and S_Z in tableau form.
- (b) Give a bijection from W to Z , and the corresponding bijection from S_W to S_Z , that would show S_W is isomorphic to S_Z . (Remember that a bijection can be thought of as a "relabeling" of elements of W as elements of Z .)
- (c) *How many possible bijections from W to Z give rise to isomorphisms from S_W to S_Z ?

◇

Exercise 14.2.6. Let $X = \{A, B, C\}$ and $Y = \{M, N, P\}$.

- (a) Write the Cayley Tables for S_X and S_Y

- (b) Give a bijection from X to Y , and the corresponding bijection from S_X to S_Y , that would show S_X is isomorphic to S_Y .
- (c) *How many possible bijections from X to Y produce isomorphisms from S_X to S_Y ?
- (d) *Now let $X = \{A, B, \dots, M\}$ and $Y = \{N, O, \dots, Z\}$. How many different bijections from X to Y produce isomorphisms from S_X to S_Y ?

◇

14.2.3 Subgroups and permutation groups

Let's summarize this section so far. The permutations on a set X of n elements is a group under function composition (denoted by S_n). Further, for any figure with n sides, the symmetries of that figure is a subset of S_n containing at least the identity permutation, and that subset is itself a group under function composition. This example motivates the following definition.

Definition 14.2.7. A subset of a group G that is itself a group under the same operation as G is called a *subgroup* of G . △

The notion of subgroup is a key concept in abstract algebra, which will be used throughout the rest of the book.

Example 14.2.8. From the above definition of subgroup it follows that:

- The symmetries of a rectangle are a subgroup of S_4 .
- The symmetries of an isosceles triangle are a subgroup of S_3 .
- D_5 is a subgroup of S_5 .
- The permutations of $\{1, 2, 3\}$ are a subgroup of the permutations of $\{1, 2, 3, 4\}$. Hence S_3 is a subgroup of S_4 . By the same token, S_m can be considered as a subgroup of S_n whenever $m < n$.

◆

Definition 14.2.9. A subgroup of S_n is called a *permutation group*. △

Exercise 14.2.10. Consider the subset G of S_5 consisting of the identity permutation id and the permutations

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix} \\ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \\ \mu &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}.\end{aligned}$$

- (a) Write the Cayley table for G . Label your rows and columns as: $\text{id}, \sigma, \tau, \mu$.
 (b) Use the Cayley table to explain whether G is a subgroup of S_5 or not.

Remember: you don't need to show the associative property, since function composition is associative.

◇

Exercise 14.2.11. Consider the subset G of S_4 consisting of the identity permutation id and the permutations

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \\ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \\ \mu &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}.\end{aligned}$$

- (a) Write the Cayley table for G (Label your rows and columns as: $\text{id}, \sigma, \tau, \mu$).
 (b) Use the Cayley table to explain whether or not G is a subgroup of S_4 .

◇

As the example shows, a permutation group need not comprise all symmetries of a figure or all rearrangements of a set. Many permutation groups have no evident practical interpretation whatsoever. Nonetheless they are still useful, because as we shall see they can be used to characterize the groups that contain them.

14.3 Cycle notation

14.3.1 Tableaus and cycles

In the Symmetries chapter, we introduced tableau notation to deal with bijections because of its brevity and ease of use for function composition. But as you may have noticed in the last section, even tableaus can become cumbersome to work with. To work effectively with permutation groups, we need a more streamlined method of writing down and manipulating permutations. This method is known as cycle notation.

Example 14.3.1. Suppose $\rho \in S_6$ and $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$. Then

$$\rho(1) = 2, \rho(2) = 3, \rho(3) = 4, \rho(4) = 5, \rho(5) = 6, \text{ and } \rho(6) = 1.$$

A shorter way to represent this is

$$1 \rightarrow 2, 2 \rightarrow 3, 3 \rightarrow 4, 4 \rightarrow 5, 5 \rightarrow 6 \text{ and } 6 \rightarrow 1.$$

We can visualize this as a “wheel”, as shown in Figure 14.3.1

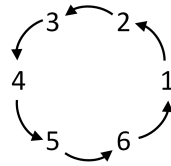


Figure 14.3.1. Cycle representation of the permutation (123456).

We shall write this trail of inputs and outputs as (123456); and rather than “wheel”, we call this a *cycle*. Reading the cycle from left to right indicates that 1 goes to 2, 2 goes to 3, ..., and the 6 at the end goes back to 1.

Exercise 14.3.2. Show that (123456) = (345612) by drawing a figure similar to Figure 14.3.1 for each cycle. \diamond

Exercise 14.3.3. Show that (123456) and (234561) both have the same tableau (so they are in fact the same permutation). \diamond

From the previous two exercises, it is clear that there are many ways to write the same cycle: we can begin with any element we want, and work our way around until we get back to the same element. To avoid possible confusion, from now on we will follow the convention of starting the cycle with the “smallest” or “first” element of the domain.

For this particular permutation, since our cycle contains all the inputs in the domain of ρ , it represents the whole function (because it gives us the outputs for every input). Therefore in cycle notation,

$$\rho = (123456)$$



Exercise 14.3.4. Write the following permutation of S_6 in cycle notation:

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 1 & 6 & 2 \end{pmatrix}.$$



Exercise 14.3.5. Given the permutation $\mu = (152634)$ in S_6 :

- (a) Write μ in tableau form.
- (b) Write μ as a figure similar to Figure 14.3.1



Exercise 14.3.6. Given the permutation $\mu = (165432)$ in S_6 :

- (a) Write μ in tableau form.
- (b) Write μ as a figure similar to Figure 14.3.1
- (c) Compare your answer to (b) with Figure 14.3.1 of $\rho = (123456)$. Explain the difference between μ and ρ .



Definition 14.3.7. The *length* of a cycle is how many elements the cycle contains; i.e. how many elements are in the parentheses. Formally,

if (a_1, a_2, \dots, a_n) is a cycle, then the length of (a_1, a_2, \dots, a_n) is n .

△

For example, the permutation ρ in Example 14.3.1 above is represented by a cycle of length six.

Remark 14.3.8. Notice how we have used the notation a_j to indicate arbitrary elements in a cycle. This is a common practice in abstract algebra. △

Now not all permutations in S_6 correspond to a cycle of length six. For instance:

Example 14.3.9. Suppose $\tau \in S_6$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 3 & 5 & 6 \end{pmatrix}$. Then

- $1 \rightarrow 1$, which means that 1 “stays put.” So we don’t use 1.
- $2 \rightarrow 4$, $4 \rightarrow 3$, and $3 \rightarrow 2$; so we have (243) .
- Finally, $5 \rightarrow 5$ and $6 \rightarrow 6$; so they also stay put.

Hence

$$\tau = (243)$$

◆

Based on the procedure in the previous example then, how would we represent the identity permutation on a set of n elements? All the elements stay put, so technically id would equal the “empty cycle”. Some references in fact use “ $()$ ” to denote the identity: but in this book we will always denote the identity permutation by id as a reminder that this is in fact the group’s identity element.

Warning 14.3.10. Cycle notation does not indicate the domain of the permutation. For instance, the permutation (243) in Example 14.3.9 had domain $\{1, 2, 3, 4, 5, 6\}$, but (243) could also refer to a permutation on the domain $\{1, 2, 3, 4\}$. When working with permutations in cycle notation, make sure you know what the domain is. (In most cases, it’s clearly specified by the context.) ◇

Exercise 14.3.11. Write each of the following permutations in S_7 in tableau form.

- (a) $\omega = (243)$
- (b) $\omega = (2365)$
- (c) $\omega = (14257)$

◇

Exercise 14.3.12. Draw a figure similar to Figure 14.3.1 depicting each of the following permutations in S_5 .

- (a) $\sigma = (25)$
- (b) $\sigma = (135)$
- (c) $\sigma = (1342)$

◇

A final question that may come to mind is: do all permutations correspond to some cycle? Certainly, as we've seen, all cycles correspond to some permutation in S_n . However, can all permutations in S_n be represented as a cycle? We will take the next several parts of this section to explore this question.

14.3.2 Composition (a.k.a. product) of cycles

Since cycles represent permutations, they can be composed together. If we change the cycles to tableaus, we know how to compose them. Now let's figure out how to compose them using the cycles themselves.

Notation 14.3.13. Given permutations σ and τ , instead of writing $\sigma \circ \tau$ we write the shorthand notation: $\sigma\tau$. Furthermore, instead of calling this the composition of σ and τ , we refer to it as the *product* of σ and τ .² △

Example 14.3.14. Suppose we want to form the product (that is, composition) $\sigma\tau$, where $\sigma, \tau \in S_6$ and $\sigma = (1532), \tau = (126)$.

²Once again we see mathematicians' annoying habit of reusing familiar terms to mean something new in a different contexts. In this case, the "product" of permutations means something quite different from ordinary multiplication.

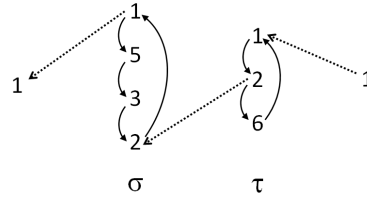


Figure 14.3.2. Product of cycles σ and τ , showing the derivation of $\sigma\tau(1) = 1$.

Figure 14.3.2 provides a visual representation of how the product $\sigma\tau$ acts on 1. Remember that we operate from right to left, so the figure shows ‘1’ coming in from the right. The action of τ takes 1 to 2. (For convenience we have “flattened” the permutations τ and σ , so they no longer appear as circles.) Then we pass over to σ , which takes 2 to 1. The final result is 1: therefore $\sigma(\tau(1)) = 1$.

Evidently 1 remains unchanged by the permutation, so let’s look at what happens to 2. We see this in Figure 14.3.3. First, τ moves 2 to 6. Moving on to σ , we find that σ leaves the 6 unchanged. The result is that $\sigma(\tau(2)) = 6$.

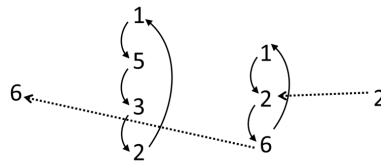


Figure 14.3.3. Product of cycles σ and τ (continued), showing $\sigma\tau(2) = 6$.

We have seen that $\sigma\tau$ takes 2 to 6: so now let’s see where $\sigma\tau$ takes 6. (Perhaps you can see that we’re trying to build a cycle here.) The top part of Figure 14.3.4 uses the same process to show the result: $\sigma(\tau(6)) = 5$. The middle part of Figure 14.3.4 shows that $\sigma(\tau(5)) = 3$; and the bottom part of Figure 14.3.4 shows that $\sigma(\tau(3)) = 2$. We already know that $\sigma(\tau(2)) = 6$, so we have closed out our cycle. We have shown $2 \rightarrow 6 \rightarrow 5 \rightarrow 3 \rightarrow 2$, which amounts to the cycle: (2653).

So far 4 is unaccounted for: but a quick inspection of Figure 14.3.4 shows that 4 is not affected by either τ or σ . So the entire action of τ followed

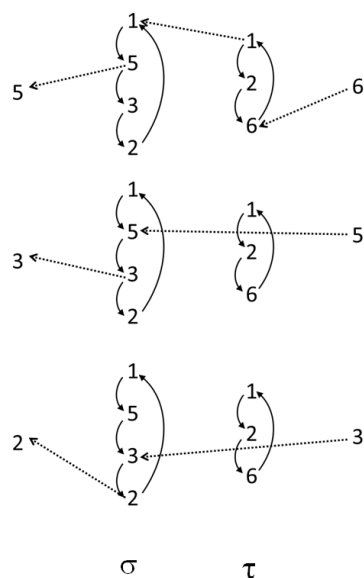


Figure 14.3.4. Product of cycles σ and τ (continued), showing $6 \rightarrow 5 \rightarrow 3 \rightarrow 2$.

by σ is summarized by the cycle (2653) , meaning that we can write: $\sigma\tau = (2653)$. \blacklozenge

Exercise 14.3.15. Using the same permutations σ and τ as above:

- (a) Write the product $\tau\sigma$ in cycle notation.
- (b) By comparing your results for $\sigma\tau$ and $\tau\sigma$, fill in the blank in the following statement: In general, permutations do not _____.

\diamond

Example 14.3.16. At the beginning it may be helpful to draw a picture, as in the previous example. However, once you gain experience, you should be able to find the product of cycles directly. Consider the product $\sigma\tau$ where $\sigma = (AEDBF)$ and $\tau = (ABDFE)$. Then we have:

- τ takes $A \rightarrow B$ and σ takes $B \rightarrow F$; hence $\sigma\tau$ takes $A \rightarrow F$.

- τ takes $F \rightarrow E$, and σ takes $E \rightarrow D$; hence $\sigma\tau$ takes $F \rightarrow D$.
- τ takes $D \rightarrow F$, and σ takes $F \rightarrow A$; hence $\sigma\tau$ takes $D \rightarrow A$.

We have finished a cycle: (AFD) . Let us check where the other letters B, C, E go:

- τ takes $B \rightarrow D$, and σ takes $D \rightarrow B$; hence $\sigma\tau$ takes $B \rightarrow B$.
- Neither τ nor σ affects C ; hence $\sigma\tau$ takes $C \rightarrow C$.
- τ takes $E \rightarrow A$, and σ takes $A \rightarrow E$; hence $\sigma\tau$ takes $E \rightarrow E$.

Since B, C, E are unaffected by $\sigma\tau$, we conclude that $\sigma\tau = (AFD)$. ◆

Exercise 14.3.17. Given that $\delta = (135)$, $\sigma = (347)$, and $\rho = (567)$ are permutations in S_7 , compute the following:

- | | | |
|--------------------|------------------|------------------|
| (a) $\delta\sigma$ | (c) $\delta\rho$ | (e) $\sigma\rho$ |
| (b) $\sigma\delta$ | (d) $\rho\delta$ | (f) $\rho\sigma$ |

◆

14.3.3 Product of disjoint cycles

Definition 14.3.18. Two cycles are *disjoint* if their parentheses contain no elements in common. Formally, two cycles (a_1, a_2, \dots, a_k) and (b_1, b_2, \dots, b_l) , are *disjoint* if $a_i \neq b_j, \forall i, j$ such that $1 \leq i \leq k$ and $1 \leq j \leq l$. △

For example, the cycles (135) and (27) are disjoint, whereas the cycles (135) and (347) are not.

Example 14.3.19. Given $\sigma = (135)$, $\tau = (27)$, $\sigma, \tau \in S_7$; let us compute $\sigma\tau$.

Notice right away that every number affected by τ is unaffected by σ ; and vice versa. Since the two cycles always remain separate, it is appropriate to represent $\sigma\tau$ as $(135)(27)$, because the cycles don't reduce any farther. ◆

Now since S_7 is closed under function composition, it follows that $\sigma\tau = (135)(27)$ must be a permutation in S_7 .

Exercise 14.3.20. Write the permutation $\sigma\tau$ from Example 14.3.19 in tableau form. \diamond

This permutation can't be represented by one cycle, but rather by *two* disjoint cycles. So we have an answer to our previous question: all cycles are permutations, but not all permutations are cycles. Some are represented by two disjoint cycles: and in fact some are represented by more than two disjoint cycles.

Example 14.3.21. Suppose $\mu \in S_7$ and $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 1 & 4 & 3 & 7 & 2 & 5 \end{pmatrix}$. Then

- $1 \rightarrow 6$, $6 \rightarrow 2$, and $2 \rightarrow 1$; therefore we have the cycle (162) .
- $3 \rightarrow 4$ and $4 \rightarrow 3$; therefore we have (34) .
- Finally, $5 \rightarrow 7$ and $7 \rightarrow 5$; therefore we have (57) .

Hence $\mu = (162)(34)(57)$, as we may verify by computing the product $(162) \circ (34) \circ (57)$ directly.

We may represent this process graphically as follows. The permutation μ can be represented as a digraph as shown in Figure 14.3.5(a). We can make the digraph appear much simpler by rearranging the vertices as in Figure 14.3.5(b). We shall see that *all* permutations can be simplified in this manner. \blacklozenge

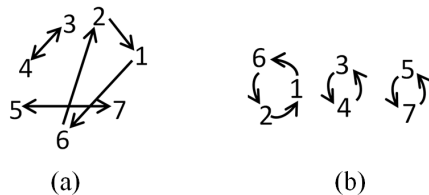


Figure 14.3.5. (a) Digraph representation of permutation (b) Rearrangement of digraph into cycles

Exercise 14.3.22. Write the following permutations in cycle notation.

(a) $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 3 & 4 \end{pmatrix}$

(c) $\omega = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 6 & 2 & 3 \end{pmatrix}$

(b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix}$

(d) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 4 & 1 & 2 & 6 \end{pmatrix}$

◇

Exercise 14.3.23. Write each of the following permutations in S_9 in tableau form.

(a) $\mu = (259)(347)$.

(c) $\tau = (286)(193)(457)$.

(b) $\sigma = (25678)(14)(39)$.

(d) $\omega = (257)(18)$.

◇

Exercise 14.3.24. Write the permutations of D_6 in cycle notation (recall that D_6 is the group of symmetries of a hexagon). ◇

Exercise 14.3.25. Write the symmetries of a square in cycle notation. ◇

There is one more issue we need to explore with the product of disjoint cycles, which we will do in the following exercise.

Exercise 14.3.26. In parts (a)–(d) below, write both permutations on the set $\{1, 2, 3, 4, 5, 6\}$ in tableau form.

(a) $(123)(45)$ and $(45)(123)$.

(c) $(1352)(46)$ and $(46)(1352)$

(b) $(14)(263)$ and $(263)(14)$

(d) $(135)(246)$ and $(246)(135)$

(e) From your results in (a)–(d), what do you conjecture about the product of disjoint cycles?

◇

The examples in Exercise 14.3.26 seem to indicate that the product of disjoint cycles is commutative. This is in fact true, as we shall now prove.

Proposition 14.3.27. Disjoint cycles commute: that is, given two disjoint cycles $\sigma = (a_1, a_2, \dots, a_j)$ and $\tau = (b_1, b_2, \dots, b_k)$ we have

$$\sigma\tau = \tau\sigma = (a_1, a_2, \dots, a_j)(b_1, b_2, \dots, b_k)$$

PROOF. We present this proof as a fill-in-the-blanks exercise:

Exercise 14.3.28. Fill in the blanks to complete the proof:

Recall that permutations are defined as bijections on a set X . In order to show that the two permutations $\sigma\tau$ and $\tau\sigma$ are equal, it's enough to show that they are the same function. In other words, we just need to show that $\sigma\tau(x) = \underline{\langle 1 \rangle}$ for all $x \in X$.

We'll define $A = \{a_1, a_2, \dots, a_j\}$ and $B = \{b_1, b_2, \dots, b_k\}$. By hypothesis A and B are disjoint, so $A \underline{\langle 2 \rangle} B = \underline{\langle 3 \rangle}$. Given an arbitrary $x \in X$, there are three possibilities: (i) $x \in A$ and $x \notin B$; (ii) $x \in \underline{\langle 4 \rangle}$ and $x \notin \underline{\langle 6 \rangle}$; (iii) $x \notin \underline{\langle 7 \rangle}$ and $x \notin \underline{\langle 8 \rangle}$.

- (i) In this case, since $x \notin B$ it follows that $\tau(x) = x$. We then have $\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x)$. Furthermore, since $x \in A$ it follows that $\sigma(x) \in A$, so $\sigma(x) \notin B$. We then have $\tau\sigma(x) = \tau(\sigma(x)) = \sigma(x)$. It follows that $\sigma\tau(x) = \tau\sigma(x)$.
- (ii) In this case, since $x \notin \underline{\langle 9 \rangle}$ it follows that $\underline{\langle 10 \rangle}(x) = x$. We then have $\tau\sigma(x) = \underline{\langle 11 \rangle} = \underline{\langle 12 \rangle}(x)$. Furthermore, since $x \in \underline{\langle 13 \rangle}$ it follows that $\underline{\langle 14 \rangle}(x) \in \underline{\langle 15 \rangle}$, so $\underline{\langle 16 \rangle}(x) \notin \underline{\langle 17 \rangle}$. We then have $\sigma\tau(x) = \underline{\langle 18 \rangle} = \underline{\langle 19 \rangle}(x)$. It follows that $\sigma\tau(x) = \tau\sigma(x)$.
- (iii) In this case, since $x \notin A$ it follows that $\underline{\langle 20 \rangle}(x) = x$. Similarly since $x \notin \underline{\langle 21 \rangle}$ it follows that $\underline{\langle 22 \rangle}(x) = x$. We then have $\tau\sigma(x) = \underline{\langle 23 \rangle}$ and $\sigma\tau(x) = \underline{\langle 24 \rangle}$. It follows that $\sigma\tau(x) = \tau\sigma(x)$.

In all three cases we have $\sigma\tau(x) = \underline{\langle 25 \rangle}$, so therefore $\sigma\tau = \tau\sigma$. ◇

□

What we've discovered about products of two disjoint cycles is also true for products of any number of disjoint cycles. Since disjoint cycles act independently, they all commute.

Exercise 14.3.29. Write each of the following permutations on $X = \{1, 2, \dots, 9\}$ in tableau form.

- (a) $(1346)(298)(57)$ (b) $(57)(1346)(298)$ (c) $(298)(57)(1346)$
- (d) Which of the above permutations are the same? Which are different? *Explain* your answer.

◇

Exercise 14.3.30. Write each of the following permutations 2 different ways using cycle notation.

- (a) $(147)(258)(369)$ (b) $(12)(35)(46)(78)$ (c) $(14359)(28)(67)$

◇

14.3.4 Products of permutations using cycle notation

Finally, now that we know how to deal with permutation compositions that simplify to disjoint cycles, we can now compose any set of permutations we want. We will start with a couple examples.

Example 14.3.31. Given the permutations $\mu = (257)(134)$ and $\rho = (265)(137)$ in S_7 , write $\mu\rho$ in cycle notation.


- $1 \rightarrow 3, 3 \rightarrow 3, 3 \rightarrow 4$, and $4 \rightarrow 4$; therefore $1 \rightarrow 4$.
- $4 \rightarrow 4, 4 \rightarrow 4, 4 \rightarrow 1$, and $1 \rightarrow 1$; therefore $4 \rightarrow 1$.

This gives us the cycle (14) . Continuing,

- $2 \rightarrow 2, 2 \rightarrow 6, 6 \rightarrow 6$, and $6 \rightarrow 6$; therefore $2 \rightarrow 6$.
- $6 \rightarrow 6, 6 \rightarrow 5, 5 \rightarrow 5$, and $5 \rightarrow 7$; therefore $6 \rightarrow 7$.
- $7 \rightarrow 1, 1 \rightarrow 1, 1 \rightarrow 3$, and $3 \rightarrow 3$; therefore $7 \rightarrow 3$.
- $3 \rightarrow 7, 7 \rightarrow 7, 7 \rightarrow 7$, and $7 \rightarrow 2$; therefore $3 \rightarrow 2$.

So we have the cycle (2673) . Now the only input not included in our cycles is 5, so logically it should stay put. But let's test it just in case we made a mistake in our work above.

- $5 \rightarrow 5$, $5 \rightarrow 2$, $2 \rightarrow 2$, and $2 \rightarrow 5$; therefore 5 does indeed stay put.


So, we finally have: $\mu\rho = (14)(2673)$ 

Example 14.3.32. Find the product $(156)(2365)(123)$ in S_6 .

- $1 \rightarrow 2$, $2 \rightarrow 3$, and $3 \rightarrow 3$; therefore $1 \rightarrow 3$.
- $3 \rightarrow 1$, $1 \rightarrow 1$, and $1 \rightarrow 5$; therefore $3 \rightarrow 5$.
- $5 \rightarrow 5$, $5 \rightarrow 2$, and $2 \rightarrow 2$; therefore $5 \rightarrow 2$.
- $2 \rightarrow 3$, $3 \rightarrow 6$, and $6 \rightarrow 1$; therefore $2 \rightarrow 1$.

So we have (1352) .

- 4 does not appear in any of the cycles, so we know it won't be acted on by any of the cycles. Hence 4 stays put.
- $6 \rightarrow 6$, $6 \rightarrow 5$, and $5 \rightarrow 6$; hence 6 stays put.

Therefore $(156)(2365)(123) = (1352)$. 

Exercise 14.3.33. Given the following permutations in S_8 ,

$$\sigma = (1257)(34), \tau = (265)(137), \text{ and } \rho = (135)(246)(78)$$

find the products:

(a) $\sigma\tau$

(c) $\tau\rho$

(b) $\tau\sigma$

(d) $\sigma\rho$



Exercise 14.3.34. Compute each of the following. Note that e.g. $(123)^2$ means the same as $(123)(123)$.

- (a) (1345)(234) (c) (143)(23)(24) (e) (1254)(13)(25)²
 (b) (12)(1253) (d) (1423)(34)(56)(132) (f) (1254)²(123)(45)

◇

14.3.5 Cycle structure of permutations

Over the last several subsections, we've seen permutations represented as no cycles (id), a single cycle, or the product of any number of disjoint cycles. This worked because both a single cycle and a product of disjoint cycles can't be reduced to a simpler form in cycle notation. Are there any other possibilities? Are there permutations that can't be represented as either a single cycle or a product of disjoint cycles? The answer to this compelling question is given in the following proposition. This type of proposition is called an "existence and uniqueness" statement, and for convenience we'll divide the statement into two parts:

Proposition 14.3.35.

- (a) Every permutation σ in S_n can be written either as the identity, a single cycle, or as the product of disjoint cycles.
 (b) These disjoint cycles are *uniquely* determined by the permutation σ .

The following proof is a formalized version of the procedure we've been using to change permutations from tableau form to cycle notation. Admittedly, it looks intimidating. However, we include it for your "cultural enrichment", because higher-level mathematics is typically like this. It's often the case that particular examples of a certain principle are relatively easy to explain, but constructing a general proof that covers *all* cases is much more difficult. Before starting the proof, we remind you that the notation $\sigma = (a_1 a_2 \dots a_n)$ means:

$$\sigma(a_1) = a_2 \qquad \sigma(a_2) = a_3 \dots \qquad \dots \sigma(a_k) = a_1,$$

and $\sigma(x) = x$ for all other elements $x \in X$.

PROOF. Let's begin with (a) We can assume that $X = \{1, 2, \dots, n\}$. Let $\sigma \in S_n$, and define $X_1 = \{1, \sigma(1), \sigma^2(1), \dots\}$. The set X_1 is finite since

X is finite. Therefore the sequence $1, \sigma(1), \sigma^2(1), \dots$ must repeat. Let j_1 be the first index where the sequence repeats, so that $\sigma^{j_1}(1) = \sigma^k(1)$ for some $k < j_1$. Then if we apply σ^{-1} to both sides of the equation we get $\sigma^{j_1-1}(1) = \sigma^{k-1}(1)$. Repeating this $k-1$ more times gives $\sigma^{j_1-k}(1) = 1$. This implies that the sequence repeats at index $j_1 - k$: but we've already specified that j_1 is the *first* index where the sequence repeats. The only way this can happen is if $k = 0$. It follows that $X_1 = \{1, \sigma(1), \sigma^2(1), \dots, \sigma^{j_1-1}(1)\}$, where $\sigma^{j_1}(1) = 1$.

Now there are two possible cases:

- (i) X_1 accounts for all the integers in X ; i.e. $X_1 = X$
- (ii) there are some integers in X not accounted for in X_1 (that is, $X \setminus X_1 \neq \emptyset$).

If case (ii) holds, then let i be the smallest integer in $X \setminus X_1$ and define X_2 by $\{i, \sigma(i), \sigma^2(i), \dots\}$. Just as with X_1 , we may conclude that X_2 is a finite set, and that $X_2 = \{i, \sigma(i), \dots, \sigma^{j_2-1}(i)\}$ where $\sigma^{j_2}(i) = i$.

We claim furthermore that X_1 and X_2 are disjoint. We can see this by contradiction: *suppose* on the other hand that X_1 and X_2 are not disjoint. Then it must be the case that $\sigma^p(1) = \sigma^q(i)$ for some natural numbers p, q with $0 \leq p < j_1$ and $0 \leq q < j_2$. Applying σ to both sides of this equation, gives $\sigma^{p+1}(1) = \sigma^{q+1}(i)$. If we continue applying σ to both sides a total of $j_2 - q$ times then we obtain $\sigma^{p+j_2-q}(1) = \sigma^{j_2}(i)$. But since $\sigma^{j_2}(i) = i$, it follows that $\sigma^{p+j_2-q}(1) = i$, which implies that $i \in X_1$. This is a contradiction, because we know $i \in X \setminus X_1$. The contradiction shows that the *supposition* must be false, so X_1 and X_2 are disjoint.

Continuing in the same manner, we can define finite disjoint sets X_3, X_4, \dots . Since X is a finite set, we are guaranteed that this process will end and there will be only a finite number of these sets. Some of these sets X_j will have only a single element: in this case, $\sigma_j = \text{id}$, and it is not necessary to include these sets in the list. We may remove these sets, and relabel the remaining sets as X_1, \dots, X_s . If σ_i is the cycle defined by

$$\sigma_i(x) = \begin{cases} \sigma(x) & x \in X_i \\ x & x \notin X_i, \end{cases}$$

then $\sigma = \sigma_1 \sigma_2 \cdots \sigma_s$. Since the sets X_1, X_2, \dots, X_r are disjoint, the cycles $\sigma_1, \sigma_2, \dots, \sigma_s$ must also be disjoint.

Now recall case (i) above. In this case, $\sigma = \sigma_1$. Hence, σ is either a single cycle or the product of r disjoint cycles. Note that if $\sigma = \text{id}$, then the process described above will yield all single-element sets, so that $r = 0$ and $\{X_1, \dots, X_r\} = \emptyset$ (this is why we treat the id as a special case). But if $\sigma \neq \text{id}$, the process will create at least one cycle of length ≥ 2 . This completes the proof of (a).

Now on to (b). To show uniqueness of the disjoint cycles, we suppose that $\sigma = \sigma_1 \dots \sigma_s$ and also $\sigma = \rho_1 \dots \rho_r$, where the σ_j 's are disjoint cycles and the ρ_j 's are also disjoint cycles. The proof may be accomplished by showing that $S = R$, where $S := \{\sigma_1, \dots, \sigma_s\}$ and $R := \{\rho_1, \dots, \rho_r\}$. To do this, we may show every cycle in S is also in R , and vice versa. So take $\sigma_j \in S$, and write $\sigma_j = (a_1 a_2 \dots a_j)$. Since $\sigma_j(a_1) = a_2$, it follows that $\sigma(a_1) = a_2$. But this means that there must be a cycle $\rho_\ell \in R$ such that $\rho_\ell(a_1) = a_2$. In the same way we may show that $\rho_\ell(a_2) = a_3, \dots, \rho_\ell(a_j) = a_1$. Since ρ_ℓ is a cycle, it follows that $\rho_\ell(x) = x$ for $x \notin \{a_1 a_2 \dots a_j\}$. It follows that $\rho_\ell(x) = \sigma_j(x)$ for all $x \in X$, and hence $\rho_\ell = \sigma_j$. Thus every element of S is also an element of R . The proof is then completed by the following exercise:

Exercise 14.3.36. Complete the proof of Proposition 14.3.35 by showing that every ρ_j in R is also in the set S . ◇

□

Proposition 14.3.35 is a *classification theorem*. You have seen classification theorems before: for instance, you know that any natural number > 1 can be written uniquely as the product of primes. Proposition 14.3.35 similarly gives us a standard way to represent permutations. It allows us to characterize the types of permutations in S_n according to their cycle sizes, as shown in the following example.

Example 14.3.37. We know that every permutation in S_5 is the product of disjoint cycles. Let us list all possible cycle lengths and number of cycles for the permutations of S_5 .

- First of all, S_5 contains the identity, which has no cycles.
- Second, some permutations in S_5 consist of a single cycle. The single cycle could have length 2, 3, 4, or 5 (remember, we don't count cycles of length 1).

- Third, some permutations in S_5 consist of the product of two disjoint cycles. To enumerate these, suppose first that one of the cycles is a cycle of length 2. Then the other cycle could be a cycle of length 2 (for instance in the case $(12)(34)$) or a cycle of length 3 (as in the case $(14)(235)$). There are no other possibilities, because we only have 5 elements to permute, and a larger disjoint cycle would require more elements.
- It's not possible to have three or more disjoint cycles, because that would require at least six elements.

To summarize then, the possible cycle structures for permutations in S_5 are:

- The identity
- single cycles of lengths 5, 4, 3, or 2
- two disjoint cycles of lengths 2 and 3; and two disjoint cycles of lengths 2 and 2



Exercise 14.3.38. Following Example 14.3.37, list all possible cycle structures of permutations in the following:

(a) S_6

(b) S_7

(c) S_8



14.4 Algebraic properties of cycles

14.4.1 Powers of cycles: definition of order

Let's revisit the product of cycles. We will look at what happens when you compose a cycle with itself multiple times.

Example 14.4.1. Consider the product $(1264)(1264)$, which we may also write as $(1264)^2$. As in the previous section, we can use a diagram (see Figure 14.4.1) to compute this product. But let's try to understand better what's really going on.

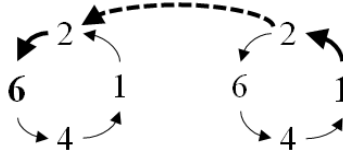


Figure 14.4.1. Diagram of $(1264)^2$, showing in particular how the permutation takes 1 to 6.

- (1) Notice for all elements $x \neq 1, 2, 6, 4$, x stays put in (1264) ; hence x stays put in $(1264)^2$. So the product $(1264)^2$ does not involve any elements except 1, 2, 6 and 4.
- (2) Now let's look at what happens when $x = 1, 2, 6$, or 4. By squaring the cycle, we are applying it twice to each input; hence each input is moved two spots around the wheel (see Figure 14.4.2). In other words,

$$1 \rightarrow 6; \quad 6 \rightarrow 1; \quad 2 \rightarrow 4; \quad 4 \rightarrow 2,$$

Altogether: $(1264)^2 = (16)(24)$.

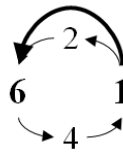


Figure 14.4.2. $(1264)^2$: streamlined notation



With this methodology in mind, let's explore powers of cycles a bit further.

Exercise 14.4.2. Compute each of the following.

- (a) $(1264)^3$ (b) $(1264)^4$ (c) $(1264)^5$



Exercise 14.4.3. Compute each of the following:



- (a) $(125843)^2$ (c) $(125843)^4$ (e) $(125843)^6$
 (b) $(125843)^3$ (d) $(125843)^5$ (f) $(125843)^7$

◇

Do you notice a pattern from these two exercises? Let us investigate in a bit more detail: this will help us build up towards a proof of a general statement.

Exercise 14.4.4. Let $X = \{1, 2, \dots, 10\}$, let $A = \{2, 5, 7, 8\}$, and let $\sigma \in S_X$ be the cycle $\sigma = (2578)$.

- (a) What is $\sigma(2)$? What is $\sigma^2(2)$? What is $\sigma^3(2)$? What is $\sigma^4(2)$ What is $\sigma^{3,482,991}(2)$?
 (b) What is $\sigma(5)$? What is $\sigma^2(5)$? What is $\sigma^3(5)$? What is $\sigma^4(5)$ What is $\sigma^{3,482,991}(5)$?
 (c) Fill in the blank: If $x \in A$ then $\sigma^k(x) = \sigma^{\text{mod}(k, _)}(x)$.
 (d) What is $\sigma(1)$? What is $\sigma(3)$?
 (e) What general statement can you make about $\sigma^k(x)$ for $x \in X \setminus A$?
 (f) ** Let $K = \{k : \sigma^k(x) = x \ \forall x \in X\}$. Is $2 \in K$? Is $3 \in K$? Is $4 \in K$? Given any positive integer k , what's a simple way of telling whether or not $k \in K$?

◇

Hopefully you're beginning to see the picture! To generalize these results, we need some additional terminology:

Definition 14.4.5. The *order* of a cycle σ is the smallest natural number k such that $\sigma^k = \text{id}$. The order of σ is denoted by the notation $|\sigma|$.³ △

After that long build-up, we now have (Ta-da!):

Proposition 14.4.6. The order of a cycle is always equal to the cycle's length.

PROOF. To prove this, we essentially have to prove two things:

³This is in keeping with our practice of using $|\dots|$ to denote the "size" of things.

- (A) If σ is a cycle of length k , then $\sigma^k = \text{id}$;
- (B) If σ is a cycle of length k , then $\sigma^j \neq \text{id} \quad \forall j : 1 \leq j < k$.

The proof for (A) follows the same lines as our investigations in Exercise 14.4.4. In that exercise, we considered separately the elements of X that are moved by the cycle, and those elements that are not moved by the cycle.

Exercise 14.4.7. Prove part (A) by filling in the blanks.

Let $\sigma \in S_X$ be an arbitrary cycle of length k . Then σ can be written as $(a_0 a_1 \dots a_{k-1})$, for some set of elements a_0, a_1, \dots, a_{k-1} in X . In order to show that $\sigma^k = \text{id}$, it is sufficient to show that $\sigma^k(x) = \underline{\langle 1 \rangle} \quad \forall x \in X$. Let A be the set $\{a_0, a_1, \dots, a_{k-1}\}$. Now for any $x \in X$, there are two possibilities:

- (i) $x \in X \setminus A$;
- (ii) $x \in A$.

We'll deal with these two cases separately (as we did in Exercise 14.4.4).

- (i) In this case, $\sigma(x) = \underline{\langle 2 \rangle}$. It follows that $\sigma^2(x) = \sigma(\sigma(x)) = \sigma(\underline{\langle 3 \rangle}) = \underline{\langle 4 \rangle}$. We can use the same argument to show that $\sigma^3(x) = \underline{\langle 5 \rangle}$, and that $\sigma^k(x) = \underline{\langle 6 \rangle}$ for any natural number $\underline{\langle 7 \rangle}$.
- (ii) In this case, then $x = a_j$ for some integer $j, 1 \leq j \leq \underline{\langle 8 \rangle}$. It follows from the definition of cycle that $\sigma(x) = \sigma(a_j) = a_{\text{mod}(j+1, k)}$. Furthermore, $\sigma^2(x) = \sigma(a_{\text{mod}(j+1, k)}) = \underline{\langle 9 \rangle}$. Similarly it follows that $\sigma^k(x) = a_{\text{mod}(j+\underline{\langle 10 \rangle}, k)} = a_{\underline{\langle 11 \rangle}} = x$.

Cases (i) and (ii) establish that $\forall x \in X, \underline{\langle 12 \rangle} = x$. It follows that $\sigma^k = \underline{\langle 13 \rangle}$.

◇

The proof of (B) is also structured as an exercise.

Exercise 14.4.8. In this exercise we use the same notation as part (A), that is: $\sigma \in S_X$ has length k and is represented as: $\sigma = (a_1 a_2 \dots a_k)$.



- (a) What is $\sigma(a_1)$? What is $\sigma^2(a_1)$? What is $\sigma^3(a_1)$? What is $\sigma^{k-1}(a_1)$?
 (b) Conclude from part (a) that $\sigma^j \neq \text{id}$ for $j = 1, 2, 3, \dots, k-1$.

◇

□

Example 14.4.9. Here's a nice application of Proposition 14.4.6, which simply uses rules of function composition. This should also give you a good start on the next exercise.

$$(1264)^6 = (1264)^4(1264)^2 = \text{id} (16)(24) = (16)(24)$$

◆

Exercise 14.4.10. Compute the following:

(a) $(1264)^{11}$

(c) $(352)(136)(1254)^{102}$

(b) $(125843)^{53}$

(d) $(348)(456)^5(1325)^{10}$

◇

Exercise 14.4.11. If σ is a cycle of odd length, prove that σ^2 is also a cycle. (*Hint*)

◇

14.4.2 Powers and orders of permutations in general

Now that we know the order of cycles, let's see if we can tackle other permutations as well:

Definition 14.4.12. The *order* of a permutation τ is the smallest positive integer k such that $\tau^k = \text{id}$. As before, the order of τ is denoted by the notation $|\tau|$. △

Proposition: Let τ be a permutation, and let $k = |\tau|$. Then $\tau^\ell = \text{id}$ if and only if $\text{mod}(\ell, k) = 0$.

Exercise 14.4.13. Fill in the blanks with the appropriate variables in the following proof of the proposition. (*Hint*)

Proof: For any integer ℓ we may write $\ell = ak + b$, where $b \in \mathbb{Z}_{\langle 1 \rangle}$. It follows that

$$\tau^\ell = \tau^{\langle 2 \rangle \cdot k + \langle 3 \rangle} = (\tau^{\langle 4 \rangle \cdot k})\tau^{\langle 5 \rangle} = (\tau^k)^{\langle 6 \rangle}\tau^{\langle 7 \rangle} = (\text{id})^{\langle 8 \rangle}\tau^{\langle 9 \rangle} = \tau^{\langle 10 \rangle}.$$

Therefore $\tau^\ell = \text{id}$ if and only if $\tau^{\langle 11 \rangle} = \text{id}$. However, we know that $\langle 12 \rangle < k$, and we also know that $\langle 13 \rangle$ is the smallest positive integer such that $\tau^{\langle 14 \rangle} = \text{id}$. Hence it must be the case that $b = \langle 15 \rangle$, which is the same thing as saying that $\text{mod}(\ell, \langle 17 \rangle) = 0$. \diamond

Can we characterize the order of a permutation that is a product of disjoint cycles? Let's explore.

Example 14.4.14. Let $\tau = (24)(16)$. Notice that (24) and (16) are disjoint, so they commute (recall Proposition 14.3.27). We also know that permutations are associative under composition. So we may compute τ^2 as follows:

$$\begin{aligned} \tau^2 &= \left((24)(16) \right) \left((24)(16) \right) \\ &= (24) \left((16)(24) \right) (16) && \text{(associative)} \\ &= (24) \left((24)(16) \right) (16) && \text{(commutative)} \\ &= \left((24)(24) \right) \left((16)(16) \right) && \text{(associative)} \\ &= \text{id id} && \text{(2-cycles have order 2)} \\ &= \text{id} \end{aligned}$$

\blacklozenge

Exercise 14.4.15.

- Let $\sigma = (237)$ and $\tau = (458)$. By following the format of Example 14.4.14, show that $(\sigma\tau)^3 = \text{id}$ (write out each step, and cite the property used).
- ** If σ and τ are disjoint cycles with $|\sigma| = |\tau| = k$, what may you conclude about $|\sigma\tau|$? (You don't need to give a proof).



◇

Associativity and commutativity are powerful tools for rearranging products of disjoint cycles, and bear in mind that any disjoint cycles commute.

Exercise 14.4.16.

- (a) Let σ and τ be *any* disjoint cycles. using associative and commutative properties (see Proposition 14.3.27, show that $(\sigma\tau)^2 = \sigma^2\tau^2$ (write out each step, and cite the property used).
- (b) If σ and τ are disjoint cycles and k is a natural number, what may you conclude about $(\sigma\tau)^k$ in terms of powers of σ and τ ? (You don't need to give a proof).

◇

Exercise 14.4.17. Suppose then $\tau = (123)(45)$. Compute each of the following

- | | | |
|--------------|--------------|--------------|
| (a) τ^2 | (c) τ^4 | (e) τ^6 |
| (b) τ^3 | (d) τ^5 | (f) τ^7 |

◇

Notice what happened to the disjoint cycles in the previous exercise. For instance $|(123)| = 3$, and in parts (a)-(f) of the exercise you had the repeating pattern $\{(132), \text{id}, (123), (132), \text{id}, \dots\}$. Similarly, the 2-cycle (45) yielded the repeating pattern $\{\text{id}, (45), \text{id}, (45), \dots\}$.

In $\tau^3, \tau^6, \tau^9, \dots$ the $(123)^k$ part of τ^k becomes id , while in $\tau^2, \tau^4, \tau^6, \dots$ the $(45)^k$ part becomes id . In order for $\tau^k = \text{id}$, we must have both $(123)^k = \text{id}$ and $(45)^k = \text{id}$, which first happens when $k = 6$. Which is the least common multiple of 2 and 3. Which makes sense. To visualize this idea, think about the question posed in the following figure:

Disjoint cycles are like gears, so they should first align back at “1”, or id , when they’ve been “turned” a number of times that is precisely the least common multiple of the number of teeth on the gears. The order of a permutation of disjoint cycles should just be the least common multiple of the orders of it’s respective cycles.

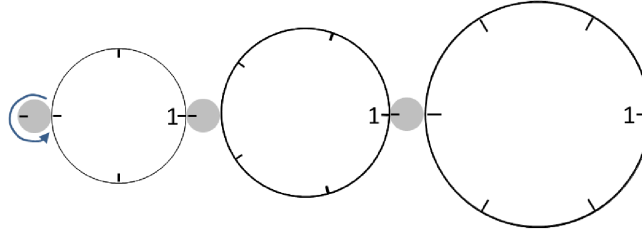


Figure 14.4.3. How many times does the small gear (at left) need to turn to return all gears to their original position? (Each turn rotates all gears clockwise by 1 position.)

In fact, we can prove it. We will start with two disjoint cycles:

Proposition 14.4.18. If σ and τ are disjoint cycles, then

$$|\sigma\tau| = \text{lcm}(|\sigma|, |\tau|),$$

where ‘lcm’ denotes least common multiple.

PROOF. Let $j \equiv |\sigma|, k \equiv |\tau|$, and $m \equiv \text{lcm}(k, j)$. Then it’s enough to prove:

- (i) $(\sigma\tau)^m = \text{id}$;
- (ii) $(\sigma\tau)^n \neq \text{id}$ if $n \in \mathbb{N}$ and $n < m$.

To prove (i), first note that k divides m , so that $m = j \cdot p$ for some natural number p . Similarly, $m = k \cdot q$ for some $q \in \mathbb{N}$. It follows:

$$\begin{aligned} (\sigma\tau)^m &= \sigma^m \tau^m && \text{(by Exercise 14.4.16)} \\ &= \sigma^{j \cdot p} \tau^{k \cdot q} && \text{(by definition of lcm)} \\ &= (\sigma^j)^p (\tau^k)^q && \text{(by exponentiation rules)}^4 \\ &= \text{id}^p \text{id}^q && \text{(by definition of order)} \\ &= \text{id} && \text{(by definition of id)}. \end{aligned}$$

To prove (ii), let $n < m$. It follows either k or j does *not* divide n . Let’s suppose it’s k (the case where it’s j is virtually identical). In this case we must have $n = p \cdot k + r$ where $p, r \in \mathbb{N}$ and $r < k$. It follows:

⁴These are the same exponentiation rules you saw in high school algebra: $x^{ab} = (x^a)^b$



$$\begin{aligned}
 (\sigma\tau)^n &= \sigma^n\tau^n && \text{(by Exercise 14.4.16)} \\
 &= \sigma^{j\cdot p+r}\tau^n && \text{(substitution)} \\
 &= (\sigma^j)^p\sigma^r\tau^n && \text{(by exponentiation rules)} \\
 &= \text{id}^p\sigma^r\tau^n && \text{(by definition of order)} \\
 &= \sigma^r\tau^n && \text{(by definition of identity)}
 \end{aligned}$$

Now since $r < k$, and $|\sigma| = k$, it follows that $\sigma^r \neq \text{id}$. Thus there is some x such that $\sigma^r(x) \neq x$. But since σ and τ are disjoint, it must be the case that $\tau(x) = x$. It follows that:

$$\sigma^r\tau^n(x) = \sigma^r(x) \neq x.$$

From this we may conclude that $(\sigma\tau)^n$ is *not* the identity. This completes the proof of (ii). \square

What Proposition 14.4.18 establishes for two disjoint cycles is also true for multiple disjoint cycles. We state the proposition without proof, because it is similar to that of Proposition 14.4.18 except with more details.

Proposition 14.4.19. Suppose $\sigma_1, \sigma_2, \dots, \sigma_n$ are n disjoint cycles, where k_1, k_2, \dots, k_n are the lengths, respectively, of the n disjoint cycles. Then

$$|\sigma_1\sigma_2\cdots\sigma_n| = \text{lcm}(k_1, k_2, \dots, k_n).$$

Now we can find the order of any permutation by first representing it as a product of disjoint cycles.

Exercise 14.4.20. What are all the possible orders for the permutations in each of the following sets (look back at your work for Exercise 14.3.38).

(a) S_6

(b) S_7

(c) S_8

\diamond

Exercise 14.4.21. Compute the following:

- (a) $|(1254)^2|$ (c) $|(13658)^{13}(1254)^{11}(473)|$
 (b) $|(13658)^2(473)^2(125)|$ (d) $|(123456789)^{300}|$

◇

Exercise 14.4.22. Let σ be a permutation in S_n .

- (a) Show that there exists an integer $k > 1$ such that $\sigma^k = \sigma$.
 (b) Show that there exists an integer $\ell > 1$ such that $\sigma^\ell = \sigma^{-1}$.
 (c) Let K be the set of *all* integers $k > 1$ such that $\sigma^k = \sigma$. Show that K is an infinite set (that is, K has an infinite number of elements).
 (d) Let L be the set of *all* integers $\ell > 1$ such that $\sigma^\ell = \sigma^{-1}$. Show that L is an infinite set.
 (e) What is the relationship between the sets K and L ?

◇

14.4.3 Transpositions and inverses

The simplest nontrivial cycles are those of length 2. We will show that these 2-cycles are convenient “building blocks” which can be used to construct all other cycles.

Definition 14.4.23. Cycles of length 2 are called *transpositions*. We will often denote transpositions by the symbol τ (the greek letter “tau”). \triangle

Exercise 14.4.24. Compute the following products:

- (a) $(14)(13)(12)$ (d) $(49)(48)(47)(46)(45)$
 (b) $(14)(18)(19)$
 (c) $(16)(15)(14)(13)(12)$ (e) $(12)(13)(14)(15)(16)(17)(18)$

◇

Exercise 14.4.25. In light of what you discovered in the previous exercise, write each cycle as a product of transpositions:



- (a) (1492) (c) (472563) (e) $(a_1a_2a_3a_5a_6)$
 (b) (12345) (d) $(a_1a_2a_3)$ (f) $(a_1a_2a_3a_5a_6a_7a_8)$

◇

The preceding exercises demonstrate the following proposition:

Proposition 14.4.26. Every cycle can be written as the product of transpositions:

$$(a_1, a_2, \dots, a_n) = (a_1a_n)(a_1a_{n-1}) \cdots (a_1a_3)(a_1a_2)$$

PROOF. The proof involves checking that left and right sides of the equation agree when they act on any a_j . We know that the cycle acting on a_j gives a_{j+1} (or a_1 , if $j = n$); while the product of transpositions sends a_j first to a_1 , then to a_{j+1} . □

Recall that we also know that any permutation can be written as a product of disjoint cycles, which leads to:

Proposition 14.4.27. Any permutation of a finite set containing at least two elements can be written as the product of transpositions.

PROOF. First write the permutation as a product of cycles: then write each cycle as a product of transpositions. □

Exercise 14.4.28. Express the following permutations as products of transpositions.

- (a) (14356) (d) (17254)(1423)(154632)
 (b) (156)(234) (e) (142637)(2359)
 (c) (1426)(142) (f) (13579)(2468)(19753)(2864)

◇

Even the identity permutation id can be expressed as the product of transpositions:

Exercise 14.4.29. Compute the following products:

- (a) $(12)(12)$ (b) $(57)(57)$ (c) $(a_1a_2)(a_1a_2)$
- (d) What can you conclude about the inverse of a transposition?

◇

The preceding exercise amounts to a proof of the following:

Proposition 14.4.30. If τ is a transposition, $\tau^{-1} = \tau$.

We can use the inverses of transpositions to build up the inverses of larger cycles:

Proposition 14.4.31. Suppose μ is a cycle: $\mu = (a_1a_2 \dots a_n)$. Then $\mu^{-1} = (a_1a_n a_{n-1} \dots a_2)$.

PROOF. By Proposition 14.4.26 we can write

$$\mu = (a_1a_n)(a_1a_{n-1}) \cdots (a_1a_3)(a_1a_2).$$

Now consider first just the last two transpositions in this expression. In the Functions chapter, we proved the formula $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ for invertible functions f and g . Since transpositions are invertible functions, we have

$$\left((a_1a_3)(a_1a_2) \right)^{-1} = (a_1a_2)^{-1}(a_1a_3)^{-1} = (a_1a_2)(a_1a_3)$$

(the second equality follows because every transposition is its own inverse.)

If we apply similar reasoning to the last three transpositions in the expression, we find

$$\left((a_1a_4)(a_1a_3)(a_1a_2) \right)^{-1} = \left[(a_1a_3)(a_1a_2) \right]^{-1}(a_1a_4)^{-1} = (a_1a_2)(a_1a_3)(a_1a_4)$$


Applying this result inductively, we obtain finally:


$$\mu^{-1} = (a_1a_2)(a_1a_3) \cdots (a_1a_{n-1})(a_1a_n),$$

from this expression we may see that $a_1 \rightarrow a_n, a_n \rightarrow a_{n-1}, a_{n-1} \rightarrow a_{n-2}, \dots, a_2 \rightarrow a_1$, which corresponds to the cycle we want. \square

Because the product of permutations is an associative operation, we may find the inverse of any product of cycles by taking the inverses of the cycles in

reverse order. (Actually, this is just a special case of the inverse of function composition: $(f_1 \circ f_2 \circ \dots \circ f_{n-1} \circ f_n)^{-1} = f_n^{-1} \circ f_{n-1}^{-1} \circ \dots \circ f_2 \circ f_1$.)


Example 14.4.32. $[(1498)(2468)]^{-1} = (2468)^{-1}(1498)^{-1} = (2864)(1894) = (164)(289)$. 

Example 14.4.33. $(1357)^{-2} = [(1357)^{-1}]^2 = (1753)^2 = (1753)(1753) = (15)(37)$. 

Exercise 14.4.34. Calculate each of the following.

- | | |
|-------------------------------|----------------------------------|
| (a) $(12537)^{-1}$ | (d) $(1254)^{-1}(123)(45)(1254)$ |
| (b) $[(12)(34)(12)(47)]^{-1}$ | (e) $(123)(45)(1254)^{-2}$ |
| (c) $[(1235)(467)]^{-2}$ | (f) $(742)^{-7}(286)^{-13}$ |



Exercise 14.4.35. In Section 14.3.5 we introduced the notion of the “cycle structure” of a permutation. Using some of the ideas that we have introduced in this section, prove that if σ is any permutation, then σ^{-1} has the *same* cycle structure as σ . 

14.5 “Switchyard” and generators of the permutation group

Switchyards are used by railroads to rearrange the order of train cars in a train (see Figure 14.5.1). In this section we will study a “switchyard” of sorts. The design of our mathematical “switchyard” is not realistic, but the example will help us understand some important fundamental properties of permutations.

Figure 14.5.2 shows how the switchyard works. The figure shows the particular case of a switchyard with 12 positions. A railroad train with 12 cars pulls in from the right, and circles around until it fills the circular track.

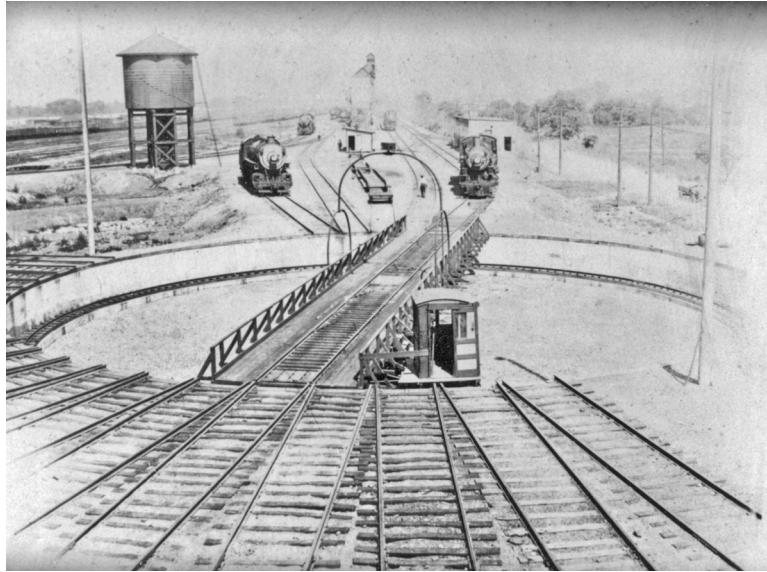


Figure 14.5.1. Grandview Yard (Pennsylvania Railroad) in Grandview Heights, OH around 1900 (source: <http://www.ghmchs.org/thisweek/photo-listing10.htm>).

The positions (we'll call them *slots* for short) are numbered 1 through 12 as are the railroad cars. At the *starting position*, each railroad car is at the corresponding numbered slot: car 1 is in slot 1, . . . car 12 is in slot 12.

From the starting position, the train can move in one of two ways:

- The train can move circularly around the track, so that car 1 can end up at any one of the 12 slots.
- Alternatively, the cars in slots 1 and 2 can switch places.

These two types of motions can be represented as permutations. In tableau notation, the first row of the tableau corresponds to the train car, while the second row corresponds to the slot it moves to. For example, if the train cars 1, 2, 3, . . . , 11, 12 move counterclockwise one slot to occupy slots 2, 3, 4, . . . , 12, 1 respectively, then the permutation (in tableau notation) is:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 1 \end{pmatrix}$$

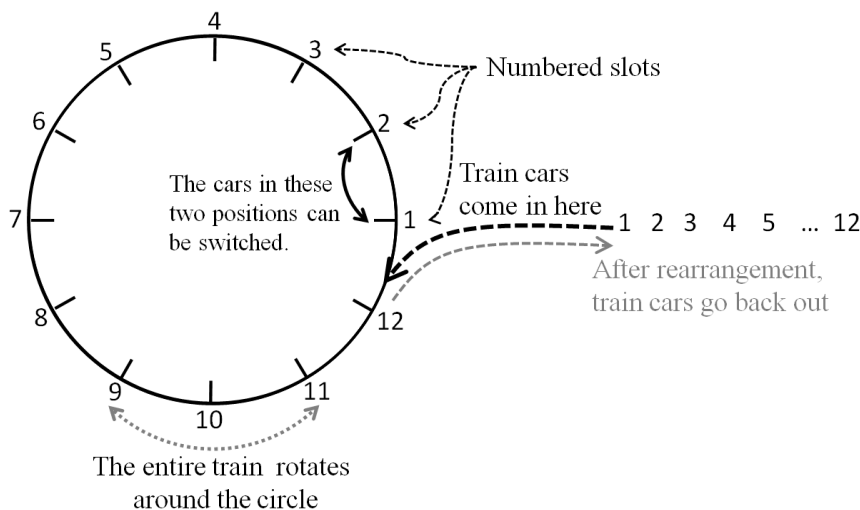


Figure 14.5.2. “Switchyard” diagram

In cycle notation, the same permutation would be $(1\ 2\ 3\ 4\ \dots\ 12)$. We will denote this permutation by r . On the other hand, if cars 1 and 2 are switched, then this corresponds to the permutation $(1\ 2)$. We will denote this permutation by t . In summary:

$$r = (1\ 2\ \dots\ 12); \quad t = (1\ 2).$$

Let’s look at some other motions of the train. Suppose for example we shift the train counterclockwise by two positions. This corresponds to performing the permutation r twice in succession, which is $r \circ r$ or r^2 . If we think about the process of composition, what’s going on is the first r moves car 1 (which occupies slot 1) to slot 2; while the second r moves whatever’s in slot 2 (which happens to be car 1) to slot 3. The resulting composition can be interpreted as showing where each of the cars end up after both moves. The same thing will be true if we compose any number of permutations.

It follows that all rearrangements of the cars that can be accomplished by the switchyard may be obtained as compositions of the permutations r and t . So what rearrangements are possible? I’m glad you asked that question! The following exercises are designed to help you figure this out. But first, let’s consider one type of rearrangement that’s particularly important. Suppose we want to switch two consecutive cars that are not 1 and 2: say for example

we want to switch cars 5 and 6, and leave the rest of the cars unchanged. Can we do this?

At this point, in order to follow along the reader may find it helpful to make his/her own model of a switchyard.⁵ Figure 14.5.3 shows a simple model made out of a jar lid with numbers stuck on with putty. We'll illus-

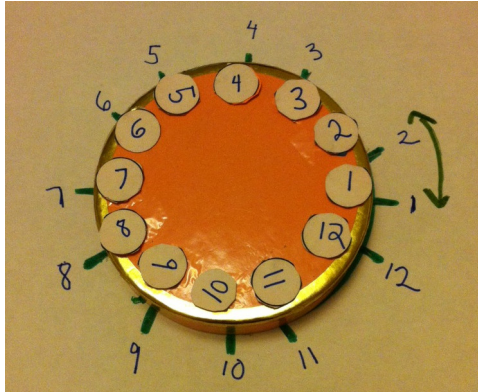


Figure 14.5.3. “Switchyard” model in home position

trate the motions necessary to switch cars 5 and 6 using the model. First, we rotate cars 5 and 6 to slots 1 and 2 by rotating 4 slots clockwise. This permutation is shown in Figure 14.5.4, and is written mathematically as r^{-4} .

Next, we exchange the two cars (which we can do since they’re in the first two positions). Figure 14.5.5 shows the switch, which is denoted by t .

Finally, all we need to do is rotate counterclockwise 4 slots (r^4), as shown in Figure 14.5.6.

Altogether, these three steps give the composition $r^4 \circ t \circ r^{-4}$ (remember that permutations are applied right to left, just like functions). Note also that in the case of a 12-slot switchyard, r^{-4} could also be written r^8 , since a clockwise rotation of 4 slots is the same as a counterclockwise rotation of 8 slots. (If the switchyard has n positions, the general rule is that $r^{-m} = r^{n-m}$, as we saw in the Symmetries chapter.)

⁵The models in this section (and photos) were made by Holly Webb.

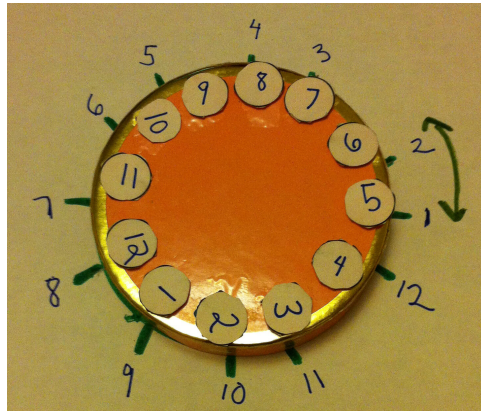


Figure 14.5.4. First stage in switching cars 5 and 6: clockwise rotation r^{-4} .

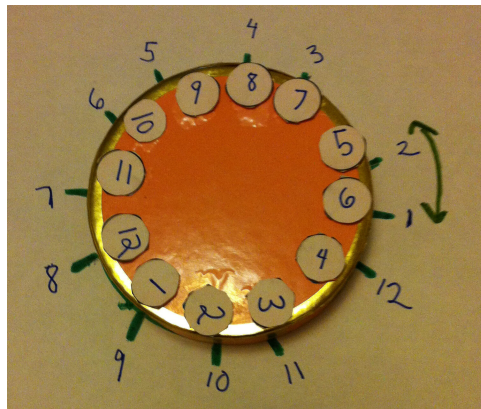


Figure 14.5.5. Second stage in switching cars 5 and 6: switch t .

Exercise 14.5.1. First we’ll look at a switchyard with 4 positions. As above, r = counterclockwise rotation by 1 position = $(1\ 2\ 3\ 4)$; while t exchanges two cars: $t = (1\ 2)$.

- Write $(2\ 3)$, $(3\ 4)$, and $(4\ 1)$ as products of powers of r and t . (Together with $(1\ 2)$, these are all the consecutive 2-cycles.)
- Write $(1\ 2\ 3)$, $(2\ 3\ 4)$, $(3\ 4\ 1)$, $(4\ 1\ 2)$ as products of powers of r and t . (These are all the counterclockwise consecutive 3-cycles.)

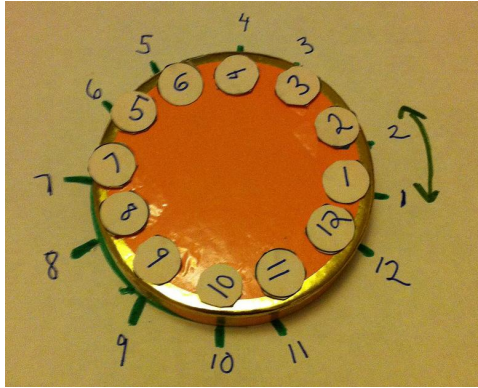


Figure 14.5.6. Third stage in switching cars 5 and 6: counterclockwise rotation r^4 .

- (c) Write (132) , (243) , (314) , (421) as products of powers of r and t . (These are all the clockwise consecutive 3-cycles.) (**Hint**)
- (d) Write (13) as products of powers of r and t .
- (e) Show that any transposition can be written as products of powers of r and t .
- (f) Show that any permutation on 4 elements (that is, any permutation in S_4) can be obtained as a product of powers of r and t .

◇

Exercise 14.5.2. Now we'll look at a general switchyard with n positions. In this case, rotation by 1 position is given by $r = (1\ 2\ \dots\ n)$. We use the same switch transposition, $t = (1\ 2)$.

- (a) Write the transposition $(k\ k \oplus 1)$ as a product of powers of r and t . Here \oplus denotes addition mod n . (Note that we use $(k\ k \oplus 1)$ instead of $(k\ k+1)$ because we want to count $(n\ 1)$ as a consecutive transposition.)
- (b) Show that any consecutive cycle of the form $(m\ m \oplus 1\ \dots\ m \oplus p)$ can be written as a product of powers of r and t by filling in the blanks:
- First, $(m\ m \oplus 1\ \dots\ m \oplus p)$ can be written as a product of consecutive transpositions as _____ (**Hint**)

- Then, by replacing each transposition in this expression with its expression in terms of products of _____, then we obtain an expression for _____ as a product of _____.
- (c) Write the transposition $(1\ k)$ as a product of a consecutive cycle of length k and the inverse of a consecutive cycle of length $k - 1$. (**Hint**)
- (d) Prove that any transposition $(1\ k)$ can be written as a product of consecutive transpositions.
- (e) Prove that any transposition $(1\ k)$ can be written as a product of powers of r and t .
- (f) Prove that any transposition $(p\ q)$ can be written as a product of powers of r and t .
- (g) Prove that any permutation in S_n can be obtained as a product of powers of r and t .

◇

What we have shown in the previous exercise is that the two permutations r and t *generate* the group S_n . In other words, all of the information contained in the huge and complicated group S_n is characterized in just two permutations! The study of group generators is an important part of group theory, but unfortunately it is beyond the level of this course.

Exercise 14.5.3. Using “switchyard”, we proved that S_n is generated by the permutations (12) and $(12\dots n)$. Prove that the group S_n is generated by the following sets of permutations.

1. $(12), (13), \dots, (1n)$
2. $(12), (23), \dots, (n - 1, n)$

◇

14.6 Other groups of permutations

14.6.1 Even and odd permutations

We saw in the previous section that any permutation can be represented as a product of transpositions. However, this representation is not unique. Consider for instance:

- $\text{id} = (12)(12)$
- $\text{id} = (13)(24)(13)(24)$
- $\text{id} = (15)(26)(79)(14)(34)(34)(14)(79)(26)(15)$

Although these representations of id are vastly different, by some “strange coincidence” they all involve the product of an even number of transpositions.

Exercise 14.6.1. ***** Write id as a product of an odd number of transpositions (If you succeed, you automatically get an A in this course!) \diamond

As you might guess from the previous exercise, there’s something fishy going on here. To get to the bottom of this, we need to get a better handle on what happens when you multiply a permutation by a transposition. In particular, we know that any permutation can be written as a product of disjoint cycles: so what happens to these cycles when we multiply by a transposition? To get warmed up, let’s first look at some special cases.

Exercise 14.6.2. Write $\tau\sigma$ as the products of disjoint cycles, where $\sigma = (12345678)$ and: (a) $\tau = (25)$; (b) $\tau = (16)$; (c) $\tau = (48)$; (d) $\tau = (35)$. \diamond

As always it is helpful to have a good representation of the situation, preferably in pictures. For the following argument, we will represent a cycle as a “pearl necklace”, as shown in Figure 14.6.1. This is not so different from our previous representation of cycles (for instance, in Figure 14.3.1), but we are not including labels for the particular elements in the cycle because we want to emphasize the general structure and not get bogged down in details.

Figure 14.6.2 shows how we may represent the multiplication $(ab)C$ of transposition (ab) with cycle C , where a and b are elements included within C . The transposition effectively redirects the arrow pointing into a , so that

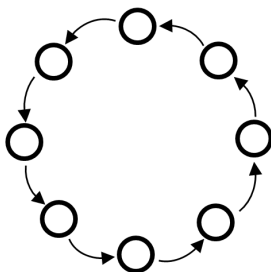


Figure 14.6.1. “Pearl necklace” representation of a cycle.

now it points into b . The transposition also redirects the arrow pointing into b so that it now points into a . As a result, there are now two cycles instead of one. The sum of the lengths of the two cycles is equal to the length of the original cycle.

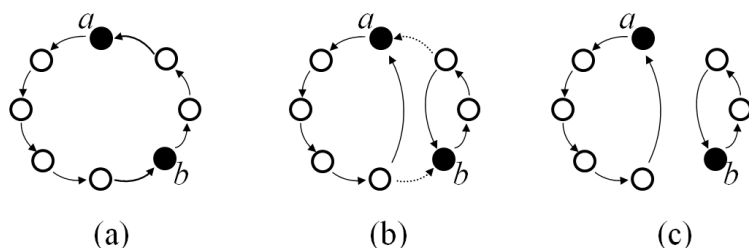


Figure 14.6.2. (a) Cycle C , including elements a and b ; (b) Product of transposition (ab) with cycle C , showing redirection of arrows into a and b ; (c) The result of $(ab)C$ is two separate cycles.

Using this representation, we can now investigate what happens when we multiply a transposition (ab) times an *arbitrary* permutation σ . We already know that σ can be thought of as a collection of disjoint cycles (plus stationary elements, that are unaffected by σ). There are several possibilities for how a and b can fit within the cycles of σ , as shown in Figure 14.6.3. Each possibility may or may not change the number of cycles, as well as the sum of the lengths of all cycles.

Exercise 14.6.3. In each of the following situations, we are considering the multiplication of a transposition (ab) with a permutation σ . Match

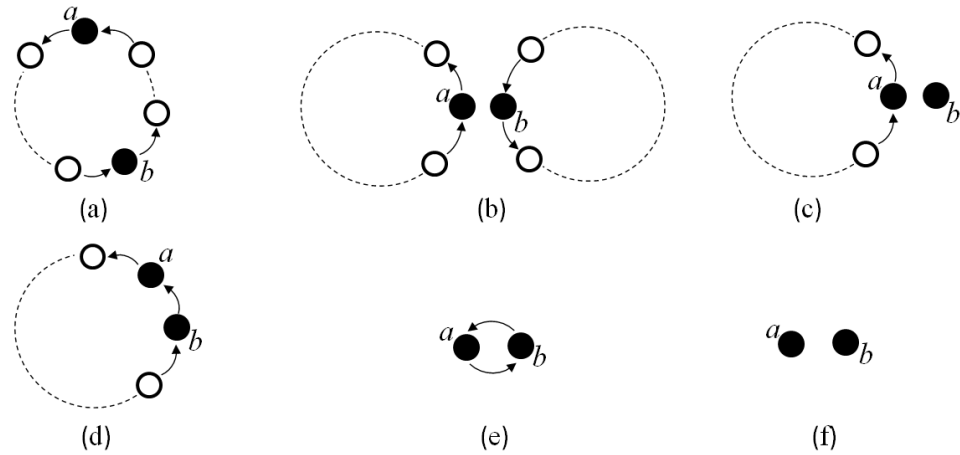


Figure 14.6.3. Multiplication of (ab) times a permutation σ , showing the different ways that a and b can be situated within the cycles and stationary elements of σ . Note that case (a) corresponds to the situation described in Figure 14.6.2.

each situations to the correct case (a)–(f) in Figure 14.6.3. For example, $(ab) = 12$ and $\sigma = (1234)(567)$ corresponds to case (d), because a and b are consecutive elements in one of the cycles of σ .

(a) $(ab) = (36), \sigma = (123)(456)(78)$

(b) $(ab) = (45), \sigma = (123)(678)$

(c) $(ab) = (34), \sigma = (123)(567)$

(d) $(ab) = (45), \sigma = (23)(45)(67)$

(e) $(ab) = (34), \sigma = (278)(13546)$

◇

Exercise 14.6.4. Draw a set of pictures (similar to Figure 14.6.2(c)) for each of the possibilities (a)–(f) in Figure 14.6.3 showing the effect of the transposition (ab) on the cycles. Keep in mind that the transposition merely redirects the arrows into a and b so that they point into b and a , respectively.

◇

Exercise 14.6.5. Using your results from the previous exercise, complete Table 14.1. \diamond

| Diagram in Fig. 14.6.3 | Change in number of cycles | Change in sum of cycle lengths | Is column 3 minus column 2 even or odd? |
|------------------------|----------------------------|--------------------------------|---|
| (a) | +1 | 0 | odd |
| (b) | ----- | ----- | ----- |
| (c) | ----- | ----- | ----- |
| (d) | ----- | ----- | ----- |
| (e) | -1 | -2 | ----- |
| (f) | ----- | ----- | ----- |

Table 14.1: Multiplication of permutation by transpositions

If you did the previous exercise correctly, you will find that no matter where the transposition falls, the entry in the last column is always ‘odd’. Consider what this means. Suppose I have a permutation σ whose sum of cycle lengths minus number of cycles is equal to N . I then multiply σ by a transposition to obtain another permutation τ , whose sum of cycle lengths minus number of cycles is equal to M . The last column of Table 14.1 shows that it must be true that $M - N$ is *always* odd. In other words, if M is even then N is odd: and vice versa. We may express this concisely using the following definition:

Definition 14.6.6. for any permutation σ written in disjoint cycle notation, the number

$$\text{mod}(\text{sum of cycle lengths minus number of cycles}, 2)$$

is called the **parity** of σ . A permutation with parity 0 is called an **even permutation**, while a permutation with parity 1 is called an **odd permutation**. Often books will use the terms “even parity” and “odd parity” instead of parity 0 and 1, respectively. \triangle

We may summarize our argument so far as follows:

Proposition 14.6.7. Given a permutation σ and a transposition (ab) , then the parity of $(ab)\sigma$ is different from the parity of σ .

So far we have considered multiplying permutations on the *left* by a transposition. What about multiplying them on the *right*? It turns out we can use the “direction-reversing” property of permutation inverses to answer this very elegantly.

Exercise 14.6.8.

- (a) Consider the “necklace” diagrams (a)-(f) of permutations shown in Figure 14.6.3. If we take the *inverse* of each permutation, how does its diagram change? What happens to the arrows? How do the shapes of the cycles change (if at all)?
- (b) In Exercise 14.6.4 you multiplied each of the permutations (a)-(f) in Figure 14.6.3 on the left by (ab) . How do the results change if you multiply the *inverses* of each permutation on the left by (ab) ?
- (c) Prove that $((ab)\sigma^{-1})^{-1} = \sigma(ab)$.
- (d) Using (a-c) above, prove the following statement: For any permutation σ and any transposition (ab) , $(ab)\sigma$ and $\sigma(ab)$ have the same cycle structure.

◇

Now here’s the punch line. We know that *every* permutation can be written as a product of transpositions. From what we have just shown, an odd permutation must be the product of an odd number of transpositions; while an even permutation must be the product of an even number of transpositions. It is *impossible* to write an even permutation as the product of an odd number of transpositions; and vice versa. We summarize our conclusions in the following proposition.

Proposition 14.6.9. A permutation σ can be written as the product of an even number of transpositions if and only if σ is an even permutation. Also, σ can be written as the product of an odd number of transpositions if and only if σ is an odd permutation.

Exercise 14.6.10. Prove that it is impossible to write the identity permutation as the product of an odd number of transpositions. \diamond

Exercise 14.6.11. Suppose σ is an n -cycle. How can you tell whether σ is an even or odd permutation? \diamond

In the following exercises you will explore a bit further the parity properties of permutations.

Exercise 14.6.12.

- (a) Prove that the product of two even permutations is even.
- (b) Prove that the product of two odd permutations is even.
- (c) What is the parity of the product of an even permutation and an odd permutation? What about the product of an odd permutation and an even permutation? *Prove* your answers.

\diamond

Exercise 14.6.13. For each of the following sets, describe which permutations are even and which are odd, according to their cycle structure. (**Hint**)

- (a) S_6
- (b) S_7
- (c) S_8

\diamond

Exercise 14.6.14. This exercise requires some knowledge of linear algebra. It also relates back to the discussion of Levi-Civita symbols in Section 11.8.1

Suppose σ is a permutation in S_4 . We can define a 4×4 matrix P_σ using index notation as follows:

$$[P_\sigma]_{ij} = \begin{cases} 1 & \text{if } j = \sigma(i), \\ 0 & \text{if } j \neq \sigma(i). \end{cases}$$

(Here i and j can take any values from 1 to 4.) The matrix P_σ is in fact known as the *permutation matrix* associated with the permutation σ .

- (a) Write down the matrix P_σ when: (i) $\sigma = (13)$; (ii) $\sigma = (132)$; (iii) $\sigma = (12)(34)$; (iv) $\sigma = (1234)$.
- (b) Using the formula that you guessed in the previous problem, evaluate $\det P_\sigma$ when: (i) $\sigma = (24)$; (ii) $\sigma = (143)$; (iii) $\sigma = (14)(23)$; (iv) $\sigma = (1423)$. Check your answer using the row (or column) expansion method for computing determinants.
- (c) How is the value of $\det P_\sigma$ related to the “evenness” or “oddness” of the permutation σ ?
- (d) For the 4 permutations in part (a), show that when you multiply the 4×1 column vector $[1, 2, 3, 4]^T$ times the matrix P_σ , you obtain the second row of the tableau for σ . In other words, the matrix P_σ “performs” the permutation σ on column vector entries.
- (e) Show that the result in (b) is true in general: namely, that $P_\sigma[1, 2, 3, 4]^T = [\sigma(1), \sigma(2), \sigma(3), \sigma(4)]^T$.

◇

14.6.2 The alternating group

We have shown that all permutations are either even or odd. In other words, for any $n \in \mathbb{Z}$ we have that S_n is the union of two disjoint sets: $S_n = A_n \cup B_n$, where A_n and B_n are the even and odd permutations respectively. We are particularly interested in the set A_n , because it has nice properties with respect to product of permutations:

Exercise 14.6.15.

- (a) Show that $\text{id} \in A_n$.
- (b) Show that if $\sigma \in A_n$, then $\sigma^{-1} \in A_n$. (*Hint*)
- (c) Show that if $\sigma, \mu \in A_n$, then $\sigma\mu \in A_n$. (*Hint*)

◇

In light of the previous exercise, it’s beginning to look like A_n could be a group under permutation product. Let’s check off the group properties:

- Is A_n closed under permutation product? Yes, according to Ex. 14.6.15(c).
- Does A_n have an identity element? Yes, according to Ex. 14.6.15(a).
- Does A_n have inverses for every element? Yes, according to Ex. 14.6.15(b).
- Is A_n associative? Yes, because the operation is composition, and composition is associative.

We have thus essentially proven the following proposition:

Proposition 14.6.16. The set A_n is a group.

Definition 14.6.17. The group A_n of even permutations is called the *alternating group on n numbers*. \triangle

Exercise 14.6.18. Prove or disprove: the set of odd permutations B_n is also a group. \diamond

We know that A_n is a group – but how big is it? Of course, it depends on the number of odd permutations B_n , since A_n and B_n together make up S_n . So which is bigger: A_n or B_n ? The answer is ... neither!

Proposition 14.6.19. The number of even permutations in S_n , $n \geq 2$, is equal to the number of odd permutations; hence, $|A_n| = n!/2$.

PROOF. The key to the proof is showing that there is a *bijection* between A_n and B_n . Since a bijection is one-to-one and onto, this means that A_n and B_n must have exactly the same number of elements.

To construct a bijection, notice that $(12) \in S_n$ and define a function $f : A_n \rightarrow S_n$ by: $f(\sigma) = (12) \circ \sigma$. (Notice that we are taking A_n as our domain, and not S_n). To show that f is a bijection, we need to show three things:

- B_n is a valid codomain for f : that is, $f(\sigma) \in B_n \forall \sigma \in A_n$;
- $f : A_n \rightarrow B_n$ is onto: that is, $\forall \mu \in B_n \exists \sigma \in A_n$ such that $f(\sigma) = \mu$;
- f is one-to-one: that is, $f(\sigma_1) = f(\sigma_2)$ implies $\sigma_1 = \sigma_2$.

Parts (a) – (c) will be proven by (none other than) you, in the following exercise:

Exercise 14.6.20.

- (a) Show part (a). ([*Hint*](#))
- (b) Show part (b). ([*Hint*](#))
- (c) Show part (c). ([*Hint*](#))

◇

□

Exercise 14.6.21.

- (a) What is $|A_4|$?
- (b) List all the permutations of A_4 (Write them in cycle notation. Make sure you have them all – you should have as many as part (a) indicates).

◇

Exercise 14.6.22. Give all possible cycle structures for elements in each of the following sets. (You don't need to list all the permutations, just the cycle configurations e.g. “pair of 2-cycles”.)

- (a) A_6
- (b) A_7
- (c) A_8

◇

14.7 Additional exercises

1. Show that A_{10} contains an element of order 15. ([*Hint*](#))
2. Does A_8 contain an element of order 26?
3. Find an element of largest order in S_n for $n = 3, \dots, 10$.

4. In Chapter 4 we used the term ‘non-abelian’ to describe groups in which not all elements commute. To show that a group is non-abelian, it’s enough to find a single pair of elements $a, b \in S_n$ which do not commute (that is, $ab \neq ba$).
- Prove that S_n is non-abelian for every $n \geq 3$.
 - Show that A_n is non-abelian for every $n \geq 4$.
 - Prove that D_n is non-abelian for every $n \geq 3$.
5. Let $\sigma \in S_n$. Prove that σ can be written as the product of at most $n - 1$ transpositions. (*Hint*)
6. Let $\sigma \in S_n$. If σ is not a cycle, prove that σ can be written as the product of at most $n - 2$ transpositions. (*Hint*)
7. Prove that in A_n with $n \geq 3$, any permutation is a product of cycles of length 3.
8. Let G be a group and define a function $f_g : G \rightarrow G$ by $f_g(a) = ga$. Prove that f_g is a permutation of G .
9. For α and β in S_n , we say that α and β are **conjugate permutations** if there exists an $\sigma \in S_n$ such that $\sigma\alpha\sigma^{-1} = \beta$. Show that if α and β are conjugate permutations, and $\alpha \in A_n$, then also $\beta \in A_n$.
10. Let $\tau = (a_1, a_2, \dots, a_k)$ be a cycle of length k .
- Prove that if σ is any permutation, then $\sigma\tau\sigma^{-1}$ can be expressed as:

$$\sigma\tau\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)).$$
 it follows that $\sigma\tau\sigma^{-1}$ is also a cycle of length k .
 - Let μ be any cycle of length k . Prove that there is a permutation σ such that $\sigma\tau\sigma^{-1} = \mu$.
 - Using the notation of the previous exercise, show that any two cycles of length k are conjugate.
11. Show that $\alpha^{-1}\beta^{-1}\alpha\beta$ is an even permutation for all $\alpha, \beta \in S_n$.

14.8 Hints for “Permutations” exercises

Exercise 14.4.13: The first blank should be replaced by k

Exercise 14.5.1(c): Take advantage of the previous part.

Exercise 14.5.2(b): Note for instance that $(1\ 2\ 3) = (1\ 2)(2\ 3)$.

Exercise 14.5.2(c): Note for instance that $(1\ 4) = (1\ 2\ 3\ 4) \circ (1\ 2\ 3)^{-1}$.

Exercise 14.6.13: Use the cycle structures you found in Exercise 14.3.38

Exercise 14.6.15(b): If you write σ as the product of transpositions $\tau_1 \cdots \tau_n$, then what is σ^{-1} ?

Exercise 14.6.15(c): If $\sigma = \tau_1 \cdots \tau_n$ and $\mu = \lambda_1 \cdots \lambda_m$, then what about $\sigma\mu$?

Exercise 14.6.20(a): If σ is even, then what about $(1\ 2) \circ \sigma$?

Exercise 14.6.20(b): If μ is odd, then what about $(1\ 2) \circ \mu$? Also, what is $f((1\ 2) \circ \mu)$?

Exercise 14.6.20(c): If $(1\ 2)\sigma_1 = (1\ 2)\sigma_2$, then what can you conclude about σ_1 and σ_2 ? Why are you able to conclude this?

Exercise 14.4.11: Let ℓ be the length of σ : then what is the order of σ ? On the other hand, let k be the order of σ^2 : then what do you know about σ^{2k} ?

14.8.1 Hints for additional exercises (Section 14.7)

Exercise 1: Consider the cycle structure.

Exercise 5: We know that σ can be written as the product of disjoint cycles. So let $\sigma_1, \sigma_2, \dots, \sigma_m$ be disjoint cycles such that $\sigma = \sigma_1\sigma_2 \dots \sigma_m$, and let ℓ_j be the length of the cycle σ_j . How many transpositions does it take to construct each of these disjoint cycles? And what is the largest possible value of the sum of ℓ_j ?

Exercise 6: Use the notation of the previous problem, and write a formula (in terms of $\ell_1 \dots \ell_m$ and m) for the number of transpositions it takes to construct σ .

Introduction to Groups

“There are more groups in heaven and earth, Horatio, than are dreamt of in your philosophy.” Shakespeare, *Hamlet*, Act 1 Scene V (paraphrase by J. Hill)

“Groups tend to be more extreme than individuals.” (Daniel Kahneman, 2002 Nobel Prize winner in Economics)

“I am rarely bored alone; I am often bored in groups.” (Dr. Laurie Helgoe, psychologist)

You may have noticed that we have been voyaging deeper and deeper into unfamiliar mathematical territory. We’re using more symbols and fewer numbers. We introduce unfamiliar terminology and strange notation. We deal with outlandish mathematical objects that are harder and harder to visualize.

Please rest assured that these elaborations have a practical purpose¹. We live in a complicated world, and complicated mathematical structures are needed to describe it well. However, underlying this confusing tangle of complicated structures are some deep commonalities. The purpose of abstraction is to identify and characterize these commonalities. In this way we can make connections between very different fields of mathematics, and gain a much more holistic view of how things work together.

One of the commonalities that we have been (more or less) subtly emphasizing in the previous chapters is the ubiquity of *groups*, together with

¹(that is, besides tormenting math students)

related notions such as isomorphisms and subgroups. Now that you've studied several specific groups (such as \mathbb{C} , \mathbb{Z}_n , D_n , S_n , A_n and so on) our hope is that from these examples you've begun to get a feel for how groups work, and how one should think about groups in general. In this chapter, we will study groups *in the abstract*: that is, we will describe properties that are common to *all* groups, whether finite or infinite, commutative (abelian) or non-abelian, and so on.

Thanks to Tom Judson for material used in this chapter.

15.1 Formal definition of a group

Historically, the theory of groups first arose from attempts to find the roots of polynomials in terms of their coefficients. But groups have moved far beyond their original application, and now play a central role in such areas as coding theory, counting, and the study of symmetries. Many areas of biology, chemistry, and physics have benefited from group theory. In the preceding chapters we've already worked with a number of different groups, including the integers mod n and the symmetries of a rectangle or regular polygon. Recall that a group basically consists of a set and a "compatible" operation:

Exercise 15.1.1.

- (a) What operation is the set \mathbb{Z}_n a group under?
- (b) What operation is the set S_3 a group under?

◇

The following definition formalizes the notion of "operation".

Definition 15.1.2. A *binary operation* or *law of composition* on a set G is a function $G \times G \rightarrow G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b$, or ab in G , called the *composition* of a and b . △

Remark 15.1.3.

- Notice that the word "composition" is now used to denote any operation on the elements of a set, and not just composition of functions.
- When the law of composition on a set is a basic algebraic operation such as multiplication or addition, we'll call it with its usual name. When it isn't, we will often refer to $a \circ b$ as the "product" of a and b (as we did in the Permutations chapter).

△

In the Modular Arithmetic chapter we introduced what properties a set and operation must have to be called a group:

Exercise 15.1.4. What are the four properties a set G and a binary operation must exhibit in order for the set to be a group under that binary operation? ◇

Building on our previous discussion, we now proudly present the following formal definition.

Definition 15.1.5. A *group* (G, \circ) is a set G together with a law of composition $(a, b) \mapsto a \circ b$ that satisfies the following axioms.

1. The set G is *closed* under the law of composition. That is,

$$\forall a, b \in G, a \circ b = c \text{ for some } c \in G.$$

2. There exists an element $e \in G$, called the *identity element*, such that for any element $a \in G$

$$e \circ a = a \circ e = a.$$

3. For each element $a \in G$, there exists an *inverse element* in G , denoted by a^{-1} , such that

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

4. The law of composition is *associative*. That is,

$$(a \circ b) \circ c = a \circ (b \circ c)$$

for $a, b, c \in G$.

△

Remark 15.1.6. When the group operation is obvious or has been previously specified, we may denote the group by G rather than (G, \circ) . For instance, the group of integers under addition is typically denoted by \mathbb{Z} and not $(\mathbb{Z}, +)$, since the operation $+$ is understood. △

One very important class of groups is the commutative groups, which are given their own special designation:

Definition 15.1.7. A group (G, \circ) with the property that $a \circ b = b \circ a$ for all $a, b \in G$ is called *abelian*² or *commutative*. Groups not satisfying this property are said to be *non-abelian* or *noncommutative*. △

Finally, based on our discussion before about the order of sets, we have:

Definition 15.1.8. A group is *finite*, or has *finite order*, if it contains a finite number of elements. The *order* of a finite group is the number of elements that it contains. If G is a group containing n elements, we write $|G| = n$. A group that is not finite is called *infinite*, and such a group is said to be of *infinite order*. △

The group \mathbb{Z}_5 is a finite group of order 5, so $|\mathbb{Z}_5| = 5$; while the integers \mathbb{Z} form an infinite group under addition, and we sometimes write $|\mathbb{Z}| = \infty$.

Definition 15.1.9. The *trivial group*, consists of the single element e (or id , in our previous notation). △

Exercise 15.1.10. Prove that the trivial group is in fact a group according to Definition 15.1.5. ◇

²In honor of Neils Henrik Abel (1802-1829), an astounding mathematician who sadly died very young of tuberculosis. There is some discussion among mathematicians over whether ‘abelian’ should be capitalized. The word has become so common in mathematics that it’s usually treated as a regular word and not a proper name. This should be considered as a special honor to Abel, since his name has become part of the fundamental language of mathematics.

15.2 Examples

There are multitudes upon multitudes of groups besides those we've seen so far. Some are modifications of groups we are very familiar with.

Example 15.2.1. The set $\mathbb{R} \setminus \{0\}$ of non-zero real numbers is written as \mathbb{R}^* . Let's prove that (\mathbb{R}^*, \cdot) is a group.

(1) Closure:

Suppose $a, b \in \mathbb{R}^*$. Then to prove closure we must show $ab \in \mathbb{R}^*$; that is, we must show (i) $ab \in \mathbb{R}$ and (ii) $ab \neq 0$:

(i): Since $a, b \in \mathbb{R}$, and we know \mathbb{R} is closed under multiplication, then $ab \in \mathbb{R}$.

(ii): Suppose $ab = 0$. Then as we noted in Section 3.2.1, we know either $a = 0$ or $b = 0$. But $a, b \in \mathbb{R}^*$; i.e. $a, b \neq 0$. So we have a contradiction. Hence $ab \neq 0$.

Therefore $ab \in \mathbb{R}^*$; and so \mathbb{R}^* is closed under multiplication.

To finish the proof that \mathbb{R}^* is a group, we must establish axioms (2) through (4) in Definition 15.1.5. We leave this up to you in the following exercise:

Exercise 15.2.2.

- (a) Finish proving that (\mathbb{R}^*, \cdot) is a group.
- (b) Either prove or disprove that $(\mathbb{R}^*, +)$ is a group.
- (c) What is the order of (\mathbb{R}^*, \cdot) ?

◇

◆

Exercise 15.2.3. Let \mathbb{C}^* be the set of non-zero complex numbers.

- (a) Why is \mathbb{C}^* not a group under the operation of complex addition?
- (b) Prove \mathbb{C}^* is a group under the operation of (complex) multiplication.

- (c) What is $|(\mathbb{C}^*, \cdot)|$?
- (d) Is (\mathbb{C}^*, \cdot) an abelian group? Justify your answer.

◇

Remark 15.2.4. Groups based on sets of numbers that *include* 0 (such as $\mathbb{R}, \mathbb{C}, \mathbb{Q}$) are assumed to have the group operation $+$ (unless otherwise stated). For groups based on sets of numbers that *exclude* 0 such as $\mathbb{R}^*, \mathbb{C}^*, \mathbb{Q}^*$, the group operation is assumed to be multiplication (unless otherwise stated). \triangle

Exercise 15.2.5.

- (a) Why is it impossible for a set of complex numbers S which has more than one element and includes 0 to be a group under multiplication? Why is the condition $|S| > 1$ necessary?
- (b) Why is it impossible for a set of complex numbers S that excludes 0 to be a group under addition?

◇

Some groups use exotic operations that you may never have seen before:

Example 15.2.6. Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = (a + b) + (ab)$. It turns out that $(S, *)$ is an abelian group. We will prove closure and the commutative property; the rest of the proof will be left to you.

- (a) Closure: Suppose $a, b \in S$. We need to show that $a * b \in S$; i.e. firstly that $a * b \in \mathbb{R}$ and secondly $a * b \neq -1$. First, since both addition and multiplication are closed in \mathbb{R} , it follows that $(a + b) + (ab) \in \mathbb{R}$ and hence $a * b \in \mathbb{R}$. For the second point, we will use a contradiction argument and suppose that $a * b = -1$, i.e. $(a + b) + (ab) = -1$. Using basic algebra to rearrange this expression, we get $a(b - 1) = -(b - 1)$, which implies that either $a = -1$ or $b = -1$. But a and b are assumed to be in S , so this is a contradiction. Hence $a * b = -1$ is impossible, and the proof is complete.

- (b) Commutativity: Suppose $a, b \in S$. We need to show that $a * b = b * a$:
 By the definition of the operation $*$ we have $a * b = (a + b) + (ab)$,
 which is equal to $(b + a) + (ba)$ since addition and multiplication in \mathbb{R}
 are commutative. Since $b * a = (b + a) + (ba)$ by definition, it follows
 that $a * b$ is commutative.

Exercise 15.2.7. Finish the proof that $(S, *)$ is an abelian group. \diamond



The following example shows a famous (among mathematicians!) group
 that has important applications in physics:

Example 15.2.8. The *quaternion group* (denoted by Q_8) consists of 8
 elements, which are commonly denoted as follows: $1, i, j, k, -1, -i, -j,$
 $-k$. The binary operation for Q_8 is determined by the following relations:

- 1 is the identity;
- -1 commutes with all other elements, and $(-1)^2 = 1$;
- $-1 \cdot i = -i, -1 \cdot j = -j, -1 \cdot k = -k$;
- $i^2 = j^2 = k^2 = -1$.
- $i \cdot j = k, j \cdot k = i, k \cdot i = j$;
- $j \cdot i = -k, k \cdot j = -i, i \cdot k = -j$.



Exercise 15.2.9.

- (a) Use the information given above to complete the Cayley table for Q_8 .
- (b) From the Cayley table, deduce that Q_8 is closed under the binary operation we have defined above.
- (c) Find the inverses of all of the elements of Q_8 .

◇

Example 15.2.10. Recall that any point in the plane can be represented in Cartesian plane as a pair of real numbers (x, y) . We may consider these points as 2-dimensional vectors, which can be added via the usual vector addition rule. For example, $(0.5, 0.9) + (1.2, 3.4) = (0.5 + 1.2, 0.9 + 3.4) = (1.7, 4.3)$. The general formula for addition of two vectors (x_1, y_1) and (x_2, y_2) is

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Let us show that 2-d vectors in the Cartesian plane form a group. First, we prove closure. Closure means that the sum of two 2-d vectors is also a 2-d vector. This follows from the formula $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, and since $x_1 + x_2$ and $y_1 + y_2$ are both real numbers it follows that $(x_1 + x_2, y_1 + y_2)$ is also a 2-d vector.

Next, we prove that 2-d vectors have an identity. For any 2-d vector (x, y) we have $(x, y) + (0, 0) = (x, y)$ and $(0, 0) + (x, y) = (x, y)$. It follows that $(0, 0)$ is the identity for 2-d vectors.

Next, we show that 2-d vectors have inverses. For any 2-d vector (x, y) we have $(x, y) + (-x, -y) = (0, 0)$ and $(-x, -y) + (x, y) = (0, 0)$. It follows that any 2-d vector (x, y) has an inverse $(-x, -y)$.

Finally, we show that 2-d vectors are associative. For any three 2-d vectors (x_1, y_1) , (x_2, y_2) , (x_3, y_3) we have

$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = (x_1, y_1) + (x_2 + x_3, y_2 + y_3) = (x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)).$$

We also have

$$((x_1, y_1) + (x_2, y_2)) + (x_3, y_3) = (x_1 + x_2, y_1 + y_2) + (x_3, y_3) = ((x_1 + x_2) + x_3, (y_1 + y_2) + y_3).$$

By associativity of ordinary addition of real numbers, we have $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$ and $y_1 + (y_2 + y_3) = (y_1 + y_2) + y_3$. It follows therefore by substitution that

$$(x_1, y_1) + ((x_2, y_2) + (x_3, y_3)) = ((x_1, y_1) + (x_2, y_2)) + (x_3, y_3)$$

, and we have shown that 2-d vectors are associative. ◆

In the previous example, it seems that we have built up the group of 2-d vectors from two copies of the real numbers. In fact we may generalize this procedure, and use pairs of groups to build up other groups.

Exercise 15.2.11. Let $H = \mathbb{Z} \times \mathbb{Z}$ (all integer coordinate-pairs).

- (a) Define a binary operation \circ on H by $(a, b) \circ (c, d) = (a + c, b + d)$, for $(a, b), (c, d) \in H$. This operation is in fact just coordinate-pair addition. Is (H, \circ) a group? If so, is (H, \circ) abelian? Justify your answers.
- (b) Define a binary operation \circ on H by $(a, b) \circ (c, d) = (ac, bd)$, for $(a, b), (c, d) \in H$. This is just coordinate-pair multiplication. Is (H, \circ) a group? If so, is (H, \circ) abelian? Justify your answers.

◇

Exercise 15.2.12. Let $G = \mathbb{R}^* \times \mathbb{Z}$ (all pairs such that the first element is a nonzero real number, and the second is an integer)

- (a) Define a binary operation \circ on G by $(a, m) \circ (b, n) = (a + b, m + n)$. Is (G, \circ) a group? If so, is (G, \circ) abelian? Justify your answers.
- (b) Define a binary operation \circ on G by $(a, m) \circ (b, n) = (ab, mn)$. Is (G, \circ) a group? If so, is (G, \circ) abelian? Justify your answers.
- (c) Define a binary operation \circ on G by $(a, m) \circ (b, n) = (ab, m + n)$. Is (G, \circ) a group? If so, is (G, \circ) abelian? Justify your answers.

◇

The previous two exercises follow a pattern that we may generalize:

Definition 15.2.13. Given two groups G and H , we define the *product* of groups G and H (denoted by $G \times H$) as the set of pairs $\{(g, h), g \in G, h \in H\}$. If (g_1, h_1) and (g_2, h_2) are two elements of $G \times H$, then we define the group operation $(g_1, h_1) \circ (g_2, h_2)$ as follows:

$$(g_1, h_1) \circ (g_2, h_2) := (g_1 g_2, h_1 h_2),$$

where $g_1 g_2$ uses the group operation in G and $h_1 h_2$ uses the group operation in H . △

Exercise 15.2.14.

- (a) Consider $(3, 6)$ and $(2, 4)$ as elements of $\mathbb{Z}_7 \times \mathbb{Z}_7$. Compute $(3, 6) \circ (2, 4)$.

(b) Consider $(3, 6)$ and $(2, 4)$ as elements of $\mathbb{R}^* \times \mathbb{Z}_{10}$. Compute $(3, 6) \circ (2, 4)$.

(c) Consider $(3, 6)$ and $(2, 4)$ as elements of $\mathbb{Q}^* \times \mathbb{Q}^*$. Compute $(3, 6) \circ (2, 4)$.

◇

Exercise 15.2.15. Show that the product of two groups is a group. ◇

Exercise 15.2.16. Let $\mathbb{Z}_2^n = \{(a_1, a_2, \dots, a_n) : a_i \in \mathbb{Z}_2\}$. Define a binary operation on \mathbb{Z}_2^n (which we will denote as ‘+’) by

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 \oplus b_1, a_2 \oplus b_2, \dots, a_n \oplus b_n),$$

where \oplus denotes addition in \mathbb{Z}_2 . Prove that \mathbb{Z}_2^n is a group under this operation. This group is important in algebraic coding theory. ◇

In previous chapters we’ve used Cayley tables to describe group operations. With Cayley tables we can prove a set and operation are a group even when we don’t know what the elements in the set really are or what the binary operation is.

The next three exercises are very useful in helping determine whether or not a given Cayley table represents a group.

Exercise 15.2.17. Given h is an element of (G, \circ) .

1. Show that h is an identity element of G if and only if there exists a $g \in G$ such that $h \circ g = g$. (**Hint**)
2. Show that h is an identity element of G if and only if there exists a $g \in G$ such that $g \circ h = g$.

◇

In Exercise 15.2.17 we were careful to say *an* identity element. Could a group have multiple identity elements? Let’s settle the question once and for all:

Exercise 15.2.18. Use Exercise 15.2.17 to prove the following proposition:

Proposition 15.2.19. The identity element in a group G is unique; that is, there exists only one element $e \in G$ such that $eg = ge = g$ for all $g \in G$.

(*Hint*)

◇

Exercise 15.2.20. Show that if G is a group, then for every row of the Cayley table for G no two entries are the same. Show also that for every column of the Cayley table no two entries are the same. (*Hint*) ◇

Exercise 15.2.21. For each of the following multiplication tables defined on the set $G = \{a, b, c, d\}$ tell whether (G, \circ) represents a group, and if so, whether it is abelian. Support your answer in each case. Assume that the associative property holds in each case. *Note* the identity is not always the first element listed!

| | | | | | |
|-----|---------|-----|-----|-----|-----|
| (a) | \circ | a | b | c | d |
| a | a | b | c | d | d |
| b | b | a | d | c | c |
| c | c | d | a | b | a |
| d | d | a | b | c | b |

| | | | | | |
|-----|---------|-----|-----|-----|-----|
| (c) | \circ | a | b | c | d |
| a | d | c | b | a | d |
| b | c | d | a | b | c |
| c | b | c | d | a | d |
| d | a | b | c | d | a |

| | | | | | |
|-----|---------|-----|-----|-----|-----|
| (b) | \circ | a | b | c | d |
| a | b | a | d | c | d |
| b | a | b | c | d | a |
| c | d | c | b | a | b |
| d | c | d | a | b | c |

| | | | | | |
|-----|---------|-----|-----|-----|-----|
| (d) | \circ | a | b | c | d |
| a | b | c | d | a | d |
| b | c | d | a | b | c |
| c | d | a | b | c | d |
| d | a | b | c | d | a |

◇

Exercise 15.2.22. For each of the following multiplication tables, fill in the blanks to make a Cayley table for a group.

| | | | | | |
|-----|---------|-----|-----|-----|-----|
| (a) | \circ | a | b | c | d |
| a | a | b | c | - | - |
| b | - | a | - | - | - |
| c | c | - | a | - | - |
| d | d | - | - | - | - |

| | | | | | |
|-----|---------|-----|-----|-----|-----|
| (b) | \circ | a | b | c | d |
| a | c | - | - | - | - |
| b | - | b | c | d | - |
| c | - | - | - | - | - |
| d | - | - | - | - | - |

$$(c) \begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & d & - & - & - \\ b & - & d & - & - \\ c & - & - & d & - \\ d & - & - & - & d \end{array}$$

$$(d) \begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & b & - & d \\ b & - & a & - & - \\ c & c & - & - & - \\ d & d & - & - & - \end{array}$$

(There are two different ways to complete this one: find both)

◇

Exercise 15.2.23. * Show that it is *impossible* to complete the following Cayley tables to make a group.

$$(a) \begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & - & - & - & - \\ b & b & - & - & - \\ c & d & - & - & - \\ d & c & - & - & - \end{array}$$

$$(c) \begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & - & - & - \\ b & - & c & - & - \\ c & - & - & b & - \\ d & - & - & - & - \end{array}$$

$$(b) \begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & a & - & - & - \\ b & - & b & - & - \\ c & - & - & - & - \\ d & - & - & - & - \end{array}$$

$$(d) \begin{array}{c|cccc} \circ & a & b & c & d \\ \hline a & b & - & - & - \\ b & - & c & - & - \\ c & - & - & d & - \\ d & - & - & - & - \end{array}$$

◇

15.2.1 The group of units of \mathbb{Z}_n

Back in the Modular Arithmetic chapter, we used the addition table for \mathbb{Z}_8 to show that \mathbb{Z}_8 with modular addition was a group. We extended this and showed that \mathbb{Z}_n under modular addition is a group for any n . But we ran into problems with modular multiplication on \mathbb{Z}_8 , as we can see from the Cayley table (reproduced below),

From Table 15.1 we can see several problems. Notice that 0, 2, 4, 6 have no inverses. In fact, from Table 15.1 we see that only numbers that are relatively prime to 8 have inverses in \mathbb{Z}_8 . The same is true for any \mathbb{Z}_n . It follows that in order to get a group under modular multiplication using the

| \odot | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---------|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 2 | 0 | 2 | 4 | 6 | 0 | 2 | 4 | 6 |
| 3 | 0 | 3 | 6 | 1 | 4 | 7 | 2 | 5 |
| 4 | 0 | 4 | 0 | 4 | 0 | 4 | 0 | 4 |
| 5 | 0 | 5 | 2 | 7 | 4 | 1 | 6 | 3 |
| 6 | 0 | 6 | 4 | 2 | 0 | 6 | 4 | 2 |
| 7 | 0 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

Table 15.1: Cayley table for (\mathbb{Z}_8, \cdot)

elements of \mathbb{Z}_n , we'll have to kick out the non-relatively prime numbers in order to guarantee that every element has an inverse. For instance, Table 15.2 is the result when Table 15.1 is restricted to the rows and columns labeled (1, 3, 5, and 7).

| \odot | 1 | 3 | 5 | 7 |
|---------|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

Table 15.2: Multiplication table for $U(8)$

Exercise 15.2.24. Prove that the Cayley table in Table 15.2 represents a group. (Note that associativity holds because we already know that modular multiplication is associative.) \diamond

Exercise 15.2.25. Is the group in Table 15.2 abelian? Justify your answer. \diamond

For convenience, let's define some notation:

Definition 15.2.26. The set of nonzero numbers in \mathbb{Z}_n that are relatively prime to n is called the *set of units of \mathbb{Z}_n* , denoted by $U(n)$. \triangle

We have just seen that $U(8)$ is a group under modular multiplication. One might suspect that $U(n)$ is a group for any n . For starters, it is clear

that 1 serves as an identity element, because $1 \cdot k \equiv k \cdot 1 \equiv k \pmod{n}$ for any n . In fact, $U(n)$ is an abelian group, as you will show in the following exercises.

Exercise 15.2.27. In this exercise, we prove that $U(n)$ is a group under multiplication mod n for any n . We know that modular multiplication is associative, so it remains to show the closure and inverse properties.

- (a) Fill in the blanks to show that $U(n)$ is closed under modular multiplication:

Let k, m be arbitrary elements of $U(n)$. It follows that both k and $\underline{\langle 1 \rangle}$ are relatively prime to $\underline{\langle 2 \rangle}$. So neither k nor $\underline{\langle 3 \rangle}$ has any prime factors in common with $\underline{\langle 4 \rangle}$. It follows that the product $\underline{\langle 5 \rangle}$ also has no prime factors in common with $\underline{\langle 6 \rangle}$. Furthermore, the remainder of $\underline{\langle 7 \rangle}$ under division by $\underline{\langle 8 \rangle}$ also has no prime factors in common with $\underline{\langle 9 \rangle}$. Therefore the product of $\underline{\langle 10 \rangle}$ and $\underline{\langle 11 \rangle}$ under modular multiplication is also an element of $\underline{\langle 12 \rangle}$, so $\underline{\langle 13 \rangle}$ is closed under modular multiplication.

- (b) It remains to show that $U(n)$ is closed under inverse. Suppose that $m \in U(n)$ and x is the inverse of m . What modular equation must x satisfy? (**Hint**)
- (c) Show that the equation in x that you wrote in part (b) has a solution as long as m is relatively prime to n .

◇

Exercise 15.2.28. Show that $U(n)$ is abelian.

◇

Remark 15.2.29. Whenever we talk about the group $U(n)$, we always assume the operation is multiplication. Similarly, whenever we talk about \mathbb{Z}_n , we always assume the operation is addition. △

15.2.2 Groups of matrices

Matrices provide many examples of interesting groups.

Exercise 15.2.30. We use $\mathbb{M}_2(\mathbb{C})$ to denote the set of all 2×2 matrices with complex entries. That is

$$\mathbb{M}_2(\mathbb{C}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{C} \right\}$$

- (a) Show that $\mathbb{M}_2(\mathbb{C})$ a group under matrix addition. Is it abelian? If so, prove it; if not, find a counterexample.
- (b) What is the order of this group?
- (c) Is $\mathbb{M}_2(\mathbb{C})$ a group under matrix multiplication? Is it abelian? Justify your answers.

◇

Exercise 15.2.31. Let $\mathbb{M}_n(\mathbb{C})$ be the set of all $n \times n$ matrices with complex entries. Show that $\mathbb{M}_n(\mathbb{C})$ is a group under matrix addition. What is the order of this group? ◇

There are multiplicative groups of 2×2 matrices as well, but not all matrices can be included. To specify those which are included, we need the following definition

Definition 15.2.32. For the 2×2 matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, the quantity $ad - bc$ is called the *determinant* of A and is denoted by $\det(A)$. △

The following exercise is algebraically a little complicated, but turns out to be essential in order to prove properties of multiplicative groups of matrices.

Exercise 15.2.33. Using matrix multiplication and the definition of determinant, prove that if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$, then

$$\det(AB) = \det(A) \det(B)$$

. This is known as the *determinant product formula*. ◇

We're now ready to define a set of 2×2 matrices which is suitable to form a multiplicative group.

Definition 15.2.34. Let $GL_2(\mathbb{C})$ be the subset of $M_2(\mathbb{C})$ consisting of matrices A such that

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ and } \det(A) \neq 0$$

△

The proof that $GL_2(\mathbb{C})$ is a group is contained in the following exercise.

Exercise 15.2.35.

(a) Show that for any matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{C})$, the matrix

$$B = \frac{1}{\det(A)} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

satisfies

$$AB = BA = I.$$

- (b) Using Exercise 15.2.33, show that $GL_2(\mathbb{C})$ is closed under matrix multiplication.
- (c) Show that matrix multiplication in $GL_2(\mathbb{C})$ is associative.
- (d) Complete the proof that $GL_2(\mathbb{C})$ is a group under matrix multiplication.

$GL_2(\mathbb{C})$ is called the 2-dimensional **general linear group** over the complex numbers. ◇

Exercise 15.2.36. Prove or disprove: $GL_2(\mathbb{C})$ is abelian. ◇

It turns out that we can define a multiplicative group of $n \times n$ matrices for any positive integer n , in similar fashion as we defined $GL_2(\mathbb{C})$. Rather than using determinant, we present an alternative way of characterizing the $n \times n$ matrices that are suitable members of a multiplicative group.

Definition 15.2.37. An $n \times n$ matrix A is called **invertible** if there exists a $n \times n$ matrix B such that $AB = BA = I_n$, where I_n is the $n \times n$ identity matrix. △

It is fairly straightforward to prove the group properties under matrix multiplication for this limited set of matrices:

Exercise 15.2.38. Show that the set of $n \times n$ invertible matrices with complex entries form a group under matrix multiplication. You may assume that matrix multiplication is associative (this is proved in another chapter). \diamond

Definition 15.2.39. The set of $n \times n$ invertible matrices is called the n dimensional *general linear group*, and is denoted by $GL_n(\mathbb{C})$. \triangle

15.3 Basic properties of groups

Now that we have a general definition of groups, we can use this definition to prove properties that are true of *all* groups. We'll begin by proving some essential properties that we've shown for specific groups, but need to know in general:

Proposition 15.2.19 shows that group identities are unique – it turns out that inverses in a group are also unique:

Proposition 15.3.1. If g is any element in a group G , then the inverse of g is unique.

Exercise 15.3.2. Fill in the blanks to complete the following proof of Proposition 15.3.1.

- (a) By the definition of inverse, if g' is an inverse of an element g in a group G , then $g \cdot \underline{\langle 1 \rangle} = g' \cdot \underline{\langle 2 \rangle} = e$.
- (b) Similarly, if g'' is an inverse of g then $g \cdot \underline{\langle 3 \rangle} = \underline{\langle 4 \rangle} \cdot g = e$.
- (c) We may show that $g' = g''$ as follows:

$$\begin{aligned}
 g' &= g' \cdot \underline{\langle 5 \rangle} && \text{(definition of identity)} \\
 &= g' \cdot (\underline{\langle 6 \rangle} \cdot g'') && \text{(part b above, def. of inverse)} \\
 &= (g' \cdot g) \cdot \underline{\langle 7 \rangle} && \text{(associative property of group G)} \\
 &= \underline{\langle 8 \rangle} \cdot g' && \text{(part a above, def. of inverse)} \\
 &= g'' && \text{(def. of identity)}
 \end{aligned}$$

◇

Exercise 15.3.3.

- (a) Consider the group \mathbb{C}^* , and let $a = 5 + 3i \in \mathbb{C}^*$. What is a^{-1} ?
- (b) Consider the group defined by the set $S = \mathbb{R} \setminus \{-1\}$ and the binary operation $a * b = a + b + ab$. What is 5^{-1} ?
- (c) Consider the group defined by the set $G = \mathbb{R}^* \times \mathbb{Z}$ and the operation $(a, m) \circ (b, n) = (ab, m + n)$. What is $(3, 2)^{-1}$?
- (d) Consider the group $U(12)$. What is 5^{-1} ?
- (e) Consider the group $GL_2(\mathbb{R})$. What is $\begin{pmatrix} 4 & 3 \\ 3 & 2 \end{pmatrix}^{-1}$?

◇

An important property of inverses is:

Proposition 15.3.4. Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.

Remark 15.3.5. We've actually seen this property before, in the permutations chapter: recall that for two permutations σ and τ , we showed that $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$. △

PROOF. By the inverse property, $\exists a^{-1}, b^{-1} \in G$. By the closure property, $ab \in G$ and $b^{-1}a^{-1} \in G$. So we only need to verify that $b^{-1}a^{-1}$ satisfies the definition of inverse (from Proposition 15.3.1, we know the inverse is unique). First, we have:

$$\begin{aligned}
 (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} \text{ (associative property of group } G) \\
 &= aea^{-1} \text{ (def. of inverse)} \\
 &= aa^{-1} \text{ (def. of identity)} \\
 &= e. \text{ (def. of inverse)}
 \end{aligned}$$

The remainder of the proof is left as an exercise:

Exercise 15.3.6. Fill in the blanks to complete the proof of Proposition 15.3.4

$$\begin{aligned}
 (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b && (\text{-----}) \\
 &= b^{-1}eb && (\text{-----}) \\
 &= b^{-1}b && (\text{-----}) \\
 &= e. && (\text{-----})
 \end{aligned}$$

◇

□

By repeated application of Proposition 15.3.4, we may find the inverse of the product of multiple group elements, for example: $(abcd)^{-1} = d^{-1}c^{-1}b^{-1}a^{-1}$.

Proposition 15.3.4 shows that in general, when finding inverses of products it is necessary to take the products of inverses in reverse order. One might ask, Is it ever the case that it's not necessary to reverse the order? Glad you asked! We address this question in the following exercise:

Exercise 15.3.7. Given a group G and $a, b \in G$, prove that G is abelian if and only if $(ab)^{-1} = a^{-1}b^{-1}$ for all a, b in G . (*Hint*) ◇

Proposition 15.3.4 characterizes the inverse of a product: now we shall characterize the inverse of an inverse. From ordinary algebra we know that $-(-a) = a$ and $1/(1/a) = a$. This generalizes to arbitrary groups as follows:

Proposition 15.3.8. Let G be a group. For any $a \in G$, $(a^{-1})^{-1} = a$.

PROOF. If $a \in G$, then since G is a group, then $a^{-1} \in G$ exists. And again, since G is a group, there also exists $(a^{-1})^{-1} \in G$.

Now, by the definition of inverse, $a^{-1}(a^{-1})^{-1} = e$. Consequently, multiplying both sides of this equation by a , we have (the argument continues in the following exercise):

Exercise 15.3.9.

$$\begin{aligned}
 a(a^{-1}(a^{-1})^{-1}) &= ae && (\text{multiplication by } a) \\
 (aa^{-1})(a^{-1})^{-1} &= ae && (\text{-----}) \\
 e(a^{-1})^{-1} &= ae && (\text{-----}) \\
 (a^{-1})^{-1} &= a. && (\text{-----})
 \end{aligned}$$

◇

□

Exercise 15.3.10.

- (a) Suppose $a, b \in \mathbb{C}^*$, where $a = 4 + 3i$ and $b = 5 - 12i$. What is $(ab)^{-1}$? What is $(ba)^{-1}$?
- (b) Suppose $a, b \in G$, where G is the group defined by the set $S = \mathbb{R} \setminus \{-1\}$ and the binary operation $a * b = a + b + ab$. If $a = 10, b = 1$, what is $(a * b)^{-1}$? What is $(b * a)^{-1}$?
- (c) Suppose $\sigma, \tau \in S_6$, where $\sigma = (3456), \tau = (1625)$. What is $(\sigma\tau)^{-1}$? What is $(\tau\sigma)^{-1}$?
- (d) Consider the group $U(5)$. What is $(4 \odot 3)^{-1}$? What is $(3 \odot 4)^{-1}$?
- (e) Suppose $a, b \in GL_2(\mathbb{R})$, where

$$a = \begin{pmatrix} 6 & 7 \\ 2 & 3 \end{pmatrix} \text{ and } b = \begin{pmatrix} 5 & -2 \\ 2 & -1 \end{pmatrix}$$

What is $(ab)^{-1}$? What is $(ba)^{-1}$?

◇

In high school algebra we wrote equations like $6 + x = -\sqrt{2}$ or $5x = 6$, and we could always find a real number x that was a solution. Now we can see that this follows from the fact that \mathbb{R} is a group under addition and \mathbb{R}^* is a group under multiplication. Similarly, we have seen that equations like $ax = b \pmod{n}$ and $a + x = b \pmod{n}$ had solutions for $x \in U(n)$ and $x \in \mathbb{Z}_n$, respectively because $U(n)$ and \mathbb{Z}_n are groups under modular multiplication and modular addition, respectively.

Noticing a pattern here, the question then is this: does the equation $ax = b$ have a solution for any group G ? In other words, if a and b are two elements in a group G , does there exist an element $x \in G$ such that $ax = b$? If such an x does exist, is it unique? The following proposition answers both of these questions affirmatively.

Proposition 15.3.11. Let G be a group and a and b be any two elements in G . Then the equations $ax = b$ and $xa = b$ have unique solutions in G .

Note we need separate proofs to show that x exists and is unique for both $ax = b$ and $xa = b$, since we don't know whether the group is abelian. The proof for $ax = b$ is a fill-in-the-blank exercise, while the proof for $xa = b$ you'll do on your own:

Exercise 15.3.12.

- (a) Complete the proof that $ax = b$ has a unique solution by filling in the blanks:

Suppose that $ax = b$. First we must show that such an x exists. Since $a \in G$ and G is a group, it follows that a^{-1} exists. Multiplying both sides of $ax = b$ on the left by a^{-1} , we have

$$\begin{array}{ll} a^{-1}(ax) = a^{-1}b & \text{(left multiplication by } a^{-1}\text{)} \\ (a^{-1}a)x = a^{-1}b & \text{(-----)} \\ ex = a^{-1}b & \text{(-----)} \\ x = a^{-1}b. & \text{(-----)} \end{array}$$

We have thus shown that $ax = b$ implies $x = a^{-1}b$, so $ax = b$ can have at most one solution. We may also verify that $x = a^{-1}b$ is indeed a solution:

$$\begin{array}{ll} a(a^{-1}b) = (aa^{-1})b & \text{(-----)} \\ = eb & \text{(-----)} \\ = b. & \text{(-----)} \end{array}$$

This completes the proof that the solution both exists, and is unique.

- (b) Prove now the existence and uniqueness of the solution of $xa = b$ (similar to part (a)).

◇

The key method used in these proofs, the composition of both sides of the equation by a^{-1} , is something you've seen many times before. For instance in high school algebra, to solve the equation $5x = 6$ above, we teach our

kids to divide each side by 5. Remember that dividing by 5 is the same as multiplying by its reciprocal $1/5$. And $1/5$ is the multiplicative inverse of 5. So in fact we are composing (multiplying) each side of the equation by 5^{-1} in order to solve for x .

As in our example then, composing both sides of the equation by a^{-1} is not only useful for the proofs, but in actually solving for x . Therefore, no matter what crazy elements and strange binary operation make up our group, we can still solve for x using the same algebra we learned in high school. In other words, given a group G and $a, b \in G$, if $ax = b$, then $x = a^{-1}b$; if $xa = b$, then $x = ba^{-1}$; and so on. Use this methodology in the following exercises.

Exercise 15.3.13. Given $a, b \in \mathbb{C}^*$, where $a = 3 - 3i$ and $b = 2 + 12i$; solve for x in each of the following equations.

(a) $ax = b$ (b) $xa = b$ (c) $bx = a$ (d) $xb = a$.

◇

Exercise 15.3.14. Suppose G is the group defined by the set $S = \mathbb{R} \setminus \{-1\}$ and the binary operation $a * b = a + b + ab$. Solve for x in each of the following equations.

(a) $11 * x = -3$ (b) $x * 11 = -3$ (c) $-3 * x = 11$ (d) $x * (-3) = 11$.

◇

Exercise 15.3.15. Given $\rho, \mu \in S_8$, where $\rho = (532)(164)$ and $\mu = (18753)(26)$; solve for x in each of the following equations.

(a) $\rho x = \mu$ (b) $x\rho = \mu$ (c) $\mu x = \rho$ (d) $x\mu = \rho$.

◇

Exercise 15.3.16. Given the group $U(9)$, solve for x in each of the following equations.

(a) $5 \odot x = 8$ (b) $x \odot 5 = 8$ (c) $8 \odot x = 5$ (d) $x \odot 8 = 5$.

◇

Exercise 15.3.17. Given $A, B \in GL_2(\mathbb{R})$, where

$$A = \begin{pmatrix} 6 & 5 \\ 4 & 4 \end{pmatrix} \text{ and } B = \begin{pmatrix} -2 & -1 \\ 7 & 4 \end{pmatrix}$$

Solve for X in each of the following equations.

- (a) $AX = B$ (b) $XA = B$ (c) $BX = A$ (d) $XB = A$.

◇

Exercise 15.3.18.

- (a) Given a group G and $a, b \in G$, prove that if G is abelian, then any solution of $ax = b$ is also a solution of $xa = b$ (and vice versa).
 (b) Given a group G that is *not* abelian, show that it is always possible to find an equation of the form $ax = b$ which has a solution that is *not* a solution to $xa = b$.

◇

In our work so far, we've frequently used the *substitution property*. For instance if $x = y$, then we know also that $a \cdot x = a \cdot y$, regardless of the operation \cdot . But suppose I gave you the equation $a \cdot x = a \cdot y$. Is it necessarily true that $x = y$? If $a, x, y \in \mathbb{R}$ and the operation is multiplication, then it's true *as long as* $a \neq 0$. To show this, we may use the method we talked about in the previous proposition: multiply each side of the equation by a^{-1} (that is, divide by a), and the result is $x = y$. In basic algebra courses this property is often called the *law of cancellation*. Now this works for real numbers: but suppose a, x, y were elements of some other group. Would the law of cancellation still hold? In fact, using the method shown above, you can prove this property holds for any group G .

Proposition 15.3.19. If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

This proposition tells us that the *right and left cancellation laws* are true in groups. We leave the proof as an exercise.

Exercise 15.3.20.

- (a) To prove Proposition 15.3.19, we need to prove both that $ba = ca$ implies $b = c$, and that $ab = ac$ implies $b = c$. Why do these two statements require two different proofs?
- (b) Prove Proposition 15.3.19.

◇

We can use exponential notation for groups just as we do in ordinary algebra:

Definition 15.3.21. If G is a group and $g \in G$, then we define $g^0 = e$. For $n \in \mathbb{N}$, we define

$$g^n := \underbrace{g \cdot g \cdots g}_{n \text{ times}}$$

and

$$g^{-n} := (g^{-1})^n = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}.$$

△

Exercise 15.3.22. Using Definition 15.3.21, prove that

$$(g^n)^{-1} = g^{-n},$$

i.e. the inverse of g^n is equal to g^{-n} for any group element g and for any natural number n . ◇

Proposition 15.3.23. In a group, the usual laws of exponents hold; that is, for all $g, h \in G$,

1. $g^m g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$;
2. $(g^m)^n = g^{mn}$ for all $m, n \in \mathbb{Z}$;
3. $(gh)^n = (h^{-1}g^{-1})^{-n}$ for all $n \in \mathbb{Z}$. Furthermore, if G is abelian, then $(gh)^n = g^n h^n$.

PROOF. We will prove part (1), and you will do the rest. We can break part (1) into four cases: (a) $m, n \geq 0$; (b) $m, n < 0$; (c) $m \geq 0, n < 0$; (d) $m < 0, n \geq 0$.

Consider first case (a). Using Definition 15.3.21, we have

$$g^m g^n = \underbrace{g \cdot g \cdots g}_{m \text{ times}} \underbrace{g \cdot g \cdots g}_{n \text{ times}},$$

and

$$g^{m+n} = \underbrace{g \cdot g \cdots g}_{m+n \text{ times}}.$$

Since the right-hand sides of these expressions are equal, then so are the left-hand sides: so $g^m g^n = g^{m+n}$.

The proof of case (b) is exactly the same, except on the right-hand sides we should replace all g 's with g^{-1} and we should also replace ' m times', ' n times', and ' $m+n$ times' with ' $-m$ times', ' $-n$ times', and ' $-(m+n)$ times' respectively (recall that m and n are negative, so $-(m+n)$ is positive). These replacements gives us $g^m g^n = (g^{-1})^{-(m+n)}$, and according to Definition 15.3.21 we may rewrite this as $g^m g^n = g^{m+n}$. This completes the proof of case (b).

In case (c), we have

$$g^m g^n = \underbrace{g \cdot g \cdots g}_{m \text{ times}} \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-n \text{ times}}.$$

We now have two subcases to consider. First, if $m \geq -n$, then all of the g^{-1} factors cancel and we end up with

$$g^m g^n = \underbrace{g \cdot g \cdots g}_{m+n \text{ times}}.$$

Second, if $m < -n$, then all of the g factors are canceled and we end up with

$$g^m g^n = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{-(m+n) \text{ times}}.$$

In either of these subcases, the right-hand side agrees with the definition of g^{m+n} , so the equality is proved.

Case (d) is just like (c), except we exchange the signs on the g 's, m 's and n 's on the right-hand sides. This completes the proof of part (1).

Exercise 15.3.24. Prove parts (2) and (3) of Proposition 15.3.23. ◇

□

Notice that $(gh)^n \neq g^n h^n$ in general, since the group may not be abelian.

If the group is \mathbb{Z} or \mathbb{Z}_n , we write the group operation additively and the exponential operation multiplicatively; that is, we write ng instead of g^n . The laws of exponents now become

1. $mg + ng = (m + n)g$ for all $m, n \in \mathbb{Z}$;
2. $m(ng) = (mn)g$ for all $m, n \in \mathbb{Z}$;
3. $m(g + h) = mg + mh$ for all $m \in \mathbb{Z}$.

It is important to realize that the last statement can be made only because \mathbb{Z} and \mathbb{Z}_n are abelian groups.

Remark 15.3.25. (*historical background*) Although the first clear axiomatic definition of a group was not given until the late 1800s, group-theoretic methods had been employed before this time in the development of many areas of mathematics, including geometry and the theory of algebraic equations.

Joseph-Louis Lagrange used group-theoretic methods in a 1770–1771 memoir to study methods of solving polynomial equations. Later, Évariste Galois (1811–1832) succeeded in developing the mathematics necessary to determine exactly which polynomial equations could be solved in terms of the polynomials' coefficients. Galois' primary tool was group theory.

The study of geometry was revolutionized in 1872 when Felix Klein proposed that geometric spaces should be studied by examining those properties that are invariant under a transformation of the space. Sophus Lie, a contemporary of Klein, used group theory to study solutions of partial differential equations. One of the first modern treatments of group theory appeared in William Burnside's *The Theory of Groups of Finite Order* [1], first published in 1897. △

15.4 Subgroups

We first came across subgroups in the Permutations chapter. We saw that S_n , the set of permutations on a set of n elements, is a group under function

composition. Yet we also saw that the set of symmetries of an n -sided figure, which is a subset of S_n , is itself a group under function composition. So a subgroup is a subset of a larger group that is itself a group under the same operation as the larger group. Formally then:

Definition 15.4.1. A *subgroup* H of a group (G, \circ) is a subset H of G such that when the group operation of G is restricted to H , H is a group in its own right. \triangle

By definition, all subgroups are subsets: but is the reverse true? If not, what makes a *subset* a *subgroup*? What special properties must subsets possess in order to qualify as subgroups?

The key to answering this question is the observation that any subset $H \subset G$ that is a subgroup of G must also be a group in its own right: and we're already experts at deciding whether a set with a binary operation is a group:

Example 15.4.2. Consider the set of even integers $2\mathbb{Z} = \{\dots, -2, 0, 2, 4, \dots\}$. A more mathematically concise definition is:

$$2\mathbb{Z} = \{x \in \mathbb{Z} \mid x = 2n \text{ for some } n \in \mathbb{Z}\}$$

$2\mathbb{Z}$ is actually a subgroup of \mathbb{Z} , under the operation of addition. To show this, according to the definition of subgroup we need to show:

- (a) $(\mathbb{Z}, +)$ is a group;
- (b) $2\mathbb{Z} \subset \mathbb{Z}$;
- (c) $(2\mathbb{Z}, +)$ is a group.

Items (a) and (b) can be dispatched in short order. From our work in Chapters 1 and 2, we know \mathbb{Z} is a group under addition: this takes care of (a). For item (b), we have that any element $m \in 2\mathbb{Z}$ can be written as $m = 2n$, where $n \in \mathbb{Z}$: hence $m \in \mathbb{Z}$ also.

To show (c), we must verify all the group properties for $2\mathbb{Z}$ under the operation $+$:

- (*Closure*): Given $x, y \in 2\mathbb{Z}$, it follows $x = 2n$ and $y = 2m$ for some $n, m \in \mathbb{Z}$. Therefore

$$x + y = 2n + 2m = 2(n + m)$$

Since \mathbb{Z} is closed under $+$, it follows $(n + m) \in \mathbb{Z}$, so $2(n + m) \in 2\mathbb{Z}$. Since x and y were arbitrary, it follows that $2\mathbb{Z}$ is closed under addition.

- (*Associative*): Suppose $w, x, y \in 2\mathbb{Z}$. Then w, x, y are integers, and $w + (x + y) = (w + x) + y$ by the associativity of $(\mathbb{Z}, +)$. Hence $2\mathbb{Z}$ is associative under addition.

- (*Identity*): $0 \in 2\mathbb{Z}$, since $2 \cdot 0 = 0$: and for any $x \in 2\mathbb{Z}$,

$$0 + x = x + 0 = x.$$

Hence $2\mathbb{Z}$ has an identity under addition, namely 0.

- (*Inverse*): Given $x \in 2\mathbb{Z}$, where $x = 2n$,

$-x = -(2n) = 2(-n)$, [associative and commutative properties of \mathbb{Z} under multiplication]

and since $-n \in \mathbb{Z}$ (closure of \mathbb{Z} under multiplication) it follows that $-x \in 2\mathbb{Z}$. Now since

$$-x + x = x + (-x) = 0,$$

it follows $\forall x \in 2\mathbb{Z}, \exists x^{-1} \in 2\mathbb{Z}$, namely $x^{-1} = -x$.

This completes the proof that $2\mathbb{Z}$ is a subgroup of \mathbb{Z} under addition. \blacklozenge

Exercise 15.4.3. Given any fixed integer m , prove that

$$m\mathbb{Z} = \{\dots, -2m, -m, 0, m, 2m, \dots\}$$

is a subgroup of \mathbb{Z} under the operation of addition. \diamond

Notice that by definition, the operation used in the subgroup must be the *same* operation that's used in the group it's contained in. For example, \mathbb{R}^* is not a subgroup of \mathbb{R} , because $(\mathbb{R}^*, +)$ is not a group.

Exercise 15.4.4. Prove or disprove:

- (a) $GL_2(\mathbb{R})$ is a subgroup of $M_2(\mathbb{R})$.
- (b) $U(n)$ is a subgroup of \mathbb{Z}_n .

◇

We can make the task of proving subgroups a bit easier. First notice that in Example 15.4.2, $2\mathbb{Z}$ was associative simply by virtue of the fact that it's contained in the group \mathbb{Z} and has the same operation. This will be true in general: the associate property will always hold for any subset of a group G under that group's operation. We may also make the following observation about identity elements:

Exercise 15.4.5. Prove the following: Suppose G is a group with identity element e , and let H be a subgroup of G with identity element f . Then $e = f$. ◇

Exercise 15.4.5 and our observation about associativity lead to the following simplified subgroup criteria (which we state as a proposition):

Proposition 15.4.6. A subset H of a group G is a subgroup if and only if:

- (a) The identity e of G is in H .
- (b) If $h_1, h_2 \in H$, then $h_1 h_2 \in H$ (that is, H is closed under the group operation),
- (c) If $h \in H$, then $h^{-1} \in H$.

Exercise 15.4.7. The set \mathbb{T} is defined as the subset of \mathbb{C} whose elements all have a modulus of 1; that is

$$\mathbb{T} = \{c \in \mathbb{C} : |c| = 1\}$$

- (a) Using Proposition 15.4.6 above, prove that \mathbb{T} is a subgroup of \mathbb{C}^* .
- (b) What is $|\mathbb{T}|$?
- (c) Prove or disprove that \mathbb{T} is abelian.

◇

Exercise 15.4.8. Let $H_4 = \{1, -1, i, -i\}$, (these are the fourth roots of unity, which we studied in Section 4.4.1).

- (a) Using Proposition 15.4.6, prove that H_4 is a subgroup of \mathbb{T} . (Note you should first verify that H_4 is a subset of \mathbb{T} .)
- (b) What is $|H_4|$?
- (c) Prove or disprove that H_4 is abelian.

◇

Exercise 15.4.9. Let's generalize the last exercise. Suppose now that H_n is the set of n^{th} roots of unity. That is

$$H_n = \{z \in \mathbb{C} : z^n = 1\}$$

- (a) Prove that H_n is a subset of \mathbb{T} .
- (b) Using Proposition 15.4.6, prove that H is a subgroup of \mathbb{T} .
- (c) What is $|H_n|$?
- (d) Prove or disprove that H_n is abelian.

◇

Exercise 15.4.10. Let \mathbb{Q}^* be defined in the following way:

$$\mathbb{Q}^* = \{p/q : p, q \text{ are nonzero integers}\}$$

In other words \mathbb{Q}^* is the set of non-zero rational numbers ($\mathbb{Q}^* = \mathbb{Q} \setminus 0$).

- (a) Using Proposition 15.4.6, prove that \mathbb{Q}^* is a subgroup of \mathbb{R}^* .
- (b) Prove or disprove that \mathbb{Q}^* is abelian.

◇

Exercise 15.4.11. Prove that

$$G = \{a + b\sqrt{2} : a, b \in \mathbb{Q} \text{ and } a \text{ and } b \text{ are not both zero}\}$$

is a subgroup of \mathbb{R}^* under the group operation of multiplication. ◇

Exercise 15.4.12. Let G be the group of 2×2 matrices under addition and

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + d = 0 \right\}.$$

- (a) Prove that H is a subgroup of G .
- (b) Prove or disprove that H is abelian

◇

Exercise 15.4.13. We define $SL_2(\mathbb{R})$ to be the set of 2×2 matrices of determinant one; that is, a matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $SL_2(\mathbb{R})$ exactly when $ad - bc = 1$. We call this the **Special Linear Group**.

- (a) Using Proposition 15.4.6, prove that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.
- (b) Prove or disprove that $SL_2(\mathbb{R})$ is abelian.

◇

Exercise 15.4.14. Let G consist of the 2×2 matrices of the form

$$\begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$$

where $\theta \in \mathbb{R}$.

- (a) Prove that G is a subgroup of $SL_2(\mathbb{R})$. (Recall your angle addition formulas from trigonometry!)
- (b) Prove or disprove that G is abelian.

(G is called the set of 2×2 *rotation matrices*.) ◇

There is an alternative way to prove a subset H of G is a subgroup of G that can save some time. It turns out that the three conditions in Proposition 15.4.6 can be combined into a single statement:

Proposition 15.4.15. Let H be a subset of a group G . Then H is a subgroup of G if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then gh^{-1} is in H .

PROOF. We first prove the “if” direction, so we assume H be a nonempty subset of G and whenever $g, h \in H$ then gh^{-1} is in H . Proposition 15.4.6 says that if H contains the identity and is closed under inverse and the group operation, then H is a subgroup. Let’s prove these one by one. First, since H is nonempty, it contains some element g : and letting $h = g$ we obtain $gg^{-1} = e$ is in H . Second, since $e \in H$ and $g \in H$, then $eg^{-1} = g^{-1}$ is also in H : so H is closed under inverse. Finally, let $g, h \in H$. We must show that their product is also in H . But we have already shown that $h \in H$ implies that $h^{-1} \in H$, so that, $g(h^{-1})^{-1} = gh \in H$. We have established the three required conditions, so we may conclude that H is a subgroup of G .

To prove the “only if” direction, we may assume that H is a subgroup of G . Given any elements $g, h \in H$, we need to show that $gh^{-1} \in H$. Since h is in H , its inverse h^{-1} must also be in H . Because of the closure of the group operation, $gh^{-1} \in H$. This completes the proof. □

Example 15.4.16. Using the proposition above, let’s re-prove that \mathbb{T} is a subgroup of \mathbb{C}^* .

PROOF. Based on the proposition, there are four things we need to show:

- (a) \mathbb{C}^* is a group;
- (b) $\mathbb{T} \neq \emptyset$;
- (c) $\mathbb{T} \subset \mathbb{C}^*$;
- (d) Given $x, y \in \mathbb{T}$, $xy^{-1} \in \mathbb{T}$.

Items (a), (b), and (c) we have shown before. As to item (d),

$$\begin{aligned} x, y &\in \mathbb{T} \\ \Rightarrow |x| = 1 \text{ and } |y| = 1 \\ \Rightarrow |xy^{-1}| &= |x| \cdot |y^{-1}| = |x|/|y| = 1/1 = 1 \\ \Rightarrow |xy^{-1}| &\in \mathbb{T} \end{aligned}$$

□

◆

Exercise 15.4.17. Use Proposition 15.4.15 to re-prove the following:

- (a) \mathbb{Q}^* is a subgroup of \mathbb{R}^* .
- (b) $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

◇

15.5 Cyclic groups

In this section we will explore an important property of some groups and subgroups.

15.5.1 Definitions

Example 15.5.1. Consider the group \mathbb{Z} . Let us try to find the smallest subgroup of \mathbb{Z} that contains the number 1.

- (1) We start with the smallest subset possible, $P = \{1\}$.
- (2) The subset has to be a group under addition. But so far P does not contain an additive identity. So we need to add 0 to the set, giving us $P = \{0, 1\}$.
- (3) Zero is its own inverse under addition, but notice that our set does not include an inverse for 1. So we add -1 to P , giving us $P = \{-1, 0, 1\}$.
- (4) Is P closed under addition? Certainly when we add 0 to 1 and -1 , we get 1 and -1 , respectively. And $-1 + 1 = 0$. But what about when we add 1 and 1, or -1 and -1 ? So we need to add 2 and -2 to the set, giving us $P = \{-2, -1, 0, 1, 2\}$.

- (5) Now, what about $1 + 2$, or $(-1) + (-2)$? So we need 3 and -3 , giving us $P = \{-3, -2, -1, 0, 1, 2, 3\}$.
- (6) And we can see that this process would keep going until we get all the integers. In other words,
- $$P = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \mathbb{Z}.$$

Therefore the smallest subgroup of \mathbb{Z} that contains 1 is \mathbb{Z} itself. ♦

From the last example, we saw that P was generated through repeated additions of 1 and repeated additions of -1 (with 0 thrown in for good measure). Zero in fact can be calculated by adding 1 and -1 , and can be thought of as a zero multiple of 1. In addition, the repeated additions of 1 and -1 can be thought of as positive and negative multiples of 1. Therefore we can think of all the elements of P as integer multiples of 1. We denote the set of all integer multiples of 1 as $\langle 1 \rangle$; therefore,

$$\langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}\} = P.$$

In Example 15.5.1 we also saw that P was in fact \mathbb{Z} ; therefore $\mathbb{Z} = \langle 1 \rangle$. We say that \mathbb{Z} is *generated by* 1, as per the following definition:

Let us extend this concept to groups in general:

Definition 15.5.2. Given a group G and an element $a \in G$, then *the set generated by the element a* is denoted by $\langle a \rangle$, and is defined as the set obtained by repeated multiplication of the identity e by the group elements a and a^{-1} . Using the notation we introduced right before Proposition 15.3.23, we can write this as

$$\langle a \rangle = \{\dots, a^{-3}, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}$$

or

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

$\langle a \rangle$ is sometimes called the *orbit* of a . △

Remark 15.5.3. If we are using the “+” operation, as in the case of the integers above, we write $\langle a \rangle = \{na : n \in \mathbb{Z}\}$. △

Exercise 15.5.4. List the set $\langle 3 \rangle$ for $3 \in \mathbb{R}^*$. ◇

We have special terminology for the case where all the elements of a group are generated by a single element:

Definition 15.5.5. If a group G contains some element a such that $G = \langle a \rangle$, then G is a *cyclic group*. In this case a is a *generator* of G . \triangle

We have seen above that 1 is a generator of \mathbb{Z} , and thus \mathbb{Z} is a cyclic group. A cyclic group may have more than one generator:

Exercise 15.5.6. Show that -1 is a generator of \mathbb{Z} ; that is that $\mathbb{Z} = \langle -1 \rangle$. \diamond

Example 15.5.7. Consider the group \mathbb{Z}_6 . $\langle 1 \rangle$ is computed as follows:

- $1 \equiv 1$
- $1 + 1 \equiv 2$
- $1 + 1 + 1 \equiv 3$
- $1 + 1 + 1 + 1 \equiv 4$
- $1 + 1 + 1 + 1 + 1 \equiv 5$
- $1 + 1 + 1 + 1 + 1 + 1 \equiv 0$
- Notice that we've already generated all the elements in \mathbb{Z}_6 . So we don't have to worry about finding the additive integer multiples of 1^{-1} (Note that $(1^{-1} = 5)$), because these calculations can't produce any new elements.
- So $\langle 1 \rangle = \{1, 2, 3, 4, 5, 0\} = \mathbb{Z}_6$.

Therefore \mathbb{Z}_6 is a cyclic group generated by 1. \blacklozenge

We've just seen that 1 is a generator of \mathbb{Z}_6 , but that doesn't mean it's the *only* generator. A cyclic group can have more than one generator:

Exercise 15.5.8.

(a) In the group \mathbb{Z}_6 , show that $\langle 5 \rangle = \mathbb{Z}_6$.

- (b) Find all generators of \mathbb{Z}_6 : that is, find all numbers $a \in \mathbb{Z}_6$ such that $\langle a \rangle = \mathbb{Z}_6$.

◇

Exercise 15.5.9. Given a group G , suppose that $G = \langle a \rangle$. Prove that $G = \langle a^{-1} \rangle$. ◇

Exercise 15.5.10.

- (a) Show that \mathbb{Z}_n is cyclic for any integer $n > 1$ by identifying a number a such that $\langle a \rangle = \mathbb{Z}_n$.
- (b) For $n > 2$, show that \mathbb{Z}_n has at least 2 generators by finding a number b_n such that $\langle b_n \rangle = \mathbb{Z}_n$.

◇

Example 15.5.11. The group of units, $U(9)$ is a cyclic group. As a set, $U(9)$ is $\{1, 2, 4, 5, 7, 8\}$. Computing $\langle 2 \rangle$, we get

$$\begin{aligned} \langle 2 \rangle &= \{2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1\} \\ &= \{2, 4, 8, 7, 5, 1\} \\ &= U(9) \end{aligned}$$

So $\langle 2 \rangle = \{2^n \pmod{9} : n \in \mathbb{Z}\} = U(9)$ ◆

Exercise 15.5.12. Find any other generators of $U(9)$ if they exist (say so if no others exist). ◇

15.5.2 Orbits (cyclic subgroups)

In this section we further explore properties of the set $\langle a \rangle$ for arbitrary group elements $a \in G$. We have seen that in some cases, $\langle a \rangle$ is actually a group. We'll see in a minute that in fact $\langle a \rangle$ is *always* a group. Let's look at some examples first.

Example 15.5.13. Suppose that we consider $4 \in \mathbb{Z}$.

$$\langle 4 \rangle = \{\dots, -8, -4, 0, 4, 8, \dots\}.$$

which happens to be the set $4\mathbb{Z}$.

Exercise 15.5.14. Prove that $4\mathbb{Z}$ is a subgroup of \mathbb{Z} . ◇

It follows from this exercise that $4\mathbb{Z}$ is the *cyclic subgroup* of \mathbb{Z} generated by 4. ◆

Exercise 15.5.15. Let $H = \{2^n : n \in \mathbb{Z}\} = \langle 2 \rangle$ under multiplication.

- (a) List the elements in H
- (b) Show that $H \subset \mathbb{Q}^*$.
- (c) Show that H is closed under multiplication.
- (d) Show that H is closed under inverse.
- (e) Is H a subgroup of \mathbb{Q}^* ? *Explain* your answer.

◇

It follows from this exercise that H is the *cyclic subgroup* of \mathbb{Q}^* generated by 2.

By now we've seen enough examples so that we're ready to prove the general result.

Proposition 15.5.16. Let G be a group and a be any element in G . Then the set

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

is a subgroup of G .

PROOF. The identity is in $\langle a \rangle$ since $a^0 = e$. If g and h are any two elements in $\langle a \rangle$, then by the definition of $\langle a \rangle$ we can write $g = a^m$ and $h = a^n$ for some integers m and n . So $gh = a^m a^n = a^{m+n}$ is again in $\langle a \rangle$. Finally, if $g = a^n$ in $\langle a \rangle$, then the inverse $g^{-1} = a^{-n}$ is also in $\langle a \rangle$. \square

Definition 15.5.17. Given a group G , for each $a \in G$, we call $\langle a \rangle$ the *cyclic subgroup* generated by a . \triangle

Let us now consider in particular the case of finite groups. Let G be a finite group, and let a be an element of G . Consider the set $A := \{a, a^2, a^3, \dots\}$. Since $A \subset G$ and G is finite, the set A must also be finite. In particular, the list $\{a, a^2, a^3, \dots\}$ must contain duplicate elements, since otherwise A would be infinite. We must therefore have $a^k = a^l$ for two different natural numbers k, l . This is the key fact in proving the following exercise:

Exercise 15.5.18. Let G be a finite group, and let $a \in G$ where $a \neq e$. Show there exists a natural number $m > 0$ such that $a^m = e$. (*Hint*) \diamond

In view of the preceding exercise, we may make the following definition:

Definition 15.5.19. If a is an element of a group G , we define the *order* of a to be the smallest positive integer n such that $a^n = e$, and we write $|a| = n$. If there is no such integer n , we say that the order of a is infinite and write $|a| = \infty$ to denote the order of a .³ \triangle

Example 15.5.20. Let us consider the orders of different elements in the infinite group \mathbb{Z} .

- First, what is $|0|$? According to Definition 15.5.19, we need to find the smallest positive integer such that $n \cdot 0 = 0$ (remember, \mathbb{Z} is an *additive* group. We get $n = 1$, so $|0| = 1$, and the cyclic subgroup generated by 0 is $\langle 0 \rangle = \{0\}$

³Yet another use of the term “order” and the absolute value sign. But you should be used to it by now.

- What is $|1|$? $1 + 1 = 2$; $1 + 1 + 1 = 3$; ... In fact you'll never get to 0 adding a positive number of ones. So $|1| = \infty$, and as we've seen, $\langle 1 \rangle = \mathbb{Z}$.
- Similarly, $|-1| = \infty$.

**Exercise 15.5.21.**

- (a) In the group \mathbb{Z}_6 , What is $|1|$? What is $|5|$?
- (b) Given any group G , If e is the identity element of G then what is $|e|$?



Example 15.5.22. The order of $2 \in \mathbb{Z}_6$ is 3, because under repeated modular addition we have

$$2 \oplus 2 = 4; \quad 2 \oplus 2 \oplus 2 = 0.$$

Therefore the cyclic subgroup generated by 2 is $\langle 2 \rangle = \{0, 2, 4\}$.



Exercise 15.5.23. Find the order of each element of $U(9)$. Find also the cyclic subgroup generated by each element.

**Exercise 15.5.24.**

- (a) Find the order of each element of \mathbb{Z}_{12} . Find also the cyclic subgroup generated by each element.
- (b) Based on your experience with this problem, would you say there is any relationship between the order of a group element (denoted by $|a|$) and the order of the cyclic subgroup generated by the element (denoted by $|\langle a \rangle|$)? If so, what would you say the relationship is?

◇

Let us now consider specifically the cyclic subgroups of finite groups. In the following exercises, you may wish to make use of the laws of exponents listed in Proposition 15.3.23.

Exercise 15.5.25. Let G be a finite group, and let $a \in G$ where $|a| = n$. Show that $(a^{-1})^n = e$. ◇

Exercise 15.5.26. In the following exercises, G is a finite group, and $a \in G$ where $|a| = n$.

- (a) Show that for any integer $m \in \mathbb{Z}$, $a^m = a^{\text{mod}(m,n)}$. (*Hint*)
- (b) Let $A = \{e, a, a^2, \dots, a^{n-1}\}$. Show that $\langle a \rangle \subset A$ and $A \subset \langle a \rangle$.
- (c) Prove that $|\langle a \rangle| = |A|$. (Note that $|A|$ is the number of elements in A .)
- (d) If $m, k \in \mathbb{Z}_n$ and $m \neq k$, show that $a^m \neq a^k$.
- (e) Prove that $|a| = |A|$. (This together with part (c) implies that $|a| = |\langle a \rangle|$.)

◇

Due to its importance, we will state the final result of the preceding exercise as a proposition.

Proposition 15.5.27. Let G be a finite group, and let $a \in G$. Then $|a| = |\langle a \rangle|$.

Exercise 15.5.28. Let G be a finite group, and let $a \in G$ such that $|a| = n$ for $n > 0$. Show that there exists a natural number m such that $a^{-1} = a^m$, and express m in terms of n . ◇

Example 15.5.29. Not every group is a cyclic group. Consider the symmetry group of an equilateral triangle D_3 (which is the same as S_3). D_3 has 6 elements: we saw the Cayley table for D_3 in Chapter 13 (see Table 13.1.

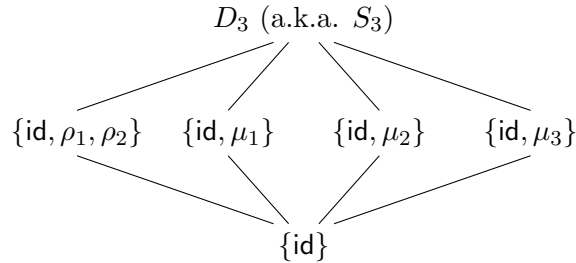


Figure 15.5.1. Subgroups of D_3 (a.k.a. S_3)

You may verify by using the table that no single element generates the entire group, so D_3 is not cyclic. The cyclic subgroups of S_3 are shown in Figure 15.5.1. \blacklozenge

Although not every group (and not every subgroup) is cyclic, we may use cyclic subgroups to help us enumerate all possible subgroups of a given group, with the benefit of the following result:

Proposition 15.5.30. Given a group G and a subgroup $H \subset G$, and suppose that $a \in H$. Then $\langle a \rangle \subset H$.

Exercise 15.5.31. Prove Proposition 15.5.30 \blacklozenge

Proposition 15.5.30 makes it much easier to find subgroups of a given group, because it greatly cuts down on the possibilities.

Example 15.5.32. We showed in Example 15.5.29 that D_3 has 4 cyclic subgroups, and that every element of D_3 is in at least one of these subgroups. Proposition 15.5.30 shows that, for example, any subgroup containing ρ_1 must also contain id and ρ_2 , since $\langle \rho_1 \rangle = \{id, \rho_1, \rho_2\}$. Let's try to find a larger subgroup $H \subset D_3$ that contains ρ_1 . If we add any other element (which must be μ_k for some $k = 1, 2$ or 3), then we must also add $\rho_1\mu_k$ and $\rho_2\mu_k$, which means that H contains all 6 elements of D_3 . It follows that $H = D_3$. Similarly, if we try to find a subgroup K that contains μ_k by adding another reflection μ_j ($j \neq k$), we find that $\mu_j\mu_k$ and $\mu_k\mu_j$ must also be in K , which means that ρ_1 must also be in K . But we've just finished shown that if $\rho_1 \in K$ and $\mu_k \in K$, then $K = G$. It follows that the only

proper nontrivial subgroups of D_3 are the four cyclic subgroups shown in Figure 15.5.1. \blacklozenge

Exercise 15.5.33.

- (a) Find all cyclic subgroups of the symmetry group of the square (i.e. D_4) by finding $\langle a \rangle$ for every element $a \in D_4$.
- (b) Find all nontrivial proper subgroups of D_4 (You may follow the procedure used in Example 15.5.32 if you wish.)
- (c) Show that at least one of the subgroups in (b) is abelian and not cyclic.

\blacklozenge

It is not true that every abelian group is cyclic (see Exercise 15.5.33). However, we can prove the converse, namely:

Proposition 15.5.34. Every cyclic group is abelian.

PROOF. Let G be a cyclic group and $a \in G$ be a generator for G . If g and h are in G , then they can be written as powers of a , say $g = a^r$ and $h = a^s$. It follows that

$$gh = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = hg.$$

Since g and h were arbitrary elements of G , it follows that G is abelian. \square

How about the converse of Proposition 15.5.34? Is it true that every abelian group is cyclic? As it turns out, No. The following proposition gives an example:

Proposition 15.5.35. The group $(\mathbb{R}, +)$ is not cyclic.

PROOF. We'll use our old workhorse, proof by contradiction. Suppose that a is a generator of \mathbb{R} , i.e. $\langle a \rangle = \mathbb{R}$. Then since $a/2 \in \mathbb{R}$, it follows that $a/2 \in \langle a \rangle$. This means $a/2 = ka$ for some integer k . Rearranging this equation, we find that $a(1/2 - k) = 0$. By the zero-divisor property of real numbers, this implies that either $a = 0$ or $1/2 - k = 0$ (or both). But a cannot be 0, because $\langle 0 \rangle = 0$. Also, $1/2 - k \neq 0$, since k is an integer. This contradiction shows that our assumption that $\mathbb{R} = \langle a \rangle$ is false. Therefore $\mathbb{R} \neq \langle a \rangle$ for any real number a , and \mathbb{R} is not cyclic. \square

Exercise 15.5.36.

- (a) Show that \mathbb{Q} is not cyclic.
(b) Show that \mathbb{C} is not cyclic.

◇

15.5.3 Subgroups of cyclic groups

We can ask some interesting questions about cyclic subgroups of a group and subgroups of a cyclic group. If G is a group, which subgroups of G are cyclic? If G is a cyclic group, what type of subgroups does G possess?

Proposition 15.5.37. Every subgroup of a cyclic group is cyclic.

PROOF. The main tools used in this proof are the division algorithm, which we mentioned in Proposition 5.2.3, and the Principle of Well-Ordering, which we mentioned in Section 3.2.2.

Let G be a cyclic group generated by a and suppose that H is a subgroup of G . If $H = \{e\}$, then trivially H is cyclic. Suppose that H contains some other element g distinct from the identity. Then g can be written as a^n for some integer n . We can assume that $n > 0$. Define the set S by: $S = \{j \in \mathbb{N} \text{ such that } a^j = g\}$. We have just shown that S is nonempty. The Principle of Well-Ordering tells us that any nonempty subset of the natural numbers has a smallest element. Let m be the smallest element of S .

We claim that $h = a^m$ is a generator for H . We must show that every $h' \in H$ can be written as a power of h . Since $h' \in H$ and H is a subgroup of G , $h' = a^k$ for some positive integer k . Using the division algorithm, we can find numbers q and r such that $k = mq + r$ where $0 \leq r < m$; hence,

$$a^k = a^{mq+r} = (a^m)^q a^r = h^q a^r.$$

So we can solve for a^r : $a^r = h^{-q} a^k$. Since a^k and h^{-q} are in H , a^r must also be in H . However, m was the smallest positive number such that a^m was in H ; consequently, $r = 0$ and so $k = mq$. Therefore,

$$h' = a^k = a^{mq} = h^q$$

and H is generated by h . □

Proposition 15.5.38. The subgroups of \mathbb{Z} are exactly $n\mathbb{Z}$ for $n = 0, 1, 2, \dots$

Exercise 15.5.39. Prove Proposition 15.5.38 ◇

Exercise 15.5.40. Let $H = \{2^k : k \in \mathbb{Z}\}$. We know that H is a subgroup of \mathbb{Q} . Find all subgroups of H . ◇

Proposition 15.5.41. Let G be a cyclic group of order n and suppose that a is a generator for G . Then $a^k = e$ if and only if n divides k .

PROOF. Since $G = \langle a \rangle$ it follows from Proposition 15.5.27 that $|a| = n$. In Exercise 15.5.26 (a) we proved that $a^k = a^{\text{mod}(k,n)}$. Let $r = \text{mod}(k,n)$. If $r = 0$ (which is the same thing as saying that n divides k) this implies $a^k = a^0 = e$. Otherwise, if it must be the case that $0 < r < n = |a|$, and by the definition of $|a|$ it follows that $a^r \neq e$. This concludes the proof. □

Proposition 15.5.42. Let G be a cyclic group of order n and suppose that $a \in G$ is a generator of the group. If $b = a^k$, then the order of b is n/d , where $d = \text{gcd}(k, n)$.

PROOF. We wish to find the smallest integer m such that $e = b^m = a^{km}$. By Proposition 15.5.41, this is the smallest integer m such that n divides km or, equivalently, n/d divides $m(k/d)$. (Note that n/d and k/d are both integers, since d divides both n and k .) Since d is the greatest common divisor of n and k , n/d and k/d are relatively prime. Hence, for n/d to divide $m(k/d)$ it must divide m . The smallest such m is n/d . □

Corollary 15.5.43. The generators of \mathbb{Z}_n are the integers r such that $1 \leq r < n$ and $\text{gcd}(r, n) = 1$.

Example 15.5.44. Let us examine the group \mathbb{Z}_{16} . The numbers 1, 3, 5, 7, 9, 11, 13, and 15 are the elements of \mathbb{Z}_{16} that are relatively prime to 16. Each of these elements generates \mathbb{Z}_{16} . For example, 9 is a generator because:

$$\begin{array}{lll}
 1 \cdot 9 = 9 & 2 \cdot 9 = 2 & 3 \cdot 9 = 11 \\
 4 \cdot 9 = 4 & 5 \cdot 9 = 13 & 6 \cdot 9 = 6 \\
 7 \cdot 9 = 15 & 8 \cdot 9 = 8 & 9 \cdot 9 = 1 \\
 10 \cdot 9 = 10 & 11 \cdot 9 = 3 & 12 \cdot 9 = 12 \\
 13 \cdot 9 = 5 & 14 \cdot 9 = 14 & 15 \cdot 9 = 7.
 \end{array}$$



15.6 Additional group and subgroup exercises

Exercise 15.6.1. Write out Cayley tables for groups formed by the symmetries of a rectangle and for $(\mathbb{Z}_4, +)$. How many elements are in each group? Are the groups the same? Why or why not? \diamond

Exercise 15.6.2. Describe the symmetries of a rhombus and prove that the set of symmetries forms a group. Give Cayley tables for both the symmetries of a rectangle and the symmetries of a rhombus. Are the symmetries of a rectangle and those of a rhombus the same? \diamond

Exercise 15.6.3. Give a multiplication table for the group $U(12)$. \diamond

Exercise 15.6.4. Prove that the set of matrices of the form

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix}$$

where $x, y, z \in \mathbb{C}$ is a group under matrix multiplication. This group, known as the **Heisenberg group**, is important in quantum physics. \diamond

Exercise 15.6.5. List all subgroups of the quaternion group Q_8 . (*Hint*) \diamond

Exercise 15.6.6. Prove or disprove: $SL_2(\mathbb{Z})$, the set of 2×2 matrices with integer entries and determinant one, is a subgroup of $SL_2(\mathbb{R})$. \diamond

Exercise 15.6.7. Prove that the intersection of two subgroups of a group G is also a subgroup of G . \diamond

Exercise 15.6.8. Prove or disprove: If H and K are subgroups of a group G , then $H \cup K$ is a subgroup of G . \diamond

Exercise 15.6.9. Prove or disprove: If H and K are subgroups of a group G , then $HK = \{hk : h \in H \text{ and } k \in K\}$ is a subgroup of G . What if G is abelian? \diamond

Exercise 15.6.10. Let G be a group. Show that

$$Z(G) = \{x \in G : gx = xg \text{ for all } g \in G\}$$

is a subgroup of G . This subgroup is called the *center* of G . \diamond

Exercise 15.6.11. Give an example of an infinite group in which every nontrivial subgroup is infinite. \diamond

Exercise 15.6.12. Prove or disprove: Every nontrivial subgroup of a non-abelian group is non-abelian. \diamond

Exercise 15.6.13.

- (a) Recall the discussion of Section 13.6, which explains how two apparently different groups can in fact be essentially the “same” group. Find two groups of order eight that we have studied are not the “same” in this sense, and explain why they can’t be considered as examples of the “same” group.
- (b) Using the previous exercise (which introduces \mathbb{Z}_2^n), give an example of a third group that is not the “same” as the two groups you found in (a), and explain why it is not the “same”.

\diamond

Exercise 15.6.14. Give a specific example of some group G and elements $g, h \in G$ where $(gh)^n \neq g^n h^n$, for some natural number n . \diamond

Exercise 15.6.15. Let a and b be elements in a group G . Prove that $ab^n a^{-1} = (aba^{-1})^n$. \diamond

Exercise 15.6.16. Given a group G which includes elements g_1, \dots, g_n . Prove that the inverse of $g_1 g_2 \cdots g_n$ is $g_n^{-1} g_{n-1}^{-1} \cdots g_1^{-1}$. \diamond

Exercise 15.6.17. Let $U(n)$ be the group of units in \mathbb{Z}_n . If $n > 2$, prove that there is an element $k \in U(n)$ such that $k^2 = 1$ and $k \neq 1$. \diamond

Exercise 15.6.18. Show that if G is a finite group of even order, then there is an $a \in G$ such that a is not the identity and $a^2 = e$. (*Hint*) \diamond

Exercise 15.6.19. Let G be a group and suppose that $(ab)^2 = a^2 b^2$ for all a and b in G . Prove that G is an abelian group. (*Hint*) \diamond

Exercise 15.6.20. Show that if $a^2 = e$ for all $a \in G$, then G must be an abelian group. (*Hint*) \diamond

Exercise 15.6.21. If $(xy)^2 = xy$ for all x and y in $G \setminus e$, prove that G must be abelian. (*Hint*) \diamond

Exercise 15.6.22. If $xy = x^{-1} y^{-1}$ for all x and y in $G \setminus e$, prove that G must be abelian. \diamond

Exercise 15.6.23. Let H be a subgroup of G and

$$N(H) = \{g \in G : gh = hg \text{ for all } h \in H\}.$$

Prove $N(H)$ is a subgroup of G . This subgroup is called the *normalizer* of H in G . \diamond

15.7 Hints for “Abstract Groups: Definitions and Basic Properties” exercises

Exercise 15.2.17: For the “if” part, assume that $g \circ h = h$, and use this to show that $g = e$. Multiply both sides of the assumed equation by h^{-1} . You will need to use associativity and properties of inverses and the identity to obtain the result. For the “only if” part, assume that $g = e$ and use this fact to show that $g \circ h = h$.

Exercise 15.2.18: Suppose that e and f are both identities of G , and use Exercise 15.2.17 to show that this implies $e = f$.

Exercise 15.2.20: Prove by contradiction. Suppose that for row “ g ”, the entries in columns “ h ” and “ h' ” are the same, where $h \neq h'$. Then what equation must be true? Show this equation leads to a contradiction.

Exercise 15.2.27(b): Refer to Section 5.5.5.

Exercise 15.3.7 In general, the way to prove statements like this is to multiply both sides of the equation by the same thing. In this case, you may multiply by ab . Some additional multiplications will give you the result $ba = ab$.

Exercise 15.5.18: Use the fact that $a^k = a^l$ for $k \neq l$. You may assume that $k < l$ in your proof.

Exercise 15.5.26: Write $\text{mod}(m, n)$ as $m + kn$, where k is an integer.

Additional exercises:

Exercise 15.6.5: You may obtain 4 cyclic subgroups of order 2 (why?) To look for more subgroups, suppose for instance there is a subgroup that contains both i and j . What other elements must it contain? Do the same for i and k , j and k , etc.

Exercise 15.6.18: This is a counting argument. Prove by contradiction. Assume the contrary, and pair each group element with its inverse. The entire group is the union of these pairs, plus the identity. What does this tell you about the order of the group?

Exercise 15.6.19: Multiply the equation by some well-chosen inverses.

Exercise 15.6.20: You may use Exercise 15.6.19.

Exercise 15.6.21: In fact, such a group must have at most two elements. Do you see why?

Further Topics in Cryptography

In this chapter we examine two specific topics in cryptography which are highly practical and are relatively recent developments: Diffie-Hellman key exchange (originated by W. Diffie and M. Hellman in 1976) and elliptic curve cryptography (proposed by N. Koblitz and V. Miller in 1985).

Prerequisites: To understand this chapter, the reader should be familiar with the material in Chapters 5,8, and 15. We also make use of one important result from Chapter 20, but we only apply the result and don't make use of the proof itself.

This chapter is written by Moses Marmolejo, with revisions by C.T.

16.1 Diffie-Hellman key exchange

In order to share a private message over a public domain a sender must "lock" or encrypt their message using a *key*. Recall from Section 9.1, that in cryptography a key is a special piece of information (usually a number) that is required to encrypt and decrypt data which is shared between the sender and receiver. There are generally three types of keys used: public, private and symmetric keys. A *public key* can be widely distributed, and is typically used for encrypting messages. For a public key to be effective, there must be a matching *private key* which is known only to the receiver. The private key can be used to decrypt the messages created using the public key. Finally, a *symmetric key* is known by the sender and receiver, and is

used to both encrypt and decrypt messages. Not all cryptosystems require all three kinds of keys, but every cryptosystem must have either a private key or a symmetric key.

If a symmetric key is used, then both parties must share their key before they can begin communicating securely. The requirement of establishing a key exchange is so essential that it is embedded into almost every technology we use today. Some examples of key exchange can be seen in media applications, cell phones, banking, online purchasing, and emails.

But what if the only way the two parties have to communicate is via a public network (such as the Internet), where eavesdroppers can listen in? Under these conditions how can they possibly establish a shared key in such a way that no one else can find out? The Diffie Hellman key exchange (DHKE) is one possible solution to the problem of creating a secret key over an insecure communication channel. Note that the DHKE is not used for encryption/decryption of messages, but only to establish a key that can be used to encrypt/decrypt subsequent messages. Follow the steps below to see the DHKE process.

- Step 1. First, Moses and Rachael agree upon a pair of numbers p and g . p is called the **modulus**, while g is called the **base**. These numbers are not secret, but Moses and Rachael do not care if eavesdroppers find out what p and g are. In practice, p and g are required to have certain properties (as explained below) to maximize secrecy. However, the DHKE procedure still works for any values of p and g .
- Step 2. Moses chooses a secret integer n , known only to himself. He then computes q where $q = \text{mod}(g^n, p)$, and sends Rachael the value of q . Rachael does not need to know the value of n .
- Step 3. Rachael similarly chooses her own secret integer m , computes r where $r = \text{mod}(g^m, p)$ and sends Moses the value of r .
- Step 4. Moses computes $\text{mod}(r^n, p) = k_M$;
- Step 5. Rachael computes $\text{mod}(q^m, p) = k_R$;

It turns out that when k_R and k_M are computed by the above procedure, then k_R is always equal to k_M . You will show this in the next exercise.

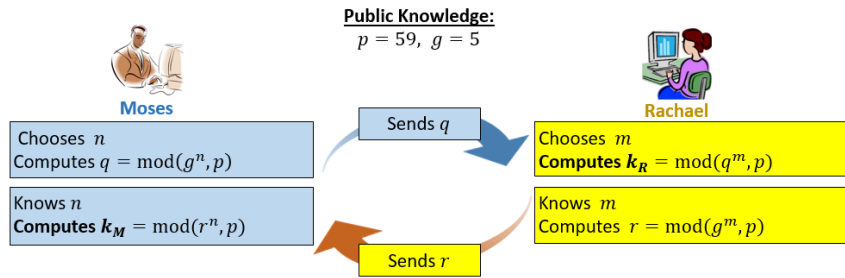


Figure 16.1.1. Key exchange between Moses and Rachael using DHKE

Exercise 16.1.1.

Fill in the blanks in the following proof that k_R is always equal to k_M .

PROOF.

$$\begin{aligned}
 k_R &= \text{mod}(q^m, \text{---}) && \text{(definition of } k_R) \\
 &\equiv \text{mod}((g\text{---})^m, p) && \text{(substitution)} \\
 &\equiv \text{mod}((g\text{---})^n, p) && \text{(rules of exponents)} \\
 &\equiv \text{mod}((r\text{---}), p) && \text{(substitution)} \\
 &= k_M
 \end{aligned}$$

If two numbers in \mathbb{Z}_p are modular equivalent, then they are the same number. Thus, $k_R = k_M$ is a symmetric key, which we may refer to as k .

□

◇

Now that you understand the process for DHKE, follow the example below. (Note that this example is just to give you the idea—it’s much too simple to use in practical applications.)

Example 16.1.2. Key exchange between a sender and receiver (Moses and Rachael) using the DHKE is shown in the following steps.

Step 1. Prior to sending data, Moses and Rachael agree $p = 13$ and $g = 7$;

Step 2. Moses chooses $n = 2$, and sends Rachael $\text{mod}(7^2, 13) = 10$;

Step 3. Rachael chooses $m = 8$, and sends Moses $\text{mod}(7^8, 13) = 3$;

Step 4. Moses computes $\text{mod}((3)^2, 13) = 9$;

Step 5. Rachael computes $\text{mod}((10)^8, 13) = 9$;

As a result of the exchange, both Moses and Rachel have obtained the same shared key, which is 9. \diamond

Following the example above you can see that the DHKE requires that you raise a given number g to a natural number (either m or n) and take the result mod p . This operation is called *discrete exponentiation*. Calculating discrete exponentials with small values of m or n is manageable, but in practice the exponent m or n can be enormous, with hundreds of digits. It would seem that in this case discrete exponentiation would take a long, long time to compute. But we can use the repeated squaring formula described in Section 9.3.3 to speed up the process. Create a spreadsheet using the repeated squaring formula to compute the following exercises.

Exercise 16.1.3. Suppose you want to conduct a DHKE with one person, and you are given $p = 32452867$; $g = 54321$; and $n = 876$.

- (a) What number do you send?
- (b) You are then sent 31975948, what is the shared key?
- (c) If $m = 123$ what number does the other party calculate for the shared key?

\diamond

Exercise 16.1.4. Suppose you want to conduct a DHKE with one person, and you are given $p = 86028157$; $g = 98765$; and $n = 123$.

- (a) What number do you send?
- (b) You are then sent 53161396, what is the shared key?
- (c) If $m = 87$ what number does the other party calculate for the shared key?

\diamond

Now that we understand the DHKE process, let us try to understand why it effectively guarantees the secrecy of the shared key. First, we need

to understand a little more about the operation of discrete exponentiation, which (as we have seen) is the foundation of the DHKE process. So we are going on a short digression, but don't worry—we will get back to the main point shortly.

In previous math courses you learned that the inverse operation of exponentiation is taking the logarithm: for example, $2^3 = 8$ while $\log_2 8 = 3$. It is possible to do the same with discrete exponentiation: an inverse operation to discrete exponentiation is referred to as 'finding a *discrete logarithm* or (DL)'. Note that since discrete exponentiation involves raising to a power which is a natural number, a DL will always be a natural number. For example, since $\text{mod}(2^5, 7) = 4$, we could say that under multiplication mod 7, 5 is a DL of 4 with base 2.

Now why have we been saying, "a DL" rather than "the DL"? Because there happens to be more than one:

Exercise 16.1.5.

- (a) Find all natural numbers n such that $\text{mod}(2^n, 7) = 4$. Use your result to complete the following sentence: "Under multiplication mod 7, the discrete logarithm(s) of 4 with base 2 are"
- (b) Find all natural numbers n such that $\text{mod}(2^n, 7) = 3$. Use your result to complete the following sentence: "Under multiplication mod 7, the discrete logarithm(s) of 3 with base 2 are"
- (c) Find all nonzero elements of $\mathbb{Z}_7 \setminus \{0\}$ which have no discrete logarithms with base 2.
- (d) Find all nonzero elements of $\mathbb{Z}_7 \setminus \{0\}$ which have no discrete logarithms with base 3.

◇

The preceding exercise points out some key issues with discrete logarithms. Sometimes there are lots of them, and sometimes there aren't any! These phenomena are related to the one-to-oneness and onto-ness properties of the discrete exponential function (recall Definitions 8.3.6 and 8.4.4, respectively):

Exercise 16.1.6.

- (a) We may define a function $f : \mathbb{Z}_7 \setminus \{0\} \rightarrow \mathbb{Z}_7 \setminus \{0\}$ by the equation: $f(n) = \text{mod}(2^n, 7)$. Use parts (a) and (b) of Exercise 16.1.5 to prove that f is neither one-to-one nor onto.
- (b) We may also define a function $g : \mathbb{Z}_7 \setminus \{0\} \rightarrow \mathbb{Z}_7 \setminus \{0\}$ by the equation: $g(n) = \text{mod}(3^n, 7)$. Prove or disprove: g is one-to-one.
- (c) With the same g as in part (b), prove or disprove: g is onto.

◇

This exercise suggests the following question: Under what conditions can we guarantee that the discrete exponentiation function is onto and/or one-to-one? (This turns out to be more than just an idle question, as we shall see shortly.) To gain some leverage against this problem, we will take advantage of Proposition 20.6.3 from Chapter 20, which tells us that the multiplicative group $\mathbb{Z}_p \setminus \{0\}$ is *cyclic*, whenever p is a prime. (In Chapter 20 we also used the notation $U(p)$ instead of $\mathbb{Z}_p \setminus \{0\}$, and we will use this same notation in the following.) This means that for any prime p , there is a $g \in U(p)$ such that g is a *generator* of $U(p)$: that is, $U(p) = \langle g \rangle$ (recall from Chapter 15 that for a finite group, $\langle g \rangle = \{g, g^2, g^3, \dots\}$). A generator of $U(p)$ is also referred to as a *primitive root* of \mathbb{Z}_p . Any element of $U(p)$ may be expressed as a power of g (under mod p multiplication). In other words, the discrete exponentiation function $f : \mathbb{N} \rightarrow U(p)$ given by $f(n) = \text{mod}(g^n, p)$ is an onto function!

It turns out that onto-ness also gives us one-to-oneness, when we restrict f to the appropriate domain:

Exercise 16.1.7. Suppose that p is a prime, and g is a generator of $U(p)$. Consider the function $h : U(p) \rightarrow U(p)$ given by $h(n) = \text{mod}(g^n, p)$. (Note that h is the same as f defined above, only the domain has been restricted.) Show that h is a bijection. ◇

It's about time we got back to the main point of why we're talking about DL's in the first place. Suppose an eavesdropper who is listening in on Moses and Rachael's conversation wants to figure out the secret key k . The eavesdropper knows $p, g, q = \text{mod}(g^n, p)$, and $r = \text{mod}(g^m, p)$. If he could figure out m he could easily get the secret key by computing $\text{mod}(q^m, p)$ which is equal to k . But finding m is just a DL problem, since m is a DL of r with base g under multiplication mod p .

There is an issue that we should address here. We have pointed out that any DL problem has many different solutions. What if the eavesdropper finds a different solution to the DL problem, which is not equal to the m originally used by Rachael? It turns out that the eavesdropper can crack the code with *any* DL solution, as the following exercise shows:

Exercise 16.1.8. Suppose that m and m' are two different DL's of r with base g under multiplication mod p . Show that $\text{mod}(g^{mn}, p) = \text{mod}(g^{m'n}, p)$. In other words, an eavesdropper can use *any* DL of r with base g under multiplication mod p to find the shared key. \diamond

Exercise 16.1.9. Suppose another eavesdropper was able to compute a DL of q with base g under multiplication mod p . Explain how she could use this information to find Moses and Rachael's secret shared key. \diamond

The security of the DHKE leverages the easy computation of the discrete exponentials versus the difficulty of computing DL's. (A function which is easy to compute but hard to invert is referred to as a **one-way function**. Discrete exponentials (for suitable p 's and g 's) form a very important class of one-way functions.) The following simple example introduces how this works in practice.

Example 16.1.10. It is easy to calculate $\text{mod}(2^m, 11)$ for different values of m : for example, when $m = 8$ then we get $\text{mod}(2^8, 11) = \text{mod}(256, 11) = 3$. However, when you try to invert the process, you have: given $\text{mod}(2^m, 11) = 3$, calculate m . There is no easy way to do this. As you can see below the results jump around, and each solution is equally likely to be an integer between 0 and 11.

$$\text{mod}(2^1, 11) = 2$$

$$\text{mod}(2^2, 11) = 4$$

$$\text{mod}(2^3, 11) = 8$$

$$\text{mod}(2^4, 11) = 5$$

$$\text{mod}(2^5, 11) = 10$$

$$\text{mod}(2^6, 11) = 9$$

$$\text{mod}(2^7, 11) = 7$$

$$\text{mod}(2^8, 11) = 3$$

$$\text{mod}(2^9, 11) = 6$$

$$\text{mod}(2^{10}, 11) = 1$$



If you try to calculate m using a brute force method (that is, computing all possible solutions one at a time), you would have to calculate 8 different solutions before you find the right answer.

The larger the modulus, the harder the DL is to find. The exercise below is designed to show how many computations a brute force attack would take in comparison to a growing modulus.

Exercise 16.1.11. Use the Repeated Square spreadsheet from Exercise 9.3.3 to solve the following DL Problems. In each case, you will use the brute force method used in Example 16.1.10, and write down how many discrete exponentials you need to compute in order to find the answer.

- (a) Given $\text{mod}(7^m, 41) = 28$, solve for m .
- (b) Given $\text{mod}(5^m, 73) = 13$, solve for m .
- (c) Given $\text{mod}(17^m, 211) = 161$, solve for m .
- (d) What trend do you see in the number of computations required in parts (a), (b), (c), and how does it relate to the moduli in the different cases?



From the foregoing discussion, we may see why it is important to choose a prime p as a modulus and a primitive root g as a base in an effective DHKE scheme. This choice will minimize duplicate DLs and create the largest search space possible for an eavesdropper. If you do not use a primitive root as a generator, then you will end up with a smaller subgroup of $U(p)$ which will have an increased number of DLs, and an eavesdropper trying to calculate m using a brute force method is more likely to succeed.

16.1.1 Man in the middle attack

Our previous discussion indicates the DHKE is very hard to crack if it uses a large enough modulus p and a suitable base g . But, is there any way to successfully eavesdrop on Moses and Rachael’s conversation without actually cracking the code? It seems that Moses and Rachael’s security is assured, since an attacker would only be privy to $\text{mod}(g^n, p)$ and $\text{mod}(g^m, p)$, each of which cannot be used to decrypt the message since an attacker would have to compute the DL problem to find m and n .

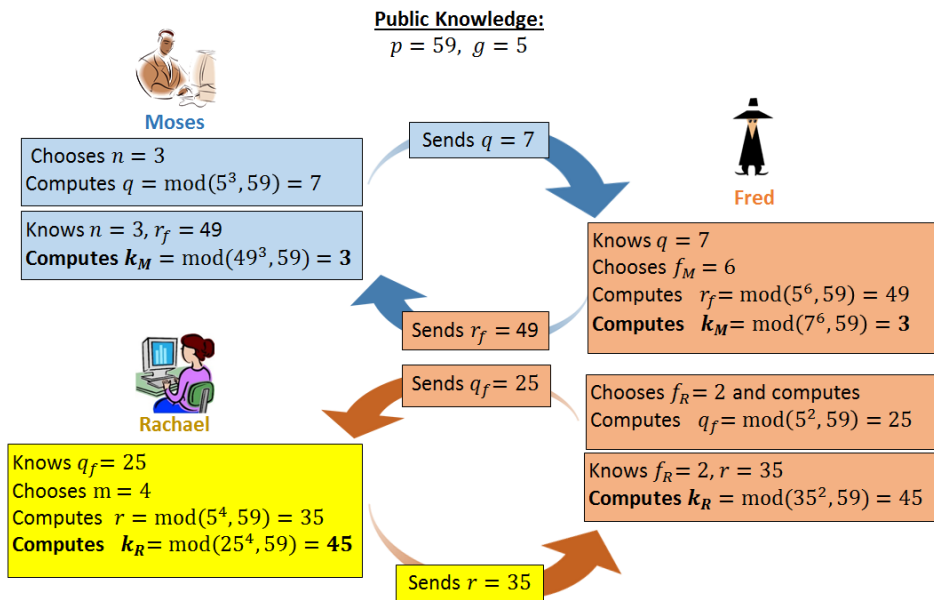


Figure 16.1.2. MiM Attack during Moses and Rachael’s key exchange

But not so fast. What would happen if an attacker, Fred (an eavesdropper) places himself between Moses and Rachael’s messages? If Fred could do this then Rachael’s message would pass through Fred first before reaching Moses, and vice-versa. Fred would then be able to intercept the public key and establish his own private keys with Moses and Rachael separately. Fred is now able to read or alter messages. This type of attack is commonly referred to as the Man in the Middle (MiM) attack. See Figure 16.1.2 to see how Fred is able to modify the key exchange.

Following Figure 16.1.2, Fred establishes one secret key k_M with Moses and a different secret key k_R with Rachael. Now Moses thinks r_f is Rachael’s

public key, and Rachael thinks that she has Moses' public key. Moses and Rachael both combine their private keys with Fred's public keys and create two different symmetric keys, k_M and k_R respectively. At this point if either Moses or Rachael sends a message, then Fred is free to decrypt and encrypt the message using the appropriate key.

Exercise 16.1.12. Redo Figure 16.1.2 using different values of p, g, n, m, f_n , and f_m , remember to choose a prime for p and a primitive root for g (there are many primitive root calculators you can find online). \diamond

Exercise 16.1.13. Replace all the numbers in the formulas found in Figure 16.1.2 with letters, as seen in Figure 16.1.1. \diamond

Exercise 16.1.14. Given $p = 73$, and $g = 11$ find q, r, r_f, q_f, k_M , and k_R if Moses chooses $n = 5$, Rachael chooses $m = 4$ and Fred chooses $f_M = 3$ and $f_R = 2$. \diamond

DHKE is vulnerable to this type of MiM attack since Moses cannot verify that Rachael was the originator of the message, and vice-versa. Fortunately, MiM attacks can be prevented if messages are sent with a so-called *digital signature* which uniquely identifies the source of the message. In Section 16.1, we described how to send uniquely-identifiable messages by using a private key to encrypt messages that can be decrypted by a public key. So Moses may share his key with Rachael by encrypting his public key, together with some known text. Even if the MiM can receive and decode this information, there is no way for him (or her) to send a bogus key to Rachel, because (s)he does not know Moses' signature key.

Diffie-Hellman is just one of many key exchange algorithms. In the next section, we will talk about a different key exchange method that is even more secure.

16.2 Elliptic curve cryptography

In the previous section we saw that the longer the key, the greater the security. Unfortunately longer keys require sending more information, thus slowing down communication. Elliptic curve cryptography (ECC) is one approach to the public key sharing dilemma that offers greater security with

smaller keys. The table in Figure 16.2.1 shows the relationship between key length and security for three different cryptosystems: RSA, Diffie-Hellman, and ECC. In the table, ‘key length’ refers to the number of binary bits in the key: for comparison, a 160 bit key has 49 decimal digits, while a 1024 bit key has 309 decimal digits. The ‘security level’ is also measured in bits (80, 128, 192, 256) where these bits refer to the size of the number of computational steps necessary to break the code. For example, a security level of 80 means that 2^{80} computations are required to break the code (from reference(5)). To give you an idea of what this means practically, in 2002 it took 10,000 computers (mainly PCs) running 24 hours a day for 549 days to break an ECC system with a 109 bit key length. A 160-bit ECC would be 2^{25} times more secure: which means that (with 2002 technology) it would take one billion computers over 500 years to crack it.

| Cryptosystem | Security Level (bit) | | | |
|----------------|----------------------|----------|----------|-----------|
| | 80 | 128 | 192 | 256 |
| RSA | 1024 bit | 3072 bit | 7680 bit | 15360 bit |
| Diffie Hellman | 1024 bit | 3072 bit | 7680 bit | 15360 bit |
| Elliptic Curve | 160 bit | 256 bit | 384 bit | 512 bit |

Figure 16.2.1. Key bit lengths of cryptosystems for different security levels recommended by the National Institute of Standards and Technology, (from reference (8))

Referencing the table in Figure 16.2.1, we can see that an ECC cryptosystem with a 160 bit key has a similar security level to RSA and Diffie-Hellman with 1024-bit keys. This means the same security with 6 times less information—a significant difference!

Exercise 16.2.1. How long would it take to crack a cryptosystem with a 128 bit security, using a billion modern computers with 2 GHz processors? (Note: A 2 GHz processor is able to perform $2 \cdot 10^9$ computations per second.)

◇

Now that we’ve described the benefits of ECC, let’s see what elliptic curves are all about. Our discussion will be quite wide-ranging, and touch on several areas of mathematics. Although we will not go into the background, elliptic curves originally arose from the study of polynomial equations in

multiple variables. Elliptic curves also have deep connections to the theory of complex functions.

16.2.1 Definition of elliptic curves

An Elliptic Curve (EC) is the set of solutions (x, y) of an equation of the form $y^2 = x^3 + ax + b$, where a and b are real coefficients. See Figure 16.2.2 below for graphs of some ECs. Additionally, ECs are not allowed to have double

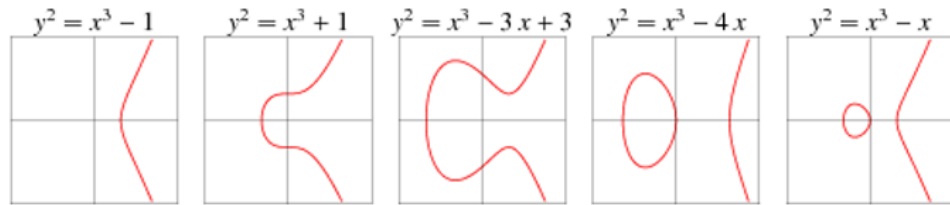


Figure 16.2.2. Geometric shapes of ECs, (from reference (15))

or triple roots in the variable x . A triple root produces a cusp in the graph, and a double root produces a self-intersection (see graphs in Figure 16.2.3). See graphs in Figure 16.2.3 for examples of ECs with double and triple roots. It turns out that we can guarantee that the curve $y^2 = x^3 + ax + b$ has no

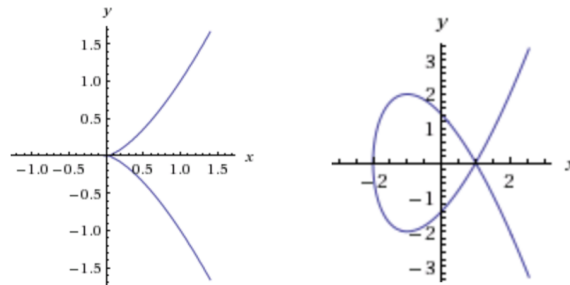


Figure 16.2.3. (Left) EC: $y^2 = x^3$ and (Right) EC: $y^2 = x^3 - 3x + 2$, (From reference (7))

double or triple roots if the coefficients a and b satisfy the following equation: $4a^3 + 27b^2 \neq 0$.

Exercise 16.2.2.

- (a) Prove that if the equation $y^2 = x^3 + ax + b$ has a double or triple root, then $4a^3 + 27b^2 = 0$. (*Hint*)
- (b) Prove the converse to part (a), that is show that if $4a^3 + 27b^2 = 0$, then the equation has a double or triple root. (*Hint*)

◇

All of the cryptosystems that we have studied so far have been based on group operations associated with a particular group. For example, Diffie-Hellman used discrete exponentiation (which is repeated multiplication in $U(p)$) to construct a one-way function. In order to use ECs to construct cryptosystems, we'll need to show that we can associate a group with each EC. In the following sections we'll define an arithmetic operation on the points of any EC, and show that this operation is in fact a group operation.

16.2.2 Elliptic curve arithmetic

In this section, we show how to do arithmetic on ECs. Specifically, we define an operation (denoted by '+') which acts on two points of an EC, to give another point on the same EC.

Suppose that P_1 and P_2 are two points on an EC. We will consider first the case where $P_1 \neq P_2$: later we will consider the case where $P_1 = P_2$. Geometrically, if the two points are different then $P_1 + P_2$ is given by drawing a line from point P_1 to point P_2 and continuing the line until it intersects the EC, then reflect that point about the x -axis. See Figure 16.2.4 for a geometric representation of the operation $P_1 + P_2$.

It turns out that $P_1 + P_2$ is always defined on the EC (except in one special case which we will explain a little bit later), even though sometimes the result of $P_1 + P_2$ is quite far away from both P_1 and P_2 . For instance, take the EC $y^2 = x^3 - x$, and points $P_1 = (2, \sqrt{6})$ and $P_2 = (3, -\sqrt{24})$. Then $P_1 + P_2 = (49, 342.93)$ (we'll show this later in Example 16.2.6), as illustrated in Figure 16.2.5.

Example 16.2.3. Given the EC: $y^2 = x^3 + ax + b$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and $P_3 = (x_3, y_3)$. Find P_3 , where $P_3 = P_1 + P_2$.

The steps of this calculation are as follows:

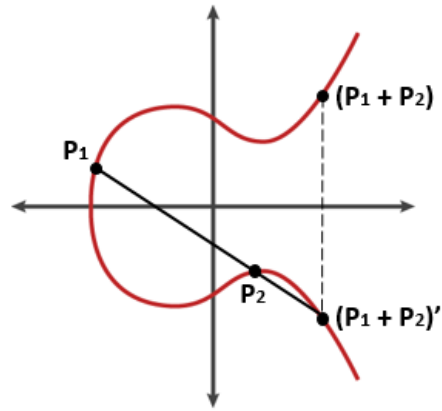


Figure 16.2.4. Adding two distinct points, $P_1 + P_2$ on the EC (from reference (9)).

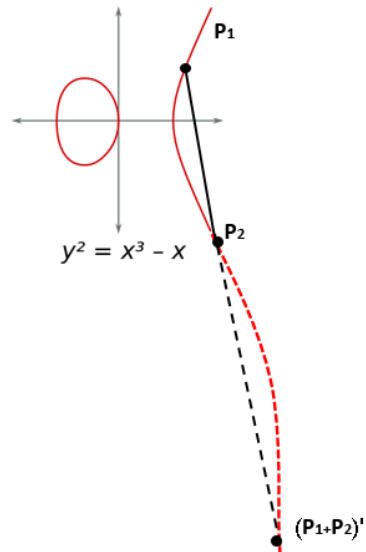


Figure 16.2.5. $P_1 + P_2$ is always defined on the EC (from reference (9)).

- (a) Compute the slope of the line m through P_1 and P_2 as follows:

$$m = (y_2 - y_1) \cdot (x_2 - x_1)^{-1}, \text{ for } P_1 \neq P_2$$

- (b) Use the point-slope formula $y - y_1 = m(x - x_1)$ in order to find equation of the line that passes through the two points. Rewrite as:

$$y = m(x - x_1) + y_1$$

- (c) It turns out that the sum of the roots is m^2 (see Exercise 16.2.4). So we have

$$x_1 + x_2 + x_3 = m^2, \text{ which implies } x_3 = m^2 - x_1 - x_2.$$

- (d) The third point of intersection is $(x_3, -y_3)$. So we may plug x_3 into $(-y_3) = m(x_3 - x_1) + y_1$ to obtain y_3 .
- (e) Finished! $P_3 = (x_3, y_3)$.



Exercise 16.2.4. In part (c) of Example 16.2.3 we mentioned that $x_1 + x_2 + x_3 = m^2$, where x_1, x_2, x_3 are the x-coordinates of three intersections of the line with the EC and m is the slope of the line. In this exercise, we will prove this.

- (a) Substitute the equation for y in (b) of Example 16.2.3 into equation E. The resulting equation can be rearranged to form a cubic equation in x of the form: $0 = x^3 + c_2x^2 + c_1x + c_0$, where c_0, c_1, c_2 depend on the parameters a, b, m, x_1, y_1 . Express the coefficient c_2 in terms of these parameters.
- (b) The cubic equation $0 = x^3 + c_2x^2 + c_1x + c_0$ has three roots, so the cubic equation can be factored: $x^3 + c_2x^2 + c_1x + c_0 = (x - x_1)(x - x_2)(x - x_3)$. Use this equality to express c_2 in terms of x_1, x_2, x_3 .
- (c) Based on your results in (a) and (b), show that $m^2 = x_1 + x_2 + x_3$.



Example 16.2.5. Given the elliptic curve $y^2 = x^3 - 2x$, $P_1 = (0, 0)$, $P_2 = (-1, 1)$, Find $P_3 = P_1 + P_2$.

- (a) Slope : $m = (1 - 0) \cdot (-1 - 0)^{-1} = -1$.
- (b) Equation of line: $y - 0 = -1(x - 0)$ or $y = -x$.
- (c) Use $x_3 = m^2 - x_1 - x_2$ to obtain: $x_3 = (-1)^2 - 0 - (-1) = 2$.
- (d) Use equation of line with $y = -y_3$ and $x = x_3$: $-y_3 = -2$ or $y_3 = 2$.
- (e) $P_3 = (2, 2)$.



Example 16.2.6. Given E: $y^2 = x^3 - x$, $P_1 = (2, \sqrt{6})$, $P_2 = (3, -\sqrt{24})$ from Figure 16.2.5 above. Find P_3 , where $P_3 = P_1 + P_2$.

- (a) Slope: $m = (-\sqrt{24} - \sqrt{6}) \cdot (3 - 2)^{-1} = -3\sqrt{6}$
- (b) Line: $y + \sqrt{24} = -3\sqrt{6}(x - 3)$, which simplifies to $y = -3\sqrt{6}x + 7\sqrt{6}$.
- (c) Use $x_3 = m^2 - x_1 - x_2$ to obtain: $x_3 = (-3\sqrt{6})^2 - 2 - 3 = 49$.
- (d) Plug $(1, -y_3)$ in for (x, y) in the equation for the line: $-y_3 = -3\sqrt{6} \cdot 49 + 7\sqrt{6}$, which implies $y_3 = 140\sqrt{6}$.
- (e) $P_3 = (49, 140\sqrt{6}) \approx (49, 342.93)$.



Exercise 16.2.7. Given E: $y^2 = x^3 - 2x$, $P_1 = (2, 2)$, $P_2 = (-1, 1)$, find P_3 , where $P_3 = P_1 + P_2$. ◇

Exercise 16.2.8. Given E: $y^2 = x^3 - x + 1$, $P_1 = (3, 5)$, $P_2 = (1, 1)$, find P_3 , where $P_3 = P_1 + P_2$. ◇

If the two points are the same, $P_1 = P_2 = (x_1, y_1)$, then a tangent line to the point is drawn and the point of intersection to the EC is then reflected about the x-axis. This is often referred to as **point doubling**. For the general EC with equation $y^2 = x^3 + ax + b$, the slope for this line is,

$$m = (3x_1^2 + a) \cdot (2y_1)^{-1},$$

which may be found using implicit differentiation. See Figure 16.2.6 below for a geometrical representation of point doubling.

Exercise 16.2.9. Derive the equation for m by taking derivatives of both sides of the general equation and solving for $\frac{dy}{dx}$. Show your steps. \diamond

In the case of point doubling, once m is found the expression for the x coordinate of the other intersection of the tangent line with the curve is:

$$x_3 = m^2 - x_1 - x_1$$

(this is because x_1 is a double root of the cubic expression which gives the x -coordinates of the intersections between the EC and the tangent line). Once we have x_3 , then we may find y_3 as before:

$$-y_3 = m(x_3 - x_1) + y_1$$

and $2P_1$ is given by (x_3, y_3) .

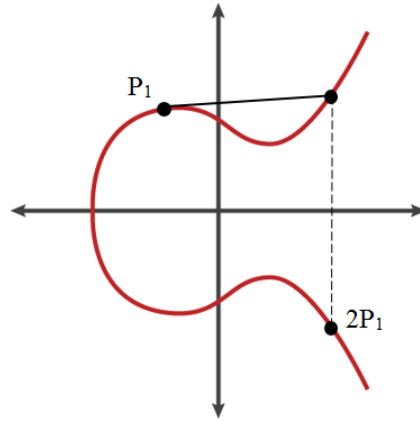


Figure 16.2.6. Point doubling on the EC (from reference (7)).

There is one scenario where addition of two points doesn't give a point on the curve. Given a point P , we define $-P$ as the reflection of P about the x axis: so if $P = (x, y)$, then $-P = (x, -y)$. The line through P and $-P$ is vertical, and does not intersect the curve at any other point. In order to make addition well-defined in this case we may create a notional *point at infinity*. See Figure 16.2.7 below for a geometrical representation of

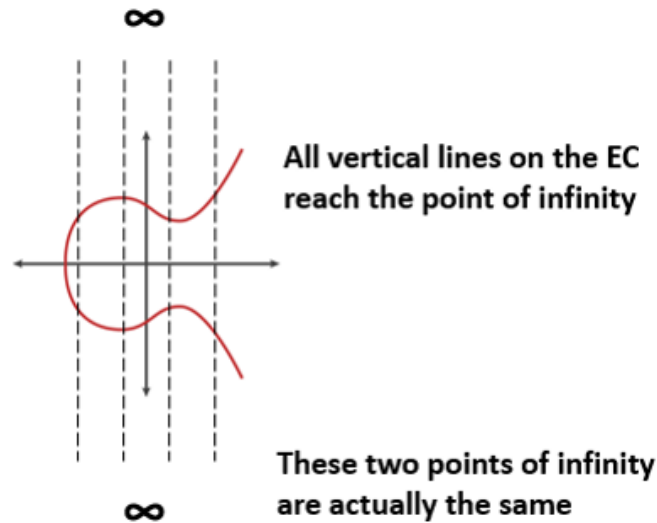


Figure 16.2.7. The point at infinity located at $(0, \infty)$ (from reference (9)).

the point at infinity. The point at infinity can be thought of as located at the point $(0, \infty)$, so that the line through any point (x, y) and the point at infinity is a vertical line with infinite slope. Additionally, the point at infinity is its own reflection, so we consider $(0, \infty)$ and $(0, -\infty)$ as a single point, which we denote by the symbol ∞ . You may think of the y axis “wrapping around” so that when you keep moving in the $+y$ direction eventually you wrap around to the $-y$ axis.

16.2.3 Elliptic curve groups

Remarkably, it turns out that the ‘+’ operation turns the EC (plus the point at infinity) into a group. In this section we’ll verify all of the group properties.

1. **Identity:** The point at infinity serves as the identity element. The line connecting ∞ with P intersects $-P$, so its reflection about the x -axis is P . Therefore, $P + \infty = P$ and $\infty + P = P$.
2. **Inverse:** A line through P and $-P$ goes through ∞ , and ∞ is its own reflection (see Figure 16.2.8). Another way of saying this is, $P + (-P) = \infty$. In the same way, we can show that $(-P) + P = \infty$. Therefore the inverse of P is $-P$.

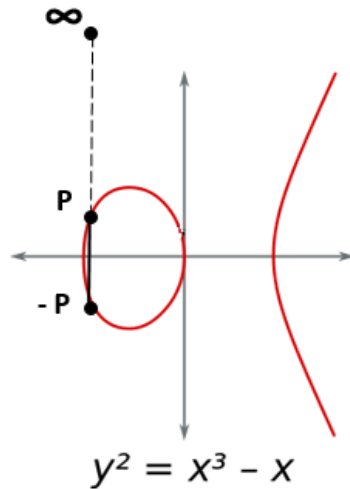


Figure 16.2.8. Identity property for EC: $\infty + P = P + \infty = P$ (from reference (9)).

3. **Closure:** if P_1 and P_2 are points on the elliptic curve then $P_1 + P_2$ is also a point on the curve; as stated (without proof) in Section 16.2.2.
4. **Associativity:** $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$. This is always true (for an example, see Figure 16.2.9 below), but it is not at all easy to prove. See for example math.rice.edu/~friedl/papers/AEELLIPTIC.PDF, which gives a 5-page “elementary” proof.

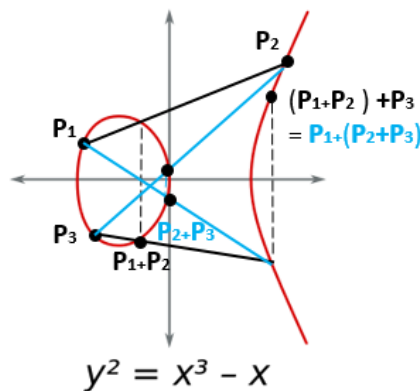


Figure 16.2.9. Associative property for EC (from reference (9)).

These properties are sufficient to establish the fact that the ‘+’ operation on an elliptic curve defines a group.

Exercise 16.2.10. Does the ‘+’ operation define an Abelian group? Prove your answer. \diamond

16.2.4 Elliptic curves over \mathbb{Z}_p

Thus far we have looked at ECs whose coefficients are real numbers. Unfortunately, computer calculations with real numbers are prone to rounding errors, so real number arithmetic is not suitable for modern cryptography. To avoid this problem, instead of using real numbers we use *finite fields*, which are finite additive groups that also have a multiplication operation with inverse. The simplest finite fields are \mathbb{Z}_p (integers mod p), where p is prime. In this section we will demonstrate how to do arithmetic with ECs over \mathbb{Z}_p .

At the end of the previous section, we showed that our new ‘+’ operation allows us to define a group on the set of points of an elliptic curve, when the curve is a subset of R^2 and is defined using real coefficients. It turns out that exactly the same argument can be used to show the very same group property for curves with coefficients in \mathbb{Z}_p , which are subsets of $\mathbb{Z}_p \times \mathbb{Z}_p$.

We saw in Section 15.5.2 that every element of a group defines a **cyclic subgroup**. Specifically, if the group G is finite, then for any element $g \in G$ the set

$$\text{id}, g, g^2, g^3, \dots, g^{n-1}$$

is a subgroup of G , where n is the *order* of g and satisfies $g^n = \text{id}$. In EC cryptography, extensive use is made of cyclic subgroups. Any EC cyptosystem is based on a single group element, which is referred to as a **generator**. In practice, the generator is added to itself repeatedly. Follow the examples below to see how this works.

Note that in the following examples we will use ‘+’ and ‘·’ to denote addition and multiplication in the particular \mathbb{Z}_p that we are working with: in other words, ‘+’ and ‘·’ in the following are the same as ‘ \oplus ’ and ‘ \odot ’ which we used in Chapter 5 (it’s simpler to write this way, and this is how it’s done in most references.) You’ll have to pay attention to what ‘+’ is operating on in order to discern its meaning: for example, in the expression $P + P$ we’re referring to the EC operation defined in the previous section, while in the polynomial $x^3 + 2x + 2$ the ‘+’ refers to modular addition.

Example 16.2.11. In this example we'll use arithmetic mod 17, so all coefficients and variables take values on \mathbb{Z}_{17} .

Given the EC $y^2 = x^3 + 2x + 2$, and $P = (5, 1)$, we want to find $2P$, where $2P = P + P$.

First we use the slope of the tangent line, using the same formula we did for the real case in Example 16.2.3:

$$m = (3x_1^2 + a) \cdot (2y_1)^{-1}$$

We may then calculate (remember we're doing arithmetic in \mathbb{Z}_{17} !)

$$\begin{aligned} m &\equiv ((3 \cdot 5^2) + 2) \cdot (2 \cdot 1)^{-1} \\ &\equiv (77) \cdot (2)^{-1} \\ &\equiv (9) \cdot (9) \\ &\equiv 81 \\ &\equiv 13 \pmod{17} \end{aligned}$$

Next we use the following formulas (which we used before for real ECs) to find x_3 and y_3 :

$$x_3 = m^2 - 2x_1, \text{ and } y_3 = -(m(x_3 - x_1) + y_1)$$

where once again, arithmetic is in \mathbb{Z}_{17} :

$$\begin{aligned} x_3 &\equiv (13^2 - 5 - 5) \\ &\equiv 159 \\ &\equiv 6 \pmod{17} \end{aligned}$$

$$\begin{aligned} y_3 &\equiv -(13(6 - 5) + 1) \\ &\equiv -14 \\ &\equiv 3 \pmod{17} \end{aligned}$$

Therefore, $2P = (6, 3)$. ♦

Exercise 16.2.12. Using the equations from Example 16.2.3 parts (c) and (d), find the following: $3P, 4P, 5P, \dots, 20P$ for the point $P = (5, 1)$ that was used in Example 16.2.11. Note that $3P = 2P + P, 4P = 3P + P$, and so on.

Note also that arithmetic operations are to be performed in mod 17. What do you notice about $18P$, $19P$, and $20P$? \diamond

In view of what we have just discussed, let's reconsider the Diffie-Hellman key exchange which we described in Section 16.1. A little thought should convince you that in that section we made use of cyclic subgroups as well. So using Example 16.2.11 and Exercise 16.2.12, let's revise the Diffie-Hellman key exchange, but this time we'll use the cyclic group associated with the EC. Use Figure 16.2.10 as a guide to help you answer the following exercise.

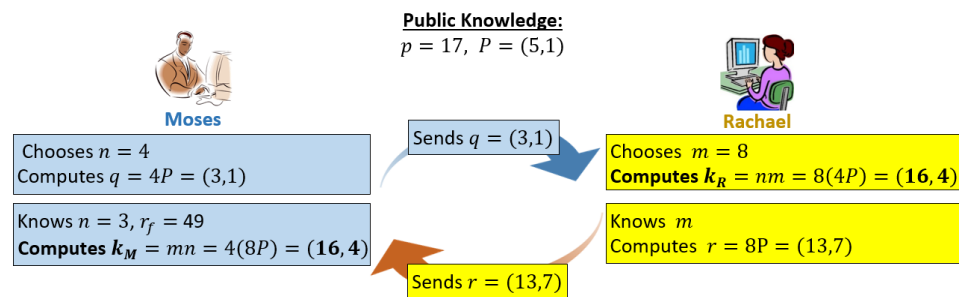


Figure 16.2.10. Elliptic Curve key exchange between Moses and Rachael

Exercise 16.2.13. Using Example 16.2.11 and Exercise 16.2.12, what is their shared key if Moses chooses $n = 9$ and Rachael chooses $m = 3$? \diamond

16.2.5 An encryption system using elliptic curves

In Chapter 9 we explained how to use RSA with a shared key to exchange secret messages. We can construct a similar cryptosystem on the basis of ECs. In this section, we'll describe one way that this may be done. The following discussion is a simplified version of reference (11).

Suppose Moses and Rachael would like to communicate a message using ECC, then they should first agree upon an EC and a code table. Each character of the encrypted message will correspond to a point on the EC.

Next, Rachael and Moses construct public and private keys as follows. First, Rachael and Moses agree upon an EC, modulus, and a random point C on the EC: in general, this will be public knowledge. Additionally, Rachael selects at random a large positive integer α which is Rachael's private key. She computes $A = \alpha C$ which is her public key (recall that αC denotes

adding the point C α times, using EC addition). Moses similarly takes a large positive integer β as his private key, and computes $B = \beta C$ as his public key.

Now if Moses wants to encrypt a message, he may do so one character at a time as follows. Suppose the character that he wants to encrypt corresponds to the point M on the EC. He chooses a random number γ (which will be different for each character in the message). He then computes:

$$E_1 = \gamma C \text{ and } E_2 = M + \gamma A.$$

Moses then communicates E_1 and E_2 to Rachael. After receiving this information, Rachael may decrypt the message by computing $E_2 - \alpha E_1$.

Exercise 16.2.14.

- a Show that by computing $E_2 - \alpha E_1$, Rachael will correctly recover the character M .
- b Suppose a third party knows E_1, E_2, A , and C . What else would a third party have to find out in order to obtain M ? Explain why it is difficult for the third party to gain this knowledge.

◇

Exercise 16.2.15.

- a Suppose Rachael wants to send a character R to Moses. What information should she send to him? Give explicit formulas for this information.
- b What equation should Moses use to decode the information from Rachael?

◇

To see how this works in practice, let's consider a simple example (reader beware: the modulus is way too small to make this a practical cryptosystem). We will consider the EC in $Z_{37} \times Z_{37}$ given by the equation $y^2 = x^3 + 2x + 9$ which is shown in Figure 16.2.11 below. Notice how the graph of the function using modular arithmetic is a collection of discrete points on the curve rather than based on a continuous graph like the ECs over the real numbers.

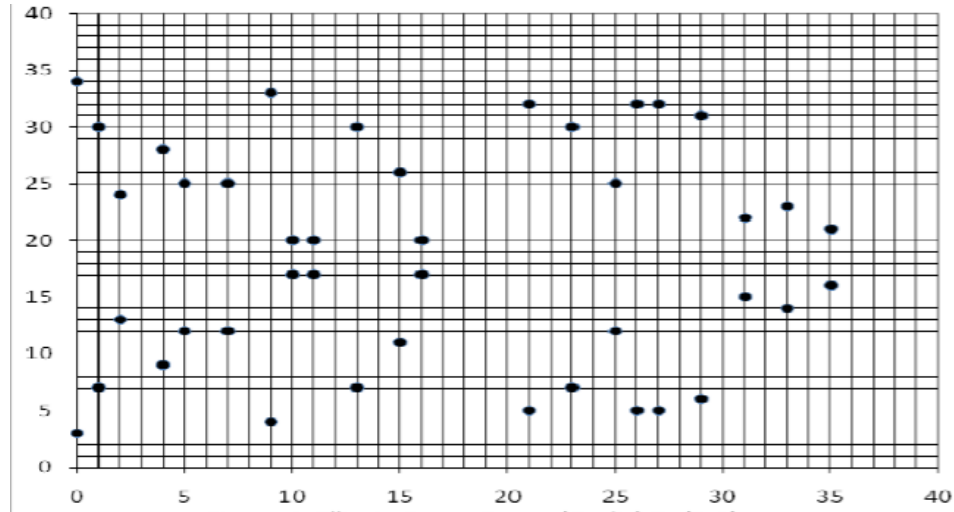


Figure 16.2.11. Elliptic Curve, $(y^2 = x^3 + 2x + 9)$ in $Z_{37} \times Z_{37}$, (from reference (11))

In order to encode letters and numbers, we first need to assign different characters to different points on the curve. The table in Figure 16.2.12 gives the character assignment that we'll use. Notice the order of points in the table: we start with $(5, 25)$, then the second number $(1, 30) = (5, 25) + (5, 25)$, the third number $(21, 32) = (5, 25) + (5, 25) + (5, 25) = 3(5, 25)$, and so on. The information required to create this table is public knowledge, so anyone can duplicate it (for a practical code, the table would be much, much larger and impossible to compute even with the fastest computers). Note that in the case of a very large modulus, there is no difficulty in assigning a single character to multiple points on the curve, as long as each point has no more than one character assigned to it.

Example 16.2.16. Moses will send the message, "attack" using the code table above. The point C is chosen as $(9, 4)$.

First, Rachael must establish her private and public key (Moses doesn't have to, because he's only sending and not receiving). Rachael chooses $\alpha = 5$, so that $A = 5C = 5(9, 4)$. In this simple case, we may use the table in Figure 16.2.12 to facilitate the calculation of A (this would be impossible in a practical system—the number of entries in the table would be much larger than the number of atoms in the universe). Notice that the point $C = (9, 4)$ is the 11th point in the table (counting ∞ as the zeroth point,

| | | | | | | | | |
|----------|---------|---------|---------|---------|---------|---------|---------|---------|
| * | a | b | c | d | e | f | g | h |
| ∞ | (5,25) | (1,30) | (21,32) | (7,25) | (25,12) | (4,28) | (0,34) | (16,17) |
| I | j | k | l | m | n | o | p | q |
| (15,26) | (27,32) | (9,4) | (2,24) | (26,5) | (33,14) | (11,17) | (31,22) | (13,30) |
| r | s | t | u | v | w | x | y | z |
| (35,21) | (23,7) | (10,17) | (29,6) | (29,31) | (10,20) | (23,30) | (35,16) | (13,7) |

| | | | | | | | | | |
|---------|---------|---------|---------|--------|--------|--------|---------|---------|-------|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 |
| (31,15) | (11,20) | (33,23) | (26,32) | (2,13) | (9,33) | (27,5) | (15,11) | (16,20) | (0,3) |
| # | @ | ! | & | \$ | % | | | | |
| (4,9) | (25,25) | (7,12) | (21,5) | (1,7) | (5,12) | | | | |

Figure 16.2.12. Code table using the EC agreed upon by Moses and Rachael, (from reference (11))

(5,25) as the first point, (1,30) as the second point, etc). This means that $C = 11(5, 25)$, and thus $5C = 5 \cdot 11(5, 25) = 55(5, 25)$. However the point (5, 25) generates a cyclic group of order 43 (note there are 43 elements in the table in Figure 16.2.12), and $55 \bmod 43 = 12$, so $55(5, 25) = 12(5, 25)$. The 12th entry in the table is (2, 24), which is Rachael's public key A .

Now Moses must encrypt his message one character at a time. The first character of "attack" is "a", which according to the table corresponds to $M = (5, 25)$. Let's suppose that Moses chooses $\gamma = 7$ for this character. We thus obtain:

$$E_1 = \gamma C = 7(9, 4) = (15, 11) \text{ and } E_2 = M + \gamma A = (5, 25) + 7(2, 24) = (5, 12).$$

Thus Moses should send the pair of points (15, 11) and (5, 12) to Rachael.

Exercise 16.2.17.

- Verify the values of E_1 and E_2 computed above. Show your calculation.
- Verify that using these values of E_1 and E_2 and $\alpha = 5$, Rachael can correctly decode the character.

◇

Exercise 16.2.18. To encode t, t, a, c, k Moses chooses $\gamma = 12, 19, 2, 3, 23$ respectively.

- a Give the 5 pairs of numbers that Moses sends as cyphertext
- b Verify that Rachael decodes each pair of numbers correctly.

◇

◆

Exercise 16.2.19. There is a serious drawback with the above encryption scheme. Another person could easily impersonate Moses, and send a message to Rachael. Come up with a strategy whereby Moses and Rachael can ensure that the messages actually come from each other, and not from someone else
◇

16.2.6 Next steps

The examples we've given show the basic idea of ECC, but genuinely practical ECC systems are somewhat more complicated. Notice the progression from Section 16.2.2 to 16.2.4. We first introduced ECs as solution sets in \mathbb{R}^2 for a certain type of polynomial equation. But we then remarked that unfortunately these curves are not suitable for practical cryptography, because computers have trouble with real numbers. So in the next section we looked at ECs that are subsets of $\mathbb{Z}_p \times \mathbb{Z}_p$ where p is a prime, as in Figure 16.2.11. But there are disadvantages to \mathbb{Z}_p as well: finding enormous primes is not all that easy. It turns out there is yet another alternative for sets for ECs to live in: these sets are called ***Galois Fields***. Galois fields are derived from polynomials, where the polynomials have coefficients in \mathbb{Z}_p (in practice, usually $p = 2$). Since we haven't really looked into polynomials yet, we're not quite ready to dive into this aspect of ECC just yet. So, you have something to look forward to!

16.3 References and suggested reading

- (1) Azad, Saiful, and Pathan, Al-Sakib Khan. "Elliptic Curve Cryptography" in *Practical Cryptography*, CRC Press, January 2015.
- (2) Bidgoli, Hossein. "Diffie-Hellman Key Exchange" in *Handbook of Information Security: Information Warfare, Social, Legal, and International*

Issues and Security Foundations, Volume 2, John Wiley and Sons, January 2006.

- (3) Bos, Joppe, Kaihara, Marcelo, Kleinjung, Thorsten, Lenstra, Arjen, and Montgomery, Peter. (2009, September 01). *On the Security of 1024-bit RSA and 160-bit Elliptic Curve Cryptography*. Retrieved from <https://eprint.iacr.org/2009/389.pdf>.
- (4) Caldwell, Chris. (2016, January 07). *The Prime Pages*. Retrieved from <http://www.primes.utm.edu>.
- (5) "Certicom Announces Elliptic Curve Cryptosystem (ECC) Challenge Winner", 2002. Retrieved from <https://www.certicom.com/content/certicom/en/about/news/release/2002/certicom-announces-elliptic-curve-cryptosystem--ecc--challenge-w.html>
- (6) Christensen, Chris. (2015, November 14). *Key Exchanges*. Retrieved from <http://www.nku.edu/~christensen/092mat483>.
- (7) Corbellini, Andrea. (2015, May). *Elliptic Curve Cryptography: A Gentle Introduction*. Retrieved from <http://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/>.
- (8) "ECC: A Case for Mobile Encryption", 2014. Retrieved from <http://resources.infosecinstitute.com/ecc-case-mobile-encryption/#gref>
- (9) "Elliptic Curve", 2017. Retrieved from https://en.wikipedia.org/wiki/Elliptic_curve.
- (10) Franco, Pedro. "Elliptic Curve Cryptography" in *Understanding Bitcoin: Cryptography, Engineering and Economics*, John Wiley and Sons, February 2015.
- (11) Kumar, Suneetha, Chandrasekhar. (2012, January). *Encryption of Data Using Elliptic Curve Over Finite Fields*. Retrieved from <https://arxiv.org/ftp/arxiv/papers/1202/1202.1895.pdf>.
- (12) Mandal, Surajit, Manna, Nilotpal, and Saha, Arijit. "Diffie-Hellman Key Exchange" in *Information Theory, Coding, and Cryptography*, Pearson India, May 2013.
- (13) Pomerance, Carls. (n.d.). *Discrete Logarithms*. Retrieved from <https://math.dartmouth.edu/~carlp/dltalk09.pdf>.

- (14) Sullivan, Nick. (2013, October). *A (relatively easy to understand) primer on elliptic curve cryptography*. Retrieved from <https://arstechnica.com/security/2013/10/a-relatively-easy-to-understand-primer-on-elliptic-curve-cryptography>.
- (15) Weisstein, Eric W. (2017, March). *Elliptic Curve*. Retrieved from <http://mathworld.wolfram.com/EllipticCurve.html>

16.4 Hints for “Further Topics in Cryptography” exercises

Exercise 16.2.2 (a): If there is a double root r_1 , then it must be that $0 = x^3 + ax + b$ has a double root. This means that the equation can be factored: $x^3 + ax + b = (x - r_1)^2(x - r_2)$. Express a and b in terms of r_1 and r_2 . (A similar approach can be used in the case of a triple root.)

Exercise 16.2.2 (b): There are 2 cases: (i) $b = 0$, (ii) $b \neq 0$. In the case $b \neq 0$, first, show that $a > 0$. Then use part (a) to express r_1 and r_2 in terms of a and b , and show the equation factors properly.

Equivalence Relations and Equivalence Classes

In the previous chapter we introduced the abstract concept of *group*, which was defined in terms of properties that we'd seen in many previous examples. We may say that “group” is a generalization which includes many Generalizations like this play a key role in mathematics: if we can prove that a particular mathematical structure is a group, then all of the general group properties must also be true for that particular structure. In this way, we learn a great deal about the structure with very little effort.

In this chapter we introduce another generalization: the idea of a mathematical *relation*, which generalizes the concept of function as formally defined in Definition 8.2.11. We explore various types of relations and their properties, and use these new ideas to envision modular arithmetic from a different perspective. The new concepts that we introduce in this chapter are foundational to the notions of *coset* and *conjugacy class*, two key group-theoretic structures which play central roles in group theory (as we shall see in subsequent chapters).

This chapter is based on material by D. and J. Morris, which was extensively revised and expanded by Mark Leech.

17.1 Binary relations

Recall that according to Definition 8.2.11, any function $f: A \rightarrow B$ can be represented as a set of ordered pairs. More precisely, each element of f is

an ordered pair (a, b) , such that $a \in A$ and $b \in B$. Therefore, every element of f is an element of $A \times B$, so f is a subset of $A \times B$. There are however subsets of $A \times B$ that are not functions.

Example 17.1.1. Let P be the set of all professional basketball players in the NBA¹ and let T be the set of NBA teams. $f_T : P \rightarrow T$ as follows:

$$f_T(p) = \text{the team that } p \text{ plays for.}$$

Alternatively, f_T can be represented as the set of ordered pairs:

$$f_T = \{ (p, t) \in P \times T \mid p \text{ is a member of } t \}.$$

On the other hand, we may be interested not just in players' current teams, but in *all* teams that players have played for. This relationship could also be characterized by a set of ordered pairs:

$$\{ (p, t) \in P \times T \mid p \text{ has at one time or another played for } t \}.$$

This is *not* a function, because many NBA players have played on more than one team. 

In light of the previous example, it makes mathematical sense to define a relation between sets A and B to be a set of ordered pairs; that is, a relation between A and B is any subset of $A \times B$. Unlike the case of functions, there are no restrictions—every subset is a relation.

Definition 17.1.2. Suppose A and B are sets.

- (a) Any subset of $A \times B$ is called a **relation from A to B** .
- (b) For the special case where $A = B$, any subset of $A \times A$ is called a **binary relation** on A .



Example 17.1.3. Let P be the set of all professional basketball players in the NBA. Consider the following subset of $P \times P$:

$$\{ (p, p') \in P \times P \mid p' \text{ is the tallest teammate of } p \}.$$

¹National Basketball Association, “men’s professional basketball league in North America . . . widely considered to be the premier men’s professional basketball league in the world.” (Wikipedia)

This is a binary relation, according to Definition! 17.1.2, and it also can be identified with the function $f_h : P \rightarrow P$ defined by: $f_h(p) =$ the tallest teammate of p .

On the other hand, consider a different subset of $P \times P$:

$$\{(p, p') \in P \times P \mid p' \text{ is a teammate of } p\}.$$

This is a binary relation, but *not* a function because any player will have many teammates. \blacklozenge

Exercise 17.1.4. Express the following relations on NBA players as subsets of $P \times P$ (as in Example 17.1.3).

- (a) Players that both play the same positions
- (b) Players that have birthdays in the same month
- (c) The second player is taller than the first
- (d) The first player has a higher jersey number than the second

\diamond

So far we've been discussing relations in a non-numerical context, but our definitions apply to relations on sets of numbers as well. Relations on \mathbb{R} (or subsets of \mathbb{R}) are discussed in many middle or high school algebra courses. Any graph in the \mathbb{R}^2 plane gives a relation; and conversely, any relation involving subsets of \mathbb{R} can be represented as a graph in the plane. Relations in \mathbb{R}^2 are often taught along with functions: for example, students are given a graph of some discrete or continuous relation in the \mathbb{R}^2 plane and asked to determine if the given relation is a function.

Example 17.1.5. Consider the graphs in Figure 17.1.1, where the set $A \times B$ is indicated at the top of each graph. Which are relations in $A \times B$? Which are binary relations? Which are functions?

- All three graphs are relations because all graphs are subsets of $A \times B$ (as specified at the top of each graph).
- The first and third relations are binary relations, but the second relation isn't because $A \neq B$.

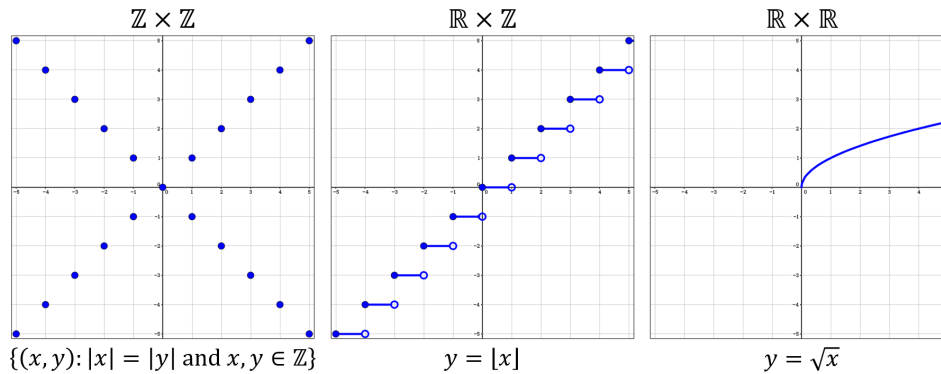


Figure 17.1.1. Graphs of relations. Constructed using GeoGebra

- The first is not a function, because e.g. both $(1, 1)$ and $(1, -1)$ are in the graph. The second is a function because it is uniquely defined on all of A (in this case $A = \mathbb{R}$). The third is not a function because e.g. there is no pair of the form $(-1, y)$, so the function is not defined on all of A .



Example 17.1.6. If $A = \{1, 2, 3\}$ and $B = \{4, 5, 6\}$, some examples of relations from A to B are:

$$\{(1, 4), (2, 5), (3, 6)\},$$

$$\{(1, 6), (3, 4)\},$$

$$\{(2, 5), (3, 5)\},$$

$$\emptyset,$$

$$\{(1, 4), (1, 5), (1, 6), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6)\}.$$

Notice that all of these sets are subsets of $A \times B$. The final example is the set $A \times B$ itself. Notice that \emptyset is a valid relation because it's a subset of $A \times B$ (a subset with no elements). On the other hand, the set $\{\emptyset\}$ is *not* a relation, because it is a set with one element (namely \emptyset), and this element is not an element of $A \times B$. For similar reasons, $\{(1, \emptyset)\}$ is *not* a relation. \blacklozenge

Example 17.1.7. Let $A = \{\text{all cities in the U.S.}\}$ and $B = \{\text{all states in the U.S.}\}$. some examples of relations from A to B are:

$\{(\text{Springfield, Illinois}), (\text{Springfield, Missouri}), (\text{Springfield, Texas}), (\text{Springfield, Wisconsin})\}$,
 $\{(\text{Corinth, Texas}), (\text{Liverpool, Texas}), (\text{Paris, Texas}), (\text{Sudan, Texas}), (\text{Troy, Texas})\}$,
 $\{(\text{Austin, Texas}), (\text{Boston, Massachusetts}), (\text{Phoenix, Arizona})\}$,
 $\{(x, y) \text{ such that } x \text{ is the capital of } y\}$.

The third of these relations is a *subset* of the last. ♦

Exercise 17.1.8.

- (a) Let $A = \{a\}$ and $B = \{1\}$. List *all* relations from A to B . (*Hint*)
- (b) Let $A = \{a\}$ and $B = \{1, 2\}$. List *all* relations from A to B . (*Hint*)
- (c) Let $A = \{a, b\}$ and $B = \{1\}$. List *all* relations from A to B . (*Hint*)
- (d) ** Let $A = \{a, b\}$. List *all* the binary relations on A . (*Hint*)
- (e) ** Let $A = \{a, b, c\}$. How many binary relations are there on the set A ? (*Hint*)

♦

We'll mostly be concerned with binary relations, not relations from some set A to some other set B .

Exercise 17.1.9. Let S be the set of all living people. Which of the follow relationships define binary relations on S ? brother, pet, favorite color, dentist, college major, and professor? ♦

Definition 17.1.10. We can draw a picture to represent any given binary relation on any given set A :

- Draw a dot for each element of A .
- For $a, b \in A$, draw an arrow from a to b if and only if (a, b) is an element of the relation.

The resulting picture is called a **digraph**. (The word is pronounced “DIE-graff” — it is short for “directed graph.” \triangle)

Example 17.1.11. Let $A = \{1, 2, 3, 4, 5\}$. We can define a binary relation R_1 on A by letting

$$R_1 = \{(x, y) \mid x \neq y \text{ and } x^2 + y \leq 10\}.$$

This binary relation is represented by the digraph in Figure 17.1.2:

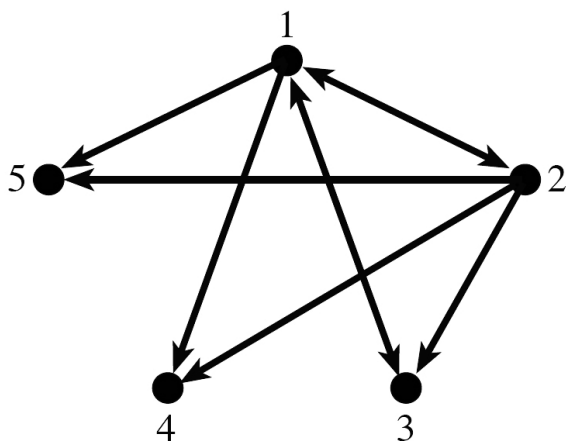


Figure 17.1.2. Digraph of the binary relation of R_1

Note that there’s a bidirectional arrow between 1 and 3 because $(1, 3) \in R_1$ and $(3, 1) \in R_1$. On the other hand there’s only a one directional arrow from 2 to 3 because $(2, 3) \in R_1$, but $(3, 2) \notin R_1$.

We can also define a binary relation R_2 on A by letting

$$R_2 = \{(x, y) \text{ such that } x \mid y\},$$

where $x \mid y$ means x divides y . This binary relation is represented by the digraph in Figure 17.1.3.

In this digraph there are loops at each number because $a \mid a$ for each a .



Exercise 17.1.12. Choose your favorite NBA team, and find a team roster (a good place to look is ESPN.com). Choose 6 players that have complete

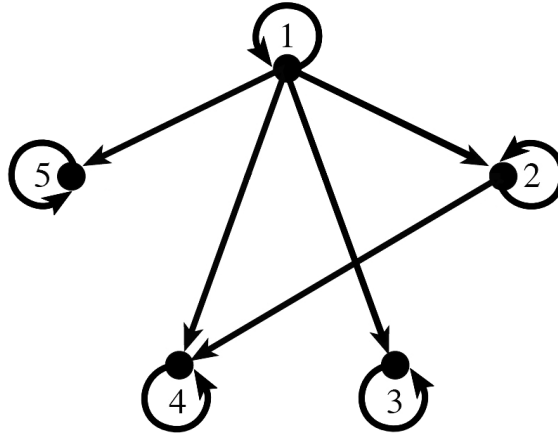


Figure 17.1.3. Digraph of the binary relation of R_2

data, and let that be your set A . draw a digraph for each of the following binary relations on A :

- (a) $\{(x, y) \in F \times F \mid x\text{'s height is within 2 inches of } y\text{'s height}\}$
- (b) $\{(x, y) \in A \times A \mid x\text{'s age is within the same decade as } y\text{'s}\}$
- (c) The relation “is taller than”.
- (d) The relation “is less than 10 pounds heavier than”.

◇

Exercise 17.1.13. Let $A = \{-2, -1, 0, 1, 2\}$ Draw a digraph for each of the following binary relations on A :

- (a) $R_a = \{(x, y) \mid x^2 = y^2\}$.
- (b) $R_b = \{(x, y) \mid x^2 - y^2 < 2\}$.
- (c) $R_c = \{(x, y) \mid (x - y)^2 < 2\}$.
- (d) $R_d = \{(x, y) \mid x \equiv y \pmod{3}\}$.

◇

Exercise 17.1.14. It is also possible to draw digraphs for relations that are not binary relations. In this case, your digraph should have a dot for each element of $A \cup B$.

- (a) Draw digraph representations of the relations given in Example 17.1.6.
- (b) The graphs you drew in (a) are all examples of *bipartite* graphs. Complete the following definition: A bipartite graph is a graph in which the vertices (dots) can be divided into two sets, such that . . .

◇

We commonly use symbols such as $=, <, \subset, \dots$ that are used to compare elements of a set. You may have called these “relations” in your high school algebra class – and in fact, they can all be considered as binary relations in the sense of Definition 17.1.2. For example, using the symbol $<$ we can define the following binary relation on \mathbb{R} :

$$R_{<} := \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$$

(here the symbol “:=” means “defined as”). Note that $R_{<}$ here is a subset of $\mathbb{R} \times \mathbb{R}$, so it is indeed a binary relation according to Definition 17.1.2.

Exercise 17.1.15.

- (a) Define the set $R_{>}$ associated with the symbol “ $>$ ” applied to the natural numbers.
- (b) Define the set $R_{=}$ associated with the symbol “ $=$ ” applied to the complex numbers. In your definition assume that equality of real numbers has been defined, and write complex numbers in rectangular form (for example, $a + bi$ or $c + di$).
- (c) List all the elements of the set R_{\subset} associated with the symbol “ \subset ” applied to the subsets of $A := \{1, 2\}$. (The set of subsets of A is denoted as $\mathcal{P}(A)$, the *power set* of A .) (*Hint*)
- (d) Consider the set R_{\subset} associated with the symbol “ \subset ” applied to the subsets of $A := \{1, 2, 3\}$. How many elements does R_{\subset} have?

◇

Exercise 17.1.15 shows that any comparison symbol applied to a set gives rise to a binary relation. So rather than writing $R_<$, $R_>$, $R_=>$ and so on, we simply use the comparison symbol itself to represent the binary relation. Notice that technically, ' $<$ ' defined on \mathbb{R} is a different relation from ' $<$ ' defined on \mathbb{N} : we will always make it very clear on which set the relation is being defined.

We will use the symbol \sim (which may be read as “is related to”, “tilde”, or “twiddle”) to denote a generic comparison symbol. If we are working with the set A , then the symbol \sim also represents the binary relation $A_\sim := \{(x, y) \in A \times A \mid x \sim y\}$.

We have shown that comparison symbols give rise to relations: the reverse is also true. Given a relation R defined on the set A , we can define a comparison symbol \sim applied to $a, b \in A$ as follows: $a \sim b$ iff $(a, b) \in R$.

17.2 Partitions and properties of binary relations



We've defined binary relations in general. In this section we present one very important situation where binary relations are very useful. It turns out that the binary relations which arise in this situation have some very special properties, which will become very important later.

Given any set A with 2 or more elements, it's possible to split up the elements of A into disjoint subsets. We call such a division a *partition*. The mathematical definition is:

Definition 17.2.1. A *partition* \mathcal{P} of a set A is a collection of nonempty subsets of A , such that each element of A is in exactly one of the subsets in \mathcal{P} . In other words:

- (a) the union of the subsets in \mathcal{P} is all of A , and
- (b) the subsets in \mathcal{P} are pairwise disjoint: that is the intersection of any two subsets is empty.

Conditions (a) and (b) imply that every element of A is in exactly one subset in \mathcal{P} . △

Remark 17.2.2. Note that \mathcal{P} is defined as a set of subsets of A . This means that the elements of \mathcal{P} are *subsets* which may contain multiple elements of A . The examples below will make this clearer. \triangle

Example 17.2.3.

- (a) Consider the set of real numbers \mathbb{R} . We know that every element of \mathbb{R} belongs to one of two sets: the set of rational numbers, \mathbb{Q} , or the set of irrational numbers, \mathbb{I} . The union of these two subsets, $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$, and \mathbb{Q} and \mathbb{I} are disjoint sets, so based on the definition $\{\mathbb{Q}, \mathbb{I}\}$ is a partition of \mathbb{R} . Alternatively the word “partition” can be used as a verb, so we could also say that \mathbb{Q} and \mathbb{I} partition \mathbb{R} .
- (b) Let \mathbb{E} and \mathbb{O} be the even and odd integers, respectively. Then $\{\mathbb{E}, \mathbb{O}\}$ is a partition of \mathbb{Z} . Alternatively we could also say that \mathbb{E} and \mathbb{O} partition \mathbb{Z} .
- (c) Let S be the set of all single-element subsets of \mathbb{Z} , so that for example $\{-552\}$, $\{7\}$, $\{1492\}$ are all elements of S . Then S is also a partition of \mathbb{Z} . Here S has an infinite number of elements (all the single-element subsets of \mathbb{Z}), but each element of S is a finite set.
- (d) Consider the set of complex numbers \mathbb{C} . Every element of \mathbb{C} has a real part which we denote as $\text{Re}[z]$ (as in Chapter 2). Let R_a be the set of all complex numbers with real part a , i.e. $R_a := \{z \in \mathbb{C} \mid \text{Re}[z] = a\}$. Let \mathcal{P} be the set consisting of all of the R_a 's, i.e. $\mathcal{P} := \{R_a \mid a \in \mathbb{R}\}$. Then \mathcal{P} is a partition of \mathbb{C} . Here \mathcal{P} has an infinite number of elements, where each element of \mathcal{P} is an infinite set.



From the previous example you can see how partitions of sets of numbers are collections of subsets that divide up bigger sets. You could imagine it's like a little kid with a bucket of LEGO[®] bricks who's sorting them out into different piles. The LEGOs could be sorted by color, shape, number of studs, or the original set in which they were bought. Similarly there are lots of different ways to sort out sets of numbers, mathematical objects, or any arbitrary sets with elements of any kind. Each different way of sorting gives rise to a different partition.

Example 17.2.4.

- (a) When making an inventory of the animals in a zoo, we may wish to count the number of antelopes, the number of baboons, the number of cheetahs, and so forth. In this case, all of the animals of the same species might be grouped together in a single set. Each species give rise to a different set and these sets form a partition of the animals in that zoo.
- (b) If we are concerned only with people's given names (what Americans would call "first name"), we can partition any set of people according to given name. Each set in the partition consists of all people who share a particular given name.
- (c) In geometry, sometimes we are interested only in the shape of a triangle and not its location or orientation. In this case, we talk about *congruent* triangles, where congruent means that corresponding sides of the two triangles are equal, and corresponding angles are also equal. For any triangle we may define the set of all triangles congruent to that triangle. There are an infinite number of such sets which form a partition of the set of all triangles.



What do partitions have to do with relations? We will illustrate with the following example.

Let $A = \{1, 2, 3, 4, 5, 6\}$ and partition these six numbers into evens and odds. Then we would have two subsets each with three elements. Suppose we use a six-sided die to determine a random outcome: where if we get an even number we win a dollar, but an odd number we lose a dollar. We don't care whether we get a 2, 4, or 6 – only that we get an even number because we win the same amount regardless. In this way, rolling a 2, 4, or 6 are *related*. Formally we can define a relation on A as follows: Given $a, b \in A$, then $a \sim b$ iff a and b are either both even or both odd.

We generalize the previous example in the following definition.

Definition 17.2.5. Given a partition \mathcal{P} on A , we may define a binary relation $\sim_{\mathcal{P}} \subset A \times A$ as follows: for $a, b \in A$, $a \sim_{\mathcal{P}} b$ iff a and b are both contained in the same subset in the partition. △

We already know that binary relations can be represented graphically. In the following exercise, we investigate graphical representations of some binary relations that come from partitions.

Exercise 17.2.6. In the following parts we will be considering partitions of \mathbb{R} and the associated binary relations defined by Definition 17.2.5.

- (a) Let $\mathcal{P} = \{R_1, R_2\}$ where $R_1 = \{x \mid x \in \mathbb{R}, x \geq 0\}$ and $R_2 = \{x \mid x \in \mathbb{R}, x < 0\}$.
- Draw the real number line from -5 to 5 , and indicate the sets $R_1, R_2 \in \mathcal{P}$ (you may indicate the two sets by circling them separately).
 - Graph the associated binary relation $\sim_{\mathcal{P}}$. You only need to graph from -5 to 5 . (Recall that the graph of a binary relation is a set in the Cartesian plane, as in Figure 17.1.1.)
- (b) Let $\mathcal{P} = \{\dots, R_{-2}, R_{-1}, R_0, R_1, R_2, \dots\}$ where $R_n = \{x \mid x \in \mathbb{R}, \lfloor x \rfloor = n\}$ for any integer n .²
- Draw the real number line from -5 to 5 , and indicate the visible sets in \mathcal{P} .
 - Graph the associated binary relation $\sim_{\mathcal{P}}$. You only need to graph from -5 to 5 .
- (c) Let $\mathcal{P} = \{\mathbb{E}, \mathbb{O}\}$ where $\mathbb{E} = \{x \mid x \in \mathbb{R}, \lfloor x \rfloor \text{ is even}\}$ and $\mathbb{O} = \{x \mid x \in \mathbb{R}, \lfloor x \rfloor \text{ is odd}\}$.
- Draw the real number line from -5 to 5 , and indicate the sets $\mathbb{E}, \mathbb{O} \in \mathcal{P}$ (a good way to do this is to color the intervals belonging to \mathbb{E} and \mathbb{O} with different colors).
 - Graph the associated binary relation $\sim_{\mathcal{P}}$. You only need to graph from -5 to 5 .

◇

To further explore Definition 17.2.5, we let $A = \{a, b, c, \dots, i\}$ which has been partitioned into subsets A_1, \dots, A_5 . Figure 17.2.1 has a drawing of A .

From Figure 17.2.1, we can tell some properties of $\sim_{\mathcal{P}}$:

²The ‘L’ brackets $\lfloor \dots \rfloor$, represent the **floor function**, also known as the greatest integer function. The floor function takes a real number, $x \in \mathbb{R}$ as input and outputs the greatest integer that is less than or equal to x . For example: $\lfloor 4 \rfloor = 4$, $\lfloor \pi \rfloor = 3$, and $\lfloor -2.3 \rfloor = -3$.

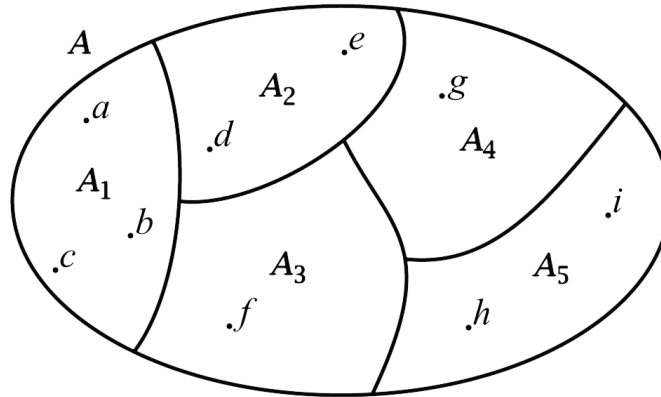


Figure 17.2.1. A partition of A into subsets A_1, \dots, A_5 . (Each element of A is in one and only one of the subsets.)

- Each element of A is related to itself, that is:

$$a \sim_{\mathcal{P}} a$$

(this is called the **reflexive** property). We know this is true because a is certainly in the same set of the partition as itself.

- If an element is related to another element the relation also goes in the other direction. That is:

$$a \sim_{\mathcal{P}} b \Rightarrow b \sim_{\mathcal{P}} a$$

(this is called the **symmetric** property). We know this is true because if a is related to b , then that means that a and b are in the same set of the partition. Since they are in the same set of the partition as each other b is also related to a . This argument can easily be repeated in the other direction.

- If an element is related to another element and that element is related to a third element, then the first element is related to the third. That is:

$$a \sim_{\mathcal{P}} b \text{ and } b \sim_{\mathcal{P}} c \Rightarrow a \sim_{\mathcal{P}} c$$

(this is called the **transitive** property). We know this is true because if a is related to b then they are in the same set of the partition, and

if b is related to c then they too are in the same set of the partition. This means that a , b , and c are all in the same set of the partition, therefore a is related to c .

We have seen that the partition depicted in Figure 17.2.1 produces a binary relation with three distinctive properties. What about other partitions? Let's consider some of the partitions that we've defined previously.

Example 17.2.7. In this example we will define a binary relation from the given partition, and show that the relation has the above three properties.

(a) Given the partition in Example 17.2.3(a), we can define a binary relation \sim_R on \mathbb{R} by

$$x \sim_R y \text{ iff } (x, y \in \mathbb{Q} \text{ or } x, y \in \mathbb{I}).$$

- First property (reflexive): $x \sim_R x$ (x is always in the same set, \mathbb{Q} or \mathbb{I} , as itself);
- Second property (symmetric): $x \sim_R y \Rightarrow y \sim_R x$ (x is in the same set as y implies y is in the same set as x);
- Third property (transitive): $x \sim_R y$ and $y \sim_R z \Rightarrow x \sim_R z$ (if x is in the same set as y and y is in the same set as z , then x is in the same set as z);

(b) Given the partition in Example 17.2.4(a), we can define a binary relation \sim_S on the set of animals in the zoo by

$$x \sim_S y \text{ iff } x \text{ and } y \text{ are animals in the same species.}$$

- Reflexive: $x \sim_S x$ (x is always the same species as itself);
- Symmetric: $x \sim_S y \Rightarrow y \sim_S x$ (x is the same species as y implies y is the same species as x);
- Transitive: $x \sim_S y$ and $y \sim_S z \Rightarrow x \sim_S z$ (if x is the same species as y and y is the same species as z , then x is the same species as z);



Exercise 17.2.8. Define a binary relation from the given partition, and show that the relation has the above three properties.

- (a) The partition in Example 17.2.3(b)
- (b) The partition in Example 17.2.3(c)
- (c) The partition in Example 17.2.3(d)
- (d) The partition in Example 17.2.4(b)
- (e) The partition in Example 17.2.4(c)

◇

The three properties seem to pop up whenever we define a binary relation from a partition. It's time to prove it.

Proposition 17.2.9. Given a partition \mathcal{P} on set A , define a binary relation of A as $a \sim b$ iff there exists a subset $C \in \mathcal{P}$ such that a and b are both elements of C , then the binary relation, \sim , satisfies the following 3 properties:

- (a) **reflexivity:**

$$\sim \text{ is reflexive } \iff \forall a \in A, a \sim a.$$

- (b) **symmetry:**

$$\sim \text{ is symmetric } \iff (\forall a, b \in A, (a \sim b) \Rightarrow (b \sim a)).$$

- (c) **transitivity:**

$$\sim \text{ is transitive } \iff \forall a, b, c \in A, ((a \sim b) \text{ and } (b \sim c)) \Rightarrow (a \sim c).$$

PROOF. Earlier in the chapter we showed that the binary relation $\sim_{\mathcal{P}}$ from the partition in Figure 17.2.1 was reflexive, symmetric, and transitive. The arguments that we used are generally applicable, and can be used for any partition. □

Remark 17.2.10.

- In Proposition 17.2.9 parts (a),(b), and (c) we used mathematical symbolism to express the concepts that were explained verbally in the discussion prior to Example 17.2.7. Increasingly, you'll be expected to understand symbolism without verbal explanation. Here's a chance for you to practice: what does the following symbolism mean, and where have you seen it before?

$$a \sim b \iff \exists C \in \mathcal{P}, (a \in C \text{ and } b \in C).$$

(Answer: this is the definition of the relation \sim defined in Proposition 17.2.9, expressed symbolically. We'll be using this symbolism in later propositions, e.g. Proposition 17.2.12.)

- Even though the definition of symmetry begins with " $\forall a, b \in A \dots$ " ("for every a and b in $A \dots$ ") symmetry doesn't require *every* pair of elements to be related to each other: symmetry only requires that whenever the *if* clause ($a \sim b$) is true, the *then* clause ($b \sim a$) must also be true. A similar caveat applies to transitivity.

△

These properties are so important that we have a special term for binary relations that satisfy all three properties:

Definition 17.2.11. An *equivalence relation* on a set A is a binary relation on A that is reflexive, symmetric, and transitive. △

The following is a restatement of Proposition 17.2.9, using our new terminology.

Proposition 17.2.12. Given a partition \mathcal{P} on set A , define a binary relation \sim on A as follows:

$$a \sim b \iff \exists C \in \mathcal{P}, (a \in C \text{ and } b \in C).$$

Then the binary relation, \sim , is an equivalence relation.

At one stroke, this proposition immediately proves that all the relations defined from partitions in Examples 17.2.3 and 17.2.4 are equivalence relations.

In the following sections we'll consider more examples of equivalence relations, but first let's make sure we understand reflexivity, symmetry and transitivity:

Example 17.2.13. Consider the following binary relations on \mathbb{R} :

- (a) $=$ is reflexive, symmetric, and transitive.
- Reflexive: any real number x equals itself, so $x = x \forall x \in \mathbb{R}$.
 - Symmetric: for any real numbers x and y , if $x = y$, then $y = x$.
 - Transitive: for any real numbers x , y , and z , if $x = y$ and $y = z$, then $x = z$.
 - Therefore $=$ on \mathbb{R} is an equivalence relation because $=$ is reflexive, symmetric, and transitive.
- (b) $<$ is transitive, but neither reflexive nor symmetric.
- Not Reflexive: For example, it is not true that $1 < 1$.
 - Not Symmetric: For example, $1 < 2$ but it is not true that $2 < 1$.
 - Transitive: given three real numbers x , y , and z , if $x < y$ and $y < z$, then $x < z$.
 - Therefore $<$ on \mathbb{R} is not an equivalence relation.
- (c) The binary relation $a \sim b$ iff $a = b + 1$ [for instance $(3.5, 2.5) \in \mathbb{R}_{\sim}$] is neither reflexive, symmetric, or transitive.
- Not Reflexive: $3 \neq 3 + 1$.
 - Not Symmetric: $4 \sim 3$, since $4 = 3 + 1$, but $3 \not\sim 4$, since $3 \neq 4 + 1$.
 - Not Transitive: $4 \sim 3$ and $3 \sim 2$, but $4 \not\sim 2$ ($4 \neq 2 + 1$).
 - Therefore \sim when $a \sim b$ iff $a = b + 1$ on \mathbb{R} is not an equivalence relation.



Notice that in the above examples, we used specific counterexamples to demonstrate when properties were not true. We recommend that you do the same—and remember, it only takes *one* counterexample to show a property is not true!

Exercise 17.2.14. For each of the following, explain your answers.

- (a) Is the binary relation \leq defined on the set \mathbb{R} reflexive? Is it symmetric? Is it transitive? Is it an equivalence relation? (**Hint**)
- (b) Is the binary relation \subset defined on the set $\mathcal{P}(\mathbb{N})$ reflexive? Is it symmetric? Is it transitive? Is it an equivalence relation? (Recall that $\mathcal{P}(\mathbb{N})$ is the set of subsets of \mathbb{N}).
- (c) Define the binary relation \sim on \mathbb{C} as follows: $z_1 \sim z_2$ iff $z_1 = |z_2|$. Is \sim reflexive? Is it symmetric? Is it transitive? Is it an equivalence relation? (**Hint**)
- (d) Define the binary relation \sim on \mathbb{Z} as follows: $a \sim b$ iff $|a - b| < 4$. Is \sim reflexive? Is it symmetric? Is it transitive? Is it an equivalence relation?

◇

Example 17.2.15. Given the set $B = \{1, 2, 3\}$, consider the relation \sim on B defined by

$$B_{\sim} = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}$$

The relation is shown in Figure 17.2.2.

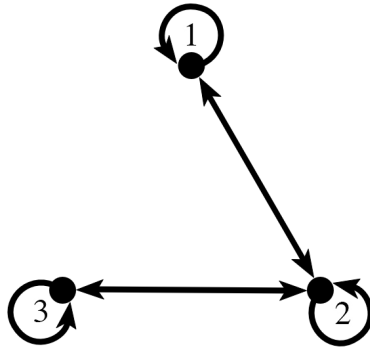


Figure 17.2.2. Diagram of the relation in Example 17.2.15

- \sim is reflexive, because $1 \sim 1$, $2 \sim 2$, and $3 \sim 3$ (Note we had to check *all* elements of the set B),

- \sim is symmetric, because, for each $(a, b) \in \sim$, the reversal (b, a) is also in \sim .
- \sim is *not* transitive, because $1 \sim 2$ and $2 \sim 3$, but $1 \not\sim 3$.



Transitivity can sometimes be a little tricky, as the following examples show.

Example 17.2.16. Let's think about binary relations on $\{1, 2, 3\}$ as seen in Figure 17.2.3. Which of the binary relations, A, B, or C, are transitive? Why or why not?

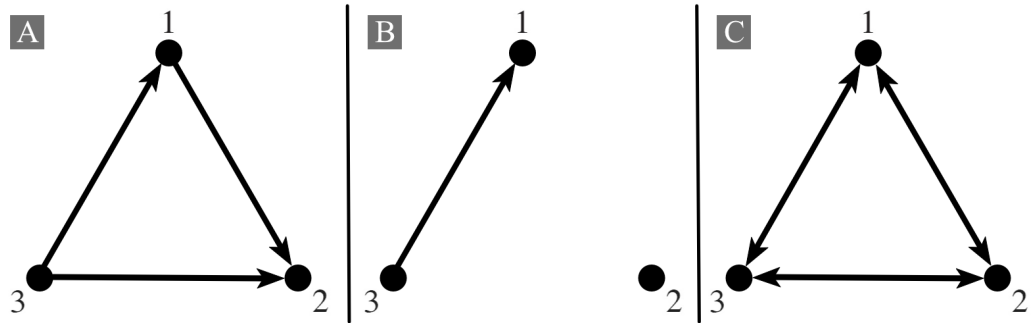


Figure 17.2.3. Digraphs to correspond with Example 17.2.16

Is the relation in A transitive? Let's consider. Remember how transitivity is defined: if $a \sim b$ and $b \sim c$ then $a \sim c$. In more prosaic terms, if there's an arrow from a to b and another arrow from b to c , then there's an arrow directly from a to c . We may conceptualize this as follows. Suppose a , b , and c represent airports, and arrows represent flights between airports. In terms of this example, transitivity means that whenever there's an indirect route between airports (with multiple stops), then there's also a direct route. So in the case of relation A, we may notice there's an indirect route from 3 to 2 by going through 1, but there's also a direct route from 3 to 2 (or more formally, $3 \sim 1$, $1 \sim 2$, and $3 \sim 2$). Furthermore this is the only example in A of an indirect route. Therefore this relation is transitive. If $3 \sim 2$ is removed from this binary relation, then the relation isn't transitive because it's still be possible to get from 3 to 2 via 1, but there's no longer a direct route.

How about the relation in digraph B? This may be the most confusing of the bunch. One might think that B is not transitive, since there's only a single arrow—but think again. The definition of transitive says: *if* $a \sim b$ and $b \sim c$ then $a \sim c$. You may also read the “if” as “whenever”: *Whenever* $a \sim b$ and $b \sim c$ then it's also true that $a \sim c$. But in relation B, the “whenever” *never holds*, because there are no cases of $a \rightarrow b$ and $b \rightarrow c$ (i.e. there are no indirect routes). This being the case, the “if” statement is considered true by default, so B is transitive. This is an important point worth remembering: in mathematical logic, a statement is considered true if no counterexample exists. In other words, if you can *prove* that there's no counterexample to a mathematical statement, then the statement is true! ³

Lastly, the relation in digraph C is *not* transitive. At first glance it seems like it should be transitive because so many transitivity conditions are satisfied (e.g. $1 \sim 2$ and $2 \sim 3 \Rightarrow 1 \sim 3$, etc), however we can also find transitivity conditions that fail (see part (a) of the following exercise)—and it only takes one counterexample to disprove a statement. \blacklozenge

Exercise 17.2.17.

- (a) Give a counterexample that proves that the binary relation C in Figure 17.2.3 is *not* transitive. (*Hint*)
- (b) Explain why the binary relation

$$R_{\sim} = \{(1, 4), (1, 1), (4, 1)\}$$

is *not* transitive. (*Hint*)

- (c) Explain why the binary relation

$$R_{\sim} = \{(1, 2), (1, 3), (1, 4)\}$$

is transitive. (*Hint*)

\diamond

³Here are some “true statements”, according to this rule: (i) If you see a rainbow in the sky and follow it to where it touches the ground, you will find a leprechaun with a pot of gold; (ii) If you pick up an ordinary guinea pig by its tail, then its eyes will fall out. (iii) If you give a correct proof that $1=0$, then Bill Gates will give you his entire fortune.

Exercise 17.2.18. Find binary relations on $\{1, 2, 3\}$ that meet each of the following conditions. Express each relation as a set of ordered pairs, and draw the corresponding digraph. (Note: each part can have more than one answer, but you only need to find one.)

- (a) symmetric, but neither reflexive nor transitive.
- (b) reflexive, but neither symmetric nor transitive.
- (c) transitive and symmetric, but not reflexive.
- (d) neither reflexive, nor symmetric, nor transitive.

◇

Digraphs are useful because they represent the relation in such a way that it is easy to deduce the relation's properties:

Exercise 17.2.19.

- (a) How can you tell from looking at a digraph whether or not the corresponding relation is reflexive?
- (b) How can you tell from looking at a digraph whether or not the corresponding relation is symmetric?
- (c) **How can you tell from looking at a digraph whether or not the corresponding relation is transitive?

◇

17.3 Examples of equivalence relations


Let's take a look at some examples of equivalence relations (recall Definition 17.2.11). We will see shortly that they all have something in common.

Example 17.3.1. Define a binary relation \sim on \mathbb{R} by $x \sim y$ iff $x^2 = y^2$. Then \sim is an equivalence relation.

PROOF. We wish to show that \sim is reflexive, symmetric, and transitive.

(reflexive) Given $x \in \mathbb{R}$, we have $x^2 = x^2$, so $x \sim x$.

(symmetric) Given $x, y \in \mathbb{R}$, such that $x \sim y$, we have $x^2 = y^2$. Since equality is symmetric, this implies $y^2 = x^2$, so $y \sim x$.

(transitive) Given $x, y, z \in \mathbb{R}$, such that $x \sim y$ and $y \sim z$, we have $x^2 = y^2$ and $y^2 = z^2$. Therefore $x^2 = z^2$, since equality is transitive. Hence $x \sim z$.
□ 

Example 17.3.2. Define a binary relation \sim on $\mathbb{N} \times \mathbb{N}$ by $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1 + b_2 = a_2 + b_1$. Then \sim is an equivalence relation.


PROOF. We wish to show that \sim is reflexive, symmetric, and transitive.

(reflexive) Given $(a, b) \in \mathbb{N} \times \mathbb{N}$, we have $a + b = a + b$, so $(a, b) \sim (a, b)$.

(symmetric) Given $(a_1, b_1), (a_2, b_2) \in \mathbb{N} \times \mathbb{N}$, such that $(a_1, b_1) \sim (a_2, b_2)$, we have $a_1 + b_2 = a_2 + b_1$. Since equality is symmetric, this implies $a_2 + b_1 = a_1 + b_2$, so $(a_2, b_2) \sim (a_1, b_1)$.

(transitive) Given $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{N} \times \mathbb{N}$, such that $(a_1, b_1) \sim (a_2, b_2)$ and $(a_2, b_2) \sim (a_3, b_3)$, we have

$$\begin{aligned} (a_1 + b_3) + (a_2 + b_2) &= (a_1 + b_2) + (a_2 + b_3) && \text{(rearrange terms)} \\ &= (a_2 + b_1) + (a_2 + b_3) && ((a_1, b_1) \sim (a_2, b_2) \text{ and substitution}) \\ &= (a_2 + b_1) + (a_3 + b_2) && ((a_2, b_2) \sim (a_3, b_3) \text{ and substitution}) \\ &= (a_3 + b_1) + (a_2 + b_2) && \text{(rearrange terms)}. \end{aligned}$$

Subtracting $a_2 + b_2$ from both sides of the equation, we conclude that $a_1 + b_3 = a_3 + b_1$, so $(a_1, b_1) \sim (a_3, b_3)$.
□ 

Exercise 17.3.3. Show that each of these binary relations is an equivalence relation.

- (a) The binary relation \sim on \mathbb{R} defined by $x \sim y$ iff $x^2 - 3x = y^2 - 3y$.
- (b) The binary relation \sim on \mathbb{R} defined by $x \sim y$ iff $x - y \in \mathbb{Z}$. (**Hint**)
- (c) The binary relation \sim on $\mathbb{N} \times \mathbb{N}$ defined by $(a_1, b_1) \sim (a_2, b_2)$ iff $a_1 b_2 = a_2 b_1$. (**Hint**)
- (d) The binary relation \sim on \mathbb{C} defined by $z_1 \sim z_2$ iff $|z_1| = |z_2|$.

- (e) The binary relation \sim on \mathbb{C} defined by $z_1 \sim z_2$ iff $\operatorname{Re}[z_1] = \operatorname{Re}[z_2]$.
(Recall that $\operatorname{Re}[z]$ is the real part of z)
- (f) The binary relation \sim on the collection of all finite sets defined by
 $A \sim B$ iff $|A| = |B|$ (that is, A and B have the same number of elements)

◇

Equivalence relations are often defined in terms of *functions*. For instance, Example 17.3.1 involves the function $f : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2$, and $x \sim y$ if and only if $f(x) = f(y)$. Similarly, Exercise 17.3.3 involves the function $g : \mathbb{R} \rightarrow \mathbb{R}$ defined by $f(x) = x^2 - 3x$, and $x \sim y$ if and only if $g(x) = g(y)$. Both of these cases follow the following pattern:

Given a function $f : A \rightarrow B$, define a binary relation on A by: $a_1 \sim a_2$ iff $f(a_1) = f(a_2)$.

Other examples that we've seen also follow this same pattern:

Exercise 17.3.4. Following the pattern that we've shown for Example 17.3.1 and Exercise 17.3.3, define the following equivalence relations in terms of functions.

- (a) Exercise 17.3.3 part (d)
 (b) Exercise 17.3.3 part (e)
 (c) The binary relation in Example 17.3.2.

◇

The previous examples have all involved sets of numbers, but we may see that the same thing happens even when we consider functions on other types of sets.

Example 17.3.5.

- (a) Every animal has only one species, so *Species* is a function that is defined on the set of all animals. The equivalence relation \sim_S of Example 17.2.7 can be characterized by

$$x \sim_S y \iff \text{Species}(x) = \text{Species}(y).$$

- (b) If we assume that every person has a given name, then `GivenName` is a function on the set of all people. Let \sim_N be the equivalence relation of Exercise 17.2.8 can be characterized by

$$x \sim_N y \iff \text{GivenName}(x) = \text{GivenName}(y).$$



We've given enough examples to (hopefully) convince you that functions always produce equivalence relations. But examples are never enough! The bottom line is that we need a proof—and here it is.

Proposition 17.3.6. Suppose $f: A \rightarrow B$. If we define a binary relation \sim on A by

$$a_1 \sim a_2 \iff f(a_1) = f(a_2),$$

then \sim is an equivalence relation on A .

Exercise 17.3.7. Prove Proposition 17.3.6: that is, prove that the relation defined in the proposition is (a) reflexive, (b) symmetric, and (c) transitive. (If you like, you may model your proof on the discussion prior to Exercise Example 17.2.7, where we proved the three properties for binary relations arising from partitions.)



Let's take a step back and take stock of where we are. We've shown (Proposition 17.2.9) that any partition has an associated equivalence relation. We've also shown (Proposition 17.3.6) that any function has an associated equivalence relation. Is there any relationship between these two facts? Indeed, we'll see in subsequent discussions that partitions, functions, and equivalence relations are closely interrelated. In the following exercise, we'll show that any equivalence relation that comes from a partition also comes from a function.

Exercise 17.3.8. Given a set A and a partition $\mathcal{P} = \{A_1, A_2, A_3, \dots\}$ of A . Let $\sim_{\mathcal{P}}$ be the equivalence relation associated with the partition \mathcal{P} . Now define a function $f: A \rightarrow \mathbb{N}$ as follows:

$$f(a) = \begin{cases} 1 & \text{if } a \in A_1 \\ 2 & \text{if } a \in A_2 \\ \vdots & \vdots \\ n & \text{if } a \in A_n \end{cases}$$

In general: $f(a) = j$ iff $a \in A_j$.

- (a) Show that $a \sim_{\mathcal{P}} b \iff f(a) = f(b)$.
- (b) Let \sim_f be the equivalence relation defined from f as in Proposition 17.3.6. Show that $\sim_{\mathcal{P}} = \sim_f$ by showing that $a \sim_{\mathcal{P}} b \iff a \sim_f b$.

◇

Exercise 17.3.8 amounts to a proof of the following proposition.

Proposition 17.3.9. Given a set A with partition $\mathcal{P} = \{A_1, A_2, A_3, \dots\}$. Let $\sim_{\mathcal{P}}$ be the associated equivalence relation. Then there exists a function $f : A \rightarrow \mathbb{N}$ with associated equivalence relation \sim_f such that $\sim_{\mathcal{P}} = \sim_f$.

In other words, whenever we have a partition, we can also define a function that gives us the same equivalence relation as the partition. ⁴

Exercise 17.3.10. From the relation \sim_R in Examples 17.2.3(a) and 17.2.7(a) (the \mathbb{Q} and \mathbb{I} example) define a function such that $a_1 \sim a_2 \iff f(a_1) = f(a_2)$ where $a_1, a_2 \in \mathbb{R}$. (Note that we've already proved that \sim_R is an equivalence relation by a different proposition, so this example is a particular case of Proposition 17.3.9.) ◇

Exercise 17.3.8 starts with a partition, and constructs a function that gives the same equivalence relation as the partition. We may go backwards as well: starting with a function, we may produce a partition with the same equivalence relation. The following exercise gives an example of this.

Exercise 17.3.11. Let $f : \{-3, -2, -1, 0, 1, 2, 3\} \rightarrow \mathbb{Z}$ be defined by $f(x) = x^2$.

⁴This statement is true, but the proof in Exercise 17.3.8 isn't quite complete. The reason is that we've assumed that the partition \mathcal{P} is *countable*, i.e. we can assign a unique natural number index to each set in \mathcal{P} . There are many sets in mathematics that are *not* countable (such as the real numbers). To make a truly general proof, we should specify an index set that may depend on the partition.

- (a) What is the range of f ?
- (b) For every number n in the range of f , find the set of all numbers in the domain of f that map to n . Denote this set as A_n (for example, if we let $n = 0$, then only 0 maps to 0, so $A_0 = 0$). List the elements of A_n for each n in the range of f .
- (c) Show that the sets $\{A_n\}$ that you listed in part (b) form a partition of the domain of f .
- (d) According to Proposition 17.4.11, this partition produces an equivalence relation on the domain of f . Draw a digraph that represents the equivalence relation.
- (e) We also know that the function f produces an equivalence relation on the domain of f , as in Proposition 17.3.6. Draw a digraph that represents this equivalence relation.
- (f) What may you conclude from your results in (d) and (e)?

◇

The following proposition generalizes the results of the previous exercise.

Proposition 17.3.12. Suppose $f : A \rightarrow B$. For each $b \in \text{Range}(f)$ define a subset $A_b \subset A$ as follows:

$$A_b := \{a \in A \mid f(a) = b\}.$$

Then the collection of sets $\mathcal{P} := \{A_b \mid b \in B\}$ form a partition of A . Furthermore, the equivalence relation \sim_f derived from f is identical to the equivalence relation $\sim_{\mathcal{P}}$ derived from \mathcal{P} : that is, $a_1 \sim_f a_2 \iff a_1 \sim_{\mathcal{P}} a_2$.

PROOF. The proof is broken up into steps in the following exercise.

Exercise 17.3.13.

- (a) Given any $b \in \text{Range}(f)$, show that A_b is nonempty
- (b) Given $b_1, b_2 \in \text{Range}(f)$ with $b_1 \neq b_2$, show that A_{b_1} and A_{b_2} are disjoint, i.e. $A_{b_1} \cap A_{b_2} = \emptyset$.
- (c) Given any $a \in A$, show there exists a $b \in \text{Range}(f)$ such that $a \in A_b$.

- (d) Show that $\{A_b \mid b \in B\}$ includes all of A ; that is, $A = \cup_{b \in B} A_b$.
- (e) Verify that the (a)-(d) imply that $\{A_b \mid b \in B\}$ is a partition of A .

◇

□

17.4 Obtaining partitions from equivalence relations

Proposition 17.2.12 tells us that given any partition \mathcal{P} of a set S , we can define an equivalence relation which says that two elements of S are equivalent iff they belong to the same set in the partition. We'll see in this section that we can go the other way as well: namely, given any equivalence relation on S we can construct a partition on S which divided all the elements of S among disjoint subsets.

To make this work, we first must define a key notion: *equivalence classes*. Here we go!

17.4.1 From equivalence relations to equivalence classes

Let's ramp up to our key definition by means of an example.

Example 17.4.1. Suppose we're studying a set of people, and we're only interested in their given names. Of course there may be several Johns, several Marys, a couple of Sylvesters, and so on— but as far as given names are concerned, any two Johns can be considered as equivalent: indeed, we formalized this sense of equivalence in Example 17.3.5(b). We can group all Johns into a single set or class, which we'll refer to as an *equivalence class*. We can do the same thing with Marys, Sylvesters, Xyleenas, Zenobias, and so on. It follows that every person in the set belongs to her or his own equivalence class (even if the equivalence class consists of a single person!)

◆

Let's generalize this example. Essentially, the only fact about given names that we used to define equivalence classes was that given name defines an equivalence relation on the set of interest. So it stands to reason that we can do something similar with any equivalence relation:

Definition 17.4.2. Suppose \sim is an equivalence relation on a set A . For each $a \in A$, the **equivalence class** of a is the following subset of A :

$$[a] = \{s \in A \mid s \sim a\}.$$

That is, the equivalence class of the element $a \in A$ is the set of all elements of A that are equivalent to a . \triangle

Example 17.4.3. For the equivalence relation N described in Example 17.3.5(b), we have

$$[\text{Woodrow Wilson}] = \{x \in \text{People} \mid \text{GivenName}(x) = \text{GivenName}(\text{Woodrow Wilson})\}.$$

In other words, $[\text{Woodrow Wilson}]$ is the set of all people whose given name is Woodrow. \blacklozenge

Warning 17.4.4. The notation $[a]$ does not tell us which equivalence relation is being used. You should be able to figure out which relation it is from the context. \diamond

Let's give a a more “mathy” example.

Example 17.4.5. Suppose $A = \{1, 2, 3, 4, 5\}$ and

$$R = \{(1, 1), (1, 3), (1, 4), (2, 2), (2, 5), (3, 1), (3, 3), (3, 4), (4, 1), (4, 3), (4, 4), (5, 2), (5, 5)\}$$

One can verify that R is an equivalence relation on A . The equivalence classes are:

$$[1] = [3] = [4] = \{1, 3, 4\}, \quad [2] = [5] = \{2, 5\}.$$

\blacklozenge

Exercise 17.4.6.

(a) Let $B = \{1, 2, 3, 4, 5\}$ and

$$S = \{(1, 1), (1, 4), (2, 2), (2, 3), (3, 2), (3, 3), (4, 1), (4, 4), (5, 5)\}.$$

Assume (without proof) that S is an equivalence relation on B . Find the equivalence class of each element of B .

- (b) Let $C = \{1, 2, 3, 4, 5\}$ and define \sim_C by

$$x \sim_C y \iff x + y \text{ is even.}$$

Assume (without proof) that \sim_C is an equivalence relation on C . Find the equivalence class of each element of C .

- (c) Draw the arrow diagrams for the relations in R in Example 17.4.5, and for the relations in parts (a) and (b) of this exercise.

◇

The following proposition presents some very important properties of equivalence classes:

Proposition 17.4.7. Suppose \sim is an equivalence relation on a set S . Then:

- (a) For all $a \in S$, we have $a \in [a]$.
 (b) For all $a \in S$, we have $[a] \neq \emptyset$.
 (c) The union of the equivalence classes is all of S . This can be written mathematically as follows:

$$\bigcup_{a \in S} [a] = S$$

- (d) For any $a_1, a_2 \in S$, such that $a_1 \sim a_2$, we have $[a_1] = [a_2]$.
 (e) For any $a_1, a_2 \in S$, such that $a_1 \not\sim a_2$, we have $[a_1] \cap [a_2] = \emptyset$.

Exercise 17.4.8. Prove the assertions in Proposition 17.4.7. You may use the following hints:

- (a) Use the reflexive property of \sim , together with Definition 17.4.2
 (b) Use part (a).
 (c) This can be done by showing:

(i) $\bigcup_{a \in S} [a] \subset S$

(ii) $S \subset \bigcup_{a \in S} [a]$

In (i), use the fact that $[a] \subset S$. In (ii), use (a) above to show that every element of S is in at least one equivalence class. (Recall also that ‘ \subset ’ means “contained in”, and includes the case where the two sets are equal.)

- (d) Remember that two sets are equal if they have all their elements in common. So you want to show that given $a_1 \sim a_2$, then every element of $[a_1]$ is also an element of $[a_2]$, and vice versa. Do this as follows:
- Choose any $a_3 \in [a_1]$. Use Definition 17.4.2 together with the transitive property to show that $a_3 \in [a_2]$. Conclude that every element of $[a_1]$ is also an element of $[a_2]$.
 - Use a similar proof to show that every element of $[a_2]$ is also an element of $[a_1]$.
- (e) You can prove this one by contradiction. Suppose the intersection is non-empty. Choose an element in the intersection. Use Definition 17.4.2 and the transitive property to derive a contradiction.

◇

Proposition 17.4.7 parts (d) and (e) can be restated as follows:

Proposition 17.4.9. Suppose \sim is an equivalence relation on a set S . Then any two equivalence classes are either equal or disjoint; that is, either they have exactly the same elements, or they have no elements in common.

17.4.2 From equivalence classes to partitions

It’s time to come full circle, and show that partitions arise from equivalence classes. As in the previous section, we’ll ramp up with an example.

Example 17.4.10. In Example 17.4.5, the equivalence classes are $\{1, 3, 4\}$ and $\{2, 5\}$. Since 1, 2, 3, 4, 5 each belong to exactly one of these sets, we see that the set

$$\{\{1, 3, 4\}, \{2, 5\}\}$$

of equivalence classes is a partition of $\{1, 2, 3, 4, 5\}$.

◆

Intuitively, equivalence classes resulting from an equivalence relation on S will always break S up into disjoint sets which, taken together, include all the elements of S . We've seen this description before—this is exactly what a partition does. This observation places us at the doorstep of the following proposition:

Proposition 17.4.11. Suppose \sim is an equivalence relation on a set A . Then

$$\{[a] \mid a \in A\}$$

is a partition of A .

PROOF. From parts (b), (c), and (e) of Proposition 17.4.7, we know that the equivalence classes are nonempty, that their union is A , and that they are pairwise disjoint. \square

The following exercises illustrate Proposition 17.4.11.

Exercise 17.4.12. Consider the set \mathbb{C}^* defined by $\mathbb{C}^* := \mathbb{C} \setminus 0$, i.e. the set of nonzero complex numbers. Define a binary relation \sim_r on this set as follows. Let $r_1 \operatorname{cis}(\theta_1)$ and $r_2 \operatorname{cis}(\theta_2)$ be two elements of \mathbb{C}^* expressed in polar form, where $0 \leq \theta < 2\pi$. Then

$$r_1 \operatorname{cis}(\theta_1) \sim_r r_2 \operatorname{cis}(\theta_2) \iff r_1 = r_2.$$

- (a) Prove that \sim_r thus defined is an equivalence relation.
- (b) Sketch $[1]$, $[1 + i]$, and $[\pi \operatorname{cis}(\pi/3)]$ in the complex plane (show all three on a single sketch). Give geometrical descriptions (using words) of each of these sets (i.e. what can you say about the shape, size, and location of these three sets?)
- (c) Give a geometrical description of the equivalence classes of \sim_r in the following form: “The equivalence classes of \sim_r are all _____ centered at _____”.
- (d) Based on your description in part (c), show that the equivalence classes of \sim_r form a partition of \mathbb{C}^* .
- (e) We've seen that functions produce equivalence relations. Give a function with domain \mathbb{C}^* that produces the equivalence relation \sim_r .

◇

Exercise 17.4.13. Consider the set \mathbb{C}^* as defined in Exercise 17.4.12. Define a binary relation \sim_θ on this set as follows. Let $r_1 \operatorname{cis}(\theta_1)$ and $r_2(\operatorname{cis} \theta_2)$ be two elements of \mathbb{C}^* expressed in polar form, where $0 \leq \theta < 2\pi$. Then

$$r_1 \operatorname{cis}(\theta_1) \sim_\theta r_2(\operatorname{cis} \theta_2) \iff \theta_1 = \theta_2.$$

- Prove that \sim_θ thus defined is an equivalence relation.
- Sketch $[1]$, $[1 + i]$, and $[\pi \operatorname{cis}(\pi/3)]$ in the complex plane (show all three on a single sketch). Give geometrical descriptions (using words) of each of these sets (i.e. what can you say about the shape, size, and location of these three sets?)
- Give a geometrical description of the equivalence classes of \sim_θ in the following form: “The equivalence classes of \sim_θ are all _____ which begin at _____”.
- Based on your description in part (c), show that the equivalence classes of \sim form a partition of \mathbb{C}^* .
- Give a function with domain \mathbb{C}^* that produces the equivalence relation \sim_θ .

◇

We close this section with an exercise that reinforces the idea that partitions and equivalence classes are really two different ways of looking at the same thing.

Exercise 17.4.14. We know from Proposition 17.2.12 that any partition produces an equivalence relation. We also know from Proposition 17.4.11 that any equivalence relation produces a partition.

- Suppose we begin with a partition \mathcal{P} on the set A , and define an equivalence relation $\sim_{\mathcal{P}}$ as in Proposition 17.2.12. Next, suppose that following Proposition 17.4.11 we define a partition \mathcal{P}' consisting of the equivalence classes of $\sim_{\mathcal{P}}$. Show that $\mathcal{P} = \mathcal{P}'$. (One way to do this is to show that every set in \mathcal{P} is also a set in \mathcal{P}' , and vice versa.)

- (b) Suppose we begin with an equivalence relation \sim on the set A , and define a partition of A as in Proposition 17.4.11. Let's call this partition \mathcal{Q} . Next, suppose that following Proposition 17.2.12 we define an equivalence relation $\sim_{\mathcal{Q}}$. Show that the relations \sim and $\sim_{\mathcal{Q}}$ are identical: that is, $a \sim b \iff a \sim_{\mathcal{Q}} b$.

◇

17.5 Modular arithmetic redux

Abstract algebra often involves looking at familiar concepts and structures in a more general more abstract and “elegant” way. As an example of this, we will now revisit modular arithmetic and describe it from an entirely different point of view, with the benefit of the concepts we have been developing in previous sections.

In the Modular Arithmetic chapter we defined the concept of “modular equivalence”. You may recall that we actually gave two definitions, which we repeat here:

Definition 17.5.1. (*Modular Equivalence, first definition*)

$a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n . △

Definition 17.5.2. (*Modular Equivalence, second definition*)

$a \equiv b \pmod{n}$ iff $a - b = k \cdot n$, where k is an integer (that is, $k \in \mathbb{Z}$). △

Exercise 17.5.3. Using Definition 17.5.2, show that equivalence mod n is an equivalence relation. (That is, show that equivalence mod n is (a) reflexive, (b) symmetric, and (c) transitive) ◇

Exercise 17.5.3 enables us to apply the concepts we've been developing to modular arithmetic. In particular, it enables us to describe modular arithmetic in terms of equivalence classes. We will do this first with a simple example: the integers mod 3.

17.5.1 The integers modulo 3

We have proven in Exercise 17.5.3 that equivalence mod 3 is a bona fide equivalence relation. So what are the equivalence classes? And how many are there?

We can use Definition 17.5.1 to answer this question. The possible remainders when an integer is divided by 3 are either 0, 1, or 2. This tells us that every integer is equivalent (modulo 3) to either 0, 1, or 2. Using Proposition 17.4.7(d), it follows that:

for every $k \in \mathbb{Z}$, the equivalence class $[k]_3$ must be either $[0]_3$, $[1]_3$, or $[2]_3$.

(To emphasize the fact that $n = 3$, we have included a subscript 3 in the notation for the equivalence classes).

Specifically:

$$[0]_3 = \{\dots, -6, -3, 0, 3, 6, \dots\},$$

$$[1]_3 = \{\dots, -5, -2, 1, 4, 7, \dots\},$$

$$[2]_3 = \{\dots, -4, -1, 2, 5, 8, \dots\}$$

are three equivalence classes that partition the set of all integers. In the Modular Arithmetic chapter we defined the integers mod 3 as the set of remainders under division mod 3. Here we will give another definition that looks very different, but turns out to amount to basically the same thing.

Remark 17.5.4. What do we really mean by, “basically the same thing”? Hold that thought—we’ll come back to this point later (in Section 17.5.3). \triangle

Definition 17.5.5. (*Integers mod 3, equivalence class definition*) The set of equivalence classes $\{[0]_3, [1]_3, [2]_3\}$ is identified as the set of **integers mod 3**, and is represented by the symbol \mathbb{Z}_3 .

We may also use the simpler notation \bar{k} to represent the equivalence class $[k]_3$. So we may write either $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$ or $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. \triangle

Take a moment to appreciate the difference between this definition of \mathbb{Z}_3 and the one we gave in Section 5.4. Previously we took \mathbb{Z}_3 as the set

of integers $\{0, 1, 2\}$ and defined new addition and multiplication operations that had the property of closure. But now we're taking a different tack. We are saying that the elements of \mathbb{Z}_3 are *equivalence classes* rather than numbers. In other words, the elements of \mathbb{Z}_3 are *sets*.

To complete the connection with our previous definition of \mathbb{Z}_3 , we need to define arithmetic operations on \mathbb{Z}_3 , using our new characterization in terms of equivalence classes. Note the additional level of abstraction here: these arithmetic operations are defined on equivalence classes, which are *sets* rather than numbers. But we've seen this before: recall that in the Sets chapter we defined operations on sets. So you're old hands at this!

Definition 17.5.6. (Rules of modular arithmetic) The *arithmetic operations modulo 3* are defined as follows:

- $[a]_3 + [b]_3 = [a + b]_3$ (or $\bar{a} + \bar{b} = \overline{a + b}$),
- $[a]_3 - [b]_3 = [a - b]_3$ (or $\bar{a} - \bar{b} = \overline{a - b}$),
- $[a]_3 \cdot [b]_3 = [ab]_3$ (or $\bar{a} \cdot \bar{b} = \overline{ab}$).

△

In Definition 17.5.6 we're actually giving *new meanings* to the symbols $+$, $-$, and \cdot . We could make this explicit by using different symbols. But this is not really necessary: whenever we're doing arithmetic with equivalence classes mod 3 (or mod n , for that matter), you should always presume that we're using the modular definitions of $+$, $-$, and \cdot .

Example 17.5.7. We have $[1]_3 + [2]_3 = [1 + 2]_3 = [3]_3$. However, since 3 and 0 are in the same equivalence class, we have $[3]_3 = [0]_3$, so the above equation can also be written as $[1]_3 + [2]_3 = [0]_3$. Equivalently, $\bar{1} + \bar{2} = \bar{0}$. ◇

Example 17.5.7 illustrates the following general rule:

If r is the remainder when $a + b$ is divided by 3, then $\bar{a} + \bar{b} = \bar{r}$.

You may recognize that this is essentially the same rule that we used in our previous discussion of modular arithmetic.

Exercise 17.5.8. Write down similar rules for (a) subtraction mod 3; (b) multiplication mod 3. ◇

Example 17.5.9. Here is a table that shows the results of addition modulo 3. (Recall that in the Modular Arithmetic chapter we referred to such tables as *Cayley tables*.)

| | | | |
|-----------|-----------|-----------|-----------|
| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{0}$ | $\bar{1}$ |

◇

Exercise 17.5.10. Make tables that show the results of:

- (a) multiplication modulo 3.
- (b) subtraction modulo 3 (For $\bar{a} - \bar{b}$, put the result in row \bar{a} and column \bar{b} .)

For both (a) and (b), all table entries should be either $\bar{0}$, $\bar{1}$, or $\bar{2}$. ◇

17.5.2 The integers modulo n

The preceding discussion can be generalized to apply with any integer n in place of 3. This results in *modular arithmetic*.

Definition 17.5.11. Fix some natural number n .

- (a) For any integer k , we use $[k]_n$ to denote the equivalence class of k under congruence modulo n . When n is clear from the context, we may write \bar{k} , instead of $[k]_n$.
- (b) The set of these equivalence classes is called the *integers modulo n* . It is denoted \mathbb{Z}_n .
- (c) Addition, subtraction, and multiplication modulo n are defined by:
 - $\bar{a} + \bar{b} = \overline{a + b}$,
 - $\bar{a} - \bar{b} = \overline{a - b}$, and
 - $\bar{a} \cdot \bar{b} = \overline{ab}$.

Just as in the case of mod 3, whenever we're doing arithmetic mod n you should understand that we are using these definitions of $+$, $-$, and \cdot .

△

Note that $|\mathbb{Z}_n| = n$. (Recall that for a set S , $|S|$ means the number of elements in S .) We may enumerate the elements precisely as follows:

Proposition 17.5.12. For any $n \in \mathbb{N}^+$, we have

$$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$$

and $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$ are all distinct.

Exercise 17.5.13. Prove Proposition 17.5.12. It is sufficient to show (a) $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$ are distinct; and (b) for any integer, the equivalence class \bar{k} is one of $\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}$. ◇

Exercise 17.5.14. Using the definitions of addition, subtraction, and multiplication given in part (c) of Definition 17.5.11, make tables that show the results of:

- (a) addition modulo 4.
- (b) subtraction modulo 5.
- (c) multiplication modulo 6.

◇

Exercise 17.5.15. Find $x, y \in \mathbb{Z}_{12}$ such that $x \neq \bar{0}$ and $y \neq \bar{0}$, but $x \cdot y = \bar{0}$. ◇

17.5.3 What do we mean by “the same thing”?

Now it's time to go back to our statement in Section 17.5.1 that the definition of \mathbb{Z}_n and its operations in terms of equivalence classes is the “same thing” as the definition in terms of remainder arithmetic that we gave in the Modular Arithmetic chapter.

One way to see this is to consider the Cayley tables. There is a striking similarity between the Cayley tables for \oplus and \odot that we computed in Section 5.4.2 and the tables that we just finished computing in the previous section:

Exercise 17.5.16.

- Compute Cayley tables for \oplus and \odot for \mathbb{Z}_7 using remainder arithmetic (as we did in Section 5.4.2).
- Compute Cayley tables for $+$ and \cdot for \mathbb{Z}_7 using the method we used in the previous section.
- Make profound comments about what you observe.

◇

Whether we think of \mathbb{Z}_n as a subset of \mathbb{Z} with operations \oplus and \odot , or whether we think of \mathbb{Z}_n as a set of equivalence classes, as far as practical computation is concerned it really makes no difference. The operations give the same result. Any equation that holds for the one version, also hold for the other. Mathematically we describe this situation as saying that the two versions of \mathbb{Z}_n are *isomorphic*. We've encountered isomorphism before (in Section 4.3.6), and later on we'll devote an entire chapter to this concept (Chapter 20).

We should hasten to add that although the two versions work the same computationally, the conceptual differences between the two are important. Looking at the “same thing” in different ways can inspire new ideas that may bring deep insights and breakthroughs in understanding. In fact, this is one of the most powerful tools in the mathematician's toolbox.

17.5.4 Something we have swept under the rug

The discussion of modular arithmetic ignored a very important point. When we evaluate $\bar{a} + \bar{b}$, we use the following process:

- Choose an element from \bar{a} and an element from \bar{b} ;
- Add them together (using regular integer arithmetic);
- Find the equivalence class of the result.

But suppose we had chosen *different* elements to represent \bar{a} and \bar{b} : how do we know that we would come up with the same answer? In other words: how do we know that $\bar{a} + \bar{b}$ is independent of the choice of representatives from \bar{a} and \bar{b} ?

So there's a little more work we have to do here to make sure that we don't get into trouble. We need to show that the operations of addition, subtraction, and multiplication are *well-defined*: that is, if $a_1, a_2, b_1,$ and b_2 are integers such that $\bar{a}_1 = \bar{a}_2$ and $\bar{b}_1 = \bar{b}_2$, then we need to show that

- (a) $\bar{a}_1 + \bar{b}_1 = \bar{a}_2 + \bar{b}_2$,
- (b) $\bar{a}_1 - \bar{b}_1 = \bar{a}_2 - \bar{b}_2$,
- (c) $\bar{a}_1 \cdot \bar{b}_1 = \bar{a}_2 \cdot \bar{b}_2$.

Fortunately, these statements are all true, as you will show in the following exercise.

Exercise 17.5.17.

- (a) Fill in the blanks in the following proof of statement (a) above that $+$ is well-defined (that is, that $\bar{a}_1 = \bar{a}_2$ and $\bar{b}_1 = \bar{b}_2$ implies that $\bar{a}_1 + \bar{b}_1 = \bar{a}_2 + \bar{b}_2$):

Suppose $\bar{a}_1 = \bar{a}_2$ and $\bar{b}_1 = \bar{b}_2$.

- (i) From the definition of equivalence class, it follows that $a_1 \equiv \underline{\langle 1 \rangle} \pmod{n}$ and $b_1 \equiv \underline{\langle 2 \rangle} \pmod{n}$.
- (ii) By Definition 17.5.2, it follows that $a_1 = a_2 + k_1 \cdot \underline{\langle 3 \rangle}$ and $b_1 = b_2 + k_2 \cdot \underline{\langle 4 \rangle}$, where k_1 and k_2 are $\underline{\langle 5 \rangle}$.
- (iii) By substitution and integer arithmetic, it follows that $(a_1 + b_1) - (a_2 + b_2) = \underline{\langle 6 \rangle}$.
- (iv) Since $k_1 + k_2$ is an integer it follows from Definition 17.5.2 that $(a_1 + b_1) \equiv \underline{\langle 7 \rangle} \pmod{\underline{\langle 8 \rangle}}$.
- (v) It follows from Proposition 17.4.7(d) that $\underline{\langle 9 \rangle}$.

- (vi) From Definition 17.5.11 (c) we have $\overline{a_1} + \overline{b_1} = \underline{\langle 10 \rangle}$ and $\overline{a_2} + \overline{b_2} = \underline{\langle 11 \rangle}$.
- (vii) By substitution we obtain that $\overline{a_1} + \overline{b_1} = \overline{a_2} + \overline{b_2}$, which implies that $+$ is well-defined on equivalence classes.
- (b) By following the proof in part (a), prove that subtraction mod n is well-defined.
- (c) By following the proof in part (a), prove that multiplication mod n is well-defined.

◇

Actually, finding operations that are well-defined on equivalence classes is somewhat of a big deal. In many cases, candidate operations turn out to be *not* well-defined:

Exercise 17.5.18. Suppose we try to define an exponentiation operation on \mathbb{Z}_3 by:

$$[a]_3 \wedge [b]_3 = [a^b]_3 \quad \text{for } [a]_3, [b]_3 \in \mathbb{Z}_3.$$

Show that \wedge is not well-defined: that is, find $a_1, b_1, a_2, b_2 \in \mathbb{Z}$, such that $[a_1]_3 = [a_2]_3$ and $[b_1]_3 = [b_2]_3$, but $[a_1^{b_1}]_3 \neq [a_2^{b_2}]_3$. ◇

Exercise 17.5.19.

- (a) Show that absolute value does *not* produce a well-defined function from \mathbb{Z}_7 to \mathbb{Z}_7 . That is, show there exist $a, b \in \mathbb{Z}$, such that

$$[a]_7 = [b]_7, \text{ but } |[a]|_7 \neq |[b]|_7.$$

- (b) Show that part (a) is true for *every* $n > 2$. That is, show that absolute value does *not* provide a well-defined function from \mathbb{Z}_n to \mathbb{Z}_n .

◇

Exercise 17.5.20.

- (a) Show that there is a well-defined function $f: \mathbb{Z}_{12} \rightarrow \mathbb{Z}_4$, given by $f([a]_{12}) = [a]_4$. That is, show that if $[a]_{12} = [b]_{12}$, then $[a]_4 = [b]_4$.

- (b) Generalize part (a) by showing that if m divides n , then there is a well-defined function $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$, given by $f([a]_n) = [a]_m$. That is, show that if $[a]_n = [b]_n$, then $[a]_m = [b]_m$.

◇

Exercise 17.5.21.

- (a) Show that if we try to define a function $g: \mathbb{Z}_3 \rightarrow \mathbb{Z}_2$ by $g([a]_3) = [a]_2$, then the result is *not* well-defined. That is, show that there exist $a, b \in \mathbb{Z}$ such that $[a]_3 = [b]_3$ but $[a]_2 \neq [b]_2$.
- (b) Generalize part (a) by showing that m, n are integers and m does not divide n , then the function $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_m$ given by $f([a]_n) = [a]_m$ is *not* well-defined. That is, show that there exists integers a, b such that $[a]_n = [b]_n$ and $[a]_m \neq [b]_m$.

◇

Recall that \mathbb{Z}_n replaces integers a and b that are congruent modulo n with objects \bar{a} and \bar{b} that are exactly equal to each other. This was achieved by letting \mathbb{Z}_n be the set of all equivalence classes. The set \mathbb{Z}_n applies only to congruence modulo n , but the same thing can be done for any equivalence relation:

Definition 17.5.22. Suppose \sim is an equivalence relation on a set A . The set of all equivalence classes is called A *modulo* \sim . It is denoted A/\sim . \triangle

Example 17.5.23. Suppose we define an equivalence relation \sim on \mathbb{Z} by $a \sim b$ iff $a \equiv b \pmod{n}$. Then \mathbb{Z}/\sim is simply another name for \mathbb{Z}_n . \blacklozenge

17.6 Hints for “Equivalence Relations and Equivalence Classes” exercises

Exercise 17.1.8(a): There are two. (b): There are four. (c): There are four. (d): There are sixteen. (e): The answer is *bigger* than 500!

Exercise 17.2.6(a.ii): The graph consists of shaded areas, not points or lines.

Exercise 17.1.15(c): There are 9.

Exercise 17.2.14(a): \leq is *not* symmetric – you may show this by giving a counterexample.

Exercise 17.2.14(c): The “Is it transitive?” question amounts to answering the following: Given $z_1 \sim z_2$ and $z_2 \sim z_3$. Is it always true that $z_1 \sim z_3$? If yes, prove it; and if no, give a counterexample.

Exercise 17.2.17(a): There are actually three counterexamples, you only need to find one.

Exercise 17.2.17(b): Give a specific example where $a \sim b$ and $b \sim c$ but $a \not\sim c$. In other words, (a, b) and (b, c) are elements of R_{\sim} , but (a, c) is not in R_{\sim} . It is not necessary for a, b , and c to be distinct.

Exercise 17.2.17(c): Explain why it is impossible to find a counterexample.

Exercise 17.3.3(b): You may assume (without proof) that the negative of any integer is an integer, and that the sum of any two integers is an integer. For transitivity, notice that $x - z = (x - y) + (y - z)$.

Exercise 17.3.3(c): This is similar to the proof in Example 17.3.2, but with multiplication in place of addition.

Cosets and Quotient Groups (a.k.a. Factor Groups)

SHREK: For your information, there's a lot more to ogres than people think.

DONKEY: Example?

SHREK: Example... uh... ogres are like onions!

DONKEY: They stink?

SHREK: Yes... No!

DONKEY: Oh, they make you cry?

SHREK: No!

DONKEY: Oh, you leave 'em out in the sun, they get all brown, start sproutin' little white hairs...

SHREK: NO! Layers. Onions have layers. Ogres have layers... You get it? We both have layers.

Source: *Shrek* (movie), 2001.

Groups, like onions and ogres, also have layers. As we've seen, many groups have subgroups inside them. These subgroups can be used to define

“layers” which are called *cosets*. And in some cases, the “layers” (cosets) themselves form groups, which are called *quotient groups* (or *factor groups*).

Our examination of cosets will give us deep insight into the nature and structure of groups. We will be leaning heavily on the material from Chapter 5 (which will furnish us with motivating examples), Chapter 17 (which will aid us in our characterization of cosets), and of course Chapter 15. In the course of reading this chapter, you may want to review these chapters. So, here we go!

Thanks to Tom Judson for material used in this chapter.

18.1 Definition of cosets

The concept of “coset” brings together two ideas that we’ve seen before, namely *subgroups* and *equivalence classes*. We’ll see how cosets arise from this mix by using a familiar example.

Example 18.1.1. (*Modular addition déjà vu all over again*)

Back in Chapter 5 we defined modular equivalence (Definition 5.2.6), and in Proposition 5.2.10 we gave an alternative characterization:

$$a \equiv b \pmod{m} \text{ iff } a - b = k \cdot m, \text{ where } k \text{ is an integer (that is, } k \in \mathbb{Z}\text{).}$$

Exercise 18.1.2.

- (a) Give 4 integers a that satisfy the equation: $a \equiv 0 \pmod{3}$.
- (b) Give 4 integers a that satisfy the equation: $a \equiv 2 \pmod{3}$.

◇

In Section 17.5 in the Equivalence Relations chapter, we saw that modular equivalence was indeed an *equivalence relation*, and gave rise to *equivalence classes*:

$$[0]_3 = \{\text{All integers equivalent to } 0 \pmod{3}\} = \{\dots -9, -6, -3, 0, 3, 6, 9 \dots\}.$$

$$[1]_3 = \{\text{All integers equivalent to } 1 \pmod{3}\} = \{\dots -8, -5, -2, 1, 4, 7, 10 \dots\}.$$

$$[2]_3 = \{\text{All integers equivalent to } 2 \pmod{3}\} = \{\dots -7, -4, -1, 2, 5, 8, 11 \dots\}.$$

Then in the Groups chapter we introduced an alternative notation for $[0]_3$, namely $3\mathbb{Z}$. Since every element of $[1]_3$ is $1 +$ an element of $3\mathbb{Z}$ (and similarly for $[2]_3$) it makes sense to introduce the notation:

$$[1]_3 = 1 + 3\mathbb{Z}.$$

$$[2]_3 = 2 + 3\mathbb{Z}.$$

Notice the pattern here. Recall that $3\mathbb{Z}$ is a *subgroup* of \mathbb{Z} . In order to “create” the equivalence class $1 + 3\mathbb{Z}$, we added a specific group element (namely, 1) to *every* element of the subgroup $3\mathbb{Z}$. The same holds true for $2 + 3\mathbb{Z}$. In both cases, the notation follows the pattern:

$$(\text{selected group element}) (\text{group operation}) (\text{subgroup}).$$

And, since every element of $[1]_3$ can also be viewed as an element of $3\mathbb{Z} + 1$ (and similarly for $[2]_3$), an alternative notation that makes sense is:

$$[1]_3 = 3\mathbb{Z} + 1$$

$$[2]_3 = 3\mathbb{Z} + 2,$$

which follows the pattern:

$$(\text{subgroup}) (\text{group operation}) (\text{selected group element}). \quad \blacklozenge$$

Exercise 18.1.3.

- (a) Write the 5 equivalence classes (subsets of \mathbb{Z}) which make up \mathbb{Z}_5 using our new notation.
- (b) Write all elements of \mathbb{Z}_7 using our new notation.

◇

The same pattern that we saw in the preceding example can actually be generalized to any group possessing a subgroup:

Definition 18.1.4. Let G be a group and H a subgroup of G . The *left coset* of H with *representative* $g \in G$ is defined as the following set:

$$gH = \{gh : h \in H\}.$$

Right cosets are defined similarly by

$$Hg = \{hg : h \in H\}.$$

(Note that in the preceding equations, “ gh ” denotes $g \circ h$ where \circ is the group operation. This is similar to our writing xy to denote $x \cdot y$ in conventional algebra). \triangle

Definition 18.1.4 looks a little different from Example 18.1.1, e.g. we have gH instead of $3 + \mathbb{Z}$. But in fact the pattern is the same: (group element) (group operation) (subgroup). If the group operation is $+$, we will typically write left cosets as $g + H$ and right cosets as $H + g$. For all other group operations, we’ll use the more compact notation gH and Hg .

We should note also that Definition 18.1.4 enables us to express the same coset in multiple ways. For example, the coset $1 + 3\mathbb{Z}$ described above could also be written as $4 + 3\mathbb{Z}$ or $7 + 3\mathbb{Z}$ or $-8 + 3\mathbb{Z}$. These all refer to the same subset of \mathbb{Z} .

Now Definition 18.1.4 distinguishes between *left* and *right* cosets. In our earlier discussion, the left coset $1 + 3\mathbb{Z}$ and the right coset $3\mathbb{Z} + 1$ were in fact the same set, as were $2 + 3\mathbb{Z}$ and the right coset $3\mathbb{Z} + 2$. But left and right cosets are not always equal, as the following example shows.

Example 18.1.5. Let H be the subgroup of S_3 defined by the permutations $\{(1), (123), (132)\}$. (Here we are using (1) to denote the identity permutation id.) To find cosets, we should take each element of S_3 and multiply it by the three permutations in H . Recall the elements of S_3 are $(1), (123), (132), (12), (13),$ and (23) . The left cosets of H are thus:

$$\begin{aligned} (1)H &= (123)H = (132)H = \{(1), (123), (132)\}, \\ (12)H &= (13)H = (23)H = \{(12), (13), (23)\}. \end{aligned}$$

There are 2 left cosets, and each coset can be expressed in 3 different ways.

On the other hand, the right cosets of H may be computed similarly as:

$$\begin{aligned} H(1) &= H(123) = H(132) = \{(1), (123), (132)\}, \\ H(12) &= H(13) = H(23) = \{(12), (13), (23)\}. \end{aligned}$$

So in this case once again the left cosets and right cosets are the same.

On the other hand, let K be the subgroup of S_3 defined by the permutations $\{(1), (12)\}$. Then the left cosets of K are

$$\begin{aligned}(1)K &= (12)K = \{(1), (12)\} \\ (13)K &= (123)K = \{(13), (123)\} \\ (23)K &= (132)K = \{(23), (132)\};\end{aligned}$$

and the right cosets of K are

$$\begin{aligned}K(1) &= K(12) = \{(1), (12)\} \\ K(13) &= K(132) = \{(13), (132)\} \\ K(23) &= K(123) = \{(23), (123)\}.\end{aligned}$$

The left and right cosets are *not* the same.

Take note of something very striking about the previous two examples. First look at the case of $H \subset S_3$. In this case we ended up with 2 different left cosets, each of which could be expressed as gH in 3 different ways. For example, we saw that $(12)H = (13)H = (23)H$. In fact, these three different g 's are exactly the elements of the coset! The very same thing applies to all other cases. For example, we found $K(23) = K(123)$, and that both were equal to $\{(23), (123)\}$. This turns out to be a general property of cosets, which we will prove in the next section. \blacklozenge

Unequal left and right cosets are actually very common. So let's get some practice determining both left and right cosets.

Exercise 18.1.6. Let H be the subgroup of $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ consisting of the elements 0 and 3. (We are using our simplified notation here: '0' represents $\bar{0}$, etc.) The left cosets are

$$\begin{aligned}0 + H &= 3 + H = \{0, 3\} \\ 1 + H &= 4 + H = \{1, 4\} \\ 2 + H &= 5 + H = \{2, 5\}.\end{aligned}$$

What are the right cosets? Are the left and right cosets equal? \diamond

Exercise 18.1.7. List the left and right cosets of the subgroups in each of the following. Tell whether the left and right cosets are equal.

(Recall the following notations: $\langle a \rangle$ is the cyclic group generated by the element a in a given group G ; A_n (the alternating group) is the set of even permutations, on n objects; D_4 is the group of symmetries of a square; and \mathbb{T} is the group of complex numbers with modulus 1, under the operation of multiplication.)

- | | |
|--|------------------------------------|
| (a) $\langle 8 \rangle$ in \mathbb{Z}_{24} | (f) A_4 in S_4 (*Hint*) |
| (b) $\langle 3 \rangle$ in $U(8)$ | (g) A_n in S_n (*Hint*) |
| (c) $4\mathbb{Z}$ in \mathbb{Z} | |
| (d) $H = \{(1), (123), (132)\}$ in S_4 | (h) D_4 in S_4 (*Hint*) |
| (e) $H = \{1, i, -1, -i\}$ in Q_8 (See Example 15.2.8) | (i) \mathbb{T} in \mathbb{C}^* |

◇

Remark 18.1.8. From now on, if the left and right cosets coincide, or if it is clear from the context to which type of coset that we are referring, we will simply use the word “coset” without specifying left or right. △

From what we’ve seen so far, you might have noticed that it seems that left and right cosets are always equal for *abelian* groups. This makes sense, because abelian means you get the same result whether you compose on the left or on the right. In fact, it is true in general:

Exercise 18.1.9. Show that if G is an abelian group and H is a subgroup of G , then any left coset gH is equal to the right coset Hg . (*Hint*) ◇

But abelian groups are not the only groups in which left cosets are equal to right cosets—see for example the first case in Example 18.1.5. So we still haven’t answered the question of what is the most general situation in which left cosets and right cosets are equal. We’ll take this issue up again in Section 18.4.1.

18.2 Cosets and partitions of groups

In Example 18.1.1, the cosets that we described were equivalence classes. We saw in Chapter 17 that equivalence classes form a *partition* which divides

up the containing set into disjoint subsets. This is actually a general fact that is true for all cosets, and we will prove this below. In the proof, we will need the following proposition, which shows that there are several different ways to characterize the situation when two cosets are equal.

Proposition 18.2.1. Let H be a subgroup of a group G and suppose that $g_1, g_2 \in G$. The following conditions are equivalent.

1. $g_1H = g_2H$;
2. $g_1^{-1}g_2 \in H$.
3. $g_2 \in g_1H$;
4. $g_2H \subset g_1H$; (Note: “ \subset ” means that equality is also possible)
5. $Hg_1^{-1} = Hg_2^{-1}$;

The proof of this Proposition is laid out in the Exercise 18.2.2 below, and you are asked to fill in the details. Parts (a)-(f) of the exercise establish the following steps:

$$(1) \underset{(a)}{\Rightarrow} (2) \underset{(b)}{\Rightarrow} (3) \underset{(c)}{\Rightarrow} (4) \underset{(d)}{\Rightarrow} (1) \quad \text{and} \quad (2) \underset{(e,f)}{\Leftrightarrow} (5).$$

Exercise 18.2.2.

- (a) Show that condition (1) implies condition (2). (*Hint*)
- (b) Show that condition (2) implies condition (3). (*Hint*)
- (c) Show that condition (3) implies condition (4). (*Hint*)
- (d) Show that condition (4) implies condition (1). (*Hint*)
- (e) Show that condition (2) implies condition (5). (*Hint*)
- (f) Show that condition (5) implies condition (2).

◇

Exercise 18.2.3. Proposition 18.2.1 deals with *left* cosets. A parallel proposition holds for right cosets. List the five equivalent conditions for *right* cosets that correspond to the five conditions given in Proposition 18.2.1. ◇

Now we're ready to prove that the cosets of a subgroup always form a partition of the group that contains it:

Proposition 18.2.4. Let H be a subgroup of a group G . Then the left cosets of H in G partition G . That is, the group G is the disjoint union of the left cosets of H in G .

PROOF. The proof has two parts, namely (1) Cosets are disjoint; and (2) The union of cosets is all of G .

(1) Let g_1H and g_2H be two cosets of H in G . We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose that $g_1H \cap g_2H \neq \emptyset$ and $a \in g_1H \cap g_2H$. Then by the definition of a left coset, $a = g_1h_1 = g_2h_2$ for some elements h_1 and h_2 in H . Hence, $g_1 = g_2h_2h_1^{-1}$ or $g_1 \in g_2H$. By Proposition 18.2.1, $g_1H = g_2H$.

(2) **Exercise 18.2.5.** Complete part (2) of the proof: that is, prove that $\bigcup_{g \in G} gH = G$. ◇

□

Remark 18.2.6. Right cosets also partition G . The partition may not be the same as the partition using the left cosets, since the left and right cosets aren't necessarily equal. The proof of this fact is exactly the same as the proof for left cosets except that all group multiplications are done on the right side of H . △

Let's consider now the question of how many cosets there are for a particular subgroup within a given group. First, we define some convenient notation:

Definition 18.2.7. Let G be a group and H be a subgroup of G . The *index* of H in G is the number of left cosets of H in G . We will denote the index of H in G by $[G : H]$. △

Example 18.2.8. Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then looking back at Exercise 18.1.6, we see that $[G : H] = 3$. \blacklozenge

Exercise 18.2.9. Based on your work in Exercise 18.1.6, how many right cosets of $H = \{0, 3\}$ were there in \mathbb{Z}_6 ? \diamond

Example 18.2.10. Suppose that $G = S_3$, $H = \{(1), (123), (132)\}$, and $K = \{(1), (12)\}$. Then looking back at Example 18.1.5, we can see that $[G : H] = 2$ and $[G : K] = 3$. \blacklozenge

Exercise 18.2.11. How many right cosets of $H = \{(1), (123), (132)\}$ in S_3 were there? How about right cosets of $K = \{(1), (12)\}$ in S_3 ? \diamond

Exercise 18.2.12. Using your work from Exercise 18.1.7, find:

- (a) $[\mathbb{Z}_{24} : \langle 8 \rangle]$ and the number of right cosets of $\langle 8 \rangle$ in \mathbb{Z}_{24} .
- (b) $[U(8) : \langle 3 \rangle]$ and the number of right cosets of $\langle 3 \rangle$ in $U(8)$.
- (c) $[\mathbb{Z} : 4\mathbb{Z}]$ and the number of right cosets of $4\mathbb{Z}$ in \mathbb{Z} .
- (d) $[S_4 : \{(1), (123), (132)\}]$ and the number of the right cosets of $\{(1), (123), (132)\}$ in S_4 .
- (e) $[S_4 : A_4]$ and the number of right cosets of A_4 in S_4 .
- (f) $[S_n : A_n]$ and the number of right cosets of A_n in S_n .
- (g) $[S_4 : D_4]$ and the number of right cosets of D_4 in S_4 .
- (h) $[\mathbb{C}^* : \mathbb{T}]$ and the number or right cosets of \mathbb{T} in \mathbb{C}^* .

\diamond

The last several examples seem to suggest that although the the left and right cosets of a subgroup aren't always equal, it seems the *number* of them is always the same. Indeed we can prove this:

Proposition 18.2.13. Let H be a subgroup of a group G . The number of left cosets of H in G is the same as the number of right cosets of H in G .

PROOF. Let L and R denote the set of left and right cosets of H in G , respectively. If we can define a bijection $\phi : L \rightarrow R$, then the proposition will be proved. If $gH \in L$, let $\phi(gH) = Hg^{-1}$. By Proposition 18.2.1, the map ϕ is well-defined; that is, if $g_1H = g_2H$, then $Hg_1^{-1} = Hg_2^{-1}$. To show that ϕ is one-to-one, suppose that

$$Hg_1^{-1} = \phi(g_1H) = \phi(g_2H) = Hg_2^{-1}.$$

Again by Proposition 18.2.1, $g_1H = g_2H$. The map ϕ is onto since $\phi(g^{-1}H) = Hg$. \square

Exercise 18.2.14. Consider the left cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$. Show that two matrices in $GL_2(\mathbb{R})$ are in the same left coset of $SL_2(\mathbb{R})$ if and only if they have the same determinant. Is the same true for right cosets? (Prove your answer.) (*Hint*) \diamond

18.3 Lagrange's theorem, and some consequences

18.3.1 Lagrange's theorem

At the beginning of the chapter, we compared cosets to layers of an onion. Indeed, as we saw in the last section, this is a good analogy because the cosets of a subgroup partition the group. However, an even better analogy is to slices of a loaf of sandwich bread—because as we'll see in this section, every coset of a particular subgroup within a given group has exactly the same size.

What may we conclude from this? Let's push our analogy with sandwich bread a little farther. Suppose the bread has raisins in it, and each slice has exactly the same number of raisins. Then the number of raisins in the loaf must be equal to the sum of all raisins in all the slices, that is:

$$|\text{raisins in loaf}| = |\text{raisins in each slice}| \cdot |\text{slices}|,$$

where as usual the $|\dots|$ notation signifies “size” or “number of”. Applying this same reasoning to groups and their subgroups leads to a very general result called *Lagrange's theorem*. This far-reaching theorem will enable us to prove some surprising properties of subgroups, their elements, and even some results in number theory. So let's get started.



Remark 18.3.1. In the following discussion, for specificity's sake we will use left coset notation. However, just like we saw in the last section (Remark 18.2.6), everything we say about left cosets is also true for right cosets. Indeed, to prove the cases for the right cosets, you simply need to take the left coset proofs given below and switch around each coset expression and group operation. \triangle

As mentioned above, to prove Lagrange's theorem we first need to prove that every left coset of a subgroup has the exactly the same size:

Proposition 18.3.2. Let H be a subgroup of G with $g \in G$ and define a map $\phi : H \rightarrow gH$ by $\phi(h) = gh$. The map ϕ is a bijection; hence, the number of elements in H is the same as the number of elements in gH .

PROOF. We first show that the map ϕ is one-to-one. Suppose that $\phi(h_1) = \phi(h_2)$ for elements $h_1, h_2 \in H$. We must show that $h_1 = h_2$, but $\phi(h_1) = gh_1$ and $\phi(h_2) = gh_2$. So $gh_1 = gh_2$, and by left cancellation $h_1 = h_2$. To show that ϕ is onto is easy. By definition every element of gH is of the form gh for some $h \in H$ and $\phi(h) = gh$. \square

Given this proposition Lagrange's theorem falls right out:

Proposition 18.3.3. (Lagrange's theorem) Let G be a finite group and let H be a subgroup of G . Then $|G|/|H| = [G : H]$ is the number of distinct left cosets of H in G . In particular, the number of elements in H must divide the number of elements in G .

PROOF. The group G is partitioned into $[G : H]$ distinct left cosets. Each left coset has $|H|$ elements; therefore, $|G| = [G : H]|H|$. \square

Consider for a moment what we've just proven. The number of elements in a subgroup *must* divide evenly into the number of elements in the group; you can't have just any number of elements in a subgroup. This is a very powerful tool to give insight into the structure of groups.

Example 18.3.4. Let G be a group with $|G| = 25$. Then since 2 doesn't divide 25 evenly, Lagrange's theorem implies that G can't possibly have a subgroup with 2 elements. \blacklozenge

Exercise 18.3.5. Suppose that G is a finite group with an element g of order 5 and an element h of order 7.

- (a) Show that G has subgroups of order 5 and 7. (*Hint*)
 (b) Why must $|G| \geq 35$?

◇

Exercise 18.3.6. Suppose that G is a finite group with 60 elements. What are the possible orders for subgroups of G ? ◇

We can take the result in Lagrange's theorem a step farther by considering subgroups of subgroups. We can prove a multiplication rule for indices:

Proposition 18.3.7. Let H and K be subgroups of a finite group G such that $G \supset H \supset K$. Then

$$[G : K] = [G : H][H : K].$$

PROOF. Observe that

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H][H : K].$$

□

Remark 18.3.8. (*historical background*) Joseph-Louis Lagrange (1736–1813), born in Turin, Italy, was of French and Italian descent. His talent for mathematics became apparent at an early age. Leonhard Euler recognized Lagrange's abilities when Lagrange, who was only 19, communicated to Euler some work that he had done in the calculus of variations. That year he was also named a professor at the Royal Artillery School in Turin. At the age of 23 he joined the Berlin Academy. Frederick the Great had written to Lagrange proclaiming that the “greatest king in Europe” should have the “greatest mathematician in Europe” at his court. For 20 years Lagrange held the position vacated by his mentor, Euler. His works include contributions to number theory, group theory, physics and mechanics, the calculus of variations, the theory of equations, and differential equations. Along with Laplace and Lavoisier, Lagrange was one of the people responsible for designing the metric system. During his life Lagrange profoundly influenced the development of mathematics, leaving much to the next generation of mathematicians in the form of examples and new problems to be solved. △

18.3.2 Orders of elements, Euler's theorem, Fermat's little theorem, and prime order

Now let's really put Lagrange's theorem to work. Note that Lagrange's theorem is an extremely general result—it applies to *any* subgroup of *any* finite group. So let's consider one particular type of subgroup, namely cyclic subgroups of the form $\langle g \rangle$ where g is an element of a given group G . (See Proposition 15.5.16 in Section 15.5.2 for the definition of $\langle g \rangle$ and the proof that it is indeed a group).

Proposition 18.3.9. Suppose that G is a finite group and $g \in G$. Then the order of g must divide the number of elements in G .

PROOF. The order of a group element g , which is denoted as $|g|$, is defined in Definition 15.5.19 in Section 15.5.2. We indicated in Exercise 15.5.26 in that same section that $|g|$ is equal to $|\langle g \rangle|$, which is the order of the cyclic subgroup generated by g . It follows immediately from Lagrange's theorem that $|g|$ must divide $|G|$. \square

To show the power of this result, we'll apply it to the group of units $U(n)$ which was introduced in Section 15.2.1.

But before we do this, let's do some exploration. Recall that the elements of $U(n)$ are the positive integers that are less than n and relatively prime to n (we showed in Exercise 15.2.27 of Section 15.2.1 that these elements actually form a group. There is a special notation for the number of elements in $U(n)$:

Definition 18.3.10. For $n > 1$, define $\phi(n)$ as the number of natural numbers that are less than n and relatively prime to n . Alternatively, we can say that $\phi(n)$ is the number of natural numbers m where $m < n$ and $\gcd(m, n) = 1$. In order to make ϕ a function on the natural numbers, we also define $\phi(1) = 1$. The function ϕ is called the **Euler ϕ -function**. \triangle

Exercise 18.3.11. Evaluate the following:

- | | |
|----------------|-------------------------------------|
| (a) $\phi(12)$ | (d) $\phi(23)$ |
| (b) $\phi(16)$ | (e) $\phi(51)$ |
| (c) $\phi(20)$ | (f) $\phi(p)$, where p is prime. |

- (g) $\phi(p^2)$, where p is prime (*justify your answer*). (i) $\phi(pq)$, where p and q are primes and $p \neq q$ (*justify your answer*).
- (h) $\phi(p^n)$, where p is prime and $n \in \mathbb{N}$ (*justify your answer*).

(*Hint*)

◇

If we now apply Lagrange's theorem to $U(n)$, we obtain an important result in number theory which was first proved by Leonhard Euler in 1763.

Proposition 18.3.12. (*Euler's theorem*) Let a and n be integers such that $n > 0$ and $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

PROOF. First, let r be the remainder when a is divided by n . We may consider r as an element of $U(n)$.

As noted above, the order of $U(n)$ is $\phi(n)$. Lagrange's theorem then tells us that $|r|$ divides $\phi(n)$, so we can write: $\phi(n) = k|r|$, where $k \in \mathbb{N}$. Consequently, considering r as an element of $U(n)$, we have $r^{\phi(n)} = r^{k|r|} = (r^{|r|})^k = (1)^k = 1$ (take note that the multiplication that is being used here is *modular* multiplication, not regular multiplication).

Finally, we may use the fact that $a \equiv r \pmod{n}$ and apply Exercise 5.4.7 in Section 5.4.1 to conclude that $a^{\phi(n)} \equiv 1 \pmod{n}$.

□

Exercise 18.3.13.

- (a) Verify Euler's theorem for $n = 15$ and $a = 4$.
 (b) Verify Euler's theorem for $n = 22$ and $a = 3$.

◇

Exercise 18.3.14. Evaluate the following, using the results of Exercise 18.3.11

- (a) $\text{mod } (5^{200}, 12)$ (c) $\text{mod } (15^{221}, 23)$
 (b) $\text{mod } (13^{48}, 16)$ (d) $\text{mod } (9^{111}, 121)$

- (e) $\text{mod } (10^{195}, 221)$ (g) $\text{mod } ((p+1)^{p^2}, p^2)$, where p is prime.
- (f) $\text{mod } \left(\left(\frac{p+1}{2} \right)^p, p \right)$, where p is prime.

◇

In the following exercise you will prove *Fermat's little theorem*, which may be thought of as a special case of Euler's theorem:

Exercise 18.3.15. Suppose that p is a prime number, and a is a natural number which is relatively prime to p . Show that $a^{p-1} \equiv 1 \pmod{p}$. ◇

We can also apply Proposition 18.3.9 to groups of prime order, as in the following exercise.

Exercise 18.3.16. Let G be a group such that $|G| = p$, where p is a prime number.

- (a) Let a be an element of $G \setminus \{e\}$. What does Proposition 18.3.9 tell us about $|a|$? (Recall that ' \setminus ' is the set difference operation, defined in Definition 7.1.17). (*Hint*)
- (b) Prove that G is cyclic.
- (c) Describe the set of generators of G (recall that $g \in G$ is a generator of G if $\langle g \rangle = G$.)

◇

The results of the preceding exercise can be summarized as follows:

Proposition 18.3.17. Let $|G| = p$ with p a prime number. Then G is cyclic and any $g \in G$ such that $g \neq e$ is a generator.

Later we will use this proposition to show that all groups of prime order p are the "same" in some sense (see Section 20.4.1).

Finally, we can use Lagrange's theorem to show that groups of prime order have a very simple structure:

Exercise 18.3.18. Let G be a group of prime order. Use Proposition 18.3.17 to show that the only proper subgroup of G is the trivial subgroup $\{e\}$. \diamond

Exercise 18.3.18 shows that groups of prime order (such as \mathbb{Z}_p) are “simple” in the sense that they don’t contain any nontrivial subgroups. In Section 18.5.1 we will talk more about “simple” groups.

18.4 Normal subgroups and factor groups

We saw in Section 18.1 that if H is a subgroup of a group G , then right cosets of H in G are not always the same as left cosets. It’s true the *number* of right cosets and left cosets are always equal, and the number of elements in the left and right cosets match; but the right and left cosets *themselves* may not equal each other: in other words, it’s not always the case that $gH = Hg$ for all $g \in G$. Those subgroups for which this property does hold play a critical role in group theory: they allow for the construction of a new class of groups, called *quotient groups* (or *factor groups*).

18.4.1 Normal subgroups

First, let’s give a name to these nice subgroups:

Definition 18.4.1. A subgroup H of a group G is **normal** in G if $gH = Hg$ for all $g \in G$. That is, a normal subgroup of a group G is one in which the right and left cosets for every group element are precisely the same. \triangle

Example 18.4.2. Think back to Example 18.1.5 earlier in the chapter. H was the subgroup of S_3 consisting of elements (1) and (12). Since

$$(123)H = \{(123), (13)\} \quad \text{and} \quad H(123) = \{(123), (23)\},$$

H cannot be a normal subgroup of S_3 . However, the subgroup N , consisting of the permutations (1), (123), and (132), is normal since the cosets of N are

$$\begin{aligned} N &= \{(1), (123), (132)\} \\ (12)N &= N(12) = \{(12), (13), (23)\}. \end{aligned}$$

\blacklozenge

Exercise 18.4.3. Looking back at Exercise 18.1.7, which of the subgroups were normal? \diamond

Exercise 18.4.4. Is $SL_2(\mathbb{R})$ a normal subgroup of $GL_2(\mathbb{R})$? Prove or disprove. (*Hint*) \diamond

Exercise 18.4.5. Prove or disprove: $\{1, -1, i, -i\}$ is a normal subgroup of Q_8 . (*Hint*) \diamond

Now let's see if you can prove some general facts about normal subgroups. We'll start with a warm-up:

Exercise 18.4.6. Prove that for *any* group G , the set $\{e\}$ is a normal subgroup of G (in other words the identity of group is always a normal subgroup). \diamond

This next one often comes in handy.

Proposition 18.4.7. Let G be a group, and let H be a subgroup of G with index 2. Then H is a normal subgroup of G .

Exercise 18.4.8. Prove Proposition 18.4.7 by proving each of the following steps.

- (a) Prove that $G \setminus H$ is a left coset of H in G .
- (b) Prove that $G \setminus H$ is a right coset of H in G .
- (c) Prove that H is normal in G .

\diamond

Exercise 18.4.9. Prove that any subgroup of an abelian group is normal. (*Hint*) \diamond

Here's an alternative way to characterize normal subgroups:

Proposition 18.4.10. Let H be a subgroup of G . Then H is normal iff every left coset of H is also a right coset of H .

Exercise 18.4.11. Prove Proposition 18.4.10. \diamond

The following proposition can be useful when trying to prove that a certain subgroup is normal. It gives several different characterizations of normal subgroups.

Proposition 18.4.12. Let G be a group and N be a subgroup of G . Then the following statements are equivalent.

1. The subgroup N is normal in G .
2. For all $g \in G$, $gNg^{-1} \subset N$.
3. For all $g \in G$, $gNg^{-1} = N$.

PROOF. (1) \Rightarrow (2). Since N is normal in G , $gN = Ng$ for all $g \in G$. Hence, for a given $g \in G$ and $n \in N$, there exists an n' in N such that $gn = n'g$. Therefore, $gng^{-1} = n' \in N$ or $gNg^{-1} \subset N$.

(2) \Rightarrow (3). Let $g \in G$. Since $gNg^{-1} \subset N$, we need only show $N \subset gNg^{-1}$. For $n \in N$, $g^{-1}ng = g^{-1}n(g^{-1})^{-1} \in N$. Hence, $g^{-1}ng = n'$ for some $n' \in N$. Therefore, $n = gn'g^{-1}$ is in gNg^{-1} .

(3) \Rightarrow (1). Suppose that $gNg^{-1} = N$ for all $g \in G$. Then for any $n \in N$ there exists an $n' \in N$ such that $gng^{-1} = n'$. Consequently, $gn = n'g$ or $gN \subset Ng$. Similarly, $Ng \subset gN$. \square

Proposition 18.4.12 enables us to formulate an alternative definition for normal subgroups:

Definition 18.4.13. Given a group G , a subgroup $H \subset G$ is called a **normal subgroup** if for every $g \in G$ and for every $h \in H$, we have that $ghg^{-1} \in H$. \triangle

Exercise 18.4.14. Define the set gHg^{-1} as follows: $gHg^{-1} = \{ghg^{-1}, h \in H\}$. Show that Definition 18.4.13 is equivalent to the condition that $gHg^{-1} = H$. \diamond

Exercise 18.4.15. Prove that Definition 18.4.13 is equivalent to Definition 18.4.1. (*Hint*) \diamond

Exercise 18.4.16. We showed in Exercise 15.6.7 that the intersection of two subgroups of the same group is also a subgroup. Show that if the two subgroups are normal, then the intersection is also a normal. \diamond

Exercise 18.4.17. In the following exercises, G is a group and H is a subgroup of G .

- (a) Show that for any $g \in G$ then gHg^{-1} is also a subgroup of G .
- (b) Define a function $f : H \rightarrow gHg^{-1}$ as follows: $f(h) = ghg^{-1}$. Show that f is a bijection, and thus $|H| = |gHg^{-1}|$.
- (c) If a group G has exactly one subgroup H of order k , prove that H is normal in G . (*Hint*)

\diamond

Finally, here's one that will be very useful in the very near future.

Exercise 18.4.18.

- (a) Let $H \subset G$ be a normal subgroup, and let $g \in G, h \in H$. Show that $g^{-1}hg \in H$.
- (b) Let $H \subset G$ be a normal subgroup, and let $g \in G, h \in H$. Use part (a) to show how that there exists an $h' \in H$ such that $hg = gh'$.
- (c) Let $H \subset G$ be a normal subgroup, and suppose $x_1 \in g_1H$ and $x_2 \in g_2H$. Prove that $x_1x_2 \in g_1g_2H$. (*Hint*)

\diamond

18.4.2 Factor groups

So what's the hubbub about these normal subgroups? We've been promising a grand revelation. It turns out that the cosets of normal subgroups have some very special properties.

Example 18.4.19. Consider the normal subgroup $3\mathbb{Z}$ of \mathbb{Z} that we started exploring at the beginning of the chapter. The cosets of $3\mathbb{Z}$ in \mathbb{Z} were

$$\begin{aligned} 0 + 3\mathbb{Z} &= \{\dots, -3, 0, 3, 6, \dots\} \\ 1 + 3\mathbb{Z} &= \{\dots, -2, 1, 4, 7, \dots\} \\ 2 + 3\mathbb{Z} &= \{\dots, -1, 2, 5, 8, \dots\}. \end{aligned}$$

Now just for curiosity's sake, let's say we took *every* element in $0 + 3\mathbb{Z}$ and added them to *every* element in $1 + 3\mathbb{Z}$. What would be the resulting set? Try some examples: take an arbitrary element of $0 + 3\mathbb{Z}$, and add to it an arbitrary element of $1 + 3\mathbb{Z}$. You will find that the result is always in $1 + 3\mathbb{Z}$. Let's give a proof of this. First let's give some notation:

Definition 18.4.20. (*Set addition*) Let A and B be two sets of real numbers. Then the *sum* $A + B$ is defined as the set:

$$A + B := \{a + b, \text{ where } a \in A \text{ and } b \in B\}.$$

△

Notice that we are giving a *new* meaning to the symbol '+', because we are applying it to *sets* rather than *numbers*.

In terms of this new notation, what we're trying to prove is:

$$(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) = 1 + 3\mathbb{Z}.$$

As we've done many times before, we may prove that these two sets are equal by showing that all elements of the left-hand set are contained in the right-hand set, and vice versa. So let's take an arbitrary element of $(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z})$. We may write this element as $(0 + 3m) + (1 + 3n)$, where $m, n \in \mathbb{Z}$. Basic algebra gives us:

$$(0 + 3m) + (1 + 3n) = 1 + 3(m + n),$$

which is in $1 + 3\mathbb{Z}$. This shows that:

$$(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) \subset 1 + 3\mathbb{Z}.$$

On the other hand, we may write an arbitrary element of $1 + 3\mathbb{Z}$ as $1 + 3k$, which is equal to $0 + (1 + 3k)$. Since $0 \in 0 + 3\mathbb{Z}$, we have

$$(0 + 3\mathbb{Z}) + (1 + 3\mathbb{Z}) \supset 1 + 3\mathbb{Z},$$

and the proof is complete.

Let's step back and see what we've done. We've taken one coset of $3\mathbb{Z}$ (i.e. $0 + 3\mathbb{Z}$), and "added" a second coset (i.e. $1 + 3\mathbb{Z}$) to it, to get a third coset of $3\mathbb{Z}$. This sounds like closure. So let's check that we have it. Doing the same thing with all pairs of cosets, we obtain the following "addition" table:

| | | | |
|-------------------|-------------------|-------------------|-------------------|
| + | $0 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ |
| $0 + 3\mathbb{Z}$ | $0 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ |
| $1 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ | $0 + 3\mathbb{Z}$ |
| $2 + 3\mathbb{Z}$ | $2 + 3\mathbb{Z}$ | $0 + 3\mathbb{Z}$ | $1 + 3\mathbb{Z}$ |

So indeed we have closure. It's beginning to look like we have a group here. Actually, we can see an identity ($0 + 3\mathbb{Z}$) and an inverse for every coset (for example $[1 + 3\mathbb{Z}]^{-1} = 2 + 3\mathbb{Z}$). It turns that the associative property also holds: this follows from the associativity of ordinary addition. So we got it: the cosets of $3\mathbb{Z}$ *themselves* form a group! (Note the Cayley table for this group looks suspiciously the same as the Cayley table for \mathbb{Z}_3 ; we'll pick up on this in Chapter 20.) ♦

So *this* is the grand revelation about normal subgroups: *the cosets of a normal subgroup form a group*. But we shouldn't jump the gun: we've only shown it's true for a special case. Now we have to get down to the hard work of proving it in general. First we have to generalize Definition 18.4.20 to other group operations.

Definition 18.4.21. (*Set composition*) Let A and B be two subsets of a group G . Then the **composition** $A \circ B$ (or AB) is defined as the set:

$$A \circ B := \{ab, \text{ where } a \in A \text{ and } b \in B\}.$$

△

The reason that normal subgroups are special is that set composition defines an operation on cosets:

Proposition 18.4.22. Let N be a normal subgroup of a group G . If $a, b \in G$, then $aN \circ bN = abN$.

PROOF. The proof parallels the argument in Example 18.4.19. Let $x \in aN$ and $y \in bN$. Using Exercise 18.4.18 part (c), we may conclude that $xy \in$

abN . This shows that $aN \circ bN \subset abN$. On the other hand, let $z \in abN$. Then $z = ae \circ bn$ for some $n \in N$, which implies that $z \in aN \circ bN$. This shows that $aN \circ bN \supset abN$, and the proof is finished. \square

Proposition 18.4.23. Let N be a normal subgroup of a group G . The cosets of N in G form a group under the operation of set composition.

PROOF. We have shown that the set composition operation is well-defined and closed on the set of cosets of N , provided that N is normal. Associativity follows by the associativity of the group operation defined on G . Using Proposition 18.4.22 we have that $eN \circ aN = aN \circ eN = aN$, so $eN = N$ is an identity. Proposition 18.4.22 also gives us that $g^{-1}N \circ gN = gN \circ g^{-1}N = eN$, so the inverse of gN is $g^{-1}N$. \square

Let's define a special notation for our new discovery.

Definition 18.4.24. If N is a normal subgroup of a group G , then the group of cosets of N under the operation of set composition is denoted as G/N . This group is called the **quotient group** or **factor group** of G and N . \triangle

Note that the order of G/N is $[G : N]$, the number of cosets of N in G .

Remark 18.4.25. In Example 18.4.19 above, the quotient group would have been labeled $\mathbb{Z}/3\mathbb{Z}$. In general, the subgroup $n\mathbb{Z}$ of \mathbb{Z} is normal. The cosets of the quotient group $\mathbb{Z}/n\mathbb{Z}$ then are

$$n\mathbb{Z}; \quad 1 + n\mathbb{Z}; \quad 2 + n\mathbb{Z}; \quad \cdots \quad (n-1) + n\mathbb{Z}.$$

and the sum of the cosets $k + \mathbb{Z}$ and $l + \mathbb{Z}$ is $k + l + \mathbb{Z}$. Notice that we have written our cosets additively, because the group operation is integer addition. \triangle

It is very important to remember that the elements in a quotient group are not the elements of the original group, but *sets of elements* in the original group. As well then, the operation for the quotient group is not the original operation of the group (which was used to compose elements), but a convenient derivative of it that we use to compose sets together. Both of these facts take a second to get use to, so let's practice:

Example 18.4.26. Consider the normal subgroup of S_3 , $H = \{(1), (123), (132)\}$ which we started exploring in Example 18.1.5. The cosets of H in S_3 were

H and $(12)N$. Using the group operation from Definition 18.4.24 to compose these cosets together, the quotient group S_3/N then has the following Cayley table.

| | | |
|---------|---------|---------|
| | N | $(12)N$ |
| N | N | $(12)N$ |
| $(12)N$ | $(12)N$ | N |

Notice that S_3/N is a smaller group than S_3 (2 elements compared to 6 elements). So the quotient group then displays a pared down amount of information about S_3 . Actually, $N = A_3$, the group of even permutations, and $(12)N = \{(12), (13), (23)\}$ is the set of odd permutations. The information captured in G/N is parity; that is, multiplying two even or two odd permutations results in an even permutation, whereas multiplying an odd permutation by an even permutation yields an odd permutation. This information, as well as the Cayley table above, might suggest to you that the quotient group is equivalent to another group we know. Again, we'll pick up on this in the Isomorphisms chapter. \blacklozenge

Now it's your turn:

Exercise 18.4.27. Give the Cayley tables for the following quotient groups:

- | | |
|---|-------------------------------|
| (a) $\mathbb{Z}/4\mathbb{Z}$ | (e) $\mathbb{Z}_6/\{0, 3\}$ |
| (b) $\mathbb{Z}/6\mathbb{Z}$ | (f) $\mathbb{Z}_8/\{0, 4\}$ |
| (c) $\mathbb{Z}_{24}/\langle 8 \rangle$ | (g) $U(8)/\langle 3 \rangle$ |
| (d) $\mathbb{Z}_{20}/\langle 4 \rangle$ | (h) $U(20)/\langle 3 \rangle$ |

\diamond

Example 18.4.28. Consider the dihedral group D_n that we studied in the Symmetries chapter, which was the group of symmetries (rotations and reflections) of a regular n sided polygon. We determined in the latter part of that chapter that D_n was actually generated by the two elements r and s , satisfying the relations

$$\begin{aligned} r^n &= id \\ s^2 &= id \\ srs &= r^{-1}. \end{aligned}$$

Any element of D_n can be written as sr^k for some integer $0 \leq k < n$.

The element r generates the cyclic subgroup of rotations, R_n , of D_n . Since $(sr^k)r(sr^k)^{-1} = sr^k r r^{-k} s = r^{-1} \in R_n$, then by Definition 18.4.13 the group of rotations is a normal subgroup of D_n ; therefore, D_n/R_n is a group. Now there are $2n$ symmetries in D_n and n rotations in R_n ; so Lagrange's theorem tells us the number of cosets, $[D_n : R_n] = \frac{|D_n|}{|R_n|} = \frac{2n}{n} = 2$.

Since R_n , the rotations, are one of the cosets, the reflections must be the other coset. So the group D_n/R_n boils down to two elements, rotations and reflections, described by a 2×2 Cayley table. \blacklozenge

Exercise 18.4.29. Construct the Cayley table for D_n/R_n . \diamond

18.5 Factoring of groups and simple groups

18.5.1 Concepts, definitions, and examples

In the previous section we talked about how a normal subgroup enables us to “factor” a group to obtain two groups with fewer elements (i.e. the group of cosets, and the normal subgroup). This seems quite similar to the idea of factoring positive integers as a product of smaller numbers. In fact, just as with positive integers, the process can be continued. To be precise: suppose that G is a group, and N_1 is a normal subgroup. Suppose further that N_2 is a normal subgroup of N_1 . Then we can “factor” G into three groups, namely G/N_1 , N_1/N_2 , and N_2 . Evidently the process can be continued: if N_2 has a normal subgroup N_3 , then we can “factor” G into four groups: G/N_1 , N_1/N_2 , N_2/N_3 , and N_3 . When does this process end? Eventually, we will reach a group in which the only normal subgroup is the trivial subgroup $\{e\}$. But factoring by $\{e\}$ doesn't give a group with fewer elements, because the number of cosets of the identity in any group G is (by Lagrange's theorem)

$$\frac{|G|}{|\{e\}|} = \frac{|G|}{1} = |G|.$$

Thus factoring a group by $\{e\}$ is kind of like dividing an integer by 1: it doesn't change anything. So a group with no nontrivial normal subgroups is like a prime number: it can't be factored any further. A group with no nontrivial normal subgroups is called a *simple group*. Just like any positive



integer uniquely factors into a product of prime numbers, it turns out that any group can be factored into a series of simple groups, and the factors are (in some sense) unique. There's a beautiful theorem, called the **Jordan-Hölder Theorem**, which characterizes these factors. Unfortunately, the precise statement of the theorem is somewhat involved, so we leave to the interested reader to research this topic further.¹

Exercise 18.5.1.

- (a) For the dihedral group D_5 , find a normal subgroup N such that D_5/N and N are both simple.
- (b) For the dihedral group D_4 , find subgroups N, P such that $P \subset N$ and D_4/N , N/M , and M are all simple groups.
- (c) For the group \mathbb{Z}_6 , find a normal subgroup N such that \mathbb{Z}_6/N and N are both simple. Find also a *different* subgroup M such that \mathbb{Z}_6/M and M are both simple. Show that \mathbb{Z}_6/N is isomorphic to M and \mathbb{Z}_6/M is isomorphic to N . (Recall our discussion of “isomorphic” in Section 14.2.2.) This exercise shows that although the factors of a group are unique (up to isomorphism), the group may be “broken down” in different ways to obtain the factors.
- (d) For the group S_3 , find a subgroup N such that S_3/N and N are both simple. Show that these groups are isomorphic to the two groups in each factorization in part (c). This shows that although the factors of any group are unique, it's possible to have two different groups with the same factors.

◇

We've been comparing simple groups to prime numbers, but actually they are somewhat more complicated than prime numbers. There are several infinite classes of simple groups (as well as a few simple groups which defy classification—see the Remark at the end of this section.) We've already seen one such class: the groups of prime order. As we noted at the end of Section 18.3, these groups are simple since they have no nontrivial proper subgroups.

¹See for example <http://turnbull.mcs.st-andrews.ac.uk/~colva/topics/ch4.pdf>.

18.5.2 Simplicity of the alternating groups A_n for $n \geq 5$

Let's consider the simplicity question for some other groups. We'll start with the symmetric groups S_n (permutations on n numbers).

Exercise 18.5.2. Show that S_n is not simple for $n \geq 3$. (*Hint*) \diamond

So the S_n 's aren't simple in general. How about the A_n 's?

Exercise 18.5.3.

- (a) Show that A_2 and A_3 are simple.
- (b) Let H be the subset of A_4 consisting of elements which are products of two disjoint transpositions (that is, the cycle structure is two 2-cycles). Show that H is a subgroup of A_4 , and in fact is a normal subgroup of A_4 .

\diamond

Although A_4 is not simple, it turns out that the alternating groups A_n are simple for $n \geq 5$. We will prove this result by looking at properties of 3-cycles. The strategy is to establish the following two facts:

- (1) The only normal subgroup of A_n ($n \geq 3$) that contains a 3-cycle is A_n itself.
- (2) Any nontrivial normal subgroup of A_n ($n \geq 5$) contains a 3-cycle.

Facts (1) and (2) then imply that the only nontrivial normal subgroup of A_n ($n \geq 5$) is A_n itself.

Before we can prove facts (1) and (2), we need first a preliminary result:

Proposition 18.5.4. The alternating group A_n is generated by 3-cycles for $n \geq 3$.

PROOF. We know that any element σ of A_n is an even permutation, so σ can be expressed as the product of an even number of transpositions. In this expression for σ we may pair up the transpositions two by two, and thus obtain an expression for σ as a product of *pairs* of transpositions. Now consider any pair of transpositions. Either the pair has both elements

in common; or the pair has one element in common; or the pair has no elements in common. In other words, the three possibilities for any pair of transpositions are:

$(ab)(ab)$ or $(ab)(bc)$ or $(ab)(cd)$ (where a, b, c, d are all different elements of A_n).

We may write all of these pairs of transpositions as follows:

$$\begin{aligned}(ab)(ab) &= e \\ (ab)(bc) &= (abc) \\ (ab)(cd) &= (abc)(bcd).\end{aligned}$$

By substituting pairs of transpositions in the product expression for σ with equivalent 3-cycle expressions, we may express the arbitrary element $\sigma \in A_n$ as a product of 3-cycles. \square

Before continuing onward with our proof, let's do a few examples to see how this works.

Exercise 18.5.5. Express the following permutations as products of 3-cycles.

(a) $(12)(34)(56)(78)$

(b) $(13)(35)(57)(79)(24)(68)$

(c) $(1357)(2468)$

(d) $(428)(1628)$

\diamond

Armed with Proposition 18.5.4 we're now able to prove fact (1).

Proposition 18.5.6. Let N be a normal subgroup of A_n , where $n \geq 3$. If N contains a 3-cycle, then $N = A_n$.

PROOF. We will first show that A_n is generated by 3-cycles of the specific form (ijk) , where i and j are fixed in $\{1, 2, \dots, n\}$ and we let k vary. Every 3-cycle is the product of 3-cycles of this form, since

$$\begin{aligned}(iaj) &= (ija)^2 \\ (iab) &= (ijb)(ija)^2 \\ (jab) &= (ijb)^2(ija) \\ (abc) &= (ija)^2(jic)(ijb)^2(ija).\end{aligned}$$

Now suppose that N is a nontrivial normal subgroup of A_n for $n \geq 3$ such that N contains a 3-cycle of the form (ija) . Using the normality of N , we see that

$$[(ij)(ak)](ija)^2[(ij)(ak)]^{-1} = (ijk)$$

is in N . Hence, N must contain all of the 3-cycles (ijk) for $1 \leq k \leq n$. By Proposition 18.5.4, these 3-cycles generate A_n ; hence, $N = A_n$. \square

Let's move on to fact (2):

Proposition 18.5.7. For $n \geq 5$, every nontrivial normal subgroup N of A_n contains a 3-cycle.

PROOF. Let σ be an arbitrary element in a normal subgroup N . The possible cycle structures for σ are as follows:

- (i) σ is a 3-cycle.
- (ii) The cycle structure of σ includes an r -cycle where $r > 3$.
- (iii) The cycle structure of σ includes at least two 3-cycles.
- (iv) The cycle structure of σ includes just one 3-cycle and an even number of 2-cycles.
- (v) the cycle structure of σ includes an even number of 2-cycles.

We may treat these cases one by one.

- (i) If σ is a 3-cycle, then we are done.
- (ii) In this case we can write $\sigma = \tau(a_1 a_2 \cdots a_r)$, where $r > 3$ and τ includes cycles that are disjoint from $(a_1 a_2 \cdots a_r)$. Then

$$(a_1 a_2 a_3) \sigma (a_1 a_2 a_3)^{-1}$$

is in N since N is normal. It follows that

$$\sigma^{-1} (a_1 a_2 a_3) \sigma (a_1 a_2 a_3)^{-1}$$

is also in N since N is closed. Now since

$$\begin{aligned} & \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \\ &= \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_3a_2) \\ &= (a_1a_2 \cdots a_r)^{-1}\tau^{-1}(a_1a_2a_3)\tau(a_1a_2 \cdots a_r)(a_1a_3a_2) \\ &= (a_1a_2 \cdots a_r)^{-1}\tau^{-1}(a_1a_2a_3)\tau(a_1a_2 \cdots a_r)(a_1a_3a_2) \\ &= (a_1a_3a_2), \end{aligned}$$

N must contain a 3-cycle; hence, $N = A_n$.

(iii) In this case we may write

$$\sigma = \tau(a_1a_2a_3)(a_4a_5a_6),$$

where the permutation τ consists of cycles that are disjoint from $\{a_1, a_2, a_3, a_4, a_5, a_6\}$. We may argue as in case (ii) that

$$\sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \in N,$$

and may compute

$$\begin{aligned} & \sigma^{-1}(a_1a_2a_4)\sigma(a_1a_2a_4)^{-1} \\ &= [\tau(a_1a_2a_3)(a_4a_5a_6)]^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_2a_4)^{-1} \\ &= (a_4a_6a_5)(a_1a_3a_2)\tau^{-1}(a_1a_2a_4)\tau(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2) \\ &= (a_4a_6a_5)(a_1a_3a_2)(a_1a_2a_4)(a_1a_2a_3)(a_4a_5a_6)(a_1a_4a_2) \\ &= (a_1a_4a_2a_6a_3). \end{aligned}$$

So N contains a disjoint cycle of length greater than 3, and we can apply case (ii) to conclude that N must also contain a 3-cycle.

(iv) In this case we may write $\sigma = \tau(a_1a_2a_3)$, where τ is the product of disjoint 2-cycles. Then $\sigma^2 \in N$ since N is closed, and

$$\begin{aligned} \sigma^2 &= \tau(a_1a_2a_3)\tau(a_1a_2a_3) \\ &= (a_1a_3a_2). \end{aligned}$$

So N contains a 3-cycle.

(v) In this case we may write

$$\sigma = \tau(a_1a_2)(a_3a_4),$$

where τ is the product of an even number of disjoint 2-cycles. We may argue as in case (ii) above that

$$\sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \in N$$

and we compute

$$\begin{aligned} & \sigma^{-1}(a_1a_2a_3)\sigma(a_1a_2a_3)^{-1} \\ &= \tau^{-1}(a_1a_2)(a_3a_4)(a_1a_2a_3)\tau(a_1a_2)(a_3a_4)(a_1a_2a_3)^{-1} \\ &= (a_1a_3)(a_2a_4). \end{aligned}$$

Since $n \geq 5$, we can find $b \in \{1, 2, \dots, n\}$ such that $b \neq a_1, a_2, a_3, a_4$. Let $\mu = (a_1a_3b)$. Then

$$\mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) \in N$$

and

$$\begin{aligned} & \mu^{-1}(a_1a_3)(a_2a_4)\mu(a_1a_3)(a_2a_4) \\ &= (a_1ba_3)(a_1a_3)(a_2a_4)(a_1a_3b)(a_1a_3)(a_2a_4) \\ &= (a_1a_3b). \end{aligned}$$

Therefore, N contains a 3-cycle.

We have thus shown that in all possible cases N contains a 3-cycle, and the proof of the proposition is complete. \square

So finally we may summarize the proof that A_n is simple ($n \geq 5$).

Proposition 18.5.8. The alternating group, A_n , is simple for $n \geq 5$.

PROOF. Let N be a normal subgroup of A_n . By Proposition 18.5.7, N contains a 3-cycle. By Proposition 18.5.6, $N = A_n$; therefore, A_n contains no proper nontrivial normal subgroups for $n \geq 5$. \square

And there we have it, A_n is a simple group for $n \geq 5$. Simple, right? :)

18.5.3 The simplicity of A_n and the impossibility of polynomial root formulas

We've just spent several pages proving that A_n is simple for $n \geq 5$. What's the big deal? It turns out that this fact played a key role in a VERY big deal in the history of mathematics.



Consider any second-degree real polynomial $a_2x^2 + a_1x + a_0$. We may find the roots of the polynomial using the quadratic formula. But what if the polynomial is of degree three ($a_3x^3 + a_2x^2 + a_1x + a_0$) or higher? It turns out there's a formula for finding the roots of an arbitrary real cubic (degree 3) polynomial. There's even a formula for finding the roots of quartic equations. All of these formulas involve arithmetic operations (+, -, ·, /) and radicals (square roots, cube roots, etc.) But how about quintic (fifth order) and higher order polynomials? It turns out that for fifth or higher order polynomials there's no such formula for finding the roots using arithmetic operations and radicals. It's not just that we haven't found one—we can prove that *such a formula is impossible*. Proving this was one of the all-time great discoveries of mathematics, in which Abel, Ruffini, and Galois all played important roles. The theoretical foundations required for this proof are found in an area of abstract algebra known as ***Galois Theory***. You may find chapters on Galois Theory in most advanced undergraduate textbooks on abstract algebra.

An outline of the proof strategy is as follows. Each of the following steps requires extensive proof (which we won't supply), but at least you can see how the argument goes:

- (i) An n th order real polynomial has up to n distinct roots, which may be real or complex and are irrational in general. (This follows from the Fundamental Theorem of Algebra.)
- (ii) Associated with the roots of a given real polynomial is a certain type of symmetry group called the ***Galois group***. For an n th order polynomial, the Galois group is a subgroup of S_n .
- (iii) In order for a formula to exist for a given real polynomial's roots that involves only arithmetic operations and radicals, the Galois group of the polynomial must be factorable in such a way that the factors are all abelian groups. (This is the hardest step.)
- (iv) There are n th order real polynomials that have S_n as their Galois group.
- (v) It isn't possible to factor S_n into abelian factors, since S_n factors into \mathbb{Z}_2 and A_n , and A_n is simple and non-abelian.
- (vi) It follows that there can be no such formula for the roots of such polynomials, so there can't be a root formula that works in general.

Exercise 18.5.9. In this exercise, we give the Galois group for quadratic polynomials, and explore some of its properties. Let $\text{id} : \mathbb{C} \rightarrow \mathbb{C}$ be the identity function: $\text{id}(z) = z$. Let $f : \mathbb{C} \rightarrow \mathbb{C}$ be the conjugation function: $f(z) = \bar{z}$.

- (a) Show that $H = \{\text{id}, f\}$ is a subgroup of the group of all bijections from $\mathbb{C} \rightarrow \mathbb{C}$
- (b) Let S be the set of roots of the real polynomial $a_2x^2 + a_1x + a_0$. Show that H is a group of symmetries for S : that is, $h(S) = S$ for any $h \in H$.
- (c) Show that H factors in such a way that all the factors are abelian simple groups. (It therefore satisfies the criterion for a root solution formula to exist.)

◇

Remark 18.5.10. (*historical background*) It is impossible to overstate the importance of simple groups in mathematics and physics. Groups are the fundamental mathematical tools used to describe the symmetries and regularities which we observe in the physical world—and simple groups, as mentioned in the text, are the building blocks from which all finite groups may be built.

The earliest work on the classification problem dates back over 200 years. The first non-abelian simple groups to be discovered were the alternating groups, and Galois was the first to prove that A_5 was simple. Later mathematicians, such as C. Jordan and L. E. Dickson, found several infinite families of matrix groups that were simple. Other families of simple groups were discovered in the 1950s. Around 1900 William Burnside conjectured that all non-abelian simple groups must have even order. But it wasn't until 1963 that Walter Feit and John Thompson published a 250-page proof of Burnside's conjecture. After this breakthrough, mathematicians redoubled their efforts to complete the classification. Hundreds of mathematicians produced thousands of pages of proofs. Success was announced in 1983, but a gap was later discovered, and it was not until 2004 that one of the great intellectual achievements of all time was finally accomplished. The final result: all finite simple groups belong to 18 countably infinite families, except for 26 exceptional "sporadic" groups. The largest of these groups (called the "monster" has over 80 trillion trillion trillion trillion entries, which is more than 100 times the number of atoms in the earth! ◇



Additional exercises

1. Let T be the multiplicative group of nonsingular upper triangular 2×2 matrices with entries in \mathbb{R} ; that is, matrices of the form

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix},$$

where $a, b, c \in \mathbb{R}$ and $ac \neq 0$. Let U consist of matrices of the form

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

where $x \in \mathbb{R}$.

- Show that U is a subgroup of T .
 - Prove that U is abelian.
 - Prove that U is normal in T .
 - Show that T/U is abelian.
 - Is T normal in $GL_2(\mathbb{R})$?
- If G is abelian, prove that G/H must also be abelian.
 - Prove or disprove: If H is a normal subgroup of G such that H and G/H are abelian, then G is abelian.
 - If G is cyclic, prove that G/H must also be cyclic.
 - Prove or disprove: If H and G/H are cyclic, then G is cyclic.
 - Define the **centralizer** of an element g in a group G to be the set

$$C(g) = \{x \in G : xg = gx\}.$$

Show that $C(g)$ is a subgroup of G . If g generates a normal subgroup of G , prove that $C(g)$ is normal in G .

- Recall that the **center** of a group G is the set

$$Z(G) = \{x \in G : xg = gx \text{ for all } g \in G\}.$$

- Calculate the center of S_3 .
- Calculate the center of $GL_2(\mathbb{R})$.

- (c) Show that the center of any group G is a normal subgroup of G .
- (d) If $G/Z(G)$ is cyclic, show that G is abelian.
8. Let G be a group and let $G' = \{aba^{-1}b^{-1}, a, b \in G\}$; that is, G' is the set of all finite products of elements in G of the form $aba^{-1}b^{-1}$.
- (a) Show that G' is a subgroup of G . G' is called the **commutator subgroup** of G .
- (b) Show that G' is a normal subgroup of G .
- (c) Let N be a normal subgroup of G . Prove that G/N is abelian if and only if N contains the commutator subgroup of G .
9. Use Fermat's little theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.
10. Show that the integers have infinite index in the additive group of rational numbers.
11. Show that the additive group of real numbers has infinite index in the additive group of the complex numbers.
12. What fails in the proof of Proposition 18.2.13 if $\phi : \mathcal{L}_H \rightarrow \mathcal{R}_H$ is defined by $\phi(gH) = Hg$?
13. Suppose that $g^n = e$. Show that the order of g divides n .
14. If $|G| = 2n$, prove that the number of elements of order 2 is odd. Use this result to show that G must contain a subgroup of order 2. (*Hint*)
15. Suppose that $[G : H] = 2$. If $a, b \in G \setminus H$, show that $ab \in H$.
16. If $[G : H] = 2$, prove that $gH = Hg$.
17. Let H and K be subgroups of a group G . Prove that $gH \cap gK$ is a coset of $H \cap K$ in G .
18. Let H and K be subgroups of a group G . Define a relation \sim on G by $a \sim b$ if there exists an $h \in H$ and a $k \in K$ such that $hak = b$. Show that this relation is an equivalence relation. The corresponding equivalence classes are called **double cosets**. In the case where $G = A_4$, compute the double cosets for:
- (a) $H = K = \{(1), (123), (132)\}$.

(b) $H = \{(1), (123), (132)\}$, $K = \{(1), (124), (142)\}$.

19. If G is a group of order p^n where p is prime, show that G must have a proper subgroup of order p . If $n \geq 3$, is it true that G will have a proper subgroup of order p^2 ?
20. Let G be a cyclic group of order n . Show that there are exactly $\phi(n)$ generators for G .
21. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ be the factorization of n into distinct primes. Prove that

$$\phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

22. Show that

$$n = \sum_{d|n} \phi(d)$$

for all positive integers n .

18.6 Hints for “Cosets” exercises

Exercise 18.1.7:

For part (f), consider that any even permutation times A_4 will produce a set of even permutations with 12 elements (Why?), and there are exactly 12 even permutations in S_4 . Similar reasoning applies when you take any odd permutation times A_4 .

For part (g), generalize your result in part (f).

For part (h), your task will be simplified if you notice that all elements in a given coset produce the same coset. So once you’ve found a coset, you don’t need to do any work to find the cosets of elements in the coset that you’ve found.

Exercise 18.1.9: (*Hint*: You’re trying to show that the two sets gH and Hg are equal. One way to do this is to show every element of gH is an element of Hg , and vice versa.)

Exercise 18.2.2(a): The hypothesis $g_1H = g_2H$ implies that there exists $h \in H$ such that $g_1h = g_2e$, where e is the group identity.

Exercise 18.2.2(b): $g_1^{-1}g_2 \in H$ means that $g_1^{-1}g_2 = h$ for some $h \in H$.

Exercise 18.2.2(c): You need to show that $g_2H \subset g_1H$. From (3), deduce that $g_2 = g_1h$ for some $h \in H$. Then, show that any element of the form g_2h' for $h' \in H$ can be expressed as g_1h'' where $h'' \in H$. You should be able to express h'' in terms of h and h' .

Exercise 18.2.2(d): You need to show that (4) implies $g_1H \subset g_2H$. It’s enough to show that for any $h \in H$, $g_1h \in g_2H$. To do this, express g_1 in terms of g_2 .

Exercise 18.2.2(e): Condition (2) implies that $g_1^{-1}g_2 = h$ for some $h \in H$.

Exercise 18.2.14: You may use the equivalence of conditions (3) and (2) in Proposition 18.2.1. You will also need the following facts about determinants: (a) $\det(AB) = \det(A)\det(B)$ and (b) $\det(A^{-1}) = 1/\det(A)$ (note that (b) follows from (a)).

Exercise 18.3.5: Remember cyclic subgroups.

Exercise 18.3.11: For part (g), use the fact that the numbers less than p^2 that are *not* relatively prime to p^2 are $p, 2p, 3p, \dots, (p-1)p$: how many numbers remain? For parts (h) and (i) use a similar logic.

Exercise 18.3.16: You may refer to Proposition 15.5.27.

Exercise 18.4.4: Look back at your work on Exercise 18.2.14.

Exercise 18.4.5: Compute the left and right cosets.

Exercise 18.4.9: Use Exercise 18.1.9 earlier in this chapter.

Exercise 18.4.15: Let H be a subgroup of the group G that satisfies the property that for any $g \in G$ and any $h \in H$, then ghg^{-1} is also in H . Show that every right coset of H in G is also a left coset, and vice versa (and hence H is a normal subgroup of G).

Exercise 18.4.17: Use part (a) and Definition 18.4.13.

Exercise 18.4.18(c): We may write $x_1 = g_1h_1$ and $x_2 = g_2h_2$, so that $x_1x_2 = g_1h_1g_2h_2$. Use part (b) with $h = h_1$, $g = g_2$.

Exercise 18.5.2: S_n has a subgroup of index 2. This shows S_n is not simple (why?).

Additional exercises

Exercise 14: Define an equivalence relation on G as follows: $g_1 \sim g_2$ if and only if either $g_1 = g_2$ or $g_1 = g_2^{-1}$. Prove that this is indeed an equivalence relation; and show that the equivalence class of g has an odd number of elements if and only if $g = g^{-1}$. Use the partition of G to show that there must be an even number of equivalence classes with an odd number of elements (including the equivalence class of the identity).

Error-Detecting and Correcting Codes

In Chapter 9 we looked at cryptography, which is concerned with the encoding of information to make it secret. But coding is used for other purposes as well. When data is transmitted, it is often subject to processes which may corrupt the data and produce transmission errors. This situation arises in many areas of communications, including radio, telephone, television, computer communications, and even compact disc player technology. In order to guarantee accurate communication, the data must be encoded (before transmission) and decoded (after transmission) so that transmission errors can be detected and, if possible, corrected. As you may imagine, some of the world's leading high-tech companies are heavily involved in this area—and breakthroughs can mean big bucks for the discoverers!

Prerequisites: In this chapter we will make extensive use of the group \mathbb{Z}_2^n , which is the direct product of n copies of \mathbb{Z}_2 (direct products were introduced in Section 20.5. The discussion of linear block codes (Section 19.2 and following) uses concepts from linear algebra such as matrix, vector, and matrix multiplication. Section 19.6 uses some basic ideas about cosets, which were introduced in Chapter 18.

Thanks to Tom Judson for material used in this chapter.

19.1 Definitions and basic properties

Let's examine a simple model of a communications system for transmitting and receiving coded messages (Figure 19.1.1). Uncoded messages consist of

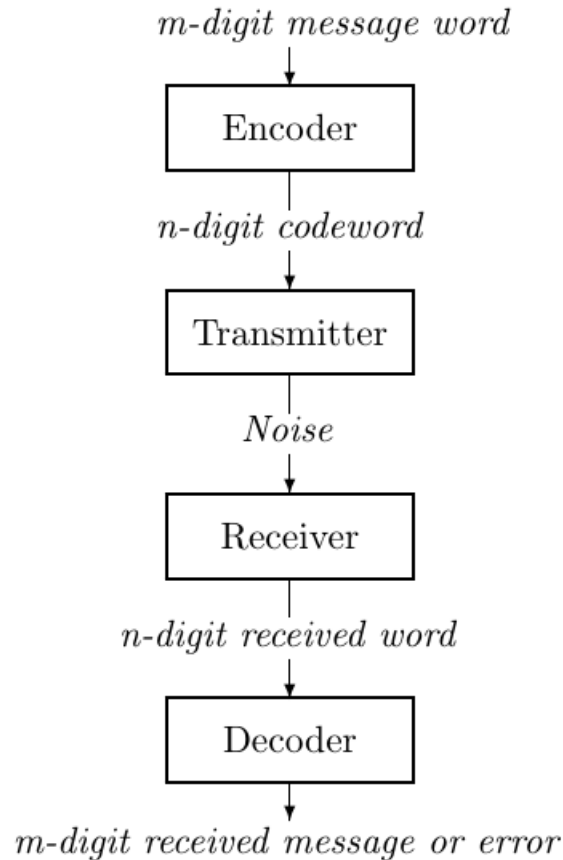


Figure 19.1.1. Encoding and decoding messages

a sequence of symbols, such as letters or characters. Now when computers do calculations they can't understand letters: they can only understand sequences consisting of 0's and 1's (0 and 1 are referred to as binary digits or *bits*). So before coding, individual symbols are re-expressed as sequences of binary bits, and then these bits are strung together to form a single sequence of bits which expresses the message content. This sequence is divided up into chunks (or tuples) of m bits apiece: these binary m -tuples are referred to as *message words*. Message words are then encoded into *codewords* of n bits apiece by a device called an *encoder*. These codewords are transmitted over a channel and received by a receiver. Random noise in this transmission process causes some of the bits to be corrupted: and

we say that an *error* occurs every time a bit is changed from 0 to 1 or vice-versa due to transmission noise. The *decoder* converts each received n -tuple into a message word or gives an error message for that n -tuple. If the received codeword was not corrupted by random noise during transmission, then the decoded message word will agree with the original message word. For received words that are not codewords, the decoding scheme will give an error indication, or (in the case of error-correcting codes) will try to correct the error and reconstruct the original message word. The goal is to transmit error-free messages as cheaply and quickly as possible.

Exercise 19.1.1. Why is the following encoding scheme not acceptable?

| | | | | | | | | | |
|--------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| Information: | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Codeword: | 000 | 001 | 010 | 011 | 101 | 110 | 111 | 000 | 001 |

◇

Example 19.1.2. *Even parity* is a commonly used coding scheme, which (as we shall see) can be generalized to form powerful and versatile codes. Computers use the ASCII (American Standard Code for Information Interchange) coding system to encode the letters and special characters that appear on your keyboard (these may be considered as the "message words", according to the above terminology). There are 128 of these characters, so it is possible to represent them using 7 bits (since $128 = 2^7$). For example, the 7-bit representations for A, B, and C are

$$\begin{aligned} A &= 1000001, \\ B &= 1000010, \\ C &= 1000011. \end{aligned}$$

Although 7 bits are sufficient, the ASCII code uses 8 bits for each character. A bit is added to the front of the codeword according to the following rule: if the number of 1's in the seven-bit representation is even, then the front bit is 0; otherwise, the front bit is 1. According to this rule, the 8-bit codes for A, B, and C now become

$$\begin{aligned} A &= && 01000001, \\ B &= && 01000010, \\ C &= && 11000011. \end{aligned}$$

Notice that these 8-bit codes all have an *even* number of 1's.

Now suppose an A is sent and a transmission error in the sixth bit is caused by noise over the communication channel so that (01000101) is received. We know an error has occurred since the received word has an odd number of 1's, and we can now request that the codeword be transmitted again. When used for error checking, the leftmost bit is called a *parity check bit*.

Adding a parity check bit allows the detection of all single errors because changing a single bit either increases or decreases the number of 1's by one, and in either case the parity has been changed from even to odd, so the new word is not a codeword. (We could equally well construct an error detection scheme based on *odd parity*, where the parity check bit is set so that codewords always have an odd number of 1's.) \blacklozenge

The even parity system is easy to implement, but has two drawbacks. First, multiple errors are not detectable. Suppose an A is sent and the first and seventh bits are changed from 0 to 1. The received word is a codeword, but will be decoded into a C instead of an A. Second, we do not have the ability to correct errors. If the 8-tuple (10011000) is received, we know that an error has occurred, but we have no idea which bit has been changed. We will now investigate a coding scheme that will not only allow us to detect transmission errors but will actually correct the errors.

Example 19.1.3. Suppose that our original message is either a 0 or a 1, and that 0 encodes to (000) and 1 encodes to (111). If only a single error occurs during transmission, we can detect and correct the error. For example, if a 101 is received, then the second bit must have been changed from a 1 to a 0. The originally transmitted codeword must have been (111). This method will detect and correct all single errors.

In Table 19.1, we present all possible words that might be received for the transmitted codewords (000) and (111). Table 19.1 also shows the number of bits by which each received 3-tuple differs from each original codeword.

This triple-repetition method will automatically detect and correct all single errors, but it's not very efficient (just imagine having to repeat everything you say three times in order to make yourself understood!) We'll see shortly that there are much better alternatives. \blacklozenge

| | | Received Word | | | | | | | |
|-------------|-----|---------------|-----|-----|-----|-----|-----|-----|-----|
| | | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |
| Transmitted | 000 | 0 | 1 | 1 | 2 | 1 | 2 | 2 | 3 |
| Codeword | 111 | 3 | 2 | 2 | 1 | 2 | 1 | 1 | 0 |

Table 19.1: A repetition code

19.2 Block Codes

In the examples we've seen so far, all message words are the same size, and all codewords are the same size (but message words and code words could be of different sizes, as in Example 19.1.3). This is certainly not the only possibility. For instance, we could encode different message words with codewords of differing sizes. Alternatively, we could use some kind of scheme which doesn't break the message into words at all. Such coding schemes have extremely important practical uses. Nonetheless, we will focus on the simple case where message words all have equal size, and all codewords also have equal size. These are called "block codes", because both the original and encoded message are divided into "blocks" (e.g. codewords) of fixed size, and encoding /decoding proceeds block by block. We shall see shortly that group theory can be used to design block codes with very nice properties.

We begin with a formal definition of block code, which generalizes the examples discussed in the previous section. In the following, the notation \mathbb{Z}_2^m denotes the set of binary m -tuples.

Definition 19.2.1. a (n, m) **block code** consists of a one-to-one **encoding function**

$$E : \mathbb{Z}_2^m \rightarrow \mathbb{Z}_2^n$$

and an onto **decoding function**

$$D : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^m.$$

The functions E and D satisfy $D \circ E(z) = z$ for any $z \in \mathbb{Z}_2^m$ (in other words, $D \circ E$ is the identity function on the set \mathbb{Z}_2^m).

We refer to the elements of the domain of E as **message words**, and elements of the range of E as **codewords**. \triangle

Remark 19.2.2. In Definition 19.2.1, the encoding function E for a block code is required to be one-to-one so that two different message words are

never assigned to the same codeword (which would make decoding impossible). On the other hand, the decoding function D is required to be onto so that any encoded message can be decoded (although the decoded message may have errors). \triangle

Exercise 19.2.3.

- (a) Explain why the definition requires that $D \circ E$ is the identity function on the domain of E . (In other words, what property of encoding and decoding does this guarantee?)
- (b) Show that the condition $D \circ E = \text{id}$ implies that D is onto (in other words, to prove that D is a decoding function it's enough to prove that $D \circ E = \text{id}$, and you don't have to prove onto-ness separately).
- (c) Show that in Example 19.1.3, it is not true that $E \circ D$ is the identity function on the domain of D .
- (d) Suppose that E and D are encoding and decoding functions for an error-correcting code. Prove that $E \circ D$ is *not* equal to the identity function on the domain of D .
- (e) Prove that for an error-correcting code, E and D are not inverse of each other.

\diamond

Exercise 19.2.4. According to Definition 19.2.1, is it possible to have a (n, m) block code where $n > m$? Is $m > n$ possible? *Explain* your answer. \diamond

Example 19.2.5. The even-parity coding system developed to detect single errors in ASCII characters is an $(8, 7)$ -block code. The encoding function is

$$E(x_7, x_6, \dots, x_1) = (x_8, x_7, \dots, x_1),$$

where $x_8 = x_7 + x_6 + \dots + x_1$ (the addition here is in \mathbb{Z}_2).

One possible decoding function takes the 8-bit codeword and removes the front bit:

$$D(x_8, x_7, x_6, \dots, x_1) = (x_7, \dots, x_1).$$

This is a natural choice of decoding function, but it's not the only possibility, as you will explore in the following exercise. There are several other possible decoding functions as well. ♦

Exercise 19.2.6.

- (a) Show that the function $D(x)$ given above is a decoding function (remember that based on Exercise 19.2.3(b) it's enough to prove that $D \circ E = \text{id}$).
- (b) Prove that the following function is also a decoding function for the even parity code:

$$D(x_8, x_7, x_6, \dots, x_1) = (x_8 + x_6 + \dots + x_1, x_6, \dots, x_1) \quad (\text{addition in } \mathbb{Z}_2).$$

- (c) Give two more possible decoding functions for the even parity code.

♦

Exercise 19.2.7.

- (a) Consider an even-parity coding system in which codewords have k bits.
- (b) Is the code a block code? If so, what are the parameters n and m ?
- (c) What is the encoding function?
- (d) Give two possible decoding functions.

♦

In order to characterize error detection and correction properties of codes, we need to quantify the degree of “similarity” between code words, since two code words that are similar are liable to be mistaken for each other. This leads naturally to the idea of “distance” between code words, defined as follows.

Definition 19.2.8. Let $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ be binary n -tuples. The **Hamming distance** or **distance**, $d(\mathbf{x}, \mathbf{y})$ between \mathbf{x} and \mathbf{y} is the number of bit positions where \mathbf{x} and \mathbf{y} differ. The distance between

two codewords is the minimum number of transmission errors required to change one codeword into the other. The *minimum distance* for a code, d_{\min} is the minimum of all distances $d(\mathbf{x}, \mathbf{y})$, where \mathbf{x} and \mathbf{y} are distinct codewords. The *weight*, $w(\mathbf{x})$ of a binary codeword \mathbf{x} is the number of 1's in \mathbf{x} . It follows that $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$, where $\mathbf{0} = (00 \cdots 0)$, since \mathbf{x} differs from $\mathbf{0}$ in exactly its '1' bits. \triangle

Example 19.2.9. Let $\mathbf{x} = (10101)$, $\mathbf{y} = (11010)$, and $\mathbf{z} = (00011)$ be all of the codewords in some code C . Then we have the following Hamming distances:

$$\begin{aligned}d(\mathbf{x}, \mathbf{y}) &= 4, \\d(\mathbf{x}, \mathbf{z}) &= 3, \\d(\mathbf{y}, \mathbf{z}) &= 3.\end{aligned}$$

The minimum distance for this code is 3. We also have the following weights:

$$\begin{aligned}w(\mathbf{x}) &= 3, \\w(\mathbf{y}) &= 3, \\w(\mathbf{z}) &= 2.\end{aligned}$$

◆

Exercise 19.2.10. Compute the Hamming distances between the following pairs of n -tuples.

- | | |
|------------------------|---|
| (a) (011010), (011100) | (b) (11110101), (01010100) ◆ |
| (c) (00110), (01111) | (d) (1001), (0111) |

Exercise 19.2.11. Compute the weights of the following n -tuples.

- | | |
|--------------|----------------|
| (a) (011010) | (b) (11110101) |
| (c) (01111) | (d) (1011) |

◆

Exercise 19.2.12. What is the minimum distance for each of the following block codes?

1. (011010) (011100) (110111) (110000)
2. (011100) (011011) (111011) (100011)
(000000) (010101) (110100) (110011)
3. (000000) (011100) (110101) (110001)
4. (0110110) (0111100) (1110000) (1111111)
(1001001) (1000011) (0001111) (0000000)

◇

The weights in a particular block code are usually much easier to compute than the Hamming distances between all codewords in the code. As we shall see later, if a code is set up carefully then we can use this fact to our advantage.

In order to prove statements about Hamming distance and weight, it is useful to have a concrete formula for the distance between two codewords. Such a formula is given in the following proposition.

Proposition 19.2.13. Let $\mathbf{x} = (x_1, \dots, x_n)$ and $\mathbf{y} = (y_1, \dots, y_n)$ be binary n -tuples. Then the Hamming distance $d(\mathbf{x}, \mathbf{y})$ may be computed by the following formula:

$$d(\mathbf{x}, \mathbf{y}) = (x_1 \oplus y_1) + \dots + (x_n \oplus y_n),$$

where “ \oplus ” denotes addition mod 2 and “+” denotes ordinary addition. Using summation notation, the formula can also be written

$$d(\mathbf{x}, \mathbf{y}) = \sum_{j=1}^n x_j \oplus y_j.$$

PROOF. For each j , we have the 4 possibilities for x_j and y_j shown in Table 19.2. The table shows that $x_j \oplus y_j = 0$ when $x_j = y_j$, and $x_j \oplus y_j = 1$ when $x_j \neq y_j$. So if we sum these terms for all j , we obtain the number of bit positions where \mathbf{x} and \mathbf{y} differ, which by definition is $d(\mathbf{x}, \mathbf{y})$. □

We have been referring to $d(\mathbf{x}, \mathbf{y})$ as “Hamming distance”. To justify this terminology, we will prove that the function $d(\dots)$ does indeed possess the properties that we usually associate with a notion of “distance”:

Proposition 19.2.14. Let \mathbf{x} , \mathbf{y} , and \mathbf{z} be binary n -tuples. Then

| x_j | y_j | $x_j \oplus y_j$ |
|-------|-------|------------------|
| 0 | 0 | 0 |
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 0 |

Table 19.2: Bit sums (mod 2)

- (a) $d(\mathbf{x}, \mathbf{y}) \geq 0$, and $d(\mathbf{x}, \mathbf{y}) = 0$ exactly when $\mathbf{x} = \mathbf{y}$;
- (b) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{y}, \mathbf{x})$;
- (c) $d(\mathbf{x}, \mathbf{y}) \leq d(\mathbf{x}, \mathbf{z}) + d(\mathbf{z}, \mathbf{y})$.

In higher mathematics, any function that satisfies the properties listed in Proposition 19.2.14 is called a *metric*.

Exercise 19.2.15. Using the formula in Proposition 19.2.13, prove the statements in Proposition 19.2.14. \diamond

In order to see how distance relates to error correction, consider the case where $\mathbf{x} = (1101)$ and $\mathbf{y} = (1100)$ are codewords in some code. If we transmit (1101) and an error occurs in the rightmost bit, then (1100) will be received. Since (1100) is a codeword, the decoder will decode (1100) as the transmitted message. This code is clearly not very appropriate for error detection. The problem is that $d(\mathbf{x}, \mathbf{y}) = 1$, so a single-bit error can change one codeword into a different codeword.

On the other hand, given the two codewords $\mathbf{x} = (1100)$ and $\mathbf{y} = (1010)$ then $d(\mathbf{x}, \mathbf{y}) = 2$. If \mathbf{x} is transmitted and a single error occurs, then no matter which bit is in error it's still impossible for \mathbf{y} to be received. If for example the third bit is mistransmitted and received word is (1110) , then we can tell something is wrong – that is, we can detect that an error has taken place. In general, single-bit errors are detectable in any code where the distance between any two codewords is bigger than 1.

Example 19.2.16. Consider the $(4, 3)$ code in which the first three bits carry information and the fourth is an even parity check bit. (Note that now we're putting the parity bit on the *right* instead of on the *left* as we did in Example 19.1.2. This will turn out to be more useful in the development

of the general theory.) Table 19.3 gives the distances between all codewords in this code. We can see that the minimum distance here is 2; hence, the code is suitable as a single error-detecting code.

| | 0000 | 0011 | 0101 | 0110 | 1001 | 1010 | 1100 | 1111 |
|------|------|------|------|------|------|------|------|------|
| 0000 | 0 | 2 | 2 | 2 | 2 | 2 | 2 | 4 |
| 0011 | 2 | 0 | 2 | 2 | 2 | 2 | 4 | 2 |
| 0101 | 2 | 2 | 0 | 2 | 2 | 4 | 2 | 2 |
| 0110 | 2 | 2 | 2 | 0 | 4 | 2 | 2 | 2 |
| 1001 | 2 | 2 | 2 | 4 | 0 | 2 | 2 | 2 |
| 1010 | 2 | 2 | 4 | 2 | 2 | 0 | 2 | 2 |
| 1100 | 2 | 4 | 2 | 2 | 2 | 2 | 0 | 2 |
| 1111 | 4 | 2 | 2 | 2 | 2 | 2 | 2 | 0 |

Table 19.3: Distances between 4-bit codewords



Let's generalize based on this example. Given codewords \mathbf{x} and \mathbf{y} :

- If $d(\mathbf{x}, \mathbf{y}) = 1$ and an error occurs where \mathbf{x} and \mathbf{y} differ, then \mathbf{x} is changed to \mathbf{y} . The received codeword is \mathbf{y} and no error message is given.
- If $d(\mathbf{x}, \mathbf{y}) = 2$, then a single error can't change \mathbf{x} to \mathbf{y} . Therefore, if $d_{\min} = 2$, we have the ability to detect single errors. However, suppose that $d(\mathbf{x}, \mathbf{y}) = 2$, \mathbf{y} is sent, and a noncodeword \mathbf{z} is received such that

$$d(\mathbf{x}, \mathbf{z}) = d(\mathbf{y}, \mathbf{z}) = 1.$$

Then the decoder can't decide between \mathbf{x} and \mathbf{y} . Even though we are aware that an error has occurred, we do not know what the error is.

- If $d_{\min} \geq 3$, then using the same reasoning it follows that we can detect errors of up to two bits.

Furthermore, the maximum-likelihood decoding scheme *corrects* all single errors. Starting with a codeword \mathbf{x} , an error in the transmission of a single bit gives \mathbf{y} with $d(\mathbf{x}, \mathbf{y}) = 1$, but $d(\mathbf{z}, \mathbf{y}) \geq 2$ for any other codeword $\mathbf{z} \neq \mathbf{x}$. Hence the correct codeword is the closest, and will be selected by the decoding scheme.

This line of reasoning leads us to the following general proposition.

Proposition 19.2.17. Let C be a code with $d_{\min} = 2n + 1$. Then C can correct any n or fewer errors. Furthermore, any $2n$ or fewer errors can be detected in C .

PROOF. Suppose that a codeword \mathbf{x} is sent and the word \mathbf{y} is received with at most n errors. Then $d(\mathbf{x}, \mathbf{y}) \leq n$. If \mathbf{z} is any codeword other than \mathbf{x} , then

$$2n + 1 \leq d(\mathbf{x}, \mathbf{z}) \leq d(\mathbf{x}, \mathbf{y}) + d(\mathbf{y}, \mathbf{z}) \leq n + d(\mathbf{y}, \mathbf{z}).$$

Hence, $d(\mathbf{y}, \mathbf{z}) \geq n + 1$ and \mathbf{y} will be correctly decoded as \mathbf{x} . Now suppose that \mathbf{x} is transmitted and \mathbf{y} is received and that at least one error has occurred, but not more than $2n$ errors. Then $1 \leq d(\mathbf{x}, \mathbf{y}) \leq 2n$. Since the minimum distance between codewords is $2n + 1$, \mathbf{y} can't be a codeword. Consequently, the code can detect between 1 and $2n$ errors. \square

Example 19.2.18. In Table 19.4, the codewords $\mathbf{c}_1 = (00000)$, $\mathbf{c}_2 = (00111)$, $\mathbf{c}_3 = (11100)$, and $\mathbf{c}_4 = (11011)$ determine a single error-correcting code. \blacklozenge

| | 00000 | 00111 | 11100 | 11011 |
|-------|-------|-------|-------|-------|
| 00000 | 0 | 3 | 3 | 4 |
| 00111 | 3 | 0 | 4 | 3 |
| 11100 | 3 | 4 | 0 | 3 |
| 11011 | 4 | 3 | 3 | 0 |

Table 19.4: Hamming distances for an error-correcting code

Exercise 19.2.19. What are the error detection and correction capabilities for the codes given in Exercise 19.2.12? \diamond

Exercise 19.2.20. Suppose that a block code C has a minimum weight of 7. What are the error-detection and error-correction capabilities of C ? \diamond

Exercise 19.2.21. Construct a $(5, 2)$ -block code. Discuss the error-detection and error-correction capabilities of your code. \diamond

19.3 Group codes

So far in this book, we've tried to relate everything we've talked about to groups. Codes are no exception to this rule! In fact, we know that all codewords of length n are elements of \mathbb{Z}_2^n , which in fact turns out to be a group. To show this, we must first define a group operation:

Definition 19.3.1. The group \mathbb{Z}_2^n consists of the set of all binary n -tuples, together with an operation “+” defined as follows:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 \oplus y_1, \dots, x_n \oplus y_n),$$

where “ \oplus ” means addition mod 2. △

Remark 19.3.2. Please note that in the following, if \mathbf{x} and \mathbf{y} are binary n -tuples then the expression $\mathbf{x} + \mathbf{y}$ *always* refers to the operation “+” defined in Definition 19.3.1 rather than ordinary addition. This is just one more example of the fact that in mathematics, the meaning of symbols is determined by the context. △

So it's time to get our hands dirty and verify that \mathbb{Z}_2^n is indeed a group.

Exercise 19.3.3.

- (a) Show that if \mathbf{x} and \mathbf{y} are in \mathbb{Z}_2^n , then $\mathbf{x} + \mathbf{y}$ is also in \mathbb{Z}_2^n .
- (b) What is the identity of \mathbb{Z}_2^n under the + operation?
- (c) In \mathbb{Z}_2^9 , what is $(11000101) + (11000101)$?
- (d) If $\mathbf{x} \in \mathbb{Z}_2^n$, then what is $\mathbf{x} + \mathbf{x}$?
- (e) Explain why the above results show that \mathbb{Z}_2^n is a group under the operation +.
- (f) Is the group abelian? *Prove* your answer.

◇

Exercise 19.3.4. We may define a subtraction operation on \mathbb{Z}_2^n as we usually do on additive groups: namely, $\mathbf{x} - \mathbf{y}$ is defined as $\mathbf{x} + \mathbf{y}'$, where \mathbf{y}'

is the additive inverse of \mathbf{y} . Based on the previous exercise, what can you conclude about the difference between $\mathbf{x} - \mathbf{y}$ and $\mathbf{x} + \mathbf{y}$? \diamond

It turns out that weight and Hamming distance are in some sense “compatible” with the operation $+$ defined on \mathbb{Z}_2^n , as shown in the following proposition.

Proposition 19.3.5. Let \mathbf{x} , \mathbf{y} , and \mathbf{z} be binary n -tuples. Then

- (a) $w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0})$
- (b) $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} + \mathbf{y})$
- (c) $d(\mathbf{x}, \mathbf{y}) = d(\mathbf{x} + \mathbf{z}, \mathbf{y} + \mathbf{z})$

We have already shown (a) in the definition of weight (Definition 19.2.8). Parts (b) and (c) are for you to prove:

Exercise 19.3.6.

- (a) Prove part (b) of Proposition 19.3.5 by using part (a) of Proposition 19.3.5 and the formula in Proposition 19.2.13.
- (b) Prove part (c) (*Hint*)

\diamond

The codes we discussed in Section 19.1 were all subsets of \mathbb{Z}_2^n , for some positive integer n . We shall now see that codes that are also *subgroups* have special properties that enable efficient encoding and decoding. Accordingly, we define:

Definition 19.3.7. A *group code* is a set of codewords that is also a subgroup of \mathbb{Z}_2^n . \triangle

Remark 19.3.8. At this point we are simply thinking of a group code as a set of codewords with certain properties. Of course, practical codes also require encoding and decoding functions: we’ll talk about these later. \triangle

To check that a set of codewords is a group code, we need only verify closure under addition. It turns out that identity and inverse are guaranteed by closure:

Exercise 19.3.9.

- (a) Show that a set of codewords in \mathbb{Z}_2^n which is closed under the operation $+$ must also contain $\mathbf{0}$
- (b) Show that any set of codewords always includes the inverses of those codewords.
- (c) Prove that any set of codewords of length n that is closed under $+$ is a subgroup of \mathbb{Z}_2^n .

◇

Exercise 19.3.10. Without doing any addition, explain why the following set of 4-tuples in \mathbb{Z}_2^4 can't be a group code.

$$(0110) \quad (1001) \quad (1010) \quad (1100)$$

◇

Example 19.3.11. Suppose that we have a code that consists of the following 7-tuples:

$$\begin{array}{cccc} (0000000) & (0001111) & (0010101) & (0011010) \\ (0100110) & (0101001) & (0110011) & (0111100) \\ (1000011) & (1001100) & (1010110) & (1011001) \\ (1100101) & (1101010) & (1110000) & (1111111). \end{array}$$

It's possible to verify directly (for instance, by computing the Cayley table) that this code is a group code (later we will show there are much, much quicker ways to do this). To find the minimum distance, one may compute the distances between all pairs of codewords. The result is $d_{\min} = 3$, so the code can detect 2 errors and correct 1 error. ◆

From the previous example, it seems like finding the error detection/correction capabilities of a code is a long and tedious process. However, for group codes there is a far simpler way:

Proposition 19.3.12. Let d_{\min} be the minimum distance for a group code C . Then d_{\min} is the minimum weight of all nonzero codewords in C . That is,

$$d_{\min} = \min\{w(\mathbf{x}) : \mathbf{x} \neq \mathbf{0}\}.$$

PROOF. Observe that

$$\begin{aligned} d_{\min} &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} \neq \mathbf{y}\} \\ &= \min\{d(\mathbf{x}, \mathbf{y}) : \mathbf{x} + \mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{x} + \mathbf{y}) : \mathbf{x} + \mathbf{y} \neq \mathbf{0}\} \\ &= \min\{w(\mathbf{z}) : \mathbf{z} \neq \mathbf{0}\}. \end{aligned}$$

□

Warning 19.3.13. Proposition 19.3.12 *only* applies to *group codes*, and not to codes in general. \diamond

19.4 Linear Block Codes

Using Proposition 19.3.12, it is now a simple matter to find the error detection and correction capabilities of a group code. However, so far we don't have a good method for creating group codes. In this section, we will use some techniques from linear algebra to give one such method. This method is widely used in digital information processing: for instance, in CDs, DVDs, and satellite communications.

To understand this section, readers should familiar with basic notions of linear algebra such as systems of linear equations, vectors, linear combination, matrix multiplication, and transpose. Readers may find a brief refresher on matrix multiplication in Chapter 10.

Definition 19.4.1. The *inner product* of two binary n -tuples is

$$(x_1, x_2, \dots, x_n) \cdot (y_1, y_2, \dots, y_n) \equiv x_1y_1 + \dots + x_ny_n \pmod{2}.$$

For example, $(011001) \cdot (110101) = 0 + 1 + 0 + 0 + 0 + 1 \equiv 0 \pmod{2}$.

(The astute reader will recognize this definition from our discussion of UPC codes in Section 5.3). \triangle

Note the difference between inner product and weight. When computing the weight of a codeword, the entries are added using ordinary addition. However, when computing the inner product in \mathbb{Z}_2^n , the terms are added with mod 2 addition.

We can also look at an inner product as the matrix product of a row vector with a column vector. Recall that transpose (denoted by “T”) changes a row vector into a column vector with the same entries in the same order. Then we have

$$\begin{aligned} \mathbf{x} \cdot \mathbf{y} &= \mathbf{xy}^T \\ &= (x_1 \ x_2 \ \cdots \ x_n) \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \\ &= x_1y_1 + x_2y_2 + \cdots + x_ny_n. \end{aligned}$$

Again, we emphasize the addition here is mod 2 addition.

Example 19.4.2. Suppose that the words to be encoded consist of all binary 3-tuples, and that our encoding scheme is even-parity. To encode an arbitrary 3-tuple, we add a fourth bit to obtain an even number of 1’s. Notice that an arbitrary n -tuple $\mathbf{x} = (x_1, x_2, \dots, x_n)$ has an even number of 1’s exactly when $x_1 + x_2 + \cdots + x_n = 0$; hence, a 4-tuple $\mathbf{x} = (x_1, x_2, x_3, x_4)$ has an even number of 1’s if $x_1 + x_2 + x_3 + x_4 = 0$, or

$$\mathbf{1} \cdot \mathbf{x} = \mathbf{1x}^T = (1 \ 1 \ 1 \ 1) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = 0.$$

◆

Example 19.4.2 shows that an even-parity codeword can be verified by an inner product, which is a special case of a matrix multiplication. We will now show that codewords in other types of group codes can also be verified by matrix multiplication. But first, as usual, a definition:

Definition 19.4.3. Let $\mathbb{M}_{k \times n}(\mathbb{Z}_2)$ denote the set of all $k \times n$ matrices with entries in \mathbb{Z}_2 . We do matrix operations as usual except that all our addition and multiplication operations occur in \mathbb{Z}_2 . Define the *null space*

of a matrix $H \in \mathbb{M}_{k \times n}(\mathbb{Z}_2)$ to be the set of all binary n -tuples \mathbf{x} such that $H\mathbf{x}^T = \mathbf{0}$. We denote the null space of a matrix H by $\text{Null}(H)$. \triangle

Example 19.4.4. Suppose that

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

For a 5-tuple $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5)$ to be in the null space of H it must satisfy $H\mathbf{x}^T = \mathbf{0}$.

This means that,

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

So the following system of equations must be satisfied (note that “+” is binary addition):

$$\begin{aligned} x_2 + x_4 &= 0 \\ x_1 + x_2 + x_3 + x_4 &= 0 \\ x_3 + x_4 + x_5 &= 0. \end{aligned}$$

This set of equations may be solved using conventional methods such as substitution or elimination (remember to use binary arithmetic!). Since there are more variables than equations, there is more than one solution. Here we use Gaussian elimination to obtain our solutions.

First we have,

$$\begin{aligned} x_2 + x_4 &= 0 \\ x_1 + x_2 + x_3 + x_4 &= 0 \\ x_3 + x_4 + x_5 &= 0 \end{aligned}$$

Then we switch the first and second equations to obtain the following system.

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_2 + x_4 &= 0 \\ x_3 + x_4 + x_5 &= 0 \end{aligned}$$

Then we replace the first equation with the sum of the first two equations.

$$\begin{aligned}x_1 + x_3 &= 0 \\x_2 + x_4 &= 0 \\x_3 + x_4 + x_5 &= 0\end{aligned}$$

Finally, we replace the first equation with the sum of the first and third equations to obtain the following system.

$$\begin{aligned}x_1 + x_4 + x_5 &= 0 \\x_2 + x_4 &= 0 \\x_3 + x_4 + x_5 &= 0.\end{aligned}$$

Solving for x_1 , x_2 , and x_3 we have the following dependent solutions,

$$\begin{aligned}x_1 &= -x_4 + (-x_5) \\x_2 &= -x_4 \\x_3 &= -x_4 + (-x_5).\end{aligned}$$

Now since we are working in \mathbb{Z}_2^5 , $-1 \equiv 1$. Therefore, we have the following dependent equations.

$$\begin{aligned}x_1 &= x_4 + x_5 \\x_2 &= x_4 \\x_3 &= x_4 + x_5.\end{aligned}$$

Notice that x_1 and x_3 both depend on x_4 and x_5 . Also x_2 depends on x_4 . In this case, x_1 , x_2 , and x_3 are called *pivot variables* and x_4 and x_5 are called *free variables*. The free variables can take on values of 0 or 1, since we are working in \mathbb{Z}_2^5 . Because the free variables can take on two values, the number of solutions is equal to 2^k , where k is the number of free variables. So we should get four solutions.

If $x_4 = 1$ and $x_5 = 1$, then we substitute those values into our system and use binary addition to find that $x_1 = 0$, $x_2 = 1$, and $x_3 = 0$. So one solution is $(x_1, x_2, x_3, x_4, x_5) = (0, 1, 0, 1, 1)$. Likewise, if $x_4 = 1$ and $x_5 = 0$, then we have as a solution $(x_1, x_2, x_3, x_4, x_5) = (1, 1, 1, 1, 0)$ and if $x_4 = 0$

and $x_5 = 1$, we have $(x_1, x_2, x_3, x_4, x_5) = (1, 0, 1, 0, 1)$. Finally, if $x_4 = 0$ and $x_5 = 0$, then we have as a solution $(x_1, x_2, x_3, x_4, x_5) = (0, 0, 0, 0, 0)$.

So the set of all solutions is

$$\{(0, 0, 0, 0, 0), (1, 1, 1, 1, 0), (1, 0, 1, 0, 1), (0, 1, 0, 1, 1)\}.$$

This code is easily determined to be a group code (for example, by constructing the Cayley table).

(You may have noticed that the solution set is finite, unlike similar systems of linear equations that you may have seen in linear algebra. Indeed the solution set must be finite, because the set of vectors in \mathbb{Z}_2^5 is finite. The difference is that we're now dealing with \mathbb{Z}_2^n rather than \mathbb{R}^n or \mathbb{C}^n .) \blacklozenge

Let's do another example in \mathbb{Z}_2^n , but this time in \mathbb{Z}_2^4 .

Example 19.4.5. Suppose that

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

For a 4-tuple $\mathbf{x} = (x_1, x_2, x_3, x_4)$ to be in the null space of H it must satisfy $H\mathbf{x}^T = \mathbf{0}$.

This means that,

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

So the following system of equations must be satisfied.

$$\begin{aligned} x_1 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_3 &= 0. \end{aligned}$$

We proceed again with Gaussian elimination and replace the second equation with the sum of the two equations to obtain the following system.

$$\begin{aligned} x_1 + x_3 + x_4 &= 0 \\ x_2 + x_4 &= 0. \end{aligned}$$

Solving for x_1 and x_2 , and replacing -1 with its modular equivalent, 1, we have the following dependent solutions,

$$\begin{aligned}x_1 &= x_3 + x_4 \\x_2 &= x_4.\end{aligned}$$

Notice that there are two free variables x_3 and x_4 . Therefore, there are $2^2 = 4$ solutions. If $x_3 = 1$ and $x_4 = 1$, then $x_1 = 0$, $x_2 = 1$. So one solution is $(x_1, x_2, x_3, x_4, x_5) = (0, 1, 1, 1)$. Likewise, if $x_3 = 1$ and $x_4 = 0$, then we have as a solution $(x_1, x_2, x_3, x_4, x_5) = (1, 0, 1, 0)$ and if $x_3 = 0$ and $x_4 = 1$, we have $(x_1, x_2, x_3, x_4, x_5) = (1, 1, 0, 1)$. Finally, if $x_3 = 0$ and $x_4 = 0$, then we have as a solution $(x_1, x_2, x_3, x_4, x_5) = (0, 0, 0, 0)$.

So the set of all solutions is

$$\{(0, 0, 0, 0), (1, 1, 0, 1), (1, 0, 1, 0), (0, 1, 1, 1)\}.$$

◆

Exercise 19.4.6. Compute the null space of each of the following matrices. In cases (a) and (b), show that the result is a group code.

$$\text{(a)} \quad \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{(b)} \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\text{(c)} \quad \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \quad \text{(d)} \quad \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

◇

Example 19.4.4 shows a case where the null space of a matrix with entries in \mathbb{Z}_2 turns out to be a group code. In fact, the null space of such a matrix is *always* a group code:

Proposition 19.4.7. Let H be in $\mathbb{M}_{k \times n}(\mathbb{Z}_2)$. Then the null space of H is a group code.

PROOF. As mentioned previously, to show that $\text{Null}(H)$ is a group code we just need to show that it's closed under the group operation $+$. Let $\mathbf{x}, \mathbf{y} \in \text{Null}(H)$ for some matrix H in $\mathbb{M}_{k \times n}(\mathbb{Z}_2)$. Then $H\mathbf{x}^T = \mathbf{0}$ and $H\mathbf{y}^T = \mathbf{0}$. So

$$H(\mathbf{x} + \mathbf{y})^T = H(\mathbf{x}^T + \mathbf{y}^T) = H\mathbf{x}^T + H\mathbf{y}^T = \mathbf{0} + \mathbf{0} = \mathbf{0}.$$

Hence, $\mathbf{x} + \mathbf{y}$ is in the null space of H and therefore must be a codeword. \square

We give a special name to group codes that are obtained as null spaces:

Definition 19.4.8. A code is a *linear code* if it is determined by the null space of some matrix $H \in \mathbb{M}_{k \times n}(\mathbb{Z}_2)$. \triangle

Note that at this point, all we know is that linear codes are group codes – we haven't yet proven that all group codes in \mathbb{Z}_2^n are linear codes (although this turns out to be true also!)

Example 19.4.9. Let C be the code given by the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Suppose that the 7-tuple $\mathbf{x} = (0, 1, 0, 0, 1, 1)$ is received. It is a simple matter of matrix multiplication to determine whether or not \mathbf{x} is a codeword. Since

$$H\mathbf{x}^T = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix},$$

the received word is not a codeword. We must either attempt to correct the word or request that it be transmitted again. \blacklozenge

Exercise 19.4.10. Which of the following are codewords for the code in Example 19.4.9?

- (a) $(1, 1, 1, 1, 1, 0)$

(b) $(1, 0, 0, 0, 1, 1)$ (c) $(1, 0, 1, 0, 1, 0)$

◇

19.5 Code words and encoding in block linear codes

We have shown how to define a set of codewords for a block linear code. But so far we don't understand too well what code words look like, and we haven't considered encoding and decoding. One of the great advantages of linear codes is that they enable very efficient methods of encoding and decoding. It's easiest to see how this works in the case where H has a special form, which we will now define.

19.5.1 Canonical Parity-check matrices

Definition 19.5.1. Suppose that H is a $k \times n$ matrix with entries in \mathbb{Z}_2 and $n > k$. If the last k columns of the matrix form the $k \times k$ identity matrix, I_k , then the matrix is called a **canonical parity-check matrix**. More specifically, $H = (A \mid I_k)$, where A is the $k \times (n - k)$ matrix

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1,n-k} \\ a_{21} & a_{22} & \cdots & a_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{k,n-k} \end{pmatrix}$$

and I_k is the $k \times k$ identity matrix

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

△

Exercise 19.5.2. Only one of the matrices in Exercise 19.4.6 is a canonical parity-check matrix. Which one is it? ◇

Readers who have had a class in linear algebra may notice the similarity between canonical parity-check matrices and reduced row-echelon form. The only difference is that reduced row-echelon matrices have the identity submatrix on the *left*, while the canonical parity-check matrix has it on the *right*.

In the following example, we will explore the relation between the canonical parity-check matrix H and the structure of the codewords.

Example 19.5.3. Suppose the matrix A is given by

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix},$$

then the associated canonical parity-check matrix is

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix},$$

Observe that the rows in H represent the parity checks on certain bit positions in a 6-tuple. The 1's in the identity matrix serve as parity checks for the 1's in the same row. If $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5, x_6)$, then

$$\mathbf{0} = H\mathbf{x}^T = \begin{pmatrix} x_2 + x_3 + x_4 \\ x_1 + x_2 + x_5 \\ x_1 + x_3 + x_6 \end{pmatrix},$$

which yields a system of equations:

$$\begin{aligned} x_2 + x_3 + x_4 &= 0 \\ x_1 + x_2 + x_5 &= 0 \\ x_1 + x_3 + x_6 &= 0 \end{aligned}$$

(remember that all of these equations are using binary arithmetic!) Here each of the bits in $\{x_4, x_5, x_6\}$ serves as a parity check bit for two of the bits in the set $\{x_1, x_2, x_3\}$. Hence, x_1, x_2 , and x_3 can be arbitrary but x_4, x_5 , and x_6 must be chosen to ensure parity. By following this method, we find that the vectors in $\text{Null}(H)$ are

$$\begin{array}{cccc} (000000) & (001101) & (010110) & (011011) \\ (100011) & (101110) & (110101) & (111000). \end{array}$$



The following proposition generalizes some of our findings from Example 19.5.3.

Proposition 19.5.4. Let $H \in \mathbb{M}_{k \times n}(\mathbb{Z}_2)$ be a canonical parity-check matrix. Then $\text{Null}(H)$ consists of all $\mathbf{x} \in \mathbb{Z}_2^n$ whose first $n - k$ bits are arbitrary but whose last k bits are determined by $H\mathbf{x}^T = \mathbf{0}$. Each of the last k bits serves as an even parity check bit for some of the first $n - k$ bits. Hence, H gives rise to an $(n, n - k)$ -block code (according to the notation that we introduced in Definition 19.2.1).

The proof of Proposition 19.5.4 simply follows the same steps as in Example 19.5.3, except that instead of 3 equations in 6 unknowns we have k equations in n unknowns. Readers who've had linear algebra may recognize that this is exactly the same as the method for solving linear equations using row-echelon form: the k equations in n unknowns give rise to $n - k$ free variables, that determine the other variables in the solution.

Proposition 19.5.4 motivates the following definitions.

Definition 19.5.5. Let H be a canonical parity-check matrix, and let \mathbf{x} be a codeword in $\text{Null}(H)$. Then the first $n - k$ bits of \mathbf{x} are called *information bits* and the last k bits are called *check bits*. \triangle

In Example 19.5.3, the first three bits are the information bits and the last three are the check bits.

Exercise 19.5.6.

- (a) Find the canonical parity-check matrix for a code that performs a single even parity check for three information bits (i.e. 3 information bits, 1 check bit).
- (b) Same as (a), except with seven information bits.
- (c) Is it possible to implement the odd parity-check code using a parity-check matrix? *Explain* your answer.



19.5.2 Standard Generator Matrices

We now have a relatively straightforward way to generate the codewords in $\text{Null}(H)$, if H is a canonical parity-check matrix. But there's an even easier way – and one that gives us an encoding function in the bargain.

Before jumping into this discussion, we should simplify our notation. Up to now we've been very careful to identify code words as row vectors, as opposed to column vectors: so for instance we've always written the parity check condition as $H\mathbf{x}^T = \mathbf{0}$, in order to ensure that \mathbf{x} is interpreted as a column vector. But when you come right down to it, vectors are vectors, no matter whether they're written horizontally or vertically. In the following discussion we'll be more casual, and simply denote the codeword by \mathbf{x} whether it's arranged as a row or column vector. So for instance, we'll simply write $H\mathbf{x} = \mathbf{0}$ instead of $H\mathbf{x}^T = \mathbf{0}$. The context will determine whether the row or column vector is meant.

Now that that's out of the way, let's begin on our new code generation method. First, a definition:

Definition 19.5.7. With each $k \times n$ canonical parity-check matrix $H = (A \mid I_k)$ we can associate an $n \times (n - k)$ **standard generator matrix** G , given by

$$G = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix}$$

△

In order to explore the connection between parity-check and generator matrices, we continue our previous example of a particular 3×3 matrix A .

Example 19.5.8. (*Example 19.5.3 continued*) For the matrix A used in Example 19.5.3, you may check that the associated generator matrix is:

$$G = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

By comparing G with the list of vectors in $\text{Null}(H)$, we find that all the columns of G “just happen” to be contained in $\text{Null}(H)$ (this is no accident,

as we shall see!). In fact, any linear combination of the columns of G will also be in $\text{Null}(H)$. To see this, denote the columns of G by $\mathbf{g}_1, \mathbf{g}_2, \mathbf{g}_3$, and let $x_1, x_2, x_3 \in \mathbb{Z}_2$. Then we have (by ordinary matrix multiplication, except all operations are binary)

$$H(x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + x_3\mathbf{g}_3) = x_1H\mathbf{g}_1 + x_2H\mathbf{g}_2 + x_3H\mathbf{g}_3 = x_1\mathbf{0} + x_2\mathbf{0} + x_3\mathbf{0} = \mathbf{0}.$$

The linear combination of columns of G can in fact be represented more simply using matrix-vector multiplication:

$$x_1\mathbf{g}_1 + x_2\mathbf{g}_2 + x_3\mathbf{g}_3 = G\mathbf{x}$$

This gives us another way to generate codewords that are in $\text{Null}(H)$ —namely, take any element in \mathbb{Z}_2^3 and multiply it by G . In fact, this gives us our long-sought encoding function! For any message word in \mathbb{Z}_2^3 we multiply on the left by G and voilà! The result is a codeword. Table 19.5 shows the results of this procedure. From the table, we find that this method of generating codewords gives us all of the vectors in $\text{Null}(H)$. Furthermore, each different message word produces a different codeword, as a proper encoding function should.

| Message Word \mathbf{x} | Codeword $G\mathbf{x}$ |
|------------------------------|---------------------------|
| 000 | 000000 |
| 001 | 001101 |
| 010 | 010110 |
| 011 | 011011 |
| 100 | 100011 |
| 101 | 101110 |
| 110 | 110101 |
| 111 | 111000 |

Table 19.5: A matrix-generated code



Exercise 19.5.9. For each of the following canonical parity-check matrices, find the corresponding standard generator matrix. Use the standard generator matrix to compute codewords (make a table similar to Table 19.5), and verify that the codewords are in the null space of the canonical parity-check matrix.

(a)

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b)

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(c)

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

(d)

$$\begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

◇

The following proposition generalizes what we found in the previous example.

Proposition 19.5.10. Suppose that G is an $n \times m$ standard generator matrix. Then $C = \{\mathbf{y} : G\mathbf{x} = \mathbf{y} \text{ for } \mathbf{x} \in \mathbb{Z}_2^m\}$ is an (n, m) -block code. More specifically, C is a group code.

PROOF. Let $G\mathbf{x}_1 = \mathbf{y}_1$ and $G\mathbf{x}_2 = \mathbf{y}_2$ be two codewords. Then $\mathbf{y}_1 + \mathbf{y}_2$ is in C since

$$G(\mathbf{x}_1 + \mathbf{x}_2) = G\mathbf{x}_1 + G\mathbf{x}_2 = \mathbf{y}_1 + \mathbf{y}_2.$$

We must also show that two message blocks can't be encoded into the same codeword. That is, we must show that if $G\mathbf{x} = G\mathbf{y}$, then $\mathbf{x} = \mathbf{y}$. Suppose that $G\mathbf{x} = G\mathbf{y}$. Then

$$G\mathbf{x} - G\mathbf{y} = G(\mathbf{x} - \mathbf{y}) = \mathbf{0}.$$

However, the first k coordinates in $G(\mathbf{x} - \mathbf{y})$ are exactly $x_1 - y_1, \dots, x_k - y_k$, since they are determined by the identity matrix, I_k , part of G . Hence, $G(\mathbf{x} - \mathbf{y}) = \mathbf{0}$ exactly when $\mathbf{x} = \mathbf{y}$. \square

In order to complete the link between canonical parity-check matrices and standard generating matrices, we first need the following useful result.

Proposition 19.5.11. Let $H = (A \mid I_k)$ be an $k \times n$ canonical parity-check matrix and $G = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix}$ be the corresponding $n \times (n - k)$ standard generator matrix. Then $HG = \mathbf{0}$, where $\mathbf{0}$ denotes the $k \times (n - k)$ matrix of all 0's.

PROOF. It is possible to prove this by writing out the matrix product HG using summation notation (see Chapter 10). This is however somewhat long-winded. A much easier way is to multiply H and G as *block matrices*.¹ Since the block sizes are compatible, we have

$$HG = (A \mid I_k) \begin{pmatrix} I_{n-k} \\ A \end{pmatrix} = (A + A),$$

but since we are adding in binary, it follows that $A + A$ is the $k \times (n - k)$ matrix of all 0's. \square

We now top things off by establishing equality between $\text{Null}(H)$ and the code generated by G .

Proposition 19.5.12. Let $H = (A \mid I_k)$ be a $k \times n$ canonical parity-check matrix and let $G = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix}$ be the $n \times (n - k)$ standard generator matrix associated with H . Let C be the code generated by G . Then \mathbf{y} is in C if and only if $H\mathbf{y} = \mathbf{0}$. In particular, C is a linear code with canonical parity-check matrix H .

PROOF. First suppose that $\mathbf{y} \in C$. Then $G\mathbf{x} = \mathbf{y}$ for some $\mathbf{x} \in \mathbb{Z}_2^{n-k}$. By Proposition 19.5.11, $H\mathbf{y} = HG\mathbf{x} = \mathbf{0}$.

Conversely, suppose that $\mathbf{y} = (y_1, \dots, y_n)$ is in the null space of H . We can split \mathbf{y} into two parts as follows:

$$\mathbf{y} = (\mathbf{y}_a \mid \mathbf{y}_b), \text{ where } \mathbf{y}_a := (y_1, \dots, y_{n-k}) \text{ and } \mathbf{y}_b := (y_{n-k+1}, \dots, y_n).$$

¹see for example mathworld.wolfram.com/BlockMatrix.html.

Since \mathbf{y} is in the null space of H we have $H\mathbf{y} = \mathbf{0}$, which we can also write as (using partitioned matrix multiplication)

$$H\mathbf{y} = (A \mid I_m) \begin{pmatrix} \mathbf{y}_a \\ \mathbf{y}_b \end{pmatrix} = A\mathbf{y}_a + \mathbf{y}_b = \mathbf{0}.$$

Since we are adding in binary, it follows that $A\mathbf{y}_a = \mathbf{y}_b$, so that we may write

$$\mathbf{y} = \begin{pmatrix} \mathbf{y}_a \\ \mathbf{y}_b \end{pmatrix} = \begin{pmatrix} I_{n-k} \\ A \end{pmatrix} \mathbf{y}_a,$$

so that \mathbf{y} is in C . □

19.5.3 Error detection and correction

In this section, we will show how to obtain the error correction and detection properties of a code directly from its matrix H . First, we will look at detection and correction of single errors.

Suppose that a codeword \mathbf{x} is transmitted with a single error. Then the resulting transmitted word can be written as $\mathbf{x} + \mathbf{e}_j$, where \mathbf{e}_j has a nonzero entry only in the j 'th position:

$$\begin{aligned} \mathbf{e}_1 &= (100 \cdots 00) \\ \mathbf{e}_2 &= (010 \cdots 00) \\ &\vdots \\ \mathbf{e}_n &= (000 \cdots 01) \end{aligned}$$

In this case, when we apply the parity check matrix to the transmitted codeword we obtain

$$H(\mathbf{x} + \mathbf{e}_j) = H\mathbf{x} + H\mathbf{e}_j = \mathbf{0} + H\mathbf{e}_j = H\mathbf{e}_j.$$

It appears that $H\mathbf{e}_j$ plays an important role in determining the error detection and correction properties of the code.

Exercise 19.5.13. Let H be the parity-check matrix given by

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

1. Compute $H\mathbf{e}_j$ for $j = 1, 2, 3, 4, 5$.
2. What is the relationship between your answers in (a) and the columns of H ?

◇

We generalize our findings in this exercise as follows:

Proposition 19.5.14. Let \mathbf{e}_i be the binary n -tuple with a 1 in the i th coordinate and 0's elsewhere and suppose that $H \in \mathbb{M}_{m \times n}(\mathbb{Z}_2)$. Then $H\mathbf{e}_i$ is the i th column of the matrix H .

Proposition 19.5.14 is a well-known fact in linear algebra, so we refer the reader to a linear algebra textbook for proof.²

This result leads immediately to a simple rule for single error detection.

Proposition 19.5.15. Let H be an $m \times n$ binary matrix. Then the null space of H is a single error-detecting code if and only if no column of H consists entirely of zeros.

PROOF. Suppose that $\text{Null}(H)$ is a single error-detecting code. Then the minimum distance of the code must be at least 2. Since the null space is a group code, it is sufficient to require that the code contain no codewords of less than weight 2 other than the zero codeword. That is, \mathbf{e}_i must not be a codeword for $i = 1, \dots, n$. Since $H\mathbf{e}_i$ is the i th column of H , the only way in which \mathbf{e}_i could be in the null space of H would be if the i th column of H were all zeros, which is impossible; hence, the code must have the capability to detect at least single errors.

Conversely, suppose that no column of H is the zero column. By Proposition 19.5.14, $H\mathbf{e}_i \neq \mathbf{0}$. □

Exercise 19.5.16. Which of the following parity-check matrices determine single error-detecting codes? *Explain* your answer.

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} ; \quad H_2 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix} .$$

²See for example: David C. Lay, "Linear Algebra and its Applications" (Third Edition), Section 1.4.

◇

Using similar reasoning, we can also come up with a method for determining single error-correction from the parity-check matrix.

Example 19.5.17. Consider the parity-check matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

The corresponding code is single error-correcting if all nonzero codewords have weight greater than two. Since there are no zero columns, Proposition 19.5.15 tells us that no codewords have weight 1. We thus only need to check that $\text{Null}(H)$ does not contain any 4-tuples of weight 2, so that (1100), (1010), (1001), (0110), (0101), and (0011) must not be in $\text{Null}(H)$.

◆

Exercise 19.5.18. Does the code in Example 19.5.17 correct single errors? Explain your answer. ◇

For larger codewords, the task of checking all tuples of weight 2 can be tedious. Fortunately, there is a much easier way that avoids exhausting checking:

Proposition 19.5.19. Let H be a binary matrix. The null space of H is a single error-correcting code if and only if H does not contain any zero columns and no two columns of H are identical.

PROOF. The n -tuple $\mathbf{e}_i + \mathbf{e}_j$ has 1's in the i th and j th entries and 0's elsewhere, and $w(\mathbf{e}_i + \mathbf{e}_j) = 2$ for $i \neq j$. Since

$$\mathbf{0} = H(\mathbf{e}_i + \mathbf{e}_j) = H\mathbf{e}_i + H\mathbf{e}_j$$

can only occur if the i th and j th columns are identical, the null space of H is a single error-correcting code. □

Exercise 19.5.20. Which of the parity-check matrices in Exercise 19.5.9 produce codes that can correct single errors? ◇

Suppose now that we have a canonical parity-check matrix H with three rows. Then we might ask how many more columns we can add to the matrix and still have a null space that is a single error-detecting and single error-correcting code. Since each column has three entries, there are $2^3 = 8$ possible distinct columns. We can't add the columns

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

So we can add as many as four columns and still maintain a minimum distance of 3.

In general, if H is an $k \times n$ canonical parity-check matrix, then there are $n - k$ information bits in each codeword. Each column has k bits, so there are 2^k possible distinct columns. It is necessary that the columns $\mathbf{0}, \mathbf{e}_1, \dots, \mathbf{e}_n$ be excluded, leaving $2^k - (1 + n)$ remaining columns for information if we are still to maintain the ability not only to detect but also to correct single errors.

Exercise 19.5.21. Suppose we want to design a code that encodes each of the 128 ASCII characters as a single codeword, such that the code also can detect and/or correct single-bit errors. We also want codewords to be as short as possible to speed up transmission.

- (a) How many information bits are in each codeword?
- (b) In order to *detect* single-bit errors, what is the smallest possible codeword size?
- (c) In order to *correct* single-bit errors, what is the smallest possible codeword size? (*Hint*)
- (d) Redo parts (a), (b), (c) if we want instead to encode the extended ASCII character set of 256 characters.

◇

Exercise 19.5.22.

- (a) What is the smallest possible codeword size for a single error-correcting code with 20 information bits per codeword?

- (b) What is the smallest possible codeword size for a single error-correcting code with 32 information bits per codeword?

◇

19.6 Efficient Decoding

We are now at the stage where we are able to generate linear codes that detect and correct errors fairly easily. However, we haven't yet seen a good way to decode a received n -tuple that has some errors. The only thing we can do so far is compare the received n -tuple, to each possible codeword, and find the closest one. If the code is large, this may be very time-consuming.

In the following subsections, we will explore two different decoding methods which are much efficient and practical.

19.6.1 Decoding using syndromes

The following example introduces the notion of *syndrome*.

Example 19.6.1. Given the binary matrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and the 5-tuples $\mathbf{x} = (11011)$ and $\mathbf{y} = (01011)$, we can compute

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

and

$$H\mathbf{y} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Hence, \mathbf{x} is a codeword and \mathbf{y} is not, since \mathbf{x} is in the null space and \mathbf{y} is not. Notice that $H\mathbf{x}$ is identical to the first column of H . In fact, this is where the error occurred. If we flip the first bit in \mathbf{y} from 0 to 1, then we obtain \mathbf{x} . ◇

It appears from this example that the vector $H\mathbf{x}$ has special importance, so we create a special term for it:

Definition 19.6.2. If H is an $k \times n$ matrix and $\mathbf{x} \in \mathbb{Z}_2^n$, then $H\mathbf{x}$ is called the *syndrome* of \mathbf{x} \triangle

The following proposition allows the quick detection and correction of errors.

Proposition 19.6.3. Let the $k \times n$ binary matrix H determine a linear code and let \mathbf{x} be the received n -tuple. Write \mathbf{x} as $\mathbf{x} = \mathbf{c} + \mathbf{e}$, where \mathbf{c} is the transmitted codeword and \mathbf{e} is the transmission error. Then the syndrome $H\mathbf{x}$ of the received codeword \mathbf{x} is also the syndrome of the error \mathbf{e} .

PROOF. $H\mathbf{x} = H(\mathbf{c} + \mathbf{e}) = H\mathbf{c} + H\mathbf{e} = \mathbf{0} + H\mathbf{e} = H\mathbf{e}$. \square

This proposition tells us that the syndrome of a received word depends solely on the error and not on the transmitted codeword. The proof of the following proposition follows immediately from Proposition 19.6.3 and from the fact that $H\mathbf{e}_j$ is the j th column of the matrix H .

Proposition 19.6.4. Let $H \in \mathbb{M}_{k \times n}(\mathbb{Z}_2)$ and suppose that the linear code corresponding to H is single error-correcting. Let \mathbf{r} be a received n -tuple that was transmitted with at most one error. If the syndrome of \mathbf{r} is $\mathbf{0}$, then no error has occurred; otherwise, if the syndrome of \mathbf{r} is equal to some column of H , say the i th column, then the error has occurred in the i th bit.

Example 19.6.5. Consider the matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

and suppose that the 6-tuples $\mathbf{x} = (111110)$, $\mathbf{y} = (111111)$, and $\mathbf{z} = (010111)$ have been received (technically these are column vectors, but we write them as row vectors for convenience). Then

$$H\mathbf{x} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, H\mathbf{y} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, H\mathbf{z} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Hence, \mathbf{x} has an error in the third bit and \mathbf{z} has an error in the fourth bit. The transmitted codewords for \mathbf{x} and \mathbf{z} must have been (110110) and (010011) ,

respectively. The syndrome of \mathbf{y} does not occur in any of the columns of the matrix H , so multiple errors must have occurred to produce \mathbf{y} . \blacklozenge

Exercise 19.6.6. Let

$$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Compute the syndrome caused by each of the following transmission errors.

1. An error in the first bit.
2. An error in the third bit.
3. An error in the last bit.
4. Errors in the third and fourth bits.

\blacklozenge

Exercise 19.6.7. Let C be the code obtained from the null space of the matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Decode the message

11101 11011 10101 01101

if possible. \blacklozenge

Exercise 19.6.8. List all possible syndromes for the codes associated with each the parity matrices in Exercise 19.5.9. \blacklozenge

| | Cosets | | | |
|---------------|---------|---------|---------|---------|
| C | (00000) | (01101) | (10011) | (11110) |
| $(10000) + C$ | (10000) | (11101) | (00011) | (01110) |
| $(01000) + C$ | (01000) | (00101) | (11011) | (10110) |
| $(00100) + C$ | (00100) | (01001) | (10111) | (11010) |
| $(00010) + C$ | (00010) | (01111) | (10001) | (11100) |
| $(00001) + C$ | (00001) | (01100) | (10010) | (11111) |
| $(10100) + C$ | (00111) | (01010) | (10100) | (11001) |
| $(00110) + C$ | (00110) | (01011) | (10101) | (11000) |

Table 19.6: Cosets of C

19.6.2 Coset Decoding

We can use group theory to obtain another way of decoding messages that makes use of *cosets*. (If you've forgotten what cosets are, you may look back at Chapter 18 to refresh your memory.)

Since the linear code C is a subgroup of \mathbb{Z}_2^n , it follows that \mathbb{Z}_2^n may be partitioned into cosets of C . In particular, if C is an (n, m) -linear code, then a coset of C in \mathbb{Z}_2^n is written in the form $\mathbf{x} + C$, where $\mathbf{x} \in \mathbb{Z}_2^n$. By Lagrange's Theorem, there are 2^{n-m} distinct cosets of C in \mathbb{Z}_2^n . The following example shows how this works in a particular case:

Example 19.6.9. Let C be the $(5, 3)$ -linear code given by the parity-check matrix

$$H = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

The code consists of the codewords

$$(00000) \quad (01101) \quad (10011) \quad (11110),$$

There are $2^{5-2} = 2^3$ cosets of C in \mathbb{Z}_2^5 , each with order $2^2 = 4$. These cosets are listed in Table 19.6. \blacklozenge

Let's see how knowing the cosets helps us to decode a message. Suppose that \mathbf{x} was the original codeword sent and that \mathbf{r} is the n -tuple received. If \mathbf{e} is the transmission error, then $\mathbf{r} = \mathbf{e} + \mathbf{x}$ or, equivalently, $\mathbf{x} = \mathbf{e} + \mathbf{r}$. However, this is exactly the statement that \mathbf{r} is an element in the coset $\mathbf{e} + C$. In maximum-likelihood decoding we expect the error \mathbf{e} to be as small

as possible; that is, \mathbf{e} will have the least weight. An n -tuple of least weight in a coset is called a *coset leader*. Once we have determined a coset leader for each coset, the decoding process becomes a task of calculating $\mathbf{r} + \mathbf{e}$ to obtain \mathbf{x} .

Example 19.6.10. In Table 19.6, notice that we have chosen a representative of the least possible weight for each coset. These representatives are coset leaders. Now suppose that $\mathbf{r} = (01111)$ is the received word. To decode \mathbf{r} , we find that it is in the coset $(00010) + C$; hence, the originally transmitted codeword must have been $(01101) = (01111) + (00010)$. \blacklozenge

A potential problem with this method of decoding is that we might have to examine every coset for the received codeword. The following proposition shows us that we can avoid this because the syndrome that we calculate from the received codeword points to exactly one coset:

Proposition 19.6.11. Let C be an (n, k) -linear code given by the matrix H and suppose that \mathbf{x} and \mathbf{y} are in \mathbb{Z}_2^n . Then \mathbf{x} and \mathbf{y} are in the same coset of C if and only if $H\mathbf{x} = H\mathbf{y}$. That is, two n -tuples are in the same coset if and only if their syndromes are the same.

PROOF. Two n -tuples \mathbf{x} and \mathbf{y} are in the same coset of C exactly when $\mathbf{x} - \mathbf{y} \in C$; however, this is equivalent to $H(\mathbf{x} - \mathbf{y}) = \mathbf{0}$ or $H\mathbf{x} = H\mathbf{y}$. \square

This proposition gives us a three-step process for finding decoding:

- (a) Compute the syndrome for the received codeword;
- (b) Find the coset leader of the coset associated with this syndrome;
- (c) Subtract the coset leader from the received codeword to find the most likely transmitted codeword.

To facilitate step (b) of this process, we may make a lookup table that displays the coset leader associated with each syndrome. Such a table is called a *decoding table*.

Example 19.6.12. Table 19.7 is a decoding table for the code C given in Example 19.6.9. If $\mathbf{x} = (01111)$ is received, then its syndrome can be computed to be

$$H\mathbf{x} = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

Examining the decoding table, we determine that the coset leader is (00010). It is now easy to decode the received codeword. \blacklozenge

Given an (n, k) -block code, the question arises of whether or not coset decoding is a manageable scheme. A decoding table requires a list of cosets and syndromes, one for each of the 2^{n-k} cosets of C . Suppose that we have a $(32, 24)$ -block code. We have a huge number of codewords, 2^{24} , yet there are only $2^{32-24} = 2^8 = 256$ cosets.

| Syndrome | Coset Leader |
|----------|--------------|
| (000) | (00000) |
| (001) | (00001) |
| (010) | (00010) |
| (011) | (10000) |
| (100) | (00100) |
| (101) | (01000) |
| (110) | (00110) |
| (111) | (10100) |

Table 19.7: Syndromes for each coset

Exercise 19.6.13. Let C be the group code in \mathbb{Z}_2^3 defined by the codewords (000) and (111). Compute the cosets of H in \mathbb{Z}_2^3 . Why was there no need to specify right or left cosets? Give the single transmission error, if any, to which each coset corresponds. \blacklozenge

Exercise 19.6.14. For each of the following matrices, find the cosets of the corresponding code C . Give a decoding table for each code if possible.

(a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

(d)
$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \end{pmatrix}$$

◇

19.7 Additional algebraic coding exercises

Exercise 19.7.1. Let C be a linear code. Show that either the i th coordinates in the codewords of C are all zeros or exactly half of them are zeros. (*Hint*) ◇

Exercise 19.7.2. Show that the codewords of even weight in a linear code C are also a linear code. (*Hint*) ◇

Exercise 19.7.3. Let C be a linear code. Show that either every codeword has even weight or exactly half of the codewords have even weight. (*Hint*) ◇

Exercise 19.7.4. Let C be an (n, k) -linear code. Define the *dual* or *Orthogonal code* of C to be

$$C^\perp = \{\mathbf{x} \in \mathbb{Z}_2^n : \mathbf{x} \cdot \mathbf{y} = 0 \text{ for all } \mathbf{y} \in C\}.$$

(a) Find the dual code of the linear code C where C is given by the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

(b) Show that C^\perp is an $(n, n - k)$ -linear code.

(c) Find the standard generator and parity-check matrices of C and C^\perp . What happens in general? Prove your conjecture.

◇

Exercise 19.7.5. Let H be an $m \times n$ matrix over \mathbb{Z}_2 , where the i th column is the number i written in binary with m bits. The null space of such a matrix is called a *Hamming code*.

- (a) Show that the matrix

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

generates a Hamming code. What are the error-correcting properties of a Hamming code?

- (b) The column corresponding to the syndrome also marks the bit that was in error; that is, the i th column of the matrix is i written as a binary number, and the syndrome immediately tells us which bit is in error. If the received word is (101011), compute the syndrome. In which bit did the error occur in this case, and what codeword was originally transmitted?
- (c) Give a binary matrix H for the Hamming code with six information positions and four check positions. What are the check positions and what are the information positions? Encode the messages (101101) and (001001). Decode the received words (0010000101) and (0000101100). What are the possible syndromes for this code?
- (d) What is the number of check bits and the number of information bits in an (m, n) -block Hamming code? Give both an upper and a lower bound on the number of information bits in terms of the number of check bits. Hamming codes having the maximum possible number of information bits with k check bits are called *perfect*. Every possible syndrome except $\mathbf{0}$ occurs as a column. If the number of information bits is less than the maximum, then the code is called *shortened*. In this case, give an example showing that some syndromes can represent multiple errors.

◇

Exercise 19.7.6. Write a program to implement a $(16, 12)$ -linear code. Your program should be able to encode and decode messages using coset decoding. Once your program is written, write a program to simulate a binary symmetric channel with transmission noise. Compare the results of your simulation with the theoretically predicted error probability. ◇

Remark 19.7.7. (*historical background*) Modern coding theory began in 1948 with C. Shannon's paper, "A Mathematical Theory of Information" [7]. This paper offered an example of an algebraic code, and Shannon's Theorem proclaimed exactly how good codes could be expected to be. Richard Hamming began working with linear codes at Bell Labs in the late 1940s and early 1950s after becoming frustrated because the programs that he was running could not recover from simple errors generated by noise. Coding theory has grown tremendously in the past several years. *The Theory of Error-Correcting Codes*, by MacWilliams and Sloane [5], published in 1977, already contained over 1500 references. Linear codes (Reed-Muller (32, 6)-block codes) were used on NASA's Mariner space probes. More recent space probes such as Voyager have used what are called convolution codes. Currently, very active research is being done with Goppa codes, which are heavily dependent on algebraic geometry. \triangle

19.8 References and Suggested Readings

- [1] Blake, I. F. "Codes and Designs," *Mathematics Magazine* **52** (1979), 81–95.
- [2] Hill, R. *A First Course in Coding Theory*. Oxford University Press, Oxford, 1986.
- [3] Levinson, N. "Coding Theory: A Counterexample to G. H. Hardy's Conception of Applied Mathematics," *American Mathematical Monthly* **77** (1970), 249–58.
- [4] Lidl, R. and Pilz, G. *Applied Abstract Algebra*. Springer-Verlag, New York, 1984.
- [5] MacWilliams, F. J. and Sloane, N. J. A. *The Theory of Error-Correcting Codes*. North Holland, Amsterdam, 1977.
- [6] Roman, S. *Coding and Information Theory*. Springer-Verlag, New York, 1992.
- [7] Shannon, C. E. "A Mathematical Theory of Communication," *Bell System Technical Journal* **27** (1948), 379–423, 623–56.
- [8] Thompson, T. M. *From Error-Correcting Codes through Sphere Packing to Simple Groups*. Carus Monograph Series, No. 21. Mathematical Association of America, Washington, DC, 1983.
- [9] van Lint, J. H. *Introduction to Coding Theory*. Springer-Verlag, New York, 1982.

19.9 Hints for “Error Detecting and Correcting Codes” exercises

Exercise 19.3.6(c): Apply part (b) to both sides of the equation, and show they are equal.

Exercise 19.3.9(a): Add any codeword to itself.

Exercise 19.5.21(c): Use the paragraph just above this exercise.

Exercise 19.7.1: Show that the codewords in C that have i 'th coordinate equal to 0 form a subgroup of C , and consider the cosets of this subgroup in C .

Exercise 19.7.2: What row should you add to the parity check matrix?

Exercise 19.7.3: Use the previous exercise to show the codewords of even weight in C form a subgroup. Then consider the cosets of this subgroup in C .

Isomorphisms of Groups

Thanks to Tom Judson for providing the foundational material for this chapter.

20.1 Preliminary examples

Several times in the book so far we have run into the idea of *isomorphic groups*. For instance:

Example 20.1.1. In Chapter 4 we pointed out that \mathbb{C} under complex addition and $\mathbb{R} \times \mathbb{R}$ under pairwise addition act exactly the same. In order to introduce the new concepts of this chapter, let's go over this again.

If $z = a + bi$ and $w = c + di$ are complex numbers, we can identify them as real ordered pairs according to the following “translation” function $f : \mathbb{C} \rightarrow \mathbb{R} \times \mathbb{R}$:

$$f(a + bi) = (a, b),$$

which we may also represent as

$$a + bi \xrightarrow{f} (a, b).$$

If we add two complex numbers and “translate” the result to an ordered pair, we find:

$$z + w = (a + bi) + (c + di) \xrightarrow{f} (a + b, c + d).$$

On the other hand, if we map z and w separately we get:

$$z = a + bi \xrightarrow{f} (a, b); \quad w = c + di \xrightarrow{f} (c, d),$$

and then if we add the resulting coordinate pairs, we obtain

$$(a, b) + (c, d) = (a + c, b + d).$$

which is the same as before. So we get the same result whether we add the complex numbers or their corresponding ordered pairs.

What we've shown is illustrated in Figure 20.1.1. If we start with the complex numbers z, w , we get the same result whether we follow first the arrow to the right ("translate" to $\mathbb{R} \times \mathbb{R}$) and then go down (addition in $\mathbb{R} \times \mathbb{R}$), or whether we follow first the down arrow (addition in \mathbb{C}) and then go right ("translate" to $\mathbb{R} \times \mathbb{R}$).

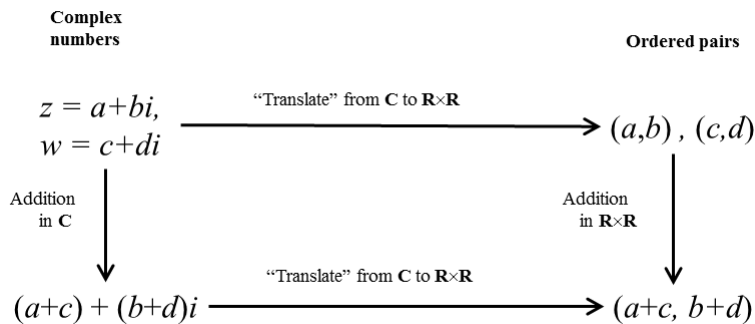


Figure 20.1.1. Addition is the "same" for complex numbers and real ordered pairs.



Remark 20.1.2. Readers with an eidetic memory may recognize the similarity between Figure 20.1.1 and Figure 5.4.1. In fact, this type of diagram pops up a lot in higher mathematics, so much so that it has a special name: *commutative diagram*. △

Exercise 20.1.3. Let f be the function used in Example 20.1.1 to rename complex numbers as ordered pairs. Recall that $r \operatorname{cis} \theta$ is the polar form of a complex number. How would you write $f(r \operatorname{cis} \theta)$? ◇

Previously when we talked informally about two groups being isomorphic, we emphasized that the two groups are "equivalent" in some sense. So

for instance, in the case of Example 1 it should be possible to exchange the roles of \mathbb{C} and $\mathbb{R} \times \mathbb{R}$ and get the same result. For this to work, there should be a function from $\mathbb{R} \times \mathbb{R}$ to \mathbb{C} that shows how to replace ordered pairs with complex numbers without “changing anything”. What would that function be? A prime suspect is the inverse of f —assuming, that is, that f actually has an inverse. What type of function does f have to be in order to have an inverse? You guessed it—a bijection.

Exercise 20.1.4. Prove that the function f defined in Example 20.1.1 is a bijection. \diamond

Exercise 20.1.5. Draw a diagram similar to Figure 20.1.1 for the function $g : \mathbb{C} \rightarrow \mathbb{R} \times \mathbb{R}$ defined by $g(a + bi) = (3a, 3b)$. Show that the same “arrow-following” property holds: that is, you can follow the arrows from the upper left to lower right in either order, and still end up with the same result. \diamond

Exercise 20.1.6. Prove that the function $h(a + bi) = (a + 2, b + 2)$ is **not** an isomorphism from \mathbb{C} to $\mathbb{R} \times \mathbb{R}$. (**Hint**) \diamond

Example 20.1.7. In the Symmetries chapter we also saw some examples of isomorphic groups. In particular, we saw that \mathbb{Z}_4 , the 4th roots of unity, and the rotations of a square act exactly the same under modular addition, modular multiplication, and function composition respectively. Let’s remind ourselves why. The following are the Cayley tables for \mathbb{Z}_4 , the 4th roots of unity (which we’ll denote by $\langle i \rangle$), and the rotations of a square (R_4):

| | | | | |
|----------|---|---|---|---|
| \oplus | 0 | 1 | 2 | 3 |
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Table 20.1: Cayley table for \mathbb{Z}_4

| | | | | |
|------|------|------|------|------|
| · | 1 | i | -1 | $-i$ |
| 1 | 1 | i | -1 | $-i$ |
| i | i | -1 | $-i$ | 1 |
| -1 | -1 | $-i$ | 1 | i |
| $-i$ | $-i$ | 1 | i | -1 |

Table 20.2: Cayley table for $\langle i \rangle$

| | | | | |
|-----------|-----------|-----------|-----------|-----------|
| o | id | r_{90} | r_{180} | r_{270} |
| id | id | r_{90} | r_{180} | r_{270} |
| r_{90} | r_{90} | r_{180} | r_{270} | id |
| r_{180} | r_{180} | r_{270} | id | r_{90} |
| r_{270} | r_{270} | id | r_{90} | r_{180} |

Table 20.3: Cayley table for R_4

- (1) Comparing \mathbb{Z}_4 and $\langle i \rangle$, notice that if we take the Cayley table for \mathbb{Z}_4 and make the following replacements:

$$0 \rightarrow 1 \quad 1 \rightarrow i \quad 2 \rightarrow -1 \quad 3 \rightarrow -i,$$

then the result exactly matches the Cayley table for $\langle i \rangle$. This means that if you add any two elements in \mathbb{Z}_4 (say 1 and 2), and also multiply their corresponding elements in $\langle i \rangle$ (i and -1), your results from each of these actions are corresponding elements (3 and $-i$).

Hence the function $f : \mathbb{Z}_4 \rightarrow \langle i \rangle$ that takes

$$0 \xrightarrow{f} 1, \quad 1 \xrightarrow{f} i, \quad 2 \xrightarrow{f} -1, \quad 3 \xrightarrow{f} -i$$

is an isomorphism from \mathbb{Z}_4 to the 4th roots of unity, and these groups are isomorphic to each other.

- (2) Now if we compare $\langle i \rangle$ and R_4 , using the function $g : \langle i \rangle \rightarrow R_4$ defined by

$$1 \xrightarrow{g} \text{id}, \quad i \xrightarrow{g} r_{90}, \quad -1 \xrightarrow{g} r_{180}, \quad -i \xrightarrow{g} r_{270},$$

we see that their Cayley tables are in fact exactly the same. Hence the 4th roots of unity and the rotations of a square are isomorphic to each other, and g is an isomorphism between them.

(3) Finally, using the function $h : \mathbb{Z}_4 \rightarrow R_4$ that takes

$$0 \xrightarrow{h} \text{id}, \quad 1 \xrightarrow{h} r_{90}, \quad 2 \xrightarrow{h} r_{180}, \quad 3 \xrightarrow{h} r_{270},$$

we see that the Cayley tables for \mathbb{Z}_4 and R_4 are exactly the same. Hence \mathbb{Z}_4 and the rotations of a square are isomorphic to each other, and h is an isomorphism between them.

So \mathbb{Z}_4 , R_4 , and $\langle i \rangle$ are all isomorphic to each other. Mathematically we state this as follows:

$$\mathbb{Z}_4 \cong R_4 \cong \langle i \rangle$$

◆

Exercise 20.1.8. Determine whether each of the following functions are isomorphisms between the groups in Example 20.1.7. Justify your answers.

(a) $f : \mathbb{Z}_4 \rightarrow \langle i \rangle$ defined by

$$f(0) = 1, \quad f(1) = -1, \quad f(2) = i, \quad f(3) = -i.$$

(b) $g : \mathbb{Z}_4 \rightarrow R_4$ defined by

$$g(0) = \text{id}, \quad g(1) = r_{270}, \quad g(2) = r_{90}, \quad g(3) = r_{180}.$$

(c) $h : R_4 \rightarrow \langle i \rangle$ defined by

$$h(1) = \text{id}, \quad h(i) = r_{270}, \quad h(-1) = r_{180}, \quad h(-i) = r_{90}.$$

(d) $h : R_4 \rightarrow \langle i \rangle$ defined by

$$h(\text{id}) = 1, \quad h(r_{270}) = i, \quad h(r_{180}) = -i, \quad h(r_{90}) = -1.$$

◇

Exercise 20.1.9. Come up with a *different* isomorphism for each pairing of groups in Example 20.1.7. For instance, find a function different from f that maps $\mathbb{Z}_4 \rightarrow \langle i \rangle$ that matches the the two Cayley tables. Do the same thing with g and h . ◇

20.2 Formal definition and basic properties of isomorphisms

So let's buckle down and get mathematical. We start with a rigorous definition of isomorphism:

Definition 20.2.1. Two groups (G, \cdot) and (H, \circ) are *isomorphic* if there exists a bijection $\phi : G \rightarrow H$ such that the group operation is preserved; that is,

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

for all a and b in G . If G is isomorphic to H , we write $G \cong H$. The function ϕ is called an *isomorphism*. \triangle

Remark 20.2.2. We'll often use Greek letters (ϕ ('phi'), γ ('gamma'), ψ ('psi'), etc.) to denote isomorphisms—partially because 'phi' is reminiscent of isomor'phi'sm, and partially because we don't want to confuse isomorphisms with group elements (which are denoted by g, h , and so on.) \triangle

Remark 20.2.3. Definition 20.2.1 specifies that any isomorphism must be a bijection, i.e. a function that is 1-1 and onto. Proposition 8.7.11 tells us that any function that has an inverse is a bijection, and vice versa. You'll find that often the easiest way to show that a function is a bijection is to show it has an inverse. \triangle

Exercise 20.2.4.

- (a) Let consider the function $\phi : \mathbb{R} \rightarrow \mathbb{R}$ defined by: $\phi(x) = 5x$. Use Definition 20.2.1 to show that ϕ defines an isomorphism. What are the two isomorphic groups involved?
- (b) Let a be a nonzero real number, and consider the function $\phi_a : \mathbb{R} \rightarrow \mathbb{R}$ defined by: $\phi_a(x) = ax$. Show that ϕ_a defines an isomorphism. What are the two isomorphic groups involved?

\diamond

Some important properties of isomorphisms follow directly from the above definition. First we have:

Proposition 20.2.5. Given that $\phi : G \rightarrow H$ is an isomorphism, then ϕ takes the identity to the identity: that is, if e is the identity of G , then $\phi(e)$ is the identity of H (see Figure 20.2.1).

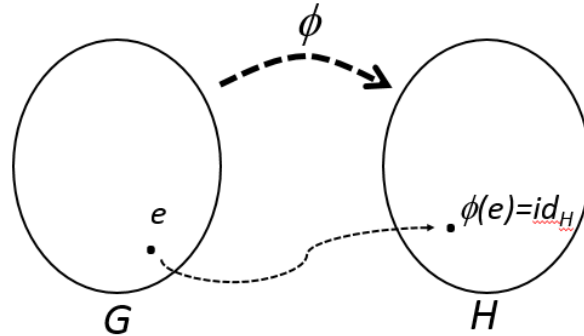


Figure 20.2.1. Isomorphic image of inverse elements are inverse elements.

Exercise 20.2.6. Fill in the blanks in the following proof of Proposition 20.2.5:

Given that e is the identity of < 1 > and h is an arbitrary element of < 2 >. Since ϕ is a bijection, then there exists $g \in$ < 3 > such that ϕ (< 4 >) = h . Then we have:

$$\begin{aligned}
 \phi(e) \circ h &= \phi(e) \circ \phi(\text{< 5 >}) && \text{(substitution)} \\
 &= \phi(e \cdot \text{< 6 >}) && \text{(definition of < 7 >)} \\
 &= \phi(\text{< 8 >}) && \text{(definition of < 9 >)} \\
 &= h && \text{(substitution)}
 \end{aligned}$$

Following the same steps, we can also show

$$h \circ \phi(e) = \text{< 10 >}.$$

It follows from the definition of identity that < 11 > is the identity of the group < 12 >. \diamond

Another important property of isomorphisms is illustrated in Figure 20.2.2, and stated in Proposition 20.2.7:

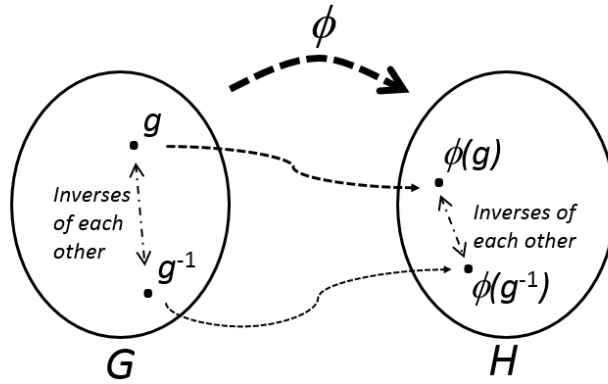


Figure 20.2.2. Isomorphic image of an identity element is an identity element.

Proposition 20.2.7. Given that $\phi : G \rightarrow H$ is an isomorphism, then ϕ preserves the operation of inverse: that is, for any $g \in G$ we have

$$\phi(g^{-1}) = (\phi(g))^{-1}.$$

Exercise 20.2.8. Fill in the blanks in the following proof of Proposition 20.2.7:

Let e and f be the identities of G and H , respectively. Given that $g \in$ < 1 >, we have:

$$\begin{aligned} \phi(g) \circ \phi(g^{-1}) &= \phi(g \cdot g^{-1}) && \text{(definition of < 2 >)} \\ &= \phi(e) && \text{(definition of < 3 >)} \\ &= f && \text{(Proposition < 4 >).} \end{aligned}$$

Using the same steps, we can also show

$$\phi(g^{-1}) \circ \phi(g) = \text{< 5 > .}$$

By the definition of inverse, it follows that

$$(\phi(g))^{-1} = \text{< 6 > .}$$

◇

It's possible to use isomorphisms to create other isomorphisms:

Exercise 20.2.9.

- (a) Given that $\phi : G \rightarrow H$ is an isomorphism, show that $\phi^{-1} : H \rightarrow G$ is also an isomorphism. (*Hint*)
- (b) Given that $\phi : G \rightarrow H$ and $\psi : H \rightarrow K$ are isomorphisms, show that $\psi \circ \phi : G \rightarrow K$ is also an isomorphism. (*Hint*)

◇

We said in the previous section that isomorphic groups are “equivalent” in some sense. This fact has a formal mathematical statement as well:

Proposition 20.2.10. Isomorphism is an equivalence relation on groups.

Exercise 20.2.11. Prove Proposition 20.2.10. (*Hint*)

◇

20.3 Examples and generalizations

20.3.1 Examples of isomorphisms

Now that we have a formal definition of what it means for two groups to be isomorphic, let’s look at some more examples, in order to get a good feel for identifying groups that are isomorphic and those that aren’t.

From high school and college algebra we are well familiar with the fact that when you multiply exponentials (with the same bases), the result of this operation is the same as if you had just kept the base and added the exponents. This equivalence of operations is a telltale sign for identifying possible isomorphic groups. The next two examples illustrate this observation.

For our first example, we denote the set of integer powers of 2 as $2^{\mathbb{Z}}$, that is:

$$2^{\mathbb{Z}} \equiv \{\dots, 2^{-2}, 2^{-1}, 2^0, 2^1, 2^2, \dots\}.$$

Exercise 20.3.1. Show that $2^{\mathbb{Z}}$ with the operation of multiplication is a subgroup of \mathbb{Q}^* .

◇

Example 20.3.2. When elements of $2^{\mathbb{Z}}$ are multiplied together, their exponents add: we know this from basic algebra. This suggests there should be an isomorphism between \mathbb{Z} and $2^{\mathbb{Z}}$. In fact, we may define the function

$\phi : \mathbb{Z} \rightarrow 2^{\mathbb{Z}}$ by $\phi(n) = 2^n$. To show that this is indeed an isomorphism, by our definition we must show two things: (a) that the function preserves the operations of the respective groups; and (b) that the function is a bijection:

(a) We may compute

$$\phi(m+n) = 2^{m+n} = 2^m 2^n = \phi(m)\phi(n).$$

(b) By definition the function ϕ is onto the subset $\{2^n : n \in \mathbb{Z}\}$ of \mathbb{Q}^* . To show that the map is injective, assume that $m \neq n$. If we can show that $\phi(m) \neq \phi(n)$, then we are done. Suppose that $m > n$ and assume that $\phi(m) = \phi(n)$. Then $2^m = 2^n$ or $2^{m-n} = 1$, which is impossible since $m - n > 0$.

This completes the proof that $\mathbb{Z} \cong 2^{\mathbb{Z}}$. ◆

Example 20.3.3. As in the previous example, the real powers of e under multiplication acts exactly like addition of those real exponents. This suggests that the function $\psi(x) = e^x$ is an isomorphism between an additive group and a multiplicative group. The reader will complete this proof of this fact as an exercise. ◆

Exercise 20.3.4. Define the function ψ by: $\psi(x) = e^x$ for $x \in \mathbb{R}$.

- (a) Given that the domain of ψ is all real numbers, what is the range of ψ ?
- (b) Prove that $\psi(x)$ is a bijection between its domain and range.
- (c) Find group operations on the domain and range of ψ such that $\psi(x)$ preserves operations; i.e. $\psi(x \cdot y) = \psi(x) \circ \psi(y)$, where \cdot and \circ are the group operations on the domain and range, respectively. Verify that ψ does indeed preserve operations for these two operations.
- (d) Now that we know $\psi(x)$ is an isomorphism, what can we conclude about (\mathbb{R}^+, \cdot) and $(\mathbb{R}, +)$?

◇

Exercise 20.3.5.

- (a) What is the largest possible domain and range of the natural logarithm function $\ln(x)$? (Consider only real logarithms, and not complex-valued logarithms or logarithms of complex numbers.)
- (b) Using the previous exercise, the relation between natural logarithm and exponential function, as well as a result from earlier in this chapter, show that the natural logarithm function is an isomorphism. What are the two isomorphic groups?
- (c) Using the fact that $\log_{10}(x) = \ln(x)/\ln(10)$, show that the base 10 logarithm function is also an isomorphism. What are the two isomorphic groups?
- (d) Given any two positive real numbers (a and b) in scientific notation that are accurate to 3 decimal places, show how you may estimate ab using addition and a table containing the base 10 logarithms of all integers from 100 to 999. For example, how would you compute the product $(1.75 \times 10^{15})(9.53 \times 10^{-27})$?

◇

Exercise 20.3.6. Prove that $\mathbb{Z} \cong n\mathbb{Z}$, for every nonzero integer n .

◇

Exercise 20.3.7. Prove that \mathbb{C}^* is isomorphic to the subgroup of $GL_2(\mathbb{R})$ consisting of all matrices of the form (a and b are real numbers)

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

, where $a^2 + b^2 \neq 0$.

(In your proof, you should verify that this set of matrices is indeed a subgroup of $GL_2(\mathbb{R})$: in other words, check that the determinant is never zero, when $a^2 + b^2 \neq 0$.)

◇

Example 20.3.8. Consider the groups \mathbb{Z}_8 and \mathbb{Z}_{12} . Can you tell right away that there can't be an isomorphism between them? Remember, an isomorphism is a one-to-one and onto function: but since $|\mathbb{Z}_{12}| > |\mathbb{Z}_8|$ there is no onto function from \mathbb{Z}_8 to \mathbb{Z}_{12} , and so they can't be isomorphic to

each other. Similarly it can be shown that any two finite groups that have differing numbers of elements can't be isomorphic to each other. \blacklozenge

Let's look at some more examples where Cayley tables can help determine isomorphism.

Example 20.3.9. The following are the Cayley tables for \mathbb{Z}_4 and $U(5)$.

| | | | | |
|----------|---|---|---|---|
| \oplus | 0 | 1 | 2 | 3 |
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

Table 20.4: Cayley table for \mathbb{Z}_4

| | | | | |
|---------|---|---|---|---|
| \odot | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

Table 20.5: Cayley table for $U(5)$

Notice that the main diagonals (left to right) of the Cayley tables seem to have a different pattern. The main diagonal for \mathbb{Z}_4 is the alternating sequence, 0, 2, 0, 2, while the main diagonal of $U(5)$ is the non-alternating sequence 1, 4, 4, 1. It appears at first sight that these two groups must be non-isomorphic. However, we may rearrange the row and column labels in Table 20.5 to obtain Table 20.6. From the rearranged table we may read off the isomorphism: $0 \rightarrow 1, 1 \rightarrow 2, 2 \rightarrow 4, 3 \rightarrow 3$.

| | | | | |
|---------|---|---|---|---|
| \odot | 1 | 2 | 4 | 3 |
| 1 | 1 | 2 | 4 | 3 |
| 2 | 2 | 4 | 3 | 1 |
| 4 | 4 | 3 | 1 | 2 |
| 3 | 3 | 1 | 2 | 4 |

Table 20.6: Rearranged Cayley table for $U(5)$

Note the important point that when we rearranged the table, we used the *same* ordering (1, 2, 4, 3) for both rows and columns. You don't want to use one ordering for rows, and a different ordering for columns. \blacklozenge

Example 20.3.10. Consider the group of units of \mathbb{Z}_8 and the group of units of \mathbb{Z}_{12} ; i.e. $U(8)$ and $U(12)$. We've seen that these consist of the elements in \mathbb{Z}_8 and \mathbb{Z}_{12} , that are relatively prime to 8 and 12, respectively, so

$$\begin{aligned}U(8) &= \{1, 3, 5, 7\} \\U(12) &= \{1, 5, 7, 11\}.\end{aligned}$$

Exercise 20.3.11. Give the Cayley tables for $U(8)$ and $U(12)$. \diamond

An isomorphism $\phi : U(8) \rightarrow U(12)$ is given by

$$\begin{aligned}1 &\xrightarrow{\phi} 1 \\3 &\xrightarrow{\phi} 5 \\5 &\xrightarrow{\phi} 7 \\7 &\xrightarrow{\phi} 11.\end{aligned}$$

ϕ is one-to-one and onto by observation, and we can verify that ϕ preserves the operations of $U(8)$ and $U(12)$ by showing that replacing elements in the Cayley table of $U(8)$ according to the isomorphism ϕ gives the Cayley table of $U(12)$. Hence $U(8) \cong U(12)$. \blacklozenge

The function ϕ is not the only possible isomorphism between $U(8)$ and $U(12)$.

Exercise 20.3.12.

(a) Using Cayley tables, show that the function ψ defines an isomorphism between $U(8)$ and $U(12)$, where:

$$\begin{aligned}1 &\xrightarrow{\psi} 1 \\3 &\xrightarrow{\psi} 7 \\5 &\xrightarrow{\psi} 11 \\7 &\xrightarrow{\psi} 5.\end{aligned}$$

(You will have to rearrange rows and columns to get the identification between tables.)

- (b) Define a different isomorphism between $U(8)$ and $U(12)$, and use Cayley tables to verify that it's an isomorphism.

◇

Exercise 20.3.13. Prove that both $U(8)$ and $U(12)$ are isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (recall $\mathbb{Z}_2 \times \mathbb{Z}_2$ is the set of all pairs (a, b) with $a, b \in \mathbb{Z}_2$, where the group operation is addition mod 2 on each element in the pair). ◇

Exercise 20.3.14. Prove that $U(8)$ is isomorphic to the group of matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

◇

Exercise 20.3.15. Show that the matrices

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \right. \\ \left. \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

form a group. Find an isomorphism of G with a more familiar group of order 6. ◇

Example 20.3.16. In Example 18.4.26 of the Cosets chapter, we looked at the normal subgroup $N = \{(1), (123), (132)\}$ of S_3 . The cosets of N in S_3 were N and $(12)N$; and the quotient group S_3/N had the following multiplication table.

| | | |
|---------|---------|---------|
| | N | $(12)N$ |
| N | N | $(12)N$ |
| $(12)N$ | $(12)N$ | N |

You may verify that N is in fact the group of all even permutations on three elements, that is A_3 ; and $(12)N = \{(12), (13), (23)\}$ is the set of odd permutations. The information captured in S_3/N is parity; that is, multiplying two even or two odd permutations results in an even permutation, whereas multiplying an odd permutation by an even permutation yields an odd permutation. This suggests a possible isomorphism to \mathbb{Z}_2 . \blacklozenge

Exercise 20.3.17. Prove that the quotient group $S_3/A_3 \cong \mathbb{Z}_2$. \diamond

In Section 18.4.2 of the Cosets chapter we hinted at several examples of possible isomorphisms, which we'll have you prove now:

Exercise 20.3.18. Prove the following:

- (a) $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$
- (b) $D_n/R_n \cong \mathbb{Z}_2$

\diamond

Exercise 20.3.19. Based on your work in Exercise 18.4.27 prove the following:

- (a) $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_6$
- (b) $\mathbb{Z}_{24}/\langle 8 \rangle \cong \mathbb{Z}_8$
- (c) $U(20)/\langle 3 \rangle \cong \mathbb{Z}_2$

\diamond

We've seen several examples where Cayley tables were used to show that two groups are isomorphic. (Of course, this works best if the groups are not too large, and it certainly doesn't work if the groups are infinite!) Let's now consider how we can use Cayley tables to show when groups are *not* isomorphic to each other. Caution: it's not enough to have Cayley tables for the two groups that don't match—we saw in Example 20.3.9 that even when tables don't match, it may still be possible to rearrange one of the tables to create a matchup.

Suppose that if T is a Cayley table of a group G . Then $g \in G$ appears on the diagonal of T if and only if there is an element $g' \in G$ such that $g' \cdot g' = g$. It turns out that this property is preserved under isomorphism:

Proposition 20.3.20. Given a Cayley table T for a finite group G , and let $g \in G$ appear on the diagonal of T . Let $\phi : G \rightarrow H$ be an isomorphism, and let T' be a Cayley table of H . Then $\phi(g)$ appears on the diagonal of T' .

PROOF. As stated above, g appears on the diagonal of T if and only if there exists $g' \in G$ such that $g' \cdot g' = g$. Since ϕ is an isomorphism, this implies $\phi(g') \cdot \phi(g') = \phi(g)$, which in turn implies that $\phi(g)$ appears on the diagonal of T' . \square

Proposition 20.3.21. Given a Cayley table T for a finite group G , and suppose the element $g \in G$ appears m times on the diagonal of T . Let $\phi : G \rightarrow H$ be an isomorphism, and let T' be a Cayley table of H . Then $\phi(g)$ appears m times on the diagonal of T' .

Exercise 20.3.22. Prove Proposition 20.3.21. \diamond

Proposition 20.3.23. Given a Cayley table T for a finite group G , and suppose n distinct elements of G appear on the diagonal of T . Let $\phi : G \rightarrow H$ be an isomorphism, and let T' be a Cayley table of H . Then n distinct elements of H appear on the diagonal of T' .

Exercise 20.3.24. Prove Proposition 20.3.23. \diamond

Exercise 20.3.25. By using the preceding propositions and comparing diagonal elements of Cayley tables, prove that $\mathbb{Z}_4 \not\cong U(12)$. \diamond

Exercise 20.3.26. Prove or disprove: $U(8) \cong \mathbb{Z}_4$. \diamond

Exercise 20.3.27. Let σ be the permutation (12), and let τ be the permutation (34). Let G be the set $\{\text{id}, \sigma, \tau, \sigma\tau\}$ together with the operation of composition.

- (a) Give the Cayley table for the group G .
- (b) Prove or disprove: $G \cong \mathbb{Z}_4$.
- (c) Prove or disprove: $G \cong U(12)$.

◇

Example 20.3.28. Even though D_3 and \mathbb{Z}_6 possess the same number of elements, we might suspect that they are not isomorphic, because \mathbb{Z}_6 is abelian and D_3 is non-abelian. Let's see if the Cayley tables can help us here:

| \circ | id | ρ_1 | ρ_2 | μ_1 | μ_2 | μ_3 |
|----------|----------|----------|----------|----------|----------|----------|
| id | id | ρ_1 | ρ_2 | μ_1 | μ_2 | μ_3 |
| ρ_1 | ρ_1 | ρ_2 | id | μ_3 | μ_1 | μ_2 |
| ρ_2 | ρ_2 | id | ρ_1 | μ_2 | μ_3 | μ_1 |
| μ_1 | μ_1 | μ_2 | μ_3 | id | ρ_1 | ρ_2 |
| μ_2 | μ_2 | μ_3 | μ_1 | ρ_2 | id | ρ_1 |
| μ_3 | μ_3 | μ_1 | μ_2 | ρ_1 | ρ_2 | id |

Table 20.7: Cayley table for D_3

| \oplus | 0 | 1 | 2 | 3 | 4 | 5 |
|----------|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

Table 20.8: Cayley table for \mathbb{Z}_6

Note that the Cayley table for \mathbb{Z}_6 is symmetric across the main diagonal while the Cayley table for D_3 is not. Furthermore, no matter how we rearrange the row and column headings for the Cayley table for \mathbb{Z}_6 , the table will always be symmetric. It follows that there is no way to match up the two groups' Cayley tables: so $D_3 \not\cong \mathbb{Z}_6$.

This argument via Cayley table works in the case where the two groups being compared are both small, but if the groups are large then it's far

too time-consuming (especially if the groups are infinite!). So let us take a different approach, and fall back on our time-tested strategy of proof by contradiction. In the case at hand, this means that we first suppose that $D_3 \cong \mathbb{Z}_6$, and then find a contradiction based on that supposition.

So, suppose that the two groups are isomorphic, which means there exists an isomorphism $\phi : \mathbb{Z}_6 \rightarrow D_3$. Let $a, b \in D_3$ be two elements such that $a \circ b \neq b \circ a$. Since ϕ is an isomorphism, there exist elements m and n in \mathbb{Z}_6 such that

$$\phi(m) = a \quad \text{and} \quad \phi(n) = b.$$

However,

$$a \circ b = \phi(m) \circ \phi(n) = \phi(m \oplus n) = \phi(n \oplus m) = \phi(n) \circ \phi(m) = b \circ a,$$

which contradicts the fact that a and b do not commute. \blacklozenge

Although we have only proven the non-isomorphism of abelian and non-abelian groups for one particular case, the same method of proof can be used to prove the following general result.

Proposition 20.3.29. If G is an abelian group and H is a non-abelian group, then $G \not\cong H$.

Exercise 20.3.30. Prove Proposition 20.3.29 by imitating the proof in Example 20.3.28. \blacklozenge

Exercise 20.3.31. Prove $D_4 \not\cong \mathbb{Z}_8$. \blacklozenge

Exercise 20.3.32. Prove $\mathbb{Z}/6\mathbb{Z} \not\cong S_3$. \blacklozenge

Finally, let's look at \mathbb{Z} and \mathbb{R} . We know \mathbb{Z} is a cyclic group with 1 as the generator, while \mathbb{R} is not cyclic. (Do you remember why?) We might suspect that $\mathbb{Z} \not\cong \mathbb{R}$, since one group is cyclic and the other isn't. This is in fact true, and we'll prove it. Since \mathbb{Z} and \mathbb{R} are infinite groups we can't use Cayley tables, so we have to use another method (three guesses as to what it is):

Proposition 20.3.33. \mathbb{Z} is not isomorphic to \mathbb{R} .

PROOF. We will use a proof by contradiction. Suppose that there exists an isomorphism $\phi : \mathbb{Z} \rightarrow \mathbb{R}$. Choose any $x \in \mathbb{R}$, and let $m \in \mathbb{Z}$ be the pre-image of x , so that $\phi(m) = x$. It follows that:

$$x = \phi(m) = \phi(\underbrace{1 + \dots + 1}_{m \text{ times}}) = \underbrace{\phi(1) + \dots + \phi(1)}_{m \text{ times}}.$$

Thus $x \in \langle \phi(1) \rangle$. But since this is true for *any* $x \in \mathbb{R}$, this means that $\phi(1)$ is a generator of \mathbb{R} , which means that \mathbb{R} is cyclic. But we've already seen that \mathbb{R} is *not* cyclic. This contradiction shows that our original supposition must be false: namely, there *cannot* exist an isomorphism $\phi : \mathbb{Z} \rightarrow \mathbb{R}$. This completes the proof. \square

Again we can generalize this proof to prove that a cyclic group cannot be isomorphic to a non-cyclic group. The contrapositive of this statement is:

Proposition 20.3.34. If G is cyclic and $G \cong H$, then H is also cyclic.

Exercise 20.3.35. Prove Proposition 20.3.34. (*Hint*) \diamond

Exercise 20.3.36.

- (a) Prove that \mathbb{Q} is not isomorphic to \mathbb{Z} .
- (b) Prove that $\mathbb{Z}_3 \times \mathbb{Z}_3$ is not isomorphic to \mathbb{Z}_9 .
- (c) Prove that $D_4 \not\cong \mathbb{Z}_{24}/\langle 8 \rangle$

\diamond

In the foregoing examples, the reader might develop the impression that isomorphisms must be functions between two different groups. But such is not the case! It is quite possible for a group to be isomorphic to itself.

Exercise 20.3.37.

- (a) Given any group G , let $\text{Id} : G \rightarrow G$ be the identity map, that is, $\text{Id}(g) = g$ for all $g \in G$. show that Id is an isomorphism.

- (b) Let $\mathbb{M}_n(\mathbb{R})$ be the group of $n \times n$ matrices with real entries under the addition operation. Prove that the transpose function $M \rightarrow M^T$ is an isomorphism from $\mathbb{M}_n(\mathbb{R})$ to $\mathbb{M}_n(\mathbb{R})$.

◇

An isomorphism from a group to itself is called an *automorphism*.

20.3.2 General properties of isomorphisms

In the last two sections we proved several properties of isomorphic groups and their corresponding isomorphisms. We collect these properties (and add a few more) in the following proposition:

Proposition 20.3.38. Let $\phi : G \rightarrow H$ be an isomorphism of two groups. Then the following statements are true.

- (1) $|G| = |H|$.
- (2) $\phi^{-1} : H \rightarrow G$ is an isomorphism.
- (3) G is abelian if and only if H is abelian.
- (4) G is cyclic if and only if H is cyclic.
- (5) If $g \in G$ is an element of order n (that is, $|\langle g \rangle| = n$), then $\phi(g) \in H$ is also an element of order n .
- (6) If G' is a subgroup of G , then $\phi(G')$ is a subgroup of H and $G' \cong \phi(G')$ (Recall that $\phi(G') = \{\phi(g), g \in G'\}$.)

PROOF. Assertion (1) follows from the fact that ϕ is a bijection. The proofs of (2)–(6) are indicated in the following exercises.

Exercise 20.3.39.

- (a) Show part (2) of Proposition 20.3.38. (*Hint*)
- (b) Show part (3) of Proposition 20.3.38. (*Hint*)
- (c) Show part (4) of Proposition 20.3.38. (*Hint*)

◇

Exercise 20.3.40. Suppose, G, H, ϕ are as given in Proposition 20.3.38, and suppose $g \in G$ is an element of order n , where $n > 1$. Show that $\phi(g)^k \neq \text{id}_H$ for $k = 1, \dots, n-1$, where id_H is the identity of H . Use your result to prove part (5) of Proposition 20.3.38. ◇

We will complete the proof of part (6) in two steps:

Step (I): $\phi(G')$ is a subgroup of H ;

Step (II): $\phi(G')$ is isomorphic to G' .

Exercise 20.3.41. Fill in the blanks of the following proof of Step (I) (that is, $\phi(G')$ is a subgroup of H):

Let us suppose that G' is a subgroup of G . We claim that $\phi(G')$ is actually a subgroup of < 1 >. To show this, by Proposition 15.4.15 it's enough to show that if h_1 and h_2 are elements of $\phi(G')$, then $h_1 h_2^{-1}$ is also an element of < 2 >.

Now given that $h_1, h_2 \in \phi(G')$, by the definition of $\phi(G')$ it must be true that there exist $g_1, g_2 \in$ < 3 > such that $\phi(g_1) = h_1, \phi(g_2) = h_2$. But then we have

$$\begin{aligned} h_1 h_2^{-1} &= \phi(g_1) \phi(g_2)^{-1} && \text{(by substitution)} \\ &= \phi(g_1) \phi(g_2^{-1}) && \text{(by Proposition < 4 >)} \\ &= \phi(g_1 g_2^{-1}) && \text{(by the definition of < 5 >).} \end{aligned}$$

Since $g_1 g_2^{-1}$ is an element of G' , it follows that $h_1 h_2^{-1} \in$ < 6 >. This completes the proof of Step (I). ◇

Exercise 20.3.42. Complete the following proof of Step (II) (that is, G' and $\phi(G')$ are isomorphic).

Consider the function ϕ restricted to the set G' : that is, $\phi : G' \rightarrow \phi(G')$. To prove this gives an isomorphism from G' to $\phi(G')$, we need to show (i) $\phi : G' \rightarrow \phi(G')$ is a bijection; and (ii) $\phi : G' \rightarrow \phi(G')$ has the operation-preserving property.

To show (i), we note that by the definition of $\phi(G')$, for every $h \in \phi(G')$ there exists a $g \in \underline{\langle 1 \rangle}$ such that $\phi(\underline{\langle 2 \rangle}) = h$. It follows that ϕ maps G' onto $\underline{\langle 3 \rangle}$. Also, if $g_1, g_2 \in G'$ and $\phi(g_1) = \phi(g_2)$, then since ϕ is a one-to-one function on G it follows that $g_1 = \underline{\langle 4 \rangle}$. From this it follows that ϕ is also a one-to-one function on $\underline{\langle 5 \rangle}$. We conclude that $\underline{\langle 6 \rangle}$ is a bijection.

To show (ii), given $g_1, g_2 \in \underline{\langle 7 \rangle}$ we have that $\phi(g_1 g_2) = \underline{\langle 8 \rangle}$ since by assumption ϕ is an isomorphism from $\underline{\langle 9 \rangle}$ to $\underline{\langle 10 \rangle}$. This implies that ϕ also has the operation-preserving property when it's considered as a function from $\underline{\langle 11 \rangle}$ to $\underline{\langle 12 \rangle}$. This completes the proof of Step (II). \diamond

□

Exercise 20.3.43. Prove S_4 is not isomorphic to D_{12} . \diamond

Exercise 20.3.44. Prove A_4 is not isomorphic to D_6 . (Recall that A_4 is the alternating group (group of even permutations) on 4 letters.) \diamond

Exercise 20.3.45. The *quaternion group* (denoted by Q_8) was introduced in Example 15.2.8 and Exercise 15.2.9. Show that the quaternion group is not isomorphic to D_4 . \diamond

20.4 Classification up to isomorphism

We have been emphasizing that two groups that are isomorphic are the “same” as far as all group properties are concerned. So if we can characterize a class of groups as isomorphic to a well-understood set of groups, then all of the properties of the well-understood groups carry over to the entire class of groups. We will see two examples of this in the following subsections.

20.4.1 Classifying cyclic groups

Our first classification result concerns cyclic groups.

Proposition 20.4.1. If G is a cyclic group of infinite order, then G is isomorphic to \mathbb{Z} .

PROOF. Let G be a cyclic group with infinite order and suppose that a is a generator of G . Define a map $\phi : \mathbb{Z} \rightarrow G$ by $\phi : n \mapsto a^n$. Then

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n).$$

To show that ϕ is one-to-one, suppose that m and n are two elements in \mathbb{Z} , where $m \neq n$. We can assume that $m > n$. We must show that $a^m \neq a^n$. Let us suppose the contrary; that is, $a^m = a^n$. In this case $a^{m-n} = e$, where $m-n > 0$, which contradicts the fact that a has infinite order. Our map is onto since any element in G can be written as a^n for some integer n and $\phi(n) = a^n$. \square

Exercise 20.4.2.

- (a) Using Proposition 20.4.1, prove again that $\{2^n | n \in \mathbb{Z}\} \cong \mathbb{Z}$.
 (b) Give a similar proof that $n\mathbb{Z} \cong \mathbb{Z}$, for every nonzero integer n .

\diamond

Proposition 20.4.3. If G is a cyclic group of order n , then G is isomorphic to \mathbb{Z}_n .

PROOF. Let G be a cyclic group of order n generated by a and define a map $\phi : \mathbb{Z}_n \rightarrow G$ by $\phi : k \mapsto a^k$, where $0 \leq k < n$. The proof that ϕ is an isomorphism is left as the next exercise. \square

Exercise 20.4.4. Prove that ϕ defined in Proposition 20.4.3 is an isomorphism. \diamond

Exercise 20.4.5.

- (a) In fact, the *converse* of Proposition 20.4.3 is true: that is, If G is isomorphic to \mathbb{Z}_n then G is a cyclic group of order n . How do we know this? (*Hint*)
 (b) Is the converse of Proposition 20.4.1 also true? *Justify* your answer.

◇

Exercise 20.4.6. Show that the multiplicative group of the complex n th roots of unity is isomorphic to \mathbb{Z}_n . ◇

Proposition 20.4.7. If G is a group of order p , where p is a prime number, then G is isomorphic to \mathbb{Z}_p .

Exercise 20.4.8. Prove Proposition 20.4.7 (*Hint*). ◇

20.4.2 Characterizing all groups: Cayley's theorem

In the previous section, we saw that any cyclic group is “equivalent” (in the sense of isomorphism) to one of the groups \mathbb{Z}_n . This enables us to easily conceptualize any cyclic group in terms of a standardized set of groups that we're very familiar with.

Now, can we do something similar with *all* groups? In other words, can we find a standardized set of groups so that any group can be characterized as equivalent (up to isomorphism) to one of these standard groups?.

In a way we already have a standardized characterization of finite groups, because we have seen that every finite group can be represented with a Cayley table. But this is not really satisfactory, because there are many Cayley tables which do not correspond to any group.

Exercise 20.4.9. Give examples of Cayley tables for binary operations that meet each of the following criteria. (You can make your row and column labels be the set of integers $\{1, 2, \dots, n\}$, for an appropriate value of n .)

- (a) The binary operation has no identity.
- (b) The binary operation has an identity, but not inverses for every element
- (c) *The binary operation has an identity and inverses, but the associative law fails.

◇

Although Cayley tables are not adequate for our purpose, it turns out that they provide the key to the characterization we're seeking. Consider first the following simple example.

Example 20.4.10. The Cayley table for \mathbb{Z}_3 is

| | | | |
|----------|---|---|---|
| \oplus | 0 | 1 | 2 |
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

The addition table of \mathbb{Z}_3 suggests that it is isomorphic to the permutation group $\{\text{id}, (012), (021)\}$. One possible isomorphism is

$$\begin{aligned} 0 &\mapsto \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix} = \text{id} \\ 1 &\mapsto \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix} = (012) \\ 2 &\mapsto \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix} = (021). \end{aligned}$$

Notice the interesting “coincidence” that the rows of the Cayley table ($(0\ 1\ 2)$, $(1\ 2\ 0)$ and $(2\ 1\ 0)$ respectively) “just happen” to agree exactly with the second rows of the three tableaus!

Of course, this “coincidence” is no accident. For example, the second row of the Cayley table is obtained as $(1 \oplus 0\ 1 \oplus 1\ 1 \oplus 2)$, and the permutation $\begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$ that is the isomorphic image of 1 is actually the function from $\mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ that takes n to $1 \oplus n$. ◆

In Example 20.4.10 it was fairly easy to obtain permutations directly from the Cayley table, because the elements of the group were 0, 1, 2. But what if the group has different elements? No problem—we can just relabel the elements, and then read off the permutations in the same way, as the following exercise shows:

Exercise 20.4.11.

- (a) Give the Cayley table for $U(8)$.
- (b) Rewrite the table you gave in (a) except make the following replacements: $1 \rightarrow 1, 3 \rightarrow 2, 5 \rightarrow 3, 7 \rightarrow 4$.
- (c) From the table you created in (b), obtain 4 permutations from the 4 rows of the Cayley table (just as we did in Example 20.4.10).
- (d) Give the Cayley table for the four permutations that you obtained in (c).
- (e) Explain how your result shows that $U(8)$ is isomorphic to a subgroup of the permutation group $S(4)$.

◇

What we've discovered in Example 20.4.10 and Exercise 20.4.11 can be generalized to any finite group of any size, whether abelian or nonabelian:

Proposition 20.4.12. (*Cayley's theorem*) Every finite group is isomorphic to a group of permutations.

PROOF. Let G be a group with $|G|$ elements. We seek a group of permutations $P \subset S_{|G|}$ that is isomorphic to G . For any $g \in G$ we may define a function $\phi_g : G \rightarrow G$ by

$$\phi_g(a) := ga.$$

We claim that ϕ_g is a permutation on G : you will show this in Exercise 20.4.13 below. Let us define the set $P \subset S_{|G|}$ as

$$P = \{\phi_g : g \in G\}.$$

Let us now define a function $\Phi : G \rightarrow P$ just as we did in Example 20.4.10:

$$\Phi(g) := \phi_g.$$

Let's pause for a minute here, to make sure that you understand what's going on. According to the definition, Φ is a function whose domain is the group G and whose range is a subset of the permutation group on $|G|$ letters. Now permutations are functions in their own right: so Φ is a function (from G to P), and for each $g \in G$, $\Phi(g)$ is *also* a function (from G to G). We could say that Φ is a function-valued function. (This can be quite unnerving the first time you see it – but such constructions are common in higher mathematics,

so it's best to get used to them!) In this case, you should understand that $\Phi(g)$ is a permutation, and $\Phi(g)(a)$ is the permutation $\Phi(g)$ applied to the group element a . According to the definition of $\Phi(g)$, $\Phi(g)(a)$ is equal to $\phi_g(a)$, which by the definition of ϕ_g is equal to ga .

OK, now let's get back to the argument. To show that Φ is an isomorphism, we must show that Φ is one-to-one, onto, and preserves the group operation. You will show that Φ is one-to-one and onto in Exercise 20.4.13 below. To show that Φ preserves the group operation, we need to show that $\Phi(gh) = \Phi(g) \circ \Phi(h)$ for any elements $g, h \in G$. We may show this element-by-element: that is, we show that $\Phi(gh)(a) = (\Phi(g) \circ \Phi(h))(a)$ for an arbitrary $a \in G$ as follows:

$$\begin{aligned} \Phi(gh)(a) &= (gh)a && \text{[definition of } \Phi(gh)\text{]} \\ &= g(ha) && \text{[associativity of } G\text{]} \\ &= g(\Phi(h)(a)) && \text{[definition of } \Phi(h)\text{]} \\ &= \Phi(g) \circ \Phi(h)(a). && \text{[definition of } \Phi(g)\text{]} \end{aligned}$$

□

Exercise 20.4.13.

- (a) Show that $\phi_g : G \rightarrow G$ defined in the above proof is a permutation on G . (It is enough to show that ϕ_g is one-to-one and onto.)
- (b) Complete the proof of Proposition 20.4.12 by showing that $\Phi : G \rightarrow P$ is one-to-one and onto.

◇

The isomorphism $\Phi : G \rightarrow S_{|G|}$ defined in the above proof is known as the *left regular representation* of G .

Exercise 20.4.14.

- (a) Using the left regular representation, find a subgroup of $S(6)$ that is isomorphic to $U(7)$.
- (b) Using the left regular representation, find a subgroup of $S(8)$ that is isomorphic to $U(16)$.

◇

This isomorphism Φ defined in Proposition 20.4.12 is not the only possible isomorphism between G and S_G . Another isomorphism is presented in the following exercise.

Exercise 20.4.15. The *right regular representation* $\tilde{\Phi} : G \rightarrow S_{|G|}$ is defined as follows. For any $g \in G$ define the function $\tilde{\phi}_g : G \rightarrow G$ by

$$\tilde{\sigma}_g(a) := ag^{-1}.$$

Define the set \tilde{P} as

$$\tilde{P} = \{\tilde{\phi}_g : g \in G\},$$

and define the function $\tilde{\Phi} : G \rightarrow \tilde{P}$ as

$$\tilde{\Phi}(g) := \tilde{\phi}_g.$$

- Show that $\tilde{\phi}_g : G \rightarrow G$ defined in the above proof is a permutation on G . (It follows that the set \tilde{P} is a subset of $S_{|G|}$.)
- Show that $\tilde{\Phi} : G \rightarrow \tilde{P}$ is one-to-one and onto.
- Complete the proof that $G \cong \tilde{P}$ by showing that $\tilde{\Phi}$ preserves the group operation, that is: $\tilde{\Phi}(gh) = \tilde{\Phi}(g) \circ \tilde{\Phi}(h)$ for any elements $g, h \in G$.

◇

Exercise 20.4.16.

- Give the isomorphism based on the right regular representation for the group \mathbb{Z}_3 . Is this isomorphism different from the isomorphism in Example 20.4.10?
- Give the isomorphism based on the right regular representation for the group \mathbb{Z}_3 . Is this isomorphism different from the isomorphism in Exercise 20.4.11?

◇

Exercise 20.4.17.

- (a) Using the right regular representation, find a subgroup of $S(6)$ that is isomorphic to $U(7)$.
- (b) Using the right regular representation, find a subgroup of $S(8)$ that is isomorphic to $U(16)$.

◇

Remark 20.4.18. (*historical background*) Arthur Cayley was born in England in 1821, though he spent much of the first part of his life in Russia, where his father was a merchant. Cayley was educated at Cambridge, where he took the first Smith's Prize in mathematics. A lawyer for much of his adult life, he wrote several papers in his early twenties before entering the legal profession at the age of 25. While practicing law he continued his mathematical research, writing more than 300 papers during this period of his life. These included some of his best work. In 1863 he left law to become a professor at Cambridge. Cayley wrote more than 900 papers in fields such as group theory, geometry, and linear algebra. His legal knowledge was very valuable to Cambridge; he participated in the writing of many of the university's statutes. Cayley was also one of the people responsible for the admission of women to Cambridge. △

20.5 Direct products and classification of abelian groups

In Section 8.1 we introduced the notion of the Cartesian product of sets. The formal definition is given in Definition 8.1.3—the basic idea is to take the set of all pairs of elements (a, b) where a is an element of the first set and b is an element of the second. A simple example to keep in mind is $\mathbb{R} \times \mathbb{R}$, which is the plane with Cartesian coordinates (x, y) . Notice that $\mathbb{R} \times \mathbb{R}$ is an additive group, where the addition is defined by performing addition separately on both coordinates.

It turns out that this example can be generalized. Given two groups G and H , it is possible to construct a new group based on the Cartesian product $G \times H$. Even more exciting, it is sometimes possible to “factor” a large group by expressing it as the Cartesian product of smaller groups. In this case, all of the properties of the large group can be derived from the properties of the

smaller groups, which can lead to tremendous simplification. This process of factoring groups into simpler groups can be compared to the factorization of integers into primes. (We will in fact see some deep connections between these two processes.)

We begin by showing that the Cartesian product of groups does indeed yield a group.

20.5.1 Direct Products

If (G, \cdot) and (H, \circ) are groups, then we can make the Cartesian product of G and H into a new group. As a set, our group is just the ordered pairs $(g, h) \in G \times H$ where $g \in G$ and $h \in H$. We can define a binary operation on $G \times H$ by

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2);$$

that is, we just multiply elements in the first coordinate as we do in G and elements in the second coordinate as we do in H . We have specified the particular operations \cdot and \circ in each group here for the sake of clarity; we usually just write $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$.

Proposition 20.5.1. Let G and H be groups. The set $G \times H$ is a group under the operation $(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2)$ where $g_1, g_2 \in G$ and $h_1, h_2 \in H$.

The proof is outlined in the following exercise.

Exercise 20.5.2.

- (a) Show that the set $G \times H$ is closed under the binary operation defined in Proposition 20.5.1.
- (b) Show that (e_G, e_H) is the identity of $G \times H$, where e_G and e_H are the identities of the groups G and H respectively.
- (c) Show that the inverse of $(g, h) \in G \times H$ is (g^{-1}, h^{-1}) .
- (d) Show that the operation defined in Proposition 20.5.1 is associative.

(*Hint*)

◇

The group $G \times H$ is called the *direct product* of G and H . Notice the important difference between ‘Cartesian product’ and ‘direct product’: the direct product is a group whose underlying set is a Cartesian product; but in addition, the direct product has a group operation, which generic off-the-shelf Cartesian products don’t ordinarily have.

Example 20.5.3. Let \mathbb{R} be the group of real numbers under addition. The Cartesian product of \mathbb{R} with itself, $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$, is also a group, in which the group operation is just addition in each coordinate; that is, $(a, b) + (c, d) = (a + c, b + d)$. The identity is $(0, 0)$ and the inverse of (a, b) is $(-a, -b)$. \blacklozenge

Example 20.5.4. Let \mathbb{R}^* be the group of real numbers under multiplication. The Cartesian product of \mathbb{R}^* with itself, $\mathbb{R}^* \times \mathbb{R}^*$, is also a group, in which the group operation is given by $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$. \blacklozenge

Exercise 20.5.5.

- (a) Find the identity of the group $\mathbb{R}^* \times \mathbb{R}^*$ that was introduced in Example 20.5.4
- (b) Find the inverse of the element $(a, b) \in \mathbb{R}^* \times \mathbb{R}^*$.

\diamond

Exercise 20.5.6.

- (a) Consider the function $f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{C}$ defined by $f((a, b)) = a + bi$. Prove or disprove whether f is an isomorphism.
- (b) Consider the function $g : \mathbb{R}^* \times \mathbb{R}^* \rightarrow \mathbb{C}^*$ defined by $f((a, b)) = a + bi$. Prove or disprove whether g is an isomorphism. (Note that the function g is almost identical to f as far as sets are concerned, but the group operations behave quite differently.)

\diamond

Example 20.5.7. We have previously seen that the elements of the dihedral group D_4 can be listed as $\{id, r, r^2, r^3, sr, sr^2, sr^3\}$ where r is counterclockwise rotation by $\pi/2$ and s is a reflection. We also know that $S = \{1, s\}$

and $R_4 = \{id, r, r^2, r^3\}$ are subgroups of D_4 and thus groups in their own right. It is very tempting to conjecture that D_4 can be written as $S \times R_4$, where the notation (s^j, r^k) is just another way of writing $s^j r^k$ for $j = 0, 1$ and $k = 0, 1, 2, 3$. But as it happens, this doesn't work out: things are not so simple (and much more interesting!), as you will show in the following exercise. \blacklozenge

Exercise 20.5.8. Consider the function $f : S \times R_4 \rightarrow D_4$ defined by $f((s^j, r^k)) = s^j r^k$ for $j = 0, 1$ and $k = 0, 1, 2, 3$. Give an example of two elements for which the operation preserving property fails. \diamond

One may notice from Example 20.5.7 that S and R_4 were abelian groups, and D_4 is not. Our experience with this example suggests that this may be a recipe for failure—perhaps it's not possible to take the direct product of abelian groups and get a nonabelian group. This time our conjecture is correct, as you will show in the following exercise.

Exercise 20.5.9.

- (a) Suppose that the groups G and H are abelian. Prove that $G \times H$ is also abelian.
- (b) * Show the *converse* of part (a): that is, given that $G \times H$ is abelian, then G and H must both be abelian. (*Hint*)

\diamond

So that takes care of abelian groups. Another important type of group is cyclic groups. We'll talk a lot more later about direct products of cyclic groups. For now, let's consider first of all whether the product of cyclic groups is always cyclic:

Example 20.5.10. Consider

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}.$$

Although $\mathbb{Z}_2 \times \mathbb{Z}_2$ and \mathbb{Z}_4 both contain four elements, they are not isomorphic. We can prove this by noting that \mathbb{Z}_4 is cyclic, while every element (a, b) in $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2 (verify this). \blacklozenge

So we've shown that the direct product of cyclic groups is not necessarily cyclic. How about the converse: that is, if a direct product is cyclic, are the factor groups necessarily cyclic? This time, the answer is yes:

Exercise 20.5.11. Prove the following statement: Suppose G and H are groups, and $G \times H$ is cyclic. Then G and H are both cyclic. (*Hint*) \diamond

Let's now consider a different type of question. What's the difference between $G \times H$ and $H \times G$? Not much, as the following exercise shows:

Exercise 20.5.12. Show that for any two groups G and H , $G \times H \cong H \times G$. (*Hint*) \diamond

So far we've been considering the products of two groups. But there's no reason to stop with two! The direct product

$$\prod_{i=1}^n G_i = G_1 \times G_2 \times \cdots \times G_n$$

of the groups G_1, G_2, \dots, G_n may be defined in a similar way.

Exercise 20.5.13. How would you write an element in $\prod_{i=1}^n G_i$? Write two different elements of $\prod_{i=1}^n G_i$, and show how you would define the group operation in terms of these two elements. (You may denote the group operation on each group G_i by the symbol ' \cdot '.) \diamond

If we're taking the direct product of copies of the same group, we may use power notation: $G \times G = G^2$, $G \times G \times G = G^3$, and so on.

Example 20.5.14. The group \mathbb{Z}_2^n , considered as a set, is just the set of all binary n -tuples. The group operation is the "exclusive or" of two binary n -tuples. For example, the following equation is true in \mathbb{Z}_2^8 :

$$(01011101) + (01001011) = (00010110).$$

The groups $\{\mathbb{Z}_2^n, n = 1, 2, 3, \dots\}$ are important in coding theory and cryptography, as well as other areas of computer science. \blacklozenge

The result of Exercise 20.5.9 is generalized in the following proposition:

Proposition 20.5.15. Let G_1, G_2, \dots, G_n be groups. Then $\prod_{i=1}^n G_i$ is abelian if and only if all of the groups G_1, G_2, \dots, G_n are abelian.

Exercise 20.5.16. Use induction and the results of Exercise 20.5.9 to prove Proposition 20.5.15 \diamond

The result of Exercise 20.5.18 may be similarly generalized:

Proposition 20.5.17. Suppose G_1, \dots, G_n are groups, and $\prod_{i=1}^n G_i$ is cyclic. Then all of the groups G_1, G_2, \dots, G_n are cyclic.

Exercise 20.5.18. Prove Proposition 20.5.17 \diamond

By extending the results of Exercise 20.5.12, we find that we can rearrange the groups in a direct product arbitrarily and still end up with the “same” group:

Proposition 20.5.19. Let G_1, G_2, \dots, G_n be arbitrary groups, and let $\sigma \in S_n$ be any permutation on $\{1, 2, \dots, n\}$. Then

$$G_1 \times G_2 \times \dots \times G_n \cong G_{\sigma(1)} \times G_{\sigma(2)} \times \dots \times G_{\sigma(n)}.$$

The following exercise outlines the proof of Proposition 20.5.19.

Exercise 20.5.20.

- (a) What function would you define in order to prove Proposition 20.5.19?
- (b) Prove that the function that you defined in (a) is a bijection by showing that it has an inverse.
- (c) Prove that the function that you defined in (a) preserves group operations, and hence is an isomorphism.

\diamond

Suppose you start out with groups that are isomorphic, and take direct products of them. Are the direct products also isomorphic? It just so happens that they are:

Proposition 20.5.21. Suppose that $G_1 \cong H_1, G_2 \cong H_2, \dots, G_n \cong H_n$. Then $G_1 \times \dots \times G_n \cong H_1 \times \dots \times H_n$.

We won't give the full proof, but you can get the idea of how it goes by doing the following exercise.

Exercise 20.5.22. Prove Proposition 20.5.21 for the case where $n = 2$. (Remember that the default method for proving that groups are isomorphic is to define a suitable function and prove that it's an isomorphism.) \diamond

20.5.2 Classifying finite abelian groups by factorization

We have used isomorphisms to classify cyclic groups (Proposition 20.4.1), as well as to characterize groups in general (Cayley's theorem, Proposition 20.4.12). In this section, we will make use of direct products to prove a classification of finite abelian groups up to isomorphism. The bottom line is that every finite abelian group is isomorphic to a direct product of cyclic groups of prime power orders. To get to this bottom line, we'll have to establish some more properties of direct products, especially in relation to cyclic groups. The following proposition characterizes the order of the elements in a direct product.

Proposition 20.5.23. Let $(g, h) \in G \times H$. If g and h have finite orders r and s respectively, then the order of (g, h) in $G \times H$ is the least common multiple of r and s .

PROOF. Suppose that m is the least common multiple of r and s and let $n = |(g, h)|$. Then

$$\begin{aligned}(g, h)^m &= (g^m, h^m) = (e_G, e_H) \\ (g^n, h^n) &= (g, h)^n = (e_G, e_H).\end{aligned}$$

Hence, n must divide m , and $n \leq m$. However, by the second equation, both r and s must divide n ; therefore, n is a common multiple of r and s . Since m is the *least* common multiple of r and s , $m \leq n$. Consequently, m must be equal to n . \square

By applying Proposition 20.5.23 inductively, it is possible to prove an analogous result for direct products of more than two groups. We'll leave it to you to fill in the details of the proof.

Proposition 20.5.24. Let $(g_1, \dots, g_n) \in \prod_{i=1}^n G_i$. If g_i has finite order r_i in G_i , then the order of (g_1, \dots, g_n) is the least common multiple of r_1, \dots, r_n .

Exercise 20.5.25. Prove Proposition 20.5.24 using induction. \diamond

For the rest of the section, we'll be dealing with direct products of \mathbb{Z}_n (keep in mind that any cyclic group is isomorphic to \mathbb{Z}_n for some n).

Example 20.5.26. Let $(8, 56) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60}$. Since $\gcd(8, 12) = 4$, the order of 8 is $12/4 = 3$ in \mathbb{Z}_{12} . Similarly, the order of 56 in \mathbb{Z}_{60} is 15. The least common multiple of 3 and 15 is 15; hence, $(8, 56)$ has order 15 in $\mathbb{Z}_{12} \times \mathbb{Z}_{60}$. \blacklozenge

Example 20.5.27. The group $\mathbb{Z}_2 \times \mathbb{Z}_3$ consists of the pairs

$$(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2).$$

In this case, unlike that of $\mathbb{Z}_2 \times \mathbb{Z}_2$ and \mathbb{Z}_4 , it is true that $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. We need only show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic. By trial and error, we may find that $(1, 1)$ is a generator for $\mathbb{Z}_2 \times \mathbb{Z}_3$, so that $\mathbb{Z}_2 \times \mathbb{Z}_3 = \langle (1, 1) \rangle$. \blacklozenge

Exercise 20.5.28. Find the order of each of the following elements.

- (a) $(3, 4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_6$
- (b) $(6, 15, 4)$ in $\mathbb{Z}_{30} \times \mathbb{Z}_{45} \times \mathbb{Z}_{24}$
- (c) $(5, 10, 15)$ in $\mathbb{Z}_{25} \times \mathbb{Z}_{25} \times \mathbb{Z}_{25}$
- (d) $(8, 8, 8)$ in $\mathbb{Z}_{10} \times \mathbb{Z}_{24} \times \mathbb{Z}_{80}$

\diamond

Exercise 20.5.29.

- (a) Show that $\mathbb{Z}_4 \times \mathbb{Z}_9$ is cyclic, and find 6 different generators for the group.
- (b) Show that $\mathbb{Z}_3 \times \mathbb{Z}_5$ is cyclic. How many different generators does it have?

- (c) Show that $\mathbb{Z}_4 \times \mathbb{Z}_6$ is *not* cyclic by showing that none of its elements is a generator (i.e. all elements have order less than 24).

◇

The next proposition tells us exactly when the direct product of two cyclic groups is cyclic.

Proposition 20.5.30. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is isomorphic to \mathbb{Z}_{mn} if and only if $\gcd(m, n) = 1$.

PROOF. Assume first that if $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, then $\gcd(m, n) = 1$. To show this, we will prove the contrapositive; that is, we will show that if $\gcd(m, n) = d > 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n$ cannot be cyclic. Notice that mn/d is divisible by both m and n ; hence, for any element $(a, b) \in \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\underbrace{(a, b) + (a, b) + \cdots + (a, b)}_{mn/d \text{ times}} = (0, 0).$$

Therefore, no (a, b) can generate all of $\mathbb{Z}_m \times \mathbb{Z}_n$.

The converse follows directly from Proposition 20.5.23 since $\text{lcm}(m, n) = mn$ if and only if $\gcd(m, n) = 1$. \square

Recall that Proposition 20.4.3 says that a group of order mn is cyclic if and only if it is isomorphic to \mathbb{Z}_{mn} . So Proposition 20.5.30 tells us that the product of two cyclic groups is cyclic if and only if their orders are relatively prime.

This idea extends directly to arbitrary direct products: a product of cyclic groups is cyclic if and only if the orders of the groups in the product are all relatively prime.

Proposition 20.5.31. Let n_1, \dots, n_k be positive integers. Then

$$\prod_{i=1}^k \mathbb{Z}_{n_i} \cong \mathbb{Z}_{n_1 \cdots n_k}$$

if and only if $\text{lcm}(n_1, \dots, n_k) = \prod_{i=1}^k n_i$ (in other words, n_1, \dots, n_k are all relatively prime).

PROOF. Use the argument in Proposition 20.5.30 first with n_1 and n_2 , then with n_1n_2 and n_3 , then with $n_1n_2n_3$ and n_4 , and so on. (The best way to do this proof is using induction.) \square

Exercise 20.5.32. Prove Proposition 20.5.31 using induction. \diamond

A special case of this proposition is:

Corollary 20.5.33. If

$$m = p_1^{e_1} \cdots p_k^{e_k},$$

where the p_i 's are distinct primes, then

$$\mathbb{Z}_m \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}.$$

PROOF. Since $\gcd(p_i^{e_i}, p_j^{e_j}) = 1$ for $i \neq j$, the proof follows from the Corollary to 20.5.31. \square

Exercise 20.5.34. Find three non-isomorphic abelian groups of order 8, and show that they are not isomorphic. \diamond

Remember that in the Permutations chapter we showed that every permutation can be “factored” as the product of disjoint cycles. (At that time, we compared this to the factorization of integers into prime factors). It turns out that finite abelian groups can also be “factored”. This beautiful and general result is summarized in the following proposition. We will not give a complete proof of the proposition (which uses induction), but we hope that it makes sense to you in light of what we’ve seen so far.¹

Proposition 20.5.35. (*Factorization of finite abelian groups*) If G is a finite abelian group, then there exist prime numbers $p_1 \dots p_k$ and exponents $e_1 \dots e_k$ such that

$$G \cong \mathbb{Z}_{p_1^{e_1}} \times \cdots \times \mathbb{Z}_{p_k^{e_k}}$$

Note that the prime numbers p_1, \dots, p_k may not necessarily be distinct.

¹Many proofs can be found on the web: search for “structure of finite abelian groups”.

Remark 20.5.36. Proposition 20.5.19 informs us that these factors can be written in any order, because all rearrangements of a direct product are isomorphic to each other. \triangle

Exercise 20.5.37.

- (a) It turns out that for each k , the number $p_k^{e_k}$ in Proposition 20.5.35 is the largest power of p_k that divides $|G|$. How do we know this?
- (b) For the group G in Proposition 20.5.35, if q is any prime number that is not equal to any of the primes p_1, \dots, p_n , then G has no element of order q . How do we know this?

\diamond

Exercise 20.5.38. Show that the primes $p_1 \dots p_k$ and exponents $e_1 \dots e_k$ in Proposition 20.5.35 must satisfy $|G| = p_1^{e_1} \dots p_k^{e_k}$. \diamond

Proposition 20.5.35 shows that abelian groups are essentially a souped-up versions of modular addition. (Now do you see why we spent a whole chapter on modular arithmetic?) From this proposition, we may derive a host of consequences. Following are just a few examples.

First, we can tell quite a lot about when abelian groups must be cyclic, depending on their orders:

Example 20.5.39. All abelian groups G of order 21 are isomorphic and cyclic. This is because $21 = 3^1 \times 7^1$, so by Proposition 20.5.35 it must be the case that $G \cong \mathbb{Z}_3 \times \mathbb{Z}_7$. In particular, $Z_{21} \cong \mathbb{Z}_3 \times \mathbb{Z}_7$. So all groups of order 21 are isomorphic to the cyclic group \blacklozenge

Exercise 20.5.40.

- (a) Prove or disprove: There is an abelian group of order 22 that is *not* cyclic.
- (b) Prove or disprove: There is an abelian group of order 24 that is *not* cyclic.

- (c) Prove or disprove: There is an abelian group of order 30 that is *not* cyclic.
- (d) *Prove or disprove: If G is an abelian group and the order of G is a product of distinct primes, then G must be cyclic.

◇

We know from Euler's theorem (Proposition 18.3.12) that the order of a group element $g \in G$ must divide the order of the group. However, this does not necessarily imply that every divisor of $|G|$ has a group element of that order. For abelian groups though, thanks to Proposition 20.5.35 we can actually guarantee that for certain divisors of $|G|$

Example 20.5.41. Any group G of order 54 must have an element of order 3. This is because $54 = 3^3 \cdot 2$, and according to Proposition 20.5.35 it must be the case that either $G \cong \mathbb{Z}_{27} \times \mathbb{Z}_2$, or $G \cong \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_2$, or $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2$. In the first case, then the isomorphic image of $(9, 0) \in \mathbb{Z}_{27} \times \mathbb{Z}_2$ has order 3 (verify this). In the second case, the isomorphic image of $(3, 0, 0) \in \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_2$ has order 3 (verify this also). In the third case, the isomorphic image of $(1, 0, 0, 0) \in \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_2$ has order 3 (verify this too!) ◆

Exercise 20.5.42.

- (a) Show that \mathbb{Z}_{5^n} contains an element of order 5, for any positive integer n .
- (b) Show that every abelian group of order divisible by 7 contains an element of order 7.

◇

What we've shown for specific primes in Example 20.5.41 and Exercise 20.5.42 is true in general: groups with orders divisible by p always contain elements of order p . This is true for nonabelian as well as abelian groups: this fact is known as **Cauchy's theorem**. At this point we're not able to prove Cauchy's theorem for nonabelian groups, but Cauchy's theorem for abelian groups can be proved using methods similar to those above. We'll state the theorem formally, then ask you to prove it.

Proposition 20.5.43. (*Cauchy's theorem for abelian groups*) Let G be an abelian group such that $|G|$ is divisible by the prime p . Then G has an element of order p .

Exercise 20.5.44. Prove Cauchy's theorem for abelian groups. \diamond

Exercise 20.5.45. (All of the exercises below assume that G is an abelian group.)

- (a) Show that if the prime p divides $|G|$, then G has at least $p - 1$ elements of order p .
- (b) Show that if p^2 divides $|G|$, then G has at least $p^2 - p$ elements of order p .
- (c) Show that if p^n divides $|G|$, then G has at least $p^n - p$ elements of order p .
- (d) Suppose that p^n is the largest power of p that divides $|G|$. Show that there are at most $p - 1$ element in G with order p^n .

\diamond

We may also recall that Lagrange's theorem (Proposition 18.3.3) enables us to conclude that the order of any subgroup $H \in G$ must divide $|G|$. Proposition 20.5.35 enables us to go one better.

Example 20.5.46. Suppose that $|G| = 125$. Let us show that G has a subgroup of order 25. From Proposition 20.5.35, we know that there are 3 possible cases for G : (i) $G \cong \mathbb{Z}_{125}$; (ii) $G \cong \mathbb{Z}_{25} \times \mathbb{Z}_5$; (iii) $G \cong \mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5$. In case (i), then the isomorphic image of $\langle 5 \rangle$ is a subgroup of order 25. In case (ii), then the isomorphic image of $\langle (1, 0) \rangle$ is a subgroup of order 25. In case (iii), then the isomorphic image of $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \{0\}$ is a subgroup of order 25. \blacklozenge

Example 20.5.47. Suppose that 7^2 divides $|G|$. Let us show that G has a subgroup of order 49. From Proposition 20.5.35, we know that either (i) G has a factor \mathbb{Z}_{7^k} where $k \geq 2$; or (ii) G has at least two factors of \mathbb{Z}_7 . In case (i), then G can be written as $\mathbb{Z}_{7^k} \times H$, where $k \geq 2$ and H is a

direct product of copies of \mathbb{Z}_n for different values of n . In this case, then the isomorphic image of $\langle(7^{k-2}, id_H)\rangle$ is a subgroup of order 7^2 (verify this). In case (ii), then G can be written as $\mathbb{Z}_7 \times \mathbb{Z}_7 \times H$, where once again H is a direct product of copies of \mathbb{Z}_n for different values of n . In this case, the isomorphic image of $\mathbb{Z}_7 \times \mathbb{Z}_7 \times id_H$ is a subgroup of order 49 (verify this). So in either case, G has a subgroup of order 49. \blacklozenge

Exercise 20.5.48.

- (a) Let p be a prime. Show that if p^2 divides the order of the abelian group G , then G has a subgroup of order p^2 .
- (b) * Let p be a prime, and let k be a positive integer. Show that if p^k divides the order of the abelian group G , then G has a subgroup of order p^k .
- (c) Let p_1, p_2 be primes such that $p_1 \neq p_2$. Show that if $p_1 p_2$ divides the order of the abelian group G , then G has a subgroup of order $p_1 p_2$.
- (d) Let p_1, p_2 be primes such that $p_1 \neq p_2$, and let k_1, k_2 be positive integers. Show that if $p_1^{k_1} p_2^{k_2}$ divides the order of the abelian group G , then G has a subgroup of order $p_1^{k_1} p_2^{k_2}$.

\diamond

The following proposition is the culmination of the train of thought expressed in Example 20.5.47 and Exercise 20.5.48

Proposition 20.5.49. Let G be an abelian group and suppose G is divisible by the positive integer n . Then G has a subgroup of order n .

Exercise 20.5.50. prove Proposition 20.5.49. \diamond

20.6 Proof that $U(p)$ is cyclic

Mathematics has many mysterious and wonderful connections. In this section, we will pull together several ideas from previous chapters to prove a key property of an important family of abelian groups.

Recall that $U(n)$ is the group of units in \mathbb{Z}_n , where a *unit* is an element with a multiplicative inverse. If p is a prime, then $U(p)$ is the set of all nonzero elements of \mathbb{Z}_p . In some coding theory applications, it's important to find elements of $U(p)$ which have a very larger order (recall that the *order* of a group element $g \in G$ (denoted by $|g|$) is the smallest positive integer n such that $g^n = \text{id}$). Now, we know from Lagrange's theorem that $|g|$ divides $|G|$ for any $g \in G$. It follows that $|g| \leq |G|$. We also have the following necessary and sufficient conditions for when $|g| = |G|$:

Exercise 20.6.1. Given a finite group G , prove G is cyclic if and only if $|G| = |g|$ for some $g \in G$. \diamond

Now, we know from Proposition 20.4.7 that any group of prime order is cyclic. Does this imply that $U(p)$ must be cyclic? Alas, the answer is negative:

Exercise 20.6.2. Show that if p is a prime greater than 3, then $|U(p)|$ is *not* a prime. \diamond

But all is not lost! Even though $|U(p)|$ is not prime, we can still prove that $U(p)$ is cyclic. To do this, we will need results from the Polynomials and Cosets chapters, as well as from this chapter. Here we go:

Proposition 20.6.3. $U(p)$ is cyclic for every prime p .

PROOF. First, notice that Proposition 12.6.18 says that there are at most m solutions to the equation $x^m = 1$ in \mathbb{Z}_p . Since 0 is not a solution, it follows that all of these solutions are also in $U(p)$.

Also, according to the factorization of Abelian groups (Proposition 20.5.35), there exists an isomorphism ϕ :

$$\phi : U(p) \rightarrow \mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_k^{e_k}},$$

where p_1, p_2, \dots, p_k are all primes. It's not necessarily true a priori that all of the p_j 's are distinct: but if they are, then Proposition 20.5.31 tells us that $U(p)$ must be cyclic.

So it all comes down to proving that all of the p_j 's are distinct. We will prove this by contradiction. We begin as usual by supposing the opposite of

what we want to prove: namely, that $p_i = p_j$ for some $i \neq j$. Now consider the following two elements of the direct product:

$$g_i = (0, \dots, \underbrace{p_i^{e_i-1}}_{i'\text{th place}}, \dots, 0) \text{ and } g_j = (0, \dots, \underbrace{p_j^{e_j-1}}_{j'\text{th place}}, \dots, 0).$$

It is then possible to prove that (recall that “ $|g|$ ” is the order of the group element g)

$$|g_i| = p_i \text{ and } |g_j| = p_j.$$

Exercise 20.6.4. Given the above definitions of g_i and g_j , show that $|g_i| = p_i$ and $|g_j| = p_j$. (*Hint*) \diamond

As a result of the above exercise, Proposition 18.3.17 enables us to conclude that

$$|g_i^n| = p_i \text{ and } |g_j^n| = p_j \text{ for } (n = 1, \dots, p_i - 1).$$

Since $p_i = p_j$, we have at least $2(p_i - 1)$ elements in $\mathbb{Z}_{p_1^{e_1}} \times \mathbb{Z}_{p_2^{e_2}} \times \dots \times \mathbb{Z}_{p_k^{e_k}}$ of order p_i . By Proposition 20.3.38, this means there are $2(p_i - 1)$ elements of $U(p)$ which have order p_i , and all of these elements are solutions of the equation $x^{p_i} - 1 = 0$ (Why?). But at the beginning of this proof, we demonstrated that there can only be at most p_i solutions. This contradiction shows us our supposition is false, so all of the p_i 's in the direct product must be unequal. \square

Exercise 20.6.5.

- Show that $U(6)$, $U(8)$, and $U(9)$ are cyclic.
- Give an example of a positive integer n for which $U(n)$ is *not* cyclic.
- Is it possible to specify exactly the positive integers n for which $U(n)$ is cyclic? (You'll probably have to do some internet research to answer this one.)

\diamond

20.6.1 Internal direct products

The direct product of two groups builds a large group out of two smaller groups. We would like to be able to reverse this process and conveniently break down a group into its direct product components; that is, we would like to be able to say when a group is isomorphic to the direct product of two of its subgroups.

Definition 20.6.6. Let G be a group with subgroups H and K satisfying the following conditions.

- $G = HK = \{hk : h \in H, k \in K\}$;
- $H \cap K = \{e\}$;
- $hk = kh$ for all $k \in K$ and $h \in H$.

Then G is the *internal direct product* of H and K . △

Example 20.6.7. The group $U(8)$ is the internal direct product of

$$H = \{1, 3\} \quad \text{and} \quad K = \{1, 5\}.$$

◆

Example 20.6.8. The dihedral group D_6 is an internal direct product of its two subgroups

$$H = \{\text{id}, r^3\} \quad \text{and} \quad K = \{\text{id}, r^2, r^4, s, r^2s, r^4s\}.$$

It can be shown that $K \cong S_3$; consequently, $D_6 \cong \mathbb{Z}_2 \times S_3$. ◆

Example 20.6.9. Not every group can be written as the internal direct product of two of its proper subgroups. If the group S_3 were an internal direct product of its proper subgroups H and K , then one of the subgroups, say H , would have to have order 3. In this case H is the subgroup $\{(1), (123), (132)\}$. The subgroup K must have order 2, but no matter which subgroup we choose for K , the condition that $hk = kh$ will never be satisfied for $h \in H$ and $k \in K$. ◆

Proposition 20.6.10. Let G be the internal direct product of subgroups H and K . Then G is isomorphic to $H \times K$.

PROOF. Since G is an internal direct product, we can write any element $g \in G$ as $g = hk$ for some $h \in H$ and some $k \in K$. Define a map $\phi : G \rightarrow H \times K$ by $\phi(g) = (h, k)$.

The first problem that we must face is to show that ϕ is a well-defined map; that is, we must show that h and k are uniquely determined by g . Suppose that $g = hk = h'k'$. Then $h^{-1}h' = k(k')^{-1}$ is in both H and K , so it must be the identity. Therefore, $h = h'$ and $k = k'$, which proves that ϕ is, indeed, well-defined.

To show that ϕ preserves the group operation, let $g_1 = h_1k_1$ and $g_2 = h_2k_2$ and observe that

$$\begin{aligned}\phi(g_1g_2) &= \phi(h_1k_1h_2k_2) \\ &= \phi(h_1h_2k_1k_2) \\ &= (h_1h_2, k_1k_2) \\ &= (h_1, k_1)(h_2, k_2) \\ &= \phi(g_1)\phi(g_2).\end{aligned}$$

We will leave the proof that ϕ is a bijection as an exercise:

Exercise 20.6.11. Prove that ϕ defined in the proof of Proposition 20.6.10 is a bijection, thus completing the proof of the proposition. \diamond

□

Example 20.6.12. The group \mathbb{Z}_6 is an internal direct product isomorphic to $\{0, 2, 4\} \times \{0, 3\}$. \blacklozenge

Exercise 20.6.13. Prove that the subgroup of \mathbb{Q}^* consisting of elements of the form 2^m3^n for $m, n \in \mathbb{Z}$ is an internal direct product isomorphic to $\mathbb{Z} \times \mathbb{Z}$. \diamond

Exercise 20.6.14. In this problem, we define $G \subset S_2 \times S_n$ by:

$$G = (\text{id}, A_n) \cup ((12), (S_n \setminus A_n)).$$

(a) Show that $S_2 \times S_n$ is isomorphic to a subgroup of S_{n+2} .

- (b) Show that G is a subgroup of $S_2 \times S_n$.
- (c) Show that G is isomorphic to a subgroup of A_{n+2} .
- (d) Show that G is isomorphic to S_n .
- (e) Show that S_n is isomorphic to a subgroup of A_{n+2} .

◇

A (sort of) converse of Proposition 20.6.10 is also true:

Proposition 20.6.15. Let H and K be subgroups of G , and define the map $\phi : H \times K \rightarrow G$ by $\phi((h, k)) = hk$. Suppose that ϕ is an isomorphism. Then G is the internal direct product of H and K .

Exercise 20.6.16. Prove Proposition 20.6.15.

◇

Exercise 20.6.17. Let G be a group of order 20. If G has subgroups H and K of orders 4 and 5 respectively such that $hk = kh$ for all $h \in H$ and $k \in K$, prove that G is the internal direct product of H and K .

◇

Exercise 20.6.18. Prove the following: Let G , H , and K be groups such that $G \times K \cong H \times K$. Then it is also true that $G \cong H$. (*Hint*)

◇

We can extend the definition of an internal direct product of G to a collection of subgroups H_1, H_2, \dots, H_n of G , by requiring that

- $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n : h_i \in H_i\}$;
- $H_i \cap \langle \cup_{j \neq i} H_j \rangle = \{e\}$;
- $h_i h_j = h_j h_i$ for all $h_i \in H_i$ and $h_j \in H_j$.

We will leave the proof of the following proposition as an exercise.

Proposition 20.6.19. Let G be the internal direct product of subgroups H_i , where $i = 1, 2, \dots, n$. Then G is isomorphic to $\prod_i H_i$.

Exercise 20.6.20. Prove Proposition 20.6.19.

◇

Additional exercises

- (1) Let $\omega = \text{cis}(2\pi/n)$. Show that $\omega^n = 1$, and prove that the matrices

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^{-1} \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

generate a multiplicative group isomorphic to D_n .

- (2) Show that the set of all matrices of the form

$$B = \begin{pmatrix} \pm 1 & n \\ 0 & 1 \end{pmatrix},$$

where $n \in \mathbb{Z}_n$, is a group isomorphic to D_n .

- (3) Let $G = \mathbb{R} \setminus \{-1\}$ and define a binary operation on G by

$$a * b = a + b + ab.$$

Prove that G is a group under this operation. Show that $(G, *)$ is isomorphic to the multiplicative group of nonzero real numbers.

- (4) Find all the subgroups of D_4 . Which subgroups are normal? What are all the quotient groups of D_4 up to isomorphism?
- (5) Prove that D_4 cannot be the internal direct product of two of its proper subgroups.
- (6) * Prove that $S_3 \times \mathbb{Z}_2$ is isomorphic to D_6 . Can you make a conjecture about D_{2n} ? Prove your conjecture. (*Hint*)
- (7) Find all the subgroups of the quaternion group, Q_8 . Which subgroups are normal? What are all the quotient groups of Q_8 up to isomorphism?
- (8) Prove $U(5) \cong \mathbb{Z}_4$. Can you generalize this result to show that $U(p) \cong \mathbb{Z}_{p-1}$?
- (9) Write out the permutations associated with each element of S_3 in the proof of Cayley's Theorem.
- (10) Prove that $A \times B$ is abelian if and only if A and B are abelian.
- (11) Let H_1 and H_2 be subgroups of G_1 and G_2 , respectively. Prove that $H_1 \times H_2$ is a subgroup of $G_1 \times G_2$.
- (12) Let $m, n \in \mathbb{Z}$, so that $(m, n) \in \mathbb{Z} \times \mathbb{Z}$. Prove that $\langle (m, n) \rangle \cong \langle d \rangle$ if and only if $d = \text{gcd}(m, n)$.
- (13) Let $m, n \in \mathbb{Z}$. Prove that $\langle m \rangle \cap \langle n \rangle \cong \langle l \rangle$ if and only if $d = \text{lcm}(m, n)$.

The following exercises will require this definition:

Definition 20.6.21.n *automorphism* of a group G is an isomorphism with itself. △

- (14) Prove that complex conjugation is an automorphism of the additive group of complex numbers; that is, show that the map $\phi(a + bi) = a - bi$ is an isomorphism from \mathbb{C} to \mathbb{C} .
- (15) Prove that $a + ib \mapsto a - ib$ is an automorphism of \mathbb{C}^* .
- (16) Prove that $A \mapsto B^{-1}AB$ is an automorphism of $SL_2(\mathbb{R})$ for all B in $GL_2(\mathbb{R})$.
- (17) We will denote the set of all automorphisms of G by $Aut(G)$. Prove that $Aut(G)$ is a subgroup of S_G , the group of permutations of G .
- (18) Find $Aut(\mathbb{Z}_6)$.
- (19) Find $Aut(\mathbb{Z})$.
- (20) Find two nonisomorphic groups G and H such that $Aut(G) \cong Aut(H)$.
- (21) (a) Let G be a group and $g \in G$. Define a map $i_g : G \rightarrow G$ by $i_g(x) = gxg^{-1}$. Prove that i_g defines an automorphism of G . Such an automorphism is called an **inner automorphism**.
- (b) The set of all inner automorphisms is denoted by $Inn(G)$. Prove that $Inn(G)$ is a subgroup of $Aut(G)$.
- (c) What are the inner automorphisms of the quaternion group Q_8 ? Is $Inn(G) = Aut(G)$ in this case?
- (22) Let G be a group and $g \in G$. Define maps $\sigma_g : G \rightarrow G$ and $\tau_g : G \rightarrow G$ by $\sigma_g(x) = gx$ and $\tau_g(x) = xg^{-1}$. Show that $i_g := \tau_g \circ \sigma_g$ is an automorphism of G .

20.7 Hints for “Isomorphisms” exercises

Exercise 20.1.6: Show a counterexample where the sum of two complex numbers is not the same as the sum of their corresponding ordered pairs.

Exercise 20.2.9(a): According to Definition 20.2.1, this involves proving two things about ϕ^{-1} . What are they?

Exercise 20.2.9(b): You need to prove the same two things as in part (a). Use results from the Functions chapter.

Exercise 20.2.11: Recall that this involves proving the three properties: reflexive, symmetric, and transitive. You may find that Exercise 20.2.9 is useful.

Exercise 20.3.35: the proof follows Proposition 20.3.33 very closely.

Exercise 20.3.39(a): Use Exercise 20.2.9. (b): Use Proposition 20.3.29. (c): Use Proposition 20.3.34.

Exercise 20.4.5(a): Use Proposition 20.3.34.

Exercise 20.4.8: This is a direct result of Proposition 18.3.17 in the Cosets chapter..

Exercise 20.5.2: For each group property to be proved, use the corresponding group property for G and H independently.

Exercise 20.5.9: To show that G is abelian, for arbitrary group elements $g_1, g_2 \in G$ consider the elements (g_1, id_H) and (g_2, id_H) in $G \times H$, where id_H is the identity of the group H . Show that if (g_1, id_H) and (g_2, id_H) commute, then g_1 and g_2 must also commute.

Exercise 20.5.18: Since $G \times H$ is cyclic, it must have a generator (g, h) . Show that g is a generator for G and h is a generator for H .

Exercise 20.5.12: Define a function $\phi : G \times H \rightarrow H \times G$ by: $\phi(g, h) = \underline{\hspace{2cm}}$ (you fill in the blank). Show that this function is in fact an isomorphism.

Exercise 20.5.42(c): Consider 2 cases: (i) 9 divides one of the factors $p_i^{e_i}$ in Proposition 20.5.35; (ii) 9 does not divide any of the factors.

Exercise 20.6.18: Show that $G \times id_K$ is a subgroup of $G \times K$, and that $G \times id_K \cong G$; and similarly for H .

Additional exercises

Exercise 6: If you take every other vertex in a hexagon, you get an equilateral triangle. Also note that 180-degree rotation is an element of order 2.

Exploration: Relating polynomials and matrices

In the previous chapter, we formally introduced the concept of *isomorphism* as it relates to groups. Intuitively, two groups are isomorphic if any algebraic statement about one group is also true about the other, just expressed in different symbology. For example, given that group a finite group G is isomorphic to group H , it is then possible to obtain the Cayley table for H simply by making letter-for-letter substitutions in the Cayley table for G .

The concept of isomorphism applies to other mathematical structures besides groups. A great deal of mathematics is concerned with showing that two apparently different mathematical structures are in fact the same, just expressed in different terminology. When the structures involved are rings, vector spaces, etc., then we may talk about ring isomorphisms, vector space isomorphisms, and so on.

In this chapter, we will give an example of a *ring isomorphism*. This isomorphism is quite important in *digital signal processing*, is a key area of modern technology that powers our CD players, cell phones, wireless internet, and many other electronic devices.

To understand this chapter you will need some background in linear algebra. In particular, you will need to understand algebraic operations on vectors and matrices. In the first section, we'll give a brief review of some basic properties of vectors and vector spaces.

21.1 Definition of vector space

The most basic idea of a “vector” is a quantity that has magnitude and direction, and which can be represented by an arrow. This simple representation was good enough for basic math and physics classes. However, in upper-level math (and physics) there’s a lot more to vectors than this. Vectors are defined as objects in a *vector space*, which can have 1, 2, 3, 4, or millions of dimensions. Besides this, vectors in a vector space must have two operations (called *addition* and *scalar multiplication*) which must satisfy certain requirements.

Here is the formal definition of a vector space:

Definition 21.1.1. *vector space over the real numbers* consists of a set V along with two operations ‘+’ and ‘ \cdot ’, subject to the conditions that for all vectors $\vec{v}, \vec{w}, \vec{u} \in V$ and all scalars $r, s \in \mathbb{R}$:

- (1) The set V is closed under vector addition: $\vec{v} + \vec{w} \in V$
- (2) Vector addition is commutative: $\vec{v} + \vec{w} = \vec{w} + \vec{v}$
- (3) Vector addition is associative: $(\vec{v} + \vec{w}) + \vec{u} = \vec{v} + (\vec{w} + \vec{u})$
- (4) There exists a **zero vector** $\vec{0} \in V$ such that $\vec{v} + \vec{0} = \vec{v}$ for all $\vec{v} \in V$
- (5) Each $\vec{v} \in V$ has an additive inverse $\vec{w} \in V$ such that $\vec{w} + \vec{v} = \vec{0}$
- (6) The set V is closed under scalar multiplication: $r\vec{v} \in V$
- (7) Addition of scalars distributes over scalar multiplication: $(r + s) \cdot \vec{v} = r \cdot \vec{v} + s \cdot \vec{v}$
- (8) Scalar multiplication distributes over vector addition: $r \cdot (\vec{v} + \vec{w}) = r \cdot \vec{v} + r \cdot \vec{w}$
- (9) Ordinary multiplication of scalars associates with scalar multiplication: $(rs) \cdot \vec{v} = r \cdot (s \cdot \vec{v})$
- (10) Multiplication by the scalar 1 is an identity operation: $1 \cdot \vec{v} = \vec{v}$.

△

Let us recall how these definitions apply to a familiar example.

Example 21.1.2. The set \mathbb{R}^3 is a vector space if the operations '+' and '\cdot' have their usual meaning of vector addition and scalar multiplication, respectively:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} + \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ x_2 + y_2 \\ x_3 + y_3 \end{pmatrix} \quad \text{and} \quad r \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} rx_1 \\ rx_2 \\ rx_3 \end{pmatrix}.$$

Let's check the 10 conditions. We'll take

$$\vec{v} := \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}; \quad \vec{w} := \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}; \quad \vec{u} = \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix}$$

as arbitrary vectors in \mathbb{R}^3 (u_j, v_j and w_j are real numbers for $j = 1, 2, 3$).

For (1) to show that vector addition is closed we have

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \\ v_3 + w_3 \end{pmatrix} \in \mathbb{R}^3,$$

So addition is closed.

For (2), we show addition of vectors commutes:

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} v_1 + w_1 \\ v_2 + w_2 \\ v_3 + w_3 \end{pmatrix} = \begin{pmatrix} w_1 + v_1 \\ w_2 + v_2 \\ w_3 + v_3 \end{pmatrix} = \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} + \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}.$$

For (3), we show vector addition is associative:

$$\begin{aligned} \left(\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \right) + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} &= \begin{pmatrix} (v_1 + w_1) + u_1 \\ (v_2 + w_2) + u_2 \\ (v_3 + w_3) + u_3 \end{pmatrix} \\ &= \begin{pmatrix} v_1 + (w_1 + u_1) \\ v_2 + (w_2 + u_2) \\ v_3 + (w_3 + u_3) \end{pmatrix} \\ &= \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \left(\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} + \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} \right). \end{aligned}$$



Conditions 4,5,6,7 are reserved for exercises.

To show that scalar multiplication distributes from the left over vector addition (property 8), we may proceed as follows:

$$\begin{aligned}
 r \cdot \left(\begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} \right) &= \begin{pmatrix} r(v_1 + w_1) \\ r(v_2 + w_2) \\ r(v_3 + w_3) \end{pmatrix} \\
 &= \begin{pmatrix} rv_1 + rw_1 \\ rv_2 + rw_2 \\ rv_3 + rw_3 \end{pmatrix} \\
 &= r \cdot \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} + r \cdot \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix}
 \end{aligned}$$

Exercise 21.1.3. Prove conditions 4,5,6,7,9,10 for column vectors in \mathbb{R}^3 . \diamond

21.2 Polynomials are also vectors

At this point the “abstract” of abstract algebra comes into play. Once we have defined vector space, then *any* set of any objects that satisfies all ten requirements qualifies as a bona fide vector space, and objects in the set can be called vectors. Do polynomials qualify? We already know that we can add polynomials together, and we can also multiply polynomials by scalars. To see whether or not the set of polynomials with real coefficients (that is, $\mathbb{R}[x]$) is a vector space, we will need to check all 10 conditions:

Exercise 21.2.1. Let $p(x)$, $q(x)$, and $r(x)$ be polynomials in $\mathbb{R}[x]$, and let $\alpha, \beta \in \mathbb{R}$ be scalars. Write the 10 conditions in terms of $p(x)$, $q(x)$, $r(x)$, α , β . For example, we have:

1. (Closure under +) $p(x) + q(x)$ is in the set $\mathbb{R}[x]$.
5. (Additive inverse) $p(x) + (-1) \cdot p(x) = 0$
8. $\alpha(p(x) + q(x)) = \alpha p(x) + \alpha q(x)$

To complete the exercise, write conditions 2,3,4,6,7,9,10. \diamond

Exercise 21.2.2. Use summation notation to prove properties 5,7,8 for polynomials. \diamond

The preceding exercises show that the set $\mathbb{R}[x]$ over \mathbb{R} is a vector space, using the standard operations on polynomials. In fact, the polynomial ring $\mathbb{R}[x]$ is an *infinite-dimensional* vector space. It's true that each individual polynomial has finite degree, but the set has no single bound on the degree of all of its members. For instance, We can think of $1 + 4x + 7x^2$ as corresponding to the vector $(1, 4, 7, 0, 0, \dots)$.

Another vector space that we will want to examine is the set of $n \times n$ matrices with real entries.

Exercise 21.2.3. Let M be the set of $n \times n$ matrices with real entries. Let A, B , and C be elements of M , and let $\alpha, \beta \in \mathbb{R}$ be scalars. Write the 10 vector space conditions in terms of A, B, C, α, β . \diamond

21.3 Identifying polynomials with matrices

We have seen that both vectors and matrices define vectors spaces. But matrices (in particular, square matrices) have something that vectors don't have: namely, two square matrices of the same size can be multiplied together to get a square matrix of the same size. In contrast, we don't know of any way in general to multiply two $n \times 1$ vectors to obtain another $n \times 1$ vector.

Now recall that two polynomials can be multiplied together to obtain another polynomial. This suggests that polynomials are more like matrices than column vectors. In fact, we will show in this section that the polynomials $\mathbb{R}[x]$ are "isomorphic" to a particular set of matrices. We put "isomorphic" in quotes because the isomorphism doesn't merely preserve a single operation, like the group isomorphisms that we've seen up till now. Rather, this will be an *isomorphism of rings* (or *ring isomorphism*) that preserves both addition and multiplication.

Let's begin with an example that shows how polynomials can be related to matrices:

Example 21.3.1. Let $p(x) = 3x^2 - 7x + 2$. We may represent $p(x)$ as a column vector:

$$p(x) \rightarrow \begin{bmatrix} 2 \\ -7 \\ 3 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

where the coefficients of $1, x, x^2 \dots$ are listed from top to bottom. (We have added some extra zeros to the bottom of the vector for a reason that will become clear later.) Now notice that

$$x \cdot p(x) \rightarrow \begin{bmatrix} 0 \\ 2 \\ -7 \\ 3 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ -7 \\ 3 \\ 0 \\ 0 \\ 0 \end{bmatrix}.$$

Thus it seems that when we represent polynomials as column vectors, multiplying a polynomial by x corresponds to matrix multiplication by a matrix with 1's on the *subdiagonal* (that is, the entries lying just below the diagonal). We may similarly verify that

$$x^2 \cdot p(x) \rightarrow \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 \\ -7 \\ 3 \\ 0 \\ 0 \\ 0 \end{bmatrix},$$

where this time the 1's are on the sub-subdiagonal. You may check that this matrix is in fact the square of the matrix that represents multiplication by x . \blacklozenge

Exercise 21.3.2. Compute the vector representation of $x^3 \cdot p(x)$ for the polynomial in the previous example, and show that this vector can be obtained as a matrix-vector multiplication, where the matrix is the cube of the subdiagonal matrix that represents multiplication by x and the vector represents $p(x)$. \diamond

Exercise 21.3.3.

- (a) What matrix can we multiply the vector representation of $p(x)$ by to give the vector representation of $5 \cdot p(x)$?
- (b) What matrix can we multiply the vector representation of $p(x)$ by to give the vector representation of $-8x \cdot p(x)$?

◇

Exercise 21.3.4. Describe what happens when you try to represent $x^4 \cdot p(x)$ as a 6×1 vector, as in the previous exercises. How may the vector be changed to correct this? ◇

Let's generalize the previous example. Given any polynomial $p(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$, we can represent $p(x)$ as a column vector with m entries ($m > n$) as follows:

$$p(x) \rightarrow \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_n \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Then in order to multiply $p(x)$ by x , we can represent x as a $m \times m$ square matrix with 1's on the subdiagonal:

$$x \rightarrow \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

Now what do we really mean by “ \rightarrow ”? Really we're talking about a mapping from polynomials to matrices—in other words, a *function*. Accordingly

we'll define a function $\varphi_m : \mathbb{R}[x] \rightarrow M_{m,m}$ such that $\varphi_m(x)$ is the $m \times m$ subdiagonal matrix that represents polynomial x :

$$\varphi_m(x) = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix}.$$

(Note that the Greek letter φ is pronounced “fee” or “fie”.¹ The subscript “ m ” emphasizes that technically there is a different map for each matrix size.)

So far we've only defined φ_m for the polynomial x , but we'd certainly like to define it for any polynomial. There is a natural way to do this. First let's consider the simplest nonzero polynomial we can think of, namely the constant 1. Since 1 is the multiplicative identity for polynomials, it stands to reason that $\varphi_m(1)$ should be the multiplicative identity for matrices. Accordingly we define

$$\varphi_m(1) := I_{m \times m},$$

where $I_{m \times m}$ is the $m \times m$ identity matrix.

Constant polynomials are the next simplest case. It makes sense to map the constant polynomial a to the matrix $aI_{m \times m}$, so that

$$\varphi_m(a) := aI_{m \times m},$$

In view of the exercises that we did a little while ago, the next reasonable step is to define $\varphi_m(ax)$ as:

$$\varphi_m(ax) = \varphi_m(a) \cdot \varphi_m(x) = a\varphi_m(x).$$

We also saw in Example 21.3.1 and Exercise 21.3.2 that $\varphi_m(x^2) = \varphi_m(x)^2$ and; $\varphi_m(x^3) = \varphi_m(x)^3$. This suggests the following general rule:

$$\varphi_m(ax^n) := \varphi_m(a) \cdot \varphi_m(x)^n = a\varphi_m(x)^n.$$

Finally, in light of our previous experience with isomorphisms of groups, it's reasonable to impose the following requirement on φ_m :

$$\varphi_m(p(x) + q(x)) = \varphi_m(p(x)) + \varphi_m(q(x))$$

¹But not “fo” or “fum”.

We now have enough rules so that we can build up $\varphi_m(p(x))$ for any polynomial $p(x)$.

Example 21.3.5. We may find the 6×6 matrix which represents the polynomial $x^2 + 3x - 7$ as follows:

$$\begin{aligned} \varphi_6(x^2 + 3x - 7) &= \varphi_6(x^2) + \varphi_6(3x) + \varphi_6(-7) \\ &= \varphi_6(x^2) + 3\varphi_6(x) - 7\varphi_6(1) \\ &= \begin{bmatrix} -7 & 0 & 0 & 0 & 0 & 0 \\ 3 & -7 & 0 & 0 & 0 & 0 \\ 1 & 3 & -7 & 0 & 0 & 0 \\ 0 & 1 & 3 & -7 & 0 & 0 \\ 0 & 0 & 1 & 3 & -7 & 0 \\ 0 & 0 & 0 & 1 & 3 & -7 \end{bmatrix} \end{aligned}$$

◆

Exercise 21.3.6. Find the matrix $\varphi_6(p(x))$ related to each polynomial $p(x)$.

(a) $p(x) = 7x^2 - 2x + 3$

(c) $p(x) = 3x^5$

(b) $p(x) = 3x^4 + 5x^2 - 2$

(d) $p(x) = -4x^3 + 4$

◇

Exercise 21.3.7. In each case, find the polynomial $p(x)$ such that $\varphi(p(x))$ equals the given matrix:

(a)

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 \\ 6 & 1 & 3 & 0 & 0 & 0 \\ 4 & 6 & 1 & 3 & 0 & 0 \\ 8 & 4 & 6 & 1 & 3 & 0 \\ 0 & 8 & 4 & 6 & 1 & 3 \end{bmatrix}$$

(b)

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 1 & 0 & 0 & 0 \\ 9 & 4 & 0 & 1 & 0 & 0 \\ 0 & 9 & 4 & 0 & 1 & 0 \end{bmatrix}$$

◇

Notice the special structure of all these matrices. They all have no entries above the main diagonal. Furthermore they are constant along the subdiagonal, sub-subdiagonal, sub-sub-subdiagonal, and so on. By working with examples, you may see that these same properties will hold in general for any matrix that can be written as $\varphi_m(p(x))$ for some polynomial $p(x)$.

Exercise 21.3.8. For each of the following matrices, determine whether or not it corresponds to a polynomial. If it does, give the polynomial; and if not, explain why not.

(a)

$$\begin{bmatrix} 5 & 0 & 0 & 1 \\ 1 & 3 & 0 & 0 \\ 5 & 1 & 3 & 0 \\ 0 & 5 & 1 & 3 \end{bmatrix}$$

(b)

$$\begin{bmatrix} 9 & 0 & 0 & 0 \\ 1 & 9 & 0 & 0 \\ 7 & 1 & 9 & 0 \\ 0 & 7 & 1 & 9 \end{bmatrix}$$

(c)

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 \\ 4 & 2 & -1 & 0 & 0 \\ 0 & 4 & 2 & -1 & 0 \\ 0 & 0 & 0 & 2 & -1 \end{bmatrix}$$

(d)

$$\begin{bmatrix} 3 & 0 & 0 & 0 & 0 & 0 \\ 1 & 3 & 0 & 0 & 0 & 0 \\ 5 & 1 & 3 & 0 & 0 & 0 \\ 0 & 3 & 1 & 3 & 0 & 0 \\ 0 & 0 & 3 & 1 & 3 & 0 \\ 0 & 0 & 0 & 5 & 1 & 3 \end{bmatrix}$$

(e)

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ -1 & 0 & 2 & 1 & 0 & 0 \end{bmatrix}$$

◇

Now let's play around with polynomial arithmetic. Remember our basic rule for polynomial addition:

$$\varphi_m(p(x) + q(x)) = \varphi_m(p(x)) + \varphi_m(q(x)).$$

We may use this rule to easily find the matrix for the sum of polynomials by adding the matrices for the individual polynomials.

Example 21.3.9. Let $p(x) = 2x^2 + x + 1$ and $q(x) = 5x + 6$: then $p(x) + q(x) = 2x^2 + 6x + 7$. We get the same result when we add the matrices that represent $p(x)$ and $q(x)$:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 0 & 2 & 1 & 1 \end{bmatrix} + \begin{bmatrix} 6 & 0 & 0 & 0 \\ 5 & 6 & 0 & 0 \\ 0 & 5 & 6 & 0 \\ 0 & 0 & 5 & 6 \end{bmatrix} = \begin{bmatrix} 7 & 0 & 0 & 0 \\ 6 & 7 & 0 & 0 \\ 2 & 6 & 7 & 0 \\ 0 & 2 & 6 & 7 \end{bmatrix}$$

◆

Exercise 21.3.10. Find the matrices that represent the polynomials $p(x)$ and $q(x)$ in each case, and verify that the sum is equal to $\varphi_m(p(x) + q(x))$ for the given m .

- (a) $p(x) = x^5 + 1$ and $q(x) = x^3 + 5^2$ ($m = 7$)
- (b) $p(x) = 7x^4 + 1$ and $q(x) = x^3 + 5^2 + 10x - 3$ ($m = 5$)
- (c) $p(x) = 2x^2 - 2x + 5$ and $q(x) = x^2 + 2x - 5$ ($m = 3$)

◇

It would be nice to do the same with multiplication. Our previous examples suggest the following rule:

$$\varphi_m(p(x))\varphi_m(q(x)) = \varphi_m(p(x)q(x))$$

Let's see if this works.

Example 21.3.11. You can see that $\varphi_3(x)\varphi_3(x) = \varphi_3(x^2)$:

$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$



Example 21.3.12. You can see that $\varphi_4(x^2)\varphi_4(x) = \varphi_4(x^3)$.

$$\begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$



The previous 2 examples show that $\varphi_m(x^k)\varphi_m(x) = \varphi_m(x^{k+1})$.

Example 21.3.13. Let $p(x) = -4x^2 + 3x - 2$ and $q(x) = 7x^2 - 2x - 5$. Then multiplying $\varphi_6(p(x))\varphi_6(q(x))$ gives.

$$\begin{bmatrix} -2 & 0 & 0 & 0 & 0 & 0 \\ 3 & -2 & 0 & 0 & 0 & 0 \\ -4 & 3 & -2 & 0 & 0 & 0 \\ 0 & -4 & 3 & -2 & 0 & 0 \\ 0 & 0 & -4 & 3 & -2 & 0 \\ 0 & 0 & 0 & -4 & 3 & -2 \end{bmatrix} \begin{bmatrix} -5 & 0 & 0 & 0 & 0 & 0 \\ -2 & -5 & 0 & 0 & 0 & 0 \\ 7 & -2 & -5 & 0 & 0 & 0 \\ 0 & 7 & -2 & -5 & 0 & 0 \\ 0 & 0 & 7 & -2 & -5 & 0 \\ 0 & 0 & 0 & 7 & -2 & -5 \end{bmatrix} = \begin{bmatrix} 10 & 0 & 0 & 0 & 0 & 0 \\ -11 & 10 & 0 & 0 & 0 & 0 \\ 0 & -11 & 10 & 0 & 0 & 0 \\ 29 & 0 & -11 & 10 & 0 & 0 \\ -28 & 29 & 0 & -11 & 10 & 0 \\ 0 & -28 & 29 & 0 & -11 & 10 \end{bmatrix},$$

which is the matrix that corresponds to $-28x^4 + 29x^3 - 11x + 10$. You may verify that this polynomial is equal to the product of the two polynomials that we started out with. ◆

Exercise 21.3.14. Find the $m \times m$ matrices that represent the polynomials $p(x)$ and $q(x)$ and verify that the product of these two matrices is the matrix which represents $p(x)q(x)$.

(a) $p(x) = x^5 + 1$ and $q(x) = x^3 + 5^2$ (with $m = 10$)

- (b) $p(x) = 7x^4 + 1$ and $q(x) = x^3 + 5^2 + 10x - 3$ (with $m = 8$)
- (c) $p(x) = 2x^2 - 2x + 5$ and $q(x) = x^2 + 2x - 5$ (with $m = 7$)
- (d) Can you choose different value of m in part (a), (b), and (c)? What is the minimum value you can choose for m in each part?

◇

One problem with our investigations so far is that φ_m can't accommodate polynomials of degree greater than or equal to m . The only way to deal with this is to make the matrices infinitely large. So let's define $\varphi : P[x] \mapsto M_{\infty \times \infty}$ as follows: given

$$p(x) = \sum_{m=0}^N a_m x^m$$

then we define $\varphi(p(x))$ as a matrix with entries:

$$[\varphi(p)]_{i,j} = \begin{cases} a_m & \text{if } i - j = m, m = 0, \dots, N \\ 0 & \text{otherwise} \end{cases}$$

We may give an algebraic proof that the map φ is 1-1 as follows. Suppose $p(x)$ and $q(x)$ are polynomials and $p(x) \neq q(x)$. Then we can write

$$p(x) = \sum_{m=0}^N a_m x^m \quad \text{and} \quad q(x) = \sum_{m'=0}^{N'} b_{m'} x^{m'}$$

Since $p(x) \neq q(x)$, there must be some k such that $a_k \neq b_k$. But then according to the definition it follows that:

$$[\varphi(p)]_{k+1,1} = a_k \quad \text{and} \quad [\varphi(q)]_{k+1,1} = b_k.$$

Therefore, $\varphi(p) \neq \varphi(q)$ since $a_k \neq b_k$.

Is φ onto? That's for you to find out:

Exercise 21.3.15.

- (a) Find an infinite matrix M such that $M \neq \varphi(p(x))$ for any polynomial $p(x)$. What does this tell you about whether or not φ is onto?

- (b) Using the definition of φ , show that if $M = \varphi(p(x))$ for some polynomial $p(x)$ then M is **lower triangular** that is, all entries above the diagonal are 0.
- (c) Using the definition of φ , show that if $M = \varphi(p(x))$ then M is **banded**, that is, $M_{i+k,j+k} = M_{i,j}$ for any positive integers i, j, k .

◇

Let's define $B \subset M_{\infty \times \infty}$ as the set of all banded subdiagonal matrices. The previous exercise (parts (c),(d)) have shown that φ maps $P[x]$ into B . In fact, φ maps $P[x]$ onto B :

Exercise 21.3.16. Let M be an arbitrary matrix in B . Suppose the first column of M is the column vector:

$$\begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ \vdots \end{pmatrix}.$$

Find a polynomial $p(x)$ such that $\varphi(p(x)) = M$. (*Hint*)

◇

So we have that $\varphi : P[x] \rightarrow B$ is a 1-1 and onto map. In fact, φ is an isomorphism between the additive group of polynomials and the subdiagonal banded matrices B . To finish proving this, we need to show the operation-preserving property of φ :

Proposition 21.3.17. Let

$$p(x) = \sum_{m=0}^N a_m x^m \quad \text{and} \quad q(x) = \sum_{m'=0}^{N'} b_{m'} x^{m'}$$

Then $\varphi(p+q) = \varphi(p) + \varphi(q)$.

Proof : We can suppose that $N \geq N'$ (if $N' > N$, we just exchange p and q in the proof). For all b_j when $j > N'$, we have $b_j = 0$. Then we will have:

$$p(x) + q(x) = \sum_{m=0}^N a_m x^m + \sum_{m=0}^N b_m x^m$$

$$= \sum_{m=0}^N (a_m + b_m)x^m.$$

Now, using our formula for φ we have

$$[\varphi(p+q)]_{i,j} = \begin{cases} a_m + b_m & \text{if } i - j = m, m = 0, \dots, N \\ 0 & \text{otherwise} \end{cases}$$

Comparing this with the 2 formulas

$$[\varphi(p)]_{i,j} = \begin{cases} a_m & \text{if } i - j = m, m = 0, \dots, N \\ 0 & \text{otherwise} \end{cases}$$

and

$$[\varphi(q)]_{i,j} = \begin{cases} b_m & \text{if } i - j = m, m = 0, \dots, N \\ 0 & \text{otherwise} \end{cases}$$

It's clear that $[\varphi(p+q)]_{i,j} = [\varphi(p)]_{i,j} + [\varphi(q)]_{i,j}$ for every i and j . In other words, all of the matrix entries of $\varphi(p+q)$ are equal to the sum of corresponding entries of $\varphi(p)$ and $\varphi(q)$.

Therefore $\varphi(p+q) = \varphi(p) + \varphi(q)$.

Exercise 21.3.18. Show that B (that is, the lower-triangular banded matrices) is a group under addition. \diamond

Exercise 21.3.19. Show that $\varphi : P[x] \mapsto B$ is an isomorphism between the addition groups $(P[x], +)$ and $(B, +)$. \diamond

So it's true that φ is an additive isomorphism. It would be nice if it were a multiplicative isomorphism as well. Unfortunately this is impossible, since polynomials don't form a multiplicative group. Still, let's see if φ has any special properties under multiplication.

Example 21.3.20. This example can show that $\varphi(x)\varphi(x) = \varphi(x^2)$ is still true (just as it was for φ_m) if we represent x by an infinite matrix:

$$\begin{bmatrix} 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ 1 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$



In general, we have $\varphi(x^m)\varphi(x^n) = \varphi(x^{m+n})$. This suggests that φ preserves the operation of multiplication that is, $\varphi(pq) = \varphi(p)\varphi(q)$.

Be careful here! On the left-hand side we're taking the product of polynomials and taking φ of the result. On the right-hand side, we're converting two polynomials into matrices, and multiplying the matrices. So there are two different multiplication operations on the two sides of the equation.

Now, with the following proposition, we can show that φ does preserve multiplication operation.

Proposition 21.3.21. Let

$$p(x) = \sum_{m=0}^N a_m x^m \quad \text{and} \quad q(x) = \sum_{m'=0}^{N'} b_{m'} x^{m'}$$

Then $\varphi(pq) = \varphi(p)\varphi(q)$.

Proof : we'll start from the left-hand side of the equation $\varphi(pq) = \varphi(p)\varphi(q)$ and show it's equal to the right-hand side as in the next exercise.

Exercise 21.3.22. Fill in the blanks the following proof. (*Hint*)

$$\begin{aligned}
\varphi(pq) &= \varphi\left(\left(\sum_{m=0}^N a_m x^m\right)\left(\sum_{m'=0}^{N'} b_{m'} x^{m'}\right)\right) \\
&= \varphi\left(\sum_{m=0}^N \sum_{m'=0}^{N'} a_m b_{m'} x^{\langle 1 \rangle}\right) \\
&= \sum_{m=0}^N \sum_{m'=0}^{N'} \varphi(a_m b_{m'} x^{\langle 2 \rangle}) \\
&= \sum_{m=0}^N \sum_{m'=0}^{N'} \varphi(\langle 3 \rangle) \varphi(\langle 4 \rangle) \\
&= \left(\sum_{m=0}^N \varphi(\langle 5 \rangle)\right) \left(\sum_{m'=0}^{N'} \varphi(\langle 6 \rangle)\right) \\
&= \varphi\left(\sum_{m=0}^N (\langle 7 \rangle)\right) \varphi\left(\sum_{m'=0}^{N'} (\langle 8 \rangle)\right) \\
&= \varphi(\langle 9 \rangle) \varphi(\langle 10 \rangle)
\end{aligned}$$

◇

So we finally proved that φ preserves the operation of multiplication.

21.4 Hints for “Polynomials and Matrices” exercises

Exercise 21.3.16: Look at the examples of $M = \varphi_m(p(x))$ that we’ve computed so far, and see how the first column of M relates to the coefficients of $p(x)$.

Exercise 21.3.22: Use the distributive property, exponent rules, and the operation-preserving properties of φ .

Homomorphisms of Groups

In this chapter we will introduce homomorphisms, which are a powerful tool in the study of the structure of abstract groups. Our brief treatment only gives the reader a taste of this important topic, and the reader wanting to go deeper is encouraged to look at other algebra texts.

Thanks to Tom Judson for material used in this chapter.

22.1 Preliminary examples

In the previous chapter we talked about isomorphisms, which are bijections between two groups that also preserve the group operation. We've seen that isomorphic groups are essentially the "same" group (thinking groupwise).

For instance, we saw that the integers mod 4 and the 4th roots of unity were isomorphic ($\mathbb{Z}_4 \cong \langle i \rangle$) by the following bijection (isomorphism):

$$0 \rightarrow 1, \quad 1 \rightarrow i, \quad 2 \rightarrow -1, \quad 3 \rightarrow -i.$$

The group operation is preserved by this bijection: for instance, $1 \oplus 2 = 3$ maps to $i \cdot -1 = -i$. In general, for $a, b \in \mathbb{Z}_4$ we have

$$f(a \oplus b) = f(a) \cdot f(b).$$

Now let us think about the groups \mathbb{Z}_8 and $\langle i \rangle$. Do they have the same relationship? Are they isomorphic?

Well, there is *one* immediate problem that comes up: $|\mathbb{Z}_8| \neq |\langle i \rangle|$. And as we saw in the Isomorphism chapter, there's no way then to create a bijection from \mathbb{Z}_8 to $\langle i \rangle$: specifically, there is just no way to create a one-to-one function from a domain of 8 elements to a codomain of 4 elements; the number of elements have to match. But let's look at their Cayley tables:

| | | | | | | | | |
|----------|---|---|---|---|---|---|---|---|
| \oplus | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 7 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 7 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 7 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 7 | 0 | 1 | 2 | 3 | 4 | 5 |
| 7 | 7 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

Table 22.1: Addition table for \mathbb{Z}_8

| | | | | |
|---------|------|------|------|------|
| \cdot | 1 | i | -1 | $-i$ |
| 1 | 1 | i | -1 | $-i$ |
| i | i | -1 | $-i$ | 1 |
| -1 | -1 | $-i$ | 1 | i |
| $-i$ | $-i$ | 1 | i | -1 |

Table 22.2: Cayley table for $\langle i \rangle$

While we can't say that \mathbb{Z}_8 and $\langle i \rangle$ are isomorphic, there are some similarities in the patterns of their Cayley tables. Notice for instance the pattern of 2's in the upper left portion of the \mathbb{Z}_8 table. This matches exactly with the pattern of -1's in the $\langle i \rangle$ table. In fact, we can see that in both tables the entries in each "anti-diagonal" are all the same. This similarity in structure suggests a similarity in the behavior of the group operations. So although we can't create a bijection, could we possibly create another function that preserves the group operations?

Example 22.1.1. Let's try to create a function from \mathbb{Z}_8 to $\langle i \rangle$ which preserves group operations. Since there are twice as many elements in \mathbb{Z}_8 as in $\langle i \rangle$, it seems natural that 2 elements from \mathbb{Z}_8 should each go to one element in $\langle i \rangle$. The question then is, Which two? Because of the nature of modular

addition, it makes some sense to pick elements of \mathbb{Z}_8 that are spaced evenly throughout \mathbb{Z}_8 if we want them to correspond to the same action in $\langle i \rangle$. So let's look at the function $g : \mathbb{Z}_8 \rightarrow \langle i \rangle$ that takes

$$0, 4 \xrightarrow{g} 1, \quad 1, 5 \xrightarrow{g} i, \quad 2, 6 \xrightarrow{g} -1, \quad 3, 7 \xrightarrow{g} -i,$$

as shown in Figure 22.1.1.

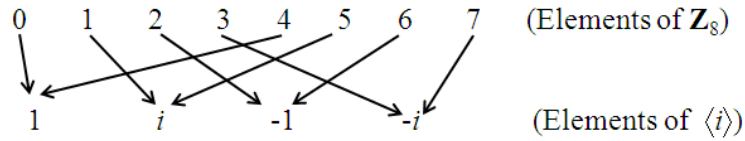


Figure 22.1.1. Function g between \mathbb{Z}_8 and $\langle i \rangle$.

Let's take the \mathbb{Z}_8 table then and start transforming it according to g . First we replace all the elements of \mathbb{Z}_8 with their counterparts in $\langle i \rangle$:

| \oplus | 1 | i | -1 | $-i$ | 1 | i | -1 | $-i$ |
|----------|------|------|------|------|------|------|------|------|
| 1 | 1 | i | -1 | $-i$ | 1 | i | -1 | $-i$ |
| i | i | -1 | $-i$ | 1 | i | -1 | $-i$ | 1 |
| -1 | -1 | $-i$ | 1 | i | -1 | $-i$ | 1 | i |
| $-i$ | $-i$ | 1 | i | -1 | $-i$ | 1 | i | -1 |
| 1 | 1 | i | -1 | $-i$ | 1 | i | -1 | $-i$ |
| i | i | -1 | $-i$ | 1 | i | -1 | $-i$ | 1 |
| -1 | -1 | $-i$ | 1 | i | -1 | $-i$ | 1 | i |
| $-i$ | $-i$ | 1 | i | -1 | $-i$ | 1 | i | -1 |

Table 22.3: First Transformation of \mathbb{Z}_8 into $\langle i \rangle$.

Then we remove redundant rows/columns and change the group operation, and voilà:

| | | | | |
|------|------|------|------|------|
| · | 1 | i | -1 | $-i$ |
| 1 | 1 | i | -1 | $-i$ |
| i | i | -1 | $-i$ | 1 |
| -1 | -1 | $-i$ | 1 | i |
| $-i$ | $-i$ | 1 | i | -1 |

Table 22.4: Second Transformation of \mathbb{Z}_8 into $\langle i \rangle$.

This is exactly the Cayley table for $\langle i \rangle$ (see Table 22.2). So g does it! It preserves the group operations: if we take any two elements of \mathbb{Z}_8 and add them (say $3 \oplus 5 = 0$), the result is the same as taking their corresponding elements in $\langle i \rangle$ and multiplying them ($-i \cdot i = 1$). In other words, for all $a, b \in \mathbb{Z}_8$,

$$g(a \oplus b) = g(a) \cdot g(b).$$

A bijection that preserved group operations was called an isomorphism. So what do we call g ? We say that g is a *homomorphism* from \mathbb{Z}_8 to $\langle i \rangle$, and that \mathbb{Z}_8 is *homomorphic* to $\langle i \rangle$. \blacklozenge

We see some interesting things in Example 22.1.1. The elements in \mathbb{Z}_8 that map to 1 are 0 and 4. The set $\{0, 4\}$ is a subgroup of \mathbb{Z}_8 . Naturally it's a normal subgroup, since \mathbb{Z}_8 is abelian. On the other hand, the sets $\{1, 5\}$, $\{2, 6\}$, and $\{3, 7\}$ which map to i , -1 , and $-i$ respectively are *not* subgroups of \mathbb{Z}_8 . Instead, we may recognize them as the *cosets* of $\{0, 4\}$ in \mathbb{Z}_8 . We saw in Section 18.4.1 that the cosets of a normal subgroup themselves form a group called the *quotient group*. You may want to go back and refresh your memory on the contents of that section before attempting the following exercise.

Exercise 22.1.2. Compute the Cayley table for $\mathbb{Z}_8/\{0, 4\}$. Label the rows and columns in the following order: $\{0, 4\}, \{1, 5\}, \{2, 6\}, \{3, 7\}$. \diamond

This table possesses an eerie similarity to another table that we've seen before:

Exercise 22.1.3.

(a) Compute the Cayley table for $\langle i \rangle$. Label the rows and columns in the following order: $1, i, -1, -i$.

- (b) By comparing Cayley tables, show that the function $h : \mathbb{Z}_8/\{0,4\} \rightarrow \langle i \rangle$ is an isomorphism, where

$$\{0,4\} \xrightarrow{h} 1, \quad \{1,5\} \xrightarrow{h} i, \quad \{2,6\} \xrightarrow{h} -1, \quad \{3,7\} \xrightarrow{h} -i.$$

◇

So $\mathbb{Z}_8/\{0,4\} \cong \langle i \rangle$! (See Figure 22.1.2.)

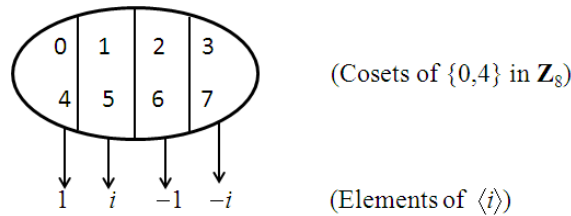


Figure 22.1.2. Isomorphism h between $\mathbb{Z}_8/\{0,4\}$ and $\langle i \rangle$.

Example 22.1.1 exhibited lots of interesting properties. Let's see if these properties hold for other examples as well. We may then formalize our observations and provide proofs.

Example 22.1.4. The function g which we constructed in Example 22.1.1 was not one-to-one, but it was onto. Is “onto” necessary? Or could we possibly find a function from \mathbb{Z}_8 to $\langle i \rangle$ that still preserves the group operation, whose range is not all of $\langle i \rangle$?

Let's consider the function $q : \mathbb{Z}_8 \rightarrow \langle i \rangle$ defined by:

$$0, 2, 4, 6 \xrightarrow{q} 1, \quad 1, 3, 5, 7 \xrightarrow{q} -1.$$

Exercise 22.1.5. Prove that $\{1, -1\}$ is a subgroup of $\langle i \rangle$. ◇

If we relabel the Cayley table for \mathbb{Z}_8 according to 1, we get the following:

| | | | | | | | | |
|----|----|----|----|----|----|----|----|----|
| · | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 |
| 1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 |
| -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 |
| 1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 |
| -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 |
| 1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 |
| -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 |
| 1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 |
| -1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 |

Table 22.5: First Transformation of \mathbb{Z}_8 into $\{1, -1\}$.

And then if we remove the redundant rows and columns, we get:

| | | |
|----|----|----|
| · | 1 | -1 |
| 1 | 1 | -1 |
| -1 | -1 | 1 |

Table 22.6: Second Transformation of \mathbb{Z}_8 into $\{1, -1\}$.

Now this isn't the *whole* Cayley table for $\langle i \rangle$ (Table 22.4), but it *is* the part of the Cayley table that corresponds to the elements 1 and -1 (remove rows 2 and 4 as well as columns 2 and 4). So q preserves the operations between \mathbb{Z}_8 and $\langle i \rangle$, since for all $a, b \in \mathbb{Z}_8$ we have

$$q(a \oplus b) = q(a) \cdot q(b).$$

In other words, q is a homomorphism. ♦

In Example 22.1.4 we find several similarities to 22.1.1:

- The set $\{0, 2, 4, 6\} \subset \mathbb{Z}_8$ which maps to the identity of $\langle i \rangle$ is a normal subgroup of \mathbb{Z}_8 . (We will use H to denote this subgroup.)
- The set $\{1, 3, 5, 7\}$ which maps to -1 is a coset of H in \mathbb{Z}_8 . (We may write $\{1, 3, 5, 7\}$ as $1 + H$).
- We may use the homomorphism q to construct an isomorphism, as you will show in the following exercise.

Exercise 22.1.6.

- (a) Create the Cayley Table for the quotient group \mathbb{Z}_8/H .
 (b) Show that the function from \mathbb{Z}_8/H to $\langle i \rangle$ which maps

$$H \longrightarrow 1, \quad 1 + H \longrightarrow -1$$

is an isomorphism from \mathbb{Z}_8/H to the subgroup $\{1, -1\}$ of $\langle i \rangle$.

◇

22.2 Definition and several more examples

In the previous section we saw that homomorphisms give us a way of finding structural similarity between groups, even when those groups are not isomorphic. A homomorphism only needs to map elements from one group to another in such a way that it preserves the operations between the two groups. That's it. Unlike isomorphisms, it doesn't have to be one-to-one or onto.

Let's now formally state the definition:

Definition 22.2.1. A *homomorphism* between groups (G, \cdot) and (H, \circ) is a function $f : G \rightarrow H$ such that

$$f(g_1 \cdot g_2) = f(g_1) \circ f(g_2)$$

for all $g_1, g_2 \in G$. The range of f in H is called the *homomorphic image* of f .¹ △

Exercise 22.2.2.

- (a) For the homomorphism g from \mathbb{Z}_8 to $\langle i \rangle$ in Example 22.1.1, what is the homomorphic image of g ?
 (b) For the homomorphism q from \mathbb{Z}_8 to $\langle i \rangle$ in Example 22.1.4, what is the homomorphic image of q ?

¹You may have noticed that in the Isomorphisms chapter we used Greek letters (ϕ etc.) for isomorphisms, whereas here we typically use the letter f to denote a homomorphism. There is no special reason for this—both notations are used in math books, and you should be comfortable either way.

◇

All of our examples so far have been with finite groups; let's look at infinite groups instead. As we saw in the Isomorphisms chapter, with finite groups we can use Cayley tables to verify the equality of the group operations, but with infinite groups we don't have Cayley tables, so we need to use the definition of a homomorphism.

Example 22.2.3. Recall that the circle group \mathbb{T} consists of all complex numbers z such that $|z| = 1$. So geometrically, the circle group consists of the complex numbers that trace out a circle of radius 1 about the origin in the complex plane (hence the name), as shown in the figure below:

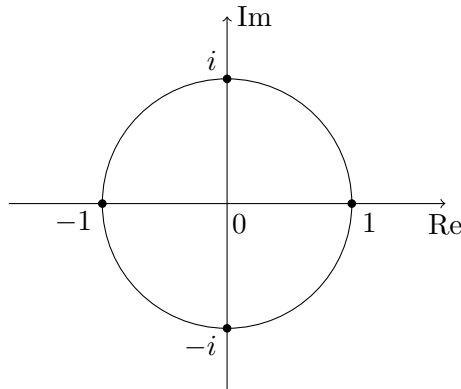


Figure 22.2.1. Circle group \mathbb{T} in complex plane

Now imagine wrapping the real number line around this circle like it was a tape measure, with 0 on the real number line corresponding to 1 on the unit circle. Then we would have a correspondence between each real number and a complex number in \mathbb{T} . Every 2π units the real numbers start around the circle again, so that an infinite set of real numbers corresponds to each complex number z in \mathbb{T} . For instance not only 0, but $2\pi, 4\pi, 6\pi$, etc. would correspond to 1. Evidently for a given complex number z , any real number α that corresponds to z is an *argument* for z (see Figure 4.3.2), so that $z = \text{cis } \alpha$. From this point of view, we may conceive of cis as a function from \mathbb{R} to \mathbb{T} . Does cis preserve the operations between \mathbb{R} and \mathbb{T} ? We've shown this before in Proposition 4.3.8 in the Complex Numbers chapter, but it

won't hurt to see it again:

$$\begin{aligned} \operatorname{cis}(\alpha + \beta) &= \cos(\alpha + \beta) + i \sin(\alpha + \beta) \\ &= (\cos \alpha \cos \beta - \sin \alpha \sin \beta) + i(\sin \alpha \cos \beta + \cos \alpha \sin \beta) \\ &= (\cos \alpha + i \sin \alpha)(\cos \beta + i \sin \beta) \\ &= \operatorname{cis}(\alpha) \operatorname{cis}(\beta). \end{aligned}$$

So we have it; cis is a homomorphism from the additive group of real numbers to the circle group. This means that in some sense, complex multiplication on the unit circle is like addition of real numbers. \blacklozenge

In the following exercise, we relate the previous example to the properties observed in Examples 22.1.1 and 22.1.4 in the previous section.

Exercise 22.2.4. As we mentioned above, cis maps $0, \pm 2\pi, \pm 4\pi$, etc to 1, the identity, in \mathbb{T} . Another way to say the same thing is:

$$\operatorname{cis}^{-1}(1) = \{\dots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \dots\}.$$

- (a) Prove that $\{\dots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \dots\}$ is a normal subgroup of \mathbb{R}
- (b) What are the cosets of $\{\dots, -4\pi, -2\pi, 0, 2\pi, 4\pi, \dots\}$ in \mathbb{R} ?
- (c) Define a function $F : \mathbb{R}/2\pi\mathbb{Z} \rightarrow \mathbb{T}$ by: $F(x + 2\pi\mathbb{Z}) = \operatorname{cis}(x)$. Show that the function is well-defined: that is, show that if x_1 and x_2 are both elements of the same coset of $2\pi\mathbb{Z}$, then $F(x_1 + 2\pi\mathbb{Z}) = F(x_2 + 2\pi\mathbb{Z})$.
- (d) Show that F defined above is a bijection: that is, F maps different cosets to different elements of \mathbb{T} .
- (e) Show that F defined above is an isomorphism.
- (f) What is the homomorphic image of the function $\operatorname{cis} : \mathbb{R} \rightarrow \mathbb{T}$?

\blacklozenge

Example 22.2.5. The circle group \mathbb{T} also gives us a completely different way of constructing a homomorphism between complex and real numbers. Every complex number in \mathbb{T} has modulus 1; i.e. they lie all on a circle of radius 1 in the complex plane. If we increase radius of the circle to 2, all of those complex numbers have the same modulus 2. In fact if you

keep increasing or decreasing the radius of the circle, you can catch all the complex numbers in the plane with the concentric circles you've created. So every complex number (except 0) corresponds to a positive real number by its modulus. Since we can represent any complex number as $r \operatorname{cis} \theta$, we can define a function $f : \mathbb{C}^* \mapsto \mathbb{R}^*$ by

$$f(r \operatorname{cis} \theta) = r.$$

Let's see whether f is a homomorphism. If $r_1 \operatorname{cis} \theta_1$ and $r_2 \operatorname{cis} \theta_2$ are arbitrary nonzero complex numbers, we have:

$$\begin{aligned} f((r_1 \operatorname{cis} \theta_1) \cdot (r_2 \operatorname{cis} \theta_2)) &= f(r_1 \operatorname{cis} \theta_1 r_2 \operatorname{cis} \theta_2) \\ &= f((r_1 r_2) \operatorname{cis}(\theta_1 + \theta_2)) \\ &= r_1 r_2 \\ &= f((r_1 \operatorname{cis} \theta_1) \cdot f(r_2 \operatorname{cis} \theta_2)). \end{aligned}$$

So f is indeed a homomorphism from \mathbb{C}^* to \mathbb{R}^* . ◆

Once again, we may compare this example to the remarks of the previous section.

Exercise 22.2.6. With reference to the function f defined in Example 22.2.5:

- (a) What is the homomorphic image of f ?
- (b) Prove that the homomorphic image of f is a subgroup of \mathbb{R}^* .
- (c) Find all the elements in \mathbb{C}^* that map to the identity in \mathbb{R}^* ; that is, find all $r \operatorname{cis} \theta \in \mathbb{C}^*$ such that $f(r \operatorname{cis} \theta) = 1$.
- (d) Is the set from part (b) a normal subgroup of \mathbb{C}^* ? Prove or disprove.
- (e) What are the cosets in \mathbb{C}^* of the set in part (b)?
- (f) Define the quotient group created by the normal subgroup in (e), and prove that it's isomorphic to the homomorphic image of f .

◆

Now it's your turn. In the following exercises, you'll have a chance to verify some homomorphisms for yourself.

Exercise 22.2.7. Consider the group $GL_2(\mathbb{R})$ (that is, the group of invertible 2×2 matrices under matrix multiplication). If

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is in $GL_2(\mathbb{R})$, then the determinant is nonzero; that is, $\det(A) = ad - bc \neq 0$.

- (a) Prove that $\det(AB) = \det(A)\det(B)$ for $A, B \in GL_2(\mathbb{R})$. This shows that the function \det is a homomorphism from $GL_2(\mathbb{R})$ to \mathbb{R}^* .
- (b) What is the homomorphic image of \det ?
- (c) In the Groups chapter we defined $SL_2(\mathbb{R})$ as the set of 2×2 real matrices whose determinant is 1. It follows that $SL_2(\mathbb{R})$ is the subset of $GL_2(\mathbb{R})$ which maps under \det to the identity of \mathbb{R}^* . Prove that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.
- (d) Describe the cosets of $SL_2(\mathbb{R})$ in $GL_2(\mathbb{R})$.
- (e) Prove that $SL_2(\mathbb{R})$ is a normal subgroup of $GL_2(\mathbb{R})$. (*Hint*)
- (f) Prove that the quotient group $GL_2(\mathbb{R})/SL_2(\mathbb{R})$ is isomorphic to \mathbb{R}^* .

◇

Remark 22.2.8. This last exercise wasn't as easy to visualize as the previous ones. So we had to rely on *properties* rather than intuition. This is typically what happens in mathematics: you start with visualizable examples, and use these as a springboard to leap into higher abstractions. △

Exercise 22.2.9.

- (a) Define a function $f : \mathbb{C} \rightarrow \mathbb{R}$ as follows: $f(a+bi) = a$. Prove or disprove: f is a homomorphism.
- (b) Define a function $g : \mathbb{C} \rightarrow \mathbb{R}$ as follows: $g(a+bi) = b$. Prove or disprove: g is a homomorphism.

- (c) Define a function $h : \mathbb{C}^* \rightarrow \mathbb{R}^*$ as follows: $h(a + bi) = a$. Prove or disprove: h is a homomorphism. (Note this is a different situation from part (a)!) ◇

Exercise 22.2.10. Remember that $\mathbb{M}_2(\mathbb{R})$ is the group of real-valued 2×2 matrices under addition. Define and prove a homomorphism from $\mathbb{M}_2(\mathbb{R})$ to \mathbb{R} . ◇

Now let's deal with homomorphisms in a more general context, to prepare us for the task of proving properties of homomorphisms in general (which we'll get to in the next section).

Exercise 22.2.11. Let G be a group and $g \in G$. In the Groups chapter we saw that the set of all integer powers (positive, negative, and zero) of g form a group, which is called the *cyclic subgroup* generated by g and is denoted by $\langle g \rangle$. Since each integer corresponds to a power of g , we may define a map $f : \mathbb{Z} \rightarrow G$ by $f(n) = g^n$.

- (a) Show that f is a group homomorphism.
- (b) What is the homomorphic image of f ?
- (c) Find all the elements in \mathbb{Z} that map to the identity in G .
- (d) Is the set from part (c) a subgroup of \mathbb{Z} ? Prove or disprove.
- (e) What are the cosets in \mathbb{Z} of the set in part (c)?
- (f) Show the set in part (c) is a normal subgroup in \mathbb{Z} .
- (g) Define the quotient group created by the normal subgroup in (f), and prove that it's isomorphic to the homomorphic image of f .

◇

Exercise 22.2.12. If G is an abelian group and $n \in \mathbb{N}$, show that $\phi : G \rightarrow G$ defined by $\phi(g) = g^n$ is a group homomorphism. ◇

Finally, let's look at one more pattern for the homomorphisms we've developed so far before we go proving these patterns/properties hold for homomorphisms of groups in general:

Exercise 22.2.13.

- (a) In the group \mathbb{Z}_8 , the inverse of 3 is 5 (we may write this as $3^{-1} = 5$). Using the homomorphism g from Example 22.1.1, what is $g(5)$? What is the inverse of $g(3)$ in the group $\langle i \rangle$? What does this example show about the relation between $g(3^{-1})$ and $(g(3))^{-1}$?
- (b) In \mathbb{Z}_8 , $2^{-1} = 6$. Using the homomorphism q from Example 22.1.4, what is $q(2^{-1})$? What is $(q(2))^{-1}$? What do you notice about your two answers?
- (c) In \mathbb{C}^* , $(r \operatorname{cis} \theta)^{-1} = \frac{1}{r} \operatorname{cis}(2\pi - \theta)$. Using f from Example 22.2.5, compute $f((r \operatorname{cis} \theta)^{-1})$ and $(f(r \operatorname{cis} \theta))^{-1}$. What do you notice about your two answers?
- (d) In $GL_2(\mathbb{R})$, what is the inverse of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$? Using f from Exercise 22.2.7, does $f\left(\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)^{-1}\right) = [f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)]^{-1}$? Verify or give a counterexample.
- (e) What general property of homomorphisms can you infer from these examples? (You don't need to give a proof if you don't want to.)

◇

22.3 Proofs of homomorphism properties

So it seems there are several properties of homomorphisms that have consistently held true in our examples so far. For any homomorphism f with domain G and the codomain H , it seems that:

- The elements in G that map under f to the identity of H are in fact a normal subgroup of G .
- The quotient group created by that normal subgroup is then isomorphic to the image of the homomorphism.

- If f maps g to h , then f also maps g^{-1} to h^{-1} .

These properties are indeed true for all homomorphisms, and we'll take the next two sections to prove these as well as other properties of homomorphisms. We begin with

Proposition 22.3.1. Let $f : G \rightarrow H$ be a homomorphism of groups. Then

1. If e is the identity of G , then $f(e)$ is the identity of H ;
2. For any element $g \in G$, $f(g^{-1}) = [f(g)]^{-1}$;
3. If S is a subgroup of G , then $f(S)$ is a subgroup of H ;
4. If T is a subgroup of H , then $f^{-1}(T) = \{g \in G : f(g) \in T\}$ is a subgroup of G . Furthermore, if T is normal in H , then $f^{-1}(T)$ is normal in G .

PROOF.

(1) Suppose that e and e' are the identities of G and H , respectively. Then

$$e'f(e) = f(e) = f(ee) = f(e)f(e).$$

By cancellation, $f(e) = e'$.

(2) This statement follows from the fact that

$$f(g^{-1})f(g) = f(g^{-1}g) = f(e) = e.$$

(3) The set $f(S)$ is nonempty since the identity of T is in $f(S)$. Suppose that S is a subgroup of G and let x and y be in $f(S)$. There exist elements $a, b \in S$ such that $f(a) = x$ and $f(b) = y$. Since

$$xy = f(a)f(b) = f(ab) \in f(S),$$

and

$$x^{-1} = f(a)^{-1} = f(a^{-1}) \in f(S),$$

it follows that $f(S)$ is a subgroup of H (since it is closed under the group operation and inverse).

(4) Let T be a subgroup of H and define S to be $f^{-1}(T)$; that is, S is the set of all $g \in G$ such that $f(g) \in T$. The identity is in S since $f(e) = e$. If

a and b are in S , then $f(ab^{-1}) = f(a)[f(b)]^{-1}$ is in T since T is a subgroup of H . Therefore, $ab^{-1} \in S$ and S is a subgroup of G . If T is normal in H , we must show that $g^{-1}hg \in S$ for $h \in S$ and $g \in G_1$. But

$$f(g^{-1}hg) = [f(g)]^{-1}f(h)f(g) \in T,$$

since T is a normal subgroup of H . Therefore, $g^{-1}hg \in S$. □

Now that we have these properties down, we can use them to prove some other properties of homomorphisms. We know that homomorphisms preserve group operations, which suggests that homomorphisms may preserve other group properties as well. We'll look at two group properties in the next exercise.

Exercise 22.3.2. Prove the following:

- (a) If $f : G \rightarrow H$ is a group homomorphism and G is abelian, prove that $f(G)$ is also abelian.
- (b) If $f : G \rightarrow H$ is a group homomorphism and G is cyclic, prove that $f(G)$ is also cyclic.

◇

One of the patterns we saw in our examples that we haven't verified yet was that the elements in G that map to the identity of H formed a normal subgroup in G . We can now prove this in general, but first a definition:

Definition 22.3.3. Let $f : G \rightarrow H$ be a homomorphism and suppose that e_H is the identity of H . The set $f^{-1}(\{e_H\})$ is called the **kernel** of f , and will be denoted by $\ker f$. △

Proposition 22.3.4. Let $f : G \rightarrow H$ be a group homomorphism. Then the kernel of f is a normal subgroup of G .

Exercise 22.3.5. Prove Proposition 22.3.4. (*Hint*) ◇

Exercise 22.3.6. What were the kernels of the homomorphisms in:

- (a) Example 22.1.1
- (b) Example 22.1.4
- (c) Example 22.2.3
- (d) Example 22.2.5
- (e) Exercise 22.2.7

◇

Exercise 22.3.7. Which of the following functions are homomorphisms? If the map is a homomorphism, what is the kernel?

1. $f : \mathbb{R} \rightarrow GL_2(\mathbb{R})$ defined by

$$f(a) = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

2. $f : GL_2(\mathbb{R}) \rightarrow \mathbb{R}$ defined by

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = a + d$$

3. $f : M_2(\mathbb{R}) \rightarrow \mathbb{R}$ defined by

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = b,$$

where $M_2(\mathbb{R})$ is the additive group of 2×2 matrices with entries in \mathbb{R} .

◇

Exercise 22.3.8. Let $f : \mathbb{Z} \rightarrow \mathbb{Z}$ be given by $f(n) = 7n$. Prove that f is a group homomorphism. Find the kernel and the image of f . ◇

Example 22.3.9. Suppose that we wish to determine all possible homomorphisms f from \mathbb{Z}_7 to \mathbb{Z}_{12} . Since the kernel of f must be a subgroup of \mathbb{Z}_7 , there are only two possible kernels, $\{0\}$ and all of \mathbb{Z}_7 . The image of a subgroup of \mathbb{Z}_7 must be a subgroup of \mathbb{Z}_{12} . Hence, there is no injective

homomorphism; otherwise, \mathbb{Z}_{12} would have a subgroup of order 7, which is impossible. Consequently, the only possible homomorphism from \mathbb{Z}_7 to \mathbb{Z}_{12} is the one mapping all elements to zero. \blacklozenge

Exercise 22.3.10. Describe all of the homomorphisms from \mathbb{Z}_{24} to \mathbb{Z}_{18} . \diamond

Exercise 22.3.11. Describe all of the homomorphisms from \mathbb{Z} to \mathbb{Z}_{12} . \diamond

Exercise 22.3.12. Find all of the homomorphisms $f : \mathbb{Z} \rightarrow \mathbb{Z}$. Which of these are isomorphisms? (*Hint*) \diamond

22.4 The First Isomorphism Theorem

There's one property that we observed in earlier sections of this chapter that we haven't proven so far, namely, the quotient group created by the kernel of a homomorphism is isomorphic to the image of the homomorphism. In order to do this, we'll need a clearer idea of how homomorphisms actually work. Figure 22.4.1 gives a schematic diagram of a general homomorphism f with kernel K .

The figure shows the cosets of K , which form a partition of G as we showed in the Cosets chapter. These cosets can be thought of as elements of the quotient group G/K .

The arrangement of arrows in the figure indicate that any two points in the same coset gK map to the same element of H . This is true because

$$f(gk) = f(g)f(k) = f(g)e' = f(g) \quad (\text{given that } g \in G, k \in K).$$

This implies that we can actually define a function F from G/K to H as follows:

$$F(gK) = f(g).$$

The function is well-defined because if $g'K = gK$ then $F(g'K) = f(g') = f(g) = F(gK)$.

So what's the point? It turns out that this function F is exactly the isomorphism that we're looking for. We've already shown that it's well-defined: all that's left is to show that it's one-to-one and onto, and that it preserves the operation. We state these results as a proposition.

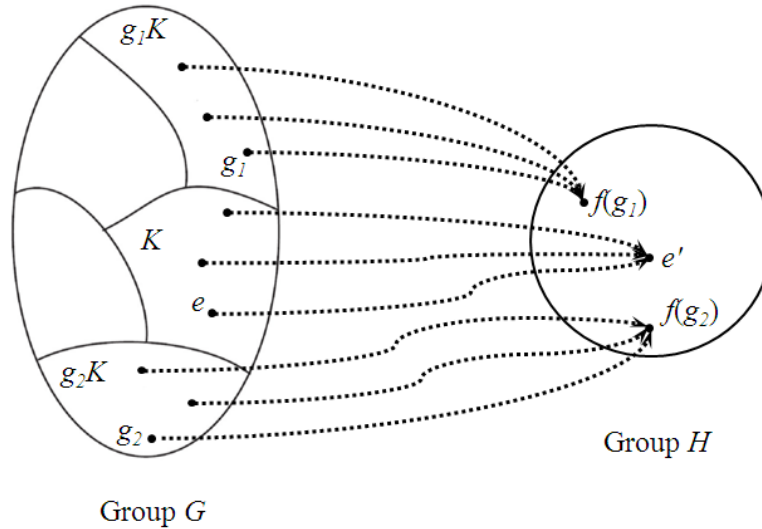


Figure 22.4.1. Homomorphism $f : G \rightarrow H$ with kernel K .

Proposition 22.4.1. (*First Isomorphism Theorem*)

Suppose $f : G \rightarrow H$ is a homomorphism with $K = \ker f$. Let the function $F : G/K \rightarrow f(G)$ be defined according to $F(gK) = f(g)$. Then F is an isomorphism.

PROOF. As mentioned above, we only need to show that F is 1-1, onto, and preserves the operation.

- 1-1: Suppose that $F(g_1K) = F(g_2K)$. Then according to the definition of F , this means that $f(g_1) = f(g_2)$. From this we obtain (using the homomorphism property of f):

$$f(g_1^{-1}g_2) = f(g_1^{-1})f(g_2) = f(g_1)^{-1}f(g_2) = f(g_1)^{-1}f(g_1) = e' \Rightarrow g_1^{-1}g_2 \in K.$$

By Proposition 18.2.1 in the Cosets chapter (parts (1) and (2)), this implies that $g_1K = g_2K$.

- Onto: Let h be an arbitrary element of $f(G)$. Then there exists $g \in G$ such that $f(g) = h$. By the definition of F , we have also that $F(gK) = h$.
- Preserves operations: Using properties of normal subgroups, we have:

$$F(g_1K g_2K) = F(g_1 g_2 K) = f(g_1 g_2) = f(g_1) f(g_2) = F(g_1K) F(g_2K).$$

□

Example 22.4.2. Let G be a cyclic group with generator g . Define a map $f : \mathbb{Z} \rightarrow G$ by $n \mapsto g^n$. This map is a surjective homomorphism since

$$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n).$$

Clearly f is onto. If $|g| = m$, then $g^m = e$. Hence, $\ker f = m\mathbb{Z}$ and $\mathbb{Z}/\ker f = \mathbb{Z}/m\mathbb{Z} \cong G$. On the other hand, if the order of g is infinite, then $\ker f = 0$ and ϕ is an isomorphism of G and \mathbb{Z} . Hence, two cyclic groups are isomorphic exactly when they have the same order. We may conclude that up to isomorphism, the only cyclic groups are \mathbb{Z} and \mathbb{Z}_n . ♦

Additional Exercises

1. Let $f : G \rightarrow H$ be a homomorphism. Show that f is one-to-one if and only if $f^{-1}(e') = \{e\}$, where e and e' are the identities of G and H , respectively.
2. For $k \in \mathbb{Z}_n$, define a map $f_k : \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ by $a \mapsto ka$. Prove that f_k is a homomorphism.
3. Show that a homomorphism defined on a cyclic group is completely determined by its action on the generator of the group. (*Hint*)
4. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \cong \mathbb{Q}$. (*Hint*)
5. Let G and H be groups, and let M and N be normal subgroups of G and H respectively. Let $f : G \rightarrow H$ be a homomorphism which satisfies $f(M) \subset N$. Show that f can be used to define a homomorphism $F : G/M \rightarrow H/N$.
6. Let $f : G \rightarrow H$ be a homomorphism that is onto. Let M be a normal subgroup of G and suppose that $f(M) = N$. Prove that $G/M \cong H/N$.

22.5 Hints for “Homomorphism” exercises

Exercise 22.2.7(d): Use Definition 18.4.13 from the Cosets chapter, and the multiplicative property of determinants.

Exercise 22.3.5: Use Part (d) of Proposition 22.3.1, using $T = \{e\}$.

Exercise 22.3.12: The function f is completely determined by the value of $f(1)$. For instance, if $f(1) = 2$, then the operation-preserving property implies that $f(n) = 2n$ for any integer n (Why?).

Additional exercises:

Exercise 3: Use the operation-preserving property.

Exercise 4: What is the order of $0.5 + \mathbb{Z}$?

Group Actions

We've defined a "group" as a set with an operation defined on it. From this point of view, group elements are "objects" in a set. We have many examples of this: like the integers with addition, the integers mod n , the group of units $U(n)$, groups of matrices, and so on.

Later on we introduced the idea that permutations form a group. Permutations are actually bijections (1-1, onto functions) that map a set of objects to itself. Another way of saying this is that permutations "act on" a set by moving the elements around. Similarly, we saw in Figure 13.3.1 in Section 13.3 that the symmetries of an equilateral triangle (which are elements of the group S_3) move the vertices of the triangle from one position to another. As a third example, in the group \mathbb{Q}^* of non-zero rational numbers we can think of left multiplying by 2 as "moving" -5 over to -10 . Left multiplying again by 2 "moves" -10 to -20 : and so on.

The examples in the previous paragraph illustrate a general concept called *group actions*. We will see in this chapter how group actions can give us deeper insight into the symmetries that we see in the world around us. In particular, we will focus on what group actions can tell us about regular polyhedra such as the tetrahedron and cube.

This chapter is by Holly Webb, with numerous additions by Mark Leech. Thanks to Tom Judson for material used in this chapter.

23.1 Basic definitions

We'll get to definitions momentarily, but first it's helpful to look at an example.

Example 23.1.1. Consider the group $S_3 = \{id, (AB), (AC), (BC), (ABC), (ACB)\}$ and the set $X = \{A, B, C\}$. Each element of S_3 “does something” to each element of X . See the Figure 23.1.1 below.

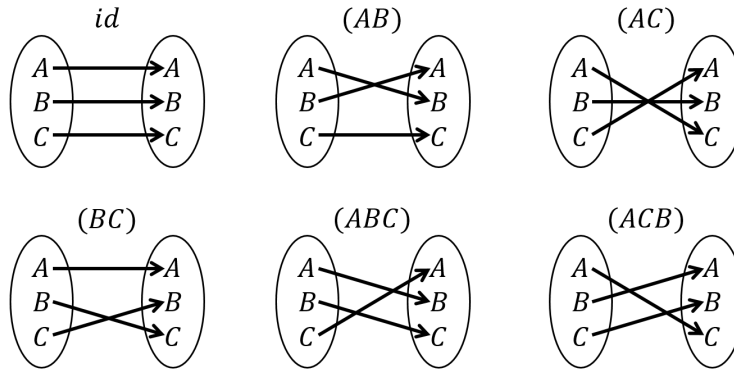


Figure 23.1.1. S_3 acting on $X = \{A, B, C\}$.

Let’s discuss the last element of S_3 , (ACB) . Notice (ACB) “does something” to each element of X . It maps $A \rightarrow C$, $B \rightarrow A$, and $C \rightarrow B$, so the map images are also elements of X . The same is true for all other elements of S_3 . In fact, each element of S_3 produces a bijection on the set $X = \{A, B, C\}$. We refer to this as the group S_3 *acting on* the set X . \blacklozenge

Example 23.1.2. Let R be the group of all rotations around the origin in \mathbb{R}^2 . Let $r_d \in R$ denote a counterclockwise rotation of d degrees. Also, let X be the set of all lines through the origin, where x_d denote the line which makes an angle of d degrees with the x -axis. See Figure 23.1.2 below.

Note that both R and X are infinite sets (unlike the previous example). As in Example 23.1.1, each element of R “does something” to each element of X . In this case, each element of R rotates an element of X , producing another element of X . For example, rotating the line x_{15} by r_{30} produces the line x_{45} . Furthermore r_{30} can rotate every element of X and *only* produces elements of X . This is true for all other rotations in R : each element of R produces a bijection on the set X . We again say that the group R *acts on* the set X . \blacklozenge

In the previous two examples we have been talking about a group “action” which is *different* from the group operation. For example, the group

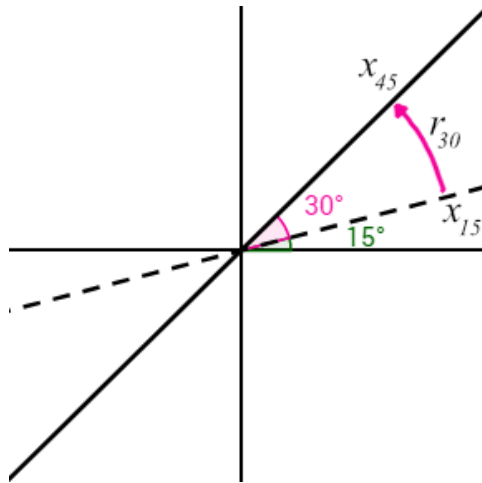


Figure 23.1.2. $r_d = r_{30}$ acting on the line $x_d = x_{15}$

operation in Example 23.1.1 is composition of permutations, but the action is a mapping of points in $\{A, B, C\}$. In Example 23.1.2 the group operation is composition of rotations, but the action is a mapping of lines. In order to distinguish the two operations, we will use the period (\cdot) to represent group action. For example the rotation illustrated in Figure 23.1.2 can be expressed mathematically as $r_{30}.x_{15} = x_{45}$.

Since we have two different operations (the group operation and the group action), we should determine how they interact with each other. We know that two group elements, g_1 and g_2 , can produce a third group element via the group operator because of closure, and that group element can act on a set element, x . We would represent this symbolically as $(g_1g_2).x$. But could that process be done differently? Yes, in fact one group element, g_2 , could act on the set element, x , then that resulting set element could be acted on by a different group element, g_1 . Symbolically we would write this as $g_1.(g_2.x)$. It turns out (and we will verify) that these two processes are equal to each other: $(g_1g_2).x = g_1.(g_2.x)$. We refer to this equality as *compatibility*.

Example 23.1.3. To investigate this idea of compatibility let's compare $[(AB)(ACB)].C$ and $(AB).[(ACB).C]$ where $(AB), (ACB) \in S_3$ and $B \in X = \{A, B, C\}$. Note: square brackets were used to group because per-

mutations use parentheses. Figure 23.1.3 below has the work and a visual representation of the work.

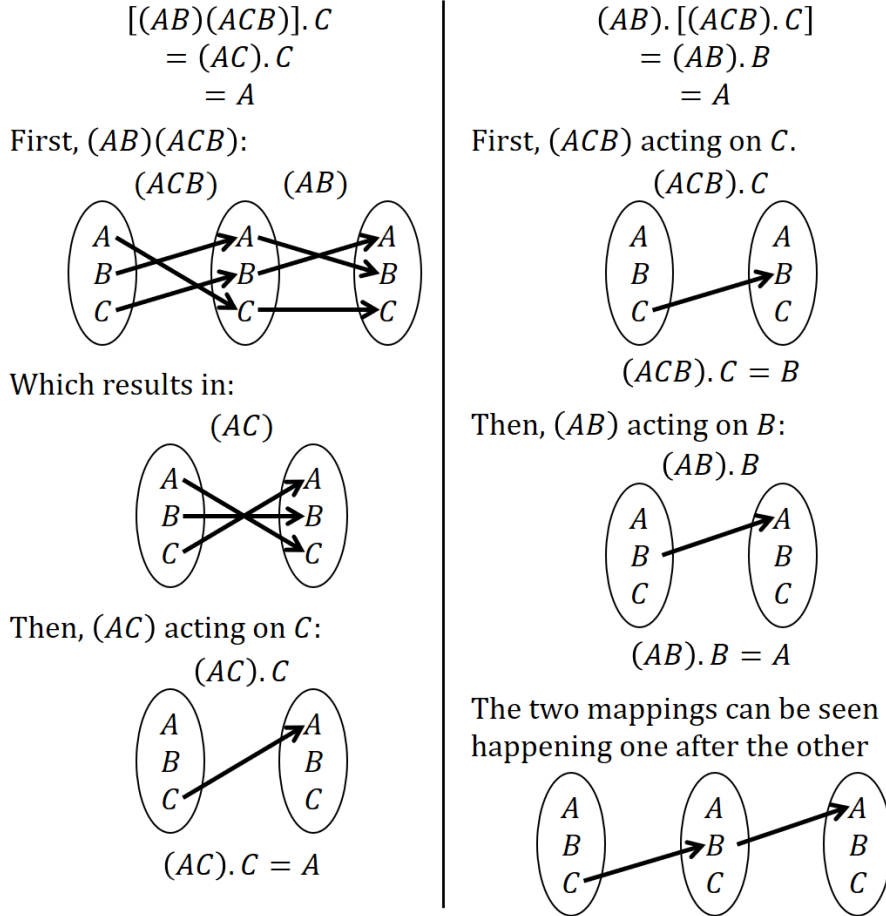


Figure 23.1.3. Formulas and diagrams demonstrating $[(AB)(ACB)].C = (AB).[(ACB).C]$

So, $[(AB)(ACB)].C = A = (AB).[(ACB).C]$, therefore, we can see compatibility in this specific case. Compatibility can be easily shown to hold for the other elements of X because S_3 produces a bijection on X .

Note the visual difference in the two operations. The group operation of composition of permutations has all the mapping arrows for all elements (the top left two illustrations). This is because the result of a composition of

permutations is another permutation. The other illustrations have only one mapping arrow because S_3 is acting on X producing only a single element of X . \blacklozenge

Example 23.1.4. Recall R and X from Example 23.1.2, show that $(r_{40} \circ r_{30}) \cdot x_{15} = r_{40} \cdot (r_{30} \cdot x_{15})$.

$$\begin{aligned} (r_{40} \circ r_{30}) \cdot x_{15} &\stackrel{?}{=} r_{40} \cdot (r_{30} \cdot x_{15}) \\ r_{70} \cdot x_{15} &\stackrel{?}{=} r_{40} \cdot x_{45} \\ x_{85} &\stackrel{\checkmark}{=} x_{85} \end{aligned}$$

\blacklozenge

Exercise 23.1.5. Let G be a group acting on the set X , and $\sigma, \tau \in G$ and $x \in X$. Using these elements, write a general rule for compatibility between G and X . \diamond

These ideas motivate the following definitions of action and G -Set:

Definition 23.1.6. Let G be a group and X be a set. A *(left) action* of G on X is a map $G \times X \rightarrow X$ given by $(g, x) \rightarrow g \cdot x$, such that

- (1) Identity: $e \cdot x = x$ for all $x \in X$, and e is the identity element of the group G ;
- (2) Compatibility: $(g_1 g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

We will use the period to represent group action. The set X on which G acts is called a *G -set*. \triangle

Remark 23.1.7.

- (1) X is not required to be a group, it only needs to be a set. G is the group. In some cases, as we will see, X can be a group.
- (2) $g \cdot x$ is not group multiplication. It is the result when g acts on x , and is always an element of X .

- (3) We call the set X a G -set because G is acting on it. If \mathbb{R}^2 is acting on X we will call X an \mathbb{R}^2 -set; $GL_2(\mathbb{R})$ acting on X would be a $GL_2(\mathbb{R})$ -set.
- (4) Notice that the second condition in Definition 23.1.6 is NOT associativity. It is not associativity because the group operation between g_1 and g_2 is not the action between g and x . Recall we refer to this property as compatibility.

△

It is also possible to define right group actions.

Exercise 23.1.8. Fill in the blanks with the missing information for the definition of right action. Let G be a group and X be a set. A (*right*) *action* of G on X is a map $\underline{\langle 1 \rangle} \times \underline{\langle 2 \rangle} \rightarrow \underline{\langle 3 \rangle}$ given by $(\underline{\langle 4 \rangle}, \underline{\langle 5 \rangle}) \rightarrow \underline{\langle 6 \rangle}$, such that

- (1) Identity: $\underline{\langle 7 \rangle} = \underline{\langle 8 \rangle}$ for all $x \in X$, and e is the identity element of the group G ;
- (2) Compatibility: $\underline{\langle 9 \rangle} = \underline{\langle 10 \rangle}$ for all $x \in X$ and all $g_1, g_2 \in G$.

◇

Moving forward in this chapter we'll focus just on left group actions. Following are some more examples of group actions.

Example 23.1.9. Consider $GL_2(\mathbb{R})$ (the group of invertible 2×2 matrices) and \mathbb{R}^2 . Show that $GL_2(\mathbb{R})$ acts on \mathbb{R}^2 by left multiplication on vectors which means that \mathbb{R}^2 is a $GL_2(\mathbb{R})$ -set. To check we must show identity and compatibility:

- (1) Check identity: If $v \in \mathbb{R}^2$ and I is the identity matrix, then $I.v = v$.
- (2) Check compatibility: If A and B are 2×2 invertible matrices, then $(AB).v = A.(B.v)$ (see Exercise 23.1.10 below)

Therefore, by definition, \mathbb{R}^2 is a $GL_2(\mathbb{R})$ -set. ◆

Exercise 23.1.10. Let

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}; \quad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}; \quad v = \begin{bmatrix} x \\ y \end{bmatrix}.$$

Verify the compatibility condition $(AB).v = A.(B.v)$ by using the properties of matrix multiplication. \diamond

Example 23.1.11. Let G be a group and \mathcal{E}_n be the set of all subsets of G with n elements where n is a positive integer and $n \leq |G|$. Let $S \in \mathcal{E}_n$, meaning S is a subset of G with n elements. Then G acts on \mathcal{E}_n by $g.S := \{gs \mid s \in S\}$. Note that $g.S$ is a subset of G with n elements. Let's verify that this is an action:

- (1) Check the identity condition: $e.S = \{es \mid s \in S\} = S$
- (2) Check the compatibility condition: Let $g, h \in G$, then $(gh).S = \{(gh)s \mid s \in S\} = \{g(hs) \mid s \in S\} = g.(h.S)$

Parts (1) and (2) verify that \mathcal{E}_n is a G -set. \blacklozenge

To show that (G, X) is *not* an action (in other words X is not a G -set), one may show any one of the following:

- $g.x \notin X$ for some $g \in G$ and $x \in X$;
- the identity condition fails $e.x \neq x$ for some $x \in X$; or
- the compatibility condition fails: $(g_1g_2).x \neq g_1.(g_2.x)$ for some $x \in X$ and some $g_1, g_2 \in G$.

Usually the easiest way to show one of the above items is by a counterexample.

Exercise 23.1.12.

- (a) Let $G = 2\mathbb{Z}$ and let $X = \mathbb{Z}$. Show that X is a G -set.
- (b) Let $X = 2\mathbb{Z}$. Show that X is *not* a \mathbb{Z} -set. ([*Hint*](#))
- (c) Let $G = H_6$ (the complex 6-th roots of unity (see Section 4.4.1 in Chapter 4)) and let $X = \mathbb{C}$. Show that X is a G -set.
- (d) Let $X = H_8$. Is X a \mathbb{C} -set? Explain. ([*Hint*](#))

\diamond

23.2 Symmetries of regular polyhedra

We want to apply our new ideas to gain insight about the groups of rotational symmetries of **regular polyhedra**. In general, a *polyhedron* can be thought of as a collection of faces, edges and vertices: for example, a cube has 6 faces, 12 edges and 8 vertices. A *regular polyhedron* is a polyhedron in which all faces are congruent regular polygons, and the same number of edges meet at every vertex. The group of rotational symmetries of a polyhedron act on the faces, edges and vertices. Any rotational symmetry will always take faces to faces, edges to edges and vertices to vertices.

In the following discussion we'll be introducing a bunch of new ideas. As usual, we'll illustrate these ideas first on a particular example. So let's begin with the cube, which is perhaps the regular polyhedron which is easiest to understand.

23.2.1 G -equivalence and orbits

Some of the rotational symmetries of the cube are indicated in Figure 23.2.1.

¹ The figure shows three possible rotation axes. We will denote the 90° counterclockwise rotations around the x, y and z axes as r_x, r_y, r_z respectively. We will also denote the faces of the cube as $x_-, x_+, y_-, y_+, z_-, z_+$. For example the rotation $r_x \circ r_x = r_x^2$ will take the bottom face (z_-) to the top face (z_+).

Remark 23.2.1. When we rotate the cube, the axes remain *fixed* while the cube rotates around them. So in Figure 23.2.1 you may imagine the axes to be like “laser beams” going through the cube, where the laser beams are labeled x, y and z according to their axes. These laser beams and labels do not move when the figure is rotated. For example, consider the rotation r_z followed by r_x (which is written as $r_x \circ r_z$). Under r_z , the face x_+ will rotate where the y_+ face was. Then following rotation r_x will occur around the original laser beam x axis, and not the axis to where the x_+ face has moved (which would be the rotation r_y). The cube ends up with the face x_+ on the top with the z axis, y_+ on the negative side of the x axis, and z_+ on the negative side of the y axis. \triangle

¹Note that these are NOT the only rotational symmetries of the cube—we'll discuss the others later (see this excellent video: <http://www.youtube.com/watch?v=gBg4-1J19Gg>).

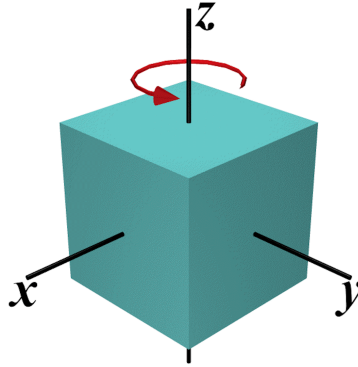


Figure 23.2.1. Cube with 3 axes of rotation that give symmetries.

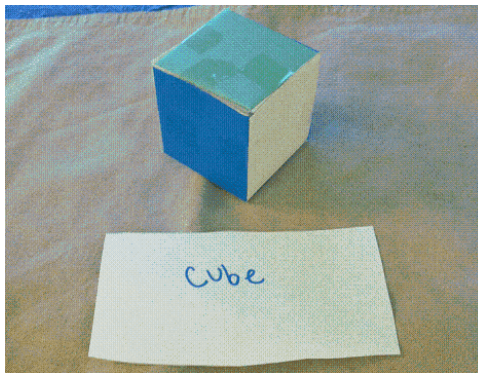


Figure 23.2.2. A paper cube to print, cut and fold (from <http://www.korthalsaltes.com>).

Remark 23.2.2. Make or find a physical manipulative of a cube. This can be a 6-sided die or constructed from paper as seen in Figure 23.2.2. When working with a manipulative of your polyhedron it is a good idea label each face uniquely, whether by color, letter, number, or symbol. If you label your faces x_+ , x_- , y_+ , etc., make sure to remember that these refer to *faces* and not *axes* (as we said above, the axes are like fixed laser beams that don't move with the cube). It also helps to take a picture or two of your manipulative when in its starting position. You might also draw a pair of x and y axes on a spare sheet of paper, set this on the table, and rotate your cube above this paper. \triangle

Exercise 23.2.3.

- (a) Give rotations that take the bottom face (z_-) to each of the faces x_-, x_+, y_-, y_+ .
- (b) Give rotations that take the face y_- to each of the faces x_-, x_+, y_+, z_-, z_+ .
- (c) Let's define a notation for the cube's vertices as follows. For example, $+++$ represents the vertex in the first octant ($x > 0, y > 0, z > 0$). The vertex $+- -$ will be in the octant where $x > 0, y < 0, z < 0$ (Which is the vertex at lower left in Figure 23.2.1). Give rotations that take the vertex $+- -$ to each of the of the vertices

$$+++ , - ++ , + - + , ++ - , - - + , - + - , - - - .$$

- (d) Let's denote the edges of the cube as follows. For example, $\overline{x_+, z_-}$ represents the edge where the faces x_+ and z_- meet. The edge $\overline{x_+, y_-}$ is where the faces x_+ and y_- meet. (This is the left, front-facing edge of cube in Figure 23.2.1.)
- (i) Using the above notation, list all edges of the cube.
- (ii) Give rotations that take the edge $\overline{x_+, y_-}$ to each of the other edges.

◇

From the previous exercise it's pretty clear that for any two faces of a cube there is at least one symmetry that takes the first face to the second. In other words, if A and B represent faces then there always exists a symmetry g such that $gA = B$. This example motivates the following definition.

Definition 23.2.4. If a group G acts on a set X and $x, y \in X$, then x is said to be *G -equivalent* to y if there exists a $g \in G$ such that $g.x = y$. We write $x \sim_G y$ or $x \sim y$ if two elements are G -equivalent. \triangle

By this definition we can say that all faces of a cube are G -equivalent to each other under the group of rotational symmetries of a cube, because given any two faces we can always find a rotation that takes the first face to the second face (and the inverse rotation takes the second face back to the first face). The notation we're using strongly suggests that \sim_G must be an equivalence relation. In fact this is true:

Proposition 23.2.5. Let X be a G -set. Then G -equivalence is an equivalence relation on X .

PROOF. The relation \sim is reflexive since $ex = x$. Suppose that $x \sim y$ for $x, y \in X$. Then there exists a g such that $g.x = y$. In this case $g^{-1}.y = x$; hence, $y \sim x$. To show that the relation is transitive, suppose that $x \sim y$ and $y \sim z$. Then, there must exist group elements g and h such that $g.x = y$ and $h.y = z$. So $z = h.y = (hg).x$, and x is equivalent to z . \square

Recall from Chapter 17 that every equivalence relation on a set X is associated with a partition of X , where a partition is a collection of disjoint subsets whose union is X . Each set in this partition is called an *equivalence class*.

Exercise 23.2.6. Consider the edge $\overline{y_+, z_+}$ of a cube. What is the equivalence class of this edge under G -equivalence, where G is the group of rotational symmetries of a cube? *Explain* your answer. \diamond

In the case of a cube where $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$ The three sets $\{\text{faces}\}, \{\text{edges}\}, \{\text{vertices}\}$ are disjoint equivalence classes whose union is X . We call each of these sets an *orbit* of X under G . In general, we have the following definition.

Definition 23.2.7. If X is a G -set, then each set in the partition of X associated with G -equivalence is called an *orbit* of X under G . We will denote the orbit that contains an element x of X by \mathcal{O}_x . \triangle

The next example shows how these concepts apply to permutation groups as well.

Example 23.2.8. Let G be the permutation group defined by

$$G = \{(1), (123), (132), (45), (123)(45), (132)(45)\}$$

and $X = \{1, 2, 3, 4, 5\}$. Then X is a G -set. There are permutations in G that take $1 \rightarrow 2, 1 \rightarrow 3, 2 \rightarrow 3$, and vice versa. There are also permutations that take $4 \rightarrow 5$ and vice versa. So the orbits are $\{1, 2, 3\}$ and $\{4, 5\}$. \blacklozenge

Exercise 23.2.9.

- (a) Let $G = \{\text{id}, \mu_1\}$ which is a subgroup of S_3 (the symmetry group of an equilateral triangle) (See Figure 13.3.1 in Section 13.3.) Let $X = \{A, B, C\}$ be the set of vertices of an equilateral triangle. List the orbits of X under G
- (b) Let G be the permutation group defined by

$$G = \{(1), (1358), (15)(38), (1853), (247), (274), (1358)(247), (15)(38)(247), \\ (1853)(247), (1358)(274), (15)(38)(274), (1853)(274)\}$$

and $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. Then X is a G -set. List the orbits of X under G .

◇

23.2.2 Stabilizers, stabilizer subgroups, and fixed point sets

Let's return to the cube to illustrate another new concept. Every rotation of a cube has an axis of rotation as well as an angle. For rotations which are symmetries we've considered 3 possible axes, passing through opposite pairs of faces. Take for instance the axis which passes through x_+ and x_- , and consider the set of all the rotational symmetries having this axis. In fact, this set of symmetries forms a subgroup of the symmetries of the cube (in this case, the subgroup is isomorphic to the rotations of the square or $(\mathbb{Z}_4, +)$). Now all of the elements of this subgroup leave the face x_+ fixed (although x_+ rotates, it remains in the same place). Similarly, the rotations about the axis through y_+ and y_- form a subgroup whose elements leave y_+ fixed; and the rotations about the axis through z_+ and z_- behave the same way for z_+ .

These are all examples of *stabilizer subgroups*. The general definition is as follows.

Definition 23.2.10. Given that X is a G -set and $x \in X$, let G_x be the set of group elements g that fix x : in other words, $g.x = x$. Then G_x is called the *stabilizer subgroup* or *isotropy subgroup* for the element x . △

The above definition presumes that G_x is in fact a subgroup of G , which up until now we haven't proved. The following exercise remedies this deficiency:

Exercise 23.2.11. Given any x in X , prove that the stabilizer subgroup G_x is indeed a subgroup of G . (Recall this involves proving closure under composition and inverse.) \diamond

Definition 23.2.10 talks about elements of the group G which leave a particular element of set X fixed. We can turn this around and consider elements of X which are fixed by a particular element of G . In fact, each element of G has an associated subset of X that it leaves unchanged.

Consider for instance the group of rotations of a cube. We may describe the cube as consisting of faces, edges, and vertices. So let's take $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. Rotations about the x axis (which can all be expressed as r_x^n for some n) leave the faces x_+ and x_- fixed. Similarly, $\{y_+, y_-\}$ and $\{z_+, z_-\}$ are fixed by rotations about the y axis and z axis, respectively. Thus, $\{x_+, x_-\}, \{y_+, y_-\}, \{z_+, z_-\}$, are all examples of *fixed point sets* in X . This leads to another definition:

Definition 23.2.12. Let G be a group acting on a set X , and let g be an element of G . The **fixed point set** of g in X , denoted by X_g , is the set of all $x \in X$ such that $g.x = x$. \triangle

It is important to remember that $X_g \subset X$ and $G_x \subset G$.

Let's use this notation to describe some stabilizer subgroups and fixed point sets for familiar examples of group actions.

Example 23.2.13. Let G be the rotational symmetries of a cube and $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. The fixed point set of id is:

$$X_{\text{id}} = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\},$$

since the identity rotation leaves the entire cube unchanged. \blacklozenge

Example 23.2.14. Let's consider the stabilizer subgroups for the faces of a cube. These contain the elements of the group G of rotations of the cube that leave each face unchanged. The stabilizer subgroups for the faces are:

$$\begin{aligned} G_{x_+} &= G_{x_-} = \{\text{id}, r_x, r_x^2, r_x^3\} \\ G_{y_+} &= G_{y_-} = \{\text{id}, r_y, r_y^2, r_y^3\} \\ \dots\dots G_{z_+} &= G_{z_-} = \{\text{id}, r_z, r_z^2, r_z^3\} \end{aligned}$$

\blacklozenge

Example 23.2.15. Let $X = \{1, 2, 3, 4, 5, 6\}$ and suppose that G is the permutation group given by the permutations

$$\{(1), (12)(3456), (35)(46), (12)(3654)\}.$$

Then the fixed point sets of X under the action of G for the different group elements are

$$\begin{aligned} X_{(1)} &= X, \\ X_{(35)(46)} &= \{1, 2\}, \\ X_{(12)(3456)} &= X_{(12)(3654)} = \emptyset, \end{aligned}$$

and the stabilizer subgroups for the different elements of X are

$$\begin{aligned} G_1 &= G_2 = \{(1), (35)(46)\}, \\ G_3 &= G_4 = G_5 = G_6 = \{(1)\}. \end{aligned}$$

◆

Exercise 23.2.16.

Let $G = S_4$ (the permutations of 4 elements), and let $X = \{1, 2, 3, 4\}$. X is a G -set.

- Give G_2 , G_4 , and $G_2 \cap G_4$. Is $G_2 \cap G_4$ a group? *Explain* your answer.
- Give $X_{(123)}$, $X_{(234)}$, and $X_{(123)} \cap X_{(234)}$.
- Repeat part (a) with $G = A_4$ (the group of even permutations on 4 elements).
- Repeat part (b) with $G = A_4$ (the group of even permutations on 4 elements).

◇

As usual, we will denote the number of elements in the fixed point set of an element $g \in G$ by $|X_g|$, the number of elements of the stabilizer subgroup of $x \in X$ as $|G_x|$ and the number of elements in the orbit of $x \in X$ by $|O_x|$.

Exercise 23.2.17. Let $G = S_n$ (the permutations of n elements), and let $X = \{1, 2, \dots, n\}$. X is a G -set.

- What is $|G_1|$? What is $|G_2|$? What is $|G_k|$ where $k \in X$? (Recall that $|S_n| = n!$)

- (b) If g is a 3-cycle, then what is $|X_g|$? What if g is a 5-cycle? (You may assume that $n \geq 5$).
- (c) Give a general formula for $|X_g|$, where g is a k -cycle ($2 \leq k \leq n$).
- (d) Repeat part (a) with $G = A_n$ (the even permutations of n elements).
- (e) Repeat part (b) with $G = A_n$.
- (f) Repeat part (c) with $G = A_n$.

◇

23.2.3 Counting formula for the order of polyhedral rotational symmetry groups

It is possible to characterize the size of the rotational symmetry group G for a regular polyhedron in terms of $|\mathcal{O}_x|$ and $|G_x|$. We'll show this with an example.

Example 23.2.18. Consider our old friend the group of rotational symmetries of a cube acting on $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. We've seen that $G_{x_+} = \{\text{id}, r_x, r_x^2, r_x^3\}$ is the stabilizer subgroup for x_+ . Thus there are four rotations that take x_+ to itself. We've also seen that there's at least one rotation that takes x_+ to each of the six faces of the cube: this is the same thing as saying that the orbit of a face is the set of all faces. Each of these rotations can be composed with any of the elements of G_{x_+} for a total of $6 \cdot 4 = 24$ rotational symmetries of a cube. To summarize, we've discovered that

$$|G| = |G_{x_+}| \cdot |\mathcal{O}_{x_+}|.$$

Note that x_+ was an arbitrary choice: we could use this argument with any of the faces and obtain the same result. ◆

In the previous example we used faces to count the rotational symmetries of a cube but we could use edges or vertices as well. In the next exercise we'll consider edges and in the following one we'll consider vertices. Remember that a model of a cube might help with these exercises (see Figure 23.2.2).

Exercise 23.2.19.

- (a) Find the stabilizer subgroup for the edge $\overline{x_+, z_+}$. (*Hint*)
- (b) Find the stabilizer subgroup for the edge $\overline{x_-, y_+}$.
- (c) In Example 23.2.18 we constructed a formula for $|G|$ in terms of $|G_{x_+}|$ and $|\mathcal{O}_{x_+}|$. Construct a similar formula using $G_{\overline{x_+, z_+}}$ and $|\mathcal{O}_{\overline{x_+, z_+}}|$, and show that you get the same answer. Do the same thing with $G_{\overline{x_-, y_+}}$ and $|\mathcal{O}_{\overline{x_-, y_+}}|$.
- (d) Find the stabilizer subgroup for the vertex $+, +, +$ (*Hint*)
- (e) Find the stabilizer subgroup for the vertex $+, -, +$.
- (f) Using parts (d) and (e), construct alternative formulas for $|G|$.

◇

From the previous example and exercises, it seems we have a general formula: if G acts on X and $x \in X$, then

$$|G| = |G_x| \cdot |\mathcal{O}_x|.$$

This may remind you of *Lagrange's Theorem*, which we proved in Section 18.3 of the Cosets chapter:

$$|G| = |H| \cdot [G : H],$$

where H is any subgroup of G . If we replace H with G_x , this becomes

$$|G| = |G_x| \cdot [G : G_x].$$

Comparing with our previous formula, we get

$$|\mathcal{O}_x| = [G : G_x].$$

Let's give a bona fide mathematical proof of this.

Proposition 23.2.20. (*Counting formula*): Let G be a group and X a G -set. If $x \in X$, then $|\mathcal{O}_x| = [G : G_x]$.

PROOF. In general, a good way to show that two sets are the same size is to show that there is a *bijection* (1-1 and onto map) between the two sets. We will define a map ϕ between the orbit \mathcal{O}_x and the set of left cosets of G_x in G as follows. Let $y \in \mathcal{O}_x$. Then there exists a g in G such that $gx = y$.

Define ϕ by $\phi(y) = gG_x$. Note that this coset contains an element $ge = g$: so it contains an element that takes $x \rightarrow y$.

Before we can show that ϕ is a bijection, we must first show that $\phi(y)$ is well-defined for any y , and does not depend on our selection of g . Suppose that g' is another element in G such that $g'x = y$. Then $gx = g'x$ or $x = g^{-1}g'x$. By the definition of the stabilizer subgroup G_x , $g^{-1}g' \in G_x$. By Proposition 18.2.1 in Section 18.2, it follows that $gG_x = g'G_x$. Thus, y gets mapped to the same coset regardless of the choice of group element.

To show that ϕ is one-to-one, we'll assume that $\phi(x_1) = \phi(x_2)$, and show that this means that $x_1 = x_2$. Here we go:

Recall that $\phi(x_1)$ is defined as a coset of G_x that contains an element g_1 that satisfies $g_1x = x_1$. Similarly, $\phi(x_2)$, contains an element g_2 that satisfies $g_2x = x_2$. But we're assuming that $\phi(x_1) = \phi(x_2)$. This means that g_1 and g_2 are in the same coset of G_x .

Now consider the expression $g_1(g_1^{-1}g_2)x$. On the one hand, by the associative law we get:

$$(g_1g_1^{-1})g_2x = g_2x = x_2.$$

On the other hand, by Proposition 18.2.1 in the Cosets chapter, it follows that $g_1^{-1}g_2$ is in G_x , so that $g_1^{-1}g_2x = x$. This means that we also have:

$$g_1(g_1^{-1}g_2)x = g_1x = x_1.$$

Therefore $x_1 = x_2$. This completes the proof that ϕ is 1-1.

Finally, we must show that the map ϕ is onto: that is, every coset of G_x is in the range of ϕ . This is much quicker than the proof of 1-1. Let gG_x be any left coset. If $gx = y$, then $\phi(y) = gG_x$. Thus gG_x is in the range of ϕ , and the proof is finished. \square

At this point, it is straightforward to put Proposition 23.2.20 together with Lagrange's Theorem to obtain:

Proposition 23.2.21. (*Orbit-Stabilizer Theorem*): Let G be a group and X a G -set. Given $x \in X$, let \mathcal{O}_x be the orbit of x under G , and let G_x be the stabilizer subgroup for the element x . then $|G| = |\mathcal{O}_x||G_x|$.

Exercise 23.2.22. Prove Proposition 23.2.21. \diamond

The Orbit-Stabilizer Theorem enables us to quickly find some nifty relationships among numbers of faces, vertices, and edges:

Exercise 23.2.23.

- (a) Show using Proposition 23.2.21 that for the cube, the ratio (number of edges / (number of faces)) = $4/2$.
- (b) Use the same method to find the ratio (number of edges) / (number of vertices) for the cube.
- (c) For the dodecahedron (regular polyhedron with 12-sided faces), find the ratio of (number of faces) / (number of vertices). (*Hint*)

◇

23.2.4 Representing a symmetry group in terms of stabilizer subgroups

We can approach the structure of the group of rotational symmetries of a cube from another direction. We've talked about stabilizer subgroups, and we can see how these subgroups "fit together" within G . For example, we've seen that for every face there are three rotations (besides the identity) that leaves that face fixed. These rotations correspond to 90, 180, and 270 degree rotations of a square: so they have order 4, 2, and 4 respectively.² So for each face, there are two rotations of order 4 and one rotation of order 2 in the stabilizer of that face. Since there are 6 faces of a cube, this seems to imply that there must be twelve rotations of order 4 and six rotations of order 2 associated with the stabilizers of the different faces.

Unfortunately, this is not quite true. The reason is that any rotation that leaves the front face fixed also leaves the back face fixed. So the stabilizer of the front face is the same as the stabilizer of the back face. In fact, the faces of the cube are stabilized in pairs: front-back, left-right, and top-bottom. Since there are 3 pairs, this means that we only have 6 rotations of order 4 and 3 rotations of order 2. If we add in the identity, this gives a total of 10 rotations. But we've already shown that the group of rotational symmetries of a cube has 24 elements. So where are the other 14?

Well, we haven't exhausted the possible stabilizers. Consider for instance the stabilizer of a vertex. We know that 3 faces meet at each vertex. So if I twirl the cube around the vertex, the three faces can rotate into each

²Recall that the "order" of a group element g is the smallest positive integer n such that $g^n = \text{id}$.

other. So besides the identity, there are two rotations of order 3. As with the faces, each vertex has a corresponding opposite vertex—so the vertices are stabilized in pairs. Since there are 8 vertices, this means there are 4 pairs, which means there are 8 rotations of order 3. This brings us up to a total of 18 rotations. So where are the other six?

Exercise 23.2.24. Consider the edges of a cube.

- For each edge, how many rotations (besides the identity) leave that edge fixed?
- What are the orders of the rotations (besides the identity) that leave an edge fixed?
- Do edges come in pairs or not? If so give the pairs, if not, explain why not.
- Altogether how many group elements (besides the identity) stabilize at least one edge?

◇

Exercise 23.2.25. Based on the information given in the preceding discussion, complete the following table to characterize the group elements of the rotational symmetries of a cube according to their orders and fixed point sets (you may also find this video to be helpful: <http://www.youtube.com/watch?v=gBg4-1J19Gg>). (*Hint*)

| Number of group elements | order | Fixed point set |
|--------------------------|-------|------------------------|
| 1 | 1 | entire cube (identity) |
| 6 | 4 | opposite faces |
| – | – | opposite faces |
| – | – | opposite vertices |
| – | – | opposite edges |

◇

Exercise 23.2.26. The table in Exercise 23.2.25 is suspiciously like something that we’ve seen before.

- Consider the group S_4 , which has 24 elements. Make a table with three columns labeled, “number of elements”, “order of the element”, “cycle

structure”. In the right-hand column, list the possible cycle structures: identity, one 4-cycle, two 2-cycles, one 3-cycle, and one 2-cycle. Then fill in the other two columns according to the cycle structure listed in each row.

- (b) Based on the table you created in part (a) and the table in Exercise 23.2.25, what do you conjecture?

◇

23.2.5 Examples of other regular polyhedral rotation groups

Let’s get to know some other regular polyhedra using orbits and stabilizer subgroups to describe their rotational symmetry groups.

The tetrahedron

Consider a regular tetrahedron, as shown in Figure 23.2.3. This polyhedron has 4 faces, 6 edges and 4 vertices. Each face is a triangle and each face is opposite a vertex. We will consider the rotations of a tetrahedron around 4 axes. Each axis passes through a vertex and the face opposite that vertex. See Figure 23.2.3. For example, a rotation of the axis through vertex A will also stabilize face a . We can call this axis \overleftrightarrow{Aa} . Similarly, we will call the other axes \overleftrightarrow{Bb} , \overleftrightarrow{Cc} and \overleftrightarrow{Dd} .

Each of these axes rotates a triangular face. We’ll write one counter-clockwise rotation of face a around \overleftrightarrow{Aa} as r_{Aa} (and similarly for the other axes). An animation of the rotations of a tetrahedron is available at:

<https://www.youtube.com/watch?v=qAR8BFMS3Bc>

You can also make your own tetrahedron like the one in Figure 23.2.4.

Exercise 23.2.27.

- (a) How many degrees does r_{Aa} rotate face a ?
- (b) What is the order of r_{Aa} ?

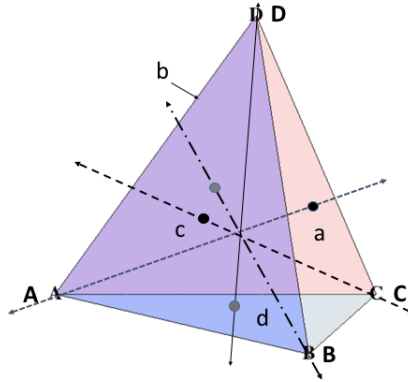


Figure 23.2.3. Tetrahedron with 4 axes of rotation that give symmetries. Figure modified from <https://inspirehep.net/record/1228365/plots>.

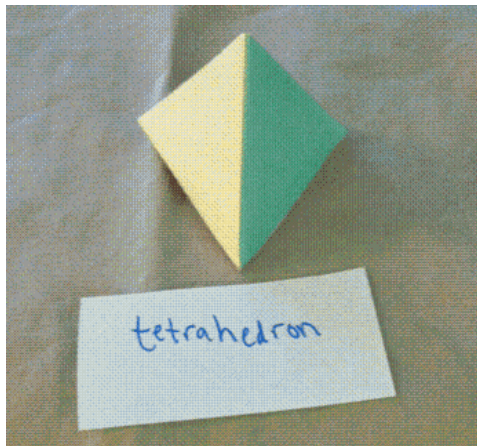


Figure 23.2.4. Tetrahedron to print, cut and fold (from <http://www.korthalsaltes.com>).

◇

Consider the tetrahedron in Figure 23.2.3. The rotation r_{C_c} takes vertex D to vertex A and face d to face a .

Exercise 23.2.28. We'll find it useful later to represent these rotations as permutations.

- (a) Represent each of the rotations r_{Aa} , r_{Bb} , r_{Cc} , r_{Dd} as permutations on the set of vertices.
- (b) Represent each of the rotations r_{Aa} , r_{Bb} , r_{Cc} , r_{Dd} as permutations on the set of faces.

◇

Exercise 23.2.29.

- (a) Give rotations that takes face c to each to each of the other faces a, b, d .
- (b) Give rotations that takes vertex D to each of the other vertices.
- (c) Consider the edges of the tetrahedron. Denote the edge between the vertices C and D as \overline{CD} : and other edges similarly. Use this notation to name each of the edges of the tetrahedron.
- (d) Give a rotation that takes edge \overline{CD} to each of the other edges.

◇

Exercise 23.2.30. Consider the vertex A of a tetrahedron. What is the equivalence class of this vertex under G -equivalence, where G is the groups of rotational symmetries of a tetrahedron? (Note: This G -equivalence class is the same as orbit of A . which we denote as \mathcal{O}_A .) ◇

Just as with the cube, the rotation group G of any polyhedron acts on the set $X = \{\text{faces}\} \cup \{\text{edges}\} \cup \{\text{vertices}\}$. Recall that each group element $g \in G$ has a *fixed point set* $X_g \in X$ that it leaves unchanged: that is, $g.x = x$ for any $x \in X_g$. Let's find some fixed point sets for rotations of the tetrahedron.

Exercise 23.2.31. Let G be the rotational symmetries of a tetrahedron

- (a) What is the fixed point set of r_{Bb} ?
- (b) What is the fixed point set of $r_{Bb} \circ r_{Dd}$? (*Hint*)
- (c) What is the fixed point set of $r_{Bb}^{-1} \circ r_{Dd}$?

- (d) Give all rotations that fix the set $\{D, d\}$.

◇

Let's consider the stabilizer subgroups for the faces and vertices of a tetrahedron.

Exercise 23.2.32. Find the following stabilizer subgroups: $G_A, G_B, G_C, G_D, G_a, G_b, G_c, G_d$. Which subgroups are equal? (**Hint**) ◇

Let's use the stabilizer subgroups above to determine the total number of rotational symmetries of a tetrahedron. So far we've found 4 rotational axes and two rotations around each axis. Together with the identity, this gives nine rotations. But there are more rotational symmetries of a tetrahedron than we've discovered so far. Let's try to find them.

Exercise 23.2.33.

- (a) Find the stabilizer subgroup for the edge \overline{CD} .
 (b) Find the stabilizer subgroup for the edge \overline{AB} .
 (c) How many different group elements (besides the identity) stabilize at least one edge?
 (d) Are there any group elements that are not stabilizers of either an edge or a face? Explain your answer.

◇

Exercise 23.2.34. The Orbit-Stabilizer Theorem gives us a formula for $|G|$ in terms of $|G_A|$ and $|\mathcal{O}_A|$. Alternatively, it also gives a formula for $|G|$ in terms of $|G_{\overline{AB}}|$ and $|\mathcal{O}_{\overline{AB}}|$. Show that both formulas give the same answer for $|G|$. ◇

Exercise 23.2.35. Complete the following table (similar to the table in Exercise 23.2.25) to characterize the group elements of the rotational symmetries of a tetrahedron according to the type(s) of sets they stabilize. We show two rows: fill in the blanks, and add as many rows as necessary to complete the table.

| Number of group elements | Order | Fixed point set |
|--------------------------|-------|-------------------------------|
| 1 | – | entire tetrahedron (identity) |
| – | 3 | vertex + face |

◇

Exercise 23.2.36. Recalling Exercise 23.2.26, we may suppose that there is a permutation group which resembles the symmetry group of the tetrahedron, in the same way that S_4 resembles the symmetry group of the cube. Identify a well-known symmetry group with 12 elements and make a table for this group which is arranged like the table in Exercise 23.2.26. What do you conjecture based on your results? ◇

The octahedron

Another regular polyhedron is the octahedron. We will see that in some ways an octahedron is like a cube. When opposite points are lined up on a vertical z axis, the octahedron has no vertical or horizontal faces, as shown in Figure 23.2.5. We denote a 90° counterclockwise rotation around the z axis by r_z (and similarly for rotations around the x , and y axes). Since each vertex of the octahedron lies on an axis, we can use the x , y , and z axis to label the vertices. For example y_+ is the vertex on the positive y axis. We can also name the edges using this notation for their endpoints. Let's use the axes to label the faces of the octahedron too. Consider Figure 23.2.5, we'll refer to the the face in the first octant as Δ_{+++} (the other faces will be labeled similarly).

Exercise 23.2.37.

- List all the faces of the octahedron using the notation above.
- Based on Figure 23.2.5 how many faces does an octahedron have? How many vertices? How many edges?

◇

A model of an octahedron might help with the following exercises. You can make one like the one in Figure 23.2.6. There's also a virtual octahedron on GeoGebra that you can manipulate at: <https://www.geogebra.org/m/KtTGGrSp>. A Youtube video that shows the rotational symmetries

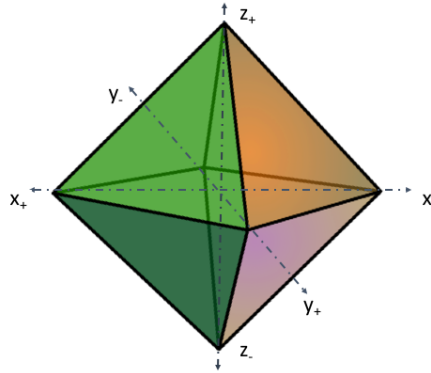


Figure 23.2.5. Octahedron with 3 axes of rotation that give symmetries (figure modified from <https://en.wikipedia.org/wiki/File:Octahedron.svg>)



Figure 23.2.6. A paper octahedron to print, cut and fold (from <http://www.korthalsaltes.com>).

of an octahedron may be found at: <https://www.youtube.com/watch?v=CCaX5eTteEg>.

Exercise 23.2.38. What is the order of r_z ?

◇

Exercise 23.2.39.

- (a) Give rotations that take Δ_{+++} to each of the other faces.
- (b) Give rotations that take x_- to each of the other vertices.
- (c) Give a rotation that takes edge $\overline{x_+y_+}$ to each of the other edges.

◇

Exercise 23.2.40. Consider the edge $\overline{x-y_+}$ of an octahedron. What is $\mathcal{O}_{\overline{x-y_+}}$? ◇

Exercise 23.2.41. Let G be the rotational symmetries of an octahedron

- (a) What is the fixed point set of $r_y \circ r_z$?
- (b) What is the fixed point set of $r_y^2 \circ r_x$?
- (c) What is the fixed point set of $r_x^2 \circ r_y$?

◇

Let's consider the stabilizer subgroups for the faces and vertices of an octahedron.

Exercise 23.2.42. Find the stabilizer subgroups for each of the vertices of the octahedron. ([*Hint*](#)) ◇

Let's find the total number of rotational symmetries for the octahedron.

Exercise 23.2.43. Let G be the rotational symmetries of an octahedron. Construct a formula for $|G|$ in terms of $|G_{y_+}|$ and $|\mathcal{O}_{y_+}|$ (see Example 23.2.18). ◇

So far we have discovered 10 rotational symmetries of an octahedron. Three axis of 3 rotations each plus the identity. By the previous exercise, there are still more to discover. Here we go!

Exercise 23.2.44.

- (a) Find the stabilizer subgroup for the edge $\overline{y_+ z_+}$.
- (b) Find the stabilizer subgroup for the edge $\overline{y_- z_-}$.
- (c) How many different group elements (besides the identity) stabilize at least one edge?

◇

Exercise 23.2.45.

- (a) Find the stabilizer subgroup for the face Δ_{+++} .
- (b) Find the stabilizer subgroup for the face Δ_{---} .
- (c) How many different group elements stabilize at least one face?

◇

Exercise 23.2.46. In Exercise 23.2.43 we constructed a formula for $|G|$ in terms of $|G_{y_+}|$ and $|\mathcal{O}_{y_+}|$. Do the same thing using $|G_{\Delta_{+++}}|$ and $|\mathcal{O}_{\Delta_{+++}}|$, and show that you get the same value for $|G|$. ◇

Exercise 23.2.47. Complete the following table to characterize the group elements of the rotational symmetries of an octahedron. We show two rows, how many more to complete the table?

| Number of group elements | Order | Fixed point set |
|--------------------------|-------|------------------------------|
| — | — | entire octahedron (identity) |
| — | — | opposite vertices |

◇

Exercise 23.2.48. There are some striking similarities between the tables in Exercises 23.2.47 and 23.2.25. Describe the similarities, and see if you can explain them. Figure 23.2.7 may give you some ideas. ◇

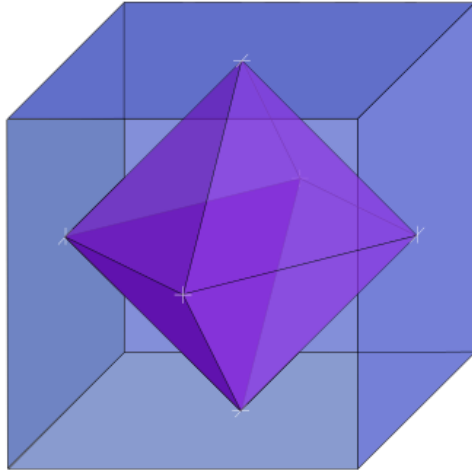


Figure 23.2.7. Figure for Exercise 23.2.48 (source: <https://en.wikipedia.org>)

The dodecahedron

Let's practice finding the elements of the rotation group of another regular polyhedron. Consider the regular dodecahedron in Figure 23.2.8. A dodecahedron has 12 faces and each face is a regular pentagon. How many edges does this polyhedron have and how many vertices? Well, since each of the twelve faces is a pentagon that seems to give $12 \cdot 5 = 60$ edges. But two faces meet at each edge, so we actually have $(12 \cdot 5)/2 = 30$ edges.

You can also make your own dodecahedron to help you explore its rotational symmetries. See Figure 23.2.9.

Exercise 23.2.49. Determine the number of vertices of a regular dodecahedron. \diamond

Let f_1 be one face of the dodecahedron. An axis through the center of f_1 also passes the opposite face which is parallel to f_1 . We'll call this opposite face f_1^* and denote a counterclockwise rotation of f_1 about this axis as r_{f_1} .

Exercise 23.2.50.

(a) What is the order of r_{f_1} ?

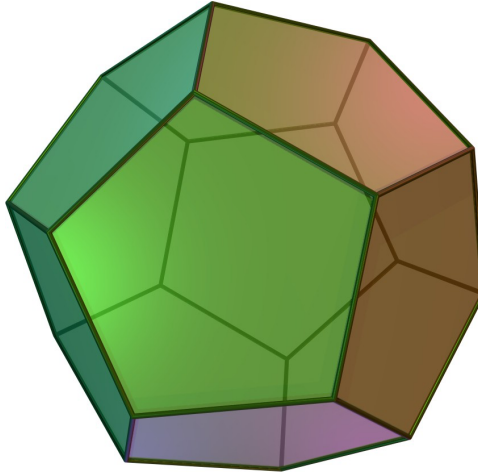


Figure 23.2.8. Dodecahedron (source:<https://en.wikipedia.org>)

- (b) Let G be the rotational symmetry group of a dodecahedron. List all rotations in the stabilizer subgroup G_{f_1} . What else do they stabilize?
- (c) What is $|G_{f_1}|$?
- (d) How many group elements in G stabilize at least 1 face?
- (e) What is $|\mathcal{O}_{f_1}|$?

◇

Now we can find the total number of rotational symmetries in G .

Exercise 23.2.51. Find $|G|$ in terms of $|G_{f_1}|$ and $|\mathcal{O}_{f_1}|$.

◇

So far we've found the number of the stabilizers of faces of the dodecahedron. But, as with the cube and tetrahedron, we need axes of symmetry through edges and vertices as well. Let v_1 be one vertex of the dodecahedron. An axis of symmetry through v_1 will also pass through the opposite vertex, which we will call v_1^* . A counterclockwise rotation about this axis is called r_{v_1} .

Exercise 23.2.52.

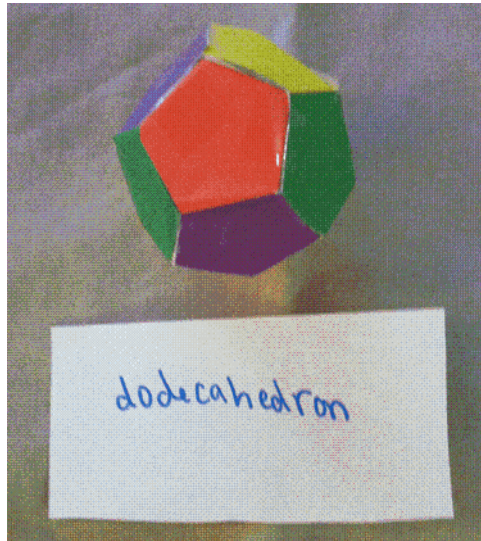


Figure 23.2.9. A dodecahedron to print, cut and fold (from <http://www.korthalsaltes.com>).

1. Find the order of r_{v_1} .
2. List all rotations in the stabilizer subgroup G_{v_1} . What else do they stabilize?
3. How many group elements in G (besides the identity) stabilize at least 1 vertex?
4. What is $|\mathcal{O}_{v_1}|$?
5. Find $|G|$ in terms of $|G_{v_1}|$ and $|\mathcal{O}_{v_1}|$.

◇

Let's consider the edges of the dodecahedron. We've seen already that there are 30 edges. Based on this information and previous exercises, complete the following.

Exercise 23.2.53.

- (a) Let e_1 be one edge of the dodecahedron. What is $|G_{e_1}|$?

- (b) Are the edges of a dodecahedron stabilized in pairs? Explain your answer. (**Hint**)

◇

Exercise 23.2.54.

- (a) How many group elements of G besides the identity stabilize at least 1 edge?
- (b) Complete the following table to characterize the group elements of the rotational symmetries of a dodecahedron. We show two rows, how many more to complete the table?

| Number of group elements | order | Fixed point set |
|--------------------------|-------|--------------------------------|
| – | – | entire dodecahedron (identity) |
| – | – | – |

◇

Exercise 23.2.55.

Identify a group of permutations with the same number of elements as the symmetry group of the dodecahedron. Make a table for this group which is arranged like the table in Exercise 23.2.26. What do you conjecture based on your results?

◇

Football (a.k.a. “soccer ball”)

All the polyhedra we’ve studied so far have congruent regular faces. These are also known as *Platonic solids*. Let’s explore the rotation group of a polyhedron whose faces are not all congruent. A familiar example is the football (following American usage, we’ll call it a “soccer ball”), as shown in Figure 23.2.10. The soccer ball has 32 faces, 12 regular pentagons and 20 hexagons.

Let’s try to count the rotations of a soccer ball that preserve symmetry. Axes can be placed through the center of pentagonal faces, which are stabilized in pairs.

Exercise 23.2.56.

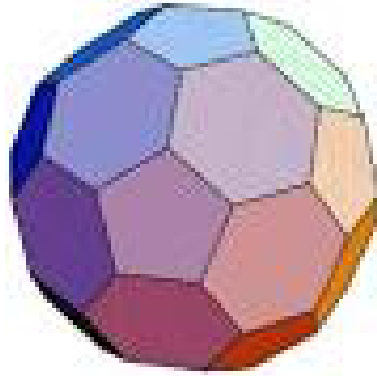


Figure 23.2.10. The soccer ball has both pentagonal and hexagonal faces. Source: <http://mathworld.wolfram.com/TruncatedIcosahedron.html>.

- (a) Given one particular pentagonal face of the soccer ball, what is the order of its stabilizer?
- (b) Given that there are 12 pentagonal faces, find $|G|$ where G is group of rotational symmetries of the soccer ball. (*Hint*)

◇

Axes can also be placed through the center of hexagonal faces. However, not all rotations about an axis through a hexagonal face will result in symmetry.

Exercise 23.2.57.

- (a) Given one particular hexagonal face of the soccer ball, what is the order of its stabilizer?
- (b) Using your answers to (a) and part (b) of Exercise 23.2.56, determine the number of hexagonal faces. (*Hint*)

◇

Axes of rotation also pass through *some* of the edges. Notice that there are two types of edges: those which join two hexagonal faces, and those which join a hexagonal face and a pentagonal face.

Exercise 23.2.58.

- (a) Consider an edge which joins a hexagonal face and a pentagonal face. How many rotations (besides the identity) stabilize this edge? *Explain* your answer.
- (b) Consider an edge which joins two hexagonal faces. How many rotations stabilize this edge? *Explain* your answer.
- (c) Using the counting formula and your answers to previous exercises, determine the number of edges which join two hexagons.
- (d) Note each pentagon touches 5 hexagons. Use this information and information from Exercise 23.2.56 to determine the number of edges which join a pentagon and hexagon.

◇

What about vertices?

Exercise 23.2.59.

- (a) Consider a particular vertex. How many rotations (besides the identity) stabilize this edge? *Explain* your answer.
- (b) Note each vertex touches one pentagon, and each pentagon has five vertices. Use this information and information from Exercise 23.2.56 to determine the number of vertices.

◇

Exercise 23.2.60.

- (a) Create a table similar to the table in Exercise 23.2.25 which characterizes the rotational symmetries of the soccer ball.
- (b) Does this table resemble one of the tables that we constructed previously for regular polyhedra? If so, which? Can you explain this?

◇

23.2.6 Euler's formula for regular polyhedra

In this section we'll play with counting the order of the rotation group G of a regular polyhedron in different ways. It turns out that this will lead us to an interesting and useful formula relating the number of edges, vertices, and faces in a polyhedron. Let's start by reviewing our previous examples and noticing a pattern.

Exercise 23.2.61.

- (a) Complete the table and compare $|G|$ to the number of edges of each polyhedron. The number of edges is equal to the order of the orbit of any edge e , denoted as $|\mathcal{O}_e|$.

| polyhedron | number of edges ($ \mathcal{O}_e $) | order of group ($ G $) |
|--------------|---------------------------------------|--------------------------|
| cube | 12 | 24 |
| tetrahedron | – | – |
| octahedron | – | – |
| dodecahedron | – | – |

- (b) Based on the table, guess an equation for $|G|$ in terms of \mathcal{O}_e .
- (c) Prove your equation using Proposition 23.2.21.

◇

Now in Exercises 23.2.25, 23.2.35, and 23.2.47 we showed another way of counting the elements of G : by counting the stabilizers of faces, vertices, and edges (plus the identity). But does this work for *every* polyhedron? Could there possibly be a rotational symmetry that doesn't stabilize *anything*? It turns out that this isn't possible (at least in three dimensions). The argument (which depends on a key fact proved by the famous mathematician Leonhard Euler) goes as follows.

Euler proved in 1775 that any rotation in three dimensions has a unique fixed axis. (We won't give the proof here, but it's related to the cross product discussed in Section 11.8.1.) Now if we rotate a polyhedron, then the axis must intersect the polyhedron twice: that is, it must intersect two elements of X where $X = \{\text{faces, vertices, edges}\}$. Let's call these two elements ϵ_1 and ϵ_2 . Since the rotation leaves the two intersections unchanged, there's one point of ϵ_1 which maps to itself (and similarly for ϵ_2). If the rotation is a symmetry, then ϵ_1 must be fixed by the rotation, because there's no

way it couldn't map to a different element of X and still have one point which remains in ϵ_1 . The same argument holds for ϵ_2 . This shows that any rotational symmetry must stabilize at least two elements of X .

We can take the argument even further. The rotational symmetry which stabilizes ϵ_1 and ϵ_2 can't possibly stabilize any other elements of X : this is because the center point of any stabilized element (be it face, vertex, or edge) is unchanged by a rotational symmetry, and Euler tells us that there is only one fixed axis and hence exactly two fixed points.

So since every rotational symmetry (besides the identity) stabilizes *exactly* two elements, then if we sum up all of the (non-identity) stabilizers for all elements of X then we will count each (non-identity) symmetry exactly twice. It follows that

$$2(|G| - 1) = \sum_{x \in X} (|G_x| - 1)$$

(note that we use $|G| - 1$ and $|G_x| - 1$ because we're not counting the identity symmetry).

Let's apply this formula to a regular polyhedron with $|\mathcal{O}_f|$ faces, $|\mathcal{O}_v|$ vertices and $|\mathcal{O}_e|$ edges. Applying Proposition 23.2.21 to faces, edges, and vertices gives:

$$|G_f| = \frac{|G|}{|\mathcal{O}_f|}; \quad |G_e| = \frac{|G|}{|\mathcal{O}_e|}; \quad |G_v| = \frac{|G|}{|\mathcal{O}_v|}.$$

Now for the sum. Since there are \mathcal{O}_f faces, \mathcal{O}_e edges, and \mathcal{O}_v vertices we have:

$$\begin{aligned} 2(|G| - 1) &= \sum_{x \in X} (|G_x| - 1) \\ &= \sum_{\text{faces}} (|G_f| - 1) + \sum_{\text{edges}} (|G_e| - 1) + \sum_{\text{vertices}} (|G_v| - 1) \\ &= |\mathcal{O}_f| \left(\frac{|G|}{|\mathcal{O}_f|} - 1 \right) + |\mathcal{O}_e| \left(\frac{|G|}{|\mathcal{O}_e|} - 1 \right) + |\mathcal{O}_v| \left(\frac{|G|}{|\mathcal{O}_v|} - 1 \right) \\ &= 3|G| - |\mathcal{O}_f| - |\mathcal{O}_e| - |\mathcal{O}_v|. \end{aligned}$$

Rearranging, we find:

$$|\mathcal{O}_f| + |\mathcal{O}_v| + |\mathcal{O}_e| = |G| + 2.$$

But we've also seen that $|G| = 2\mathcal{O}_e$ for regular polyhedra. Substituting and rearranging a little further gives:

$$|\mathcal{O}_f| + |\mathcal{O}_v| - |\mathcal{O}_e| = 2.$$

This powerful equation is called ***Euler's formula***. Let's see how it can be useful in determining properties of regular polyhedra.

Exercise 23.2.62. A certain regular polyhedron has 20 triangular faces.

- (a) Using Proposition 23.2.21, find the number of edges.
- (b) Using Euler's formula, find the number of vertices.
- (c) Using Proposition 23.2.21, find the number of edges which meet at each vertex.

◇

Exercise 23.2.63.

- (a) Verify Euler's formula for the cube and tetrahedron.
- (b) Explain why the proof we have given does not apply to the soccer ball. Verify that notwithstanding, Euler's formula still works for the soccer ball anyway!

◇

Remark 23.2.64. Euler's formula has far more general application than we've shown here. It works for any network of edges and vertices which can be drawn on a sphere. Variants of the formula work for networks drawn on other shapes (like a donut, or a donut with multiple holes). Pursuing this topic further would lead us into the area of mathematics known as ***algebraic topology***, which is a fascinating topic but unfortunately a much bigger mouthful than we can swallow at this point. △

We don't need to limit ourselves to Euler's formula. There are lots of other fun facts we can prove:

Exercise 23.2.65.

- (a) Modify the proof of Euler's formula to prove the following formula for the soccer ball:

$$2 = |\text{faces}| + |\text{edges}| + |\text{vertices}| - X \cdot |G|,$$

where $|G|$ is the order of the symmetry group of the soccer ball. Find the value of X .

- (b) Prove that the following formula is true for *any* network of edges and vertices which can be drawn on a sphere:

$$|\text{faces}| + |\text{edges}| + |\text{vertices}| - 2 \equiv 0 \pmod{|G|},$$

where $|G|$ is the order of the rotational symmetry group of the network.

◇

Exercise 23.2.66. Let X be a polyhedron consisting of faces, edges and vertices. The symmetry group of X is G . X is not a regular polyhedron—the vertices and edges are not all identical. This is what we know about X :

- There are two types of vertices, and two types of edges.
 - Type I vertices are all G -equivalent; and every Type I vertex has 5 edges which are all G -equivalent. (This implies that the stabilizer subgroup of any Type I vertex has order 5.)
 - Type II vertices are all G -equivalent.
 - Type I edges are all G -equivalent; and the 180-degree rotation about the axis through the origin and the center of any Type I edge is a symmetry. (In other words, the stabilizer subgroup of any Type I edge has order 2.)
 - Type II edges are all G -equivalent; and Type II edges are not fixed by any symmetries.
 - All faces are triangles, and all are G -equivalent.
- (a) Use the Orbit-Stabilizer Theorem (Proposition 23.2.21) to express the number of Type I vertices, Type I edges, and Type II edges in terms of $|G|$.

- (b) Prove that $|G|$ is divisible by 10.
- (c) Since every edge is shared by two faces, it follows that:
- $$2 \cdot (\text{number of edges}) = (\text{number of faces})(\text{number of edges per face}).$$
- Use this fact to express the number of faces in terms of $|G|$.
- (d) Compute the order of the stabilizer subgroup of any face in X .
- (e) Use Euler's formula to express the number of Type II vertices in terms of $|G|$.
- (f) Using the Counting Formula applied to Type II vertices, show that the order of the stabilizer subgroup of any Type II vertex is 3 or less. Then show that order 1 and order 2 are both impossible, so that the order must be 3.
- (g) Using Euler's formula, compute $|G|$. Give explicitly the number of vertices and edges of each type, and the number of faces.
- (h) Look up on the web, and see if you can identify this polyhedron (this is an example of an *Archimedean solid*).

◇

23.2.7 Are there other regular polyhedra?

We have investigated four regular polyhedra: cube, tetrahedron, octahedron, and dodecahedron. Could there be any others? What does group theory tell us?

Exercise 23.2.67. Let us suppose we have a regular polyhedron with n_f faces, n_e edges, and n_v vertices. Let us further suppose that each face has f edges per face and v edges which meet at each vertex. (Note in particular that $v \geq 3$, because 2 parallel edges which join together form a single edge and not a vertex.) Let G be the group of rotational symmetries.

- (a) Use the Counting Formula to obtain three different equations for $|G|$ in terms of n_f, n_e, n_v, f , and v .

- (b) Use part (a) and Euler's formula to find an equation that relates f, v , and $|G|$ (that is, these are the only 3 variables in the equation).
- (c) Suppose that $f = 3$. Find the possible values of v . For each value of v , find the corresponding values of $|G|, n_f, n_e$, and n_v .
- (d) Suppose that $f = 4$. Find the possible values of v . For each value of v , find the corresponding values of $|G|, n_f, n_e$, and n_v .
- (e) Suppose that $f = 5$. Find the possible values of v . For each value of v , find the corresponding values of $|G|, n_f, n_e$, and n_v .
- (f) Suppose that $f \geq 6$. Show that this would imply $v < 3$, which is impossible.
- (g) Besides the four polyhedra we have investigated, could there be any others? If so, what are their properties?

◇

Take a moment to appreciate how amazing these results are. Since polyhedra are geometrical objects, one would think that one would have to consider geometrical facts about angles and how they fit together in order to determine which ones are possible. In particular, we know from geometry that a regular polyhedron couldn't have more than 6 regular polygons meeting at an edge, because then we'd have more than 360 degrees. Geometry also tells us that polyhedral faces couldn't have more than 6 sides, since then we couldn't have more than 2 meeting at a vertex. But we have figured out which regular polyhedra can exist, purely on the basis of algebra with no considerations of angles whatsoever!

The other wonderfully mysterious fact is that all of the regular polyhedra that we have determined to be possible do actually exist. It seems that our simple algebraic representations have captured some deep properties of the three-dimensional world that we live in.

23.2.8 Reflection symmetries of polyhedra

We have never shown that the rotational symmetries are the *only* symmetries of the regular solids. In fact, there are others! Recall that in the dihedral group, besides rotations there were reflections. Consider for example the hexagon: it had 6 rotations (including the identity) and 6 reflections. It's

possible to rotate the hexagon and keep the hexagon in the same plane. However, to reflect the hexagon, you have to “flip” it, which requires three dimensions. It turns out that something similar is true for the regular solids. There are also reflection symmetries for the regular solids: in fact, there are as many reflections as rotations, just as in the dihedral group. Also like the dihedral group, to reflect a solid requires one extra dimension. It is rather mind-blowing to think that if we lived in a world with four physical dimensions, it would be possible to turn your right hand into your left hand just by “flipping” in the fourth dimension!

23.2.9 Finite subgroups of the group of rotations in 3 dimensions

The set of all possible rotations in 3 dimensions forms a group, which is called the *special orthogonal group* and is denoted by the symbol SO_3 . (SO_3 is actually the intersection of the “orthogonal group” O_3 with the special linear group in three dimensions, which is why it’s called “special”.) All of the rotational symmetry groups of regular polyhedra which we’ve been considering are finite subgroups of SO_3 .

In Chapter 13 we encountered another class of finite subgroups of SO_3 , namely the dihedral groups D_n which consist of rotations and flips (we should be careful to include D_2 , which is generated by a single 180-degree rotation and a flip). Although a flip is not a 2-d rotation, it is a rotation in 3-dimensions (as we indicated in Section 23.2.8). Naturally, the rotation groups for the different n -gons (which are subgroups of the D_n form another class of finite subgroups of SO_3 .

Are there any other finite subgroups of SO_3 . The answer is *no*. For a proof, the reader may consult “Classifying Finite Subgroups of SO_3 ” by Hannah Mark, which (as of April 1 2020) can be found at: homepages.math.uic.edu/~kauffman/FiniteRot.pdf (if the link doesn’t work, you may try a Google search).

Once again, note the amazing power of mathematics. Mathematics tells reality what it can and cannot do. Mathematics commands the universe, and the universe must obey.

23.3 Group actions associated with subgroups and cosets

It turns out that if the set X is also a group, then it's always possible to define a group action of X on itself, where the group action is identical to the group operation: $g.x := gx$.

Example 23.3.1. Consider the group \mathbb{Z}_5 which as we know is a group under addition. We will show that \mathbb{Z}_5 is a \mathbb{Z}_5 -set where the group action is $g.x := g + x$. To do this we must show the identity and compatibility conditions. First, $0.x = 0 + x = x$ for all $x \in \mathbb{Z}_5$, so the identity condition is met. Secondly, we need to show compatibility: by the associative property of addition in \mathbb{Z}_5 , we have $(g_1 + g_2).x = (g_1 + g_2) + x = g_1 + (g_2 + x) = g_1.(g_2.x)$ for all $x, g_1, g_2 \in \mathbb{Z}_5$. So the compatibility condition is met. Therefore, by definition of G -set, \mathbb{Z}_5 is a \mathbb{Z}_5 -set. \blacklozenge

Exercise 23.3.2.

- Recall \mathbb{Q}^* is the nonzero rational numbers under multiplication. Show that \mathbb{Q}^* is a \mathbb{Q}^* -set.
- Recall H_5 is the complex 5th roots of unity under complex multiplication (see Section 4.4.1). Show that H_5 is an H_5 -set.
- Let T be the unit circle in the complex numbers under multiplication (see Figure 4.4.1 in Section 4.4.1). Find a group G such that T is a G -set, and prove the statement.

\diamond

We can generalize the results of the preceding exercise in the following proposition:

Proposition 23.3.3. For any group G , G is a G -set with action equal to the group operation in G : $g.h := gh$ for any $g, h \in G$.

Exercise 23.3.4.: Prove the above proposition. \diamond

Exercise 23.3.5.

23.3 GROUP ACTIONS ASSOCIATED WITH SUBGROUPS AND COSETS 831

- (a) Let $G = \{2^n \mid n \in \mathbb{Z}\}$: G is a multiplicative subgroup of \mathbb{Q}^* . Show that \mathbb{Q}^* is a G -set.
- (b) Let T be the unit circle in the complex numbers under multiplication. Show T is an H_5 -set.

◇

In Exercises 23.1.12 and 23.3.5, we've seen cases where G is a group and H is a subgroup of G . In this situation, H will always produce a group action on G :

Proposition 23.3.6. If G is a group, and H is a subgroup of G , then G is an H -set using the definition $h.g := hg$.

Exercise 23.3.7. Prove the above proposition.

◇

Recall our discussion of cosets in Chapter 18. In particular, a left coset consists of a group element g acting on a subgroup H of G . The group element acts on each element of the subgroup to create a coset. In other words, a coset is a subgroup shifted by action of a group element. If G is a group, we can let L be the set of left cosets. We will see in the following examples that we can define a group action on L . That is the set of left cosets, L is a G -set. Let G be the additive group of real numbers. That is, $G = (\mathbb{R}, +)$, and let H be all integer multiples of 2π . That is, $H = \{2k\pi : k \in \mathbb{Z}\}$, or $H = 2\pi\mathbb{Z}$ for short.

Exercise 23.3.8. Prove that $2\pi\mathbb{Z}$ is a subgroup of $(\mathbb{R}, +)$.

◇

Example 23.3.9. Let L be the set of left cosets of $2\pi\mathbb{Z}$ in the group $(\mathbb{R}, +)$. Recall from Definition 18.1.4 in Chapter 18 that the set of left cosets L is defined as $x + 2\pi\mathbb{Z} = \{x + h : h \in 2\pi\mathbb{Z}\}$. For example, the left coset which contains $\pi/3$ is the set $\{\pi/3 + 2k\pi, k \in \mathbb{Z}\}$, which we could also write as $\{\dots \pi/3 - 4\pi, \pi/3 - 2\pi, \pi/3, \pi/3 + 2\pi, \pi/3 + 4\pi, \dots\}$. It turns out that L is G -set under the action $(g, x + 2\pi\mathbb{Z}) \rightarrow g + x + 2\pi\mathbb{Z}$. Let's verify the two conditions of a G -set:

- (a) For the identity condition note that $e \in G = 0$. Then, $0 + x + 2\pi\mathbb{Z} = x + 2\pi\mathbb{Z}$ for any $x + 2\pi\mathbb{Z} \in L$. So the identity condition is true.

- (b) For the compatibility condition consider two real numbers a, b . Then, by associativity of real number addition, $(a+b)+x+2\pi\mathbb{Z} = a+(b+x+2\pi\mathbb{Z})$ for any $x+2\pi\mathbb{Z}$ in L . So the compatibility condition is true. L is a G -set of the additive group of real numbers.

This example has a very practical significance. We know that angles on a unit circle are arbitrary up to multiples of 2π . So we can think of each angle as a coset: that is, the angle θ where $0 \leq \theta < 2\pi$ corresponds to the coset $\theta + 2\pi\mathbb{Z}$, which represents the set of values $\{\theta + 2k\pi\}$, where $k \in \mathbb{Z}$. Now consider what an arbitrary rotation ϕ does to the angle θ . For instance, consider the case where $\theta = \frac{\pi}{4}$ – then $\theta + H = \{\frac{\pi}{4} + 2k\pi\}$. We'll suppose that the rotation angle is $\phi = \frac{15\pi}{2}$. According to the group action, $\phi + \theta + H = \frac{15\pi}{2} + \{\frac{\pi}{4} + 2k\pi\}$ which will result in the new coset $\{\frac{31\pi}{4} + 2k\pi\} = \{\frac{7\pi}{4} + 2k\pi\}$. As we can see, the action of the additive group $(\mathbb{R}, +)$ on the cosets $\theta + 2\pi\mathbb{Z}$ corresponds to rotation by arbitrary angles around the unit circle. If the rotation is more than 2π , the action still works because the cosets take care of any extra factors of 2π . \blacklozenge

In the following exercise you will generalize the above example by showing how the set of all left cosets from a particular subgroup of group G is a G -set.

Exercise 23.3.10. Let G be a group and H be a subgroup of G . Let $L = \{xH \mid x \in G\}$ which is the set of all left cosets of H in G . Then G acts on L by $g.xH = (gx)H$, which is also a coset of H . Show that G is acting on L , which means that L is a G -set. \diamond

23.3.1 The integer lattice

In this section we'll take a close look at a group action on a set of cosets. This example can be thought of as a two-dimensional version of Example 23.3.9, and can be envisioned using computer graphics.

Let G be the xy -plane under addition (that is, $G = (\mathbb{R}^2, +)$). Let $H = \mathbb{Z} \times \mathbb{Z}$, which is a subgroup of G (H is called the *integer lattice*: see Figure 23.3.1). Cosets of H in G may be written as $a + H = \{(x + m, y + n) : m, n \in \mathbb{Z}\}$, where $a := (x, y)$ can be any element of G . Recall from Proposition 18.2.4 that cosets form a partition, so H and its cosets partition \mathbb{R}^2 .

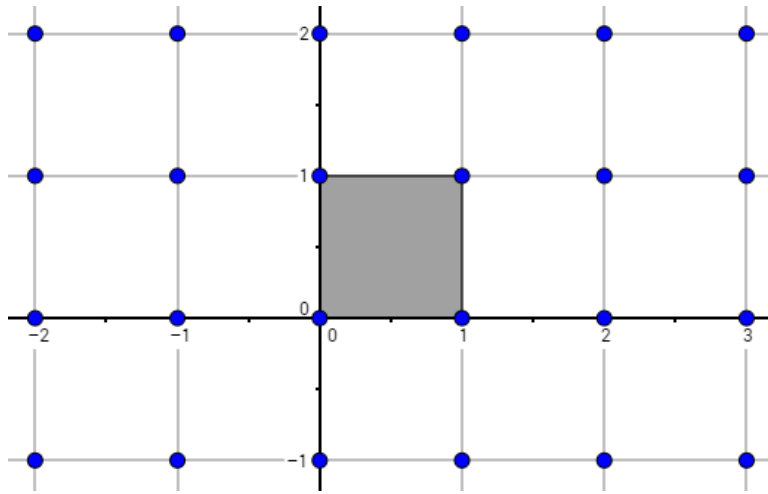


Figure 23.3.1. Diagram showing H (the integer lattice) with the unit square shaded. This figure and the similar figures in the section were created using the software “GeoGebra” (see <http://www.geogebra.org>).

The *unit square* (the shaded area in Figure 23.3.1) is the area on the xy -plane that is $[0, 1) \times [0, 1)$, meaning the square includes the points on the x and y axes, but not on the lines $x = 1$ and $y = 1$. Note that H has only one point in the unit square, namely $(0, 0)$, similarly any coset of the form $a + H$ has only one point in the unit square (we will prove this mathematically later). We can say that $a \in \mathbb{R}^2$ maps H to produce a coset $a + H$.

Example 23.3.11. Consider a particular group element $a = (0.7, 0.5)$. Let’s use a graphical illustration to model the point a mapping the integer lattice H which results in the coset $a + H$.

You can duplicate the above illustration by physically by drawing the coset points (red diamonds) on a plastic transparency, placing it over a graph of the integer lattice (blue points) and moving the transparency 0.7 units to the right and 0.5 units upwards. ♦

We will be needing to use the *floor function*, also known as the greatest integer function. The floor function takes a real number, $x \in \mathbb{R}$ as input and outputs the greatest integer that is less than or equal to x . We will use these brackets, $\lfloor \]$, to represent the floor function. Mathematically we can

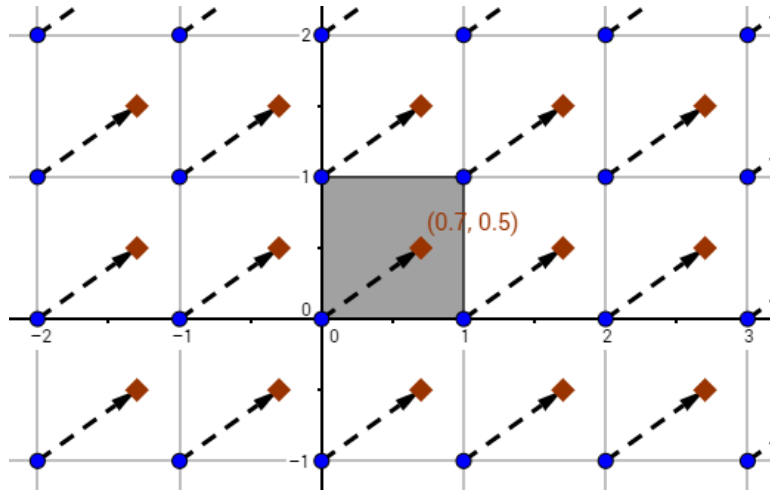


Figure 23.3.2. The integer lattice, H , is represented by blue points, while the elements of the coset $(0.7, 0.5) + H$ are represented by red diamonds. The dotted black arrows show the creation of the coset.

express this as:

$$\lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\}.$$

Here are just a few quick examples: $\lfloor 4 \rfloor = 4$, $\lfloor \pi \rfloor = 3$, and $\lfloor -2.3 \rfloor = -3$.

Exercise 23.3.12. In the following you will show that there is a bijection between cosets of the form $a + H$, where $a \in \mathbb{R}^2$ and points of the unit square.

- Let (m, n) be the lower left point of the lattice square which contains the point a . Using the floor function, give expressions for m and n .
- Show that $a + (-m, -n)$ is inside the unit square. This implies that $a + H$ contains at least one point inside the unit square.
- Use proof by contradiction to show that the coset $a + H$ cannot have two different points inside the unit square.

Since each coset $a + H$ contains exactly one point in the unit square, and each point in the unit square is contained in exactly one coset $a + H$, it follows

that there exists a one-to-one and onto correspondence (i.e. a bijection) between points in the unit square and cosets of H . \diamond

Example 23.3.13. Continuing from Example 23.3.11: let $b = (0.8, 0.3)$, where $b \in G$. Find the point $h = (m, n) \in H$ such that $b + a + h$ is inside the unit square (recall $a = (0.7, 0.5)$).

The element b acts on the coset $a + H$ as follows:

$$\begin{aligned} b + a + H &= \{(0.8 + (0.7 + m), 0.3 + (0.5 + n)) : m, n \in \mathbb{Z}\} \\ &= \{(0.8 + 0.7 + m, 0.3 + 0.5 + n) : m, n \in \mathbb{Z}\} \\ &= \{(1.5 + m, 0.8 + n) : m, n \in \mathbb{Z}\}. \end{aligned}$$

If $m = -1$ and $n = 0$, then $b + a + h = (1.5 - 1, 0.8 + 0) = (0.5, 0.8)$, so $h = (-1, 0)$. \blacklozenge

Exercise 23.3.14. Generalize the above example as follows. Let $a, b \in \mathbb{R}^2$ such that $a = (a_x, a_y)$ and $b = (b_x, b_y)$. Let $h = (m, n)$ where $m = -\lfloor b_x + a_x \rfloor$ and $n = -\lfloor b_y + a_y \rfloor$ (note that $h \in H$). Verify graphically the formulas for m and n , and show algebraically that $b + a + h$ is in the unit square. \diamond

The point $b + a + h = (0.5, 0.8)$ is the *only* point of the coset $b + a + H$ which is inside the unit square. By basic properties of cosets, it follows that $b + a + H = (0.5, 0.8) + H$. Recall that by definition a left coset of the integer lattice $a + H$ means adding the same point, $a = (x, y)$, to each point in the integer lattice, H . A group action simply changes one coset of H in G to a different coset. The top illustration in Figure 23.3.3 show the displacement of the coset $a + H$ when acted on by b on the left from Example 23.3.13.

Our above discussion can help us describe the motion of a character on the screen of a “wraparound” video game. Imagine the unit square is your TV or computer screen. Suppose the character starts near the right edge at the point $a = (0.7, 0.5)$, and undergoes linear motion to the right and up in the direction of the displacement vector $b = (0.8, 0.3)$. Then he moves off the right edge of the screen and re-appears instantly at the left edge, ending up at the previously found point $c = (0.5, 0.8)$ as shown in Figure 23.3.4. So the point $b + a + h = c$ where $h = (-1, 0)$.

In our conclusion of Exercise 23.3.12, we found that there’s a bijection between the points of the unit square and the cosets of H . So instead of observing an entire coset, we only need to look at the point that is currently

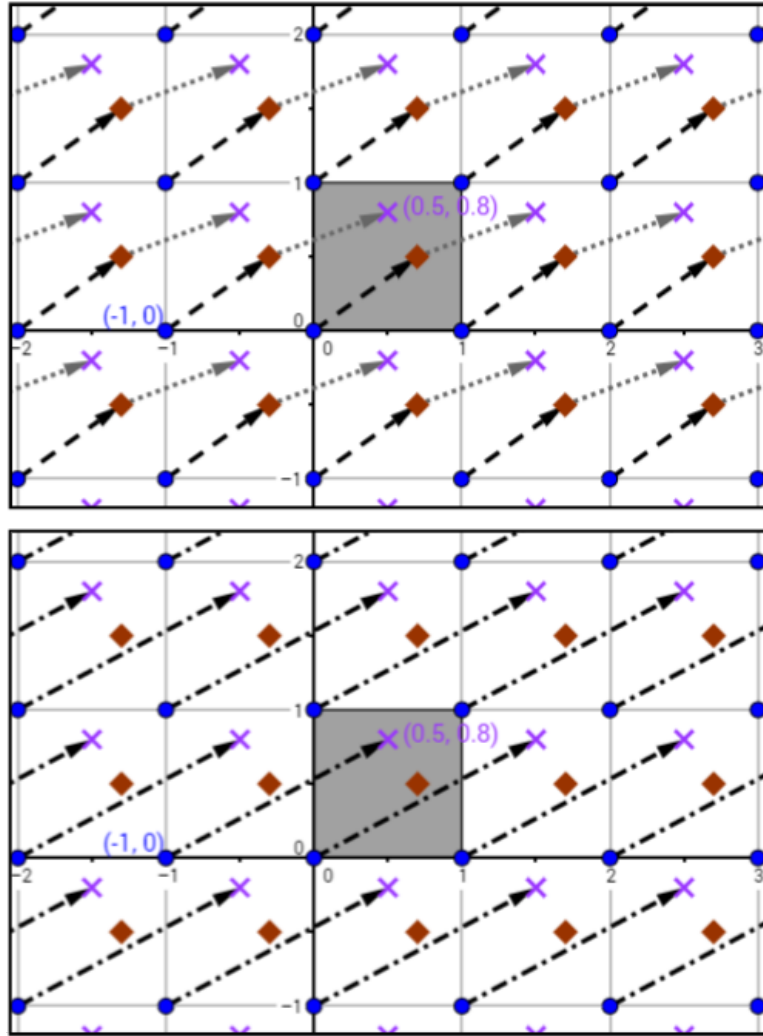


Figure 23.3.3. From Example 23.3.13, the top figure is illustrating the displacement of the coset $a + H$ for $a = (0.7, 0.5)$ when acted on by $b = (0.8, 0.3)$ on the left. The bottom figure is illustrating the coset $c' + H$, where $c' = b + a$. The lattice, H is represented by blue points, the elements of the coset $a + H$ are represented by red diamonds, and the elements of the final coset $b + a + H = c' + H$ are represented by purple crosses.

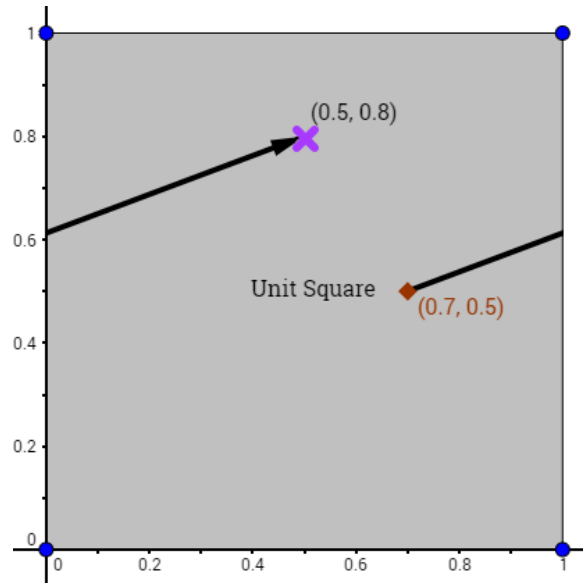


Figure 23.3.4. Demonstrating the “wraparound” effect, when only viewing the unit square, when $b = (0.8, 0.3)$ acts on the coset $a + H$ where $a = (0.7, 0.5)$.

inside the unit square, as seen in Figure 23.3.4 for example. What appears to be a jumpy motion in the unit square (i.e. when the point jumps from the right edge to the left edge) can also be understood in terms of a continuous “motion” of cosets.

Example 23.3.15. Consider group elements $a = (-0.6, -0.4)$ and $b = (0.9, 1.6)$ where $a, b \in \mathbb{R}^2$. Let’s first find the point $h = (m, n) \in H$ such that $b + a + H$ is inside the unit square. From Exercise 23.3.14, $m = -[-0.6 + 0.9] = -[0.3] = 0$ and $n = -[-0.4 + 1.6] = -[1.2] = -1$, so $h = (0, -1)$

Next, let’s find the point $b + a + h$ in the unit square, let’s call this point c .

$$c = (0.9, 1.6) + (-0.6, -0.4) + (0, -1) = (0.3, 0.2)$$

So $c = (0.3, 0.2)$ and is a point inside the unit square.

Lastly, let’s graph the “movement” of the points that are visible to only the unit square throughout the group action b on $a + H$. Similar to Figure 23.3.4.

The Figure 23.3.5 (top) we have shown “paths” which follow the action of b on $a + H$. Note that each path is a continuous straight segment. However, if we restrict our field of view to the unit square (see Figure 23.3.5 (bottom)), there appears to be four disconnected segments, but the top figure shows us how these can be envisioned as a continuous motion.



Exercise 23.3.16.

- (a) Given $a = (0.8, 0.6)$ and $b = (1.4, 0)$ find the point $h \in H$ such that $b + a + h$ is inside the unit square, and find c in the unit square, such that $c + H = b + a + H$.
- (b) Given $a = (0.8, 0.6)$ and $b = (1.2, 1.3)$ find the point $h \in H$ such that $b + a + h$ is an element of the unit square, and find c in the unit square, such that $c + H = b + a + H$.
- (c) Given $a = (0.8, 0.6)$ and $b = (0, 3.5)$ find the point $h \in H$ such that $b + a + h$ is inside the unit square, and find c in the unit square, such that $c + H = b + a + H$.
- (d) Illustrate the first part (a) with a graph. Graph the point $a + h$. Then graph the point $b + a + h$, or simply c . Include ordered pairs to indicate the position of these points. Include arrows to indicate the apparent “movement” from the point $a + h$ to the point c within the unit square.
- (e) Create similar graphs illustrating parts (b) and (c).



Exercise 23.3.17. Show that H is *not* an \mathbb{R}^2 -set. (*Hint*)



Exercise 23.3.18. Show that the set of all cosets of the form $\{a + H, a \in \mathbb{R}^2\}$ is a \mathbb{R}^2 -set by answering the following:

- (a) Let $b \in \mathbb{R}^2$. Define the action of b on $(a + H)$ (in other words complete the following equation: $b.(a + H) = ?$).
- (b) Prove the identity condition.

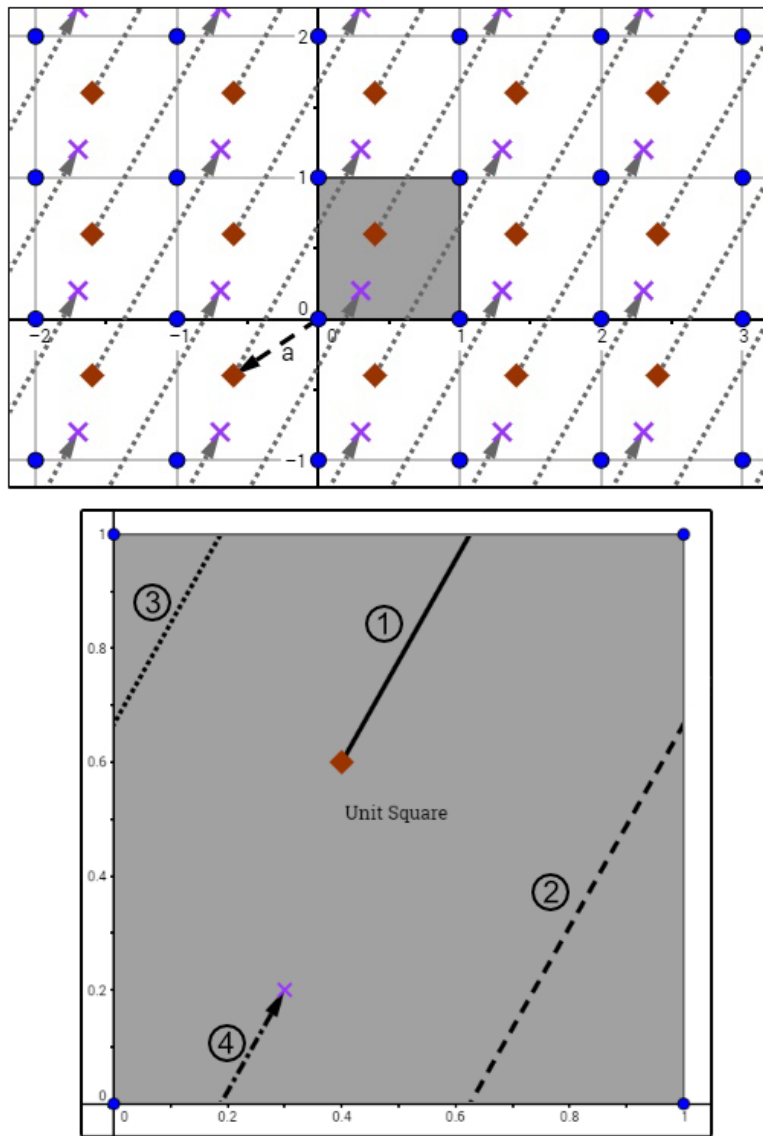


Figure 23.3.5. The top figure is illustrating the movement of the coset $a + H$ for $a = (-0.6, -0.4)$ when acted on by $b = (0.9, 1.6)$ on the left (only one arrow, labeled a , representing the movement of a acting on H is shown so the image wouldn't be cluttered). The bottom figure is illustrating the “wraparound” effect when only viewing the unit square. The movements are numbered in order and there are different patterns for clarity.

(c) Prove the compatibility condition.

◇

We can think about this example in another way. Suppose we have a *torus*, which is the mathematical word for a donut shape. We could imagine creating a “map” of the surface of the torus by cutting the torus apart as shown in Figure 23.3.6. If we spread this map out flat, it would look like a square (see Figure 23.3.7). If we wanted to use the map to chart motion on the surface of the torus, then any motion that goes off the right edge would reappear at the left edge; and any motion that goes off the top edge would reappear at the bottom. So you see this is exactly what we saw for the previous example. So using cosets of \mathbb{Z}^2 in \mathbb{R}^2 , we’ve created a mathematical representation for motion on the surface of a torus.

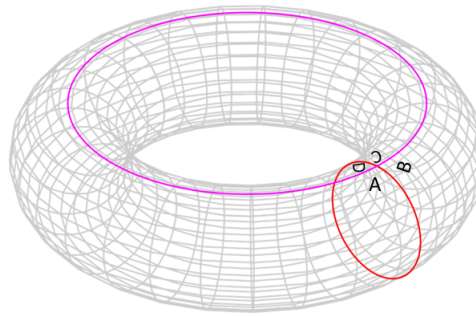


Figure 23.3.6. Torus, showing two cut lines.

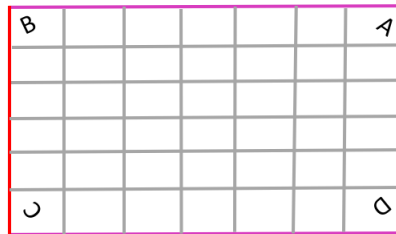


Figure 23.3.7. The cut torus, flattened out.

We can generalize the two previous examples by considering cosets of a subgroup H in a group G that contains H .

Example 23.3.19. Let H be a subgroup of G and L_H the set of left cosets of H . The set L_H is a G -set under the action $g.(xH) = (gx)H$ (note that $gx \in G$ so $(gx)H$ is a coset of H). Again, it is easy to see that the identity condition is true. Since $(gg').(xH) = (gg'x)H = g.((g'x)H) = g.(g'.(xH))$, the compatibility condition is also true. \blacklozenge

So far, we've been looking at group actions on left cosets. What about right cosets? Let's investigate.

Exercise 23.3.20. Consider the case where $G = S_3$, $H = \{\text{id}, (12)\}$, and R is the set of right cosets of H . Define a function from $G \times R \rightarrow R$ by $(g, R) \rightarrow Rg$. Does this function define a group action of G on R ? (*Hint*) \diamond

The previous exercise shows that we can't always do the same thing with right cosets that we can do with left cosets. Let's look at an alternative:

Exercise 23.3.21.

- (a) Repeat the previous exercise, but this time use the function $(g, R) \rightarrow Rg^{-1}$.
- (b) Show that in general the function $(g, R) \rightarrow Rg^{-1}$ defines an action of G on the right cosets of H .

\diamond

23.4 Conjugation

23.4.1 Commutative diagrams and the definition of conjugation

When we talked about permutations, we saw that the objects we were permuting didn't really change the situation. For example, we saw that permuting $\{1, 2, 3, 4\}$ was the "same thing" as permuting $\{A, B, C, D\}$. Now what do we really mean by the "same thing"? Well for example, if we take any

permutation of $\{1, 2, 3, 4\}$ and replace 1 with A , 2 with B and so on, then we'll get a permutation of $\{A, B, C, D\}$. To be specific let's take $\sigma = (123)$ and $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ A & B & C & D \end{pmatrix}$. It's possible to represent this situation with diagram in Figure 23.4.1. This type of diagram is called a **commutative diagram**.

The commutative diagram illustrates the construction of a conjugation. We can begin in the upper right corner and move to the upper left, in the opposite direction of the f arrow. This motion corresponds to applying the inverse of f , that is f^{-1} (this naturally requires that f must be a *bijection*). Then, moving from upper left to lower left represents applying the permutation $\sigma = (123)$, as shown in the diagram. Finally, by moving from lower left to lower right (which corresponds to applying the function f), we end up at the lower right-hand corner. The three motions, performed one after the other thus corresponds to the composition of functions f^{-1} , then σ , then f , which we write as $f\sigma f^{-1}$ (recall that function composition proceeds from right to left).

On the other hand, moving directly from upper right to lower right corresponds to the application of the permutation μ . Since this motion starts at upper right and ends at lower right just like the previous one, it should represent the same permutation as before. This gives us the result: $\mu = f\sigma f^{-1}$.

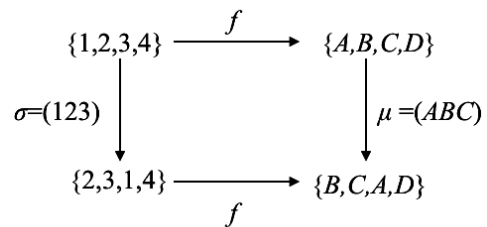


Figure 23.4.1. Commutative diagram of a conjugate mapping.

We may also think of this another way. The paths $f\sigma$ and μf both take us from upper left to lower right. So we can write $f\sigma = \mu f$. By right multiplying by f^{-1} we discover the algebraic structure of the conjugate of σ , $f\sigma f^{-1} = \mu$.

There's a shortcut way to obtain μ . Actually, μ is simply σ relabeled according to f . That is, if we take the cycle representation of σ and replace the numbers according to f ($1 \rightarrow A, 2 \rightarrow B, 3 \rightarrow C$), then we end up with μ . We will call this shortcut, "the relabeling method".

Exercise 23.4.1. For each σ and f , complete a commutative diagram like the one in Figure 23.4.1. Find the conjugate mapping using the relabeling method, and verify that the result agrees with $f \circ \sigma \circ f^{-1}$.

$$(a) \sigma = (12)(35) \text{ and } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ A & B & C & D & E \end{pmatrix}$$

$$(b) \sigma = (2346) \text{ and } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ A & B & C & D & E & F \end{pmatrix}$$

$$(c) \sigma = (147)(2563) \text{ and } f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ A & B & C & D & E & F & G \end{pmatrix}$$

◇

Now instead of f going between different sets, we can choose f to map $\{1, 2, 3, 4\}$ to itself. In this case, f itself is a permutation. To be more consistent with our earlier notation for permutations, we'll use the symbol τ instead of f in the following discussion. What τ corresponds to is just relabeling the objects that we're permuting. Figure 23.4.2 shows an example where both τ and σ are permutations on the set $\{1, 2, 3, 4\}$. The diagram shows that if we do a permutation σ on the originally-labeled objects, and compare to the same permutation of the relabeled objects, we find that the relabeled permutation is exactly given by $\tau\sigma\tau^{-1}$. The permutations σ and $\tau\sigma\tau^{-1}$ are called *conjugate permutations*, and the operation which takes σ to $\tau\sigma\tau^{-1}$ is called *conjugation*.³

Conjugate permutations and cycle structure

Two permutations that are conjugate are in many ways very similar. We could almost call them the "same" permutation, only they act on a relabeled set of objects. In particular, it's true that two conjugate permutations must have the same cycle structure. For instance, in the example we did earlier

³Note this is quite different from conjugation of complex numbers. Unfortunately, "conjugation" is a very popular word in mathematics, and is used in many different senses.

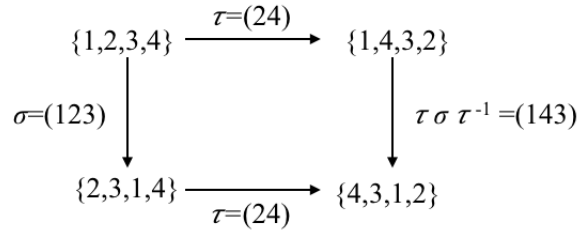


Figure 23.4.2. Conjugate mapping with τ and σ permuting $\{1, 2, 3, 4\}$.

in Figure 23.4.1 we saw that both permutations were three-cycles. This will be true in general because conjugation simply means relabeling the objects that are permuted, without changing anything else.

Example 23.4.2. Let $\sigma = (153)(276)$ and $\tau = (427)(165)$. Then

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Relabeling σ according to τ gives the conjugate $(136)(457)$. You can check that computing $\tau\sigma\tau^{-1}$ will give the same result as the relabeling method. \blacklozenge

Exercise 23.4.3. Given σ and τ use the relabeling method to find the permutation conjugate to σ . Check your work by computing $\tau\sigma\tau^{-1}$.

- (a) $\sigma = (6247)$ and $\tau = (527)(63)$. σ and τ act on the set $\{1, 2, 3, 4, 5, 6, 7\}$.
- (b) $\sigma = (256)(134)$ and $\tau = (21643)$. σ and τ act on the set $\{1, 2, 3, 4, 5, 6\}$.
- (c) $\sigma = (14)(27356)$ and $\tau = (463)$. σ and τ act on the set $\{1, 2, 3, 4, 5, 6, 7\}$.

\diamond

We've proved and tested that conjugate permutations have the same cycle structure. It turns out that the reverse is also true: namely, any two permutations with the same cycle structure are conjugate.

Example 23.4.4. Let $\sigma = (12)(3456)(789)$, $\mu = (149)(2658)(37)$. Notice that σ becomes μ if we use the following relabeling:

$$1 \rightarrow 3; \quad 2 \rightarrow 7; \quad 3 \rightarrow 2; \quad 4 \rightarrow 6; \quad 5 \rightarrow 5; \quad 6 \rightarrow 8; \quad 7 \rightarrow 1; \quad 8 \rightarrow 4; \quad 9 \rightarrow 9.$$

We can use this information to write τ in tableau notation:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 2 & 6 & 5 & 8 & 1 & 4 & 9 \end{pmatrix},$$

from which we find, $\tau = (1327)(468)$. Then you may check that σ and μ are conjugate according to: $\mu = \tau\sigma\tau^{-1}$. \blacklozenge

Exercise 23.4.5. In each of the following find a permutation τ that makes σ and μ conjugate. Check that σ and μ are conjugate according to: $\mu = \tau\sigma\tau^{-1}$.

(a) $\sigma = (135)(792)(468)$, $\mu = (236)(189)(457)$

(b) $\sigma = (2879)(3561)$, $\mu = (2461)(5793)$

(c) $\sigma = (25)(13578)$, $\mu = (36)(28154)$

\diamond

These examples lead up to the following theorem:

Proposition 23.4.6. Given a permutation group G , and two permutations $\sigma, \mu \in G$. Then σ and μ are conjugate if and only if they have exactly the same cycle structure.

PROOF. The “only if” part follows from remarks we have made above: the conjugation operation simply re-labels the elements of the permuted set, so two conjugate permutations must have the same cycle structure. For the “only if” part, we may write σ in cycle notation as

$$\sigma = (a_{11} \ a_{12} \ \dots \ a_{1n_1})(a_{21} \ a_{22} \ \dots \ a_{2n_2}) \dots (a_{k1} \ a_{k2} \ \dots \ a_{kn_k}).$$

Suppose that τ has the same cycle structure, which means that τ can be written as

$$\tau = (b_{11} \ b_{12} \ \dots \ b_{1n_1})(b_{21} \ b_{22} \ \dots \ b_{2n_2}) \dots (b_{k1} \ b_{k2} \ \dots \ b_{kn_k}).$$

Then we can define a bijection f by: $f(a_{ij}) = b_{ij}$, for any i and j . Using the above cycle structures, we can show that τ is equal to $f\sigma f^{-1}$. All we have to do is show that this works for any b_{ij} . For example, consider b_{11} : then $f\sigma f^{-1}(b_{11}) = f\sigma(a_{11}) = f(a_{12}) = b_{12}$, which is exactly equal to $\tau(b_{11})$. \square

23.4.2 Conjugacy and group action

We will now relate the idea of conjugacy with the notion of group action that was introduced earlier in the chapter.

Example 23.4.7. Let G be the dihedral group D_4 . Recall that D_4 consists of four rotations and four reflections. In fact we can write $D_4 = \{e, r, r^2, r^3, s, s \circ r, s \circ r^2, s \circ r^3\}$, where r is counterclockwise rotation by 90° , and s is the reflection that leaves vertices labeled 1 and 3 fixed. Let H be the subgroup $\{e, s\}$. We'll define our mapping from $H \times G \rightarrow G$ as follows:

$$(h, g) \rightarrow hgh^{-1}.$$

For example, consider the case $h = s$ and $g = r$. Then $(s, r) \rightarrow s \circ r \circ s^{-1}$. We can simplify this, since s is a reflection, so $s^{-1} = s$. Furthermore, by part c of Proposition 13.4.15 in Section 13.4, we can show $r \circ s = s \circ r^3$. This gives us

$$s \circ r \circ s^{-1} = s \circ r \circ s = s \circ s \circ r^3 = r^3.$$

◆

Exercise 23.4.8. Complete the previous example with $G = D_4$ and $H = \{e, s\}$ by listing all the pairs (h, g) with $h \in H$ and $g \in G$ together with the result of the mapping hgh^{-1} . Simplify your expression for hgh^{-1} as much as possible. ◇

Note something very interesting in the previous exercise. When $h = e$ the all elements of G remain unchanged by the mapping, but when $h = s$ all the rotations map to their inverses. We can generalize Example 23.4.7 using the following definition.

Definition 23.4.9. Given two group elements g, h in G , then hgh^{-1} is said to be a *conjugate element* to g . In this case, we would say that h acts on g by conjugation. △

The definition of conjugation gives us a new group action for any subgroup H acting on a group G which contains H :

Proposition 23.4.10. If H is a subgroup of G , then G is an H -set under conjugation. That is, we can define an action $H \times G \rightarrow G$, by $h.g = hgh^{-1}$ for $h \in H$ and $g \in G$.

The proof is contained in the following exercise.

Exercise 23.4.11. Fill in the blanks to prove the proposition:

First, we have that $\underline{\langle 1 \rangle}$ is in H and $e.g = \underline{\langle 2 \rangle} . g . \underline{\langle 3 \rangle} = g$. So the identity condition for a group action holds.

Also, observing that

$$(h_1 h_2).g = \underline{\langle 4 \rangle} . g . \underline{\langle 5 \rangle} = h_1(h_2 g . \underline{\langle 6 \rangle} .) . \underline{\langle 7 \rangle} = h_1.(\underline{\langle 8 \rangle} . g),$$

we see that the compatibility condition is also satisfied. \diamond

23.4.3 Order of conjugate elements

In order to illustrate some properties of the action of conjugation, we will take a familiar example: the group of rotational symmetries of a cube. What are the conjugate elements? We've seen that the rotations can be classified into:

- Stabilizers of faces;
- Stabilizers of vertices;
- Stabilizers of edges;
- Stabilizers of everything (the identity).

Which of these are conjugate?

Consider the conjugates of r_z , which is a 90° counterclockwise rotation around the z axis. Supposing that g is an arbitrary rotational symmetry, what does $g r_z g^{-1}$ do? First, the g^{-1} will rotate another pair of faces to the top and bottom positions. Then, r_z will rotate that pair of faces by 90° . Then g will rotate the two rotated faces back to their original places. The net result will always be a 90° rotation of an opposite pair of faces of the cube. The question now is, are *all* such 90° rotations conjugate to each other? In particular, are 90° *counterclockwise* rotations the same as 90° *clockwise* rotations? For instance, is r_z conjugate to r_z^{-1} . In fact it is, as we'll see in the next example.

Example 23.4.12. Let $g = r_x^2$ then consider $r_x^2 \circ r_z \circ r_x^{-2}$. What will this rotation do? First r_x^{-2} will take the top face to the bottom face and vice versa.

Then r_z will rotate the face z_- (which is now on top) 90° counterclockwise and z_+ (which is now on the bottom) 90° clockwise. Then r_x^2 will rotate z_- back to the bottom and z_+ back to the top. So we see $r_x^2 \circ r_z \circ r_x^{-2} = r_z^{-1}$. (This is related to the formula $srs^{-1} = r^{-1}$, which we saw in Chapter 13.)

◆

We have also seen that it's possible to rotate any pair of opposite faces to the top and bottom face. This means that any 90-degree rotation of any pair of opposite faces of the cube is conjugate to r_z .

Exercise 23.4.13.

- Find g such that $r_y = g \circ r_z \circ g^{-1}$.
- Find g such that $r_x^{-1} = g \circ r_z \circ g^{-1}$.
- What are the orders of r_z , r_y , and r_x^{-1} ? On the basis of your findings, make a conjecture about the orders of conjugate elements.

◇

The order of rotations appears to play an important role in determining which group elements are conjugate.

Exercise 23.4.14.

- Find two different rotations that are conjugate to r_z^2 , and express them both in the form $g \circ r_z^2 \circ g^{-1}$.
- What do you notice about the orders of these three rotations?

◇

Let's consider stabilizers of vertices.

Example 23.4.15. $r_y \circ r_z$ is a 120 degree stabilizer of vertex $+++$. Consider the conjugation of $r_y \circ r_z$ by the group element r_y , that is, $r_y \circ (r_y \circ r_z) \circ r_y^{-1}$. First, r_y^{-1} takes $++-$ to $+++$. Then $r_y \circ r_z$ rotates $++-$ 120 degrees counterclockwise. Then r_y rotates $++-$ back to its original place. The net result is a 120 degree counterclockwise rotation of the vertex $++-$.

◆

Exercise 23.4.16.

- (a) Which elements of the cube are stabilized by $r_z \circ r_y$ stabilize? What is the order of this stabilizer?
- (b) Consider the conjugate $r_x^2 \circ (r_z \circ r_y) \circ r_x^{-2}$. Which cube elements will this stabilize? What is the order of this stabilizer? (*Hint*)
- (c) Express $r_y \circ r_z$ as a conjugate of $r_z \circ r_y$: that is, find g such that $r_y \circ r_z = g r_z \circ r_y \circ g^{-1}$. (*Hint*)

◇

Finally, let's consider conjugates of stabilizers of edges.

Example 23.4.17. The rotation $r_z^2 \circ r_y^{-1}$ stabilizes the edge $\overline{x_- z_-}$. It's a 180 degree rotation about an axis through this edge $\overline{x_- z_-}$ and $\overline{x_+ z_+}$. Consider the conjugate $r_z^2 \circ (r_z^2 \circ r_y^{-1}) \circ r_z^{-2}$. What does this rotation do? First, r_z^{-2} takes $\overline{x_+ z_-}$ to $\overline{x_- z_-}$. Then $(r_z^2 \circ r_y^{-1})$ rotates about the axis through $\overline{x_+ z_-}$ 180 degrees, switching the two faces. Then r_z^2 rotates $\overline{x_+ z_-}$ back to its original position. The net result is a 180 degree rotation about the axis through $\overline{x_+ z_-}$ and $\overline{x_- z_+}$. ◆

Exercise 23.4.18.

- (a) The rotation $r_y^2 \circ r_z$ stabilizes the edge $\overline{x_+ y_+}$. One conjugate of this rotation is $r_y \circ (y^2 \circ z) \circ r_y^{-1}$. What does the conjugate stabilize?
- (b) What is the order of any conjugate of a stabilizer of an edge of a cube? Is the order always the same? Explain your answer.

◇

For all the examples we've seen so far, the order of a conjugate of any stabilizer is the same as the order of the stabilizer itself. Of course, examples are not proof—but in this case they're a strong indication that this may be a general property. In fact, we can show:

Proposition 23.4.19. Let G be a group, $g \in G$, and \tilde{g} is conjugate to g . Then $|g| = |\tilde{g}|$: that is, g has the same order as \tilde{g} .

PROOF. The proof is outlined in the following exercise.

Exercise 23.4.20. Fill in the blanks to complete the proof that a group element and its conjugate always have the same order.

Suppose that \tilde{g} is conjugate to g . This means that there exists an $x \in G$ such that $\tilde{g} = \underline{\langle 1 \rangle}$. Suppose $|g| = n$. Compute \tilde{g}^n as follows:

$$\begin{aligned}
 \tilde{g}^n &= (\tilde{g} \dots \tilde{g}) && (n \text{ times}) \\
 &= (\underline{\langle 2 \rangle}) \dots (\underline{\langle 3 \rangle}) && (n \text{ substitutions}) \\
 &= xg(\underline{\langle 4 \rangle})g \dots g(\underline{\langle 5 \rangle})gx^{-1} && (\text{associative property}) \\
 &= xg(\underline{\langle 6 \rangle})g \dots g(\underline{\langle 7 \rangle})gx^{-1} && (\text{inverse property}) \\
 &= x(\underline{\langle 8 \rangle})x^{-1} && (\text{identity property}) \\
 &= x(\underline{\langle 9 \rangle})x^{-1} && (\text{definition of order}) \\
 &= \underline{\langle 10 \rangle} && (\text{identity and inverse properties})
 \end{aligned}$$

From Proposition 15.5.41, it follows that $|\tilde{g}|$ divides $|\underline{\langle 11 \rangle}|$. On the other hand,

$$(\underline{\langle 12 \rangle})\tilde{g}(\underline{\langle 13 \rangle}) = g \quad (\text{inverse property}).$$

The same proof with g and \tilde{g} interchanged shows that $|g|$ divides $|\underline{\langle 14 \rangle}|$. Therefore, $|g| = \underline{\langle 15 \rangle}$ \diamond

□

Exercise 23.4.21. We've shown that if elements are conjugate they must have the same order.

- What is the converse of the above statement?
- Prove or disprove the converse using previous examples to help you.

◇

23.4.4 Conjugacy classes and the class equation

We have seen before that g -equivalent elements form an equivalence class. This means that the operation of conjugacy defines an equivalence relation, and every set of conjugate elements is an equivalence class. These equivalence classes are known as **conjugacy classes**. The upshot is that we have the group G partitioned into 5 conjugacy classes, consisting of:

- the identity,
- 90° stabilizers of faces,
- 180° stabilizers of faces,
- stabilizers of vertices,
- stabilizers of edges.

This is exactly the method we used before to count up the number of elements in G . What we've just done for the rotational symmetries of a cube can be done for any group. We have the general formula:

$$|G| = \sum (\text{orders of conjugacy classes}).$$

This is known as the *class equation*.

Example 23.4.22. We can verify that the class equation correctly calculates the order of the group of rotational symmetries of a cube.

$$\begin{aligned} |G| &= |\text{conjugacy class of } 90 \text{ degree stabilizers of faces}| \\ &\quad + |\text{conjugacy class of } 180 \text{ degree stabilizers of faces}| \\ &\quad + |\text{conjugacy class of stabilizers of vertices}| \\ &\quad + |\text{conjugacy class of stabilizers of edges}| \\ &\quad + |\text{conjugacy class of identity}| \\ &= 6 + 3 + 8 + 6 + 1 \\ &= 24. \end{aligned}$$



Let's use the class equation to verify $|G|$ for some other familiar groups.

Example 23.4.23.

Consider the group S_3 . Note this is the same as the dihedral group of an equilateral triangle. Let s be the reflection that leaves the vertex labeled '1' fixed, and let r be the counterclockwise rotation by 120 degrees. We can find the conjugacy classes of S_3 by creating a table with a column for each of the elements in the group. Each row will represent a conjugacy class.

It's clear that id has its own conjugacy class of one element. For example, $r^2 \circ \text{id} \circ r = r^2 \circ r = \text{id}$. We can verify that id is only conjugate to itself.

We can see that r has two conjugates. For example:

$$\text{id} \circ r \circ \text{id} = r$$

$$s \circ r \circ s = s \circ s \circ r^2 = \text{id} \circ r^2 = r^2 \text{ by Proposition 13.4.15 in Chapter 13.}$$

We don't need a row for r^2 because it belongs to the same conjugacy class as r . Computing the row for s completes the table, since s is conjugate to all the other reflections.

| | | | | | | | |
|----------------------------------|-------------|-------------|---------------|-------------|---------------|-------------|---------------|
| | g | id | r | r^2 | s | $s \circ r$ | $s \circ r^2$ |
| $g \circ \text{id} \circ g^{-1}$ | id | id | id | id | id | id | id |
| $g \circ r \circ g^{-1}$ | r | r | r | r^2 | r^2 | r^2 | r^2 |
| $g \circ s \circ g^{-1}$ | s | $s \circ r$ | $s \circ r^2$ | s | $s \circ r^2$ | $s \circ r$ | $s \circ r$ |

The table shows that S_3 is partitioned into three conjugacy classes, corresponding to the three rows of the table: id , rotations (r and r^2) and reflections ($s, s \circ r, s \circ r^2$): the classes have orders 1, 2, and 3 respectively. The class equation verifies the order of S_3 .

$$|S_3| = 1 + 2 + 3 = 6 \quad \blacklozenge$$

Exercise 23.4.24.

- (a) Complete a conjugacy table like the one in Example 23.4.23 for $G = D_4$. As in the example r is a counterclockwise rotation by 90° and s is the reflection that leaves the vertex labeled "1" fixed. Compute and simplify the conjugate expressions as compositions of r and s . We show one row. How many more rows are needed to complete the table?

| | | | | | | | | | |
|----------------------------------|-----|-------------|-----|-------|-------|-----|-------------|---------------|---------------|
| | g | id | r | r^2 | r^3 | s | $s \circ r$ | $s \circ r^2$ | $s \circ r^3$ |
| $g \circ \text{id} \circ g^{-1}$ | — | — | — | — | — | — | — | — | — |

Remember, once a group element appears in a row, you don't need to compute a row for that element, because you have already found its conjugacy class.

- (b) Verify that the class equation correctly calculates $|D_4|$.

◇

Example 23.4.25. We can also create a conjugacy table for using permutation notation. Here is the conjugacy table for S_3 using permutations.

| | | | | | | |
|------------------------------|-------|-------|-------|-------|-------|-------|
| g | (1) | (123) | (132) | (23) | (13) | (12) |
| $g \circ (1) \circ g^{-1}$ | (1) | (1) | (1) | (1) | (1) | (1) |
| $g \circ (123) \circ g^{-1}$ | (123) | (123) | (123) | (132) | (132) | (132) |
| $g \circ (23) \circ g^{-1}$ | (23) | (13) | (12) | (23) | (12) | (13) |

Recall the relabeling method in Exercise 23.4.3. We recommend using this method to save time when making conjugacy tables.

For instance, to simplify $(12) \circ (23) \circ (12)$ we can relabel (23) according to (12) . That is: $2 \rightarrow 1$ and $3 \rightarrow 3$. So, $(12) \circ (23) \circ (12) = (13)$. ◆

In the next exercise you may practice creating a conjugacy table using both permutation notation and the relabeling method.

Exercise 23.4.26.

- (a) Create a conjugacy table for A_4 (the subgroup of even permutations in S_4 —see Section 14.6.2). We show one a table with one row. How many more rows are needed to complete the table? (Use the relabeling method to save time in creating your table.)

| | | | | | | |
|----------------------------|-----|----------|----------|----------|-------|-----|
| x | (1) | (12)(34) | (13)(24) | (14)(23) | (123) | ... |
| $g \circ (1) \circ g^{-1}$ | — | — | — | — | — | ... |

- (b) Verify that the class equation correctly calculates $|A_4|$.

◇

Exercise 23.4.27. Let G be an abelian group of finite order and $x, g \in G$. Simplify the conjugate expression $x \circ g \circ x^{-1}$. How many conjugacy classes are in the abelian group G ? How many elements are in each conjugacy class?

◇

23.5 Hints for “Group Actions, with Applications” exercises

Exercise 23.1.12(b): Notice $0 \in 2\mathbb{Z}$, but $1 + 0$ is not in $2\mathbb{Z}$. So the action of \mathbb{Z} on $2\mathbb{Z}$ is not well-defined. (d) Note that the group operation of \mathbb{C} is addition.

Exercise 23.2.25: Note there are two rows for stabilizers of faces, because some stabilizers of faces have order 2 and some have order 4.

Exercise 23.2.19(a): There are two elements. (d): There are three elements.

Exercise 23.2.23(a): Express $|G|$ two different ways by applying the Counting Formula to edges, and then to faces.

Exercise 23.2.23(c): You may take the ratio (faces/edges) / (vertices/edges).

Exercise 23.2.25: There are two rows for faces, because there are two kinds of stabilizers for faces.

Exercise 23.2.31(b): It may be helpful to calculate the rotation using cycle notation.

Exercise 23.2.32 For example, R_{Bb} and $R_{\overleftrightarrow{Bb}}^2$ are the 120- and 240- degree rotations around the axis \overleftrightarrow{Bb} . Both stabilize face b . So $G_b = \{\text{id}, R_{Bb}, R_{\overleftrightarrow{Bb}}^2\}$. The same group stabilizes another set as well—can you figure out which one?

Exercise 23.2.42: How many group elements (rotations) are in G_{x_+} ? What else do they stabilize?

Exercise 23.2.53(b): What is $|G|$ according to the counting formula? How many stabilizers have we found so far?

Exercise 23.2.56(b): Use the Counting Formula.

Exercise 23.2.57(b): See the previous hint.

Exercise 23.3.17: Does $a + h$ have to be in H ?

Exercise 23.3.20: H itself is a coset, and take $g_1 = (123)$ and $g_2 = (23)$. Is it true that acting on H by g_1 followed by g_2 is the same as acting on H by g_2g_1 ?

Exercise 23.4.16: (b) Take the answer to part (a), and apply the rotation r_x^2 (why does this work?) (c) Find a rotation that map the fixed point set of $r_y \circ r_z$ to the fixed point set of $r_z \circ r_y$.

Introduction to Rings and Fields

The integers are like a golden ring in a chain, whose beginning is a glance and whose ending is eternity. (*Source: Khalil Gibran (paraphrase)*)

The kingdom of heaven is like treasure hidden in a field. When a man found it, he hid it again, and then in his joy went and sold all he had and bought that field. (Source: Jesus of Nazareth (quoted by Matthew))

Groups and *rings* are the two basic abstract structures in study of abstract algebra, These are not the only abstract structures studied, but most others are modifications of these two. groups and rings are basic in the areas of particle physics, cryptography, and coding theory (see Section 24.11 for more information). They also creep into other areas of mathematics like analysis and number theory. As we proceed, you may notice many similarities between the properties of rings and those of groups. Let's begin with a review of common number systems.

This chapter is by Christy Douglass and Chris Thron, with contributions by Jennifer Lazarus and Adam McDonald.

24.1 Definitions and Examples

Some of the number systems we've studied in previous chapters are:

- \mathbb{Z} =integers
- \mathbb{Q} =rational numbers
- \mathbb{R} =real numbers
- \mathbb{C} =complex numbers
- \mathbb{Z}_n =integers mod n .
- $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \dots$ = polynomials with coefficients in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \dots$

When studying rings (and groups), we put a lot of focus on the integers. The integers \mathbb{Z} have two operations: addition(+) and multiplication(\cdot). These operations have the following properties:

- (I) Closure: if $a, b \in \mathbb{Z}$ then $a + b$ and $a \cdot b$ are in \mathbb{Z} .
- (II) Associativity: if $a, b, c \in \mathbb{Z}$ then $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
- (III) Zero: there is an element $0 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, $a + 0 = 0 + a = a$.
- (IV) One: there is an element $1 \in \mathbb{Z}$ such that for all $a \in \mathbb{Z}$, $a \cdot 1 = 1 \cdot a = a$.
- (V) Commutativity of Addition: if $a, b \in \mathbb{Z}$, then $a + b = b + a$.
- (VI) Additive Inverses: for every $a \in \mathbb{Z}$, there exists an element $-a \in \mathbb{Z}$ such that $a + (-a) = 0$.
- (VII) Distributivity: for every $a, b, c \in \mathbb{Z}$ we have that $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Note that commutativity of multiplication is not a property of all rings, so $a(b + c) = (b + c)a$ is not necessarily true for a ring.

All of the number systems listed at the beginning of this chapter have properties I-VII. Similar properties are found in other number systems.¹

Definition 24.1.1. Any number system with the two arithmetic operations (+ and \cdot) that satisfy properties I-VII is called a *ring*. \triangle

¹The reader may recall that some of these same properties were listed in Section 12.5, when we were talking about coefficients of polynomials.



As well as having properties *I – VII*, multiplication is commutative in all of the above number systems. This leads us to the following definition:

Definition 24.1.2. A number system is a *commutative ring* if it is a ring where multiplication is also commutative. \triangle

The properties of a ring are so similar to those of a group that it warrants a short discussion. The main difference between a ring and a group is that a ring has two binary operations (usually called addition and multiplication) while a group has only one operation. In fact, if you consider just the operation of addition, then a ring is a group with respect to addition. As far as multiplication, a ring is “almost” a group with respect to multiplication except that not all elements have multiplicative inverses.

Now that we know what a ring is, how do we prove a number system forms a ring? If you said that we would have to prove that the number system fulfills properties *I – VII*, then you would be correct! Let’s look at some examples that will show us how to prove a number system forms a ring.

The rings we’ve talked about so far ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) have all been infinite rings. But there are finite rings as well. In fact \mathbb{Z}_n is also a ring for any integer $n \geq 2$. We’ll show this in the following example:

Example 24.1.3. Prove that \mathbb{Z}_n is a ring for any integer $n \geq 2$.

PROOF. Recall that $\mathbb{Z}_n = \{0, 1, 2, \dots, n - 1\}$. It is also important to note that the operations of addition and multiplication will be defined as *modular sum* and *modular product*, notated as \oplus and \odot , respectively. We should address each of the seven properties listed above to show that we have a ring. It turns out that we have already shown each of these properties in the chapter on modular arithmetic, Chapter 5. Let’s divide our proof into seven steps, one for each required ring property.

- (I) First we must show that \mathbb{Z}_n is closed under \oplus and \odot . In Proposition 5.4.13, we showed that the modular sum and modular product of two elements of \mathbb{Z}_n are also in \mathbb{Z}_n . In other words, $a \oplus b \in \mathbb{Z}_n$ and $a \odot b \in \mathbb{Z}_n$, for all $a, b \in \mathbb{Z}_n$. So \mathbb{Z}_n is closed under \oplus and \odot .
- (II) Second, we must show that the associative property holds for \mathbb{Z}_n . In Proposition 5.4.23 (b), we show that $(a \oplus b) \oplus c = a \oplus (b \oplus c)$ and $(a \odot b) \odot c = a \odot (b \odot c)$. So the associative property holds for \mathbb{Z}_n .

- (III) Third, we will show that the zero property holds for \mathbb{Z}_n . In Proposition 5.4.17, we show that $0 \in \mathbb{Z}_n$ and $a \oplus 0 = 0 \oplus a = a$, for any $a \in \mathbb{Z}_n$, so 0 is the additive identity of \mathbb{Z}_n and the zero property holds.
- (IV) Our next step is to show that \mathbb{Z}_n has the multiplicative identity property (one). Again, we will refer to Section 5.4.1. In particular, Exercise 5.4.18 showed us that $1 \in \mathbb{Z}_n$ and $1 \odot a = a \odot 1 = a$, for any $a \in \mathbb{Z}_n$. So, the identity property of multiplication holds for \mathbb{Z}_n .
- (V) The commutative property of \oplus for \mathbb{Z}_n must be proven next. Proposition 5.4.23 (a) shows us that $a \oplus b = b \oplus a$ and $a \odot b = b \odot a$, for all $a, b \in \mathbb{Z}_n$. Note that for a set to be a ring, we only need to show that commutativity of *addition* holds. Because commutativity of *multiplication* also holds for \mathbb{Z}_n , we may also have a *commutative* ring. Let's continue with our proof that \mathbb{Z}_n is a ring before we jump to that conclusion.
- (VI) The sixth property that we must show is that of the additive inverse. We will refer back to Proposition 5.4.19. Here we let $a' = n - a$, for any $a \in \mathbb{Z}_n$. We show that $a' \in \mathbb{Z}_n$ and $a \oplus a' = a' \oplus a = 0 \pmod{n}$: that is, a' is the additive inverse of a .
- (VII) For our last step, we will show that the distributive property holds true for \mathbb{Z}_n . Once again, we have already shown that this is true. In Proposition 5.4.23 (c), we show that $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$. Since \odot commutes in \mathbb{Z}_n , it follows that $a \odot (b \oplus c) = (b \oplus c) \odot a = (a \odot b) \oplus (a \odot c)$ and the distributive property holds.

We have shown that all seven ring properties hold true in \mathbb{Z}_n over \oplus and \odot . Additionally, we have shown that \mathbb{Z}_n commutes over \odot . So, \mathbb{Z}_n is a *commutative* ring and our proof is complete. \square \blacklozenge

We've already mentioned that \mathbb{Q} is a ring. Sometimes we can use rings to create larger rings by adding additional elements. Such rings are called *extension rings*. We will discuss these further in Section 24.3. For now, let's look at a particular example.

Example 24.1.4. Prove that $\mathbb{Q}[\sqrt[3]{2}] = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{4}) \mid a_0, a_1, a_2 \in \mathbb{Q}\}$ forms a ring.

Note: $\mathbb{Q}[\sqrt[3]{2}]$ is the set of all polynomials of the form:



$a_0(\sqrt[3]{2})^0 + a_1(\sqrt[3]{2})^1 + a_2(\sqrt[3]{2})^2 + \cdots + a_n(\sqrt[3]{2})^n$, where $a_0, a_1, a_2, \dots, a_n \in \mathbb{Q}$.

In this case, we have defined $\mathbb{Q}[\sqrt[3]{2}]$ using only the first three terms. (We will explain why three terms is enough later on in the proof.)

PROOF. To prove that $\mathbb{Q}[\sqrt[3]{2}]$ forms a ring, we must show $\mathbb{Q}[\sqrt[3]{2}]$ has all seven ring properties listed above. It will be useful to define a couple of arbitrary elements in our set: let $a, b \in \mathbb{Q}[\sqrt[3]{2}]$ such that: $a = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ and $b = b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{4}$.

Property (1): First, we need to prove that $\mathbb{Q}[\sqrt[3]{2}]$ is closed under addition and multiplication. We will divide this task into two parts:

- (a) If $a, b \in \mathbb{Q}[\sqrt[3]{2}]$ then $a + b \in \mathbb{Q}[\sqrt[3]{2}]$. This is called *additive closure*.
- (b) If $a, b \in \mathbb{Q}[\sqrt[3]{2}]$ then $ab \in \mathbb{Q}[\sqrt[3]{2}]$. This is called *multiplicative closure*.

First, we will look at additive closure (a).

Remember that we have already defined two arbitrary elements in $\mathbb{Q}[\sqrt[3]{2}]$, a and b . So,

$$\begin{aligned} a + b &= (a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}) + (b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{4}) \\ &= (a_0 + b_0) + (a_1 + b_1)\sqrt[3]{2} + (a_2 + b_2)\sqrt[3]{4}. \end{aligned}$$

Now let $c_0 = (a_0 + b_0)$, $c_1 = (a_1 + b_1)$ and $c_2 = (a_2 + b_2)$. Since \mathbb{Q} is closed under addition, then $c_0, c_1, c_2 \in \mathbb{Q}$ and $a + b = c_0 + c_1\sqrt[3]{2} + c_2\sqrt[3]{4}$. It should now be clear that this sum is indeed an element of $\mathbb{Q}[\sqrt[3]{2}]$. We have shown that adding any two elements in $\mathbb{Q}[\sqrt[3]{2}]$ will always produce another element of $\mathbb{Q}[\sqrt[3]{2}]$. So, $\mathbb{Q}[\sqrt[3]{2}]$ is closed under addition.

Now let's prove multiplicative closure (b). We will again use a and b as defined earlier, so that:

$$\begin{aligned} ab &= (a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4})(b_0 + b_1\sqrt[3]{2} + b_2\sqrt[3]{4}) \\ &= (a_0b_0 + 2a_1b_2 + 2a_2b_1) + (a_0b_1 + a_1b_0 + 2a_2b_2)\sqrt[3]{2} \\ &\quad + (a_0b_2 + a_1b_1 + a_2b_0)\sqrt[3]{4}. \end{aligned}$$

Again, we must show that this product is also an element of $\mathbb{Q}[\sqrt[3]{2}]$. Let's use a strategy similar to the one we used for additive closure.

Suppose we let $d_0, d_1, d_2 \in \mathbb{Q}$ such that $d_0 = (a_0b_0 + 2a_1b_2 + 2a_2b_1)$, $d_1 = (a_0b_1 + a_1b_0 + 2a_2b_2)$, and $d_2 = (a_0b_2 + a_1b_1 + a_2b_0)$. Since \mathbb{Q} is closed under multiplication, then $d_0, d_1, d_2 \in \mathbb{Q}$ and $ab = d_0 + d_1\sqrt[3]{2} + d_2\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$. We have shown that multiplying any two elements in $\mathbb{Q}[\sqrt[3]{2}]$ produces another element in $\mathbb{Q}[\sqrt[3]{2}]$, so $\mathbb{Q}[\sqrt[3]{2}]$ is closed under multiplication.

Exercise 24.1.5. Recall that in our definition of $\mathbb{Q}[\sqrt[3]{2}]$, we only included three terms in the polynomial expansion. In this exercise, we will see why.

- Show that if we include 4 terms, then we get the same set. In other words, show that any polynomial of the form $d_0 + d_1\sqrt[3]{2} + d_2\sqrt[3]{4} + d_3(\sqrt[3]{2})^3$ can also be rewritten in the form $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ where $a_0, a_1, a_2 \in \mathbb{Q}$.
- Show similarly that if we include 5 terms, we still get the same set (use a similar method).
- Given a polynomial of the form $d_0 + d_1\sqrt[3]{2} + d_2\sqrt[3]{4} + \dots + d_n(\sqrt[3]{2})^n$, show that it can be rewritten in the form $a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4}$ where $a_0, a_1, a_2 \in \mathbb{Q}$ by giving explicit formulas for a_0, a_1, a_2 .
- In the definition of $\mathbb{Q}[\sqrt[3]{2}]$, we included a term proportional to $\sqrt[3]{4}$. Show that this term is necessary, by showing that $a_0 + a_1\sqrt[3]{2}$ is *not* closed under multiplication.

◇

Let's continue with our proof of Example 24.1.4. We have shown that $\mathbb{Q}[\sqrt[3]{2}]$ satisfies the first property of rings. Now, let's take a look at property (2). We must show associativity for addition and multiplication. In other words, we must show that:

- If $a, b, c \in \mathbb{Q}[\sqrt[3]{2}]$ then $(a + b) + c = a + (b + c)$, and
- If $a, b, c \in \mathbb{Q}[\sqrt[3]{2}]$ then $(ab)c = a(bc)$.

For associativity of addition, let $a, b, c \in \mathbb{Q}[\sqrt[3]{2}]$. Since all of the numbers in $\mathbb{Q}[\sqrt[3]{2}]$ are real numbers, and the real numbers are associative, then it follows automatically that numbers in $\mathbb{Q}[\sqrt[3]{2}]$ also associate. We can make a similar argument for associativity of multiplication. Associativity is an example of an *inherited property*.



Definition 24.1.6. An *inherited property* is a property such that, if the property is true for a set of numbers S , then it's also true for any subset of S . \triangle

Exercise 24.1.7. Show that additive closure is *not* an inherited property by providing a counterexample. \diamond

Back to our proof of Example 24.1.4.

Property (3): This is known as the *zero property*. To prove this property, we must show that $0 \in \mathbb{Q}[\sqrt[3]{2}]$ and also that $a + 0 = 0 + a = 0$ for all $a \in \mathbb{Q}[\sqrt[3]{2}]$. Notice that $0 = 0 + 0\sqrt[3]{2} + 0\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}]$. Since all numbers, $a \in \mathbb{Q}[\sqrt[3]{2}]$ are real numbers, it follows that $a + 0 = 0 + a = 0$. So 0 is the zero element of $\mathbb{Q}[\sqrt[3]{2}]$ and property (3) holds true.

The proof of property (4) is left as an exercise.

Exercise 24.1.8. Prove that 1 is the identity of $\mathbb{Q}[\sqrt[3]{2}]$. (You may use the proof of the zero element as a model.) \diamond

The proofs of properties (5) and (7) resemble the proof of property (2).

Exercise 24.1.9. Prove properties (5) and (7). (You may use the proof of property (2) as a model.) \diamond

We have shown that $\mathbb{Q}[\sqrt[3]{2}]$ satisfies all seven properties of rings. Therefore, by Definition 24.1.1, $\mathbb{Q}[\sqrt[3]{2}]$ is a ring and our proof is complete. \square



Exercise 24.1.10. Let $\mathbb{Q}[2^{\frac{1}{2}}]$ be the set of all numbers $\{a + b \cdot 2^{\frac{1}{2}}\}$ with $a, b \in \mathbb{Q}$. Is $\mathbb{Q}[2^{\frac{1}{2}}]$ a ring? \diamond

Exercise 24.1.11.

(a) Let $M_2(\mathbb{R})$ be the set of 2×2 matrices with entries in \mathbb{R} . Show that $M_2(\mathbb{R})$ is a ring under the operations of matrix addition and multiplication.

- (b) Give an example to show that $\mathbb{M}_2(\mathbb{R})$ is not commutative under multiplication.
- (c) Show that although the distributive law holds in $\mathbb{M}_2(\mathbb{R})$, it is *not* true that $X(Y + Z) = YX + ZX$ for all $a, b, c \in \mathbb{M}_2(\mathbb{R})$. This shows that you have to be very careful about the order of multiplication when dealing with rings that aren't commutative.

◇

Exercise 24.1.12. Define the set $C_3(\mathbb{R})$ as the set of all 3×3 *circulant matrices* of the form: $\begin{bmatrix} a & c & b \\ b & a & c \\ c & b & a \end{bmatrix}$, where $a, b, c \in \mathbb{R}$. Prove or disprove that $C_3(\mathbb{R})$ is a ring.

◇

Exercise 24.1.13. Suppose R is a ring. Prove that $\mathbb{M}_2(R)$ is also a ring. ◇

24.1.1 Polynomial rings

Take any ring R and the set of polynomials over that ring $R[x]$. It turns out that $R[x]$ is also a ring. In this section, we will prove this, and explore some properties of $R[x]$.

Actually, we've already completed most of the proof that $R[x]$ is a ring. Recall that in Section 12.5 we proved several properties of polynomials $R[x]$, under very general assumptions about the set of coefficients R . In fact, properties (I)-(V) in Section 12.5 are all included in the ring properties listed in Section 24.1. So all of the properties shown in Section 12.5 apply to $R[x]$ as long as R is a ring.

Exercise 24.1.14. Go back to Section 12.5 and identify the propositions that prove that the set $R[x]$ satisfies the ring properties (I,II,III,V,VI,VII) from Section 24.1. ◇

We are still missing property IV, the identity property. We can take care of this in short order.

Exercise 24.1.15. Show that the polynomial $p(x) = 1x^0$ is a multiplicative identity for the set of polynomials $\mathbb{C}[x]$. ◇

Proposition 24.1.16. Suppose that R is a ring with a multiplicative identity 1 . Then $1x^0$ is a multiplicative identity of $R[x]$.

Exercise 24.1.17. Prove Proposition 24.1.16. ◇

Putting Exercise 24.1.14 and Proposition 24.1.16 together, we have immediately:

Proposition 24.1.18. The set of polynomials over a ring is also a ring. That is, if R is a ring, then $R[x]$ is also a ring.

Proposition 24.1.18 is a powerful result. We may use this proposition to build larger and larger rings. For example, Proposition 24.1.18 tells us that $((\mathbb{Z}[x])[y])[z]$ is a ring of polynomials in x, y, z (usually this is written as $\mathbb{Z}[x, y, z]$). Apparently there are many examples of mathematical structures that are rings, which makes them an interesting and fruitful object of study.

24.1.2 Some Ring Proofs

Remember that rings must satisfy the multiplicative identity property. For the set of integers, the multiplicative identity is uniquely 1 . We can show that the multiplicative identity for any ring is unique.

Proposition 24.1.19. The multiplicative identity of a ring, R , is unique.

PROOF. We need to show that if x is a multiplicative identity, then $x = 1$.

| | |
|----------------------------------|---------------------------------------|
| x is a multiplicative identity | Given |
| $x \cdot 1 = 1 \cdot x = 1$ | Definition of Multiplicative Identity |
| 1 is a multiplicative identity | Given |
| $1 \cdot x = x \cdot 1 = x$ | Definition of Multiplicative Identity |
| $x = 1$ | Substitution |

□

Exercise 24.1.20. Show that the additive identity of a ring R is unique. (You may model your proof on the proof of Proposition 24.1.19). ◇

Way back in Section 3.2.1 we mentioned the *zero divisor property* for real numbers: the product of two real numbers is zero if and only if at least one of the two numbers is zero. In fact, the “only if” part of this statement is *not true* for general rings:

Exercise 24.1.21.

- (a) Show that two nonzero numbers can multiply to give zero in \mathbb{Z}_6 .
- (b) Show that if n is not prime, then there are two nonzero numbers in \mathbb{Z}_n that multiply to give zero.

◇

We can, however, show the “if” part:

Proposition 24.1.22. Given a ring, R , for any $x \in R$ we have $x \cdot 0 = 0 \cdot x = 0$.

PROOF. We will use properties of rings in our proof.

| | |
|---|--------------------------------|
| $0 = 0 + 0$ | Definiton of Additive Identity |
| $x \cdot 0 = x \cdot (0 + 0)$ | Substitution |
| $x \cdot 0 = x \cdot 0 + x \cdot 0$ | Distributive Property |
| $x \cdot 0 + -(x \cdot 0) = (x \cdot 0 + x \cdot 0) + -(x \cdot 0)$ | Substitution |
| $x \cdot 0 + -(x \cdot 0) = x \cdot 0 + (x \cdot 0 + -(x \cdot 0))$ | Associativity of Addition |
| $0 = x \cdot 0 + (0)$ | Additive Inverse |
| $0 = x \cdot 0$ | Additive Identity |

We have shown that $0 = x \cdot 0$. It remains to show that $0 = 0 \cdot x$, since multiplication in rings is not always commutative.

Exercise 24.1.23. Complete the proof of Proposition 24.1.22 by showing that $0 = 0 \cdot x$, for $x \in R$.

◇

□

In the following proposition, we show that we may construct the additive inverse of any ring element by multiplying the element by the additive inverse of 1.

Proposition 24.1.24. Let R be a ring, let -1 be the additive inverse of 1 , and let $-x$ denote the additive inverse of $x \in R$. Then $-x = (-1) \cdot x$.

Exercise 24.1.25. Prove Proposition 24.1.24. \diamond

Since there are many rules that ring operations obey, we can simplify algebraic expressions in rings in much the same way as we do in basic algebra.

Exercise 24.1.26. Given $A, B, C \in R$ where R is a commutative ring, we can show that $(B + (-C)) \cdot (A \cdot (B + C)) = A \cdot (B \cdot B + (-C) \cdot C)$. Give the reasons for the following steps in the simplification:

$$\begin{aligned}
 (B + (-C)) \cdot (A \cdot (B + C)) &= (A \cdot (B + C)) \cdot (B + (-C)) && \text{Comm. prop.} \\
 &= A \cdot ((B + C) \cdot (B + (-C))) && \text{Assoc. prop.} \\
 &= A \cdot (((B + C) \cdot B) + ((B + C) \cdot (-C))) && \underline{< 1 >} \\
 &= A \cdot ((B \cdot B + C \cdot B) + (B \cdot (-C) + C \cdot (-C))) && \underline{< 2 >} \\
 &= A \cdot ((B \cdot B + B \cdot C) + ((-C) \cdot (B) + (-C) \cdot C)) && \underline{< 3 >} \\
 &= A \cdot (B \cdot B + (B \cdot C + (-C) \cdot (B) + (-C) \cdot C)) && \underline{< 4 >} \\
 &= A \cdot (B \cdot B + (B \cdot C + B \cdot (-C)) + (-C) \cdot C) && \underline{< 5 >} \\
 &= A \cdot (B \cdot B + (B \cdot (C + (-C))) + (-C) \cdot C) && \underline{< 6 >} \\
 &= A \cdot (B \cdot B + (B \cdot (0)) + (-C) \cdot C) && \underline{< 7 >} \\
 &= A \cdot (B \cdot B + (0 + (-C) \cdot C)) && \underline{< 8 >} \\
 &= A \cdot (B \cdot B + (-C) \cdot C) && \underline{< 9 >}
 \end{aligned}$$

\diamond

24.2 Subrings

Earlier we mentioned that two important topics studied in Abstract Algebra are groups and rings. Just like groups have subgroups, rings have *subrings*.

Definition 24.2.1. A ring that is a subset of another ring is called a *subring*. \triangle

Suppose R is a ring, and $S \subset R$. To prove S is a subring, we must show that S satisfies all seven ring properties. S will inherit certain properties

(associativity, commutativity, and distributive) from R , making lighter work of our proof that S is also a ring.

To show that $S \subset R$ is a ring, we must show the following:

- Additive Inverse: $a \in S \Rightarrow -a \in S$.
- Closure: $a, b \in S \Rightarrow a + b \in S$ and $ab \in S$.
- Zero: $0 \in S$, such that $0 + a = a + 0 = a$, for all $a \in S$.
- One: $1 \in S$, such that $1 \cdot a = a \cdot 1 = a$, for all $a \in S$. Note that for S to be a subring of R , the multiplicative identities must be the same.

If S is a subring of R *except* that $1 \notin S$, then S is a **subring** of R *without unity*.

Examples of subrings:

- (a) \mathbb{Z} is a subring in \mathbb{Q} .
- (b) \mathbb{R} is a subring of \mathbb{C} .
- (c) If R is a ring, then R is a subring of $R[x]$.

Let's look at a subring proof together:

Example 24.2.2. Given two rings R_1 and R_2 which share the same $+$ and \cdot operations, show that $R_1 \cap R_2$ is a subring of both R_1 and R_2 .

PROOF. Let's begin by showing that $R_1 \cap R_2 \subset R_1$ and R_2 . By definition of \cap , $a \in R_1 \cap R_2 \Rightarrow a \in R_1$ and $a \in R_2$. So $R_1 \cap R_2 \subset R_1$ and R_2 .

Next, we will show the additive inverse property. Let a be an arbitrary element in $R_1 \cap R_2$. Then $a \in R_1$ and R_2 , by the definition of \cap . Remember that R_1 and R_2 are rings with the same $+$ operation, so $-a \in R_1$ and R_2 . This means that $-a \in R_1 \cap R_2$ and the additive inverse property holds.

Our next task is to show that $R_1 \cap R_2$ contains the zero element. Since R_1 and R_2 are rings with the same $+$ operation, then $0 \in R_1$ and R_2 . By definition of \cap , $0 \in R_1 \cap R_2$, and the zero property holds.

In the following exercise, you will complete the proof that $R_1 \cap R_2$ is a subring by showing that it has a multiplicative identity.

Exercise 24.2.3. Given rings R_1 and R_2 , with the same \cdot operation, Show that $1 \in R_1 \cap R_2$. You can model your proof after the zero property proof. \diamond

□

◆

We have shown in Exercise 24.1.11 that $\mathbb{M}_2(\mathbb{R})$, forms a ring. In the following exercise, we will consider some subrings of $\mathbb{M}_2(\mathbb{R})$.

Exercise 24.2.4.

(a) Show that the set of all matrices of the form:

$$\begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$$

is a subring of all 2x2 matrices, $\mathbb{M}_2(\mathbb{R})$.

(b) Show that the set of all matrices of the form:

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

is a subring of $\mathbb{M}_2(\mathbb{R})$.

(c) Prove or disprove: The set of all matrices of the form:

$$\begin{bmatrix} a & 0 \\ b & d \end{bmatrix}$$

is a subring of $\mathbb{M}_2(\mathbb{R})$.

◆

In Section 24.1, we learned that \mathbb{C} , the set of all complex numbers, forms a ring. Consider the following subset of \mathbb{C} :

Exercise 24.2.5. Prove or disprove: $\{1, -1, i, -i\}$ forms a subring of \mathbb{C} . \diamond

Exercise 24.2.6. Let $\mathbb{Z} + \mathbb{Z}i$ denote the set of complex numbers with real and imaginary parts that are both integers. Prove or disprove $\mathbb{Z} + \mathbb{Z}i$ is a subring of \mathbb{C} . \diamond

The set $n\mathbb{Z}$ represents the set of all integers, $n \cdot k \in \mathbb{Z}$, such that n is some integer and $k \in \mathbb{Z}$. For example, $2\mathbb{Z}$ represents the set of all even integers. It should be clear that $n\mathbb{Z} \subset \mathbb{Z}$, for all $n \in \mathbb{N}$, but is it a subring as well?

Exercise 24.2.7.

- (a) Prove or disprove: $2\mathbb{Z}$ is a subring (with or without unity) of \mathbb{Z} .
- (b) Prove or disprove: $3\mathbb{Z}$ is a subring (with or without unity) of \mathbb{Z} .
- (c) Show that $m\mathbb{Z}$ is a subring (without unity) of $n\mathbb{Z}$ iff n divides m .

◇

If R is a finite ring, the addition and multiplication Cayley tables for S can be obtained from the corresponding tables of R . We can cross out the rows and columns with heading elements in R that are *not* also in S . Let's look at an example.

Example 24.2.8. $\{0, 2, 4\}$ is a subring of \mathbb{Z}_6 without unity.

PROOF. The Cayley tables for modular addition and modular multiplication of \mathbb{Z}_6 are:

| | | | | | | | | | | | | | | |
|----------|---|---|---|---|---|---|--|---------|---|---|---|---|---|---|
| \oplus | 0 | 1 | 2 | 3 | 4 | 5 | | \odot | 0 | 1 | 2 | 3 | 4 | 5 |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 | | 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 | | 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 | | 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 | | 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 | | 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Now, we are wanting only $\{0, 2, 4\}$ of \mathbb{Z}_6 . We will keep those values and cross out all rows and columns that are not $\{0, 2, 4\}$.

| \oplus | 0 | 1 | 2 | 3 | 4 | 5 |
|----------|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

| \odot | 0 | 1 | 2 | 3 | 4 | 5 |
|---------|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

This results in the following:

| \oplus | 0 | 2 | 4 |
|----------|---|---|---|
| 0 | 0 | 2 | 4 |
| 2 | 2 | 4 | 0 |
| 4 | 4 | 0 | 2 |

| \odot | 0 | 2 | 4 |
|---------|---|---|---|
| 0 | 0 | 0 | 0 |
| 2 | 0 | 4 | 2 |
| 4 | 0 | 2 | 4 |

Since all the rows and columns have all the elements $\{0, 2, 4\}$ in the modular addition and modular multiplication tables, then all four subring properties are satisfied and $\{0, 2, 4\}$ is a subring of \mathbb{Z}_6

□

◆

We can generalize this idea with the following exercise.

Exercise 24.2.9. If $R = \mathbb{Z}_{mn}$ and $S = \{0, m, 2m, \dots, (n-1)m\}$, then S is a subring of R without unity. ($\mathbb{Z}_6 = \mathbb{Z}_{mn}$, where $m = 2$ and $n = 3$.)

◇

24.3 Extension Rings

We have learned that a subring can be formed from a subset of a ring. One example we used was that $\{0, 2, 4\}$ is a subring of \mathbb{Z}_6 . We can also extend a ring into a larger set, called an extension ring. We would say that \mathbb{Z}_6 is an extension ring of $\{0, 2, 4\}$.

Definition 24.3.1. If R is a subring of S , then we can say that S is an *extension ring* of R .

△

Extension rings can be used to create number systems that are more "complete" in some sense. In fact, you've seen extension rings several times before. The integers form a very simple number system, but integers lack

multiplicative inverses. The set of rational numbers is in fact an extension ring of the integers, which includes the multiplicative inverses that integers lack. Similarly, real numbers are "incomplete" in the sense that some real numbers do not have roots (e.g. there is no real square root of -1). The complex numbers form a larger number system that includes the real numbers, and also has the missing roots.

Another example of extension ring that we've seen before is the polynomial ring $\mathbb{Q}[x]$, which contains the ring \mathbb{Q} . Some polynomials lack multiplicative inverses as the following proposition shows.

Proposition 24.3.2. $p(x) = 1 + x$ has no multiplicative inverse in $\mathbb{Q}[x]$.

PROOF. We will show by contradiction that $1 + x$ has no multiplicative inverse in $\mathbb{Q}[x]$. Suppose on the contrary that $1 + x$ has an inverse that can be written as $q(x) = \sum_{n=0}^N a_n x^n$, where a_N is the leading nonzero coefficient and $N \geq 0$. Then

$$(1 + x)q(x) = (1 + x) \cdot \sum_{n=0}^N a_n x^n = a_N x^{N+1} + \cdots + a_0.$$

Since $a_N \neq 0$, it follows that the degree of $(1 + x)q(x)$ is equal to $N + 1$, so it is not a constant polynomial. In particular, $(1 + x)q(x) \neq 1$. This contradicts the supposition that $q(x)$ is the multiplicative inverse of $1 + x$. Therefore, $(1 + x)$ does not have a multiplicative inverse in $\mathbb{Q}[x]$. \square

We can actually go further, and take infinite power series in addition to finite polynomials. This gives us an even larger extension ring:

Example 24.3.3. Let $\widehat{\mathbb{Q}}[x]$ be the set of power series with rational coefficients:

$$\widehat{\mathbb{Q}}[x] = \left\{ \sum_{n=0}^{\infty} a_n x^n \right\}, \text{ where } a_n \in \mathbb{Q}.$$

Show that $\widehat{\mathbb{Q}}[x]$ is an extension ring of $\mathbb{Q}[x]$.

Now, the question is does $p(x)$ have a multiplicative inverse in $\widehat{\mathbb{Q}}[x]$? There are 3 methods we can do to figure this out.

1. Taylor series
2. Long division

3. Linear recurrence relation

We will explore all three methods in the following example.

Example 24.3.4. Find the multiplicative inverse of $(1+x)$ in $\widehat{\mathbb{Z}}[x]$

1. First Method: Taylor series

The Taylor series expansion for the function $f(x)$ about the point $a = 0$ is given by:

$$f(x) = f(0) + f'(0)x + \frac{f''(0)x^2}{2!} + \frac{f'''(0)x^3}{3!} + \dots$$

For $f(x) = \frac{1}{1+x}$, we have:

$$\begin{aligned} \left(\frac{1}{1+x}\right)' &= ((1+x)^{-1})' = -1!(1+x)^{-2} \Rightarrow \text{when } x = 0, f'(x) = -1 \\ ((1+x)^{-1})'' &= -1(-2)(1+x)^{-3} = 2!(1+x)^{-3} \Rightarrow \text{when } x = 0, f''(x) = 2 \\ ((1+x)^{-1})''' &= 2(-3)(1+x)^{-4} = -3!(1+x)^{-4} \Rightarrow \text{when } x = 0, f'''(x) = -3 \end{aligned}$$

In general:

$$((1+x)^{-1})^{(n)} = (-1)^n n!(1+x)^{-n-1} \Rightarrow \text{when } x = 0, f^{(n)}(x) = (-1)^n n!$$

Therefore,

$$(1+x)^{-1} = 1 - x + x^2 - x^3 + \dots = \sum_{n=0}^{\infty} (-1)^n x^n \in \widehat{\mathbb{Q}}[x] \quad (24.3.5)$$

This is a multiplicative inverse of $(1+x)$ in $\widehat{\mathbb{Z}}[x]$ (also in $\widehat{\mathbb{Q}}[x]$).

2. Second Method: Long Division

Use long division to divide $\frac{1}{1+x}$:

$$\begin{array}{r}
 1 + x \left[\begin{array}{cccccc}
 1 & - & x & + & x^2 & - & x^3 & + & \cdots \\
 1 & + & 0x & + & 0x^2 & + & 0x^3 & + & \cdots \\
 \hline
 -1 & + & -x & & & & & & \\
 & & -x & + & 0x^2 & & & & \\
 & & +x & + & x^2 & & & & \\
 & & & & \hline
 & & & & x^2 & + & 0x^3 & & \\
 & & & & -x^2 & - & x^3 & & \\
 & & & & & & \hline
 & & & & & & -x^3 & + & \cdots \\
 & & & & & & & & \vdots
 \end{array} \right.
 \end{array}$$

3. Third Method: Linear Recurrence Relation:

We want:

$$1 = (a + x) \sum_{n=0}^{\infty} a_n x^n = 1 + 0x + 0x^2 + \cdots$$

Use distributive law:

$$\begin{aligned}
 1 &= a \sum_{n=0}^{\infty} a_n x^n + x \sum_{n=0}^{\infty} a_n x^n && \text{distributive law} \\
 &= \sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} a_n x^{n+1} && \text{simplify} \\
 &= \sum_{n=0}^{\infty} a_n x^n + \sum_{n=1}^{\infty} a_{n-1} x^n && \text{change second summation index} \\
 &= a_0 + \sum_{n=1}^{\infty} a_n x^n + \sum_{n=1}^{\infty} a_{n-1} x^n && \text{separate one term from sum} \\
 &= a_0 + \sum_{n=1}^{\infty} (a_n x^n + a_{n-1} x^n) && \text{combine two sums} \\
 &= a_0 + \sum_{n=1}^{\infty} (a_n + a_{n-1}) x^n && \text{factor out } x_n
 \end{aligned}$$

Now we can write:

$$1 + 0x + 0x^2 + \cdots = a_0 + \sum_{n=1}^{\infty} (a_n + a_{n-1})x^n$$

Equate like powers of x for the two polynomials:

$$\begin{aligned} 1 &= a_0 \\ 0 &= a_1 + a_0 = a_1 + 1 \Rightarrow a_1 = -1 \\ 0 &= a_2 + a_1 = a_2 - 1 \Rightarrow a_2 = 1 \\ 0 &= a_3 + a_2 = a_3 + 1 \Rightarrow a_3 = -1 \\ 0 &= a_4 + a_3 = a_4 - 1 \Rightarrow a_4 = 1 \\ &\vdots \\ 0 &= a_n + a_{n-1} \Rightarrow a_n = (-1)^n \end{aligned}$$

◆

Exercise 24.3.6. Find the inverse of $a + x$ in $\widehat{\mathbb{Q}}[x]$ by the:

1. long division method
2. recurrence relation method

◇

Exercise 24.3.7. Find the inverse of $1 + x$ in $\widehat{\mathbb{Z}}_2[x]$ by the:

- (a) long division method
- (b) recurrence relation method

◇

Exercise 24.3.8. Find the inverse of $3 + 2x$ in $\widehat{\mathbb{Z}}_5[x]$ by the:

- (a) long division method

(b) recurrence relation method

◇

Exercise 24.3.9. Find the multiplicative inverse of $(1 + 2x + 3x^2)$ in $\widehat{\mathbb{Z}}_5[x]$, in $\widehat{\mathbb{Z}}_7[x]$, and in $\widehat{\mathbb{Q}}[x]$ by the:

(a) long division method

(b) recurrence relation method

◇

◆

24.4 Product Rings

In certain situations, we may want to combine two or more rings to form a larger ring. Product rings allow us to do just that. In fact, the product operation for rings is very similar to the product of groups (see Definition 15.2.13).

Definition 24.4.1. If R_1, R_2 are rings, then the *product ring*, $R_1 \times R_2$ is the set of pairs (a, b) , $a \in R_1$ and $b \in R_2$, with the following operations:

1. $(a, b) + (c, d) = (a +_1 c, b +_2 d)$
2. $(a, b) \cdot (c, d) = (a \cdot_1 c, b \cdot_2 d)$

where $+_1, \cdot_1$ is the addition and multiplication for R_1 and $+_2, \cdot_2$ is the addition and multiplication for R_2

△

How do we know that the product ring is a ring? As with any ring, we must show that the seven ring properties hold true.

PROOF.

(I) Closure:

- (a) Additive closure: If (a, b) , and (c, d) are in $R_1 \times R_2$, then $(a, b) + (c, d)$ is also in $R_1 \times R_2$.

$$\begin{aligned} (a, b) + (c, d) &= (a +_1 c, b +_2 d) && \text{Def. of product add.} \\ a +_1 c &\in R_1 \text{ and } b +_2 d \in R_2 && \text{Closure of } R_1, R_2 \\ (a +_1 c, b +_2 d) &\in R_1 \times R_2 && \text{Definition of } R_1 \times R_2 \end{aligned}$$

- (b) Multiplicative closure: If (a, b) and (c, d) are in $R_1 \times R_2$, then $(a, b)(c, d)$ is also in $R_1 \times R_2$.

$$\begin{aligned} (a, b)(c, d) &= (a \cdot_1 c, b \cdot_2 d) && \text{Def. of product mult.} \\ a \cdot_1 c &\in R_1 \text{ and } b \cdot_2 d \in R_2 && \text{Closure of } R_1 \text{ and } R_2 \\ (a \cdot_1 c, b \cdot_2 d) &\in R_1 \times R_2 && \text{Definition of } R_1 \times R_2 \end{aligned}$$

(II) Associativity:

- (a) Associativity of Addition: For $(a, b), (c, d), (e, f) \in R_1 \times R_2$,
 $((a, b) + (c, d)) + (e, f) = (a, b) + ((c, d) + (e, f))$.

$$\begin{aligned} &((a, b) + (c, d)) + (e, f) \\ &= ((a +_1 c) +_1 e, (b +_2 d) +_2 f) && \text{Def. of product add.} \\ &= (a +_1 (c +_1 e), b +_2 (d +_2 f)) && \text{Assoc. of add. in } R_1 \times R_2 \\ &= (a, b) + ((c, d) + (e, f)) && \text{Def. of product addition} \end{aligned}$$

- (b) Associativity of Multiplication: For $(a, b), (c, d), (e, f) \in R_1 \times R_2$,
 $((a, b)(c, d))(e, f) = (a, b)((c, d)(e, f))$.

We leave this part of the proof as an exercise.

Exercise 24.4.2. Prove the associative property of multiplication for $R_1 \times R_2$. \diamond

- (III) Commutativity of Addition: For all $a, b, c \in R_1 \times R_2$,
 $(a, b) + (c, d) = (c, d) + (a, b)$.

$$\begin{aligned} (a, b) + (c, d) &= (a +_1 c, b +_2 d) && \text{Definition of product addition} \\ &= (c +_1 a, d +_2 b) && \text{Commutativity of } +_1 \text{ and } +_2 \\ &= (c, d) + (a, b) && \text{Definition of product addition} \end{aligned}$$

(IV) Zero: Show that the additive identity for $R_1 \times R_2$ is $(0_1, 0_2)$.

$$\begin{aligned} (a, b) + (0_1, 0_2) &= (a +_1 0_1, b +_2 0_2) && \text{Definition of product addition} \\ &= (a, b) && \text{Additive identities for } R_1 \text{ and } R_2 \\ (0_1, 0_2) + (a, b) &= (a, b) && \text{(similar to above)} \end{aligned}$$

(V) One: Show that the multiplicative identity for $R_1 \times R_2 = (1_1, 1_2)$.

The proof of this property is left as an exercise.

Exercise 24.4.3. Prove that the multiplicative identity for $R_1 \times R_2 = (1_1, 1_2)$. \diamond

(VI) Additive inverse: The additive inverse of $(a, b) = (-a, -b)$.

$$\begin{aligned} (a, b) + (-a, -b) &= (a +_1 -a, b +_2 -b) && \text{Def. of product addition} \\ &= (0_1, 0_2) && \text{Additive inverses of } R_1 \text{ and } R_2 \\ &= \text{additive identity of } R_1 \times R_2 && \text{proven in part(IV)} \end{aligned}$$

(VII) Distributive property: For $(a, b), (c, d), (e, f) \in R_1 \times R_2$:

- $(a, b)((c, d) + (e, f)) = (a, b)(c, d) + (a, b)(e, f)$ and
- $((c, d) + (e, f))(a, b) = (c, d)(a, b) + (e, f)(a, b)$.

Exercise 24.4.4. Prove the distributive property for the product ring $R_1 \times R_2$. \diamond

\square

Exercise 24.4.5. Give the addition and multiplication tables for the following product rings:

1. $\mathbb{Z}_2 \times \mathbb{Z}_2$ with elements: $\{(0, 0), (0, 1), (1, 0), (1, 1)\}$
2. $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2$ with elements: $\{0, 0, 0), (0, 0, 1), \text{etc}\}$
3. $\mathbb{Z}_2 \times \mathbb{Z}_3$ (6 elements)

\diamond

24.5 Isomorphic rings

Sometimes we encounter rings that are basically the “same”. In this section we will give a mathematical definition for what the “same” means in this context. Before we give the definition, we will start out with an example.

Example 24.5.1. Consider the two rings $R_1 = \mathbb{Z}[x]$ and $R_2 = \mathbb{Z}[y]$. Obviously, these two rings are basically the same except we replace x with y . We can make a formal correspondence between the two rings by defining a function $\phi : R_1 \rightarrow R_2$ as follows: $\phi(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) = (a_n y^n + a_{n-1} y^{n-1} + \dots + a_0)$. Note that ϕ is a bijection because it has an inverse (see Proposition 8.7.11). Additionally, ϕ preserves the operations of addition and multiplication: $\phi(x+y) = \phi(x) + \phi(y)$ and $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$. In other words, ϕ gives us a way to “translate” every operation we do in R_1 to a corresponding operation in R_2 . \blacklozenge

The above example may seem trivial, but it turns out that in some cases similar construction can make deep connections between rings that seem quite different:

Example 24.5.2. Consider the function $\phi : R_1 \rightarrow R_2$, where $R_1 = \{z = a + bi \in \mathbb{C}\}$, $R_2 = \left\{ A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbb{M}_2 \right\}$ and ϕ is defined as: $\phi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. We can see that ϕ is also a bijection since $\phi^{-1} \left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \right) = a + bi$, for all $A \in R_2$.

To further explore the structure of the function ϕ , let's consider two arbitrary elements of R_1 , say $z = a + bi$ and $w = c + di$. Using addition of complex numbers, then applying the ϕ function, we get

$$\begin{aligned} \phi(z + w) &= \phi(a + bi + c + di) \\ &= \phi((a + c) + (b + d)i) \\ &= \begin{bmatrix} a + c & b + d \\ -b - d & a + c \end{bmatrix}. \end{aligned}$$

We get the same result if we first apply the ϕ function on z and w , then use addition of matrices:

$$\begin{aligned}\phi(z) + \phi(w) &= \phi(a + bi) + \phi(c + di) \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \begin{bmatrix} a + c & b + d \\ -b - d & a + c \end{bmatrix}.\end{aligned}$$

In other words, $\phi(z +_1 w) = \phi(z) +_2 \phi(w)$, where $+_1$ and $+_2$ are addition as defined by R_1 and R_2 , respectively. But what about multiplication?

Let's consider z and w as defined earlier. We can see that

$$\begin{aligned}\phi(z \cdot w) &= \phi((a + bi) \cdot (c + di)) \\ &= \phi((ac - bd) + (ad + bc)i) \\ &= \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}.\end{aligned}$$

Note that multiplication of complex numbers was used here. Also,

$$\begin{aligned}\phi(z) \cdot \phi(w) &= \phi(a + bi) \cdot \phi(c + di) \\ &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \\ &= \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix},\end{aligned}$$

where multiplication of matrices was used. So, $\phi(z \cdot_1 w) = \phi(z) \cdot_2 \phi(w)$, where \cdot_1 and \cdot_2 are multiplication as defined by R_1 and R_2 , respectively. \blacklozenge

The two examples above show how we can relate different rings that have the same structure. In both examples we use a bijection that preserves the addition and multiplication operations to make a correspondence between two rings. We may generalize this type of bijection as follows.

Definition 24.5.3. Let $\phi : R_1 \rightarrow R_2$ be a bijection between rings R_1 and R_2 . We say that ϕ is an *isomorphism* from R_1 to R_2 if the following two equations are satisfied for all $x, y \in R_1$:

$$\phi(x +_1 y) = \phi(x) +_2 \phi(y) \tag{24.5.4}$$

$$\phi(x \cdot_1 y) = \phi(x) \cdot_2 \phi(y) \quad (24.5.5)$$

Two rings R_1 and R_2 are called *isomorphic* if there exists an isomorphism from R_1 to R_2 . \triangle

Exercise 24.5.6. Show that isomorphism is an equivalence relation on rings: that is show that isomorphism satisfies the reflexive, symmetric and transitive properties. \diamond

Exercise 24.5.7. Let $\phi : R_1 \rightarrow R_2$, where $R_1 = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ and $R_2 = \left\{ \begin{bmatrix} a & b\sqrt{2} \\ b\sqrt{2} & a \end{bmatrix} \in \mathbb{M}_2 \right\}$. Prove or disprove that ϕ is an isomorphism. \diamond

Example 24.5.8. Show that $f : \mathbb{C} \rightarrow \mathbb{C}$ is an isomorphism, where f maps every element of \mathbb{C} to its complex conjugate in \mathbb{C} . In other words, if $z = a + bi \in \mathbb{C}$, where $a, b \in \mathbb{R}$, then $f(z) = a - bi \in \mathbb{C}$.

PROOF. In order for f to be an isomorphism, we must first show that the sets are indeed rings and that the function f is a bijection. Then we must show that the two equations above are true for all $z, w \in \mathbb{C}$. At the beginning of this chapter, we concluded that \mathbb{C} satisfies all seven properties of a ring. Also, given any $w = a - bi \in \mathbb{C}$, $f^{-1}(w) = a + bi \in \mathbb{C}$. So f is a bijection.

As we continue, remember that $+_1, \cdot_1$ and $+_2, \cdot_2$ refer to addition and multiplication as defined by the first and second rings, respectively. In our case, both additions are regular complex addition and both multiplications are regular complex multiplication. So we will use $+$ to represent both $+_1$ and $+_2$ and similarly for \cdot .

(1) First we must show that $f(z + w) = f(z) + f(w)$, for any $z, w \in \mathbb{C}$. We begin with our two arbitrary elements of \mathbb{C} , $z = a + bi$ and $w = c + di$,

where $a, b, c, d \in \mathbb{R}$. Then

$$\begin{aligned} f(z + w) &= f((a + bi) + (c + di)) \\ &= f((a + c) + (b + d)i) \\ &= (a + c) - (b + d)i \\ &= a + c - bi - di \\ &= (a - bi) + (c - di) \\ &= f(z) + f(w). \end{aligned}$$

So property one of isomorphisms is satisfied.

- (2) Secondly, we must show that $f(z \cdot w) = f(z) \cdot f(w)$. Using z and w as defined above,

$$\begin{aligned} f(z \cdot w) &= f((a + bi) \cdot (c + di)) \\ &= f((ac - bd) + (ad + bc)i) \\ &= (ac - bd) - (ad + bc)i. \end{aligned}$$

On the other hand,

$$\begin{aligned} f(z) \cdot f(w) &= f(a + bi) \cdot f(c + di) \\ &= (a - bi)(c - di) \\ &= (ac - bd) - (ad + bc)i \end{aligned}$$

This shows $f(z \cdot w) = f(z) \cdot f(w)$, so property two of isomorphisms is satisfied.

□

◆

Note that there can be more than one isomorphism between two rings.

Exercise 24.5.9. In Example 24.5.8 we gave an isomorphism from \mathbb{C} to itself. Give another example of an isomorphism from \mathbb{C} to itself. (*Hint:* Make your example as easy as possible.) ◇

Exercise 24.5.10. Given $\phi : \mathbb{Q}[x, y] \rightarrow \mathbb{Q}[x, y]$, defined by $\phi(p(x, y)) = p(y, x)$:

- (a) Show that ϕ is an isomorphism.
- (b) Give another isomorphism between $\mathbb{Q}[x, y]$ and $\mathbb{Q}[x, y]$.

◇

When we restrict the isomorphism, so that $R_1 = R_2$, we have a special type of isomorphism known as an *automorphism*.

Definition 24.5.11. A *ring automorphism* is a ring isomorphism whose domain is equal to its range. △

Example 24.5.12. Show that $f(a + bi) = a - bi$ is a ring automorphism from \mathbb{C} to \mathbb{C} .

We showed in Example 24.5.8 that this function is a ring isomorphism. It should be clear that the domain and range of f are the same, so f is also a ring automorphism. ◆

Exercise 24.5.13. Consider the function $f((a, b, c)) = (a, -b, c)$, where $a, b, c \in \mathbb{R}$.

- (a) show that f is a homomorphism by proving that:
- (1) $f((a, b, c) + (d, e, f)) = f((a, b, c)) + f((d, e, f))$, and
 - (2) $f((a, b, c) \cdot (d, e, f)) = f((a, b, c)) \cdot f((d, e, f))$.
- (b) Is f an isomorphism? (*Hint*)
- (c) Is f an automorphism?

◇

24.6 Ring homomorphisms: kernels, and ideals

As we have seen above, ring isomorphisms are functions that are bijections and preserve the additive and multiplicative operations. It is possible to have functions that are not bijections but still preserve the additive and

multiplicative operations. One important example is a function that we are very familiar with:

Example 24.6.1. Define the function $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ defined by $f(x) = \text{mod}(x, n)$, where n is a fixed integer > 1 . In Proposition 5.4.4 we showed that for any $\ell, m \in \mathbb{Z}$ we have:

$$(a) \text{ mod}(\ell + m, n) = \text{mod}(\ell, n) \oplus \text{mod}(m, n), \text{ and}$$

$$(b) \text{ mod}(\ell \cdot m, n) = \text{mod}(\ell, n) \odot \text{mod}(m, n).$$

We may rewrite these equations in terms of f as $f(\ell + m) = f(\ell) \oplus f(m)$ and $f(\ell \cdot m) = f(\ell) \odot f(m)$. \blacklozenge

We may generalize this example with the following definition.

Definition 24.6.2. A function $f : R_1 \rightarrow R_2$ between rings R_1, R_2 is called a *ring homomorphism* if f has the following properties:

$$f(\ell +_1 m) = f(\ell) +_2 f(m) \tag{24.6.3}$$

and

$$f(\ell \cdot_1 m) = f(\ell) \cdot_2 f(m). \tag{24.6.4}$$

\triangle

Notice that a homomorphism is an isomorphism without the bijection requirement. Figure 24.6.1 shows the relationship between homomorphisms, isomorphisms and automorphisms.

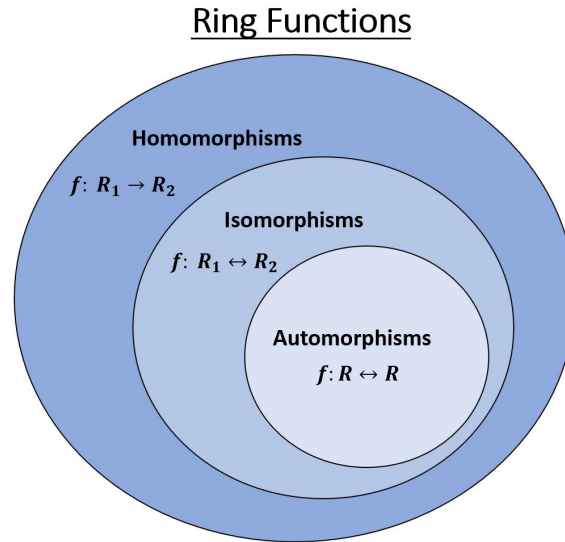


Figure 24.6.1. Ring Functions

Following are a number of examples of ring homomorphisms.

Example 24.6.5. Prove or disprove that $f: \mathbb{Q} \rightarrow \mathbb{Q}$ defined by $f(x) = 2x$ is a ring homomorphism.

PROOF. f is *not* a homomorphism since it does not follow Equation 24.6.4: For example, $f(1 \cdot 1) = 2(1 \cdot 1) = 2$ but $f(1) + f(1) = 2(1) \cdot 2(1) = 4$. Many other counterexamples can be found.

□



Example 24.6.6. Prove or disprove that $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_3$ defined by: $f(x) = \text{mod}(x, 3)$ is a ring homomorphism.

PROOF. f is a homomorphism since,

$$f(x +_6 y) = \text{mod}(x +_6 y, 3) = \text{mod}(x, 3) +_3 \text{mod}(y, 3),$$

where $+_n$ is addition in \mathbb{Z}_n , and

$$f(x \cdot_6 y) = \text{mod}(x \cdot_6 y, 3) = \text{mod}(x, 3) \cdot_3 \text{mod}(y, 3),$$

where \cdot_n is multiplication in \mathbb{Z}_n

□

◆

Exercise 24.6.7. Given integers $m, n > 1$, define $g : \mathbb{Z}_{mn} \rightarrow \mathbb{Z}_n$ defined by $g(x) = \text{mod}(x, n)$. Show that g is a homomorphism. ◇

Example 24.6.8. Prove or disprove that $f : \mathbb{R}[x] \rightarrow \mathbb{R}$, defined by $f(p(x)) = p(0)$, is a homomorphism. (Note that this function maps a polynomial to its constant term.)

PROOF. We will divide this proof into two parts, one for each property of ring homomorphisms:

(a) Let $p(x), q(x)$ be arbitrary elements of $\mathbb{R}[x]$, where $p(x)$ and $q(x)$ have constant terms of $a_0, b_0 \in \mathbb{R}$, respectively. Then $p(x) +_1 q(x)$ is some polynomial in $\mathbb{R}[x]$, with a constant term equal to $a_0 + b_0$. So,

$$f(p(x) +_1 q(x)) = a_0 + b_0.$$

$$\text{Also, } f(p(x)) +_2 f(q(x)) = a_0 + b_0.$$

The first ring homomorphism property holds. Let's look at the second property:

(b) $p(x) \cdot_1 q(x)$ is some polynomial in $\mathbb{R}[x]$, with a constant term equal to $a_0 \cdot b_0$. So,

$$f(p(x) \cdot_1 q(x)) = a_0 \cdot b_0.$$

$$\text{Also, } f(p(x)) \cdot_2 f(q(x)) = a_0 \cdot b_0.$$

So, the second ring homomorphism property holds and we can say that f is a ring homomorphism.

□

◆

The homomorphism in Example 24.6.8 is just one example of an important class of homomorphisms.

Exercise 24.6.9. Give $a \in \mathbb{Q}$ define the function $f_a : \mathbb{Q}[x] \rightarrow \mathbb{Q}$ by $f_a(p(x)) = p(a)$. For what values of a is f_a a homomorphism? ◇

Exercise 24.6.10. Define the function $f : \mathbb{R}[x] \rightarrow C_3(\mathbb{R})$ by

$$f(a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0) = a_n B^n + a_{n-1} B^{n-1} + \cdots + a_0,$$

where $B = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$.

- (a) Show that f is onto. You may show this by showing that for any matrix $A \in C_3(\mathbb{R})$ there exists some $p(x) \in \mathbb{R}[x]$ such that $f(p(x)) = A$.

◇

24.6.1 Homomorphism kernels and ideals

When we discussed homomorphisms of groups, we introduced the notion of the kernel of a homomorphism. According to Definition 22.3.3, the kernel of a group homomorphism is the inverse image of the identity element of the codomain. We may make a similar definition for ring homomorphisms.

Definition 24.6.11. If $f : R_1 \rightarrow R_2$ is a ring homomorphism, then the set $\{x \in R_1 \mid f(x) = 0\}$ is called the **kernel** of f , notated $\text{Ker}(f)$. \triangle

Example 24.6.12. Find the kernel of $f : \mathbb{R}[x] \rightarrow \mathbb{R}$, given by $f(p(x)) = p(0)$.

We are looking for the set of all $p(x)$ such that $p(0) = 0$. We know from the polynomials chapter that $p(0) = 0$ implies that x divides $p(x)$. (So, there is no constant term!) In summary, $\text{Ker}(f) = \{xp(x) : p(x) \in \mathbb{R}[x]\}$. \blacklozenge

Exercise 24.6.13. Given $f_a : \mathbb{Q}[x] \rightarrow \mathbb{Q}$, where $f_a(p(x)) = p(a)$. Find $\text{Ker}(f_a)$. \diamond

Exercise 24.6.14. In Exercise 24.6.10, we defined a function $f : \mathbb{R}[x] \rightarrow C_3(\mathbb{R})$.

- (a) For what values of a is $x^3 + a$ in $\text{Ker}(f)$?
- (b) Consider the polynomial $p(x) = (x^3 - 1) \cdot q(x) + a_2x^2 + a_1x + a_0$. Show that $p(x) \in \text{Ker}(f)$ if and only if $a_0 = a_1 = a_2 = 0$.

◇

We saw previously that the kernel of a group homomorphism is always a subgroup of the domain (see Proposition 22.3.4). We may ask the same question of rings: Given a ring homomorphism f , is $\text{Ker}(f)$ also a ring?

Exercise 24.6.15.

- (a) Given the homomorphism f defined in Example 24.6.1, show that $f^{-1}(0)$ is *not* a ring. Which properties fail?
- (b) Given the same example, show that $f^{-1}(1)$ is *also not* a ring. Which ring properties fail?

◇

Although the set $f^{-1}(0)$ is not a ring, nonetheless it does have some nice properties.

Exercise 24.6.16. Given the function f defined in Example 24.6.1, and let $S = f^{-1}(0)$.

- (a) Show that if $a, b \in S$, then $a + b \in S$. In other words, S is closed under addition.
- (b) Show that if $a, b \in S$, then $a \cdot b \in S$. In other words, S is closed under multiplication.
- (c) Show that if $a \in S$, then $-a \in S$. In other words, S is closed under additive inverse.

◇

The following proposition generalizes the results in Exercise 24.6.16.

Proposition 24.6.17. The kernel of a homomorphism $f : R_1 \rightarrow R_2$ satisfies the following properties:

1. If $a, b \in f^{-1}(0)$, then $a + b \in f^{-1}(0)$.
2. If $a \in f^{-1}(0)$ and $b \in R_1$ then $ab \in f^{-1}(0)$.

3. $0 \in f^{-1}(0)$.
 4. If $a \in f^{-1}(0)$, then $-a \in f^{-1}(0)$.

PROOF.

1.

$$\begin{array}{ll}
 a, b \in f^{-1}(0) & \text{given} \\
 f(a) = 0, f(b) = 0 & \text{def. of inverse} \\
 f(a + b) = f(a) + f(b) & \text{def. of homomorphism} \\
 f(a + b) = 0 + 0 = 0 & \text{substitution \& zero property} \\
 a + b \in f^{-1}(0) & \text{def. of inverse}
 \end{array}$$

2.

$$\begin{array}{ll}
 a \in f^{-1}(0), b \in R_1 & \text{given} \\
 f(a) = 0 & \text{def. of inverse} \\
 f(a \cdot b) = f(a)f(b) & \text{def. of homomorphism} \\
 f(a \cdot b) = 0 \cdot f(b) = 0 & \text{substitution \& Prop. 24.1.22} \\
 ab \in f^{-1}(0) & \text{def. of inverse}
 \end{array}$$

3.

$$\begin{array}{ll}
 f(a) = f(a + 0) & \text{additive identity} \\
 f(a + 0) = f(a) + f(0) & \text{def. of homomorphism} \\
 f(a) = f(a) + f(0) & \text{substitution} \\
 -f(a) + f(a) = -f(a) + f(a) + f(0) & \text{substitution} \\
 0 = 0 + f(0) & \text{additive inverse} \\
 0 = f(0) & \text{additive identity} \\
 0 \in f^{-1}(0) & \text{def. of inverse}
 \end{array}$$

4.

| | |
|-----------------------|----------------------|
| $a \in f^{-1}(0)$ | given |
| $f(a) = 0$ | def. of inverse |
| $-a \in R_1$ | def. of homomorphism |
| $f(0) = f(a + (-a))$ | additive inverse |
| $f(0) = f(a) + f(-a)$ | def. of homomorphism |
| $f(0) = 0$ | proven above |
| $0 = 0 + f(-a)$ | substitution |
| $0 = f(-a)$ | additive identity |
| $-a \in f^{-1}(0)$ | def. of inverse |

□

Any set J which has properties (1-4) is called an *ideal*. We formalize the definition of ideal as follows.

Definition 24.6.18. Given a ring R , suppose $J \subset R$ satisfies the following properties:

- (a) J is closed under the ring's additive operation: in other words if $j_1, j_2 \in J$ then $j_1 + j_2 \in J$.
- (b) J is closed under multiplication by elements in R : in other words, if $j \in J$ and $r \in R$ then $rj \in J$.
- (c) J is closed under additive inverse in R .

Then J is called an *ideal* of R .

△

Exercise 24.6.19. In Example we showed the property that for any homomorphism $f : R_1 \rightarrow R_2$, we have $0_1 \in \text{Ker}(f)$. Using Definition 24.6.18, show that for any ideal J the zero element is an element of J . ◇

In view of Definition 24.6.18, we may restate Proposition 24.6.17 as follows.

Proposition 24.6.20. The kernel of a homomorphism is always an ideal.

Exercise 24.6.21. Find the kernel for the functions in Examples 24.6.5 and 24.6.6, and Exercise 24.6.7. Determine whether or not these kernels are ideals. \diamond

Example 24.6.22. Let $f : \mathbb{Z} \rightarrow \mathbb{Z}_7$ be defined by $f(x) = \text{mod}(x, 7)$

- (a) Prove or disprove f is a ring homomorphism.
- (b) What is the kernel of f ?
- (c) Is $\text{Ker}(f)$ an ideal?

(a) To determine whether f is a ring homomorphism, we must verify Equations (24.6.3) and (24.6.4):

$$\begin{aligned} f(x + y) &= \text{mod}(x + y, 7) = \text{mod}(x, 7) +_7 \text{mod}(y, 7) && \text{definition of } +_7 \\ &= f(x) +_7 f(y) && \text{definition of } f \end{aligned}$$

Also,

$$\begin{aligned} f(x \cdot y) &= \text{mod}(x \cdot y, 7) = \text{mod}(x, 7) \cdot_7 \text{mod}(y, 7) && \text{definition of } \cdot_7 \\ &= f(x) \cdot_7 f(y) && \text{definition of } f \end{aligned}$$

It follows that f is a ring homomorphism.

- (b) Remember that the kernel is the set $\{x \in R \mid f(x) = 0\}$. If $f(x) = 0$, then x is a multiple of 7. So, the kernel of f is $\{x \mid x = 7n, n \in \mathbb{Z}\}$.
- (c) Proposition 24.6.20 shows that $\text{Ker}(f)$ must be an ideal. You may also show the three properties directly.

Exercise 24.6.23. Show that $\text{Ker}(f)$ is closed under addition, multiplication, and additive inverse. \diamond

\blacklozenge

Exercise 24.6.24. Look back at Proposition 5.4.4. What is the relationship between this proposition and part(a) of Example 24.6.22? \diamond

Exercise 24.6.25. Let $f : \mathbb{C} \rightarrow \mathbb{R}$ be defined by $f(a + bi) = a$.

- (a) Prove or disprove: f is a ring homomorphism:
- (b) What is the kernel of f ?
- (c) Is $\text{Ker}(f)$ an ideal?

◇

Exercise 24.6.26. Let $f : \mathbb{C} \rightarrow \mathbb{R}$ be defined by: $f(a + bi) = b$.

- (a) Prove or disprove that f is a ring homomorphism.
- (b) What is the kernel of f ?
- (c) Is $\text{Ker}(f)$ an ideal?

◇

Exercise 24.6.27. Let $f : \mathbb{Z}_2 \times \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ be defined by: $f(a, b) = a$. (Remember that $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$).

- (a) Prove or disprove: f is a ring homomorphism.
- (b) Find the kernel of f .
- (c) Determine if $\text{Ker}(f)$ is an ideal.

◇

Exercise 24.6.28. Let $f : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$ be defined by: $f(a, b) = b$

- (a) Prove or disprove: f is a ring homomorphism.
- (b) Find the kernel of f .
- (c) Determine if the kernel of f is an ideal.

◇

24.7 Further properties of ideals and principal ideals

We arrived at the concept of ‘ideal’ by studying kernels of ring homomorphisms. It turns out that ideals are objects of interest in their own right, without any reference to homomorphisms. In the following, we will investigate some additional properties of ideals.

Example 24.7.1. Given the ring \mathbb{Z} and $J = \{0, 7, 14, 21, \dots\}$. Prove or disprove J is an ideal. \blacklozenge

PROOF. We can see that $J \subset \mathbb{Z}$, and J is closed under addition however J fails properties (b) and (c). \square

Exercise 24.7.2. Give examples that show the set J in Example 24.7.1 fails to satisfy properties (b) and (c). \blacklozenge

Exercise 24.7.3.

- (a) Given a ring R show that every ideal in R is a group under the ring’s additive operation.
- (b) Give an example of a ring which has an additive subgroup that is not an ideal.

\blacklozenge

Exercise 24.7.4. Show that condition (c) in Definition 24.6.18 is not really necessary: in other words, show that conditions (a) and (b) imply (c). \blacklozenge

In Exercise 15.6.7 we showed that the intersection of subgroups is also a subgroup. It turns out the same is true for ideals:

Proposition 24.7.5. The intersection of ideals is an ideal.

Exercise 24.7.6. Prove Proposition 24.7.5. \blacklozenge

We will now look at an important class of ideals.

Definition 24.7.7. If $a \in R$, then the *set generated by a* is
 $Ra \equiv \{ra, r \in R\}$ △

Proposition 24.7.8. For every $a \in R$, the set Ra is an ideal.

Exercise 24.7.9. Prove Proposition 24.7.8 by showing that Ra satisfies all properties of an ideal. ◇

Definition 24.7.10. A *principal ideal* is an ideal that is generated by a single element. In other words, $Ra \equiv \{ra, r \in R\}$ is a *principal ideal*. △

Exercise 24.7.11. Show that every ring R is also a principal ideal. (**Hint**)
◇

Example 24.7.12. Consider the ring of integers \mathbb{Z} . Then $2\mathbb{Z} = \{0, \pm 2, \pm 4, \dots\}$ is a principal ideal and is generated by 2. In fact, for any integer k , the set $k\mathbb{Z} = \{0, \pm k, \pm 2k, \dots\}$ is a principal ideal. ◆

Not all ideals are principal ideals.

Example 24.7.13. $\mathbb{Z}[x] : J \equiv \{2p(x) + xq(x), p(x), q(x) \in \mathbb{Z}[x]\}$

Show that J is an ideal, but not a principal ideal.

PROOF.

| | |
|--|---------------------------|
| $2 \in J$ and $x \in J$ | definition of J |
| Suppose $J = a\mathbb{Z}[x]$ for some $a \in \mathbb{Z}[x]$ | supposition |
| Since $2 \in J$, $a = 1$ or $a = 2$ | only elements to divide 2 |
| If $a = 1$, then $1\mathbb{Z}[x] = \mathbb{Z}[x] \neq J$ | |
| If $a = 2$, then $x \notin 2\mathbb{Z}[x]$. So $2\mathbb{Z}[x] \neq J$ | x has no even coef. |

Therefore, there does not exist an a such that $a \in \mathbb{Z}[x] = J$. Which means J is not a principal ideal by the definition of principal ideal. □ ◆

24.8 Quotient Rings

Quotient rings allow us to form a ring of equivalence classes, much like quotient groups studied in Chapter 18. Follow the next example to make sense of this concept.

Example 24.8.1. Define $f : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_5$ by $f(n) = \text{mod}(n, 5)$.

- (a) Show that f is a ring homomorphism.
- (b) Find the kernel of f .
- (c) Find $f^{-1}(m)$ for all $m \in \mathbb{Z}_5$.

(a)

$$\begin{aligned} f(a + b) &= \text{mod}(a + b, 5) = \text{mod}(a, 5) + \text{mod}(b, 5) = f(a) + f(b) \\ \text{and } f(ab) &= \text{mod}(ab, 5) = \text{mod}(a, 5) \text{ mod } (b, 5) = f(a)f(b). \end{aligned}$$

So f is a ring homomorphism.

- (b) The $\text{Ker}(f)$ is $f^{-1}(0) = \{0, 5\}$.

(c)

$$\begin{aligned} f^{-1}(0) &= \text{the set of all } n \in \mathbb{Z}_{10} \text{ such that } f(n) = 0 = \{0, 5\} \\ f^{-1}(1) &= \text{the set of all } n \in \mathbb{Z}_{10} \text{ such that } f(n) = 1 = \{1, 6\} \\ f^{-1}(2) &= \text{the set of all } n \in \mathbb{Z}_{10} \text{ such that } f(n) = 2 = \{2, 7\} \\ f^{-1}(3) &= \text{the set of all } n \in \mathbb{Z}_{10} \text{ such that } f(n) = 3 = \{3, 8\} \\ f^{-1}(4) &= \text{the set of all } n \in \mathbb{Z}_{10} \text{ such that } f(n) = 4 = \{4, 9\}. \end{aligned}$$

Notice that $f^{-1}(0) \cup f^{-1}(1) \cup f^{-1}(2) \cup f^{-1}(3) \cup f^{-1}(4) = \mathbb{Z}_{10}$ and $f^{-1}(m) \cap f^{-1}(n) = \emptyset$ if $m \neq n$.

We may recall the definition of *partition* from Section 17.2 (Definition 17.2.1), which we repeat here for convenience.

Definition 24.8.2. A *partition* of a set S is a set of subsets A_1, \dots, A_n such that:

- (a) $\cup_{m=1}^n A_m = S$
 (b) $A_i \cap A_j = \emptyset$ whenever $i \neq j$

△

The sets $f^{-1}(0) \dots f^{-1}(4)$ are called *inverse images*. The inverse images of f divide \mathbb{Z}_{10} into *equivalence classes*. (Review Definition 17.4.2.) (Actually, we showed in Proposition 17.3.12 that the inverse images of a function always divide the domain into equivalence classes.)

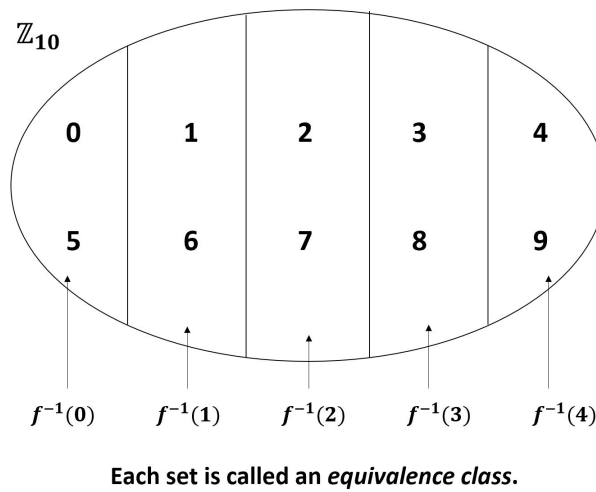


Figure 24.8.1. Equivalence classes

We can create an addition and multiplication table on the equivalence classes. For example: $\{4, 9\} + \{1, 6\}$:

$$\begin{aligned} 4 + 1 &= 5 \\ 9 + 1 &= 0 \\ 4 + 6 &= 0 \\ 9 + 6 &= 5 \end{aligned}$$

Addition table:

| | | | | | |
|--------|--------|--------|--------|--------|--------|
| + | {0, 5} | {1, 6} | {2, 7} | {3, 8} | {4, 9} |
| {0, 5} | {0, 5} | {1, 6} | {2, 7} | {3, 8} | {4, 9} |
| {1, 6} | {1, 6} | {2, 7} | {3, 8} | {4, 9} | {0, 5} |
| {2, 7} | {2, 7} | {3, 8} | {4, 9} | {0, 5} | {1, 6} |
| {3, 8} | {3, 8} | {4, 9} | {0, 5} | {1, 6} | {2, 7} |
| {4, 9} | {4, 9} | {0, 5} | {1, 6} | {2, 7} | {3, 8} |

Multiplication table:

| | | | | | |
|--------|--------|--------|--------|--------|--------|
| · | {0, 5} | {1, 6} | {2, 7} | {3, 8} | {4, 9} |
| {0, 5} | {0, 5} | {0, 5} | {0, 5} | {0, 5} | {0, 5} |
| {1, 6} | {0, 5} | {1, 6} | {2, 7} | {3, 8} | {4, 9} |
| {2, 7} | {0, 5} | {2, 7} | {4, 9} | {1, 6} | {3, 8} |
| {3, 8} | {0, 5} | {3, 8} | {1, 6} | {4, 9} | {2, 7} |
| {4, 9} | {0, 5} | {4, 9} | {3, 8} | {2, 7} | {1, 6} |

◆

The equivalence classes form a ring. This is our first example of a *quotient ring*. We write this ring as $\mathbb{Z}_{10}/\mathbb{Z}_5$. (Recall we used a similar notation for quotient groups.) We will formally define quotient rings below.

Definition 24.8.3. Let J be an ideal of ring R . The *quotient ring* of R by J is the set R/J consisting of all equivalence classes modulo J in R , together with binary operations $+$ and \cdot defined by the following:

$$(x + J) + (y + J) = (x + y) + J \text{ and}$$

$$(x + J) \cdot (y + J) = (x \cdot y) + J.$$

△

Exercise 24.8.4. The quotient ring $\mathbb{Z}_{10}/\mathbb{Z}_5$ is isomorphic to another ring that we are familiar with. Can you identify this familiar ring? (**Hint**) ◇

In the example above, we can say that $\mathbb{Z}_{10}/\mathbb{Z}_5$ is a quotient ring of \mathbb{Z}_{10} by \mathbb{Z}_5 with four elements: $\mathbb{Z}_{10}/\mathbb{Z}_5 = \{0 + \mathbb{Z}_5, 1 + \mathbb{Z}_5, 2 + \mathbb{Z}_5, 3 + \mathbb{Z}_5, 4 + \mathbb{Z}_5\}$.

Exercise 24.8.5. Define $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ by $f(a, b) = a$.

- (a) Show that f is a ring homomorphism.
- (b) What is the kernel of f ?
- (c) What are the inverse images of f ?
- (d) Use the definition of partition to show that the inverse images form a partition of the domain of f .
- (e) Make an addition and multiplication tables for the quotient ring, which consist of the inverse images.
- (f) What ring is isomorphic to the quotient ring? (**Hint**)

◇

24.9 Integral domains, Principal ideal domains and fields

In high school algebra, we learn that if $a \cdot b = 0$, then either $a = 0$ or $b = 0$. This real number property is helpful when solving polynomial equations. We will see that ring elements do not *always* follow this rule.

Definition 24.9.1. If $a, b \in R$ with $a \neq 0$, $b \neq 0$, and $ab = 0$, then a and b are called *zero divisors*. △

Before looking at general properties of zero divisors, let's look at some examples.

Example 24.9.2. In Z_{21} , $\{3, 6, 9, 12, 15, 18, 7, 14\}$ are all zero divisors, since: $3 \cdot 7 = 6 \cdot 7 = 9 \cdot 7 = 12 \cdot 7 = 15 \cdot 7 = 18 \cdot 7 = 14 \cdot 3 = 0$. ◆

Exercise 24.9.3. Find the zero divisors in Z_4 and Z_{15} . ◇

In general, in $Z_{p \cdot q}$, the elements $\{p, 2p, \dots, (q-1)p\}$ and $\{q, 2q, \dots, (p-1)q\}$ are all zero divisors.

Exercise 24.9.4. Which of the following rings have zero divisors: Z , R , C , and/or Q ? ◇

The zero divisor property is closely related to invertibility, as shown in the following proposition.

Proposition 24.9.5. Suppose that R is a ring, and suppose $a \in R$ has a multiplicative inverse. Then a is not a zero divisor—in other words, there is no $b \in R$ such that $b \neq 0$ and $ab = 0$.

Exercise 24.9.6. Prove Proposition 24.9.5(*Hint*) ◇

Many rings have no zero divisors, other than zero itself.

Definition 24.9.7. A commutative ring that has no zero divisors is called an *integral domain*. △

\mathbb{Z} , \mathbb{R} , \mathbb{C} , and \mathbb{Q} are all integral domains.

Example 24.9.8. Show that \mathbb{Z}_p is an integral domain if p is prime.

PROOF. We have shown in Example 24.1.3 that \mathbb{Z}_p is a commutative ring for all $p \in \mathbb{Z}$. It remains to show that \mathbb{Z}_p has no zero divisors. We will show this by contradiction.

Suppose \mathbb{Z}_p has a zero divisor $a \in \mathbb{Z}_p$ such that $a \neq 0$. Then by Definition 24.9.1, there is some $b \in \mathbb{Z}_p$ such that $b \neq 0$ and $a \odot b = 0$. So:

| | |
|-------------------------------------|--------------------|
| $a \odot b = \text{mod}(ab, p) = 0$ | Def. of \odot |
| p divides ab | Proposition 5.2.10 |
| p divides a or b | Euclid's Lemma |

But how can p divide a or b when $p > a$ and $p > b$? It is not possible. So our assumption that \mathbb{Z}_p has a zero divisor a is false. So \mathbb{Z}_p has no zero divisors and \mathbb{Z}_p is an integral domain. □ ◆

Example 24.9.9. Prove that $\mathbb{Q}[\sqrt[3]{2}]$ is an integral domain.

PROOF. In Example 24.1.4 we showed that $\mathbb{Q}[\sqrt[3]{2}]$ is a ring. It remains to show that $\mathbb{Q}[\sqrt[3]{2}]$ is commutative and contains no zero divisors. We know that elements of $\mathbb{Q}[\sqrt[3]{2}]$ are real numbers, which are commutative by nature. Thus, $\mathbb{Q}[\sqrt[3]{2}]$ inherits commutativity from the real numbers. Additionally,

real numbers have no zero divisors. So again, this property is inherited by $\mathbb{Q}[\sqrt[3]{2}]$ and we can conclude that $\mathbb{Q}[\sqrt[3]{2}]$ is an integral domain. \square \blacklozenge

Exercise 24.9.10. Prove that \mathbb{Z}_n is an integral domain if and only if n is prime. \diamond

Exercise 24.9.11. Let R and S be integral domains. Prove that $R \times S$ is also an integral domain. \diamond

Exercise 24.9.12. Prove or disprove:

- (a) The ring $M_2(R)$ is an integral domain.
- (b) The subring of $M_2(R)$ consisting of diagonal matrices is an integral domain. (By “diagonal matrix” we mean matrices of the form $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$).
- (c) The subring of $M_2(R)$ consisting of upper triangular matrices is an integral domain. (Upper triangular matrices have the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$).

\diamond

An important property of integral domain is the cancellation law of multiplication, as shown in the following proposition.

Proposition 24.9.13. Given integral domain D and $a, b, c \in D$. If $ab = ac$ and $a \neq 0$, then $b = c$.

PROOF.

$$\begin{array}{ll}
 ab = ac & \text{Given} \\
 ab - ac = 0 & \text{Substitution} \\
 a(b - c) = 0 & \text{Distributive Law}
 \end{array}$$

Since D is an integral domain, then D has no zero divisors. This means that $a = 0$ or $b - c = 0$. But we know that $a \neq 0$. So $b - c = 0$ and $b = c$. \square

In Definition 24.7.10 we learned that a principal ideal is generated by a single element of a ring, R . We can now combine this idea with that of the integral domain.

Definition 24.9.14. A *principal ideal domain* is an integral domain, all of whose ideals are principal. \triangle

It turns out that \mathbb{Z} , \mathbb{R} , \mathbb{C} , \mathbb{Q} , \mathbb{Z}_p , $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Q}[x]$, and $\mathbb{Z}_p[x]$ are all principal ideal domains. Unfortunately, we are not prepared to prove this here.²

Let's explore another important ring subset known as the *prime ideal*. We shall see that the concept of prime ideal is closely related to prime numbers.

Example 24.9.15. Suppose we are given the set $J \subset \mathbb{Z} : J = \{\dots, -12, -6, 0, 6, 12, \dots\}$. Prove or disprove that $p, q \in \mathbb{Z}$ and $p \cdot q \in J$ implies $p \in J$ or $q \in J$. \blacklozenge

PROOF. We can disprove this by counterexample. Consider, for example, $3, 4 \in \mathbb{Z}$. It is true that $3 \cdot 4 = 12 \in J$, but neither 3 nor 4 is in J . (Many other counterexamples can be found.) \square

Exercise 24.9.16.

- (a) Suppose $J = \{\dots, -14, -7, 0, 7, 14, \dots\}$ in the example above. Prove or disprove that $p, q \in \mathbb{Z}$ and $p \cdot q \in J$ implies $p \in J$ or $q \in J$.
- (b) Suppose $J = \{\dots, -2a, -a, 0, a, 2a, \dots\}$ for some $a \in \mathbb{Z}$ and $p, q \in \mathbb{Z}$. For what values of a is it true that $p \cdot q \in J$ implies $p \in J$ or $q \in J$?

\diamond

The previous exercise is an example of a *prime ideal*, defined below.

Definition 24.9.17. A *prime ideal* $J \subset R$ is an ideal such that if $p, q \in R$ and $p \cdot q \in J$, then either $p \in J$ or $q \in J$. \triangle

²The proof that \mathbb{Z} is a principal ideal domain makes use of the *well-ordering principle* which states that any subset of \mathbb{N} has a smallest element. The interested reader may consult <https://faculty.atu.edu/mfinan/4033/abstractbk.pdf> (p. 219) for more details.

Definition 24.9.18. When a principal ideal Ra is also a prime ideal, then the generator a is called a *prime element* \triangle

In Exercise 24.9.16 (a) you showed that 7 is a prime element. However, the result of (b) implies that 7^n where $n > 1$ is *not* a prime element. The following definition applies to powers of prime elements.

Definition 24.9.19. Suppose a is a prime element in the ring R . Then for any positive integer n , a^n is called a *prime power* and $R(a^n)$ is called a *prime power ideal*. \triangle

We will explore these concept in the next exercise.

Exercise 24.9.20.

- (a) In the ring of integers, show that $2\mathbb{Z}$ is a prime ideal.
- (b) In the ring of integers, show that $8\mathbb{Z}$ is *not* a prime ideal, but it is a prime power ideal.

\diamond

We will conclude this section with an important result in abstract algebra that closely resembles prime factorization of integers.

Proposition 24.9.21. In a principal ideal domain, any principal ideal is the intersection of prime power ideals.

PROOF. This is a more difficult proof and will not be studied in this class. \square

In the following example, we will see that all principal ideals factor as an intersection of prime power ideals.

Example 24.9.22. Show that $12\mathbb{Z} = 2^2\mathbb{Z} \cap 3\mathbb{Z}$. \blacklozenge

PROOF. Recall that:

$$\begin{aligned} 12\mathbb{Z} &= \{12n : n \in \mathbb{Z}\} = \{\dots, -24, -12, 0, 12, 24, \dots\}, \\ 2^2\mathbb{Z} = 4\mathbb{Z} &= \{4n : n \in \mathbb{Z}\} = \{\dots, -8, -4, 0, 4, 8, \dots\}, \text{ and} \\ 3\mathbb{Z} &= \{3n : n \in \mathbb{Z}\} = \{\dots, -6, -3, 0, 3, 6, \dots\}. \end{aligned}$$

Since 4 and 3 are relatively prime, then the only common multiples of 4 and 3 will be multiples of $4 \cdot 3$ or 12. In other words, $2^2\mathbb{Z} \cap 3\mathbb{Z} = 4\mathbb{Z} \cap 3\mathbb{Z} = (4 \cdot 3)\mathbb{Z} = 12\mathbb{Z}$. \square

Exercise 24.9.23. Show that $42\mathbb{Z} = 2\mathbb{Z} \cap 3\mathbb{Z} \cap 7\mathbb{Z}$. \diamond

Proposition 24.9.21 is the algebraic way of proving that any integer is the product of primes. The proposition also shows that polynomial can be factored uniquely. We will explore this more in Section 24.10 when we discuss polynomial rings. We need a bit more ring theory first.

24.9.1 Division rings and fields

All of the rings we have seen so far have multiplicative identities. But it is impossible to define multiplicative inverses for all the elements. In fact, it's (almost) *never* possible to have a multiplicative inverse of the additive identity (which we denote as 0), as long as the distributive property holds.

Exercise 24.9.24. There is one and only one case of a ring R in which every element has a multiplicative inverse. What is R ? \diamond

Exercise 24.9.25. Suppose the ring R has more than one element. Show that the additive identity of R has no multiplicative inverse. \diamond

Although the zero element never has a multiplicative inverse, there are cases where multiplicative inverses exist for every *nonzero* element of a ring. Such a ring is called a *division ring*.

Definition 24.9.26. Given a ring R suppose every nonzero element of R has a multiplicative inverse in R , then R is called a ***division ring***. \triangle

Let's explore an important example of division rings. In Example 15.2.8 we introduced a special group called the quaternion group, $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$, with the following relations:

- (a) 1 is the identity
- (b) -1 commutes with all other elements, and $(-1)^2 = 1$
- (c) $-1 \cdot i = -i, -1 \cdot j = -j, -1 \cdot k = -k$

$$(d) \quad i^2 = j^2 = k^2 = -1$$

$$(e) \quad i \cdot j = k, j \cdot k = i, k \cdot i = j$$

$$(f) \quad j \cdot i = -k, k \cdot j = -i, i \cdot k = -j$$

Exercise 24.9.27. Show that all of the equalities in parts (e) and (f) above may be derived from (a), (b), (c) and the equation $ijk = -1$. \diamond

We can extend the quaternion group by taking linear combinations of the elements of \mathbb{Q}_8 with real coefficients. This new set, simply known as the *quaternions*, was discovered by William Rowan Hamilton of Dublin in 1843. Hamilton's quaternions, notated by \mathbb{H} in his honor, are widely used today in computer graphics to describe motion in three dimensional space and multiple antennae communications systems. We may define this set formally as follows.

Definition 24.9.28. The set of real *quaternions*, denoted by \mathbb{H} , is defined by:

$$\mathbb{H} = \{a_0 + a_1i + a_2j + a_3k : a_0, a_1, a_2, a_3 \in \mathbb{R}\},$$

$$\text{where } i^2 = j^2 = k^2 = ijk = -1.$$

Note that $ij = -ji$, $ik = -ki$, and $jk = -kj$, so \mathbb{H} does *not* commute over multiplication.

Using the distributive law and the commutative law of addition, we define addition on \mathbb{H} as follows.

$$\begin{aligned} (a_0 + a_1i + a_2j + a_3k) + (b_0 + b_1i + b_2j + b_3k) \\ = (a_0 + b_0) + (a_1 + b_1)i + (a_2 + b_2)j + (a_3 + b_3)k. \end{aligned} \tag{24.9.29}$$

Multiplication of quaternions is also defined using the distributive law and commutative law of addition. \triangle

Exercise 24.9.30. Evaluate the following products of quaternions.

$$(a) \quad (1 + i + j + k)^2$$

$$(b) \quad (1 + i + j + k) \cdot (1 - i - j - k)$$

(c) $(1 + i + j + k) \cdot (1 + 2i + 3j + 4k)$

(d) $(a_0 + a_1i + a_2j + a_3k) \cdot (a_0 - a_1i - a_2j - a_3k)$

◇

In the following exercises, we will show that \mathbb{H} forms a division ring.

Exercise 24.9.31. Prove that the set of quaternions \mathbb{H} , defined above, forms a ring. ◇

Of course, not all rings are division rings. In order to show that \mathbb{H} is a division ring, we must show that every nonzero element of \mathbb{H} has a multiplicative inverse in \mathbb{H} . This proof is more advanced so you will be guided through it.

We will begin by defining the *conjugates* in \mathbb{H} . (Note that the term *conjugates*, like many other mathematical terms, can refer to different things in different contexts. The reader must always consider context to fully understand the meaning of such terms.)

Definition 24.9.32. Let $a = a_0 + a_1i + a_2j + a_3k \in \mathbb{H}$. Then the *conjugate* of a is denoted by \bar{a} and given by:

$$\bar{a} = a_0 - a_1i - a_2j - a_3k.$$

△

Note the following relationship between a and \bar{a} :

$$\begin{aligned} a \cdot \bar{a} &= (a_0 \cdot a_0 + a_1 \cdot a_1 + a_2 \cdot a_2 + a_3 \cdot a_3) + (-a_0 \cdot a_1 + a_0 \cdot a_1 - a_2 \cdot a_3 + a_2 \cdot a_3)i \\ &\quad + (-a_0 \cdot a_2 + a_0 \cdot a_2 - a_1 \cdot a_3 + a_1 \cdot a_3)j + (-a_0 \cdot a_3 + a_0 \cdot a_3 - a_1 \cdot a_2 + a_1 \cdot a_2)k \\ &= a_0 \cdot a_0 + a_1 \cdot a_1 + a_2 \cdot a_2 + a_3 \cdot a_3 \\ &= a_0^2 + a_1^2 + a_2^2 + a_3^2 \end{aligned}$$

Exercise 24.9.33.

(a) Using a and \bar{a} as defined above, show that $\bar{a} \cdot a = a \cdot \bar{a}$.

- (b) Note that if $a \neq 0$, $a \cdot \bar{a}$ is a nonzero real number and thus has a multiplicative inverse $(a \cdot \bar{a})^{-1}$. Show that $a \cdot ((a \cdot \bar{a})^{-1} \cdot \bar{a}) = 1$ and $((a \cdot \bar{a})^{-1} \cdot \bar{a}) \cdot a = 1$.
- (c) Give an expression for the multiplicative inverse of $a \in \mathbb{H}$ for $a \neq 0$.

◇

We have shown that the set of quaternions \mathbb{H} is a ring and that every nonzero element of \mathbb{H} has a multiplicative inverse in \mathbb{H} . So, \mathbb{H} is a division ring.

Exercise 24.9.34.

- (a) Give three examples of infinite division rings.
- (b) Give three examples of finite division rings.

◇

Division rings with commutative multiplication are called **fields**. Fields are one of the most important objects of study in all of mathematics.

Definition 24.9.35. A division ring F is called a **field** if the multiplication operation is commutative. △

In many of the rings we've seen so far, the field axioms are also satisfied. Figure 24.9.1 shows the relationship between the ring classes.

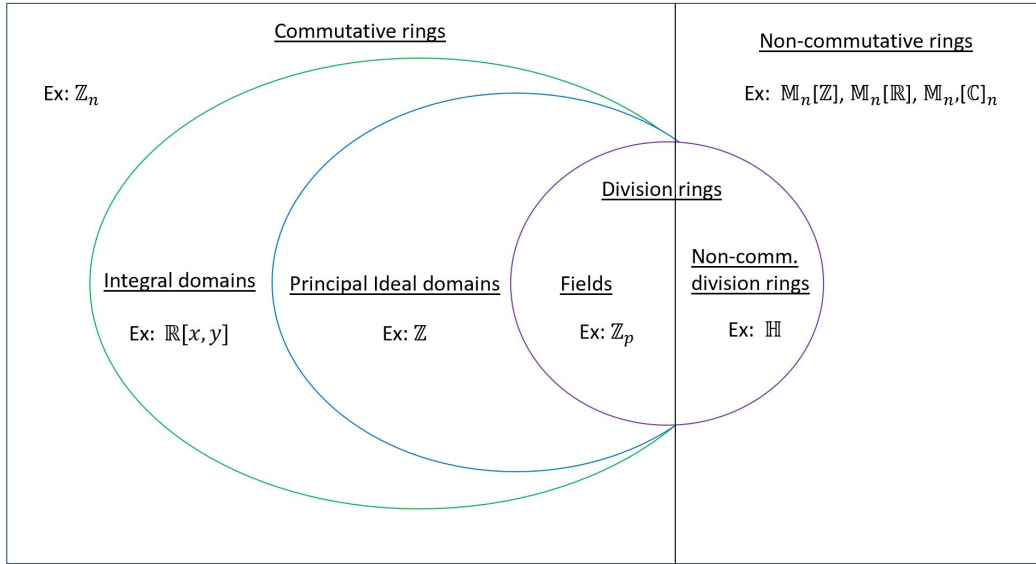


Figure 24.9.1. Ring Classes

Exercise 24.9.36. Which of the following rings are also fields? Explain your answers.

- (a) \mathbb{Z} (b) \mathbb{Q} (c) \mathbb{R} (d) \mathbb{C} (e) $\mathbb{R}[x]$ (f) $M_n(\mathbb{R})$ (g) $3\mathbb{Z}$ (h) \mathbb{Z}_4
 (i) \mathbb{Z}_p where p is prime ◇

Example 24.9.37. Let S be the set of all real 2×2 matrices of the form $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ where $a, b \in \mathbb{R}$. Show that S is a field.

PROOF. We know from Exercise 24.1.11 that the set of all 2×2 matrices form a ring. It remains to show that S is a division ring with multiplicative commutativity. It will be important in our proof to know that S has the multiplicative inverse property. Let's show that first.

Let $A \in S$ be defined by $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$. Then $A^{-1} = \begin{bmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{bmatrix}$ (as long as a and b are not both 0) because $A \cdot A^{-1} = A^{-1} \cdot A = 1$. It should be clear that $A^{-1} \in S$. Thus every nonzero element of S has an inverse in S and the multiplicative inverse property holds. We are now ready to show that S is a division ring.

We will show that S is a division ring by showing that it has no zero divisors. At this point, Proposition 24.9.5 comes in handy. We've already seen that every nonzero element $A \in S$ has an inverse. Proposition 24.9.5 immediately tells us that A is not a zero divisor. Since A was an arbitrary element of S , then there are no zero divisors in S and S is a division ring.

We have shown that S is a division ring, but we must now prove commutativity of multiplication.

Given $X = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ and $Y = \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \in S$, then:

$$X \cdot Y = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix} \text{ and } Y \cdot X = \begin{bmatrix} ac - bd & ad + bc \\ -ad - bc & ac - bd \end{bmatrix}.$$

We have shown that $X \cdot Y = Y \cdot X$ for any $X, Y \in S$, so S is commutative over multiplication. So S is a division ring with commutativity of multiplication, which means S is a field. \square \blacklozenge

Exercise 24.9.38. Show that the set of matrices $S = \begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$ where $a, b \in \mathbb{R}$ is *not* a field. \diamond

Looking bac at Section 24.3 we can see that we were creating fields without knowing it! The sets $\widehat{\mathbb{Q}}[x]$, $\widehat{\mathbb{R}}[x]$, $\widehat{\mathbb{Z}}_p[x]$, $\widehat{\mathbb{C}}[x]$ are all fields that are extensions of $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_p[x]$, $\mathbb{C}[x]$.

24.9.2 Further properties of fields

We've just introduced several new concepts, including integral domain, principal ideal domain, division ring, and field. Let's consider how they are related. We know that every field is a division ring (by definition). We also know that not every division ring is an integral domain (\mathbb{H} is an example). What about the relation between integral domain and field?

Exercise 24.9.39. Show that every field is an integral domain. \diamond

Now, what about the relation between field and principal ideal domain? This is a very interesting question. To answer it, we will need a series of propositions.

Proposition 24.9.40. If J is an ideal of the ring R and $1 \in J$, then $J = R$.

Exercise 24.9.41. Prove Proposition 24.9.40 ◇

Proposition 24.9.42. Given J is an ideal in ring R and $a \in J$. If a has a multiplicative inverse $a^{-1} \in R$, then $J = R$.

PROOF. To show that $J = R$, we can show that $J \subset R$ and $R \subset J$. We already know that $J \subset R$, by definition of ideal. To show that $R \subset J$, we must show that every element in R is also in J . Consider arbitrary element $r \in R$. We will show that $r \in J$ also.

| | |
|---|-----------------------|
| $a \in J$ implies $a^{-1} \in R$ | Given |
| $a \cdot a^{-1} = 1$ | Def. of mult. inverse |
| $a \in J$ and $a^{-1} \in R$ implies $a \cdot a^{-1} = 1 \in J$ | Def. of ideal |
| $J = R$ | Proposition 24.9.40 |

□

Proposition 24.9.43. Given field F , the only two ideals in F are $\{0\}$ and all of F .

PROOF. Suppose J is an ideal in field F . Then either $J = \{0\}$ or J has a nonzero element a . By the definition of field, a must have an inverse; and by Proposition 24.9.42, it follows that $J = F$. □

We've also discussed principal ideal domain which is a special type of integral domain.

Exercise 24.9.44. What is the relationship between fields and principal ideal domains? ◇

See if you can prove this final proposition that relates the ideas of field and ideal.

Proposition 24.9.45. Suppose that R is a commutative ring such that every ideal contains the multiplicative identity 1. Then every element in R has a multiplicative inverse. In other words, R is a field.

Exercise 24.9.46. Prove Proposition 24.9.45 ◇

24.10 Polynomials over fields

We saw in the previous section that $R[x]$ is a ring whenever R is a ring. We may ask a similar question about fields: If F is a field, then is $F[x]$ also a field? We investigate this question in the following exercises.

Exercise 24.10.1.

- (a) Give the zero divisors of \mathbb{Z}_4 and \mathbb{Z}_{15} .
- (b) Find two nonzero polynomials in $\mathbb{Z}_4[x]$ of degree 1 and 3 respectively whose product is 0.
- (c) Suppose $n = pq$, where p and q are integers greater than 1. Show that there exist two nonzero polynomials in $\mathbb{Z}_n[x]$ with degree greater than 1 whose product is 0.

◇

Do polynomials have multiplicative inverses? Be careful here. In high-school algebra or in calculus, the polynomial $p(x)$ has a perfectly good multiplicative inverse, namely $1/p(x)$. But $1/p(x)$ is not a polynomial, so for us it doesn't count! For a set of polynomials to be a field, the nonzero elements must have inverses that are polynomials themselves.

Exercise 24.10.2.

- (a) Consider the polynomial $p(x) = 1x$ as an element of $\mathbb{R}[x]$. Show there is no polynomial in $\mathbb{R}[x]$ that is a multiplicative inverse of $p(x)$.
- (b) Prove or disprove: Polynomial rings over fields are also commutative groups over multiplication.

◇

Exercise 24.10.3. Which elements of $\mathbb{R}[x]$ have multiplicative inverses? ◇

Exercise 24.10.4. Given a field F , which elements of $F[x]$ have multiplicative inverses? ◇

Exercise 24.10.5. Suppose that F is a field. Does this mean that $F[x]$ is also a field? Either prove the implication, or give a counterexample. \diamond

We may ask the question, Can $F[x]$ have zero divisors if F is a field? First let's look at an example.

Exercise 24.10.6. Let $p(x) = \sum_{i=0}^5 a_i x^i$ and $q(x) = \sum_{j=0}^3 b_j x^j$ be polynomials in $\mathbb{Z}_p[x]$, where $a_5 \neq 0$ and $b_3 \neq 0$.

- (a) What is the degree of $p(x)q(x)$?
- (b) Give an expression for the highest order term in $p(x)q(x)$. How do you know that this expression is not zero? (**Hint**)

Note that since $p(x)q(x)$ has a nonzero term, then it can't be the zero polynomial. \diamond

We may generalize the results of the previous exercise:

Exercise 24.10.7. Let $p(x) = \sum_{i=0}^n a_i x^i$ and $q(x) = \sum_{j=0}^m b_j x^j$ be polynomials in $F[x]$, where F is a field and $a_n \neq 0$, $b_m \neq 0$.

- (a) What is the degree of $p(x)q(x)$?
- (b) Give an expression for the highest order term in $p(x)q(x)$. How do you know that this expression is not zero?

\diamond

Exercise 24.10.7 establishes the following proposition:

Proposition 24.10.8. If F is a field, then $F[x]$ has no zero divisors.

The property of having no zero divisors turns out to be a very important consideration in the process of polynomial division, which we discuss in the next section.

And here's the result we've been waiting for. Now that we've prepared the ground, it's not so difficult to prove.

Proposition 24.10.9. (*Fundamental Theorem of Algebra: easy part*) Let F be a field and let $f(x)$ be a polynomial in $F[x]$ of degree n . Then the

equation $f(x) = 0$ has at most n solutions: that is, there are at most n distinct elements $\{x_1, \dots, x_n\}$ of F such that $f(x_m) = 0$ for $1 \leq m \leq n$.

PROOF. Suppose a_1 is a solution to $f(x) = 0$. Then by Proposition 12.6.14 it follows that $x - a_1$ divides $f(x)$. Therefore $f(x) = (x - a_1)g_{n-1}(x)$ where the degree of $g_{n-1}(x) = n - 1$.

Now if $a_2 \neq a_1$ is another solution then using our above result we have

$$f(a_2) = (a_2 - a_1)g_{n-1}(a_2) = 0.$$

Since $a_2 - a_1 \neq 0$, it follows that $g_{n-1}(a_2) = 0$. So we can write $g_{n-1}(x) = (x - a_2)g_{n-2}(x)$ where the degree of $g_2(x) = n - 2$.

Continuing in the same way, if there are distinct roots a_1, a_2, \dots, a_n then

$$f(x) = (x - a_1)(x - a_2)\dots(x - a_n)g_0,$$

where the degree of g_0 is 0 (in other words, g_0 is a constant.). So there can't be any more solutions, a_{n+1} , because $(x - a_{n+1})$ doesn't divide g_0 . \square

The previous theorem immediately gives us an extremely important general property of fields:

Proposition 24.10.10. Let F be a field, and let c be any element F . Then c has at most n n^{th} roots.

PROOF. Given the field F let $F[x]$ be the associated polynomial ring over the field F . The polynomial $x^n - c$ is an element of $F[x]$. By Proposition 24.10.9, the equation $x^n - c = 0$ has at most n solutions. This is exactly the same thing as saying that c has at most n n^{th} roots. \square

Exercise 24.10.11.

- (a) Find all fourth roots of 5625 in $\mathbb{R}[x]$. Give exact solutions.
- (b) Find all fifth roots of $3125i$ in $\mathbb{C}[x]$. Give exact solutions.
- (c) Find all fifth roots of 5 in \mathbb{Z}_7 .
- (d) Find all sixth roots of 1 in \mathbb{Z}_7 .

◇

Take note of the “at most” qualification in Proposition 24.10.9. There are cases of polynomials in $F[x]$ which do not have *any* roots in F . For example, there are polynomials in $\mathbb{R}[x]$ that have no roots at all in $\mathbb{R}[x]$, as the next examples illustrate.

Example 24.10.12. Find the roots of $p(x) = 2x^2 + 2x + 5$.

Since this is a quadratic polynomial we can use the famous quadratic formula:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

In $p(x)$, $a = 2$, $b = 2$, and $c = 5$. We substitute those values into the formula and obtain the following:

$$\begin{aligned} x &= \frac{-2 \pm \sqrt{2^2 - 4 \cdot 2 \cdot 5}}{2 \cdot 2} = \frac{-2 \pm \sqrt{-36}}{4} = \frac{-2 \pm 6i}{4} \\ &= \frac{-1 \pm 3i}{2}. \end{aligned}$$

So the roots of $p(x)$ are $x = -\frac{1}{2} + \frac{3}{2}i, -\frac{1}{2} - \frac{3}{2}i$. ◆

The next example is a cubic polynomial in $\mathbb{Z}[x]$. To find the rational roots, we will make use of the following proposition.

Proposition 24.10.13. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ be a polynomial in $\mathbb{Z}[x]$. Any rational roots of $f(x)$ expressed in lowest terms have numerators, p , which are factors of a_0 and denominators, q , which are factors of a_n .

PROOF. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ be a polynomial in $\mathbb{Z}[x]$ and suppose that p/q is a root of $f(x)$, where the fraction p/q is in lowest terms (so p and q are relatively prime).

First we will show that p is a factor of a_0 . Since p/q is a root of $f(x)$ we have $f\left(\frac{p}{q}\right) = 0$, which implies

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_0 = 0.$$

Multiplying both sides by q^n , we have,

$$\left(a_n \left(\frac{p}{q} \right)^n + a_{n-1} \left(\frac{p}{q} \right)^{n-1} + \dots + a_0 \right) q^n = 0,$$

which simplifies to

$$a_n p^n + a_{n-1} (p^{n-1} q) + \dots + a_0 q^n = 0.$$

This expression can be rearranged to obtain:

$$p (-a_n p^{n-1} - a_{n-1} (p^{n-2} q) - \dots - a_1 q^{n-1}) = a_0 q^n.$$

Since $f(x) \in \mathbb{Z}[x]$, all the coefficients a_i are also integers. p and q are also integers. Since integers are closed under addition and multiplication, it follows that both sides of the above equation are integers. Since p divides the left-hand side, it must also divide the right-hand side. Therefore p divides $a_0 q^n$. Now p and q are relatively prime: so in order for p to divide $a_0 q^n$, it must divide a_0 . In other words, p is a factor of a_0 —which is just what we wanted to prove.

It turns out the proof that q is a factor of a_n is basically the same, if we use a little trick. The first equation that we wrote down above was:

$$a_n \left(\frac{p}{q} \right)^n + a_{n-1} \left(\frac{p}{q} \right)^{n-1} + \dots + a_0 = 0.$$

Let's multiply both sides by $(q/p)^n$. After simplifying, and rearranging we get:

$$a_0 \left(\frac{q}{p} \right)^n + a_1 \left(\frac{q}{p} \right)^{n-1} + \dots + a_n = 0.$$

Now, this new equation corresponds exactly to the first equation with the following replacements:

$$a_n \rightarrow a_0; a_{n-1} \rightarrow a_1; \dots; a_0 \rightarrow a_n; p \leftrightarrow q.$$

We can then go through the entire previous argument, making these replacements. We concluded previously that p is a factor of a_0 —so if we apply the identical argument to the equation with replacements, we obtain that q is a factor of a_n . You may fill in the details in the following exercise.

Exercise 24.10.14. Starting with the equation $a_0 (q/p)^n + a_1 (q/p)^{n-1} + \dots + a_n = 0$, give the complete argument which shows that q is a factor of a_n . \diamond

□

Now let's get some practice using Proposition 24.10.13.

Example 24.10.15. Find the roots of $f(x) = 3x^3 + 10x^2 + 11x + 6$.

Since this is a cubic polynomial, we can't use the quadratic formula, at least not to begin with. The coefficients are integers, so we may use Proposition 24.10.13, which says that *any* rational roots of $p(x)$ have numerators that are factors of a_0 and denominators that are factors of a_n . This does not guarantee that there are rational roots: sometimes polynomials are irreducible, but we still try every method possible to find those roots unless we know that we can't reduce the polynomial. So we will proceed with trying to find the roots of $f(x)$ using Proposition 24.10.13.

In $f(x)$, possible numerators of any rational roots are: $p = \pm 1, \pm 2, \pm 3, \pm 6$. The possible denominators are: $q = \pm 1, \pm 3$. So we have as possible rational roots the following: $p/q = \pm 1, \pm \frac{1}{3}, \pm 2, \pm \frac{2}{3}, \pm 3, \pm 6$. By Proposition 12.6.14, if $f(p/q) = 0$ then $(x - p/q)$ is a factor of $f(x)$; which would make p/q a root of $f(x)$. After testing all possibilities we find the following rational root: $f(-2) = 3(-2)^3 + 10(-2)^2 + 11(-2) + 6 = 0$. Therefore, $x = -2$ is a root of $f(x)$ and $(x + 2)$ is a factor of $f(x)$. We then use long division to factor $f(x)$.

$$\begin{array}{r}
 \quad 3x^2 \quad + \quad 4x \quad + \quad 3 \\
 x+2 \overline{) 3x^3 \quad + \quad 10x^2 \quad + \quad 11x \quad + \quad 6} \\
 \underline{3x^3 \quad + \quad 6x^2} \\
 \quad 4x^2 \quad + \quad 11x \quad + \quad 6 \\
 \quad \underline{4x^2 \quad + \quad 8x} \\
 \quad 3x \quad + \quad 6 \\
 \quad \underline{3x \quad + \quad 6} \\
 \quad 0
 \end{array}$$

So now we have $f(x) = (x + 2)(3x^2 + 4x + 3)$. We use the quadratic formula to find the following roots for $3x^2 + 4x + 3$. $x = \frac{-2 \pm \sqrt{5}i}{3}$. So there are two complex roots and one real root. They are $x = \frac{-2 - \sqrt{5}i}{3}, -2, \frac{-2 + \sqrt{5}i}{3}$. \blacklozenge

Exercise 24.10.16.

- (a) Find the roots of $f(x) = 2x^2 + x + 1$. Give exact solutions.
- (b) Find the roots of $f(x) = 5x^3 + 17x^2 + 7x + 3$. Give exact solutions.

◇

In the exercises above, the leading coefficient is not 1. The situation is especially simple if the leading coefficient is 1. In such a case, the rational roots are integers:

Exercise 24.10.17.

- (a) Given that $p(x) \in \mathbb{Z}[x]$, and $p(x)$ has leading coefficient 1, show that all rational roots of $p(x)$ are integers.
- (b) Find the roots of $f(x) = x^3 - 13x + 12$.

◇

24.10.1 Algebraic closure of fields

In Section 24.10.2 we discussed the so-called *Fundamental Theorem of Algebra (hard part)*, (Proposition 12.6.28) which states that any polynomial in $\mathbb{C}[x]$ has a root in $\mathbb{C}[x]$. This property leads to a host of important consequences. Since this property is so important, it's been given a name:

Definition 24.10.18. A field F is *algebraically closed* if and only if every nonconstant polynomial in $F[x]$ has a root in F (see Figure 24.10.1).
△

With this new definition in mind, we can restate Proposition 12.6.28 as follows:

Proposition 24.10.19. \mathbb{C} is algebraically closed.

There are fields besides \mathbb{C} that are algebraically closed, but there are also lots of fields that aren't:

Exercise 24.10.20.

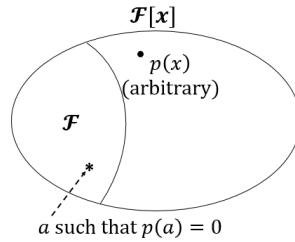


Figure 24.10.1. F is algebraically closed: every $p(x) \in F[x]$ has an $a \in F$ such $p(a) = 0$.

- (a) Are the rational numbers algebraically closed? Justify your answer.
 (b) Are the real numbers algebraically closed? Justify your answer.

◇

Exercise 24.10.21.

- (a) In the field \mathbb{Z}_5 , evaluate the polynomial $x^4 + 2$ for all elements of \mathbb{Z}_5 .
 (b) Using part (a), show that \mathbb{Z}_5 is not algebraically closed.
 (c) Use the polynomial $x^6 + 2$ to determine whether or not \mathbb{Z}_7 is algebraically closed.

◇

In Section 12.6.4 we proved polynomial factorization (Proposition 12.6.32), namely that any polynomial in $\mathbb{C}[x]$ factors as a product of linear factors. The very same proof goes through for any algebraically closed field F . Thus we have:

Proposition 24.10.22. Let F be an algebraically closed field. Then any polynomial $p(x)$ of degree n in $F[x]$ can be completely factored as a constant times a product of n linear terms, as follows:

$$p(x) = b(x - a_1)(x - a_2) \dots (x - a_n), \quad (24.10.23)$$

where $b, a_1, \dots, a_n \in F$.

24.10.2 Field extensions and algebraic elements

We've seen quite a few fields that are not algebraically closed. For example, the rational numbers \mathbb{Q} are not algebraically closed, because e.g. $x^2 - 2$ has no roots in \mathbb{Q} . However, we were able to find a larger field (namely \mathbb{R}) that contains \mathbb{Q} which has the root that \mathbb{Q} is lacking. In this section, we'll talk about situations like this in a general context.

First we need some terminology to describe the case where one field is contained in another:

Definition 24.10.24. Given a field E and $F \subset E$, then F is called a **subfield** of E if F is also a field with the same field operations as E . Conversely, E is called an **extension field** of F . \triangle

The following exercise should bolster your understanding of Definition 24.10.24

Exercise 24.10.25.

- (a) Give an example of a field F that has a nontrivial extension field (that is, the extension field contains elements that are not in F).
- (b) Give an example of a field, F that is a subset of a field E , but is not a subfield of E . Explain.

\diamond

We also need terminology to describe roots of polynomials in $F[x]$ that aren't in F :

Definition 24.10.26. Let F be a subfield of E , and let $a \in E$. If $p(a) = 0$ for some $p(x) \in F[x]$, then a is **algebraic** over F (see Figure 24.10.2). Otherwise, a is **transcendental** over F . \triangle

Exercise 24.10.27.

- (a) Give an example of a complex number $z \in \mathbb{C} \setminus \mathbb{R}$ which is algebraic over \mathbb{Q} (in other words, z satisfies $f(z) = 0$ where $f(x) \in \mathbb{Q}[x]$). Justify your answer.

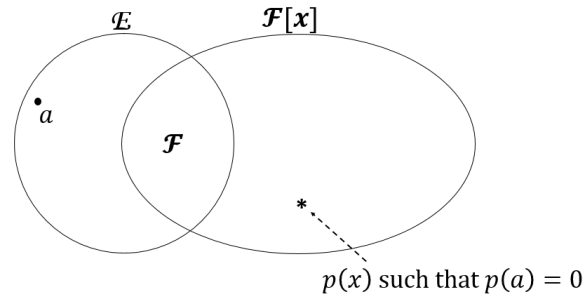


Figure 24.10.2. $a \in E$ is algebraic over F : there exists $p(x) \in F[x]$ such that $p(a) = 0$.

- (b) Suppose that $z \in \mathbb{C}$ is algebraic over \mathbb{R} . Show that \bar{z} is also algebraic over \mathbb{R} .
- (c) Show that every element of \mathbb{C} is algebraic over \mathbb{R} .

◇

Exercise 24.10.28.

- (a) Given that $a \in \mathbb{C}$ is algebraic over \mathbb{Q} , show that \sqrt{a} is also algebraic over \mathbb{Q} .
- (b) Given that $a \in \mathbb{C}$ is algebraic over \mathbb{Q} , show that $a^{1/n}$ is also algebraic over \mathbb{Q} for any natural number n .

◇

Remark 24.10.29. It's not so easy to show that elements are transcendental. This is because to show that a is transcendental over F , you need to show that there's no polynomial whatsoever in $F[x]$ which has a as a root. Let's consider in particular the case $F = \mathbb{Q}$. We saw in Chapter 4 that \mathbb{R} has lots of *irrational* numbers, but so far we haven't definitely identified any real number that is transcendental over \mathbb{Q} .

In 1844, Joseph Liouville gave the first proof that a transcendental number exists. Liouville constructed a number (using infinite series) with special

properties, and was able to show that it's impossible to construct a polynomial in $\mathbb{Q}[x]$ that has that number as a root. Hermite showed about 30 years later that e was transcendental, and π was added to the list (by Lindemann) 10 years after that.

Even today, only a handful of classes of numbers have been shown to be transcendental. This is not to say that there aren't lots of them. In fact, Georg Cantor in 1874 was able to show that "almost all" real numbers are transcendental over \mathbb{Q} . This is a fascinating topic, and there's lots of information on the Internet if you're interested in pursuing it further (one place to look is <http://mathworld.wolfram.com/TranscendentalNumber.html>). \triangle

For field extensions which have no transcendental elements, the following definition applies:

Definition 24.10.30. Suppose E is an extension field of F . Then E is called an *algebraic extension* of F if every $a \in E$ is algebraic over F . \triangle

Exercise 24.10.31.

- (a) Give an example of a extension field that is algebraic. Justify your answer.
- (b) Give an example of a field extension that is not algebraic. Justify your answer.

\diamond

A field extension may be algebraic, but still contain polynomials that have no roots. There's a special term for field extensions which contain roots for *all* their polynomials:

Definition 24.10.32. Let E be an algebraic extension field of F . Suppose that for every $p(x) \in E[x]$, there exists $a \in E$ such that $p(a) = 0$. Then E is an *algebraic closure* of F (see Figure 24.10.3). \triangle

Here's an example of an algebraic closure:

Proposition 24.10.33. \mathbb{C} is an algebraic closure of \mathbb{R} .

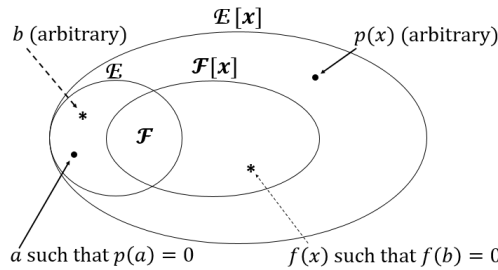


Figure 24.10.3. E is an algebraic closure of F : every $p(x) \in E[x]$ has an $a \in E$ such that $p(a) = 0$; and every $b \in E$ has an $f(x) \in F[x]$ such that $f(b) = 0$.

PROOF. Let $a+bi \in \mathbb{C}$ be arbitrary and let $p(x) = (x-(a+bi))(x-(a-bi)) = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x]$. We see that $a + bi$ is a root of $p(x)$. Since $a + bi$ is arbitrary, we can say that any element of \mathbb{C} is a root of some polynomial in $\mathbb{R}[x]$. By Definition 24.10.30 this makes \mathbb{C} an algebraic extension of \mathbb{R} . Additionally, by Proposition 24.10.19, \mathbb{C} is algebraically closed. Therefore, by Definition 24.10.32, \mathbb{C} is the algebraic closure of \mathbb{R} . \square

Does every field have an algebraic closure? Let’s look at some field extensions we’re already familiar with:

Exercise 24.10.34.

- (a) Give an example that shows that \mathbb{C} is not an algebraic closure of \mathbb{Q} . Explain.
- (b) Give an example that shows that \mathbb{R} is not an algebraic closure of \mathbb{Q} . Explain.

\diamond

Although we won’t prove it here, it can be shown that every field has an algebraic closure. ³ In particular, there is a subfield of \mathbb{C} which is an algebraic closure of \mathbb{Q} : this subfield is called the field of **algebraic numbers**.

Exercise 24.10.35. Draw a set diagram that shows the relationships between the sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, and \mathbb{A} , where \mathbb{A} denotes the set of algebraic numbers.

³see <https://soffer801.wordpress.com/2011/10/25/every-field-has-an-algebraic-closure/> for a nice discussion.

(For example, the “set bubble” representing \mathbb{Q} should be inside the bubble representing \mathbb{C} , since $\mathbb{Q} \subset \mathbb{C}$.) \diamond

24.10.3 Applications of algebraic field extensions

We’ve already seen how field extensions play an important role in mathematics. The irrational numbers were first introduced using an algebraic field extension of \mathbb{Q} (although later it was discovered that not all irrational numbers are algebraic over \mathbb{Q}). Similarly, the complex numbers were created as an algebraic field extension of the real numbers. But this is just the beginning. Algebraic field extensions have played a pivotal role in a great number of deep mathematical results obtained over the last 200 years. Here is a short list of results which make use of algebraic field extensions:

- The quadratic formula expresses the roots of quadratic polynomials in terms of algebraic operations on the coefficients plus a square root. There are similar (but vastly more complicated) formulas for solving cubic and quartic (3rd and 4th degree) polynomial equations, which involve algebraic operations and taking n th roots, for different values of n . How about quintic (5th degree) polynomials? Amazingly, it is possible to prove that there is no general formula for the solution of a quintic equation in terms of roots and algebraic operations. Not just the formula is not known—there is *no formula*. Period. This stupendous result is associated with the mathematicians Evariste Galois, Niels Henrik Abel, and Paolo Ruffini, and was proved in the mid-19th century.

This result relates to field extensions because every solution to an equation that involves only roots and algebraic operations must belong to certain type of field extension of the rationals. This fact imposes conditions on the type of numbers that can be expressed in such a form. It can be shown that there are roots of 5th-degree equations that don’t meet these conditions—hence they can’t possibly satisfy such an equation.

- Beginning with the Greeks, mathematicians tried for thousands of years to find a way to trisect an angle, using only straightedge and compass. In 1837, Pierre Wantzel finally showed that it is *impossible*. His proof built on previous results of Galois. (Think of how many hours over how many centuries were spent on a futile quest!)

This result relates to field extensions in similar fashion as the previous one. Geometrical points in the plane are identified as complex numbers (as we described in Section 4.4). Every point constructed based on a set of points is an algebraic combination of the corresponding complex numbers, together with square roots. This means that every constructable point must be contained in a series of field extensions created by successively adding square roots to an existing field. It can be shown that trisecting an angle involves finding a cube root which cannot possibly belong to such a series of extensions. You may consult:

<https://terrytao.wordpress.com/2011/08/10/a-geometric-proof-of-the-impossibility-of-angle-trisection-by-straightedge-and-compass/>

to get a flavor of how this proof goes.

- A similar constructability problem is known as “squaring the circle”: Given a square of side 1, find a circle with the same area using only straightedge and compass. This can be shown to be impossible, as a consequence of the transcendence of π alluded to in Remark 24.10.29.

24.11 References

The following links talk about different applications of rings:

<https://pdfs.semanticscholar.org/8ff4/9f31c24cc10b72af379fa364becc89eb5a36.pdf>

<https://wdjoyner.files.wordpress.com/2018/04/sm462-notes-on-ring-thry.pdf>

<http://www.ihes.fr/~brown/GergenLectureI.pdf>

<https://www.wireilla.com/ns/math/Papers/3414ijscmc05.pdf>

<http://math.mit.edu/~mckernan/Teaching/12-13/Spring/18.703/book.pdf>

<https://www.math.ias.edu/~avi/PUBLICATIONS/HrubesWi2013.pdf>

http://ijgt.ui.ac.ir/article_5453_9f9342e7224465dd42f3537a6a7fe39a.pdf

24.12 Hints for “Introduction to Rings” exercises

Exercise 24.8.4: Look at the Cayley tables and imagine that the tables contain only the first element in each pair.

Exercise 24.8.5: This is similar to Exercise 24.8.4.

Exercise 24.5.13: Part (b): Check if f has an inverse.

Exercise 24.7.11: Can you think of an element in R that generates all of R ?

Exercise 24.9.6: Take the expression $ab = 0$ and multiply both sides on the left by a^{-1} .

Exercise 24.10.7: Use Proposition 24.9.5 part b and remember that \mathbb{Z}_p is a field.

Polynomial Codes

25.1 Polynomials with coefficients in \mathbb{Z}_2

We are used to polynomials with coefficients that are integers or real numbers. But as we mentioned in the previous chapter, it is also possible to have polynomials with coefficients from other number systems. In this chapter, we will be looking particularly at the the set of polynomials with coefficients in \mathbb{Z}_2 : this set is denoted by $\mathbb{Z}_2[x]$. For a polynomial in $\mathbb{Z}_2[x]$, all coefficients are either 0 or 1.

Example 25.1.1. The polynomials in $\mathbb{Z}_2[x]$ are:

- . The constant polynomials: 1 and 0 (there are only 2)
- . The linear polynomials: x and $x + 1$ (there are only 2)
- . The quadratic polynomials: $x^2, x^2 + 1, x^2 + x, x^2 + x + 1,$

And so on for higher-degree polynomials. ♦

Exercise 25.1.2.

- (a) How many different polynomials in $\mathbb{Z}_2[x]$ have degree 3?
- (b) How many different polynomials in $\mathbb{Z}_2[x]$ have degree 4?
- (c) How many different polynomials in $\mathbb{Z}_2[x]$ have degree n , where $n \geq 1$?
Make a guess.

- (d) Prove that your guess is correct (*Hint*: Use induction, if you know how. Otherwise, you can make a more informal argument.)

◇

A polynomial in $\mathbb{Z}_2[x]$ can also be represented as a **binary n -tuple** (or binary vector) whose entries are 1's and 0's. If the degree of the polynomial is n , then there must be at least $n + 1$ entries in the tuple.

Example 25.1.3. The polynomial $f(x) = x^3 + x^2 + x$ can be represented by the binary 4-tuple: (1 1 1 0). It can also be represented by the 5-tuple (0 1 1 1 0) or the 6-tuple (0 0 1 1 1 0): these representations may be useful when adding or subtracting polynomials, as we'll see in a moment. ◆

Addition, subtraction and multiplication are best explained by examples.

Example 25.1.4. Let $f(x) = x^2 + x + 1$ and $g(x) = x^3 + x + 1$ be polynomials in $\mathbb{Z}_2[x]$. We may represent $f(x)$ and $g(x)$ by the 4-tuples (0 1 1 1) and (1 0 1 1) respectively (note that we have used n -tuples of the same length: the length is determined by the highest degree of the two polynomials). Adding the polynomials is the same as adding corresponding entries of the in mod 2. It follows that the sum $f(x) + g(x)$ is:

$$((0 \oplus 1) \quad (1 \oplus 0) \quad (1 \oplus 1) \quad (1 \oplus 1)) = (1 \quad 1 \quad 0 \quad 0),$$

which corresponds to the polynomial $x^3 + x^2$. (Actually, when we represent polynomials as n -tuples in this way, polynomial addition is identical to addition in \mathbb{Z}_2^n , where $\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \dots \times \mathbb{Z}_2}_{n \text{ times}}$.)

If on the other hand we take $f(x) - g(x)$, we find that we get the same answer (Try it!). This will *always* be the case, because in \mathbb{Z}_2 addition and subtraction are the *same* operation. ◆

We will be using these polynomials to represent certain special types of codes, as we shall see shortly.

25.2 Cyclic Binary Codes

Recall from the chapter on algebraic encoding, that a code is linear if the code is determined by the null space of some matrix $H \in \mathbb{M}_{m \times n}(\mathbb{Z}_2)$.¹ So consider the codes generated by the following generator matrix:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Using the methods in the previous chapter we find the resulting code words for the matrix are as follows:

$$\begin{array}{ll} (000) \mapsto (000000) & (100) \mapsto (100100) \\ (001) \mapsto (001001) & (101) \mapsto (101101) \\ (010) \mapsto (010010) & (110) \mapsto (110110) \\ (011) \mapsto (011011) & (111) \mapsto (111111). \end{array}$$

This matrix follows the typical rules of linear codes. However there is an additional interesting and useful property of these codewords. In order to describe the property we need the following definition.

Definition 25.2.1. The *cyclic 1-shift* of a codeword is the codeword obtained by taking the leftmost bit in the codeword and moving it to the rightmost position. The *cyclic n -shift* of a codeword is the result of n 1-shifts applied to that codeword. In the following we sometimes leave off the word “cyclic” for short: so “1-shift” means the same as “cyclic 1-shift”, etc. \triangle

According to this definition, (00101) when cyclic 1-shifted results in (01010), or when cyclic 3-shifted results in (01001).

Exercise 25.2.2. Shift the following codewords by the given cyclic shift.

(a) (1011) 1-shifted

¹ $M_{m \times n}(\mathbb{Z}_2)$ is the set of matrices of dimension $m \times n$ whose elements are elements of \mathbb{Z}_2 .

- (b) (1010101) 1-shifted
- (c) (1001011) 3-shifted
- (d) (0101011010101) 5-shifted
- (e) (0101001111001) 7-shifted
- (f) $(z_n, z_{n-1} \cdots z_1, z_0)$ 1-shifted, where $z_n \in \mathbb{Z}_2$
- (g) $(z_n, z_{n-1} \cdots z_1, z_0)$ 3-shifted, where $z_n \in \mathbb{Z}_2$
- (h) $(z_{n-2}, z_{n-3} \cdots z_1, z_0, z_n, z_{n-1})$ $(n-2)$ -shifted where $z_n \in \mathbb{Z}_2$

◇

Now let's return to the code generated by the matrix G_1 given above. Notice that each cyclic 1-shift of a codeword is also a codeword. For example, the cyclic 1-shift of the codeword (001001) is (010010), which is also a code word. This is the same as stating that the set of codewords is *closed* under cyclic 1-shifts.

Definition 25.2.3. A linear code that is closed under cyclic 1-shifts is said to be a *cyclic code*. △

Not all linear codes are cyclic codes. Take the following generator matrix:

$$G_2 = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

The resulting code words for the G_2 are as follows

$$\begin{array}{ll} (000) \mapsto (000000) & (100) \mapsto (111100) \\ (001) \mapsto (001111) & (101) \mapsto (110011) \\ (010) \mapsto (011110) & (110) \mapsto (100010) \\ (011) \mapsto (010001) & (111) \mapsto (101101). \end{array}$$

Notice that (101101) is a code word but (011011) is not a code word. Therefore the code that uses G_2 as a generator matrix is not a cyclic code.

Cyclic codes may be easily implemented on computers using *shift registers*. Figure 25.2.1 gives some indication of how this is done for the code with generator matrix G_1 .

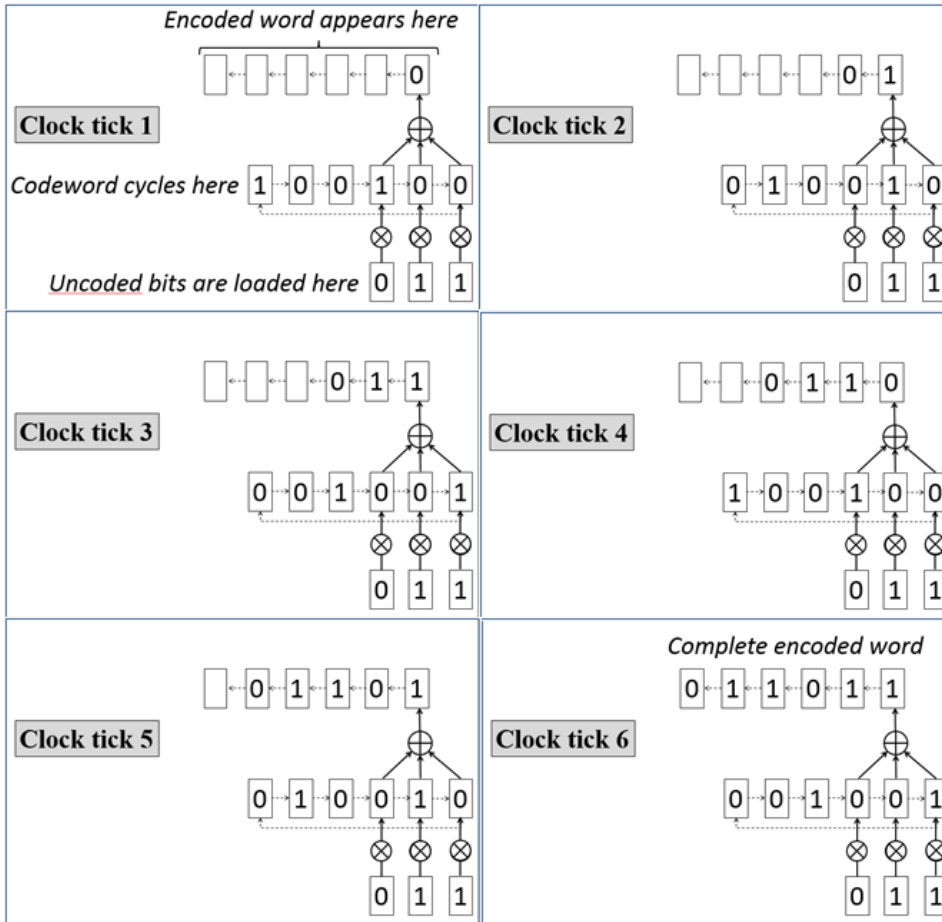


Figure 25.2.1. Shift register implementation of the code generated by matrix G_1 . The uncoded bits are placed in the bottom “registers” (represented by rectangles) for six “clock ticks”. At each “clock tick”, the other bits all move according to the dotted arrows. Binary multiplication and addition are performed on the bits according to the \otimes and \oplus symbols.

Exercise 25.2.4. For each of the following sets of code words, prove or disprove that they are closed under cyclic 1-shifts.

- (a)
- | | | | |
|----------|----------|----------|----------|
| (000000) | (111100) | (001111) | (110011) |
| (011110) | (100010) | (010001) | (100101) |
- (b)
- | | | | |
|----------|----------|----------|----------|
| (000000) | (011100) | (111100) | (110011) |
| (011110) | (100010) | (010001) | (101101) |
- (c)
- | | | | |
|----------|----------|----------|----------|
| (000000) | (111000) | (000111) | (101010) |
| (001110) | (010101) | (011100) | (111111) |

◇

Exercise 25.2.5.

- (a) Prove or disprove: A cyclic code is closed under cyclic 2-shifts.
- (b) Prove or disprove: A cyclic code is closed under cyclic 3-shifts.
- (c) Prove or disprove: A cyclic code is closed under cyclic n -shifts for any $n \in \mathbb{N}$. (Use induction if you can—otherwise, you may make a more informal argument.)

◇

Example 25.2.6. An interesting (and sometimes useful) property of some binary codes is that the reverse of each codeword is also a codeword. Take for example the following cyclic code of length 4 :

$$S = \{(0000), (1010), (0101), (1111)\}$$

The codewords (0000) and (1111) read the same backwards and forwards: such codewords are called *palindromic*. The remaining two codewords (1010) and (0101) are reverses of each other. Thus the reverse of every codeword in S is also a codeword in S .

Codes for which the reverse of every codeword is a codeword are called *reversible codes*. Such codes are interesting because they can be read either backwards or forwards (although the forward and backward readings will be different!), and are useful in certain data storage applications². ◆

²See Massey, J. L. (1964). “Reversible codes”. *Information and Control*, 7(3), 369-380.

Exercise 25.2.7.

- (a) Give an example of a binary code that is not reversible.
- (b) Show that all cyclic codes of length 2 and 3 are reversible codes.
- (c) Show that all cyclic codes of lengths 4 are reversible codes. (*Hint:* How many code words are palindromic? You don't need to check these. The remaining code words divide into pairs, where the two code words in a pair are reverses of each other. You just need to show that the two code words in each pair are cyclic shifts of each other.)
- (d) *Show that all cyclic codes of length 5 are reversible codes. (*Hint:* You will need to use the cyclic codes are defined to be linear.)

◇

Exercise 25.2.8. Let S be a binary cyclic code, and suppose that S contains a palindromic codeword w . Show that the reverse of every cyclic shift of w is also a cyclic shift of w .

◇

Exercise 25.2.9. Suppose a code C has a generator matrix G with two columns, such that the two columns are reverses of each other. Show that C is a reversible code.

◇

Exercise 25.2.10. Suppose a code C is reversible, and has an odd number of codewords. Prove that at least one codeword in C is palindromic. Is it possible that C could have exactly two codewords are palindromic in this case?

◇

25.3 Polynomial Codes: definition and basic properties

In Section 25.1 we mentioned that any polynomial in $\mathbb{Z}_2[x]$ can be written as a binary n -tuple: for example, the polynomial $x^6 + x^4 + x$ would be represented as (1010010). Notice that in the n -tuple, the coefficient of the highest order term is on the *left*, and the coefficient of the lowest-order term

written on the *right*. We did this because this is how you write polynomials in high school or college algebra. However, the reader should take note that many references on polynomial codes *reverse* this order, and list the lowest-order coefficient on the *left*.

Now we'll turn the relationship around. Any list or vector of binary digits, similar to the code words in the previous section, can be represented as a polynomial. For example (101101) can be represented as the polynomial $1x^5 + 0x^4 + 1x^3 + 1x^2 + 0x + 1 = x^5 + x^3 + x^2 + 1$.

Exercise 25.3.1. Suppose a vector contains 10 binary digits (binary digits are also referred to as *bits*).

- (a) What is the highest possible degree of the polynomial corresponding to the vector?
- (b) If the degree of the corresponding polynomial is 6, what can you say about the vector?
- (c) If the corresponding polynomial has only even powers of x , what can you say about the vector?

◇

Recall that we have defined a code of length n (or n -bit code) as a set of binary n -tuples. We can use polynomials to generate codes as shown in the following example.

Example 25.3.2. Let $p(x) = x^3 + 1$. Consider all polynomials of degree ≤ 2 : they are

$$0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1.$$

Take $p(x)$ times each of these polynomials and represent the results as binary 6-tuples:

$$\begin{aligned}
0 \cdot p(x) &= 0x^5 + 0x^4 + 0x^3 + 0x^2 + 0x + 0 = (000000), \\
1 \cdot p(x) &= x^3 + 1 = (001001), \\
x \cdot p(x) &= x^4 + x = (010010), \\
x^2 \cdot p(x) &= x^5 + x^2 = (100100), \\
(x+1)p(x) &= (010010) + (001001) = (011011), \\
(x^2+1)p(x) &= (100100) + (001001) = (101101), \\
(x^2+x)p(x) &= (100100) + (010010) = (110110), \text{ and} \\
(x^2+x+1)p(x) &= (100100) + (010010) + (001001) = (111111).
\end{aligned}$$

So we have the following set:

$$\begin{array}{cccc}
(000000) & (100100) & (001001) & (101101) \\
(010010) & (110110) & (011011) & (111111).
\end{array}$$

We call this set of codewords the code of length 6 (or 6-bit code) generated by $p(x)$. \blacklozenge

We generalize this example with the following definition.

Definition 25.3.3. Let $p(x)$ be a polynomial of degree d with coefficients in \mathbb{Z}_2 and S be the set of all polynomials in $\mathbb{Z}_2[x]$ with degree m or less. The **polynomial code generated by $p(x)$ of length $d+m+1$** is the subset of \mathbb{Z}_2^{d+m+1} corresponding to the set of products of $p(x)$ with each polynomial in S . \triangle

Exercise 25.3.4. Find the 7-bit codes generated by the following polynomials.

- (a) $x^5 + x^3 + x^2 + 1$
- (b) $x^4 + x^3 + x$
- (c) $x^5 + x^4 + x^2 + x$
- (d) $x^4 + x^2$

◇

Exercise 25.3.5. Find the 5-bit codes generated by each of the following polynomials:

- (a) $x + 1$
- (b) $x^3 + x + 1$
- (c) $x^2 + x$

◇

In our previous discussion of binary codes in Chapter 19, we made a big deal about *linear codes*. Recall that a linear code is a code that is closed under addition:

Exercise 25.3.6. Show that the following code is a linear code

$$\{(0000), (1010), (0101), (1111)\}$$

◇

Notice that in Exercise 25.3.6, we used the cyclic polynomial code from Example 25.2.6. Therefore it is possible for a polynomial code to be a linear code. But are all polynomial codes linear codes? That's the million-dollar question. Let's explore a bit:

Exercise 25.3.7. Let $p(x) = x^3 + x + 1$, let G_1 be the set of 6-tuples that are multiples of $p(x)$.

- (a) Show that (100111) and (010110) are multiples of $p(x)$.
- (b) Show that (100111) + (010110) is a multiple of $p(x)$. (Here '+' is in the sense of $\mathbb{Z}_2[x]$.)
- (c) Show that the polynomial code consisting of multiples of $p(x)$ is a linear code (that is, it is closed under addition).

◇

The preceding exercise is not a general proof, but it is possible to generalize the method used to show that polynomial codes are indeed linear codes. It's actually not difficult to obtain the generator matrix for a given polynomial code, as the following example shows.

Example 25.3.8. Consider the $(6, 3)$ code corresponding to the polynomial $x^3 + 1$. We therefore have

$$\begin{aligned} 1 &\text{ encodes as } x^3 + 1, \\ x &\text{ encodes as } x^4 + x, \\ x^2 &\text{ encodes as } x^5 + x^2. \end{aligned}$$

All of the above polynomials also have n -tuple representations. Using n -tuples, the same encoding information can be written as

$$\begin{aligned} (001) &\mapsto (001001), \\ (010) &\mapsto (010010), \\ (100) &\mapsto (100100). \end{aligned}$$

To obtain the generator matrix, we simply write the codewords for (100) , (010) , and (001) as column vectors next to each other.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Since the smallest weight of any of the nonzero codewords is 2, this code has the ability to detect all single errors.

◆

Exercise 25.3.9. Give the generator matrix for the codes generated by the following polynomials.

- (a) The $(5, 3)$ code generated by $x^2 + x$.

- (b) The (7,4) code generated by $x^3 + x$.
- (c) The (9,5) code generated by $x^4 + x^2 + 1$.

◇

We now have enough information to approach the question of when a polynomial code is a cyclic code. We must first define a cyclic shift in terms of polynomials. We understand to perform a cyclic shift on an n -tuple, we just take the left most digit in the n -tuple and put it on the right of the n -tuple. (1011) would turn into (0111). However moving the terms of a polynomial does not change its value. In this case we have to multiply the whole polynomial by x to shift the terms up a degree, but there is an additional step needed to move the highest term to the lowest. To do this, we have to use modular polynomial division.

Example 25.3.10. The n -tuple (0111) when cyclically shifted once, results in (1110). So the polynomial $p(x) = x^2 + x + 1$ when cyclically shifted once is $x^3 + x^2 + x$. When we multiply $p(x)$ by x , we get $x^3 + x^2 + x$. In this case, multiplication by x gives the cyclic shift.

The n -tuple (1011) when cyclically shifted once results in (0111). So the polynomial $p(x) = x^3 + x + 1$ when cyclically shifted once is $x^2 + x + 1$. We multiply $p(x)$ by x to yield $xp(x) = x^4 + x^2 + x$, which is not the same codeword as (0111). Therefore, we must divide by $x^4 + 1$.

$$x^4 + x^2 + x = 1 \cdot (x^4 + 1) + (x^2 + x - 1)$$

and the last term -1 gets taken (mod 2) to yield.

$$x^2 + x + 1$$

Which is the same as the n -tuple (1110). ◆

Proposition 25.3.11. A cyclic shift of a n -bit polynomial codeword $p(x)$ is the same as multiplying the codeword $p(x)$ by x then taking the remainder after dividing by $x^n + 1$.

PROOF.

Case 1: The polynomial codeword has a degree of less than $n - 1$. In this case, a polynomial of the form $p(x) = 0x^{n-1} + a_{n-2}x^{n-2} + a_{n-3}x^{n-3} \cdots +$

$a_1x + a_0$ where $a_n \in \mathbb{Z}_2$, when multiplied by x would result in $xp(x) = a_{n-2}x^{n-1} + a_{n-3}x^{n-2} \cdots + a_1x^2 + a_0x + 0$. Which is the cyclically shifted code word. Then when taking the remainder after division by $x^n + 1$, we notice that the degree of $x^n + 1$ is larger than $xp(x)$, so the quotient must be 0 and the remainder will be $xp(x)$.

Case 2: The polynomial codeword has a degree equal to $n - 1$. In this case, a polynomial of the form $p(x) = a_{n-1}x^{n-1} + a_{n-2}x^n - 2 + a_{n-3}x^n - 3 \cdots + a_1x + a_0$, where $a_n \in \mathbb{Z}_2$, when multiplied by x would result in $xp(x) = a_{n-1}x^n + a_{n-2}x^{n-1} \cdots + a_1x^2 + a_0x + 0$. This is close to the cyclically shifted codeword, but has an x^n term that is not in any codeword. We then divide by $x^n + 1$, since both $xp(x)$ and $x^n + 1$ have a x^n term, the quotient is 1. Then taking the remainder will yield, $a_{n-2}x^{n-1} \cdots + a_1x^2 + a_0x - 1$. But remember we're doing arithmetic in \mathbb{Z}_2 , so $-1 = 1$. Thus the remainder is $a_{n-2}x^{n-1} \cdots + a_1x^2 + a_0x + 1$ which is the cyclically shifted codeword. \square

Exercise 25.3.12. For the following polynomials, calculate their cyclic shift by multiplying by x then taking the remainder after division of $x^n + 1$.

a $x^3 + x^2 + 1$ where $n = 4$

b $x^7 + x^4 + x^2$ where $n = 8$

c $x^9 + x^8 + x^7 + x^5 + x^4 + x^2 + 1$ where $n = 10$

\diamond

Proposition 25.3.13. Any cyclic shift of $p(x)$ can be written as a sum of $p(x) + q(x)(x^n + 1)$, where $p(x)$ is a codeword and $q(x)$ is some polynomial.

PROOF. Given a n -bit codeword $p(x)$, the cyclic shift of $p(x)$ is calculated by $xp(x) = q(x)(x^n + 1) + r(x)$ where $q(x)$ is some polynomial and $r(x)$ is a polynomial of degree less than n . Simply subtract $q(x)(x^n + 1)$ from both sides to yield $xp(x) - q(x)(x^n + 1) = r(x)$. \square

We next introduce the notion of a complete polynomial, which resembles the idea of a generator of a cyclic group.³

Definition 25.3.14. A *complete polynomial* is a polynomial $f(x) \in \mathbb{Z}_2[x]$ of degree n such that for every nonzero polynomial $g(x) \in \mathbb{Z}_2[x]$ of

³In fact, a complete polynomial IS the generator of a group of nonzero polynomials under multiplication.

degree n or less, there exists a positive integer k such that $g(x) - x^k$ is divisible by $f(x)$. \triangle

Example 25.3.15. The polynomial $x^3 + x + 1$ is complete. First, we set the equation equal to 0. $x^3 + x + 1 = 0$ Add $x + 1$ from both sides to yield: $x^3 = x + 1$. (Remember, addition is the same as subtraction in $\mathbb{Z}_2[x]$.) Multiply by x to get

$$x^4 = x^2 + x,$$

and again to get

$$x^5 = x^3 + x^2.$$

Now substitute $x + 1$ for x^3 to get $x^5 = x + 1 + x^2$. Multiply again by x to yield.

$$x^6 = x^3 + x^2 + x,$$

and substitute again for x^3 to get (after some algebra)

$$x^6 = x^2 + 1$$

Multiply once more by x to get $x^7 = x^3 + x = 1$.

So if we list the possible polynomials of degree 2 or less, each is paired to a power of x .

$$\begin{array}{rcl} x^0 & = & 1 \\ x^1 & = & x \\ x^2 & = & x^2 \\ x^3 & = & x + 1 \\ x^4 & = & x^2 + x \\ x^5 & = & x^2 + x + 1 \\ x^6 & = & x^2 + 1 \\ x^7 & = & 1 \end{array}$$

Therefore the polynomial $x^3 + x + 1$ is complete for polynomials of degree 2 or smaller. \blacklozenge

With these properties in place, we can now show how to generate a cyclic code with polynomials.

Example 25.3.16. Let $p(x)$ be $x + 1$ and $f(x) = x^5 + 1$ be a polynomial to be encoded. The product of the two would be the codeword $f(x)p(x) = x^6 + x^5 + x + 1$. To cycle the codeword left, we would need to multiply by

x . This would yield $x^7 + x^6 + x^2 + x$. However, since this is a 7-bit code, there is no place for an x^7 term. So we need to shift the x^7 term to an x^0 term. This is done by taking the remainder after dividing by $x^7 + 1$.

$x^7 + 1$ goes into $x^7 + x^6 + x^2 + x$ once, this cancels the x^7 term and has $x^6 + x^2 + x - 1$ as the remainder, but remember that this operation is done (mod 2) so the remainder is $x^6 + x^2 + x - 1$. $x^7 + 1$ does not divide any further as all the remaining terms are of a lesser degree. This new term we can then divide by $x + 1$ to show that it is in the code. $x + 1$ goes into $x^6 + x^2 + x + 1$ exactly $x^5 + x^4 + x^3 + x^2 + 1$ times (mod 2). We can continue multiplying by x and taking the remainder after division by $x^7 + 1$ to generate additional codewords.

So for the 7-bit polynomial code generated to be cyclic, $p(x)$ must divide $x^7 + 1$. Using polynomial division we can show that $x^7 = (x + 1)(x^6 - x^5 + x^4 - x^3 + x^2 - x + 1) + 0$. So $p(x)$ divides any product of $x^7 + 1$.

We can show that $x + 1$ divides $x^n + 1$. First let's show that $p(x)$ divides $x^2 + 1$. $(p(x))^2 = x^2 + 2x + 1$, but remember $2x = 0$ in \mathbb{Z}_2 so $(p(x))^2 = x^2 + 1$. Likewise we can show that $x + 1$ divides $x^3 + 1$. Using polynomial multiplication, we can show that $(x + 1)(x^2 - x + 1) = (x^3 + 1)$. However we need to show that $x + 1$ divides $x^n + 1$ for any n . ♦

Proposition 25.3.17. If a polynomial $p(x)$ divides $x^n + 1$, then the n -bit polynomial code generated by $p(x)$ is cyclic.

PROOF. Let C be the code generated by $p(x)$, and let $f(x)$ be an arbitrary codeword in C . Then by Definition 25.3.3, $f(x) = a(x)p(x)$. Let $g(x)$ be the cyclic shift of $f(x)$ by 1. By Proposition 25.3.11, $g(x)$ is the remainder of $xf(x)$ when divided by $x^n + 1$. By Proposition 25.3.13, $g(x) = xf(x) + q(x)(x^n + 1)$. Since $p(x)$ divides $x^n + 1$, then $x^n + 1 = s(x)p(x)$. By substitution, $g(x) = xa(x)p(x) + q(x)s(x)p(x) = p(x)\left(xa(x) + q(x)s(x)\right)$. Therefore, $g(x)$ is a multiple of $p(x)$: in other words, $g(x)$ is in the code generated by $p(x)$, which is none other than C . We have thus shown that any cyclic shift of an arbitrary codeword in C is also in C . This is exactly what it means for the code C to be a cyclic code. Thus the proposition is proved. □

Appendix: Induction proofs—patterns and examples

26.1 Basic examples of induction proofs

Below is a complete proof of the formula for the sum of the first n integers, that can serve as a model for proofs of similar sum/product formulas. ¹

Proposition 26.1.1. For all $n \in \mathbb{N}$, the following equation (which we denote as $P(n)$) is true:

$$\sum_{i=1}^n i = \frac{n(n+1)}{2}. \quad (P(n))$$

PROOF. (*By induction*):

Base case: When $n = 1$, the left side of $P(n)$ is 1, and the right side is $1(1+1)/2 = 1$, so both sides are equal and $P(n)$ holds for $n = 1$.

¹This section was taken (with permission!) from A. J. Hildebrand's excellent notes on induction (reformatted and minor edits by C.T.).

Induction step: Let $k \in \mathbb{N}$ be given and suppose formula $P(n)$ holds for $n = k$. Then

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \sum_{i=1}^k i + (k+1) \quad (\text{by definition of } \sum \text{ notation}) \\ &= \frac{k(k+1)}{2} + (k+1) \quad (\text{by induction hypothesis}) \\ &= \frac{k(k+1) + 2(k+1)}{2} \quad (\text{by algebra}) \\ &= \frac{(k+1)((k+1) + 1)}{2} \quad (\text{by algebra}). \end{aligned}$$

Thus, $P(n)$ holds for $n = k + 1$, and the proof of the induction step is complete.

Conclusion: By the principle of induction, we have proved that $P(n)$ holds for all $n \in \mathbb{N}$. \square

26.2 Advice on writing up induction proofs

Here are four things to keep in mind as you write up induction proofs.

#1: Begin any induction proof by stating precisely, and prominently, the statement you plan to prove. This statement typically involves an equation (or assertion) in the variable n , and we're trying to prove this equation (or assertion) for all natural numbers n bigger than a certain value. A good idea is to write out the statement and label it as " $P(n)$ ", so that it's easy to spot, and easy to reference; see the sample proofs for examples.

#2: Be sure to properly begin and end the induction step. From a logical point of view, an induction step is a proof of a statement of the form, "for all $k \in \mathbb{N}$, $P(k) \Rightarrow P(k+1)$ ". To prove such a statement, you need to start out by asserting, "let $k \in \mathbb{N}$ be given", then assume $P(k)$ is true ("Suppose $P(n)$ is true for $n = k$ "), and, after a sequence of logical deductions, derive $P(k+1)$ ("Therefore $P(n)$ is true for $n = k+1$ ").

#3: Use different letters for the general variable appearing in the statement you seek to prove (n in the above example) and the variable used for the induction step (k in the above example). The reason for this distinction is that in the induction step you want to be able to say something like the following: "Let $k \in \mathbb{N}$ be given, and suppose $P(k)$

[Proof of induction step goes here] ... Therefore $P(k + 1)$ is true.” Without introducing a second variable k , such a statement wouldn’t make sense.

#4: Always clearly state, at the appropriate place in the induction step, when the induction hypothesis is being used. E.g., say “By the induction hypothesis we have ...”, or use a parenthetical note “(by induction hypothesis)” in a chain of equations as in the above example. The induction hypothesis is the case $n = k$ of the statement we seek to prove (i.e., the statement “ $P(k)$ ” and it is what you assume at the start of the induction step. The place where this hypothesis is used is the most crucial step in an induction argument, and you must get this hypothesis into play at some point during the proof of the induction step—if not, you are doing something wrong.

26.3 Induction proof patterns & practice problems

Induction proofs, type I: Sum/product formulas

The most common, and the easiest, application of induction is to prove formulas for sums or products of n terms. Many of these proofs follow the same pattern. Here are some examples of formulas that can be proved by induction:

- (i) $\sum_{i=1}^n i(i+1) = \frac{n(n+1)(n+2)}{3}$
- (ii) $\sum_{i=0}^n i!i = (n+1)! - 1$.
- (iii) $\sum_{i=0}^n r^i = \frac{1-r^{n+1}}{1-r}$ ($r \neq 1$) (sum of finite geometric series)
- (iv) $\sum_{i=0}^n 2^i = 2^{n+1} - 1$ (sum of powers of 2)

In the following exercises, we will guide you through the proofs of (i) and (ii). For parts (iii) and (iv), you’re on your own!

Exercise 26.3.1. Fill in the blanks for the following induction proof of formula (i) above.

PROOF. We seek to show that, for all $n \in \mathbb{N}$,

$$\sum_{i=1}^n i(i+1) = \frac{n(n+1)(n+2)}{3}. \quad (P(n))$$

Base case: When $n = 1$, the left side of $P(1)$ is equal to $\underline{\langle 1 \rangle}$, and the right side is equal to $\underline{\langle 2 \rangle}$, so both sides are equal and $P(1)$ is true.

Induction step: Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true. Then

$$\begin{aligned} \sum_{i=1}^{k+1} i(i+1) &= \sum_{i=1}^k i(i+1) + \underline{\langle 3 \rangle} \\ &= \frac{k(k+1)(k+2)}{3} + \underline{\langle 4 \rangle} \quad (\text{by induction hypothesis}) \\ &= \frac{(k+1)(k+2)(k+3)}{3}. \end{aligned}$$

Thus, $P(\underline{\langle 5 \rangle})$ holds, and the proof of the induction step is complete,

Conclusion: By the principle of induction, it follows that $\underline{\langle 6 \rangle}$ is true for all $n \in \mathbb{N}$. \square

\diamond

Exercise 26.3.2. Provide an outline for the proof of formula (ii) by responding to each of the parts below.

- What is the equation that must be shown for all $n \in \mathbb{N}$? (Call this equation " $P(n)$ ").
- Identify the base case, and show that equation $P(n)$ holds for the base case.
- Write the left-hand side of $P(k+1)$.
- Separate off the last term in the sum, so that you have a sum from 1 to k plus an additional term.
- Use the induction hypothesis to replace the sum from 1 to k with a simpler expression.
- Use algebra to obtain $P(k+1)$, which completes the proof of the induction step.
- What is the final conclusion which can be drawn from the above argument?

◇

Exercise 26.3.3.

- (a) Prove formula (iii) above using induction.
 (b) Prove formula (iv) above using induction.

◇

Induction proofs, type II: inequalities

A second general type of application of induction is to prove inequalities involving a natural number n . These proofs also tend to be on the routine side; in fact, the algebra required is usually very minimal, in contrast to some of the summation formulas.

In some cases the inequalities don't "kick in" until n is large enough. By checking the first few values of n one can usually quickly determine the first n -value, say n_0 , for which the inequality holds. Then one may use $n = n_0$ as the base case, instead of $n = 0$.

Here are some examples of integer inequalities that can be proved using induction:

- (i) $2^n > n$
 (ii) $2^n \geq n^2$ ($n \geq 4$)
 (iii) $n! > 2^n$ ($n \geq 4$)
 (iv) $(1 - x)^n \geq 1 - nx$ ($0 < x < 1$)
 (v) $(1 + x)^n \geq 1 + nx$ ($x > 0$)

In the following exercises, we will guide you through the proofs of (iii) and (iv). For the others, you'll have to wing it.

Exercise 26.3.4. Fill in the blanks in the following proof of (iii).

PROOF.

We are trying to show that

$$n! > 2^n \quad (P(n))$$

holds for all $n \geq 4$. (Note that the inequality fails for $n = 1, 2, 3$. But this doesn't matter, because we only have to show that it works for all n from 4 onwards.)

Base case: For $n = 4$, the left and right sides of $P(4)$ are equal to $\underline{< 1 >}$ and $\underline{< 2 >}$, respectively, so $P(4)$ is true.

Induction step: Let $k \geq 4$ be given and suppose $\underline{< 3 >}$ is true. Then

$$\begin{aligned} (k+1)! &= k! \cdot (k+1) \\ &> 2^k \cdot \underline{< 4 >} \quad (\text{by } \underline{< 5 >}) \\ &\geq 2^k \cdot 2 \quad (\text{since } k \geq 4 \text{ and so } k+1 \geq 2) \\ &= \underline{< 6 >}. \end{aligned}$$

Thus, $\underline{< 7 >}$ holds, and the proof of the induction step is complete.

Conclusion: By the principle of induction, it follows that $P(n)$ is true for all $n \geq 4$. \square

\diamond

Exercise 26.3.5. Provide an outline for the proof of the inequality (iv) by giving answers for each of the parts below.

PROOF.

- (a) What statement do you need to prove for every real number $0 < x < 1$ and any $n \in \mathbb{N}$? Call this statement " $P(n)$ ".
- (b) **Base case:** Show that the left and right sides of $P(n)$ are equal in the base case.
- (c) **Induction step:** Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true for any real number $0 < x < 1$. What do we seek to show?
- (d) Rewrite $(1-x)^{k+1}$ as $(1-x)^k \cdot (1-x)$. Then use $P(k)$ to obtain an inequality. Using basic algebra, simplify the right-hand side until you obtain a quantity that is greater than $1 - (k+1)x$.

- (e) What may you conclude about $P(k + 1)$?
- (f) **Conclusion:** What is the ultimate conclusion of the argument?

□

◇

Exercise 26.3.6.

- (a) Prove inequality (i) above using induction.
- (b) Prove inequality (ii) above using induction.
- (c) Prove inequality (v) above using induction.

◇

Induction proofs, type III: Extension of theorems from 2 variables to n variables

Another very common and usually routine application of induction is to extend general results that have been proved for the case of 2 variables to the case of n variables. Below are some examples. In proving these results, use the case $n = 2$ as base case. To see how to carry out the general induction step (from the case $n = k$ to $n = k + 1$), it may be helpful to first try to see how get from the base case $n = 2$ to the next case $n = 3$.

Here are some examples of multiple-variable theorems that can be proved using induction:

- (i) Show that if x_1, \dots, x_n are odd, then $x_1 x_2 \dots x_n$ is odd.
- (ii) Show that if a_i and b_i ($i = 1, 2, \dots, n$) are real numbers such that $a_i \leq b_i$ for all i , then

$$\sum_{i=1}^n a_i \leq \sum_{i=1}^n b_i.$$

- (iii) Show that if x_1, \dots, x_n are real numbers, then

$$\left| \sin \left(\sum_{i=1}^n x_i \right) \right| \leq \sum_{i=1}^n |\sin x_i|.$$

(Use the trig identity for $\sin(\alpha + \beta)$.)

(iv) Show that if A_1, \dots, A_n are sets, then

$$(A_1 \cup \dots \cup A_n)^c = A_1^c \cap \dots \cap A_n^c.$$

(This is a generalization of De Morgan's Law to unions of n sets. Use De Morgan's Law for two sets $((A \cup B)^c = A^c \cap B^c)$ and induction to prove this result.)

We'll give outlines of the proofs of (i) and (ii).

Exercise 26.3.7. This exercise will provide a proof of (i).

(a) We will need the following assertion in the proof:

If x and y are odd, then xy is also odd.

We know that x is odd if and only if $\text{mod}(x,2)=1$. Use this and facts from modular arithmetic to prove the needed assertion.

(b) Fill in the blanks in the following proof of (i).

PROOF. We will prove by induction on n the following statement:

If x_1, \dots, x_n are odd numbers, then $x_1x_2 \dots x_n$ is odd. $(P(n))$

Base case: For $n = 1$, the product $x_1 \dots x_n$ reduces to < 1 >, which is odd whenever x_1 is odd. Hence $P(n)$ is true for $n = 1$.

Induction step.

- Let $k \geq 1$, and suppose $(*)$ is true for $n = k$, i.e., suppose that any product of < 2 > odd numbers is again odd.
- We seek to show that < 3 > is true, i.e., that any product of < 4 > odd numbers is odd.
- Let x_1, \dots, x_{k+1} be odd numbers.
- Applying the induction hypothesis to x_1, \dots, x_k , we obtain that the product < 5 > is odd.
- Since x_{k+1} is < 6 > and, by part (a) the product of two odd numbers is again odd, it follows that $x_1x_2 \dots x_{k+1} = (x_1 \dots x_k)x_{k+1}$ is odd.

- As x_1, \dots, x_{k+1} were arbitrary odd numbers, we have proved $\underline{\quad} < 7 > \underline{\quad}$, so the induction step is complete.

Conclusion: By the principle of induction, it follows that $P(n)$ is true for all $n \in \mathbb{N}$. □

◇

Exercise 26.3.8. Complete an outline of a proof of (ii) by responding to the following items.

- (a) What statement do we want to prove for all natural numbers n and for all real numbers a_i and b_i ($i = 1, \dots, n$) such that $a_i \leq b_i$? Call this statement “P(n)”. (Note that the condition “for all real numbers a_i and b_i ” must be part of the induction statement we seek to prove.)
- (b) **Base case:** Show that $P(1)$ is true.
- (c) **Induction step:** Let $k \geq 1$. Write $P(k)$.
- (d) We seek to prove that $P(k)$ implies $P(k+1)$. We may rewrite $P(k+1)$ as follows (fill in the blanks): Let a_1, \dots, a_{k+1} and b_1, \dots, b_{k+1} be given real numbers such that $\underline{\quad}$ for each i . Then

$$\sum_{i=1}^{k+1} a_i = \underline{\quad} + a_{k+1}.$$

- (e) Assuming that $P(k)$ is true, use Proposition 3.2.17 to show that $P(k+1)$ is also true. This is equivalent to showing that $P(k)$ implies $P(k+1)$.
- (f) **Conclusion:** What is the final conclusion?

◇

26.4 Strong Induction, with applications

One of the most common applications of induction is to problems involving recurrence sequences such as the Fibonacci numbers, and to representation problems such as the representation of integers as a product of primes

(Fundamental Theorem of Arithmetic), sums of powers of 2 (binary representation), and sums of stamp denominations (postage stamp problem).

In applications of this type, the case $n = k$ in the induction step is not enough to deduce the case $n = k + 1$; one usually needs additional predecessors predecessors to get the induction step to work, e.g., the two preceding cases $n = k$ and $n = k - 1$, or *all* preceding cases $n = k, k - 1, \dots, 1$. This variation of the induction method is called **strong induction**. The induction principle remains valid in this modified form.

Strong induction and recurrences

In the induction proofs we've looked at so far, we first had to prove a base case, and then used a preceding case ($n = k$) to prove the case $n = k + 1$ in the induction step. But when we apply induction to two-term recurrence sequences like the Fibonacci numbers, we'll need *two* preceding cases, $n = k$ and $n = k - 1$, in the induction step, and *two* base cases (e.g., $n = 1$ and $n = 2$) to get the induction going. The logical structure of such a proof is of the following form:

Base step: $P(n)$ is true for $n = 1, 2$.

Induction step: Let $k \in \mathbb{N}$ with $k \geq 2$ be given and assume $P(n)$ holds for $n = k$ and $n = k - 1$.

[... Work goes here ...]

Therefore $P(k + 1)$ holds.

Conclusion: By the principle of strong induction, $P(n)$ holds for all $n \in \mathbb{N}$.

Note that in the induction step, one could also say "Assume $P(n)$ holds for " $n = 1, 2, \dots, k$ "; this is a bit redundant as only the last two of the cases $n = 1, 2, \dots, k$ are needed, though logically correct.

Here is a worked-out example of a proof by strong induction.

Proposition 26.4.1. Let a_n be the sequence defined by $a_1 = 1$, $a_2 = 8$, and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geq 3$. Then $a_n = 3 \cdot 2^{n-1} + 2(-1)^n$ for all $n \in \mathbb{N}$.

PROOF. We'll prove by strong induction that, for all $n \in \mathbb{N}$,

$$a_n = 3 \cdot 2^{n-1} + 2(-1)^n. \quad (P(n))$$

Base case: When $n = 1$, the left side of $P(1)$ is $a_1 = 1$, and the right side is $3 \cdot 2^0 + 2 \cdot (-1)^1 = 1$, so both sides are equal and $P(1)$ is true.

When $n = 2$, the left and right sides of $P(2)$ are $a_2 = 8$ and $3 \cdot 2^1 + 2 \cdot (-1)^2 = 8$, so $P(2)$ also holds.

Induction step: Let $k \in \mathbb{N}$ with $k \geq 2$ be given and suppose $P(n)$ is true for $n = 1, 2, \dots, k$. Then

$$\begin{aligned} a_{k+1} &= a_k + 2a_{k-1} \quad (\text{by recurrence for } a_n) \\ &= 3 \cdot 2^{k-1} + 2 \cdot (-1)^k + 2 \left(3 \cdot 2^{k-2} + 2 \cdot (-1)^{k-1} \right) \quad (\text{by } P(k) \text{ and } P(k-1)) \\ &= 3 \cdot \left(2^{k-1} + 2^{k-1} \right) + 2 \left((-1)^k + 2(-1)^{k-1} \right) \quad (\text{by algebra}) \\ &= 3 \cdot 2^k + 2(-1)^{k+1} \quad (\text{more algebra}). \end{aligned}$$

Thus, $P(k+1)$ holds, and the proof of the induction step is complete.

Conclusion: By the strong induction principle, it follows that $P(n)$ is true for all $n \in \mathbb{N}$. \square

Strong Induction and representation problems

For applications to representation problems one typically requires the induction hypothesis in its strongest possible form, where one assumes *all* preceding cases (i.e., for $n = 1, 2, \dots, k$) instead of just the immediate predecessor (as in simple induction) or two predecessors (as in strong induction applied to two-term recurrences).

Below is a classic example of this type, a proof that every integer ≥ 2 can be written as a product of prime numbers. This is the existence part of what is called the Fundamental Theorem of Arithmetic; the other part guarantees uniqueness of the representation, which we will not be concerned with here (it can also be proved by induction, but the proof is a little more complicated).

Recall the definition of *prime* from Chapter 4: an integer $n > 1$ is called *prime* if it has no factor greater than 1 other than itself. An integer $n > 1$ that is not prime is called *composite*: in other words, n can be written as $n = ab$ with integers a, b satisfying $2 \leq a, b < n$. Using these definitions, we may now state and prove:

Proposition 26.4.2. (*Fundamental Theorem of Arithmetic: existence*)

Any integer $n \geq 2$ is either a prime or can be represented as a product of (not necessarily distinct) primes, i.e., in the form $n = p_1 p_2 \dots p_r$, where the p_i are primes.

PROOF. We will prove by strong induction that the following statement holds for all integers $n \geq 2$.

n can be represented as a product of one or more primes. $(P(n))$

Base case: The integer $n = 2$ is a prime since it cannot be written as a product ab , with integers $a, b \geq 2$, so $P(n)$ holds for $n = 2$.

Induction step:

- Let $k \geq 2$ be given and suppose $P(n)$ is true for all integers $2 \leq n \leq k$, i.e., suppose that all such n can be represented as a product of one or more primes.
- We seek to show that $k + 1$ also has a representation of this form.
- If $k + 1$ itself is prime, then $P(n)$ holds for $n = k + 1$, and we are done.
- Now consider the case when $k + 1$ is composite.
- By definition, this means that $k + 1$ can be written in the form $k + 1 = ab$, where a and b are integers satisfying $2 \leq a, b < k + 1$, i.e., $2 \leq a, b \leq k$.
- Since $2 \leq a, b \leq k$, the induction hypothesis can be applied to a and b and shows that a and b can be represented as products of one or more primes.
- Multiplying these two representations gives a representation of $k + 1$ as a product of primes.
- Hence $k + 1$ has a representation of the desired form, so $P(n)$ holds for $n = k + 1$, and the induction step is complete.

Conclusion: By the strong induction principle, it follows that $P(n)$ is true for all $n \geq 2$, i.e., every integer $n \geq 2$ is either a prime or can be represented as a product of primes. \square

26.5 More advice on induction and strong induction proofs

Should I use ordinary induction or strong induction? With some standard types of problems (e.g., sum formulas) it is clear ahead of time what type of induction is *likely* to be required, but usually this question answers itself during the exploratory/scratch phase of the argument. In the induction step you will need to reach the $k + 1$ case, and you should ask yourself which of the previous cases you need to get there. If all you need to prove the $k + 1$ case is the case k of the statement, then ordinary induction is appropriate. If two preceding cases, $k - 1$ and k , are necessary to get to $k + 1$, then (a weak form of) strong induction is appropriate. If one needs the full range of preceding cases (i.e., all cases $n = 1, 2, \dots, k$), then the full force of strong induction is needed.

How many base cases are needed? The number of base cases to be checked depends on how far back one needs to “look” in the induction step. In standard induction proofs (e.g., for summation formulas) the induction step requires only the immediately preceding case (i.e., the case $n = k$), so a single base case is enough to start the induction.

- For Fibonacci-type problems, the induction step usually requires the result for the two preceding cases, $n = k$ and $n = k - 1$. To get the induction started, one therefore needs to know the result for two consecutive cases, e.g., $n = 1$ and $n = 2$.
- In postage stamp type problems, getting the result for $n = k + 1$ might require knowing the result for $n = k - 2$ and $n = k - 6$, say. This amounts to “looking back” 7 steps (namely $n = k, k - 1, \dots, k - 6$), so 7 consecutive cases are needed to get the induction started.
- On the other hand, in problems involving the full strength of the strong induction hypothesis (i.e., if in the induction step one needs to assume the result for *all* preceding cases $n = k, k - 1, \dots, 1$), a single base case may be sufficient. An example is the Fundamental Theorem of Arithmetic.

How do I write the induction step? As in the case of ordinary induction, at the beginning of the induction step *state precisely what you are assuming, including any constraints on the induction variable k* . Without

an explicitly stated assumption, the argument is incomplete. The appropriate induction hypothesis depends on the nature of the problem and the type of induction used. Here are some common ways to start out an induction step:

- “Let $k \in \mathbb{N}$ be given and assume $P(k)$ is true.” (typical form for standard induction proofs)
- “Let $k \geq 2$ be given and assume $P(n)$ holds for $n = k - 1$ and $n = k$.” (typical form for induction involving recurrences)
- “Let $k \in \mathbb{N}$ be given and assume $P(n)$ holds for $n = 1, 2, \dots, k$.” (typical form for representation problems)

26.6 Common mistakes

The following examples illustrate some common mistakes in setting up base case(s) and the induction step.

Example 1.

- **Base step:** $n = 3$.
- **Induction step:** Let $k \in \mathbb{N}$ with $k \geq 3$ be given and assume $P(n)$ is true for $n = k$ and $n = k - 1$.
- **Comment: BAD:** When $k = 3$ (the first case of the induction step), the induction step requires the cases 3 and 2, but only 2 is covered in the base step.
FIX: Add the case $n = 2$ to the base step.

Example 2.

- **Base step:** $n = 1$ and $n = 2$.
- **Induction step:** Let $k \in \mathbb{N}$ with $k > 2$ be given and assume $P(n)$ is true for $n = k$ and $n = k - 1$.
- **Comment: BAD.** Gap between base case and the first case of the induction step: The first case $k = 3$ of the induction step requires the cases 3 and 2, but the base step only gives the cases 1 and 2.
FIX: Start induction step at $k = 2$ rather than $k = 3$: “Let $k \in \mathbb{N}$ with $k \geq 2$ be given ...”

Example 3.

- **Base step:** $n = 1$ and $n = 2$.
- **Induction step:** Assume $P(n)$ is true for $n = k$ and $n = k - 1$. Then ...
- **Comment: BAD.** The variable k in the induction step is not quantified.
FIX: Add “Let $k \in \mathbb{N}$ with $k \geq 2$ be given.”

Example 4.

- **Base step:** $n = 1$ and $n = 2$.
- **Induction step:** Let $k \in \mathbb{N}$ be given and assume $P(n)$ is true for $n = k$ and $n = k - 1$.
- **Comment: BAD.** Here the first case induction step is $k = 1$, with the induction hypothesis being the cases $n = k$ and $n = k - 1$. But when $k = 1$, the second of these cases, $n = k - 1 = 0$, is out of range.
FIX: Add the restriction $k \geq 2$ to the induction step: “Let $k \in \mathbb{N}$ with $k \geq 2$ be given.”

26.7 Strong induction practice problems

1. **Recurrences:** The first few problems deal with properties of the Fibonacci sequence and related recurrence sequences. The Fibonacci sequence is defined by $F_1 = 1$, $F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$. Its first few terms are 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

In the following problems, use an appropriate form of induction (standard induction or strong induction) to establish the desired properties and formulas. (Note that some of these problems require only ordinary induction.)

- (a) **Fibonacci sums:** Prove that $\sum_{i=1}^n F_i = F_{n+2} - 1$ for all $n \in \mathbb{N}$.
- (b) **Fibonacci matrix:** Show that, for all $n \in \mathbb{N}$,

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}. \quad (P(n))$$

- (c) **Odd/even Fibonacci numbers:** Prove that the Fibonacci numbers follow the pattern odd,odd,even: that is, show that for any positive integer m , F_{3m-2} and F_{3m-1} are odd and F_{3m} is even.
- (d) **Inequalities for recurrence sequences:** Let the sequence T_n (“Tribonacci sequence”) be defined by $T_1 = T_2 = T_3 = 1$ and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ for $n \geq 4$. Prove that

$$T_n < 2^n \quad (P(n))$$

holds for all $n \in \mathbb{N}$.

We’ll give an outline for the proof of (d).

We will prove $P(n)$ by strong induction.

Base step: For $n = 1, 2, 3$, T_n is equal to __, whereas the right-hand side of $P(n)$ is equal to $2^1 = 2$, $2^2 = 4$, and $2^3 = 8$, respectively. Thus, $P(n)$ holds for $n = 1, 2, 3$.

Induction step: Let $k \geq 3$ be given and suppose $P(n)$ is true for all $n = 1, 2, \dots, k$. Then

$$\begin{aligned} T_{k+1} &= T_k + T_{k-1} + _ \quad (\text{by recurrence for } T_n) \\ &< 2^k + 2^{k-1} + _ \quad (\text{strong ind. hyp. \& } (P(k), P(k-1), P(k-2))) \\ &= 2^{k+1} \left(\frac{1}{2} + \frac{1}{4} + _ \right) \\ &= 2^{k+1} \cdot _ < 2^{k+1}. \end{aligned}$$

Thus, __ holds, and the proof of the induction step is complete.

Conclusion: By the strong induction principle, it follows that $P(n)$ is true for all $n \in \mathbb{N}$.

2. **Representation problems.** One of the main applications of strong induction is to prove the existence of representations of integers of various types. In these applications, strong induction is usually needed in its full force, i.e., in the induction step, one needs to assume that all predecessor cases $n = 1, 2, \dots, k$.

- (a) **The postage stamp problem:** Determine which postage amounts can be created using the stamps of 3 and 7 cents. In other words, determine the exact set of positive integers n that can be written in the form $n = 3x + 7y$ with x and y nonnegative integers. (*Hint:* Check the first few values of n directly, then use strong induction to show that, from a certain point n_0 onwards, all numbers n have such a representation.)

- (b) **Binary representation:** Using strong induction prove that every positive integer n can be represented as a sum of *distinct* powers of 2, i.e., in the form $n = 2^{i_1} + \cdots + 2^{i_h}$ with integers $0 \leq i_1 < \cdots < i_h$. (*Hint:* To ensure distinctness, use the *largest* power of 2 as the first “building block” in the induction step.)
- (c) **Factorial representation.** Show that any integer $n \geq 1$ has a representation in the form $n = d_1 1! + d_2 2! + \cdots + d_r r!$ with “digits” d_i in the range $d_i \in \{0, 1, \dots, i\}$. (*Hint:* Use again the “greedy” trick (pick the largest factorial that “fits” as your first building block), and use the fact (established in an earlier problem) that $\sum_{i=1}^k i!i = (k+1)! - 1$.)

26.8 Non-formula induction proofs

Below is a sample proof of the statement that any n -element set (i.e., any set with n elements) has 2^n subsets. This illustrates a case where the result we seek to prove is not a formula, but a statement that must be expressed verbally, and where the induction step requires some verbal explanation, and not just a chain of equalities. Additional practice problems follow below.

Proposition 26.8.1. For all $n \in \mathbb{N}$, the following holds:

$$\text{Any } n\text{-element set has } 2^n \text{ subsets.} \quad (P(n))$$

PROOF. (*By induction*):

Base case: Since any 1-element set has 2 subsets, namely the empty set and the set itself, and $2^1 = 2$, the statement $P(n)$ is true for $n = 1$.

Induction step:

- Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true, i.e., that any k -element set has 2^k subsets. We seek to show that $P(k+1)$ is true as well, i.e., that any $(k+1)$ -element set has 2^{k+1} subsets.
- Let A be a set with $k+1$ elements.
- Let a be an element of A , and let $A' = A - \{a\}$ (so that A' is a set with k elements).

- We classify the subsets of A into two types: (I) subsets that do *not* contain a , and (II) subsets that do contain a .
- The subsets of type (I) are exactly the subsets of the set A' . Since A' has k elements, the induction hypothesis can be applied to this set and we conclude that there are 2^k subsets of type (I).
- The subsets of type (II) are exactly the sets of the form $B = B' \cup \{a\}$, where B' is a subset of A' . By the induction hypothesis there are 2^k such sets B' , and hence 2^k subsets of type (II).
- Since there are 2^k subsets of each of the two types, the total number of subsets of A is $2^k + 2^k = 2^{k+1}$.
- Since A was an arbitrary $(k+1)$ -element set, we have proved that any $(k+1)$ -element set has 2^{k+1} subsets. Thus $P(k+1)$ is true, completing the induction step.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$.

□

26.9 Practice problems for non-formula induction

1. **Number of subsets with an even (or odd) number of elements:** Using induction, prove that an n -element set has 2^{n-1} subsets with an even number of elements and 2^{n-1} subsets with an odd number of elements.
2. **Number of regions created by n lines:** How many regions are created by n lines in the plane such that no two lines are parallel and no three lines intersect at the same point? Guess the answer from the first few cases, then use induction to prove your guess.
3. **Sum of angles in a polygon:** The sum of the interior angles in a triangle is 180 degrees, or π . Using this result and induction, prove that for any $n \geq 3$, the sum of the interior angles in an n -sided polygon is $(n-2)\pi$.
4. **Pie-throwing problem:** Here is a harder, but fun problem. Consider a group of n fraternity members standing in a yard, such that their mutual distances are all distinct. Suppose each of throws a pie at his

nearest neighbor. Show that if n is odd, then there is one person in the group who does not get hit by a pie. (*Hint:* Let $n = 2m + 1$ with $m \in \mathbb{N}$, and use m as the induction variable. Consider first some small cases, e.g., $n = 3$ and $n = 5$.)

26.10 Fallacies and pitfalls

By now, induction proofs should feel routine to you, to the point that you could almost do them in your sleep. However, it is important not to become complacent and careless, for example, by skipping seemingly minor details in the write-up, omitting quantifiers, or neglecting to check conditions and hypotheses.

Below are some examples of false induction proofs that illustrate what can happen when some minor details are left out. In each case, the statement claimed is clearly nonsensical (e.g., that all numbers are equal), but the induction argument sounds perfectly fine, and in some cases the errors are quite subtle and hard to spot. Try to find them!

Example 26.10.1. Let us “prove” that for all $n \in \mathbb{N}$,

$$\sum_{i=1}^n i = \frac{1}{2}\left(n + \frac{1}{2}\right)^2 \quad (P(n))$$

Proof: We prove the claim by induction.

Base step: When $n = 1$, $P(n)$ holds.

Induction step: Let $k \in \mathbb{N}$ and suppose $P(k)$ holds. Then

$$\begin{aligned} \sum_{i=1}^{k+1} i &= \sum_{i=1}^k i + (k+1) \\ &= \frac{1}{2} \left(k + \frac{1}{2} \right)^2 + (k+1) \quad (\text{by ind. hypothesis}) \\ &= \frac{1}{2} \left(k^2 + k + \frac{1}{4} + 2k + 2 \right) \quad (\text{by algebra}) \\ &= \frac{1}{2} \left(\left(k + 1 + \frac{1}{2} \right)^2 - 3k - \frac{9}{4} + k + \frac{1}{4} + 2k + 2 \right) \quad (\text{more algebra}) \\ &= \frac{1}{2} \left((k+1) + \frac{1}{2} \right)^2 \quad (\text{simplifying}). \end{aligned}$$

Thus, $P(k+1)$ holds, so the induction step is complete.

Conclusion: By the principle of induction, $P(n)$ holds for all $n \in \mathbb{N}$. \blacklozenge

Example 26.10.2. Now we will “prove” that all real numbers are equal. To prove the claim, we will prove by induction that, for all $n \in \mathbb{N}$, the following statement holds:

For any real numbers a_1, a_2, \dots, a_n , we have $a_1 = a_2 = \dots = a_n$. ($P(n)$)

Base step: When $n = 1$, the statement is trivially true, so $P(1)$ holds.

Induction step: Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true, i.e., that any k real numbers must be equal. We seek to show that $P(k+1)$ is true as well, i.e., that any $k+1$ real numbers must also be equal.

Let a_1, a_2, \dots, a_{k+1} be given real numbers. Applying the induction hypothesis to the first k of these numbers, a_1, a_2, \dots, a_k , we obtain

$$a_1 = a_2 = \dots = a_k. \quad (1)$$

Similarly, applying the induction hypothesis to the last k of these numbers, $a_2, a_3, \dots, a_k, a_{k+1}$, we get

$$a_2 = a_3 = \dots = a_k = a_{k+1}. \quad (2)$$

Combining (1) and (2) gives

$$a_1 = a_2 = \dots = a_k = a_{k+1}, \quad (3)$$

so the numbers a_1, a_2, \dots, a_{k+1} are equal. Thus, we have proved $P(k+1)$, and the induction step is complete.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. Thus, any n real numbers must be equal. \blacklozenge

Example 26.10.3. Here is a “proof” that for every nonnegative integer n ,

$$5n = 0. \quad (P(n))$$

Proof: We prove that $P(n)$ holds for all $n = 0, 1, 2, \dots$, using strong induction with the case $n = 0$ as base case.

Base step: When $n = 0$, $5n = 5 \cdot 0 = 0$, so $P(n)$ holds in this case.

Induction step: Suppose $P(n)$ is true for all integers n in the range $0 \leq n \leq k$, i.e., that for all integers in this range $5n = 0$. We will show that $P(k+1)$ also holds, so that

$$5(k+1) = 0. \quad (P(k+1))$$

Write $k+1 = i+j$ with integers i, j satisfying $0 \leq i, j \leq k$. Applying the induction hypothesis to i and j , we get $5i = 0$ and $5j = 0$. Then

$$5(k+1) = 5(i+j) = 5i + 5j = 0 + 0 = 0,$$

proving $P(k+1)$. Hence the induction step is complete.

Conclusion: By the principle of strong induction, $P(n)$ holds for all nonnegative integers n . \blacklozenge

Example 26.10.4. Let’s “prove” that for every nonnegative integer n ,

$$2^n = 1 \quad (P(n))$$

Proof: We prove that $P(n)$ holds for all $n = 0, 1, 2, \dots$, using strong induction with the case $n = 0$ as base case.

Base step: When $n = 0$, $2^0 = 1$, so $P(0)$ holds. (Note: it is perfectly OK to begin with a base case of $n = 0$.)

Induction step: Suppose $P(n)$ is true for all integers n in the range $0 \leq n \leq k$, i.e., assume that for all integers in this range $2^n = 1$. We will show that $P(k+1)$ also holds, i.e.,

$$2^{k+1} = 1 \quad (P(k+1))$$

We have

$$\begin{aligned}
 2^{k+1} &= \frac{2^{2k}}{2^{k-1}} && \text{(by algebra)} \\
 &= \frac{2^k \cdot 2^k}{2^{k-1}} && \text{(by algebra)} \\
 &= \frac{1 \cdot 1}{1} && \text{(by strong ind. hypothesis applied to each term)} \\
 &= 1 && \text{(simplifying),}
 \end{aligned}$$

proving $P(k+1)$. Hence the induction step is complete.

Conclusion: By the principle of strong induction, $P(n)$ holds for all nonnegative integers n . \blacklozenge

Example 26.10.5. We will “prove” that all positive integers are equal. To prove this claim, we will prove by induction that, for all $n \in \mathbb{N}$, the following statement holds:

$$\text{For any } x, y \in \mathbb{N}, \text{ if } \max(x, y) = n, \text{ then } x = y. \quad (P(n))$$

(Here $\max(x, y)$ denotes the larger of the two numbers x and y , or the common value if both are equal.)

Base step: When $n = 1$, the condition in $P(1)$ becomes $\max(x, y) = 1$. But this forces $x = 1$ and $y = 1$, and hence $x = y$.

Induction step: Let $k \in \mathbb{N}$ be given and suppose $P(k)$ is true. We seek to show that $P(k+1)$ is true as well.

Let $x, y \in \mathbb{N}$ such that $\max(x, y) = k+1$. Then $\max(x-1, y-1) = \max(x, y) - 1 = (k+1) - 1 = k$. By the induction hypothesis, it follows that $x-1 = y-1$, and therefore $x = y$. This proves $P(k+1)$, so the induction step is complete.

Conclusion: By the principle of induction, $P(n)$ is true for all $n \in \mathbb{N}$. In particular, since $\max(1, n) = n$ for any positive integer n , it follows that $1 = n$ for any positive integer n . Thus, all positive integers must be equal to 1 \blacklozenge

GNU Free Documentation License

Version 1.2, November 2002

Copyright © 2000,2001,2002 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The purpose of this License is to make a manual, textbook, or other functional and useful document “free” in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of “copyleft”, which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. Applicability And Definitions

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The “**Document**”, below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as “**you**”. You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A “**Modified Version**” of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A “**Secondary Section**” is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document’s overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The “**Invariant Sections**” are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The “**Cover Texts**” are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A “**Transparent**” copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not “Transparent” is called “**Opaque**”.

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using

a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The “**Title Page**” means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, “Title Page” means the text near the most prominent appearance of the work’s title, preceding the beginning of the body of the text.

A section “**Entitled XYZ**” means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as “**Acknowledgements**”, “**Dedications**”, “**Endorsements**”, or “**History**”.) To “**Preserve the Title**” of such a section when you modify the Document means that it remains a section “Entitled XYZ” according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. Verbatim Copying

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. Copying In Quantity

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. Modifications

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

- B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C. State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D. Preserve all the copyright notices of the Document.
- E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H. Include an unaltered copy of this License.
- I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.
- J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. Combining Documents

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. Collections Of Documents

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. Aggregation With Independent Works

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an “aggregate” if the copyright resulting from the compilation is not used to limit the legal rights of the compilation’s users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document’s Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. Translation

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled “Acknowledgements”, “Dedications”, or “History”, the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. Termination

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. Future Revisions Of This License

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <http://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License “or any later version” applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

Addendum: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

Copyright © YEAR YOUR NAME. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled “GNU Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the “with ... Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Index

- direct product, [732](#)
- Abelian group, [506](#)
 - classification, [736](#)
- Actions
 - compatibility property of, [792](#)
 - group, [790](#), [794](#), [795](#)
 - left and right, [795](#)
- Adleman, L., [285](#)
- Algebra
 - high school and college, [11](#)
- Algebraic
 - element, of a field, [916](#)
- Algebraic closure
 - of a field, [918](#)
- Algebraically closed
 - field, [914](#)
- Amplitude, [77](#)
- Argument
 - of complex number, [48](#)
- Arithmetic
 - modular, [94](#)
- Arrow diagram, [210](#)
- Associative
 - in ordinary arithmetic, [12](#)
- Associative property, [41](#)
- modular
 - addition/multiplication, [125](#)
- Associativity
 - of function composition, [244](#)
- Automorphism
 - inner, [750](#)
 - of a group, [721](#), [749](#)
- Axiom, [11](#)
- BAC – CAB* rule, [357](#)
- Balanced operations
 - in ordinary arithmetic, [17](#)
- Banded matrix, [765](#)
- Bijection
 - as a permutation, [451](#)
 - definition of, [235](#)
 - relation to inverse functions, [255](#)
- Binary
 - operation, [504](#)
- Binary n -tuple, [924](#)
- Binary Relation, [581](#)
- Bits
 - check bits, [683](#)
 - information bits, [683](#)
- Block code, [663](#), [683](#)

- Burnside's conjecture, 653
- Burnside, William, 528
- Caesar, Julius, 269
- Cancellation law
 - for groups, 525
- Carmichael numbers, 297
- Cartesian product
 - formal definition, 202
- Cayley table, 512
- Cayley's Theorem, 727
- Cayley, Arthur, 730
- Ceiling
 - of a real number, 291
- Center
 - of a group, 548
- Centralizer
 - of an element, 654
- Check bits, 683
- Chinese Remainder Theorem, 149
- Cipher, 267
- Ciphertext, 267
- Cis
 - definition, 49
- Class equation, 851
- Classification
 - abelian groups, 736
- Closure
 - integers mod n , 121
- Code
 - block code, 683
 - dual, 698
 - group, 672
 - Hamming, 698
 - ISBN, 105
 - linear, 680
 - minimum distance of, 666
 - orthogonal, 698
 - reversible, 928
 - UPC, 103
- Codeword, 660
 - palindromic, 928
 - weight of, 666, 674
- Codomain, 205
 - of a function, 212
- Commutative
 - diagram, 842
 - in ordinary arithmetic, 12
- Commutative property, 41
 - for compositions, 244
 - modular
 - addition/multiplication, 125
 - of disjoint cycles, 466
- Complement
 - definition, 187
- Complete polynomials, 935
- Complex numbers
 - addition, 35
 - additive properties, 41
 - complex conjugate, 43
 - definition, 29
 - definition of, 29
 - division rule, 38
 - imaginary part, 29
 - modulus, 42
 - polar representation, 48
 - real part, 29
 - rectangular or Cartesian representation, 46
 - subtraction, 37
 - vector representation, 47
- Complex plane, 46
- Composite number
 - definition, 948
- Composition
 - Associative property, 244
 - definition of, 243
 - law of, 504
 - of cycles, 461

- of permutations, 452
 - of sets, 642
 - of symmetries, 452
- Conjugacy
 - class, 850
- Conjugate
 - element, 846
- Conjugate, complex, 43
- Conjugation
 - of permutations, 843
 - operation on groups, 846
 - relabeling method, 843
- Contrapositive, 99, 223
- Converse, 99
- Coset
 - double, 655
 - leader, 696
 - left, 624
 - representative, 624
 - right, 625
- Cryptanalysis, 270
- Cryptoquip, 275
- Cryptosystem
 - affine, 272
 - definition of, 267
 - monoalphabetic, 275
 - polyalphabetic, 276
 - private key, 268
 - public key, 268
 - single key, 268
- Cycle
 - as products of transpositions, 483
 - composition, 461
 - disjoint, 464
 - inverse of, 485
 - length of, 459
 - order of, 475
 - powers of, 473
 - transposition, 482
- Cycle notation, 458
- Cyclic
 - n -shift, 925
 - 1-shift, 925
 - code, 926
- Cyclic group, 537
 - generator, 537
- Cyclic subgroup
 - in EC cryptography, 570
- De Morgan's laws for sets, 193
- Decimal representation
 - of integers, 158
- Decoding function, 663
- Decoding table, 696
- Decryption
 - definition, 268
 - function, 268
- Degree
 - of a polynomial, 379
- Determinant
 - of a 2×2 matrix, 517
- Dickson, L. E., 653
- Diffie, W., 283
- Digraph, 584
 - of a permutation, 465
- Diophantine equation, 138
- Direct product
 - of groups, 732
 - order of elements, 736
- Direct product of groups
 - internal, 746
- Disjoint
 - definition of, 186
- Disjoint cycles
 - order of, 481
 - powers of, 481
- Distributive
 - in ordinary arithmetic, 12
- Distributive property

- modular
 - addition/multiplication, 125
- Division algorithm
 - for polynomials, 399
- Domain, 205
 - of a function, 212
- Element
 - centralizer of, 654
 - identity, 505
 - inverse, 505
 - of a set, 178
 - order of, 540
- Element by element proof, 190
- Empty set, 182
- Encoder, 660
- Encoding function, 664
- Encryption
 - definition, 267
 - function, 268
- Equality
 - of polynomials, 381
- Equation, Diophantine, 138
- Equivalence class, 607, 800
- Equivalence relation, 595
- Error, 661
- Error detection codes
 - ISBN, 105
- Euclid's lemma, 33
 - proof, 145
- Euclidean algorithm, 134
- Euler ϕ -function, 634
- Euler's formula
 - For networks on a sphere, 825
- Euler's theorem, 635
- Euler, Leonhard, 633
- Even parity
 - coding scheme, 661
- Exponent laws, 526
- Fermat
 - factorization algorithm, 292
 - last theorem, 76
 - little theorem, 296, 636
- Field
 - algebraic closure of, 918
 - algebraic element of, 916
 - algebraic extension, 918
 - algebraically closed, 914
 - extension, 916
 - transcendental element of, 916
- Finite fields
 - in EC cryptography, 570
- First Isomorphism Theorem
 - for groups, 787
- Fixed point set
 - of a group element, 802
- Floor function, 591, 833
- FOIL (FLOI) method, 36, 377
- Fractions
 - in ordinary arithmetic, 17
- Frequency analysis, 271
- Function
 - as a bijection, 255
 - decryption, 268
 - encoding, 663
 - encryption, 268
 - formal definition, 211
 - inverse of, 254
 - invertible, 256
 - onto, 227
 - strictly increasing, 224
- G -equivalent, 799
- G -set, 794
- Galois, Évariste, 528
- Generator
 - in EC cryptography, 570
 - of a cyclic group, 537

- Geometric series
 - sum of, 318
- Group
 - abelian, 506
 - alternating, 499
 - automorphism, 721
 - automorphism of, 749
 - center of, 654
 - commutative, 506
 - cyclic, 537
 - definition, 126, 195, 505
 - dihedral, 435
 - factor, 643
 - finite, 506
 - Heisenberg, 547
 - homomorphism of, 776
 - infinite, 506
 - isomorphic, 455, 702, 707
 - isomorphism of, 707
 - monster, 653
 - non-abelian, 506
 - noncommutative, 506
 - of units $U(n)$, 515
 - order of, 506
 - permutation, 456
 - quotient, 643
 - simple, 645
 - special linear ($SL_n(\mathbb{R})$), 533
 - sporadic, 653
 - symmetric, 454
 - trivial, 506
 - wallpaper, 446
- Group code, 672, 680
- Hamming code
 - definition, 698
 - perfect, 699
 - shortened, 699
- Hamming distance, 665, 666
- Hamming, R., 700
- Hellman, M., 283
- Homomorphic image, 776
- Homomorphism, 776
 - kernel, 784
 - surjective, 788
- Horizontal line test
 - for one-to-one functions, 220
 - for onto functions, 231
- Identity
 - additive, 40
 - element, 505
 - in ordinary arithmetic, 12
 - of a permutation, 452
 - of permutation groups, 460
 - of transpositions, 483
- Identity map, 257
- Image
 - of an element under a function, 212
- Imaginary number, 29
- Imaginary part, 29
- Index of a subgroup, 629
- Induction, 56
- Inequality
 - nonstrict, 16
 - strict, 16
- Inequality reversal
 - in ordinary arithmetic, 17
- Information bits, 683
- Injective (one-to-one), 217
- Inner product, 674
 - notation, 104
- Integer lattice, 832
- Integers mod n , 103
 - as equivalence classes, 613
- Integers mod n
 - additive identity, 123
- Integers modulo, 615
- Internal direct product, 746

- Intersection, 183
- Inverse
 - additive, 40
 - element, 505
 - function, 254
 - in ordinary arithmetic, 12
 - integers mod n , 123
 - multiplicative, 37
 - of a cycle, 485
 - of permutations, 453
 - of transpositions, 484
- Inverse function
 - in cryptography, 268
 - notation, 257
 - relation to bijection, 255
- Invertible function, 256
- Irrational number
 - definition of, 31
 - existence proof, 31
- Isomorphic groups, 455
- Isomorphism
 - definition of, 455
 - of groups, 707
 - of rings, 756
- Jordan, C., 653
- Kernel
 - as a normal subgroup, 784
 - of a homomorphism, 784
- Key
 - definition of, 268
 - private, 268
 - public, 268
 - single, 268
- key
 - in cryptography, 551
- Klein, Felix, 528
- Kronecker delta, 330
- Lagrange, Joseph-Louis, 528, 633
- Law of cancellation, 525
- Law of cosines, 68
- Left regular representation, 728
- Length
 - of a vector, 339
- Lie, Sophus, 528
- Lower-triangular matrix, 765
- Mandelbrot set, 83
- Matrices
 - invertible, 518
 - similar, 345
- Matrix
 - backward difference, 335
 - banded, 765
 - determinant, 278
 - discrete second derivative, 334
 - forward difference, 335
 - generator, 684
 - lower triangular, 765
 - null space of, 675
 - invertible, 518
 - parity-check, 681
 - rotation, 534
 - transpose, 337
- Matrix groups
 - GL_2 , 518
 - M_2 , 517
- Maximum-likelihood decoding, 669
- Message block, 686
- Metric
 - definition, 668
- Minimum distance, 674
- Modular addition, 113
- Modular arithmetic
 - on equivalence classes, 614
- Modular equations, 103
 - addition, 107

- Modular equivalence
 - alternative definition, [100](#)
 - first definition, [98](#)
- Modulus, [42](#), [94](#)
- Natural number, [181](#)
- non-abelian operations, [67](#)
- Normal subgroup, [637](#), [784](#)
- Normalizer, [549](#)
- Null space
 - of a matrix, [675](#)
- Number
 - natural, [181](#)
- One-to-one
 - alternate definition, [224](#)
 - definition, [217](#)
 - horizontal line test, [220](#)
 - informal definition, [216](#)
- Onto, [227](#)
 - formal definition, [229](#)
 - horizontal line test for, [231](#)
- Operation
 - binary, [504](#)
 - definition of, [196](#)
- operations
 - non-abelian, [67](#)
- Orbit
 - of a group element, [536](#)
 - Of a G -set, [800](#)
- Order
 - of a group element, [540](#)
 - of a set, [454](#)
 - disjoint cycles, [481](#)
 - of a cycle, [475](#)
 - of a group, [506](#)
 - of a permutation, [477](#)
 - of group elements
 - in product group, [736](#)
- Order relation
 - in ordinary arithmetic, [15](#)
- Ordered pair
 - as a function, [210](#)
 - definition of, [201](#)
- Palindromic
 - codeword, [928](#)
- Parity
 - canonical parity-check matrix, [681](#)
 - odd, [662](#)
 - parity check bit, [662](#)
- Partition, [588](#)
 - definition of, [588](#)
- Period, [77](#)
- Permutation, [347](#)
 - conjugate, [843](#)
 - cycle, [458](#)
 - definition of, [451](#)
 - identity, [452](#), [460](#)
 - inverse, [453](#)
 - matrix, [497](#)
 - odd and even, [347](#), [495](#)
 - parity, [495](#)
- Permutation group, [456](#)
- Permutation matrix
 - determinant, [498](#)
- Permutations
 - conjugate, [501](#)
- Phase shift, [78](#)
- Phasor, [81](#)
- Plaintext, [267](#)
- Platonic solids, [820](#)
- Point doubling
 - in elliptic curves, [566](#)
- Polar coordinates, [48](#)
- Polygon
 - regular, [435](#)
- Polyhedron
 - regular, [797](#)

- Polynomial
 - leading coefficient, 379
 - addition, 374
 - coefficients, 378
 - monic, 416
 - roots, 374
 - scalar multiplication of, 374
- Polynomial code
 - generated by a polynomial, 931
- Polynomials
 - over M_n , 389
 - over $\mathbb{R}[x]$, 388
 - over \mathbb{Z}_n , 386
 - over $n\mathbb{Z}$, 387
 - product, 383
 - sum, 381
- Power set, 587
- Prime
 - definition, 33
 - Miller-Rabin test for, 296
 - relatively, 145
- Private Key
 - in cryptography, 551
- Product
 - of groups, 511
 - of polynomials, 383
- Proof
 - statement-reason format, 19
- Proof by contradiction, 26
- Proofs
 - “statement–reason” format, 32
- Proposition
 - mathematical, 11
- Pseudoprime, 296
- Public Key
 - in cryptography, 551
- Quaternion group (Q_8), 509, 723
- Quotient
 - under integer division, 97
- Range, 207
- Recursive process, 160
- Reflection, 347
- Reflection (rigid motion), 421
- Reflexive, 594
 - property of relations, 592
- Regular representation
 - left, 728
 - right, 729
- Relation
 - binary, 581
 - definition of, 581
 - reflexive, 592, 594
 - symmetric, 592, 594
 - transitive, 592, 594
- Relatively prime
 - definition, 145
- Remainder
 - under integer division, 97
- Repetition
 - encoding, 662
- Representatives
 - as coset leaders, 696
- Reversible code, 928
- Rhombus, 69, 70
- Right regular representation, 729
- Rigid motion, 421
- Ring isomorphism, 756
- Rivest, R., 285
- Root
 - of a real function, 28
- Roots
 - of polynomial equations, 73
 - of unity, 61
- roots
 - of polynomial, 374
- Rotation

- as rigid motion, [421](#)
- scalar multiplication
 - of polynomials, [374](#)
- Set
 - definition of, [178](#)
 - elements, [178](#)
 - empty set, [182](#)
 - generated by group element, [536](#)
- Set difference, [187](#)
- Set operations, [183](#)
 - complement, [187](#)
 - De Morgan's laws for sets, [193](#)
 - disjoint, [186](#)
 - intersection, [183](#)
 - set difference, [187](#)
 - symmetric difference, [197](#)
 - union, [183](#)
- Sets
 - disjoint, [186](#)
- Shamir, A., [285](#)
- Shannon, C., [700](#)
- Sieve of Eratosthenes, [292](#)
- Simple group, [645](#)
- Soccer ball, [820](#)
- Standard generator matrix, [684](#)
- Statement-reason
 - proof, [19](#)
- Step size
 - for arithmetic sum, [318](#)
- Subdiagonal
 - of a matrix, [757](#)
- Subgroup, [456](#)
 - commutator, [655](#)
 - cyclic, [540](#)
 - definition of, [529](#)
 - index of, [629](#)
 - isotropy, [801](#)
 - necessary conditions, [531](#)
 - normal, [637](#), [639](#)
 - relation to subset, [529](#)
 - stabilizer, [801](#)
- Subring
 - Without unity, [866](#)
- Subset
 - definition of, [181](#)
 - proper, [182](#)
- Substitution
 - as proof technique, [33](#)
 - in ordinary arithmetic, [17](#)
- Substitution property, [525](#)
- Sum
 - of polynomials, [381](#)
 - of sets, [641](#)
- Surjective
 - also see onto, [227](#)
- Symmetric, [594](#)
 - property of relations, [592](#)
- Symmetric Key
 - in cryptography, [551](#)
- Symmetry
 - definition, [420](#)
- Syndrome of a code, [693](#)
- Table
 - multiplication, [120](#)
- Theorem, [11](#)
- Trace
 - of a matrix, [343](#)
- Transcendental
 - element, of a field, [916](#)
- Transitive, [594](#)
 - property of relations, [592](#)
- Translation
 - as a rigid motion, [421](#)
- Transpose
 - of a matrix, [337](#)
- Transposition

- definition of, [482](#)
- error, [104](#)
- triangle inequality
 - for complex numbers, [83](#)
- Union, [183](#)
- Unit
 - in \mathbb{Z}_n , [744](#)
- Unit square, [833](#)
- Units
 - group of $(U(n))$, [515](#)
- Universal set, [180](#)
- Vector space
 - infinite dimensional, [756](#)
 - vector space
 - over \mathbb{R} , [753](#)
- Wallpaper groups, [446](#)
- Wave superposition, [80](#)
- Wavelength, [77](#)
- Weight of a codeword, [666](#)
- Well defined, [618](#)
- zero
 - vector, [753](#)
- Zero divisors
 - in ordinary arithmetic, [13](#)