

Finite Euclidean and Non-Euclidean Geometries

R. De Vogelaere¹

¹Department of Mathematics
University of California, Berkeley, CA

Foreword

The author of this monograph was my father, Professor René De Vogelaere. He received his PhD in Mathematics in 1948 from the University Louvain, Belgium. Shortly after graduation, he immigrated to Canada and taught at l'Université Laval in Quebec, followed by Notre Dame in South Bend, Indiana and then the University of California, Berkeley, where he spent most of his career. He studied and taught a wide range of subjects, including differential equations, numerical analysis, number theory, group theory, and Euclidean geometry, to mention a few.

Georges Lemaître, the founder of the “Big Bang” theory, was my father’s thesis advisor and lifelong mentor. He was often a guest in our home, and at these meetings he encouraged my father to study astronomy and planetary motion. After earning his doctorate degree, Professor Lemaître spent a year working with Arthur Eddington. Professor Eddington postulated that there were a finite number of protons in the universe. This is known as Eddington’s number.

René spent much of his career modeling the continuous world with discrete, finite numbers. In the late 70’s he asked himself: what if the world was discrete rather than continuous? Would the proofs found in different mathematical branches still work? That is when his research in finite geometry began, culminating in this monograph, to which he dedicated the last 10 years of his life. In my family, I was the only one who had studied math at the graduate level, and so I was uniquely qualified to share in the excitement of his discoveries and the number of theorems he was able to prove. He was like an archeologist having found a new field of dinosaur bones—discovering something new, then examining and documenting it. He taught classes on his findings, and wrote many papers (see the bibliography). He did not publish his book; there were too many exciting theorems to prove, which were much more interesting to him than working with a publisher.

Upon his passing in 1991, I inherited his unfinished book. I worked with a good friend and past classmate, Michael Thwaites, to try to compile the book written in LaTeX. But life was busy with family and work. It wasn’t easy stepping into my father’s shoes to complete this very involved task. Throughout the following 25 years, I looked for a way to preserve the book and disseminate its knowledge. Eventually technology and the right person came together. One late evening I was discussing my father’s Finite Geometry book with William Gilpin. He has just completed his PhD in Physics from Stanford University. He knew LaTeX very well, and was able to assemble all the files. He also knew of the Cornell’s arXiv and recommended posting it there. It is the perfect place to store Professor De Vogelaere’s magnum opus.

I would like to thank:

- My mother, Elisabeth De Vogelaere, who made it possible for my father to dedicate his career to mathematics, which he loved
- Arthur Eddington, for inspiring my father

- Georges Lemaître, for inspiring and teaching my father
- The University of California, Berkeley, for providing the facilities and allowing him time to do his research, as well as for archiving the work he did over the 43 years of his career.
- Michael Thwaites, for helping me get started on the book, and for encouraging me to continue the work
- My wife Cynthia Haines, for carefully keeping and storing the computer disks, files and papers all these years
- My daughter Beth, for finding William Gilpin
- William Gilpin, for his extreme generosity of time to rapidly assemble the book and for facilitating having it stored at Cornell's arXiv.
- My siblings, Helene, Andrew, and Gabrielle for their patience and faith that this would happen!
- And Cornell's arXiv, for being there to disseminate knowledge.

Charles De Vogelaere
Mountain View, CA
August 2019

Contents

0	Preface	15
1	MAIN HISTORICAL DEVELOPMENTS	25
1.0	Introduction.	25
1.1	Before Euclid.	26
1.1.1	The Babylonians and Plimpton 322.	26
1.1.2	The Pythagorean school.	27
1.2	Euclidean Geometry.	28
1.2.1	Euclid.(3-th Century B.C.)	28
1.2.2	Menelaus (about 100 A.D) and Ceva (1647-1734?).	33
1.2.3	Euler (1707-1783) and Feuerbach (1800-1834).	34
1.2.4	The Geometry of the Triangle. Lemoine (1840-1912).	35
1.2	Projective Geometry.	36
1.2.1	The preparation. Menaechmus (about 340 B.C.), Apollonius (260? B.C - 200? B.C.), Pappus (300 - ?).	36
1.2.2	Gérard Desargues (1593-1661) and Blaise Pascal (1623-1662).	37
1.2.3	Lazare Carnot (1783-1823).	38
1.2.4	Jean Poncelet (1788-1867).	38
1.2.5	Joseph Gergonne (1771-1858).	39
1.2.6	Michel Chasles (1793-1880).	39
1.3	Relation between Projective and Euclidean Geometry.	39
1.3.0	Introduction.	39
1.3.1	Affine Geometry.	40
1.3.2	Involutive geometry.	41
1.4	Analytic Geometry.	43
1.4.1	René Descartes (1596-1650)[La Géométrie].	43
1.4.2	After Descartes.	44
1.4.3	Jean Poncelet (1788-1867).	45
1.4.4	James Singer on Difference sets and finite projective Geometry.	46
1.5	Trigonometry and Spherical Trigonometry.	50
1.5.1	Aryabatha I (476-?).	50
1.5.2	Jean Henri Lambert (1728-1777).	51
1.5.3	Menelaus of Alexandria (about 100 A. D.)	51
1.5.4	al-Battani, or Albategnius (850?-929?).	52
1.6	Algebra, Modular Arithmetic.	61

1.6.0	Introduction.	61
1.6.1	The integers.	61
1.6.2	The integers modulo p	61
1.6.3	Quadratic Residues and Primitive Roots.	65
1.6.4	Non Linear Diophantine Equations and Geometry.	67
1.6.5	Farey sets and Partial Ordering.	68
1.6.6	Complex and quaternion integers.	74
1.6.7	Loops.	75
1.6.8	Groups.	76
1.6.9	Veblen-Wederburn system.	77
1.6.10	Ternary Rings.	79
1.6.11	Felix Klein (1849-1925). Transformation groups.	80
1.6.12	Functions.	80
1.6.13	Cyclotomic polynomials. Constructibility with ruler and compass. . .	81
1.7	The real numbers.	81
1.7.1	The arithmetization of analysis. [Karl Weierstrass (1815-1897) and Riemann (1826-1866)]	81
1.7.2	Algebraic and transcendental numbers. [Hermite (1822-1901) and Lin- demann (1852-1939)]	82
1.8	The pendulum and the elliptic functions.	82
1.8.0	Introduction.	82
1.8.1	The pendulum.	83
1.8.2	The elliptic integral and the arithmetico-geometric mean.	87
1.8.3	The elliptic functions of Jacobi.	89
1.8.4	The theta functions of Jacobi.	91
1.8.5	Spherical trigonometry and elliptic functions.	92
1.8.6	The p function of Weierstrass.	93
1.8.7	References.	93
1.8.8	Texts on and tables of elliptic Functions.	94
1.9	Model of Finite Euclidean Geometry in Classical Euclidean Geometry. . . .	95
1.9.0	Introduction.	95
1.9.1	Points and lines in finite Euclidean geometry.	96
1.9.2	Parallels, parallelograms, distance.	104
1.9.3	Perpendicularity.	106
1.9.4	Circles, tangents and diameters.	108
1.9.5	The ideal line, the isotropic points and the isotropic lines.	115
1.9.6	Equality of angles and measure of angles.	118
1.9.7	Finite trigonometry.	123
1.10	Axiomatic	125
1.10.0	Introduction to Axiomatic.	125
1.10.1	The Perspective Plane.	126
1.10.2	Veblen-Wedderburn Planes.	133
1.10.3	Moufang Planes.	136
1.10.4	Desarguesian Planes.	139
1.10.5	Pappian planes.	140

1.10.6	Separable Pappian Planes.	141
1.10.7	Continuous Pappian or Classical Projective Planes.	144
1.10.8	Isomorphisms of Synthetically and Algebraically defined Planes.	144
1.10.9	Examples of Perspective Planes.	145
1.10.10	Collineations and Correlations in Perspective to Pappian Planes.	147
1.10.11	Three Nets in Perspective Geometry.	148
1.10.12	Bibliography.	150
1.11	Mechanics.	152
1.11.0	Introduction.	152
1.11.1	Kepler (1571-1630).	152
1.11.2	Newton (1642-1727).	153
1.11.3	Hamilton (1805-1865).	153
1.11.4	Preliminary remarks extending mechanics to finite geometry.	156
1.11.5	Eddington (18?-1944). The cosmological constant.	157
1.12	Description of Algorithms and Computers.	158
1.13	Notes.	159
1.13.1	On Babylonian Mathematics.	159
1.13.2	On Plimpton 322, Pythagorean numbers in Babylonean Mathematics.	159
1.90	Answers to problems and miscellaneous notes.	162
1.90.1	Algebra and modular arithmetic.	162
1.90.2	Linear Associative Planes.	162
1.90.3	Veblen-Wedderburn Planes.	163
2	FINITE PROJECTIVE GEOMETRY	165
2.0	Introduction.	165
2.1	Synthetic Finite Projective Geometry.	165
2.1.0	Introduction.	165
2.1.1	Notation.	165
2.1.2	Axioms.	166
2.1.3	Axiom (the finite field).	167
2.1.4	Basic consequences.	167
2.1.5	The Theorem of Desargues.	168
2.1.6	Configurations.	169
2.1.7	Other Configurations.	173
2.1.8	Proof of the Theorem of Desargues. The hexagon of Pappus-Brianchon. The configuration of Reidemeister.	178
2.1.9	The extended Pappus configuration and a remarkable Theorem.	182
2.1.10	Duality.	187
2.1.11	Complete quadrangles and homologic quadrangles.	187
2.1.12	Collineation and Correlation.	189
2.1.13	Finite projective planes for small p	190
2.1.90	Answer to exercises.	195
2.1.91	Relation between Synthetic and Algebraic Finite Projective Geometry.	197
2.2	Algebraic Model of Finite Projective Geometry.	198
2.2.0	Introduction.	198

2.2.1	Representation of points, lines and incidence.	199
2.2.2	Line through 2 points and point through 2 lines.	200
2.2.3	The model satisfies the axioms of the projective Pappus plane of order p	201
2.2.4	Finite vector calculus and simple applications.	204
2.2.5	Anharmonic ratio, harmonic quatern, equiharmonic quatern.	206
2.2.6	Projectivity of lines and involution on a line.	211
2.2.7	Collineation, central collineation, homology and elation.	215
2.2.8	Correlations, polarity.	218
2.2.9	Conics.	220
2.2.10	The general conic.	224
2.2.11	The Theorem of Pascal and Brianchon.	226
2.2.12	The Theorems of Steiner, Kirkman, Cayley and Salmon.	231
2.2.13	Bézier Curves for drawing Conics, Cubics,	235
2.2.14	Projectivity determined by a conic.	239
2.2.15	Cubics.	240
2.2.16	Other models for projective geometry.	241
2.2.17	Notes.	243
2.3	Geometric Models on Regular Pythagorean Polyhedra.	243
2.3.0	Introduction.	243
2.3.1	The selector.	244
2.3.2	The tetrahedron.	247
2.3.3	The cube.	248
2.3.4	The dodecahedron.	250
2.3.5	Difference Sets with a Difference.	252
2.3.6	Generalization of the Selector Function for higher dimension.	255
2.3.7	The conics on the dodecahedron.	259
2.3.8	The truncated dodecahedron.	273
3	FINITE PRE INVOLUTIVE GEOMETRY	291
3.1	An Overview of the Geometry of the Hexal Complete 5-Angles.	291
3.1.0	Introduction.	291
3.1.1	Notation and application to the special configuration of Desargues and to the pole and polar of with respect to a triangle.	292
3.1.2	An overview of theorems associated with equality of distances and angles. The ideal line, the orthic line, the line of Euler, the circle of Brianchon-Poncelet, the circumcircle, the point of Lemoine.	296
3.1.3	The fundamental $3 * 4 + 11 * 3$ & $3 * 5 + 10 * 3$ configuration.	299
3.1.4	An overview of theorems associated with bisected angles. The inscribed circle, the point of Gergonne, the point of Nagel.	300
3.2	The Geometry of the Hexal Complete 5-Angles.	303
3.2.0	Introduction.	303
3.2.1	The points of Euler, the center of the circle of Brianchon-Poncelet, and of the circumcircle, the points of Schröter, the point of Gergonne of the orthic triangle, the orthocentroidal circle.	304

3.2.2	Isotropic points and foci of conics.	305
3.2.3	Perpendicular directions.	305
3.2.4	The circle of Taylor, the associated circles, the circle of Brocard the points of Tarry and Steiner, the conics of Simson and of Kiepert, the associated circumcircles, the circles of Lemoine.	306
3.2.5	Theorems associated with bisected angles. The outscribed circles, the circles of Spieker, the point of Feuerbach, the barycenter of the ex- scribed triangle.	308
3.2.6	Duality and symmetry for the inscribed circle.	313
3.2.7	Summary of the incidence properties obtained so far	314
3.2.8	The harmonic polygons. [Casey]	319
3.2.9	Cubics.	322
3.2.10	The cubics of Grassmann.	327
3.2.11	Grassmannian cubics in Involutive Geometry.	333
3.2.12	Answer to	341
3.2.13	The cubics of Tucker.	342
3.2.14	NOTES	345
3.2.15	The cubic of 17 points.	348
3.2.16	The cubic of 21 points.	351
3.2.17	The Barbilian Cubics.	351
3.3	Finite Projective Geometry.	357
3.3.0	Introduction.	357
3.4	Finite Involutive Geometry.	358
3.4.0	Introduction.	358
3.4.1	Fundamental involution, perpendicularity, circles.	359
3.4.2	Altitudes and orthocenter.	361
3.4.3	The geometry of the triangle, I.	361
3.4.4	The geometry of the triangle. II.	368
3.4.5	Geometry of the triangle. III.	370
3.4.6	Geometry of the triangle. IV.	370
3.4.7	Geometry of the triangle. V.	371
3.4.8	Sympathic projectivities.	373
3.4.9	Equiangularity.	374
3.4.10	Equidistance, congruence.	376
3.4.11	Special triangles.	377
3.4.12	Other special triangles.	380
3.4.13	Geometry of the triangle. V.	381
3.90	Answers to problems and miscellaneous notes.	381
3.90.1	Answer to exercises.	382
4	FINITE INVOLUTIVE SYMPATHIC AND GALILEAN GEOMETRY	395
4.0	Introduction.	395
4.1	Finite involutive geometry.	396
4.1.9	Theorems in finite involutive Geometry, which do not correspond to known theorems in Euclidean Geometry.	396

4.1.10	The geometry of the triangle of degree 2.	396
4.1.11	Some theorems involving circles.	396
4.1.12	The parabola, ellipse and hyperbola.	397
4.1.13	Cartesian coordinates in involutive Geometry.	399
4.1.14	Correspondence between circles in finite and classical Euclidean geometry.	402
4.1.15	Answers to problems.	404
4.1.9	The conic of Kiepert.	407
4.1.10	The Theorem of Vectem and related results.	412
4.1.11	Representation of involutive geometry on the dodecahedron.	417
4.2	Finite Sympathic Geometry.	419
4.2.0	Introduction.	419
4.2.1	Trigonometry in a Finite Field for p . The Hyperbolic Case.	419
4.2.2	Trigonometry in a Finite Field for $q = p^e$. The Hyperbolic Case.	422
4.2.1	Trigonometry in a Finite Field for p . The Hyperbolic Case.	425
4.2.2	Trigonometry in a Finite Field for $q = p^e$. The Hyperbolic Case.	428
4.2.3	Trigonometry in a Finite Field for $q = p^e$. The Elliptic Case.	430
4.2.4	Periodicity.	440
4.2.5	Orthogonality.	441
4.2.6	Conics in sympathic geometry.	442
4.2.7	Regular polygons and Constructibility.	443
4.2.8	Constructibility of the second degree.	445
4.4	Contrast with classical Euclidean Geometry.	445
4.4.0	Introduction.	445
4.3	Parabolic-Euclidean or Cartesian Geometry.	446
4.3.0	Introduction.	446
4.3.1	Fundamental Definitions.	447
4.3.2	The Geometry of the Triangle in Galilean Geometry.	449
4.3.3	The symmetric functions.	451
4.5	Transformation associated to the Cartesian geometry.	452
4.5.0	Introduction.	452
4.5.1	The geometry of the triangle, the standard form.	453
4.5.2	The cubic γ a of Gabrielle.	457
4.6	Problems	463
4.6.1	Problems for Affine Geometry.	464
4.6.2	Problems for Involutive Geometry.	464
4.90	Answers to problems and miscellaneous notes.	465
5	FINITE NON-EUCLIDEAN GEOMETRY	479
5.0	Introduction.	479
5.1	Finite Polar geometry.	480
5.1.0	Introduction.	480
5.1.1	The ideal conic, elliptic, parabolic and hyperbolic points and lines.	480
5.1.2	Circles in finite polar geometry.	483
5.1.3	Perpendicularity.	485

5.1.4	Special triangles.	486
5.1.5	Mid-points, medians, mediatrices, circumcircles.	488
5.1.6	The center V of a triangle.	490
5.1.7	An alternate definition of the center V of a triangle.	492
5.1.8	Intersections of the 4 circumcircles.	494
5.1.9	Other results in the geometry of the triangle.	497
5.1.10	Circumcircle of a triangle with at least one ideal vertex.	499
5.1.11	The parabola in polar geometry.	500
5.1.12	Representation of polar geometry on the dodecahedron.	504
5.2	Finite Non-Euclidean Geometry.	510
5.2.0	Introduction.	510
5.2.1	Trigonometry for the general triangle.	510
5.2.2	Trigonometry for the right triangle.	513
5.2.3	Trigonometry for other triangles	513
5.3	Tri-Geometry	514
5.3.1	The primitive case.	514
5.3.2	The case of 1 root. Inverse geometry.	520
5.3.4	The case of a double root and a single root.	524
5.3.5	The case of a triple root. Solar geometry.	526
5.3.6	The case of 3 distinct roots.	528
5.3.7	Conjecture.	530
5.3.8	Notes.	533
5.3.9	On the tetrahedron.	535
6	GENERALIZATION TO 3 DIMENSIONS	537
6.0	Introduction.	537
6.0.1	Relevant historical background.	538
6.0.2	Grassmann algebra applied to incidence properties of points, lines and planes	538
6.1	Affine Geometry in 3 Dimensions.	545
6.1.0	Introduction.	545
6.1.1	The ideal plane and parallelism.	545
6.2	Polar Geometry in 3 Dimensions.	547
6.2.0	Introduction.	547
6.2.1	The fundamental quadric, poles and polars.	548
6.2.2	Orthogonality in space and the ideal polarity.	550
6.2.3	The general tetrahedron.	554
6.2.4	The orthogonal tetrahedron.	560
6.2.5	The isodynamic tetrahedron.	563
6.1.3	The orthogonal tetrahedron.	563
6.1.4	The isodynamic tetrahedron.	567
6.1.5	The antipolarity.	568
6.1.6	Example.	573
6.90	Answers to problems and miscellaneous notes.	580

7	QUATERNIONIAN GEOMETRY	583
7.0	Introduction.	583
7.1	Quaternionian Geometry over the reals.	584
7.1.1	Points, Lines and Polarity.	584
7.1.2	Quaternionian Geometry of the Hexal Complete 5-Angles.	589
7.2	Finite Quaternionian Geometry.	595
7.2.1	Finite Quaternions.	595
7.2.2	Example in a finite quaternionian geometry.	596
7.3	Miniquaternionian Plane Ψ of Veblen-Wedderburn.	598
7.3.0	Introduction.	598
7.3.1	Miniquaternion near-field.	598
7.3.2	The miniquaternionian plane Ψ	600
7.4	Axiomatic.	607
7.4.1	Veblen-MacLagan planes.	607
7.4.2	Examples of Perspective planes.	608
7.5	Desarguesian Geometry.	610
7.5.1	Desarguesian Geometry of the Hexal Complete 5-Angles.	611
7.5.2	Perpendicularity mapping.	615
7.6	The Hughes Planes.	616
7.6.0	Introduction.	616
7.6.1	Nearfield and coordinatization of the plane.	616
7.6.2	Miniquaternion nearfield.	618
7.6.3	The first non-Pappian plane, by Veblen and Wedderburn.	620
7.6.4	The miniquaternionian plane Ψ	621
7.7	Axiomatic.	627
7.7.1	Veblen-MacLagan planes.	627
7.7.2	Examples of Perspective planes.	628
7.8	Bibliography.	628
7.90	Answer to problems and Comments.	630
8	FUNCTIONS OVER FINITE FIELDS	633
8.0	Introduction.	633
8.1	Polynomials over Finite Fields.	633
8.1.1	Definition and basic properties.	633
8.1.2	Derivatives of polynomials.	634
8.2	Orthogonal Polynomials over Finite Fields.	634
8.2.0	Introduction.	634
8.2.1	Basic Definitions and Theorems.	634
8.2.2	Symmetry properties for the Polynomials of Chebyshev of the first and second kind.	636
8.2.3	Symmetry properties for the Polynomials of Legendre.	637
8.2.4	Symmetry properties for the Polynomials of Laguerre.	639
8.2.5	Symmetry properties for the Polynomials of Hermite.	640
8.3	Addition Formulas for Functions on a Finite Fields.	642
8.3.0	Introduction.	642

8.3.1	The Theorem of Ungar.	642
8.3.2	The case of 3 functions.	643
8.3.3	The case of 4 Functions.	655
8.3.4	The case of 5 functions.	657
8.4	Application to geometry.	658
8.4.0	Introduction.	658
8.4.1	k-Dimensional Affine Geometry.	658
8.4.2	Ricatti geometry.	667
8.4.3	3 - Dimensional Equidistance Curves.	676
8.4.4	Generalization of the Selector Function.	681
8.5	Generalization of the Spheres in Riccati Geometry.	684
8.5.1	Dimension k	684
8.5.2	Dimension 3.	685
8.5.3	Dimension 4.	691
9	FINITE ELLIPTIC FUNCTIONS	693
9.0	Introduction.	693
9.1	The Jacobi functions.	693
9.1.1	Definitions and basic properties of the Jacobian elliptic group.	693
9.1.2	Finite Jacobian elliptic groups for small p	698
9.1.3	Finite Jacobian Elliptic Function.	700
9.1.4	Identities and addition formulas for finite elliptic functions.	701
9.1.5	Double and half arguments.	704
9.1.6	The Jacobi Zeta function.	706
9.1.7	Example.	707
9.1.8	Other results.	709
9.1.9	Isomorphisms and homomorphisms.	709
9.2	Applications.	712
9.2.1	The polygons of Poncelet.	712
9.3	The Weierstrass functions.	713
9.3.1	Complex elliptic functions.	713
9.3.2	Weierstrass' elliptic curves and the Weierstrass elliptic functions.	714
9.3.3	The isomorphism between the elliptic curves in 3 and 2 dimensions.	718
9.3.4	Correspondance between the Jacobi elliptic curve (cn, sd) and the Weierstrass elliptic curve	721
9.4	Complete elliptic integrals of the first and second kind.	723
9.5	P-adic functions, polynomials, orthogonal polynomials.	729
9.5.1	Trigonometric Functions.	733
9.5.2	Integration.	737
9.6	P-adic field.	737
9.6.1	Generalities.	737
9.6.2	Extension to the half argument.	743
9.6.3	The logarithm.	745
9.6.4	P-adic Geometry and Related Finite Geometries.	748

10 DIFFERENTIAL EQUATIONS AND FINITE MECHANICS	751
10.0 Introduction.	751
10.1 The first Examples of discrete motions.	751
10.1.1 The harmonic polygonal motion.	751
10.1.2 The Parabolic Motion.	754
10.1.3 Attempts to Generalize Kepler's Equation.	755
10.1.4 The circular motion.	755
10.2 Approximation to the Solution of Differential Equations.	756
10.2.0 Introduction.	756
10.2.1 Some Algorithms.	756
10.3 The Parabolic Motion.	757
10.3.0 Introduction.	757
10.4 Attempts to Generalize Kepler's Equation.	758
10.4.1 The circular motion.	758
10.5 Approximation to the Solution of Differential Equations.	759
10.5.1 On the existence of primitive roots.	760
11 COMPUTER IMPLEMENTATION	763
11.0 Introduction.	763

Chapter 0

Preface

Purpose

The purpose of this book and of others that are in progress is to give an exposition of Geometry from a point of view which in some sense complements Klein's Erlangen program. The emphasis is on extending the classical Euclidean geometry to the finite case, but it goes way beyond that.

Plan

In this preface, after a brief introduction, which gives the main theme, and was presented in some details at the first Berkeley Logic Colloquium of Fall 1989, I present the main results, according to a synthetic view of the subject, rather than chronologically. First, some variation on the axiomatic treatment of projective geometry, then new results on quaternionian geometry, then results in geometry over the reals which are generalized over arbitrary fields, then those which depend on properties of finite fields, then results in finite mechanics. The role of the computer, which was essential for these inquiries is briefly surveyed. The methodology to obtain illustrations by drawings is described. The interaction between Teaching and Research is then given. I end with a table which enumerates enclosed additional material which constitutes a small but representative part of what I have written.

Introduction

My inquiry started with rethinking Geometry, by examining first, what could be preserved among the properties of Euclidean geometry when the field of reals is replaced by a finite field. This led me to a separation of the notions concerned with the distance between 2 points and the angle between an ordered pair of lines, into two sets, those concerned with equality and those concerned with measure. Properties relating to equality are valid for a Pappian geometry, whatever the underlying field, those pertaining to measure require specifying the field.

I have also come to the conclusion that the more fruitful approach to the axiomatic of Euclidean geometry is to reduce it to that of Projective geometry followed by a preference of certain elements, namely the isotropic points on the ideal line. This preference can be

presented alternately by choosing 2 points relatively to a triangle of coordinates, namely the barycenter and the orthocenter. The barycenter is used to define the ideal line, the orthocenter is then used to define the fundamental involution of this line, for which the isotropic points are the (imaginary) fixed points. This program extends to all non-Euclidean geometries.

The preference method, which I call the “Berkeley Program”, can be considered as the synthetic equivalent of the group theoretical relations between geometries, as advocated in Felix Klein’s Erlangen program.

When I refer to Euclidean geometry, I always mean that the set of points and lines of the geometry of Euclid have been completed by the ideal line and the ideal points on that line.

Axiomatic of projective geometry

Projective Geometry

Axiomatic.

The approach, used by Artzy, has the advantage of giving the equivalence between the synthetic axioms and the algebraic axioms, at each stage of the axiomatic development: for perspective planes, Veblen-Wedderburn planes, Moufang planes, Desarguesian planes, Pappian planes, ordered planes, and finally, projective planes. I have revised it, to give a uniform treatment (particularly lacking at the intermediate step of the Veblen-Wedderburn plane, in which, for instance, vectors are introduced by Artzy and others, to prove commutativity of addition) and by giving, for all proofs, explicit, rather than implicit constructions, together with drawings.

Notation.

The Theorems of Desargues, Pappus and Pascal play an important role in synthetic proofs in Projective geometry. A notation has been introduced for the repeated use of these theorems and their converse, in an efficient and unambiguous way. A notation for configurations has been introduced, which further helps in distinguishing non isomorphic configurations.

Desarguesian geometry

Quaternionian Geometry.

With Relative Preference of 2 Points.

A quaternionian plane is a well known, particularly important, example of a Desarguesian plane. I have introduced in it, the relative preference of 2 points, the barycenter and the cobarycenter and have obtained several Theorems, which in the sub-projective planes of the geometry correspond to Theorems in involutive geometry which are associated with the circumcircle and with the point of Lemoine. But these Theorems cannot be considered as simple generalizations. For instance, in the involution on the ideal line, defined by the circumcircular polarity, which corresponds to a circumcircle, the direction of a side and that

of the comedian, which generalizes an altitude, are not corresponding elements, although these correspond to each other, in the sub-projective planes. Moreover, what I call the Lemoine polarity degenerates in the sub-projective planes into all the lines through the point of Lemoine. The proofs given are all algebraic. These investigations are just the beginning of what should become a very rich field of inquiries.

Finite Quaternionian Geometry.

The Theorems in quaternionian geometry were conjectured using a geometry whose points and lines are represented by 3 homogeneous coordinates in the ring of finite quaternions over Z_p . In the corresponding plane, the axioms of alignment are not always satisfied. If they are, Theorems and proofs for the quaternionian plane extend to the finite case.

Pappian geometry over arbitrary fields

Pappian Geometry.

This can be considered as a projective geometry over an arbitrary field.

On Steiner's Theorem.

Pappus' Theorem is one of the fundamental axioms of Projective geometry. If the 3 points on one of the lines are permuted, we obtain 6 Pappian lines which pass 3 by 3 through 2 points, this is the Theorem of Jakob Steiner. By duality, we can obtain from these, 6 points on 2 lines. That these 2 lines are the same as the original ones is a new Theorem. Detailed computer analysis of the mapping in special cases leads to conjectures in which twin primes appear to play a role.

Generalization of Wu's Theorem.

I obtained some 80 new Theorems in Pappian geometry, generalizing a Theorem, in projective geometry, of Wen-Tsen Wu, related to conics through 6 Pascal points of 6 points on a conic, I have obtained a computer proof for all of these Theorems by means of a single program, which includes convincing checks, and then succeeded in obtaining a synthetic proof for each of these Theorems, using several different patterns and approaches including duality and symmetry. These proofs have benefited from the projective geometry notation. Drawings have been made for a large number of these Theorems which have suggested 2 new Theorems and a (solid) Conjecture. Many of the Theorems can be considered as Theorems in Euclidean geometry, (only one of which was known, the Theorem of Brianchon-Poncelet), others can be considered as Theorems in Affine or in Galilean geometry.

Generalization of Euclidean Theorems.

The Theorems, given for involutive geometry, can be considered, alternately, as Theorems in Pappian geometry, because they involve only the preference of 2 elements of the projective plane and not additional axioms.

Involutive Geometry.

I call involutive plane, a Pappian plane in which I prefer 2 points relative to a triangle, M , the barycenter and \overline{M} , the orthocenter. M allows for the definition of the ideal line, \overline{M} allows, subsequently, for the definition of the fundamental involution on that line.

Generalization of Theorems in Euclidean and Minkowskian Geometry over Arbitrary Fields.

In this, which constitutes the more extensive part of my research, I have generalized, when the involution is elliptic, a very large number of Theorems in Euclidean geometry, namely those which are characterized by not using the measure of distance and of angles and not involving elements whose construction leads to more than one solution. When the fundamental involution is hyperbolic, each of the Theorems gives a corresponding Theorem in the geometry of Hermann Minkowski.

Symmetry and Duality.

The barycenter and orthocenter have a symmetric role for many Theorems of Euclidean geometry, the line of Euler and the circle of Brianchon-Poncelet being the simpler examples. This has been systematically exploited, to almost double the number of Theorems known in that part of Euclidean geometry which involves congruence and not measure. Duality can also be extended to Euclidean geometry by associating to M and \overline{M} , the ideal line and the orthic line and vice-versa. This also has been systematically exploited to help me, in obtaining constructions of new elements, and should be helpful in future constructions.

Notation.

A set of notations was introduced, to allow for a compact description of some 1006 definitions, 1073 conclusions and for the corresponding proofs. The counts correspond to one form of counting, other forms give higher numbers. All these Theorems are valid for any Pappian plane and give directly both statement and new proofs in both Euclidean and Minkowskian geometry.

The Geometry of the Triangle.

During the period 1870 to 1900, there was an explosion of results in what has been called the geometry of the triangle, prepared by Theorems due to Leonhard Euler, Jean Poncelet, Charles Brianchon, Emile Lemoine and others. The synthesis of the subject was never successfully accomplished, not only because of the wealth of Theorems, but because of the difficulty of insuring that elements defined differently were in fact, in general, distinct. The proofs, used in involutive geometry, not only throw a new light on the reason for the explosive number of results for the geometry of the triangle but also gives a exhaustive synthetic view of the subject.

Diophantine Equations.

Because an algebraic expression of the homogeneous coordinates of points and lines and the coefficients for conics is given in terms of polynomials in 3 variables, a large number of particular results on diophantine equations in 3 variables are implicitly obtained in these investigations.

Construction with the Ruler only.

In all of the classical investigations, the most extensive one being that of Henri Lebesgue, the impression is given that the compass is indispensable for most constructions in geometry. More than half of the Theorems for which a count is given above, can be characterized as using the ruler only. Implicit, in this part of my Research, is, that many constructions, which usually or by necessity were assumed to require the compass, in fact need the ruler only, the simplest one is that for constructing the perpendicular to a line. The more remarkable one is that the circles of Apollonius can be constructed with the ruler only. These are defined as the circles which have as diameter the intersections of the bisectrices of an angle of a triangle with the opposite sides. It is this reduction to construction with the ruler alone, which allows for the straightforward proofs which constitutes a major success of these investigations.

Construction with the Ruler and Compass.

The construction with compass can be envisioned as follows. Given M and \overline{M} , by finding the intersection of 2 circles centered at 2 of the vertices of a triangle with the adjacent sides and by constructions with the ruler, we can construct the bissectrices of these angles, the incenter (center of the inscribed circle) and the point of Joseph Gergonne (the common intersection of the lines through a vertex of the triangle and the point of tangency of the inscribed circle with the opposite side). From these, a very large number of other points, lines and circles can be constructed with the ruler only, for instance, the point of Karl Feuerbach, the excribed circles and the circles of Spieker. One can therefore, in the framework of involutive geometry, prefer instead of M and \overline{M} , the incenter I and the point of Gergonne J . Starting from I and J , we can construct M and \overline{M} , using the ruler alone. This allows to extend the proof methodology considerably, allowing the generalization to arbitrary fields of Theorems involving elements whose construction, in the classical case, would requires the compass.

Cubics.

Very little has been written on the construction of cubics by the ruler. Starting with the work of Herman Grassmann of R. Tucker and of Ian Barbilian, I have obtaining a few results in this direction, one of which, incidentally, gives a illustration of the procedure of construction with the compass as I am envisioning it, which is much simpler than those involving bissectrices.

Galilean geometry.

When the fundamental involution is parabolic and when the field is the field of reals, the geometry is called Galilean, because its group is the group of Galilean transformations of classical mechanics. Extending to the Pappian case and starting from the definitions and conclusions of involutive geometry, I have made appropriate modifications to obtain Theorems which are valid in Galilean geometry, but I have not yet completed the careful check that is required to insure the essential accuracy. Again a very large number of Theorems have been obtained, which are new, even in the case of the field of reals.

Polar Geometry.

The extension, to n dimensions, can be obtained using an appropriate adaptation of the algebra of Herman Grassmann. A first set of Theorems has been obtained in the case of 3 dimensions, again for a Pappian space over arbitrary fields, in which preference is given to one plane, the ideal plane and one quadric. These Theorems generalize Theorems on the tetrahedron due to E. Prouhet, Carmelo Intrigila and Joseph Neuberg. The special case of the orthogonal tetrahedron has also been studied in a way which puts in evidence the reasons behind many of the Theorems obtained in this case.

Non-Euclidean Geometry.

The beginning of the preference approach to obtain new results in non-Euclidean geometry was started in January 1982. The confluence, in the case of a finite field, of the geometries of Janos Bolyai and of Nikolai Lobachevsky was then explored. A new point, called the center of a triangle was discovered and its properties were proven.

Pappian geometry over finite fields

The Case of Finite Fields.

All the results given for involutive geometry and in the following sections are true, irrespective of fields. In what follows, we describe results for finite fields.

Projective Geometry.

Representation on Pythagorean and Archimedean solids.

Fernand Lemay has shown how to represent the projective planes corresponding to the Galois fields, 2, 3 and 5 respectively on the tetrahedron, the cube (or octahedron) and the dodecahedron (or icosahedron). I have shown, that if we choose instead of the Pythagorean solids, the Archimedean ones, the results extend to 2^2 and the 5-gonal antiprism and to 3^2 and the truncated dodecahedron. I have studied also the corresponding representations of the conics on the dodecahedron. This is useful for the representation on it of the finite non-Euclidean Geometry associated with $GF(5)$.

Involutive Geometry.

Partial Ordering.

In the case of finite fields, ordering and therefore the notions of limits and continuity are not present. By using Farey sets or, alternately, by using a symmetry property of the continued fraction algorithm, I have introduced partial ordering in Z_p . If only, the properties of order have to be preserved which are related to the additive inverse and multiplicative inverse, then a Theorem of Mertens allows me to estimate the cardinality of the ordered subset of Z_p by $.61 p$, when p is large. The cardinality is decreased logarithmically, by a factor 2, for each additional operation of addition and multiplication, for which order needs to be preserved.

Orthogonal polynomials.

Orthogonal polynomials can be defined in a straightforward way in Z_p . For those I have studied, it turns out, that the classical scaling used in defining the classical orthogonal polynomials, there is a symmetry which is exhibited in each case, with the exception of those of Charles Hermite. In this case, by using an alternate scaling, with different expressions for the polynomials of even and odd degree, symmetry can also be obtained.

Finite Trigonometry.

Once the measure of angles between an ordered pair of non ideal lines and the measure of the square of the distance between two ordinary points has been defined, it is straightforward to obtain the trigonometric functions in Z_p . There are in fact, for each prime p , two sets of trigonometric functions, one corresponding to the circular ones, one to the hyperbolic ones. The proofs required, depend on the existence of primitive roots, in the case corresponding to Minkowskian geometry, and on a generalization to the Galois field $GF(p^2)$ in the case corresponding to Euclidean geometry.

Finite Riccati Functions.

The functions of Vincenzo Riccati, which are generalization of the trigonometric functions have been defined and studied in the finite case. They enable the definition of a Riccati geometry. An invariant defines distances, the addition formulas, which correspond to multiplication of associated Toeplitz matrices, define addition of angles. This again should be a fruitful field of inquiry.

Finite Elliptic Functions.

After I conjectured that the Theorem of Poncelet on polygons inscribed to a conic and cir-

cumscribed to an other conic extended to the finite case, I knew that Finite Elliptic functions could be defined in the finite case, because I had learned from Georges Lemaître the relation between Theorems on elliptic functions and the Theorem of Poncelet. The functions I defined, correspond to the functions sn , cn and dn of Karl Jacobi. After I found that John Tate had defined the Weierstrass type of finite elliptic functions I established the relation between the 2.

Construction with the compass.

In the case of finite fields, the points I and J will only exist if 2 and therefore all angles of the triangle are even. Preferring I and J instead of M and \overline{M} , insures that the triangle is even.

Isotropic Geometry.

Many of the Theorems in involutive and polar geometry do not apply to the case of fields of characteristic 2, because the diagonal points of a complete quadrilateral are collinear, because every conics has all its tangents incident to a single point and because in the algebraic formulations, 2, which occurs in many of the algebraic expressions involved in corresponding proofs of involutive geometry is to be replaced by 0. I call isotropic plane, a Pappian plane, with field of characteristic 2 and with the relative preference of 2 points, M , the barycenter and, O , the center. The orthocenter does not exist when the characteristic is 2 because each line can be considered as perpendicular to itself. The difference sets of J. Singer, called selectors by Fernand Lemay, were an essential tool in these investigations. In an honor Thesis, Mark Spector, now a Graduate Student in Physics at M.I.T. wrote a program to check the consistency of the notation in the statements of the Theorems and the accuracy of the proofs. He obtained new results. My results on cubics are not retained in his honors Thesis. Some of the results in isotropic geometry were anticipated by the work of J. W. Archbold, Lawrence Graves, T. G. Ostrom and D. W. Crowe.

Finite mechanics and symplectic integration

I was asked to participate in a discussion, Spring 1988, at Los Alamos, on the field of symplectic integration which I originated in 1955. Symplectic integration methods are methods of numerical integration which preserve the properties of canonical or symplectic transformations. It then occurred to me, that these methods were precisely what was needed to extend to the finite case the solution of problems in Mechanics. I had searched for a solution to this problem since I obtained, as first example, the solution, using finite elliptic functions, for the motion in Z_p of the pendulum with large amplitude, as well as the polygonal harmonic motion, whose study was suggested by a Theorem of John Casey, and led to an equation similar to Kepler's equation.

More specifically, whenever the classical Hamiltonian describing a motion has no singularities, a set of difference equations can be produced whose solutions at successive steps have the properties associated with symplectic transformations. To confirm the solidity of this approach, I studied, in detail, the bifurcation properties for one particular Hamiltonian. The study can be made in a more complete fashion than in the classical case and requires a much

simpler analysis using the p -adic analysis of Kurt Hensel.

The role of the computer for conjectures and verification

The computer was an essential tool in the conjecture part of the Research described above, in the verification of the order of the statements and to insure the consistency of the notation used in the statements of the Theorems as well as in the verification of the proofs. In particular, the Theorem referred to in the Steiner section was conjectured from examples from finite geometry. All of the Theorems generalizing Wu's Theorem were conjectured by examining, in detail, one appropriately chosen example, for a single finite field. Many Theorems in involutive geometry and all the Theorems in quaternionian geometry were so conjectured and the methodology used was such that almost all conjectures could be proven. The remaining ones could easily be disposed of, by a counterexample or algebraically. The only exception are the conjectures, indicated in the section on Steiner's Theorem, which refer to twin primes.

Illustrations by drawings

Responding to natural requests for figures which illustrate the many Theorems obtained, I have also prepared a large number of drawings. These have been done for the case of the field of reals and therefore in the framework of classical Euclidean geometry. These are created by means of a VMS-BASIC program, which constructs a POSTSCRIPT file, for any set of data, including points, lines, conics and cubics. The position of the labels of points and lines can be adjusted by adding the appropriate information to the data file in order to position the labels properly. One such illustration was chosen by George Bergman, for this year's poster on "Graduate opportunities in Mathematics for minority and women students".

Interaction between research and teaching

These 2 obligations are for me very closely intertwined, my specific contributions to teaching are given in a separate document. The conjecture aspect of my research was exclusively dependent on VMS-BASIC programs which were a natural extension of programs which I wrote for my classes. Many of the proofs are dependent on material contained in notes I prepared for students while teaching courses not related to my original specialty of Numerical Analysis and of Ordinary Differential Equations.

Many results have been presented in courses, a few, in Computation Mathematics, (Math. 100), Abstract Algebra (Math. 113) and Number Theory (Math. 115), a large number, in a seminar on Geometry, 2 years ago, and in Foundations of Geometry (Math. 255), Fall 1989.

Notes and publication

The scope of the results and their constant interaction during the years made it impractical to publish incrementally without slowing down considerably the pace of the inquiry. I have only given a brief overview in 1983 and in 1986.

Finite Euclidean and non-Euclidean Geometry with application to the finite Pendulum and the polygonal harmonic Motion. A first step to finite Cosmology.

The Big Bang and Georges Lemaître, Proc. Symp. in honor of 50 years after his initiation of Big-Bang Cosmology, Louvain-la-Neuve, Belgium, October 1983., D. Reidel Publ. Co, Leyden, the Netherlands. 341-355.

Géométrie Euclidienne finie. Le cas p premier impair. La Gazette des Sciences Mathématiques du Québec, Vol. 10, Mai 1986.

Basic Discoveries in Mathematics using a Computer. Symposium on Mathematics and Computers, Stanford, August 1986.

A short guide to the reader.

The reader may want to start directly with Chapter II and to read sections of the introductory Chapter as needed. He may perhaps wish to read the section on a model of finite Euclidean geometry with the framework of classical geometry, if he wishes to be more comfortable about the generalization of the Euclidean notions to the finite case. If at some stage the readers wants a more thorough axiomatic treatment it will want to read the section on axiomatic of the first Chapter.

Chapter II is written in terms of finite projective geometry associated to the prime p , but, except in obvious places, all definitions and Theorem apply to Pappian planes over arbitrary fields. Among the new results, included in this Chapter, are, a Theorem related to the Steiner-Pappus Theorem, considerations on a “general conic”, a description of the Theorems of Steiner, Kirkmanm Cayley and Salmon in terms of permutation maps. After describing the representation of the finite projective planes for $p = 2, 3$ and 5 on Pythagorean solids, the generalization to the projective plane of order p^2 on the truncated dodecahedron is given as well as that of the plane of order on the antiprism. Difference sets involving non primitive polynomials are studied which allow a definition of the notion of distance for affine as well as other planes.

Attention is also drawn to Bézier curves, which have not yet entered the classical repertoire of Projective Geometry. These are used extensively in the computer drawing of curves and surfaces.

One of the reason for the historical delay of extended the Euclidean notions associated with distance between points and angle between lines is the lack of early distinction between equality and measure. Equality is a simpler notion which can be dealt with over arbitrary fields, while measure requires greater care. This is exemplified by the comment on finite projective geometries by O’Hara and Ward, p. 289.

Their analytic treatment involves the theory of numbers, and, in particular the theory of numerical congruences; it may be assumed that the synthetic treatment of them is correspondingly complicated.

It is my fondest hope that some of the material on finite geometry will be assimilated to form the basis of renewal of the teaching of geometry at the high school level, combined with a well-thought related use of computers at that level.

Chapter 1

MAIN HISTORICAL DEVELOPMENTS

1.0 Introduction.

In this chapter, I give the main historical developments in Mathematics which have a bearing on the generalization of Euclidean Geometry to the finite case and to non Euclidean Geometries.

What could be consider as the first contribution to Mathematics which covers number theory, geometry and trigonometry is a tablet in the Plimpton collection, this is briefly described and discussed in a note at the end of the Chapter. The key to the treatment of geometry and its use of continuity dates from the discovery of the irrationals by the school of Pythagoras. This is commented upon to suggest an alternative which is consistent with finite Euclidean geometry. I thought it would be handy for many readers to have at hand the definitions and postulates of Euclid, as well as a brief description of his 13 books, if only to see how we have travelled in getting a more precise description of concepts and theorems in geometry. Distances play an essential, if independent role, in the development of geometry, until recently, after some comments on the subject, I give some post Euclidean theorems involving distnaces on the sides of a triangle due to Menelaus and Ceva. The geometry of the triangle, which has played an important historical role, is illustrated by theorems due to Euler, Brianchon and Poncelet, Feuerbach, Lemoine and Schröter.

I then review quickly some of the major developments in projective geometry due to Menaechmus, Apollonius, Desargues, Pascal, MacLaurin, Carnot, Poncelet, Gergonne and Chasles. In the next section, I start the process of going back from projective, to affine, to involutive, to Euclidean geometry.

I then review the algebraization of geometry starting with Descartes and Poncelet and ending with James Singer, who spured by a paper of Veblen and MacLagan-Wedderburn, introduced the notion of difference sets which allows the representation of every point and line in a finite Pappian plane by an integer, allowing an easy determination of incidence, without coordinatization.

This is followed by a section on trigonometry which gives the Lambert formulas valid in the case of finite fields.

The section on algebra is for the reader which has been away from the subject for some time. It includes algorithms to solve linear diophantine equations and to obtain the representation of numbers as sum of 2 squares, the definition of primitive roots and the application to the extraction of square roots in a finite field, contrasting with the solution of the school of Pythagoras.

The section on Farey sets includes original material on partial ordering of distances, which at least suggest that the essential notion of ordering in the classical case can be extended to the finite case.

Definition of complex and quaternion integers, loops, groups, Veblen-Wedderburn systems and ternary rings are given as a preparation for the section on axiomatic. The important relevant contributions of Klein, Gauss, Weierstrass, Riemann, Hermite and Lindenbaum are then recalled.

The subject of elliptic functions and the application of geometry to mechanics has lost, at the present time, the great interest it had during last century. Because this too generalizes to the finite case and because this is not now part of the Mathematics curriculum, I have a long section introducing one of its components, the motion of the pendulum to introduce elliptic integrals, the elliptic functions of Jacobi as well as his theta functions, ending with the connection given first by Lagrange between spherical trigonometry and elliptic functions. To add credibility to the existence of non Euclidean geometries, models were devised to give models within the framework of Euclidean geometry. The next section gives a model of finite Euclidean geometry also within this framework. It can be used as an introduction to the subject.

The axiomatic of geometry in the next section is done using a uniform treatment, and explicit constructions. It includes a plane which is, like the Moufang plane, intermediate between the Veblen-Wedderburn plane and the Desarguesian plane. The geometry of Lenz-Barlotti of type I.1 discovered by Veblen and MacLagan-Wedderburn and studied by Hughes is an example of this intermediate plane.

1.1 Before Euclid.

1.1.1 The Babylonians and Plimpton 322.

Introduction.

Besides estimating areas and volumes, the Babylonians had a definite interest in so called Pythagorean triples, integers a , b and c such that $a^2 = b^2 + c^2$.

In tablet 322 of the Plimpton library collection from Columbia University, dated 1900 to 1600 B.C., a table gives, with 4 errors, and in hexadesimal notation, 15 values of

$$a, b, \text{ and } \left(\frac{a}{c}\right)^2 = \sec^2(B),$$

corresponding to angles varying fairly regularly from near 45° to near 32° . (See Note 1.13.2).

It is still debated if their interest was purely arithmetical or was connected with geometry (See Note 1.13.1).

1.1.2 The Pythagorean school.

That the ratio of the length of the sides of a triangle is equal to the ratio of 2 integers was first contradicted by the counterexample of an isosceles right triangle A_0, A_1, A_2 , with right angle at A_0 and with sides a_1 and hypotenuse a_0 . The theorem of Pythagoras states that

$$a_0^2 = a_1^2 + a_1^2 = 2a_1^2, a_0 > a_1 > 0. \quad (1)$$

If a_0 and a_1 are positive integers, it follows from the fact that the square of an odd integer is odd and that of an even integer is even, and from (1), that a_0^2 and therefore a_0 is even, therefore $a_0 = 2a_2$ and

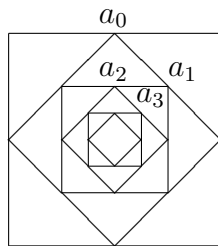
$$a_1^2 = 2a_2^2, a_1 > a_2 > 0. \quad (2)$$

The argument can be repeated indefinitely and an infinite sequence of decreasing positive integers is obtained,

$$a_0 > a_1 > \dots > a_n > \dots > 0. \quad (3)$$

But this contradicts the fact that only a finite number of positive integers exist which are less than a_0 .

Geometrically, the proof follows from the following figure:



This argument has been refined through the ages, by a careful construction of the integers, see for instance the Appendix by Professor A. Morse in Professor J. Kelley's book on Topology, by an analysis of their divisibility properties (see the Theorem of Aryabatha) and by their ordering properties (the well ordering axiom of the integers). What is implicit in the geometry considered by the Greeks, after Pythagoras, is that the circle with center A_1 and radius a_0 meets the line through A_1 and A_0 at a point, but this assumption is not made explicitly. From it follows the existence of points on the line corresponding to the irrational $\sqrt{2}$ and also the existence of the unrelated irrationals, $\sqrt{3}, \dots, \sqrt{17}, \dots$, more generally, \sqrt{p} , for p prime, eventually this lead Euclid to consider that the set of points on each line forms a continuous set.

Moreover the theorem of Pythagoras assumes the axiom on parallels of Euclid.

In finite affine geometry, I will keep the axiom of parallels but assume that the number of points on each line is finite. In finite Euclidean Geometry most of the notions of ordinary Euclidean geometry are preserved, the measure of angles presents no difficulties and the measure of distances requires the introduction of one irrational. On the other hand circles meet half of the lines through their center in 2 points and the other half in no point and $\sqrt{2}$ need not be irrational. See 1.6.3.

1.2 Euclidean Geometry.

1.2.1 Euclid.(3-th Century B.C.)

The greek geometer Euclid (300 B.C) constructed a careful theory of geometry based on the primary notions of points, lines and planes and on a set of axioms, the last one being the axiom on parallels.

His first 3 books are devoted to a study of the triangle, of the circle and of similitude.

I will list here the definitions, postulates and common notions as translated by Heath, p. 153 to 155:

Definitions.

0. A *point* is that which has no parts.
1. A *line* is breadthless length.
2. The extremities of a line are points.
3. A *straight line* is a line which lies evenly with the points on itself.
4. A *surface* is that which has length and breath only.
5. The extremities of a surface are lines.
6. A *plane surface* is a surface which lies evenly with the straight lines on itself.
7. A *plane angle* is the inclination to one another of two lines in a plane which meet one another and do not lie in a straight line.
8. And when the lines containing the angle are straight, the *angle* is called *rectilinear*.
9. When a straight line set up on a straight line makes the adjacent angles equal to one another, each of the equal *angles* is *right*, and the straight line standing on the other is called a *perpendicular* to that on which it stands.
10. An *obtuse angle* is greater than the right angle.
11. An *acute angle* is an angle less than a right angle.
12. A *boundary* is that which is an extremity of anything.
13. A *figure* is that which is contained by any boundary or boundaries.
14. A *circle* is a plane figure contained by one line such that all the straight lines falling upon it from one point among those lying within the figure are equal to one another.
15. And the point is called the *center of the circle*.

16. A *diameter* of the circle is any straight line through the center and terminated in both directions by the circumference of the circle, and such a straight line also *bisects the circle*.
17. A *semicircle* is the figure contained by the diameter and the circumference cut off by it. And the center of the semicircle is the same as that of the circle.
18. *Rectilineal figures* are those which are contained by straight lines, trilateral figures being those contained by three, quadrilateral those contained by four, and multilateral those contained by more than four straight lines.
19. Of trilateral figures, an *equilateral triangle* is that which has its three sides equal, an *isosceles triangle* that which has two of its sides alone equal, and a *scalene triangle* that which has its three sides unequal.
20. Further, of trilateral figures, a *right-angled triangle* is that which has a right angle, an *obtuse-angled triangle* that which has an obtuse angle, and an *acute-angled triangle* that which has three angles acute.
21. Of quadrilateral figures, a *square* is that which is both equilateral and right-angled; an *oblong* that which is right-angled but not equilateral; a *rhombus* that which is equilateral but not right-angled; and a *rhomboid* that which has opposites sides and angles equal to one another but is neither equilateral or right-angled. And let quadrilaterals other than these be called *trapezia*.
22. *Parallel straight lines* are straight lines which, being in the same plane and being produced indefinitely in both directions, do not meet one another in either direction.

Postulates.

Let the following be postulated.

0. To draw a straight line from one point to any point.
1. To produce a finite straight line continuously in a straight line.
2. To describe a circle with any center and distance.
3. That all right angles are equal to one another.
4. That, if a straight line falling on two straight lines make the interior angles on the same side less than two right angles, the two straight lines, if produced indefinitely, meet on that side on which are the angles less than the two right angles.

Common notions.

0. *Things which are equal to the same thing are also equal to one another.*
1. *If equals be added to equals, the wholes are equal.*
2. *If equals be subtracted from equals, the remainders are equal.*
3. *Things which coincide with one another are equal to one another.*
4. *The whole is greater than the part.*

Short description of the Books of Euclid.

The work of Euclid consists of 13 books which contain propositions which are either theorems proving properties of geometrical figures or theorems concerned with proving that certain figures can be constructed. It also consists of a study of integers, rationals and reals.

- Book 1 is devoted mainly to congruent figures, area of triangles and culminates with the Theorem of Pythagoras (Proposition 47).
- Book 2 is concerned with construction of which the following is typical, determine P on AB such that $AP^2 = AB.BP$.
- Book 3 studies in detail circles, tangent to circles, tangent circles.
- Book 4 constructs polygons inscribed and outscribed to circles.
- Book 5 gives the theory of proportions.
- Book 6 applies the theory of proportions to geometrical figures.
- Book 7 studies integers, their greatest common divisor (Proposition 2) and their least common multiple (Proposition 34).
- Book 8 studies proportional numbers.
- Book 9 studies geometrical progression, in Proposition 20, the proof that the number of primes is infinite is given.
- Book 10 studies the commensurables and incommensurables.
- Book 11 is on 3 dimensional or solid geometry.
- Book 12 studies similar figures in solid geometry.
- Book 13 studies properties of pentagons and decagons as well as the regular solids.

Comment.

These definitions, postulates and axioms have been discussed since the time of Euclid. The reader is urged to study some of these discussion, for instance those in the book of Heath. Already Proclus (see Paul van Eecke) criticizes Postulate 5, and claim that it should be proven. Let me only observe here that except for the notion of being on the same side and the notion of continuity, which are absent from finite Euclidean geometry, in some sense all of the definitions and postulates given above are valid in finite Euclidean geometry. It should be stressed that the expression “produced indefinitely” (eis apeiron) cannot be translated by “to infinity” (see Heath, p. 190).

Heath observes also (p. 234) that Euclid implies that “straight lines and circles determine by their intersections other points in addition to those given” and that “the existence of such points of intersection must be postulated”. He concludes that “the deficiency can only be made good by the Principle of Continuity” and proceed by giving the axioms of Killing.

We will see that the alternate route of finite Euclidean geometry disposes of the problem quite differently and that some figures cannot always be constructed.

It will also be seen that the great emphasis given to distance between points and angles of two straight lines and their equality are notions which we will derive from more basic notions and that following the point of view adopted since the 19-th century no attempt will be made to define points and lines, as in Euclid, but we will give instead properties that they possess. In this connection the critique of Laurent, H., 1906, p.69 is of interest:

Euclid and Legendre have imagined that the word ‘distance’ has a meaning and they believed that the proofs using superposition have a ‘logical’ value. Moreover few of the present day geometers have observed that Legendre and Euclid have erred. And that is, I believe, one of the more curious psychological phenomenons that for more than two thousand years one does geometry without realizing that its fundamental propositions have no sense from a ‘logical’ point of view ¹.

I will now state a few theorems which play an important role in Part II. a few of which are not in Euclid or Legendre.

Definition.

The *altitude* through A_0 is the line through A_0 which is perpendicular to A_1A_2 . The *foot of the altitude* through A_0 is the point H_0 on the altitude and on A_1A_2 .

Theorem.

The altitudes through A_0 , A_1 and A_2 are concurrent in H .

¹Euclide et Legendre se sont figuré que le mot ‘distance’ avait un sens et ils ont cru que les démonstrations par superposition avaient une valeur ‘logique’. D’ailleurs peu de géomètres aujourd’hui s’aperçoivent que Legendre et Euclide ont divagué. Et c’est là, à mon avis, un des phénomènes psychologiques les plus curieux que, depuis plus de deux milles ans, on fait de la géométrie sans s’apercevoir que ses propositions fondamentales n’ont aucun sens au point de vue ‘logique’.

Definition.

The point H is called the *orthocenter*.

Theorem.

Let M_0 be the mid-point of A_1A_2 , let M_1 be the mid-point of A_2A_0 and let M_2 be the mid-point of A_0A_1 , then A_0M_0 , A_1M_1 and A_2M_2 are concurrent in M .

Definition.

The point M is called the *barycenter* or *center of mass*.

Definition.

m_0 is the *mediatrix* of A_1A_2 if m_0 passes through M_0 and is perpendicular to A_1A_2 .

Theorem. [Euclid, Book 4, Proposition 5.]

The mediatrices m_0 , m_1 and m_2 are concurrent in O .

Definition.

The point O is called the *center of the circumcircle of the triangle* $A_0A_1A_2$.

Theorem. [Euler]

The points H , M and O are on the same line e .

Definition.

The line e is called the *line of Euler*.

Comment.

The usual proof of 1.2.1 is geometric. The proof given by Euler is entirely algebraic. It is based on an expression for the distances of HG , HO and OG in terms of the sides of the triangle. Let a , b and c be the sides of the triangle. Let

$$p = a + b + c, q = bc + ca + ab, r = abc,$$

(the symmetric functions of a , b and c).

The area A is given by $AA = \frac{1}{16}(-p^4 + 4ppq - 8pr)^2$.

Euler obtains

$$\begin{aligned} HM HM &= \frac{1}{4} \frac{rr}{AA} - \frac{4}{9}(pp - 2q), \\ HO HO &= \frac{9}{16} \frac{rr}{AA} - (pp - 2q), \\ MO MO &= \frac{1}{16} \frac{rr}{AA} - \frac{1}{9}(pp - 2q). \end{aligned}$$

²I use here the notation of Euler and of mathematicians before the middle of the 19th century, namely AA for $A.A$.

Therefore $MO = \frac{1}{2}HM = \frac{3}{2}HO$ and $HO = HM + MO$ therefore the points H , M and O are collinear.

If I is the center of the inscribed circle, Euler determines also HI , GI and IO .

Theorem. [Euclid, Book 3, Propositions 35 and 36.]

If 2 lines through M , not on a circle meet that circle, the first one in A and B , the second one in C and D , then

$$|MA||MB| = |MC||MD|.$$

Theorem.

Let $A_0A_1A_2$ be a triangle and $H_0H_1H_2$ be the feet of the perpendiculars from the vertices to the opposite sides. then A_0H_0 bisects the angle $H_1H_0H_2$.

Proof: If H is the orthocenter, the quadrangle $HH_1A_2H_0$ can be inscribed in a circle and therefore the angles $A_0H_0H_1$ and $H_2A_2A_0$ are equal. Similarly the angles $H_2H_0A_0$ and $A_0A_1H_1$ are equal, but the angles $H_2A_2A_0$ and $A_0A_1H_1$ are equal because their sides are perpendicular, therefore $A_0H_0H_1$ and $A_0A_1H_1$ are equal.

Definition.

The triangle $H_0H_1H_2$ is called the *orthic triangle*.

1.2.2 Menelaus (about 100 A.D) and Ceva (1647-1734?).

Introduction.

The following theorems give a metric characterization of three points on the sides of a triangle which are collinear or which are such that the line joining these points to the opposite vertex are concurrent. For these theorems, an orientation is provided on each of the sides and therefore the distances have a sign. The theorems are as follows:

Theorem. [Menelaus]

If X_0 is on a_0 , X_1 is on a_1 and X_2 is on a_2 , then the points X_0 , X_1 and X_2 are collinear iff

$$|A_1X_0||A_2X_1||A_0X_2| = |A_2X_0||A_0X_1||A_1X_2|.$$

Theorem. [Ceva]

If X_0 is on a_0 , X_1 is on a_1 and X_2 is on a_2 , then the lines A_0X_0 , A_1X_1 and A_2X_2 are concurrent iff

$$|A_1X_0||A_2X_1||A_0X_2| = -|A_2X_0||A_0X_1||A_1X_2|.$$

The following theorem is a direct consequence of the theorem of Ceva. Theorem ... see Coxeter, I believe I saw it later ???

Theorem.

Let X be a point not on the sides of a triangle $A_0A_1A_2$, let X_0, X_1, X_2 be the intersection of XA_0 with A_1A_2 , of XA_1 with A_2A_0 , and of XA_2 with A_0A_1 , let Y_0, Y_1, Y_2 be the other intersection of the circle through X_0, X_1 and X_2 with the sides of the triangle, then A_0Y_0, A_1Y_1 and A_2Y_2 are concurrent.

Proof: If we eliminate $|A_iX_j|$ from the relation of Ceva and from the relations

$$|A_0X_2||A_0Y_2| = |A_0X_1||A_0Y_1|$$

$$|A_1X_0||A_1Y_0| = |A_1X_2||A_1Y_2|$$

$$|A_2X_1||A_2Y_1| = |A_2X_0||A_2Y_0|$$

obtained from Theorem 1.2.1, we obtain

$$|A_1Y_0||A_2Y_1||A_0Y_2| = -|A_2Y_0||A_0Y_1||A_1Y_2|.$$

Therefore by the Theorem of Ceva, the lines A_0Y_0, A_1Y_1 and A_2Y_2 are concurrent.

1.2.3 Euler (1707-1783) and Feuerbach (1800-1834).**Introduction.**

The geometry of the triangle has its origin in the following theorems.

Theorem.

The 3 medians of a triangle meet at a point called the barycenter or, in mechanics, the center of mass.

Theorem.

The 3 altitudes of a triangle meet at a point called the orthocenter.

Theorem.

The 3 mediatrices of a triangle meet at a point which is the center of the circumcircle.

Theorem.

The 3 bisectrices of a triangle meet at a point which is the center of the inscribed circle.

Theorem. [Euler]

The points H, G and O are on a line, called the line of Euler, moreover

$$|HG| = 2|GO| \text{ and } |HO| = 3|GO|.$$

The proof of Euler is algebraic. He determines the distance HG, GO and HO in terms of the length of the sides of the triangle. Other distances are also determined in the same paper.

Theorem. [Brianchon and Poncelet]

The mid-points of the sides of a triangle, the feet of the altitudes and the mid-points of the segments joining the orthocenter to the vertices of the triangle are on a circle, called the circle of Brianchon-Poncelet. It is also called the 9 point circle or the circle of Feuerbach, who discovered it independently, and improperly the circle of Euler.

Theorem. [Feuerbach]

The circle of Brianchon-Poncelet is tangent to the inscribed circle and to the three excircled circles, the point of tangency for the inscribed circle is called the point of Feuerbach.

The proof given by Feuerbach is algebraic and trigonometric in character. It expresses distances in terms of the length of the sides and of the trigonometric functions of the angles of the triangle.

1.2.4 The Geometry of the Triangle. Lemoine (1840-1912).**Introduction.**

An interesting development of Euclidean geometry occurred during the 19-th century, known under the name of the geometry of the triangle. The activity in this area was most intense during the period 1870-1900. A large number of elementary results were obtained especially in Belgium and France, but also in England, Germany and elsewhere. Strictly speaking, the Theorem of Euler of 1.2.3 can be considered as the first important new result in this connection since Euclid. Others which prepared the way were the theorems of Brianchon-Poncelet of 1.2.3 and the Theorem of Feuerbach of 1.2.3. A few theorems will be extracted from the long list.

Theorem. [Schröter]

*If $a \times b$ denotes the point on a and b and $A \times B$ denotes the line through A and B ,
Let*

$$\begin{aligned} F_0 &:= (M_1 \times H_2) \times (M_2 \times H_1), \\ F_1 &:= (M_2 \times H_0) \times (M_0 \times H_2), \\ F_2 &:= (M_0 \times H_1) \times (M_1 \times H_0). \\ G_0 &:= (M_1 \times M_2) \times (H_1 \times H_2), \\ G_1 &:= (M_2 \times M_0) \times (H_2 \times H_0), \\ G_2 &:= (M_0 \times M_1) \times (H_0 \times H_1). \end{aligned}$$

0. F_0, F_1 and F_2 are on the line e of Euler.
1. $A_0 \times G_0, A_1 \times G_1$ and $A_2 \times G_2$ are parallel and are perpendicular to e .
2. A_0, F_0, G_1 and G_2 are collinear, and so are A_1, F_1, G_2 and G_0 as well as A_2, F_2, G_0 and G_1 .
3. G_0, G_1, G_2 are the vertices of a triangle conjugate to the circle of Brianchon-Poncelet.

4. $M_0 \times G_0$, $M_1 \times G_1$ and $M_2 \times G_2$ pass through the same point S .
5. $H_0 \times G_0$, $H_1 \times G_1$ and $H_2 \times G_2$ pass through the same point S' .
6. S and S' are on the circle of Brianchon-Poncelet.
7. S and S' are on the polar of H with respect to the triangle A_0, A_1, A_2 .

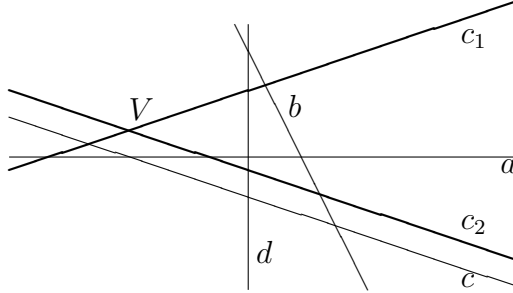
S and S' are called the *points of Schröter*.

The proof of this Theorem published by Schröter in “Les Nouvelles Annales de Mathématiques” in 1864, was obtained by several people. The published proof is that of a student of Sainte-Barbe, L. Lacachie. The Theorem is generalized to Projective Geometry in III.D8.1,D8.2,C8.0. It is stated in finite involutive geometry in III.??.

1.2 Projective Geometry.

1.2.1 The preparation. Menaechmus (about 340 B.C.), Apollonius (260? B.C - 200? B.C.), Pappus (300 - ?).

The projective geometry has its source in the discovery of the conic sections, the ellipse, the parabola and the hyperbola, which is ascribed by Proclus to the Greek mathematician Menaechmus, a pupil of Plato and Eudoxus. The conic sections were studied by Aristaeus the Elder, Euclid, Archimedes, Pappus of Alexandria and finally by Apollonius of Perga. The conics are defined as the intersection of a (circular) cone by a plane not passing through its vertex. If we make a cut of the cone with a plane through the vertex we obtain two lines c_1 and c_2 . Line a is the cut of a plane giving an hyperbola, line b is the cut of a plane giving a parabola, line c gives an ellipse and line d gives the special case of a circle.



Among the many contributions of Pappus I will cite the discovery that the anharmonic ratio of 4 points is unchanged after projection, where the anharmonic ratio of A, B, C and D is $\frac{\text{dist}(C,A) \text{dist}(D,B)}{\text{dist}(C,B) \text{dist}(D,A)}$. This is a fundamental property in geometry.

The important notion of point at infinity can be traced to Kepler, in 1604, and Desargues, in 1639 (see Heath, I, p. 193). This leads to the notion of the extended Euclidian plane which contains besides the ordinary points, the directions, each one is what is common to the set of parallel line, and the set of all directions, or line at infinity.

1.2.2 Gérard Desargues (1593-1661) and Blaise Pascal (1623-1662).

Introduction.

The extensive study of the conics by Apollonius was eventually taken up again by Pascal. One of his many new results is Theorem 2.2.11 which allows the construction 2.2.11 and 1.2.2 of a conic using the ruler only. The second construction is attributed to MacLaurin. But the two constructions are closely related to each other as will be seen. The Theorem of Pascal was generalized to n dimension by Arthur Buchheim in 1984.

Notation.

I will introduce in III.?? detailed notations which allow a compact description of constructions. For instance,

$$a_0 := A_1 \times A_2$$

means that the line a_0 is defined as the line through the 2 points A_1 and A_2 .

Theorem. [Pascal]

Given the points A_0, A_1, A_2, A_3, A_4 and A_5 .

Let P_0 be the point common to $A_0 \times A_1$ and $A_3 \times A_4$, let P_1 be the point common to $A_1 \times A_2$ and $A_4 \times A_5$, let P_2 be the point common to $A_2 \times A_3$ and $A_5 \times A_0$. A necessary and sufficient condition for A_0, A_1, A_2, A_3, A_4 and A_5 to be on the same conic is that P_0, P_1 and P_2 be collinear.

This theorem leads to 2 construction of conics.

Construction.[Pascal]

Given 5 points A_0, A_1, A_2, A_3 and A_4 . To each line through A_4 corresponds a point A_5 on the conic.

$$\begin{aligned} a_0 &:= A_0 \times A_1, a_1 := A_1 \times A_2, a_2 := A_2 \times A_3, a_3 := A_3 \times A_4, \\ P_0 &:= a_0 \times a_3, a_4 \text{ is an arbitrary line through } A_4, \\ P_1 &:= a_1 \times a_4, e := P_0 \times P_1, P_2 := e \times a_2, \\ a_5 &:= A_0 \times P_2, A_5 := a_4 \times a_5. \end{aligned}$$

Construction. [MacLaurin] ³

If the sides of a triangle pass through three fixed points, and two vertices trace straight lines, the third vertex will trace a conic through two of the given points.

The proof follows from Pascal's Theorem. The construction can be given in the following explicit form:

A_0, A_1, A_2, A_3, A_4 are 5 given points.

To each line l through P_0 will correspond a point A_5 on the conic.

$$\begin{aligned} a_0 &:= A_0 \times A_1, a_1 := A_1 \times A_2, a_2 := A_2 \times A_3, a_3 := A_3 \times A_4, \\ P_0 &:= a_0 \times a_3, P_1 := l \times a_1, P_2 := l \times a_2, \end{aligned}$$

³as stated by Braikenridge

$a_4 := A_4 \times P_1$, $a_5 := A_0 \times P_2$, $A_5 := a_4 \times a_5$.

The triangle is $\{P_1, P_2, A_5\}$, P_1 is on a_1 , P_2 is on a_2 , $P_1 \times P_2$ passes through P_0 , $P_1 \times A_5$ passes through A_4 , $P_2 \times A_5$ passes through A_0 .

Comment.

Pascal would not have easily accepted a finite geometry. Indeed in his “Pensées”, he says (p. 567),

that there are no geometers which do not believe that space is infinitely divisible.

Also discussing both the infinitely large and the infinitely small, he writes (p. 564)

In one word, whatever the motion, whatever the number, whatever the space, whatever the time, there is always one which is larger and one which is smaller, in such a way they they sustain each other between nothing and infinity, being always infinitely removed from those extremes. All these truths cannot be proven, and still they are the foundations and the principles of geometry.

1.2.3 Lazare Carnot (1783-1823).

A contemporary of Poncelet, Carnot obtained many results of which the following is in the line of Manelaus and Ceva applied to conics.

Theorem. [Carnot]

If a conic cuts the side $A \times B$ of a triangle $\{A, B, C\}$ at C_1 and C_2 , and similarly the side $B \times C$ cut the conic at A_1 and A_2 and the side $C \times A$ at B_1 and B_2 , then the oriented distances satisfy

$$AC_1.AC_2.BA_1.BA_2.CB_1.CB_2 = AB_1.AB_2.BC_1.BC_2.CA_1.CB_2$$

This is generalized to curves of degree n .⁴

Theorem.

Let $A_0B_0C_0$ be a triangle and X be a point not on its sides,

Let $A_0 \times X$ meet $A_1 \times A_2$ at X_0 , $A_1 \times X$ meet $A_2 \times A_0$ at X_1 and $A_2 \times X$ meet $A_0 \times A_1$ at X_2 . Let Y_0 be a point on $A_1 \times A_2$, Y_1 be a point on $A_2 \times A_0$ and Y_2 be a point on $A_0 \times A_1$, then a necessary and sufficient condition for $X_0, X_1, X_2, Y_0, Y_1, Y_2$ to be on the same conic is that the lines $A_0 \times Y_0, A_1 \times Y_1, A_2 \times Y_2$ be concurrent.

This is a consequence of the Theorem of Carnot.

1.2.4 Jean Poncelet (1788-1867).

The work of Poncelet done while a prisoner of Russia at the end of Napoleon’s campaign, was fundamental in isolating those properties of Euclidean geometry which are independent

⁴Eves p.358

of the notions of distances and measure of angles and dependent only on incidence properties and appropriate axioms which involve only incidence. One of is celebrated Theorems is the following.

Theorem.

If a n sided polygon is inscribed in a conic and outscribed to an other conic, then if with start from any point on the first conic and draw a tangent to the second, then obtain the other intersection with the first conic and repeat the construction, the new polygon closes after n steps.

There are many proofs of this Theorem. The proofs which are done using the theory of elliptic functions, suggested to me that the Jacobi elliptic functions could be generalized to the finite case.

1.2.5 Joseph Gergonne (1771-1858).

Gergonne was the first to recognize the property of duality which plays a fundamental role in projective geometry.⁵

1.2.6 Michel Chasles (1793-1880).

Chasles greatest contribution to projective geometry, according to Coolidge ⁶ is the study of the cross ratio also called anharmonic ratio.⁷

1.3 Relation between Projective and Euclidean Geometry.

1.3.0 Introduction.

Projective geometry is concerned only with those properties in geometry which are preserved under projection. Euclidean, as well as non Euclidean geometry can be derived from projective geometry. The connection through transformation groups will be described in section 1.6.11.

The first connection goes back to the work of Poncelet, but it is has been deemphasized in the teaching of the subject, except for the first step (affine geometry). I will presently summarize this approach. Terms which are unknown to the reader, will be defined in the later Chapters.

In projective geometry, no line is distinguished from any other, no point is similarly distinguished. The main notions are those of incidence, perspectivity, projectivity, involution

⁵Coxeter, p.13

⁶p.96.

⁷See also Coxeter, p.165.

¹G13.TEX [MPAP], September 9, 2019

and polarity, the last notion leading naturally to conics. Euclidean geometry can be considered as derived from projective geometry by choosing some elements in it and distinguishing them from all others. I will proceed in 3 steps.

1.3.1 Affine Geometry.

Introduction.

In this first step one line is distinguished. This line is called the ideal line, or line at infinity. When we do so, we obtain the so called affine geometry. Points fall now into two categories, the ordinary points, which are not on the ideal line and the ideal points which are. Lines fall in two categories, the ideal line and the others which we can call ordinary. From the basic notion of parallelism follow the derived notions of parallelogram, equality of vectors on the same line or on parallel lines, trapeze or rhombus, mid-point, barycenter, center of a conic, area of triangles.

Definition.

Two distinct ordinary lines are *parallel* iff their common point is an ideal point.

Definition.

A *vector* $\overrightarrow{B,C}$ is an ordered pair of points.

Definition.

If the lines $B \times C$ and $D \times E$ are parallel, the vectors $\overrightarrow{B,C}$ and $\overrightarrow{D,E}$ are *equal* iff the lines $B \times D$ and $C \times E$ are also parallel.

Definition.

If B, C, D and E are on the same line, the vectors $\overrightarrow{B,C}$ and $\overrightarrow{D,E}$ are *equal* iff there exists 2 points F and G on a parallel line, such that $\overrightarrow{B,C} = \overrightarrow{F,G}$ and $\overrightarrow{F,G} = \overrightarrow{D,E}$. This definition has, of course, to be justified. It can be replaced by: $\overrightarrow{B,C}$ and $\overrightarrow{D,E}$ are *equal* iff there exists a parabolic projectivity, with the fixed point being the ideal point on the line, which associates C to B and E to D .

Definition.

The *center* of a conic is the pole of the ideal line, in the polarity whose fixed points are the conic.

Definition.

Two points are *conjugate* iff one is on the polar of the other.

Theorem.

Conjugate points on a given line determine an involution.

Definition.

A *parabola* is a conic tangent to the ideal line. The point of tangency is called the *direction of the parabola*.

Example.

The parabola $y^2 = 4cx$, in homogeneous coordinates is

$$Y^2 = 4cXZ. \quad (1)$$

Its intersection with $Z = 0$ is $Y = 0$. The parabola is tangent to $Z = 0$ at $(1,0,0)$.

Definition.

The *focus of a parabola* is the intersection of the ordinary tangents to the parabola from the isotropic points. The *directrix* of the parabola is the polar of the focus. The *axis* of the parabola is the line through the focus and the direction of the parabola. The *vertex* of the parabola is the point of the parabola on its axis.

Example.

The tangent to the parabola at $(X_0, Y_0, 1)$ is

$$2cX - Y_0Y + 2cX_0Z = 0. \quad (2)$$

It passes through the isotropic point $(1, i, 0)$ if $2c = Y_0 i$, hence because of (1), $X_0 = -c$. The tangent is therefore $X + Y i - c = 0$. The tangent from the other isotropic point is $X - Y i - c = 0$. They both intersect at $(c, 0, 1)$.

The polar is obtained by substituting in (2) this point for $(X_0, Y_0, 1)$, this gives $X = -cZ$. The axis is $Y = 0$, the vertex is $(0, 0, 1)$.

Comment.

The terminology can be changed by accepting as points and lines only those which are ordinary. An ideal point is renamed a direction. We obtain in this way, something which is closer to the terminology used by Euclid.

1.3.2 Involution geometry.

Introduction.

The second step consists in considering the involutions on the ideal line. Among all the involutions we can distinguish one of them and call it the fundamental involution. Three cases are possible, the involution may have 2 fixed ideal points, in which case it is called hyperbolic, one fixed point in which case it is called parabolic and no fixed point, in which case it is called elliptic. If we extend the projective geometry to the complex case, these

ideal points then exist, but are not real.

The elliptic case, which leads to Euclidean Geometry and the hyperbolic case which leads to the Geometry of Minkowski can be studied together. The parabolic case, which leads to the Galilean Geometry is studied separately.

Using the fundamental involution, either elliptic or hyperbolic, we can introduce the basic notion of perpendicularity and from it follow the derived notion of right triangle, rectangle, altitude, orthocenter, circle, equal segment, isosceles and equilateral triangles, center of circumcircle, Euler line, circle of Brianchon-Poncelet.

In the alternate second step, one involution with 2 real fixed points is distinguished. It is only if we stay with real projective geometry as opposed to complex projective geometry that the hyperbolic involutive geometry is distinct from the elliptic involutive geometry. Staying with real projective geometry, the notions which are introduced can be given the same name as in the elliptic involutive geometry, the definitions may differ slightly, but properties are quite analogous.

Definition.

When the fundamental involution has no real fixed points, I will call the geometry *elliptic involutive geometry*.

When the fundamental involution has no real fixed points, I will call the geometry *hyperbolic involutive geometry*.

Definition.

The fixed points of the fundamental involution are called *isotropic points*. Any ordinary line through an isotropic point is called an *isotropic line*. Strictly speaking, the *ideal points* are those on the ideal line which are not isotropic, and the *ordinary lines* are those which are not isotropic.

Definition.

Two *lines are perpendicular* iff their ideal points are pairs of the fundamental involution.

Definition.

A conic is a *circle* iff the involution that the conic determines on the ideal line is the fundamental involution.

Theorem.

A conic which passes through the 2 isotropic points is a circle .

Definition.

A *segment* $[AB]$ is an unordered pair of points.

Definition.

The segment $[AB]$ and the segment $[CD]$ are equal iff the point E constructed in such a way that $ACDE$ is a parallelogram, is such that E and B are on the same circle centered at A .

Definition.

The center of a circle is the intersection of the tangents to the circle at the isotropic points.

Comment.

A geometry could also be constructed in which the correspondence on the ideal line associates every point to one of them. This corresponds, using algebra, to the transformation

$$T(x) = \frac{ax+b}{cx-a}, aa + bc = 0.$$

This is the parabolic involutive geometry.

Before leaving the subject of involutive geometry, I would like to make the following observation, which will be useful to understand terminology in non-Euclidean geometry. The step to construct non-Euclidean geometry from projective geometry, which correspond to involutive geometry, is to choose a particular conic as ideal, or set of ideal points. In view of the fact that a line conic can degenerate in the set of lines passing through either one or the other of 2 points, we can observe that the ideal in the involutive geometry is such a degenerate conic. This analogy will be pursued to define, using the ideal conic, notions in non-Euclidean geometry which are related to notions of Euclidean geometry and will help in an economy of terminology, but nothing more.

1.4 Analytic Geometry.

1.4.1 René Descartes (1596-1650)[La Géométrie].

The prime motivation of Descartes when he wrote, “La Géométrie” appears to have been a long standing problem, the determination of the locus of Pappus.⁸

In present day notation, given lines l_i and angles α_i , the problem is to determine the locus of a point C and its α_i projections U_i on l_i , such that the angle of $C \times U_i$ with l_i is α_i , and for instance, with $i = 0, 1, 2, 3$, such that

$$|CU_0| |CU_2| = k |CU_1| |CU_3|. \quad (1)$$

Descartes chooses as axis l_0 and $u_0 := C \times U_0$, he chooses also some orientation which allows him to associate to the points on these axis, some real number. If $x := |U_0, A_1|$, $y := |C, U_0|$, $a_i := |A_1, A_i|$, $i = 1, 2, 3$, if X_i are the intersection of l_i with a , then the prescribed angles imply by similarity

$$\frac{|U_0 X_i|}{|U_0 A_i|} = \frac{b_i}{e}, \frac{|CU_i|}{|CX_i|} = \frac{c_i}{e},$$

for some b_i, c_i and unit of distance e .

The distances $|CU_i|$ are linear functions of x and y and therefore replacing in (1) gives the equation of a conic through A_1 . By symmetry, the conic passes through A_3, B_1 and B_3 .

¹G14.TEX [MPAP], September 9, 2019

⁸p. 8

Indeed,

$$\begin{aligned} |CU_0| &= y, \\ U_0A_1 &= x, U_0X_1 = \frac{b_1}{e}x, |CX_1| = |CU_0| + |U_0X_1| = y + \frac{b_1}{e}, CU_1 = (y + \frac{b_1}{e})\frac{c_1}{e}, \\ |U_0A_2| &= x + a_2, U_0X_2 = (x + a_2)\frac{b_2}{e}, CX_2 = y + (x + a_2)\frac{b_2}{e}, \\ CU_2 &= (y + (x + a_2)\frac{b_2}{e})\frac{c_2}{e}, CU_3 = (y + (x + a_3)\frac{b_3}{e})\frac{c_3}{e}. \end{aligned}$$

Nowhere, in his work are the axis or arrows on them indicated specifically or are the axis chosen at a right angle, except if convenient to solve the problem at hand.

1.4.2 After Descartes.

Using modern terminology, the problem posed by Descartes, was to construct an algebraic structure which is isomorphic to Euclidean geometry. More precisely the problem is to obtain algebraic elements P' which are in one to one correspondence with points P , algebraic elements l' which are in one to one correspondence with lines l , an algebraic relation $P' \cdot l' = 0$ associated to the incidence relation in geometry, P is on l or l is through P , written $P \cdot l = 0$, such that if l' corresponds to l and P' to P , $P' \cdot l' = 0$ if and only if $P \cdot l = 0$.

Similar correspondences have to be given for perpendicularity, equality of angles and segments, measure of angle and segments, etc. Descartes' solution is to choose 2 lines xx and yy in the Euclidean plane and to associate, if these are perpendicular, to a point P the 2 real numbers x and y which are the distances from P to yy and to xx .

$$P' = \delta(P) = (x, y).$$

This correspondence is not one to one. If $x, y \neq 0$, there are four points which will give the same pair (x, y) . To solve this problem a sign must be associated to the distances, corresponding to an orientation on the lines xx and yy . Usually, with xx horizontal and yy vertical, x is positive to the right of yy , y is positive above xx .

The distance between (x, y) and (x', y') of the points P and Q is given by

$$\sqrt{(x' - x)^2 + (y' - y)^2}.$$

To represent the lines, several choices are possible, one such choice, is the pair $[m, b]$, where b is the (oriented) slope and b it the distance from the intersection of the line with yy , the so called y intercept. In this case, if (x, y) corresponds to the point P and $[m, b]$ to the line l , (x, y) is on $[m, b]$ if and only if

$$y = mx + b.$$

Perpendicularity of $[m, b]$ and $[n, c]$ is defined by $m n = -1$.

The difficulty of this representation is that lines perpendicular to xx do not have a (finite) slope. Reversing the role of xx and yy does not help.

An other representation of lines that can be chosen, is to take the pair $\{l_0, l_1\}$ of the distances l_1 and l_0 from the origin to the intersection of the line l with xx and yy ,

$$l' = \delta(l) = \{l_0, l_1\},$$

with the incidence property represented by the relation

$$l_0x + l_1y - l_0l_1 = 0.$$

In particular, the points $(l_1, 0)$ and $(0, l_0)$ are on l' . The perpendicularity property of l' and m' is represented by the bilinear relation

$$l_0m_1 + l_1m_0 = 0.$$

This again is not suitable because this representation fails for lines through the origin.

The correspondence finally chosen by Descartes is a triple of real numbers $[a, b, c]$ which are obtained from l_0, l_1 and $l_0 l_1$ by multiplication by some arbitrary non zero real k .

$$[a, b, c] = k[l_0, l_1, l_0 l_1].$$

For a line through the origin $c = 0$, $\frac{b}{a}$ is the slope, A line parallel to yy is represented by $(1, 0, c)$ where $-c$ is the x intercept.

The incidence property is the familiar linear relation

$$ax + by + c = 0.$$

But it is important to realize that the correspondence is not one to one. The line is represented by the set of all triples corresponding to all the possible value of k , a so called equivalence class, the numbers a, b, c are called the homogeneous coordinates of the line. Perpendicularity of $[a, b, c]$ and $[a', b', c']$ is represented by

$$aa' + bb' + cc' = 0.$$

By analogy, one could represent points by a triple $(x, y, 1)$ or by any equivalent set $(X, Y, Z) = k(x, y, 1)$, $k \neq 0$. This implies that $Z = k \neq 0$ and $X = kx$, $Y = ky$ or $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$.

The incidence property is then

$$aX + bY + cZ = 0. \tag{2}$$

(X, Y, Z) are the so called homogeneous coordinates of an algebraic point.

1.4.3 Jean Poncelet (1788-1867).

Poncelet was one of the first to take full advantage of the fact that parallel lines define a direction, which can be called the point at infinity and that all the points at infinity can be considered to be on a line, the line at infinity. This constitutes the decisive step towards the development of projective geometry.

The algebraic points $(X, Y, 0)$, with X and Y not both 0, correspond to these new geometric points, They are all on the line $[0, 0, 1]$ which is the line at infinity. The distance between the algebraic points (X, Y, Z) and (X', Y', Z') , with Z and $Z' \neq 0$, is given by

$$\sqrt{\left(\frac{X'}{Z'} - \frac{X}{Z}\right)^2 + \left(\frac{Y'}{Z'} - \frac{Y}{Z}\right)^2}.$$

Comment.

The extension of the Euclidian plane by adding the points at infinity and a line at infinity is distinct from the extension of the complex plane, in which to all the points $x + iy$, x and y real (and $i^2 = -1$), we add 1 point at infinity. In a complex plane, all lines pass through the point at infinity.

It is not the place here to review all the other basic formulas of analytic geometry. However, there is an important consequence of the isomorphism between synthetic geometry and analytic geometry, which is implicit in the work of Poncelet and is associated to the properties of circles, which was the basis of Poncelet's method to obtain properties for conics in general.

The equation of a circle of center (a, b) and radius R is

$$(x - a)^2 + (y - b)^2 = R^2,$$

or in homogeneous coordinates,

$$(X - aZ)^2 + (Y - bZ)^2 = R^2 Z^2.$$

The points on the circle and on the line at infinity $Z = 0$ satisfy

$$X^2 + Y^2 = 0,$$

which has no real solution. The introduction of complex numbers, whose use had become standard by the time of Poncelet, suggested the definition of a complex analytic geometry, with elements

$(X, Y, Z) = k(X, Y, Z)$, k, X, Y, Z complex, $k \neq 0$ and not all X, Y, Z equal to zero, and with elements

$(a, b, c) = k'(a, b, c)$, k', a, b, c complex, $k' \neq 0$ and not all a, b, c equal to zero, The incidence property being again (1).

The complex elements which are not real correspond to new points and lines in synthetic geometry, the complex points and the complex lines. In this structure, $(1, i, 0)$ and $(1, -i, 0)$ are 2 points on the line at infinity which are also on every circle. They are called isotropic points and play an essential role in both Euclidean geometry, extended to the complex and in what I call involutive geometry.

1.4.4 James Singer on Difference sets and finite projective Geometry.

Introduction.

Inspired by the paper of Veblen and MacLagan-Wedderburn of 1907, Singer introduced in October 1934 (Singer, 1938, Baumert, 1971) the important concept of cyclic difference sets which allows for an arithmetization of projective geometry which is as close to the synthetic point of view as is possible. With this notion, it becomes possible to label points and hyperplanes in N dimensional projective geometry of order p^k . With it, in the plane, it is not only trivial to determine all the points on a line, and lines incident to a point but also the lines through 2 points and points on 2 lines.

Completely independently, one of my first students at the “Université Laval”, Quebec City, made the important discovery that the regular polyhedra can be used as models for finite geometries associated with 2, 3 and 5. Then, he introduced the nomenclature of selector (sélecteur) for the notion of cyclic difference sets, to construct an appropriate numbering of the points and lines on the polyhedra. The definition of selector function and selector correlation is implicit in his work.

The notion of cyclic difference sets makes duality explicit through the correlation, which is the polarity when $p \geq 5$, introduced by Fernand Lemay.

After defining selector and selector function, I associate with them points and lines in the projective plane, represented by integers and give Singer’s results which prove the existence of selectors using the notion of primitive polynomials, 1.4.4.

1.4.4 is a special case of what is needed to determine when an irreducible polynomial is a primitive polynomial. ⁹ 1.4.4 gives a form of the primitive polynomial and the generator, so chosen that the polynomials whose coefficient define the homogeneous coordinates of points and lines satisfy the same 4 term recurrence relation.

⁹Baumert, p. 101

Definition.

Given a power $q = p^k$ of a prime p , a *selector* or *difference set* is a subset of $q + 1$ distinct integers, such that their $q(q + 1)$ differences modulo $n := q^2 + q + 1$ are all of the integers from 1 to $q^2 + q$.

Example. [Singer.]

The following are selectors with $q = p^k$:

For $p = 2$: 0, 1, 3, modulo 7.

For $p = 3$: 0, 1, 3, 9, modulo 13.

For $q = 2^2$: 0, 1, 4, 14, 16, modulo 21.

For $p = 5$: 0, 1, 3, 8, 12, 18, modulo 31.

For $p = 7$: 0, 1, 3, 13, 32, 36, 43, 52, modulo 57.

For $q = 2^3$: 0, 1, 3, 7, 15, 31, 36, 54, 63, modulo 73.

For $q = 3^2$: 0, 1, 3, 9, 27, 49, 56, 61, 77, 81, modulo 91.

For $q = 11$: 0, 0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109 modulo 133.

Theorem.

If s_i , $i = 0$ to p is a selector then, for any j ,

0. $s'_i = a + ks_{i+j}$, is also a selector.

The indices are computed modulo $q + 1$ and the selector numbers, modulo n .

Definition.

If $a = 1$ and $k = -1$, the selector $s'_i := 1 - s_i$ is called the *complementary selector* or *co-selector* of s_i . The selectors obtained using $k = 2, \frac{1}{2}$, are called respectively *bi-selector*, *semi-selector*.

Example.

0. For $q = 4$, other selectors are 10, 12, 17, 18, 21 and 0, 1, 6, 8, 18.

1. For $p = 7$, if
the selector is 0, 1, 7, 24, 36, 38, 49, 54,
then
the co-selector is 0, 1, 4, 9, 20, 22, 34, 51,
the bi-selector is 0, 1, 5, 27, 34, 37, 43, 45,
the semi-selector is 0, 1, 9, 11, 14, 35, 39, 51.

Definition.

The *selector function* f is the function from Z_n to Z_n

$$f(s_j - s_i) = s_i, i \neq j.$$

Theorem.

$$f(j - i) - i = f(i - j) - j.$$

Example.

For $p = 3$, and $n = 13$, the selector function associated with the selector 0,1,3,9 is

i	1	2	3	4	5	6	7	8	9	10	11	12
$f(i)$	0	1	0	-4	-4	3	-4	1	0	3	3	1

Definition.

Given a selector, points in the projective plane associated with $q = p^k$, with $n = q^2 + q + 1$ elements are integers in Z_n , and lines are integers in Z_n followed by $*$, with the incidence defined by

a is on b^* iff $f(a + b) = 0$ or $a + b = 0$.

Theorem.

$$0. a \times b = (f(b - a) - a)^*.$$

$$1. a^* \times b^* = f(b - a) - a.$$

$$2. a \text{ on } b^* \Rightarrow b \text{ on } a^*.$$

The Statements immediately reflect the duality in projective geometry.

Example.

For $p = 3$, and the selector 0,1,3,9, the lines and the points on them are

lines	0*	1*	2*	3*	4*	5*	6*	7*	8*	9*	10*	11*	12*
points	0	12	11	10	9	8	7	6	5	4	3	2	1
on	1	0	12	11	10	9	8	7	6	5	4	3	2
*	3	2	1	0	12	11	10	9	8	7	6	5	4
	9	8	7	6	5	4	3	2	1	0	12	11	10

Theorem.

In the projective geometry associated with $q = p^k$ and the selector $\{s_0, s_1, \dots, s_q\}$

$$i + s_0, i + s_1, \dots, i + s_p$$

are the $q + 1$ points on the line $-i^*$, the addition being done modulo $n = q^2 + q + 1$.

Definition. [Singer]

P is a *primitive polynomial* in the Galois Field $GF(p^k)$ iff P is of degree k and $I^{p^{k-1}}$ is the smallest power of I , modulo P , which is identical to 1.

Example.

0. $I^3 + I + 1 = 0$ is primitive in $GF(2^3)$.

With $2 \equiv 0$ modulo 2, we have, modulo P, $I^3 = I + 1$, $I^4 = I^2 + I$, $I^5 = I^2 + I + 1$, $I^6 = I^2 + 1$, $I^7 = 1$.

It is well known that

Theorem.

A primitive polynomial always exists.

Theorem.

P is a *primitive polynomial of degree m* over the *Galois field $GF(q)$* , iff P is an irreducible polynomial of degree m over $GF(q)$ and for a given primitive root ρ of $GF(q^m)$, $P(\rho) = 0$.

Theorem. [Singer]

For each value of $q = p^k$, a selector can be obtained by choosing a primitive polynomial of degree 3 over $GF(q)$. It is, with 0, the set of exponents of I such that the coefficient of I^2 is 0.

Example.

For $p = 3$, $P = I^3 - I + 1$, $I^3 = I - 1$, $I^4 = I^2 - I$, $I^5 = I^2 - I + 1$, $I^6 = I^2 + I + 1$, $I^7 = I^2 - I - 1$, $I^8 = I^2 + 1$, $I^9 = I + 1$, $I^{10} = I^2 + I$, $I^{11} = I^2 + I - 1$, $I^{12} = I^2 - 1$, $I^{13} = 1$. Therefore the selector is 0, 1, 3, 9.

Theorem.

*Let the primitive polynomial be $P_3 := I^3 + bI - c$ and the generator be $G := I + g$, let $g' := 3g^2 + b$, $h' = g^3 + bg + c$, $h = \frac{1}{h'}$, let $J^{(n)} := h^{-n}G^{-n+1} * G^{-n}$, then*

0. $G^2 = I^2 + 2gI + g^2$,
 1. $G^3 = 3gI^2 + (3g^2 - b)I + (g^3 + c)$,
 2. $G^{-1} = hI^2 - ghI + (g^2 + b)h$,
 3. $G^{-2} = g'h^2I^2 + (1 - g'gh)hI + (-2gh + g'(g^2 + b)h^2)$.
1. $G^{n+3} = 3gG^{n+2} - g'G^{n+1} + h'G^n$,
 1. $G^n = h(g'G^{n+1} - 3gG^{n+2} + G^{n+3})$.
2. $J^{(0)} = I^2$,
 1. $J^{(1)} = gI^2 + I$,
 2. $J^{(2)} = (g^2 - b)I^2 + 2gI + 1$.
3. $J^{(n+3)} = 3gJ^{(n+2)} - g'J^{(n+1)} + h'J^{(n)}$,
 1. $J^{(n)} = h(g'J^{(n+1)} - 3gJ^{(n+2)} + J^{(n+3)})$.

In other words the 4 term recurrence relation is the same for the points associated to G^n (1.) as for the lines associated to $J^{(n)}$ (3.).

Proof: 0.0. is immediate.

$G^3 = (I + g)^3$, or because of P_3 we get 0.1. Eliminating 1, I and I^2 from G^1 , G^2 and G^3 gives $G^3 = 3gG^2 - g'G + h'$. Multiplying by G^n gives 1.0 hence 1.1.

From this recurrence relation is it easy to get 0.2. and 0.3. $J^{(n)} := h^{-n}G^{1-n} * G^{-n}$, this gives easily 2.0., 2.1, 2.2. We should be careful not to scale.

The definition of $J^{(n)}$ implies

$$\begin{aligned} J^{(n+3)} &= h^{-n-3}G^{-n-2} * G^{-n-3} \\ &= h^{-n-2}G^{-n-2} * (g'G^{-n-2} - 3gG^{-n-1} + G^{-n}) \\ &= 3gJ^{(n+2)} - h^{-n-2}G^{-n} * G^{-n-2} \\ &= 3gJ^{(n+2)} - h^{-n-1}G^{-n} \times (g'G^{-n-1} - 3gG^{-n} + G^{-n+1}) \\ &= 3gJ^{(n+2)} - g'J^{(n+1)} + h'J^{(n)}. \end{aligned}$$

Example.

$p = 5, g = -2, b = -1, c = 2, g' = 1, h' = 1, h = 1,$
 $P_3 = I^3 - I - 2, G^3 = -G^2 - G + 1. J^{(3)} = -J^{(2)} - J^{(1)} + 1.$

i	G^i	$J^{(i)}$	i	G^i	$J^{(i)}$	i	G^i	$J^{(i)}$
-2	(1, 3, 2)	[3, 3, 1]	9	(2, 4, 3)	[0, 4, 2]	20	(4, 2, 4)	[3, 2, 4]
-1	(1, 2, 3)	[4, 2, 1]	10	(0, 2, 3)	[3, 2, 0]	21	(4, 4, 0)	[4, 4, 4]
0	(0, 0, 1)	[1, 0, 0]	11	(2, 4, 4)	[1, 4, 2]	22	(1, 1, 3)	[4, 1, 1]
1	(0, 1, 3)	[3, 1, 0]	12	(0, 3, 1)	[1, 3, 0]	23	(4, 2, 1)	[0, 2, 4]
2	(1, 1, 4)	[0, 1, 1]	13	(3, 0, 3)	[1, 0, 3]	24	(4, 1, 1)	[0, 1, 4]
3	(4, 3, 4)	[3, 3, 4]	14	(4, 1, 0)	[4, 1, 4]	25	(3, 3, 1)	[4, 3, 3]
4	(0, 2, 0)	[0, 2, 0]	15	(3, 2, 3)	[1, 2, 3]	26	(2, 3, 4)	[1, 3, 2]
5	(2, 1, 0)	[2, 1, 2]	16	(1, 2, 0)	[1, 2, 1]	27	(4, 0, 1)	[0, 0, 4]
6	(2, 0, 4)	[1, 0, 2]	17	(0, 2, 2)	[2, 2, 0]	28	(2, 0, 1)	[3, 0, 2]
7	(1, 1, 1)	[2, 1, 1]	18	(2, 3, 1)	[3, 3, 2]	29	(1, 3, 2)	[3, 3, 1]
8	(4, 0, 0)	[4, 0, 4]	19	(4, 2, 2)	[1, 2, 4]	30	(1, 2, 3)	[4, 2, 1]

The selector is

0,1,4,10,12,17. Line 1* is incident to points -1=30, 0,3,9,11 and 16.

1.5 Trigonometry and Spherical Trigonometry.

1.5.1 Aryabatha I (476-?).

The first known table of trigonometric functions corresponds

$$crd(\alpha) = 2\sin(\frac{1}{2}\alpha)$$

and to $\alpha = 0$ to 90° step $15'$, using two sexagesimal places. for instance, $crd(36^\circ) = 2\sin(18^\circ) = 37, 4, 55$. (See ...).

The trigonometric functions were first defined as ratios of the sides of a triangle by Rhäticus, who constructed 10 place tables for \sin , \cos , \tan , \cot , \sec and \csc , in increments of $10''$,

¹G15.TEX [MPAP], September 9, 2019

and 15 place tables for \sin , with first second and third difference. They were edited by Pitiscus.

1.5.2 Jean Henri Lambert (1728-1777).

Lambert gives, in 1770 (I, 190-191), the values of the trigonometric function sine for arguments in units $\frac{\pi}{60}$.

These require $s3 = \sqrt{3}$, $s2 = \frac{\sqrt{2}}{2}$, $s5 = \sqrt{5}$, $s5p = \sqrt{5 + s5}$, $s5m = \sqrt{5 - s5}$.

His table can then be rewritten as follows: $\sin(1) = \frac{-s3 s5p + s5p + s2 s3 s5 + s2 s5 - s2 s3 - s2}{8}$,

$$\sin(2) = \frac{2s2 s3 s5m - s5 - 1}{8},$$

$$\sin(3) = \frac{s5 s2 + s2 - s5m}{4},$$

$$\sin(4) = \frac{2s2 s5p - s3 s5 + s3}{8},$$

$$\sin(5) = \frac{s3 s2 - s2}{2},$$

$$\sin(6) = \frac{s5 - 1}{4},$$

$$\sin(7) = \frac{s3 s5m + s5m - s2 s3 s5 + s2 s5 - s2 s3 + s2}{8},$$

$$\sin(8) = \frac{-2s2 s5m + s3 s5 + s3}{8},$$

$$\sin(9) = \frac{-s5 s2 + s2 + s5p}{4},$$

$$\sin(10) = \frac{1}{2} \sin(11) = \frac{s3 s5p - s5p + s2 s3 s5 + s2 s5 - s2 s3 - s2}{8},$$

$$\sin(12) = \frac{1}{2} s2 s5m,$$

$$\sin(13) = \frac{-s3 s5m + s5m + s2 s3 s5 + s2 s5 + s2 s3 + s2}{8},$$

$$\sin(14) = \frac{2s2 s3 s5p - s5 + 1}{8},$$

$$\sin(15) = s2,$$

$$\sin(16) = \frac{2s2 s5p + s3 s5 - s3}{8},$$

$$\sin(17) = \frac{s3 s5m + s5m + s2 s3 s5 - s2 s5 + s2 s3 - s2}{8},$$

$$\sin(18) = \frac{s5 + 1}{4},$$

$$\sin(19) = \frac{s3 s5p + s5p - s2 s3 s5 + s2 s5 + s2 s3 - s2}{8},$$

$$\sin(20) = \frac{3s}{2},$$

$$\sin(21) = \frac{s5 s2 - s2 + s5p}{4},$$

$$\sin(22) = \frac{2s2 s3 s5m + s5 + 1}{8},$$

$$\sin(23) = \frac{s3 s5m - s5m + s2 s3 s5 + s2 s5 + s2 s3 + s2}{8},$$

$$\sin(24) = \frac{1}{2} s2 s5p,$$

$$\sin(25) = \frac{s3 s2 + s2}{2},$$

$$\sin(26) = \frac{2s2 s3 s5p + s5 - 1}{8},$$

$$\sin(27) = \frac{s5 s2 + s2 + s5m}{4},$$

$$\sin(28) = \frac{2s2 s5m + s3 s5 + s3}{8},$$

$$\sin(29) = \frac{s3 s5p + s5p + s2 s3 s5 - s2 s5 - s2 s3 + s2}{8},$$

$$\sin(30) = 1.$$

These tables are given here, because they can be used in the case of finite fields for appropriate values of p .

1.5.3 Menelaus of Alexandria (about 100 A. D.)

The first appearance of a spherical triangle is in book I of Menelaus' treatise *Sphaerica*, known through its translation into Arabic. In it appears the first time a study of spherical

triangles and of the formula for a spherical triangle ABC with points L, M, N on the sides corresponding to IV...?

$$\sin(AN)\sin(BL)\sin(CM) = -\sin(NB)\sin(LC)\sin(MA).$$

1.5.4 al-Battani, or Albategnius (850?-929?).

The law of cosine for a spherical triangle was given by al-Battani, it will be generalized to finite non-Euclidean geometry in IV...2.0.

The formula, for a spherical right triangle, called Geber's Theorem, will be generalized in IV ...1.1.

Introduction.

This section uses extensively, material learned from Professor George Lemaître, in his class on Analytical Mechanics, given to first year students in Engineering and in Mathematics and Physics, University of Louvain, Belgium, 1942. We first determine the differential equation for the pendulum 6.1.3. using the Theorem of Toricelli 6.1.1. , we then define the elliptic integral of the first kind and the elliptic functions of Jacobi 6.1.5., we then derive the Landen transformation which relates elliptic functions with different parameters 6.1.10., use it to obtain the Theorem of Gauss which determines the complete elliptic integrals of the first kind from the arithmetico-geometric mean of its 2 parameters 6.1.14. and obtain the addition formulas for the these functions 6.1.16. using the Theorem of Jacobi on pendular motions which differ by their initial condition 6.1.7. We also derive the Theorem of Poncelet on the existence of infinitely many polynomials inscribed in one conic and circumscribed to another 6.1.9. We state, without proof, the results on the imaginary period of the elliptic functions of Jacobi 6.1.19. and 6.1.20. A Theorem of Lagrange is then given which relates identities for spherical trigonometry and those for elliptic function 6.1.23. Finally we state the definitions and some results on the theta functions. Using this approach, the algebra is considerably simplified by using geometrical and mechanical considerations.

Theorem. [Toricelli]

If a mass moves in a uniform gravitational field its velocity v is related to its height h by

$$0. \quad v = \sqrt{2g(h_0 - h)},$$

where g is the gravitational constant and h_0 is a constant, corresponding to the height at which the velocity would be 0.

Proof: The laws of Newtonian mechanics laws imply the conservation of energy. In this case the total energy is the sum of the kinetic energy $\frac{1}{2}mv^2$ and the potential energy mgh , therefore

$$\frac{1}{2}mv^2 + mgh = mgh_0, \text{ for some } h_0.$$

Definition.

A *circulatory pendular motion* is the motion of a mass m restricted to stay on a vertical frictionless circular track, whose total energy allows the mass to reach with positive velocity

the highest point on the circle. An *oscillatory pendular motion* is one for which the total energy is such that the highest point on the circle is not reached. The mass in this case oscillates back and forth. The following Theorem gives the equation satisfied by a pendular motion.

Theorem.

If a mass m moves on a vertical circle of radius R , with lowest point A , highest point B and center O , its position M at time t , can be defined by $2\phi(t) = \angle(AOM)$ which satisfies

$$0. D\phi = \sqrt{a^2 - c^2 \sin^2 \phi}, \text{ where}$$

$$1. a^2 := 2gh_0 \frac{1}{4R^2}, c^2 = \frac{g}{R}, \text{ for some } h_0.$$

Proof: If the height is measured from A ,

$$h(t) = R - R \cos(2\phi(t)) = 2R \sin^2 \phi(t),$$

the Theorem of Toricelli gives

$$RD(2\phi)(t) = v(t) = \sqrt{2gh_0 - 4gR \sin^2 \phi(t)},$$

hence 0. The motion is circulatory if $h_0 > 2R$ or $a > c$, it is oscillatory if $0 < h_0, 2R$ or $c > a$.

Notation.

$$0. k := \frac{c}{a}, b^2 := a^2 - c^2, k' := \frac{b}{a},$$

Definition.

If $a = 1$, and we express t in terms of $\phi(t)$,

0. $t = \int_0^{\phi(t)} \frac{1}{\sqrt{1-k^2 \sin^2 \phi}} d\phi$. The integral 0. is called the *incomplete elliptic integral of the first kind*. Its inverse function ϕ is usually noted

1. $am(t)$, the *amplitude function*,

The functions

2. $sn := \sin \circ am$, $cn := \cos \circ am$, $dn := \sqrt{1 - k^2 sn^2}$,
are called the *elliptic functions of Jacobi*.

3. $K := \int_0^{\frac{1}{2}\pi} \frac{1}{\sqrt{1-k^2 \sin^2 \phi}} d\phi$. is called the *complete integral of the first kind*, it gives half the period, $\frac{K}{a}$, for the circular pendulum. The functions which generalize \tan , \csc , \dots are

$$4. ns := \frac{1}{sn}, nc := \frac{1}{cn}, nd := \frac{1}{dn},$$

$$5. sc := \frac{sn}{cn}, cd := \frac{cn}{dn}, ds := \frac{dn}{sn},$$

$$6. cs := \frac{cn}{dn}, dc := \frac{dn}{cn}, sd := \frac{sn}{dn}.$$

Theorem.*If*

0. $s_1 := sn(t_1)$, $c_1 = cn(t_1)$, $d_1 = dn(t_1)$ and
1. $s_2 := sn(t_2)$, $c_2 = cn(t_2)$, $d_2 = dn(t_2)$,
we have
2. $sn^2 + cn^2 = 1$, $dn^2 + k^2 sn^2 = 1$, $dn^2 - k^2 cn^2 = k'^2$.
3. $1 - k^2 s_1^2 s_2^2 = c_1^2 + s_1^2 d_2^2 = c_2^2 + s_2^2 d_1^2$.

Theorem. [Jacobi]

Let $M(t)$ describes a pendular motion, Given the circle γ which has the line r at height h_0 as radical axis and is tangent to $AM(t_0)$, if $N(t)M(t)$ remains tangent to that circle, then $N(t)$ also describes a pendular motion, with $N(t_0) = A$.

Proof: With the abbreviation $M = M(t)$, $N = N(t)$, let NM meets r at D , let M' , N' be the projections of M and N on r , let T be the point of tangency of MN with γ ,

0. $DM DN = DT^2$,
therefore

$$1. \frac{DT}{ND} = \frac{DM}{DT} = \frac{DT-DM}{ND-DT} = \frac{MT}{NT} = \sqrt{\frac{DT}{ND} \frac{DM}{DT}} = \sqrt{\frac{DM}{ND}} = \sqrt{\frac{M'M}{N'N}}$$

When t is replaced by $t + \epsilon$,

$$2. \frac{v_M}{v_N} = \lim_{t \rightarrow t+\epsilon} \frac{M(t+\epsilon)-M(t)}{N(t+\epsilon)-N(t)} = \lim_{t \rightarrow t+\epsilon} \frac{M(t)T}{N(t+\epsilon)T} = \frac{MT}{NT},$$

because the triangles $T, M, M(t+\epsilon)$ and $T, N, N(t+\epsilon)$ are similar, because $\angle(T, N, N(t+\epsilon)) = \angle(T, M(t+\epsilon), M)$ as well as $\angle(M(t+\epsilon), T, M) = \angle(N(t+\epsilon), T, N)$.

Therefore

$$3. \frac{v_M}{v_N} = \sqrt{\frac{M'M}{N'N}}.$$

The Theorem of Toricelli asserts that $v_M = \sqrt{2gM'M}$, this implies, as we have just seen, $v_N = \sqrt{2gN'N}$, therefore N describes the same pendular motion with a difference in the origin of the independent variable.

Corollary.

If $M = B$ and $N = A$, the line $M(t) \times N(t)$ passes through a fixed point L on the vertical through O called point of Landen.

Moreover, if $b := BL$ and $a := LA$, we have

$$\frac{v_M}{v_N} = \frac{b}{a} \text{ and } h_0 = \frac{a^2}{a-b}.$$

This follows at once from from 6.1.7.2. and 6.1.7.1.

Theorem. [Poncelet]

Given 2 conics θ and γ , if a polygon P_i , $i = 0$ to n , $P_n = P_0$, is such that P_i is on θ and $P_i \times P_{i+1}$ is tangent to γ , then there exists infinitely many such polygons.

Any such polygon is obtained by choosing Q_0 on θ drawing a tangent Q_0Q_1 to γ , with Q_1 on θ and successively Q_i , such that Q_i is on θ and $Q_{i-1} \times Q_i$ is tangent to γ , the Theorem asserts that $Q_n = Q_0$.

The proof follows at once from 6.1.7. after using projections which transform the circle θ and the circle γ into the given conics. The Theorem is satisfied if the circle have 2 points in common or not.

Theorem.

If $M(t)$ describes a circular pendular motion, then the mid-point $M_1(t)$ of $M(t)$ and $M(t+K)$ describes also a circular pendular motion. More precisely, $M_1(t)$ is on a circle with diameter LO , with $LA = a$, $LB = b$, and if $\phi_1(t) = \angle(O, L, M_1(t))$,

$$0. \quad t = \int_0^{\phi(t)} \frac{D\phi}{\Delta} = \frac{1}{2} \int_0^{\phi_1(t)} \frac{D\phi_1}{\Delta_1}.$$

where

$$1. \quad \Delta^2 := a^2 \cos^2 \phi + b^2 \sin^2 \phi \text{ and } \Delta_1^2 := a_1^2 \cos^2 \phi_1 + b_1^2 \sin^2 \phi_1,$$

where the relation between ϕ and ϕ_1 is given by

$$2. \quad \tan(\phi_1 - \phi) = k' \tan \phi, \text{ or}$$

$$3. \quad \sin(2\phi - \phi_1) = k_1 \sin \phi_1,$$

with

$$4. \quad a_1 := \frac{1}{2}(a + b), \quad b_1 := \sqrt{ab}, \quad c_1 := \frac{1}{2}(a - b), \text{ therefore}$$

$$5. \quad a = a_1 + c_1, \quad b = a_1 - c_1, \quad c = 2\sqrt{a_1 c_1}.$$

Proof: First, it follows from the Theorem of Toricelli that the velocity v_A at A and v_B at B satisfy

$$v_A = \sqrt{2gh_0} = 2Ra, \quad v_B = \sqrt{2gh_0 - 2R} = \sqrt{4R^2a^2 - 4c^2R^2} = 2Rb,$$

therefore $\frac{BL}{LA} = \frac{b}{a}$.

If P is the projection of L on BM and Q the projection of L on AM ,

$$LM^2 = LP^2 + LQ^2 = a^2 \cos^2 \phi + b^2 \sin^2 \phi = \Delta^2.$$

$$LQ = LM \cos(\phi_1 - \phi) = a \cos \phi.$$

We can proceed algebraically. Differentiating 2. gives

$$\begin{aligned} a(1 + \tan^2(\phi_1 - \phi))(D\phi_1 - D\phi) &= b(1 + \tan^2 \phi)D\phi, \text{ or } a(1 + \tan^2(\phi_1 - \phi))D\phi_1 = (a(1 + \tan^2(\phi_1 - \phi) + b(1 + \tan^2 \phi))D\phi \\ &= (a + b + \frac{b^2}{a} \tan^2 \phi + b \tan^2 \phi)D\phi \\ &= (a + b)(1 + \frac{b}{a} \tan^2 \phi)D\phi \\ &= (a + b)(1 + \tan \phi \tan(\phi_1 - \phi))D\phi, \end{aligned}$$

or

$$\frac{a}{\cos^2(\phi_1 - \phi)} D\phi_1 = 2a_1 \frac{\cos(2\phi - \phi_1)}{\cos \phi \cos(\phi_1 - \phi)} D\phi, \text{ or}$$

$$\frac{\frac{D\phi}{\frac{a \cos \phi}{\cos(\phi_1 - \phi)}}}{\Delta} = \frac{\frac{D\phi_1}{2a_1 \cos(2\phi - \phi_1)}}{2\Delta_1},$$

or because $LM = \Delta$

$$\frac{D\phi}{\Delta} = \frac{D\phi_1}{2\Delta_1}.$$

We can also proceed using kinematics.

The velocity at M is

$$v_M = 2RD\phi = 2R\Delta,$$

If we project the velocity vector on a perpendicular to LM ,

$$LMD\phi_1 = v_M \cos(2\phi_1 - \phi) = 2R \cos(2\phi_1 - \phi) \Delta \phi.$$

Therefore

$$\frac{D\phi}{\Delta} = \frac{D\phi_1}{2R \cos(2\phi_1 - \phi)} = \frac{a_1}{2R} \frac{D\phi_1}{\Delta_1} = \frac{D\phi_1}{2\Delta_1}.$$

Definition.

The transformation from ϕ to ϕ_1 is called the *forward Landen transformation*. The transformation from ϕ_1 to ϕ is called the *backward Landen transformation*.

Comment.

The formulas 3. and 1. are the formulas which are used to compute t from $\phi(t)$. The formulas 4. and 2. are used to compute $\phi(t)$ from t .

Theorem. [Gauss]

Given $a_0 > b_0 > 0$, let

$$0. \ a_{i+1} := \frac{1}{2}(a_i + b_i),$$

$$1. \ b_{i+1} := \sqrt{a_i b_i},$$

then the sequence a_i and b_i have a common limit a_∞ . The sequence a_i is monotonically decreasing and the sequence b_i is monotonically increasing.

Proof: Because

$$a_i > a_{i+1}, \ b_{i+1} > b_i,$$

it follows that the sequence a_i is bounded below by b_0 , the sequence b_i is bounded above by a_0 , therefore both have a limit a_∞ and b_∞ . Taking the limit of 0. gives at once $a_\infty = b_\infty$.

Theorem.

For the complete integrals we have

$$0. \ \frac{K}{a} = \int_0^{\frac{1}{2}\pi} \frac{1}{\sqrt{a^2 \cos^2 + b^2 \sin^2}} = \frac{\frac{\pi}{2}}{a_\infty}.$$

Proof: If $\phi(K) = \frac{\pi}{2}$, then $\phi_1(K) = \pi$, therefore

$$1. \ K = \int_0^{\frac{\pi}{2}} \frac{D\phi}{\Delta} = \int_0^\pi \frac{D\phi_1}{2\Delta_1} = \frac{1}{2} \int_0^{\frac{\pi}{2}} \frac{D\phi_1}{\Delta_1} + \frac{1}{2} \int_{\frac{\pi}{2}}^\pi \frac{D\phi_1}{\Delta_1} = \int_0^\pi \frac{D\phi_1}{\Delta_1} = \int_0^{\frac{\pi}{2}} \frac{D\phi_n}{\Delta_n} = \int_0^{\frac{\pi}{2}} \frac{1}{a_\infty} = \frac{\frac{\pi}{2}}{a_\infty}.$$

Lemma.

0. $c_2 = c_1 cn(t_1 + t_2) + d_2 s_1 sn(t_1 + t_2),$
1. $d_2 = d_1 dn(t_1 + t_2) + k^2 s_1 c_1 sn(t_1 + t_2).$

Proof: We use the Theorem 6.1.7. of Jacobi. Let R be the radius of θ and O its center, let r be the radius of γ and O' its center, let $s := OO'$. Let A, N, M', M be the position of the mass at time 0, $t_1, t_2, t_1 + t_2$.

The lines $A \times M'$ and $N \times M$ are tangent to the same circle γ at T' and T .

Let X be the intersection of $O \times M$ and $O' \times T$, $2\phi := \angle(A, O, N)$,

2. $2\phi' := \angle(A, O, M),$
we have $\angle(N, O, M) = 2(\phi' - \phi), \angle(M, X, T) = \phi' - \phi, \angle(T, O', O) = \phi' + \phi.$
If we project MOO' on $O'T$,
$$r = R \cos(\phi' - \phi) s \cos(\phi' + \phi), \text{ or}$$

3. $r = (R + s) \cos \phi \cos \phi' + (R - s) \sin \phi \sin \phi'.$
 $\phi = amt_1, \phi' = am(t_1 + t_2),$
 $\sin \phi' = sn(t_1 + t_2), \cos \phi' = cn(t_1 + t_2),$
 $\sin \phi = sn t_1 = s_1,$
 $\cos \phi = cn t_1 = c_1,$

when $t_1 = 0$,

$$\cos(\angle(A, B, M')) = cn t_2 = c_2 = \frac{BM'}{AB} = \frac{O'T'}{AO'} = \frac{r}{R+s},$$

the ratio of the velocities is

$$\frac{v_{M'}}{v_A} = \frac{dn t_2}{dn 0} = d_2 = \frac{TM'}{AT} = \frac{O'B}{AO'} = \frac{R-s}{R+s}, \text{ substituting in 2. gives 0.}$$

The proof of 1. is left as an exercise.

Theorem. [Jacobi]

0. $\frac{sn u_1 cn u_2 dn u_2 + sn u_2 cn u_1 dn u_1}{sn(u_1 + u_2)} = 1 - k^2 sn^2 u_1 sn^2 u_2.$
1. $\frac{cn u_1 cn u_2 - sn u_1 dn u_1 sn u_2 dn u_2}{cn(u_1 + u_2)} = 1 - k^2 sn^2 u_1 sn^2 u_2.$
2. $\frac{dn u_1 dn u_2 - k^2 sn u_1 sn u_2 cn u_1 cn u_2}{dn(u_1 + u_2)} = 1 - k^2 sn^2 u_1 sn^2 u_2.$

Proof: Let $w = \frac{1}{1 - k^2 s_1^2 s_2^2}.$

Let s_1, s_2, \dots denote $sn u_1, sn u_2, \dots$, define S and C such that

$$sn(u_1 + u_2) = Sw, cn(u_1 + u_2) = Cw.$$

The 6.1.15.0. gives

$$c_2 = c_1 Cw + d_2 s_1 Sw \text{ or}$$

3. $c_1 Cw = -d_2 s_1 Sw + c_2,$

6.1.6.2. gives

$$S^2 w^2 + C^2 w^2 = 1,$$

eliminating C gives the second degree equation in Sw :

$$(c_1^2 + d_2^2 s_1^2 (Sw)^2 - 2s_1 c_2 d_2 (Sw) + c_2^2 - c_1^2 = 0,$$

one quarter of the discriminant is

$$\begin{aligned} & s_1^2 c_2^2 d_2^2 - (c_2^2 - c_1^2)(c_1^2 + d_2^2 s_1^2) \\ &= s_1^2 c_2^2 d_2^2 - c_1^2 c_2^2 + c_1^4 - s_1^2 c_2^2 d_2^2 + s_1^2 c_1^2 d_2^2 \\ &= c_1^2 (c_1^2 - c_2^2 + s_1^2 d_2^2) = c_1^2 s_2^2 d_1^2, \end{aligned}$$

therefore

$$Sw = (s_1 c_2 d_2 \pm c_1 d_1 s_2)w.$$

One sign correspond to one tangent from M to γ , the other to the other tangent, therefore one corresponds to the addition, the other to the subtraction formula. From the special case $k = 0$, follows that, by continuity, the $+$ sign should be used. This gives 0., 1. follows from 3, 2. is left as an exercise.

Corollary.

- 0. $sn(u + K) = cd(u)$, $cn(u + K) = -k' sd(u)$, $dn(u + K) = k' nd(u)$.
- 1. $sn(u + 2K) = -sn(u)$, $cn(u + 2K) = -cn(u)$, $dn(u + 2K) = dn(u)$.
- 2. $sn(u + 4K) = sn(u)$, $cn(u + 4K) = cn(u)$, $dn(u + 4K) = dn(u)$.

Definition.

$$K'(k^2) = K(k'^2).$$

Theorem.

- 0. $ksn \circ I + iK' = sn$,
- 1. $ikcn \circ I + iK' = ds$,
- 2. $idn \circ I + iK' = cs$,
- 1. $sn \circ I + 2iK' = sn$,
- 1. $cn \circ I + 2iK' = -cn$,
- 2. $dn \circ I + 2iK' = -dn$,

Theorem.

- 0. sn has periods $4K$ and $2iK'$ and pole $\pm iK'$,
- 1. cn has periods $4K$ and $4iK'$ and pole $\pm iK'$,
- 2. dn has periods $2K$ and $4iK'$ and pole $\pm iK'$.

Theorem.

- 0. $k = 0 \Rightarrow sn = \sin$, $cn = \cos$, $dn = \underline{1}$,
- 1. $k = 1 \Rightarrow sn = \tanh$, $cn = \operatorname{sech}$, $dn = \operatorname{sech}$.

Theorem. [Lagrange]

From the addition formulas of elliptic functions we can derive those for a spherical triangle as follows. Let

$$0. \ u_1 + u_2 + u_3 = 2K, \\ \text{define}$$

$$1. \ \begin{aligned} \sin a &:= -snu_1, \cos a := -cnu_1, \\ \sin b &:= -snu_2, \cos b := -cnu_2, \\ \sin c &:= -snu_3, \cos c := -cnu_3, \\ \sin A &:= -ksnu_1, \cos A := -dnu_1, \\ \sin B &:= -ksnu_2, \cos B := -dnu_2, \\ \sin C &:= -ksnu_3, \cos C := -dnu_3, \end{aligned}$$

then to any formula for elliptic functions of u_1, u_2, u_3 , corresponds a formula for a spherical triangle with angles A, B, C and sides a, b, c . For instance,

$$2. \ \frac{\sin A}{\sin a} = \frac{\sin B}{\sin b} = \frac{\sin C}{\sin c} = k.$$

$$3. \ \cos a = \cos b \cos c + \sin b \sin c \cos A,$$

$$4. \ \cos A = -\cos B \cos C + \sin B \sin C \cos a,$$

$$5. \ \sin B \cot A = \cos c \cos B + \sin c \cot a.$$

Proof. 2. follows from the definition. 3. follows from $c_2 = c_1 \operatorname{cn}(t_1 + t_2) + d_2 s_1 \operatorname{sn}(t_1 + t_2)$ after interchanging t_1 and t_2 and using

$$6. \ \begin{aligned} 0. \ \operatorname{sn}(t_1 + t_2) &= \operatorname{sn}(2K - t_1 - t_2) = \operatorname{sn} t_3 = s_3, \\ 1. \ \operatorname{cn}(t_1 + t_2) &= -\operatorname{cn}(2K - t_1 - t_2) = -\operatorname{cn} t_3 = -c_3, \\ 2. \ \operatorname{dn}(t_1 + t_2) &= \operatorname{dn}(2K - t_1 - t_2) = \operatorname{dn} t_3 = d_3, \end{aligned}$$

similarly, 4. follows from

$$c_2 = c_1 \operatorname{cn}(t_1 + t_2) + d_2 s_1 \operatorname{sn}(t_1 + t_2)$$

after interchanging t_1 and t_2 and using 6 and 5. from

$$\operatorname{sn} t_2 \operatorname{dn} t_1 = \operatorname{cn} t_1 \operatorname{sn}(t_1 + t_2) - \operatorname{sn} t_1 \operatorname{dn} t_2 \operatorname{cn}(t_1 + t_2)$$

after division by $\operatorname{sn} t_1$.

Definition.

Given the parameter q , called the nome,

$$0. \ q := e^{-\pi \frac{K'}{K}}, \\ \text{the functions}$$

$$1. \ \theta_1 := 2q^{\frac{1}{4}} \sum_{n=0}^{\infty} (-1)^n q^{n(n+1)} \sin(2n+1)I$$

$$2. \ \theta_2 := 2q^{\frac{1}{4}} \sum_{n=0}^{\infty} q^{n(n+1)} \cos(2n+1)I$$

$$3. \ \theta_3 := 1 + 2 \sum_{n=1}^{\infty} q^{n^2} \cos 2nI$$

$$4. \ \theta_4 := 1 + 2 \sum_{n=1}^{\infty} (-1)^n q^{n^2} \cos 2nI \text{ are the theta functions of Jacobi.}$$

Definition.

The functions, with $v = \pi \frac{I}{2K}$

$$0. \theta_s := \frac{2K\theta_{1\circ v}}{D\theta_1(0)}, \theta_c := \frac{\theta_{2\circ v}}{\theta_2(0)}, \theta_d := \frac{\theta_{3\circ v}}{\theta_3(0)}, \theta_n := \frac{\theta_{4\circ v}}{\theta_4(0)},$$

are called the *theta functions of Neville*.

Theorem.

If p, q denote any of s, c, d, n ,

$$pq = \frac{\theta_p}{\theta_q}. \text{ For instance}$$

$$sn = \frac{\theta_s}{\theta_n} = \frac{2K\theta_{1\circ v}}{D\theta_1(0)} \cdot \frac{\theta_4(0)}{\theta_{4\circ v}}.$$

Theorem.

The Landen transformation replaces the parameter q , by q^2 .

References.

Jacobi, Fundamenta Nova Theoriae Functionum Ellipticarum, 1829.

Legendre, Traité des fonctions elliptiques et des intégrales elliptiques. III, 1828.

Gauss, Ostwald Klasiker?

Landen John, Phil. Trans. 1771, 308.

Abel, Oeuvres, 591.

Bartky, Numerical Calculation of generalized complete integrals, Rev. of Modern Physics, 1938, Vol. 10, 264-

Lemaitre G. Calcul des integrales elliptiques, Bull. Ac. Roy. Belge, Classe des Sciences, Vol. 33, 1947, 200-211.

Fettis, Math. of Comp., 1965.

Appell, Cours de Mechanique,

Notes

$$(Dy)^2 = C_0(y^2 - A_0)(y^2 + B_0),$$

$$(Dz)^2 = C_1(z^2 - A_1)(z^2 + B_1),$$

$$z = d(y + \frac{1}{y}), l \neq 0, d > 0.$$

The equations are compatible iff (l in the beginning of next expres.?)

$$d^2(1 - \frac{2}{y^2})C_0(y^2 + A_0)(y^2 + B_0) = C_1(d^2(\frac{y^2+l}{y})^2 + A_1)(d^2(\frac{y^2+l}{y})^2 + B_1)$$

this requires \sqrt{l} to be a root of one of the factore of the second member, let it be the second factor, this implies

$$d^2 4l + B_1 = 0,$$

then, the second factor becomes,

$$d^2(\frac{y^2+l}{y})^2 + B_1 = d^2((\frac{y^2+l}{y})^2 - 4K) = d^2(\frac{y^2-l}{y})^2$$

therefore \sqrt{l} is a double root of the second memeber and

$$C_0(y^4 + (A_0 + B_0)y^2 + A_0B_0) = d^2C_1(y^4 + (2l + A_1)y^2 + l^2), \text{ therefore}$$

$C_0 = d^2 C_1$, $A_0 B_0 = \frac{B_1^2}{16d^4}$, $A_0 + B_0 = \frac{A_1 - \frac{1}{2}B_1}{d^2}$,
 For real transformations, $A_0 B_0 > 0$, if $j_0 = \text{sign}(B_0)$ and $j_1 = \text{sgn}(B_1)$,
 $B_1 = 4j_0 d^2 \sqrt{A_0 B_0}$, $A_1 = d^2(A_0 + B_0 + 2j_1 \sqrt{A_0 B_0})$
 $= j_0(\sqrt{|A_0|} + j_0 j_1 \sqrt{|B_0|})^2$.
 If we want $A_1 B_1 \neq 0$ then $j_0 = j_1$.

1.6 Algebra, Modular Arithmetic.

1.6.0 Introduction.

Geometry can be handled synthetically, with little or no reference to algebra. But it was discovered little by little that an underlying algebraic structure lurks behind geometry. If we deal with a geometry with a finite number of points on each line, we have to deal with an underlying algebraic structure which involves a finite number of integers. Such structure presented itself in connection with application of mathematics to astronomy (and astrology), in studying the relative motion of sun and moon and the relative motion of the planets, mainly Jupiter. If the smallest unit of time used is t , the period of the sun around the earth, is $s.t$, the position of the sun is the same after 2 revolutions hence $2s$ is equivalent to s and $2s + 1$ is equivalent to $s + 1$ as well as 1. This led to the notion of working modulo s .

1.6.1 The integers.

Definition.

p is a *prime* iff p is an integer larger than 1, which is only divisible by 1 and p .

Restriction.

In the sequel, it is always assumed that p is odd.

1.6.2 The integers modulo p .

Introduction.

Although much of what I will do can be generalized, to the case of powers of primes, I will, for simplicity, restrict myself to the case of a prime p .

Definition.

The *integers modulo p* are the integers x satisfying

$$0 \leq x < p.$$

The set of these integers is denoted Z_p . The operations modulo p are defined in terms of the operations on the integers as follows:

¹G16.TEX [MPAP], September 9, 2019

Definition.

0. If x and y are integers modulo p , *addition modulo p* , denoted $+_p$ is defined as the least non negative remainder of the division of the integer $x + y$ by p .
1. *Multiplication modulo p* , denoted \cdot_p , is defined as the least non negative remainder of the division of $x \cdot y$ by p .
2. *Subtraction modulo p* , denoted $-_p$, is defined as the inverse operation of addition, $c +_p b = a \implies a -_p b = c$.
3. *Division modulo p* , denoted $/_p$, is defined as the inverse operation of addition, $c \cdot_p b = a \implies a /_p b = c$, provided $b \neq 0$.

Convention.

As I will not use simultaneously 2 different primes, and as it will usually be clear from the context that the addition, multiplication, \dots , are done modulo p , I will replace $+_p$ by $+$, \dots . An alternate notation, useful when several different moduli are used, is to use

$$a + b \equiv c \pmod{p}.$$

Example.

We have, $0 +_5 3 = 3$, $5 +_7 4 = 2$, $5 +_{11} 6 = 0$.

Modulo 7: $5 + 4 = 2$, $5 - 4 = 1$, $5 \cdot 4 = 6$, $5/4 = 3$, $5 + 0 = 5$.

Modulo 7: the inverses of 1 through 6 are respectively 1, 4, 5, 2, 3, 6. Modulo 11: $9 + 5 = 3$, $9 - 5 = 4$, $9 \cdot 5 = 1$, $9/5 = 4$, $9 \cdot 0 = 0$.

Comment.

Addition, subtraction and multiplication are easy to perform, moreover hand calculators and languages for microprocessors have functions which allow easy computations. Division requires either a table of inverses or the inverses can be obtained, for large primes p , using the Euclid-Aryabatha algorithm.^{10 11}

Algorithm. [Euclid]

Let $a \geq b > 0$. We determine in succession

$$a_0 := a, a_1 := b, q_1, a_2, q_2, \dots, a_n = 0 \ni$$

$$0. \quad a_{j-1} := a_j q_j + a_{j+1}, 0 \leq a_{j+1} < a_j.$$

¹⁰To appreciate this contribution of the Hindus, Aryabatha lived at the end of the fifth Century, while an equivalent algorithm was only developed in the Western World by Bachet de Meziriac in 1624.

¹¹Pulverizing a is meant to convey what we would now express by finding the inverse of a modulo n .

Algorithm. (Pulverizer of Aryabatha)

Given q_1, q_2, \dots, q_{n-1} , determine

- $$b_{n-1} := 0, b_{n-2} := 1,$$
- $$0. \quad b_{j-1} := b_j q_j + b_{j+1}, \text{ for } j = n-2, \dots, 1.$$

Algorithm. (Continued fraction algorithm)

Given q_1, q_2, \dots, q_{n-1} , determine

- $$c_0 := 0, c_1 := 1, d_0 := 1, d_1 := 0,$$
- $$0. \quad c_{j+1} := c_j q_j + c_{j-1}, \text{ for } j = 1, \dots, n-1.$$
- $$1. \quad d_{j+1} := d_j q_j + d_{j-1}, \text{ for } j = 1, \dots, n-1.$$

Algorithm.

$$u_j := c_j^2 + d_j^2.$$

$$v_j := c_j c_{j+1} + d_j d_{j+1}.$$

Example.

Let $a = 10672$ and $b = 4147$, 1.6.2, 1.6.2, 1.6.2 and 1.6.2 give

$a_0 =$	10672	$=$	4147.2	$+$	2378	$\uparrow b_0 =$	175	$\downarrow c_0 =$	0	$d_0 =$	1
$a_1 =$	4147	$=$	2378.1	$+$	1769	$b_1 =$	68	$c_1 =$	1	$d_1 =$	0
$a_2 =$	2378	$=$	1769.1	$+$	609	$b_2 =$	39	$c_2 =$	2	$d_2 =$	1
$a_3 =$	1769	$=$	609.2	$+$	551	$b_3 =$	29	$c_3 =$	3	$d_3 =$	1
$a_4 =$	609	$=$	551.1	$+$	58	$b_4 =$	10	$c_4 =$	5	$d_4 =$	2
$a_5 =$	551	$=$	58.9	$+$	29	$b_5 =$	9	$c_5 =$	13	$d_5 =$	5
$a_6 =$	58	$=$	29.2	$+$	0	$b_6 =$	1	$c_6 =$	18	$d_6 =$	7
$a_7 =$	29	$=$				$\uparrow b_7 =$	0	$c_7 =$	175	$d_7 =$	68
								$\downarrow c_8 =$	368	$d_8 =$	143

$n = 8, 4147 \cdot 175 - 10673 \cdot 68 = 29.$

$u_7 = 35249, u_8 = 155873, v_7 = 74124.$

The bold-faced number are initial values, the italicized numbers are final values. Notice that all a 's have to be computed before the b 's are computed, but this is not so for the c 's and the d 's.

For instance, for the line starting with a_3 , 1769 and 609 come from the preceding line, 2 is the quotient of the division of 1769 by 609 and 551 is the remainder,

$$b_4 = q_5 \cdot b_5 + b_6 = 1.9 + 1 = 10.$$

$$c_4 = c_3 \cdot q_3 + c_2 = 3.1 + 2 = 5, d_4 = d_3 \cdot q_3 + d_2 = 1.1 + 1 = 2.$$

Observe that 175 and 68 are obtained in 2 different ways.

Definition.

The *greatest common divisor* of a and b is the largest positive integer which divides a and b , it is denoted (a, b) .

Theorem.

0. The algorithm 1.6.2 terminates in a finite number of steps.

1. $(a, b) = (a_0, a_1) = (a_1, a_2) = \dots = (a_{n-1}, a_n) = a_{n-1}$.
2. $b_j a_{j-1} - b_{j-1} a_j = (-1)^{n-j}(a, b)$, in particular, $b_0 b - b_1 a = (-1)^n(a, b)$.
3. $b_j < a_j$. in particular, $b_1 < b$, $b_0 < a$.

Theorem.

0. $a_0/a_1 = q_1 + 1/(q_2 + 1/(q_3 + \dots + 1/q_{n-1}))$.
 1. $b < \frac{a}{2} \implies c_i < c_{i+1}$, $i = 0, \dots, n-1$.
 2. $a_i c_{i+1} + a_{i+1} c_i = a$, $a_i d_{i+1} + a_{i+1} d_i = b$.
 3. $b.c_i \equiv (-1)^{i+1} a_i \pmod{a}$, $a.d_i \equiv (-1)^i a_i \pmod{b}$.
- If $\frac{a}{2} \leq b < a$ then $q_1 = 1$ and $c_2 = c_1$.

Definition.

The second member in 1.6.2.0. is called a *terminating continued fraction*.

Theorem. [Symmetry property]

If $(a, b) = 1$, $b < \frac{a}{2}$, and we repeat the algorithm with $a' := a$ and $b' := \pm b^{-1} \pmod{a}$, $b' \leq \frac{a}{2}$, then this algorithm terminates in the same number n of steps and

$a'_j = c_{n-j}$, $c'_j = a_{n-j}$, $q'_j = q_{n-j}$.
In particular, if $b^2 \equiv -1 \pmod{a}$ and $b < a$, then $n = 2n' + 1$ is odd and
 $c_j = a_{n-j}$, $q_j = q_{n-j}$ and $a_{n'}^2 + a_{n'+1}^2 = a$.

Example.

i	a_i	q_i	c_i		i	a_i	q_i	c_i	
0	378		0	8	0	65		0	7
1	143	2	1	7	1	18	3	1	6
2	82	1	2	6	2	11	1	3	5
3	61	1	3	5	3	7	1	4	4
4	21	2	5	4	4	4	1	7	3
5	19	1	13	3	5	3	1	11	2
6	2	9	18	2	6	1	3	18	1
7	1	2	175	1	7	0		65	0
8	0		368	0					
$c'_j \quad q'_j \quad a'_j \quad j$					$c'_j \quad q'_j \quad a'_j \quad j$				

$18^2 + 1 \equiv 0 \pmod{65}$.
 $7^2 + 4^2 = 65$.

Theorem. [Euler]

Every integer whose prime factors to an odd power are congruent to 1 modulo 4, can be written as a sum of 2 squares and vice-versa.

Example.

$$13 = 2^2 + 3^2, 52 = 4^2 + 6^2.$$

$$585 = 9^2 + 24^2 = 12^2 + 21^2.$$

1.6.3 Quadratic Residues and Primitive Roots.

Definition.

n is a *quadratic residue* of p iff there exist an integer x such that x^2 is congruent to n modulo p . We write, with Gauss, $n \text{ R } p$. n is a *non residue* of p , if there are no integer whose square is congruent to n modulo p , and we write $n \text{ N } p$.

Theorem.

The product of 2 quadratic residues or of 2 non residues is a quadratic residue. The product of a quadratic residue by a non residue is a non residue.

Theorem. [Fermat]

If a is not divisible by p then $a^{p-1} \equiv 1 \pmod{p}$.

Definition.

g is a *primitive root* of p iff $a^i \equiv 1 \pmod{p}$ and $0 < i < p \implies i = p - 1$. In other words, $p - 1$ is the smallest positive power of g which is congruent to 1 modulo p .

Notation. [Euler]

$\phi(n)$ denotes the number of integers between 1 and p , relatively prime to p .

Theorem. [Gauss]

0. *There are $\phi(p - 1)$ primitive roots of p .*
1. *If g is a primitive root of p , all primitive roots are g^i with $(i, p - 1) = 1$.*

Example.

For $p = 13$, 2 is a primitive root,

i	0	1	2	3	4	5	6	7	8	9	10	11	12	$(\text{mod } 12)$
g^i	1	2	4	-5	3	6	-1	-2	-4	5	-3	-6	1	$(\text{mod } 13)$

The other primitive roots are $2^5 = 6$, $2^7 = -2$ and $2^{11} = -6$.

The easiest method to obtain all inverses modulo p is to first obtain a primitive root and then to use $g^i \cdot (g^{p-1-i})^{-1} = 1$.

Theorem.

If δ is a primitive root of p , the square root of an integer can be unambiguously defined if we chose a particular primitive root.

It is sufficient to choose a or $a\delta$, with $0 \leq a < \frac{p-1}{2}$.

Examples.

Modulo 5, δ^2 can be chosen equal to 2 or 3, with $\delta^2 = 3$, we have

i	0	1	2	3	4
\sqrt{i}	0	1	2δ	1δ	2.

Modulo 7, $\delta^2 = 3$ can be chosen equal to 3 or 5, with $\delta^2 = 5$, we have

i	0	1	2	3	4	5	6
\sqrt{i}	0	1	3	1δ	2	2δ	3δ

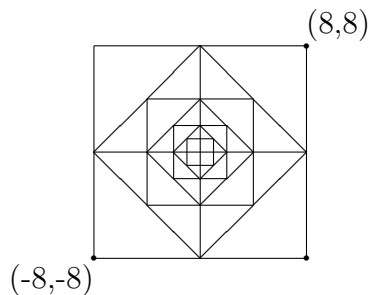
Theorem.

0. $p \equiv 1 \pmod{4} \Leftrightarrow -1Rp$ and p odd.
1. $p \equiv 1, -1 \pmod{8} \Leftrightarrow 2Rp$ and p odd.

Theorem.

$\sqrt{2}$ is rational in the field Z_{17} .

This follows at once from the following figure and the fact that the mid-point of the segment joining $(1,0)$ to $(0,1)$ is $(-8,-8)$ when $p = 17$. This figure originates with the geometric construction corresponding to the proof by the school of Pythagoras that there is no rational number whose square is 2. In fact, $\sqrt{2} = \pm 6$, when $p = 17$. In the case of real numbers, a corresponding figure corresponds to the geometric interpretation of the classical proof of the irrationality of $\sqrt{2}$, the squares becoming smaller and smaller. I suggest that the reader reflects on this, from a geometric point of view, together with the atomic structure of our Universe.



1.6.4 Non Linear Diophantine Equations and Geometry.

Introduction.

There has been, historically, a constant interplay between geometry and diophantine equations, the former suggesting problems of the latter kind which also indicate the interest of having problems in geometry solved using integers only. As evidence I will give just one such problem considered by Euler¹².

Definition.

The *median problem* consists in constructing a triangle with integer sides and medians.

Theorem.

If a_i are the length of the sides and g_i are twice the length of the medians, then

$$0. \ 2a_{i+1}^2 + 2a_{i-1}^2 = a_i^2 + g_i^2.$$

Proof:

$$a_0^2 + a_2^2 - 2a_0a_2\cos(A_1) = a_1^2,$$

$$\frac{1}{4}a_0^2 + a_2^2 - a_0a_2\cos(A_1) = \frac{1}{4}g_0^2,$$

eliminating the terms involving the angle gives

$$2a_1^2 + 2a_2^2 = a_0^2 + g_0^2.$$

Theorem. [Euler]

The solution of the preceding problem can be expressed in terms of 2 parameters a and b , using

$$C = (4ab)^2, \ D = (9a^2 + b^2)(a^2 + b^2), \ F = 2(3a^2 + b^2)(3a^2 - b^2),$$

$$a_0 = 2a(D - F), \ a_1 + a_2 = 2a(C + D), \ a_1 - a_2 = 2b(C - D),$$

$$g_0 = 2b(D + F), \ g_1 + g_2 = 6a(C - D), \ g_1 - g_2 = 2b(C + D),$$

Theorem. [Euler]

An other solution can be obtained corresponding to $a' = b$ and $b' = 3a$ for which

$$a'_i = g_i \text{ and } g'_i = 3a_i.$$

An example is provided with the pair (1,2) giving the pair (2,3) in the Example. In fact we have the following

Theorem.

If both a and b are not divisible by 3, then $3|g_i$ and 3 does not divide a_0 therefore the preceding Theorems gives a solution and for this solution b' is divisible by 3.

Indeed, $a^2 \equiv b^2 \equiv 1$, $C \equiv F \equiv 1$, $D \equiv -1$, $a_0 \equiv -a$, $-a_1 \equiv a_2 \equiv b$, $g_i \equiv 3$. It is therefore sufficient, if we use Theorem 1.6.4 to consider all pairs in which one of the integers in the pair is divisible by 3. Similarly we have the following Theorem.

¹²Opera Minora Collecta, II, (1778) 294-301, (1779) 362-365, (1782) 488-491

Theorem.

If a is not divisible by 3 and b is divisible by 9, then $9|a_i$, $27 \nmid a_i$, $27|g_i$ and the solution is the same as that obtained from $a' = b/3$ and $b' = a$.

Proof:

If $9|b$, then modulo 27, $C \equiv 0$, $D \equiv 9$ and $F \equiv 18$, therefore $9|a(0)$ but $27 \nmid a(0)$ while $27|g(i)$.

Example.

The solutions for the pairs $(a, b) = (1, 3), (1, 2), (2, 3), (1, 6), (3, 1), (3, 5)$ are given by Euler. Except for the pair $(1, 2)$, They are ordered by increasing maximum values of a_i .

a	1	1	2	1	5	3	*4	7	3	5	*3
b	3	2	3	6	3	1	3	3	5	6	2
a_0	3	158	68	314	145	477	184	1099	2547	2690	1926
a_1	1	127	85	159	207	277	739	810	2699	5277	3985
a_2	2	131	87	325	328	446	1077	1339	2704	5953	6101
g_0	1	204	158	404	529	569	1838	1921	4765	10924	10124
g_1	5	261	131	619	463	881	1357	2312	4507	7583	8123
g_2	4	255	127	377	142	640	5	1391	4498	5893	1399

a	3	11	3	8	*7	*3	10	*3
b	7	3	4	3	6	11	3	13
a_0	8163	12287	8874	18288	42	40563	59820	75123
a_1	5050	6416	13703	11663	15091	4232	32621	6953
a_2	5897	9897	14671	19105	20567	28531	51439	58580
g_0	7343	11281	26968	25838	36076	4301	61982	36283
g_1	13316	21370	20005	35537	24865	70006	106699	134543
g_2	12227	16921	17827	23999	5699	50125	81481	89174

The pair $(1, 2)$ corresponds to a degenerate triangle $(1+2=3)$.

The pairs marked with * are solutions only in a geometry with complex coordinates because $a_{i+1} + a_{i-1} < a_i$ for some i . The other degenerate solutions are obtained by observing that, in Euler's proof, other solutions are obtained when $b^2 = a^2$ or $9a^2$.

1.6.5 Farey sets and Partial Ordering.**Introduction.**

The basic idea is the following, a subset $T_1(n)$, $n > 0$, of the set Z_p can be placed into one to one correspondance with the set H_n of irreducible rationals whose numerator, in modulus, and denominator are not larger than n , provided $2n^2 - 2n + 1 < p$. The ordering \leq in $H_n \in Q$ induces an ordering in $T_1(n)$ such that $a \leq b$ and $b \leq c \implies a \leq c$ and $-b \leq -a$. If, moreover, $0 \leq a$ then $b^{-1} \leq a^{-1}$. If order is to be preserved, when we do one addition or one multiplication, we have to use $T_2(n) := T_1(n')$ instead of $T_1(n)$, with $n = 2n'^2$. This insures that the sum or product of 2 elements in $T_2(n)$ is in $T_1(n)$. T_1, T_2 are defined as the sets $T_1(n), T_2(n)$ corresponding to the largest n . This can be repeated for a finite number of additions and multiplications provided p is large enough.

H_n is related to the Farey set F_n which is its subset in $[0,1]$. Farey sets have been used, for instance, by my colleague and friend Professor R. Sherman Lehman to factor medium sized numbers.

The cardinality of the partially ordered set is estimated in 1.6.5.

The complement $(Z_p - H_n - \{\pm\sqrt{-1}\})$ can be partitioned into 4 sets ϵ , $-\epsilon$, λ and $-\lambda$ which might play the role of the sets of smallest elements and the sets of largest elements as given in 1.6.5 to 1.6.5. Given an integer k , we can determine the corresponding irreducible rationals, or in which of the small or large set k belongs, using algorithm 1.6.5, which depends on the symmetry Theorem 1.6.2. We end by contrasting with the notion of continuity in the set of real numbers.

Definition.

A *Farey set* F_n is the set of irreducible rationals $\frac{a_i}{b_i}$, in ascending order, between 0 and 1, whose numerator and denominator do not exceed n .

A *Haros set* H_n is the set of irreducible rationals $\frac{a_i}{b_i}$, in ascending order, between $-n$ and n , whose numerator, in modulus, and denominator do not exceed n .

Theorem. [Haros]

If $\frac{a_i}{b_i}$ and $\frac{a_{i+1}}{b_{i+1}}$ are any 2 successive rationals of a Farey set F_n , then

0. $a_{i+1}b_i - a_ib_{i+1} = 1$.
1. The numerators and denominators of 2 successive rationals are relatively prime.
2. $\frac{a_i}{b_i} = \frac{a_{i-1} + a_{i+1}}{b_{i-1} + b_{i+1}}$.
3. The set F_n can be constructed starting from $\frac{0}{1}$ and $\frac{1}{1}$ by inserting rationals using formula 2 while the resulting numerators and denominators of the second member are not larger than n .

For a proof see Hardy and Wright, p. 23 to 26.

The set H_n can be deduced from F_n , by multiplicative symmetry with respect to 1 and then by additive symmetry with respect to 0. It can also be obtained from $\frac{-n}{1}$ and $\frac{n}{1}$ using formula 2, but reduction is required and the termination condition is not as simple as for the set F_n .

Definition.

A set S is *partially ordered* by \leq iff, with $a, b, c \in S$,

0. $a \leq a$ for all a in S ,
1. $a \leq b$ and $b \leq a \implies a = b$.
2. $a \leq b$ and $b \leq c \implies a \leq c$.

But, for any 2 distinct elements a and b in S , we need not have $a \leq b$ or $b \leq a$.

Notation.

$a < b$ if $a \leq b$ and $a \neq b$.

Definition.

We define the set $T_1(n)$ by:

0. The set $T_1(n) := \{ \frac{a_i}{b_i}, a_i \text{ and } b_i \text{ relatively prime, } |a_i| \leq n, 0 < b_i \leq n \}$.

Theorem.

If $0 < n$ and $2n(n-1) + 1 < p$ or equivalently if $0 < n < \frac{\sqrt{2p-1}+1}{2}$,

0. *there is a bijection between the irreducible rationals in H_n and the elements in the subset $T_1(n) \in Z_p$.*
1. *If the order in $T_1(n)$ is that induced by the order in $H_n \in Q$ and if $x, y \in T_1(n)$, then*
0. *the set H_n is partially ordered,*
1. *$x < y \Rightarrow -y < -x$,*
2. *$0 < x < y \Rightarrow 0 < 1/y < 1/x$.*

Proof: It is sufficient to prove, that under the given hypothesis, if $\frac{a_i}{b_i}$ and $\frac{a_j}{b_j}$ are any 2 distinct elements in Q , they correspond to distinct elements of $T_1(n)$ in Z_p . Indeed, if $\frac{r}{s} \equiv \frac{t}{u}$ then $ru - ts \equiv 0$ modulo p , but $|ru - ts| \leq n^2 + (n-1)^2 = 2n(n-1) + 1 < p$, hence, by hypothesis, $\frac{r}{s} = \frac{t}{u}$. The bound cannot be improved for T_1 , because, $\frac{n}{n-1} \equiv -\frac{n-1}{n}$ if $n^2 + (n-1)^2 = p$, whose positive root is $\frac{\sqrt{2p-1}+1}{2}$, and the sequence of primes of the form $\frac{m^2+1}{2}$ is infinite.

Definition.

For a given p , let n_p be the largest positive integer such that

0. $2n_p(n_p - 1) + 1 < p$,
 then
 0. $T_1 := T_1(n_p)$,
 1. $T_2 := T_1(\lfloor \sqrt{\frac{n_p}{2}} \rfloor)$.

Theorem.

If $x, y, x', y' \in T_2$,

0. $x.y, x+y \in T_1$,
1. $0 < x', x < y \Rightarrow x.x' < y.x'$.
2. $x \leq y, x' \leq y' \Rightarrow x+x' \leq y+y'$.

Indeed, if $|a|, |b|, |c|, |d| \leq m := \lfloor \sqrt{\frac{n_p}{2}} \rfloor$ then $|ad + bc| \leq 2m^2$, $|ac| \leq m^2$, and $|bd| \leq m^2$, therefore if $x, y, x', y' \in T_2$, $x + x'$ and $y + y' \in T_1(2m^2) = T_1(n_p) = T_1$. Of course, for multiplication only, we could replace $2m^2$ by m^2 .

Example.

In this, and in other examples, I have chosen as representative of an element in Z_p , that which is in modulus less than $\frac{p}{2}$.

0. For $p = 31$, $n_{31} = 4$, $T_1 = T_1(4)$ is

$$\begin{aligned} & -4 < -3 < -2 < 14 < 9 < -1 < 7 < -11 < 15 < 10 < -8 < 0 \\ & < 8 < -10 < -15 < 11 < -7 < 1 < -9 < -14 < 2 < 3 < 4. \end{aligned}$$

Indeed, the Farey set F_4 is

$$\frac{0}{1} < \frac{1}{4} < \frac{1}{3} < \frac{1}{2} < \frac{2}{3} < \frac{3}{4} < \frac{1}{1},$$

the values in Z_{31} are

$$0 < 8 < -10 < -15 < 11 < -7 < 1,$$

their inverses are

$$4 > 3 > 2 > -14 > -9 > 1.$$

$T_2 = T_1(1)$ is

$$-1 < 0 < 1.$$

For one multiplication we could use $T'_2 = T_1(2)$ ($2^2 = 4$) which is

$$-2 < -1 < 15 < 0 < -15 < 1 < 2.$$

1. For $p = 617$, $n_{617} = 18$, the positive elements of T_1 are

$$\begin{aligned} & 240 < -254 < 270 < 288 < -44 < 95 < -257 < -56 < -185 < -137 \\ & < 109 < -77 < -41 < 88 < 190 < 103 < -145 < -112 < 193 < 247 \\ & < -132 < -274 < 285 < 218 < -154 < -82 < -168 < -34 < -176 < -36 \\ & < 62 < -237 < 116 < 206 < -290 < -220 < -224 < -231 < -142 < -171 \\ & < -123 < 73 < -51 < -264 < 39 < 69 < -280 < -47 < 165 < -181 \\ & < -308 < 182 < -164 < 48 < 281 < -68 < -38 < 265 < 52 < -72 \\ & < 124 < 172 < 143 < 232 < 225 < 221 < 291 < -205 < -115 < 238 \\ & < -61 < 37 < 177 < 35 < 169 < 83 < 155 < -217 < -284 < 275 \\ & < 133 < -246 < -192 < 113 < 146 < -102 < -189 < 89 < 42 < 78 \\ & < -108 < 138 < 186 < 57 < 258 < -94 < 45 < -287 < -269 < 255 \\ & < -239 < 1 \\ & < -253 \\ & < 271 < 289 < -43 < 96 < -256 < -55 < -184 < -136 < -76 < -40 \\ & < -87 < 191 < 104 < -111 < 248 < -131 < -273 < 286 < -153 < -167 \\ & < -175 < 63 < -236 < 207 < -223 < -230 < -141 < -122 < -50 < -263 \\ & < 70 < -279 < -307 < 282 < -67 < 266 < 125 < 233 < 226 < -204 \\ & < -60 < 178 < 156 < 276 < -245 < -101 < 90 < 79 < 139 < 2 \\ & < -75 < -86 < 105 < 249 < -152 < -174 < 208 < -121 < -262 < -306 \\ & < 267 < 126 < -203 < 157 < -244 < -100 < 3 < 250 < -151 < 209 \\ & < -120 < -305 < 127 < -202 < 158 < 4 < -150 < 210 < -304 < -201 \\ & < 5 < 211 < -303 < -200 < 6 < -302 < 7 < -301 < 8 < -300 \\ & < 9 < 10 < 11 < 12 < 13 < 14 < 15 < 16 < 17 < 18. \end{aligned}$$

The positive elements in $T_2 = T_1(3)$ are

$$206 < -308 < -205 < 1 < -307 < 2 < 3.$$

Theorem (Mertens).

$$\sum_{b=1}^n (\phi(b)) = \frac{3n^2}{\pi^2} + O(n \log(n)),$$

where the last notation implies that the error divided by $n \log(n)$ is bounded as n tends to infinity.

Theorem.

The number of terms in T_1 is of the order of

$$\frac{6}{\pi^2}p + O(p^{\frac{1}{2}} \log(p)),$$

or approximately $0.6079p$.

This follows at once from the fact that the number of irreducible rationals with denominator b is $\phi(b)$, from $T_1 = 4 \sum_{b=2}^n (\phi(b)) + 3$ from $p = 2n^2 + O(n)$, from $\phi(1) = 1$ and from the Theorem of Mertens.

For $p = 31$, $23 = .74p$, for $p = 617$, $405 = .656p$.

The following Theorem gives a method to determine if a given integer in Z_p is in T_1 .

Algorithm. [Modified continued fraction]

Given $a_0 := p$, let $n := n_p$, $0 < a_1 := a < \frac{p}{2}$, $c_0 := 0$, $d_0 = 1$, $c_1 := 1$, $d_1 := 0$, $i := 1$

l: $q_i := a_{i-1}/a_i$, $a_{i+1} = a_{i-1} - a_i q_i$,
 $c_{i+1} = c_{i-1} + c_i q_i$, $d_{i+1} = d_{i-1} + d_i q_i$,
if $a_{i+1} \geq c_{i+1}$ then begin $i := i + 1$; goto l end,
if $a_i < n$ then $a \equiv \frac{(-1)^{i+1}}{c_{i+1}} \pmod{p} \in T_1$,
if $c_{i+1} < n$ then $a \equiv \frac{(-1)^i c_i}{a_i} \pmod{p} \in T_1$,
if $a_i a_{i+1} > c_i c_{i+1}$ then $a \in (-1)^{i+1} \lambda$,
if $a_i a_{i+1} < c_i c_{i+1}$ then $a \in (-1)^i \epsilon$,
if $a_i a_{i+1} = c_i c_{i+1}$ then $a = -1/a$.

i is therefore the largest index for which $a_i \geq c_i$.

We observe that if we start with $a' := a$ and $b' := \pm b^{-1} \pmod{a}$, the $+$ sign is to be chosen when n is even, and that by the symmetry property, when the algorithm stops, $c'_j \geq a'_j$, $c'_{j+1} < a'_{j+1}$, therefore $j = i + 1$ and we have consistent conditions.

Example.

For $p = 31$, $n_{31} = 4$,

0. if $a = 14$, the continued fraction algorithm gives

i	a_i	q_i	c_i		i	a_i	q_i	c_i		i	a_i	q_i	c_i	
0	31		0	5	0	31		0	6	0	31		0	3
1	14	2	1	4	1	12	2	1	5	<u>1</u>	<u>6</u>	5	<u>1</u>	2
<u>2</u>	<u>3</u>	4	<u>2</u>	<u>3</u>	2	7	1	2	4	2	<u>1</u>	6	<u>5</u>	<u>1</u>
3	2	1	9	2	<u>3</u>	<u>5</u>	1	<u>3</u>	<u>3</u>	3	0		31	0
4	1	2	11	1	4	<u>2</u>	2	<u>5</u>	2					
5	0		31	0	5	1	2	13	1					
					6	0		31	0					
c'_j q'_j a'_j j					c'_j q'_j a'_j j					c'_j q'_j a'_j j				

1. For $a = 14$, $i = 2$, $14.2 - 31.1 = -3$, $|-3| \leq 4$, $14 \equiv -\frac{3}{2} \pmod{31}$, which is in T_1 .
2. For $a = 12$, $i = 3$, $12.3 - 31.1 = 5 > 4$, $14 \equiv \frac{5}{3} \pmod{31}$, which is not in T_1 . But $12 \in -\epsilon$ and $13 \in -\lambda$.
3. For $a = 6$, $i = 1$, $6.1 - 31.1 = -25$, $|-25| > 4$, $6 \equiv -\frac{6}{1} \pmod{31}$, which is in T_1 . But $6 \in \lambda$ and $5 \in -\epsilon$.
4. In conclusion, $\lambda = \{6, -13\}$, $\epsilon = \{-5, -12\}$.

Example.

For $p = 617$, the elements in λ and, below them, their inverse in ϵ , are given below. Those in $-\lambda$ and $-\epsilon$ are obtained by replacing x by $-x$.

λ :	19	20	21	23	24	25	26	28	29	30	32	53	58
ϵ :	65	216	-235	161	180	-74	-261	-22	-234	144	135	163	-117
λ :	64	80	85	91	92	-98	-99	106	107	-118	-119	128	129
ϵ :	-241	54	-196	278	-114	-170	-268	-227	173	183	-140	188	-110
λ :	159	160	162	187	-195	-197	-198	-199	213	214	215	-228	-229
ϵ :	260	27	-179	33	-212	-166	-134	31	-84	-222	-66	46	-97
λ :	-242	-243	251	252	259	-272	277	-293	-294	-296	-297	-298	-299
ϵ :	283	-292	59	-71	81	93	-49	219	149	-148	-295	147	130

Definition.

Let $x \notin T_1$, let a_i and c_i be defined as in 1.6.5, with b replaced by x and let a_{i+1} and c_{i+1} be the next pair, let a'_i and c'_i , a'_{i+1} and c'_{i+1} , be the corresponding quadruple for $b' := \pm x^{-1}$, the sign so chosen that $b' < a/2$, if

$$0. \ c'_{i+1} = a_i, \ a'_{i+1} = c_i, \ c'_i = a_{i+1}, \ a'_i = c_{i+1},$$

then

1. 0. $a_i a_{i+1} < c_i c_{i+1}$ and i even $\Rightarrow x \in \epsilon$,
1. $a_i a_{i+1} < c_i c_{i+1}$ and i odd $\Rightarrow x \in -\epsilon$,
2. 0. $a_i a_{i+1} > c_i c_{i+1}$ and $i + 1$ even $\Rightarrow x \in \lambda$,
1. $a_i a_{i+1} > c_i c_{i+1}$ and $i + 1$ odd $\Rightarrow x \in -\lambda$.

and we have the partial ordering of these sets by $<<$,

$$-\lambda << -\epsilon << 0 << \epsilon << \lambda.$$

Theorem.

0. $x \in \epsilon \Rightarrow -x \in -\epsilon, 1/x \in \lambda, -1/x \in -\lambda.$
1. For a given p , all integers in the set $[0, p-1]$ are either in the set $T_1(n_p)$ or in one of the sets $\epsilon, -\epsilon, \lambda$, or $-\lambda$, with the exception of $\pm\sqrt{-1}$ when $p \equiv -1 \pmod{4}$.

We leave the proof as an exercise.

Theorem.

If for all $\epsilon \in (0, \epsilon_1) \exists \delta(\epsilon) > 0 \ni x_0 - \delta(\epsilon) < x < x_0 + \delta(\epsilon) \Rightarrow |f(x) - f(x_0)| < \epsilon$, then f is continuous at x_0 .

Indeed for the continuity criterium, we can choose $\delta(\epsilon) = \delta(\epsilon_1)$ for $\epsilon \geq \epsilon_1$.

Comment.

The preceding Theorem is implicit in most text. In the older texts, it is alluded to by adding in the definition of continuity the phrase “however small is ϵ ”. If we choose $\epsilon_1 = 10^{-100}$, say, and assume that for a given f and x_0 , the hypothesis of the preceding Theorem is satisfied, it follows that the continuity at x_0 depends only on the value of the function in the interval $(x_0 - 10^{-100}, x_0 + 10^{-100})$. If we now try to give an example from the world we live in, no meaning can be given to physical objects which have distances from each other less than ϵ_1 . The definition of continuity gives therefore problems of interpretation in Atomic Physics. The same is true in Cosmology when the distances are of the order of the dimension of the Universe. Continuity requires the notion of ordered set. We need to apply the more general concept of partially ordered set, to allow for a criterium which test values which are small, but not too small, or large but not too large. This is what is achieved using Farey sets.

1.6.6 Complex and quaternion integers.

Introduction.

Hamilton introduced the notion of quaternions, to try to generalize the notion of complex number for application to 3 dimensional geometry.

The elements are of the form $a + bi + cj + dk$, with a, b, c, d not all zero, with

$$\mathbf{j} \cdot \mathbf{k} = -\mathbf{k} \cdot \mathbf{j} = \mathbf{i}, \mathbf{k} \cdot \mathbf{i} = -\mathbf{i} \cdot \mathbf{k} = \mathbf{j}, \mathbf{i} \cdot \mathbf{j} = -\mathbf{j} \cdot \mathbf{i} = \mathbf{k}, \mathbf{i} \cdot \mathbf{i} = \mathbf{j} \cdot \mathbf{j} = \mathbf{k} \cdot \mathbf{k} = 0,$$

and real numbers commute with $\mathbf{i}, \mathbf{j}, \mathbf{k}$, addition of quaternions is commutative and is distributive over multiplication.

Definition.

Given a prime p and a non quadratic residue d , the set of *complex integers* C_p is the set

$$a + b\delta, a, b \in \mathbb{Z}_p, \delta^2 = d.$$

The operations are those of *addition*,

$$(a_0 + b_0\delta) + (a_1 + b_1\delta) = a_2 + b_2\delta,$$

where $a_2 := a_0 + a_1 \pmod{p}$, $b_2 := b_0 + b_1 \pmod{p}$.

and of *multiplication*,

$$(a_0 + b_0\delta).(a_1 + b_1\delta) = a_3 + b_3\delta,$$

where $a_3 := a_0.a_1 + b_0.b_1.d \pmod{p}$, $b_3 := a_0.b_1 + a_1.b_0 \pmod{p}$.

This is entirely similar to the introduction of complex numbers,

$$\delta^2 = d \text{ replacing } i^2 = -1.$$

Example.

For $p = 5$ and $d = 2$,

$$(1 + \delta) + (1 + 3\delta) = 2 + 4\delta,$$

$$(1 + \delta).(1 + 3\delta) = 2 + 4\delta.$$

Definition.

A *quaternion integer* is a quaternion with coefficients in Z_p .

Theorem.

If $p \equiv 1, 3 \pmod{8}$, the quaternion integers are isomorphic to 2 by 2 matrices over Z_p .

The isomorphism is deduced from the correspondance

$$\mathbf{1} \sim \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} \sim \begin{pmatrix} 1 & b \\ b & -1 \end{pmatrix}, \mathbf{j} \sim \begin{pmatrix} -b & 1 \\ 1 & b \end{pmatrix}, \mathbf{k} \sim \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

with $b^2 = -2$. For instance, for $p = 11$, $b = 3$, for $p = 17$, $b = 7$.

Theorem.

0. The quaternions form a skew field (or division ring).
1. The quaternion integers form a non commutative ring with unity for which if a right inverse exists then it is also a left inverse.

1.6.7 Loops.

Definition.

A *loop* $(L, +)$ is a non empty set of elements L together with a binary operation “+” such that, if l_1, l_2, l_3 , are elements in L ,

0. $l_1 + l_2$ is a *well defined* element of L .
1. There exists a *neutral element* $e \in L$, such that $e + l_1 = l_1 + e = l_1$.
2. $l_1 + x = l_2$ has a unique solution $x \in L$, denoted $x = l_1 \vdash l_2$ (or $x = l_1 \setminus l_2$, for $(L, .)$),
3. $y + l_1 = l_2$ has a unique solution $y \in L$ denoted $y = l_2 \dashv l_1$, (or $y = l_2 / l_1$, for $(L, .)$)

1.6.8 Groups.

Definition.

A *group* $(G, .)$ is a non empty set of elements G together with an operation $.$ such that

0. If g_1 and g_2 are any elements of G , $g_1.g_2$ is a *well defined* element of G .
1. The operation is *associative*, or for any elements g_1, g_2, g_3 of G ,

$$(g_1.g_2).g_3 = g_1.(g_2.g_3).$$
2. There exists a *neutral element* e in G , such that for all elements
 $g \in G$, $e.g = g.e = g$.
3. Every element g of G has an *inverse*, written g^{-1} , such that

$$g.g^{-1} = g^{-1}.g = e.$$

Notation.

If the operation is noted $+$ instead of $.$, the neutral element is called a zero and is noted 0.

Comment.

$(G, +)$ or $(G, .)$ is often abbreviated as G , if the operation is clear from the context.

Theorem.

In a group, the neutral element is unique and in element has only one inverse.

Definition.

A group $(G, +)$ is *abelian* or *commutative* iff for every element g_1 and g_2 of G ,

$$g_1.g_2 = g_2.g_1.$$

Notation.

In a group $(G, +)$, we define

0. $g = e$, $1.g = g$, $(n+1).g = n.g + g$ and $(-n).g = -(n.g)$ where n is any positive integer.

In a group $(G, .)$, we use instead of $0.g$, $1.g$ and $n.g$, g^0 , g^1 and g^n , where n is any positive or negative integer.

Definition.

A *cyclic group* $(G, .)$ is a group for which there exist an element g , called a generator of the group such that every element of G is of the form g^n . ($n.g$ if the operation is $+$).

Examples.

0. $(Z, +)$ is a cyclic group, 1 and -1 are generators.
1. $(Z_p, +)$, p prime, is a cyclic group, every element different from 0 is a generator.
2. $(Z_n, +)$, n composite, is an abelian group which is not cyclic.
3. $(Z_p - \{0\}, \cdot)$, p prime, is a cyclic group, any primitive root is a generator.

1.6.9 Veblen-Wederburn system.**Definition.**

A *Veblen-Wederburn system* $(\Sigma, +, \cdot)$, is a set Σ , containing at least the elements 0 and 1 which is such that for $a, b, c \in \Sigma$,

0. Σ is closed under the binary operations “+” and “ \cdot ”,
1. $(\Sigma, +)$ is an abelian group,
2. $(\Sigma - \{0\}, \cdot)$ is a loop,
3. $(a + b) \cdot c = a \cdot c + b \cdot c$,
4. $a \cdot 0 = 0$,
5. is right distributive,

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$
6. $a \neq b \Rightarrow x \cdot a = x \cdot b + c$ has a unique solution.

Definition.

A *division ring* is a Veblen-Wederburn system which is left distributive.

Definition.

A *alternative division ring* is a division ring for which for all elements $a \neq 0$, the right inverse a^R and left inverse a^L are equal, so that we can write it as a^{-1} and such that for all b in the set

$$(a \cdot b) \cdot b^{-1} = b^{-1} \cdot (b \cdot a) = a.$$

Theorem.

In an alternative division ring,

$$(b \cdot a) \cdot a = b \cdot a^2, a \cdot (a \cdot b) = a^2 \cdot b.$$

Definition.

The *Cayley numbers* or *octaves* consist of $(\mathbf{p} + \bar{\mathbf{q}}\mathbf{e}, +, \cdot)$, with (see also Stevenson p. 379)

0. \mathbf{p} and \mathbf{q} are quaternions over the reals,
1. $(\mathbf{p} + \bar{\mathbf{q}}\mathbf{e}) + (\mathbf{p}' + \bar{\mathbf{q}}'\mathbf{e}) = (\mathbf{p} + \mathbf{p}') + \overline{(\mathbf{q} + \mathbf{q}')}\mathbf{e}$,
2. $(\mathbf{p} + \bar{\mathbf{q}}\mathbf{e}) \cdot (\mathbf{p}' + \bar{\mathbf{q}}'\mathbf{e}) = (\mathbf{p}\mathbf{p}' - \bar{\mathbf{q}}'\mathbf{q} + \bar{\mathbf{q}}'\mathbf{p} + \mathbf{q}\bar{\mathbf{p}}'\mathbf{e})$,

Comment.

With \mathbf{l} and \mathbf{l}' denoting \mathbf{i} or \mathbf{j} or \mathbf{k} ,

$$\mathbf{e} \cdot \mathbf{l} = -\mathbf{l} \cdot \mathbf{e} = -\mathbf{l}\mathbf{e},$$

$$\mathbf{l}^2 = (\mathbf{l} \cdot \mathbf{e})^2 = -1,$$

$$\mathbf{e} \cdot (\mathbf{l}\mathbf{e}) = -(\mathbf{l}\mathbf{e}) \cdot \mathbf{e} = \mathbf{l},$$

$$(\mathbf{l}\mathbf{e}) \cdot \mathbf{l}' = -(\mathbf{l}'\mathbf{e}), \mathbf{l} \neq \mathbf{l}' \Rightarrow (\mathbf{l}\mathbf{e}) \cdot (\mathbf{l}'\mathbf{e}) = -\mathbf{l}\mathbf{l}'.$$

Definition.

The *conjugate* of an octave $\mathbf{o} = \mathbf{p} + \bar{\mathbf{q}}\mathbf{e}$ is defined by

$$\bar{\mathbf{o}} = \bar{\mathbf{p}} - \bar{\mathbf{q}}\mathbf{e},$$

the *norm* of an octave is defined by

$$N(\mathbf{o}) = \mathbf{o} \cdot \bar{\mathbf{o}}.$$

Theorem.

If $\mathbf{o} = \mathbf{p} + \bar{\mathbf{q}}\mathbf{e}$, then

0. $\bar{\bar{\mathbf{o}}} = \mathbf{o}$,
1. $\overline{\mathbf{o} \cdot \mathbf{o}'} = \bar{\mathbf{o}}' \cdot \bar{\mathbf{o}}$,
2. $N(\mathbf{o}) = N(\bar{\mathbf{o}}) = N(\mathbf{p}) + N(\mathbf{q})$,
3. $N(\mathbf{o}) = 0$ iff $\mathbf{o} = 0$,
4. $N(\mathbf{o} \cdot \mathbf{o}') = N(\mathbf{o}) N(\mathbf{o}')$.

Theorem.

0. *The octaves is an alternative division ring which is non associative.*

For instance, $(\mathbf{i} \cdot \mathbf{j}) \cdot \mathbf{e} = \mathbf{k}\mathbf{e}$, and $\mathbf{i} \cdot (\mathbf{j} \cdot \mathbf{e}) = -\mathbf{k}\mathbf{e}$.

1.6.10 Ternary Rings.

Definition.

A *ternary ring* $(\Sigma, *)$ is a set of elements Σ with at least 2 distinct elements 0 and 1, together with an ternary operation “ $*$ ” such that if a_1, a_2, a_3, a_4 are elements in Σ , then

0. $a_1 * a_2 * a_3$ is a well defined element of Σ ,
1. $a_1 * 0 * a_2 = a_2$,
2. $0 * a_1 * a_2 = a_2$,
3. $1 * a_1 * 0 = a_1$,
4. $a_1 * 1 * 0 = a_1$,
5. $a_1 \neq a_2 \Rightarrow x * a_1 * a_3 = x * a_2 * a_4$, has a unique solution $x \in \Sigma$,
6. $a_1 * a_2 * y = a_3$ has a unique solution $y \in \Sigma$,
7. $a_1 \neq a_2 \Rightarrow a_1 * x * y = a_3$ and $a_2 * x * y = a_4$ have a unique solution (x, y) , $x \in \Sigma$, $y \in \Sigma$.

Theorem.

0. $a \neq 0 \Rightarrow \exists a^R \ni a \cdot a^R = 1$, a^R is called the right inverse of a .
1. $a \neq 0 \Rightarrow \exists a^L \ni a^L \cdot a = 1$, a^L is called the left inverse of a .

Definition.

The *addition* in a ternary ring is defined by

$$a + b := a * 1 * b,$$

the *multiplication* in a ternary ring is defined by

$$a \cdot b := a * b * 0.$$

Theorem.

In a ternary ring $(\Sigma, *)$,

0. $(\Sigma, +)$ is a loop with neutral element 0.
1. $(\Sigma - \{0\}, \cdot)$ is a loop with neutral element 1 and $a \cdot 0 = 0 \cdot a = 0$.

1.6.11 Felix Klein (1849-1925). Transformation groups.

The approach which has dominated the non axiomatic study of geometry during the last one hundred years has been influenced, almost exclusively¹³, by the celebrated Inaugural address given by Felix Klein, when he became Professor of the Faculty of Philosophy of University of Erlangen and a member of its senate in 1872. In it¹⁴, Klein states that Geometries are characterized by a subgroup of the projective group, with, for instance, the group of congruences characterizing the Euclidean Geometry. The success of this approach to the study of Geometry has been such that in may very well have led to the decline of the synthetic Research and Teaching. It is hoped that this work, with its underlying program, which I call the Berkeley program, will revitalize the subject from the high school level on.

1.6.12 Functions.

Definition.

A *function* f from a set D to a set R is a set of *ordered* pairs (d_0, r_0) , d_0 in D , r_0 in R , such that if two pairs have the same first elements, they have the same second element. We write $r_0 = f(d_0)$.

Definition.

The *domain* of a function is the set D' which is the union of all the first elements of the pairs, the *range* of a function is the set R' which is the union of all the second pairs.

Definition.

A *function is one to one* or *bijective* iff for every pair (d_0, r_0) (d_1, r_1) such that $r_0 = r_1$ then $d_0 = d_1$.

Theorem.

If a function is one to one, the set of pairs (r_0, d_0) is a function f^{-1} from R to D .

Definition.

The function f^{-1} is called the *inverse* of f .

Definition.

Given 2 functions f and g such that the domain of g is a subset of the range of f , the *composition* $g \circ f$ is the function $(d_0, g(f(d_0)))$.

¹³Diedonné characterizes it as a “ligne de partage des eaux” in the reedition of the French translation

¹⁴Abhandlungen, p.460-497

Theorem.

The composition is associative. In other words,

$$(h \circ g) \circ f = h \circ (g \circ f).$$

1.6.13 Cyclotomic polynomials. Constructibility with ruler and compass.

One of the most extensive type of problems in Euclidean Geometry is the constructibility of geometric figures using the ruler and the compass. The construction of regular polygons lead Gauss, in his celebrated *Disquisitiones Arithmeticae* of 1801, to the study of roots of cyclotomic polynomials and his discovery that the regular polygon with 17 sides is so constructible. More generally, this is the case whenever the number of sides has the form $2^n \prod F_j^{i_j}$, where the F_j 's are Fermat primes (of the form $2^k + 1$)¹⁵. In so doing Gauss introduced, for the special case of cyclotomic equations, the method, which could be described as baby Galois Theory, which was generalized by Galois to the case of general polynomial equations. But in his case Gauss gives explicitly the various subgroups required to analyze completely the solution to the problem.

The general problem of constructibility has been extensively studied, I will mention only here the work Emile Lemoine (1902), of Henri Lebesgue (1950) and of A. S. Smogorzhevskii (1961). In finite geometry, it would appear at first that the ruler is sufficient for all constructions because any point in the plane can be obtained from 4 points forming a complete quadrangle. But this interpretation should be rejected in favor of that which implies that the construction of geometric figures should be given completely independently of the prime, or power of prime, which characterizes the finite Euclidean geometry. The impression is given that with the ruler very little can be constructed. One of the consequences of the results of Chapter 3, is to demonstrate, that both in the finite and classical case many more points, lines, circles, . . . can be constructed with the ruler than heretofore assumed, and that it is a useful exercise to reduce the problem of construction with the compass to that of a few points obtained with it and then the ruler alone. This is pursued extensively starting with the construction, first of the center of the inscribed circle. Of note is that the circle of Apollonius can be constructed with the ruler alone.

1.7 The real numbers.

1.7.1 The arithmetization of analysis. [Karl Weierstrass (1815-1897) and Riemann (1826-1866)]

In his *Introduction to the History of Mathematics*, Eves¹⁶ ascribed the beginning the arithmetization of analysis by Weierstrass and his followers to the problem presented by the

¹⁵Gauss gives, in n. 366, the polygons with number of sides less than 300, constructible with rule and compass, namely, 2, 4, 8, 16, 32, 64, 128, 256, 3, 6, 12, 24, 48, 96, 192, 5, 10, 20, 40, 80, 160, 15, 30, 60, 120, 240, 17, 34, 68, 136, 272, 51, 102, 204, 85, 170, 255, 257.

¹G17.TEX [MPAP], September 9, 2019

¹⁶p.426

existence (Riemann, 1874) of a continuous curve having no tangents at any of its points and that (Riemann) of a function which is continuous for all irrational values and discontinuous for all rational values in its domain of definition.

1.7.2 Algebraic and transcendental numbers. [Hermite (1822-1901) and Lindemann (1852-1939)]

Introduction.

We have seen that the Pythagoreans discovered that if we want any circle centered at the origin and passing to a point with rational coordinates to intersect always the x axis, irrationals have to be introduced. If that was all that was desired, it would be sufficient to construct first the extension field

$$Q(\sqrt{2}) = \{u + v\sqrt{2}\},$$

where u and v are in Q then

$$Q(\sqrt{2}(\sqrt{5})) = \{u_1 + v_1\sqrt{5}\},$$

where u_1 and v_1 are in $Q(\sqrt{2})$, The successive integers 5, 13, 17 are all the primes congruent to 1 modulo 4, because of the result of Euler ... and because all we would need was to obtain the square root of integers which can be written as a sum of 2 squares.

But, in fact we would like that circles centered at the origin, through a point with coordinates in one of these extension fields also intersect the x axis at a number in our system. This requires the introduction of algebraic numbers:

Definition.

An *algebraic number* is one which can be obtained as the real solution of a polynomial with integer coefficients.

A *transcendental number* is a real number which is not algebraic.

Example.

$\sqrt{2}$ is algebraic, being a root of $x^2 - 2 = 0$,

An outstanding problems of the last part of the 19-th century was the following, is π , which is the limit of the ratio of the length of a regular polygon with n sides to the diameter, algebraic or not.

The proof that it was not algebraic was first give by Lindemann in 1882, using an earlier result of Hermite of 1873, that e is not algebraic.

1.8 The pendulum and the elliptic functions.

1.8.0 Introduction.

This section uses extensively, material learned from George Lemaître, in his class on Analytical Mechanics, given to first year students in Engineering and in Mathematics and Physics, University of Louvain, Belgium, 1942 and from de la Vallée Poussin in his class on elliptic

functions in 1946.

We first determine the differential equation for the pendulum 1.8.1 using the Theorem of Toricelli 1.8.1, we then define the elliptic integral of the first kind and the elliptic functions of Jacobi 1.8.2 and 1.8.3, we then derive the Landen transformation which relates elliptic functions with different parameters 1.8.1, use it to obtain the Theorem of Gauss which determines the complete elliptic integrals of the first kind from the arithmetico-geometric mean of its 2 parameters 1.8.2. and obtain the addition formulas for the these functions 1.8.3 using the Theorem of Jacobi on pendular motions which differ by their initial condition 1.8.1. We also derive the Theorem of Poncelet on the existence of infinitely many polynomials inscribed in one conic and circumscribed to another 1.8.1. We state, without proof, the results on the imaginary period of the elliptic functions of Jacobi 1.8.3 and 1.8.3. A Theorem of Lagrange is then given which relates identities for spherical trigonometry and those for elliptic function 1.8.5. Finally we state the definitions and some results on the theta functions. Using this approach, the algebra is considerably simplified by using geometrical and mechanical considerations.

For references, see, Landen (1771), Legendre (1828), Jacobi (1829), Eisenstein (1847), Lagrange (Oeuvres), Gauss (Ostwald Klassiker), Abel (Oeuvres), Weierstrass (Werke), Cayley (1884), Emch (1901), Appell (1924), Bartky (1938), Lemaître (1947), Fettis (1965).

1.8.1 The pendulum.

Theorem. [Toricelli]

If a mass moves in a uniform gravitational field, its velocity v is related to its height h by

$$0. \quad v = \sqrt{2g(h_0 - h)},$$

where g is the gravitational constant and h_0 is a constant, corresponding to the height at which the velocity would be 0.

Proof: The laws of Newtonian mechanics laws imply the conservation of energy. In this case the total energy is the sum of the kinetic energy $\frac{1}{2}mv^2$ and the potential energy mgh , therefore

$$\frac{1}{2}mv^2 + mgh = mgh_0, \text{ for some } h_0.$$

Definition.

A *circulatory pendular motion* is the motion of a mass m restricted to stay on a vertical frictionless circular track, whose total energy allows the mass to reach with positive velocity the highest point on the circle. An *oscillatory pendular motion* is one for which the total energy is such that the highest point on the circle is not reached. The mass in this case oscillates back and forth. The following Theorem gives the equation satisfied by a pendular motion.

Theorem.

If a mass m moves on a vertical circle of radius R , with lowest point A , highest point B and center O , its position M at time t , can be defined by

$2\phi(t) = \angle(AOM)$ which satisfies

0. $D\phi = \sqrt{a^2 - c^2 \sin^2 \phi}$, where
1. $a^2 := \frac{gh_0}{2R^2}$, $c^2 = \frac{g}{R}$, for some h_0 .
2. $D^2\phi = -\frac{g}{2R} \sin \circ (2\phi)$.

Proof: If the height of the mass is measured from A ,

$$h(t) = R - R \cos(2\phi(t)) = 2R \sin^2 \phi(t),$$

the Theorem of Toricelli gives

$$RD(2\phi)(t) = v(t) = \sqrt{2gh_0 - 4gR \sin^2 \phi(t)},$$

hence 0.

The motion is circulatory if $h_0 > 2R$ or $a > c$, it is oscillatory if $0 < h_0 < 2R$ or $c > a$.

2, follows by squaring 0 and taking the derivative.

Notation.

$$0. \ k := \frac{c}{a}, \ b^2 := a^2 - c^2, \ k' := \frac{b}{a}, \ m := k^2.$$

Theorem. [Jacobi]

Let $M(t)$ describes a pendular motion. Given the circle γ which has the line r at height h_0 as radical axis and is tangent to $AM(t_0)$, if $N(t)M(t)$ remains tangent to that circle, then $N(t)$ describes the same pendular motion, with $N(t_0) = A$.

Proof: With the abbreviation $M = M(t)$, $N = N(t)$, let NM meets r at D , let M' , N' be the projections of M and N on r , let T be the point of tangency of MN with γ ,

$$0. \ DM \ DN = DT^2,$$

therefore

$$1. \ \frac{DT}{ND} = \frac{DM}{DT} = \frac{DT-DM}{ND-DT} = \frac{MT}{NT} = \sqrt{\frac{DT}{ND} \frac{DM}{DT}} = \sqrt{\frac{DM}{ND}} = \sqrt{\frac{M'M}{N'N}}$$

When t is replaced by $t + \epsilon$,

$$2. \ \frac{v_M}{v_N} = \lim_{\epsilon \rightarrow 0} \frac{M(t+\epsilon) - M(t)}{N(t+\epsilon) - N(t)} = \lim_{\epsilon \rightarrow 0} \frac{M(t)T}{N(t+\epsilon)T} = \frac{MT}{NT},$$

because the triangles $T, M, M(t+\epsilon)$ and $T, N, N(t+\epsilon)$ are similar, because $\angle(T, N, N(t+\epsilon)) = \angle(T, M, M(t+\epsilon))$ as well as $\angle(M(t+\epsilon), T, M) = \angle(N(t+\epsilon), T, N)$.

Therefore

$$3. \ \frac{v_M}{v_N} = \sqrt{\frac{M'M}{N'N}}.$$

The Theorem of Toricelli asserts that $v_M = \sqrt{2gM'M}$, this implies, as we have just seen, $v_N = \sqrt{2gN'N}$, therefore N describes the same pendular motion with a difference in the origin of the independent variable.

Corollary.

If $M = B$ and $N = A$, the line $M(t) \times N(t)$ passes through a fixed point L on the vertical through O .

Moreover, if $b := BL$ and $a := LA$, we have

$$\frac{v_M}{v_N} = \frac{b}{a} \text{ and } h_0 = \frac{a^2}{a-b}.$$

This follows at once from from 1.8.1.2, and 1.

Definition.

The point L of the preceding Corollary is called *point of Landen*.

Theorem. [Poncelet]

Given 2 conics θ and γ , if a polygon P_i , $i = 0$ to n , $P_n = P_0$, is such that P_i is on θ and $P_i \times P_{i+1}$ is tangent to γ , then there exists infinitely many such polygons.

Any such polygon is obtained by choosing Q_0 on θ drawing a tangent Q_0Q_1 to γ , with Q_1 on θ and successively Q_i , such that Q_i is on θ and $Q_{i-1} \times Q_i$ is tangent to γ , the Theorem asserts that $Q_n = Q_0$.

The proof follows at once from 1.8.1, after using projections which transform the circle θ and the circle γ into the given conics.

The Theorem is satisfied if the circle have 2 points in common or not.

Theorem.

If $M(t)$ describes a circular pendular motion, then the mid-point $M_1(t)$ of $M(t)$ and $M(t+K)$ describes also a circular pendular motion. More precisely, $M_1(t)$ is on a circle with diameter LO , with $LA = a$, $LB = b$, and if

$$\phi_1(t) = \angle(O, L, M_1(t)),$$

$$0. \quad t = \int_0^{\phi(t)} \frac{D\phi}{\Delta} = \frac{1}{2} \int_0^{\phi_1(t)} \frac{D\phi_1}{\Delta_1}.$$

where

$$1. \quad \Delta^2 := a^2 \cos^2 \phi + b^2 \sin^2 \phi \text{ and } \Delta_1^2 := a_1^2 \cos^2 \phi_1 + b_1^2 \sin^2 \phi_1,$$

where the relation between ϕ and ϕ_1 is given by

$$2. \quad \tan(\phi_1 - \phi) = k' \tan \phi, \text{ or}$$

$$3. \quad \sin(2\phi - \phi_1) = k_1 \sin \phi_1,$$

with

$$4. \quad k' := \frac{b}{a}, \quad k_1 := \frac{c_1}{a_1},$$

$$5. \quad a_1 := \frac{1}{2}(a+b), \quad b_1 := \sqrt{ab}, \quad c_1 := \frac{1}{2}(a-b), \text{ therefore}$$

$$6. \quad a = a_1 + c_1, \quad b = a_1 - c_1, \quad c = 2\sqrt{a_1 c_1}.$$

Proof: First, it follows from the Theorem of Toricelli that the velocity v_A at A and v_B at B satisfy

$$v_A = \sqrt{2gh_0} = 2Ra, \quad v_B = \sqrt{2gh_0 - 2R} = \sqrt{4R^2a^2 - 4c^2R^2} = 2Rb,$$

therefore $\frac{BL}{LA} = \frac{b}{a}$.

If P is the projection of L on BM and Q the projection of L on AM ,

$$LM^2 = LP^2 + LQ^2 = a^2\cos^2\phi + b^2\sin^2\phi = \Delta^2.$$

$$LQ = LM\cos(\phi_1 - \phi) = a\cos\phi.$$

We can proceed algebraically. Differentiating 2. gives

$$a(1 + \tan^2(\phi_1 - \phi))(D\phi_1 - D\phi) = b(1 + \tan^2\phi)D\phi,$$

or

$$\begin{aligned} a(1 + \tan^2(\phi_1 - \phi))D\phi_1 &= (a(1 + \tan^2(\phi_1 - \phi) + b(1 + \tan^2\phi))D\phi \\ &= (a + b + \frac{b^2}{a}\tan^2\phi + b\tan^2\phi)D\phi \\ &= (a + b)(1 + \frac{b}{a}\tan^2\phi)D\phi \\ &= (a + b)(1 + \tan\phi\tan(\phi_1 - \phi))D\phi, \end{aligned}$$

or

$$\begin{aligned} \frac{a}{\cos^2(\phi_1 - \phi)}D\phi_1 &= 2a_1 \frac{\cos(2\phi - \phi_1)}{\cos\phi\cos(\phi_1 - \phi)}D\phi, \text{ or} \\ \frac{D\phi}{\frac{a\cos\phi}{\cos(\phi_1 - \phi)}} &= \frac{D\phi_1}{2a_1\cos(2\phi - \phi_1)}, \end{aligned}$$

or because $LM = \Delta$

$$\frac{D\phi}{\Delta} = \frac{D\phi_1}{2\Delta_1}.$$

We can also proceed using kinematics.

The velocity at M is

$$v_M = 2RD\phi = 2R\Delta,$$

If we project the velocity vector on a perpendicular to LM ,

$$LMD\phi_1 = v_M\cos(2\phi_1 - \phi) = 2R\cos(2\phi_1 - \phi)\Delta\phi.$$

Therefore

$$\frac{D\phi}{\Delta} = \frac{D\phi_1}{2R\cos(2\phi_1 - \phi)} = \frac{a_1}{2R} \frac{D\phi_1}{\Delta_1} = \frac{D\phi_1}{2\Delta_1}.$$

Definition.

The transformation from ϕ to ϕ_1 is called the *forward Landen transformation*.

The transformation from ϕ_1 to ϕ is called the *backward Landen transformation*.

These transformations have also been applied to the integrals of the second kind and of the third kind.

Comment.

The formulas 3. and 1. are the formulas which are used to compute t from $\phi(t)$. The formulas 4. and 2. are used to compute $\phi(t)$ from t .

Comment

Given the first order differential equations,

$$\begin{aligned} (Dy)^2 &= C_0(y^2 + A_0)(y^2 + B_0), \\ (Dz)^2 &= C_1(z^2 + A_1)(z^2 + B_1), \end{aligned}$$

with

$$z = d(y + \frac{l}{y}), l \neq 0, d > 0.$$

These equations are compatible iff

$$d^2(1 - \frac{l}{y^2})^2 C_0(y^2 + A_0)(y^2 + B_0) = C_1(d^2(\frac{y^2+l}{y})^2 + A_1)(d^2(\frac{y^2+l}{y})^2 + B_1)$$

this requires \sqrt{l} to be a root of one of the factors of the second member, let it be the second factor, this implies

$$d^2 4l + B_1 = 0,$$

then, the second factor becomes,

$$d^2(\frac{y^2+l}{y})^2 + B_1 = d^2((\frac{y^2+l}{y})^2 - 4l) = d^2(\frac{y^2-l}{y})^2,$$

therefore \sqrt{l} is a double root of the second member and

$$C_0(y^4 + (A_0 + B_0)y^2 + A_0B_0) = d^2 C_1(y^4 + (2l + \frac{A_1}{d^2})y^2 + l^2), \text{ therefore}$$

$$C_0 = d^2 C_1, A_0 B_0 = \frac{B_1^2}{16d^4}, A_0 + B_0 = \frac{A_1 - \frac{1}{2}B_1}{d^2},$$

For real transformations, $A_0 B_0 > 0$, if $j_0 = \text{sign}(B_0)$ and $j_1 = \text{sign}(B_1)$,

$$B_1 = 4j_1 d^2 \sqrt{A_0 B_0}, A_1 = d^2(A_0 + B_0 + 2j_1 \sqrt{A_0 B_0}) \\ = j_0 d^2(\sqrt{|A_0|} + j_0 j_1 \sqrt{|B_0|})^2.$$

If we want $A_1 B_1 > 0$ then $j_0 = j_1$.

1.8.2 The elliptic integral and the arithmetico-geometric mean.

Introduction.

Gauss began his investigations after he showed that the length of the lemniscate could be computed from the arithmetico geometric mean of $\sqrt{2}$ and 1. More precisely, the lemniscate is the curve $r^2 = \cos(2\theta)$, in polar coordinates. A quarter of its length is given by the integral

$$\int_0^1 \frac{dr}{\sqrt{1-r^4}},$$

which is easily deduced from the general formula for the square of the arc length in polar coordinates, $ds^2 = dr^2 + r^2(d\theta)^2$.

Gauss observed that to 9 decimal places the integral was 1.311028777 and so is $\frac{\pi/2}{\text{agm}(\sqrt{2}, 1)}$, where $\text{agm}(a, b)$ denotes the arithmetico geometric mean of 2 numbers, defined below.

Theorem. [Gauss]

Given $a_0 > b_0 > 0$, let

$$0. a_{i+1} := \frac{1}{2}(a_i + b_i),$$

$$1. b_{i+1} := \sqrt{a_i b_i},$$

2. The sequences a_i and b_i have a common limit a_∞ .

3. The sequence a_i is monotonically decreasing and the sequence b_i is monotonically increasing.

Proof: Because

$$a_i > a_{i+1}, b_{i+1} > b_i,$$

it follows that the sequence a_i is bounded below by b_0 , the sequence b_i is bounded above by a_0 , therefore both have a limit a_∞ and b_∞ . Taking the limit of 0. gives at once $a_\infty = b_\infty$.

Definition.

a_∞ is called the *arithmetico-geometric mean* of a_0 and b_0 .

Example.

With $a_0 = \sqrt{2}$ and $b_0 = 1$,
 $a_1 = 1.207106781$, $b_1 = 1.189207115$,
 $a_2 = 1.198156948$, $b_2 = 1.198123521$,
 $a_3 = 1.198140235$, $b_2 = 1.198140235$.

Definition.

If $a = 1$, and we express t in terms of $\phi(t)$,

0. $t = \int_0^{\phi(t)} \frac{1}{\sqrt{1-k^2 \sin^2}} \cdot$ This integral is called the *incomplete elliptic integral of the first kind*. Its inverse function ϕ is usually noted
1. $am := \phi$, the *amplitude function*,
2. $K := \int_0^{\frac{\pi}{2}} \frac{1}{\sqrt{1-k^2 \sin^2}}$ is called the *complete integral of the first kind*, it gives half the period, $\frac{K}{a}$, for the circular pendulum.

Theorem.

0. For the circulatory pendulum, the angle 2ϕ between the lowest position of the mass and that at time t is given by $\phi = am(at)$. The coordinates are $R \sin(2\phi)$, $R - R \cos(2\phi)$.
1. For the oscillatory pendulum, if the highest point is $2R \sin^2(\alpha)$ above the lowest point, the angle 2θ between the lowest position of the mass and that at time t is given by $\sin\theta = \sin\phi \sin\alpha$ where ϕ is given by $\phi = am(at, \sin^2\alpha)$.

Theorem.

For the complete integrals we have

$$0. \frac{K}{a} = \int_0^{\frac{\pi}{2}} \frac{1}{\sqrt{a^2 \cos^2 + b^2 \sin^2}} = \frac{\frac{\pi}{2}}{a_\infty}.$$

Proof: If $\phi(K) = \frac{\pi}{2}$, then $\phi_1(K) = \pi$, therefore

$$\begin{aligned} 1. K &= \int_0^{\frac{\pi}{2}} \frac{D\phi}{\Delta} = \int_0^\pi \frac{D\phi_1}{2\Delta_1} = \frac{1}{2} \int_0^{\frac{\pi}{2}} \frac{D\phi_1}{\Delta_1} + \frac{1}{2} \int_{\frac{\pi}{2}}^\pi \frac{D\phi_1}{\Delta_1} = \int_0^\pi \frac{D\phi_1}{\Delta_1} = \int_0^{\frac{\pi}{2}} \frac{D\phi_n}{\Delta_n} \\ &= \int_0^{\frac{\pi}{2}} \frac{1}{a_\infty} = \frac{\frac{\pi}{2}}{a_\infty}. \end{aligned}$$

1.8.3 The elliptic functions of Jacobi.

Definition.

The functions

0. $sn := \sin \circ am$, $cn := \cos \circ am$, $dn := \sqrt{1 - k^2 sn^2}$,
are called the *elliptic functions of Jacobi*.

The functions which generalize \tan , \csc , ... are

1. $ns := \frac{1}{sn}$, $nc := \frac{1}{cn}$, $nd := \frac{1}{dn}$,
2. $sc := \frac{sn}{cn}$, $cd := \frac{cn}{dn}$, $ds := \frac{dn}{sn}$,
3. $cs := \frac{cn}{dn}$, $dc := \frac{dn}{cn}$, $sd := \frac{sn}{dn}$.

Theorem.

If

0. $s_1 := sn(t_1)$, $c_1 = cn(t_1)$, $d_1 = dn(t_1)$ and
1. $s_2 := sn(t_2)$, $c_2 = cn(t_2)$, $d_2 = dn(t_2)$,
we have
2. $sn^2 + cn^2 = 1$, $dn^2 + k^2 sn^2 = 1$, $dn^2 - k^2 cn^2 = k'^2$.
3. $1 - k^2 s_1^2 s_2^2 = c_1^2 + s_1^2 d_2^2 = c_2^2 + s_2^2 d_1^2$.

Lemma.

0. $c_2 = c_1 cn(t_1 + t_2) + d_2 s_1 sn(t_1 + t_2)$,
1. $d_2 = d_1 dn(t_1 + t_2) + k^2 s_1 c_1 sn(t_1 + t_2)$.

Proof: We use the Theorem 1.8.1 of Jacobi. Let R be the radius of θ and O its center, let r be the radius of γ and O' its center, let $s := OO'$. Let A , N , M' , M be the position of the mass at time 0, t_1 , t_2 , $t_1 + t_2$.

The lines $A \times M'$ and $N \times M$ are tangent to the same circle γ at T' and T .

Let X be the intersection of $O \times M$ and $O' \times T$, $2\phi := \angle(A, O, N)$,

2. $2\phi' := \angle(A, O, M)$,
we have $\angle(N, O, M) = 2(\phi' - \phi)$, $\angle(M, X, T) = \phi' - \phi$, $\angle(T, O', O) = \phi' + \phi$.

If we project MOO' on $O'T$,

$$r = R \cos(\phi' - \phi) \sin(\phi' + \phi), \text{ or}$$

3. $r = (R + s) \cos \phi \cos \phi' + (R - s) \sin \phi \sin \phi'$.
 $\phi = amt_1$, $\phi' = am(t_1 + t_2)$,
 $\sin \phi' = sn(t_1 + t_2)$, $\cos \phi' = cn(t_1 + t_2)$,
 $\sin \phi = sn t_1 = s_1$,
 $\cos \phi = cn t_1 = c_1$,

when $t_1 = 0$,

$$\cos(\angle(A, B, M')) = cn t_2 = c_2 = \frac{BM'}{AB} = \frac{O'T'}{AO'} = \frac{r}{R+s},$$

the ratio of the velocities is

$$\frac{v_{M'}}{v_A} = \frac{dn t_2}{dn 0} = d_2 = \frac{TM'}{AT} = \frac{O'B}{AO'} = \frac{R-s}{R+s}, \text{ substituting in 2. gives 0.}$$

The proof of 1. is left as an exercise.

Theorem. [Jacobi]

0. $\frac{sn u_1 cn u_2 dn u_2 + sn u_2 cn u_1 dn u_1}{sn(u_1 + u_2)} = 1 - k^2 sn^2 u_1 sn^2 u_2.$
1. $\frac{cn u_1 cn u_2 - sn u_1 dn u_1 sn u_2 dn u_2}{cn(u_1 + u_2)} = 1 - k^2 sn^2 u_1 sn^2 u_2.$
2. $\frac{dn u_1 dn u_2 - k^2 sn u_1 sn u_2 cn u_1 cn u_2}{dn(u_1 + u_2)} = 1 - k^2 sn^2 u_1 sn^2 u_2.$

Proof: Let $w = \frac{1}{1 - k^2 s_1^2 s_2^2}.$

Let s_1, s_2, \dots denote $sn u_1, sn u_2, \dots$, define S and C such that

$$sn(u_1 + u_2) = Sw, \quad cn(u_1 + u_2) = Cw.$$

The 1.8.3.0. gives

$$c_2 = c_1 Cw + d_2 s_1 Sw \text{ or}$$

$$3. \quad c_1 Cw = -d_2 s_1 Sw + c_2,$$

1.8.3.2. gives

$$S^2 w^2 + C^2 w^2 = 1,$$

eliminating C gives the second degree equation in Sw :

$$(c_1^2 + d_2^2 s_1^2 (Sw)^2 - 2s_1 c_2 d_2 (Sw) + c_2^2 - c_1^2 = 0,$$

one quarter of the discriminant is

$$\begin{aligned} & s_1^2 c_2^2 d_2^2 - (c_2^2 - c_1^2)(c_1^2 + d_2^2 s_1^2) \\ &= s_1^2 c_2^2 d_2^2 - c_1^2 c_2^2 + c_1^4 - s_1^2 c_2^2 d_2^2 + s_1^2 c_1^2 d_2^2 \\ &= c_1^2 (c_1^2 - c_2^2 + s_1^2 d_2^2) = c_1^2 s_2^2 d_1^2, \end{aligned}$$

therefore

$$Sw = (s_1 c_2 d_2 \pm c_1 d_1 s_2)w.$$

One sign correspond to one tangent from M to γ , the other to the other tangent, therefore one corresponds to the addition, the other to the subtraction formula. From the special case $k = 0$, follows that, by continuity, the $+$ sign should be used. This gives 0., 1. follows from 3, 2. is left as an exercise.

Corollary.

0. $sn(u + K) = cd(u), \quad cn(u + K) = -k' sd(u), \quad dn(u + K) = k' nd(u).$
1. $sn(u + 2K) = -sn(u), \quad cn(u + 2K) = -cn(u), \quad dn(u + 2K) = dn(u).$
2. $sn(u + 4K) = sn(u), \quad cn(u + 4K) = cn(u), \quad dn(u + 4K) = dn(u).$

Definition.

$$K'(k^2) = K(k'^2).$$

Theorem.

- 0. $ksn \circ I + iK' = sn,$
 - 1. $ikcn \circ I + iK' = ds,$
 - 2. $idn \circ I + iK' = cs,$
- 1. $sn \circ I + 2iK' = sn,$
 - 1. $cn \circ I + 2iK' = -cn,$
 - 2. $dn \circ I + 2iK' = -dn,$

Theorem.

- 0. sn has periods $4K$ and $2iK'$ and pole $\pm iK'$,
- 1. cn has periods $4K$ and $4iK'$ and pole $\pm iK'$,
- 2. dn has periods $2K$ and $4iK'$ and pole $\pm iK'$.

Theorem.

- 0. $k = 0 \Rightarrow sn = \sin, cn = \cos, dn = \underline{1},$
- 1. $k = 1 \Rightarrow sn = \tanh, cn = \operatorname{sech}, dn = \operatorname{sech}.$

1.8.4 The theta functions of Jacobi.**Definition.**

Given the parameter q , called the nome,

- 0. $q := e^{-\pi \frac{K'}{K}},$
the functions
- 1. $\theta_1 := 2q^{\frac{1}{4}} \sum_{n=0}^{\infty} (-1)^n q^{n(n+1)} \sin(2n+1)I$
- 2. $\theta_2 := 2q^{\frac{1}{4}} \sum_{n=0}^{\infty} q^{n(n+1)} \cos(2n+1)I$
- 3. $\theta_3 := 1 + 2 \sum_{n=1}^{\infty} q^{n^2} \cos 2nI$
- 4. $\theta_4 := 1 + 2 \sum_{n=1}^{\infty} (-1)^n q^{n^2} \cos 2nI$ are the *theta functions of Jacobi*.

Definition.

The functions, with $v = \frac{\pi I}{2K}$

- 0. $\theta_s := \frac{2K \theta_1 \circ v}{D\theta_1(0)}, \theta_c := \frac{\theta_2 \circ v}{\theta_2(0)}, \theta_d := \frac{\theta_3 \circ v}{\theta_3(0)}, \theta_n := \frac{\theta_4 \circ v}{\theta_4(0)},$
are called the *theta functions of Neville*.

Theorem.

If p, q denote any of s, c, d, n ,

$$pq = \frac{\theta_p}{\theta_q}.$$

For instance

$$sn = \frac{\theta_s}{\theta_n} = \frac{2K\theta_1\phi v}{D\theta_1(0)} \cdot \frac{\theta_4(0)}{\theta_4\phi v}.$$

Theorem.

The Landen transformation replaces the parameter q , by q^2 .

1.8.5 Spherical trigonometry and elliptic functions.**Theorem. [Lagrange]**

From the addition formulas of elliptic functions, we can derive those for a spherical triangle as follows. Let

$$0. \quad u_1 + u_2 + u_3 = 2K,$$

define

$$\begin{aligned} 1. \quad & \sin a := -snu_1, \cos a := -cnu_1, \\ & \sin b := -snu_2, \cos b := -cnu_2, \\ & \sin c := -snu_3, \cos c := -cnu_3, \\ & \sin A := -k snu_1, \cos A := -dnu_1, \\ & \sin B := -k snu_2, \cos B := -dnu_2, \\ & \sin C := -k snu_3, \cos C := -dnu_3, \end{aligned}$$

then to any formula for elliptic functions of u_1, u_2, u_3 , corresponds a formula for a spherical triangle with angles A, B, C and sides a, b, c . For instance,

$$2. \quad \frac{\sin A}{\sin a} = \frac{\sin B}{\sin b} = \frac{\sin C}{\sin c} = k.$$

$$3. \quad \cos a = \cos b \cos c + \sin b \sin c \cos A,$$

$$4. \quad \cos A = -\cos B \cos C + \sin B \sin C \cos a,$$

$$5. \quad \sin B \cot A = \cos c \cos B + \sin c \cot a.$$

Proof. 2. follows from the definition. 3. follows from

$$c_2 = c_1 cn(u_1 + u_2) + d_2 s_1 sn(u_1 + u_2) \text{ after interchanging } u_1 \text{ and } u_2 \text{ and using}$$

$$6. \quad 0. \quad sn(u_1 + u_2) = sn(2K - u_1 - u_2) = sn u_3 = s_3,$$

$$1. \quad cn(u_1 + u_2) = -cn(2K - u_1 - u_2) = -cn u_3 = -c_3,$$

$$2. \quad dn(u_1 + u_2) = dn(2K - u_1 - u_2) = dn u_3 = d_3,$$

similarly, 4. follows from

$$c_2 = c_1 cn(u_1 + u_2) + d_2 s_1 sn(u_1 + u_2)$$

after interchanging u_1 and u_2 and using 6, and 5. from

$$sn u_2 dn u_1 = cn u_1 sn(u_1 + u_2) - sn u_1 dn u_2 cn(u_1 + u_2)$$

after division by $sn u_1$.

1.8.6 The p function of Weierstrass.

Introduction.

Because it is not germane in this context, I will only mention briefly the important contribution of Weierstrass, which proved that all doubly periodic meromorphic functions can be expressed in terms of one of them, the p function. The addition formulas for this function and for the Jacobi functions and many other properties generalize to the finite case (De Vogelaere, 1983)..

1.8.7 References.

0. Abel, Niels Henrik, *Oeuvres Complètes*, Nouv. ed., publiées aux frais de l'Etat norvégien par L. Sylow et S. Lie, Christiania, Grondahl & Son, 1881, Vol. 1,2.
1. Appell, Paul Emile & Dautheville, S., *Précis de Mécanique Rationnelle*, Paris, Gauthier-Villars, 1924, 721 pp.
2. Bartky, *Numerical Calculation of Generalized Complete Integrals*, Rev. of Modern Physics, 1938, Vol. 10, 264-
3. Cayley, Arthur, *On the Addition of Elliptic Functions*, Messenger of Mathematics, Vol. 14, 1884, 56-61.
4. Cayley, Arthur, *Note sur l'Addition des Fonctions Elliptiques*, Crelle J., Vol. 41, 57-65.
5. De Vogelaere, René, *Finite Euclidean and non-Euclidean Geometry with application to the Finite Pendulum and the Polygonal Harmonic Motion. A First Step to Finite Cosmology*. The Big Bang and Georges Lemaître, Proc. Symp. in honor of 50 years after his initiation of Big-Bang Cosmology, Louvain-la-Neuve, Belgium, October 1983., D. Reidel Publ. Co, Leyden, the Netherlands. 341-355.
6. Eisenstein, Ferdinand Gotthold Max, *Mathematische Abhandlungen*, besonders aus dem Gebiete der höheren Arithmetik und den elliptischen Functionen, Mit einer Vorrede von C.F. Gauss. (Reprografischer Nachdruck der Ausg., Berlin 1847.) Hildesheim, G. Olms, 1967.
7. Emch, *An Application of Elliptic Functions*, Annals of Mathematics, Ser. 2, Vol. 2, 1901. III.4.4.0.
8. Fettis, Henri E., Math. of Comp., 1965.
9. Gauss, Carl Friedrich, Ostwald Klassiker der Exakten Wissenschaften, Nr 3.
10. Jacobi, Karl Gustav Jakob, *Fundamenta Nova Theoriae Functionum Ellipticarum*, 1829.
11. Landen, John, Phil. Trans. 1771, 308.

12. Lagrange, Joseph Louis, comte, *Oeuvres*, publiées par les soins de m. J.-A. Serret, sous les auspices de Son Excellence le ministre de l'instruction publique, Paris, Gauthier-Villars, 1867-92.
13. Legendre, Adrien Marie, *Traité des Fonctions Elliptiques et des Intégrales Euleriennes*, avec des tables pour en faciliter le calcul numérique, Paris, Huzard-Courcier, Vol. 1-3, 1825-1828.
14. Lemaître, Georges, *Calcul des Intégrales Elliptiques*, Bull. Ac. Roy. Belge, Classe des Sciences, Vol. 33, 1947, 200-211.
15. Weierstrass, Karl, *Mathematische Werke*, Hildesheim, G. Olms, New York, Johnson Reprint 1967.

1.8.8 Texts on and tables of elliptic Functions.

0. Abramowitz, Milton & Stegun, Irene A. Edit., *Handbook of Mathematical Functions*, U.S. Dept of Commerce, Nat. Bur. of Stand., Appl. Math, Ser., number 55, 1964, 1046 pp.
1. Adams, Edwin Plimpton, Ed., *Smithsonian Mathematical Formulae and Tables of Elliptic Functions*, under the direction of Sir George Greenhill, 3d reprint, City of Washington, 1957, Its Smithsonian miscellaneous collections, v.74, no.1, Smithsonian Institution, Publication 2672.
2. Halphen, Georges Henri, *Traité des Fonctions Elliptiques et de leurs Applications*, Paris, Gauthier-Villars, 1886-91.
3. Hancock, Harris, *Lectures on the Theory of Elliptic Functions*, v. 1. 1st ed., 1st thousand, New York, J. Wiley, 1910. Dover Publ., 1958.
4. Jahnke, Eugen & Emde, Fritz, *Tables of Functions with Formulae and Curves*, 4th ed., New York, Dover Publications, 1945.
5. Jahnke, Eugen & Emde, Fritz & Losch, Friedrich, *Tables of Higher Functions*, 6th ed. rev. by Losch, New York, McGraw-Hill, 1960.
6. Jordan, Camille, *Fonctions Elliptiques*, New York, Springer-Verlag, 1981.
7. King, Louis Vessot, *On the Direct Numerical Calculations of Elliptic Functions and Integrals*, Cambridge, Eng., Univ. Press, 1924.
8. Lang, Serge, *Elliptic functions*, 2nd ed., New York, Springer-Verlag, 1987, Graduate texts in mathematics, 112.
9. Mittag-Leffler, Magnus Gustaf, *An Introduction to the Theory of Elliptic Functions*, Lancaster, Pa., 1923, Hamburg, Germany, Lutcke & Wulff.

10. Neville, Eric Harold, *Elliptic Functions, a primer*, Prepared for publication by W. J. Langford, 1st d. Oxford, New York, Pergamon Press, 1971.
11. Neville, Eric Harold, *Jacobian Elliptic Functions*, Oxford, The Clarendon Pr., 1944.
12. Oberhettinger, Fritz Wilhelm & Magnus, Wilhelm, *Anwendung der elliptischen Funktionen in Physik und Technik*, Berlin, Springer, 1949, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Bd. 55.
13. Riemann, Bernhard, *Elliptische Functionen*, Mit zusatzen herausgegeben von Hermann Stahl ... Leipzig, B. G. Teubner, 1899.
14. Schuler, Max & Gebelein, H., *Eight and Nine Place Tables of Elliptical Functions based on Jacobi Parameter q* , with an English text by Lauritz S. Larsen, Berlin, Springer-Verlag, 1955, XXIV+296 pp.
15. Spenceley, G.W. & Spenceley, R.M., *Smithsonian Elliptic Functions Tables*, Washington, Smithsonian Institution 1947, Smithsonian miscellaneous collections v. 109.
16. Sturm, Charles François, *Cours d'Analyse de l'Ecole Polytechnique*, revu et corrigé par E. Prouhet et augmenté de la Théorie élémentaire des fonctions elliptiques, par H. Laurent, 14. ed., rev. et mise au courant du nouveau programme de la licence, par A. de Saint-Germain, Paris, Gauthier-Villars, 1909.
17. Tannery, Jules & Molk, Jules, *Eléments de la théorie des fonctions elliptiques*, Paris, Gauthier-Villars, Vol. 1-4, 1893-1902.
18. Tölke, Friedrich, *Praktische Funktionenlehre*, Berlin, Springer, Vol. I to VI ab. Vol. 3 and 4 deal with the elliptic functions of Jacobi.
19. Tricomi, Francesco Giacomo, *Elliptische Funktionen*, übers. und bearb. von Maximilian Krafft. Leipzig, Akademische Verlagsgesellschaft Geest & Portig, 1948, Mathematik und ihre Anwendungen in Physik und Technik, Bd. 20.
20. Whittaker, Edmund Taylor & Watson, G. N., *A Course of Modern Analysis*, an introduction to the general theory of infinite processes and of analytic functions, Cambridge, Eng., Univ. Pr., 1963, 606 pp., (1927).

1.9 Model of Finite Euclidean Geometry in Classical Euclidean Geometry.

1.9.0 Introduction.

The purpose of this section is to give an informal introduction to finite Euclidean geometry for those familiar with classical Euclidean geometry and analytic geometry.

The definitions of points and lines will be given in terms of equivalence classes. The Theorems will be derived from these definitions or can be derived from the classical Theorems. I will

restrict myself to the 2 dimensional case and will not attempt to give the most general results. In particular, I will assume that distances are defined in only one way.

In this restricted framework there is one finite geometry for each prime integer p . p is assumed to be larger than 2, non degenerate circles require p larger than 3. The examples correspond to small p . The reader is encouraged to think of the implications when p is very large, for instance of the order of 10^{32} say, and is looking at points with coordinates of the order of 10^8 to 10^{20} .

1.9.1 Points and lines in finite Euclidean geometry.

Notation.

A point P' in Euclidean geometry will be denoted by its cartesian coordinates $((x, y))$ given between double parenthesis. A line l' will be denoted by the coefficients $[[a, b, c]]$ of its equation

$$ax + by + c = 0,$$

given between double brackets. These coefficients are not unique. They can be replaced by

$$[[ka, kb, kc]]$$

where k is any real number different from 0.

For the points P and lines l in finite geometry, I will use the same notation with single parenthesis and single brackets.

Definition.

Given a prime p , if x is an integer, $x \bmod p$ denotes the smallest positive remainder of the division of x by p .

$$\text{For instance, } 28 \bmod 13 = 2, -5 \bmod 11 = 6.$$

We observe that if x and y are non negative integers less than p , for any integers l and m ,

$$x + lp \bmod p = x, y + mp \bmod p = y.$$

Definition.

Let x and y be integers. For any integers l and m , the points

$$((x + lp, y + mp))$$

are called *equivalent points*. A set of equivalent points is called a *point* (x, y) in finite geometry.

Let a, b, c be integers, a and b not both zero. For any integers l, m and n , the lines

$$[[k(a + lp), k(b + mp), k(c + np)]], k \neq 0,$$

are called *equivalent lines*. A set of equivalent lines is called a *line* in finite geometry.

If $P = (x + mp, y + np)$ is on $l = [a + k'p, b + m'p, c + n'p]$, then

$$(a + k'p)(x + mp) + (b + m'p)(y + np) + (c + n'p) = 0$$

and therefore

$$(ax + by + c) \bmod p = 0,$$

this is 1.9.1 below. This method of reducing modulo p allows us to extend many of the properties of Euclidean geometry to the finite case.

Example.

Let $p = 7$. The line $a = [[1, -1, -5]]$ is equivalent to the lines $a_0 = [[1, -1, -12]]$, $a_1 = [[1, -1, 2]]$, $a_2 = [[1, -1, 9]]$.

The line $b = [[1, 2, -17]]$ is equivalent to the lines $b_0 = [[1, 2, -3]]$, $b_1 = [[1, 2, -10]]$, $b_2 = [[1, 2, -24]]$, $b_3 = [[1, 2, -31]]$.

The intersection $P = ((9, 4))$ of a and b is equivalent to the points all labelled Q , $((2, 4))$, $((16, 4))$, $((2, 11))$, $((9, 11))$, $((16, 11))$. Only one of the points equivalent to P is in the domain

$$0 \leq x, y < p, \text{ namely } ((2, 4)).$$

\hat{y}																			
.	.	Qb2	Qb3	Qb4	.	.	.
.	a2	.	.	b2	.	.	.	a1	.	.	b3	.	.	.	a
a2	b2	a1	b3	a
.	b	a1	.	b2	a	.	b3	.	.	.
.	.	.	b	.	a1	b2	.	a	b3	.

.	.	.	.	a1	b	a	b2
b1	.	.	a1	.	.	.		b	.	.	a	.	.	.	b2	.	.	a0	.
.	.	Qb1	Pb	Qb2	.	.
.	a1	.	.	b1	.	.		.	a	.	.	b	.	.	.	a0	.	.	.
a1	b1		a	b	a0
.	b0	a		.	b1	a0	.	b	.	.	.
.	.	.	b0	.	a	b1	.	a0	b	.
$x >$																			

Equivalence of points and lines.

Fig.0a, $p = 7$.

In Fig.0a, I have not given those lines which are equivalent to a but have a different slope, if R is any point on such a line which is in the lower right square it is either Q or a point labelled a or a_1 .

In finite geometry, we do not distinguish points labelled a_1 from those labelled a or the points labelled b_0 and b_1 from those labelled b . We have therefore Fig.0b below.

.	.	.	.	a	b	.	
b	.	.	a	.	.	.	
.	.	Qb	
.	a	.	.	b	.	.	
a	b	
.	b	a	
.	.	.	b	.	a	.	
							x >

Points and lines in finite Euclidean geometry.

Fig.0b, $p = 7$.

The point $Q = (2, 4)$ is on the lines $a = [1, 6, 2] = [4, 3, 1]$ and $b = [1, 2, 4] = [2, 4, 1]$ in the finite Euclidean geometry associated with $p = 7$.

Observe that from one point on a , the others are obtained by moving one to the right and one up, for b , we move 2 to the right and one down. Observe also what happens at the boundary using, if needed Fig. 0a.

If we attempt to use the equivalence method when p is not a prime, the situation for 6 points is typical. If $a = [[1, 1, -5]]$, $b = [[1, 3, 1]]$ and $c = [[1, 3, 4]]$, the points $P = ((2, 3))$ and $Q = ((5, 0))$ are both on the lines a and b , while the lines a and c or their equivalent have no point in common with coordinates reduced modulo 6.

$p = 7,$													
i	0	1	2	3	4	5	6						
$p\ i$	0	7	14	21	28	35	42						
$\frac{1}{i}$	—	1	4	5	2	3	6						
i^2	0	1	4	2	2	4	1						
$p = 11,$													
i	0	1	2	3	4	5	6	7	8	9	10		
$p\ i$	0	11	22	33	44	55	66	77	88	99	110		
$\frac{1}{i}$	—	1	6	4	3	9	2	8	7	5	10		
i^2	0	1	4	9	5	3	3	5	9	4	1		
$p = 13,$													
i	0	1	2	3	4	5	6	7	8	9	10	11	12
$p\ i$													
$\frac{1}{i}$													
i^2													
$p = 17,$													
i	0	1	2	3	4	5	6	7	8	9	10	11	12
$p\ i$													
$\frac{1}{i}$													
i^2													
i	13	14	15	16									
$p\ i$													
$\frac{1}{i}$													
i^2													
$p = 19,$													
i	0	1	2	3	4	5	6	7	8	9	10	11	12
$p\ i$													
$\frac{1}{i}$													
i^2													
i	13	14	15	16	17	18							
$p\ i$													
$\frac{1}{i}$													
i^2													

Theorem.

A point (x, y) is on a line $[a, b, c]$ if and only if
 $(ax + by + c) \bmod p = 0$.

For instance, with $p = 11$, from $((12, 14))$ on the line $[[16, -10, 4]]$, it follows that
 $(1, 2)$ is on line $[5, 1, 4]$ or $[4, 3, 1]$.

Theorem.

There are p^2 points and $p^2 + p$ lines.

Theorem.

2 distinct points determine a unique line.

Moreover, if $A = (A_0, A_1)$ and $B = (B_0, B_1)$, the line a through A and B is $a = [A_1 - B_1, B_0 - A_0, A_0B_1 - B_0A_1]$.

For instance, for $p = 11$, if $A = (9, 8)$ and $B = (8, 6)$, $a = [2, 10, 1]$.

Theorem.

2 distinct lines have at most one point in common.

Moreover, if $l = [l_0, l_1, l_2]$ and $m = [m_0, m_1, m_2]$, let $d := l_0m_1 - l_1m_0$, if d is different from 0, then the point P common to l and m is

$$P = \left(\frac{l_1m_2 - l_2m_1}{d}, \frac{l_2m_0 - l_0m_2}{d} \right).$$

For instance, with $p = 11$, if $l = [2, 10, 1]$ and $m = [9, 9, 1]$, $d = 5$,
 $\frac{1}{5} \bmod 11 = 9$, $P = (1 \cdot 9, 7 \cdot 9) = (9, 8)$.

Definition.

If 2 lines have no points in common, they are called *parallel*.

This will occur if $d = 0$, because of 1.9.1.

For instance, with $p = 11$, $a = [2, 10, 1]$ is parallel to $b = [5, 3, 1]$.

The following figure gives also a representation of points in finite geometry. The representative which is chosen is that with integer coordinates, non negative and less than p ($0 \leq x, y < p$).

The reader is asked to ignore for now the information at the left of the figure. The possible points are indicated with “.”, a named point has its name just to the right of it. All points on a line a are indicated by replacing “.” by “ a ”. If 2 lines have a point in common, one of the 2 lines is chosen. The other could be indicated by the reader, if he so desires.

Comment.

If p is very large, and the unit used for the representation is very small, the Angström = 10^{-8} cm, say, the points on a line will appear as we imagine them in the classical case. But it is clear that they are not connected. Connectedness is a property in classical Euclidean geometry, which has no counterpart in the finite case. Moreover, the finite case should, when fully understood, give a better model for a world which is atomic, whatever the smallest particle is and which is finite, whatever the size of the universe is.

1.9.2 Parallels, parallelograms, distance.**Introduction.**

Parallels have been defined in 1.9.1. In this section, I will give properties of parallel lines and define parallelograms. It is appropriate at this stage to define distances between points. In the finite case, the square of a distance is the appropriate basic concept, if we do not want to introduce “imaginaries”. Properties of the parallelogram allow us then to derive a construction for the mid-point of a segment. The barycenter will be define in section 1.9.4.

Theorem.

Given a line l and a point P not on l , there exists a unique line m through P parallel to l . Moreover, if $P = (P_0, P_1)$ and $l = [l_0, l_1, l_2]$ then

$$m = [l_0, l_1, -(P_0 l_0 + P_1 l_1)],$$
Definition.

Given 3 points A, B, C not on the same line, let c be the line through C parallel to the line a through A and B , let d be the line through A parallel to the line b through B and C , $\{A, B, C, D\}$ is called a *parallelogram*. The lines $A \times C$ and $B \times D$ are called *diagonals*, their intersection is called the *center* of the parallelogram.

Comment.

In Euclidean geometry, opposites sides of a parallelogram are equal. To generalize, I observe first, that distances in Euclidean geometry are always considered positive. This is consistent with the distance of AB equal to the distance of BA . But when working modulo p , we cannot introduce positive numbers, keeping the requirement that the product and sum of positive integers modulo p is positive. Also not every integer modulo p has a square root hence we use the square of the distance instead. To use a terminology reminiscent of that used in Euclid's time, I will say the square on AB , for the square of the distance between A and B .

Definition.

Given 2 points $A = (A_0, A_1)$ and $B = (B_0, B_1)$, the *square on AB* , denoted $(AB)^2$ is

$$(B_0 - A_0)^2 + (B_1 - A_1)^2 \text{ mod } p.$$

For instance, for $p = 19$, if $A = (8, 11)$, $B = (12, 9)$, the square on AB is $(AB)^2 = (16 + 4) \pmod{19} = 1$. But, for $p = 13$, the square on AB , where $A = (1, 2)$ and $B = (2, 7)$ is $(1 + 25) \pmod{13} = 0$, therefore the square can be zero for distinct points A and B . See 1.9.5.

Definition.

2 segments $\{AC\}$ and $\{BD\}$ are equal if the square on AC equals the square on BD . I write $AC = BD$.

For instance, with $p = 19$, if $A = (7, 11)$, $B = (11, 9)$, $C = (9, 7)$ and $D = (9, 13)$ then $(AC)^2 = 1$, $(BD)^2 = 1$, $(AB)^2 = 1$, $(CD)^2 = 17$. Therefore $AC = BD$.

Definition.

A point M on the line through A and C such that the square on AM is equal to the square on CM is called the *mid-point* of AC .

Theorem.

In a parallelogram $\{A, B, C, D\}$ with $A \times B$ parallel to $C \times D$ and $A \times D$ parallel to $B \times C$, the square on AB is equal to the square on CD , the square on AD is equal to the square on BC . The center M is the midpoint of the diagonals $A \times C$ and $B \times D$.

Moreover, if $A = (A_0, A_1)$, $B = (A_0 + B_0, A_1 + B_1)$, $D = (A_0 + C_0, A_1 + C_1)$, then $C = (A_0 + B_0 + C_0, A_1 + B_1 + C_1)$, $M = (A_0 + \frac{B_0+C_0}{2}, A_1 + \frac{B_1+C_1}{2})$,
 $(AB)^2 = (CD)^2 = B_0^2 + B_1^2$, $(AD)^2 = (BC)^2 = C_0^2 + C_1^2$,
 $(AM)^2 = (MC)^2 = \frac{1}{4}((B_0 + C_0)^2 + (B_1 + C_1)^2)$.

Example.

The given points are $A = (7, 11)$, $B = (9, 13)$, $C = (11, 9)$, $D = (9, 7)$, $M = (9, 10)$.
 $(AB)^2 = (CD)^2 = 1$, $(AD)^2 = (BC)^2 = 8$. $(AM)^2 = (MC)^2 = 5$, $(BM)^2 = (MD)^2 = 9$.

For instance, with $p = 11$, $l = [9, 1, 1]$ and $m = [1, 5, 1]$ are perpendicular to $a = [6, 1, 1]$ and are parallel.

Theorem.

Given a triangle A, B, C with sides a, b and c , if p is the perpendicular from A to a , q is the perpendicular from B to b and r the perpendicular from C to c , then the three lines p, q and r have a point H in common.

Definition.

The lines p, q and r of Theorem 1.9.3 are called altitudes, the point H is called the *orthocenter* of the triangle $\{A, B, C\}$.

Example.

The given points are $A = (8, 4)$, $B = (4, 8)$, $C = (3, 2)$, the sides are $a = [1, 9, 1]$, $b = [6, 7, 1]$, $c = [10, 10, 1]$, the altitudes are $p = [1, 6, 1]$, $q = [2, 3, 1]$, $r = [10, 1, 1]$ and the orthocenter is $H = (7, 6)$.

As an exercise, indicate on the figure one of the sides and compare how points are derived from each other with those of the perpendicular line, c and r are the easiest, b and q the more difficult.

$r' \bmod 19 = -1$, $60 \bmod 19 = 3$, $45 \bmod 19 = 7$, $21 \bmod 19 = 2$, $72 \bmod 19 = -4$.
 Appropriate change of signs give the other points, for instance $((-60, 45))$
 corresponds to $(-3, -7)$ is also on C' .

We can also replace in the Theorem just quoted the radius r' by the radius square $r'_2 = r'^2$.

The following solutions are especially attractive, because the points on the circle in the Euclidian plane are also the representatives in the finite Euclidean plane.

p	r'_2	points
5	1	(0, 1)
5	2	(1, 1)
5	3	(2, 2)
5	4	(0, 2)
7	5	(1, 2)
7	13	(2, 3)
11	25	(0, 5), (3, 4)
13	25	(0, 5), (3, 4)
17	65	(1, 8), (4, 7)

Definition.

Given a point A and an integer d , the points P such that the square on PA is equal to d are on a *circle of center A and radius square d* .

Notation.

From here on, it is often more convenient to have the origin at the center of the figure. We will then replace the condition

$$0 \leq x, y, a, b, c < p$$

by

$$-\frac{p}{2} < x, y, a, b, c < \frac{p}{2}.$$

Theorem.

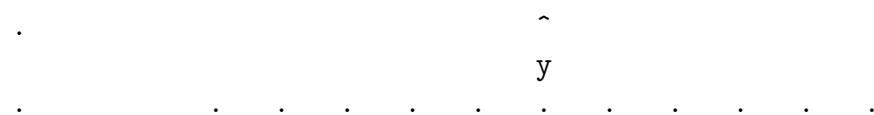
For a circle centered at the origin,

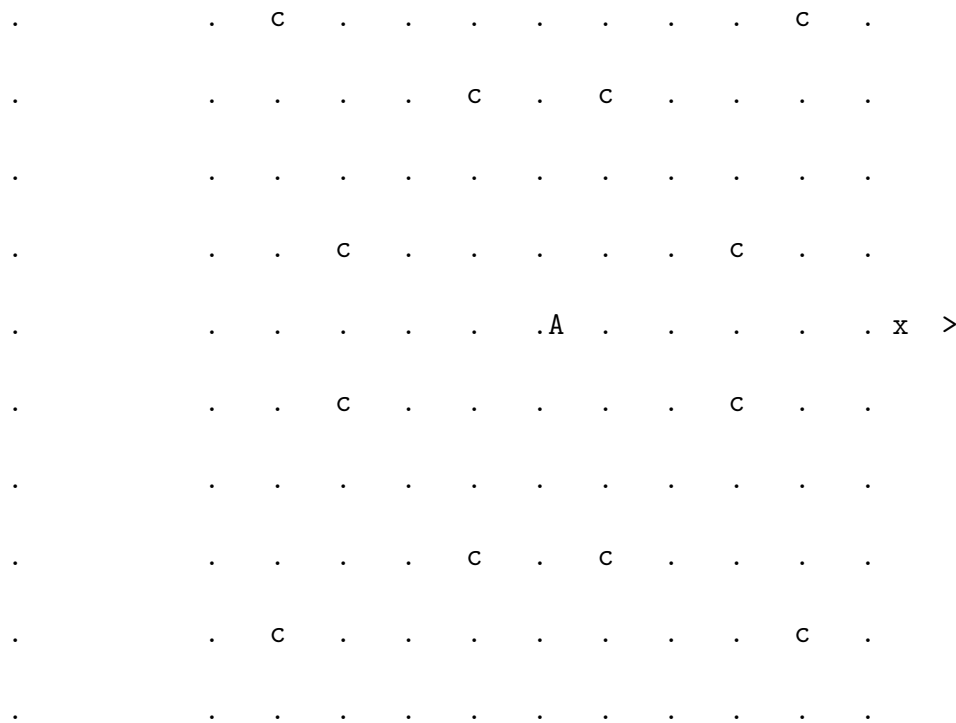
if $(x, 0)$ ($x \neq 0$) is a point, so are $(-x, 0)$, $(0, x)$, $(0, -x)$,

if (x, x) ($x \neq 0$) is a point, so are $(x, -x)$, $(-x, x)$, $(-x, -x)$,

if (x, y) is a point ($x \neq y$, both non zero), so are (y, x) , $(-x, y)$, $(y, -x)$, $(x, -y)$, $(-y, x)$, $(-x, -y)$, $(-y, -x)$.

Example.





Circle of center A . Fig. 4, $p = 11$.

$A = (0, 0)$, the points labelled c are on a circle with center A and with radius square 10. The line $[0, 1, 0]$ through A has no point in common with the circle, the line $[1, -3, 0]$ has 2 points in common with the circle, $(3, 1)$ and $(3, -1)$, the line $[1, -1, 0]$ has also 2 points in common with the circle, $(4, 4)$ and $(-4, -4)$.

Exercise.

Indicate on the Fig. 4 by r the points on a circle with radius square 3.

Theorem.

If $p+1$ is divisible by 4, there are $p+1$ points on the circle. Otherwise, there are $p-1$ points on the circle.

Definition.

If a line t through a point P on a circle has no other points in common with the circle, it is called a *tangent* to the circle.

Theorem.

If a line l through a point P of a circle is not tangent to it, it intersects the circle at an other point Q .

Definition.

A line through the center of a circle is called a *diameter*.

Theorem.

Half of the diameters have 2 points in common with the circle, half of them of no points in common with the circle.

Theorem.

The tangent at a point A of a circle is perpendicular to the diameter passing through A .

Example.

Given the point $A = (6, 6)$ and the radius square 5, the points labeled c are on the circle centered at A . The tangent t at $P = (4, 7)$ is $[9, 1, 1]$. The point $C = (2, 3)$ is on the tangent. The line $d = [3, 6, 1]$ is a diameter through P .

Definition.

The point G of 1.9.4 is called the *barycenter* of the triangle.

Definition.

The *anti-complementary triangle* $\{D, E, F\}$ has its side $E \times F$ through A parallel to $B \times C$, and similarly for E and F .

Theorem.

The mid-points M, N, O of the sides of the triangle $\{A, B, C\}$ are also the mid-points of $\{AD\}$, $\{BE\}$ and $\{CF\}$.

Example.

```
.Da      ^
          y
.         . . . o m n . . . . .
.         . . . n . . o . . . . . m . . . .
o         . n . . . m . . . o . . . . .
.         . . . . . . . . . o . . m . . n
.         . . . . . mA . . . . . oFnE .
.Dc      . . . . . . . . . n . m . o
.         . . o . . . m . . . n . . . .
.         . . . . . oO . . . nN . . . m .
.         . . . . . oG . . . . .
m         . . . . . n . . . o . . . . m
.         . . . nB . . . mM . . . oC . . .
.         m . n . . . . . . . . o .
.         n o . . . . . m . . . . .
.Db      . m . . o . . . . . n .
.         . . . . . o . . m . . n . .
.         . m . . . . . o . . n . . .
n         . . . . . n mDo . . . .
.         . . m . . . . n . . . . o .
.         o . . . . . n . . . . m . . . . x >
```

Medians and barycenter. Fig. 6a, $p = 19$.

The given points are $A = (6, 14)$, $B = (4, 8)$, $C = (14, 8)$.

The anti-complementary points are $D = (12, 2)$, $E = (16, 14)$, $F = (15, 14)$.

The mid-points are $M = (12, 2)$, $N = (15, 14)$, $O = (16, 14)$.

The medians are $m = [16, 8, 1]$, $n = [8, 3, 1]$, $o = [13, 1, 0]$. The barycenter is $G = (8, 10)$.

Exercise.

Indicate on Fig. 6a, the line $F \times D$ through 2 mid-points and observe that $F \times D$ is parallel to $C \times A$.

Definition.

The *mediatrix* of AB is the line through the mid-point of AB perpendicular to $A \times B$.

Theorem.

The mediatrices of the sides of a triangle pass through the center of the circumcircle of the triangle.

Example.

```
.Da$      ^
          y
.         . q . r . . c . . p . . c . . . . .
.         . . . . . q r . . p . . . . .
rDr       . . . . . . . . . rZ. . . . .
qDq       . . . . . . . . . p . . r q . . . . .
.         . . . . . . cA. . p . . c . . rF.Eq .
.Dc       . . q . . . . . c . p . c . . . . . r
.         . . r . . . c q . . p . . . c . . . . .
.         . c . . . . r0. . . p qN. . . . . c .
.         . . . . . . . . . r p . . . . q . . . .
.         . . . . . . . . . p . r . . . . . q
.         . . . . q cB. . . . pM. . . . cC. . . .
.         . . . . . . . q . p . . . . . r .
.         . r . . . . . . . p . q . . . . .
.Db       . . . . c . . . . . p . . . . c q . . .
.         q . . . . . . . r . p . . . . .
.         . . . . q . . . . . p r . . . . .
.         . c . . . . . . . q p . . .Dr . . . c .
.         . . . . . c . . . . p . . q c . . r . .
pDp       r . . . . . . c . p . c . . . . q . .      x >
```

Mediatrices and center of circumcircle. Fig. 6b, $p = 19$.

The given points are the same as in Example 1.9.4. The mediatrices $p = [2, 0, 1]$, $q = [13, 14, 1]$, $r = [13, 1, 0]$ pass through the center $Z = (9, 16)$ of the circumcircle \mathcal{C} of the triangle $\{A, B, C\}$.

Exercise.

Determine the radius square of the circle and check that $(AZ)^2 = (BZ)^2 = (CZ)^2$.
Check that if Y is some point on q , $(AY)^2 = (CY)^2$.

Theorem.

If A, B, C and D are points on a circle and AB is parallel to CD then the square on AC equals the square on BD and the square on AD equals the square on BC .

1.9.5 The ideal line, the isotropic points and the isotropic lines.**Introduction.**

It is now time to explain the points located at the left of each figure. In classical geometry, the plane can be extended to contain elements which are not points but have similar properties. For instance, all lines which are parallel to a given line l have no points in common, but they all have the same direction. A direction is also called a point at infinity or an ideal point. If we extend the Euclidean plane in this way we see that 2 points ideal or not determine a unique line, with the exception of 2 ideal points. To have no exceptions, we also introduce the line at infinity or ideal line, which contains all ideal points. This extended Euclidean plane, which is unfortunately not part of high school education, is a first step to the understanding of projective geometry. Other notions which are known to those familiar with complex Euclidean geometry are the isotropic points, the isotropic lines and their properties. These notions also extend to the finite case and, with the definition of distance used, give rise to real points when the prime is of the form $4k + 1$. The distance between points which are not both ordinary is not defined.

To represent points we will now use, as for lines, 3 coordinates, not all 0, and (x, y, z) will not be considered distinct from (kx, ky, kz) , $k \neq 0$.
The ordinary points (x, y) will also be noted $(x, y, 1)$ or (kx, ky, k) .

Definition.

The *ideal line* is the line $[0, 0, 1]$, the *ideal points* or *directions* are the points $(P_0, P_1, 0)$.

Definition.

A point $P = (P_0, P_1, P_2)$ is on a line $l = [l_0, l_1, l_2]$ if
 $P_0l_0 + P_1l_1 + P_2l_2 \pmod p = 0$.

Theorem.

All $p + 1$ ideal points are on the ideal line. There are $p^2 + p + 1$ ordinary and ideal points and $p^2 + p + 1$ ordinary and ideal lines.

Theorem.

If 2 lines l and m are parallel, they have an ideal point in common or have the same direction.

Moreover, if $l = [l_0, l_1, l_2]$ this point is $D_l = (l_1, -l_0, 0)$ and if $m = [m_0, m_1, m_2]$, then $d := l_0 m_1 - l_1 m_0 = 0$.

Definition.

If 2 lines l and m are perpendicular, their ideal points or directions are said to be perpendicular.

Moreover, if the direction of l is $D_l = (l_1, -l_0, 0)$, that of m is $D_m = (l_0, l_1, 0)$.

Comment.

The ideal points are represented to the left of the figures. $(1,0,0)$ is at the top the other points are from the bottom up $(0,1,0)$, $(1,1,0)$, $(2,1,0)$, $(3,1,0)$, ...

Example.

In Fig. 1, the point $D_a = (2, 1, 0)$ is the ideal point on $a = [10, 2, 1]$, and $c = [3, 5, 1]$, the point $D_b = (10, 1, 0)$ is the ideal point on $b = [9, 9, 1]$ and d .

In Fig. 2, the points $D_a = (1, 1, 0)$, $D_b = (9, 1, 0)$, $D_f = (17, 1, 0)$, $D_m = (10, 1, 0)$ are respectively the ideal points on $a = [5, 14, 1]$, $b = [3, 11, 1]$, $f = [17, 15, 1]$, $m = [14, 12, 1]$. m is the mediatrix of AC .

In Fig. 3, $D_a = (2, 1, 0)$ and $D_p = (5, 1, 0)$, $D_b = (8, 1, 0)$ and $D_q = (4, 1, 0)$, $D_c = (10, 1, 0)$ and $D_r = (1, 1, 0)$ are the direction of pairs of perpendicular lines.

In Fig. 5, $D_d = (9, 1, 0)$ is the direction of the diameter $d = [3, 6, 1]$. $D_t = [6, 1, 0]$ is the direction perpendicular to Dd and of the tangent $t = [9, 1, 1]$.

Definition.

The isotropic points are the ideal points $(i, 0, 1)$ and $(-i, 0, 1)$ where i is a solution of $i^2 + 1 = 0$.

Theorem.

The isotropic points exist if p is of the form $4k + 1$ (or p is congruent to 4 modulo 1), they do not, otherwise.

The proof of this result goes back to Euler.

For instance, if $p = 5$, $i = 2$, if $p = 13$, $i = 5$, if $p = 17$, $i = 4$.

Definition.

In the extended Euclidean plane, (X_0, X_1, X_2) is on the circle with center (C_0, C_1, C_2) and radius square R_2 if

$$0. (X_0 - C_0 X_2)^2 + (X_1 - C_1 X_2)^2 = R_2 X_2^2.$$

If $X_2 = 1$, we obtain the usual equation.

Theorem.

When the isotropic points exist, they are on each of the circles.

Indeed, if $X_0 = i$, $X_1 = 1$ and $X_2 = 0$, 1.9.50 becomes $i^2 + 1 = 0$.

Definition.

The *isotropic lines* are any ordinary line passing through an isotropic point.

Theorem.

The isotropic lines are perpendicular to themselves.

Theorem.

The isotropic lines through the center of a circle are tangent to that circle at the isotropic point.

Theorem.

If A and B are ordinary points on the same isotropic line, the square on AB is 0.

Indeed, if $A = (A_0, A_1, 1)$ and $B = (B_0, B_1, 1)$, the line $A \times B$ which is $[A_1 - B_1, B_0 - A_0, A_0B_1 - A_1B_0]$ passes through $(i, 1, 0)$ if

$$(A_1 - B_1)i = A_0 - B_0.$$

But the square on AB is $(A_0 - B_0)^2 + (A_1 - B_1)^2 = (A_1 - B_1)^2(i^2 + 1) = 0$.

Comment.

Because of 1.9.5, when p is congruent to 1 modulo 4, it is possible for the square on AB to be 0 for distinct points A and B .

Example.

The circle \mathcal{C} of center $A = (8, 8)$ passes through $P = (4, 10)$ and through the isotropic points $J = (4, 1, 0)$ and $K = (13, 1, 0)$. The isotropic lines through A are $j = [5, 14, 1]$ and $k = [14, 5, 1]$.

Theorem.

The square on $A_j A_j + 1$ is equal to the square on $A_0 A_1$.

The proof for $j = 1$ is as follows, let $C = (0, 0)$, $A_0 = (r, 0)$ and $A_q = (-r, 0)$ and $A_j = (x_j, y_j)$, the square on $A_0 A_1$ is

$$(x_1 - r)^2 + y_1^2 = 2r(r - x_1),$$

$$A_0 \times A_2 = [-y_2, x_2 - r, ry_2], \quad A_q \times A_2 = [-y_2, x_2 + r, -ry_2],$$

$$C \times A_1 = [y_1, -x_1, 0],$$

parallelism requires

$$0. \quad y_1(x_2 + r) - x_1 y_2 = 0,$$

perpendicularity requires

$$1. \quad y_1 y_2 + x_1(x_2 - r) = 0,$$

therefore,

$$\begin{aligned} (A_1 A_2)^2 &= (x_2 - x_1)^2 + (y_2 - y_1)^2 = \\ 2(r^2 - x_1 x_2 - y_1 y_2) &= 2r(r - x_1) = (a_0 A_1)^2, \end{aligned}$$

because of 1. Multiplying 0, by $x_1(x_2 - r)$ and 1, by $y_1(x_2 + r)$ and subtracting gives

$$x_1 y_1(x_2 + r)(x_2 - r) = x_1 y_2 y_1 y_2$$

or because $x_1 y_1$ is different from 0,

$$2. \quad x_2^2 + y_2^2 = r^2.$$

A_2 is therefore on the circle.

Theorem.

Given the construction 1.9.6,

$$0. \quad (A_j A_j + k)^2 = (A_0 A_k)^2,$$

$$1. \quad (j + m - k - l) \pmod{2q} = 0 \text{ implies } A_j \times A_k \text{ is parallel to } A_l \times A_m.$$

Definition.

Assume that the construction 1.9.6 gives all $2q$ points of the circle, let the direction of $A_q A_j$ be I_j and that of the tangent at A_q be I_q , the set I_0, I_1, \dots, I_{2q} define a *scale* on the ideal line.

Definition.

Let the lines l, m , have directions I_l, I_m , the *angle between* l and m is given by $(m - l) \pmod{2q}$.

Theorem.

The sum of the angles of a triangle is $0 \pmod{2q}$.

Indeed, if the directions of the sides a, b, c are I_a, I_b, I_c , the angles are $(c - b) \pmod{2q}$, $(a - c) \pmod{2q}$ and $(b - a) \pmod{2q}$.

Theorem.

If 2 angles of a triangle are even, the third angle is even.

Definition.

A triangle is called *even* if 2 of its angles and therefore all its angles are even.

Example.

The points $A_0 = (10, 5)$, $A_1 = (1, 2)$, $A_2 = (2, 1)$, $A_3 = (5, 10)$, $A_4 = (8, 1)$, $A_5 = (9, 2)$, $A_6 = (0, 5)$, $A_7 = (9, 8)$, $A_8 = (8, 9)$, $A_9 = (5, 0)$, $A_a = (2, 9)$, $A_b = (1, 8)$ are on a circle centered at C with radius square 3. These points have been obtained from A_0, A_1 and A_6 by the construction 1.9.6

The angles can be determined using the scale defined by the ideal points $I_0 = (1, 0, 0)$, $I_1 = (7, 1, 0)$, $I_2 = (5, 1, 0)$, $I_3 = (1, 1, 0)$, $I_4 = (9, 1, 0)$, $I_5 = (8, 1, 0)$, $I_6 = (0, 1, 0)$, $I_7 = (3, 1, 0)$, $I_8 = (2, 1, 0)$, $I_9 = (10, 1, 0)$, $I_a = (6, 1, 0)$, $I_b = (4, 1, 0)$. If $i + l = j + k$ then $A(i)A(j)$ is parallel to $A(k)A(l)$, for instance, b or A_8A_7 is parallel to c or A_9A_6 .

Exercise.

Theorem.

Definition.

Theorem.

More precisely, if the 3 bisectrices d, e, f , which pass respectively Through A_0, A_1, A_2 , are such that

0. $(\text{angle}(d, a) + \text{angle}(e, b) + \text{angle}(f, c)) \pmod{2q} = q$
 then
 d, e and f have a point in common.

Definition.

The 4 points C_0, C_1, C_2, C_3 are called *center of the tangent circles*.

Theorem.

There exist a circle with center C_i tangent to each of the sides of the triangle.

Example.

```

      ^
      y
.      r . c . . . . .B0 . . . a . . . r
c      . . . . .cA1 . . . . . . . . .
.      . . . . . c . . . . . a . . .
r      . . . . . a . . . c . . . . .
.      . .B1 . . . . . c . . . a . .
.      . . . . . r a . . . . r c . . .
.      . . . . . r . . . . r . . c a .
.      . . . . . a . . . . . . . cA0
a      . c . . . . . . . . . . a      x >
.      . . . c . . . . a . . . . . .B2
.      a . . . . c . . . . . . . . .
.      r . . . . . c . a . . . . . r
r      . aA2 . . . . r . c . . . . .
.      . . . . . r . . . a c . . . .
.      . a . . . . . .I. . . . c . . .
.      . . . . . r . . . r a . . . c .
.      c . . a . . . r . r . . . . .

```

Bisectrices and inscribed circle. Fig.9, $p = 17$.

The given triangle is $A_0 = (8, 1, 1)$, $A_1 = (-4, 7, 1)$, $A_2 = (-7, -4)$. Its sides are $a = [2, 1, 1]$, $b = [-7, 4, 1]$, $c = [5, -7, 1]$. The bisectrices meet the circle at $B_0 = (-1, 8)$, $B_1 = (-7, 4)$, $B_2 = (8, -1)$. They are $d = [8, 3, 1]$, $e = [-3, 3, 1]$, $f = [-4, 3, 1]$ and have the point $I = (0, -6)$ in common. The tangent circle r has radius square 5. Its points of contact with a , b , c are respectively $(2, -5)$, $(-3, 3)$, $(1, -4)$. Only a and c are given on the Figure, not to clutter it. The other centers of tangent circles are $(-1, 4)$, $(3, -3)$ and $(-2, 5)$.

Exercise.

Determine that b is tangent to the circle r and that $(-1, 4)$ is indeed a center of a tangent circle.

1.9.7 Finite trigonometry.

Definition.

If $r = 1$ and the construction 1.9.6 gives all $2q$ points $A_j = (x_j, y_j)$ of the circle with radius square 1. I define

$$\sin(2j) := y_j, \cos(2j) := x_j.$$

Comment.

Because, in general, several points A_1 can be chosen, there are several distinct but related trigonometric functions sine and cosine. Each corresponds to a different choice of the unit angle. This is similar to the real case in which many different units are used, those with angles in radians, degrees, grades, for instance.

Comment.

I will develop the properties of the trigonometric functions and obtain functions which can be considered as an analogue of the hyperbolic functions. An efficient method to obtain them for large p will also be given.

Example.

For $p = 11$,

i	A_i	$angle(i) - 180i$	A'_i
1	$(-4, -3)$	$36^\circ 87$	$((-4, -3))$
2	$(-3, -4)$	$73^\circ 74$	$((\frac{7}{5}, \frac{24}{5}))$
3	$(0, 5)$	$110^\circ 61$	$((\frac{44}{25}, -\frac{117}{25}))$
4	$(3, -4)$	$147^\circ 48$	$((-\frac{527}{125}, \frac{336}{125}))$
5	$(4, -3)$	$184^\circ 35$	$((\frac{3116}{625}, \frac{237}{625}))$
6	$(-5, 0)$	$221^\circ 22$	$((-\frac{11753}{3125}, -\frac{10296}{3125}))$

If $A_i = (-4, -3)$, then $4^2 + 3^2 = 5^2$, $\cos(i) = -\frac{4}{5} = -3$ and $\sin(i) = -\frac{3}{5} = -5$.

For $p = 13$,

i	A_i	$angle(i) - 180i$	A'_i
1	$(-3, -4)$	$53^\circ 13$	$((-3, -4))$
2	$(-4, -3)$	$106^\circ 26$	$((-\frac{7}{5}, \frac{24}{5}))$
3	$(0, 5)$	$159^\circ 39$	$((\frac{117}{25}, -\frac{44}{25}))$
4	$(4, -3)$	$212^\circ 52$	$((-\frac{527}{125}, -\frac{336}{125}))$
5	$(3, -4)$	$265^\circ 65$	$((\frac{237}{625}, \frac{3116}{625}))$
6	$(-5, 0)$	$318^\circ 78$	$((\frac{11753}{3125}, -\frac{10296}{3125}))$

For $p = 17$,

i	A_i	$angle(i) - 180i$	A'_i
-1	$(8, 1)$	$-7^\circ 125$	$((8, 1))$
1	$(8, -1)$	$7^\circ 250$	$((8, -1))$
3	$(-4, 7)$	$21^\circ 375$	$((\frac{488}{64}, -\frac{191}{65}))$
5	$(7, -4)$	$35^\circ 625$	$((\frac{27688}{4225}, -\frac{19841}{4225}))$
7	$(-1, 8)$	$49^\circ 875$	$((\frac{1426888}{274625}, -\frac{1692991}{274625}))$

9

11

13

15

Exercise.

Continue the last table obtaining the missing values.

Exercise.

Obtain trigonometric functions for $p = 11$ and check the familiar identities

$$0. \sin^2(x) + \cos^2(y) = 1,$$

$$1. \sin(x + y) = \sin(x)\cos(y) + \sin(y)\cos(x),$$

$$2. \cos(x + y) = \cos(x)\cos(y) - \sin(x)\sin(y),$$

Notation.

In a finite field there is no ambiguity in defining $\pi := 2q$.

1.10 Axiomatic

1.10.0 Introduction to Axiomatic.

The axiomatic study of Geometry has a long history, starting with Euclid. Among the main earlier contributors are Giovanni Saccheri (1667-1733), Karl Gauss (1777-1855), Janos Bolyai (1802-1860), Nikolai Ivanovich Lobachevsky (1792-1856), de Tilly (1837-1906)¹⁷, Pieri, Carl Menger, Oswald Veblen (1880-1960), William Young (1863-1942), Julius Dedekind, Frederigo Enriques (1871-1946), I. Schur, David Hilbert (1862-1943), Marshall Hall and Alfred Tarski (1901-1983).

To obtain a clear understanding of the relation between the synthetic and the algebraic point of view, an important step was the realization of the connection between the Axiom of Pappus and the commutativity of multiplication, first considered by Schur, in 1898, then by Hilbert in 1899 (p. 71), by Artin in 1957 and many others, see Artzy (1965), Hartshorne (1967).

A detailed history of the developments concerning Finite Geometry can be obtained from the monumental work of Dembowsky, 1968 and Pickert (Chapter 12).

For some authors, the word projective geometry as moved away from its original meaning, to become a synonym of incidence geometry. I will not follow that practice.

What follows can be used to obtain a justification of the relation between the synthetic and algebraic axioms of Chapter II. With the exception of the proof of associativity and commutativity of addition, I have borrowed heavily from Artzy's book, which contains proofs not given here, increasing the formalism to prepare for eventual computarization.

The axioms will progress from those of the perspective plane, with $(\Sigma, +, \cdot)$ a ternary ring, $(A * B * C)$ and $(\Sigma, +)$, $(\Sigma - \{0\}, \cdot)$ are

⁰G19.TEX [MPAP], September 9, 2019

¹⁷Blumenthal considers than in the paper of 1892, de Tilly makes a fundamental contribution by introducing n-point relations to characterize a space metrically.

loops,

to Veblen-Wedderburn plane, with $(\Sigma, +, \cdot)$ a quasifield, (linear, right distributivity) and $(\Sigma, +)$ an Abelian group,

to Moufang plane, with $(\Sigma, +, \cdot)$ an alternative division ring (left distributivity, right and left inverse property),

to Desarguesian plane, with $(\Sigma, +, \cdot)$ a skew field, (associativity of multiplication),

to Pappian plane, with $(\Sigma, +, \cdot)$ a field, (commutativity of multiplication),

to Separable Pappian plane, with $(\Sigma, +, \cdot)$ an ordered field,

to Continuous Pappian plane with $(\Sigma, +, \cdot)$ the field of reals.

The definitions of Desargues and Pappus configurations, given in Chapter II, will not be repeated here.

1.10.1 The Perspective Plane.

Introduction.

Marshall Hall and D.T. Perkins independently succeeded to construct an algebraic structure, called ternary ring, 1.10.1 to coordinatize 1.10.1 the perspective plane. Theorem 1.10.1 shows that the first 4 conditions of the definition of a ternary ring are associated with the incidence property 1.10.1.3 and the others with Theorem 1.10.1. Theorem 1.10.1 proves that the set of the ternary ring is a loop under addition and multiplication.

Axioms. [Of Allignment]

Given a set of elements called *points* and a set of elements called *lines* with the relation of *incidence*, such that

0. 2 points are incident to one and only one line.
1. 2 lines are incident to one and only one point.
2. there exists at least 4 points, any 3 of which are not collinear,

we say that the *axioms of allignment* are satisfied.

The terminology is that of Seidenberg, 1962, p. 56.

Definition.

A *perspective plane* is a set of points and lines satisfying the axioms of alignment. It is also called a *rudimentary projective plane*. (Artzy, p. 201.)

Theorem.

Duality is satisfied in a perspective plane.

Menger gives a self dual set of equivalent axioms.

Definition.

Given a point P and 2 lines a and b not incident to P , a *perspectivity* $\Pi(P, a, b)$ is the correspondance between $A_i \iota a$ and $B_i \iota b$, with $B_i := (P \times A_i) \times b$.

$\Pi^{-1}(P, a, b) := \Pi(P, b, a)$ is the inverse correspondance which associates to B_i , $A_i = (P \times B_i) \times a$.

I will also use the notation $\Pi(P, A_i, B_i)$.

A *projectivity* is a perspectivity or the composition of 2 or more perspectivities.

Theorem.

Π is a bijection.

Definition.

Given a line m , we say that l is *m-parallel* to l' iff l, l' and m are incident and we write

$$l //_m l' \text{ and } I_l^m := l \times m.$$

I_l^m is called the *m-direction* of l .

Definition.

Given a line m , 2 points A and A' , not on m and a point B neither on m nor on $a := A \times A'$, the *translation* $\mathcal{T}_{AA'}^{m,B}$ is the transformation which associates to I, I if $I \iota m$ and to points P neither on a , nor on m the point $P' := (P \times I_{A \times A'}^m) \times (A' \times I_{A \times P}^m)$, and to $C \iota a$, $C' := (I_{B \times C}^m \times B') \times a$, where $B' := \mathcal{T}_{AA'}^{m,B}(B)$.

Definition. [Marshall Hall]

18

$(\Sigma, *)$ is a *ternary ring* iff Σ is a set and $*$ is an operation which associates to an ordered triple in the set an element in the set satisfying the following properties

0. $A * 0 * C = C$,
1. $0 * B * C = C$,
2. $1 * B * 0 = B$,
3. $A * 1 * 0 = A$,
4. $A * B * X = D$ has a unique solution X ,
5. $B_1 \neq B_2 \implies X * B_1 * C_1 = X * B_2 * C_2$ has a unique solution X ,
6. $A_1 \neq A_2 \implies A_1 \times X \times X' = D_1$ and $A_2 \times X \times X' = D_2$ have a unique solution (X, X') .

¹⁸1943, also unpublished work by D. T. Perkins

Theorem.

$X * 1 * 1 = 0$ has a unique solution X .

Proof: 1.10.1.0 implies $X * 0 * 0 = 0$, $1 \neq 0$, the Theorem follows from 1.10.1.5.

Definition.

A perspective plane can be coordinatized as follows, (Fig. 20a')

H0.0. Q_0, Q_1, Q_2, U , 4 points, no 3 of which are collinear,

D0.0. $q_0 := Q_0 \times Q_1, q_1 := Q_2 \times Q_0, m := q_2 := Q_1 \times Q_2$,

D0.1. $v := Q_2 \times U, i := Q_0 \times U, V := i \times q_2, I := v \times q_0$,

D0.2. $u := V \times I$.

Let Σ be the set of points on q_2 , *distinct* from Q_2 . Define $0 := Q_1, 1 := V$.

The point Q_2 is represented by (∞) , ∞ being a new symbol.

The points Q on q_2 , distinct from Q_2 are *represented* by the element Q in Σ , placed between parenthesis, $Q = (Q)$.

A point P not on q_2 is *represented* by a pair of elements (P_0, P_1) in Σ defined by (Fig. 20a'')

$$P_0 := (((((P \times Q_2) \times i) \times Q_1) \times v) \times Q_0) \times q_2,$$

$$P_1 := (((P \times Q_1) \times v) \times Q_0) \times q_2.$$

In particular, if a point A is on q_0 , then its second coordinate $A_1 = 0$, we represent its first coordinate by A , if a point C is on q_1 , then its first coordinate $C_0 = 0$, we represent its second coordinate by C . Points on v have first coordinate 1.

The line q_2 is represented by $[\infty]$,

a line l_0 through Q_2 distinct from q_2 is *represented* by $[A]$, with $a \times q_0 = (A, 0)$,

a line m not through Q_2 is *represented* by the pair $M_0, M_1]$, where (M_0) is the representation of the point $m \times q_2$ and where the point $m \times q_1$ on q_1 is $(0, M_1)$.

Let $P := ((A, 0) \times Q_2) \times ((B) \times (0, C)) = (A, Y)$. Y is a function of A, B and C which we denote by

$$Y := A * B * C.$$

Theorem.

There is a bijection between the points $(A, 0)$ on q_0 , $(0, A)$ on q_1 and (A) on q_2 .

Proof: We use the perspectivity $\Pi(Q_2, q_0, i)$, followed by $\Pi(Q_1, i, q_1)$, or $\Pi(Q_1, q_1, u)$, followed by $\Pi(Q_0, u, q_2)$.

Comment.

If $P = (P_0, P_1)$, all points on $P \times Q_2$ have the same first coordinate, P_0 , in particular, $(P \times Q_2) \times q_0 = (P_0, 0)$, all points on $P \times Q_1$ have the same second coordinate, P_1 , in particular, $(P \times Q_1) \times q_1 = (0, P_1)$.

In Euclidean Geometry, if q_0 is the x axis, q_1 is the y axis q_2 is the ideal line and $U = (1, 1, 1)$, (A, B) corresponds to $(A, B, 1)$, (A) to $(1, A, 0)$ which is the direction of lines with slope A , (∞) to $(0, 1, 0)$ which is the direction of y axis. The slope of the line joining the origin to $(A, B, 1)$ is $\frac{B}{A}$.

Theorem.

The incidence, noted " ι " satisfies,

0. $(Q) \iota [\infty]$,
1. $(P_0) \iota [P_0, P_1]$,
2. $(P_0, P_1) \iota [P_0]$,
3. $(P_0, P_1) \iota [M_0, M_1]$ iff $P_1 = P_0 * M_0 * M_1$.

Theorem.

0. $(R_0, R_1) \iota (Q_2 \times (A, 0)) \implies R_0 = A$,
1. $(S_0, S_1) \iota (Q_1 \times (0, C)) \implies S_1 = C$,
2. $X := v \times (Q_0 \times (B)) \implies X = (1, B)$,
3. $(Y_0, Y_1) \iota (Q_0 \times V) \implies Y_0 = Y_1$.

Theorem.

The perspective plane as coordinatized in 1.10.1 satisfies the properties of a ternary ring. In particular

0. the unique solution X of $A * B * X = D$ is the second coordinate of the point $((A, D) \times (B)) \times q_1$,
1. with $B_1 \neq B_2$, the unique solution X of $X * B_1 * C_1 = X * B_2 * C_2$ is the first coordinate of the point $((0, C_1) \times (B_1)) \times ((0, C_2) \times (B_2))$,
2. with $B_1 \neq B_2$, the unique solution (X, X') of $A_1 \times X \times X' = D_1$ and $A_2 \times X \times X' = D_2$ is given by

$$X := ((A_1, D_1) \times (A_2, D_2)) \times q_2, \quad X' := ((A_1, D_1) \times (A_2, D_2)) \times q_1,$$

Proof: For 0. to 3. of 1.10.1, we consider the points

$$\begin{aligned} (R_0, R_1) &:= ((A, 0) \times Q_2) \times ((0) \times (0, C)) = (A, A * 0 * C) = (A, C), \\ (S_0, S_1) &:= ((Q_0 \times Q_2) \times ((B) \times (0, C))) = (0, 0 * B * C) = (0, C), \\ X &:= ((1, 0) \times Q_2) \times ((B) \times (0, 0)) = (1, 1 * B * 0) = (1, B), \\ (Y_0, Y_1) &:= ((A, 0) \times Q_2) \times ((V) \times (0, 0)) = (A, A * 1 * 0) = (A, A). \end{aligned}$$

Theorem.

The perspective plane satisfies also the properties:

0. $X * B * C = D$ has a unique solution, the first coordinate of the point $((0, D) \times q_1) \times ((B) \times (0, C))$,
1. $A * X * C = D$ has a unique solution, the coordinate of the point $((A, D) \times (0, C)) \times q_2$,

Proof: For 0, $(X, Y) \iota [B, C]$, $(X, Y) \iota [0, D]$, therefore $Y = X * B * C = X * 0 * D = D$. For 1, $(A, D) \iota [X, C]$ therefore $D = A * X * C$.

Example.

$Q_0 = (0, 0)$, $Q_1 = (0)$, $Q_2 = (\infty)$, $U = (1, 1)$, $V = (1)$, $I = (1, 0)$, $u = [1, z]$ with $1 * 1 * z = 0$.
 $q_0 = [0, 0]$, $q_1 = [0]$, $q_2 = [\infty]$, $v = [1]$, $i = [1, 0]$,

Let (see Fig. 20a')

D0.3, $J := u \times q_1$ $j := U \times Q_1$, $W := j \times q_1$, $w := J \times Q_1$,

D0.4. $T := v \times w$, $t := V \times W$, $R := t \times q_0$, $r := T \times Q_0$, $S := r \times q_2$,

then, with $S = (S)$,

$J = (0, S)$, $j = [0, 1]$, $W = (0, 1)$, $w = [0, S]$, $T = (1, S)$, $t = [1, 1]$, $r = [S, 0]$, $R = (y, 0)$ with $y * 1 * 1 = 0$.

Definition.

The dual coordinatization can also be chosen. I will use the subscript d to indicate the dual representation,

The notation in the preceding example is chosen to allow the dual coordinatization using as elements of Σ the lines through a given point (∞) . We choose $(\infty)_d$ as Q_2 . The line q_2 is represented by $[\infty]_d$, the line $l_0 := Q_2 \times (L_0, 0)$ is represented by $[l_0]_d = [L_0]$, the line n not through Q_2 is represented by $[n_0, n_1]_d$, with

$$n_0 := (((l \times q_2) \times I) \times q_1 \times V) \times q_0 \times Q_2,$$

$$n_1 := (((l \times q_1 \times V) \times q_0) \times Q_2.$$

in this case $q_0 = [0, 0]_d$, $q_1 = [0]_d$, $q_2 = [\infty]_d$, $u = [1, 1]_d$, $w = [0, 1]_d$, $i = [1, 0]_d$, but

$j = [0, R]_d$, with $t \times q_0 = (R, 0)_d$ and $t = [1, R]_d$. The representation of points is done dually as in 1.10.1, with N represented by $(N_0, N_1)_d$, with $N \times Q_2 = [N_0]_d$ and $N \times Q_1 = [0, N_1]_d$.

Theorem.

0. $(\Sigma, +)$ is a loop, with 0 as neutral element,
1. $(\Sigma - \{0\}, \cdot)$ is a loop with 1 as neutral element.

Proof: For the addition, the neutral element property follows from 1.10.1.1 with $B = 1$ and from .3. The solution property follows from 1.10.1.4 and .6 with $B = 1$.

For the multiplication, the neutral element property follows from 1.10.1.3 and 4. The solution property follows from 1.10.1.4 and .5 with $C = 0$.

Theorem.

If the number of elements in Σ is a small number n ,

0. If $n = 2, 3, 4, 5$, there is only one perspective plane,
1. If $n = 6$, there is no perspective plane,
2. If $n = 14, 21, 22, 30, 33, 38, 42, 46, 54, 57, 62, 66, 69, 70, 77, 78, 86, 93, 94, \dots$,
3. If $n = 10$, there is no perspective plane,

0, is easily settled, see II

*1, originates with the problem of the 36 officers, Euler (1782), was settled by Tarry (1900),
2, depends on the next Theorem,
3, has a long history, and was finally proven, using computers, by Lam, Thiel and Swiercz (1989), see also Lam (1991).*

Theorem. [Bruck and Ryser]

If $n \equiv 1, 2 \pmod{4}$ and there are no integers x, y such that $x^2 + y^2 = n$ then there are no perspective plane of order n .

Notation.

$$A + B := A * 1 * B,$$

$$A \cdot B := A * B * 0,$$

$$A + (A \vdash B) = B, (B \dashv A) + A = B.$$

$$\text{When } A \neq 0, A \cdot (A \setminus B) = B, (B/A) \cdot A = B.$$

In the Euclidean case, the line joining the point $(A, A + B)$ to the point $(0, B)$ has slope 1 and the slope of the line joining Q_0 to $(A, A \cdot B)$ is $C = A \cdot B$.

Definition.

*A ternary ring $(\Sigma, *)$ is linear iff for every A, B, C in the set*

$$(A * B * 0) * 1 * C = A * B * C.$$

Theorem.

If a ternary ring is linear then

$$A * B * C = A \cdot B + C.$$

Axiom. [Fano]

The diagonal points of every quadrangle are not collinear.

Axiom. [N-Fano]

The diagonal points of every quadrangle are collinear.

Definition.

A Fano plane is a perspective plane which satisfies the N-Fano axiom.

Theorem.

In a Fano plane $A + A = 0$.

*Proof: For the quadrangle $Q_0 = (0, 0)$, $X_A = (A, 0)$, $Y_A = (0, A)$, $A_0 = (A, A)$, 2 of the diagonal points are on q_2 , therefore the third diagonal point is $V = (Q_0 \times A_0) \times q_2$, therefore $(A, A * 1 * A)$ coincides with X_A and $A + A = 0$.*

Exercise.

0. Prove that in a Fano plane $(A * B) * (A \cdot B) = 0$.
1. Determine a subset of quadrangles with collinear diagonal points which justify the preceding property in a perspective plane.
2. Same question for the property $A + A = 0$.

Definition.

Two triangles $\{APQ\}$ and $\{A'P'Q'\}$ are m -parallel iff

$$A \times P //_m A' \times P', A \times Q //_m A' \times Q', P \times Q //_m P' \times Q'.$$

Theorem.

If $A \iota l$, $l' := A' \times I_l^m$ and $P \iota l$ then $P' \iota l'$.

In general, a line n not through A is not transformed into a line. For this to be so, if $P \iota n$ and $Q \iota n$, we want $P' := \mathcal{T}_{AB}^m(P)$ and $Q' := \mathcal{T}_{AA'}^m(Q)$ to be collinear with $I_{P \times Q}^m$. This suggest the following Definition.

Axiom. [Of Desargues]

In a perspective plane, given any 2 triangles $\{A_i, a_i\}$ and $\{B_i, b_i\}$, let $c_i := A_i \times B_i$, and $C_i := a_i \times b_i$, $\text{incidence}(c_i, C) \implies \text{incidence}(C_i, c)$. C is called the center, c is called the axis of the configuration. I write $\text{Desargues}(C, \{A_i\}, \{B_i\}; \langle C_i \rangle, c)$.

Axiom. [Elated Desargues]

The Elated Desargues axiom is the special case when we restrict Desargues' axiom to the case when the axis c passes through the center C of the configuration. More specifically, $C \iota c$, and for the 2 triangles $\{A_i\}$ and $\{B_i\}$,

let $C_i := (A_{i+1} \times A_{i-1}) \times (B_{i+1} \times B_{i-1})$,
 $c_i := (A_i \times B_i)$, $c_i \iota C$, $i = 0, 1, 2$, $\text{incidence}(A_0 \times A_j, B_0 \times B_j, c)$, $j = 1, 2$,
 $\implies \text{incidence}(A_1 \times A_2, B_1 \times B_2, c)$. We write

$$\text{Elated-Desargues}(C, \{A_i\}, \{B_i\}; \langle C_i \rangle, c).$$

The terminology comes from that in projective geometry, which calls elation, a collineation with an axis of fixed point and a center of fixed lines, with the center on the axis. This axiom is also called the minor Desargues axiom, see for instance Artzy, p. 210.

Theorem.

Given 2 triangles $\{A_i\}$ and $\{B_i\}$, let $C_i := (A_{i+1} \times A_{i-1}) \times (B_{i+1} \times B_{i-1})$, $C_i := A_i \times B_i$, and $C := c_1 \times c_2$,

$\langle C_i, c \rangle$ and $C \iota c \implies c_0 \iota C$. We write

$$\text{Elated-Desargues}^{-1}(c, \{A_i\}, \{B_i\}; \langle c_0, c_1, c_2 \rangle, C)$$

Proof: $\text{Desargues}(C_0, \{A_1, B_1, C_2\}, \{A_2, B_1, C_1\}; \langle B_0, A_0, C \rangle, c)$.

1.10.2 Veblen-Wedderburn Planes.

Definition.

A Veblen-Wedderburn plane is a perspective plane for which the elated Desargues axiom is satisfied on a specific line of the plane.

Comment.

In all the construction that follow, H0.0 and .1, D0.0 to .4, of 1.10.1 and 1.10.1 will be assumed, but not all these constructions are necessarily required.

Lemma. [For the linearity property.]

- H1.0. $X_A = (A, 0)$, $Y_C := (0, C)$, (B) , (See Fig. 21a)
 D1.0. $j_b := Q_0 \times B$, $j'_b := Y_C \times B$, $j_1 := Q_0 \times V$, $j'_1 := Y_C \times V$,
 D1.1. $x := X_A \times Q_2$, $K := x \times j_b$, $k_0 := K \times Q_1$, $L := k_0 \times j_1$,
 D1.2. $K' := x \times j'_b$, $c := L \times Q_2$, $L' := c \times j'_1$, $k'_0 := L' \times K'$,
 C1.0. $Q_1 \iota k'_0$.

Moreover,

$$K = (A, A \cdot B), L = (A \cdot B, A \cdot B), K' = (A, A * B * C), L' = (A \cdot B, A \cdot B + C),$$

$$C1.0 \implies A * B * C = A \cdot B + C.$$

Proof:

$$\text{Elated-Desargues}(Q_2, \{Q_0, K, L\}, \{Y_C, K', L'\}; \langle Q_1, V, B \rangle, q_2) \implies Q_1 \iota k'_0.$$

Lemma. [For the additive associativity law]

- H1.0. X_A, X_B, Y_C , (See Fig. 21b)
 D1.0. $a := X_A \times Q_2$,
 D1.1. $b := X_B \times Q_2$, $B_1 := b \times i$, $x_1 := B_1 \times Q_1$, $Y_1 := x_1 \times q_1$,
 D1.2. $i_2 := Y_1 \times V$, $A_1 := i_2 \times a$, $x_3 := A_1 \times Q_1$, $D_1 := x_3 \times i$,
 D1.3. $d := D_1 \times Q_2$, $i_1 := Y_C \times V$, $D_2 := d \times i_1$,
 D1.4. $B_2 := i_1 \times b$, $x_2 := B_2 \times Q_1$, $Y_2 := x_2 \times q_1$,
 D1.5. $i_3 := Y_2 \times V$, $A_2 := i_3 \times a$, $x_4 := A_2 \times D_2$,
 D1.6. $e_1 := A_1 \times B_1$, $e_2 := A_2 \times B_2$, $E := e_1 \times e_2$,
 C1.0. $E \iota q_2$,
 C1.1. $Q_1 \iota x_4$,

Moreover,

$$B_1 = (B, B), Y_B = (0, B), A_1 = (A, A + B), D_1 = (A + B, A + B),$$

$$B_2 = (B, B + C), Y_1 = (0, B + C), A_2 = (A, A + (B + C)),$$

$$D_2 = (A + B, ((A + B) + C)),$$

$$C1.1. \implies A + (B + C) = (A + B) + C.$$

Proof:¹⁹

$$\text{Elated-Desargues}(Q_2, \{A_1, B_1, Y_1\}; \{A_2, B_2, Y_2\}; \langle Q_1, V, E \rangle, q_2),$$

¹⁹variant due to Michael Sullivan, October 24, 1989.

$$\begin{aligned} &\implies \text{Elated-Desargues}^{-1}(q_2, \{A_1, B_1, D_1\}; \{A_2, B_2, D_2\}; \langle V, Q_1, E \rangle, Q_2) \\ &\implies Q_1 \iota x_4. \end{aligned}$$

Corollary.

If 2 m -parallelograms $\{A_j\}$ and $\{B_j\}$, $j = 0, 1, 2, 3$, are such that $A_k \times B_k //_m A_0 \times B_0$, $k = 1, 2$, the same is true for $k = 3$. (See Fig. 21e)

The parallelograms for which the proof is given in the Lemma are $\{A_1, Y_B, Y_1, A_2\}$ and $\{D_1, B_1, B_2, D_2\}$.

Lemma. [For the right distributive law]

$$\begin{aligned} H1.0. \quad &X_A = (A, 0), Y_1 = (0, B), (C), \text{ (See Fig. 21c)} \\ D1.0. \quad &x := X_A \times Q_2, \\ D1.1. \quad &x_1 := Q_1 \times Y_1, B_1 := x_1 \times i, i_1 := Y_1 \times V, A_1 := i_1 \times x, \\ D1.2. \quad &x_3 := A_1 \times Q_1, F_1 := x_3 \times i, f := F_1 \times Q_2, c_1 := Q_0 \times C, \\ D1.3. \quad &b := B_1 \times Q_2, B_2 := b \times c_1, F_2 := f \times c_1, \\ D1.4. \quad &x_2 := B_2 \times Q_1, Y_2 := x_2 \times q_1, e_1 := Y_2 \times A_1, e_2 := B_2 \times F_1, \\ D1.5. \quad &E := e_1 \times e_2, \\ D1.6. \quad &c_2 := Y_2 \times C, A_2 := c_2 \times x, x_4 := A_2 \times F_2, \\ C1.0. \quad &E \iota q_2. \\ C1.1. \quad &Q_1 \iota x_4. \end{aligned}$$

Moreover,

$$\begin{aligned} B_1 &= (B, B), A_1 = (A, A + B), F_1 = (A + B, A + B), B_2 = (B, B \cdot C), \\ F_2 &= (A + B, (A + B) \cdot C), Y_2 = (0, B \cdot C), A_2 = (A, A * C * (B \cdot C)), \text{ and} \\ C1.1 \implies &(A + B) \cdot C = A \cdot C + B \cdot C. \end{aligned}$$

Proof:

$$\text{Elated-Desargues}(Q_1, \{Y_1, A_1, Y_2\}, \{B_1, F_1, B_2\}; \langle E, Q_2, V \rangle, q_2) \implies E \iota q_2.$$

$$\text{Elated-Desargues}^{-1}(q_2, \{A_2, A_1, Y_2\}, \{F_2, F_1, B_2\}; \langle E, C, Q_2 \rangle, Q_1) \implies Q_1 \iota x_4.$$

Finally, from C1.0 follows $(A + B) \cdot C = A * C * (B \cdot C)$, but by linearity, the second member equals $A \cdot C + B \cdot C$.

Exercise.

Determine the identity corresponding to C1.0 or to the m -parallelism of $Y_2 \times A_1$ and $B_2 \times F_1$.

Lemma. [For the commutativity law]

$$\begin{aligned} H1.0. \quad &A_1, B_1, \text{ (See Fig. 21d)} \\ D1.0. \quad &a_0 := A_1 \times Q_0, A := a_0 \times q_2, a_2 := A \times B_1, \\ D1.1. \quad &b_0 := B_1 \times Q_0, B := b_0 \times q_2, b_2 := A_1 \times B, D := b_2 \times a_2, \\ D1.2. \quad &x_1 := A_1 \times Q_1, Y_A := x_1 \times q_1, b_1 := Y_A \times B, \\ D1.3. \quad &y_2 := B_1 \times Q_2, B_2 := y_2 \times b_1, x_2 := B_2 \times D, y_1 := A_1 \times Q_2, \\ D1.4. \quad &x_3 := B_1 \times Q_1, Y_B := x_3 \times q_1, a_1 := Y_B \times A, A_2 := a_1 \times y_1, \\ C1.0. \quad &Q_1 \iota x_2, \\ C1.1. \quad &A_2 \iota x_2, \end{aligned}$$

Moreover,

if $A_1 = (X_A, Y_A)$, and $B_1 = (X_B, Y_B)$, then $A_2 = (X_A, Y_A + Y_B)$, $B_2 = (X_B, Y_B + Y_A)$,
 $C1.0$ and $.1 \implies Y_A + Y_B = Y_B + Y_A$.

Proof:

Elated-Desargues $(B, \{Q_0, Y_A, A_1\}, \{B_1, B_2, D\}; \langle Q_1, A, Q_2 \rangle, q_2) \implies Q_1 \iota x_2$.

Elated-Desargues $(A, \{Q_0, Y_B, B_1\}, \{A_1, A_2, D\}; \langle Q_1, B, Q_2 \rangle, q_2) \implies A_2 \iota x_2$.

therefore A_2 and B_2 have the same second coordinate Y .

Because $A_1 \iota a_0 \iota (A)$, $Y_A = X_A \cdot A$, by construction and because of linearity, $A_2 = (X_A, X_A * A * Y_B) = (X_A, X_A \cdot A + Y_B)$ similarly $Y_B = X_B \cdot B$, and $B_2 = (X_B, X_B \cdot B + Y_A)$.

Corollary.

If we make the same constructions as in the lemma with $A = B = J$, then
 $Q_1 \iota (A_2 \times B_2)$.

Lemma. [Addition an Negation in Veblen-Wedderburn planes.]

$H0.0.$ $Y_A, Y_B, (Fig.21e)$

$D1.0.$ $i_1 := Y_A \times V, i_2 := Y_B \times V,$

$D1.1.$ $x_1 := Y_A \times Q_1, A_1 := x_1 \times i, a := A_1 \times Q_2, A_2 := a \times i_2,$

$D1.2.$ $x_3 := Y_B \times Q_1, B_1 := x_3 \times i, b := B_1 \times Q_2, B_2 := b \times i_1,$

$D1.3.$ $x_2 := A_2 \times B_2,$

$C1.0.$ $Q_1 \iota x_2,$

$D2.0.$ $U_1 := x_1 \times v, c := U_1 \times Q_0, A := c \times q_2,$

$D2.1.$ $c- := Y_A \times I, A- := c- \times q_2,$

Moreover,

If $Y_A = (0, A)$ and $Y_B = (0, B)$, then $A_1 = (A, A)$, $B_1 = (B, B)$, $A_2 = (A, A + B)$, $B_2 = (B, B + A)$,

$U_1 = (1, A)$, $A = (A)$, $A- = (-A)$.

Theorem.

In a Veblen-Wedderburn plane, the ternary ring $(\Sigma, *)$ is a quasifield in the terminology of Dembowski (p. 129):

0. $(\Sigma, *)$ is linear, $a * b * c = a \cdot b + c$,
1. $(\Sigma, +)$ is an abelian group,
2. $(\Sigma - \{0\}, \cdot)$ is a loop,
3. $(\Sigma, *) = (\Sigma, +, \cdot)$ is right distributive, $(a + b) \cdot c = a \cdot c + b \cdot c$.
4. $a \neq b \implies x \cdot a = x \cdot b + c$ has a unique solution.

Theorem.

In a Veblen-Wedderburn plane with ideal line m , $\mathcal{T}_{AA'}^{m,B}(C)$, $C \iota A \times A'$, is independent of B .
 We can therefore use $\mathcal{T}_{AA'}^m$ as notation for a translation.

Definition.

m-equality is defined by

$$[A, A'] =_m [P, P'] \text{ iff } P' = \mathcal{T}_{AA'}^m(P).$$

Theorem.

In a Veblen-Wedderburn plane we can use systematically 3 coordinates as follows

(Q_2) is equivalent to $(0, 1, 0)$,

(P_0) is equivalent to $(1, P_0, 0)$,

(P_0, P_1) is equivalent to $(P_0, P_1, 1)$,

$[q_2]$ is equivalent to $[0, 0, 1]$,

$[M_0]$ is equivalent to $[1, 0, -M_0]$,

$[M_0, M_1]$ is equivalent to $[M_0, -1, M_1]$.

A point (P_0, P_1, P_2) is incident to the line $[l_0, l_1, l_2]$ iff

$$P_0 l_0 + P_1 l_1 + P_2 l_2 = 0.$$

Proof: In the general case, because of linearity, a point (P_0, P_1) is incident to the line $[M_0, M_1]$ if $P_1 = P_0 \cdot M_0 + M_1$, which we can rewrite

$$P_0 \cdot M_0 + P_1 \cdot (-1) + 1 \cdot M_1.$$

The other correspondances can be verified using 1.10.1.

Theorem.

In a Veblen-Wedderburn plane with ideal line m , m -equality is an equivalence relation.

1.10.3 Moufang Planes.**Definition.**

A Moufang plane is a Veblen-Wedderburn plane in which the elated Desargues axiom is satisfied for every line in the plane. (See Fig. 3f).

Theorem.

Duality is satisfied in a Moufang plane.

Definition.

The C-Desargues Configuration is a Desargues Configuration, for which 2 corresponding sides intersect on the line joining the other vertices. The point of intersection will be underlined.

Lemma.

The Elated-Desargues Configuration for all lines in the planes implies the C-Desargues Configuration.

Proof: (See Fig 3f.) To prove $C\text{-Desargues}(C, \{A_i\}, \{\underline{B}_0, B_1, B_2\}; \langle C_i \rangle, c)$, we apply $\text{Elated-Desargues}^{-1}(c_0, \{A_1, B_1, C_2\}, \{A_2, B_2, C_1\}; \langle B_0, A_0, C \rangle, C_0)$.

Definition.

The 1-Desargues Configuration is a Desargues Configuration, for which the vertex of 1 triangle is on the side of the other, this vertex will be underlined.

Lemma.

The Elated-Desargues Configuration for all lines in the planes implies the 1-Desargues Configuration.

Proof: (See Fig 3b.) To prove $1\text{-Desargues}(C, \{A_i\}, \{B_i\}; \langle \underline{C}_0, C_1, C_2 \rangle, c)$, we apply $\text{Elated-Desargues}(B_0, \{A_0, C_1, C_2\}, \{C, B_2, B_1\}; \langle C_0, A_1, A_2 \rangle, a_0)$.

Theorem.

In a Moufang plane

- 0. the C-Desargues Theorem is true.
- 1. the 1-Desargues Theorem is true.

Lemma. [For the left distributive law]

H1.0. $X_A = (A, 0), (B), (C)$, (See Fig. 22a)

D1.0. $a := X_A \times Q_2, c_1 := Q_0 \times C, U_1 := c_1 \times u, x_1 := U_1 \times Q_1,$

D1.1. $Y_1 := x_1 \times q_1, b_1 := Y_1 \times B, U_2 := b_1 \times u,$

D1.2. $A_1 := a \times c_1, x_2 := A_1 \times Q_1, Y_2 := x_2 \times q_1,$

D1.3. $b_2 := Y_2 \times B, A_2 := b_2 \times a, d := U_2 \times Q_0,$

C1.0. $A_2 \iota d.$

Moreover,

$U_1 = (1, C), Y_1 = (0, C), U_2 = (1, 1 * B * C), A_1 = (A, A \cdot C), Y_2 = (0, A \cdot C), A_2 = (A, A * B * (A \cdot C)),$

$C1.0 \implies A \cdot B + (A \cdot C) = A * B * (A \cdot C) = A \cdot (1 * B * C) = A \cdot ((1 \cdot B) + C) = A \cdot (B + C).$

Proof:

$C\text{-Desargues}(Q_0, \{Y_1, U_1, U_2\}, \{Y_2, A_1, A_2\}; \langle \underline{Q}_2, B, Q_1 \rangle, q_2)$

$\implies ((UA_1 \times A_2) \times (U_1 \times U_2)) \iota (Y_1 \times Y_2).$

Lemma. [For the inverse property]

H1.0. A , (See Fig. 22b)

D1.0. $a := X_A \times Q_2, A_0 := a \times j, A_1 := a \times i,$

D1.1. $a_1 := A_1 \times Q_1, A_2 := a_1 \times u, a_0 := A_0 \times Q_0, A_3 := a_0 \times u,$

D1.2. $a_2 := A_2 \times Q_0, A_4 := a_2 \times j,$

D1.4. $a_3 := A_3 \times Q_1, a_4 := A_4 \times Q_2, A_5 := a_3 \times a_4,$

D1.5. $d_1 := A_0 \times A_2, d_2 := A_3 \times A_4, E := d_1 \times d_2,$

C1.0. $E \iota q_2$,

C1.1. $A_5 \iota i$.

Moreover,

$A_0 = (A, 1)$, $A_1 = (A, A)$, $A_2 = (1, A)$, $A_4 = (A^L, 1)$, $A_3 = (1, A^R)$,

$A_5 = (A^L, A^R)$,

C1.1 $\implies A^L = A^R$.

Proof:

1-Desargues($Q_0, \{\underline{A_0}, A_2, A_1\}, \{A_3, A_4, U\}; \langle Q_1, Q_2, E \rangle, q_2$) $\implies E \iota q_2$.

1-Desargues⁻¹($Q_0, \{\underline{A_4}, A_3, A_5\}, \{A_2, A_0, U\}; \langle Q_1, Q_2, E \rangle, q_2$) $\implies A_5 \iota i$.

Notation.

If $B \neq 0$, we write $B^{-1} = B^R$.

Lemma. [For the right inverse property]

H1.0. X_A, B , (See Fig. 22c)

D1.0. $a := X_A \times Q_2$, $A_1 := a \times i$, $b := Q_0 \times B$, $C_2 := j \times b$,

D1.1. $c := C_2 \times Q_2$, $C_1 := c \times i$, $x_1 := C_1 \times Q_1$, $U_1 := x_1 \times u$,

D1.2. $A_2 := a \times b$, $x_3 := A_2 \times Q_1$, $AB_2 := x_3 \times i$, $ab := AB_2 \times Q_2$,

D1.3. $b' := U_1 \times Q_0$, $AB_1 := ab \times b'$, $x_2 := A_1 \times AB_1$,

D1.4. $d := U_1 \times A_1$, $e := U \times A_2$, $S := d \times e$,

C1.0. $S \iota q_0$, C1.1. $Q_1 \iota x_2$.

Moreover,

$A_1 = (A, A)$, $C_2 = (B^{-1}, 1)$, $C_1 = (B^{-1}, B^{-1})$, $U_1 = (1, B^{-1})$, $A_2 = (A, A \cdot B)$, $AB_2 = (A \cdot B, A \cdot B)$, $AB_1 = (A \cdot B, (A \cdot B) \cdot B^{-1})$,

C1.1 $\implies (A \cdot B) \cdot B^{-1} = A$.

Proof:

1-Desargues($Q_2, \{U_1, A_1, C_1\}, \{\underline{U}, A_2, C_2\}; \langle Q_0, Q_1, S \rangle, q_0$) $\implies S \iota q_0$.

1-Desargues⁻¹($Q_2, \{U_1, \underline{A_1}, AB_1\}, \{U, A_2, AB_2\}; \langle Q_0, Q_1, S \rangle, q_0$) $\implies Q_1 \iota x_2$.

Lemma. [For the left inverse property]

H1.0. X_A, B , (See Fig. 22d)

D1.2. $b := Q_0 \times B$, $U_3 := b \times u$, $x_3 := U_3 \times Q_1$,

D1.3. $a := X_A \times Q_2$, $A_1 := a \times j$, $b' := Q_0 \times A_1$, $U_1 := b' \times u$,

D1.4. $x_1 := U_1 \times Q_1$, $C_1 := x_1 \times i$, $c := C_1 \times Q_2$, $C_2 := c \times x_3$,

D1.5. $A_2 := a \times b$, $x_2 := A_2 \times Q_1$, $U_2 := x_2 \times u$,

D1.6. $ab := U_2 \times Q_0$,

D1.7. $r_1 := U \times A_2$, $r_2 := U_3 \times C_1$, $R := r_1 \times r_2$,

C1.0. $R \iota q_2$,

C1.1. $C_2 \iota ab$,

Moreover,

$A_1 = (A, 1)$, $A_2 = (A, A \cdot B)$, $U_1 = (1, A^{-1})$, $U_3 = (1, B)$, $U_2 = (1, A \cdot B)$, $C_1 = (A^{-1}, A^{-1})$, $C_2 = (A^{-1}, A^{-1} \cdot (A \cdot B))$.

C1.1 $\implies A^{-1} \cdot (A \cdot B) = B$.

Proof:

$$\begin{aligned} & 1\text{-Desargues}(Q_0, \{A_1, \underline{U}, A_2\}, \{U_1, C_2, U_3\}; \langle R, Q_2, Q_1 \rangle, q_2) \\ \implies & 1\text{-Desargues}^{-1}(q_2, \{U, U_2, A_2\}, \{C_1, C_2, \underline{U}_3\}; \langle Q_1, R, Q_2 \rangle, Q_0) \implies C_2 \iota ab. \end{aligned}$$

Theorem.

With the coordinatization of the plane as given in 1.10.1,

$$0. \text{ the ternary ring } (\Sigma, +, \cdot) \text{ is left distributive, or} \\ A \cdot (B + C) = A \cdot B + A \cdot C.$$

$$1. B \neq 0 \implies B^R = B^L = B^{-1},$$

$$2. (A \cdot B) \cdot B^{-1} = B^{-1} \cdot (B \cdot A) = A \text{ for all } A.$$

In other words, $(\Sigma, +, \cdot)$ is an alternative division ring.

1.10.4 Desarguesian Planes.

Definition.

A Desarguesian plane is a plane in which the Desargues Axiom is always satisfied.

Theorem.

Duality is satisfied in a Desarguesian plane.

Comment.

Instead of the Axiom of Desargues one can use the equivalent axiom of Reidemeister (See Theorem II.2.1.8 and Klingenberg, 1955).

Lemma. [For Associativity]

H1.0. X_A, B, C , (See Fig. 23.)

D1.0. $b := Q_0 \times B, c := Q_0 \times C, U_1 := b \times u, x_1 := U_1 \times Q_1,$

D1.1. $D_1 := x_1 \times i, d := D_1 \times Q_2, D_2 := d \times c, x_2 := D_2 \times Q_1,$

D1.2. $U_2 := x_2 \times u, bc := U_2 \times Q_0,$

D1.3. $a := X_A \times Q_2, A_1 := a \times b, x_3 := A_1 \times Q_1, AB_1 := x_3 \times i,$

D1.4. $ab := AB_1 \times Q_2, AB_2 := ab \times c, x_4 := AB_2 \times Q_1, A_2 := x_4 \times a,$

D1.5. $r_1 := U_1 \times D_2, r_2 := A_1 \times AB_2, R := r_1 \times r_2,$

C1.0. $A_2 \iota bc,$

Moreover,

$A_1 = (A, A \cdot B), AB_1 = (A \cdot B, A \cdot B), AB_2 = (A \cdot B, (A \cdot B) \cdot C),$

$A_2 = (A, A \cdot (B \cdot C)), U_1 = (1, B), D_1 = (B, B), D_2 = (B, B \cdot C), U_2 = (1, B \cdot C).$

C1.0 $\implies A \cdot (B \cdot C) = (A \cdot B) \cdot C.$

Proof:

$\text{Desargues}(Q_0, \{D_1, D_2, U_1\}, \{AB_1, AB_2, A_1\}; \langle R, Q_1, Q_2 \rangle, q_2)$

$$\implies \text{Desargues}^{-1}(q_2, \{U_2, U_1, D_2\}, \{A_2, A_1, AB_2\}; \langle R, Q_1, Q_2 \rangle, Q_0) \implies A_2 \iota bc.$$

Theorem.

With the coordinatization of the plane as given in 1.10.1,

$$\begin{aligned} 0. \quad (\Sigma, \cdot) \text{ is associative,} \\ A \cdot (B \cdot C) = (A \cdot B) \cdot C. \end{aligned}$$

In other words, $(\Sigma, +, \cdot)$ is a skew field.

Theorem.

If a Desarguesian plane we use the coordinates of 1.10.2, we can make them homogeneous by multiplying the coordinates of points to the left by the same element in the set Σ , and those of lines to the right by the same element in the set Σ .

Associativity of multiplication is essential to allow for the left equivalence of points and the right equivalence of lines.

1.10.5 Pappian planes.**Axiom. [Of Pappus]**

In a perspective plane: If A_i are 3 distinct points on a line a and B_i are 3 distinct points on a line b and $C_i := (A_{i+1} \times B_{i-1}) \times (A_{i-1} \times B_{i+1})$ then $\text{incidence}(C_i)$.

I write $\text{Pappus}(\{A_i\}, \{B_i\}; \{C_i\})$.

Definition.

A Pappian plane is a plane in which the Pappus Axiom is always satisfied.

Comment.

There are other axioms which are equivalent to that of Pappus. The Fundamental axiom and Axiom A (See Seidenberg, p. 25 and Chapter IV). The Fundamental axiom states that there is at most one projectivity which associates 3 given distinct collinear points into 3 given distinct collinear. Axiom A states that if a projectivity which associates a line l into a distinct line l' leaves $l \times l'$ invariant then it is a perspectivity.

Theorem.

Duality is satisfied in a Pappian plane.

Theorem.

A Pappian plane is a Desarguesian plane.

Lemma. [For Commutativity]

H1.0. $(A), (B),$ (See Fig. 24)

D1.0. $a := Q_0 \times A, b := Q_0 \times B, U_1 := a \times u,$

D1.1. $x_1 := U_1 \times Q_1, C_1 := x_1 \times i, c := C_1 \times Q_2, C_2 := c \times b,$

D1.2. $U_2 := b \times u,$

D1.3. $x_2 := U_2 \times Q_1, D_1 := x_2 \times i, d := D_1 \times Q_2, D_2 := d \times a,$

D1.4. $x_3 := C_2 \times D_2,$

C1.0. $D_2 \iota x_3,$

Moreover,

$U_1 = (1, A), U_2 = (1, B), C_1 = (A, A), D_1 = (B, B), C_2 = (A, AB), D_2 = (B, BA), C1.0 \implies A \cdot B = B \cdot A.$

Proof:

$\text{Pappus}(\langle D_1, C_1, Q_0 \rangle, \langle U_1, U_2, Q_2 \rangle; \langle C_2, D_2, Q_2 \rangle) \implies D_2 \iota x_3.$

Theorem.

With the coordinatization of the plane as given in 1.10.1,

0. (Σ, \cdot) is commutative,
 $a \cdot b = b \cdot a.$

In other words, $(\Sigma, +, \cdot)$ is a field.

Theorem.

The field of a Pappus-Fano plane has characteristic 2. Vice-versa if a field has characteristic 2, the corresponding Pappian plane satisfies the axiom N-Fano.

Proof: We have seen than in a Fano plane $A + A = 0$, for all $A \in \Sigma$, therefore the characteristic of the field is 2. To prove the converse, we choose as coordinates of the vertices of the quadrangle $A_0 = (1, 0, 0), A_1 = (0, 1, 0), A_2 = (0, 0, 1)$ and $M = (1, 1, 1)$, the diagonal elements are $M_0 = (0, 1, 1), M_1 = (1, 0, 1), M_2 = (1, 1, 0)$, which are collinear iff $1 + 1 = 0$.

1.10.6 Separable Pappian Planes.

Axiom. [Of separation]

In a perspective plane, if $A_i, i = 0, 1, 2, 3, 4$ are distinct points on the same line:

0. There are at least 4 points on a line.
1. $\sigma(A_0, A_1 | A_2, A_3) \implies \sigma(A_0, A_1 | A_3, A_2)$ and $\sigma(A_3, A_2 | A_0, A_1)$
2. only one of the relations $\sigma(A_0, A_1 | A_2, A_3), \sigma(A_0, A_2 | A_1, A_3), \sigma(A_0, A_3 | A_1, A_2)$ holds.
3. $\sigma(A_0, A_1 | A_2, A_3)$ and $\sigma(A_1, A_2 | A_3, A_4) \implies \sigma(A_0, A_4 | A_2, A_3).$
4. $\Pi(P, A_j, A'_j), j = 0, 1, 2, 3,$ and $\sigma(A_0, A_1 | A_2, A_3) \implies \sigma(A'_0, A'_1 | A'_2, A'_3).$

Definition.

A separable Pappian plane is a Pappian plane in which the separation axioms are satisfied.

Theorem.

0. $\sigma(A_0, A_1|A_2, A_3) \implies \sigma(A_1, A_0|A_2, A_3), \sigma(A_0, A_1|A_3, A_2), \sigma(A_1, A_0|A_3, A_2),$
 $\sigma(A_2, A_3|A_0, A_1), \sigma(A_2, A_3|A_1, A_0) \sigma(A_3, A_2|A_0, A_1), \sigma(A_3, A_2|A_1, A_0).$
1. $\sigma(A_0, A_1|A_2, A_3) \text{ and } \sigma(A_1, A_2|A_3, A_4) \implies \sigma(A_0, A_4|A_1, A_2),$

Notation.

When we use 1.10.6.3 or 1.10.6.1, I will underline the element in each quadruple of point which is distinct, to ease the application of the axiom and write, for instance

$$\sigma(A_0, A_1|A_2, A_3) \text{ and } \sigma(A_1, A_2|A_3, \underline{A_4}) \implies \sigma(A_0, A_4|A_2, A_3), \text{ or}$$

$$\sigma(A_3, A_2|A_1, \underline{A_0}) \text{ and } \sigma(A_2, A_1|A_3, \underline{A_4}) \implies \sigma(A_0, A_4|A_2, A_1).$$

Theorem.

In a Pappus-Fano plane, given a harmonic quadrangle A, B, C, D , (See Fig. 2a"), $P, R|U, V$, where P, R are diagonal points and U, V are the intersection with $P \times R$ of the sides of the quadrangle which are not incident to P or R .

Proof:

$\Pi(C, \{P, U, R, V\}, \{D, Q, B, V\}), \Pi(A, \{D, Q, B, V\}, \{R, U, P, V\})$, therefore
 $P, R|U, V \implies R, P|U, V$, while $P, U|R, V \implies R, U|P, V$, $P, V|U, R \implies R, V|U, P$, the last 2 conclusions are contradicted by 1.10.6.2.

Corollary.

$$(O, \infty|A, -A).$$

Definition.

Given $A_i, i = 0, 1, 2$ on a line a , a segment $\text{seg}(A_0, A_1 \setminus A_2)$ is the set of points A ι a such that $\sigma(A_0, A_1|A, A_2)$.

Lemma.

If $A_i \in \Sigma$ and $\sigma(A_0, A_1|A_2, A_3)$,

0. $\sigma(P + A_0, P + A_1|P + A_2, P + A_3),$
1. $P \neq 0 \implies \sigma(P \cdot A_0, P \cdot A_1|P \cdot A_2, P \cdot A_3).$
2. More generally, if Π is a projectivity which associates to
 $X, (A \cdot X + B) \cdot (C \cdot X + D), A \cdot C \cdot D \neq 0, A \cdot D \neq B \cdot C,$
then $\sigma(\Pi(A_0), \Pi(A_1), \Pi(A_2), \Pi(A_3)).$

The same properties hold if one of the A_i is replaced by ∞ and we use $\infty + A = \infty$ and with $A \neq 0$, $\infty \cdot A = \infty$.

Proof:

$\Pi(V, q_1, p) \circ \Pi(Q_1, p, q_1)$ transforms $(0, A_i)$ into $(P, P + A_i)$ into $(0, P + A_i)$.

$\Pi(Q_1, q_1, i) \circ \Pi(Q_2, i, Q_0 \times (P)) \circ \Pi(Q_2, i, Q_0 \times (P))$ transforms $(0, A_i)$ into (A_i, A_i) into $(A_i, P \cdot A_i)$ into $(0, P \cdot A_i)$. The rest of the proof is left as an exercise.

Lemma.

In a separable Pappian plane, the characteristic is not 2.

Proof: If the characteristic was 2 and A is different from 0, 1 and ∞ , either $\sigma(0, 1|A, \infty)$ or $\sigma(0, A|\infty, 1)$ or $\sigma(0, \infty|1, A)$.

In the first case, adding 1 or A gives $\sigma(\underline{1}, 0|A + 1, \infty)$ or $\sigma(\underline{A}, A + 1|0, \infty)$, combining gives $\sigma(1, A|0, \infty)$ which contradicts $\sigma(0, 1|A, \infty)$. In the second case we add 1 or A and in the third case we add 1 or $A + 1$ and proceed similarly to show contradiction.

Definition.

P is positive, or $P > 0$, iff $\sigma(0, \infty|-1, P)$.

P is negative, or $P < 0$, iff $-P > 0$ or iff $\sigma(0, \infty|-1, -P)$ or iff $\sigma(0, \infty|1, P)$.

Theorem.

0. $1 > 0$.

1. $A, B \in \Sigma$, $A > 0$ and $B > 0 \implies A + B > 0$.

2. $A \in \Sigma$, either $A = 0$ or $A > 0$ or $-A > 0$.

3. $A, B \in \Sigma$, $A > 0$ and $B > 0 \implies A \cdot B > 0$.

Proof:

For 0, we use Corollary 1.10.6.

For 1, $A > 0 \implies \sigma(0, \infty|-1, A)$ by the projectivity which associates to X , $A - X - 1$,

4. $\sigma(A - 1, \infty|A, \underline{-1})$,

$B > 0 \implies \sigma(0, \infty|-1, B) \implies (\text{adding } A) \sigma(A, \infty|A - 1, \underline{A + B}) \implies (\text{combining with 4.}) \sigma(-1, \underline{A + B}|A, \infty)$, with $\sigma(\underline{0}, \infty|-1, A) \implies \sigma(0, \underline{A + B}|A, \infty)$, with $\sigma(0, \infty|\underline{-1}, A) \implies \sigma(-1, A + B|0, \infty) \implies A + B > 0$.

For 2, by the definition of $A > 0$ or $-A > 0$, it follows that A is not 0. $A > 0$ and $-A > 0$ are also mutually exclusive, otherwise $A + (-A) = 0$ would be positive. If $A = -1$, then $-A = 1 > 0$. It remains to examine for a given A distinct from 0 and -1, the 3 possibilities, $\sigma(0, -1|\underline{A}, \infty)$ and $\sigma(0, \infty|-1, \underline{1}) \implies \sigma(1, A|0, \infty) \implies A < 0$.

$\sigma(0, \underline{A}|\infty, -1)$ and $\sigma(0, \infty|-1, \underline{1}) \implies \sigma(1, A|0, \infty) \implies A < 0$.

$\sigma(0, \infty|-1, A) \implies A > 0$.

For 3, $\sigma(0, \infty|-1, B) \implies \sigma(0, \infty|-A, A \cdot B)$,

$A > 0 \implies$ not $\sigma(0, \infty|-1, -A)$, therefore either $\sigma(0, -1|\infty, -A)$ or $\sigma(-1, \infty|0, -A)$. In the first case, $\sigma(0, \infty|-A, \underline{A \cdot B})$ and $\sigma(0, \underline{-1}|\infty, -A) \implies \sigma(-1, A \cdot B|0, \infty)$.

In the second case, $\sigma(0, \infty|-A, \underline{A \cdot B})$, and $\sigma(\underline{-1}, \infty|0, -A) \implies \sigma(-1, A \cdot B|0, \infty)$.

Theorem.

With the coordinatization of the separable Pappian plane as given in 1.10.1,

0. $(\Sigma, +, \cdot)$ is an ordered field.

1.10.7 Continuous Pappian or Classical Projective Planes.**Axiom. [Of continuity]**

Let $\mathcal{S} \subset (\text{seg}(A, C \setminus B), \mathcal{S} \text{ non empty}, \exists L \text{ and } U \ni \text{all } P \in \mathcal{S}, \sigma(AP|LU) \implies \exists G \text{ and } H \ni \sigma(LP|GU) \text{ and } \sigma(UP|HL).$

Definition.

A Continuous Pappian or Classical Projective Plane is a separable plane for which the continuity axiom is satisfied.

Theorem.

The field associated to a Continuous Pappian plane is the real field R .

1.10.8 Isomorphisms of Synthetically and Algebraically defined Planes.**Introduction.**

We have seen that we can coordinatize the various perspective planes by ternary rings which have special properties. The converse is also true. If a ternary rings has appropriate properties there exists a plane as defined above which is isomorphic to it. More specifically:

Theorem.

There is an isomorphism between

- 0. perspective planes and ternary rings $(\Sigma, *)$.
- 1. Veblen-Wedderburn planes and ternary rings with the properties 1.90.2.
- 2. Moufang planes and alternative division rings.
- 3. Desarguesian planes and skew fields.
- 4. Pappian planes and fields.

1.10.9 Examples of Perspective Planes.

Definition.

A Moulton plane (1902) is the set of points in the Euclidean plane coordinatized with Cartesian coordinates and the lines,

- 0. the ideal line, $[0,0,1]$,
- 1. the lines $[m, -1, n]$, $m \leq 0$,
- 2. the lines consisting of two parts, first, the subset of $[m, -1, n]$, $m > 0$, which is in the lower half plane or on the ideal line, second, the subset of $[m/2, -1, n]$, $m > 0$, which is in the upper half plane.

Theorem.

- 0. The Moulton plane is a perspective plane.
- 1. The Moulton plane is not a Veblen-Wedderburn plane.

Proof: See Artzy, p. 210.

Definition.

A 2-Q plane is defined like a quaternion plane with $ij = -ji = k$ replaced by $ij = -ji = 2k$.

Theorem.

- 0. The 2-Q plane is a Veblen-Wedderburn plane.
- 1. The 2-Q plane is not a Moufang plane.

Proof: See Artzy, p. 226.

Definition.

A Cayleyian plane is defined like a quaternion plane, using Cayley numbers instead of quaternions.

Theorem.

- 0. The Cayleyian plane is a Moufang plane.
- 1. The Cayleyian plane is not a Desarguesian plane.

Proof: See Artzy, p. 226.

Definition.

A quaternion plane is defined using quaternions as coordinates instead of real numbers.

Theorem.

- 0. The quaternion plane is a Desarguesian plane.
- 1. The quaternion plane is not a Pappian plane.

Proof: See Artzy, p. 226.

Definition.

A finite Pappian plane is a Pappian plane for which the number of points on one line is finite. The field associated to it is therefore a finite field which is necessarily a Galois field $GF(p^k)$ with p prime, the number of points being $p^k + 1$.

Theorem.

- 0. The finite Pappian plane is a Pappian plane.
- 1. The finite Pappian plane is not a Separable Pappian plane.

Proof: See Artzy, p. 210.

Definition.

If the field is the field of rationals, the Pappian plane is called the Rational Pappian plane.

Theorem.

- 0. The Rational Pappian plane is a Separable Pappian plane.
- 1. The Rational Pappian plane is not a Continuous Pappian plane.

Proof: See Artzy, p. 210.

Exercise.

Give a synthetic definition of a

- 0. The rational Pappian plane.
- 1. The quaternion plane.
- 2. The Cayleyian plane.
- 3. 2-Q plane.

It is clear how to proceed for the rational plane, imitating the definition of the rational numbers as equivalence classes of the integers. It is not known to me how to solve the other exercises.

1.10.10 Collineations and Correlations in Perspective to Pappian Planes.

Introduction.

For collineations, correlations and polarities in finite planes, see Dembowski, section 3.3 and Chapter 4.

Definition.

Given 1.10.1, we say that the vectors $\overline{AA'}$ and $\overline{PP'}$ are m -equal and we write $\overline{AA'} =_m \overline{PP'}$.

Definition.

In a Veblen-Wedderburn plane with ideal line m , the elements of the set \mathcal{V} are the equivalence classes of m -equal vectors and the addition of vectors is defined by

$$\overline{P_1P_2} + \overline{Q_2Q_3} := \overline{P_1P_3},$$

where

$$0. \quad Q_2 = P_2 \implies P_3 = Q_3,$$

$$1. \quad P_2, Q_2, Q_3 \text{ non collinear} \implies P_3 \text{ is the point defined by } \overline{P_2P_3} =_m \overline{Q_2Q_3},$$

$$2. \quad \text{if } P_2, Q_2, Q_3 \text{ collinear and } X \text{ is not on } Q_2 \times Q_3 \implies P_3 \text{ is the point defined by } \overline{P_2P_3} =_m \overline{Q_2Q_3}, \overline{P_2P_3} =_m \overline{Q_2Q_3}.$$

Theorem.

The addition of vectors is well defined and $(\mathcal{V}, +)$ is an abelian group.

This follows from the fact that any vector is equivalent to a vector $\overline{(0,0)(A,B)}$ for some A and B 1.90.2.1.

Theorem.

The translations in a Veblen-Wedderburn plane with ideal line m are collineations, in other words, the image of points P on a fixed line l are points P' on a line l' . Each collineation is an elation with axis m and center $m \times (A \times A')$.

Theorem.

For any line n , the n -translations in a Moufang plane are collineations, in other words, the image of points P on a fixed line l are points P' on a line l' . Each collineation is an elation with axis n and center $n \times (A \times A')$.

Definition.

In a in Veblen-Wedderburn Plane the pre correlation configuration is defined as follows, (See Fig. 25)

Hy0. $\{Q_i\}, u \iota Q_2, i, a, b, a' \iota Q_0,$

De. $U_1 := u \times a, D_2 := d \times a, x_1 := U_1 \times Q_1, C_1 := x_1 \times i,$

De. $c := C_1 \times Q_2, C_2 := c \times b, U_2 := b \times u, x_2 := U_2 \times Q_1,$

De. $D_1 := x_2 \times i, d := D_1 \times Q_2, D_2 := d \times a, x_3 := D_2 \times Q_1,$

De. $D'_2 := a' \times x_3, d' := D'_2 \times Q_2, D'_1 := d' \times i, x'_2 := D'_1 \times Q_1,$

De. $U'_2 := x'_2 \times u, b' := U'_2 \times Q_0, B' := b' \times q_2, U'_1 := a' \times u,$

De. $x'_1 := U'_1 \times Q_1, C'_1 := x'_1 \times i, c' := C'_1 \times Q_2, C'_2 := c' \times b',$

De. $x'_3 := C'_2 \times Q_1,$

Hy1. $C'_2 \iota x'_3,$

Let $(A) = a \times q_2, (B) = b \times q_2, (A') = a' \times q_2, (B') = b' \times q_2,$
then $D_2 = (B, B \cdot A, D'_2 = (B', B' \cdot A')), C_2 = (A, A \cdot B, C'_2 = (A', A' \cdot B')),$ If b' or B' is
chosen in such a way that $B \cdot A = B' \cdot A',$ the configuration requires $A \cdot B = A' \cdot B'.$ This
defines a correspondance γ between $X = A \cdot B$ and $X' = B' \cdot A.$

Exercise.

If we associate to $(Q), [Q]$ and to $(P_0, P_1), [P_0\gamma, P_1\gamma],$ is the correspondance is a correlation?
If not which of the axioms given below are required for the correspondance to be a correlation.

1.10.11 Three Nets in Perspective Geometry.**Definition.**

A three net associated to the 3 points A, B, C in a perspective plane is the set of points P
in the plane and the set of lines $P \times A, P \times B, P \times C.$

Theorem.

The coordinates of the lines of the three net associated to the points $(0), (1), (\infty)$ are $[0, P_0],$
 $[1, P_1], [P_2],$ where

$$P_0 := (((P \times (0)) \times v) \times Q_0) \times q_2,$$

$$P_1 := (((((P \times (1)) \times q_1)) \times (0)) \times v) \times Q_0) \times q_2,$$

$$P_2 := (((((P \times (\infty)) \times i) \times (0)) \times v) \times Q_0) \times q_2.$$

Lemma.

Let $Y_A = (0, A), Y_B = (0, B),$ then

$$(((Q_0 \times (1)) \times (Y_A \times (0))) \times (\infty)) \times (((Q_0 \times (\infty)) \times (Y_B \times (0))) \times (1)) = (A, A + B).$$

Definition.

Given $Q'_0 = (F, F + G),$ the F-G-sum of A and $B, A \oplus B$ is defined by

$$(((Q'_0 \times (1)) \times (Y_A \times (0))) \times (\infty)) \times (((Q'_0 \times (\infty)) \times (Y_B \times (0))) \times (1)) = (X, A \oplus B).$$

Theorem.

$$A \oplus B = (A \dashv G) + (F \vdash B).$$

$$X = A \dashv G.$$

Proof:

$X_A := ((Q'_0 \times (1)) \times (Y_A \times (0))) = (X, A)$ and $X + G = A$, therefore $X = A \dashv G$.
 $F_B := ((Q'_0 \times (\infty)) \times (Y_B \times (0))) = (F, B)$,
 if $Y_Z := ((F, B) \times (1)) \times q_1 = (0, Z)$, then $C = F + Z$ and $Z = F \vdash C$,
 finally $X_Y := (X_A \times (\infty)) \times (F_B \times (1)) = (X_A \times (\infty)) \times (Y_Z \times (1)) = (X, A \oplus B)$, therefore
 $(A \oplus B) = X + Z$, substituting for X and Z gives the Theorem.

Theorem.

(Σ, \oplus) is a loop.

The neutral element is $F + G$.

The solutions of $A \oplus B = C$ are given by

$$A = (C \dashv (F \vdash B)) + G, \quad B = F + ((A \dashv G) \vdash C).$$

Proof: The solutions follow directly from the preceding Theorem, the neutral element property follows from

$$(F + G) \oplus H = ((F + G) \dashv G) + (F \vdash H) = F + (F \vdash H) = H,$$

$$H \oplus (F + G) = (H \dashv G) + (F \vdash (F + G)) = (H \dashv G) + G = H.$$

Theorem.

The coordinates of the lines of the three net associated to the points Q_0, Q_1, Q_2 are $[P_1, 0]$, $[0, P_0]$, $[P_2]$, where

$$P_0 := (((P \times (0)) \times v) \times Q_0) \times q_2,$$

$$P_1 := (P \times Q_0) \times q_2,$$

$$P_2 := (((((P \times (\infty)) \times i) \times (0)) \times v) \times Q_0) \times q_2.$$

Exercise.

Determine Theorems analogous to those associated with (0) , (1) and (∞) . See Artzy, p. 206 and p.210, 15.

1.10.12 Bibliography.

0. Artin, Emil, Geometric Algebra, New York, Interscience Publishers, 1957. *Inter-science tracts in pure and applied mathematics*, no. 3.
1. Artzy, Rafael, Linear Geometry, Reading Mass., Addison-Wesley, 1965, 273 pp.
2. Bolyai, Farkas, Tentamen Juventutem Studiosam ein Elementa Mathiseos Parae, introducendi, Maros-Vasarhely, 1829, see Smith D. E. p. 375.
3. Bolyai, Janos, The Science Absolute of Space Independent of the Truth and Falsity of Euclid's Axiom XI, transl. by Dr George Brus Halstead, Austin, Texas, The Neomon, Vol. 3, 71 pp, 1886.
4. Bolyai, Janos, Appendix, the theory of space, with introduction, comments, and addenda, edited by Ferenc Karteszi, supplement by Barna Szenassy, Amsterdam, New York, North-Holland, New York, Sole distributors for the U.S.A. and Canada, Elsevier Science Pub. Co., 1987, North-Holland mathematics studies, 138.
5. Bruck R. H. and Ryser H. J., The non existence of certain finite projective planes, Can. J. Math., Vol. 1, 1949, 88-93.
6. Dedekind, Julius Wilhelm, Stetigkeit und Irrationalen Zahlen, 1872, see Smith D. E., p. 35. (I,9,p.1)
7. Dembowski, Peter, Finite Geometries, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer, New-York, 1968, 375 pp.
8. Enriques, Federigo, Lezioni di Geometria Proiettiva, Bologna, 1904, French Transl., Paris 1930.
9. Enriques, Federigo, Lessons in Projective Geometry, transl. from the Italian by Harold R. Phalen. Annandale-on-Hudson, N.Y., printed by the translator, [1932?].
10. Euler, Leonhard, Recherches sur une nouvelle espèce de quarrés magiques, Verh. Zeeuwsch. Genootsch. Wetensch. Vlissengen, Vol. 9, 1782, 85-239.
11. Fano, Gino, Sui Postulati Fondamentali della Geometria Proiettiva, Giorn. di mat., Vol. 30, 1892, 106-132. ($PG(n, p)$)
12. Hall, Marshall, Jr, Projective Planes, Trans. Amer. Math. Soc., Vol. 54, 1943, 229-277.
13. Hartshorne, Robin C., Foundation of Projective Geometry, N. Y. Benjamin, 1967, 161 pp.
14. Hilbert, David, Grundlagen der Geometrie, 1899, tr. by E. J. Townsend, La Salle, Ill., Open Court Publ. Cp., 1962, 143 pp.

15. *Hilbert, David*, The Foundations of Geometry, *authorized transl. by E.J. Townsend ... Chicago, The Open court publishing company; London, K. Paul, Trench, Trubner & co., ltd., 1902.*
16. *Klingenberg, Wilhelm*, Beweis des Desargueschen Satzes aus der Reidemeisterfigur und Verwandte Sätze. *Abh. Math. Sem. Hamburg, Vol. 19, 1955, 158-175.*
17. *Klingenberg, Wilhelm*, Grundlagen der Geometrie, *Mannheim, Bibliographisches Institut, 1971, B. I.-Hochschulschriften 746-746a.*
18. *Lam, C. W. H.*, The Search for a Finite Projective Planes of Order 10, *Amer. Math. Monthly, Vo. 98, 1991, 305-318.*
19. *Lam, C. W. H., Thiel, L. H. & Swiercz S.*, The non existence of finite projective planes of order 10, *Can. J. of Mat., Vol. 41, 1989, 1117-1123.*
20. *Lobachevskii, Nikolai Ivanovich*, see *Norden A.*, Elementare Einführung in die Lobachewskische Geometrie, *Berlin, VEB Deutscher Verlag der Wissenschaften, 1958, 259 pp.*
21. *Lobachevskii, Nikolai Ivanovich*, Geometrical Researches on the Theory of Parallels, *translated from the original by George Bruce Halsted, Austin, University of Texas, 1891.*
22. *Menger, Karl*, Untersuchungen über allgemeine Metrik, *Math. Ann. Vol. 100, 1928, 75-163.*
23. *Moufang, Ruth*, Alternativkörper und der Satz vom Vollständigen Vierseit, *Abh. Math. Sem. Hamburg, Vol. 9, 1933, 207-222.*
24. *Pickert. Gunter*, Projektive Ebenen, *Berlin, Springer, 1955, 343 pp.*
25. *Pieri*, Un Sistema di Postulati per la Geometria Proiettiva, *Rev. Mathém. Torino, Vol 6, 1896. See also Atti Torino, 1904, 1906.*
26. *Pieri*, I Principii della Geometria di Posizione, composti in Sistema Logico Deduttivo, *Mem. della Reale Acad. delle Scienze di Torino, serie 2, Vol.48, 1899, 1-62.*
27. *Reidemeister, Kurt*, Grundlagen der Geometrie, *Berlin, Springer, Grundl. der math. Wissens. in Einz., Vol. 32, 1968, (1930),*
28. *Saccheri, Giovanni Girolamo*, Euclides ab omni Naevo Vindicatus, *Milan, 1732. tr. George Halstead, London Open Court Pr. 1920, 246 pp. See Stäckel.*
29. *Schur, Friedrich*, Grundlagen der Geometrie, *mit 63 figuren im text. Leipzig, Berlin, B. G. Teubner, 1909.*
30. *Schur, Issai*, Gesammelte Abhandlungen, *Hrsg. von Alfred Brauer u. Hans Rohrbach, Berlin, Heidelberg, New York: Springer, 1973.*

31. *Stackel, Paul Gustav*, Die Theorie der Parallellinien von Euklid bis auf Gauss, eine Urkundensammlung zur Vorgeschichte der nichteuklidischen Geometrie, in Gemeinschaft mit Friedrich Engel, *hrsg. von Paul Stackel*, New York, Johnson Reprint Corp., 1968, *Bibliotheca mathematica Teubneriana*, Bd. 41.
32. *Tilly, Joseph Marie de*, Essai sur les Principes fondamentaux de Géométrie et de Mécanique, Bruxelles, Mayolez, 1879, 192 pp. Also, *Mém. Soc. science phys. et natur. de Bordeaux*, Vol III, Ser. 2, cahier 1.
33. *Tilly, Joseph Marie de*, Essai de Géométrie Analytique Générale, Bruxelles, 1892.
34. *Tarry, G.*, Le problème des 36 officiers, *C. R. Assoc. Franc. Av. Sci.*, Vol. 1 (1900), 122-123, Vol. 2 (1901), 170-203.
35. *Veblen, Oswald & Wedderburn, Joseph Henri MacLagan*, Non-Desarguesian and non-Pascalian Geometries, *Trans. Amer. Math. Soc.*, Vol. 8, 1907, 279-388.
36. *Veblen, Oswald & Young, John*, Projective Geometry, Wesley, Boston, I, 1910, II, 1918.

1.11 Mechanics.

²⁰

1.11.0 Introduction.

Geometry is to be the support of the description of phenomenon in the real world. I will briefly review Newton's laws and 2 results to be generalized, the central force theorem of Hamilton and the motion of the pendulum.

1.11.1 Kepler (1571-1630).

Introduction.

Among many of the contribution of Kepler those which perpetuate his name are his 3 laws of Mechanics and his equation discovered from 1605 to 1621. The first and third law are in Astronomi Nova, the second law and his equation in section V of his Epitome. ... We also know that an ellipse can be generated by moving a segment of length $a + b$ with one point on an axis and the other point on a perpendicular axis. 1.11.1.2 shows that the angle of the line is also the eccentric anomaly.?

²⁰30.10.87

Theorem.

If a point $P(x, y)$ is restricted to move on an ellipse with major axis $2a$, minor axis $2b$ and eccentricity e , and origin at a focus,

$$0. \quad x = a(\cos \circ E - e), \quad y = b \sin \circ E,$$

where E is the excentric anomaly.

If $E(0) = 0$, then $x(0) = ae$, $y(0) = 0$.

Let I be the identity function, the motion preserves area iff *Kepler's equation*

$$1. \quad I = E - e \sin \circ E$$

is satisfied.

If $v := \angle(A, F, P)$, called *true anomaly* then

$$2. \quad \tan v = \frac{b \sin E}{a(\cos E - e)}.$$

Finally, if the line through P makes an angle E with AF , and intersect the major axis at L and the minor axis at M ,

$$3. \quad PL = b, \quad PM = a.$$

Let A be twice the area $(0, 0)$, $(a, 0)$, (x, y) along the ellipse, divided by ab .

Let T be twice the area of the triangle $(0, 0)$, (x, y) , (x', y') divided by ab , then

$$\begin{aligned} 4. \quad T &= xy' - x'y \\ &= (\cos \circ E - e) \sin \circ E' - (\cos \circ E' - e) \sin \circ E \\ &= \sin \circ (E' - E) - e(\sin \circ E' - \sin \circ E), \end{aligned}$$

If $E' = E + \Delta E$, and ΔE is small, then

$$5. \quad \Delta A = (1 - e \cos \circ E) \Delta E.$$

Integrating gives

$$6. \quad A = E - e \sin \circ E.$$

Therefore, if the area A is a linear function, with a proper choice of the unit of time, $A = I$ and we have 1. Vice-versa, if 1. is satisfied then comparing 6, and 1, gives $A = I$ and the area is proportional to the time.

1.11.2 Newton (1642-1727).**1.11.3 Hamilton (1805-1865).****Theorem. [Hamilton]**

Assuming Newton's law, if a mass is to move on an ellipse, under a force passing through a fixed point (central force),

0. this force is proportional to the distance to the center and inversely proportional to the cube of the distance to the polar of the center of force.

1. the relation between the eccentric anomaly E and the time t is given by $aE(t) + c \sin(E(t)) = C t$.

Consider a conic with major axis of length $2a$ on the x axis, with minor axis of length $2b$ and with center at (c, d) , the parametric representation is

2. $x = c + a \cos \circ E$, $y = d + b \sin \circ E$.

The acceleration is

$$3.0. D^2x = -a \cos \circ E (DE)^2 - a \sin \circ E D^2E,$$

$$1. D^2y = -b \sin \circ E (DE)^2 + b \cos \circ E D^2E,$$

If we accept Newton's law, the acceleration has to be in the direction of the force, if the force is $f \circ E g \circ E$, where

$$4. (g \circ E)^2 = (c + a \cos \circ E)^2 + (d + b \sin \circ E)^2,$$

$g \circ E$ being the distance to the center of force,

$$5.0. D^2x = f \circ E (c + a \cos \circ E),$$

$$1. D^2y = f \circ E (d + b \sin \circ E),$$

$$6.0. -a \cos \circ E (DE)^2 - a \sin \circ E D^2E = f \circ E (c + a \cos \circ E),$$

$$1. -b \sin \circ E (DE)^2 + b \cos \circ E D^2E = f \circ E (d + b \sin \circ E),$$

hence equating 3.0 and 5.0 as well as 3.1 and 5.1 we get 6.0 and 6.1, the combinations

$$(-b \sin \circ E) 6.0. + (a \cos \circ E) 6.1. \text{ and}$$

$$(-b \cos \circ E) 6.0. - (a \sin \circ E) 6.1.$$

give

$$7.0. ab D^2E = f \circ E (ad \cos \circ E - bc \sin \circ E),$$

$$1. ab (DE)^2 = -f \circ E (ad \sin \circ E + bc \cos \circ E + ab).$$

Taking the derivative of this equation and subtracting $2DE$ times 7.0. gives

$$8. D(f \circ E)(ad \sin \circ E + bc \cos \circ E + ab) + 3f \circ E (ad \cos \circ E - bc \sin \circ E) DE = 0.$$

Integrating gives

$$9. f \circ E (ad \sin \circ E + bc \cos \circ E + ab)^3 = -aC_1$$

for some constant C_1 , but the polar of the origin is the line

$$b^2cx + a^2dy - b^2c^2 - a^2d^2 + a^2b^2 = 0,$$

therefore the distance of (x, y) to it is proportional to

$$b^2c(c + a \cos \circ E) + a^2d(d + b \sin \circ E) - b^2c^2 - a^2d^2 + a^2b^2$$

or to

10. $bc \cos \circ E + ad \sin \circ E + ab$,
hence part 1 of the theorem.

Replacing in 7.1. $f \circ E$ by its value gives

$$(DE)^2 = \frac{C}{(ad \sin \circ E + bc \cos \circ E + ab)^2},$$

therefore C_1 must be positive.

Let $C_1 = C^2$, then

11. $(ad \sin \circ E + bc \cos \circ E + ab)DE = C$,
and we obtain a generalization of Kepler's equation

12. $-ad \cos \circ E + bc \sin \circ E + ab E = CI$,

Let e and A be such that

13. $bc = ab e \cos(A)$, $ad = ab e \sin(A)$,
then

14. $e^2 = (\frac{c}{a})^2 + (\frac{d}{b})^2$,

15. $\tan(A) = \frac{ad}{bc}$.

Let

16. $F = E - A$ and $M = CI - ab A$,

then

17. $e \sin(F) + F = M$.

Comment.

If the center of the conic is the center of force, $c = d = 0$, $f \circ E$ is a constant and the force is proportional to the distance. If the center of force is on the conic, 1.11.3.7 becomes

$$f \circ E(ab)^3(1 - \cos \circ (E - E_0))^3 = -aC_1,$$

when the center of force is $c + a \cos(E_0)$, $d + b \sin(E_0)$.

When the conic is a circle,

$$g \circ E^2 = 2a^2(1 - \cos \circ (E - E_0))^2,$$

therefore, the force is inversely proportional to the 5-th power of the distance.?

Comment.

1.11.3.8 is proportional to $g \circ E$ if

$$h^2((c + a \cos \circ E)^2 + (d + b \sin \circ E)^2) = (a d \sin \circ E + b c \cos \circ E + a b)^2$$

expanding will give terms in \cos^2 , $\sin \cos$, \sin , \cos and 1.

The coefficient of $\sin \cos$ must be 0, hence $cd = 0$.

Let $d = 0$, the \sin term disappears and the coefficients of 1, $\cos \circ E$, $\cos^2 \circ E$ give

$$h^2(c^2 + b^2) = a^2b^2,$$

$$h^2(2ac) = 2b^2ac,$$

$$h^2(a^2 - b^2) = b^2c^2,$$

hence

$$h = b \text{ and } a^2 = b^2 + c^2$$

or

$$e := \frac{c}{a} = \sqrt{1 - \frac{b^2}{a^2}}.$$

Definition.

Given a curve (x, y) , the hodograph of the curve is the curve (Dx, Dy) .

Comment.

The concept was first introduced by Möbius (*Mechanik des Himmels*, (1843)), the name was chosen by Hamilton when he gave, independently, the definition in the *Proc. Roy. Irish Acad.*, Vol. 3, (1845-1847) pp. 344-353.

Theorem.

If the force is central, and the center is chosen as the origin, the hodograph of the hodograph is the original curve.

Indeed, the hodograph is $(D^2x, D^2y) = f \circ E(x, y)$.

Theorem.

If the central force obeys Newton's law, the hodograph of the ellipse, 0.0. is the circle

$$b^2((Dx)^2 + (Dy)^2) + 2a e CDy - C^2 = 0,$$

The proof is straightforward, the verification using

$$Dx = -a \sin \circ EDE, Dy = b \cos \circ EDE \text{ and 1.11.3.9, .16 is even simpler.}$$

If the equation of the circle is

$$(-R \sin(G), -k + R \cos(G)),$$

equating to $(-a \sin \circ EDE, b \cos \circ EDE)$ for $E = 0$ and π and therefore $G = 0$ and π , gives

$$bC = ab(-k + R)(1 + E), -bC = ab(-k - R)(1 - e), \text{ therefore}$$

$$-k + R = \frac{C}{a(1+e)}, k + R = \frac{C}{a(1-e)},$$

hence

$$R = C\left(\frac{a}{b}\right)^2, k = Re.$$

moreover

$$\cos(G) = e + \frac{b^2}{a^2} \frac{\cos \circ E}{1 + e \cos \circ E}.$$

1.11.4 Preliminary remarks extending mechanics to finite geometry.

Introduction.

The generalization of classical mechanics to finite geometry turned out to be a thorny task.

Lemma.

If x_0, y_0 is a solution of

$$x(p+1) - yp = 1,$$

all solutions are given by

$$x = x_0 + kp, y = y_0 + k(p+1),$$

or

$$x \equiv x_0 \pmod{p}, y \equiv y_0 \pmod{p+1}.$$

Definition.

Kepler's equation associated to the prime p is given by

$$(e \sin \circ E)(p+1) - (E - M)p = 1.$$

This definition can be justified as follows, first when p is very large, we get the classical Kepler equation. Moreover from Lemma 10.4.1. all solutions are such that $e \sin \circ E$ are equal modulo p and $E - M$ are equal modulo $p+1$ which are precisely the congruence relations for $e, \sin \circ E$ and for $E - M$.

Example.

For $p = 101, \dots$

Theorem.

(Of the circular hodograph of Hamilton). ...

1.11.5 Eddington (18?-1944). The cosmological constant.

Starting with the work of Edwin P. Hubble, (1934) there had been mounting observational astronomical evidence that the Universe is finite. This lead, Monseigneur Georges Lemaître to his hypothesis of the Primeval Atom and Sir Arthur Eddington to a possible a priori determination of the cosmical number $N = 3.68.2^{256} = 2.3610^{79}$. In his article published in 1944, in the Proc. of the Camb. Phil. Soc., he first describes the number "picturesquely as the number of protons and electrons in the universe" and "interprets it by the consideration of a distribution of hydrogen in equilibrium at zero temperature, because the presence of the matter produces a curvature in space, the curvature causes the space to close when the number of particles contained in it reaches the total N ".

If the work of Eddington would be reexamined today, protons and electron would probably be replaced by quarks, if it were to be reexamined at some time in the future some other particles might play the fundamental role. In any case the lectures of Lemaître and the work of Eddington have been a primary motivation for my work on finite Euclidean and non-Euclidean geometry. As will be examined in more details when application will be made to the finite pendulum, some elementary particle occupies a position and the possible positions are discrete, they do this at a certain time, but again the time is not a continuous function but a discrete monotonic function. The fact that there are no infinitesimals in finite geometry

*may very well be related to the uncertainty principle of Heisenberg (1927).
H. Pierre Noyes and ANPA*

1.12 Description of Algorithms and Computers.

*All the earlier proofs in Mathematics were constructive, these proofs not only showed the existence of objects, for instance the existence of the orthocenter of a triangle, where the 3 perpendiculars from the vertex to the opposite sides meet, but also how to construct that point, by giving an explicit construction for a perpendicular to a line from a point outside it. Little by little mathematicians have used more and more proofs using non constructive arguments, which show the existence of the object in question, without giving a method of construction. Such proofs are essential when no finite construction is possible, and are considered by many as intellectually superior to a constructive proof when this one is possible. In finite geometry, it is desirable to limit oneself to constructive proofs, although this is not always possible, at a given point in time. I will give 2 examples later, the proof of Aryabatha's theorem and the proof of the existence of primitive roots. Because in a finite geometry it is not easy to rely on tools such as the straightedge or the compass to experiment for the purpose of conjecturing theorems, it is useful if not necessary to rely on computer experiments. Moreover, although the simpler algorithm were for centuries given in the vernacular language, see for instance the description of the so called Chinese remainder theorem by Ch'in Chiui-Shao, in Ulrich Libbrecht's translation, often the description avoids special cases or is ambiguous. Careful description of algorithms started to appear with the advent of computers.*²¹

The first formula oriented language was FORTRAN which evolved to FORTRAN 4 then FORTRAN 77. It was developed empirically. ALGOL was developed in 1958 and its syntax carefully defined in 1960 using the Backus normal form to attempt to define a priori an algorithmic language with a carefully constructed block structure. Its immediate successors were ALGOL 68 and PASCAL. APL was developed by Iverson to describe carefully the logic of the hardware of computers. It was magistrally adapted for the programming of Mathematical problems. LISP and its family of languages were developed when a list structure is required. BASIC was created at Dartmouth, to allow all undergraduates to learn programming in a friendly environment. It is the language which has evolved the most since its early days especially by a small group at the Digital Equipment Corporation. This is the language which I found most useful to discover mathematical conjectures because of the flexibility it offers in changing the program while in core and in examining easily, when needed, intermediate results without prior planning. MAXIMA and its family of languages, MABEL, MATHEMAICA and other recently developed languages are sure to play a more and more important role in discoveries.

Elsewhere, I will describe some of the BASIC programs, that I have written to investigate new areas of Mathematics, as well as the style used in the program descriptions and in their documentation and use.

²¹Already in 1957, Lemaître used precise descriptions to communicate by letter with a person doing his calculations on a EUCLID mechanical calculator.

1.13 Notes.

1.13.1 On Babylonian Mathematics.

Besides estimating areas and volumes, the Babylonians had a definite interest in so called Pythagorean triples, integers a , b and c such that $a^2 = b^2 + c^2$. It is still debated if their interest was purely arithmetical or was connected with geometry. On the one hand Neugebauer, states

“It is easy to show that geometrical concepts play a very secondary part in Babylonean algebra, however extensively a geometrical terminology is used.” (p. 41)

However, more recent discoveries, let him state (p.46), that these “contributions lie in the direction of geometry”. One tablet computes the radius r of a circle which circumscribes an isosceles triangle of sides 50, 50 and 60. An other tablet gives the regular hexagon, and from this the approximation $\sqrt{3} = 1;45(1 + \frac{45}{60})$ can be deduced. $\dots(\sqrt{2} = 1;25), \dots \pi = 3;7,30(3\frac{1}{8}), \dots$ ”.

He also describes, with Sachs, the data contained in tablet 322 of the Plimpton library collection from Columbia University (see Neugebauer and Sachs, vii and 38-41) as clearly indicating a relationship with right triangles “with angles varying regularly between almost 45 degrees to almost 31 degrees”, while Bruins interpretation of the same table is purely algebraic. In fact the variation although monotonic is not that regular and the last triangle corresponds to 31.84 degrees.

Freiberg

The tablet, dated 1900 to 1600 B.C., gives, with 4 errors, and in hexadesimal notation 15 values of

$$a, b, \text{ and } (\frac{a}{c})^2 = \sec^2(B)$$

where B is the angle opposite b ,

from 249159[159]15 or 169119 $\frac{7155}{3600}$

to 5356[1]2313464₀ or $\frac{17977600}{1296000}$.

Where the values between brackets are reconstructed values and 56 should be corrected to 28.

1.13.2 On Plimpton 322, Pythagorean numbers in Babylonean Mathematics.

The tablet gives in hexadesimal notation columns I, II, III and IV, except for the line labelled 11a in column IV. *diff.* is the difference between the numbers in column IV. The numbers in the second line give, in hexadesimal notation $\frac{u}{v}$ and $\frac{v}{u}$, for instance $2;24 = 2 + \frac{24}{60} = \frac{12}{5}$.

IV	v	u	III a	c	II b	I B	$(\frac{a}{c})^2$	diff.
1	5	12	169	120	119	44.7603	1.9834	
	2;	24,	0;	25,				
2	27	64	4825	3456	3367	44.2527	1.9492	−.034244
	2;	22, 13, 20,	0;	25, 18, 45,				
3	32	75	6649	4800	4601	43.7873	1.9188	−.030356
	2;	20, 37, 30,	0;	25, 36,				
4	54	125	18541	13500	12709	43.2713	1.8862	−.032554
	2;	18, 53, 20,	0;	25, 55, 12,				
5	4	9	97	72	65	42.0750	1.8150	−.071240
	2;	15,	0;	26, 40,				
6	9	20	481	360	319	41.5445	1.7852	−.029815
	2;	13, 20,	0;	27,				
7	25	54	3541	2700	2291	40.3152	1.7200	−.065209
	2;	9, 36,	0;	27, 46, 40,				
8	15	32	1249	960	799	39.7703	1.6927	−.027274
	2;	8,	0;	28, 7, 30,				
9	12	25	769	600	481	38.7180	1.6427	−.050040
	2;	5,	0;	28, 48,				
10	40	81	8161	6480	4961	37.4372	1.5861	−.056547
	2;	1, 30,	0;	29, 37, 46, 40,				
11	1	2	5	4	3	36.8699	1.5625	−.023623
	2;		0;	30,				
11a	64	125	19721	16000	11529	35.7751	1.5192	−.043290
	1;	57, 11, 15,	0;	30, 43, 12,				
12	25	48	2929	2400	1679	34.9760	1.4894	−.029793
	1;	55, 12,	0;	31, 15,				
13	8	15	289	240	161	33.8550	1.4500	−.039399
	1;	52, 30,	0;	32,				
14	27	50	3229	2700	1771	33.2619	1.4302	−.019779
	1;	51, 6, 40,	0;	32, 24,				
15	5	9	106	90	56	31.8908	1.3872	−.043078*
	1;	48,	0;	33, 20,				

There are 2 interpretations for the method of obtaining this table. The method of Neugebauer and Sachs, assumes the knowledge of the formulae

$$a = u^2 + v^2, b = u^2 - v^2, c = 2uv.$$

It was proven later that all integer solutions of $a^2 = b^2 + c^2$, can be obtained from these formulae and that the values of a , b and c are relatively prime if u and v are relatively prime and not both odd. They observe that u and v are always regular, it is, have only 2, 3 and 5 as divisors, this implies that the reciprocals have a finite representation if we use hexadecimal notation.

This point of view is confirmed if we observe that u and v are precisely all the regular numbers, which are relatively prime, satisfying

$$0. (\sqrt{2} - 1)u < v < u \leq 125,$$

except for the added pair, 11a, $u = 125$, $v = 64$. The first condition corresponds to requiring that the triangle has an angle B opposite b less than 45 degrees. In this range, only one pair is such that u and v are both odd. This is the pair $u = 9$, $v = 5$, which gives $a = 106$, $b = 56$, $c = 90$. The values $a = 53$, $b = 45$, $c = 28$, could have been obtained with $u = 7$ and $v = 2$, but these numbers are not both regular. It is interesting that one of the errors occurs for this pair, a being divided by 2 but not b .

The other point of view is presented by Bruins which claims that a and b are obtained from a subset of tables of reciprocals, which we could write $\frac{u}{v}$ and $\frac{v}{u}$, giving the values of a and b , because of

$$\left(\frac{u}{v} + \frac{v}{u}\right)^2 = \left(\frac{u}{v} - \frac{v}{u}\right)^2 + 2^2,$$

after removing the common factors, which are necessarily 2, 3 or 5. This would give the table for monotonically varying values of $\frac{a}{c}$.

We have given the corresponding hexadesimal values of $\frac{u}{v}$ and $\frac{v}{u}$ on alternate lines.

Condition 0. adds credibility to the point of view of Neugebauer and would strengthen the geometrical content of the table. A hope to get a deciding clue from one of the errors in the table is not easily fulfilled. Indeed the second line gives for a and b , 11521 and 3367, instead of 4825 and 3367.

One explanation, which I consider farfetched, is given by Gillings. He assumes that 11521 is obtained using $(64 + 27)^2 + 2 * 27 * 60$. This requires several errors, first to add before squaring, then to add $2 * 27 * 60$, which is explained by Gillings by the use of

$$u^2 + v^2 = (u + v)^2 - 2uv$$

with $-$ replaced by $+$ and $v = 64$ replaced by $v = 60$. An other explanation, only slightly less farfetched is to observe that, if we use Bruins approach, both numbers 2;22,13,20 and 0;25,18,45 have to be divided 3 times by 5, (or multiplied by 12 in hexadesimal notation).

This gives for a , 1,20,25 in base 60. If we assume that the scribe wrote instead 1,20,,25, using a large space, rather than a small one, and multiplies by 12 twice more, we get 3,12,1.

An other explanation could start by explaining why the scribe computed instead of

$$(64(= 60 + 4))^2 + (27(= 24 + 3))^2 = 4825,$$

$$(100(= 60 + 40))^2 + (39(= 36 + 3))^2 = 11521.$$

The argument could be decided if other tablets which continue this table are found. The table *Plimpt.tab*, gives the values for angles less than 31.5 degrees, using criteria 0.

There is an other minor controversy in the literature concerning the fact that the 1 in column IV is visible or not in the tablet. If the opinion is taken, which is contrary to Neugebauer, that 1 is not there, column I is then $(\frac{b}{c})^2 = \tan^2(\text{angle opposite } b) = (\frac{1}{2}(\frac{u}{v} - \frac{v}{u}))^2$ instead of $(\frac{a}{c})^2 = (\frac{1}{2}(\frac{u}{v} + \frac{v}{u}))^2$.

CHAPTER I

FINITE PROJECTIVE

GEOMETRY

1.90 Answers to problems and miscellaneous notes.

1.90.1 Algebra and modular arithmetic.

Example.

*Modulo 7, the inverses of 1 through 6 are respectively
1, 4, 5, 2, 3, 6.*

Answer to **??.**

Notes for section on axiomatic, Pieri (coxeter, p. 12), Menger (Coxeter, p. 14) Dedekind (Coxeter, p 22), Enriques (Coxeter, p.22)

The following does not work, leave for examination of other types, 1 where the triangles have sides through Q_1 and Q_2 may give something, see also Pickert p. 74, 75, 80

1.90.2 Linear Associative Planes.

Axiom. [2-point Desargues]

The 2-point Desargues axiom is the special case when we restrict Desargues' axiom to the case when the center C of the configuration is one of 2 given points Q_1 or Q_2 of the given axis c . More specifically, $C \iota c$, and for the 2 triangles $\{A_i\}$ and $\{B_i\}$,

let $C_i := (A_{i+1} \times A_{i-1}) \times (B_{i+1} \times B_{i-1})$,

$c_i := (A_i \times B_i)$, $c_i \iota C$, $i = 0, 1, 2$, incidence($A_0 \times A_j, B_0 \times B_j, c$), $j = 1, 2$,

\implies incidence($A_1 \times A_2, B_1 \times B_2, c$). We write

2-point-Desargues($C, \{A_i\}, \{B_i\}; \langle C_i \rangle, c$).

Theorem.

Given 2 triangles $\{A_i\}$ and $\{B_i\}$, let $C_i := (A_{i+1} \times A_{i-1}) \times (B_{i+1} \times B_{i-1})$, $C_i := A_i \times B_i$, and $C := c_1 \times c_2$,

$\langle C_i, c \rangle$ and $C \iota c \implies c_0 \iota C$. We write

2-point-Desargues $^{-1}(c, \{A_i\}, \{B_i\}; \langle c_0, c_1, c_2 \rangle, C)$

Proof: 2-point-Desargues($C_0, \{A_1, B_1, C_2\}, \{A_2, B_1, C_1\}; \langle B_0, A_0, C \rangle, c$).

Definition.

A linear associative plane is a perspective plane for which the 2-point Desargues axiom is satisfied for 2 specific points on a specific line of the plane.

If the line is q_2 and the points are Q_1 and Q_2 , we have

Theorem.

In a linear associative plane, the ternary ring $(\Sigma, *)$ is a \dots , more specifically:

- 0. $(\Sigma, *)$ is linear, $a * b * c = a \cdot b + c$,
- 1. $(\Sigma, +)$ is a group,
- 2. $(\Sigma - \{0\}, \cdot)$ is a loop,
- 3. $(\Sigma, *) = (\Sigma, +, \cdot)$ is right distributive, $(a + b) \cdot c = a \cdot c + b \cdot c$.
- 4. $a \neq b \implies x \cdot a = x \cdot b + c$ has a unique solution.

before

1.90.3 Veblen-Wedderburn Planes.

Chapter 2

FINITE PROJECTIVE GEOMETRY

2.0 Introduction.

In Section 1, I give the axiomatic definition of synthetic projective geometry. In Section 2, I give an algebraic model of projective geometry. Although I will use, whenever possible a synthetic proof, I will use extensively an algebraic proof to proceed more expeditiously, if not more elegantly. The reader is encouraged to replace these by the more satisfying synthetic proofs. In Section 3, I discuss the geometric model of the projective plane of order 2, 3 and 5, discovered by Fernand Lemay and relate each model to classical configurations.

2.1 Synthetic Finite Projective Geometry.

2.1.0 Introduction.

Projective Geometry implies usually that when we write down the equivalent algebraic axioms, the underlying field is the field of reals. Most of the properties that I will discuss in this Chapter and in the next one are valid whatever the field chosen. To deal with a set of Axioms which characterize the plane, in a simpler setting, I will assume instead that the field is finite. See 2.1.3. Most properties generalize to any field.

2.1.1 Notation.

The objects or elements of plane projective geometry are points and lines. The relation between points and lines is called incidence. A point and a line are incident if and only if the point is on the line or if the line passes through the point.

Identifiers are sequences of letters and digits, starting with a letter. If the first letter is a lower case letter, the identifier will denote a line. If the first letter is an upper case letter, the identifier will denote a point. If the line ab is constructed as the line through the points A and B , we write

$$ab := A \times B.$$

If the point A_0 is constructed as the point on both a_1 and a_2 , we write

¹G20.TEX [MPAP], September 9, 2019

$$A_0 := a_1 \times a_2.$$

The symbol “ $:=$ ” pronounced “is defined as” indicates a definition of a new point or of a new line. The symbol “ \times ” will be justified in 2.2.2.

$$A \cdot ab = 0, \text{ or } A \iota ab,$$

is an abbreviation for the statement “the point A is on the line ab ”.

$$A \cdot ab \neq 0 \text{ or } A \nmid ab,$$

is an abbreviation for the statement “the point A is not on the line ab ”.

$$A = B, x = y,$$

are abbreviations for “the points A and B or the lines x and y ”, all previously defined, “are identical”.

$$\{A, B, C\} \text{ or } \{a, b, c\}$$

denotes a triangle with vertices A, B and C or sides a, b and c .

For Projective Geometry over fields we will use the following Axioms.

2.1.2 Axioms.

Of incidence and existence or of alignment:

0. Given 2 distinct points, there exists one and only one line incident to, or passing through, the 2 points.
1. Given 2 distinct lines, there exists one and only one point incident to, or on, the 2 lines.
2. There exists at least 4 points, any 3 of which are not collinear.

Of Pappus:

3. Let A_0, A_1, A_2 be distinct points on a ,
let B_0, B_1, B_2 be distinct points on b .
Let C_0 be the intersection of $A_1 \times B_2$ and $A_2 \times B_1$ or
 $C_0 := (A_1 \times B_2) \times (A_2 \times B_1)$.
Similarly, let
 $C_1 := (A_2 \times B_0) \times (A_0 \times B_2), C_2 := (A_0 \times B_1) \times (A_1 \times B_0)$,
then the points C_0, C_1, C_2 are collinear. (Fig. 1a)

Notation.

The subscript i is usually restricted to the set $\{0, 1, 2\}$ and addition is then done modulo 3. I write

$\text{Pappus}(\langle A_i \rangle, \langle B_i \rangle; \langle C_i \rangle)$ or more generally

$\text{Pappus}(\langle A_i \rangle[a], \langle B_i \rangle[b]; \langle C_i \rangle[c], X]$.

where “ $\langle X_i \rangle$ ” indicate that the points X_i are collinear, where the brackets indicate that what is between them need not be given, and where X , if written, is the intersection of a and b .

The axiom is trivially satisfied if X is one of the points A_i or B_i . If the axiom is used in proofs, it is always assumed that the points A_i and B_i are distinct from X .

Any plane satisfying the alignment axioms and the axiom of Pappus is called a Pappian plane. For Projective Geometry over a specific field we will add one axiom or a set of associated axioms, for instance, for finite Projective Geometry over a Z_p^k , we add

2.1.3 Axiom (the finite field).

On the line l there are exactly $p^k + 1$ points, p a prime.

Exercise.

Write down the appropriate existence axiom associated with the fields,

- 0. R , classical Projective Geometry ,*
- 1. C , complex Projective Geometry,*
- 2. Q , rational Projective Geometry.*

2.1.4 Basic consequences.

Theorem.

- 0. Each line is incident to exactly $p^k + 1$ points.*
- 1. Each point is incident to exactly $p^k + 1$ lines.*
- 2. There are exactly $p^{2k} + p^k + 1$ points and lines.*

The proof is left as an exercise.

Corollary.

There exists at least 4 lines, any 3 of which are not incident.

Comment.

If, contrary to 2.1.2.2, there is only one point P not on the line l , the geometry reduces to l , to a { pencil } of $p + 1$ lines through P , to P and to a set of $p + 1$ points on l . The axiom of Pappus is satisfied vacuously because no 2 distinct lines contain 3 points each.

Definition.

The line through C_0 , C_1 and C_2 , in the axiom of Pappus, is called the Pappus line.

Notation.

I introduce in the next Chapter a detailed notation for algebraic projective geometry. An incomplete notation for the synthetic approach will now be introduced. The purpose is to formalize the Theorems, without the details of the approach of Russell and Whitehead.

$\langle X_i \rangle$ or $(\langle X_i \rangle, x)$ indicates that the points X_i are collinear and distinct, on x ,

$\langle x_i \rangle$ or $(\langle x_i \rangle, X)$ indicates that the lines x_i are incident and distinct, through X ,

$\{X_i\}$ indicates that the points X_i are distinct and not collinear, in other words form a triangle and similarly for the sides, $\{x_i\}$.

$\text{incidence}(A, B, C, l)$ or $\text{incidence}(A_j, l)$, $j \in \{0, 1, \dots, k\}$, $k \leq 2$,

is used to state that the points A, B, C or the points A_j are on the same line l . “[l]” indicates that the name of the line need not be given explicitly.

$\text{incidence}(a, b, c, L)$ or $\text{incidence}(a_j, L)$

is the corresponding statement for lines a, b, c or a_j incident to the point L .

No. $\text{Pappus}(\langle A_i \rangle, \langle B_i \rangle; \langle C_i \rangle)$ and the corresponding axioms can be written, in greater detail, as follows.

Hy0. $\langle A_i \rangle$.

Hy1. $\langle B_i \rangle$.

De. $C_i := (A_{i+1} \times B_{i-1}) \times (A_{i-1} \times B_{i+1})$.

Co. $\langle C_i \rangle$.

“No” is an abbreviation for “nomenclature” or “notation”, “Hy”, for “hypothesis”, “De”, for “Definition”, “Co” for “conclusion”.

Notice that the order of the points is important.

The reciprocal,

$\text{Pappus}^{-1}(\langle A_i \rangle, \langle C_i \rangle; \langle B_i \rangle)$

exchanges Hy1. and Co. and follows from

$\text{Pappus}(\langle A_i \rangle, \langle C_i \rangle; \langle B_i \rangle)$.

In a statement, different letters indicate different elements with no special relationship between them except as stated in the hypotheses “Hy”.

Theorem.

$\text{Pappus}(\langle A_i \rangle, \langle B_i \rangle; \langle C_i \rangle) \implies \text{Pappus}(\langle A_0, B_1, C_2 \rangle, \langle B_0, C_1, A_2 \rangle; \langle C_0, A_1, B_2 \rangle)$.

2.1.5 The Theorem of Desargues.**Theorem. [Desargues]**

Hy0. $\{A_i\}, \{B_i\}$,

De0. $c_i := A_i \times B_i$,

Hy1. $C \iota c_i$,

De1. $a_i := A_{i+1} \times A_{i-1}$,

De2. $b_i := B_{i+1} \times B_{i-1}$,

De3. $C_i := a_i \times b_i$,

Co. $(\langle C_i \rangle, c)$.

No. $\text{Desargues}(C, \{A_i\}, \{a_i\}, \{B_i\}, \{b_i\}; \langle C_i \rangle, \langle c_i \rangle, c)$.

This is the notation for the following statements.

Given two triangles $\{A_0, A_1, A_2\}$ and $\{B_0, B_1, B_2\}$, such that the lines $A_0 \times B_0$, $A_1 \times B_1$ and $A_2 \times B_2$ have a point C in common. Let

$$C_0 := (A_1 \times A_2) \times (B_1 \times B_2), C_1 := (A_2 \times A_0) \times (B_2 \times B_0),$$

$$C_2 := (A_0 \times A_1) \times (B_0 \times B_1).$$

Then C_0, C_1, C_2 are incident to the same line c (Fig. 3a). It is assumed that the triangles are distinct and that the lines c_i are distinct.

This theorem can be proven using the incidence axioms in 3 dimensions. In 2 dimensions, it can be taken as an axiom or it can be derived from the axiom of Pappus, see 2.1.8. But the axiom of Pappus does not derive from the incidence axioms and the Theorem of Desargues taken as axiom.

Theorem.

The axiom of incidence and the axiom of Pappus 2.1.2.4. imply the Theorem of Desargues. See 2.1.8.

2.1.6 Configurations.

Introduction.

One of the characteristics of synthetic geometry is to start from a set of points and lines, to construct from them new points and lines and to extract known sets which have known properties. Hence, it is useful to describe some of the important sets, which are called configurations. We have seen 2 such configurations. In that of Pappus, we have 9 points and 9 lines. In that of Desargues, we have 10 points and 10 lines. I will define here the complete quadrangle and the complete quadrilateral configuration, the special Desargues configuration, as well as closely related configurations. To characterize the configuration further, I will use the following notation:

Notation.

$$10 * 3 \& 10 * 3, (11)$$

indicates that each of the 10 points are incident to 3 lines, that each of the 10 lines are incident to 3 points and that the construction requires 11 independent data elements (2 for a given point or line, 1 for a point on a given line or a line through a given point). Or

$$3 * 6 + 8 * 3 \& 12 * 3 + 3 * 2,$$

indicates that 3 points are incident to 6 lines, that 8 points are incident to 3 lines and that 12 lines are incident to 3 points and that 3 lines are incident to 2 points. The order chosen is that of decreasing number of incident elements.

The notation does not uniquely define the configuration but is a useful tool.

Definition.

A confined configuration is a configuration in the description of which “ $ 2$ ” does not occur. Except for the triangle and the complete quadrangle or quadrilateral, I will restrict the word*

configuration to confined configuration and will use the adjective “non confined” otherwise. A self dual type configuration is one for which the information to the left of “ \mathcal{E} ” is the same as that to the right.

It should not be confused with the notion of self dual configuration that will be introduced later. A self dual configuration is a self dual type configuration but not vice-versa.

Theorem.

The configuration of Pappus is of type $9 * 3 \& 9 * 3, (10)$. It can be viewed as a degenerate case of that of Pascal. See 2.2.11. Hence the alternate name *Pappus-Pascal hexagon*: If the alternate points of the hexagon $A_0, A_1, A_2, A_3, A_4, A_5$ are on 2 lines, the three pairs of opposites sides of the hexagon meet in 3 collinear points P_0, P_1 and P_2 .

The correspondence between this notation and that used in the Theorem of Pappus is:

$$\begin{array}{cccccccccc} A_0, & A_1, & A_2, & A_3, & A_4, & A_5, & P_0, & P_1, & P_2, \\ B_2, & A_1, & B_0, & A_2, & B_1, & A_0, & C_0, & C_2, & C_1. \end{array}$$

Theorem.

The configuration of Desargues is of type $10 * 3 \& 10 * 3, (11)$.

It can also be viewed as consisting of 2 pentagons which are inscribed one into the other. The points P_0, P_1, P_2, P_3, P_4 and the points Q_0, Q_1, Q_2, Q_3, Q_4 being such that P_0 is on $Q_0 \times Q_1$, P_1 is on $Q_1 \times Q_2$, P_2 is on $Q_2 \times Q_3$, P_3 is on $Q_3 \times Q_4$ and P_4 is on $Q_4 \times Q_0$. Q_0 is on $P_1 \times P_3$, Q_1 is on $P_2 \times P_4$, Q_2 is on $P_3 \times P_0$, Q_3 is on $P_4 \times P_1$ and Q_4 is on $P_0 \times P_2$.

The correspondence between this notation and that used in the Theorem of Desargues is:

$$\begin{array}{cccccccccc} P_0, & P_1, & P_2, & P_3, & P_4, & Q_0, & Q_1, & Q_2, & Q_3, & Q_4, \\ B_1, & A_0, & B_2, & A_1, & C_1, & C_2, & B_0, & C, & A_2, & C_0. \end{array}$$

Definition.

A complete quadrangle is a configuration consisting of 4 points A_0, A_1, A_2, A_3 , no 3 of which are on the same line and of the 6 lines through each pair of points: $a_0 := A_0 \times A_1$, $a_1 := A_0 \times A_2$, $a_2 := A_0 \times A_3$, $a_3 := A_2 \times A_3$, $a_4 := A_3 \times A_1$, $a_5 := A_1 \times A_2$. (Fig. 2a)

It is of type

$$4 * 3 \& 6 * 2, (8).$$

Definition.

The 3 points $D_0 := a_0 \times a_3$, $D_1 := a_1 \times a_4$ and $D_2 := a_2 \times a_5$ are called the diagonal points of the complete quadrangle.

The lines d_i joining the diagonal points are called diagonal lines.

These form, together with the quadrangle configuration, the completed non confined quadrangle configuration. See Fig. 2a'.

Definition.

Given a complete quadrangle, a conic2 pseudo non confined configuration is the sub configuration consisting of 3 of the points and the 3 lines joining these points to the 4-th one. It

is of type

$$1 * 3 + 3 * 1 \text{ \& } 1 * 3 + 3 * 1. \quad (8)$$

See 2.2.11.

Definition.

Given a complete quadrangle, a completed quadrangle configuration is the configuration consisting of the complete quadrangle, the diagonal points and the lines joining the diagonal points.

Theorem.

0. If $p = 2$ the completed quadrangle configuration is of type

$$7 * 3 \text{ \& } 7 * 3, (8).$$

See 2.1.13 and 2.2.11

1. If $p > 2$, it is of type

$$3 * 4 + 4 * 3 \text{ \& } 6 * 3 + 3 * 2 \quad (8)$$

and is not confined.

Definition.

A complete n -angle is a configuration consisting of n points no 3 of which are on the same line and of the $\frac{n(n-1)}{2}$ lines through each pair of points.

Theorem.

A complete 5-angle does not exist if $p < 5$. Indeed, on the line through 2 of the points, we must have 3 other points which are the intersection with the 3 pairs of lines through the other 3 points. We must have therefore at least 5 points on each line.

Exercise.

For which value of p does a complete n -angle exist for $n > 5$?

Definition.

A complete quadrilateral is a configuration consisting of 4 lines a_0, a_1, a_2, a_3 , no 3 of which are incident to the same point and of the 6 points through each pair of lines: $A_0 := a_0 \times a_1$, $A_1 := a_0 \times a_2$, $A_2 := a_0 \times a_3$, $A_3 := a_2 \times a_3$, $A_4 := a_3 \times a_1$, $A_5 := a_1 \times a_2$. (Fig. 2b)

It is of type

$$6 * 2 \text{ \& } 4 * 3, (8).$$

Definition.

The 3 lines $A_0 \times A_3$, $A_1 \times A_4$ and $A_2 \times A_5$ are called the diagonal lines of the complete quadrilateral.

The points joining the diagonal lines are called diagonal points. These together with the complete quadrilateral configuration form the completed quadrilateral non confined configuration (Fig. 2b').

Definition.

The special Desargues configuration, consists of 13 points and 13 lines obtained as follows. A_0, A_1, A_2, C is a complete quadrilateral,

$$\begin{aligned} a_0 &:= A_1 \times A_2, a_1 := A_2 \times A_0, a_2 := A_0 \times A_1, \\ c_0 &:= C \times A_0, c_1 := C \times A_1, c_2 := C \times A_2, \\ B_0 &:= a_0 \times c_0, B_1 := a_1 \times c_1, B_2 := a_2 \times c_2, \\ b_0 &:= B_1 \times B_2, b_1 := B_2 \times B_0, b_2 := B_0 \times B_1, \\ C_0 &:= a_0 \times b_0, C_1 := a_1 \times b_1, C_2 := a_2 \times b_2, \\ r_0 &:= A_0 \times C_0, r_1 := A_1 \times C_1, r_2 := A_2 \times C_2, \\ R_0 &:= r_1 \times r_2, R_1 := r_2 \times r_0, R_2 := r_0 \times r_1, \\ c &:= C_1 \times C_2. \text{ (Fig. 3e')} \end{aligned}$$

This configuration is also called the quadrangle-quadrilateral configuration. The quadrangle is $\{R_i, C\}$ or $\{c_i, r_i\}$, the quadrilateral is $\{b_i, c\}$ or $\{C_i, B_i\}$. The diagonal points are A_i and the diagonal lines, a_i .

Comment.

The dual construction can be obtained with the upper case letters exchanged for the lower case ones except for the exchange of B_i and r_i and b_i and R_i .

This configuration plays an essential role in Euclidean Geometry. An example consist of a triangle $\{A_i\}$, C the barycenter, a_i , the sides, c_i , the medians, B_i , the mid-points, b_i , the sides of the complementary triangle, C_i , the directions of the sides, r_i , the sides of the anticomplementary triangle, R_i , its vertices, c , the ideal line.

Definition.

Given a complete quadrangle-quadrilateral configuration, a conic3 pseudo non confined configuration is the sub configuration consisting of the quadrangle

$\{R_i, C\}$ and the quadrilateral $\{b_i, c\}$. It is of type

$$1 * 3 + 3 * 1 \text{ \& } 1 * 3 + 3 * 1 \text{ (8).}$$

See 2.2.11.

Theorem. [Special Desargues]

0. C_0 is on c ,

1. R_0 is on c_0 , R_1 is on c_1 , R_2 is on c_2 .

2. If $p = 3$ the special Desargues configuration is of type

$$13 * 4 \& 13 * 4 \quad (8)$$

See 2.1.6

If $p > 3$, it is of type

$$9 * 4 + 4 * 3 \& 9 * 4 + 4 * 3, (8).$$

3. If we exclude $r_0, r_1, r_2, R_0, R_1, R_2$, we obtain a special case of the Desargues configuration in which

$$P_0 \text{ is on } A_1 \times A_2, P_1 \text{ is on } A_2 \times A_0 \text{ and } P_2 \text{ is on } A_0 \times A_1.$$

The proof will be given in section 2.1.8.

Definition.

c is called the polar of C with respect to the triangle $\{A_0, A_1, A_2\}$. C is called the pole of c with respect to the triangle.

Notation.

Part of Definition 2.1.6 and Theorem 2.1.6 can be noted as follows.

No. Special Desargues($C, A_i; C_i, c$).

De0. $a_i := A_{i+1} \times A_{i-1}$.

De1. $B_i := a_i \times (C \times A_i)$.

De2. $C_i := a_i \times (B_{i+1} \times B_{i-1})$.

Co. $(\langle C_i \rangle, c)$.

Exercise.

Construct the configuration starting from R_i, C , and prove the 4 incidence properties corresponding to 2.1.6 in this construction.

Exercise.

For $p = 3$, prove that B_i is on r_i and C is on c . See also 2.2.11.

For a connection between conics and the quadrangle-quadrilateral configuration, when $p = 3$, see 2.2.11.

2.1.7 Other Configurations.

Introduction.

There exist 2 other configurations of type $9 * 3 \& 9 * 3$, these will be constructed and defined. Many special cases of Desargues configurations will be defined, as well as the extended special Desargues configuration and the dodecahedral configuration. I end by making some comments on the complete triangle in the more general case of the perspective plane.

Definition.

H0.0. A_i, M, d_0 ,
 H0.1. $A_0 \iota d_0$,
 D0.0. $a_i := A_{i+1} \times A_{i-1}$,
 D1.0. $d_1 := M \times A_1, d_2 := M \times A_2$,
 D1.1. $B_i := d_i \times a_i$,
 D1.2. $mm_0 := B_1 \times B_2, MA_0 := mm_0 \times a_0$,
 D1.3. $eul := M \times MA_0, C_0 := eul \times d_0$,
 D1.4. $c_2 := B_2 \times C_0, c_1 := B_1 \times C_0$,
 D1.5. $C_1 := d_1 \times c_2, C_2 := d_2 \times c_1, c_0 := C_1 \times C_2$,
 then
 C0.0. $B_0 \iota c_0$, (Fig. 1c')

This defines the extended 2-Pappus Configuration.

Definition.

The 2-Pappus Pseudo Configuration is the subset of the extended 2-Pappus Configuration consisting of the point A_i, B_i, C_i and of the lines a_i, b_i, c_i (Fig. 1c).

Theorem.

The extended 2-Pappus Configuration is of type

$$3 * 4 + 8 * 3 \ \& \ 3 * 4 + 8 * 3, (9).$$

The 2-Pappus Pseudo Configuration is of type

$$9 * 3 \ \& \ 9 * 3, (9).$$

The proof is left as an exercise.

Definition.

H0.0. A_i, M, c_2 ,
 H0.1. $A_1 \iota c_2$,
 D0.0. $a_i := A_{i+1} \times A_{i-1}$,
 D1.0. $X_0 := c_2 \times a_1$,
 D1.1. $ma_1 := M \times A_1, ma_2 := M \times A_2, B_1 := ma_1 \times a_1, B_2 := ma_2 \times a_2$,
 D1.2. $x_0 := X_0 \times B_2, X_1 := a_0 \times x_0, x_1 := X_1 \times M, C_1 := x_1 \times c_2$,
 D1.3. $b_0 := B_1 \times B_2, C_0 := b_0 \times c_2, c_0 := A_2 \times C_1$,
 D1.4. $c_1 := A_0 \times C_0, C_2 := c_0 \times c_1$,
 D1.5. $b_1 := B_2 \times C_1, b_2 := B_1 \times C_2, B_0 := b_1 \times b_2$,
 then
 C1.0. $B_0 \iota a_0$, (Fig. 1d')

This defines the extended 1-Pappus Configuration.

Definition.

The 1-Pappus Pseudo Configuration is the subset of the extended 1-Pappus Configuration consisting of the point A_i, B_i, C_i and of the lines a_i, b_i, c_i , (Fig. 1d).

Theorem.

The extended 1-Pappus Configuration is of type

$$1 * 5 + 4 * 4 + 7 * 3 \& 3 * 4 + 11 * 3, (9).$$

The 1-Pappus Pseudo Configuration is of type

$$9 * 3 \& 9 * 3, (9).$$

Definition.

There are many special cases of the Desargues configuration.

0. 1-Desargues($\{A_i\}, \{\underline{B}_0, B_1, B_2\}, \langle C_i \rangle$), in which $B_0 \iota a_0$ (Fig. 3b).
1. 2-Desargues($\{A_0, \underline{A}_1, \underline{A}_2\}, \{B_i\}, \langle C_i \rangle$), in which $A_1 \iota b_1$ and $A_2 \iota b_2$ (Fig. 3c).
2. 1-1-Desargues($\{\underline{A}_0, A_1, A_2\}, \{\underline{B}_0, B_1, B_2\}, \langle C_i \rangle$), in which $A_0 \iota b_0$ and $B_0 \iota a_0$ (Fig. 3d).
3. 3-Desargues($\{A_i\}, \{\underline{B}_i\}, \langle C_i \rangle$), in which $B_i \iota a_i$ (Fig. 3e).
4. C-Desargues($\{A_i\}, \{B_i\}, \langle \underline{C}_0, C_1, C_2 \rangle$), in which $C_0 \iota c_0$ (Fig. 3f).
5. C-1-Desargues($\{A_i\}, \{B_i\}, \langle \underline{C}_0, C_1, C_2 \rangle$), in which $B_1 \iota a_1$ and $C_2 \iota c_2$ (Fig. 3g).
6. Elated-Desargues($\underline{C}, \{A_i\}, \{\underline{B}_0, B_1, B_2\}, \langle C_i \rangle, c$), in which $C \iota c$ (Fig. 3h).

In each case the additional incident point(s) is (are) underlined.

Definition.

The extended special Desargues or extended quadrangle-quadrilateral configuration, consists of 25 points and 25 lines, those of 2.1.6 and

$$\begin{aligned} PQ_i &:= p_{i+1} \times q_{i-1}, \quad QP_i := q_{i+1} \times p_{i-1}, \\ QR_i &:= q_i \times r_i, \quad PR_i := p \times r_i, \\ pq_i &:= P_{i+1} \times Q_{i-1}, \quad qp_i := Q_{i+1} \times P_{i-1}, \\ qr_i &:= Q_i \times R_i, \quad pr_i := P \times R_i. \end{aligned}$$

Theorem.

All 25 points are on the 6 lines p_i, r_i of the quadrangle $\{Q_i, P\}$. All 25 lines are on the 6 points P_i, R_i of the quadrilateral $\{q_i, p\}$.

If $p = 5$ the extended special Desargues configuration is of type

$$10 * 6 + 15 * 4 \& 10 * 6 + 15 * 4.$$

If $p > 5$ it is of type

$$10 * 6 + 3 * 4 + 12 * 2 \& 10 * 6 + 3 * 4 + 12 * 2, (8).$$

Definition.

The conical points and lines of the extended quadrangle-quadrilateral configuration are the 6 points and 6 lines

$$\begin{aligned} AF_i &:= a_{i+1} \times pr_{i-1}, \quad FA_i := pr_{i+1} \times a_{i-1}, \\ af_i &:= A_{i+1} \times PR_{i-1}, \quad fa_i := PR_{i+1} \times A_{i-1}, \end{aligned}$$

Theorem.

$$AF_i \cdot pq_{i+1} = FA_i \cdot qp_{i-1} = 0.$$

Proof: To show that $AF_0 \cdot pq_1 = 0$, we can use the dual of Desargues' theorem applied to

$$\{p_0, p, p_1\} = \{R_1, Q_2, R_0\}$$

and

$$\{a_1, p_2, r_1\} = \{Q_1, P_1, A_2\}$$

with axial points

$$A_0, R_2, A_1 \text{ on the axis } a_2$$

and therefore central lines QR_1, PQ_0, a_0 on the center AF_2 .

Comment.

We will see in 2.2.11 that the conical points are points on a conic. The conic therefore appears in a natural way for $p = 5$, in which case there are exactly $25 + 6$ points and lines. (The Pascal line of $N_1, M_2, N_0, M_1, N_2, M_0$ is R_0, R_1, R_2 .) Although, in some sense, the conic exists already for $p = 2$ and $p = 3$, see 2.1.6, 2.2.11.

Definition.

In view of 2.3.4, we define as the dodecahedral configuration, the configuration obtained by adding the 6 conical points to the extended special Desargues configuration.

Theorem.

If $p = 5$, the dodecahedral configuration is of type

$$25 * 6 \text{ \& } 25 * 6.$$

If $p > 5$, the dodecahedral configuration is of type

$$13 * 6 + 3 * 4 + 12 * 3 + 3 * 2 \text{ \& } 13 * 6 + 3 * 4 + 12 * 3 + 3 * 2.$$

Proof: The first part follows from 2.1.7 and 2.1.7. For $p = 5$, all the points and lines of the dodecahedral configuration are distinct and are all the points and lines of the corresponding finite projective geometry. Any of the 6 conical points can be chosen to construct the extended special Desargues configuration. Moreover, pq_i contains also PR_i, QP_i and FA_{i+1} ; qp_i contains PR_i, PQ_i and AF_{i-1} ; qr_i contains QP_i, FA_i, QR_{i+1} and QR_{i-1} ; pr_i contains PQ_i, QR_i, FA_{i-1} and AF_{i+1} ; fa_i contains QP_{i+1}, QR_i and AF_i ; af_i contains PQ_{i-1}, QR_i and FA_i .

We leave, as an exercise, the proof of the following Theorem and the generalization of the definitions given therein.

Theorem.

The dodecahedral configuration can be continued indefinitely.

Starting with $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$ and $P = (1, 1, 1)$, the coordinates of the points and lines obtained by replacing lower case letter by the corresponding upper case letter are the same, e.g. $p = [1, 1, 1]$.

These are

$$\begin{aligned} A_0 &= (1, 0, 0), R_0 = [0, 1, -1], P_0 = (0, 1, 1), Q_0 = (-1, 1, 1), \\ PQ_0 &= (-1, 2, 1), QP_0 = (-1, 1, 2), \\ QR_0 &= (2, 1, 1), PR_0 = (-2, 1, 1), \\ AF_0 &= (2, 0, -1), FA_0 = (2, -1, 0), \end{aligned}$$

More points are

$$\begin{aligned} PG_i &:= p_{i+1} \times g_{i-1}, GP_i := g_{i+1} \times p_{i-1}, \\ AG_i &:= a_{i+1} \times g_{i-1}, GA_i := g_{i+1} \times a_{i-1}, \\ QRQR_i &:= qr_{i+1} \times qr_{i-1}, PQQP_i := PQ_i \times QP_i, \end{aligned}$$

and the lines are defined similarly, e.g.

$$pg_i := P_{i+1} \times G_{i-1}.$$

We have

$$\begin{aligned} PG_0 &= (-1, 3, 1), GP_0 = (-1, 1, 3), \\ AG_0 &= (2, 0, 1), GA_0 = (2, 1, 0), \\ QRQR_0 &= (-3, 1, 1), PQQP_0 = (3, 1, 1). \end{aligned}$$

and we have

$$\begin{aligned} GP_i \cdot qp_{i+1} &= PG_i \cdot pq_{i-1} = 0, \\ GA_i \cdot pq_i &= AG_i \cdot qp_i = 0, \\ QRQR_i \cdot r_i &= 0. \end{aligned}$$

Besides the conic

$$\{AF_i, FA_i\} = 2(X_0^2 + X_1^2 + X_2^2) + 5(X_1X_2 + X_2X_0 + X_0X_1) = 0,$$

there are many more, such as

$$\begin{aligned} \{PQ_i, QP_i\} &= (X_0^2 + X_1^2 + X_2^2) + 6(X_1X_2 + X_2X_0 + X_0X_1) = 0, \\ \{PG_i, GP_i\} &= (X_0^2 + X_1^2 + X_2^2) + 11(X_1X_2 + X_2X_0 + X_0X_1) = 0, \\ \{AG_i, GA_i\} &= 2(X_0^2 + X_1^2 + X_2^2) - 5(X_1X_2 + X_2X_0 + X_0X_1) = 0. \end{aligned}$$

Comment.

We started with the special Desargues configuration with 13 points (and lines) which are all of the points when $p = 3$, the extended special Desargues configuration consists of adding 18 points and lines which are 31 distinct points and lines when $p = 5$. It would appear that we could extend the construction in such a way that we get from the configuration with 31 points a configuration with 57 points which would be all distinct when $p = 7$, of 133 points which would be all distinct when $p = 11, \dots$. But this is not possible. For $p = 7$, $(1, 1, -1) \times (2, -1, 0)$ gives $(1, 2, 3)$ and by symmetry we get 5 other points but the points $(0, 1, 3)$ give by symmetry $(3, 0, 1) = (1, 0, -2)$ which has already been constructed. Moreover, the point $(1, 2, -3)$ gives by symmetry $(-3, 1, 2) = (1, 2, -3)$ hence for $p = 7$, the same point. It is therefore not clear how to proceed in a systematic way. This may be related to the fact that there are only 5 regular polyhedra which are associated to $p = 2, 3$ and 5. See Section 3.

Exercise.

Rewrite the statement of Theorem 2.1.6. in the form of a necessary and sufficient condition for A_1, A_3, A_5 to be collinear, given that A_0, A_2 and A_4 are collinear.

Exercise.

Let ω satisfy $\omega^2 + \omega + 1 = 0$.

Let $P_0 = (0, 1, -1)$, $Q_0 = (0, 1, -\omega)$, $R_0 = (0, 1, -\omega^2)$,

$P_1 = (-1, 0, 1)$, $Q_1 = (-\omega, 0, 1)$, $R_1 = (-\omega^2, 0, 1)$,

$P_2 = (1, -1, 0)$, $Q_2 = (1, -\omega, 0)$, $R_2 = (1, -\omega^2, 0)$,

then, with

$p = [1, 1, 1]$, $q = [1, \omega^2, \omega]$, $r = [1, \omega, \omega^2]$,

$p_0 = [1, 0, 0]$, $q[0] = [1, \omega, \omega]$, $r_0 = [1, \omega^2, \omega^2]$,

0. $\omega^3 = 1$,

1. $\text{incidence}(P_i, p)$, $\text{incidence}(Q_i, q)$, $\text{incidence}(R_i, r)$,

2. $\text{incidence}(P_i, Q_i, R_i, p_i)$,

3. $\text{incidence}(P_i, Q_{i+1}, R_{i-1}, q_i), \text{incidence}(P_i, Q_{i-1}, R_{i+1}, r_i)$,

4. the configuration is therefore of type $9 * 4 \& 12 * 3$.

This configuration is that of the 9 inflection points of the cubic, $X_0^3 + X_1^3 + X_2^3 + kX_0X_1X_2 = 0$.

Comment.

Let $\{A_0, A_1, A_2, A_3\}$ be a complete quadrangle and D_0, D_1, D_2 be the diagonal points, several situation are possible in a perspective plane (See I).

0. The diagonal points are always collinear, in this case, we have the N-Fano Configuration, $N\text{-Fano}(\{A, B, C, D\}; \langle P, Q, R \rangle)$.

1. The diagonal points are never collinear, in this case, we have the Fano Configuration, $\text{Fano}(\{A, B, C, D\}; \{P, Q, R\})$.

2. The diagonal points are sometimes collinear, in this case, we have either the pseudo configuration, $(\{A, B, C, D\}, \langle P, Q, R \rangle)$ or the pseudo configuration, $(\{A, B, C, D\}, \{P, Q, R\})$.

Notice the “,” in the first 2 cases.

2.1.8 Proof of the Theorem of Desargues. The hexagon of Pappus-Brianchon. The configuration of Reidemeister.

Proof of the Theorem of Desargues.

Proof: The proof that Theorem 2.1.5 follows from the axioms of incidence and of Pappus will now be given.

Cronheim (1953)¹ showed that the proof reduces to 2 cases. In the first one, a permutation of the indices 0, 1, 2 is chosen in such a way that $A_0 \mp b_0$ and $B_2 \mp a_2$. In the second one, except perhaps for an exchange of A_i and B_i , $B_i \mp a_i$.

In the first case (Hessenberg, 1905), let

He1.0. $A_0 \mp b_0$, $B_2 \mp a_2$,

De1.0. $d := A_0 \times B_2$, $D := d \times c_1$, $e := D \times C_2$, $E := e \times b_1$,

De1.1. $f := D \times C_0$, $F := f \times a_1$, $G := a_2 \times b_0$, $g := F \times G$.

De2.0. $X := d \times a_0$, $Y := d \times b_2$, $Z := d \times g$,

The Pappus-Pascal hexagon $D, A_1, A_0, A_2, B_2, C_0 \implies G, C$ and F are collinear.

The Pappus-Pascal hexagon $D, B_1, B_2, B_0, A_0, C_2 \implies G, C$ and E are collinear.

Hence A_0, F, E, D, B_2, G is a Pappus-Pascal hexagon and C_0, C_1 and C_2 are collinear. It is easy to verify that, because of He1.0, X is distinct from $D, A_0, B_2, A_2, C_0, A_1$, that Y is distinct from $D, B_2, A_0, B_0, C_2, B_1$ and that Z is distinct from A_0, D, B_2, E, G, F .

This will be abbreviated as follows.

Pr1.0. $\text{Pappus}(\langle D, A_0, B_2 \rangle, d, \langle A_2, C_0, A_1 \rangle, a_0; \langle G, C, F \rangle, X)$,

Pr1.1. $\text{Pappus}(\langle D, B_2, A_0 \rangle, d, \langle B_0, C_2, B_1 \rangle, b_2; \langle G, C, E \rangle, Y)$,

Pr1.2. $(\langle E, G, F \rangle, g)$,

Pr1.3. $\text{Pappus}(\langle A_0, D, B_2 \rangle, d, \langle E, G, F \rangle, g; \langle C_i \rangle, Z)$,

Pr1.4. $\langle C_i \rangle$.

In the second case (Cronheim, 1953), we have the 3-Desargues configuration (Fig. 3e), let

De3.0. $r_2 := A_2 \times C_2$, $R_0 := c_0 \times r_2$, $R_1 := c_1 \times r_2$,

De4.0. $X := c_2 \times b_2$,

Pr3.0. $\text{Pappus}(\langle C, A_2, B_2 \rangle, c_2, \langle C_2, B_1, B_0 \rangle, b_2; \langle C_0, A_0, R_1 \rangle, r_0, X)$,

Pr3.1. $\text{Pappus}(\langle C, A_2, B_2 \rangle, c_2, \langle C_2, B_0, B_1 \rangle, b_2; \langle C_1, A_1, R_0 \rangle, r_1, X)$,

Pr3.2. $\text{Pappus}(\langle R_0, B_0, A_0 \rangle, c_0, \langle B_1, R_1, A_1 \rangle, c_1; \langle C_0, C_1, C_2 \rangle, c, C)$.

Exercise.

Prove the Theorem of Cronheim, on the reduction to 2 cases, referred to in 2.1.8.

Theorem. [Dual of Pappus]

If the alternate sides of the hexagon $\{a_0, a_1, a_2, a_3, a_4, a_5\}$ pass through 2 points, three pairs of opposite points of the hexagon are on 3 lines p_0, p_1 and p_2 which pass through the same point. See 2.1.10. (Fig. 1b)

We write $\text{dual-Pappus}(\langle a_2, a_0, a_4 \rangle, \langle a_5, a_3, a_1 \rangle, \langle p_0, p_1, p_2 \rangle)$.

Proof: Let $A_0 := a_0 \times a_1$, $A_1 := a_1 \times a_2$, $A_2 := a_2 \times a_3$, $A_3 := a_3 \times a_4$, $A_4 := a_4 \times a_5$, $A_5 := a_5 \times a_0$.

Let $B_0 := a_0 \times a_2$, $B_1 := a_1 \times a_3$, $p_0 := A_0 \times A_3$, $p_1 := A_1 \times A_4$, $p_2 := A_2 \times A_5$, $B_2 := p_0 \times p_2$.

By hypothesis, $B_0 \cdot a_4 = B_1 \cdot a_5 = 0$. $B_0, A_2, A_5, B_1, A_0, A_3$ is a Pappus-Pascal hexagon, therefore A_1, B_2 and A_4 are collinear, in other words p_1 passes through B_2 .

¹Proc. Amer. Math. Soc., 4, 219-221.

Definition.

The preceding configuration is a degenerate form of that of Brianchon. I will call it the Pappus-Brianchon hexagon. The point common to p_0, p_1 and p_2 is called the Pappus point.

Proof of the special Desargues Theorem.

The proof of Theorem 2.1.6 is as follows: 0. is a direct consequence of 2.1.8. 1. follows from the Axiom of Pappus 2.1.2.4. applied to the points P_1, A_2, R_1 and P_2, A_1, R_2 , proving that Q_0, P_0 and P are collinear.

Exercise.

The proof 2.1.8 of Theorem 2.1.6 is only given in the general case. Describe all the exceptional cases and give a proof for each case.

Definition.

The Reidemeister configuration consists of 11 points

$A_0, A_1, A_2, B_{00}, B_{11}, B_{22}, B_{33}, B_{01}, B_{10}, B_{23}, B_{32},$

and 15 lines,

$a_0, a_1, a_2, b_{00}, b_{01}, b_{02}, b_{03}, b_{10}, b_{11}, b_{12}, b_{13}, b_{20}, b_{21}, b_{22}, b_{23}:$

Let A_0, A_1, A_2 be a triangle, $a_0 := A_1 \times A_2, a_1 := A_2 \times A_0, a_2 := A_0 \times A_1,$

let b_{00}, b_{01}, b_{02} be 3 lines through A_0 distinct from a_1 and $a_2,$

let B_{00}, B_{22} be points on b_{01} not on $a_0, b_{10} := A_1 \times B_{00}, b_{12} := A_1 \times B_{22}, b_{20} := A_2 \times B_{00},$

$b_{22} := A_2 \times B_{22}, B_{01} := b_{00} \times b_{10}, B_{23} := b_{00} \times b_{12}, B_{10} := b_{02} \times b_{20}, B_{32} := b_{02} \times b_{22},$

$b_{11} := A_1 \times B_{10}, b_{13} := A_1 \times B_{32}, b_{21} := A_2 \times B_{01}, b_{23} := A_2 \times B_{23}, B_{11} := b_{11} \times b_{21},$

$B_{33} := b_{13} \times b_{23}, b_{03} := B_{11} \times B_{33}.$ (Fig. 11a)

Lemma.

Let $c_{00} := B_{01} \times B_{10}, c_{01} := B_{32} \times B_{23}, C_0 := c_{00} \times c_{01},$ then incidence(C_0, A_1, A_2).

Proof:

Desargues($A_0, B_{00} B_{10} B_{01}, B_{22} B_{32} B_{23}; C_0 A_1 A_2, a_0$).

Theorem. [Reidemeister]

0. $A_0 \cdot b_{03} = 0.$

1. The Reidemeister configuration is of type

$$3 * 6 + 8 * 3 \& 12 * 3 + 3 * 2.$$

Proof: After using the preceding Lemma, we use Desargues($a_0, \{c_{00}, b_{11}, b_{21}\}, \{c_{01}, b_{13}, b_{23}\}; \langle b_{03}, b_{00}, b_{02} \rangle, A_0$).

Theorem.*Let*

$$c_{02} := B_{11} \times B_{22},$$

$$c_{12} := B_{01} \times B_{32},$$

$$c_{22} := B_{23} \times B_{10},$$

then

$$\text{incidence}(c_{i2}, C).$$

Proof:

$$\text{Desargues}^{-1}(a_2, \{b_{00}, b_{12}, c_{20}\}, \{b_{02}, b_{11}, c_{21}\}; \langle c_{02}, c_{12}, c_{22} \rangle, C),$$

Theorem.*Let*

$$c_{00} := B_{01} \times B_{10}, c_{01} := B_{32} \times B_{23},$$

$$c_{10} := B_{10} \times B_{22}, c_{11} := B_{23} \times B_{11},$$

$$c_{20} := B_{22} \times B_{01}, c_{21} := B_{11} \times B_{32},$$

$$C_i := c_{i0} \times c_{i1},$$

then

$$\text{incidence}(C_i, c).$$

Proof: Using the preceding Theorem,

$$\text{Desargues}(C, \{B_{22}, B_{01}, B_{10}\}, \{B_{11}, B_{32}, B_{23}\}; \langle C_i \rangle, c).$$

Exercise.*Let*

$$c'_{00} := B_{00} \times B_{11}, c'_{01} := B_{22} \times B_{33},$$

$$c'_{10} := B_{00} \times B_{32}, c'_{11} := B_{01} \times B_{33},$$

$$c'_{20} := B_{00} \times B_{23}, c'_{21} := B_{10} \times B_{33},$$

then

$$\text{incidence}(C_i, C'_{i+1}, C'_{i-1}).$$

Definition.

The extended Reidemeister configuration consists of the points $A_0, A_1, A_2, B_{jj}, j = 0, 1, 2, 3, B_{01}, B_{10}, B_{23}, B_{32}, C, C_i, C'_i, i = 0, 1, 2$, and of the lines $a_0, a_1, a_2, b_{ij}, i = 0, 1, 2, j = 0, 1, 2, 3, c_{ik}, c'_{ik}, c'_i, i = 0, 1, 2, k = 0, 1, c_0$, see Fig. 11f.

Exercise.*Prove*

0. that for given $A_0, A_1, A_2, B_{01}, B_{10}$, the correspondance between B_{22} and B_{33} is a projectivity with center $AEul_0$ on $A_1 \times A_2$ (See 2.2.6).

1. The lines b_{01} and b_{03} coincide if the point B_{10} is on the conic through B_{01} tangent at A_1 to $A_1 \times A_0$ and tangent at A_2 to $A_2 \times A_0$, represented by the matrix

$$\begin{bmatrix} 2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{bmatrix}$$

2. that if we permute cyclically A_0, A_1, A_2 , then

0. the lines $B_{00} \times B_{11}$ and the 2 other corresponding lines pass through the same point K .

1. the lines $A_0 \times B_{22}$ and the 2 other corresponding lines pass through the same point P .
The same is true for the lines $A_0 \times B_{33}$ and the 2 other corresponding lines, giving \bar{P} .

This configuration, see Fig. 26b, which I will call the K-Reidemeister configuration is part of the Hexal configuration studied in Chapter III, with the correspondance

A_i	B_{01}	B_{10}	b_{00}	b_{10}	b_{21}	b_{02}	b_{11}	b_{20}	c_{00}	c'_{00}
A_i	M	\bar{M}	ma_0	ma_1	ma_2	$\bar{m}a_0$	$\bar{m}a_1$	$\bar{m}a_2$	eul	mMa_0
B_{00}	B_{11}	b_{01}	b_{03}							
Maa_0	$\bar{M}a_0$	cc_0	$\bar{c}c_0$							

2.1.9 The extended Pappus configuration and a remarkable Theorem.

Introduction.

If we permute in all possible way the 6 points of the Pappus configuration we obtain 6 Pappus lines. I prove in Theorem 2.1.9. that these pass 3 by 3 through 2 points. We obtain therefore a dual configuration, which therefore determines 6 Pappus points, which are 3 by 3 on 2 lines. I prove in Theorem 2.1.9 that these lines are the 2 original ones of the Pappus configuration. The points are not, in general the same. The proof of the first Theorem is synthetic, I have no synthetic proof of the second Theorem. The algebraic proof uses a notation introduced in Chapter III. Special cases of this configuration have been studied, but because some of the results are still at the conjecture stage, these will not be discussed here, others are given as exercises.

The term “rotate the points $\bar{M}_0, \bar{M}_1, \bar{M}_2$ ” means that we take the even permutations of $\bar{M}_0, \bar{M}_1, \bar{M}_2$, namely $\bar{M}_1, \bar{M}_2, \bar{M}_0$ and $\bar{M}_2, \bar{M}_0, \bar{M}_1$.

The notation is explained, in details, in Chapter III.

Theorem. [Steiner (Pappus)]²

If we fix the points M_0, M_1, M_2 on d and rotate the points $\bar{M}_0, \bar{M}_1, \bar{M}_2$ on \bar{d} , we obtain the 3 Pappus lines m_0, m_1, m_2 . These pass through the point D . Similarly if we reverse the order of the points of \bar{d} and rotate, we obtain 3 other Pappus lines, $\bar{m}_0, \bar{m}_1, \bar{m}_2$. These pass through the point \bar{D} . In detail, let

$H0. \quad M_i, \bar{M}_i,$

²Steiner, Werke, I, p. 451

- $D0.$ $a_i := M_i \times \overline{M}_i,$
 $D1.$ $b_i := M_{i+1} \times \overline{M}_{i-1}, \bar{b}_i := \overline{M}_{i+1} \times M_{i-1},$
 $D2.$ $L_i := b_i \times \bar{b}_i,$
 $D3.$ $N_i := a_i \times b_i, \bar{N}_i := a_i \times \bar{b}_i,$
 $D4.$ $m_0 := L_1 \times L_2,$
 $D5.$ $m_1 := N_1 \times N_2, m_2 = \bar{N}_1 \times \bar{N}_2,$
 $D6.$ $D := m_1 \times m_2,$
 $D7.$ $Q_i := a_{i+1} \times a_{i-1},$
 $D8.$ $P_i := b_{i+1} \times b_{i-1}, \bar{P}_i := \bar{b}_{i+1} \times \bar{b}_{i-1},$
 $D9.$ $\overline{m}_i := P_i \times \bar{P}_i,$
 $D10.$ $\overline{D} := \overline{m}_1 \times \overline{m}_2,$

then

- $C0.$ $m_0.L_0 = 0(*).$
 $C1.$ $m_1.N_0 = m_2 \cdot \bar{N}_0 = 0(*).$
 $C2.$ $D.m_0 = 0.$
 $C3.$ $\overline{m}_i \cdot Q_i = 0.$
 $C4.$ $\overline{D} \cdot \overline{m}_0 = 0(*).$ See Fig. 9,

Proof: A synthetic proof is as follows, $C0$, $C1$, $C3$, are direct consequences of Pappus' theorem applied to

$\text{Pappus}(\langle M_0, M_1, M_2 \rangle, d, \langle \overline{M}_0, \overline{M}_1, \overline{M}_2 \rangle, \bar{d}; \langle L_0, L_1, L_2 \rangle, m_0)$
 $\text{Pappus}(\langle M_2, M_0, M_1 \rangle, d, \langle \overline{M}_1, \overline{M}_2, \overline{M}_0 \rangle, \bar{d}; \langle N_0, N_1, N_2 \rangle, m_0)$
 $\text{Pappus}(\langle M_1, M_2, M_0 \rangle, d, \langle \overline{M}_2, \overline{M}_0, \overline{M}_1 \rangle, \bar{d}; \langle \bar{N}_0, \bar{N}_1, \bar{N}_2 \rangle, m_0)$
 $\text{Pappus}(\langle M_0, M_1, M_2 \rangle, d, \langle \overline{M}_0, \overline{M}_1, \overline{M}_2 \rangle, \bar{d}; \langle L_0, L_1, L_2 \rangle, m_0)$
 $\overline{M}_2, \overline{M}_0, \overline{M}_1$ or $\overline{M}_1, \overline{M}_2, \overline{M}_0$ and $\overline{M}_2, \overline{M}_1, \overline{M}_0$, or $\overline{M}_0, \overline{M}_2, \overline{M}_1$ or $\overline{M}_1, \overline{M}_0, \overline{M}_2$. The triangles L_i, N_i, \bar{N}_i have \overline{m}_0 as axis of perspectivity for $i = 1$ and 2 therefore they have a center of perspectivity D , by Desargues. I also note that for $i = 2$ and 0 the axis is \overline{m}_1 and for $i = 0$ and 1 the axis is \overline{m}_2 . Hence $C2$. Symmetrically we get $C4$.

For an algebraic proof, useful because of 2.1.9, let

- $H0.$ $M_0 = (0, 1, -1), M_1 = (-1, 0, 1), M_2 = (1, -1, 0)$
 $H1.$ $\overline{M}_0 = (0, m_2, -m_1), \overline{M}_1 = (-m_2, 0, m_0), \overline{M}_2 = (m_1, -m_0, 0).$

then

- $P0.$ $a_0 = [1, 0, 0].$
 $P1.$ $b_0 = [m_0, m_1, m_0], \bar{b}_0 = [m_0, m_0, m_2].$
 $P2.$ $L_0 = (m_0^2 - m_1 m_2, m_0(m_2 - m_0), -m_0(m_0 - m_1)).$
 $P3.$ $N_0 = (0, m_0, -m_1), \bar{N}_0 = (0, m_2, -m_0).$
 $P4.$ $m_0 = [m_0(m_1 + m_2), m_1(m_2 + m_0), m_2(m_0 + m_1)],$
 $P5.$ $m_1 = [m_0 m_1, m_1 m_2, m_2 m_0], m_2 = [m_2 m_0, m_0 m_1, m_1 m_2],$
 $P6.$ $D = (m_1 m_2(m_0^2 - m_1 m_2), m_2 m_0(m_1^2 - m_2 m_0), m_0 m_1(m_2^2 - m_0 m_1)).$
 $P7.$ $Q_0 = (1, 0, 0).$
 $P8.$ $P_0 = (m_2(m_1 - m_2), m_2(m_0 - m_1), m_1(m_2 - m_0)),$
 $\bar{P}_0 = (m_1(m_1 - m_2), m_2(m_0 - m_1), m_1(m_2 - m_0)).$
 $P9.$ $\overline{m}_0 = [0, m_1(m_2 - m_0), -m_2(m_0 - m_1)],$
 $P10.$ $\overline{D} = (m_1 m_2(m_2 - m_0)(m_0 - m_1), m_2 m_0(m_0 - m_1)(m_1 - m_2),$
 $m_0 m_1(m_1 - m_2)(m_2 - m_0)).$

Definition.

The configuration of Theorem 2.1.9 which consists of 26 points and 17 lines is called the extended Pappus configuration.

It is of type $6 * 4 + 20 * 3 \& 9 * 6 + 6 * 4 + 2 * 3$. (10)

It can also be viewed, because of the synthetic proof as a multiple Desargues configuration, with 3 triangles perspective from D and 3 triangles perspective from D' in which the axis of one are the concurrent lines of the other.

Definition. [Steiner]

The sub-configuration consisting of the points $L_i, N_i, \bar{N}_i, Q_i, P_i, \bar{P}_i, D, \bar{D}$ and of the lines $a_i, b_i, \bar{b}_i, m_i, \bar{m}_i$, is called the Steiner configuration. It is of type

$20 * 3 \& 15 * 4$. (10)

Comment.

Part of a dual of the extended configuration is described in sections 1, 3 and 4 of the involutive geometry of the triangle. The relation between the notations is as follows:

d	\bar{d}	M_i	\bar{M}_i	a_i	b_i	\bar{b}_i	L_i	N_i	\bar{N}_i
M	\bar{M}	m_a	\bar{m}_a	A_i	Maa_i	$\bar{M}aa_i$	mMa_i	cc_i	$\bar{c}c_i$
m_0	m_1	m_2	D	Q_i	P_i	\bar{P}_i	\bar{m}_i	\bar{D}	
K	P	\bar{P}	pp	a_i	pap_i	$\bar{p}ap_i$	Pap_i	pap	

In particular, K is the point of Lemoine. On the other hand there is the following correspondence \bar{m}_i and the dual of $abr1_i$, \bar{D} and the dual of Ste , which passes through BRa and Abr .

Theorem.

If we make the dual construction starting with m_0, m_1, m_2 on D and \bar{m}_i on \bar{D} , the points Ma_i dual of m_i is on the original line d and those $\bar{M}a_i$ dual of \bar{m}_i is on the original line \bar{d} :

$$C5. \quad Ma_i \cdot d = 0.$$

$$C6. \quad \bar{M}a_i \cdot \bar{d} = 0. \text{ See Fig. 10,}$$

Proof: An algebraic proof is as follows. ³

$$P'0. \quad A_0 = (2m_1m_2(m_1-m_2), m_2(m_1+m_2)(m_0-m_1), m_1(m_1+m_2)(m_2-m_0)).$$

$$A_1 = (m_1m_2(m_0-m_1), m_0(m_1^2+m_2m_0-2m_0m_1), m_0m_1(m_1-m_2)),$$

$$A_2 = (m_1m_2(m_2-m_0), m_2m_0(m_1-m_2), -m_0(m_2^2-2m_2m_0+m_0m_1)),$$

$$P'1. \quad B_0 = (m_1m_2(m_2-m_0), m_2m_0(m_1-m_2), m_1(m_2^2-2m_1m_2+m_0m_1)),$$

$$B_1 = (-m_1(m_0^2+m_1m_2-2m_0m_1), m_2m_0(m_0-m_1), m_0m_1(m_2-m_0)),$$

$$B_2 = (m_2(m_2+m_0)(m_0-m_1), 2m_2m_0(m_2-m_0), m_0(m_1-m_2)(m_2+m_0)),$$

$$\bar{B}_0 = (m_1m_2(m_0-m_1), -m_2(m_1^2-2m_1m_2+m_2m_0), m_0m_1(m_1-m_2)),$$

$$\bar{B}_1 = (m_1(m_2-m_0)(m_0+m_1), m_0(m_1-m_2)(m_0+m_1), 2m_0m_1(m_0-m_1)),$$

$$\bar{B}_2 = (m_2(m_0^2+m_1m_2-2m_2m_0), m_2m_0(m_0-m_1), m_0m_1(m_2-m_0)).$$

$$P'2. \quad l_0 = [2m_1^3m_2 + 2m_2^3m_1 - m_2^3m_0 - m_1^3m_0 - 5m_1^2m_2^2 - m_2^2m_0^2]$$

³The reader will want to wait to check these algebraic manipulations until the notation has been explained.

$$\begin{aligned}
& -m_0^2 m_1^2 + m_0 m_1 m_2 (m_0 + 2m_1 + 2m_2), \\
& m_1 (m_2^2 m_1 - 2m_1^2 m_2 + m_0^2 m_2 - 2m_2^2 m_0 - 2m_0^2 m_1 + m_1^2 m_0 + 3m_0 m_1 m_2), \\
& m_2 (m_1^2 m_2 - 2m_2^2 m_1 + m_0^2 m_1 - 2m_1^2 m_0 - 2m_0^2 m_2 + m_2^2 m_0 + 3m_0 m_1 m_2), \\
P'3. \quad & l_1 = [m_0 (s_{21} - 6m_2 m_1 m_0),^4 \\
& m_1 (3m_0^3 + 4m_1^2 m_0 - 5m_1 m_0^2 - 2m_0^2 m_2 + m_0 m_2^2 + m_2^2 m_1 - 2m_2 m_1^2), \\
& -(m_1 + m_0)(m_1 m_0^2 + m_0 m_2^2 + m_2 m_1^2 - 2(m_1^2 m_0 + m_0^2 m_2 + m_2^2 m_1) \\
& + 3m_2 m_1 m_0)], \\
& l_2 = [m_0 (s_{21} - 6m_1 m_2 m_0), \\
& -(m_2 + m_0)(m_2 m_0^2 + m_0 m_1^2 + m_1 m_2^2 - 2(m_2^2 m_0 + m_0^2 m_1 + m_1^2 m_2) \\
& + 3m_1 m_2 m_0), \\
& m_2 (3m_0^3 + 4m_2^2 m_0 - 5m_2 m_0^2 - 2m_0^2 m_1 + m_0 m_1^2 + m_1^2 m_2 - 2m_1 m_2^2)], \\
& n_0 = [-(m_1 + m_2)(m_1 m_2^2 + m_2 m_0^2 + m_0 m_1^2 - 2(m_1^2 m_2 + m_2^2 m_0 + m_0^2 m_1) \\
& + 3m_0 m_1 m_2), \\
& m_1 (3m_2^3 + 4m_1^2 m_2 - 5m_1 m_2^2 - 2m_2^2 m_0 + m_2 m_0^2 + m_0^2 m_1 - 2m_0 m_1^2), \\
& m_2 (s_{21} - 6m_0 m_1 m_2), \\
& \bar{n}_0 = [(m_1 + m_2)(-(m_1^2 m_2 + m_2^2 m_0 + m_0^2 m_1) + 2(m_2^2 m_1 + m_0^2 m_2 + m_1^2 m_0) \\
& - 3m_0 m_1 m_2), \\
& m_1 (s_{21} - 6m_0 m_1 m_2), \\
& m_2 (3m_1^3 - 5m_1^2 m_2 + 4m_2^2 m_1 - 2m_2^2 m_0 + m_0^2 m_2 + m_0^2 m_1 - 2m_0 m_1^2)], \\
& l_2 = (l_{10}, l_{12}, l_{11})(m_1, m_0, m_2). \\
& n_0 = (l_{12}, l_{11}, l_{10})(m_2, m_1, m_0). \\
& n_1 = (l_{01}, l_{02}, l_{00})(m_2, m_0, m_1). \\
& n_2 = (l_{11}, l_{12}, l_{10})(m_2, m_0, m_1). \\
P'4. \quad & Ma_0 = (2m_0 - m_1 - m_2, 2m_1 - m_2 - m_0, 2m_2 - m_0 - m_1). \\
P'5. \quad & Ma_1 = (2m_1 - m_2 - m_0, 2m_0 - m_1 - m_2, 2m_2 - m_0 - m_1), \\
& Ma_2 = (2m_2 - m_0 - m_1, 2m_1 - m_2 - m_0, 2m_0 - m_1 - m_2). \\
P'7. \quad & q_0 = [-m_0 (m_1^3 (m_2 + m_0) + m_2^3 (m_0 + m_1) - m_1^2 m_2^2 - 2m_2^2 m_0^2 - 2m_0^2 m_1^2 \\
& + m_0 m_1 m_2 (5m_0 - 2m_1 - 2m_2)), \\
& -m_1 m_2 (-(m_1^2 m_2 + m_2^2 m_0 + m_0^2 m_1) + 2(m_2^2 m_1 + m_0^2 m_2 + m_1^2 m_0) \\
& - 3m_0 m_1 m_2), \\
& m_1 m_2 (-2(m_1^2 m_2 + m_2^2 m_0 + m_0^2 m_1) + (m_2^2 m_1 + m_0^2 m_2 + m_1^2 m_0) \\
& + 3m_0 m_1 m_2)], \\
P'8. \quad & p_0 = [-m_2 m_0 (s_{21} - 6m_0 m_1 m_2), \\
& -m_1 (m_2 + m_0)(-(m_1^2 m_2 + m_2^2 m_0 + m_0^2 m_1) + 2(m_2^2 m_1 + m_0^2 m_2 + m_1^2 m_0) \\
& - 3m_0 m_1 m_2), \\
& -m_2 (m_0^3 m_2 - 2m_0^3 m_1 + 3m_1^2 m_2^2 + m_2^2 m_0^2 + 4m_0^2 m_1^2 \\
& - m_0 m_1 m_2 (2m_2 + 5m_1))], \\
& \bar{p}_0 = [-m_0 m_1 (s_{21} - 6m_0 m_1 m_2), \\
& -m_1 (m_0^3 m_1 - 2m_0^3 m_2 + 3m_1^2 m_2^2 + m_0^2 m_1^2 + 4m_2^2 m_0^2 \\
& - m_0 m_1 m_2 (2m_1 + 5m_2)), \\
& m_2 (m_0 + m_1)(-2(m_1^2 m_2 + m_2^2 m_0 + m_0^2 m_1) + (m_2^2 m_1 + m_0^2 m_2 + m_1^2 m_0) \\
& + 3m_0 m_1 m_2)]. \\
P'9. \quad & \bar{Ma}_0 = (m_1 m_2 (2m_1 m_2 - m_2 m_0 - m_0 m_1), m_2 m_0 (2m_0 m_1 - m_1 m_2 - m_2 m_0),
\end{aligned}$$

⁴ s_{21} is the symmetric function in m_i , namely, $m_0^2(m_1 + m_2) + m_1^2(m_2 + m_0) + m_2^2(m_0 + m_1)$.

$$\begin{aligned}
& m_0 m_1 (2m_2 m_0 - m_0 m_1 - m_1 m_2), \\
\overline{M}a_1 = & (m_1 m_2 (2m_2 m_0 - m_0 m_1 - m_1 m_2), m_2 m_0 (2m_1 m_2 - m_2 m_0 - m_0 m_1), \\
& m_0 m_1 (2m_0 m_1 - m_1 m_2 - m_2 m_0)), \\
\overline{M}a_2 = & (m_1 m_2 (2m_0 m_1 - m_1 m_2 - m_2 m_0), m_2 m_0 (2m_2 m_0 - m_0 m_1 - m_1 m_2), \\
& m_0 m_1 (2m_1 m_2 - m_2 m_0 - m_0 m_1)).
\end{aligned}$$

Comment.

Continuing 2.1.9 we have the following relation between the above notation and that in the involutive geometry of the triangle.

d	\bar{d}	M_i	\overline{M}_i
pp	pap	K, P, P	Pap_i
a_i	b_i	\bar{b}_i	
$kpa_0, \bar{t}pa_1, tpa_2$	$\bar{t}pa_2, tpa_0, kpa_1$	$tpa_1, kpa_2, \bar{t}pa_0$	
L_i	N_i	\bar{N}_i	
$Ttp_0, Tkp_1, Tk\bar{p}_2$	$Tk\bar{p}_1, Ttp_2, Tkp_0$	$Tkp_2, Tk\bar{p}_0, Ttp_1$	
m_i	D	\bar{m}_i	\bar{D}
apa_i	M	$\bar{a}pa_0, \bar{a}pa_2, \bar{a}pa_1$	\bar{M}
Q_i	P_i	\bar{P}_i	
$\bar{T}tp_0, \bar{T}k\bar{p}_1, \bar{T}kp_2$	$\bar{T}k\bar{p}_2, \bar{T}kp_0, \bar{T}tp_1$	$\bar{T}kp_1, \bar{T}tp_2, \bar{T}k\bar{p}_0$	

Definition.

The mapping which associates to the points M_i and \overline{M}_i , the points Ma_i and $\overline{M}a_i$, is called the Pappus-dual-Pappus mapping.

Exercise.

If a_0, a_1 and a_2 have a point in common, prove that the elements defined in 2.1.9 and their dual defined in 2.1.9 determine a self-dual configuration and the points Ma_i and $\overline{M}a_i$ coincide, as a set, with the points M_i and \overline{M}_i . If $p > 5$, there are 29 points and 29 lines.

If $p = 5$, there are 25 points and 25 lines, the type is

$$10 * 6 + 4 * 5 + 11 * 4 \ \& \ 10 * 6 + 4 * 5 + 11 * 4.$$

If $p = 7$, it is of type

$$12 * 6 + 8 * 5 + 9 * 4 \ \& \ 12 * 6 + 8 * 5 + 9 * 4.$$

If $p > 7$, it is of type

$$12 * 6 + 4 * 5 + 1 * 4 + 12 * 3 \ \& \ 12 * 6 + 4 * 5 + 1 * 4 + 12 * 3.$$

The configuration is therefore distinct from the extended special Desargues configuration of 2.1.7.

Prove that the 6 points and lines left over are also on a conic, as in 2.1.7.

2.1.10 Duality.

Introduction.

This important concept, prepared by the work of Maurolycus and Poncelet, was introduced by Joseph Diaz Gergonne. We observe that if we join Theorem 2.1.8 to the axioms 2.1.2 and to Theorems 2.1.4, and then exchange the words line and point, we obtain the same statements in some other order. Therefore in any result obtained, we can exchange the words line and point.

Definition.

The method of obtaining from a result an other result by exchange of the words line and point is called duality. In particular, the Theorem of Desargues 2.1.5, becomes:

Theorem. [Dual of Desargues' Theorem]

Given two triangles $\{a_0, a_1, a_2\}$ and $\{b_0, b_1, b_2\}$ such that the points $a_0 \times b_0$, $a_1 \times b_1$ and $a_2 \times b_2$ are on the same line c . Let $c_0 := (a_1 \times a_2) \times (b_1 \times b_2)$, $c_1 := (a_2 \times a_0) \times (b_2 \times b_0)$, $c_2 := (a_0 \times a_1) \times (b_0 \times b_1)$. Then c_0, c_1, c_2 are incident to the same point C . Fig. 3a)

This is the dual of Theorem 2.1.5.

Comment.

Fig. 1a and 1b are dual of each other, so are Fig. 2a and 2b, Fig. 2a' and 2b', Fig. 9 and 10.

Fig. 3a, Fig. 3e, Fig. 3h are self dual.

2.1.11 Complete quadrangles and homologic quadrangles.

Theorem.

If 2 quadrangles $\{A_0, A_1, A_2, A_3\}$ and $\{A'_0, A'_1, A'_2, A'_3\}$ are such that none of their points and none of their lines coincide and are such that 5 of their corresponding lines are on the same line p , then the 6-th pair of lines intersect on p .

Proof: Using the notation 2.1.6 and " " for the second quadrangle, let $B_k := a_k \times a'_k$, $k = 0$ to 5 and let B_0, B_1, B_2, B_3, B_4 , be all on the line p . Theorem 2.1.10, dual of Desargues can be applied to the triangles $\{A_0, A_2, A_3\}$ and $\{A'_0, A'_2, A'_3\}$ then to the triangles $\{A_0, A_3, A_1\}$ and $\{A'_0, A'_3, A'_1\}$. The consequence is that the lines $A_0 \times A'_0$, $A_2 \times A'_2$, $A_3 \times A'_3$ have a point P in common which is also on $A_1 \times A'_1$. Therefore the Theorem of Desargues can be applied to the triangles $\{A_0, A_1, A_2\}$ and $\{A'_0, A'_1, A'_2\}$ which implies that the lines a_5 and a'_5 intersect on the line p .

Or using the synthetic notation, let $b_j := A_j \times A'_j$, $j = 0$ to 3

Desargues⁻¹($p, \{a_3, a_2, a_1\}, \{A_0, A_2, A_3\}, \{a'_3, a'_2, a'_1\}; \{A'_0, A'_2, A'_3\}; \langle b_0, b_2, b_3 \rangle, P$),

Desargues⁻¹($p, \{a_4, a_0, a_2\}, \{A_0, A_3, A_1\}, \{a'_4, a'_0, a'_2\}; \{A'_0, A'_3, A'_1\}; \langle b_0, b_3, b_1 \rangle, Q$),

$\implies P = (A_0 \times A'_0) \times (A_3 \times A'_3) = Q$,

$\implies \text{Desargues}(P, \{A_0, A_1, A_2\}, \{a_5, a_0, a_1\}, \{A'_0, A'_1, A'_2\}, \{a'_5, a'_0, a'_1\}; \langle B_5, B_0, B_1 \rangle, p)$,

Definitions.

The quadrangles of Theorem 2.1.11 are said to be homologic. p is called the axis and P the center of the homology.

Corollary.

If two complete quadrangles with no points and lines in common are such that

$$K := a_0 \times a_3 \text{ is on } a'_0 \text{ and } a'_3, L := a_1 \times a_4 \text{ is on } a'_1 \text{ and } a'_4,$$

$$M := a_2 \times a'_2 \text{ is on } K \times L,$$

then

$$N := a_5 \times a'_5 \text{ is also on } K \times L.$$

Construction.

Given three points K, L, M on a line p , choose arbitrarily a point A_0 not on p and a point A_1 on $A_0 \times K$ distinct from A_0 and K . Define

$$A_3 := (A_1 \times L) \times (A_0 \times M), A_2 := (A_3 \times K) \times (A_0 \times L),$$

$$N := (A_1 \times A_2) \times (K \times L). \text{ See Fig. 2a''}.$$

It follows from 2.1.9 that N is independent of the choice of A_0 and A_1 .

Definition.

N is called the harmonic conjugate of M with respect to K and L .

Theorem.

If each line has $q + 1$ points on it, let $l(n, q)$ denote the number of points on a complete n -angle, let $l^*(n, q)$ denote the number of points not on a complete n -angle, let $L(n, q)$ denote the number of complete n -angles,

0. $l(n, q) = n \frac{n-1}{2} q - n(n-3) \frac{n^2-3n+6}{8}.$
1. $l^*(n, q) = q^2 - (n+1) \frac{n-2}{2} q + (n-2) \frac{n^3-4n^2+7n-4}{8}.$
2. $L(n+1, q) = \frac{1}{n+1} L(n, q) l^*(n, q).$
3. $l(n+1, q) - l(n, q) = nq - \frac{1}{2}(n-1)(n^2 - 2n + 2).$

Proof. $l(n+1, q)$ is obtained from $l(n, q)$ by adding points on each of the n lines through the new point A_n and through one of the old points A say, plus the new point itself. On each of the lines $A_n \times A$, we have $q+1$ points from which we have to subtract the points A and A_n as well as the points on the $(n-1) \frac{n-2}{2}$ lines through each pair of the old points, A excluded. This gives

$$n(q+1 - \frac{1}{2}(n-1)(n-2) - 2) + 1 = nq - \frac{1}{2}(n^3 - 3n^2 + 4n - 2).$$

Using $l(1, q) = 1, 0$. follows by induction, 1. follows from $l^*(n, q) = q^2 + q + 1 - l(n, q)$,

2. follows from the fact that to each complete n -angle and each point not on its sides is associated a complete $(n+1)$ -angle each being counted $n+1$ times.

Exercise.

0. $l(I, q)$ is a polynomial of degree 4, its successive forward differences at 0 are 1, $q - 1$, 0 and -3 .
1. $l^*(\frac{5}{2} + x, q) = l^*(\frac{5}{2} - x, q)$
2. $l^*(n, I)$ is a quadratic function. Its discriminant is $-\frac{1}{4}(n - 2)(n - 3)(n^2 - 5n + 2)$, its successive forward differences at 0 are 4, -5 , 6 and -6 .
The discriminant is negative if $n > 4$.

Table.

n	$l(n, q)$	$l^*(n, q)$	$discr.$	$L(n, q)$
0	0	$q^2 + q + 1$	-3	1
1	1	$(q + 1)q$	1	$q^2 + q + 1$
2	$q + 1$	q^2	0	$\frac{1}{2!}q(q + 1)(q^2 + q + 1)$
3	$3q$	$(q - 1)^2$	0	$\frac{1}{3!}q^3(q + 1)(q^2 + q + 1)$
4	$6q - 5$	$(q - 2)(q - 3)$	1	$\frac{1}{4!}q^3(q^2 - 1)(q^3 - 1)$
5	$10q - 20$	$q^2 - 9q + 21$	-3	$\frac{1}{5!}q^3(q^2 - 1)(q^3 - 1)(q - 2)(q - 3)$
6	$15q - 54$			
7	$21q - 119$			
8	$28q - 230$			

Exercise.

Complete the last 3 lines of the preceding table.

2.1.12 Collineation and Correlation.**Definition.**

A collineation consists of a one to one function γ from the set of points of the plane onto itself, such that all points on a line have their image also on a line and of the induced function γ' from the set of lines of the plane onto itself.

Definition.

A correlation consists of a one to one function ρ from the set of lines of the plane onto itself, such that all lines through a point have their image also through a point and of the induced function ρ' from the set of points of the plane onto itself.

Theorem.

If the geometry is of prime order, a collineation or a correlation is determined by the image of a complete quadrangle onto a complete quadrangle or quadrilateral. (See 2.2.7)

2.1.13 Finite projective planes for small p .

Introduction.

There is a well known, see for instance Stevenson, p. 72, or Dembowski, p. 144, 14. that there is, up to isomorphism, only one plane satisfying the incidence axioms, the axiom of Pappus and the finite field axiom 2.1.3. In the general case, the proof will require a full knowledge of the material not only of section 1, but also of the existence of fundamental projectivities of order $p - 1$ and $p + 1$. The axiom of Pappus is not required for $p \leq 7$, as proven by MacInnes in 1907 for $p = 2, 3$ and 5. For $p = 7$, see Bose and Nair, 1941, Hall 1953, 1954b, Pierce, 1953, Pickert, 1955.

Theorem.

For $p = 2$,

0. There exists, up to isomorphism, only one plane satisfying the incidence axioms.
1. The diagonal points of a complete quadrangle configuration are collinear.

Proof: Assume that line $[3]$ contains the points (0) , (1) and (2) . Let (3) be an other point. Define line $[0]$ as the line through (1) and (3) , we abbreviate this as $[0] := (1) \times (3)$. Similarly, $[1] := (0) \times (3)$, $[2] := (2) \times (3)$. Let the third point on $[0]$ be (5) , on $[1]$ be (4) and on $[2]$ be (6) . Let $[4] := (4) \times (6)$, $[5] := (5) \times (6)$, $[6] := (4) \times (5)$. The incidence properties imply (0) is on $[5]$, which we abbreviate $(0) \cdot [5] = 0$, similarly $(1) \cdot [4] = 0$ and $(2) \cdot [6] = 0$. This completes the incidence tables:

line : Points on line	Point : lines through Point
0 : 1 3 5	0 : 1 3 5
1 : 0 3 4	1 : 0 3 4
2 : 2 3 6	2 : 2 3 6
3 : 0 1 2	3 : 0 1 2
4 : 1 4 6	4 : 1 4 6
5 : 0 5 6	5 : 0 5 6
6 : 2 4 5	6 : 2 4 5

Theorem.

For $p = 3$,

0. there exists, up to isomorphism, only one plane satisfying the incidence axioms.

Proof: Assume that the line $[4]$ contains the points (0) , (1) , (2) and (3) . Let (4) be a point not on $[4]$. Let $[0] := (1) \times (4)$, $[1] := (0) \times (4)$, $[2] := (3) \times (4)$, $[3] := (2) \times (4)$. Let (7) and (10) be the other points on $[0]$. Let $[7] := (0) \times (10)$, $[10] := (0) \times (7)$, $[9] := (2) \times (10)$, $[11] := (2) \times (7)$, $[8] := (3) \times (10)$, $[12] := (3) \times (7)$. Let $(9) := [2] \times [10]$, $(11) := [2] \times [7]$, $(8) := [3] \times [10]$, $(12) := [3] \times [7]$, $(5) := [1] \times [9]$, $(6) := [1] \times [8]$. Let $[5] := (1) \times (9)$, $[6] := (1) \times (8)$.

At this stage we have the following incidence table:

line : Points on line	Point : lines through Point
0 : 1 4 7 10	0 : 1 4 7 10
1 : 0 4 5 6	1 : 0 4 5 6
2 : 3 4 9 11	2 : 3 4 9 11
3 : 2 4 8 12	3 : 2 4 8 12
4 : 0 1 2 3	4 : 0 1 2 3
5 : 1 9	5 : 1 9
6 : 1 8	6 : 1 8
7 : 0 10 11 12	7 : 0 10 11 12
8 : 3 6 10	8 : 3 6 10
9 : 2 5 10	9 : 2 5 10
10 : 0 7 8 9	10 : 0 7 8 9
11 : 2 7	11 : 2 7
12 : 3 7	12 : 3 7

It remains to complete the table using the incidence axioms:

Line [8] contains (3), (6) and (10), but (3) is already on line [2] with (4) hence (4) cannot be on [8]. Similarly (3) excludes (9), (11), (0), (1), (2), (6), (7); (6) excludes (5) and (10) excludes (12). The only point left is (8).

Line [9] contains (2), (5) and (10), (2) excludes (4), (8), (12), (0), (1), (3), (7) and (10) excludes (11), (3), (6), only (9) remains.

Line [5] contains (1) and (9), (1) excludes (4), (7), (10), (0), (2), (3), (8) and (10) excludes (11), (5), only (6) and (12) remain.

Line [6] contains (1) and (8), (1) excludes (4), (7), (10), (0), (2), (3), (6), (9), (12), only (5) and (11) remain.

Line [11] contains (2) and (7), (2) excludes (4), (8), (12), (0), (1), (3), (5), (9), (10), only (6) and (11) remain.

Line [12] contains (3) and (7), (3) excludes (4), (9), (11), (0), (1), (2), (6), (8), (10), only (5) and (12) remain.

This completes the incidence tables:

line : Points on line	Point : lines through Point
5 : 1 6 9 12	5 : 1 6 9 12
6 : 1 5 8 11	6 : 1 5 8 11
8 : 3 6 8 10	8 : 3 6 8 10
9 : 2 5 9 10	9 : 2 5 9 10
11 : 2 6 7 11	11 : 2 6 7 11
12 : 3 5 7 12	12 : 3 5 7 12

Exercise.

D and \bar{D} , are harmonic conjugates to d and \bar{d} . Comes from Steiner for conics.

Exercise.

Let

... complete this, change notation for BM in D2.

$D0.$ $AM_i := a_{i+1} \times m_{i+1},$
 $D2.$ $BM_i := m_{i+1} \times \bar{b}_{i-1},$
 $D3.$ $ab_i := BM_{i+1} \times AM_{i-1},$
 then

$C0.$ $P_i.ab_i = 0.$

Proof: ab_2 is the axis of perspectivity of the triangles N_0 , with center of perspectivity M_0 .

Comment.

A configuration associated to antipolarity in 3 dimensions implies a configuration of 20 points and 22 lines in 2 dimensional geometry, see VI.6.1.5.

INTEGRATE THERE

$Dx.$ $ce_i := M\bar{M}a_{i+1} \times M\bar{M}a_{i-1},$
 $\quad \quad \bar{M}M a_{i-1},$
 $Dy.$ $PQ_i := ce_i \times \bar{c}e_i,$
 $Px.$ $ce_0 = [m_1(m_1-m_2), m_2(m_0-m_1), m_1(m_2-m_0)],$
 $\quad \quad \bar{c}e_0 = [m_2(m_1-m_2), m_2(m_0-m_1), m_1(m_2-m_0)],$
 $Py.$ $PQ_0 = (0, m_1(m_2-m_0), -m_2(m_0-m_1)).$

Examples.

In the following examples we can replace γ and γ' by ρ and ρ' . ρ composed with ρ' gives a collineation σ . Properties and special cases of collineations and correlations will be discussed in 2.1.12 and 2.2.8. In these examples, the complete quadrangle in the domain is always $(0), (1), (6), (12)$. $t(i)$ denotes the smallest positive integer such that $(\gamma^t)(i) = i$. $C_3 = C_1^3$ indicates that the function γ of the collineation C_3 corresponds to the function γ of the collineation C_1 composed with itself 3 times. The examples will be used in 1.8.12.

For $p = 5$, 4 points? 0, 1, 6, 12

C_0 4 image points? 1, 6, 12, 3

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	1	6	21	11	26	16	12	22	7	17	27	2	3	0	4	5
$\gamma'(i)$	5	10	18	26	14	22	0	2	1	4	3	9	17	30	13	21
$t(i)$	31	31	31	31	31	31	31	31	31	31	31	31	31	31	31	31
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		30	20	10	25	15	18	13	8	28	23	24	29	9	14	19
$\gamma'(i)$		7	11	20	24	28	8	29	25	16	12	6	23	15	27	19
$t(i)$		31	31	31	31	31	31	31	31	31	31	31	31	31	31	31

C_1 4 image points? 1, 6, 12, 5

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	1	6	16	26	11	21	12	27	17	7	22	2	5	4	0	3
$\gamma'(i)$	5	10	22	14	26	18	0	3	4	1	2	9	21	13	30	17
$t(i)$	24	24	24	6	24	24	24	6	24	24	24	24	24	1	6	24
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		30	15	25	10	20	18	23	28	8	13	24	19	14	9	29
$\gamma'(i)$		7	28	24	20	11	8	12	16	25	29	6	19	27	15	23
$t(i)$		6	24	24	24	24	24	24	6	24	24	24	24	24	24	6

$C_7 = C_1^{12}$ 4 image points? 16,30,29,9

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	16	30	14	3	23	7	29	5	8	12	25	28	9	22	2	15
$\gamma'(i)$	11	18	25	3	27	9	20	7	28	5	24	0	15	13	14	12
$t(i)$	2	2	2	1	2	2	2	1	2	2	2	2	2	1	1	2
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		0	17	19	18	20	27	13	4	24	10	26	21	11	6	1
$\gamma'(i)$		16	21	1	26	6	17	29	23	10	2	19	4	8	22	30
$t(i)$		1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

C_8 4 image points? 0,1,12,19

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	0	1	3	5	2	4	12	14	11	13	15	17	19	16	18	20
$\gamma'(i)$	10	26	14	18	5	22	6	7	0	8	9	1	25	30	15	20
$t(i)$	4	5	20	20	20	20	1	1	4	4	4	5	20	20	20	20
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		22	24	21	23	25	27	29	26	28	30	7	9	6	8	10
$\gamma'(i)$		21	19	28	3	12	11	2	29	17	23	16	13	27	24	4
$t(i)$		5	20	20	20	20	5	20	20	20	20	5	20	20	20	20

$C_9 = C_8^2$ 4 image points? 0,1,19,23

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	0	1	5	4	3	2	19	18	17	16	20	24	23	22	21	25
$\gamma'(i)$	9	16	15	28	22	2	6	7	10	0	8	26	23	4	20	12
$t(i)$	2	5	10	10	10	10	1	1	2	2	2	5	10	10	10	10
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		29	28	27	26	30	9	8	7	6	10	14	13	12	11	15
$\gamma'(i)$		11	3	27	18	25	1	14	24	19	29	21	30	13	17	5
$t(i)$		5	10	10	10	10	5	10	10	10	10	5	10	10	10	10

$C_{10} = C_8^4$ 4 image points? 0,1,26,7

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	0	1	2	3	4	5	26	27	28	29	30	6	7	8	9	10
$\gamma'(i)$	0	11	12	13	14	15	6	7	8	9	10	21	24	22	25	23
$t(i)$	1	5	5	5	5	5	1	1	1	1	1	5	5	5	5	5
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$\gamma'(i)$		26	28	30	27	29	16	20	19	18	17	1	5	4	3	2
$t(i)$		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

C_{11} 4 image points? 0,1,26,14

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\gamma(i)$	0	1	5	4	3	2	26	29	27	30	28	11	14	12	15	13
$\gamma'(i)$	0	11	15	14	13	12	6	8	10	7	9	16	19	17	20	18
$t(i)$	1	4	4	4	4	4	1	4	4	4	4	4	4	4	4	4
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\gamma(i)$		21	24	22	25	23	6	9	7	10	8	16	19	17	20	18
$\gamma'(i)$		21	22	23	24	25	1	4	2	5	3	26	30	29	28	27
$t(i)$		4	4	4	4	4	4	4	4	4	4	1	2	2	2	2

C_{12} 4 image points? 0,6,12,23																	
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
$\gamma(i)$	0	6	9	7	10	8	12	15	13	11	14	24	23	22	21	25	
$\gamma'(i)$	5	26	18	10	22	14	1	4	3	0	2	6	23	15	27	19	
$t(i)$	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
$\gamma(i)$		18	19	20	16	17	30	27	29	26	28	2	5	3	1	4	
$\gamma'(i)$		16	12	8	29	25	11	20	24	28	7	21	9	17	30	13	
$t(i)$		1	5	5	5	5	5	5	5	5	5	5	5	5	5	5	
C_{13} 4 image points? 11,7,2,12																	
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
$\gamma(i)$	11	7	24	28	20	5	2	17	29	23	10	13	12	15	14	0	
$\gamma'(i)$	15	27	6	19	23	5	30	1	25	20	10	0	12	11	14	13	
$t(i)$	4	4	4	4	4	1	4	4	4	4	1	4	1	4	1	4	
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
$\gamma(i)$		25	27	18	3	9	19	22	4	30	8	26	1	21	16	6	
$\gamma'(i)$		29	7	18	21	4	28	22	9	2	16	26	17	3	8	24	
$t(i)$		4	4	1	4	4	4	1	4	4	4	1	4	4	4	4	
C_{14} 4 image points? 10,25,11,0																	
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
$\gamma(i)$	10	25	15	1	30	20	11	23	17	29	2	9	0	6	8	7	
$\gamma'(i)$	29	27	30	0	28	26	7	15	4	18	21	17	23	10	11	2	
$t(i)$	31	31	31	31	31	31	31	31	31	31	31	31	31	31	31	31	
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
$\gamma(i)$		18	22	14	5	26	3	21	28	12	19	27	24	4	16	13	
$\gamma'(i)$		12	5	16	25	8	22	6	13	3	20	1	19	24	9	14	
$t(i)$		31	31	31	31	31	31	31	31	31	31	31	31	31	31	31	
C_{15} 4 image points? 13,17,24,12																	
i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
$\gamma(i)$	13	17	30	21	9	5	24	27	16	4	10	15	12	0	14	11	
$\gamma'(i)$	13	17	30	21	9	5	24	27	16	4	10	15	12	0	14	11	
$t(i)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
i		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
$\gamma(i)$		8	1	18	28	23	3	22	20	6	29	26	7	19	25	2	
$\gamma'(i)$		8	1	18	28	23	3	22	20	6	29	26	7	19	25	2	
$t(i)$		16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	

2.1.90 Answer to exercises.

Answer to **2.1.4.**

First, prove that there are exactly $p+1$ lines through P , more generally through any point not on l . Then, prove that on any line m distinct from l and not incident to both P and Q , there are exactly $p+1$ points. If Q is not on the line join Q to all the points on l and determine the intersection with m . Then, for $P \times Q$ determine a point on an other line through P which is not on l and repeat the argument just given. To count the points, observe that any point

different from P is on a line through P . There are exactly $p+1$ such lines and on each there are p points distinct from P hence altogether $(p+1)p+1$ points.

Answer to

2.1.7.

Given the hexagon $\{A_0, A_1, A_2, A_3, A_4, A_5\}$ such that the alternate vertices A_0, A_2 and A_4 are collinear. The necessary and sufficient condition for A_1, A_3 and A_5 to be collinear is that the points P_0, P_1 and P_2 be collinear. The necessary condition follows using 1.5.1. on the hexagon $\{A_0, P_0, A_2, P_1, A_4, P_2\}$.

Answer to

2.1.6.

The construction is

$$\begin{aligned} r_0 &:= P \times Q_0, r_1 := P \times Q_1, r_2 := P \times Q_2, \\ p_0 &:= Q_1 \times Q_2, p_1 := Q_2 \times Q_0, p_2 := Q_0 \times Q_1, \\ A_0 &:= p_0 \times r_0, A_1 := p_1 \times r_1, A_2 := p_2 \times r_2, \\ a_0 &:= A_1 \times A_2, a_1 := A_2 \times A_0, a_2 := A_0 \times A_1, \\ P_0 &:= a_0 \times r_0, P_1 := a_1 \times r_1, P_2 := a_2 \times r_2, \\ q_0 &:= P_1 \times P_2, q_1 := P_2 \times P_0, q_2 := P_0 \times P_1, \\ R_0 &:= a_0 \times q_0, R_1 := a_1 \times q_1, R_2 := a_2 \times q_2, \\ p &:= R_1 \times R_2. \end{aligned}$$

We have to prove

R_0 is on p and R_i is on p_i .

... ..

This gives the configuration

p on R_i ; a_i on $P_i, R_i, A_{i+1}, A_{i-1}$; p_i on $A_i, R_i, Q_{i+1}, Q_{i-1}$,
 q_i on R_i, P_{i+1}, P_{i-1} ; r_i on P, A_i, P_i, Q_i .

Similarly for lower case and upper case exchanged.

If $p = 3$, q_i and p must contain a fourth point which is one of the 13 known point. By necessity P is on p and Q_i is on q_i . See 2.1.13

Answer to

2.1.8 and 2.1.8.

I will not repeat the computations of Chapter III.

$b_{01} = b_{03}$ if $\frac{m_0}{m_2} = \frac{-m_1}{-m_0}$, therefore if \overline{M} is on the conic $X_0^2 - X_1X_2 = 0$, which is represented

by the matrix $\begin{vmatrix} -2 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{vmatrix}$.

If $B_{22} = (a, m_1, m_0)$, then $b_{12} = [m_0, 0, -a]$, $b_{22} = [m, -a, 0]$, $B_{23} = (a, m_0, m_0)$, $B_{32} = (a, m_1, m_2)$, $b_{23} = [m_0, -a, 0]$, $b_{13} = [m_2, 0, -a]$, $B_{33} = (a, m_0, m_2)$, hence $B_{33} \cdot b_{03}$, hence 2.1.8.

$B_{22} \times B_{33} = [m_1m_2 - m_0^2, -a(m_2 - m_0), a(M - 0 - m_1)]$, line incident to $(0, m_0 - m_1, m_2 - m_0) = AEul_0$, hence 2.1.8.0. 1, and 2, follow from Chapter III.

2.1.91 Relation between Synthetic and Algebraic Finite Projective Geometry.

Introduction.

I start with affine geometry by choosing a particular line m as the ideal line and 2 ordinary lines x and y which intersect at O , as well as an ordinary point M on neither x nor y . I will first associate to ordinary points on the line integers from 0 to $p - 1$, by defining the successor. I will then define addition of points on the line and prove commutativity using the axiom of Pappus. I will then define multiplication of points on the line and prove commutativity using the axiom of Pappus. It remains to prove the distributivity law.

Definition.

*Let $Y := x \times m$, $M_1 := (Y \times M) \times y$.
 $A_0 := O$,
 $A_{i+1} := (((A_i \times M_1) \times m) \times M) \times x$, for $i = 0, 1, \dots$ until $A_n = A_0$.
 A_{i+1} is called the successor of A_0 .*

Theorem.

$$n = p.$$

Proof: The parabolic projectivity associates to A_0, A_1, σ with fixed point Y which associates to A_0, A_1 , associates to A_i, A_{i+1} . By definition $\sigma^n = \epsilon$, the identity mapping. If $n < p$, any other ordinary point on the line distinct from A_i has therefore the same period n , after exhausting all points in the line it follows that n must divide p , therefore $n = p$. We could also give a group theory proof of this Theorem and use the Theorem of Lagrange.

Definition.

*Given 2 points A and B on x , the addition of the 2 points, $C := A + B$ is defined as follows,
 \dots*

Theorem.

The addition is commutative, in other words, $A + B = B + A$.

*Let $u := Y \times M$, $A_0 := (M_2 \times B) \times m$, $A_1 := (M_1 \times A) \times m$,
 $C_0 := (A_1 \times M_1) \times (X \times B_1)$, $C_1 := (A_0 \times M_1) \times (X \times B_0)$.*

The axiom of Pappus applied to the points A_0, A_1, X on m and B_0, B_1, M_1 on u implies that $A_0 \times B_1, B_0 \times A_1$ intersect on the line $A \times B$, therefore $C = D$ or $A + B = B + A$.

Definition.

Given 2 points A and B on x , the multiplication of the 2 points, $C := A \cdot B$ is defined as follows,

*Let $X := y \times m$, $M_0 := (M \times X) \times x$, $Z := (M_0 \times M_1) \times m$,
 $B' := (B \times Z) \times y$, $A'' := (A \times M_1) \times m$, $C := (A'' \times B') \times x$.*

Theorem.

The multiplication is commutative, in other words, $A \cdot B = B \cdot A$.

Proof: We have by definition

$A' := (A \times Z) \times y$, $B'' := (B \times M_1) \times m$, $D := (B'' \times A') \times x$, The axiom of Pappus applied to the points A' , B' , M' on y and A'' , B'' , Z on m implies that $A'' \times B'$, $B'' \times A'$ intersect on the line $A \times B$, therefore $C = D$ or $A \cdot B = B \cdot A$.

Theorem.

The distributive law applies, in other words

$$A \cdot (B + C) = (A \cdot B) + (A \cdot C).$$

Proof: Let Z be a point on m distinct from X and Y .

Let $B' := (B \times Z) \times y$, $C' := (C \times Z) \times y$, $BpC' := (BpC \times Z) \times y$,

Let A'' be the direction of $M_1 \times A$ or $(M_1 \times A) \times m$.

$B \times AtB$, $B \times AtB$ and $B \times AtB$ have the same direction therefore, if $U := (B \times Y) \times (ZtC \times X)$, then $OB = AtCU$, therefore $AtCAtB + C = OAtB$, therefore

.....

2.2 Algebraic Model of Finite Projective Geometry.

2.2.0 Introduction.

In the general descriptions, I will from time to time give, between braces, information to the reader with advanced knowledge. This information is not required for the reader without prior knowledge, and may be explained in later sections or not. In the next paragraph, there are several examples of such use of braces. To construct finite Euclidean geometries I will use a model which depends on the {field of} integers modulo p . The properties of the integers Z are assumed. The model will be constructed in 4 steps.

In the first step, described in this section, I will not distinguish between points and directions, and use the well known algebraization of the finite projective plane {associated with a Galois field, corresponding to the prime p }, see also I.3.

In the second step, (Section 8) I will introduce an ideal line {which plays the role of line at infinity in the Euclidean plane}, the notion of parallelism and of mid-points.

In the third step (III.1), I will introduce the notion of perpendicularity {associated to an involution on the ideal line}. {All these steps are valid in any field.}

In the fourth step (III.2 and 3), I will introduce measure of angles and of distances, together with a finite trigonometry.

¹G21.TEX [MPAP], September 9, 2019

2.2.1 Representation of points, lines and incidence.

Definition.

A point is represented by an ordered triple of integers modulo p , placed between parenthesis. Not all 3 integers can be simultaneously 0. Two triples are equivalent iff one of them can be derived from the other using multiplication, modulo p , by an integer which is not zero modulo p .

Example.

If $p = 3$, there are 13 points:

$(0,0,1), (0,1,0), (0,1,1), (0,1,2), (1,0,0), (1,0,1),$
 $(1,0,2), (1,1,0), (1,1,1), (1,1,2), (1,2,0), (1,2,1), (1,2,2).$
 $(2,2,0)$ is the same as $(1,1,0)$, $(2,1,2)$ is the same as $(1,2,1)$.

Convention.

When I will compute numerically, I will always choose the representation of triples in such a way that the first non zero integer in the triple is 1. This representation will be called the normal representation. When I perform algebraic manipulations, I will multiply by the most convenient expression, to simplify the components or, if appropriate, to make the symmetry evident.

Notation.

A more compact notation for the triples is to use a single integer, as follows,

(0) for $(0,0,1)$,
 $(i+1)$ for $(0,1,i)$, $0 \leq i < p$,
 $((i+1)p+j+1)$ for $(1,i,j)$, $0 \leq i, j < p$.

When there is no ambiguity, I will often drop the parenthesis.

Exercise.

Justify the Notation 2.2.1 and therefore check that there are p^2+p+1 points in the projective geometry associated to p .

Definition.

A line is represented by an ordered triple of integers, modulo p , placed between brackets. Again, not all 3 integers can be simultaneously equal to 0, and 2 triples which can be obtained from each other by multiplication of each integer by the same non zero integer modulo p are considered equal.

Notation.

The notation $[0]$ for $[0,0,1]$, ..., similar to 2.2.1 will be used for lines. I will, also drop the bracket around the single integer, if there is no ambiguity.

Definition.

The point $P = (P_0, P_1, P_2)$ and the line $l = [l_0, l_1, l_2]$ are incident, or P is on l or l goes through P , iff

$$P \cdot l := P_0 \cdot l_0 + P_1 \cdot l_1 + P_2 \cdot l_2 = 0 \pmod{p}.$$

P and l are not incident iff $P \cdot l \neq 0$.

Example.

For $p = 5$, $(1, 0, 1)$ is on $[1, 2, 4]$, $(1, 2, 3)$ is on $[1, 4, 2]$.

The points $(5) = (0, 1, 4)$, $(10) = (1, 0, 4)$, $(14) = (1, 1, 3)$, $(18) = (1, 2, 2)$, $(22) = (1, 3, 1)$, $(26) = (1, 4, 0)$ are the 6 points on the line $[12] = [1, 1, 1]$.

2.2.2 Line through 2 points and point through 2 lines.**Definition.**

I recall the definition of the cross product of 2 three dimensional vectors.

$$X * Y := (X_0, X_1, X_2) * (Y_0, Y_1, Y_2) := \\ (X_1 Y_2 - X_2 Y_1, X_2 Y_0 - X_0 Y_2, X_0 Y_1 - X_1 Y_0)$$

Notation.

When I use the cross product of 2 vectors and then normalize using the convention 2.2.1, I will use the symbol “ \times ”, which recalls the symbol “ $*$ ”, instead of that symbol. The result is unique, if I compute numerically. It is not unique, if I proceed algebraically. In this case, equality implies that an appropriate scaling has been used on either side of the equation or on both sides. See Chapter V, for some examples.

Theorem.

$P \times Q$ is the line through the distinct points P and Q .

$p \times q$ is the point on the distinct lines p and q .

This follows from $(P \times Q) \cdot P = (P \times Q) \cdot Q = 0$ or $(p \times q) \cdot p = (p \times q) \cdot q = 0$.

Example.

For $p = 5$, $[1, 1, 3] := (1, 2, 4) \times (1, 3, 2)$ and $(1, 1, 3) := [1, 2, 4] \times [1, 3, 2]$.

Theorem.

0. $k_1 A * B - k_2 C * D$ is a line incident to $A \times B$ and $C \times D$.

1. The lines $k_0 A * B - k_1 C * D$, $k_1 C * D - k_2 E * F$ and $k_2 E * F - k_0 A * B$, are incident.

Example.

For any p , let $A = (0,1,1)$, $B = (1,2,1)$, $C = (2,1,1)$, $D = (1,3,1)$, $E = (2,4,1)$, $F = (4,3,1)$, then $A * B = [-1, 1, -1]$, $C * D = [-2, -1, 5]$, $E * F = [1, 2, -10]$. If $k_0 = k_1 = k_2 = 1$, we obtain the lines $[1, 2, -6]$, $[-3, -3, 15]$, $[2, 1, -9]$ incident to $(4,1,1)$.

Comment.

The algebraic method allows the representation of points or lines by a single symbol. This method which was well used in 19-th Century text, see for instance Salmon, 1879, Chapter XIV, has somehow fallen in disfavor.

2.2.3 The model satisfies the axioms of the projective Pappus plane of order p .

Introduction.

After proving that the algebraic model satisfies the axioms of finite projective geometry, I give construction of points on a line whose coordinates have a simple algebraic relationship. These could be used as a tool for the construction of points whose coordinates are known in terms of points constructed earlier. The notation $O + kM$ used in Theorem 2.2.2 is partially justified in section 2.2.4.

Theorem.

Each line l contains exactly $p + 1$ points, each point P is on exactly $p + 1$ lines, therefore The model satisfies axiom 2.1.2.3 and its dual.

Proof: We want to find the points (x, y, z) on the line $[a, b, c]$. At least one of the 3 integers, a , b or c is different from 0, let it be c , in this case x and y cannot both be 0. Given x and y we can solve $ax + by + cz = 0$ for the integer z , using the algorithm of Euclid-Aryabatha, $z := -(ax + by)/c$. (See I.??)

If $x = 1$, to each value of y from 0 to $p - 1$ corresponds a value of z , namely $-(a + by)/c$.

If $x = 0$ and $y = 1$, we obtain one value of z , namely $-b/c$.

Therefore we obtain altogether $p + 1$ points.

Exchanging brackets and parenthesis gives the dual property.

Theorem.

The model satisfies the axiom 2.1.2.4. of Pappus.

Proof: I will give the proof in the special case in which the lines are $[0] = [0, 0, 1]$ and $[1] = [0, 1, 0]$.

The general case can be deduced from general considerations on projectivity or can be proven directly. This direct proof is left as an exercise.

We choose $A_0 = (1, a_0, 0)$, $A_1 = (1, a_1, 0)$, $A_2 = (1, a_2, 0)$ and $B_0 = (1, 0, b_0)$, $B_1 = (1, 0, b_1)$, $B_2 = (1, 0, b_2)$, with $a_0 a_1 a_2 b_0 b_1 b_2 \neq 0$. Then

$$C_0 = (a_2 b_2 - a_1 b_1, a_1 a_2 (b_2 - b_1), b_1 b_2 (a_2 - a_1)),$$

$$\begin{aligned} C_1 &= (a_0 b_0 - a_2 b_2, a_2 a_0 (b_0 - b_2), b_2 b_0 (a_0 - a_2)), \\ C_2 &= (a_1 b_1 - a_0 b_0, a_0 a_1 (b_1 - b_0), b_0 b_1 (a_1 - a_0)). \end{aligned}$$

It is easy to verify that $a_0 b_0 C_0 + a_1 b_1 C_1 + a_2 b_2 C_2 = 0$, therefore the points C_0 , C_1 and C_2 are collinear as will be seen shortly, in 2.2.4.

The special cases, where $A_2 = (0, 1, 0)$ or $B_2 = (0, 0, 1)$ or a_0 or $b_0 = 0$, can be verified easily.

Theorem.

The algebraic model satisfies the axioms 2.1.2 of finite projective geometry and therefore it can be used to prove all the theorems of finite projective geometry.

Definition.

Given a triangle $\{a_0, a_1, a_2\}$, and 2 arbitrary lines, x and y , the Pappus line of x and y , is the line z associated to the application of the axiom of Pappus to the intersection with x and y of the lines a_0 , a_1 and a_2 .

Theorem.

If $a_0 = [1, 0, 0]$, $a_1 = [0, 1, 0]$, $a_2 = [0, 0, 1]$, if $x = [x_0, x_1, x_2]$ and $y = [y_0, y_1, y_2]$ then the Pappus line of x and y is

$$z = [x_0 y_0 (x_1 y_2 + x_2 y_1), x_1 y_1 (x_2 y_0 + x_0 y_2), x_2 y_2 (x_0 y_1 + x_1 y_0)].$$

The proof is left as an exercise. Hint: One of the 3 points on z is $(x_0^2 y_1 y_2 - x_1 x_2 y_0^2, x_0 y_0 (x_2 y_0 - x_0 y_2), x_0 y_0 (x_1 y_0 - x_0 y_1))$.

Comment.

Definition 2.2.3 may be new, it was suggested by one of the construction in a triangle of the point of Lemoine from the barycenter and orthocenter. See 4.2.12. The operation of deriving z from x and y is commutative but is not associative.

Exercise.

Verify that if $p = 2$ and $p = 4$ the diagonal points of a complete quadrangle are collinear. For $p = 2$, choose one such quadrangle. For $p = 4$, the coordinates of the points are $u + v\xi$, where $u, v \in \mathbb{Z}_2$ and $\xi^2 + \xi + 1 = 0$. Choose a quadrangle which is not in the subspace $v = 0$.

Exercise.

Prove algebraically the 2 cases of the Theorem of Desargues.

Definition.

Let the coordinates of the distinct points $O = (o_0, o_1, o_2)$ and $M = (m_0, m_1, m_2)$ be normalized, $O + xM$ is the point on $O \times M$ whose coordinates are $(o_0 + x m_0, o_1 + x m_1, o_2 + x m_2)$.

Comment.

The following Theorem relates specific constructions in projective geometry to algebraic operations, nothing is claimed as to the projective properties of the operation “+”, these will require the introduction of preferences associated with affine and Euclidean geometries. In this Theorem we have not used the notation “*” which appears in section 2.2.4, this the reason why the notation $O + kM$ used in Theorem 2.2.2 is only partially justified in section 2.2.4.

Theorem. [Baker]

Let A, B, C, E be points on the line $a := O \times M$ such that $A = O + aM, B = O + bM, C = O + cM, E = O + M$, the following constructions gives points $O + xM, A'$ for $x = -a, D$ for $x = a + b, D'$ for $x = a + b + c, L$ for $x = ab, I$ for $x = a^{-1}$.

Let P be a point not on a and let Q be a point on $A \times P$, distinct from A and P .

0. Let

$$\begin{aligned} q &:= O \times Q, U := q \times (P \times M), \\ p &:= O \times P, V := p \times (Q \times M), \\ A' &:= (U \times V) \times a, \end{aligned}$$

then

$$A' = O + (-a)A.$$

1. Let

$$\begin{aligned} pb &:= P \times B, R := pb \times (O \times Q), \\ b &:= R \times M, \\ pa &:= A \times P, S := pa \times b, \\ c &:= Q \times M, \\ T &:= pb \times c, \\ D &:= (S \times T) \times a, \end{aligned}$$

then

$$D = O + (a + b)M.$$

2. Let

$$\begin{aligned} R' &:= (O \times T) \times b, \\ T' &:= (C \times R') \times c, \\ D' &:= (S \times T') \times a, \end{aligned}$$

then

$$D' = O + (a + b + c)M.$$

3. Let

$$\begin{aligned} J &:= pa \times (E \times R), \\ K &:= pb \times (J \times M), \\ L &:= (Q \times K) \times a, \end{aligned}$$

then

$$L = O + abM.$$

4. Let

$$\begin{aligned} G &:= (P \times E) \times c, \\ H &= (Q \times E) \times p, \\ I &= (G \times H) \times a, \end{aligned}$$

then

$$I = O + a^{-1}M.$$

Proof: Choose the coordinate system such that

$O = (1, 0, 0)$, $M = (0, 1, 0)$, $P = (0, 0, 1)$, then, for some a, b, c and $q \neq 0$,

$$A = (1, a, 0), B = (1, b, 0), C = (1, c, 0), E = (1, 1, 0), Q = (1, a, q).$$

For 0, we have $a = [0, 0, 1]$, $q = [0, q, -a]$, $U = (0, a, q)$, $p = [0, 1, 0]$, $V = (1, 0, q)$, $A' = (1, -a, 0)$.

For 1, we have $pb = [b, -1, 0]$, $R = (a, ab, bq)$, $b = [bq, 0, -a]$, $pa = [a, -1, 0]$,

$$S = (a, a^2, bq), c = [q, 0, -1], T = (1, b, q), D = (1, a+b, 0).$$

For 2, we have $R' = (a, b^2, bq)$, $T' = (b, bc+b^2-ac, bq)$, $D' = (1, a+b+c, 0)$.

For 3, we have $J = (a(b-1), a^2(b-1), bq(a-1))$, $K = (a(b-1), ab(b-1), bq(a-1))$,

$$L = (1, ab, 0).$$

For 4, we have $G = (1, 1, q)$, $H = (1-a, 0, 1)$, $I = (a, 1, 0)$.

Exercise.

Give constructions

0. associated with the associativity, commutativity and distributivity rules $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, $b + a = a + b$,
 $b \cdot a = a \cdot b$ and $a(b + c) = a \cdot b + a \cdot c$.

1. for $F = O + ab^{-1}M$.

2.2.4 Finite vector calculus and simple applications.

Introduction.

The following properties generalize, to the finite case, well known properties of vector calculus. Capital letters will represent points, lower case letters will represent lines, the role of points and lines can be interchanged because of duality. I have chosen to give at once the relations which directly apply to geometry rather than those which correspond to vector calculus. These would be obtained if all lower case letters are replaced by upper case letters. 1 or 2 of Theorem 2.2.4 justify the representation of any point on the line $A * B$ by $kA + lB$.

Theorem.

0. $A * B = -B * A$.
1. $(A * B) * c = (A \cdot c) B - (B \cdot c) A$.
2. $a * (B * C) = (a \cdot C) B - (a \cdot B) C$.

3. $(A * B) \cdot C = (B * C) \cdot A = (C * A) \cdot B$
 $= -(B * A) \cdot C = -(C * B) \cdot A = -(A * C) \cdot B.$
4. $(A * B) \cdot (c * d) = (A \cdot c)(B \cdot d) - (A \cdot d)(B \cdot c).$
5. $(A * B) * (C * D) = (A \cdot (C * D))B - (B \cdot (C * D))A.$
6. $(C * A) * (A * B) = ((A * B) \cdot C) A.$
7. $((A * B) \cdot C) P = ((B * C) \cdot P) A + ((C * A) \cdot P) B + ((A * B) \cdot P) C.$
8. $(A * B) * C + (B * C) * A + (C * A) * B = 0.$

Proof: The proof of 0 is immediate, the proof of 1. follows from the computation of any of the components of the triples on both sides, for the 0-th component,

$$(A_2B_0 - A_0B_2)c_2 - (A_0B_1 - A_1B_0)c_1 = (A_1c_1 + A_2c_2)B_0 - (B_1c_1 + B_2c_2)A_0,$$

adding and subtracting $A_0 B_0 c_0$ gives the 0-th component of the second member of 1. 2, follows from 0 and 1. 3, give various expressions of the 3 by 3 determinant constructed with the 3 triples as the 3 columns, namely

$$A_0B_1C_2 + A_1B_2C_0 + A_2B_0C_1 - A_0B_2C_1 - A_1B_0C_2 - A_2B_1C_0.$$

for 4, $(A * B) \cdot (C * D) = ((C * D) * A) \cdot B = (A \cdot C)(D \cdot B) - (A \cdot D) \cdot (C \cdot B).$

because of 3 and then 1.

6, follows from 1.

7, follows from 0, 1 and 2 applied to $(B * A) * (C * P).$

8, follows from 1.

Theorem.

A, B and C are collinear iff $(A * B) \cdot C = 0.$

Proof: This an immediate consequence of the fact that $(A * B) \cdot C = 0$ iff C is on the line $A * B.$

Theorem. [Fano]

If p is odd and $\{A, B, C, D\}$ is a complete quadrangle, the intersections $b * b_1, c * c_1, d * d_1$ of the opposite sides are not collinear.

Proof: $(b * b_1) * (c * c_1) * (d * d_1)$

$$= 2((B * C) \cdot D)((C * D) \cdot A)((D * A) \cdot B)((A * B) \cdot C) \neq 0,$$

by repeated use of 2.2.4.0 to .3.

Comment.

$p = 2$ is excluded, because in this case, the preceding Theorem is false, in fact every complete quadrangle has its diagonal collinear. I leave as an exercise the determination of where the above theory breaks down.

Comment.

In algebraic manipulations, although $A_i = a_{i+1} \times a_{i-1}$, we can not use this expression when the sum of two or more terms is involved, because the scaling to go from “ \times ” to “ \times ” is different for each index i . It is therefore essential to do these algebraic manipulations using “ $*$ ”. For the various proof, a_i will always denote $A_{i+1} * A_{i-1}$ and use will often be made of the following Theorem:

Theorem.

If $a_i := A_{i+1} * A_{i-1}$ and $t := (A_0 * A_1) \cdot A_2$, then

$$a_{i+1} * a_{i-1} = t A_i.$$

Again, $i = 0, 1, 2$ and subscript addition is made modulo 3.

Proof: The conclusion follows from 2.2.4.7 and from 2.2.4.3.

Comment.

The identity 2.2.4.8 is the fundamental identity in Lie algebras. The set of points or the set of lines form a Lie algebra, if we use as multiplication “ $*$ ”. See, for instance, Cohn, Lie groups.

Notation.

$\det(A, B, C)$ will denote $(A * B) \cdot C = (B * C) \cdot A = (C * A) \cdot B =$.

Theorem.

$$\begin{aligned} & \det(A, C, E) \det(B, D, E) \det(A, B, F) \det(C, D, F) \\ &= \det(A, C, F) \det(B, D, F) \det(A, B, E) \det(C, D, E) \text{ iff} \\ & (((A \times E) \times (D \times C)) \times ((E \times B) \times (C \times F))) \cdot ((B \times D) \times (A \times F)) = 0. \end{aligned}$$

Proof: By 2.2.4.1 and .2, the second equation is equivalent to
 $((A \times E) \times (D \times C)) \cdot (C \times F) ((B \times D) \times (A \times F)) \cdot (E \times B) =$
 $((A \times E) \times (D \times C)) \cdot (E \times B) ((B \times D) \times (A \times F)) \cdot (C \times F),$
 by 2.2.4.3 this is equivalent to
 $((D \times C) \times (C \times F)) \cdot (A \times E) ((E \times B) \times (B \times D)) \cdot (A \times F) =$
 $((E \times B) \times (A \times E)) \cdot (D \times C) ((A \times F) \times (C \times F)) \cdot (B \times D),$
 by 2.2.4.6 this is equivalent to
 $(\det(C, F, D) C) \cdot (A \times E) (\det(B, D, E) B) \cdot (A \times F) =$
 $(\det(A, B, E) E) \cdot (D \times C) (\det(A, F, C) F) \cdot (B \times D).$

This can be considered as an algebraic form of Pascal’s Theorem. for the order A, E, B, D, C, F .

2.2.5 Anharmonic ratio, harmonic quatern, equiharmonic quatern.**Convention.**

In this section, I will use the convention that if point is on the line $[0, 1, 0]$,
 $(\infty, 0, 1)$ denotes the point $(1, 0, 0)$.

Definition.

Given 4 points on the line $[0, 1, 0]$,

$A_0 = (m_0, 0, 1)$, $A_1 = (m_1, 0, 1)$, $A_2 = (m_2, 0, 1)$, $A_3 = (m_3, 0, 1)$.

The anharmonic ratio is defined by

$$\text{anhr}(A_0, A_1, A_2, A_3) := \text{anhr}(m_0, m_1, m_2, m_3) := \frac{(m_2 - m_0)(m_3 - m_1)}{(m_2 - m_1)(m_3 - m_0)}.$$

If $m_i = \infty$ then the 2 factors containing m_i are dropped, e.g.

if $m_0 = \infty$ then $\text{anhr}(A_0, A_1, A_2, A_3) := \text{anhr}(\infty, m_1, m_2, m_3) := \frac{m_3 - m_1}{m_2 - m_1}$.

Lemma.

Let a, b, c and d be such that $ad - bc \neq 0$, if $t(m) := \frac{am+b}{cm+d}$ then $\text{anhr}(m_0, m_1, m_2, m_3) = \text{anhr}(t(m_0), t(m_1), t(m_2), t(m_3))$.

If we project 4 points A_i on a onto 4 points B_i on b from the point B , it is easy to see that each coordinate of B is a linear functions of m , therefore the ratio of 2 of some specific coordinates of B are functions of the form $t(m)$. This justifies the following 2 Theorems.

Theorem.

Given 4 points B_i on a line b , the anharmonic ratio of the 4 points is the anharmonic ratio of the 4 ratios obtained by dividing the j -th coordinate of B_i by the k -th coordinate for appropriate $j \neq k$.

Theorem.

If 4 points B_i are obtained by successive projections from 4 points A_i , then $\text{anhr}(B_0, B_1, B_2, B_3) = \text{anhr}(A_0, A_1, A_2, A_3)$.

Theorem.

If $r := \text{anhr}(A_0, A_1, A_2, A_3)$, then if we permute the points in all possible way we obtain, in general 6 different values of the anharmonic ratio:

For					the anharmonic ratio is
A_0, A_1, A_2, A_3	A_1, A_0, A_3, A_2	A_2, A_3, A_0, A_1	A_3, A_2, A_1, A_0	r	
A_0, A_1, A_3, A_2	A_1, A_0, A_2, A_3	A_2, A_3, A_1, A_0	A_3, A_2, A_0, A_1	$\frac{1}{r}$	
A_0, A_2, A_1, A_3	A_1, A_3, A_0, A_2	A_2, A_0, A_3, A_1	A_3, A_1, A_2, A_0	$1 - r$	
A_0, A_2, A_3, A_1	A_1, A_3, A_2, A_0	A_2, A_0, A_1, A_3	A_3, A_1, A_0, A_2	$\frac{1}{1-r}$	
A_0, A_3, A_1, A_2	A_1, A_2, A_0, A_3	A_2, A_1, A_3, A_0	A_3, A_0, A_2, A_1	$\frac{r-1}{r}$	
A_0, A_3, A_2, A_1	A_1, A_2, A_3, A_0	A_2, A_1, A_0, A_3	A_3, A_0, A_1, A_2	$\frac{r}{r-1}$	

Theorem.

There are 3 cases for which the 6 values are not distinct:

0. $0, \infty, 1, 1, \infty, 0$, when 2 points are identical.
1. $-1, -1, 2, \frac{1}{2}, 2, \frac{1}{2}$.
2. $v, \frac{1}{v}, \frac{1}{v}, v, v, \frac{1}{v}$, with $v^2 - v + 1 = 0$ or $v = \frac{1+\sqrt{-3}}{2}$
 v is real, if $p \equiv 1 \pmod{6}$.

For instance, if $p = 7$, then $v = -2$ or 3 , if $p = 19$, then $v = -7$ or 8 .

Theorem.

Given a complete quadrangle A, B, C, D , the intersection of 2 of lines through opposite vertices and the line through 2 diagonal points make a harmonic quatern with these diagonal points. More precisely, let $E := (A \times B) \times (C \times D)$ and $F := (A \times D) \times (B \times C)$ be 2 of the diagonal points, let $a := E \times F$, $G := a \times (B \times D)$ and $H := a \times (A \times C)$, then $r := \text{anhr}(E, F, G, H) = -1$.

Let I be the third diagonal point, projecting the 4 points from B on $A \times C$ and these from D on a gives $r = \text{anhr}(A, C, I, H) = \text{anhr}(F, E, G, H) = \frac{1}{r}$, therefore $r^2 = 1$ but we do not have case 0, $r = 1$, therefore $r = -1$ which is case 1.

Definition.

In the special case of the preceding Theorem:

Case 1, we say that A_2, A_3 are harmonic conjugate of A_0, A_1 , or that A_0, A_1, A_2, A_3 form a harmonic quatern.

Case 2, we say that A_0, A_1, A_2, A_3 form a equiharmonic quatern.

Definition.

The pre-equiharmonic non confined configuration is defined as follows:

Given a complete quadrangle A, B, F, K , determine

$$q := A \times B, p := A \times F, b := B \times F, r := A \times K, f := B \times K,$$

$$H := p \times f, J := b \times r,$$

choose C on q , distinct from A and B , determine

$$c := C \times K, P := b \times c, R := p \times c, g := C \times F, Q := f \times g, L := g \times r,$$

$$d := P \times L, h := Q \times R, D := d \times h.$$

Theorem.

Given 2.2.5

1. $D \cdot q = 0$.
2. $J \cdot h = 0 \Rightarrow H \cdot d = 0$.
3. The geometric condition $J \cdot h = 0$ is equivalent to A, B, C, D is an equiharmonic quatern.

Proof: Let $A = (0, 0, 1)$, $B = (0, 1, 1)$, $F = (1, 0, 1)$, $K = (1, 1, 1)$. We have $q = [1, 0, 0]$, $p = [0, 1, 0]$, $b = [-1, -1, 1]$, $r = [-1, 1, 0]$, $f = [0, -1, 1]$, $H = (1, 0, 0)$, $J = (1, 1, 2)$. Let $C = (0, c, 1)$, then $c = [1-c, -1, c]$, $g = [c, 1, -c]$, $P = (1-c, 1, 2-c)$, $R = (c, 0, c-1)$, $Q = (c-1, c, c)$, $L = (c, c, c+1)$, $d = [c^2-c+1, 2c-1, -c^2]$, $h = [c^2-c, 2c-1, -c^2]$, $D = (0, c^2, 2c-1)$. $J \cdot h = 0$ or $H \cdot d = 0$ are equivalent to $c^2-c+1 = 0$.

Definition.

Given 2.2.5 and $J \cdot h = 0$, the pre-equi-harmonic configuration is then called an equiharmonic configuration.

Theorem.

A pre-equi-harmonic configuration is of type

$$10 \times 3 + 2 \times 2 \text{ \& } 7 \times 4 + 2 \times 3,$$

unless it is equiharmonic, in which case, it is of type

$$12 \times 3 \text{ \& } 9 \times 4.$$

The sets of 4 points on each of the 9 lines is an equiharmonic quatern.

Proof: The configuration, with projections as given below is as follows.

<i>Points:</i>	<i>lines:</i>	<i>from</i>
$A: q, p, r,$	$q: A, B, C, D,$	
$B: q, b, f,$	$p: A, F, R, H,$	$P (Q, H)$
$C: q, c, g,$	$r: A, J, K, L,$	$P (Q, K)$
$D: q, h, d,$	$b: F, B, P, J,$	$R (L, J)$
$P: b, c, d,$	$f: H, B, K, Q,$	$R (L, K)$
$R: p, c, h,$	$c: R, K, C, P,$	$H (J, K)$
$H: p, f, d,$	$g: F, Q, C, L,$	$H (J, L)$
$K: r, f, c,$	$d: L, H, P, D,$	$K (F, H)$
$Q: f, g, h,$	$h: J, Q, R, D,$	$K (F, R)$
$L: r, g, d,$		
$J: r, b, h,$		
$F: p, b, g,$		

If we project A, B, C, D from P on p we get A, F, R, H ; if we project A, B, C, D from Q on p we get A, H, F, R ; therefore $r = \frac{1}{1-r}$. To establish the results for the other sets, it is sufficient to project from a point, those of the line q . The points on each line have been arranged correspondingly. For instance, for f , the point of projection is R and the lines are p, c and h ; if the point of projection is L , the order is K, B, Q, H , (the second point corresponds to A or B for p and r the others are obtained circularly).

Exercise.

Prove that the configuration of 2.1.7 is equiharmonic.

Exercise.

Study the configuration which starts with P_0, P_1, P_3, P_5 and P_7 on $P_1 \times P_5$. Constructs $l_0 := P_0 \times P_1, l_1 := P_0 \times P_3, l_3 := P_0 \times P_5, l_5 := P_3 \times P_5, l_4 := P_1 \times P_5, l_8 := P_3 \times P_7, P_6 := l_2 \times l_8, l_3 := P_1 \times P_6, P_4 := l_1 \times l_3, l_7 := P_4 \times P_7, P_2 := l_0 \times l_5$.

Using a coordinate system such that $P_0 = (1, 0, 0), P_1 = (0, 1, 0), P_3 = (0, 0, 1)$ and $P_5 = (1, 1, 1)$, determine an algebraic condition involving the coordinates of P_7 for P_2 to be on l_7 . Prove that if P_2 is on l_7 , the configuration is of type 8×3 & 8×3 .

Exercise.

Study the configuration which starts with A_0, A_1, B_0, B_1 and A_2 on $A_0 \times A_1$, constructs $d_0 := A_0 \times B_0, d_1 := A_1 \times B_1, d_3 := A_0 \times B_1, d_4 := A_1 \times B_0, d_6 := A_2 \times B_0, d_8 := A_2 \times B_1, a := A_0 \times A_1, b := B_0 \times B_1, P := a \times b, C_0 := d_3 \times d_4, C_1 := d_1 \times d_6, C_2 := d_0 \times d_8, a_0 := C_0 \times C_1, d_5 := A_0 \times C_1, d_7 := A_1 \times C_2, B_2 := d_5 \times d_7$.

Determine a geometric condition on A_2 for P, A_0, A_1, A_2 to be an equiharmonic quatern, prove that in this case P, B_0, B_1, B_2 is also a equiharmonic quatern.

2.2.6 Projectivity of lines and involution on a line.

Introduction.

In the next section we will study algebraically the isomorphisms of the plane into itself. The special case of the mapping of a line of the plane into a line will be defined here. The justification will follow from the general definition. Such a mapping is called a projectivity. Special cases will be studied and appropriate constructions will be given. The notion of amicable projectivities, which are at the basis of the definition of equality of angles is also introduced. The concept of harmonic conjugates is due to LaHire⁵. The term projectivity will be used here only for correspondances between points on lines not for correspondance of a plane with itself as done by some authors. Theorem 2.2.6 gives a construction, when 2 points A and B are fixed, and D corresponds to C .

Convention.

For simplicity, I will assume that the line is $[0,0,1]$, the last component of all the points is 0, I will therefore only write the first 2 components.

Definition.

The mapping which associates to the point (x_0, x_1) the point (y_0, y_1) given by

$$(y_0) = (ab)(x_0),$$

$$(y_1) = (cd)(x_1)$$

with $ad - bc \neq 0$, is called a projectivity.

Theorem.

If C is the intersection of c and $A \times B$, the point D such that A, B, C and D form a harmonic quatern is given by

$$D := B \cdot cA + A \cdot cB.$$

Definition.

D is called the harmonic conjugate of C with respect to A and B .

Theorem.

0. If $K = (1, k, 0)$, $L = (1, l, 0)$ and $M = (1, m, 0)$ then N , the conjugate of M with respect to K and L , is given by

$$N = (2m - l - k, k m + l m - 2k l, 0).$$

1. If N is the harmonic conjugate of M with respect to K and L ,

then

M is the harmonic conjugate of N with respect to K and L ,

⁵Coxeter, p.16

K is the harmonic conjugate of L with respect to M and N , and
 L is the harmonic conjugate of L with respect to M and N .

Theorem.

If $A := (1, 0, 0)$, $B := (0, 0, 1)$, $C := (1, k, 0)$, $D := (1, l, 0)$, the projectivity on $c := A \times B$ which associates A to A , B to B and C to D , can be constructed by choosing a line b through a , distinct from c , a line a through b distinct from c , a point P on a not on b or c , then

$$S := (P \times C) \times b, T := (P \times D) \times b.$$

The mapping N of $M := (1, m, 0)$ is obtained by the construction

$$Q := (M \times S) \times a, N := (Q \times T) \times c \text{ and } N = (k, lm, 0).$$

The proof is left as an exercise.

Theorem.

Let $u := \frac{l}{k}$, $\phi(M) = (1, um, 0)$ and $\phi^j(M) = (1, u^j m, 0)$. If u is a primitive root of p , the projectivity has order $p - 1$.

The proof is left as an exercise.

Theorem.

If K , L and M are distinct, N is distinct from M .

Proof. The last theorem would imply that $m(2m - l - k) = km + lm - 2kl$ or $(m - l)(k - m) = 0$.

Theorem.

If K and M are exchanged and L is replaced by N , then N is replaced by L .

Indeed, $n(2m - k - l) = km + lm - 2kl$ can be written $l(2k - m - n) = mk + nk - 2mn$.

The following theorem gives a construction of a projectivity on a line in which B_i corresponds to A_i , $i = 0, 1, 2$.

Theorem.

Given $A_i, B_i, i = 0, 1, 2$, 6 points on a line u , such that the A_i are distinct and the B_i are distinct. Choose the line $s \neq u$ and the point S , with $S \cdot u \neq 0, S \cdot s \neq 0$.

Construct

$C_i := (S \times A_i) \times s, D_j := (B_0 \times C_j) \times (C_0 \times B_j), j = 1, 2, d := D_1 \times D_2$, then for any A_l on u , construct

$$C_l := (S \times A_l) \times s, D_l := (B_0 \times C_l) \times d, B_l := (C_0 \times D_l) \times u.$$

The mapping which associates B_l to A_l is a projectivity.

Theorem.

Given $A_0 = (1, 0, 0)$, $A_1 = (1, a_1, 0)$, $A_2 = (1, a_2, 0)$ and $B_0 = (0, 1, 0)$, $B_1 = (1, b_1, 0)$, $B_2 = (1, b_2, 0)$, then the projectivity which is defined in the preceding theorem and associates

to $A_i, B_i, i = 0, 1, 2$, associates to

$A_j = (1, a_j, 0)$, the point

$B_j = ((a_2 - a_1)a_j, (a_2b_2 - a_1b_1)a_j - a_1a_2(b_2 - b_1), 0), j > 2$.

The proof is left as an exercise.

Theorem.

Let $g = \frac{a_2b_2 - a_1b_1}{2(a_2 - a_1)}$ and $h = a_1a_2 \frac{b_2 - b_1}{a_2 - a_1}$,

The projectivity, which associates to $(1, u, 0), (1, 2g - \frac{h}{u}, 0)$

0. is an involution iff $g = 0$,
1. is an hyperbolic projectivity if $g^2 - h$ is a quadratic residue modulo p ,
2. is an elliptic projectivity if $g^2 - h$ is a non residue and
3. is a parabolic projectivity if $h = g^2$, the fixed point being g .

Proof. If we eliminate u_1 from $u_1 = 2g - \frac{h}{u_0}$ and $u_0 = 2g - \frac{h}{u_1}$, we get $2g(u_0^2 - gu_0 + h)$. If this relation is to be satisfied for all u_0 , it is necessary that $g = 0$. The condition is sufficient because if $\phi(u) := \frac{h}{u}$, then $\phi \circ \phi$ is the identity.

Theorem.

Given 3 distinct points A_0, A_1 and A_2 on the line a and 3 distinct points B_0, B_1 and B_2 on the line b ,

let $A_2 = r_0A_0 + r_1A_1$ and $B_2 = s_0B_0 + s_1B_1$, then

if $A_j = t_0A_0 + t_1A_1, B_j = \phi(A_j) := \frac{s_0t_0}{r_0}B_0 + \frac{s_1t_1}{r_1}B_1$

is a projectivity which associates A_j to B_j for all j .

Proof. The correspondance clearly associates A_j to B_j for $j = 0$, using $t_1 = 0$, for $j = 1$ using $t_0 = 0$ and for $j = 2$ using $t_0 = r_0$ and $t_1 = r_1$. The proof that it is a projectivity is left as an exercise.

Theorem.

0. If the lines a and b of the preceeding Theorem coincide, there exists constants f_0, f_1, f_2 and f_3 such that

$$B_j = (f_0t_0 + f_1t_1)A_0 + (f_2t_0 + f_3t_1)A_1.$$

If $B_0 = b_{00}A_0 + b_{01}A_1$ and $B_1 = b_{10}A_0 + b_{11}A_1$, then

$$f_0 = \frac{s_0b_{00}}{r_0}, f_1 = \frac{s_1b_{10}}{r_1}, f_2 = \frac{s_0b_{01}}{r_0}, f_3 = \frac{s_1b_{11}}{r_1}.$$

1. The values t_0 and t_1 for which A_j is a fixed point, in other words, for which $A_j = B_j$ satisfy

$$f_1t_1^2 - (f_3 - f_0)t_0t_1 - f_2t_0^2 = 0.$$

2. The projectivity is hyperbolic, parabolic or elliptic if $(f_3 - f_0)^2 + 4f_1f_2$ is positive, zero or negative.

3. The projectivity is an involution iff $f_0 + f_3 = 0$.

The proof is left as an exercise.

Definition.

Using the notation of 2.2.6 and of 2.2.6 with primes used for an other projectivity, we say that 2 projectivities on the same line are amicable iff there exists a constant k different from 0 such that

$$f'_1 = kf_1, f'_2 = kf_2, f'_3 - f'_0 = k(f_3 - f_0).$$

Theorem.

Two amicable projectivities are either both hyperbolic, or both parabolic or both elliptic. If they are both hyperbolic, they have the same fixed points.

Example.

For $p = 5$, a projectivity ϕ associates to

$A_0 = (5), A_1 = (10), A_2 = (14), (18), (22), (26), B_0 = (26), B_1 = (5), B_2 = (18), (22), (10), (14).$
 $r_0 = r_1 = 1, s_0 = 1, s_2 = -2, b_{00} = -1, b_{01} = 1, b_{10} = 1, b_{11} = 0, f_0 = -1, f_1 = -2, f_2 = 1,$
 $f_3 = 0.$ A second projectivity ϕ' associates to

$A'_0 = (5), A'_1 = (10), A'_2 = (14), (18), (22), (26), B'_0 = (18), B'_1 = (14), B'_2 = (10), (5), (26), (22).$
 $r'_0 = r'_1 = 1, s'_0 = -1, s'_2 = 2, b_{00'} = 2, b_{01'} = 1, b'_{10} = 1, b'_{11} = 1, f'_0 = -2, f'_1 = 2, f'_2 = -1,$
 $f'_3 = 2.$ ϕ' is an involution an $f'_0 + f'_3 = 0$. ϕ and ϕ' are sympathic, with $k = -1$. The fixed points are complex and correspond to $t_0 = 1$ and $t_1 = 1 + \sqrt{-2}$ or $t_1 = 1 - \sqrt{-2}$.

Comment.

The definition 2.2.6 will be used in III.1.3. to define equality of angles.

Theorem.

If x is one of the coordinates, the projectivity takes the form

$$F(x) = \frac{a+bx}{c+dx}$$

and the fixed points are the roots of

$$dx^2 + (c - b)x - a = 0.$$

Exercise.

Prove that the following construction defines a projectivity on u in which A_{i+1} corresponds to A_i , the points A_0 to A_3 being given. Let l_f is a line through A_2 distinct from u , E is a point on l_f distinct from A_2 , F is a point on l_f distinct from A_2 and E , l_d is a line through A_0 distinct from u , $D_1 := l_f \times l_d$, D is a point on $A_1 \times D_1$ distinct from A_1 and D_1 , $E_0 := (A_0 \times E) \times (A_1 \times F)$, $E_2 := (A_3 \times F) \times (E \times (l_d \times (A_2 \times D)))$, $A_{i+1} := (((((A_i \times D) \times l_d) \times E) \times l_e) \times F) \times i$, $i = 4, \dots$. The preceding construction is less efficient than that in 2.2.6.

2.2.7 Collineation, central collineation, homology and elation.

Introduction.

Collineations, {which are isomorphisms of the plane onto itself} have been defined in 2.1.12. They will now be studied algebraically. The point mapping which associates points to points is represented by a non singular matrix, and so is the line mapping which associates lines to lines. Two matrices which can be obtained from each other by multiplication, modulo p , by an integer different from 0 correspond to the same collineation.

Theorem.

Given 2 complete quadrangles A_j and B_j , $j = 0, 1, 2, 3$,

Let $a_i := A_{i+1} * A_{i-1}$ and $b_i := B_{i+1} * B_{i-1}$,

let $A_3 = r_0 A_0 + r_1 A_1 + r_2 A_2$, $B_3 = s_0 B_0 + s_1 B_1 + s_2 B_2$

$$q_i := \frac{s_i}{r_i}, u_i := q_{i+1} q_{i-1},$$

then, up to a proportionality constant, $q_i = \frac{b_i \cdot B_3}{a_i \cdot A_3}$.

Moreover,

0. the mapping γ defined by

$$B_l := \gamma(A_l) := q_0(a_0 \cdot A_l)B_0 + q_1(a_1 \cdot A_l)B_1 + q_2(a_2 \cdot A_l)B_2$$

is the point mapping of a collineation which associates to A_j , B_j for $j = 0$ to 3 .

1. the mapping γ' defined by

$$\gamma'(a_l) := u_0(A_0 \cdot a_l)b_0 + u_1(A_1 \cdot a_l)b_1 + u_2(A_2 \cdot a_l)b_2 \text{ is the corresponding line mapping.}$$

Proof: By hypothesis, $r_0 \neq 0$, because A_3 is not on $A_1 \times A_2$, similarly, r_1, r_2 , as well as s_0, s_1 and s_2 are $\neq 0$, therefore, q_0, q_1 and q_2 are well defined and $\neq 0$.

$$a_0 \cdot A_3 = (A_1 * A_2) \cdot (r_0 A_0 + r_1 A_1 + r_2 A_2) = r_0 \det(A_0, A_1, A_2),$$

$$\text{similarly, } a_i \cdot A_3 = r_i \det(A_0, A_1, A_2), b_i \cdot B_3 = r_i \det(B_0, B_1, B_2),$$

hence the alternate expression for q_i .

0. follows from 2.2.4 by observing that $(A_i * A_3) * a_i = r_{i+1} A_{i+1} - r_{i-1} A_{i-1}$.

The details are left as an exercise.

*If M and N are any 2 points on a_l and $a_l = M * N$,*

$$\begin{aligned} \gamma'(a_l) &= \gamma'(M * N) = \gamma(M) * \gamma(N) \\ &= q_1 q_2 (a_1 \cdot M a_2 \cdot N - a_2 \cdot M a_1 \cdot N) b_0 + \dots \\ &= q_1 q_2 ((a_1 * a_2) \cdot (M * N)) b_0 + \dots, \\ &= u_0 t (A_0 \cdot a_l) b_0 + \dots, \end{aligned}$$

because of 2.2.4. Dividing by t , we get 1.

Theorem.

If a collineation transforms each of the points of a complete quadrangle into itself, every point is transformed into itself.

Definition.

The collineation of 2.2.7 is called the identity collineation ϵ .

Comment.

Theorem 2.2.6 for 1 dimensional sets and Theorem 2.2.7 for 2 dimensional sets generalize by induction to n dimensions.

Example.

For $p = 5$, let $A_0 = (0) = (0, 0, 1)$, $A_1 = (1) = (0, 1, 0)$, $A_2 = (6) = (1, 0, 0)$ and $A_3 = (12) = (1, 1, 1)$,

let $B_0 = (1)$, $B_1 = (6)$, $B_2 = (12)$, $B_3 = (3) = (0, 1, 2)$, to obtain the point mapping γ which associates to A_j , B_j , $a_0 = [0, 0, -1]$, $a_1 = [0, -1, 0]$, $a_2 = [-1, 0, 0]$, $b_0 = [0, -1, 1]$, $b_1 = [-1, 0, 1]$, $b_2 = [0, 0, -1]$.

$q_0 = -1$, $q_1 = -2$, $q_2 = 2$, $u_0 = -4$, $u_1 = -2$, $u_2 = 2$, therefore

$$\gamma \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{pmatrix} -2 & 2 & 0 \\ -2 & 0 & 1 \\ -2 & 0 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} = \begin{bmatrix} -2X + 2Y \\ -2X + Z \\ -2X \end{bmatrix},$$

$$\gamma' \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 0 \\ -1 & -2 & -2 \end{pmatrix} \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{pmatrix} 2y \\ -z \\ -2x - 2y + z \end{pmatrix}.$$

Comment.

The following mapping can be used in certain cases but not in all cases:

$\phi(M) := q_0(M \cdot A)\phi(A) + q_1(M \cdot B)\phi(B) + q_2(M \cdot C)\phi(C)$, with

$q_0 = \frac{1}{A \cdot P}(\phi(B) * \phi(C))\phi(P)$, $q_1 = \frac{1}{B \cdot P}(\phi(C) * \phi(A))\phi(P)$,

$q_2 = \frac{1}{C \cdot P}(\phi(A) * \phi(B))\phi(P)$.

Indeed, one of the scalar product $A \cdot P$ or $B \cdot P$ or $C \cdot P$ can be 0, and cases exists for which whatever permutation of the 4 points A , B , C and P is used, the same difficulty occurs.

Theorem.

2.2.7 can be rewritten using matrix notation. Let \mathbf{a} be a matrix whose rows are the components of the sides of the triangle A_0 , A_1 , A_2 , $\mathbf{a}_{i,j} := \mathbf{a}_{j,i}$, etc.

Let \mathbf{Q} be the matrix $\mathbf{Q}_{i,i} := q_i$, $\mathbf{Q}_{i,j} := 0$ for $i \neq j$,

let $\mathbf{U}_{i,i} := q_{i+1}q_{i-1}$, $\mathbf{U}_{i,j} := 0$, $i \neq j$.

Let \mathbf{A}_l and \mathbf{B}_l be column vectors,

then $\mathbf{M} := \mathbf{B} \mathbf{Q} \mathbf{a}^T$ defines the collineation $\mathbf{B}_l = \mathbf{M} \mathbf{A}_l$ and $\mathbf{M}' := \mathbf{b} \mathbf{U} \mathbf{A}^T$ gives $\mathbf{b}_l = \mathbf{M}' \mathbf{a}_l$.

Moreover $\mathbf{M}' = \mathbf{M}^{-1}$ is the adjoint matrix.

Example.

Let $A_0 = (7)$, $A_1 = (15)$, $A_2 = (19)$, $A_3 = (28)$,

$B_0 = (27)$, $B_1 = (3)$, $B_2 = (10)$, $B_3 = (14)$.

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 1 & 0 \\ 1 & 2 & -1 \end{pmatrix}, \quad \mathbf{Q} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad \mathbf{a}^T = \begin{pmatrix} 0 & 1 & 1 \\ 2 & 2 & -2 \\ -1 & 2 & 1 \end{pmatrix},$$

$$\mathbf{M} = \mathbf{B} \mathbf{Q} \mathbf{a}^T = \begin{pmatrix} -2 & 2 & 0 \\ -2 & 0 & -1 \\ -2 & 0 & 0 \end{pmatrix},$$

$$\mathbf{b} = \begin{pmatrix} -1 & -1 & 2 \\ 2 & -2 & -2 \\ -1 & -1 & 1 \end{pmatrix}, \mathbf{U} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \mathbf{A}^T = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & -1 \\ 1 & 2 & -2 \end{pmatrix},$$

$$\mathbf{m} = \mathbf{b} \mathbf{U} \mathbf{A}^T = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ -2 & -2 & -1 \end{pmatrix},$$

Definition.

A collineation is called a central collineation if the collineation transforms every point of a given line into itself, and it is not the identity.

The line is called the axis of the central collineation.

Theorem.

Let a collineation be given by 2 complete quadrangles with 2 fixed points A_0 and B_0 and 2 other pairs A_2, B_2 and A_3, B_3 , the necessary and sufficient condition for this collineation to be a central collineation is that $A_2 \times A_3, B_2 \times B_3$ and $A_0 \times B_0$ have a point in common.

Theorem.

In a central collineation, if B_l corresponds to A_l and is distinct from A_l , then $A_l \times B_l$ passes through a fixed point F .

Definition.

F is called the center of the central collineation.

Definition.

A central collineation is a homology iff its center is not on its axis.

A central collineation is an elation iff its center is on its axis.

Comment.

Theorem 2.2.7 or 2.2.7 could serve as an alternate definition of collineation.

Exercise.

Characterize the matrix of a central collineation, and of an elation.

Notation.

When matrices are used to represent collineations correlations it is convenient to have a notation for the inverse matrix scaled by a convenient non zero factor, meaning that each entry is multiplied by that factor, N^I will be used.

2.2.8 Correlations, polarity.**Introduction.**

Correlations have been defined in 2.1.12. Their algebraic study follows directly from that of collineations. Their importance is due to their intimate relation with conics as will be seen in 2.2.9.

Definition.

The mapping which associates to the point (m) , the line $[m]$, for all $m = 0\text{top}^{2k} + p^k$ is called a basic duality. It will be denoted by δ .

Theorem.

The mapping δ is a correlation.

Theorem.

Given a point collineation γ and the corresponding line collineation γ' , then the mapping

$$\rho := \delta \circ \gamma$$

is a point correlation, and the corresponding line correlation is

$$\rho' := \delta \circ \gamma'.$$

In particular,

if $Q = \gamma(P)$ and $q = \gamma'(p)$, then $\rho(P) = \overline{Q}$ and $\rho'(p) = \overline{q}$.

Theorem.

Given a complete quadrangle A_j and a complete quadrilateral b_j , $j = 0, 1, 2, 3$,

Let $a_i := A_{i+1} * A_{i-1}$ and $B_i = b_{i+1} * b_{i-1}$,

$A_3 = r_0 A_0 + r_1 A_1 + r_2 A_2$, $b_3 = s_0 b_0 + s_1 b_1 + s_2 b_2$

$q_i := \frac{s_i}{r_i}$, $u_i := q_{i+1} q_{i-1}$,

then $q_i := \frac{B_i \cdot b_3}{a_i \cdot A_3}$.

Moreover, the correlation which associates to A_j , a_j , $j = 0$ to 3 , is given by

0. the point to line mapping

$$b_l := \rho(A_l) := q_0(a_0 \cdot A_l)b_0 + q_1(a_1 \cdot A_l)b_1 + q_2(a_2 \cdot A_l)b_2,$$

1. and the line to point mapping $\rho'(a_l) := u_0(A_0 \cdot a_l)B_0 + u_1(A_1 \cdot a_l)B_1 + u_2(A_2 \cdot a_l)B_2$.

The proof follows from 2.2.6 and from 2.2.8.

Example.

For $p = 5$, the correlation ρ defined by

$\rho(0) = [0]$, $\rho(1) = [1]$, $\rho(6) = [12]$, $\rho(12) = [19]$, $= (1, 2, 3)$, implies

$a_0 = [0, 0, 1]$, $a_1 = [0, 1, 0]$, $a_2 = [1, 0, 0]$ and

$\rho'(a_0) = (1, 0, -1)$, $\rho'(a_1) = (1, -1, 0)$, $\rho'(a_2) = (-1, 0, 0)$.

$q_0 = 2$, $q_1 = 1$, $q_2 = 1$, $u_0 = 1$, $u_1 = 2$, $u_2 = 2$, therefore

$\rho(X, Y, Z) = [-X, -X - Y, -X - 2Z]$, $\rho'[x, y, z] = (2x - 2y - z, 2y, z)$.

Theorem.

Using the notation of 2.2.6, 2.2.6, and 2.2.8 can be written in matrix notation.

Let $\mathbf{Q}_{i,i} := Q_i$ and $\mathbf{Q}_{i,j} := 0$ for $i \neq j$,

let $\mathbf{R}_{i,i} := q_{i+1}q_{i-1}$ and $\mathbf{R}_{i,j} := 0$ for $i \neq j$, then

$\mathbf{N} := \mathbf{b} \mathbf{R} \mathbf{a}^T$ defines a correlation $\mathbf{b}_l = \mathbf{N} \mathbf{A}_l$, and $\mathbf{N}' := \mathbf{B} \mathbf{V} \mathbf{A}^T$ determines $\mathbf{B}_l = \mathbf{N}' \mathbf{a}_l$.

Moreover $\mathbf{N}' = \mathbf{N}^{-1^T}$ is the adjoint matrix.

Definition.

A polarity is a correlation which satisfies

$$\rho' \circ \rho = \epsilon.$$

In this case $\rho(P)$ is called the polar of P and $\rho'(p)$ is called the pole of p .

Example.

The correlation which associates to $A = (0)$, $B = (1)$, $C = (6)$ and $P = (13)$ the lines $[11]$, $[7]$, $[2]$ and $[15]$, is a polarity and

$\rho(X, Y, Z) = [Y + Z, X + Z, X + Y]$, $\rho'[x, y, z] = (-x + y + z, x - y + z, x + y - z)$.

Theorem.

If \mathbf{M} is a matrix associated to a correlation, then this correlation is a polarity iff the matrix is symmetric, in other words iff $\mathbf{M} = \mathbf{M}^T$.

Comment.

Theorem 2.2.8 or 2.2.8 could serve as an alternate definition of correlations.

Definition.

A degenerate line correlation ρ_d corresponds to a function which associates to the set of points in the plane, lines which are obtained by multiplying the vector associated to the point to the left by the matrix

$$\mathbf{D} = \begin{pmatrix} 0 & -U_2 & U_1 \\ U_2 & 0 & -U_0 \\ -U_1 & U_0 & 0 \end{pmatrix}.$$

Theorem.

If U is the point (U_0, U_1, U_2) , then \mathbf{D} associates to the point $V = (V_0, V_1, V_2)$, the line $U \times V$. In the correlation, the image of all points are lines through the point U and therefore all lines have U as their image. The matrix corresponding to ρ'_d is therefore,

$$\begin{pmatrix} U_0 & U_0 & U_0 \\ U_1 & U_1 & U_1 \\ U_2 & U_2 & U_2 \end{pmatrix}.$$

Exercise.

Prove (Seidenberg, p.193-196)

0. *that a linear transformation is the product of 2 polarities.*
1. *that the set of fixed point and fixed lines of a linear transformation form a self dual configuration.*

2.2.9 Conics.**Introduction.**

The following definition was first given by von Staudt. The connection between polarity and conics was anticipated already by Apollonius and clearly understood by La Hire.

Definition.

Given a polarity ρ with inverse ρ' , a conic is the set of points P such that

$$P \cdot \rho(P) = 0.$$

and the set of lines p such that

$$p \cdot \rho'(p) = 0.$$

In other words it is the set of points which are on their polar and the set of lines which are on their pole.

If the polarity corresponds to a symmetric matrix

$$\begin{pmatrix} a_0 & b_2 & b_1 \\ b_2 & a_1 & b_0 \\ b_1 & b_0 & a_2 \end{pmatrix},$$

the equation of the corresponding point conic is

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + 2(b_0X_1X_2 + b_1X_2X_0 + b_2X_0X_1) = 0.$$

Theorem.

0. *5 points no 3 of which are collinear determine a conic.*

1. the conic through A, B, C, D and E is given by

$$k_1[A \times B] \times [C \times D] = k_2[A \times D] \times [B \times C],$$

with

$$k_1 = [A \times D] \cdot E \cdot [B \times C] \cdot E, \quad k_2 = [A \times B] \cdot E \cdot [C \times D] \cdot E.$$

Example.

Given the data of 2.2.2, the conic through A, B, C, D and E is

$$2X_0^2 - X_1^2 - 4X_2^2 + 5X_1X_2 - 4X_2X_0 = 0.$$

Exercise.

Prove that a conic has $p + 1$ points in a finite projective plane associate with p .

If we join one point P to the p others we obtain p lines through P therefore the left over line is the tangent at P .

Comment.

For $p = 3$, the conic has 4 points, hence it cannot be constructed by giving 5 points, but it can be constructed if we give 4 points and a tangent at one of these points or 3 points and the tangents at 2 of these points. See 2.1.6.

For $p = 2$, a conic can be constructed using 3 non collinear points and the tangents at 2 of these points.

Theorem.

The pole of $[1, 1, 1]$ with respect to the conic

$$b_0X_1X_2 + b_1X_2X_0 + b_2X_0X_1 + (X_0 + X_1 + X_2)(u_0X_0 + u_1X_1 + u_2X_2) = 0,$$

is

$$(b_0(-b_0 + b_1 + b_2) + 2u_0b_0 - u_1(b_0 + b_1 - b_2) - u_2(b_0 - b_1 + b_2), \dots, \dots).$$

Theorem.

The pole of $[1, 1, 1]$ with respect to the conic

$$c_0X_1X_2 + c_1X_2X_0 + c_2X_0X_1 + u_0X_0^2 + u_1X_1^2 + u_2X_2^2 = 0,$$

is

$$(c_0(-c_0 + c_1 + c_2) - 2u_1c_1 - 2u_2c_2 + 4u_1u_2, \dots, \dots).$$

Example.

For $p = 13$, if $b_0 = 1, b_1 = 6, b_2 = 2, u_0 = -5, u_1 = 4, u_2 = 2$,

then $c_0 = -4, c_1 = 2, c_2 = 5$, and the pole of $[1, 1, 1]$ is $(1, 6, 3) = (95)$.

Theorem.

Given the conic

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + b_0X_1X_2 + b_1X_2X_0 + b_2X_0X_1 = 0.$$

and a point (P_0, P_1, P_2) , with $P_2 \neq 0$, on the conic, all the points are given by

$$\begin{aligned} X_0 &= a_1P_0u^2 - (2a_1P_1 + b_0P_2)uv - (a_0P_0 + b_2P_1 + b_1P_2)v^2, \\ X_1 &= -(b_2P_0 + a_1P_1 + b_0P_2)u^2 - (2a_0P_0 + b_1P_2)uv + a_1P_0v^2, \\ X_2 &= a_1P_2u^2 + b_2P_2uv + a_0P_2v^2, \end{aligned}$$

using the $p+1$ values of the homogeneous pair (u, v) .

Proof: The points $(v, u, 0)$ on $[0, 0, 1]$ joined to P is the line

$$l = [-P_2u, P_2v, P_0u - P_1v].$$

X is on l iff $P_2X_1v = P_2X_0u - P_0X_2u + P_1X_2v$, substituting in the equation of the conic, if A is the coefficient of X_0^2 and B that of X_2^2 , using the property of the products of the roots of the equations gives $P_2X_2 = A$, $P_0X_0 = B$, this gives X_0 and X_2 , substituting in l gives X_1 .

Theorem. [Chasles]

Given the configuration of Desargues 2.1.5 there exists a conic such that A_i is the pole of $b_i := B_{i+1} \times B_{i-1}$ and vice-versa.

Clearly B_i is also the pole of $a_i := A_{i+1} \times A_{i-1}$.

Proof: Let $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$, $C = (1, 1, 1)$, $c = (c_0, c_1, c_2)$ and $B_0 = (b, 1, 1)$. We have

$C_0 = (0, c_2, -c_1)$, $C_1 = (-c_2, 0, c_0)$, $C_2 = (c_1, -c_0, 0)$, $b_1 = [c_0, c_1, -bc_0 - c_1]$, $b_2 = [c_0, -bc_0 - c_2, c_2]$, $B_1 = (c_1, (b-1)c_0 + c_1, c_1)$, $B_2 = (c_2, c_2, (b-1)c_0 + c_2)$. The transformation which associates to a_i , $k_i B_i$, with

$k_0 := c_1c_2$, $k_1 := c_2$, $k_2 := c_1$ is

$$\begin{pmatrix} bc_1c_2 & c_1c_2 & c_1c_2 \\ c_1c_2 & ((b-1)c_0 + c_1)c_2 & c_1c_2 \\ c_1c_2 & c_1c_2 & ((b-1)c_0 + c_2)c_1 \end{pmatrix},$$

is a line to point polarity because the representative matrix is symmetric. Its inverse can easily be obtained by determining b_0 . This is left as an exercise.

Notation.

If $u = [u_0, u_1, u_2]$ and $v = [v_0, v_1, v_2]$ are 2 lines, then
 $u \rtimes v = (u_0X_0 + u_1X_1 + u_2X_2)(v_0X_0 + v_1X_1 + v_2X_2)$.

Definition.

Given 2 conics α and β if there exist integers k and l and lines u and v such that

$$k\alpha + l\beta = u \rtimes v,$$

then v is called the radical axis with respect to u of α and β .

Lemma.

If \mathbf{N} is a symmetric matrix and \mathbf{A} and \mathbf{B} are 2 vectors, then $\mathbf{A} \cdot (\mathbf{N} \mathbf{B}) = \mathbf{B} \cdot (\mathbf{N} \mathbf{A})$.

Theorem.

A conic or the corresponding polarity determines an involution on every line, by associating to each point its conjugate on that line. Moreover if A_0 and B_0 are conjugates as well as A_1 and B_1 , if $A_l = t_0 A_0 + t_1 A_1$ its conjugate B_l is given by $B_l = ((A_1.B_0)t_0 + (A_1.B_1)t_1)A_0 - ((A_0.B_0)t_0 + (A_0.B_1)t_1)A_1$.

*This property follows from the notion of conjugates and from $B_l = (A_1 * A_0) * (t_0 N A_0 + t_1 N A_1)$, with $B_0 = N A_0$ and $B_1 = N A_1$. The Lemma confirms the involutive property.*

Example.

For $p = 5$, starting with $A(0) = (6)$, $A(1) = 1$, $A(2) = 0$, $A(3) = 12$, the quadrangle-quadrilateral configuration is

$a_{1,2} = [6]$, $a_{2,0} = [1]$, $a_{0,1} = [0]$, $a_{0,3} = [5]$, $a_{1,3} = [10]$, $a_{2,3} = [26]$, $D_0 = (2)$, $D_1 = (7)$, $D_2 = (11)$, $d_0 = [30]$, $d_1 = [27]$, $d_2 = [15]$, $A_{0,3} = (5)$, $A_{1,3} = (10)$, $A_{2,3} = (26)$, $A_{1,2} = (24)$, $A_{2,0} = (17)$, $A_{0,1} = (13)$, $a_0 = [24]$, $a_1 = [17]$, $a_2 = [13]$, $a_3 = [12]$.

Example.

The points and lines of the extended quadrangle-quadrilateral configuration are those of 2.2.9 and $B_{1,0} = (9)$, $B_{2,1} = (16)$, $B_{0,2} = (3)$, $B_{2,0} = (21)$, $B_{0,1} = (4)$, $B_{1,2} = (8)$, $B_{0,3} = (15)$, $B_{1,3} = (27)$, $B_{2,3} = (30)$, $B_{3,0} = (18)$, $B_{3,1} = (22)$, $B_{3,2} = (14)$, $b_{1,0} = [4]$, $b_{2,1} = [8]$, $b_{0,2} = [21]$, $b_{2,0} = [3]$, $b_{0,1} = [9]$, $b_{1,2} = [16]$, $b_{0,3} = [2]$, $b_{1,3} = [7]$, $b_{2,3} = [11]$, $b_{3,0} = [18]$, $b_{3,1} = [22]$, $b_{3,2} = [14]$.

Example.

The conical points and lines of the extended quadrangle-quadrilateral configuration are the 6 points and 6 lines $C_{1,0} = (20)$, $C_{2,1} = (29)$, $C_{0,2} = (19)$, $C_{2,0} = (28)$, $C_{0,1} = (23)$, $C_{1,2} = (25)$, $c_{1,0} = [20]$, $c_{2,1} = [29]$, $c_{0,2} = [19]$, $c_{2,0} = [28]$, $c_{0,1} = [23]$, $c_{1,2} = [25]$.

Definition.

A degenerate conic is a set of points and lines represented by an equation corresponding to a singular 3 by 3 symmetric matrix.

Exercise.

Describe all the types of degenerate conics.

Exercise.

*The number of conics, degenerate or not is $(q^2 + q + 1)(q^3 + 1)$,
The number of degenerate conics are*

$\text{line} \times \text{line} \quad q^2 + q + 1,$
 $\text{line}_1 \times \text{line}_2 \quad \frac{1}{2}(q^2 + q + 1)q(q + 1)$
 $\text{non real line} \times \text{its conjugate} \quad \frac{1}{2}(q^2 + q + 1)q(q - 1),$
 The number of non degenerate conics is $q^5 - q^2$.

Table.

q	2	3	4	5	7	11
$\text{line} \times \text{line}$	7	13	21	31	57	133
$\text{non real line} \times \text{its conjugate}$	7	39	126	310	1197	7315
$\text{line}_1 \times \text{line}_2$	21	78	210	465	1596	8778
$\text{non degenerate conics}$	28	234	1008	3100	16758	160930
all conics	63	364	1365	3906	19608	177156

2.2.10 The general conic.

Introduction.

There is a more general connection between correlations and conics, which leads to the concept of a general conic, which is one of 4 types, the points of a conic of von Staudt and the lines of an other conic of von Staudt. It has $p + 1$ points and $p + 1$ lines; a degenerate conic consisting of $2p + 1$ points on 2 distinct lines and $2p + 1$ lines through 2 distinct points; a degenerate conic consisting of $p + 1$ points on 1 line and of $p + 1$ lines through 1 point; and finally the degenerate conic consisting of 1 point and 1 line. In the last case, in complex projective geometry, all the complex points are on a pair of complex conjugate lines and all the complex lines are through a pair of complex conjugate points. To every correlation is associated a general point conic and a general line conic.

Definition.

A general conic consists of a point conic which is the set of points in a correlation which are on their image and of a line conic which is the set of lines in a correlation which are on their image.

Theorem.

If \mathbf{N} is the matrix associated to a correlation, the equation of the point conic is

$$\mathbf{X}^T \mathbf{N} \mathbf{X} = 0, \text{ where } \mathbf{X} \text{ is the vector } (X_0, X_1, X_2).$$

The equation of the line conic is

$$\mathbf{x}^T \mathbf{N}^{-1} \mathbf{x} = 0, \text{ where } \mathbf{x} \text{ is the vector } (x_0, x_1, x_2).$$

Theorem.

Let \mathbf{A} be the most general antisymmetric matrix,

$$\mathbf{A} = \begin{pmatrix} 0 & -w & v \\ w & 0 & -u \\ -v & u & 0 \end{pmatrix},$$

all the correlations associated to $\mathbf{N} + \mathbf{A}$ define the same point conic.

Definition.

Given a matrix \mathbf{N} , its symmetric part \mathbf{N}^S is defined by

$$\mathbf{N}^S := \frac{\mathbf{N} + \mathbf{N}^T}{2},$$

and its antisymmetric part \mathbf{N}^A by

$$\mathbf{N}^A := \frac{\mathbf{N} - \mathbf{N}^T}{2}.$$

Theorem.

Given a correlation ρ, ρ' .

If T is on the point conic, then $\rho(T)$ is on the line conic.

If t is on the line conic, then $\rho'(t)$ is on the point conic.

The general conic degenerates if $\det(\mathbf{N}) = 0$.

The center corresponds to the vector which is the homogeneous solution of $\mathbf{N}^S \mathbf{C} = 0$, and the central line, to that of $(\mathbf{N}^S)^{-1} \mathbf{c} = 0$.

Definition.

Given a general conic, the tangent t at the point T of the point conic is defined by $t := \mathbf{N}^S T$.

The contact T of a line t which belongs to a line conic is defined by $T := (\mathbf{N}^S)^{-1} t$.

Theorem.

If the correlation is a polarity then the tangent at a point T of a point conic is on the corresponding line conic. Similarly, the contact of a line t of line conic is on the corresponding point conic.

Theorem.

If a conic is non degenerate, the necessary and sufficient condition for the set of tangents to a point conic to coincide with the set of lines on the line conic is that the correlation be a polarity.

Proof: Let \mathbf{N} be the matrix associated to the correlation. The line conic is $\mathbf{x}^T \mathbf{N}^{-1} \mathbf{x} = 0$.

The tangents $\mathbf{t} = \mathbf{N}^S \mathbf{X}$ to the point conic are on

$$\mathbf{t}^T (\mathbf{N}^S)^{-1} \mathbf{N} (\mathbf{N}^S)^{-1} \mathbf{t} = 0.$$

If ρ is a polarity, $\mathbf{N} = \mathbf{N}^S$ and $\mathbf{N}^{-1} = \mathbf{N}^{S^{-1}} \mathbf{N} (\mathbf{N}^S)^{-1}$. Vice-versa,

if $\mathbf{N}^{-1} = (\mathbf{N}^S)^{-1} \mathbf{N} (\mathbf{N}^S)^{-1}$ then $\mathbf{N}^S = \mathbf{N} (\mathbf{N}^S)^{-1} \mathbf{N}$.

Therefore, using $\mathbf{N} = \mathbf{N}^S + \mathbf{N}^A$, $2\mathbf{N}^A = -\mathbf{N}^A (\mathbf{N}^S)^{-1} \mathbf{N}^A$,

transposing, $-2\mathbf{N}^A = -\mathbf{N}^A(\mathbf{N}^S)^{-1}\mathbf{N}^A$, because $\mathbf{N}^{A^T} = -\mathbf{N}^A$, therefore $\mathbf{N}^A = 0$, \mathbf{N} is symmetric and therefore ρ is a polarity.

2.2.11 The Theorem of Pascal and Brianchon.

Introduction.

A fundamental theorem associated to conics was discovered by Blaise Pascal. It allows construction of any point on a conic given by 5 points and in particular the other intersection of a line through one point of a conic. See I,

There is a general principle of linear construction that if a point or line is uniquely define, that point or line can be obtained by a linear construction. The points of intersection of a conic with a general line are not uniquely defined and therefore do not admit a linear construction on the other hand if the line passes to a known point of the conic, the other intersection of the line and the conic is uniquely defined. The Pascal construction of 2.2.11 is a solution to this problem which follows from the following Theorem.

Theorem [Pascal].

If 6 points $A_0, A_1, A_2, A_3, A_4, A_5$ are on a conic and the Pascal points are defined as

$$P_0 := (A_0 \times A_1) \times (A_3 \times A_4),$$

$$P_1 := (A_1 \times A_2) \times (A_4 \times A_5),$$

$$P_2 := (A_2 \times A_3) \times (A_5 \times A_0),$$

then the points P_0, P_1, P_2 are collinear (Pascal, 1639, Lemma 1 and 3).

There are “degenerate” forms of this theorem in which 2 consecutive points coincide and the cord is replaced by the tangent at these points for instance if the tangent at A_0 is t_0 , the Pascal points are

$$P_0 := t_0 \times (A_3 \times A_4),$$

$$P_1 := (A_0 \times A_2) \times (A_4 \times A_5),$$

$$P_2 := (A_2 \times A_3) \times (A_5 \times A_0),$$

and the points P_0, P_1, P_2 are collinear.

Proof: The Theorem of Pascal will now be proven in the 4 cases, 6 points, 5 points and the tangents at one of them, 4 points and the tangents at 2 of them and finally 3 points and their tangents. In each case, the coordinates will be chosen to simplify the algebra. See also 2.2.2.

0. Let the 6 points of the conic be $A_0, C_0, A_1, B_1, A_2, B_2$. Choose the coordinates such that $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$ and $A_2 = (0, 0, 1)$, choose the barycenter $M = (1, 1, 1)$ at the intersection of $A_1 \times B_1$ and $A_2 \times B_2$, let the line $A_0 \times B_0$ be $[0, r, -s]$.

Because the conic passes through A_i , it has an equation of the form

$$0. uX_1X_2 + vX_2X_0 + wX_0X_1 = 0.$$

$$A_1 \times B_1 = A_1 \times M = [1, 0, -1], A_2 \times B_2 = A_2 \times M = [1, -1, 0], \text{ therefore,}$$

$$B_1 = (u + w, -v, u + w), B_2 = (u + v, u + v, -w),$$

$$C_0 = (-urs, s(vr + ws), r(vr + ws)),$$

hence the Pascal points are

$$P_0 = (A_0 \times C_0) \times (B_1 \times A_2) = (s(u + w), -vs, -vr),$$

$$P_1 = (C_0 \times A_1) \times (A_2 \times B_2) = (urs, urs, -r(vr + ws)),$$

$$P_2 = (A_1 \times B_1) \times (B_2 \times A_0) = (w, -(u + v), w).$$

which are all on $[v(ru + rv + sw), w(su + rv + sw), su(u + v + w)]$.

1. Let the 5 points of the conic be A_0, A_1, B_1, A_2, B_2 , and let the tangent t be chosen at A_0 .

With the coordinates chosen as above and the conic again of the form 0.0, the tangent is $[0, w, v]$ and the Pascal points are

$$P_0 = t \times (B_1 \times A_2) = (u + w, -v, w),$$

$$P_1 = (A_0 \times A_1) \times (A_2 \times B_2) = (1, 1, 0),$$

$$P_2 = (A_1 \times B_1) \times (B_2 \times A_0) = (w, -(u + v), w).$$

which all are on $[-w, w, u + v + w]$.

2. Let the 4 points be A_0, A_1, A_2 and B_0 and the tangents be t_1 at A_1 and t_2 at A_2 . Choose the coordinates as above, except for M on $A_0 \times B_0 = [0, 1, -1]$, then $r = s = 1$.

$$B_0 = (-u, v + w, v + w),$$

the tangents are $t_1 = [w, 0, u]$ and $t_2 = [v, u, 0]$.

The Pascal points are

$$P_0 = (A_0 \times A_1) \times t_2 = (-u, v, 0),$$

$$P_1 = (A_1 \times A_2) \times (A_0 \times B_0) = (0, 1, 1),$$

$$P_2 = t_1 \times (A_2 \times B_0) = (-u, v + w, w),$$

which all are on $[v, u, -u]$.

3. Let the points be A_0, A_1 and A_2 and the tangents be those at these points, using again 0.0. as the equation of the conic, the tangents are

$$t_0 = [0, w, v], t_1 = [w, 0, u], t_2 = [v, u, 0].$$

the Pascal points are

$$P_0 = t_0 \times (A_1 \times A_2) = (0, v, -w),$$

$$P_1 = t_1 \times (A_2 \times A_0) = (-u, 0, w),$$

$$P_2 = t_2 \times (A_0 \times A_1) = (u, -v, 0),$$

which are all on $[vw, wu, uv]$.

4. The other cases, 4 tangents and 2 points of contact, 5 tangents and 1 point of contact, 6 tangents, can be proven by duality.

Theorem [Pascal].

The reciprocal of the preceding Theorem is true. In other words, if the Pascal points P_i are collinear, the 6 points A_k are on a conic.

The proof is left as an exercise.

Notation.

The property that 6 points are on a conic γ will be noted

$$\text{incidenceconic}(A, B, C, D, E, F[, \gamma]) \text{ or } \text{incidenceconic}(A_k[, \gamma]).$$

Similar notation will be used for degenerate or for dual forms, for instance

$$\text{incidenceconic}(A, t, B, C, D, E), \text{ where } t \text{ is the tangent at } A.$$

incidenceconic(a, b, c, d, e, f) where a, b, c, d, e, f are 6 tangents to the conic.

Theorem 2.2.11 will be denoted as follows.

No. $Pascal(A_k[, a_k]; \langle P_i[, p] \rangle)$

Hy. $incidenceconic(A_k)$.

De. $P_i := (A_i \times A_{i+1}) \times (A_{i+3} \times A_{i+4})$

Co. $\langle P_i, p \rangle$.

If t_k is the tangent at A_k , A_k is followed by t_k .

The Pascal line associated to the points A_k will be denoted by $p := Pascal(A_k)$.

Definition.

The dual of the Theorem of Pascal is called the Theorem of Brianchon. Brianchon discovered the Theorem before Gergonne discovered the important principle of duality.

In the degenerate case of a triangle inscribed in a conic and of the triangle outscribed to the conic at these points (2.2.11.3), the line is called the Pascal line of the triangle and the point of the dual Theorem, the Brianchon point of the triangle. von Staudt (1863) calls them, pole and polar of the triangle.

Theorem. [Generalization of von Staudt]

If p is the Pascal line of the hexagon $A_0, A_1, A_2, A_3, A_4, A_5$ inscribed in a conic γ and P is the Brianchon point of the outscribed hexagon formed by the tangents at A_j , then P is the pole of p .

The proof follows at once from the properties of poles and polars.

Corollary. [von Staudt]

If $\{A_0, A_1, A_2\}$ is a triangle inscribed in a conic, then its Pascal line is the polar of its Brianchon point.

Theorem. [von Staudt]

If 2 triangles $\{A_0, A_1, A_2\}$ and $\{B_0, B_1, B_2\}$ are inscribed in a conic γ and are perspective with center C and axis c , and P, Q are their Brianchon points and p and q are their Pascal lines, then $\langle P, Q, C; pq \rangle$ and $\langle p, q, c; PQ \rangle$, moreover, $quatern(P, Q, C, pq \times c)$ and $quatern(p, q, c, PQ \times C)$.

Notation.

$$(A_{i,j,k}) := det(A_i, A_j, A_k).$$

Theorem.

If 6 points $A_k, k = 0$ to 5, are on a conic then

$$(A_{k+2,k+3,k+1})(A_{k+3,k+4,k})(A_{k+4,k+5,k+1})(A_{k+5,k,k+2}) \\ - (A_{k+2,k+3,k})(A_{k+3,k+4,k+1})(A_{k+4,k+5,k+1})(A_{k+5,k,k+2})$$

$$\begin{aligned}
& + (A_{k+3,k+4,k+1})(A_{k+4,k+5,k+2})(A_{k+5,k,k+2})(A_{k,k+1,k+3}) \\
& - (A_{k+3,k+4,k+1})(A_{k+4,k+5,k+2})(A_{k+5,k,k+3})(A_{k,k+1,k+2}) = 0.
\end{aligned}$$

The addition for the subscript is done modulo 6.

Proof: The Theorem will be proven for $k = 0$. Let $a_k := A_k \times A_{k+1}$. The Pascal points are $P_k := a_k \times a_{k+3}$, we have

$$(P_{0,1,2}) := \det(P_0, P_1, P_2) = (P_0 * P_1) \cdot P_2 = 0,$$

but

$$\begin{aligned}
P_0 &= (A_0 * A_1) * (A_3 * A_4) = \det(A_0, A_3, A_4)A_1 - \det(A_1, A_3, A_4)A_0, \\
&= (A_{0,3,4})A_1 - (A_{1,3,4})A_0,
\end{aligned}$$

similarly,

$$\begin{aligned}
P_1 &= (A_{1,4,5})A_2 - (A_{2,4,5})A_1, \\
P_2 &= (A_{2,5,0})A_3 - (A_{3,5,0})A_2 = (A_{0,2,5})A_3 - (A_{0,3,5})A_2,
\end{aligned}$$

therefore

$$\begin{aligned}
\det(P_0, P_1, P_2) &= (A_{0,3,4})(A_{1,4,5})(A_{0,2,5})(A_{1,2,3}) - (A_{1,3,4})(A_{1,4,5})(A_{0,2,5})(A_{0,2,3}) \\
&+ (A_{1,3,4})(A_{2,4,5})(A_{0,2,5})(A_{0,1,3}) - (A_{1,3,4})(A_{2,4,5})(A_{0,3,5})(A_{0,1,2}) = 0. \square
\end{aligned}$$

Construction.

$$\text{point Pascal}(A_0, A_1, A_2, A_3, A_4, A'_5; [P_0, P_1, P_2,]A_5)$$

is used as an abbreviation for the Pascal construction

$$\begin{aligned}
P_0 &:= (A_0 \times A_1) \times (A_3 \times A_4), \\
P_1 &:= (A_1 \times A_2) \times (A_4 \times A'_5), \\
P_2 &:= (A_2 \times A_3) \times (P_0 \times P_1), \\
A_5 &:= (A_4 \times A'_5) \times (P_2 \times A_0).
\end{aligned}$$

It gives the point A_5 on the conic through A_0 to A_5 on the line $A_4 \times A'_5$.

line

$$\text{Pascal}(a_0, a_1, a_2, a_3, a_4, a'_5; [p_0, p_1, p_2,]a_5)$$

is used for the dual construction.

Theorem.

When $p = 2$, the points and lines of a conic2 configuration 2.1.6 are the points and lines of a conic.

Proof: The Pascal points are the diagonal points of the complete quadrangle configuration which are collinear because of Theorem 2.1.13.

Theorem.

Let $p = 3$, in a quadrangle quadrilateral configuration, Q_i, P, q_i, p (2.1.6), there is a conic whose tangent at P is p and at Q_i is p_i .

In other words the elements of a conic3 configuration (2.1.6 are the points and lines of a conic.

Proof: From 2.1.6, Q_i is on q_i , the Pascal-Brianchon theorem gives $\text{Pascal}(P, p, Q_{i+1}, q_{i+1}, Q_{i-1}, q_{i-1}; \langle R_0, P_{i-1}, P_{i+1}, p \rangle)$.

Theorem.

The conical points of Definition 2.1.7 are on a conic and the conical lines are on a conic.

Proof: *Pascal*($AF_0, FA_2, AF_0, FA_2, AF_0, FA_2; \langle R_1, R_2, R_3, p \rangle$).

Theorem.

The following points of the extended Pappus configuration are on a conic, 1 point on each of the lines d, \bar{d} , say M_0 and \bar{M}_0 and the intersection with the lines joining the other points say a_1 and a_2 with the lines joining M_0 or \bar{M}_0 with the other points on d or \bar{d} .

This gives the 18 conics

0. $M_i, \bar{N}_{i+1}, N_{i+1}, \bar{M}_i, \bar{N}_{i-1}, N_{i-1},$
1. $M_i, \bar{P}_{i-1}, P_{i-1}, \bar{M}_i, \bar{P}_{i+1}, P_{i+1},$
2. $M_{i+1}, \bar{N}_{i+1}, L_{i-1}, \bar{M}_{i-1}, \bar{N}_{i-1}, L_{i-1},$
3. $M_{i+1}, Q_{i-1}, \bar{P}_{i-1}, \bar{M}_{i-1}, Q_{i+1}, \bar{P}_{i-1},$
4. $M_{i-1}, Q_{i+1}, P_{i+1}, \bar{M}_{i+1}, Q_{i-1}, P_{i-1},$
5. $M_{i-1}, L_{i+1}, \bar{N}_{i+1}, \bar{M}_{i+1}, L_{i-1}, \bar{N}_{i-1}.$

Proof: This follows from Pascal's Theorem applied to the points in the given order, order which was chosen in such a way that the Pascal line was always \bar{m}_0 , containing P_0, \bar{P}_0, Q_0 and \bar{D} . Exchanging N_{i+1} and \bar{N}_{i-1} for 0. gives an other Pascal line m_0 . The 9 Pappus lines are therefore the Pascal lines of the 18 conics.

Theorem.

The conics 0. and 1. have the same tangent at their common point.

Proof: The coefficients of conic 0. are, for $i = 0$, $a_0 = m_0 m_1 m_2$,
 $a_1 = m_1^2 m_2$, $a_2 = m_2^2 m_1$, $b_0 = m_1 m_2 (m_1 + m_2)$, $b_1 = m_2 (m_1^2 + m_2 m_0)$,
 $b_2 = m_1 (m_2^2 + m_0 m_1)$,

This follows easily because M_0, \bar{M}_0 are on a_0 , giving a_1, a_2 and b_0 , N_1, \bar{N}_1 are on a_1 , this gives a_0 and b_1 , N_2, \bar{N}_2 are on a_2 , giving b_2 . The coefficients of conic 1, for $i = 0$ are the same except for $a_0 = m_0 (m_1^2 - m_1 m_2 + m_2^2)$. The algebra is simplified by noting that the equation for P_1 and \bar{P}_1 , gives after subtraction b_1 from a_2 and b_0 , and for P_2 and \bar{P}_2 , gives after subtraction b_2 from a_1 and b_0 .

The Theorem follows at once. The tangent at M_0 is
 $[m_0 (m_1 + m_2 - m_1 m_2, m_1 m_2, m_1 m_2)]$ and at \bar{M}_0 is $[m_1 + m_2 - m_0, m_1, m_2]$.

Exercise.

Study the configuration of all 18 conics associated to the extended Pappus configuration.

2.2.12 The Theorems of Steiner, Kirkman, Cayley and Salmon.

Introduction.

The set of Theorems given here originates with the work of Steiner (1828, 1832 - Werke I, p.451). Proofs have been given using Pascal's Theorem and Desargues Theorem in the plane or starting with properties of the configuration

*5 * 3 & 5 * 3 in three (Cremona, 1877) or four (Richmond, 1894, 1899, 1900, 1903) dimensions, subjected to a linear condition. An alternate approach starts with the work of Sylvester 1844 (Papers, I, p.92), 1862 (II, p.265.) For a good summary, see Salmon, 1879, p. 379-383, Baker, II, (2d Ed. 1930), p. 219-236 and Friedrich Levi, 1929, p.192-199..*

The cyclic permutation notation allows the results to be given in a simple algebraic way and suggests the related synthetic construction.

Definition.

*Given 6 points A_j , $j = 0$ to 5 , on a conic, a conical hexagon abbreviated here by hexagon is a permutation h of 0 to 5 . Given h this defines a specific Pascal line $p(h) := \text{Pascal}(A_{h(0)}, A_{h(1)}, A_{h(2)}, A_{h(3)}, A_{h(4)}, A_{h(5)})$,
A map will denote here a permutation which acts on h .*

Example.

Let $h = [013524] = \begin{pmatrix} 012345 \\ 013524 \end{pmatrix} = (2354)$. The ordered set of point associated to h is $A_0A_1A_3A_5A_2A_4$. The map $\sigma = (135)$ associates to this set, the set $(2354)(135) = (15)(234) = [053421] = h'$ or $A_0A_5A_3A_4A_2A_1$, for instance, $h'(2) = h\sigma(2) = h(2) = 3$, $h'(3) = h\sigma(3) = h(5) = 4$. The multiplication of permutations is done from right to left.

Definition.

0. The Steiner map is $\sigma = (135)$,
1. the Steiner conjugate map is $\gamma = (35)$.
2. the Kirkman map is $\kappa = (021)(345)$,
3. the Cayley-Salmon map is $\chi = (14)$,
4. the Salmon map is $\lambda = (2354)$.
5. the line-Steiner maps are $\sigma_0 = (23)$ and $\sigma_1 = (45)$.

Theorem.

*Given $r = (012345)$ and $s = (05)(14)23$,
 $h = (\dots ij \dots)$, $r^{-1}hr = r^{-1}(r \dots i-1, j-1 \dots)$ and $s^{-1}hs = (\dots s(i), s(j) \dots)$ have the same Pascal line.*

The permutations $r^{-k}hr^k$ and $s^{-1}hs$ are called Pascal equivalent.

Theorem.

0. $(024), (042), (153)$ are Pascal equivalent to the Steiner map (135) .
1. $(02), (04), (13), (15), (24)$ are Pascal equivalent to the Steiner conjugate map (35) .
2. $(012)(354), (015)(243), (045)(132), (051)(234), (054)(123)$ are Pascal equivalent to the Kirkman map $(021)(345)$.
3. $(03), (25)$ are Pascal equivalent to the Cayley-Salmon map (14) .
4. $(0132), (0215), (0451), (0534), (1243)$ are Pascal equivalent to the Salmon map (2354) .
5. $(024), (042), (153)$ are Pascal equivalent to the line-Steiner maps (23) and (45) .

Theorem. [Steiner (Pascal)]

0. $\langle p(h), p(h\sigma), p(h\sigma^2); S(h) \rangle, S(h)$ is called the Steiner point of h .
1. $S(h\gamma)$, called the Steiner conjugate point of h , is on the polar of $S(h)$ with respect to the conic.
2. there are 10 pairs of conjugate Steiner points.

See 2.1.9.

Proof: Let $h = [012345] = ()$. I will use here the abbreviations

ij for the line $A_i \times A_j$,

$ijkl$ for the Pascal point $(A_i \times A_j \times (A_k \times A_l))$.

$p(h) = P_0 \times P'_0$, with $P_0 = 0134, P'_0 = 0523$,

$p(h\kappa) = P_1 \times P'_1$, with $P_1 = 0125, P'_1 = 1423$,

$p(h\kappa^2) = P_2 \times P'_2$, with $P_2 = 2534, P'_2 = 0514$,

Let $Q_0 := (P_1 \times P_2) \times (P'_1 \times P'_2) = 2514$,

$Q_1 := (P_2 \times P_0) \times (P'_2 \times P'_0) = 3450$,

$Q_2 := (P_0 \times P_1) \times (P'_0 \times P'_1) = 0123$,

Pascal($A_1A_4A_3A_2A_5A_0; \langle Q_0, Q_1, Q_2 \rangle$), therefore

$Desargues^{-1}(\{P_0, P_1, P_2\}, \{P'_0, P'_1, P'_2\}; \langle Q_0, Q_1, Q_2 \rangle, S(h))$,

or

$Desargues^{-1}(\{2435, 0312, 0514\}, \{p34125, p25135, p35124\} \{p13245 \times p12354, 1245, 0523\}, \{p12345, p13245, p12354\}; \langle S(e), S(\sigma), S(\sigma^2) \rangle, s(e))$,

Theorem. [Kirkman 1849, 1850]

0. $\langle p(h), p(h\kappa), p(h\kappa^2); K(h) \rangle, K(h)$ is called the Kirkman point of h .
1. there are 60 Kirkman points which are 3 by 3 on the 60 Pascal lines, giving a configuration of type $60 * 3 \ \& \ 60 * 3^6$.

⁶Levi, p. 194

Proof: Let $h = [012345] = ()$. The proof, for $i = 0$ is as follows.
 $p(h) = P_0 \times P'_0$, with $P_0 = 0134$, $P'_0 = 0523$,
 $p(h\kappa) = P_1 \times P'_1$, with $P_1 = 0134$, $P'_1 = 1245$,
 $p(h\kappa^2) = P_2 \times P'_2$, with $P_2 = 2534$, $P'_2 = 0312$,
Let $Q_0 := (P_1 \times P_2) \times (P'_1 \times P'_2) = 0325$,
 $Q_1 := (P_2 \times P_0) \times (P'_2 \times P'_0) = 0145$,
 $Q_2 := (P_0 \times P_1) \times (P'_0 \times P'_1) = 1234$,
Pascal($A_2A_5A_4A_3A_0A_1; \langle Q_0, Q_1, Q_2 \rangle$), therefore
Desargues $^{-1}(\{P_0, P_1, P_2\}, \{P'_0, P'_1, P'_2\}; \langle Q_0, Q_1, Q_2 \rangle, S(h))$,
or
Pascal(014235) $\implies \langle 1435, 0524, 0123; p14235 \rangle$,
Desargues $^{-1}(p14235, \{0523, 1423, 0514\}, \{14, 05, 23\}, \{0134, 0135, 1235\},$
 $\{35, p12435, 01\}; \langle p12345, p14523, p21435 \rangle, K(e))$,

Theorem [Salmon]

If 2 triangles have their vertices on a conic, their sides are tangent to a conic⁷.

Proof:

Desargues $^{-1}(\{0135, 0145, 0245\}, \{45, p14523, 01\}, \{0234, 1234, 1235\},$
 $\{12, p21435, 34\}; \langle 1245, K(e), 0134; P \rangle)$.

Exercise.

Prove $\langle p12345, p125423, p34215 \rangle$.

Theorem. [Steiner]

0. $\langle S(h), S(h\sigma_0), S(h\sigma_1); s(h) \rangle$, $s(h)$ is called the Steiner line of h ,
1. $S(h\sigma_0\sigma_1) \iota s(h)$,
2. there are 15 Steiner lines $s(h)$.

The proofs follows from 2.2.11.0 and from the fact that the Brianchon lines of the conic inscribed in the 2 triangles are Pascal lines of the original conic.

Theorem. [Cayley and Salmon]

0. $\langle K(h\chi), K(h\chi), K(h\chi); cs(h) \rangle$, $cs(h)$ is called the Cayley-Salmon line of h ,
1. $S(h) \iota cs(h)$,
2. there are 20 Cayley-Salmon lines.
3. The 60 Kirkman points, the 20 Steiner points, the 60 Pascal lines and the 20 Cayley-Salmon lines form a $80 * 4 \& 80 * 4$ configuration (See Levi, p. 199).

⁷Salmon, p. 381

Theorem.

18 Pascal points and 12 Pascal lines are used in the preceding Theorem and these are vertices and sides of 3 complete quadrilaterals.

Theorem. [Salmon]

0. $\langle cs(h), cs(h\lambda), cs(h\lambda^2); Sa(h) \rangle$, $Sa(h)$ is called the Salmon point of h ,
1. $cs(h\lambda^3) \iota Sa(h)$,
2. there are 15 Salmon points $Sa(h)$.

Theorem.

In the preceding Theorem:

0. Each of the 24 Pascal lines occurs exactly twice.
1. The Pascal points of h occur 4 times, the other 30 Pascal points occur twice.
2. The 3 Pascal points of h , the 8 points $S(h\lambda^i)$, $K_i(h\chi)$, $i = 0, 1, 2, 3$ and the 12 associated Pascal lines form a pseudo configuration of type $3 * 4 + 8 * 3 \& 12 * 3$, (11).

Example.

In all cases $h = e = [012345] = ()$.

0. The Theorem of Steiner.

$$\begin{array}{cccc}
 S(e) \iota & S(\sigma_0) \iota & S(\sigma_1) \iota & S(\sigma_0\sigma_1) \iota \\
 () = [012345] & (23) = [013245] & (45) = [012354] & (23)(45) = [013254] \\
 (135) = [032541] & (1235) = [023541] & (1345) = [032451] & (12345) = [023451] \\
 (153) = [052143] & (1523) = [053142] & (1453) = [042153] & (14523) = [043152] \\
 \langle \langle p12345, p14523, p34125 \rangle, \langle p13245, p14523, p24135 \rangle, \langle p12354, p15423, p35124 \rangle, \\
 \langle p13254, p15432, 15234 \rangle \rangle. \text{ (Fig. 200b)}
 \end{array}$$

1. The Theorem of Cayley-Salmon.

$$\begin{array}{cccc}
 S(e) \iota & K(\chi) \iota & K(\sigma\chi) \iota & K(\sigma^2\chi) \iota \\
 () = [012345] & (14) = [042315] & (1435) = [042531] & (1453) = [042153] \\
 (135) = [032541] & (024531) = [204153] & (0241) = [204315] & (024351) = [204531] \\
 (153) = [052143] & (043512) = [420531] & (045312) = [420153] & (0412) = [420315] \\
 \langle \langle p12345, p14523, p34125 \rangle, \langle p42315, p23514, p24135 \rangle, \langle p13524, p25134, p15342 \rangle, \\
 \langle p35124, p21354, p24513 \rangle \rangle. \text{ (Fig. 200b')}
 \end{array}$$

2. The Theorem of Salmon.

Add to Example 1, (Fig. 200b" and b4)

$S(\lambda) \iota$	$K(\lambda) \iota$	$K(\lambda\sigma\chi) \iota$	$K(\lambda\sigma^2\chi) \iota$
$(2354) = [013524]$	$(12354) = [023514]$	$(12345) = [023451]$	$(123) = [023145]$
$(15)(234) = [053421]$	$(031) = [302145]$	$(03541) = [302514]$	$(03451) = [302451]$
$(1423) = [043125]$	$(02)(1345) = [230451]$	$(02)(13) = [230145]$	$(02)(1354) = [230514]$
$\langle\langle p13524, p12435, p43125 \rangle, \langle p23514, p21453, p32154 \rangle, \langle p15432, p25143, p14523 \rangle, \langle p23145, p24513, p32415 \rangle\rangle. (Fig. 200b1)$			
$S(\lambda) \iota$	$K(\lambda) \iota$	$K(\lambda\sigma\chi) \iota$	$K(\lambda\sigma^2\chi) \iota$
$(25)(34) = [015432]$	$(134)(25) = [035412]$	$(1325) = [035241]$	$(13)(254) = [035124]$
$(14325) = [045231]$	$(054231) = [503124]$	$(052341) = [503412]$	$(051)(23) = [503241]$
$(12543) = [025134]$	$(0322)(15) = [350241]$	$(031542) = [350124]$	$(034152) = [350412]$
$\langle\langle p15432, p13254, p25134 \rangle, \langle p21453, p31245, p24135 \rangle, \langle p14253, p34125, p12435 \rangle, \langle p35124, p32415, p41235 \rangle\rangle. (Fig. 200b2)$			
$S(\lambda) \iota$	$K(\lambda) \iota$	$K(\lambda\sigma\chi) \iota$	$K(\lambda\sigma^2\chi) \iota$
$(2453) = [04253]$	$(15324) = [054213]$	$(15)(24) = [054321]$	$(15243) = [054132]$
$(1245) = [024351]$	$(0431)(25) = [405132]$	$(041)(253) = [405213]$	$(04251) = [405321]$
$(13)(245) = [034152]$	$(05142) = [540321]$	$(052)(143) = [540132]$	$(0532)(14) = [540213]$
$\langle\langle p14253, p15342, p25143 \rangle, \langle p31245, p42315, p32154 \rangle, \langle p12345, p43125, p13254 \rangle, \langle p23145, p41235, p21354 \rangle\rangle. (Fig. 200b3)$			

Exercise.

0. Give the geometric interpretation of the Theorems in this section.
1. Determine the pseudo configuration associated to the Theorem of Salmon.

2.2.13 Bézier Curves for drawing Conics, Cubics,**Introduction.**

The drawing of curves is facilitated by the notion of Bézier curves. These originate with the work of de Casteljau at Citroën in 1959 and were popularized and generalized by Bézier. To describe easily complicated curves in 2, 3, . . . dimensions, we start with a Bézier polygon 2.2.13 to construct a parametric representation of points on the curve iteratively. The associated theory is briefly given here. The curve can be expressed in terms of the Bézier polygon by means of Bernstein polynomials (2.2.13), the derivatives and differences of the curve can be similarly expressed and related to each other. The example for a curve whose i -th coordinates can be approximated by cubic polynomials is given in 2.2.13.

Theorem.

Let $P := (w_0(1 - I)^2, 2w_1I(1 - I), w_2I^2)$, $w_0w_1w_2 \neq 0$ then

0. P is the parametric equation of a conic, which passes through the points $P(0) = (1, 0, 0)$, $P(1) = (0, 0, 1)$, $P(\infty) = (w_0, -2w_1, w_2)$,
1. the tangent t at P is

$$[w_1w_2I^2, -w_2w_0I(1 - I), w_0w_1(1 - I)^2],$$

in particular, the tangent at $P(0)$ is $[0, 0, 1]$, at $P(1)$ is $[1, 0, 0]$, (which meet at $U = (0, 1, 0)$) and at $P(\infty)$ is $[w_1 w_2, w_2 w_0, w_0 w_1]$,

2. t meets $t(0)$ at

$$T = [w_0(1 - I), w_1 I, 0],$$

in particular, $T(\infty) = [-w_0, w_1, 0]$,

3. the anharmonic ratio

$$\text{anhr}(U, P(0), T(\infty), T) = \frac{w_0 - w_1}{w_0} I.$$

The proof starts with the observation that the coordinates P_0, P_1, P_2 , satisfy the equation

$$4w_1^2 P_0 P_2 = w_2 w_0 P_1^2,$$

which is indeed the equation of a conic with the prescribed properties. The corresponding polarity matrix is

$$\begin{pmatrix} 0 & 0 & 2w_1^2 \\ 0 & -w_2 w_0 & 0 \\ 2w_1^2 & 0 & 0 \end{pmatrix}.$$

Notice that $T(0) = (1, 0, 0)$ and is not undefined.

The tangent can either be obtained from the polarity or using $P \times DP$, where its direction $DP = (-w_0(1 - I), w_1(1 - 2I), w_2 I)$.

The last statement of the Theorem is associated with the four tangents Theorem of J. Steiner. It can be used as a method to draw conics. In the excellent language Postscript (see Reference Manual), a general method is given to draw curves based on the work of de Casteljau and Bézier as well as a method to draw ellipses using the Euclidean concepts of rotation and scaling differently in the direction of its axis. This method does not allow to draw hyperbolas or parabolas and ignores the fact that a conic is a projective concept. The following gives a method which allows to draw conics using 3 points A, B, C , and the tangents t_A, t_B at two of the 2 points.

It is then generalized to other curves.

Algorithm.

If the barycentric coordinates are chosen in such a way that $A = (1, 0, 0)$, $B = (0, 0, 1)$, $t_A \times t_B = (0, 1, 0)$ and $C = (1, 1, 1)$, then the points on the conic are given by P of the preceding Theorem, with, for instance, $w_0 = 2$, $w_1 = -1$, $w_2 = 2$. In the case of a finite field, we compute P for each element of the field or for an appropriate subset of it. In the case of the field of reals, we can compute P for $\tan(\pi t)$, $t = 0$ to 1 , avoiding $1/2$, a section of the conic can be obtained by appropriately limiting the set $\{t\}$, joining the successive points by segments will automatically give the asymptotes for an hyperbola, which is appropriate because their directions are indeed points in the Euclidean plane, as we prefer to consider it (in its extended form). An other approach is to limit the domain of P to $[0, 1]$ to obtain one section of the conic and to replace w_1 by $-w_1$, which is equivalent to compose \mathbf{P} with $\frac{I}{2I-1}$, to obtain the complement, see Farin, p.185.

For some of the Theorems, see Farin.

In what follows, the superscript of B, P and \mathbf{P} are indices and not exponents.

Definition.

The Bernstein polynomials are

$$B_i^n := \binom{n}{i} I^i (1-I)^{n-i}, \quad 0 \leq i \leq n.$$

By convention $B_{-1}^n = B_{n+1}^n := 0$.

In particular,

$$B_0^2 = (1-I)^2, \quad B_1^2 = 2I(1-I), \quad B_2^2 = I^2.$$

Theorem.

$$0. \quad B_0^0 = 1, \quad B_i^n = (1-I)B_i^{n-1} + IB_{i-1}^{n-1},$$

$$1. \quad DB_i^n = n(B_{i-1}^{n-1} - B_i^{n-1}).$$

$$2. \quad \sum_{j=0}^n B_j^n = 1.$$

Definition.

A weighted point \mathbf{P} is a set of 3 non homogeneous coordinates which are not all 0. We can add weighted points and multiply by scalars, but two weighted points which differ by a multiplicative constant are not equivalent. I will use the notation P for the equivalent point.

Definition. [de Casteljau]

Given $n+1$ weighted points $\mathbf{P}_0, \mathbf{P}_1, \dots, \mathbf{P}_n$, called the Bézier polygon, define

$$\mathbf{P}_i^0 := \mathbf{P}_i, \quad 0 \leq i \leq n,$$

$$\mathbf{P}_i^j := (1-I)\mathbf{P}_{i-1}^{j-1} + I\mathbf{P}_{i+1}^{j-1}, \quad 1 \leq j \leq n, \quad 0 \leq i \leq n-j.$$

$$\mathbf{P}^n := \mathbf{P}_0^n,$$

The curve P^n is called the de Casteljau curve of order n .

The same curve is also called the Bézier curve.

Theorem.

$$0. \quad P^n(0) = \mathbf{P}_0, \quad P^n(1) = \mathbf{P}_n.$$

$$1. \quad \mathbf{P}_i^j = \sum_{k=0}^j \mathbf{P}_{i+k} B_k^j, \quad 0 \leq j \leq n, \quad 0 \leq i \leq n-j,$$

in particular,

$$2. \quad \mathbf{P}^n = \sum_{k=0}^n \mathbf{P}_k B_k^n,$$

$$3. \quad D\mathbf{P}^n = n \sum_{k=0}^{n-1} (\mathbf{P}_{k+1} - \mathbf{P}_k) B_k^{n-1}.$$

Definition.

$$\Delta \mathbf{Q}_k = \mathbf{Q}_{k+1} - \mathbf{Q}_k,$$

$$\Delta^{r+1} \mathbf{Q}_k = \Delta^r \mathbf{Q}_{k+1} - \Delta^r \mathbf{Q}_k,$$

Theorem.

$$\Delta \mathbf{Q}_0 = \sum_{k=0}^r (-1)^{r-j} \binom{r}{j} \mathbf{Q}_{i+k}.$$

Theorem.

$$D^r \mathbf{P}^n = \frac{n!}{(n-r)!} \sum_{k=0}^{n-r} \Delta^r \mathbf{P}_k B_k^{n-r}.$$

$$D^r \mathbf{P}^n = \frac{n!}{(n-r)!} \Delta^r \mathbf{P}_0^{n-r}.$$

In particular,

$$D\mathbf{P}_n = n(\mathbf{P}_1^{n-1} - \mathbf{P}_0^{n-1}).$$

Curves with cubic parametrization.

For $n = 3$,

$$\mathbf{P}^3 = \mathbf{P}_0(1 - I)^3 + 3\mathbf{P}_1(1 - I)^2I + 3\mathbf{P}_2(1 - I)I^2 + \mathbf{P}_3I^3.$$

$$D\mathbf{P}^3(0) = \mathbf{P}_1 - \mathbf{P}_0,$$

$$D\mathbf{P}^3(1) = \mathbf{P}_3 - \mathbf{P}_2.$$

In other words the direction of the tangents at the end points is that of the line joining the end points to the nearest point.

If the cubic associated with the i -th coordinate of the curve \mathbf{P}^3 is

$$f = c_0 + c_1I + c_2I^2 + c_3I^3,$$

then the i -th coordinate a_j of the Bézier polygon \mathbf{P}_j is given by

$$a_0 = c_0, a_1 = c_0 + \frac{1}{3}c_1, a_2 = a_1 + \frac{1}{3}(c_1 + c_2), a_3 = c_0 + c_1 + c_2 + c_3.$$

Indeed, $a_0(1 - I)^3 + 3a_1(1 - I)^2I + 3a_2(1 - I)I^2 + a_3I^3 = f$.

These last formulas allows for the determination of the weighted points \mathbf{P}_i of the cubic (approximation) given the 3 non homogeneous coordinates of the parametrized curve. If the cubic associated with the i -th coordinate reduces to a linear function then $\mathbf{P}_i = \mathbf{P}^3(i/3)$, $i = 0, 1, 2, 3$.

It is often convenient to choose -1 and 1 for the end points instead of 0 and 1 by means of a change of variable. If $g = d_0 + d_1I + d_2I^2 + d_3I^3$ is the new polynomial, $f = c_0 + c_1I + c_2I^2 + c_3I^3 = g \circ \phi$, with $\phi = 2I - 1$. In this case, we obtain the symmetric formulas, $a_0 = d_0 - d_1 + d_2 - d_3$, $a_1 = d_0 - \frac{1}{3}d_1 - \frac{1}{3}d_2 + d_3$, $a_2 = d_0 + \frac{1}{3}d_1 - \frac{1}{3}d_2 - d_3$, $a_3 = d_0 + d_1 + d_2 + d_3$,

Example.

For the curve $(I - 3I^3, 1 - I^2, 1)$, for the first coordinate, $d_0 = d_2 = 0$, $d_1 = 1$, $d_3 = -3$, therefore $a_0 = 2$, $a_1 = -\frac{10}{3}$, $a_2 = \frac{10}{3}$, $a_3 = -2$. for the second coordinate, $d_1 = d_3 = 0$, $d_0 = 1$, $d_2 = -1$, therefore $a_0 = 0$, $a_1 = \frac{4}{3}$, $a_2 = \frac{4}{3}$, $a_3 = 0$. Therefore the Bézier polygon is $\mathbf{P}_0 = (2, 0, 1)$, $\mathbf{P}_1 = (-\frac{10}{3}, \frac{4}{3}, 1)$, $\mathbf{P}_2 = (\frac{10}{3}, \frac{4}{3}, 1)$, $\mathbf{P}_3 = (-2, 0, 1)$.

This gives the Cartesian coordinates of the following points on the curve associated with $i/20$, $i = 0$ to 20 :

2.000,0.00; 1.287,0.19; 0.736,0.36; 0.329,0.51; 0.048,0.64; -0.125,0.75; -0.208,0.84; -0.219,0.91; -0.176,0.96; -0.097,0.99; 0.000,1.00; 0.097,0.99; 0.176,0.96; 0.219,0.91; 0.208,0.84; 0.125,0.75; -0.048,0.64; -0.329,0.51; -0.736,0.36; -1.287,0.19; -2.000,0.00.

The complement of the curve using $\frac{i/20}{2i/20-1}$ is

$2.0000, 0.0000; 3.0041, -0.2346; 4.6094, -0.5625; 7.3178, -1.0408; \dots, -7.3178, -1.0408; -4.6094, -0.5625; -3.0041, -0.2346; -2.0000, 0.0000.$

Problem.

Given a curve in the plane, what are the condition for a representation of the 3 non-homogeneous coordinates by polynomials of degree n . For conics, we have seen that $n = 2$.

2.2.14 Projectivity determined by a conic.

Definition.

Joining 2 distinct points of a conic, is to determine the line through the 2 points. Joining a point of a conic to itself is to determine the tangent to the conic at that point.

Example.

For $p = 3$, The conic $X^2 + 2YZ = 0$ has the points (0) , (1) , (13) , (17) , (25) and (29) .

The tangents at (X_0, Y_0, Z_0) is $[X_0, Z_0, Y_0]$.

The tangent at (0) is $[1]$ and the tangent at (1) is $[0]$.

These points joined to (0) give the lines $[6]$, $[26]$, $[16]$, $[21]$, $[11]$. These points joined to (1) give $[0]$, $[8]$, $[10]$, $[7]$, $[9]$.

These lines determine on the ideal line $[12]$, the projectivity which associates to (26) , (5) , (14) , (18) , (22) , (26) , the points (5) , (26) , (18) , (22) , (10) , (14) .

This is precisely the projectivity ϕ of 2.2.6.

Theorem.

Let N be a symmetric matrix associated to a conic.

0. P is on the conic if $P \cdot NP = 0$.

1. If P is on the conic and C is not, the other point on the conic, if any, is

$$P + yC, \text{ with } y = -2 \frac{C \cdot NP}{C \cdot NC}.$$

Proof: $(P + yC) \cdot N(P + yC) = 0,$

or

$$P \cdot NP + yC \cdot NP + yP \cdot NC + y^2C \cdot NC = 0,$$

but $P \cdot NP = 0$ and $C \cdot NC \neq 0$ and N is symmetric, therefore $C \cdot NP = P \cdot NC$, hence $y = -2 \frac{C \cdot NP}{C \cdot NC}.$

Theorem.

Let l be a line and A, B be 2 points on the line but not on the conic associated with the symmetric matrix N ,

let $a := A \cdot NA$, $b := B \cdot NB$, $c := A \cdot NB = B \cdot NA$,

let C be an arbitrary point on the line, $C = A + kB$.

Let P_1 and P_2 be 2 distinct points on the conic, let $a_1 = (P_1 \cdot A * P_2)$, $b_1 := (P_1 \cdot B * P_2)$,

$c_1 := (A \cdot B * P_1)$, $c_2 := (A \cdot B * P_2)$, $d_1 := A \cdot NP_1$, $d_2 := B \cdot NP_2$. If $C \times P_1$ meets the conic at Q and $P_2 \times Q$ meets l at D , then

$$0. \ D = ((aa_1) + 2(ca_1 - d_1c_1)k + (ba_1 + 2d_2c_1)k^2)B \\ - ((ab_1 - 2d_1c_2) + 2(cb_1 - d_2c_2)k + bb_1k^2)A.$$

1. The correspondance between C and D is a projectivity.

Proof: $Q = (C \cdot NC)P_1 - 2(C \cdot NP_1)C$,
 $D = (A * B) * (P_2 * Q) = (A \cdot P_2 * Q)B - (B \cdot P_2 * Q)A$
 $= (Q \cdot A * P_2)B - (Q \cdot B * P_2)A$
 $= ((C \cdot NC)(P_1 \cdot A * P_2) - 2(C \cdot NP_1)(C \cdot A * P_2))B$
 $- ((C \cdot NC)(P_1 \cdot B * P_2) - 2(C \cdot NP_1)(C \cdot B * P_2))A$,
but $C \cdot NC = a + 2kc + k^2b$
therefore
 $D = ((a + 2ck + bk^2)a_1 - 2(d_1 + kd_2)(-c_1k))B$
 $- ((a + 2kc + bk^2)b_1 - 2(d_1 + d_2k)(c_2))A$

Theorem.

If the line l is $[1, 1, 1]$ then the conic $X^2 + Y^2 + kZ^2 = 0$ determines on l the involution η

$$\eta(1, Y, -1 - Y) = (1, f(Y), -1 - f(Y)), \text{ with } \\ f(Y) = -\left(\frac{1+k+Y}{k+(1+k)Y}\right).$$

Proof. The point $(1, Y, -1 - Y)$ on l has the polar $[1, Y, -k(1 + Y)]$, which meets l at $(Y + k(1 + Y), -1 - k(1 + Y), 1 - Y) = (1, f(Y), -1 - f(Y))$.

2.2.15 Cubics.

Notation.

In this section, the cubic is denoted by γ , (I, i) will denote an inflection point and the corresponding tangent, (A, a) a point on the cubic and its tangent,

Theorem.

Given I , there exists 3 (A_i, a_i) such that $a_i \cdot I = 0$ and A_i are collinear.

Theorem.

Let B_j , $j = 0$ to 5 be on γ and a conic θ , if C_j is the third point on $B_j \times B_{j+3}$, then C_j are collinear.

Corollary.

Given (A_i, a_i) , $i = 0$ to 2, let B_i be the other point on a_i then B_i are collinear.

Corollary.

If B_k , $k = 0$ to 3 are on γ . Let a conic θ_l meet γ also at $C_{l,0}$ and $C_{l,1}$, $C_{l,0} \times C_{l,1}$ passes through a fixed point D of γ .

Theorem.

The third point on $I_1 \times I_2$ is an inflection point.

Theorem.

Given (A_l, a_l) , $l = 0, 1$, and B_l is the other point on a_l , $(A_0 \times A_1) \times (B_0 \times B_1)$ is on the cubic.

Theorem.

The anharmonic ratio of the 4 tangents through A distinct from a is constant.

2.2.16 Other models for projective geometry.**Introduction.**

Many models can be derived from the model given in section 1. This is most easily accomplished by starting with a correspondence between points in the plane and adjusting for special cases. One such correspondence is (x_0, x_1, x_2) to $(\frac{1}{x_0}, \frac{1}{x_1}, \frac{1}{x_2})$, and will be studied in some detail. It assumes some given triangle $\{A_0, A_1, A_2\}$, whose vertices have coordinates $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$.

Definition.

In inversive geometry, the “points” are the points (x_0, x_1, x_2) , with $x_0x_1x_2 \neq 0$ together with the lines $[0, x_1, x_2]$, $[x_0, 0, x_2]$, $[x_0, x_1, 0]$, the “lines” are the point conics

$$a_0x_1x_2 + a_1x_2x_0 + a_2x_0x_1 = 0.$$

degenerate or not. A “point” is on a “line”, which is a non degenerate point conic, iff it belongs to it or is tangent to it. If the point conic degenerates in 2 lines, one which is a side of the triangle and the other passes through the opposite vertex, then the “points” who belong to it are the two lines and the points on the line through the opposite vertex but not on the sides of triangle. If the point conic degenerates in 2 lines, which are 2 sides of the triangle, the “points” which belong to it are the lines through the common vertex.

Example.

The “line” $x_1x_2 + 2x_2x_0 + 3x_0x_1 = 0$ belongs to the “points” $(-x_1x_2, (2x_1+3x_2)x_2, (2x_1+3x_2)x_1)$, $(2x_1+3x_2)x_1x_2 \neq 0$ and to the “points” $[0, 3, 2]$, $[3, 0, 1]$, $[2, 1, 0]$ tangent respectively at A_0 , A_1 and A_2 .

¹G24.TEX [MPAP], September 9, 2019

The “line” $2x_2x_0 + 3x_0x_1 = 0$ belongs to the “points” $(x_0, 2, -3)$, $x_0 \neq 0$ and to the “points” $[1, 0, 0]$ and $[0, 3, 2]$.

The “line” $x_1x_2 = 0$ belongs to the “points” $[0, x_1, x_2]$.

Theorem.

The model 2.2.16 satisfies the axioms 2.1.2 of projective geometry.

This is most easily seen if we associate to the point $P = (x_0, x_1, x_2)$, $x_0x_1x_2 \neq 0$ the “point” $P' = (\frac{1}{x_0}, \frac{1}{x_1}, \frac{1}{x_2})$ or (x_1x_2, x_2x_0, x_0x_1) , to the point $Q_0 = (0, x_1, x_2)$, the “point” $Q'_0 = [0, x_1, -x_2]$, to the point $Q_1 = (x_0, 0, x_2)$, the “point” $Q'_1 = [x_0, 0, -x_2]$, to the point $Q_2 = (x_0, x_1, 0)$, the “point” $Q'_2 = [x_0, x_1, 0]$, and to the line $l = [a_0, a_1, a_2]$, the line l' , $a_0x_1x_2 + a_1x_2x_0 + a_2x_0x_1 = 0$.

Indeed if $P \cdot l = 0$, P' is on l' and if $Q_0 \cdot l = 0$, $a_1x_1 + a_2x_2 = 0$, while the tangent to l' at A_0 is $[0, a_2, a_1] = [0, x_1, -x_2]$.

Theorem.

The “lines” are the conics through the vertices A_0, A_1, A_2 .

Theorem.

The “conics” are the quartics

$$0. \quad b_0x_1^2x_2^2 + b_1x_2^2x_0^2 + b_2x_0^2x_1^2 + (c_0x_0 + c_1x_1 + c_2x_2)x_0x_1x_2 = 0.$$

The quartic has double points (or nodes) at the vertices A_0, A_1, A_2 .

The branches through A_0 are real if and only if $c_0^2 > 4b_1b_2$,

the branches through A_1 are real if and only if $c_1^2 > 4b_2b_0$,

the branches through A_2 are real if and only if $c_2^2 > 4b_0b_1$.

Vice versa if a quartic as double points at A_0, A_1 and A_2 it is of the form 0.

Theorem.

If the quartic has double points with real branches at A_0, A_1 and A_2 , the tangents $P'_0P'_1$ at A_0 , $P'_2P'_3$ at A_1 and $P'_4P'_5$ at A_2 are such that if K'_0 is the tangent to the conic $(A_0, (A_1, P'_3), (A_2, P'_4))$, if K'_1 is the tangent to the conic $(A_1, (A_2, P'_5), (A_0, P'_0))$, and if K'_2 is the tangent to the conic $(A_2, (A_0, P'_1), (A_1, P'_2))$, then there is a conic through A_0, A_1, A_2 with tangents K'_0, K'_1, K'_2 .

This is a direct consequence of the Theorem of Pascal associated to the model.

Theorem.

If a quartic has double points with real branches at A_0, A_1 and A_2 , then the 6 tangents at these points belong to the same line conic.

Proof: Let the tangents at A_0, A_1, A_2 be $[0, 1, z]$, $[0, 1, z']$, $[x, 0, 1]$, $[x', 0, 1]$, $[1, y, 0]$, $[1, y', 0]$, the tangents $[0, 1, z]$ at A_0 satisfy $b_1z^2 + c_0z + b_2$, therefore $zz' = \frac{b_2}{b_1}$, similarly, $yy' = \frac{b_0}{b_2}$ and $xx' = \frac{b_1}{b_0}$.

On the other hand, applying Brianchon's theorem to these tangents gives the Brianchon lines $[0, x'y, -1]$, $[-1, 0, y'z]$, $[z'x, -1, 0]$ and these belong to the same point if $x'yy'zz'x = 1$. This conjecture was most strongly confirmed by a computer program and proven within an hour.

Theorem.

If $b_0 = 0$, then the quartic degenerates in the side $A_1 \times A_2$ and a cubic with double point at A_0 passing through A_1 and A_2 .

The conic $c_1c_2yz + b_1c_1zx + b_2c_2xy = 0$ plays, in the invertible geometry, the role of the "line" tangent at the "point" $[1, 0, 0]$.

2.2.17 Notes.

Theorem. [Jones]

Let n be even. If an n -gon is inscribed in a conic and $n-1$ sides meet a line at fixed points, then the n -th side also meets the line at a fixed point and dually.

Theorem. [Jones]

The preceding Theorem, when $n = 4$ is equivalent to Pascal's Theorem.

2.3 Geometric Models on Regular Pythagorean Polyhedra.

2.3.0 Introduction.

Completely independently, one of my first student at the "Université Laval", Quebec City, made the important discovery that the regular polyhedra can be used as models for finite geometries associated with 2, 3 and 5. Then, he introduced the nomenclature of selector (sélecteur) for the notion of cyclic difference sets, introduced by J. Singer, in 1938, to label points and hyperplanes in N dimensional projective geometry of order p^k (See Baumert, 1971) and to construct an appropriate numbering of the points and lines on the polyhedra. Except for the fundamental contribution of Singer, the introduction of selector polarity (prepared by the use of $f(a+b)$ instead of $f(a-b)$ in the definition of incidence), the introduction of auto-polars and those on the conics for the dodecahedron, all the results in this section are due to Fernand Lemay.

Clearly we have only to study the tetrahedron, the cube and the dodecahedron, because the octahedron is dual to the cube and the icosahedron is dual to the dodecahedron.

¹G25.TEX [MPAP], September 9, 2019

2.3.1 The selector.

Introduction.

The important concept of the cyclic difference sets allows for an arithmetization of projective geometry which is as close to the synthetic point of view as is possible. With it, it is not only trivial to determine all the points on a line, and lines incident to a point, but also the lines through 2 points and points on 2 lines. This concept makes duality explicit through the correlation, which is a polarity when $p \geq 5$. The definitions of selector function and selector correlation is implicit in Lemay's work.

Definition.

A difference set associated to $q = p^k$ is a set of $q + 1$ integers $\{s_0, s_1, \dots, s_q\}$ such that the $q^2 + q$ differences $s_i - s_j$, $i \neq j$ modulo $n := q^2 + q + 1$ are distinct and different from 0. When applied to Geometry, I will prefer the terminology of Lemay and use the synonym selector. The elements of the selector are called selector numbers.

Theorem. [Singer]

For any $q = p^k$ there exists difference sets.

Theorem.

If $\{s_i\}$, $i = 0$ to q , is a difference set and k is relatively prime to n , then

0. $\{s'_i = a + ks_{i+1}\}$, is also a difference set.

The indices are computed modulo $q + 1$ and the selector numbers, modulo n .

Using 0, we can always find a selector for which 0 and 1 are selector numbers.

Example. [Singer]

The following are difference sets associated with $q = p^k$:

For $p = 2$: $\{0, 1, 3\}$ modulo 7.

For $p = 3$: $\{0, 1, 3, 9\}$ modulo 13.

For $q = 2^2$: $\{0, 1, 4, 14, 16\}$ modulo 21.

For $p = 5$: $\{0, 1, 3, 8, 12, 18\}$ modulo 31.

For $p = 7$: $\{0, 1, 3, 13, 32, 36, 43, 52\}$ modulo 57.

For $q = 2^3$: $\{0, 1, 3, 7, 15, 31, 36, 54, 63\}$ modulo 73.

For $q = 3^2$: $\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$ modulo 91.

For $q = 11$: $\{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109\}$ modulo 133.

Definition.

If $a = 1$ and $k = -1$, the selector $s'_i := 1 - s_i$ is called the complementary selector or co-selector of s_i .

The selectors obtained using $k = 2, \frac{1}{2}, -2, -\frac{1}{2}$ are called respectively bi-selector, semi-selector, co-bi-selector, co-semi-selector.

Example.

For $q = 4$, other selectors are

$$\{10, 12, 17, 18, 21\}, \{0, 5, 20, 7, 17\} \text{ and } \{0, 1, 6, 8, 18\}.$$

For $p = 7$, if

the selector is $\{0, 1, 7, 24, 36, 49, 54\}$, then

the co-selector is $\{0, 1, 4, 9, 20, 22, 34, 51\}$,

the bi-selector is $\{0, 1, 5, 27, 34, 37, 43, 45\}$,

the co-bi-selector is $\{0, 1, 13, 15, 21, 24, 31, 53\}$,

the semi-selector is $\{0, 1, 9, 11, 14, 35, 39, 51\}$,

the co-semi-selector is $\{0, 1, 7, 19, 23, 44, 47, 49\}$.

Program.

All selectors derived by multiplication from one of them are given in [113]MODP30.

Definition.

The selector function f associated to the selector $\{s_i\}$ is the function from Z_n to Z_n

$$f(0) = 0, f(s_j - s_i) = s_i, i \neq j.$$

Example.

For $p = 2$, the selector function associated with $\{0, 1, 3\} \pmod{7}$ is

$$\begin{array}{ccccccc} i & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ f(i) & 0 & 0 & 1 & 0 & 3 & 3 & 1 \end{array}$$

For $p = 3$, the selector function associated with $\{0, 1, 3, 9\} \pmod{13}$ is

$$\begin{array}{cccccccccccccc} i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ f(i) & 0 & 0 & 1 & 0 & -4 & -4 & 3 & -4 & 1 & 0 & 3 & 3 & 1 \end{array}$$

For $p = 5$, the selector function associated with $\{0, 1, 3, 8, 12, 18\} \pmod{31}$ is

$$\begin{array}{cccccccccccccccccc} i & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ f(i) & 0 & 0 & 1 & 0 & 8 & 3 & 12 & 1 & 0 & 3 & 8 & 1 & 0 & 18 & 18 & 3 \\ \hline i & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\ f(i) & 18 & 1 & 0 & 12 & 12 & 18 & 12 & 8 & 8 & 18 & 8 & 12 & 3 & 3 & 1 \end{array}$$

Theorem.

$$0. f(j - i) - i = f(i - j) - j \pmod{n}.$$

Points, lines and incidence in the 2 dimensional geometry associated with $q = p^k$ and $n := q^2 + q + 1$ are defined as follows.

Definition.

The points are elements of the set $\{0, 1, \dots, n - 1\}$,

The lines are elements of the set $\{0, 1, \dots, n - 1\}$.

A point a is incident to a line b iff $f(a + b) = 0$.

Notation.

The points are denoted by a lower case letter or by an integer in Z_n . The lines are denoted by a lower case letter or by an integer in Z_n followed by an asterix. The line incident to the points a and b is denoted $a \times b$, the point incident to the lines a^* and b^* is denoted $a^* \times b^*$.

Theorem.

Given a selector $\{s_j\}$ associated with $q = p^k$ and the corresponding selector function f :

0. The $q + 1$ points incident to or on the line i^* are $s_j - i \pmod n$.
1. The $q + 1$ lines incident to or on the point i are $(s_j - i \pmod n)^*$.
2. $a \neq b \implies a \times b = (f(b - a) - a)^*$.
3. $a \neq b \implies a^* \times b^* = f(b - a) - a$.
4. a on b^* iff b on a^* .

The statements in the preceding Theorem reflect the duality in projective geometry.

Definition.

The selector polarity is the correlation which associates to the point i the line i^* . The points x which are on x^* are called auto-polars.

The name "polarity" is appropriate because of 2.3.1.4.

The selector polarity and the auto-polars play an important role in a natural way of labeling the elements of the Pythagorean solids.

Theorem.

The auto-polars are given by

$$a_i = \frac{s_i}{2}, \text{ modulo } n.$$

Indeed we should have for an auto-polar x , $x = s_i - x$.

Definition.

A primitive polynomial of degree 3 over $GF(q)$, is an irreducible polynomial P of degree 3 such that

$$I^k \neq \underline{1} \text{ for } k = 1 \text{ to } q - 2,$$

where I is the identity function and $\underline{1}$ the constant polynomial 1.

The multiplication is done modulo P and polynomials which differ by a multiplicative constant $\neq 0$ modulo q are equivalent.

Theorem. [Singer]

For each value of $q = p^k$ a selector can be obtained by choosing a primitive polynomial of degree 3 over $GF(q)$. The selector is the set of exponents of I between 0 and $q - 2$ which are of degree less than 2.

Example.

For $p = 3$, $P = I^3 - I + 1$,
 $I^0 = 1$, $I^1 = I$, $I^2 = I^2$, $I^3 = I - 1$, $I^4 = I^2 - I$, $I^5 = I^2 - I + 1$, $I^6 = I^2 + I + 1$,
 $I^7 = I^2 - I - 1$, $I^8 = I^2 + 1$, $I^9 = I + 1$, $I^{10} = I^2 + I$, $I^{11} = I^2 + I - 1$, $I^{12} = I^2 - 1$ and we
have $I^{13} = 1$.

Therefore the selector is $\{0, 1, 3, 9\}$.

2.3.2 The tetrahedron.**Introduction.**

I have found useful to introduce the adjectives vertex, edge and in later sections, face, to distinguish points and lines which have different representation in the Pythagorean solids.

Definition.

The points in the tetrahedron model consist of

0. *The 4 vertex-points, which are the 4 vertices (or the opposite planes or the line through the center C of the tetrahedron perpendicular to one of the 4 planes).*
1. *The 3 edge-points, which are the pairs of orthogonal edges, (or the mid-points of 3 non orthogonal edges or the line through these points and the center C).*

The lines in the tetrahedron model consist of

2. *The 6 edge-lines, which are incident to the 2 vertex-points and to the edge-point on them.*
3. *The tetrahedron-line, which is incident to the 3 edge-points.*

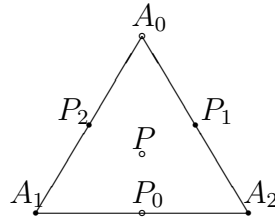
Theorem.

The model satisfies the axioms of projective geometry for $p = 2$.

Theorem.

With the selector $\{0,1,3\} \pmod{7}$, the 3 points, 0, 4 and 5 are auto-polars. It is therefore natural to associate them to the 3 edge-points. These points are on the line 3^* , it is natural to associate it to the tetrahedral line. Any of the vertex-points can be chosen as the polar 3 of 3^* . We will choose the 3 adjacent edge-lines as 0^* , 4^* and 5^* such that $0 \cdot 0^* = 4 \cdot 4^* = 5 \cdot 5^* = 0$. The other vertex-points are the third point on 0^* , 4^* and 5^* , therefore 2 is on the line and 2^* is the line orthogonal to the line associated to 5, similarly for 1 and 1^* , to 0 and 6 and 6^* , to 4.

Figure.



Theorem.

A complete quadrangle configuration consists of the 4 vertex-points A_0, A_1, A_2, P and the 6 edge-lines $a_0 = A_1 \times A_2, a_1 = A_2 \times A_0, a_2 = A_0 \times A_1, p_0 = P \times A_0, p_1 = P \times A_1, p_2 = P \times A_2$. It has the 3 edge-points $P_i = p_i \times a_i$ as its diagonal points, and these are on the tetrahedron-line p .

Exercise.

0. For $q = 2$, determine the primitive polynomial giving the selector $\{0, 1, 3\}$.
1. Determine the correspondence between the selector notation and the homogeneous coordinates for points and lines. Note that these are not the same.
2. The correspondence i to i^* is a polarity whose fixed points are on a line. Determine the matrix representation and the equation satisfied by the fixed points.
3. Determine the degenerate conic through 0, 1, 2 and 5 with tangent 5^* at 5, its matrix representation and its equation in homogeneous coordinates.
4. Determine all the non degenerate conics.

2.3.3 The cube.

Convention.

In what follows we identify elements of the cube, which are symmetric with respect to its center C , for instance, the parallel faces. There are therefore 3 independent faces, 4 independent vertices and 6 independent edges.

Definition.

The points in the cube model consist of

0. The 3 face-points, which are the square faces or their centers or the lines joining C to these points.
1. The 4 vertex-points, which are the vertices or the lines joining C to these vertices.

2. The 6 edge-points, which are the edges, or the mid-points of the edges or the lines joining C to these points.

The lines in the cube model consist of

3. The 3 face-lines, corresponding to a face f , which are incident to the 2 face-points and to the 2 edge-points in the plane through C parallel to f .
4. The 4 vertex-lines, corresponding to a vertex V , which are incident to the vertex-points V and to the 3 edge-points not adjacent to V .
5. The 6 edge-lines, corresponding to an edge e , which are incident to the face-point perpendicular to e , to the 2 vertex-points and the edge-point on e .

Theorem.

The cube model satisfies the axioms of projective geometry for $p = 3$.

Theorem.

With the selector 2.3.1 for $p = 3$, the auto-polars are 0, 7, 8 and 11. If we examine the quadrangle-quadrilateral configuration, we observe that p and q_i are the lines which require a 4-th point, it is easy to verify that, with $p = 3$, P is on p and Q_i is on q_i . Moreover

$0^* \cdot 0 = 0$, this suggest to take $P = 0$, $Q_i = 7, 8, 11$. Hence

$r_i := P \times Q_i = 9, 1, 3$; $p_i := Q_{i+1} \times Q_{i-1} = 5, 2, 6$;

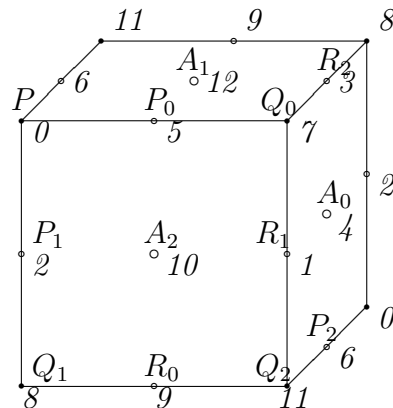
$A_i := r_i \times p_i = 4, 12, 10$; $a_i := A_{i+1} \times A_{i-1} = A_i$; $P_i := a_i \times r_i = p_i$;

$q_i := P_{i+1} \times P_{i-1} = Q_i$; $R_i := a_i \times q_i = r_i$; $p := R_1 \times R_2 = p$.

Theorem.

Because of 2.3.3, the vertex-points are auto-polars, we can choose them as 0, 7, 8 and 11, the other elements of the cube follow from 2.3.3. The edge-points are R_i and P_i , the face-points are A_i .

Figure.



Exercise.

0. For $p = 3$, determine the primitive polynomial giving the selector $\{0, 1, 3, 9\}$.
1. Determine the correspondence between the selector notation and the homogeneous coordinates for points and lines. Note that these are not the same.
2. The correspondence i to i^* is a polarity whose fixed points are on a line. Determine the matrix representation and the equation satisfied by the fixed points.
3. Determine the degenerate conic through 0, 1, 2 and 5 with tangent 4^* at 5, its matrix representation and its the equation in homogeneous coordinates. Hint: use 2.2.11.
4. Determine all the conics.

2.3.4 The dodecahedron.**Convention.**

In what follows we identify elements of the dodecahedron which are symmetric with respect to its center C , for instance, the parallel faces. There are therefore 6 independent faces, $\frac{5}{3}6 = 10$ independent vertices and $\frac{5}{2}6 = 15$ independent edges.

Definition.

The points in the dodecahedron model consist of

0. The 6 face-points, which are the pentagonal faces or their center or the lines joining C to these points.
1. The 10 vertex-points, which are the vertices or the lines joining C to these vertices.
2. The 15 edge-points, which are the edges, or the mid-points of the edges or the lines joining C to these points.

The lines in the dodecahedron model consist of

3. The 6 face-lines, which are incident to the corresponding face-point F and to the 5 edge-points in the plane through C perpendicular to CF .
4. The 10 vertex-lines, corresponding to a vertex V , which are incident to the 3 edge-points in the plane through C perpendicular to CV and to the 3 vertex-points which joined to V form an edge.
5. The 15 edge-lines, corresponding to an edge E , which are incident to the 2 face-points, the 2 vertex-points and the 2 edge-points in the plane through C and E .

Theorem.

The dodecahedron model satisfies the axioms of projective geometry for $p = 5$.

Example.

For $p = 5$, the selector function associated with the selector $\{0, 1, 3, 8, 12, 18\}$ is

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$f(i)$	0	0	1	0	8	3	12	1	0	3	8	1	0	-13	-13	3
type	f	e	e	e	f	v	f	v	e	f	v	v	e	v	e	s

i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$f(i)$	-13	1	0	12	12	-13	12	8	8	-13	8	12	3	3	1
type	f	f	e	v	v	v	e	e	v	e	e	e	e	v	e

The auto-polars are $\{0, 4, 6, 9, 16, 17\}$.

The “type” is explained in the following Theorem.

Theorem.

A natural labeling of the points of the dodecahedron and of the dodecahedral configuration, associated with the selector 2.3.1, for $p = 5$, can be obtained as follows. If we examine the dodecahedron configuration,

$$FA_i \cdot fa_i = AF_i \cdot af_i = 0,$$

it is therefore natural to choose FA_i and AF_i as the auto-polars, but this cannot be done arbitrarily. Let us choose any 3 of them as FA_i , 0, 16 and 17. To obtain P and A_i , we can proceed as follows.

$$pq_i = FA_i \times FA_{i+1} = 18, 15, 1; PQ_i = pq_i;$$

$$PR_i = pq_i \times FA_{i-1} = 14, 3, 2;$$

$$qp_i = PR_i \times PQ_i = 25, 28, 30;$$

$$AF_i = QP_i \times QP_{i+1} = 6, 4, 9;$$

$$a_i = FA_{i+1} \times AF_{i-1} = 23, 26, 8; A_i = a_i;$$

$$p = PR_1 \times PR_2 = 29.$$

We therefore choose $P = 29$ and $A_i = 23, 26, 8$. We obtain, according to 2.1.6, 2.1.7 and 2.1.7:

$$a_i = A_i, r_i = 20, 5, 10,$$

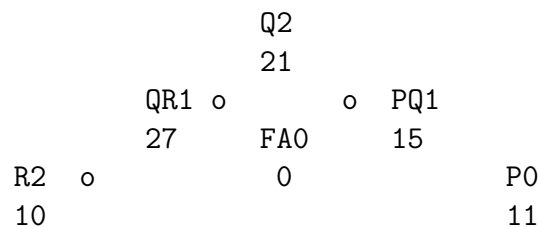
$$P_i = 11, 13, 24, q_i = 19, 7, 21, R_i = r^i, p_i = P_i, p = 29,$$

$$PQ_i = pq_i = 18, 15, 1, QP_i = qp_i = 25, 28, 30,$$

$$QR_i = qr_i = 12, 27, 22, PR_i = pr_i = 14, 3, 2,$$

$$AF_i = af_i = 6, 4, 9, FA_i = fa_i = 0, 16, 17.$$

Therefore the face-points are FA_i, AF_i ; the vertex-points are p_i, q_i, r_i ; the edge-points are $A_i, PQ_i, QP_i, QR_i, PR_i$.

Figure.

Definition.

A difference set associated to $q = p^k$ and to a polynomial of degree 3 with one root, is a set of q integers $\{s_0, s_1, \dots, s_{q-1}\}$ such that the $q^2 - q$ differences $s_i - s_j$, $i \neq j$ modulo $n = q^2 - 1$ are distinct and different from 0 modulo $q + 1$.

A difference set associated to $q = p^k$ and to a polynomial of degree 3 with two roots, is a set of $q - 1$ integers $\{s_0, s_1, \dots, s_{q-2}\}$ such that the $q^2 - 3q + 2$ differences $s_i - s_j$, $i \neq j$ modulo $n = q^2 - q$ are distinct and different from 0 modulo q and modulo $q - 1$.

When applied to Geometry, I will prefer the terminology of Lemay and use the synonym selector. The elements of the selector are called selector numbers.

Theorem.

There exists always a polynomial P of degree 3 with one root or 2 roots such that I is a generator of the multiplicative group of polynomials, of degree at most 2, with coefficients in Z_p , normalized to have the coefficient of the highest power 1, which are relatively prime to P . The selector numbers are the powers of I modulo P which are polynomials of degree at most 1.

The proof can be adapted easily from that of the irreducible case and is left as an exercise.

Example.

For $p = 3$, $P = I^3 + I + 1$,
 $I^0 = 1$, $I^1 = I$, $I^2 = I^2$, $I^3 = I + 1$,
 $I^4 = I^2 + I$, $I^5 = I^2 - I - 1$, $I^6 = I^2 - I + 1$, $I^7 = I^2 + 1$,
 and we have $I^8 = 1$. Therefore the selector is 0, 1, 3.

Example.

The following are difference sets associated with $q = p^k$:
 For $p = 3$: $I^3 + I + 1$, root 1, selector 0,1,3 (mod 8).
 $I^3 + I^2 - I - 1$, roots 2,2,1, selector 0,1 (mod 6).
 For $p = 5$: $I^3 - I - 1$, root 2, selector 0,1,3,11,20 (mod 24).
 $I^3 - 2I - 1$, roots 3,3,4, selector 0,1,3,14 (mod 20).
 For $p = 7$: $I^3 - I^2 - 2$, root 5, selector 0,1,7,11,29,34,46 (mod 48).
 $I^3 - 3I - 2$, roots 2,6,6, selector 0,1,3,11,16,20 (mod 42).
 For $q = 11$: $I^3 - I - 1$, root 6,
 selector 0,1,3,28,38,46,67,90,101,107,116 (mod 120).
 $I^3 - I^2 - I - 1$, roots 7,7,9,
 selector 0,1,9,15,36,38,43,62,94,107 (mod 110.)

Definition.

The selector function f associated to the selector $\{s_i\}$ is the function from Z_n to Z_n $f(s_j - s_i) = s_i$, $i \neq j$, for all other values $f(l) = -1$.

Example.

For $p = 5$, the selector function associated with $\{0, 1, 3, 11, 20\}$ is

i	0	1	2	3	4	5	6	7	8	9	10	11
$f(i)$	-1	0	1	0	20	20	-1	20	3	11	1	0

i	12	13	14	15	16	17	18	19	20	21	22	23
$f(i)$	-1	11	11	20	11	3	-1	1	0	3	3	1

Theorem.

0. If the defining polynomial has 1 root then the selector has $n := p$ elements, the selector function has $p^2 - 1$ elements and is -1 for the $p - 1$ multiples of $p + 1$.
1. If the defining polynomial has 2 distinct roots then the selector has $n := p - 1$ elements, the selector function has $p(p - 1)$ elements and is -1 for the $2p - 1$ multiples of p and $p - 1$.

Theorem.

0. If $f(i - j) \neq -1$ then $f(j - i) - i = f(i - j) - j$.

Points, lines and incidence in the 2 dimensional geometry associated with $q = p^k$ and $n := q^2 + q + 1$ are defined as follows.

Definition.

The points are elements of the set $\{0, 1, \dots, n-1\}$, the lines are elements of the set $\{0, 1, \dots, n-1\}$, a point a is incident to a line b iff $f(a + b) = 0$.

Notation.

The points are denoted by a lower case letter or by an integer in Z_n . The lines are denoted by a lower case letter or by an integer in Z_n followed by an asterix. The line incident to the points a and b is denoted $a \times b$, the point incident to the lines a^ and b^* is denoted $a^* \times b^*$.*

We leave as an exercise to state and prove Theorems analogous to those in Section 2.3.1.

Definition.

The dual affine plane, is a Pappian plane in which we prefer the “special” points which are those on a line l and a point P not on l and the “special” lines which are those through P and the line l .

The dual affine geometry can be studied by associating with it a polynomial which has 1 root. I give here some examples of Desargues, Pappus and Pascal configurations.

I illustrate Pappus and Desargues configurations using the notation of 2.1.2 and of 2.1.5 and give the points on a conic obtained using Pascal’s construction.

Example.

For $p = 11$, with the polynomial $I^3 - I - 1$, we have

$Pappus(\langle 89, 51, 79 \rangle, 69*, \langle 33, 88, 110, \rangle, 13*; \langle 92, 71, 6 \rangle, 95*),$

with $A_{i+1} \times B_{i-1} = (56*, 87*, 32*)$ and $A_{i-1} \times B_{i+1} = (28*, 77*, 115*)$.

$Desargues(98, \{7, 1, 70\}, \{37*, 31*, 100*\}, \{60, 98, 73\}, \{50*, 47*, 60*\};$

$\langle 70, 76, 7 \rangle, \langle 60*, 89*, 50* \rangle, 31*),$

$Desargues(111, \{115, 69, 13\}, \{54*, 33*, 51*\}, \{41, 119, 10\}, \{91*, 80*, 117*\};$

$\langle 67, 68, 70 \rangle, \langle 5*, 47*, 110* \rangle, 53*),$

From Pascal's construction we obtain the following points are on a conic: $9, 10, 33, 51, 58, 60, 74, 77, 79, 87, 96, 9$

Exercise.

Define a geometry corresponding to a polynomial which has 2 roots.

2.3.6 Generalization of the Selector Function for higher dimension.

Introduction.

I will briefly state one result for dimensions 3 and 4 concerning defining polynomials associated to the non irreducible case and illustrate for dimensions 3, 4 and 5.

Theorem.

If the P_i denotes a primitive polynomial of degree i .

0. For $k = 3$, the defining polynomials P can have the following form,

$$P_4, P_1P_3, P_1^2P_2,$$

there are $p^4 + p^3 + p^2 + p + 1, p^4 - 1, p^4 - p$ polynomials relatively prime to P , in these respective cases.

1. For $k = 4$, the defining polynomials P can have the following form,

$$P_5, P_1P_4, P_1^2P_3, P_2P_3.$$

there are $p^5 + p^4 + p^3 + p^2 + p + 1, (p^3 - 1)(p + 1), p^5 - 1, p^5 - p$ polynomials relatively prime to P , in these respective cases.

Proof: The polynomials in the sets are those which are relatively prime to the defining polynomial. There are p^k homogeneous polynomials of degree k . If, for instance, $k = 4$ and the defining polynomial P is P_2P_3 , there are $p^2 + p + 1$ polynomials which are multiple of P^2 and $p + 1$, which are multiples of P_3 , hence $p^4 + p^3 + p^2 + p + 1 - (p^2 + p + 1) - (p - 1)$ polynomials relatively prime to P .

Example.

a_0, a_1, \dots, a_k represent $I^{k+1} - a_0 I^k - a_1 I^{k-1} - \dots - a_k$.

k	p	period	def. pol.	sel.	roots of def. pol.
3	3	40	2, 1, 1, 1	13	--
		26	1, 1, 1, 1	9	1
		24	0, 1, 1, 1	8	2, 2
	5	156	1, 2, 0, 2	31	--
		124	1, 0, 0, 2	25	4
		120	0, 0, 1, 2	24	4, 4
	7	400	0, 1, 1, 4	57	--
		342	0, 0, 1, 1	49	3
		336	0, 0, 3, 1	48	5, 5
	11	1464	0, 0, 2, 5	133	--
		1330	0, 0, 1, 1	121	3
		1320	1, 5, 2, 4	120	1, 1
4	3	121	2, 0, 0, 0, 1	40	--
		104	0, 1, 0, 0, 1	35	$(I^2 + I - 1)(I^3 - I^2 + I + 1)$
		80	0, 2, 0, 0, 1	27	2
		78	1, 0, 0, 0, 1	26	2, 2
	5	781	4, 0, 0, 0, 1	156	--
		744	2, 2, 0, 0, 1	149	$(I^2 + I + 2)(I^3 + 2I^2 - I + 2)$
		624	2, 0, 0, 0, 1	125	3
		620	3, 0, 1, 0, 1	124	3, 3
	7	2801	3, 0, 0, 0, 1	400	--
		2736	6, 0, 0, 0, 1	391	$(I^2 + 2I - 2)(I^3 - I^2 - 3I - 3)$
		2400	3, 1, 0, 0, 1	343	3
		2394	0, 3, 3, 0, 1	342	5, 5
	11	16105	0, 0, 10, 0, 9	1464	--
		15960	0, 0, 0, 10, 8	1451	$(I^2 + I -)(I^3 - I^2 - I -)$
		14640	0, 0, 0, 10, 9	1331	10
		14630	0, 0, 0, 9, 7	1330	3, 3
	13	30941	8, 0, 0, 0, 1	2380	--
		30744	5, 0, 0, 0, 1	2365	$(I^2 - 3I + 6)(I^3 - 2I^2 + I + 2)$
		28560	2, 0, 0, 0, 1	2197	11
		28548			
5	3	364	1, 0, 0, 0, 0, 1	121	--
		242	1, 1, 0, 0, 0, 1	81	2
		240	1, 2, 1, 0, 0, 1	80	2, 2

Definition.

Given a selector s , the selector function associates to the integers in the set Z_n a set of $p+1$ integers or p integers obtained as follows,

$$s(j) \in f_i \text{ iff } sel(l) - sel(j) = i \text{ for some } l.$$

Theorem.

- 0. $f(i)$ is the set of points on the line $i^* \times 0^*$.
- 1. $f(i) - j$, where we subtract j from each element in the set, is the set of points in $(i + j)^* \times j^*$, equivalently
- 2. $f(i - j) - j$, is the set of points in $i^* \times j^*$.
- 3. $a^* \times b^* \times c^* = ((a - i)^* \times (b - i)^* \times (c - i)^*) - i$.

Theorem.

- 0. If the defining polynomial is primitive, then
 - 0. $|s| = \frac{p^k - 1}{p - 1}$,
 - 1. if $i \not\equiv \frac{p^k - 1}{p - 1}$, $|f(i)| = p + 1$.
- 1. If the defining polynomial has one root, then
 - 0. $|s| = p^k$,
 - 1. if $i \neq 0$, $|f(i)| = p$,
- 2. If the defining polynomial has a double root, then
 - 0. $|s| = p^k - 1$,
 - 1. if $i \not\equiv p, p^2 - 1$, $|f(i)| = p$,
 - 2. if $i \equiv p$ and $i \neq 0$, $|f(i)| = p - 1$,

Example.

- 0. $k = 3$, $p = 3$, defining polynomial $I^4 - 2I^3 - I^2 - I - 1 = (I - 1)(I^3 - I + 1)$,
selector: $\{0, 1, 2, 9, 10, 13, 15, 16, 18, 20, 24, 30, 37\}$

selector function:

0	-1	-1	-1	-1	14	1	2	10	16	28	2	9	13	30
1	0	1	9	15	15	0	1	9	15	29	1	13	20	24
2	0	13	16	18	16	0	2	24	37	30	0	10	20	30
3	10	13	15	37	17	1	13	20	24	31	9	10	18	24
4	9	16	20	37	18	0	2	24	37	32	9	10	18	24
5	10	13	15	37	19	1	18	30	37	33	9	16	20	37
6	9	10	18	24	20	0	10	20	30	34	15	16	24	30
7	2	9	13	30	21	9	16	20	37	35	2	15	18	20
8	1	2	10	16	22	2	15	18	20	36	1	13	20	24
9	0	1	9	15	23	1	18	30	37	37	0	13	16	18
10	0	10	20	30	24	0	13	16	18	38	2	15	18	20
11	2	9	13	30	25	15	16	24	30	39	1	2	10	16
12	1	18	30	37	26	15	16	24	30					
13	0	2	24	37	27	10	13	15	37					

1. $k = 3, p = 3$, defining polynomial $I^4 - I^3 - I^2 - I - 1 = (I - 1)^2(I^2 + I - 1)$,
selector: $\{0, 1, 2, 8, 11, 18, 20, 22, 23\}$

selector function:

0	-1	-1	-1	7	1	11	20	14	8	20	23	21	1	2	23
1	0	1	22	8	0	18	20	15	8	11	22	22	0	1	22
2	0	18	20	9	2	11	18	16	2	11	18	23	0	11	23
3	8	20	23	10	1	8	18	17	1	11	20	24	2	20	22
4	18	22	23	11	0	11	23	18	0	2	8	25	1	2	23
5	18	22	23	12	8	11	22	19	1	8	18				
6	2	20	22	13	-1	-1	-1	20	0	2	8				

2. $k = 3, p = 3$, defining polynomial $I^4 - I^2 - I - 1$.
selector: $\{0, 1, 2, 4, 14, 15, 19, 21\}$

selector function:

0	-1	-1	-1	6	15	19	-1	12	2	14	-1	18	1	21	-1
1	0	1	14	7	14	19	21	13	1	2	15	19	0	2	19
2	0	2	19	8	-1	-1	-1	14	0	1	14	20	1	4	19
3	1	21	-1	9	15	19	-1	15	0	4	-1	21	0	4	-1
4	0	15	21	10	4	14	15	16	-1	-1	-1	22	2	4	21
5	14	19	21	11	4	14	15	17	2	4	21	23	1	2	15

Example.

In the case of Example 2.3.6.0. If we denote by i^\dagger , the lines $0^* \times i^*$, these lines, which are sets of 4 points can all be obtained from

$1^\dagger = \{0, 1, 9, 15\}$, $2^\dagger = \{0, 13, 16, 18\}$, $4^\dagger = \{9, 16, 20, 37\}$ and

$10^\dagger = \{0, 10, 20, 30\}$ by adding an integer modulo n .

$1^\dagger + 0 = 1^\dagger, 9^\dagger, 15^\dagger, 1^\dagger + 1 = 39^\dagger, 8^\dagger, 14^\dagger,$

$1^\dagger + 9 = 6^\dagger, 31^\dagger, 32^\dagger, 1^\dagger + 15 = 34^\dagger, 25^\dagger, 26^\dagger,$

$2^\dagger + 0 = 2^\dagger, 24^\dagger, 37^\dagger, 2^\dagger + 2 = 22^\dagger, 35^\dagger, 38^\dagger, 2^\dagger + 37 = 3^\dagger, 5^\dagger, 27^\dagger,$

$$\begin{aligned}
&2^\dagger + 24 = 13^\dagger, 16^\dagger, 18^\dagger, \\
&4^\dagger + 0 = 4^\dagger, 21^\dagger, 33^\dagger, \quad 4^\dagger + 4 = 17^\dagger, 29^\dagger, 36^\dagger, \quad 4^\dagger + 21 = 12^\dagger, 19^\dagger, 23^\dagger, \\
&\quad 4^\dagger + 33 = 7^\dagger, 11^\dagger, 28^\dagger, \\
&10^\dagger + 0 = 10^\dagger, 20^\dagger, 30^\dagger.
\end{aligned}$$

2.3.7 The conics on the dodecahedron.

Introduction.

The reader may want to skip this section until he has become familiar with conics. In it, we summarize the various types and sub-types of conics as they relate to the representation of the finite projective plane, for $p = 5$, on the dodecahedron. We will see later, IV.1.12. that the dodecahedron can also be used to represent the finite polar and the finite non-Euclidean geometry, for $p = 5$.

Definition.

The conics are all of the same type if the classification into face-points, vertex-points and edge-points is the same. The conics are of the same sub-type if they can be derived from each other using any of the 60 collineations which exchange face-points.

Notation.

In the following Theorem we use the notation

“60 fffvve, 30 C1 (6,9,17;11,29;22), 30 C2 (9,16,17;7,13;15).“

to indicate that we have 60 conics with 3 face-points, 2 vertex-lines and 1 edge-line. These are of the sub-type C1 and C2. An example of a conic of a given sub-type is provided in parenthesis, “;” separates points of a different classification, these points are given in the order, face-point, vertex-point, edge-point, and in the same classification in increasing order. A pictorial representation of the sub-types is given in Figure 2.3.7.

Theorem.

The $31.30.25.16. \frac{6}{6!} = 3100$ conics are of the following type and sub-type.

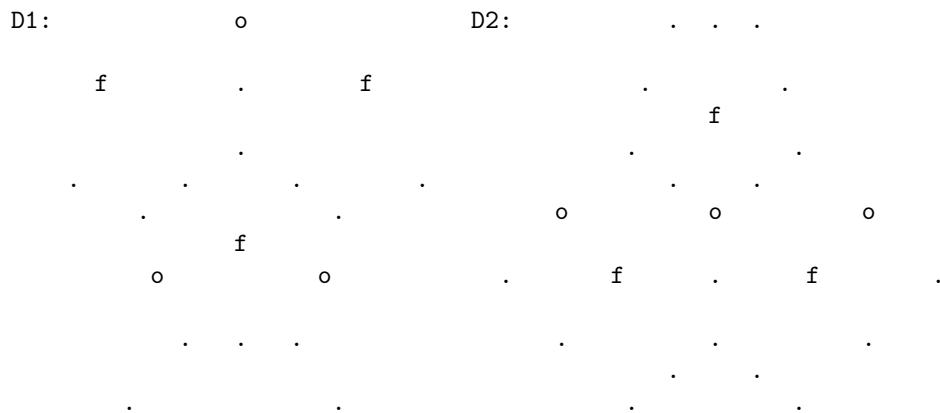
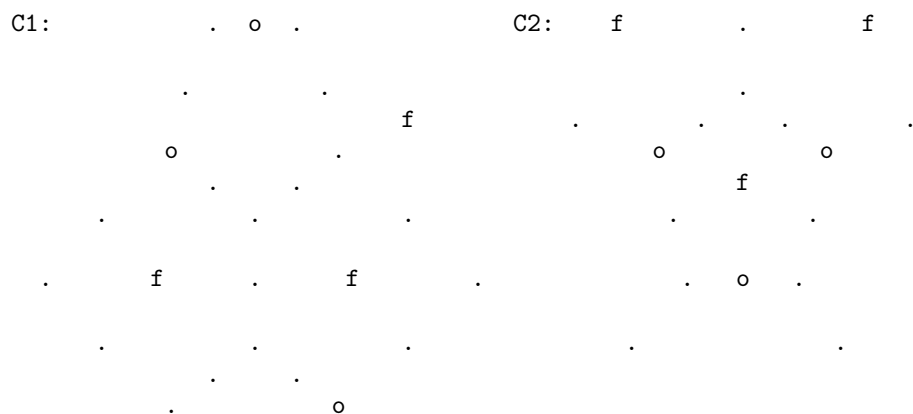
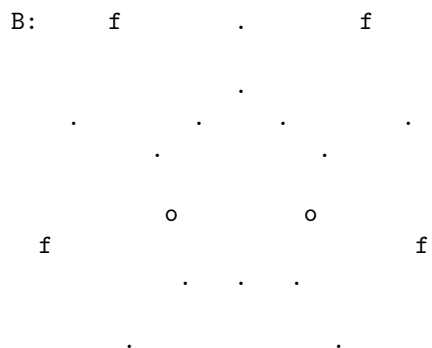
1	<i>ffffff</i> ,	1	<i>A</i>	(0, 4, 6, 9, 16, 17).			
30	<i>ffffee</i> ,	30	<i>B</i>	(6, 9, 16, 17; 2, 22).			
60	<i>fffvve</i> ,	30	<i>C1</i>	(6, 9, 17; 11, 29; 22),	30	<i>C2</i>	(9, 16, 17; 7, 13; 15).
120	<i>fffvvee</i> ,	30	<i>D1</i>	(9, 16, 17; 7; 1, 25),	30	<i>D2</i>	(9, 16, 17; 5; 1, 18),
		30	<i>D3</i>	(0, 4, 6, ; 5; 1, 4),	30	<i>D4</i>	(0, 4, 6; 13; 18, 30).
30	<i>ffvvvv</i> ,	15	<i>E1</i>	(0, 4; 5, 11, 13, 20),	15	<i>E2</i>	(0, 4; 7, 19, 21, 29).
60	<i>ffvvve</i> ,	60	<i>F</i>	(0, 4; 11, 13, 29; 8).			
360	<i>ffvvee</i> ,	30	<i>G1</i>	(0, 4; 11, 20; 1, 14),	30	<i>G2</i>	(0, 4; 5, 13; 3, 30),
		30	<i>G3</i>	(0, 4; 7, 21; 18, 27),	30	<i>G4</i>	(0, 4; 19, 21; 12, 28),
		60	<i>G5</i>	(0, 4; 11, 29; 1, 22),	60	<i>G6</i>	(0, 4; 5, 11; 14, 18),
		60	<i>G7</i>	(0, 4; 21, 29; 1, 27),	60	<i>G8</i>	(0, 4; 5, 21; 2, 27).
180	<i>ffveee</i> ,	30	<i>H1</i>	(0, 4; 11; 8, 22, 25),	30	<i>H2</i>	(0, 4; 13; 8, 15, 22),
		60	<i>H3</i>	(0, 4; 21; 2, 18, 28),	60	<i>H4</i>	(0, 4; 21; 1, 22, 30).
135	<i>ffeeee</i> ,	15	<i>I1</i>	(0, 4; 2, 15, 22, 25),	30	<i>I2</i>	(0, 4; 2, 12, 14, 15),
		30	<i>I3</i>	(0, 4; 15, 18, 22, 30),	60	<i>I4</i>	(0, 4; 1, 15, 25, 30).
12	<i>fvvvvv</i> ,	6	<i>J1</i>	(16; 7, 10, 11, 21, 24),	6	<i>J2</i>	(16; 5, 13, 19, 20, 29).
120	<i>fvvvve</i> ,	60	<i>K1</i>	(16; 5, 10, 13, 19; 27),	60	<i>K2</i>	(6; 5, 7, 10, 11; 26).
300	<i>fvvvee</i> ,	30	<i>L1</i>	(4; 10, 11, 20; 1, 12),	30	<i>L2</i>	(0; 5, 10, 13; 27, 30),
		60	<i>L3</i>	(16; 11, 21, 24; 12, 18),	60	<i>L4</i>	(0; 10, 11, 20; 1, 15),
		60	<i>L5</i>	(0; 7, 10, 21, 3, 22),	60	<i>L6</i>	(0; 5, 11, 13; 12, 26).
480	<i>fvveee</i> ,	30	<i>M1</i>	(9; 11, 21; 2, 14, 28),	30	<i>M2</i>	(0; 10, 20; 25, 28, 30),
		60	<i>M3</i>	(17; 19, 21; 2, 23, 25),	60	<i>M4</i>	(0; 19, 24; 2, 14, 15),
		60	<i>M5</i>	(9; 10, 20; 1, 15, 18),	60	<i>M6</i>	(16; 20, 29; 12, 27, 28),
		60	<i>M7</i>	(9; 7, 29; 8, 12, 30),	60	<i>M8</i>	(16; 24, 21; 1, 12, 26),
		60	<i>M9</i>	(17; 7, 21; 3, 8, 14).			
480	<i>fvveee</i> ,	60	<i>N1</i>	(0; 10; 3, 15, 27, 30),	60	<i>N2</i>	(0; 10; 14, 15, 18, 30),
		60	<i>N3</i>	(0; 10; 12, 14, 22, 30),	60	<i>N4</i>	(0; 13; 1, 23, 27, 30),
		60	<i>N5</i>	(0; 10; 1, 2, 27, 28),	60	<i>N6</i>	(0; 13; 1, 26, 28, 30),
		60	<i>N7</i>	(0; 13; 2, 3, 15, 22),	60	<i>N8</i>	(0; 13, 2, 12, 22, 23).
12	<i>feeeee</i> ,	6	<i>O1</i>	(16; 1, 8, 22, 25, 28),	6	<i>O2</i>	(16; 3, 12, 14, 26, 30).
10	<i>vvvvvv</i> ,	10	<i>P</i>	(5, 7, 10, 11, 21, 29).			
60	<i>vvvvve</i> ,	30	<i>Q1</i>	(10, 11, 20, 29; 15, 27),	30	<i>Q2</i>	(29, 5, 13; 21; 1, 12).
240	<i>vvveee</i> ,	30	<i>R1</i>	(10, 21, 29; 3, 18, 23),	30	<i>R2</i>	(10, 11, 20; 23, 27, 30),
		30	<i>R3</i>	(10, 21, 29; 14, 26, 28),	30	<i>R4</i>	(10, 20, 24; 3, 18, 23),
		60	<i>R5</i>	(10, 21, 29; 3, 25, 28),	60	<i>R6</i>	(11, 13, 29; 1, 8, 15).
270	<i>vvveee</i> ,	15	<i>S1</i>	(11, 20; 3, 18, 27, 30),	15	<i>S2</i>	(11, 20; 2, 15, 22, 25),
		30	<i>S3</i>	(11, 20; 1, 2, 12, 22),	30	<i>S4</i>	(11, 20; 1, 14, 18, 30),
		30	<i>S5</i>	(7, 21; 18, 22, 25, 27),	30	<i>S6</i>	(7, 21; 2, 12, 14, 15),
		30	<i>S7</i>	(7, 21; 3, 12, 14, 30),	30	<i>S8</i>	(7, 21; 8, 12, 14, 26),
		60	<i>S9</i>	(7, 21; 2, 3, 18, 25).			
120	<i>veeeee</i> ,	30	<i>T1</i>	(21; 3, 12, 14, 22, 28),	30	<i>T2</i>	(5; 3, 8, 22, 26, 28).
		60	<i>T3</i>	(24; 3, 12, 14, 22, 27).			
20	<i>eeeeee</i> ,	10	<i>U1</i>	(1, 2, 14, 18, 25, 30),	10	<i>U2</i>	(3, 12, 14, 15, 25, 27).

The proof of the decomposition into types was done using a computer program which took 22 minutes to run on an IBM PC.

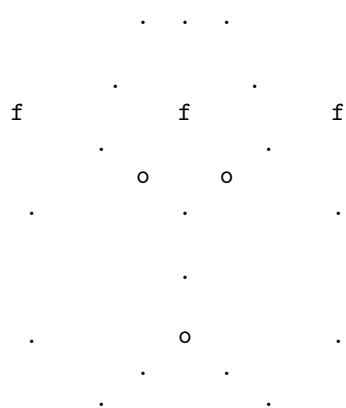
Figure.

The pictorial representation of a conic of a given sub-type on the dodecahedron is as follows.

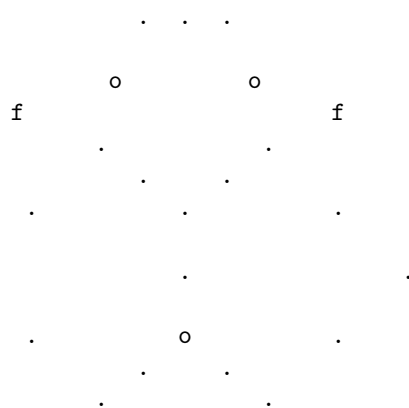
A: the 6 faces.



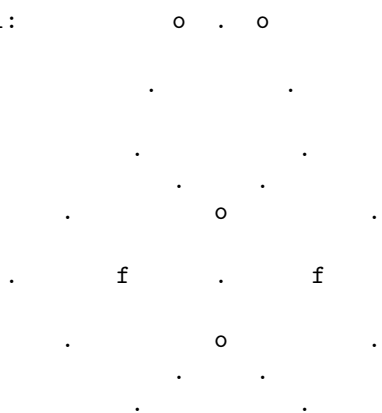
D3:



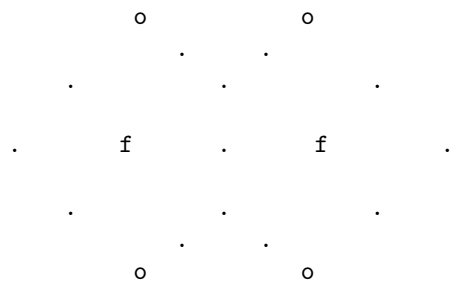
D4:



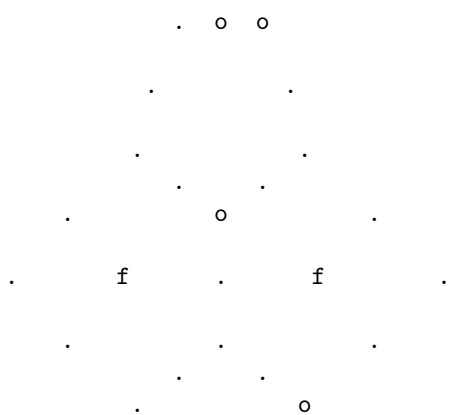
E1:



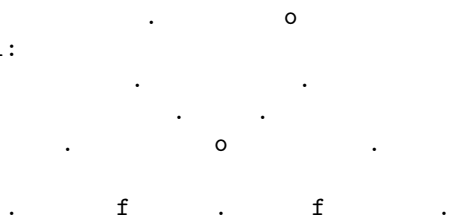
E2:



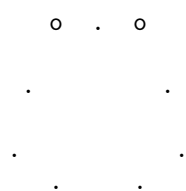
F:

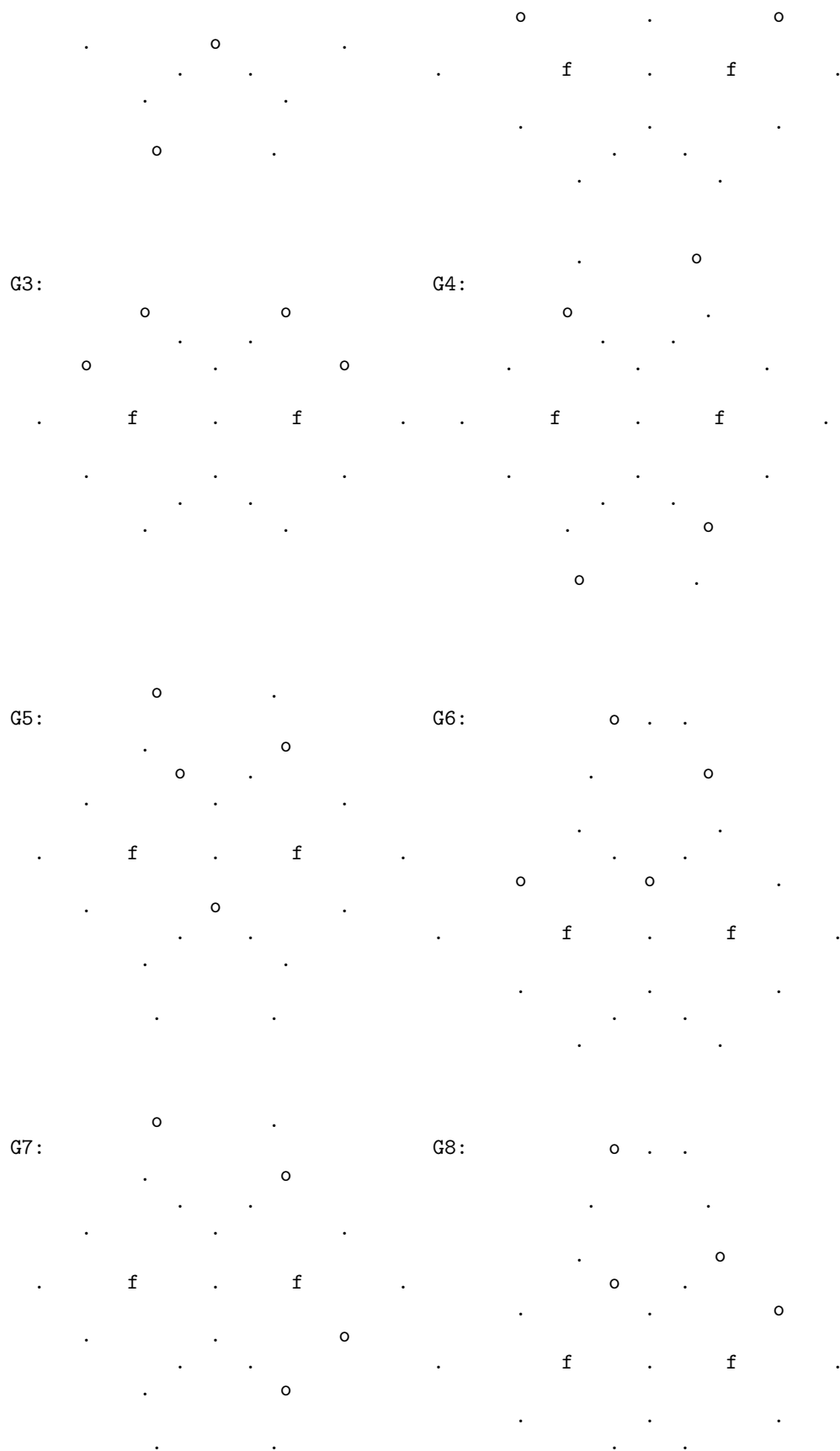


G1:

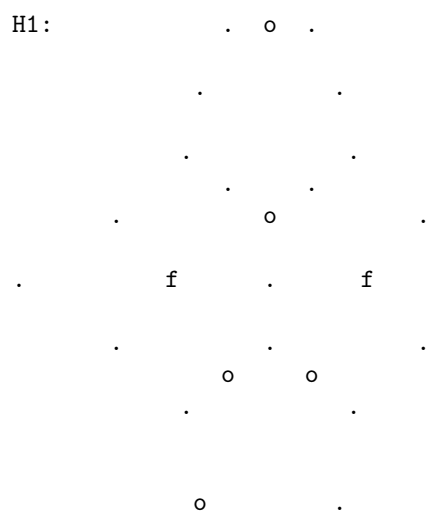


G2:

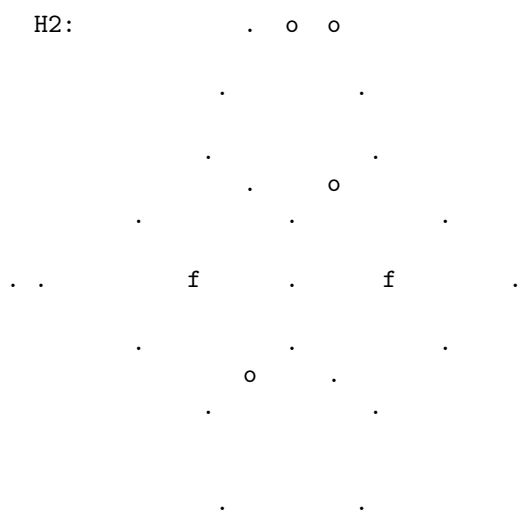




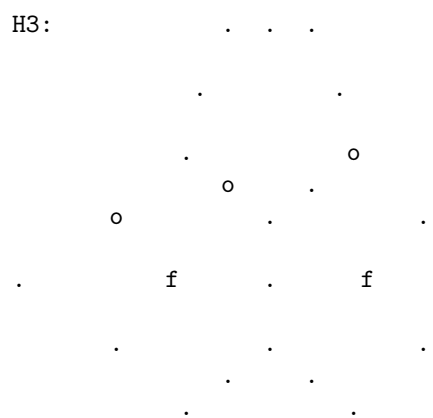
H1:



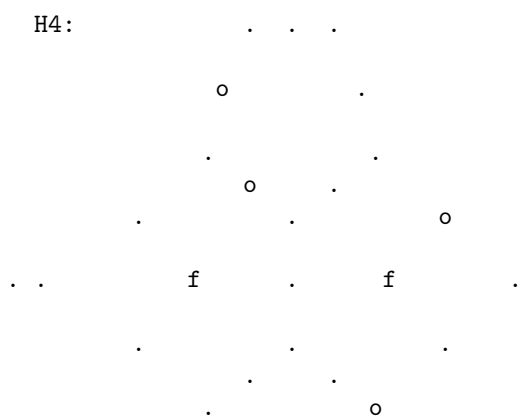
H2:



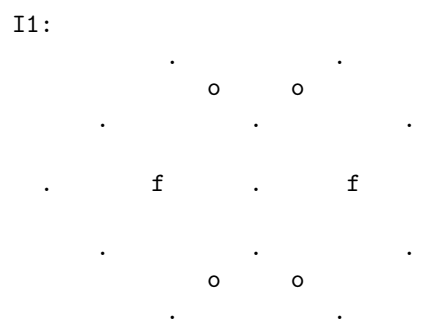
H3:



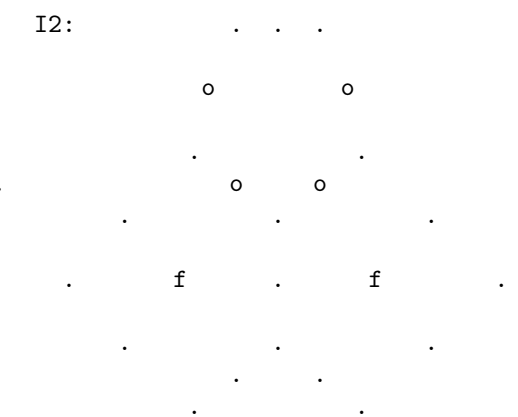
H4:

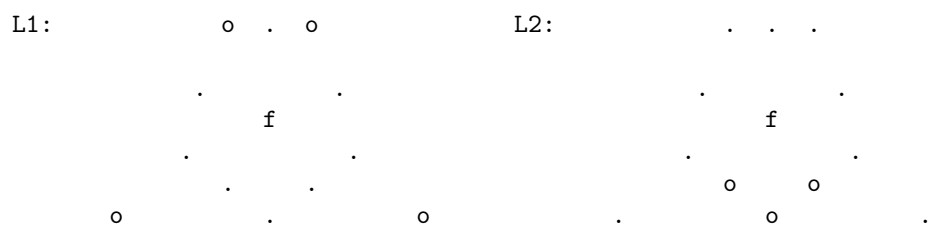
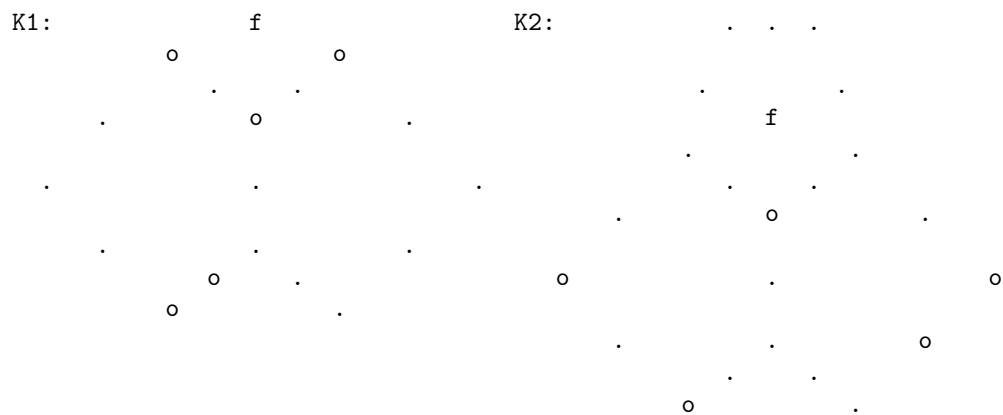
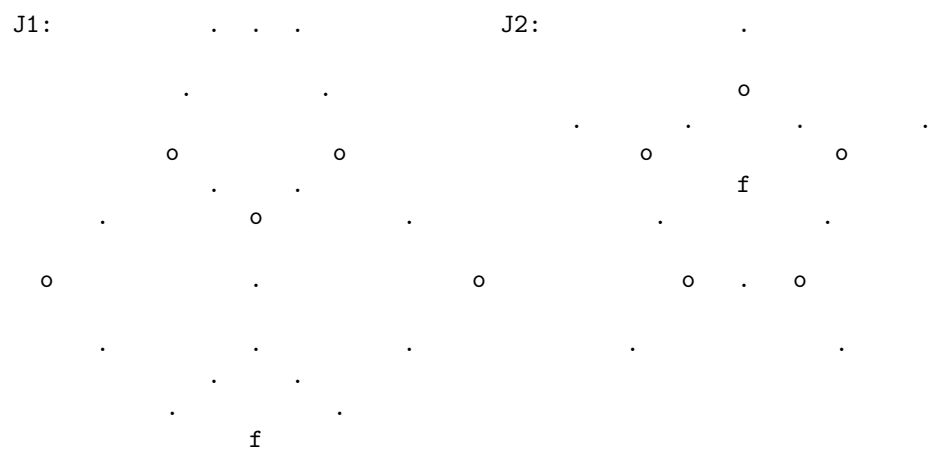
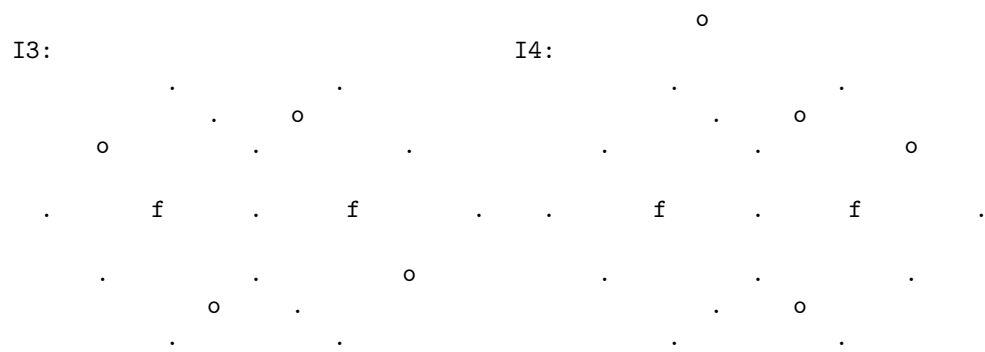


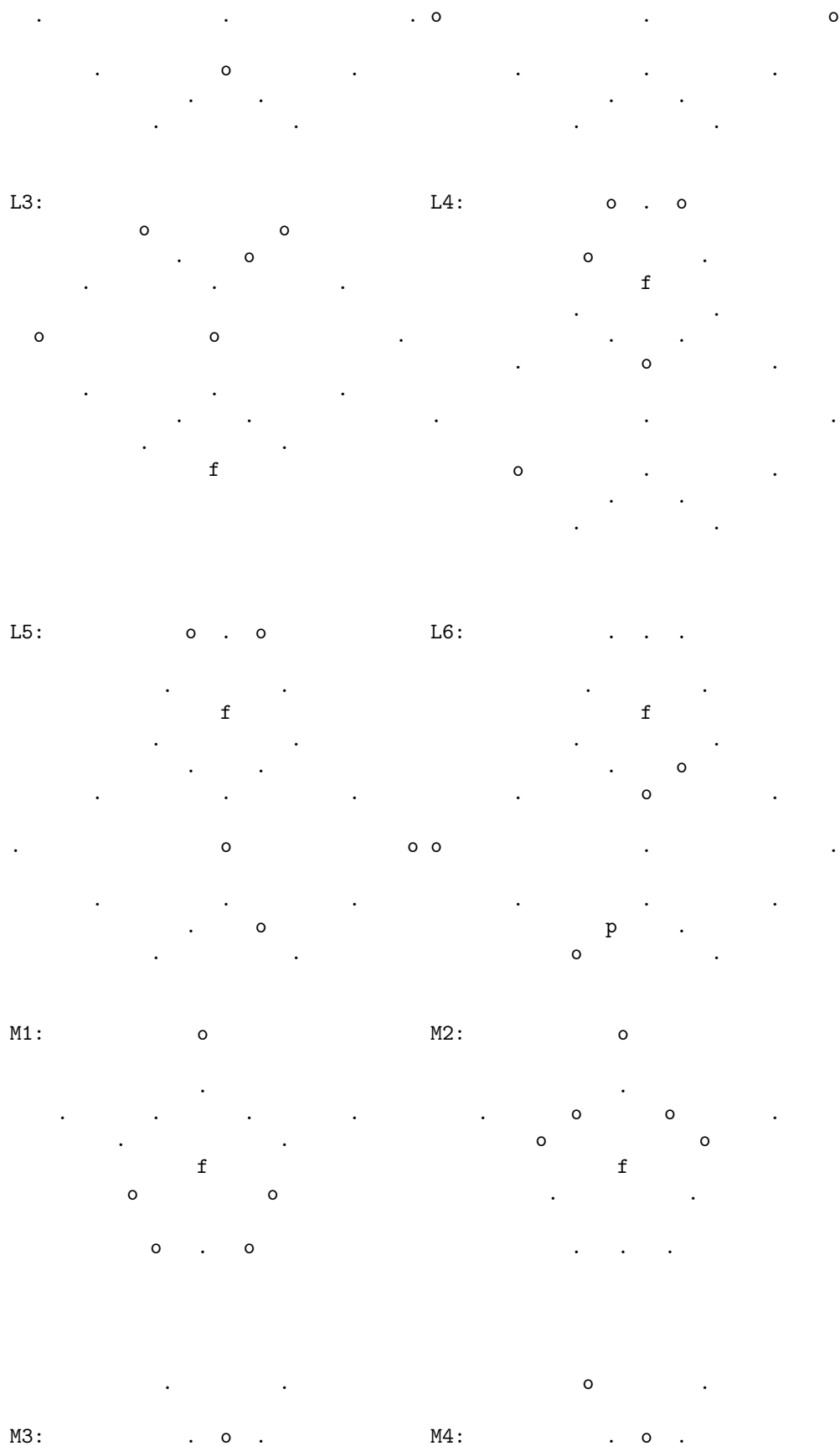
I1:

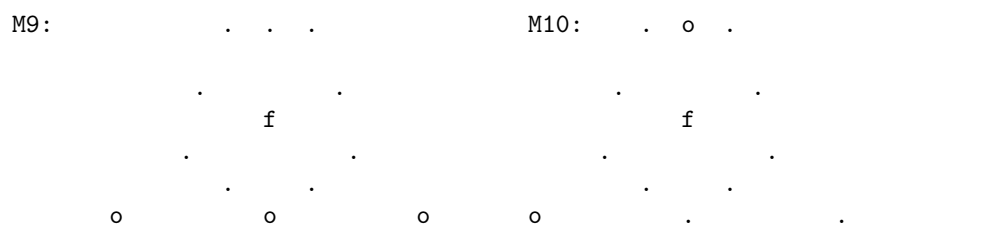
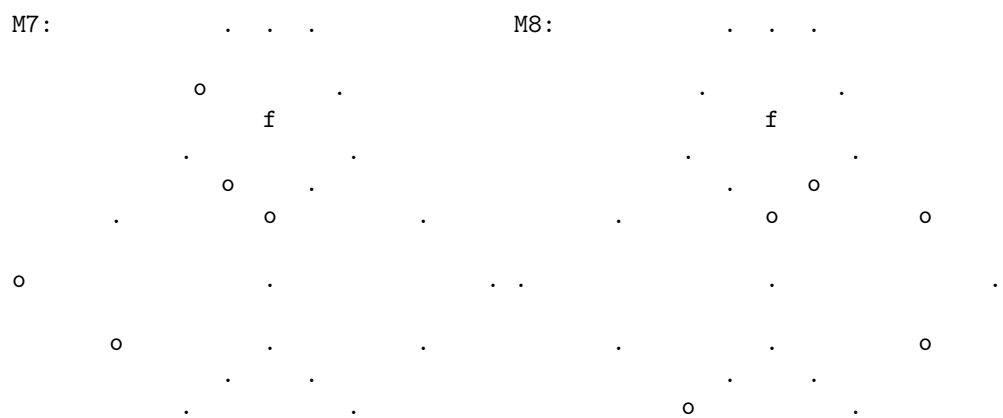
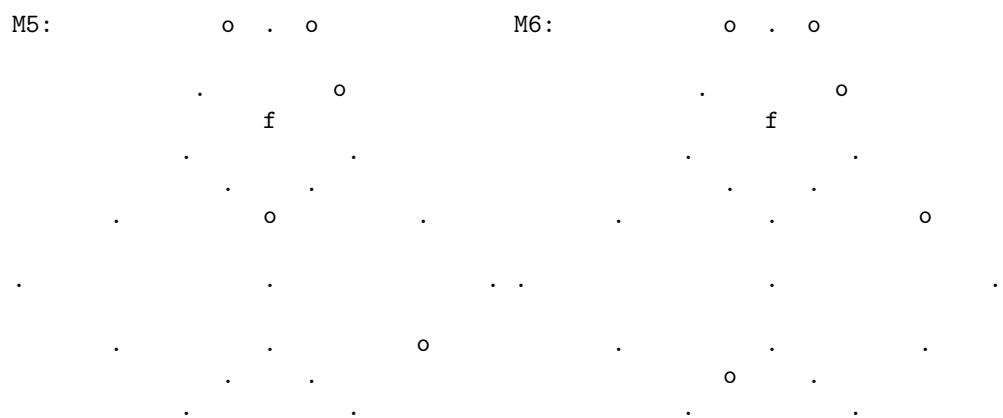
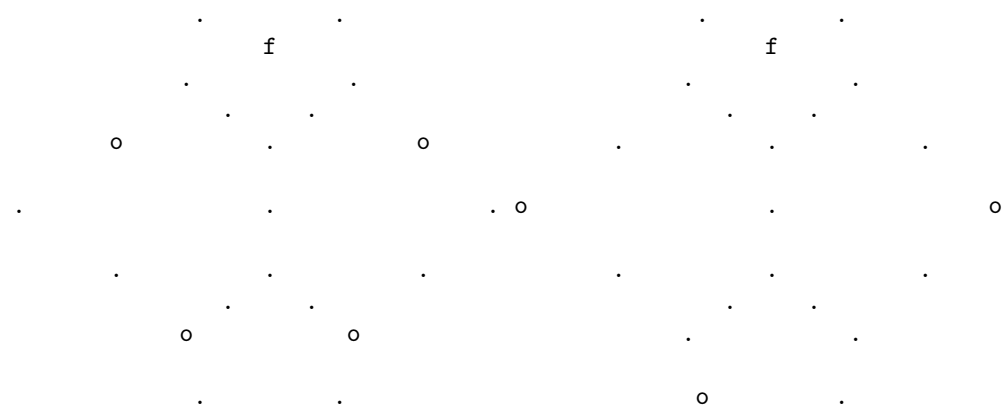


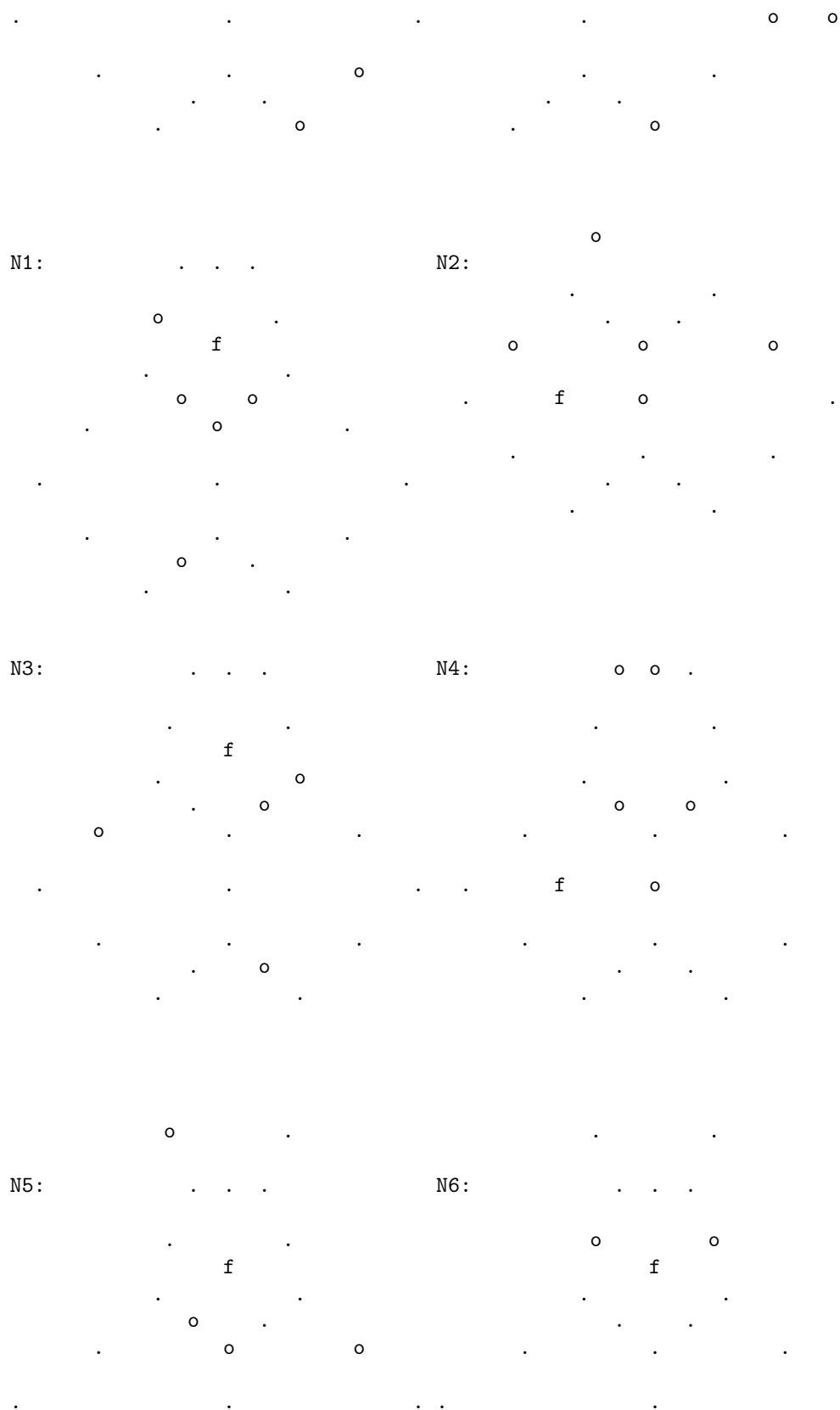
I2:

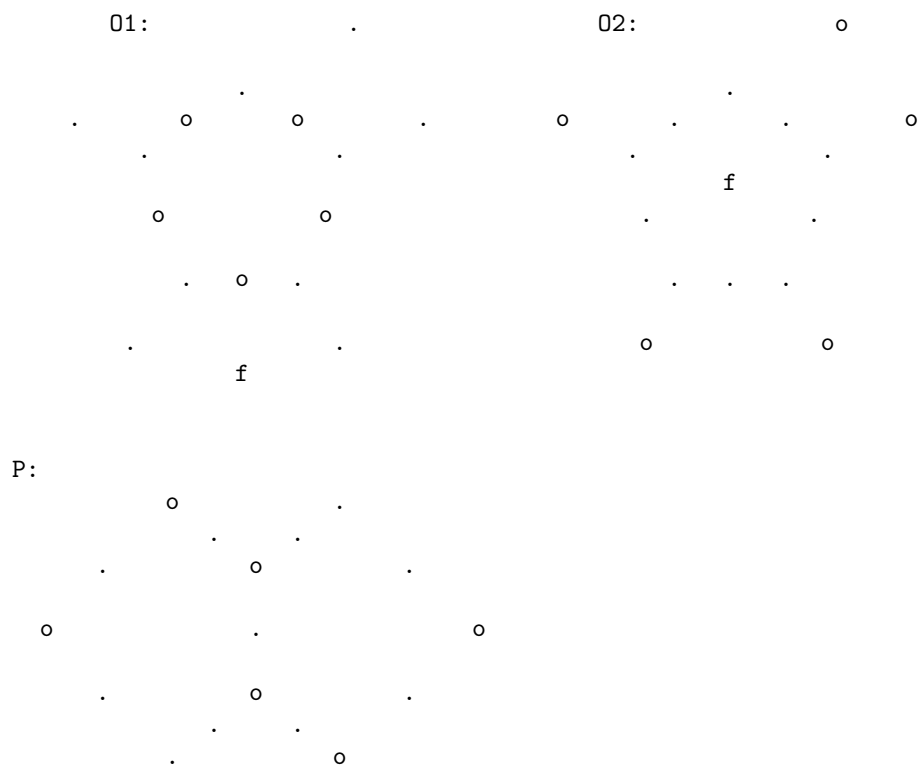
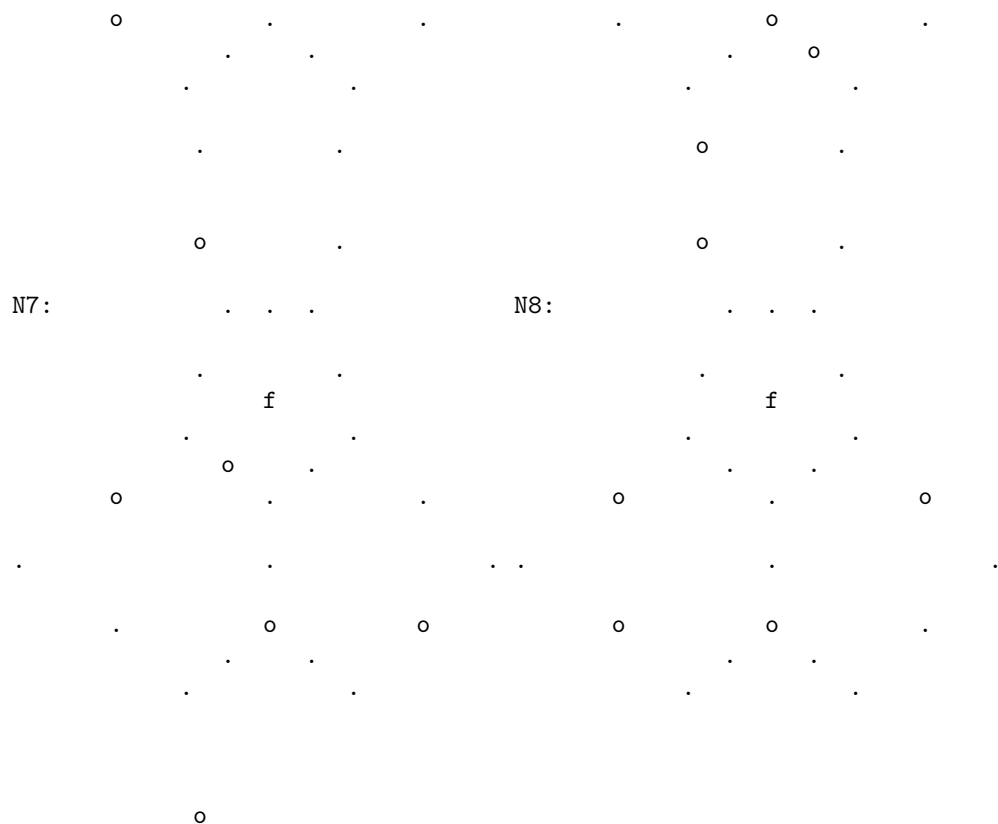




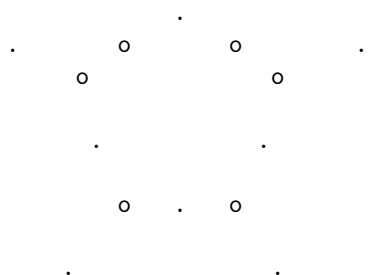




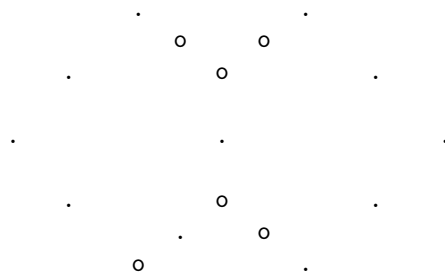




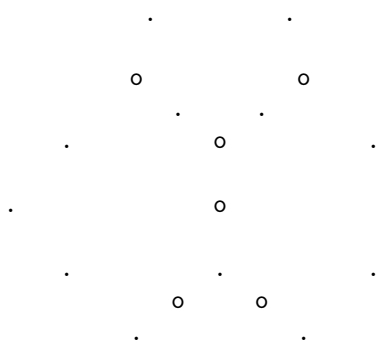
Q1: .



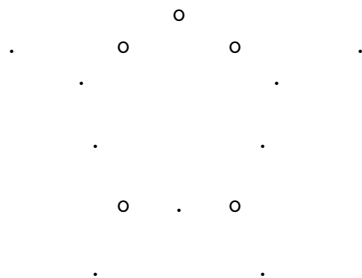
Q2: .



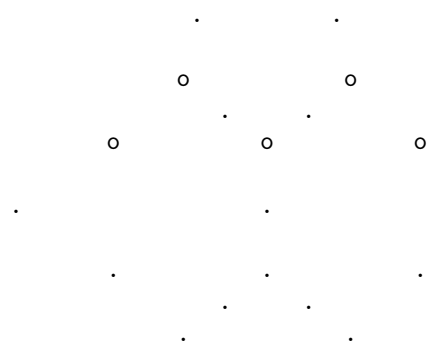
R1: . . .



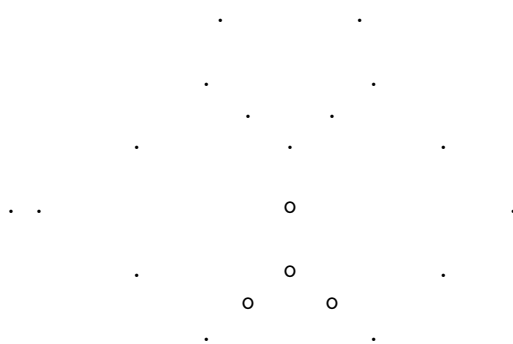
R2: . o



R3: . o .



R4: . o . o

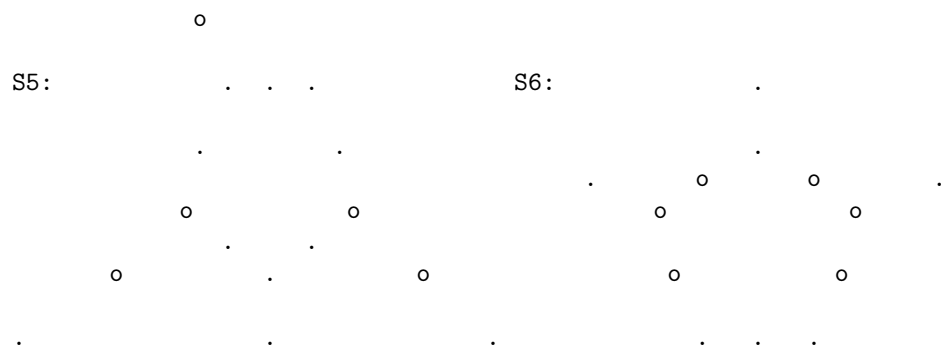
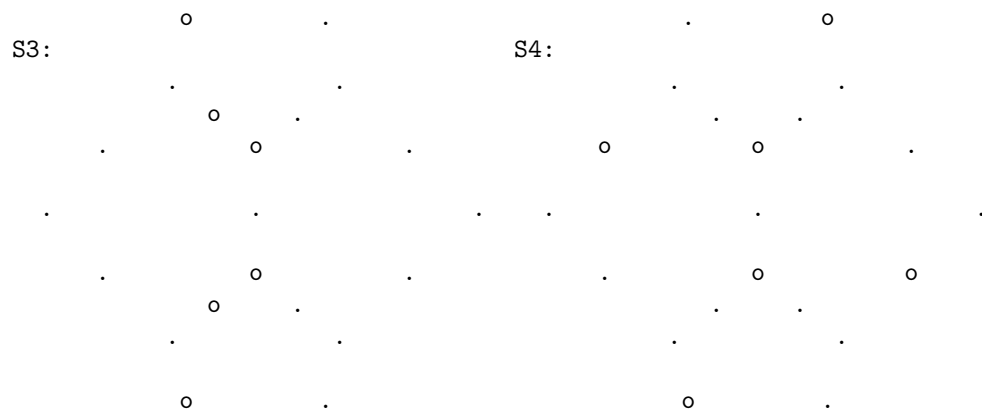
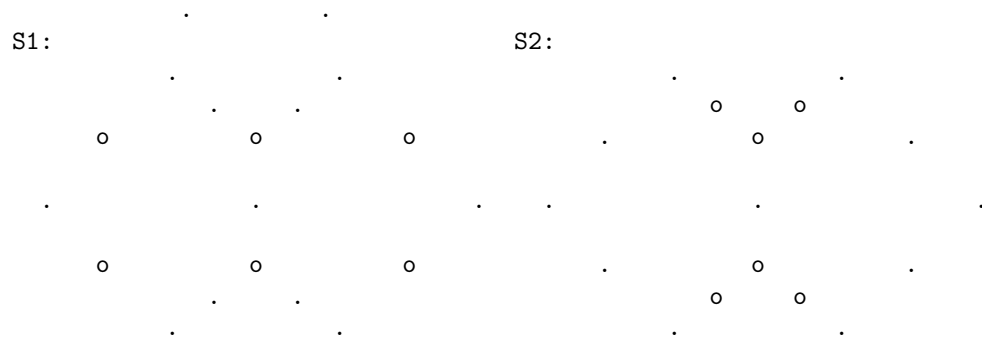
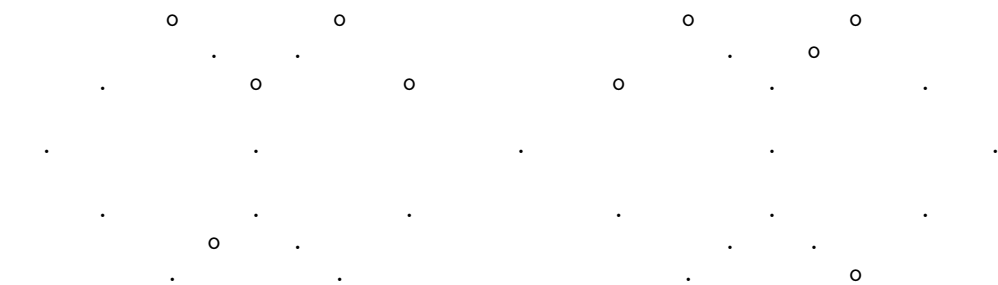


R5: . . .



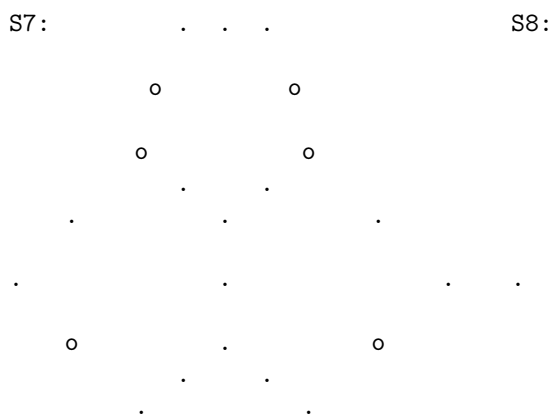
R6: . . .



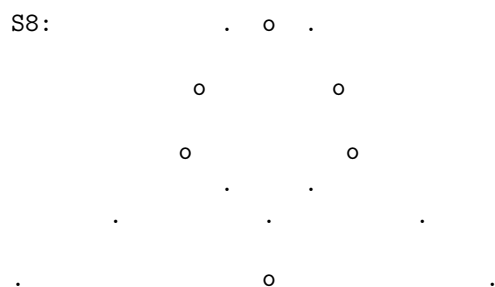




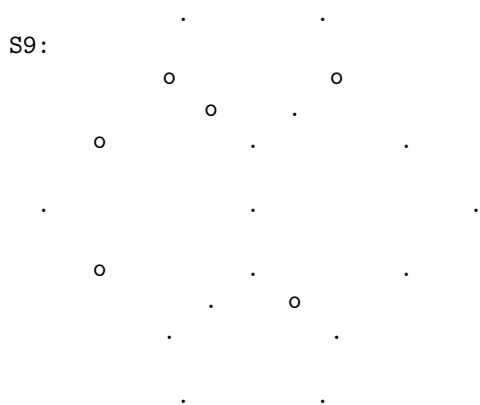
S7:



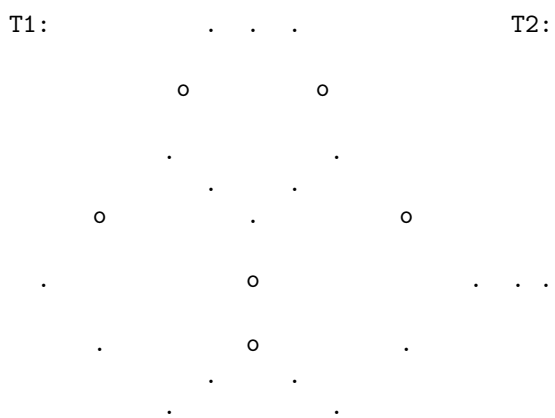
S8:



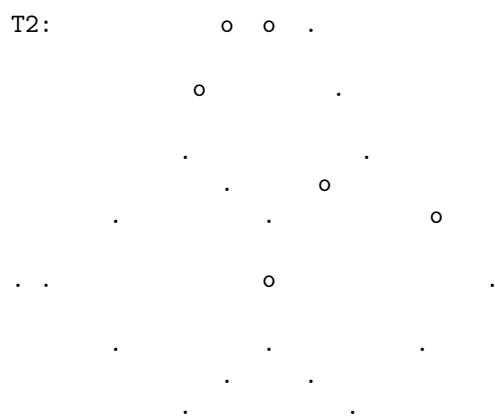
S9:



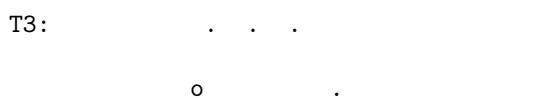
T1:

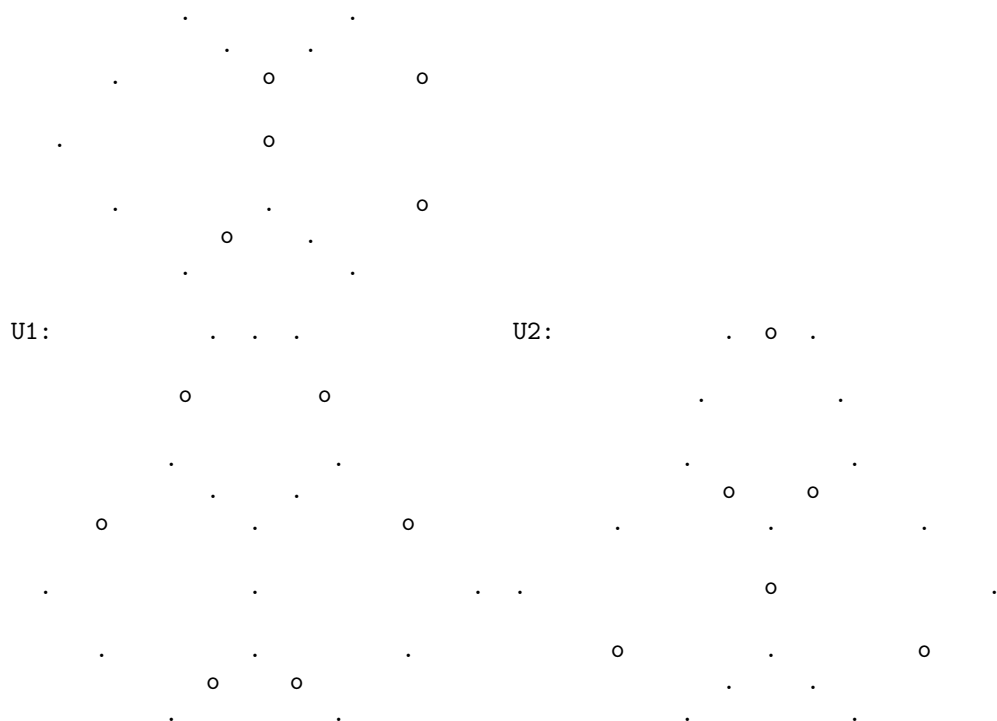


T2:



T3:





The family of types of conics was determined interactively using a computer program.

2.3.8 The truncated dodecahedron.

Introduction.

After defining convex uniform polyhedra, whose notion may go back to Archimedes and were fully studied by Kepler, we will show that one of them, the truncated dodecahedron can be used as a model for the finite projective plane of order 3^2 .

Definition.

A polyhedron with regular faces, in Euclidean 3-space is uniform if it has symmetry operations taking a given vertex into any other vertex, otherwise it is non-uniform. If, in addition, all faces are congruent, the polyhedra is regular.

Theorem. [Euclid]

There are 5 convex regular polyhedra.

Notation. [See Johnson.]

In the following Theorem, we use the following notation, developed by several Mathematicians. $\{n\}$ denotes a regular polygon with n sides, $(n.q.n.q)$ denotes a vertex with adjoining faces successively with n, q, n, q sides, $< n.q >$ denotes an edge adjoining a face with n sides and one with q sides.

Theorem. [Kepler]

Besides regular prisms and antiprisms, there are 13 convex uniform, non-regular polyhedra.

These are	Name	Faces	Vertices	Edges
	<i>Cuboctahedron</i>	$8\{3\}, 6\{4\}$	$12(3.4.3.4)$	$24 < 3.4 >$
	<i>Icosidodecahedron</i>	$20\{3\}, 12\{5\}$	$30(3.5.3.5)$	$60 < 3.5 >$
	<i>Truncated tetrahedron</i>	$4\{3\}, 4\{6\}$	$12(3.6^2)$	$12 < 3.6 >, 6 < 6.6 >$
	<i>Truncated octahedron</i>	$6\{4\}, 8\{6\}$	$24(4.6^2)$	$24 < 4.6 >, 12 < 6.6 >$
	<i>Truncated cube</i>	$8\{3\}, 6\{8\}$	$24(3.8^2)$	$24 < 3.8 >, 12 < 8.8 >$
	<i>Truncated icosahedron</i>	$12\{5\}, 20\{6\}$	$60(5.6^2)$	$60 < 5.6 >, 30 < 6.6 >$
	<i>Truncated dodecahedron</i>	$20\{3\}, 12\{10\}$	$60(3.10^2)$	$60 < 3.10 >, 30 < 10.10 >$
	<i>Rhombicuboctahedron</i>	$8\{3\}, 18\{4\}$	$24(3.4^3)$	$24 < 3.4 >, 24 < 4.4 >$
	<i>Rhombicosidodecahedron</i>	$20\{3\}, 30\{4\},$ $12\{5\}$	$60(3.4.5.4)$	$60 < 3.4 >, 60 < 4.5 >$
	<i>Truncated cuboctahedron</i>	$12\{4\}, 8\{6\},$ $6\{8\}$	$48(4.6.8)$	$24 < 4.6 >, 24 < 4.8 >,$ $24 < 6.8 >$
	<i>Truncated</i> <i>icosidodecahedron</i>	$30\{4\}, 20\{6\},$ $12\{10\}$	$120(4.6.10)$	$60 < 4.6 >, 60 < 4.10 >,$ $60 < 6.10 >$
	<i>Snubcuboctahedron</i>	$32\{3\}, 6\{4\}$	$24(3^4.4)$	$36 < 3.3 >, 24 < 3.4 >$
	<i>Snubicosidodecahedron</i>	$80\{3\}, 12\{5\}$	$60(3^4.5)$	$90 < 3.3 >, 60 < 3.5 >$
	<i>n-gonal prism</i>	$n\{4\}, 2\{n\}$	$2n(4^2.n)$	$n < 4.4 >, 2n < 4.n >$
	<i>n-gonal antiprism</i>	$2n\{3\}, 2\{n\}$	$2n(3^3.n)$	$2n < 3.3 >, 2n < 3.n >$

Theorem. [N. W. Johnson]

There are 92 convex non-uniform regular-faced polyhedra.

The fact that all vertices are of the same type does not insure uniformity, as the example of the elongated square gyrobicupola of J. C. P. Miller shows. This non-uniform polyhedra has the same characteristics as the rhombicuboctahedron, but has the part below the 8 squares turned 45 degrees.

Before discussing the truncated dodecahedron as a model for the Pappian plane associated with 3^2 , I will discuss the pentagonal antiprism as a model for the Pappian plane associated with 2^2 .

Notation.

I identify elements which are symmetrical with respect to the center of the antiprism. For the pentagonal antiprism, with $i = 0, 1, 2, 3, 4$, I will denote by t_i , the 5 triangular faces, by v_i , the 5 vertices, by e_i , the 5 pentagonal-triangular edges, by f_i , the 5 triangular-triangular edges and by p , pentagonal face. We have altogether 21 elements to represents the 21 points in the plane associated with 2^2 .

Theorem.

For $q = 2^2$,

0. The selector is $\{0, 1, 4, 14, 16\}$.

1. The corresponding selector function f is, and the representation of the points on the antiprism are

i	0	1	2	3	4	5	6	7	8	9	10
$f(i)$	0	0	14	1	0	16	16	14	14	16	4
<i>repr. of points</i>	v_2	e_2	v_4	f_3	f_2	t_3	t_1	v_0	v_1	e_0	e_3
<i>repr. of lines</i>	v_2	t_2	v_4	f_3	f_2	e_3	e_1	v_0	v_1	t_0	t_3
i	11	12	13	14	15	16	17	18	19	20	
$f(i)$	14	4	1	0	1	0	4	4	16	1	
<i>repr. of points</i>	v_3	f_4	f_1	p	t_0	t_2	e_1	f_0	e_4	t_4	
<i>repr. of lines</i>	v_3	f_4	f_1	p	e_0	e_2	t_1	f_0	t_4	e_4	

2. The incidence properties are

$$\begin{aligned}
&e_i^* \iota v_i, e_{i\pm 2}, t_{i\pm 1}, \\
&t_i^* \iota v_i, t_{i\pm 2}, f_{i\pm 1}, \\
&f_i^* \iota v_i, e_{i\pm 1}, f_{i\pm 1}, \\
&v_i^* \iota p, v_i, e_i, t_i, f_i, \\
&p \iota v_i.
\end{aligned}$$

Proof: I leave as an exercise the determination of the fundamental polynomial and the corresponding selector.

The selector function follows easily from its definition.

The selector polarity which associates i to i^* has the fixed points 7,8,11,0 and 2 on the line 14*. I will associates to 14 and to 14* the pentagonal face and its incident points or lines to v_i . Starting from that, one of the possible solution is given in 1. Notice that I use the same correspondance between e_i , v_i and f_i for the points and the lines but exchange t_i and e_i to get the corresponding points and lines.

Figure.

The corresponding drawing for the Projective plane over 2^2 is given page

Notation.

For the truncated dodecahedron, I will denote by t , a triangular face, by d , a decagonal face, by v , a vertex, by e , a $< 10, 10 >$ edge and by u , a $< 3.10 >$ edge. The lower case notation is used indifferently for points and lines, the upper case notation for points.

Lemma.

If x_Y denotes the number of points of type Y incident to a line of type x , then

$$2|f_Y, 5|d_Y, 3|t_Y \text{ for } Y \neq T, 3|t_T - 1.$$

Proof: For instance, there are 10 T -points, each is adjacent to 10 lines; on the other hand, the 30 e -lines are adjacent to 30 e_T triangles, the 15 f -lines are adjacent to 15 f_T triangular-points, This implies

$$30e_T + 15f_T + 30v_T + 10t_T + 6d_T = 100, \text{ which gives, modulo 2, } f_T = 0, \text{ modulo 5, } d_T = 0, \text{ modulo 3, } t_T = 1.$$

Theorem.

For $q = 3^2$, a primitive polynomial is

0. $I^3 - I - \epsilon$,

with $\epsilon = 1 + \alpha$, an 8-th root of unity and $\alpha^2 = -1$.

The powers of ϵ are $1, 1 + \alpha, -\alpha, 1 - \alpha, -1, -1 - \alpha, \alpha, -1 + \alpha$.

The corresponding selector is

1. $\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\}$.

The corresponding selector function is

2.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
	0	1	0	77	56	3	49	1	0	81	81	49	81	77	77	61	77	9	81	61	56	27	77
t	e	e	e	d	e	e	v	v	v	v	e	u	u	e	v	e	u	v	u	u	v	e	u
0	1	2	56	57	24	21	54	48	9	10	66	65	19	30	16	15	39	18	13	23	6	32	20
24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	
	3	56	1	0	49	27	61	61	49	61	27	56	56	81	56	61	9	77	49	49	56	49	3
v	u	u	v	t	u	v	v	v	v	v	v	u	u	u	u	u	v	v	u	v	e	t	
5	89	80	49	50	69	14	63	22	41	45	88	58	87	74	17	85	33	64	73	53	34	84	
47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	
	9	1	0	27	49	9	3	27	1	0	61	3	81	1	0	56	77	27	27	81	27	9	49
t	v	v	t	u	u	v	v	d	v	u	u	t	u	v	u	e	v	u	v	u	v	u	
47	8	27	28	67	83	44	7	60	3	4	36	59	55	77	78	31	42	12	11	51	72	29	
70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90			
	77	81	9	27	3	77	1	0	3	61	1	0	9	9	56	9	61	81	3	3	1		
t	v	e	u	u	d	t	e	d	u	d	v	v	u	t	u	t	u	e	d	e			
86	71	68	43	38	79	76	61	62	75	26	81	82	52	46	40	70	37	35	25	90			

3. $\{0, 46, 47, 50, 59, 70, 28, 76, 84, 86\}$.

The letters refer to the type. The last row gives the conjugate, for instance, 61 is the conjugate of 77.

Proof: To retrieve the primitive polynomial associated with S , the selector 1, because $3 \in S$, $I^3 = \beta I + \gamma$, β and γ are chosen in such a way that I^{56} has no term of second degree. The computations are facilitated by preparing first a table giving $g(i) \ni$

$$1 + \epsilon^i = \epsilon^{g(i)}, \quad 0 \leq i \leq t,$$

and by use of the convention $\epsilon^{-1} = 0$.

The conjugates are obtained when α is replaced by $-\alpha$.

Heuristics.

The truncated dodecahedron has 182 faces, vertices and edges. using symmetry with respect to the center we expect that a model can be found for the projective geometry of order 3^2 , with 91 points and with 10 points on each line . We will solve simultaneously the following problems, discover appropriate incidence properties, associate to the vertices, integers from 0 to 90 to take advantage of the selector and determine a fundamental projectivity on a line

to prepare for a representation of finite Euclidean geometry. I will describe here some of the steps which have led me to the solution given in 2.3.8 to 2.3.8.

The auto-correlates should be the points of a conic γ . I will choose this conic as a circle in the corresponding Euclidean plane. The intersection of the lines $0 \times 70 = 77^*$ and of $46 \times 28 = 72^*$, which is 75, is chosen as the center of the circle. The points on the polar 75^* are 2, 6, 16, 17, 19, 25, 43, 65, 72, 77.

To obtain a fundamental projectivity, we want to choose 2 points, A, B , on the circle and project from them any point X on the circle onto 75^* , giving X_A and X_B , X_A corresponds to X_B , we want to choose A and B such that the projectivity is of order 10. A trial gave a projectivity of order 5, it was then easy to obtain one of order 10 using $A = 0$ and $B = 50$. The computations start as follows: $0 \times 0 = 0^* \times 75^* = 77 \times 0 = 0^*$ with 0 as the other point on γ .

$50 \times 0 = 27^* \times 75^* = 65 \times 0 = 27^*$ with 50 as the other point on γ .

$50 \times 50 = 50^* \times 75^* = 6 \times 0 = 3^*$ with 46 as the other point on γ .

$50 \times 46 = 31^* \times 75^* = 25 \times 0 = 56^*$ with 84 as the other point on γ .

... . Hence the projectivity 2.3.8 and the equidistant points 0, 50, 46, 84, 47, 70, 86, 28, 76, 59 on γ .

With one d -face chosen as 75^* , the 10 t -faces are subdivided into 2 sets, those adjacent to the d -face and those which are not. The vertices of the pentagonal points 0, 46, 47, 86, 76 are chosen for the successive triangles adjacent to the d -face. The diametrically opposite point, e. g. 70 of 0 is chosen for the triangle not adjacent to the d -face but adjacent to the triangle 0.

Because $0 \times 46 = 3$, $46 \times 47 = 45$, ... , $0 \times 70 = 77$, $50 \times 86 = 6$, I chose the pentagonal side 3 for the e -point between the t -points 0 and 46, ... , the diameter 77 for the e -point between the t -points 0 and 70, Because $5|75^*$, we chose these 10 e -points as incident to 75^* .

These consideration suggest Definition 2.3.8 and Theorems 2.3.8 and 2.3.8.

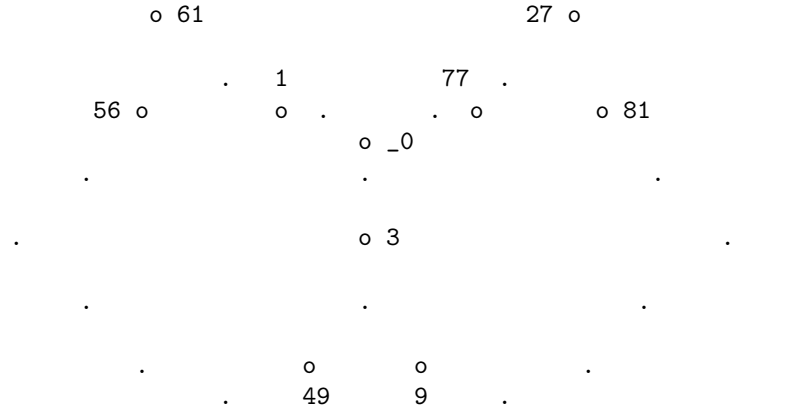
Definition.

The points in the truncated dodecahedron model consist of

0. The 10 triangular face-points T .
1. The 6 decagonal face-points D .
2. The 30 vertex-points V .
3. The 30 triangular-decagonal edge-points U .
4. The 15 decagonal-decagonal edge-points E .

The lines in the truncated dodecahedron model consist of

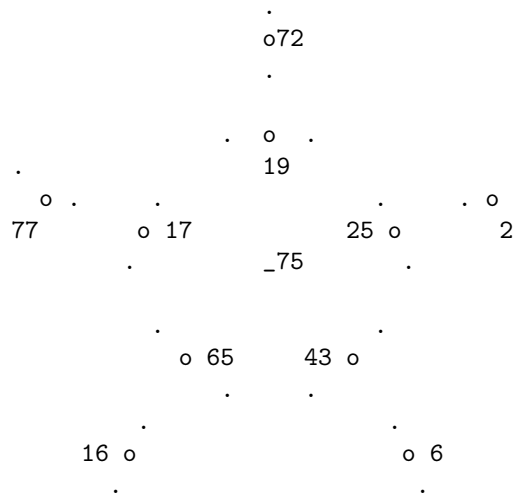
0. The 10 triangular face-lines t . Each is incident to itself as a point, to the 3 adjacent $< 12.12 >$ edge-points E , and to the 6 vertex-points V which are the vertices of the triangle adjacent to the 3 edge-points which are not themselves adjacent to these points. For instance, for $t = 0$, the incident points are $0(T), 1(E), 77(E), 3(E), 56(V), 61(V), 27(V), 81(V), 9(V), 49(V)$:



1. The 6 decagonal face-lines d . Each is incident to its 5 $< 3.12 >$ edges U , and the 5 $< 12.12 >$ edges E adjacent to its 5 adjacent triangles.

For instance 75(d) is incident to

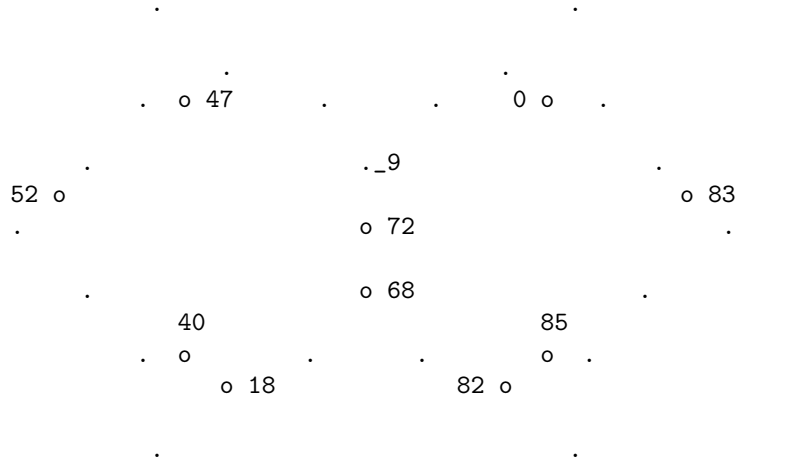
25(U), 43(U), 65(U), 17(U), 19(U) and 2(E), 6(E), 16(E), 77(E), 72(E) :



2. The 30 vertex-lines v . Each is incident to the $< 12.12 >$ edge E_0 adjacent to it and to the vertex at the other end of it, to the 2 triangular points T_1 and T_2 adjacent to the other edges E_1 and E_2 , to the 2 $< 12.12 >$ edges E_3 and E_4 opposite to E_1 or E_2 belonging to the same decagon as v , to the vertices adjacent to E_3 or E_4 closest to v , to the $< 3.12 >$ edges U belonging to the same decagon as T_1 or T_2 and the triangle opposite E_0 .

For instance, 9(v) is adjacent to

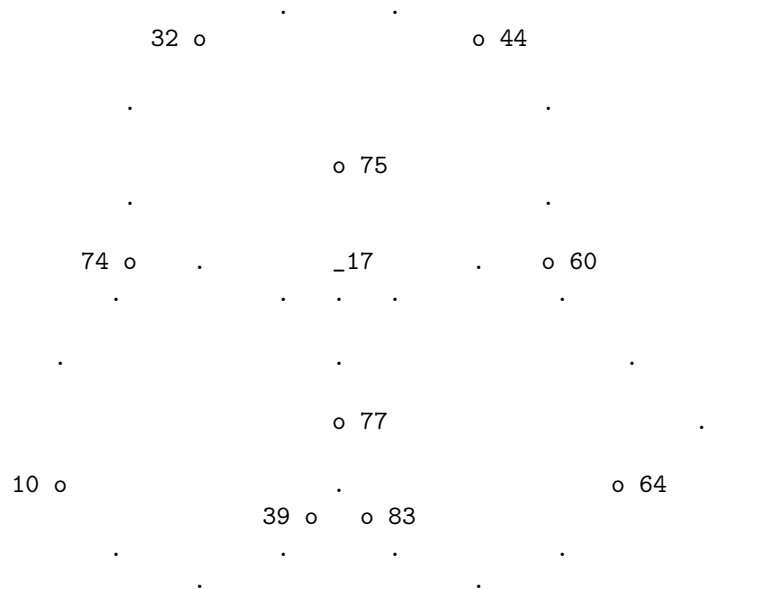
72(E), 68(V), 0(T), 47(T), 85(E), 40(E), 82(V), 40(V), 83(U), 52(U) :



3. The 30 triangular-decagonal edge-lines u . Each is incident to the adjacent decagonal point D_0 , to the $\langle 12.12 \rangle$ edge E_0 adjacent to the triangle adjacent to u and to the $\langle 3.12 \rangle$ edges U adjacent to E_0 , to the vertices in the same decagons D_1 and D_2 as E_0 opposite the vertex adjacent to E_0 and the same triangle as u , and to the $\langle 3.12 \rangle$ edges U_1 and U_2 adjacent to the triangle adjacent to D_0 and D_1 or D_2 not adjacent to these decagons and to the vertices adjacent to D_0 and the $\langle 12.12 \rangle$ edges of D_0 adjacent to U_1 or U_2 .

For instance, $17(t)$ is adjacent to

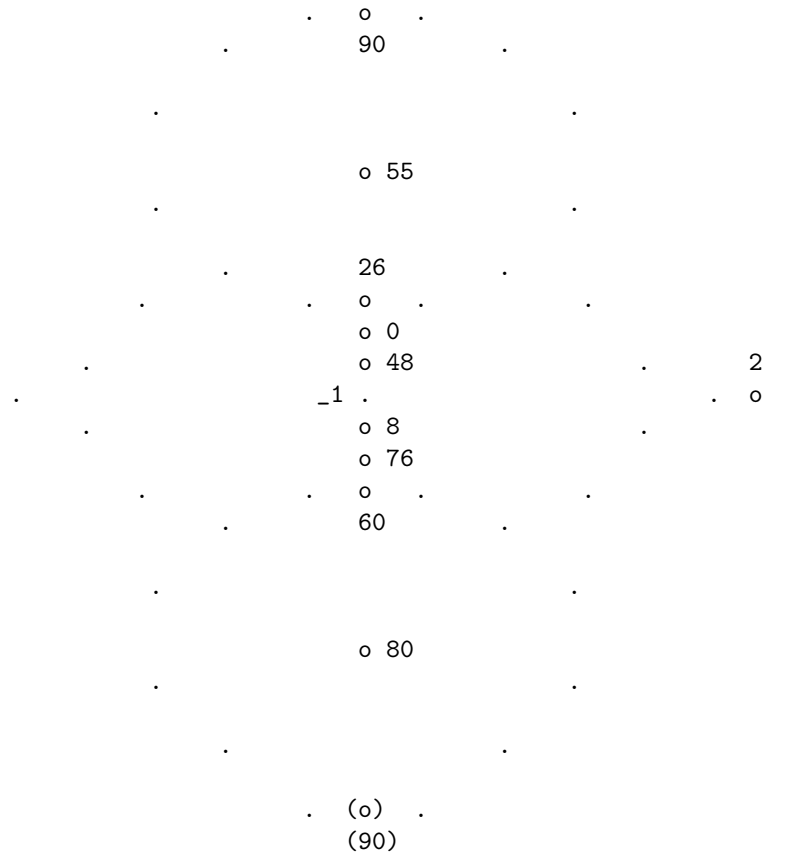
$75(D), 77(E), 83(T), 39(\bar{T}), 64(V), 10(V), 60(U), 74(U), 44(V), 32(V)$:



4. The 15 decagonal-decagonal edge-lines e . Each is incident to the 2 decagonal points, the 2 triangular points, the 2 $\langle 3.12 \rangle$ edges, the 2 vertices, the $\langle 12.12 \rangle$ edge, whose center in the the equatorial plane through e and the $\langle 12.12 \rangle$ edge perpendicular to that plane.

For instance, $1(e)$ is incident to

$55(D), 80(D), 0(T), 76(T), 26(U), 60(U), 48(V), 8(V), 90(E), 2(E)$:

**Theorem.**

The truncated docecahedron model satisfies the axioms 2.1.2 for $q = 3^2$.

Figure.

The corresponding drawing for the Projective plane over 3^2 is given page

Theorem.

A fundamental projectivity on line 75* is
 (77, 65, 6, 25, 72, 17, 16, 43, 2, 19).

The elements are alternately of type v and u .

Exercise.

Given the selector function f of 2.3.8 and the 6 dodecagonal faces, 4, 55, 75, 78, 80, 89, reconstruct the preceding figure using the following rules, which are first exemplified,

0. $4(D) \times 89(D) = 5*(e)$, 5 is the decagonal-decagonal edge line which is in the equatorial plane through the center of the decagons 4 and 89.

1. $1(E) \times 80(D) = 60 * (u)$, 1 must be adjacent to a triangular face $76(T)$ adjacent to the decagon 80, 60 is then the triangular decagonal edge line adjacent to 76 and 80.
2. $1(E) \times 3(E) = 0 * (t)$, 1 and 3 must be adjacent to the same triangular face $0(T)$, 0 is that face.
3. $0(T) \times 5(E) = 56 * (v)$, 0 must be adjacent to a decagonal-decagonal edge line $1(D)$ which must be adjacent to a triangular face $76(T)$ adjacent to the edge 5, 56 is the vertex adjacent to the latter 2.

The integers of the second member follow from the selector function for instance $5 = f(89 - 4) - 4$.

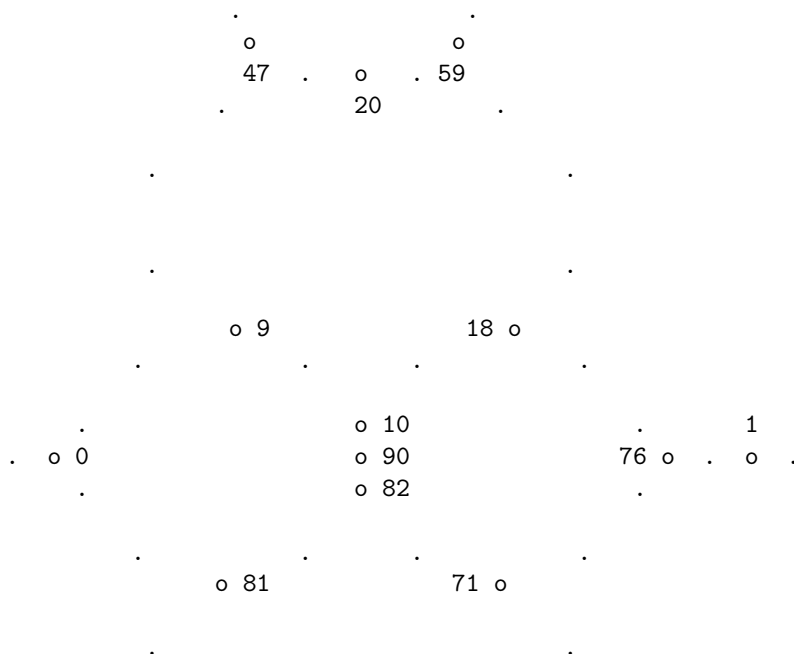
The above rules are clearly redundant.

Determine alternate rules, for instance the rule corresponding to 2 triangular faces or 2 vertices adjacent to the same decagonal-decagonal edge. Slightly more ambitious is to dermine all the possible rules.

Theorem.

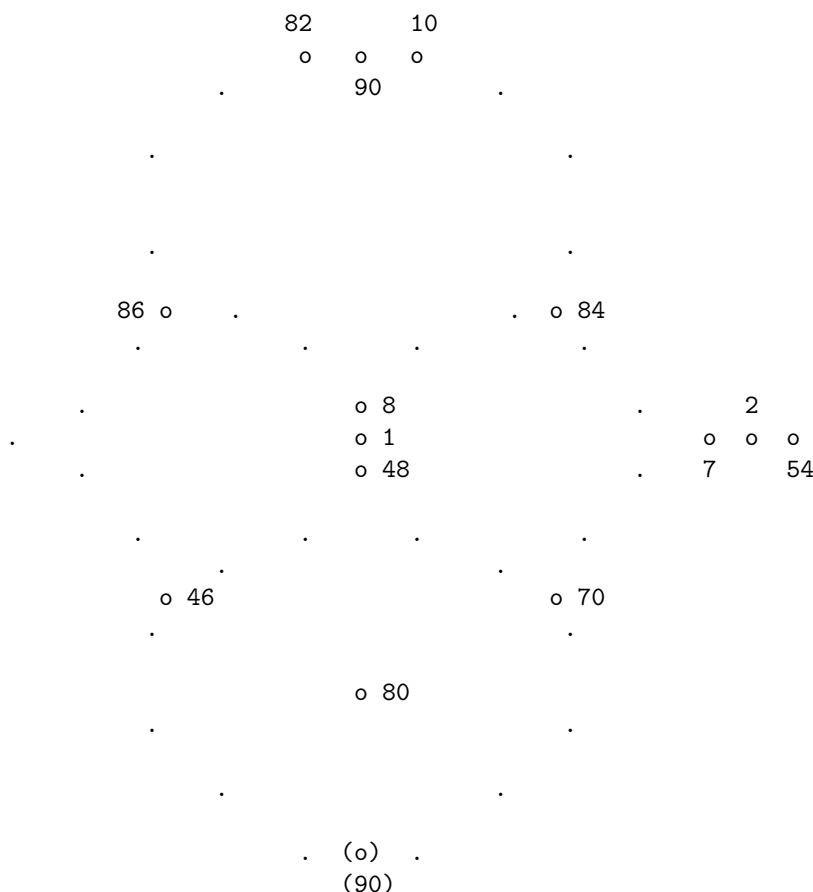
There are several configurations which represent a projective plane of order 3. The quadrangle consists of 4 triangular face-points, the diagonal points, of 3 decagonal-decagonal edge-points, the quadrilateral, of 6 vertex-points. All the other points on the truncated dodecahedron represent complex points, 6 on each of the 13 lines.

The first example is associated with the primitive polynomial 2.3.8.0.



The conjugates are given in table 2.3.8.2.

A second example is as follows



on the t -line 70^8 , the conjugates are $21(V)$ and $11(E)$, $22(E)$ and $77(E)$, $24(V)$ and $30(V)$.

on the e -line 1^* , the conjugates are $0(T)$ and $76(T)$, $26(U)$ and $60(U)$, $55(D)$ and $80(D)$.

on the v -line 8^* , the conjugates are $41(V)$ and $83(U)$, $53(V)$ and $73(U)$, $19(U)$ and $69(U)$.

Proof: For the conjugates we use the Pascal construction to determine the 6-th point on the line on a conic through 4 real points and 1 complex point.

Exercise.

For $q = 2^2$,

0. determine the primitive polynomial giving the selector 0, 1, 4, 14, 16.
1. Determine the correspondance between the selector notation and the homogeneous coordinates for points and lines. Note that these are not the same.
2. The correspondance i to i^* is a polarity whose fixed points are on a line. Determine the matrix representation, the polar of (X, Y, Z) and the equation satisfied by the fixed points.
3. Determine the fundamental projectivity on the line 14^* using a point conic which has no points on 14^* .

4. Illustrate Pascal's Theorem.

Exercise.

0. Explore the usefulness of the truncated cuboctahedron less the hexagonal faces and the $< 4.8 >$ edges as a model for the projective geometry of order 7.
1. Show that the 14-gonal antiprism can be used as a model for the projective geometry of order 7. More generally,
2. Show that the n -gonal antiprism can be used as a model for the projective geometry of order $q = p^k$ when $p \equiv -1 \pmod{4}$, with $n = \frac{q^2+q}{4}$.
3. Show that the n -gonal antiprism can be used as a model for the projective geometry of order $q = p^k$ when $q \equiv 1 \pmod{12}$, with $n = \frac{q^2+q}{2}$. Finally,
4. Show that the n -gonal prism can be used as a model for the projective geometry of order $q = p^k$ when $q \equiv -1 \pmod{3}$, with $n = \frac{q^2+q}{3}$.
5. is there a general theory when using prisms or antiprisms?

Exercise.

For $q = 2^3$.

0. to 4. Answer question similar to those of 2.3.8
5. Show that the 18-gonal antiprism can be used as a model for the projective geometry of order 2^3 . More generally,
6. Show that the n -gonal antiprism can be used as a model for the projective geometry of order $q = 2^k$, with $n = \frac{q^2+q}{4}$.

Answer to 2.3.2.

0. For $q = 2$, the primitive polynomial giving the selector 0, 1, 3, is $I^3 + I + 1$.

The auto-correlates are 0 11 2 7 8.

The selector function is

i	0	1	2	3	4	5	6	7	8	9	10	11
$f(i)$		0	14	1	0	16	16	14	14	16		
type	F_0	V_0	F_4	V_2	T_0	T_2	V_1	F_3	F_1	T_3	E_2	F_2
i	12	13	14	15	16	17	18	19	20			
$f(i)$	4	1	0	1	0	4	4	16	1			
type	T_4	E_1	P	V_3	E_0	T_1	E_3	V_4	E_4			

1. The correspondence between the selector notation and the homogeneous coordinates for points and lines is

i	I^i	i^*
0	1	$6^* : 1, 2, 4,$
1	I	$1^* : 0, 2, 6,$
2	I^2	$0^* : 0, 1, 3,$
3	$I + 1$	$5^* : 2, 3, 5,$
4	$I^2 + I$	$3^* : 0, 4, 5,$
5	$I^2 + I + 1$	$4^* : 3, 4, 6,$
6	$I^2 + 1$	$2^* : 1, 5, 6.$

2. The matrix representation is

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}. \text{ and the equation satisfied by the fixed points is } (X_0 + X_1)^2 = 0.$$

3. The degenerate conic through 0, 1, 2 and 5 with tangent 5^* at 5, is represented by the matrix

$$N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The polar of 0 is 0^* , of 1 is 0^* , of 2 is 5^* , of 4 is 4^* , of 5 is 5^* of 6 is 6^* and of 3 is undefined. The equation in homogeneous coordinates is $X_0(X_1 + X_2) = 0$.

4. A circle with center 14 can be constructed as follows. I first observe that a direction must be orthogonal to itself. Indeed, if 0 is a direction, the others form an angle $1, 2, 3, 4 \pmod{5}$, we cannot play favorites and must choose 0. If $A_0 = 1$, $C \times A_0$ and therefore the tangent has direction 0, $A_0 \times A_{i+1}$ has direction $i \pmod{5}$ or are the points 0, 7, 8, 2, 11.

It is natural to choose the pentagonal face-point as 14, and the edge-points on the pentagon as 0, 8, 11, 7, 2. The points on the circle 1, 6, 3, 15, 19 are chosen as the vertex-points opposite the corresponding edge-point, 1 opposite 0, 6 opposite 8, ... This gives the types, with subscripts indicated in 0. and the definition:

The points are represented on the 5-anti-prism as follows. The pentagonal face-point, P , the 5 triangular face-points, T_i , the 5 vertex-points, V_i , the 5 triangular-triangular edge-points, E_i , the 5 pentagonal-triangular edge-points F_i .

The lines are represented on the 5-anti-prism as follows. The pentagonal face-line, f , which is incident to F_i , the 5 triangular face-lines, t_i , which are incident to $F_i, F_i, T_{i+1}, T_{i-1}, E_{i+2}, E_{i-2}$. If f is the pentagonal edge of t_i and V, V' are on f , F_i is on it, $T_{i+1} (T_{i-1})$ share $V (V')$, $E_{i+2} (E_{i-2})$ are on an edge through $V (V')$ not on t_i the 5 vertex-lines, v_i , which are incident to

$F_i, V_{i+2}, V_{i-2}, E_{i+1}, E_{i-1}$. If t is the face with v_i on its pentagonal edge these are all the vertices, and edge-points on it distinct from v_i .

the 5 triangular-triangular edge-lines, e_i , which are incident to $F_i, T_{i+2}, T_{i-2}, V_{i+1},$

V_{i-1} , V_{i+1} and V_{i-1} are on the same edge as e_i , the line which joins the center C of the antiprism to E_i is parallel to the edge containing F_i , T_{i+2} and T_{i-2} are the triangular faces which are not adjacent to E_i or F_i .

the 5 pentagonal-triangular edge-lines. f_i , which are incident to P , T_i , V_i , E_i , F_i . T_i is adjacent to f_i , V_i is opposite f_i , E_i joined to the center of the antiprism is parallel to T_i .

Answer to 2.3.3.

For $p = 3$,

0. The primitive polynomial giving the selector 0, 1, 3, 9 is $I^3 - I - 1$.

1. The correspondence between the selector notation and the homogeneous coordinates for points and lines is

i	I^i	i^*
0	1	$12^* : 1, 2, 4, 10,$
1	I	$1^* : 0, 2, 8, 12,$
2	I^2	$0^* : 0, 1, 3, 9,$
3	$I + 1$	$7^* : 2, 6, 7, 9,$
4	$I^2 + I$	$3^* : 0, 6, 10, 11,$
5	$I^2 + I + 1$	$4^* : 5, 9, 10, 12,$
6	$I^2 + 2I + 1$	$10^* : 3, 4, 6, 12,$
7	$I_2 + I + 2$	$6^* : 3, 7, 8, 10,$
8	$I^2 + 1$	$2^* : 1, 7, 11, 12,$
9	$I + 2$	$11^* : 2, 3, 5, 11$
10	$I_2 + 2I$	$9^* : 0, 4, 5, 7,$
11	$I^2 + 2I + 2$	$5^* : 4, 8, 9, 11,$
12	$I^2 + 2$	$8^* : 1, 5, 6, 8.$

2. The matrix representation of the polarity i to i^* is

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

The equation satisfied by the fixed points is $X_0^2 + X_1^2 + 2X_2X_0 = 0$.

3. The degenerate conic through 0, 1, 2 and 5 with tangent 4^* at 5, is obtained by constructing the quadrangle-quadrilateral configuration starting with $P = 5$ and $Q_i = \{0, 1, 2\}$. We obtain $q_i = \{3^*, 2^*, 7^*\}$, which are the tangents at Q_i . The matrix representation is

$$N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \text{ with equation } X_1X_2 + X_2X_0 + X_0X_1 = 0.$$

We can check that the polar of $10 = 3^* \times 4^*$ is $9^* = 0 \times 5$.

Answer to ??.

0. For $q = 2^2$, the primitive polynomial giving the selector 0, 1, 4, 14, 16 is $I^3 - I^2 - I - \epsilon$, with
- $$\epsilon^2 + \epsilon + 1 = 0.$$

1. The correspondence between the selector notation and the homogeneous coordinates are as follows, i^* has the homogeneous coordinates associated with I^i .

i	I^i	i^*
0	1	20*
1	I	14*
2	I^2	0*
3	$I^2 + I + \epsilon$	10*
4	$I + \epsilon$	${}^2 19^*$
5	$I^2 + \epsilon$	${}^2 14^*$
6	$I^2 + \epsilon$	${}^2 I + 118^*$
7	$I^2 + 1$	15*
8	$I^2 + \epsilon$	3*
9	$I^2 + \epsilon^2 I + \epsilon$	5*
10	$I^2 + \epsilon I + 1$	9*
11	$I^2 + \epsilon^2$	13*
12	$I^2 + \epsilon I + \epsilon$	11*
13	$I^2 + I + \epsilon^2$	6*
14	$I + 1$	2*
15	$I^2 + I$	1*
16	$I + \epsilon$	12*
17	$I^2 + \epsilon I$	16*
18	$I^2 + \epsilon I + \epsilon^2$	17*
19	$I^2 + \epsilon^2 I + \epsilon^2$	8*
20	$I^2 + I + 1$	7*

To obtain the last column, for row 9, $[1, \epsilon^2, \epsilon] = (1, 1, 1) \times (1, \epsilon, 0) = 20 \times 17 = 5^*$.

2. The correspondence i to i^* is a polarity whose fixed points are on a line. The matrix representation is obtained by using the image of 4 points.

$$0 = (0, 0, 1), M(0) = 0^* = [1, 0, 0],$$

$$1 = (0, 1, 0), M(1) = 1^* = [1, 1, 0],$$

$$2 = (1, 0, 0), M(2) = 2^* = [0, 1, 1],$$

$$18 = (1, \epsilon, \epsilon^2), M(18) = 18^* = [1, \epsilon^2, 1].$$

The first 3 conditions give the polarity matrix as

The last condition gives $\beta\epsilon + \alpha\epsilon^2 = 1$, $\gamma + \beta\epsilon = \epsilon^2$, $\gamma = 1$. Hence $\gamma = 1$, $\beta = 1$, $\alpha = 1$.

Therefore

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note that M is real and could have been obtained from the reality and non singularity conditions, giving directly $\alpha = \beta = \gamma = 1$.

The polar of (X_0, X_1, X_2) is $[X_1 + X_2, X_0 + X_1, X_0]$.

The fixed points (X_0, X_1, X_2) satisfy $X_1^2 = 0$ corresponding to 14^* .

3. A point conic with no points on 14 is $1, 3, 4, 5, 13$,
the corresponding line conic is $15, 19, 10, 16, 8$.
Projecting from 1 and $3, 1, 3, 5, 13, 4$,
we get the fundamental projectivity, $8, 2, 11, 0, 7$ on 14^* .
4. To illustrate Pascal's Theorem, because there are only 5 points on a conic, we need to use the degenerate case. The conic through $0, 1, 2$ and the conjugate points 9 and 18 is The last condition gives $\beta\epsilon + \alpha\epsilon^2 = 1, \gamma + \beta\epsilon = \epsilon^2, \gamma = 1$.

Hence $\gamma = 1, \beta = 1, \alpha = 1$. Therefore

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note that M is real and could have been obtained from the reality and non singularity conditions, giving directly $\alpha = \beta = \gamma = 1$.

The polar of (X_0, X_1, X_2) is $[X_1 + X_2, X_0 + X_1, X_0]$.

The fixed points (X, X_1, X_2) satisfy $X_1^2 = 0$ corresponding to 14^* .

5. A point conic with no points on 14 is $1, 3, 4, 5, 13$,

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

The tangents at $(0,0,1), (0,1,0), (1,0,0), (1,\epsilon^2,\epsilon), (1,\epsilon,\epsilon^2)$ are $[1,1,0], [1,0,1], [0,1,1], [1,\epsilon^2,\epsilon), (1,\epsilon,\epsilon^2]$, or $1^*, 15^*, 2^*, 5^*, 17^*$. On the other hand, using Pascal's Theorem, the tangent at 0 is given by

$$\begin{aligned} & (((0 \times 1) \times (9 \times 18)) \times ((18 \times 0) \times (1 \times 2))) \times (2 \times 9) \times 0 \\ &= (((0^* \times 7^*) \times (4^* \times 20^*)) \times 12^*) \times 0 \\ &= (((14 \times 17) = 8^*) \times 12^* \text{ or } 13) \times 0 = 1^*. \end{aligned}$$

Answer to

??.

For $q = 57$, choose the auto-correlates as point on a circle although 0 is on the circle draw as it is the center. With the succession of points X_i ,

$x_i = 0 \times X_i$	36,	1,	52,	43,	3,	32,	13,
X_i	16,	35,	18,	50,	29,	26,	30,
$y_{i+1} = X_{i-1} \times X_{i+1}$	22,	42,	8,	14,	10,	28,	44,
$y_{i+2} = X_{i-2} \times X_{i+2}$	34,	2,	41,	17,	40,	20,	23,
$y_{i+3} = X_{i-3} \times X_{i+3}$	7,	31,	6,	27,	54,	25,	39,
$y_{i+1} \times x_i$	21,	51,	5,	46,	33,	4,	45,
$y_{i+2} \times x_i$	24,	56,	48,	15,	49,	38,	47,
$y_{i+3} \times x_i$	53,	12,	37,	9,	55,	11,	19.

This gives all the points in the projective plane of order 7. We observe

16*	21*	24*	53*	22*	34*	7*
36	36	36	36	36	36	36
16				35, 30	18, 26	50, 29
42, 44	22	8, 28		14, 10		
41, 20		34	17, 40		2, 23	
27, 54	31, 39		7			6, 25
		46, 33	5, 4	21		51, 45
	15, 49		56, 47	48, 38	24	
	37, 11	12, 19			9, 55	53
35*	51*	56*	12*	42*	2*31*	
1	1	1	1	1	1	1
35				16, 18	50, 30	29, 26
22, 8	42	14, 44		10, 28		
17, 23		2	40, 20		34, 41	
54, 25	7, 6		31			27, 39
		33, 4	46, 45	51		21, 5
	49, 38		24, 48	15, 47	56	
	9, 19	53, 37			55, 11	12
18*	5*48*	37*	8*14*	6*		
52	52	52	52	52	52	52
18				35, 50	16, 29	26, 30
42, 14	8	22, 10		28, 44		
34, 40		41	20, 23		2, 17	
25, 39	31, 27		6			7, 54
		4, 45	21, 33	5		51, 46
	38, 47		56, 15	24, 49	48	
	53, 55	12, 9			11, 19	37

Answer to ??.

For $q = 2^3$,

36 :	0	37	38	40	44	52	18	27	68	1*	3*	7*	2*	4*	5*
$36 \times 0 = 0^*$:	0	1	3	7	15	31	36	54	63	0	0	0	1	3	31
$36 \times 37 = 37^*$:	17	26	36	37	39	43	51	67	72	72	51	67	72	72	26
$36 \times 38 = 38^*$:	16	25	35	36	38	42	50	66	71	35	71	66	71	50	71
$36 \times 40 = 40^*$:	14	23	33	34	36	40	48	64	69	14	33	69	34	69	69
$36 \times 44 = 44^*$:	10	19	29	30	32	36	44	60	65	30	60	29	29	32	10
$36 \times 52 = 52^*$:	2	11	21	22	24	28	36	52	57	2	28	24	52	11	2
$36 \times 18 = 18^*$:	13	18	36	45	55	56	58	62	70	62	70	56	13	70	58
$36 \times 27 = 27^*$:	4	9	27	36	46	47	49	53	61	53	4	47	61	27	49
$36 \times 68 = 68^*$:	5	6	8	12	20	36	41	59	68	6	12	8	5	59	68

Conic with no point on 36: 2, 4, 5, 6, 13, 28, 31, 46, 63

line conic: 29, 59, 31, 9, 18, 43, 28, 35, 64.

Fundamental projectivity: from 2 and 5 on the conic, the points

2, 5, 6, 31, 13, 28, 4, 46, 63 give the points on 36^* :

38, 0, 68, 27, 52, 37, 40, 18, 44.
empty

Chapter 3

FINITE PRE INVOLUTIVE GEOMETRY

3.1 An Overview of the Geometry of the Hexal Complete 5-Angles.

3.1.0 Introduction.

In the geometry of Euclid, not every pair of lines have a point in common, namely the parallel ones. I call Euclidean Geometry, that geometry which consists in completing the plane of Euclid by the ideal points and the lines of Euclid by the ideal line. To each set of parallel lines correspond its direction or point at infinity or ideal point. The line at infinity or ideal line is incident to all ideal points. Figures Pl and St may help the reader to visualize. In Fig. Pl, projecting the line b on the line c from the point P establishes a one to one correspondance between the points on these lines, if we include the ideal point C_i , on c , corresponding to B_i and the ideal point B_∞ , on b , corresponding to C_∞ . Replacing lines b and c by planes, perpendicular to the plane P of figure establishes a one to one correspondance between a line through C_∞ perpendicular to P and the ideal line through B_∞ .

This led to the concept of perspectivity, which I have schematized in Fig. St. In it, the shading, corresponds to the method used by Chinese artists to represent distances in paintings. The tiling corresponds to the method used by Western painters. Johannes Vermeer's use of perspective in his paintings was so accurate as to allow P. T. A. Swillens to reconstruct, from the size of a chair, in the painting, not only the size of the rooms, but also to estimate the height of the artist.

Affine geometry is obtained from Euclidean geometry by discarding the notions associated with congruences of figures, projective geometry is obtained by discarding the notion of parallelism, thereby making the properties of any point or line in the plane indistinguishable from that of any other.

I will describe at a later time, how I was lead to the discovery of finite Euclidean geometry and to the extension of many of the properties of Euclidean geometry. While working out a proof for these results, it ocured to me, that the results can be placed in the framework of finite projective geometry. I will, as I proceed, make the connection with the results in classical

Euclidean geometry. The results can be considered as proceeding from an, apparently new, configuration consisting of 14 points and 13 lines. This configuration is defined starting from an ordered complete 5-angle, A_0, A_1, A_2, M and \overline{M} , in which the first 3 points can be rotated and the last 2 points interchanged. In other words the configuration is the same if we replace A_0, A_1 and A_2 by A_1, A_2 and A_0 and independently M by \overline{M} and \overline{M} by M . In involutive geometry, (the Euclidean geometry without measure of angles and distances), we define altitudes and their intersection, the orthocenter, we define medians and their intersection, the barycenter. In the generalization to projective geometry, the orthocenter and the barycenter become two arbitrary points, whose role is interchangeable. The proofs are constructive, and the only construction required are those of lines through 2 given points and of points at the intersection of two given lines, but these constructions must be valid for all p . They do not involve the construction of an arbitrary line through a given point, as required to obtain, for instance, an arbitrary point on a conic, by the construction of Pascal or of MacLaurin.

No special relations will be assumed here between the points obtained during the construction. The special relation \overline{M} on the polar of M with respect to the triangle A_0, A_1, A_2 will be studied in Chapter IV,

in the section on Cartesian geometry and the special case where M and \overline{M} are respectively on the polar of \overline{M} and M with respect to the triangle will also be discussed elsewhere.

The beginning of a synthetic proof is given in section 4.3. Synthetic proofs are highly desirable and are from my point of view more elegant, but require much more time to develop.

The constructions and statements are given in a compact form using a notation which will now be explained.

3.1.1 Notation and application to the special configuration of Desargues and to the pole and polar of with respect to a triangle.

Introduction.

In the preceding Chapter, I have introduced a notation for points, lines, incidence and statements. Additional notation is given here for conics, for points on conics and tangents to conics and a notation which allows to describe at once 3 points or 6 points associated to a triangle.

Notation.

The identifier for a point conic will be a lower case Greek letter or an identifier starting with a lower case preceded by a backward quote “ ‘ ”. The identifier for a line conic will be an upper case Greek letter or an identifier starting with an upper case preceded by a backward quote “ ‘ ”.

The subscript i , will have the values 0, 1 and 2. Hence A_i denotes 3 points A_0, A_1 and A_2 .

If subscripts involve the letter i and addition, the addition is done modulo 3, for instance,

$$a_i := A_{i+1} \times A_{i+2}$$

is equivalent to

$$a_0 := A_1 \times A_2, a_1 := A_2 \times A_0, a_2 := A_0 \times A_1.$$

It represents the construction of the sides a_0 , a_1 and a_2 of a triangle with vertices A_0 , A_1 and A_2 .

To indicate that a conic γ is constructed as that conic which passes through the 5 distinct points P_0 , P_1 , P_2 , P_3 , and P_4 , we write

$$\gamma := \text{conic}(P_0, P_1, P_2, P_3, P_4).$$

To indicate that a conic γ_1 is constructed as that conic whose tangent at P_0 is a_0 and at P_2 is a_2 and passes also by P_4 , we write

$$\gamma_1 := \text{conic}((P_0, a_0), (P_2, a_2), P_4). \text{ or } \gamma_1 := \text{conic}(P_0, a_0, P_2, a_2, P_4).$$

When 3 lines x_i are concurrent, the intersection X can be obtained using any of the three pairs. I have chosen, arbitrarily,

$$X := x_1 \times x_2(*),$$

as a reminder that 2 other definitions of X could have been chosen. In the special case, $x_1 = x_2$, the other choice

$$X := x_0 \times x_1,$$

will be used. “ $(*)$ ” denotes therefore not only a Definition but also a Theorem or Conclusion. A similar notation will be used for conics.

$X \cdot \gamma = 0$ and $X_i \cdot \gamma = 0$, are the notations corresponding to the point X is on the conic γ and the triple X_0, X_1, X_2 is on the conic γ .

$P = \text{Pole}(p, \alpha)$, is the notation for P is the pole of p with respect to the conic α .

γ is a circle $= 0$ or γ is a cocircle is either an hypothesis, to indicate a preferred conic from which all other circles are defined or a Conclusion,

$X = \text{Center}(\gamma)$ and $\bar{X} = \text{Cocenter}(\gamma)$ is an abbreviation for X is the center of the conic γ (not necessarily a circle) and \bar{X} is the cocenter of the conic γ , in other words $X, (\bar{X})$ is the polar of m (\bar{m}) with respect to γ . See section 4.3.3.

Example.

With this notation, the special configuration of Desargues of 0.4.6. can be defined by

$$a_i := A_{i+1} \times A_{i-1}, r_i := P \times A_i,$$

$$P_i := a_i \times r_i, q_i := P_{i+1} \times P_{i-1},$$

$$R_i := a_i \times q_i, p_i := A_i \times R_i,$$

$$Q_i := p_{i+1} \times p_{i-1}, p := R_1 \times R_2(*),$$

and the conclusions of the special Desargues Theorem are implied by the last Definition-Conclusion and by the Conclusion,

$$Q_i \cdot r_i = 0.$$

Let $P = (p_0, p_1, p_2)$, and $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$, then

$$a_0 = [1, 0, 0], r_0 = [0, p_2, -p_1],$$

$$P_0 = (0, p_1, p_2), q_0 = [-p_1 p_2, p_2 p_0, p_0 p_1],$$

$$R_0 = (0, p_1, -p_2), p_0 = [0, p_2, p_1],$$

$$Q_0 = (-p_0, p_1, p_2), p = [p_1 p_2, p_2 p_0, p_0 p_1].$$

Example.

For $p = 3$, prove that if $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$ and $P = (1, 1, 1)$ then the other elements of the quadrangle quadrilateral configuration II.2.1.6 are

$$P_0 = (0, 1, 1), Q_0 = (-1, 1, 1), R_0 = (0, 1, -1), \dots, \text{ and}$$

$$a_0 = [1, 0, 0], p = [1, 1, 1],$$

$$p_0 = [0, 1, 1], q_0 = [-1, 1, 1], r_0 = [0, 1, -1], \dots \text{ and that}$$

the conic of II.2.2.11 is

$$X_0^2 + X_1^2 + X_2^2 = 0.$$

Theorem.

With the above notation, the polar p can be obtained algebraically from the pole P or the pole P from the polar p using the first or the second formula:

$$0. \quad pA_i = P * A_i, Pa_i = p * a_i,$$

$$1. \quad pA_i = (P \cdot a_i)A_i - (A_i \cdot a_i)P, Pa_i = (p \cdot A_i)a_i - (a_i \cdot A_i)p,$$

$$\begin{aligned} 2. \quad p_i &= (P \cdot a_{i+1})(P \cdot a_{i-1})A_{i+1} * A_{i-1} + (P \cdot a_{i+1})(A_{i-1} \cdot a_{i-1})P * A_{i+1} \\ &\quad - (P \cdot a_{i-1})(A_{i+1} \cdot a_{i+1})P * A_{i-1}, \\ P_i &= (p \cdot A_{i+1})(p \cdot A_{i-1})a_{i+1} * a_{i-1} + (p \cdot A_{i+1})(a_{i-1} \cdot A_{i-1})p * a_{i+1} \\ &\quad - (p \cdot A_{i-1})(a_{i+1} \cdot A_{i+1})p * a_{i-1}. \end{aligned}$$

$$\begin{aligned} 3. \quad Pa_i &= (P \cdot a_{i+1})A_{i+1} - (P \cdot a_{i-1})A_{i-1}, \\ PA_i &= (p \cdot A_{i+1})a_{i+1} - (p \cdot A_{i-1})a_{i-1}. \end{aligned}$$

$$4. \quad p = \frac{1}{P \cdot a_0}a_0 + \frac{1}{P \cdot a_1}a_1 + \frac{1}{P \cdot a_2}a_2, P = \frac{1}{p \cdot A_0}A_0 + \frac{1}{p \cdot A_1}A_1 + \frac{1}{p \cdot A_2}A_2.$$

Proof: Only the first part of 2 to 4 needs to be proven, because of duality. To obtain 2, we use $P * P = 0$ and $A_{i+1} * P = -P * A_{i+1}$. To obtain 3, we recall that $a_i = A_{i+1} * A_{i-1}$, we use $A_i * a_j = 0$ when $i \neq j$ and $A_i * a_i = (A_0 * A_1) \cdot A_2 = t$, then divide by t and by $P \cdot a_i \neq 0$. To obtain 4, we use $p = R_{i+1} * R_{i-1}$. We divide by $(P \cdot a_i)(P \cdot a_{i+1})(P \cdot a_{i-1}) \neq 0$, and obtain $p = A_{i+1} * \frac{1}{P \cdot a_i}A_{i-1} + A_{i-1} * \frac{1}{P \cdot a_{i+1}}A_i + A_i * \frac{1}{P \cdot a_{i-1}}A_{i+1}$, or $p = \frac{1}{P \cdot a_i}a_i + \frac{1}{P \cdot a_{i+1}}a_{i+1} + \frac{1}{P \cdot a_{i-1}}a_{i-1}$.

Example.

For $p = 13$, $A_i = (36(1, 1, 9), 27(1, 1, 0), 151(1, 10, 7))$, $P = (68(1, 4, 2))$,
 $a_i = [175(1, 12, 5), 150(1, 10, 6), 170(1, 12, 0)]$, $r_i = [77, 138, 31]$,
 $S_i = (143, 63, 33)$, $p_i = [108, 46, 37]$, $R_i = (48, 16, 32)$,
 $p = \frac{1}{7}a_0 + \frac{1}{11}a_1 + \frac{1}{10}a_2 = 2a_0 + a_1 + 4a_2 = [124]$, $p_i = [140, 176, 106]$,
 $P_i = (51, 132, 84)$, $P = \frac{1}{11}A_0 + \frac{1}{9}A_1 + \frac{1}{6}A_2 = 6A_0 + 3A_1 + 11A_2 = (68)$.

Definition.

An hexal complete 5-angle configuration, is a configuration which starts with an ordered set of 5 points A_0, A_1, A_2, M and \overline{M} .

In the configuration obtained from it, if a point X_0 is constructed, 5 other points are obtained. X_1 is obtained by replacing A_0, A_1, A_2 by A_1, A_2, A_0 ; X_2 is obtained by replacing the same points by A_2, A_0, A_1 and the points \overline{X}_i are obtained by exchanging in the construction of X_i , M and \overline{M} . The same holds for lines. The first letter has a macron placed above it in the naming of the construction which exchanges M and \overline{M} . { In the group of permutation on the 5 points of the complete 5-angle, the figure is invariant under the cyclic group generated by the permutation

$$\begin{aligned} & (A_0 A_1 A_2 \overline{M} \overline{M}) \\ & (A_1 A_2 A_0 \overline{M} M) \}. \end{aligned}$$

In special cases, several of these elements or all of the elements may coincide.

Comment.

We know from II.1.5.6. that a complete 5-angle requires $p \geq 5$, therefore, the definition and results that follow are non vacuous only if $p \geq 5$. We introduce here a terminology inspired from corresponding terms in Euclidean geometry. In some instances, the correspondence will be made explicitly. For instance, the line m which will be constructed corresponds to the ideal line or line at infinity in Euclidean geometry, we will therefore call m the ideal line. In the symmetry which exchanges M and \overline{M} , to m corresponds \overline{m} , which will be called the coideal line. { \overline{m} corresponds to the orthic axis. } The conic θ which will be constructed corresponds to the circumcircle and the conic γ to the circle of Brianchon-Poncelet also called the nine-point circle.

Definition.

θ and any conic $\delta, (\overline{\delta})$ such that there exists a radical axis $u, (\overline{u})$ with respect to $m, (\overline{m})$ is called a circle (cocircle) and u is called the radical (coradical) axis of θ and $\delta, (\overline{\delta})$.

Algebraically, we have, for some integers k_1, k_2 and k_3 ,

$$k_1 \delta + k_2 \theta = k_3 (m) \times (u),$$

where θ, m, δ and u are expressed exactly as in the corresponding expressions P0.7, P1.19, 1.20, ..., below.

A triangle consists of its vertices and its sides. When we want to be specific we will use either or both, for instance the given triangle can be written as $\{A_i\}$ or $\{a_i\}$ or $\{A_i, a_i\}$. To each of the section of this Theorem corresponds a sequence of theorems in Euclidean geometry which will be given in the corresponding sections of Chapter IV.

We will give separately the construction of the various points and lines of the hexal configuration (zetetic part) and the proof that the construction satisfies the given properties (poristic part).

3.1.2 An overview of theorems associated with equality of distances and angles. The ideal line, the orthic line, the line of Euler, the circle of Brianchon-Poncelet, the circumcircle, the point of Lemoine.

Introduction.

As the generalization proceeds, the 4 points on the line of Euler, become 10 points on its generalization. The 9 (or 12) points on the circle of Brianchon-Poncelet (also called circle of Euler) become 20 points on the corresponding conic. New results, which will be given in part III, are further consequences.

The definitions are numbered starting with D, the conclusions are numbered stating with C, the proofs, which consist of the algebraic expressions of the various points, lines and conics, which can easily be checked and from which the conclusions can easily be verified, have a number corresponding to the definition, starting with P.

The numbering in this overview is the same as the number in the complete theory, given in Chapter 5 and 6.

Theorem.

If we derive a point X and a line x by a given construction from A_i , M and \overline{M} , with the coordinates as given in G0.0 and G0.1, below, and the point \overline{X} and line \overline{x} are obtain by the same construction interchange M and \overline{M} ,

$$\begin{aligned} X &= (f_0(m_0, m_1, m_2), f_1(m_0, m_1, m_2), f_2(m_0, m_1, m_2)), \\ x &= [g_0(m_0, m_1, m_2), g_1(m_0, m_1, m_2), g_2(m_0, m_1, m_2)], \end{aligned}$$

\Rightarrow

$$\begin{aligned} \overline{X} &= (m_0 f_0(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_1 f_1(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_2 f_2(m_0^{-1}, m_1^{-1}, m_2^{-1})), \\ \overline{x} &= [m_0^{-1} g_0(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_1^{-1} g_1(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_2^{-1} g_2(m_0^{-1}, m_1^{-1}, m_2^{-1})]. \end{aligned}$$

Proof: The point collineation $\mathbf{C} = \begin{pmatrix} q_0 & 0 & 0 \\ 0 & q_1 & 0 \\ 0 & 0 & q_2 \end{pmatrix}$, associates to $(1,1,1)$, (q_0, q_1, q_2) , and

to (m_0, m_1, m_2) , (r_0, r_1, r_2) , if $r_i = q_i m_i$.

In the new system of coordinates,

$$X = (q_0 f_0(q_0^{-1} r_0, q_1^{-1} r_1, q_2^{-1} r_2), q_1 f_1(q_0^{-1} r_0, q_1^{-1} r_1, q_2^{-1} r_2), q_2 f_2(q_0^{-1} r_0, q_1^{-1} r_1, q_2^{-1} r_2)).$$

Exchanging q_i and r_i and then replacing q_i by 1 and r_i by m_i is equivalent to substituting m_i for q_i and 1 for r_i , which gives \overline{X} . \overline{x} is obtained similarly.

The line collineation is

$$\begin{pmatrix} q_0^{-1} & 0 & 0 \\ 0 & q_1^{-1} & 0 \\ 0 & 0 & q_2^{-1} \end{pmatrix}.$$

Theorem.

Given a complete 5-angle, 5 distinct points, no 3 of which are on the same line, A_0, A_1, A_2, M and \overline{M} , A_i are called the vertices, M is called the barycenter and \overline{M} , the orthocenter.

1. *The ideal line and the orthic line. See Fig. 1,*

- H0.0. A_i ,
- H0.1. M, \overline{M} ,
- D0.0. $a_i := A_{i+1} \times A_{i-1}$,
- D0.1. $ma_i := M \times A_i, \overline{ma}_i := \overline{M} \times A_i$,
- D0.2. $M_i := ma_i \times a_i, \overline{M}_i := \overline{ma}_i \times a_i$,
- D0.3. $mm_i := M_{i+1} \times M_{i-1}, \overline{mm}_i := \overline{M}_{i+1} \times \overline{M}_{i-1}$,
- D0.4. $MA_i := a_i \times mm_i, \overline{MA}_i := a_i \times \overline{mm}_i$,
- D0.7. $m := MA_1 \times MA_2(*), \overline{m} := \overline{MA}_1 \times \overline{MA}_2(*)$.

The nomenclature:

- N0.0. a_i are the sides.
- N0.3. ma_i are the medians, \overline{ma}_i are the comedians or \overline{ma}_i are the altitudes, ma_i are the coaltitudes,
- N0.4. M_i are the mid-points of the sides.
 \overline{M}_i are the feet or the feet of the altitudes,
- N0.5. (M_i, mm_i) is the complementary triangle,
 $(\overline{M}_i, \overline{mm}_i)$ is the orthic triangle,
- N0.6. MA_i are the directions of the sides,
- N0.8. m is the ideal line corresponding to the line at infinity,
 \overline{m} is the coideal line or the orthic line, which is the polar of \overline{M} with respect to the triangle.

Proof:

- P0.0. $a_0 = [1, 0, 0]$,
- P0.1. $ma_0 = [0, 1, -1], \overline{ma}_0 = [0, -m_2, m_1]$,
- P0.2. $M_0 = (0, 1, 1), \overline{M}_0 = (0, m_1, m_2)$,
- P0.3. $mm_0 = [-1, 1, 1], \overline{mm}_0 = [-m_1m_2, m_2m_0, m_0m_1]$,
- P0.4. $MA_0 = (0, 1, -1), \overline{MA}_0 = (0, m_1, -m_2)$,
- P0.7. $m = [1, 1, 1], \overline{m} = [m_1m_2, m_2m_0, m_0m_1]$,

2. *The line of Euler and the circle of Brianchon-Poncelet. See Fig. 2, 2b.*

Let

- D1.0. $eul := M \times \overline{M}$
- D1.20. $\gamma := \text{conic}(M_0, M_1, M_2, \overline{M}_1, \overline{M}_2)(*)$,

then

- C1.1 γ is a circle, γ is a cocircle = 0.

The nomenclature:

- N1.0. eul is the line of Euler.
- N1.11. γ is the circle of Brianchon-Poncelet. In Euclidean geometry, the circle of Brianchon-Poncelet, is also called the circle of 9 points or circle of Feuerbach or, improperly, the circle of Euler. It passes through the midpoints of the sides, the feet of the altitudes and the midpoints of the segment joining the vertices to the orthocenter. The Definition-Conclusion D1.20. corresponds to the first part of the Theorem of Brianchon-Poncelet.

Proof:

$$P1.0. \quad eul = [m_1 - m_2, m_2 - m_0, m_0 - m_1],$$

$$P1.20. \quad \begin{aligned} \gamma : m_1 m_2 X_0^2 + m_2 m_0 X_1^2 + m_0 m_1 X_2^2 \\ - m_0(m_1 + m_2)X_1 X_2 - m_1(m_2 + m_0)X_2 X_0 - m_2(m_0 + m_1)X_0 X_1 = 0, \\ \gamma^{-1} : m_0^2(m_1 - m_2)^2 x_0^2 + m_1^2(m_2 - m_0)^2 x_1^2 + m_2^2(m_0 - m_1)^2 x_2^2 \\ - 2m_1 m_2(m_0(3s_1 - 2m_0) + m_1 m_2)x_1 x_2 \\ - 2m_2 m_0(m_1(3s_1 - 2m_1) + m_2 m_0)x_2 x_0 \\ - 2m_0 m_1(m_2(3s_1 - 2m_2) + m_0 m_1)x_0 x_1. \end{aligned}$$

3. *The circumcircle. See Fig. 4, 4b.*

Let

$$D1.6. \quad Imm_i := m \times \overline{m}m_i, \quad \overline{Imm}_i := \overline{m} \times mm_i,$$

$$D1.7. \quad ta_i := A_i \times Imm_i,$$

$$D1.19. \quad \theta := conic(A_1, ta_1, A_2, ta_2, A_0),$$

then

$$C1.2. \quad \overline{Imm}_i \cdot ta_i = 0.$$

$$H1.1. \quad \theta \text{ is a circle} = \theta \text{ is a cocircle} = 0.$$

The nomenclature:

N1.4. *Imm_i are the directions of the antiparallels a_i with respect to the sides a_{i+1} and a_{i-1} .*

N1.5. *ta_i are the tangents at A_i to the circumcircle,*

N1.10. *θ is the circumcircle.*

Proof:

$$P1.6. \quad \begin{aligned} I\overline{m}m_1 &= (m_0(m_1 - m_2), -m_1(m_2 + m_0), m_2(m_0 + m_1)), \\ \overline{I}m_1 &= (m_0(m_2 - m_1), -m_1(m_2 + m_0), m_2(m_0 + m_1)), \end{aligned}$$

$$P1.7. \quad ta_0 = [0, m_2(m_0 + m_1), m_1(m_2 + m_0)],$$

$$P1.19. \quad \begin{aligned} \theta : m_0(m_1 + m_2)X_1 X_2 + m_1(m_2 + m_0)X_2 X_0 \\ + m_2(m_0 + m_1)X_0 X_1 = 0, \\ 2\theta + \gamma = (m) \rtimes (\overline{m}). \\ \theta^{-1} : m_0^2(m_1 + m_2)^2 x_0^2 + m_1^2(m_2 + m_0)^2 x_1^2 + m_2^2(m_0 + m_1)^2 x_2^2 \\ - 2m_1 m_2(m_2 + m_0)(m_0 + m_1)x_1 x_2 \\ - 2m_2 m_0(m_0 + m_1)(m_1 + m_2)x_2 x_0 \\ - 2m_0 m_1(m_1 + m_2)(m_2 + m_0)x_0 x_1 = 0, \end{aligned}$$

4. *The point of Lemoine. See Fig. 3.*

Let

$$D1.2. \quad Maa_i := ma_{i+1} \times \overline{m}a_{i-1}, \quad \overline{M}aa_i := ma_{i-1} \times \overline{m}a_{i+1},$$

$$D1.3. \quad mMa_i := Maa_i \times \overline{M}aa_i,$$

$$D1.4. \quad K := mMa_1 \times mMa_2(*),$$

$$D1.8. \quad T_i := ta_{i+1} \times ta_{i-1},$$

$$D12.1. \quad at_i := A_i \times T_i,$$

The nomenclature:

N1.5. *(T_i, ta_i) is the tangential triangle,*

N12.1. at_i are the symmedians, of d'Ocagne,

N1.2. K is the point of Lemoine, also called point of Grebe or of Lhuillier.

Proof:

$$P1.2. \quad Maa_0 = (m_0, m_1, m_0), \quad \overline{M}aa_0 = (m_0, m_0, m_2),$$

$$P1.3. \quad mMa_0 = [q_0, m_0(m_2 - m_0), -m_0(m_0 - m_1)],$$

$$P1.4. \quad K = (m_0(m_1 + m_2), m_1(m_2 + m_0), m_2(m_0 + m_1)),$$

$$P1.8. \quad T_0 = (-m_0(m_1 + m_2), m_1(m_2 + m_0), m_2(m_0 + m_1)),$$

$$P12.1. \quad at_0 = [0, m_2(m_0 + m_1), -m_1(m_2 + m_0)],$$

3.1.3 The fundamental $3 * 4 + 11 * 3$ & $3 * 5 + 10 * 3$ configuration.

Introduction.

It would be desirable to have a synthetic proof of the sequence of Theorems given in this and in the following Chapters. In many instances, it is not difficult to obtain it, using the standard Theorems of projective geometry, mainly those of Pappus, Desargues and Pascal. In other cases, the proof is less obvious. Theorem 4.3.1., which can be considered as the starting point, has a first part which required additional constructions. The proof implies the validity of the extension of all the Theorems to finite projective geometries associated to Galois fields of order p^k , $p > 3$ and to the projective geometries associated to the field of rationals, the field of reals, the field of complex numbers, the real p -adic field, the complex p -adic field, For the second part, the proof is synthetic.

Theorem.

Let A_0, A_1, A_2, M and \overline{M} be a complete 5-angle, see Fig. 0,

$$a_i := A_{i+1} \times A_{i-1}$$

$$ma_i := M \times A_i, \quad \overline{ma}_i := \overline{M} \times A_i$$

$$M_i := ma_i \times a_i, \quad \overline{M}_i := \overline{ma}_i \times a_i,$$

$$Maa_i := ma_{i+1} \times \overline{ma}_{i-1},$$

$$cc_i := A_i \times Maa_i,$$

$$P := cc_1 \times cc_2(*),$$

$$CA_i := cc_i \times a_i,$$

$$caa_i := CA_{i+1} \times CA_{i-1},$$

$$c_i := M_{i+1} \times \overline{M}_{i-1},$$

$$CC_i := a_i \times c_i$$

$$p := CC_1 \times CC_2(*),$$

$$\gamma := \text{conic}(M_i, \overline{M}_1, \overline{M}_2)(*).$$
 then

$$CC_i \cdot caa_i = 0.$$

The configuration involves the 14 points $A_i, M_i, \overline{M}_i, C_i, M$ and \overline{M} and the 13 lines $a_i, ma_i, \overline{ma}_i, c_i$ and p .

Proof: For the first part, (see Fig. 0')

$$\text{dual-Pappus}(\langle ma_2, ma_0, ma_1 \rangle, \langle \overline{ma}_1, \overline{ma}_2, \overline{ma}_0 \rangle; \langle cc_0, cc_1, cc_2 \rangle, P),$$

therefore cc_i are incident to P ,

$$\text{Desargues}(P, \{A_i\}, \{CA_i\}; \langle CC_i \rangle, p),$$

therefore $caa_i \times a_i$ are incident to p ,

$Desargues^{-1}(cc_0, \{ma_1, cc_1, a_1\}, \{\bar{m}a_2, cc_2, a_2\}; \langle caa_0, c_0, a_0 \rangle, CC_0)$

therefore caa_0, c_0 and a_0 are incident to CC_0 .

For the second part, the Theorem of Pascal implies that the points $M_0, \bar{M}_0, M_1, \bar{M}_1, M_2, \bar{M}_2$, are on a conic, because the points C_0, C_1 and C_2 are collinear.

The conic may degenerate in two lines. This will occur if, for instance, \bar{M}_0 is on $M_1 \times M_2$ and in this case M_0 is on $\bar{M}_1 \times \bar{M}_2$. Indeed,

Theorem.

Let A_0, A_1, A_2, M and \bar{M} be a complete 5-angle such that \bar{M}_0, M_1 and M_2 are collinear then M_0, \bar{M}_1 and \bar{M}_2 are collinear.

Proof: A synthetic proof is as follows. Let $E := M_0 \times (M \times \bar{M})$, the Theorem of Pappus applied to $A_j M M_j$ and $A_0 \bar{M}_0 \bar{M}$ for $j = 1$ and 2 implies that M_0, E, \bar{M}_j are collinear, therefore M_0, \bar{M}_1 and \bar{M}_2 are collinear.

Theorem.

If $m = [1, 1, 1]$ and $\bar{m} = [m_0, m_1, m_2]$, then with respect to the line conic

$$a_{00}x_0^2 + a_{11}x_1^2 + a_{22}x_2^2 + 2(a_{12}x_1x_2 + a_{20}x_2x_0 + a_{01}x_0x_1) = 0$$

the pole of m is

$$(a_{00} + a_{01} + a_{20}, a_{01} + a_{11} + a_{12}, a_{20} + a_{12} + a_{22})$$

and the pole of \bar{m} is

$$(a_{00}m_1m_2 + a_{01}m_2m_0 + a_{02}m_0m_1, a_{01}m_1m_2 + a_{11}m_2m_0 + a_{12}m_0m_1, a_{20}m_1m_2 + a_{12}m_2m_0 + a_{22}m_0m_1).$$

3.1.4 An overview of theorems associated with bisected angles.

The inscribed circle, the point of Gergonne, the point of Nagel.

Introduction.

I will now give a construction associated to a conic inscribed in a triangle. The degenerate case of the Theorem of Brianchon implies that if JJ_i are the points of contact on $A_{i+1} \times A_{i-1}$, then the lines $A_i \times JJ_i$ pass through a point J . We can choose arbitrarily a point I or its polar i . The construction in Theorem 3.12 determines a pair of points M and \bar{M} which in the case of Euclidean geometry will correspond to the barycenter and to the orthocenter. As will be seen later, the function which associates M, \bar{M} to J, I is not one to one. It is therefore necessary to start with this construction if we want to extend to projective geometry that part of the geometry of the triangle which is related to the inscribed circles. In this case, Part 0. should precede Part 1.

Theorem.

Given a complete 5-angle, 5 distinct points, no 3 of which are on the same line, A_0, A_1, A_2, J and I, A_i are called the vertices,

J , is the *point of Gergonne* and
 I , is the center of the *inscribed circle*.

0. The barycenter and orthocenter derived from the point of Gergonne and the center of the inscribed circle.

Let

- H0.0. A_i , (See Fig. 20b)
H0.2. J, I ,
D0.0. $a_i := A_{i+1} \times A_{i-1}$,
D0.8. $ja_i := J \times A_i$,
D0.9. $JJ_i := ja_i \times a_i$,
D0.10. $j_i := JJ_{i+1} \times JJ_{i-1}$,
D0.11. $Ja_i := j_i \times a_i$,
D0.23'. $ji_i := JJ_i \times I$,
D0.26. $Jia_i := ji_{i+1} \times a_{i-1}$, $Ji\bar{a}_i := ji_{i-1} \times a_{i+1}$,
D0.27. $jia_i := Jia_{i+1} \times Ja_{i-1}$, $ji\bar{a}_i := Jia_{i-1} \times Ja_{i+1}$,
D0.28. $Jai_i := jia_{i+1} \times ji_{i-1}$, $Jai_i := jia_{i-1} \times ji_{i+1}$,
D20.0. $Ji_i := jai_{i+1} \times jai_{i-1}$,
D20.22. $\iota := \text{conic}(JJ_0, JJ_1, JJ_2, Ji_1, Ji_2)(*)$,
D0.5'. $m_i := Jai_i \times Ji\bar{a}_i$,
D0.6. $MM_i := m_{i+1} \times m_{i-1}$,
D0.1'. $ma_i := A_i \times MM_i$,
D0.4'. $MA_i := m_i \times a_i$,
D0.7. $m := MA_1 \times MA_2(*)$,
D0.H. $M := ma_1 \times ma_2(*)$,
D0.25'. $IMa_i := m \times ji_i$,
D0.1'. $\bar{ma}_i := A_i \times I\bar{ma}_i$,
D0.H. $\bar{M} := \bar{ma}_1 \times \bar{ma}_2(*)$,

then

- C0.2. $a_i \cdot \iota = 0$.
C0.5. $m_i \cdot A_i = 0$.
C20.3. ι is a circle = 0.
C20.4. $I = \text{Center}(\iota)$.

The nomenclature:

- N20.3. ι is the inscribed circle,
N0.12. JJ_i are the Gergonian points, these are the points of contact of the inscribed circle with the sides of the triangle.
 Ja_i is the pole of ja_i with respect to the inscribed circle.
 Ji_i is the point of the inscribed circle diametrically opposite to JJ_i .
Again, M is the barycenter and \bar{M} is the orthocenter.

Proof:

For a synthetic proof see section ... G272.tex.

Let $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$, $J = (j_0, j_1, j_2)$, $I = (i_0, i_1, i_2)$,
 m is constructed in such a way that I is the pole of m with respect to ι , therefore if the line m is chosen to be $[1, 1, 1]$, then

0. $I = (j_0(j_1 + j_2), j_1(j_2 + j_0), j_2(j_0 + j_1))$, therefore there is no loss of generality if we set
1. $i_0 := j_0(j_1 + j_2)$, $i_1 := j_1(j_2 + j_0)$, $i_2 := j_2(j_0 + j_1)$. We will use the abbreviations for symmetric functions of j_0, j_1, j_2 using “ p ” instead of “ s ” as used for the symmetric functions of m_0, m_1, m_2 . For instance,
2. $p_{11} = j_1 j_2 + j_2 j_0 + j_0 j_1$.
- P0.0. $a_0 = [1, 0, 0]$.
- P0.8. $ja_0 = [0, j_2, -j_1]$.
- P0.9. $JJ_0 = (0, j_1, j_2)$.
- P0.10. $j_0 = [-j_1 j_2, j_2 j_0, j_0 j_1]$.
- P0.11. $Ja_0 = (0, j_1, -j_2)$.
- P0.23. $ji_0 = [j_1 j_2(j_1 - j_2), j_2 j_0(j_1 + j_2), -j_0 j_1(j_1 + j_2)]$.
- P0.26. $Jia_0 = (j_0(j_2 - j_0), j_1(j_2 + j_0), 0)$, $Ji\bar{a}_0 = (j_0(j_1 - j_0), 0, j_2(j_0 + j_1))$.
- P0.27. $jia_0 = [j_1 j_2(j_0 + j_1), j_2 j_0(j_0 + j_1), j_0 j_1(j_1 - j_0)]$,
 $ji\bar{a}_0 = [j_1 j_2(j_2 + j_0), j_2 j_0(j_2 - j_0), j_0 j_1(j_2 + j_0)]$.
- P0.28. $Jai_0 = (j_0(j_1 + j_2), -j_1 j_2, j_1 j_2)$, $Ja\bar{i}_0 = (j_0(j_1 + j_2), j_1 j_2, -j_1 j_2)$.
- P20.0. $Ji_0 = (j_0(j_1 + j_2)^2, j_1 j_2^2, j_1^2 j_2)$.
- P20.22. $\iota : j_1^2 j_2^2 X_0^2 + j_2^2 j_0^2 X_1^2 + j_0^2 j_1^2 X_0 X_1$
 $- 2j_0 j_1 j_2 (j_0 X_1 X_2 + j_1 X_2 X_0 + j_2 X_0 X_1) = 0$.
 $j^{-1}\theta + \iota = -i \times [j_1^2 j_2^2, j_2^2 j_0^2, j_0^2 j_1^2]$.
 $\iota^{-1} : j_1 j_2 x_1 x_2 + j_2 j_0 x_2 x_0 + j_0 j_1 x_0 x_1 = 0$.
- P0.25. $IMa_0 = (j_0(j_1 + j_2)^2, j_1(j_2^2 - p_{11}), j_2(j_1^2 - p_{11}))$.
- P0.12. $\bar{m}a_0 = [0, j_2(j_1^2 - p_{11}), -j_1(j_2^2 - p_{11})]$.
- P0.16. $\bar{M} = (j_0(j_1^2 - p_{11})(j_2^2 - p_{11}), j_1(j_2^2 - p_{11})(j_0^2 - p_{11}), j_2(j_0^2 - p_{11})(j_1^2 - p_{11}))$.

For m_i , MM_i , ma_i , MA_i , m and M , see 3.7.

The following relations are useful in the derivation of some of the formulas either given above or given below:

0. $m_0 = j_0(j_1^2 - p_{11})(j_2^2 - p_{11})$
1. $m_1 + m_2 = -j_0(j_1 + j_2)^2(j_0^2 - p_{11})$,
2. $m_0(m_1 + m_2) = (j_0(j_1 + j_2))^2 jp$, with
3. $jp = -(j_0^2 - p_{11})(j_1^2 - p_{11})(j_2^2 - p_{11})$
4. $m_1 - m_2 = -(j_1 - j_2)(j_0^2 - p_{11})(p_{11} + j_1 j_2)$
5. $m_0(m_1 - m_2) = -j_0(j_1 - j_2)(p_{11} + j_1 j_2)(j_0^2 - p_{11})$
6. $s_1 = 4j_0 j_1 j_2 p_{11}$,
7. $s_1 + m_0 = j_0(\dots)$,
8. $j_1 m_2 - j_2 m_1 = (j_2^2 - j_1^2)(j_0^2 - p_{11})p_{11}$,
9. $m_1 m_2 = -j_1 j_2(j_0^2 - p_{11})jp$.

3.2 The Geometry of the Hexal Complete 5-Angles.

3.2.0 Introduction.

Section ... contains a synthesis of a very large number of Theorems in Euclidean Geometry, using the presentation introduced in section i. This is followed by a proof given also as in section 1.

The set of Theorems includes some which are always valid, some which are valid when the given triangle has a tangent circle and some which are valid when the point of Steven exits. In the second case I indicate that the definitions and Theorem are meaningful by labeling the section with (J). In the third case I label the section with (Mu), if neither case apply I label the section with (M). Definitions and conclusions contained in sections without (M), (J) or (Mu) are always meaningful.

I start with a triangle $\{A_i\}$.

In case (M), I choose the barycenter M and the orthocenter \overline{M} .

In case (Mu), I choose the barycenter $M = (m_0, m_1, m_2)$ and the point of Steven,

$Mu = (\sqrt{m_0}, \sqrt{m_1}, \sqrt{m_2})$. This assumes that km_0, km_1 and km_2 are quadratic residues for some k . I then determine the orthocenter from M and Mu .

In case (J), I assume that the triangle has a tangent circle and derive the orthocenter from the barycenter and the point of Gergonne J . The point \overline{J} , if it exist is such that the constructions obtained by use \overline{J} instead of J give eventually \overline{M} instead of M and vice-versa. If the \overline{J} does not exist these constructions are meaningless. The construction in the rightmost column of the sections marked with (J) should therefore be ignored.

At the end of section 0, whatever the variant, the ideal line and orthic line have been constructed as well as the medians and altitudes, mid-points, the feet, and the complemantary and anticomplemantary triangles.

In section 1, we construct the line eul of Euler, the point K of Lemoine, the circumcircle θ and the circle γ of Brianchon-Poncelet. Hypothesis ...

Because in finite geometry If the section starts with (M), (J) or (Mu), it is only to In this Chapter, I will give systematically most of the results which generalize the known results of the geometry of the triangle in classical Euclidean geometry. In 5.1. and in 5.4. the corresponding constructions can be done with the ruler alone. In 5.5. the corresponding constructions in classical Euclidian geometry would require also the compass. (#) is used to indicate Theorems obtained starting June 10, 1982, by systematically obtaining incidence relations on 2 examples and verifying that the conjecture so obtained is indeed a Theorem.

What corresponds to isotropic points and foci of conics in the hexal complete 5-angles configuration is given in 5.2. and what corresponds to perpendicular directions, in 5.3. A summary of all incidence properties obtained in this Chapter is given in 5.7. to allow an easier access to the results.

3.2.1 The points of Euler, the center of the circle of Brianchon-Poncelet, and of the circumcircle, the points of Schröter, the point of Gergonne of the orthic triangle, the orthocentroidal circle.

Theorem.

Given a complete 5-angle, 5 distinct points, not 3 of which are on the same line, A_0, A_1, A_2, M and \overline{M} , The vertices A_i are those of a triangle, M is the *barycenter* and \overline{M} is the *orthocenter*.

Proof of Theorem 5.1.1.

The algebraic proof will be summarized by giving the coordinates of the points and lines constructed in 5.1.1. The incidence properties follow from straightforward computation of scalar products or substitution in the equation of the conics.

For triples, the coordinates of the 0-th subscript will be given. The coordinates of subscript 1 and 2 are obtained by applying the mapping ρ and ρ^2 to it. ρ is defined as follows, we substitute m_1, m_2, m_0 for m_0, m_1, m_2 in each of the components, and rotate these, the 0-th coordinate becoming the first, the first coordinate becoming the second and the second coordinate becoming the 0-th. For instance, from em_0 of 5.0. we get

$$em_1 = [s_1 + m_1, m_2 - m_0, -(s_1 + m_1)] \text{ and } em_2 = [-(s_1 + m_2), s_1 + m_2, m_0 - m_1].$$

The hypothesis imply, $m \neq 0, m \neq 0, m \neq 0, m \neq m_2, m \neq m_0$ and $m \neq m_1$.

I will use the usual abbreviations for the symmetric functions,

$$\begin{aligned} s_1 &:= m_0 + m_1 + m_2, s_{11} := m_1 m_2 + m_2 m_0 + m_0 m_1, \\ s_2 &:= m_0^2 + m_1^2 + m_2^2, \text{ etc.} \end{aligned}$$

and

$$q_0 := m_0^2 - m_1 m_2, q_1 := m_1^2 - m_2 m_0, q_2 := m_2^2 - m_0 m_1,$$

and the identity

$$(m_1 + m_2)(m_2 + m_0)(m_0 + m_1) = s_{211} + 2s_{111}.$$

The dual of the reciprocal of all elements have also been included.

Comment.

To determine in succession the homogeneous coordinates, we have used the definition. To check the results, if for instance $x := P \times Q$, we can simply verify $x \cdot P = x \cdot Q = 0$. The construction asserts implicitly that for $x := P \times Q$, in general, P and Q are distinct, in other words for some value of p and some \overline{M} , P and Q are distinct. It may of course happen that for a particular example $P = Q$, 2 cases are possible, the coordinates of x , for this example, are not all 0, this means that some alternate construction, using for instance one of the conclusions, will determine x , in the other case, x can not be constructed. For instance, for $p = 37$ and $\overline{M} = (202) = (1, 4, 16)$, $Ste = AA_1 = (880)$, but $stAA_1 = (472) = (1, 11, 27)$ is well defined but cannot be obtained using $Ste \times AA_1$. On the hand, for any p , if $\overline{M} = (1, p-1, p-1)$, $\overline{F}_0 = M_0 = (0, 1, 1)$ and $\overline{f}m_0 = (0, 0, 0)$ and is therefore undefined.

Comment.

The determination of a conic, with known intersections $X1, X2$ with a_0 , $Y1, Y2$ with b_0 and $Z1, Z2$ with a_2 , can be obtained easily.

3.2.2 Isotropic points and foci of conics.**Introduction.**

The following pairs of point can not be obtained by the construction involving only intersection of known lines or lines through known points, they are sufficiently important to be defined.

Definition.

$$I, I' = m \times \gamma, \bar{I}, \bar{I}' = \bar{m} \times \gamma.$$

The first pair corresponds to the isotropic points, the second pair to the co-isotropic points.

Theorem.

With the definitions of Theorem 5.1, we have

$$\begin{aligned} \bar{I}, \bar{I}' &= (m_0(m_1 + m_2), -m_1(m_2 + j\sigma), -m_2(m_1 - j\sigma)), \\ j &= +1 \text{ or } -1, \sigma := \sqrt{-s_{11}}, \\ I, I' &= (m_0(m_1 + m_2), -m_0m_1 - j\tau, -m_2m_0 + j\tau), \text{ where} \\ j &:= +1 \text{ or } -1, \tau := \sqrt{-m_0m_1m_2s_1}. \end{aligned}$$

Definition.

F is a focus of a non degenerate conic iff both $F \times I$ and $F \times \bar{I}$ are tangent to the conic.

Theorem.

If the conic is not a parabola, there are 4 foci, real or complex.

3.2.3 Perpendicular directions.**Definition.**

Two directions IA and IB are perpendicular iff one direction is on the polar of the other with respect to any circle. We will write $IA \perp IB$.

Theorem.

Let (X_0, X_1, X_2) be an ideal point, the perpendicular direction is

$$(m_0(m_1X_2 - m_2X_1), m_1(m_2X_0 - m_0X_2), m_2(m_0X_1 - m_1X_0)),$$

Theorem.

(X_0, X_1, X_2) and (Y_0, Y_1, Y_2) are perpendicular directions if

$$0. \quad m_1 m_2 X_0 Y_0 + m_2 m_0 X_1 Y_1 + m_0 m_1 X_2 Y_2 = 0.$$

Theorem.

The following are perpendicular directions. Let D0. $Imeul = (s_1 - 3m_0, s_1 - 3m_1, s_1 - 3m_2)$,

then

$$C0. \quad MA_i \perp I\overline{m}a_i.$$

$$C1. \quad Im_i \perp I\overline{m}_i.$$

$$C2. \quad I \perp I', I' \perp I'.$$

$$C3. \quad EUL \perp Imeul.$$

See also C12.4, C12.5, C16.7,

Exercise.

Construct Imeul of the preceding Theorem.

3.2.4 The circle of Taylor, the associated circles, the circle of Brocard the points of Tarry and Steiner, the conics of Simson and of Kiepert, the associated circumcircles, the circles of Lemoine.

Introduction.

Besides the properties given in Theorem 5.1.1., many other properties of Euclidean geometry generalize to projective geometry. These will now be stated. The numeration started in Theorem 5.1.1. is continued.

Theorem.

Given the hypothesis of Theorem 5.1.1. and the points and lines defined (or constructed) in that Theorem.

Notation.

To make some of the algebraic expression less cumbersome, we have often used the symmetric functions

$$s_1 := m_0 + m_1 + m_2,$$

$$s_{11} := m_1 m_2 + m_2 m_0 + m_0 m_1,$$

$$s_2 := m_0^2 + m_1^2 + m_2^2,$$

$$s_{21} := m_0^2(m_1 + m_2) + m_1^2(m_2 + m_0) + m_2^2(m_0 + m_1).$$

and similarly in the equations for conics other symmetric functions. We have also used, at times,

$q_0 := m_0^2 - m_1m_2, q_1 := m_1^2 - m_2m_0, q_2 := m_2^2 - m_0m_1,$
and the following identities in the calculations:
 $m_1q_0 + m_2q_1 + m_0q_2 = 0$ and $m_2q_0 + m_0q_1 + m_1q_2 = 0.$

Proof of Theorem 5.4.1..

The proof is given in the same way as the proof of 5.1.1.

Proof of Theorem 5.4.3., P.15.16..

The details of the proof to obtain the equation of the circle of Brocard will now be given. The equation of a conic which has the radical axis m with the circle γ is

$$0. m_0(m_1 + m_2)X_1X_2 + m_1(m_2 + m_0)X_2X_0 + m_2(m_0 + m_1)X_0X_1 \\ + (X_0 + X_1 + X_2)(u_0x_0 + u_1x_1 + u_2x_2) = 0.$$

u_0, u_1 and u_2 are determined in such a way that the conic passes through $Br3_i$. For $Br3_0$ we have

$$X_0 + X_1 + X_2 = 4m_1m_2 + m_2m_0 + m_0m_1,$$

and for the first line of 0.

$$(4m_1m_2 + m_2m_0 + m_0m_1)(m_1m_2(m_2 + m_0)(m_0 + m_1)).$$

Hence we have to solve

$$2m_1m_2u_0 + m_1(m_2 + m_0)u_1 + m_2(m_0 + m_1)u_2 + m_1m_2(m_2 + m_0)(m_0 + m_1) = 0, \\ m_0(m_1 + m_2)u_0 + 2m_2m_0u_1 + m_2(m_0 + m_1)u_2 + m_2m_0(m_0 + m_1)(m_1 + m_2) = 0, \\ m_0(m_1 + m_2)u_0 + m_1(m_2 + m_0)u_1 + 2m_0m_1u_2 + m_0m_1(m_1 + m_2)(m_2 + m_0) = 0.$$

Replacing u_0, u_1 and u_2 in terms of v_0, v_1 and v_2 , given by

$$v_0 := \frac{u_0}{m_1m_2}, v_1 := \frac{u_1}{m_2m_0}, v_2 := \frac{u_2}{m_0m_1}, \text{ we get} \\ 2m_1m_2v_0 + m_1(m_2 + m_0)v_1 + m_2(m_0 + m_1)v_2 + (m_2 + m_0)(m_0 + m_1) = 0, \\ m_0(m_1 + m_2)v_0 + 2m_2m_0v_1 + m_2(m_0 + m_1)v_2 + (m_0 + m_1)(m_1 + m_2) = 0, \\ m_0(m_1 + m_2)v_0 + m_1(m_2 + m_0)v_1 + 2m_0m_1v_2 + (m_1 + m_2)(m_2 + m_0) = 0.$$

The determinant is $D = -6s_{222} + 2s_{33}$. The numerator for v_0 is $E(m_0 + m_1)(m_2 + m_0)$ with $E = (s_{211} - s_{22})$.

Hence the solution for u_0 .

To obtain P15.16., we have to determine

$$u_1 + u_2 + m_0(m_1 + m_2) = \frac{m_0(m_1 + m_2)(D + Es_{11} + Em_1m_2)}{D} \\ = \frac{m_0(m_1 + m_2)(-3s_{222} + s_{33} + Em_1m_2)}{D},$$

because $Es_{11} = s_{211}s_{11} - s_{22}s_{11}$. But $(s_{211} - s_{22})s_{11} = 3s_{222} - s_{33}$, hence the equation for PUB.

To obtain the relation between θ and β , knowing that

$$A\theta + \beta = B(m) \times (lem),$$

it is easy to obtain A and B , for instance, $K.\beta$ gives

$$A(3m_0m_1m_2(m_1 + m_2)(m_2 + m_0)(m_0 + m_1)) \\ = B(2s_{11}3m_0m_1m_2(m_1 + m_2)(m_2 + m_0)(m_0 + m_1))$$

therefore with $B = 1, A = 2s_{11}$.

ADD PERPENDICULARITY, e.g. $IiI_i \perp Iai_i$. Cross refer. at end of G2705

3.2.5 Theorems associated with bisected angles. The outscribed circles, the circles of Spieker, the point of Feuerbach, the barycenter of the exccribed triangle.

Introduction.

I will now give a construction associated to a conic inscribed in a triangle. The degenerate case of the Theorem of Brianchon implies that if JJ_i are the points of contact on $A_{i+1}A_{i-1}$, then the lines $A_i \times JJ_i$ pass through a point J . We can choose arbitrarily a point I or its polar i . The construction in Theorem 5.5.1. determines a pair of points M and \bar{M} which in the case of Euclidean geometry will correspond to the barycenter and to the orthocenter. As will be seen later, the function which associates M, \bar{M} to J, I is not one to one. It is therefore necessary to start with this construction if we want to extend to projective geometry that part of the geometry of the triangle which is related to the inscribed circles. Part 0. should therefore precede Part 1. of Theorem 5.1.1. Part 20. given next follows Part 19. of Theorem 5.1.1.

IN THE NEXT SECTION REVERSE THE ORDER. FIRST SHOW THAT THE point diametrically opposed to JJ_0 is on the line $m_0 \times j_2 \times JJ_1$, then that $m_0 \times j_2$ is on the line $j_0 \times a_0$ and $ij_0 \times a_1$

STUDY from which it follows that $m_0 \times j_2$ defines m_0 with A_0 and can be obtained from JJ_i .

Heuristics.

Before giving the construction I will look back at Euclidean geometry and determine properties which have guided me in the construction given below. Let I be the center of the circle ι inscribed in the triangle (A_0, A_1, A_2) , let JJ_i be the point of contact with a_i , let m_i be the parallel to a_i through A_i .

First, if $Ja_0 := j_0 \times a_0$, $Jia_2 := a_1 \times ji_0$, and $Jai_0 := j_2 \times m_0$, then Ja_0 , Jia_2 and Jai_0 are collinear because they are the Pascal points of the hexagon with cords or tangents $j_0, a_1, j_2, a_0, ji_0, jai_1$. If we start from A_i , J and I we can therefore construct JJ_i , Ja_0 , Jia_2 , Jai_0 and m_0 , hence $MA_0 := a_0 \times m_0$, similarly we can construct MA_1 and therefore the ideal line $m := MA_0 \times MA_1$. (The construction below is a variant which uses a "symmetric" point \bar{Jai}_0 also on m_0 .) From m we can derive the barycenter M as the polar of m with respect to the triangle $\{A_i\}$. Next, the conic through JJ_i with tangent a_1, a_2 can be defined as a circle, the altitude $\bar{m}a_0$ can be obtained as parallel to $I \times JJ_0$ and therefore the orthocenter \bar{M} can be constructed.

Finally, let $jai_1 := Jai_0 \times JJ_2$ and $Ji_0 := jai_1 \times ji_0$, I claim that Ji_0 is on the inscribed circle. Indeed, first the triangles $(JJ_{i-1}, A_i, JJ_{i+1})$ are isosceles triangles, then, for $i = 0$, the triangle (JJ_1, A_0, Jai_0) which is similar to the triangle (JJ_1, A_2, JJ_0) is therefore an isosceles triangle and $|A_0, Jai_0| = |A_0, JJ_1| = |A_0, JJ_2|$. Therefore $\text{angle}(A_0, JJ_2, Jai_0) = \frac{1}{2}(\pi - \text{angle}(JJ_2, A_0, Jai_0)) = \frac{1}{2}\text{angle}(A_0, A_1, A_2) = \text{angle}(A_0, A_1, I)$, therefore j_0 is parallel to $A_1 \times I$ and therefore perpendicular to j_1 , it follows that (Ji_0, JJ_0) is a diameter.

We can therefore construct Ji_0 on ι .

Proof of Theorem 5.5.2..

0. *Asynthetic proof of ... is as follows. Pascal's Theorem gives*

$$ct(ji_0, a_0, j_1, a_2, j_0, j\bar{a}i_2?) = (J\bar{a}i_1, Ja_0)$$

$$\Rightarrow J\bar{a}i_0 \Rightarrow j\bar{a}i_2 \Rightarrow Ji_0.$$

$$ct(ji_0, a_0, j_2, a_1, j_0, j\bar{a}i_1?) = (Jia_2, Ja_0)$$

$$\Rightarrow J\bar{a}i_0 \Rightarrow j\bar{a}i_1 \Rightarrow Ji_0, \text{ hence 0.0 and 0.2.}$$

$$ct(j_2, a_1, j\bar{a}i_2, j\bar{a}i_1, a_2, j_1) = (Jai_0, A_0, J\bar{a}i_0),$$

which are therefore collinear, hence 0.3.

$$ct(j\bar{a}i_1, j_1, a_0, j_2, j\bar{a}i_2, \text{tangent}(Ji_0)) =$$

$$(Jai_0, J\bar{a}i_0, MA_0), \text{ hence 0.4.}$$

Im_i is the pole of ji_i, therefore i is the polar of I, hence 0.5.

The coordinates of the various points are easy to derive. Let $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$, $J = (j_0, j_1, j_2)$, $I = (i_0, i_1, i_2)$, m is constructed in such a way that I is the pole of m with respect to ' ι ', therefore if the line m is chosen to be $[1, 1, 1]$, then

1. $I = (j_0(j_1 + j_2), j_1(j_2 + j_0), j_2(j_0 + j_1))$, *therefore there is no loss of generality if we set*

2. $i_0 := j_0(j_1 + j_2)$, $i_1 := j_1(j_2 + j_0)$, $i_2 := j_2(j_0 + j_1)$.

We will use the abbreviations for symmetric functions of j_0, j_1, j_2 using "p" instead of "s" as used for the symmetric functions of m_0, m_1, m_2 . For instance,

3. $p_{11} = j_1j_2 + j_2j_0 + j_0j_1$. *We have also expressed the coordinates in terms of i_0, i_1 and i_2 . The symmetric functions of i_0, i_1 and i_2 use "o" instead of "s". The expression of j_0, j_1 and j_2 in terms of i_0, i_1 and i_2 is given by*

4. $j_0 = \frac{(o_1 - 2i_1)(o_1 - 2i_2)}{ip}$, \dots , *where*

5. $ip^2 = 2(o_1 - 2i_0)(o_1 - 2i_1)(o_1 - 2i_2)$. *This alternate notation has the advantage that the information on the associate construction for the excribed circles is obtained by replacing either i_0 by $-i_0$, or i_1 by $-i_1$, or i_2 by $-i_2$.*

Proof of Theorem 5.5.2., P21.8.

The proof of the preceding theorem is straightforward, I will only give details for the determination of π : Let \mathbf{C} be the symmetric matrix associated to the polarity of π , let \mathbf{M} be the matrix whose i -th column are the coordinates of m_i , let \mathbf{J} be the matrix whose i -th column are the coordinates of Mna_i , let \mathbf{K} be a diagonal matrix of unknown scaling factors k_0, k_1, k_2 .

$$\mathbf{CJ} = \mathbf{MK} \text{ or } \mathbf{C} = \mathbf{MKJ}^{-1}$$

expresses the fact that m_i is the polar of Mna_i .

$$\mathbf{J}^{-1} = \begin{pmatrix} p_{11} & 2j_0j_1 - p_{11} & 2j_2j_0 - p_{11} \\ 2j_0j_1 - p_{11} & p_{11} & 2j_1j_2 - p_{11} \\ 2j_2j_0 - p_{11} & 2j_1j_2 - p_{11} & p_{11} \end{pmatrix}.$$

The problem is now reduced to a set of 3 homogeneous equations in the unknowns k_0, k_1, k_2 ,

which express the symmetry of \mathbf{C} , namely, after simplification,

$$-j_0j_1k_0 + j_0j_1k_1 + j_2(j_1 - j_0)k_2 = 0,$$

$$j_0(j_2 - j_1)k_0 - j_1j_2k_1 + j_1j_2k_2 = 0,$$

$$j_2j_0k_0 + j_1(j_0 - j_2)k_1 - j_2j_0k_2 = 0,$$

giving $k_0 = j_1j_2$, $k_1 = j_2j_0$, $k_2 = j_0j_1$.

Comment.

The following alternate definition for Nagel's point which is clearly more clumsy:

$$oi := O \times I,$$

$$Ioi := i \times oi,$$

$$n\overline{m} := \overline{M} \times Ioi,$$

$$N := n\overline{m} \times mi,$$

We have

$$oi = [j_1j_2(j_1 - j_2)(j_2 + j_0)(j_0 + j_1), j_2j_0(j_2 - j_1)(j_0 + j_1)(j_1 + j_2),$$

$$j_0j_1(j_0 - j_2)(j_1 + j_2)(j_2 + j_0)],$$

$$Ioi = (j_0(j_1 + j_2)(p_{21} - 2j_0p_{11}), \dots),$$

$$n\overline{m} = [j_0(j_1^2 - j_2^2)(j_0^2 - p_{11}), \dots], \text{ done backward from } N.$$

We also have

$$mj = [j_1 - j_2, j_2 - j_0, j_0 - j_1],$$

Comment.

An alternate method to obtain quickly the relation between the barycentric coordinates of the point of Gergonne and of the orthocenter is as follows.

Let $n_0 = m_0(m_1 + m_2)$, \dots , we know that are circles are

$$n_0x_1x_2 + \dots - (X_0 + X_1 + X_2)(u_0X_0 + \dots) = 0.$$

the line equation of the inscribed circle is

$$j_1j_2x_1x_2 + \dots = 0$$

to express that it is a circle we can use

$$\mathbf{A} = 2\text{adjoint}(\mathbf{B}),$$

where \mathbf{A} is the polarity matrix associated to the general circle and \mathbf{B} the matrix associated to (2). The constant is arbitrary and reflect the chosen scaling.

$$\mathbf{A} = \begin{pmatrix} -2u_0 & n_2 - u_0 - u_1 & n_1 - u_2 - u_0 \\ n_2 - u_0 - u_1 & -2u_1 & n_0 - u_1 - u_2 \\ n_1 - u_2 - u_0 & n_0 - u_1 - u_2 & -2u_2 \end{pmatrix}, \mathbf{B} = \begin{pmatrix} 0 & j_0j_1 & j_2j_0 \\ j_0j_1 & 0 & j_1j_2 \\ j_2j_0 & j_1j_2 & 0 \end{pmatrix}.$$

This gives at once

$$u_0 = (j_1j_2)^2 \text{ and}$$

$$n_0 = 2j_0^2j_1j_2 + u_1 + u_2 = (j_0(j_1 + j_2))^2.$$

Comment.

To obtain the points of contact of the outscribed circle ι_0 , Let J_0 be the corresponding point of Gergonne $[g_0, g_1, G_2]$. We have

$$g_0(g_1 + G_2) = -j_0(j_1 + j_2),$$

$$g_1(G_2 + g_0) = j_1(j_2 + j_0),$$

$$G_2(g_0 + g_1) = j_2(j_0 + j_1),$$

adding 2 equations and subtracting the third gives

$$g_1 G_2 = p_{11}, G_2 g_0 = -j_0 j_1, g_0 g_1 = -j_2 j_0, \text{ with } p_{11} = j_1 j_2 + j_2 j_0 + j_0 j_1.$$

Hence with an appropriate constant of proportionality,

$$(g_0, g_1, G_2) = (-j_0 j_1 j_2, j_2 p_{11}, j_1 p_{11}).$$

Therefore the points of contact with a_0 , a_1 and a_2 are

$$Na_0 = (0, j_2, j_1), Nai_0 = (j_2 j_0, 0, -p_{11}), Na\bar{i}_0 = (j_0 j_1, -p_{11}, 0).$$

Theorem.

The isogonal transformation of J is

$$\begin{aligned} isog(J) &= (j_0(j_1 + j_2)^2, j_1(j_2 + j_0)^2, j_2(j_0 + j_1)^2, \\ &\quad -j_0 j_1(j_2 + j_0)(j_1 + j_2)), \end{aligned}$$

Proof:

$$\begin{aligned} x_0 &= [-j_1 j_2, j_2 j_0, j_0 j_1], \\ X_0 &= (j_0(j_2 + j_1), j_1(j_2 + j_0), -j_2(j_0 + j_1)), \\ Y_0 &= (j_0(j_2 + j_0), j_1(j_2 + j_0), 2j_2 j_0), \\ y_0 &= [j_1 j_2(j_2 + j_0)(j_0 + j_1), j_2 j_0(j_0 j_1 - j_1 j_2 + 3j_2 j_0 + j_0^2), \\ Z_0 &= (j_0(j_1^2 + j_2^2 - j_1 j_2 - j_0 j_1), j_1(j_2 + j_0)^2, j_1(j_0 + j_1)^2), \\ z_0 &= [0, j_2(j_0 + j_1)^2, -j_1(j_2 + j_0)^2], \text{ hence the Theorem.} \end{aligned}$$

Definition.

Many other constructions can be easily derived from the following operation called the dual construction. Instead of the quintuple A_i, M, \bar{M} , consider instead the quintuple $A_i, M, \bar{M}' := T\bar{m}m$.

The construction associated to every point $X = (X_0, X_1, X_2)$, a point X' whose coordinates are the reciprocal $X' = (X_1 X_2, X_2 X_0, X_0 X_1)$ and to every line $x = (x_0, x_1, x_2)$ the reciprocal $x' = (x_1 x_2, x_2 x_0, x_0 x_1)$.

A few of the dual points and lines are not new but most are and lead easily to the construction of important points and lines. See for instance the exercise on the line of Longchamps. We have $ma'_i = ma_i$, $M'_i = M_i$, $m'_i = m_i$, $Im'_i = Im_i$, $AC'_i = AC_i$, $i' = i$, $O' = K$, $oa'_i = at_i$, $\bar{S}' = \bar{S}$, $Ima'_i = Ima_i$, $K' = O$, $ok' = ok$.

An example is given in ex3.3.

Corollary.

We can now summarize incidence properties associated with the historically important line of Euler and circle of Brianchon- Poncelet.

0. The following 14 points are on the line of Euler: the barycenter M , the orthocenter \bar{M} , the point PP of D3.3, the center EE and cocenter $\bar{E}E$ of the circle of Brianchon-Poncelet, the center O and cocenter \bar{O} of the circumcircle, the points $Am, \bar{A}m$ of D7.9, the points D_i of D8.4, the center G and the cocenter \bar{G} of the orthocentroidal circle.

1. The following 24 points are on the conic of Brianchon-Poncelet: the midpoints M_i , the feet \overline{M}_i , the Euler points E_i , \overline{E}_i , the points F_i and \overline{F}_i of D6.2, points of Schröter S and \overline{S} , the points of Feuerbach, Fe and Fe_i .

The complete set of incidence properties are given in detail in section 5.7.

Comment.

Given the algebraic coordinates of a point it is sometimes difficult to obtain a construction starting from M and \overline{M} . One additional tool is provided by using homologies. We will give here an example, which allows the easy construction of other points on the line of Euler.

Definition.

A barycentric homology is a homology with center M and axis m .

Example.

One such homology and its inverse is

$$\mathbf{D} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \mathbf{D}^{-1} = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{pmatrix}.$$

Theorem.

The transforms of the 14 points on the line of Euler, given in 5.10.0 are as follows:

$$\mathbf{D}(M) = M,$$

$$\mathbf{D}(\overline{M}) = O,$$

$$\mathbf{D}(PP) = (q_1 + q_2, q_2 + q_0, q_0 + q_1),$$

$$\mathbf{D}(EE) = (3s_1 - m_0, 3s_1 - m_1, 3s_1 - m_2),$$

$$\mathbf{D}(\overline{EE}) = (3s_{11} - m_1m_2, 3s_{11} - m_2m_0, 3s_{11} - m_0m_1),$$

$$\mathbf{D}(O) = EE,$$

$$\mathbf{D}(\overline{O}) = (s_{21} - m_0^2(m_1 + m_2), s_{21} - m_1^2(m_2 + m_0), s_{21} - m_2^2(m_0 + m_1)),$$

$$\mathbf{D}(Am) = \overline{M},$$

$$\mathbf{D}(\overline{Am}) = (s_{21} - s_{111} - m_0s_{11}, s_{21} - s_{111} - m_1s_{11}, s_{21} - s_{111} - m_2s_{11}),$$

$$\mathbf{D}(D_0) = (m_0(m_1 + m_2) - 2m_1m_2, m_0(m_2 + m_0) - 2m_1m_2, m_0(m_0 + m_1) - 2m_1m_2),$$

$$\mathbf{D}(G) = (5s_1 - 3m_0, 5s_1 - 3m_1, 5s_1 - 3m_2),$$

$$\mathbf{D}(\overline{G}) = (s_{21} - 9s_{111} - m_0s_{11}, s_{21} - 9s_{111} - m_1s_{11}, s_{21} - 9s_{111} - m_2s_{11}),$$

Exercise.

Complete the table for the inverse transform, $\mathbf{D}T^{-1}T(M) = M$,

$$\mathbf{D}T^{-1}T(\overline{M}) = (s_1 - 3m_0, s_1 - 3m_1, s_1 - 3m_2).$$

Observe that $\mathbf{D}T^{-1}T(\overline{M}).m = 0$.

3.2.6 Duality and symmetry for the inscribed circle.

Introduction.

...

Theorem.

If $m_1 + m_2$, $m_2 + m_0$ and $m_0 + m_1$ are all quadratic residues or or non quadratic residue, then both the dual of the inscribed circle and the symmetric of the inscribed circle are real. Moreover, if i and j are the dual of I and J and if \bar{I} and \bar{J} are the symmetric of I and J then

0. $i = [\sqrt{m_1 + m_2}, \sqrt{m_2 + m_0}, \sqrt{m_0 + m_1}]$,
1. $j = [(-i_0 + i_1 + i_2)^{-1}, (i_0 - i_1 + i_2)^{-1}, (i_0 + i_1 - i_2)^{-1}]$
and
2. $\bar{I} = (m_0 i_0, m_1 i_1, m_2 i_2)$,
3. $\bar{J} = (m_0 j_0, m_1 j_1, m_2 j_2)$,

Proof:

For the symmetric case, $\bar{I} \times (a_0 \times (A_0 \times \bar{J}))$, $A_0 \times MA_0$ and \bar{m} are concurrent, moreover \bar{I} is the pole of \bar{m} with respect to ι .

Therefore,

4. $\bar{J}_1(\bar{I}_2 m_0(m_1 + m_2) + \bar{I}_0 m_1 m_2) = \bar{J}_2(\bar{I}_0 m_1 m_2 + \bar{I}_1 m_0(m_1 + m_2))$,
and in view of P0.15,
5. $\bar{I}_0 = \bar{J}_0 \bar{J}_1 m_2 m_0 + \bar{J}_2 \bar{J}_0 m_0 m_1$. This relation and the 2 others obtained by circularity give
$$-\bar{I}_0 m_1 m_2 + \bar{I}_1 m_2 m_0 + \bar{I}_2 m_0 m_1 = 2\bar{J}_2^{-1} m_2$$

Using 4, we get

$$\bar{I}_0^2 \frac{(m_2 - m_1)}{m_0^2} - \bar{I}_1^2 \frac{(m_1 + m_2)}{m_1^2} + \bar{I}_2^2 \frac{(m_1 + m_2)}{m_2^2} = 0,$$

as well as 2 other similar equations. These equations are compatible and give using the minors

$$(\frac{\bar{I}_0}{m_0})^2 = m_1 + m_2, (\frac{\bar{I}_1}{m_1})^2 = m_2 + m_0, (\frac{\bar{I}_2/m_2}{})^2 = m_0 + m_1.$$

For the dual case, it follows from .1 and .6 (G2722), that the coordinates of I are proportional to $\sqrt{m_0(m_1 + m_2)}$, ..., those of the dual are obtained by replacing m_0 by $m_1 m_2$,

Theorem.

If m_0 , m_1 and m_2 are all quadratic residues or all non quadratic residues, then the dual of the symmetric of the inscribed circle is real. Moreover if \bar{j} and \bar{i} are the dual of the symmetric of J and I , then

$$\begin{aligned}
0. \bar{i} &= [\sqrt{\frac{m_1+m_2}{m_0}}, \sqrt{\frac{m_2+m_0}{m_1}}, \sqrt{\frac{m_0+m_1}{m_2}}], \text{ and} \\
1. \bar{j} &= [(m_0(-m_0\bar{i}_0 + m_1\bar{i}_1 + m_2\bar{i}_2))^{-1}, \\
&\quad (m_1(m_0\bar{i}_0 - m_1\bar{i}_1 + m_2\bar{i}_2))^{-1}, \\
&\quad (m_2(m_0\bar{i}_0 + m_1\bar{i}_1 - m_2\bar{i}_2))^{-1}].
\end{aligned}$$

Example.

For $p = 29$, if $M = (60)$ and $\bar{M} = (258) = (1, 7, 25)$, $(1, \frac{m_2+m_0}{m_1+m_2}, \frac{m_0+m_1}{m_2+m_0}) = (1, -1, -7)$, with a choice of the square roots, $i_0 = 1$, $i_1 = -12$, $i_2 = -14$, hence $i = [538]$ and $j = [1, -2, -9] = [833]$. Moreover $\bar{I} = (1, 3, -2) = (144)$, and $\bar{J} = (1, -14, 7) = (472)$. $(m_0, m_1, m_2) = (1, 7, 25)$, with a choice of the square roots, $(\sqrt{m_0}, \sqrt{m_1}, \sqrt{m_2}) = (1, 6, 5)$, hence $\bar{i} = [1, -2, 3] = [816]$ and $\bar{j} = [1, 7, -14] = [248]$. then $J = (164)$, $I = (448)$, $\bar{I} = (144)$, $\bar{J} = (472)$, and $i = [538]$, $j = [833]$, $\bar{i} = [816]$, $\bar{j} = [248]$.

3.2.7 Summary of the incidence properties obtained so far**Introduction.**

The incidence properties of points, lines and conics will now be summarized. There are several reasons for doing this. First, having so many elements, it is difficult to keep in ones mind at any one time all of the properties given above. Second, it is important to insure that the elements obtained are in general distinct. Third, it is important to obtain from the elements defined any incidence properties not already discovered. For this purpose, I create a program, which, for given examples, determine all incidence properties, by comparison, it was possible to eliminate a few incidence properties which were peculiar to a given example, for the others attempting an algebraic proof determined if the incidence property was indeed general. Quite a few new Theorems were obtained in this way. They have been indicated by (#).

I have ordered them in the order of the definitions. The notation is self explanatory.

Theorem.

The incidence properties are as follows:

Proof of Theorem 6.1.1.**Exercise.**

Construct the vertical tangent of the parabola of Kiepert and prove that it is

$$\begin{aligned}
&[m_0(m_1 - m_2)(s_1 - 3m_1)(s_1 - 3m_2), m_1(m_2 - m_0)(s_1 - 3m_2)(s_1 - 3m_0), \\
&m_2(m_0 - m_1)(s_1 - 3m_0)(s_1 - 3m_1)].
\end{aligned}$$

Exercise.

Construct the conic of Jerabek (Vigarie, N.99),

$$\begin{aligned}
&m_0(m_1^2 - m_2^2)X_1X_2 + m_1(m_2^2 - m_0^2)X_2X_0 \\
&+ m_2(m_0^2 - m_1^2)X_0X_1 = 0.
\end{aligned}$$

Comment.

There exist a large number of conditional theorems. For instance, if $s_{21} + 12s_{11} = 0$ then $G \cdot \bar{i} = \bar{G} \cdot i = 0$.

An example is provided by $p = 29$, $m_0 = 1$, $m_1 = 6$, $m_2 = 11$, corresponding to $J = 94$, $I = 315$.

Exercise.

The line of Simson.

Let

D.0. $Y_i := X \times Im_i$,

D.1. $y := Y_1 \times Y_2$,

H.0. $X \cdot \theta = 0$,

then

C.0. $Y_0 \cdot y = 0$.

P.0. $Y_0 = ()$,

P.1. $y = [(m_1 + m_2)(X_1 + X_2) - m_0 X_0]X_1 X_2, ((m_2 + m_0)(X_2 + X_0) - m_1 X_1)X_2 X_0, ((m_0 + m_1)(X_0 + X_1) - m_2 X_2)X_0 X_1]$.

Exercise.

The excribed circles.

Let `iii[i] := radical axis(iota[i+1],iota[i-1])`,

then

`iii[i]\cdot En = 0`.

Ex g277, `iii[] = [647,435,847]`,

Ex4.0, `iii[] = [873,651,964]`,

Ex5.0, `iii[] = [723,837,965]`.

The conic of Neuberg. (Mathesis, Ser.2, Vol.6, p. 95).

P40.2. 'Neuberg: $m_0 m_1 m_2 (m_0 X_0^2 + m_1 X_1^2 + m_2 X_2^2)$

$+ s_{11} (m_0 (m_1 + m_2) X_1 X_2 + m_1 (m_2 + m_0) X_2 X_0$

$+ m_2 (m_0 + m_1) X_0 X_1) = 0$.

(Bastin, Mathesis, p.97)

Exercise.

(Neuberg, see Casey, no 80,81,82)

The barycenter of the triangle $\{Ste, BRa, Abr\}$ (see D16.5,14,16) is M . $BRa \times Abr = [m_1 m_2 (m_2 - m_0)(m_0 - m_1), m_2 m_0 (m_0 - m_1)(m_1 - m_2), m_0 m_1 (m_1 - m_2)(m_2 - m_0)]$.

Exercise.

Some points on the circumcircle.

Construct the points $\overline{Miqm_i}$ on θ and ac_i distinct from A_i and the points $Miq\overline{m_i}$ on θ and

on $\bar{a}c_i$ distinct from A_i .

Answer to

(partial).

$$\begin{aligned} \text{Miq}\bar{m}[0] &= (m_0(m_1 + m_2), m_1(m_1 - m_2), m_2(m_2 - m_1)), \\ \bar{\text{Miq}}m[0] &= (m_1 + m_2, m_2 - m_1, m_1 - m_2), \end{aligned}$$

Example.

$$\begin{aligned} p &= 29, A_i = (30, 1, 0), M = (60), \bar{M} = (215), \\ \text{Miq}\bar{m}_i &= (545, 512, 699), \bar{\text{Miq}}m_i = (115, 261, 855). \end{aligned}$$

Exercise.

The point of Miquel.

Given an arbitrary line which does not pass through the vertices and is neither the ideal or coideal line, $q = [q_0, q_1, q_2]$, Let $Q_i := q \times a_i$. Determine

$$\mu iq_i := \text{conic}(I', I'', A_i, Q_{i+1}, Q_{i-1}),$$

$$\bar{\mu} iq_i := \text{conic}(\bar{I}', \bar{I}'', A_i, Q_{i+1}, Q_{i-1}),$$

Construct the point Miq which is on μiq_i and θ ,

the point $\bar{\text{Miq}}$ which is on $\bar{\mu} iq_i$ and θ ,

the circle μq of Miquel which passes through the center of μiq_i

and the cocircle $\bar{\mu} q$ which passes through the center of $\bar{\mu} iq_i$.

The following special cases are of interest:

$q = \bar{m}$, in which case $\text{Miq} = \bar{\text{Miq}}$, which we denote $\text{Miq}\bar{i}$,

$q = e$, we then denote the point and copoint of Miquel by $\text{Miq}e$ and $\bar{\text{Miq}}e$,

$q = \bar{m}_i$, giving $\text{Miq}\bar{m}_i$ of Exercise $j \dots j$ above,

$q = m_i$, giving $\bar{\text{Miq}}m_i$ of Exercise $j \dots j$ above.

Answer to

(Partial)

$$\text{miq}_0 = (q_0 - q_1)(q_0 - q_2)(m_0(m_1 + m_2)X_1X_2 + \dots)$$

$$+ (X_0 + X_1 + X_2)(m_2(m_0 + m_1)q_1(q_0 - q_2)X_1 + m_1(m_2 + m_0)q_2(q_0 - q_1)) = 0.$$

$$\bar{\text{miq}}_0 = (m_0q_0 - m_1q_1)(m_0q_0 - m_2q_2)(m_0(m_1 + m_2)X_0X_2 + \dots) + (m_1m_2X_0 + m_2m_0X_1 + m_0m_1X_2)$$

$$((m_0 + m_1)q_1(m_0q_0 - m_2q_2)X_1 + (m_2 + m_0)q_1(m_0q_0 - m_1q_1)X_2) = 0.$$

$$\text{Miq} = (m_0(m_1 + m_2)q_1q_2(q_0 - q_2)(q_1 - q_0), m_1(m_2 + m_0)q_2q_0(q_1 - q_0)(q_2 - q_1), m_2(m_0 + m_1)q_0q_1(q_2 - q_1)(q_0 - q_2)),$$

$$\bar{\text{Miq}} = ((m_1 + m_2)q_1q_2(m_0q_0 - m_1q_1)(m_0q_0 - m_2q_2), (m_2 + m_0)q_2q_0(m_1q_1 - m_2q_2)(m_1q_1 - m_0q_0),$$

$$(m_0 + m_1)q_0q_1(m_2q_2 - m_0q_0)(m_2q_2 - m_1q_1)),$$

$$\text{Miq}\bar{i} = ((m_1 + m_2)(m_2 - m_0)(m_0 - m_1), (m_2 + m_0)(m_0 - m_1)(m_1 - m_2), (m_0 + m_1)(m_1 - m_2)(m_2 - m_0)),$$

$$\text{Miq}e = (m_0(m_1 + m_2)(m_2 - m_0)(m_0 - m_1)(m_0 - 2m_1 + m_2)(m_0 + m_1 - 2m_2), m_1(m_2 +$$

$$\begin{aligned}
& m_0)(m_0 - m_1)(m_1 - m_2)(m_1 - 0m_2 + m_0)(m_1 + m_2 - 0m_0), \\
& m_2(m_0 + m_1)(m_1 - m_2)(m_2 - m_0)(m_2 - 1m_0 + m_1)(m_2 + m_0 - 1m_1)), \\
\overline{Miqe} = & ((m_1 + m_2)(m_2 - m_0)(m_0 - m_1)(2m_2m_0 - m_1(m_2 + m_0))(2m_0m_1 - m_2(m_0 + m_1)), \\
& (m_2 + m_0)(m_0 - m_1)(m_1 - m_2)(2m_0m_1 - m_2(m_0 + m_1))(2m_1m_2 - m_0(m_1 + m_2)), \\
& (m_0 + m_1)(m_1 - m_2)(m_2 - m_0)(2m_1m_2 - m_0(m_1 + m_2))(2m_2m_0 - m_1(m_2 + m_0))).
\end{aligned}$$

Exercise.

(Sondat, See Mathesis, Ser. 2, Vol.6, pp. 81-83)

Let $B_0 \cdot \mu iq_0 = 0$, let

D.0. $b_1 := B_0 \times Q_1$, $b_2 := Q_2 \times B_0$,

D.1. $B_1 := muiq_1 \times b_2 - Q_2$, $B_2 := muiq_2 \times b_1 - Q_1$,

D.2. $b_0 := B_1 \times B_2$,

D.3. $ab_i := A_i \times B_i$,

D.4. $S := ab_1 \times ab_2$,

Let

$S_1 \cdot muiq_1 = 0$, $S_2 \cdot \mu iq_2 = 0$,

D.5. $sa_1 := S_1 \times A_1$, $sa_2 := S_2 \times A_2$,

D.6. $T := sa_1 \times sa_2$,

D.7. $sa_0 := T \times A_0$,

D.8. $S_0 := muiq_0 \times sa_0 - A_0$,

D.9. $\sigma := conic(S_i, S, T)$,

C.0. $Q[0] \cdot b_0 = 0$.

C.1. $S \cdot ab[0] = 0$.

C.2. $S \cdot \theta = 0$.

C.3. $\sigma isacircle$,

C.4. $T = \overline{M} == \dot{center}(\sigma) \cdot q = 0$.

$j \dots j$ double check the above.

Exercise.

Construct the point common to the circumcircle and the circle through A_i , $\overline{M}_i + 1$ and $\overline{M}_i - 1$.
(See also the transformation of Hamilton.)

Partial Answer to

a) The center is E_i ,

$x_i := E_i \times I\overline{mm}_i$,

$y_i := O \times Im_i$,

$Z_i := x_i \times y_i$,

$z_i := A_i \times Z_i$,

z_i corresponds to the perpendicular to $O \times E_i$, hence contains the desired intersection HH_i .

$x_0 = [m_1m_2(s_1 + m_0), -m_2(2m_0s_1 + m_1(m_1 + m_2)), -m_1(2m_0^2 + 3m_0m_1 + m_2s_1)]$,

$y_0 = [-(s_1 + m_0), m_1 + m_2, m_1 + m_2]$,

$Z_0 = ((m_1^2 - m_2^2)(m_0 + m_2), m_1(s_1 + m_0)(m_0 + 2m_2), -m_2(s_1 + m_0)s_1)$, $z_0 = [0, m_2s_1, m_1(m_0 + 2m_2)]$,

The rest of the construction is that of Pascal:

$$aa_i := A_{i+1} \times AA_{i-1},$$

$$ZZ_i := aa_i \times z_i,$$

$$zz_i := Im_{i+1} \times ZZ_{i-1},$$

$$Y_i := a_{i+1} \times zz_{i-1},$$

$$yy_i := Y_{i+1} \times AA_{i-1},$$

$$Miq\overline{m}_i := yy_{i+1} \times z_i.$$

Exercise.

0. Complete a section on the conic of Nagel, with
 $\nu := \text{conic}(JJ_0, JJ_1, JJ_2, Na_1, Na_2),$
 $\nu_i := \text{conic}(\dots),$
1. Give a construction for the other intersection of the conic with Ja_i and Na_i .
2. Give a construction for the center of the conic.
3. Are there some other points on this conic which have already been constructed or that you can construct?

Partial Answer to

$\mu = j_0j_1j_2(X_0^2 + X_1^2 + X_2^2) - j_0(j_1^2 + j_2^2)X_1X_2 - \dots = 0$, $j\dots j$ not checked
 other intersection with $Ja_0 = (p_2 + j_0^2), j_0j_1, j_2j_0$,
 other intersection with $Na_0 = (p_{22} + j_1^2j_2^2, j_0j_1j_2^2, j_0j_1^2j_2)$,
 center $(\dots ?)(j_0(j_1^4(j_2 - j_0) + j_2^4(j_1 - j_0) + j_1^2j_2^2(2j_0 + 3j_1 + 3j_2) + j_0^2j_1^2(j_1 + 3j_2) + j_2^2j_0^2(3j_1 + j_2)), \dots)$

Exercise.

The circles of Lemoine-Tucker.

$$D.0. X_i := K - xA_i, x \text{ is some integer},$$

$$D.1. x_i := X_{i+1} \times X_{i-1},$$

$$D.2. XX_i := x_{i+1} \times a_{i-1},$$

$$D.3. X\overline{X}_i := x_{i-1} \times a_{i+1},$$

$$D.4. \xi := \text{conic}(XX_0, XX_1, XX_2, X\overline{X}_1, X\overline{X}_2),$$

then

$$C.0. x_i \cdot Im_i = 0.$$

$$C.1. \xi \cdot X\overline{X}_0 = 0.$$

C.2. ξ is a circle.

D.0., can be replaced by a construction which start with a point X_0 on the symmedian at₀, the parallel through X_0 to the side a_2 or a_1 intersect the symmedians at₁ or at₂ at X_1 or X_2 .

Proof.

$$P.0. X_0 = (m_0(m_1 + m_2) + x, m_1(m_2 + m_0), m_2(m_0 + m_1)),$$

$$P.1. x_0 = [m_0(m_1 + m_2), m_0(m_1 + m_2), -s_{11} - m_0m_1 + x],$$

$$P.2. XX_0 = (s_{11} + m_2m_0 - x, m_1(m_2 + m_0), 0),$$

$$P.3. X\overline{X}_0 = (s_{11} + m_0m_1 - x, 0, m_2(m_0 + m_1)),$$

P.4. $(2s_{11} - x)^2\theta - (m) \times (u) = 0$, with
 $u_0 = m_1m_2(m_2 + m_0)(m_0 + m_1)(s_{11} + m_1m_2 - x), \dots$

Comment.

The following are special cases:

$x = 0$ gives the first circle of Lemoine λ_1 ,

$x = s_{11}$ gives the second circle of Lemoine λ_2 ,

$x = \dots$ gives the circle of Taylor,

$x = 2s_{11}$ gives the degenerate circle $(i) \times (i)$,

$x = \frac{1}{0}$ gives θ .

Exercise.

3.2.8 The harmonic polygons. [Casey]

Definition.

Given a conic θ and a point K not on the conic, an inscribed polygon A_i , $i = 0, \dots, n-1$ is a harmonic polygon if $(A_{i-1}, A_i, A_{i+1}, A'_i)$ is harmonic for all i , where

$ka_i := K \times A_i$,

$A'_i := \theta \times ka_i - A_i$,

$k := \text{polar}(K)$,

$B_i := \text{polar}(ka_i)$,

K is called the point of Lemoine of the polygon,

k is called the line of Lemoine.

Theorem.

If A_i , $i = 0$ to $n-1$ is a harmonic polygon then A'_i , $i = 0$ to $n-1$ is a harmonic polygon.

Construction.

Given K , A_0 , A_1 ,

construct k , ka_0 , B_0 , ka_1 , B_1 ,

for $i = 1$ to $n-1$

begin

$ka_i := \text{polar } A_i, \quad B_i := ka_i \times k, \quad c_i := A_{i-1} \times B_i, \quad A_{i+1} :=$
 $\theta \times c_i - A_{i-1}, \text{ end}$

Construction.

Details.

H.0. $x(A_1 - B_1) = y(A_0 - B_0) + B_0A_1 - A_0B_1$

H.1. $x^2 + y^2 = 1$,

then

C.0. $y^2((A_0 - B_0)^2 + (A_1 - B_1)^2) + 2y(A_0 - B_0)(B_0A_1 - A_0B_1) + (B_0A_1 - A_0B_1)^2 - (A_1 - B_1)^2 = 0$,

C.1. $y = -2(A_0B_0)(B_0A_1 - A_0B_1)/((A_0 - B_0)^2 + (A_1 - B_1)^2) - A_1$.
 CHECK THE ABOVE $j \dots j$

Example.

For $p = 31$,
 let $K = (0, -8, 1)$, $A_0 = (1, 0, 1)$, $A_1 = ()$, then $A_i = (1, 0, 1)$,

Exercise.

Complete a section on polars of the vertices with respect to the conic of Brianchon-Poncelet.

0. Give an explicit construction for the tangents to gamma at the mid-points and at the feet.
1. Give an explicit construction for the polar pp_i of A_i with respect to γ .
2. Verify that the intersections $PP_i := pp_i \times A_i$ are collinear on pp .

This result can be used as the starting point for special results in the geometry of the tetrahedron. (An other approach is suggested by the theorem $j \dots j$). The lines a_i and pp correspond to the ideal lines in the four faces of a tetrahedron whose opposite vertices are perpendicular. The tetrahedron so obtained have the additional properties that $A_i \times M_i$ are concurrent as well as $A_i \times \overline{M}_i$.

Comment.

An other model of projective geometry within projective geometry is suggested by the following.

Associate to the point (X_0, X_1, X_2) , the point (X_1X_2, X_2X_0, X_0X_1) ,
 associate to the line $[a_0, a_1, a_2]$, the conic

$$a_0X_1X_2 + a_1X_2X_0 + a_2X_0X_1 = 0.$$

The ideal is the conic

$$X_1X_2 + X_2X_0 + X_0X_1 = 0,$$

and the coideal is

$$m_0X_1X_2 + m_1X_2X_0 + m_2X_0X_1 = 0.$$

Some care has to be exercised because if, for instance, two of the coordinates X_0, X_1, X_2 are 0, the image is not defined.

In the following definition “Point” and “Line” is used for the new objects which have the properties of “point” and “line” defined above.

Definition.

Given a triangle $(A_0, A_1, A_2), (a_0, a_1, a_2)$,
 the Points are

- the points not on the sides of the triangle,

- the line through the vertices, (including a_0, a_1, a_2),

the Lines are

- the conics through A_0, A_1 and A_2 , including the degenerate conics which consist of one side and a line through the opposite vertex.

A Point is on a Line if

- ...

If two of the points are the isotropic points, the lines become the circles passing through a given point. A large number of properties of circles as well as properties of projective geometry can be obtained by pursuing this approach. In particular a study of the quartics which are associated to the circles is of interest.

An early reference on circular triangles is by Miquel, J. de Liouville, Vol. 9, 1844, p. 24.

Special cases. 2 Special cases are of interest.

Notation.

$P := p_1 \times p_2$ does not denote an actual construction, but a construction in which p_1 or p_2 are assumed to be known.

"==" was suggested by the mode of drawing using dashed lines rather than continuous ones. In the example below, D is not known, hence we can not construct $A \times D$.

The following problem is of interest.

Exercise.

Given 2 conics with 3 points in common, determine by a linear construction the fourth point on both conics.

One solution is the following.

Let A, B, C be the known points and D be the unknown point. Let E and F be on the first conic γ , U and V on the second conic γ' . Determine first by the Pascal's construction point $\text{Pascal}(U, V, C, B, A, E; E')$, and point $\text{Pascal}(A, B, C, U, V, E; E')$, E' on γ' and $A \times E$, F' on γ' and $B \times F$,

let $K := (D \times A) \times (C \times B)$, $L := (A \times E) \times (B \times F)$, $M := (E \times C) \times (F \times D)$, $M' := (E' \times C) \times (F' \times D)$,

then $\text{Pascal}(D, A, E, C, B, F; K, L, M)$, and $\text{Pascal}(D, A, E', C, B, F'; K, L, M')$. This implies $\text{incidence}(L, M, M')$.

Using Desargues⁻¹($\langle L, M', M \rangle, \{C, E, E'\}, \{D, F, F'\}; G$), it follows that D is incident to $c \times G$, with

$G := (E \times F) \times (E' \times F')$,

the triangles $\{C, E, E'\}$ and $\{D, F, F'\}$ being perspective.

D follows from point $\text{Pascal}(B, A, E, F, C, G; D)$.

Construction.

The complete construction is the following:

$$\begin{aligned} P_0 &:= (U \times V) \times (B \times A), P_1 := (V \times C) \times (A \times E), P_2 := (C \times B) \times (P_0 \times P_1), E' := \\ & (A \times E) \times (P_2 \times U), \\ P'_1 &:= (V \times C) \times (B \times F), P'_2 := (C \times A) \times (P_0 \times P'_1), F' := (C \times A') \times (P'_2 \times U), \\ G &:= (E \times F) \times (E' \times F'), \\ Q_0 &:= (B \times A) \times (F \times C), Q_1 := (A \times E) \times (C \times G), Q_2 := (E \times F) \times (Q_0 \times Q_1), \\ D &:= (C \times G) \times (Q_2 \times B). \end{aligned}$$

An other solution is the following

Theorem.

Let t_A and t_B be the tangents to the first conic at A and at B ,

let t'_A and t'_B the tangents to the second conic at A and B ,

$$\begin{aligned} O_1 &:= t_A \times t_B, O'_1 := t'_A \times t'_B, oo' := O_1 \times O'_1, ab := A \times B, BA' := t_B \times t'_A, AB' := t_A \times t'_B, \\ ab' &:= BA' \times AB', E := ab \times ab', cd := C \times E, bc := B \times C, F := bc \times oo', ad := A \times F, \\ D &:= ad \times cd, \end{aligned}$$

then

D is on conic(A, t_A, B, t_B, C) and conic(A, t'_A, B, t'_B, C).

Proof: Assume that A and B are the isotropic points then the 2 conics are circles. O and O' are their centers. $cd \perp oo'$. Therefore $(A, B, D, ab \times oo')$ is a harmonic quatern. bc and ad meet on oo' . This can be checked using $A = (1, i, 0)$, $B = (1, -i, 0)$, $C = (0, 1, 1)$, $D = (0, -1, 1)$, $oo' = [1, 0, 0]$, $bc = [-i, -1, 1]$, $ad = [i, -1, -1]$, $F = (0, 1, 1)$.

3.2.9 Cubics.**Introduction.**

Cubics have extensively studied by Newton, MacLaurin, Gergonne, Plucker, Salmon,

I will give here a few properties, many of which generalize to higher degree curves, most of them taken from Salmon, 1979, sections 29 to 31 and 148 to 159?:

Theorem.

All cubics which pass through 8 fixed points pass also through a ninth.

Definition.

If 9 points are on a one parameter family of non degenerate cubics, we say that they form a cubic configuration. This configuration is not confined.

Theorem. [MacLaurin]

Let A_0 , to A_7 be 8 points of a cubic, such that $A_0, A_1, A_2, A_3, A_4, A_5$, are on a conic α and $A_0, A_1, A_2, A_3, A_6, A_7$, are on a conic β then $(A_4 \times A_5) \times (A_6 \times A_7)$ is on the cubic and the 9 points form a cubic configuration.

Proof: This follows when the preceding Theorem is applied to the degenerate cubics consisting of the conic α and the line $A_6 \times A_7$ and the conic β and the line $A_4 \times A_5$.

Corollary.

If 2 lines meet a cubic at points $B_{0,i}$ and $B_{1,i}$ then the 3 points $B_{2,i}$ on the cubic and on $B_{0,i} \times B_{1,i}$ are collinear,

or equivalently

If 6 points B_j , $j = 0$ to 5 , are on a cubic and 2 of the points $C_i := (B_i \times B_{i+1}) \times (B_{i+3} \times B_{i+4})$ are on the cubic then the third point is on the cubic and the 9 points form a cubic configuration.

Proof: This follows when the preceding Theorem is applied to the degenerate conics α through $B_{0,i}$ and $B_{1,i}$ and β through $B_{i,0}$ and $B_{i,1}$.

The alternate form corollary gives Pappus' Theorem when the cubic degenerates into 3 lines.

Notation.

I will write $C9(B_0, B_1, B_2, B_3, B_4, B_5; C_0, C_1, C_2)$.

Theorem. [Salmon]

The 3 parameter family of cubics through the 6 points A_i and B_i , which are not on a conic is

$$\Sigma_{i=0,1,2} s_i (A_i \times B_i) \times (A_{i+1} \times A_{i-1}) \times (B_{i+1} \times B_{i-1}) \\ = (A_{i+1} \times B_{i-1}) \times (A_{i-1} \times B_i) \times (A_i \times A_{i+1}).$$

Proof: It is easy to verify that each of the points is on each of the 4 degenerate cubics and that these are independent.

There are many alternate forms possible, I have chosen the above one which displays a useful symmetry property.

Definition.

The tangential point of a point C on a cubic is the third intersection of the tangent at C with the cubic.

Corollary.

If 3 points of a cubic are on a line a , their tangential points are on a line s .

This follows from the degenerate case $B_{0,i} = B_{1,i}$.

Definition.

The line s is called the satellite of the line a .

Notation.

Given 2 points A and B on a cubic, the third point on the cubic and the line $A \times B$ is denoted $A \star B$.

Theorem.

Given 6 lines a_i and b_i and their 9 intersections

$$i j := a_i \times b_j,$$

0. These 9 points form a cubic configuration.

1. If C_0 is a point on 11×22 , the cubic of the family through the points $i j$ and C_0 are such that if we define the following points,

$$C_i := i + 1, i + 1 \star i - 1, i - 1, D_i := i + 1, i - 1 \star i - 1, i + 1,$$

$$E_i := i, i + 1 \star i - 1, i, \bar{E}_i := i + 1, i \star i, i - 1,$$

$$F_i := i, i \star i + 1, i - 1, \bar{F}_i := i, i \star i - 1, i + 1,$$

$$Cc_i := C_{i+1} \star C_{i-1}, Cd_i := C_{i+1} \star D_{i-1}, Dc_i := D_{i+1} \star C_{i-1},$$

$$CF_i := C_i \star F_i, Cf_i := C_{i+1} \star F_{i-1}, Fc_i := F_{i+1} \star C_{i-1},$$

$$CF_i := C_i \star F_i, Cf_i := C_{i+1} \star F_{i-1}, Fc_i := F_{i+1} \star C_{i-1},$$

$$C\bar{F}_i := C_i \star \bar{F}_i, C\bar{f}_i := C_{i+1} \star \bar{F}_{i-1}, \bar{F}c_i := \bar{F}_{i+1} \star C_{i-1},$$

$$DE_i := D_i \star E_i, De_i := D_{i+1} \star E_{i-1}, Ed_i := E_{i+1} \star D_{i-1},$$

$$D\bar{E}_i := D_i \star \bar{E}_i, D\bar{e}_i := D_{i+1} \star \bar{E}_{i-1}, \bar{E}d_i := \bar{E}_{i+1} \star D_{i-1},$$

$$DF_i := D_i \star F_i, D\bar{F}_i := D_i \star \bar{F}_i,$$

$$Ee_i := E_{i+1} \star E_{i-1}, EF_i := E_i \star F_i, Ef_i := E_{i+1} \star F_{i-1},$$

$$Fe_i := F_{i+1} \star E_{i-1}, \bar{E}\bar{f}_i := E_{i+1} \star \bar{F}_{i-1}, \bar{F}e_i := \bar{F}_{i+1} \star E_{i-1},$$

$$\bar{E}e_i := \bar{E}_{i+1} \star \bar{E}_{i-1}, \bar{E}\bar{F}_i := \bar{E}_i \star \bar{F}_i, \bar{E}\bar{f}_i := \bar{E}_{i+1} \star F_{i-1},$$

$$F\bar{e}_i := F_{i+1} \star \bar{E}_{i-1}, \bar{E}\bar{f}_i := \bar{E}_{i+1} \star \bar{F}_{i-1}, \bar{F}e_i := \bar{F}_{i+1} \star \bar{E}_{i-1},$$

$$F\bar{F}_i := F_i \star \bar{F}_i,$$

$$C'_i := C_i \star C_i, D'_i := D_i \star D_i,$$

$$E'_i := E_i \star E_i, \bar{E}'_i := \bar{E}_i \star \bar{E}_i, F'_i := F_i \star F_i, \bar{F}'_i := \bar{F}_i \star \bar{F}_i,$$

$$K_i := C_i \star i + 1, i - 1, \bar{K}_i := C_i \star i - 1, i + 1,$$

$$L_i := D_{i+1} \star i - 1, i - 1, \bar{L}_i := D_{i-1} \star i + 1, i + 1,$$

$$M_i := E_i \star i, i, \bar{M}_i := \bar{E}_i \star i, i, N_i := E_i \star i - 1, i + 1, \bar{N}_i := \bar{E}_i \star i + 1, i - 1,$$

$$P_i := F_{i+1} \star i + 1, i, \bar{P}_i := \bar{F}_{i+1} \star i, i + 1,$$

$$Q_i := F_{i-1} \star i, i - 1, \bar{Q}_i := \bar{F}_{i-1} \star i - 1, i,$$

We have the following table for the operation \star between points on the cubic:

\star	00	11	22	12	20	01	21	02	10	C_0	C_1	C_2	D_0	D_1	D_2
C_0	D_0	22	11	K_0	\overline{CF}_2	\overline{CF}_1	\overline{K}_0	\overline{CF}_2	\overline{CF}_1	C'_0	Cc_2	Cc_1	00	Cd_2	Dc_1
C_1	22	D_1	00	\overline{CF}_2	K_1	\overline{CF}_0	\overline{CF}_2	\overline{K}_1	\overline{CF}_0	Cc_2	C'_1	Cc_0	Dc_2	11	Cd_0
C_2	11	00	D_2	\overline{CF}_1	\overline{CF}_0	K_2	\overline{CF}_1	\overline{CF}_0	\overline{K}_2	Cc_1	Cc_0	C'_2	Cd_1	Dc_0	22
D_0	C_0	L_2	\overline{L}_1	21	$F\overline{e}_2$	$\overline{E}f_1$	12	$\overline{F}e_2$	$\overline{E}f_1$	00	Dc_2	Cd_1	D'_0	$22'$	$11'$
D_1	\overline{L}_2	C_1	L_0	$\overline{E}f_2$	02	$F\overline{e}_0$	$\overline{E}f_2$	20	$\overline{F}e_0$	Cd_2	11	Dc_1	$22'$	D'_1	$00'$
D_2	L_1	\overline{L}_0	C_2	$F\overline{e}_1$	$\overline{E}f_0$	10	$\overline{F}e_1$	$\overline{E}f_0$	01	Dc_1	Cd_0	22	$11'$	$00'$	D'_2
E_0	M_0	DE_2	DE_1	\overline{F}_0	01	20	N_0	EF_2	EF_1	$21'$	\overline{E}_2	\overline{E}_1	DE_0	Ed_2	De_1
E_1	DE_2	M_1	DE_0	01	\overline{F}_1	12	EF_2	N_1	EF_0	\overline{E}_2	$02'$	\overline{E}_0	De_2	DE_1	Ed_0
E_2	DE_1	DE_0	M_2	20	12	\overline{F}_2	EF_1	EF_0	N_2	\overline{E}_1	\overline{E}_0	$10'$	Ed_1	De_0	DE_2
\overline{E}_0	\overline{M}_0	\overline{DE}_2	\overline{DE}_1	\overline{N}_0	\overline{EF}_2	\overline{EF}_1	F_0	10	02	$12'$	E_2	E_1	\overline{DE}_0	\overline{Ed}_2	\overline{De}_1
\overline{E}_1	\overline{DE}_2	\overline{M}_1	\overline{DE}_0	\overline{EF}_2	\overline{N}_1	\overline{EF}_0	10	F_1	21	E_2	$20'$	E_0	$\overline{D\overline{e}}_2$	$\overline{D\overline{E}}_1$	\overline{Ed}_0
\overline{E}_2	\overline{DE}_1	\overline{DE}_0	\overline{M}_2	\overline{EF}_1	\overline{EF}_0	\overline{N}_2	02	21	F_2	E_1	E_0	$01'$	\overline{Ed}_1	$\overline{D\overline{e}}_0$	\overline{DE}_2
F_0	12	$\overline{F}e_2$	$\overline{E}f_1$	00	Dc_2	Cd_1	\overline{E}_0	P_2	Q_1	\overline{CF}_0	$\overline{F}c_2$	$\overline{C}f_1$	\overline{DF}_0	\overline{F}_2	\overline{F}_1
F_1	$\overline{E}f_2$	20	$\overline{F}e_0$	Cd_2	11	Dc_0	Q_2	\overline{E}_1	P_0	$\overline{C}f_2$	\overline{CF}_1	$\overline{F}c_0$	\overline{F}_2	\overline{DF}_1	\overline{F}_0
F_2	$\overline{F}e_1$	$\overline{E}f_0$	01	Dc_1	Cd_0	22	P_1	Q_0	\overline{E}_2	$\overline{F}c_1$	$\overline{C}f_0$	\overline{CF}_2	\overline{F}_1	\overline{F}_0	\overline{DF}_2
\overline{F}_0	21	$F\overline{e}_2$	$\overline{E}f_1$	E_0	\overline{P}_2	\overline{Q}_1	00	Dc_2	Cd_1	\overline{CF}_0	$\overline{F}c_2$	$\overline{C}f_1$	\overline{DF}_0	F_2	F_1
\overline{F}_1	$\overline{E}f_2$	02	$F\overline{e}_0$	\overline{Q}_2	E_1	\overline{P}_0	Cd_2	11	Dc_0	$\overline{C}f_2$	\overline{CF}_1	$\overline{F}c_0$	F_2	$\overline{D\overline{F}}_1$	F_0
\overline{F}_2	$F\overline{e}_1$	$\overline{E}f_0$	10	\overline{P}_1	\overline{Q}_0	E_2	Dc_1	Cd_0	22	$\overline{F}c_1$	$\overline{C}f_0$	\overline{CF}_2	F_1	F_0	$\overline{D\overline{F}}_2$
\star	E_0	E_1	E_2	\overline{E}_0	\overline{E}_1	\overline{E}_2	F_0	F_1	F_2	\overline{F}_0	\overline{F}_1	\overline{F}_2			
E_0	E'_0	Ee_2	Ee_1	00'	C_2	C_1	EF_0	EF_2	Fe_1	12	$\overline{E}f_2$	$\overline{F}e_1$			
E_1	Ee_2	E'_1	Ee_0	C_2	11'	C_0	Fe_2	EF_1	Ef_0	$\overline{F}e_2$	20	$\overline{E}f_0$			
E_2	Ee_1	Ee_0	E'_2	C_1	C_0	22'	Ef_1	Fe_0	\overline{EF}_2	$\overline{E}f_1$	$\overline{F}e_0$	01			
\overline{E}_0	00'	C_2	C_1	\overline{E}'_0	\overline{Ee}_2	\overline{Ee}_1	21	$\overline{E}f_2$	$F\overline{e}_1$	\overline{EF}_0	$\overline{E}f_2$	$\overline{F}e_1$			
\overline{E}_1	C_2	11'	C_0	\overline{Ee}_2	\overline{E}'_1	\overline{Ee}_0	$F\overline{e}_2$	02	$\overline{E}f_0$	$\overline{F}e_2$	\overline{EF}_1	$\overline{E}f_0$			
\overline{E}_2	C_1	C_0	22'	\overline{Ee}_1	\overline{Ee}_0	\overline{E}'_2	$\overline{E}f_1$	$F\overline{e}_0$	10	$\overline{E}f_1$	$\overline{F}e_0$	\overline{EF}_2			
F_0	EF_0	Fe_2	EF_1	21	$F\overline{e}_2$	$\overline{E}f_1$	F'_0	10'	02'	FF_0	D_2	D_1			
F_1	Fe_2	EF_1	EF_0	$\overline{E}f_2$	02	$F\overline{e}_0$	10'	F'_1	21'	D_2	FF_1	D_0			
F_2	Fe_1	EF_0	\overline{EF}_2	$\overline{F}e_1$	$\overline{E}f_0$	10	02'	21'	F'_2	D_1	D_0	FF_2			
\overline{F}_0	12	$\overline{F}e_2$	$\overline{E}f_1$	\overline{EF}_0	$\overline{F}e_2$	$\overline{E}f_1$	FF_0	D_2	D_1						
ovF'_0	01'	20'													
\overline{F}_1	$\overline{E}f_2$	20	$\overline{F}e_0$	$\overline{E}f_2$	\overline{EF}_1	$\overline{F}e_0$	D_2	FF_1	D_0	01'	\overline{F}'_1	12'			
\overline{F}_2	$\overline{F}e_1$	$\overline{E}f_0$	01	$\overline{F}e_1$	$\overline{E}f_0$	\overline{EF}_2	D_1	D_0	FF_2	20'	12'	\overline{F}'_2			

Proof:

α_0	$D9(C_0$	D_0	21	20	10	11	;	00	12	22)
$\rho\alpha_0$	$D9(\overline{E}_2$	F_2	01	00	20	21	;	10	22	02)
$\rho^2\alpha_0$	$C9(E_1$	\overline{F}_1	11	10	00	01	;	20	02	12)
α_1	$C9(E_1$	\overline{E}_2	21	11	22	12	;	C_0	02	01)
$\sigma\alpha_1$	$C9(\overline{E}_1$	E_2	12	11	22	21	;	C_0	20	10)
$\beta\alpha_1$	$C9(F_2$	\overline{F}_1	11	21	12	22	;	D_0	02	01)
$\sigma\beta\alpha_1$	$C9(\overline{F}_2$	F_1	11	12	21	22	;	D_0	20	10)
α_2	$C9(C_1$	D_2	01	F_2	20	00	;	Cd_0	10	22)
$\sigma\alpha_2$	$C9(C_1$	D_2	10	\overline{F}_2	02	00	;	Cd_0	01	22)
$021021\alpha_2$	$C9(C_2$	D_1	02	\overline{F}_1	10	00	;	Dc_0	20	11)
$\sigma 021021\alpha_2$	$C9(C_2$	D_1	20	F_1	01	00	;	Dc_0	02	11)
α_3	$C9(C_0$	F_0	00	C_1	10	11	;	CF_0	12	22)
$\sigma\alpha_3$	$C9(C_0$	\overline{F}_0	00	C_1	01	11	;	$C\overline{F}_0$	21	22)
$021021\alpha_3$	$C9(C_0$	\overline{F}_0	00	C_2	20	22	;	$C\overline{F}_0$	21	11)
$\sigma 021021\alpha_3$	$C9(C_0$	F_0	00	C_2	02	22	;	CF_0	12	11)
α_4	$C9(D_0$	E_0	20	E_2	11	21	;	DE_0	01	12)
$\sigma\alpha_4$	$C9(D_0$	\overline{E}_0	02	\overline{E}_2	11	12	;	$D\overline{E}_0$	10	21)
$021021\alpha_4$	$C9(D_0$	\overline{E}_0	10	\overline{E}_1	22	12	;	$D\overline{E}_0$	02	21)
$\sigma 021021\alpha_4$	$C9(D_0$	E_0	01	E_1	22	21	;	DE_0	20	12)
α_5	$C9(E_0$	F_0	12	E_2	02	01	;	EF_0	00	20)
$\sigma\alpha_5$	$C9(\overline{E}_0$	\overline{F}_0	21	\overline{E}_2	20	10	;	$\overline{E}\overline{F}_0$	00	02)
$021021\alpha_5$	$C9(\overline{E}_0$	\overline{F}_0	21	\overline{E}_1	01	02	;	$\overline{E}\overline{F}_0$	00	10)
$\sigma 021021\alpha_5$	$C9(E_0$	F_0	12	E_1	10	20	;	EF_0	00	01)
α_6	$C9(E_1$	\overline{F}_2	22	F_2	11	12	;	$E\overline{f}_0$	10	01)
$\sigma\alpha_6$	$C9(E_1$	F_2	22	\overline{F}_2	11	21	;	$\overline{E}f_0$	01	10)
α_7	$C9(F_1$	\overline{E}_2	02	\overline{F}_1	22	20	;	$F\overline{e}_0$	21	11)
$\sigma\alpha_7$	$C9(\overline{F}_1$	E_2	20	F_1	22	02	;	$\overline{F}e_0$	12	11)
α_8	$C9(C_0$	E_0	20	21	21	11	;	$21'$	01	22)
$\sigma\alpha_8$	$C9(C_0$	\overline{E}_0	02	12	12	11	;	$12'$	10	22)
$012210\alpha_8$	$C9(F_1$	F_2	22	21	21	11	;	$21'$	01	20)
$\sigma\alpha_8$	$C9(\overline{F}_1$	\overline{F}_2	22	12	12	11	;	$12'$	10	02)
$210102\alpha_8$	$C9(\overline{E}_0$	E_0	01	00	00	10	;	$00'$	20	02)
$120102\alpha_8$	$C9(D_2$	D_1	01	00	00	20	;	$00'$	10	02)
α_9	$C9(C_1$	10	11	C_2	02	22	;	CF_0	12	00)
$\sigma\alpha_9$	$C9(C_1$	01	11	C_2	20	22	;	$C\overline{F}_0$	21	00)
$210012\alpha_9$	$C9(D_1$	10	11	F_1	22	02	;	$\overline{F}e_0$	12	20)
$\sigma 210012\alpha_9$	$C9(D_1$	01	11	\overline{F}_1	22	20	;	$F\overline{e}_0$	21	02)
$012102\alpha_9$	$C9(F_2$	11	10	D_2	02	22	;	$E\overline{f}_0$	12	01)
$\sigma 012102\alpha_9$	$C9(\overline{F}_2$	11	01	D_2	20	22	;	$\overline{E}f_0$	21	10)
$102210\alpha_9$	$C9(E_2$	02	01	E_1	10	20	;	EF_0	00	12)
$\sigma 102210\alpha_9$	$C9(\overline{E}_2$	20	10	\overline{E}_1	01	02	;	$\overline{E}\overline{F}_0$	00	21)
$120201\alpha_9$	$C9(E_1$	22	20	E_2	11	01	;	DE_0	21	12)
$\sigma 120201\alpha_9$	$C9(\overline{E}_1$	22	02	\overline{E}_2	11	10	;	$D\overline{E}_0$	12	21)
$102120\alpha_9$	$C9(F_1$	01	02	\overline{F}_1	10	20	;	Dc_0	00	11)
$201210\alpha_9$	$C9(\overline{F}_2$	02	01	F_2	20	10	;	Cd_0	00	22)

3.2.10 The cubics of Grassmann.

Definition.

Given 6 lines a_i and b_i , among the 15 intersections we choose the following 9,

$$D1.0. A_i := a_{i+1} \times a_{i-1},$$

$$D1.1. B_i := b_{i+1} \times b_{i-1},$$

$$D1.2. E_i := a_i \times b_i,$$

the non confined configuration consisting of these 9 points and 6 lines each containing 3 of the points is called a Grassmann configuration. It is noted $(\{A_i\}, \{B_i\}, \{E_i\})$.

Theorem. [Grassmann]

Given 2 triangles $\{A_i, a_i\}$ and $\{B_i, b_i\}$, the locus of the points X is a cubic, if X is such that the points obtained by finding the intersections of the lines joining X to the vertices of one of the triangles and the corresponding sides of the second triangle, namely $(X \times A_i) \times b_i$, are collinear.

Theorem.

Let

$$D2.0. aB_i := A_{i+1} \times B_{i-1}, a\overline{B}_i := A_{i-1} \times B_{i+1},$$

$$D2.1. AB_i := aB_i \times a\overline{B}_i,$$

$$D2.2. abE_i := AB_{i+1} \times E_{i-1}, ab\overline{E}_i := AB_{i-1} \times E_{i+1},$$

$$D2.3. DE_i := abE_i \times ab\overline{E}_i,$$

$$D2.4. de_i := DE_i \times E_i,$$

$$D2.5. ab_i := A_i \times B_i,$$

$$D2.6. D_i := de_i \times ab_i,$$

$$D2.6. ba_i := AB_{i+1} \times AB_{i-1},$$

$$D2.8. abd_i := D_i \times AB_i,$$

$$D2.9. C_i := ba_i \times abd_i,$$

$$D4.0. ae_i := A_i \times E_i, be_i := B_i \times E_i,$$

$$D4.1. ce_i := C_i \times E_i,$$

$$D4.2. aab_i := A_i \times AB_i, bab_i := B_i \times AB_i,$$

$$D4.3. F_i := be_i \times aab_i, \overline{F}_i := ae_i \times bab_i,$$

$$D4.4. f_i := F_{i+1} \times F_{i-1}, \overline{f}_i := \overline{F}_{i+1} \times \overline{F}_{i-1},$$

$$D4.5. A'_i := ce_i \times \overline{f}_i, B'_i := ce_i \times f_i,$$

$$D4.6. aC_i := A_{i+1} \times C_{i-1}, a\overline{C}_i := A_{i-1} \times C_{i+1},$$

$$D4.6. bC_i := B_{i+1} \times C_{i-1}, b\overline{C}_i := B_{i-1} \times C_{i+1},$$

$$D4.7. CF_i := bC_i \times b\overline{C}_i, C\overline{F}_i := aC_i \times a\overline{C}_i,$$

$$D4.8. cD_i := C_{i+1} \times D_{i-1}, c\overline{D}_i := C_{i-1} \times D_{i+1},$$

$$D4.9. aF_i := A_{i+1} \times F_{i-1}, a\overline{F}_i := A_{i-1} \times F_{i+1},$$

$$D4.10. Cd_i := cD_i \times aF_i, Dc_i := c\overline{D}_i \times a\overline{F}_i,$$

$$D4.11. aD_i := A_{i+1} \times D_{i-1}, a\overline{D}_i := A_{i-1} \times D_{i+1},$$

$$D4.12. eF_i := E_{i+1} \times F_{i-1}, e\overline{F}_i := E_{i-1} \times F_{i+1},$$

$$D4.13. Ef_i := aD_i \times eF_i, Fe_i := a\overline{D}_i \times e\overline{F}_i,$$

- $D4.14. bD_i := B_{i+1} \times D_{i-1}, \overline{bD}_i := B_{i-1} \times D_{i+1},$
 $D4.15. \overline{fE}_i := E_{i+1} \times \overline{F}_{i-1}, \overline{fE}_i := E_{i-1} \times \overline{F}_{i+1},$
 $D4.16. E\overline{f}_i := bD_i \times \overline{fE}_i, \overline{F}e_i := b\overline{D}_i \times \overline{fE}_i,$
 $D4.17. ef_i := E_i \times F_i, e\overline{f}_i := E_i \times \overline{F}_i,$
 $D5.0. a'D_i := A'_{i+1} \times D_{i-1}, a'\overline{D}_i := A'_{i-1} \times D_{i+1},$
 $D5.1. abe_i := AB_i \times E_i,$
 $D5.2. M_i := a'D_i \times abe_i,$
 $D5.3. dAB_i := D_{i+1} \times AB_{i-1}, d\overline{AB}_i := D_{i-1} \times AB_{i+1},$
 $D5.4. a'E_i := A'_{i+1} \times E_{i-1}, a'\overline{E}_i := A'_{i-1} \times E_{i+1},$
 $D5.5. L_i := dAB_i \times a'E_i, \overline{L}_i := d\overline{AB}_i \times a'\overline{E}_i,$
 $D5.6. fB_i := F_{i+1} \times B_{i-1}, \overline{fB}_i := F_{i-1} \times B_{i+1},$
 $D5.7. \overline{fA}_i := \overline{F}_{i+1} \times A_{i-1}, \overline{fA}_i := \overline{F}_{i-1} \times A_{i+1},$
 $D5.8. P_i := fB_i \times \overline{fA}_i, Q_i := \overline{fB}_i \times \overline{fA}_i,$
 $D5.9. ac_i := A_i \times C_i, bc_i := B_i \times C_i,$
 $D5.10. bde_i := B_i \times DE_i, ade_i := A_i \times DE_i,$
 $D5.11. K_i := ac_i \times bde_i, \overline{K}_i := bc_i \times ade_i,$
 $D5.12. dE_i := D_{i+1} \times E_{i-1}, eD_i := E_{i+1} \times D_{i-1},$
 $D5.13. bK_i := B_{i+1} \times K_{i-1}, kB_i := B_{i-1} \times K_{i+1},$
 $D5.14. Ed_i := eD_i \times bK_i, De_i := dE_i \times kB_i,$
 $D6.0. cL_i := C_{i+1} \times L_{i-1}, c\overline{L}_i := C_{i-1} \times \overline{L}_{i+1},$
 $D6.1. C'_i := cL_i \times c\overline{L}_i,$
 $D6.2. k\overline{f}_i := K_i \times \overline{F}_i, \overline{kf}_i := \overline{K}_i \times F_i,$
 $D6.3. D'_i := k\overline{f}_i \times \overline{kf}_i,$
 $D6.4. a'f_i := A'_i \times F_i, a'\overline{f}_i := A'_i \times \overline{F}_i,$
 $D6.5. df_i := D_i \times F_i, d\overline{f}_i := D_i \times \overline{F}_i,$
 $D6.6. DF_i := a'\overline{f}_i \times df_i, D\overline{F}_i := a'f_i \times d\overline{f}_i,$
 $D6.7. fC_i := F_{i+1} \times C_{i-1}, \overline{fC}_i := F_{i-1} \times C_{i+1},$
 $D6.8. \overline{fC}_i := \overline{F}_{i+1} \times C_{i-1}, \overline{fC}_i := \overline{F}_{i-1} \times C_{i+1},$
 $D6.9. fDE_i := F_{i+1} \times DE_{i-1}, fD\overline{E}_i := \overline{F}_{i+1} \times DE_{i-1},$
 $D6.10. aM_i := A_{i+1} \times M_{i-1}, bM_i := B_{i+1} \times M_{i-1},$
 $D6.11. Fc_i := fC_i \times fD\overline{E}_i, \overline{Fc}_i := \overline{fC}_i \times fDE_i,$
 $D6.12. C\overline{f}_i := \overline{fC}_i \times aM_i, C\overline{f}_i := \overline{fC}_i \times bM_i,$
 $D6.13. c_i := C_{i+1} \times C_{i-1}, ll_i := L_i \times \overline{L}_i,$
 $D6.14. Cc_i := c_i \times ll_i,$
 $D6.15. ccL_i := Cc_{i+1} \times L_{i-1}, cc\overline{L}_i := Cc_{i-1} \times \overline{L}_{i+1},$
 $D6.16. AB'_i := ccL_i \times cc\overline{L}_i,$
 $D6.17. lQ_i := L_{i+1} \times Q_{i-1}, p\overline{L}_i := P_{i+1} \times \overline{L}_{i-1},$
 $D6.18. F'_i := lQ_i \times p\overline{L}_i,$
 $D6.19. f\overline{f}_i := F_i \times \overline{F}_i, dab'_i := D_i \times AB'_i,$
 $D6.20. FF_i := f\overline{f}_i \times dab'_i,$
 $D7.0. a'_i := A_i \times A'_i,$
 $D7.1. b'_i := B_i \times A'_i,$
 $D7.2. c'_i := C_i \times C'_i,$
 $D7.3. d'_i := D_i \times D'_i,$
 $D7.4. ab'_i := AB_i \times AB'_i,$

$$D7.5. e'_i := E_i \times AB'_i,$$

$$D7.6. f'_i := F_i \times F'_i,$$

$$D7.7. \overline{f}'_i := \overline{F}_i \times F'_i,$$

then

$$C2.0. C_i \iota e_i,$$

$$C2.1. X_i = Y_i,$$

$$C2.2. A'_i = B'_i,$$

$$C2.3. A_i \iota e \overline{f}_i, B_i \iota e f_i,$$

$$C2.4. A'_{i+1} \times D_{i-1} = M_i,$$

$$C2.5. A'_{i+1} \times E_{i-1} = L_i,$$

$$C2.6. E_{i+1} \times A'_{i-1} = M_i,$$

$$C2.7. F'_i = \overline{F}'_i,$$

Theorem.

Given a Grassmann configuration, $(\{A_i\}, \{B_i\}, \{E_i\})$,

0. the points $C_i, AB_i, D_i, F_i, \overline{F}_i, Cd_i, Dc_i, CF_i, C\overline{F}_i, DE_i, Ef_i, Fe_i, E\overline{f}_i, \overline{F}e_i$, are on the cubic γ through A_i, B_i, E_i .
1. $(A_i a'_i), (B_i b'_i), (C_i c'_i), (D_i d'_i), (AB_i ab'_i), (E_i e'_i), (F_i f'_i), (\overline{F}_i \overline{f}'_i) \iota \gamma$.
2. $E_i \star E_i = AB_i \star AB_i$.
3. The points A_i, B_i, AB_i , are on a cubic configuration.
4. $\langle A'_{i+1}, A'_{i-1}, AB'_i \rangle$,
5. $\langle B'_{i+1}, B'_{i-1}, AB'_i \rangle$,
6. $\langle AB'_{i+1}, AB'_{i-1}, C'_i \rangle$,
7. $\langle AB'_i, C'_i, D'_i \rangle$,
8. $\langle A'_i, AB'_i, F'_i \rangle$,

Proof: To prove that AB_0 is on the cubic, we have to prove, because of 3.2.10, $\langle (AB_0 \times A_0) \times b_0, (AB_0 \times A_1) \times b_1, (AB_0 \times A_2) \times b_2 \rangle$, but the second point is B_2 and the third is B_1 and both are on b_0 . The rest of the proof follows from 6.0.2 given below.

Comment.

The preceding Theorem was conjectured in the process of construction the third point on a Grassmann cubic and the line through 2 points of the cubic, using intersection of conics and lines, (Fig. hd.c) using the Theorem of Grassmann, (Henry White, 1925, p. 109, Fig. 27.) For instance, the conic through $B = B_{01}, C = B_{02}, A' = B_{10}, D = (B \times C' = B_{12}) \times (C \times B' = B_{11})$ and X , intersects $A \times X$ at the third point $A \star X$.

Theorem.

We have the following table for the operation \star between points on a Grassmann cubic:

\star	AB_0	AB_1	AB_2	A_0	A_1	A_2	B_0	B_1	B_2						
AB_0	AB'_0	C_2	C_1	F_0	B_2	B_1	\overline{F}_0	A_2	A_1						
AB_1	C_2	AB'_1	C_0	B_2	F_1	B_0	A_2	\overline{F}_1	A_0						
AB_2	C_1	C_0	AB'_2	B_1	B_0	F_2	A_1	A_0	\overline{F}_2						
A_0	F_0	B_2	B_1	A'_0	E_2	E_1	D_0	AB_2	AB_1						
A_1	B_2	F_1	B_0	E_2	A'_1	E_0	AB_2	D_1	AB_0						
A_2	B_1	B_0	F_2	E_1	E_0	A'_2	AB_1	AB_0	D_2						
B_0	\overline{F}_0	A_2	A_1	D_0	AB_2	AB_1	A'_0	E_2	E_1						
B_1	A_2	\overline{F}_1	A_0	AB_2	D_1	AB_0	E_2	A'_1	E_0						
B_2	A_1	A_0	\overline{F}_2	AB_1	AB_0	D_2	E_1	E_0	A'_2						
\star	AB_0	AB_1	AB_2	A_0	A_1	A_2	B_0	B_1	B_2	C_0	C_1	C_2	D_0	D_1	D_2
C_0	D_0	AB_2	AB_1	K_0	$C\overline{F}_2$	$C\overline{F}_1$	\overline{K}_0	$C\overline{F}_2$	$C\overline{F}_1$	C'_0	Cc_2	Cc_1	AB_0	Cd_2	Dc_1
C_1	AB_2	D_1	AB_0	$C\overline{F}_2$	K_1	$C\overline{F}_0$	$C\overline{F}_2$	\overline{K}_1	$C\overline{F}_0$	Cc_2	C'_1	Cc_0	Dc_2	AB_1	Cd_0
C_2	AB_1	AB_0	D_2	$C\overline{F}_1$	$C\overline{F}_0$	K_2	$C\overline{F}_1$	$C\overline{F}_0$	\overline{K}_2	Cc_1	Cc_0	C'_2	Cd_1	Dc_0	AB_2
D_0	C_0	L_2	\overline{L}_1	B_0	Fe_2	Ef_1	A_0	$\overline{F}e_2$	$E\overline{f}_1$	AB_0	Dc_2	Cd_1	D'_0	AB'_2	AB'_1
D_1	\overline{L}_2	C_1	L_0	Ef_2	B_1	Fe_0	$E\overline{f}_2$	A_1	$\overline{F}e_0$	Cd_2	AB_1	Dc_1	AB'_2	D'_1	AB'_0
D_2	L_1	\overline{L}_0	C_2	Fe_1	Ef_0	B_2	$\overline{F}e_1$	$E\overline{f}_0$	A_2	Dc_1	Cd_0	AB_2	AB'_1	AB'_0	D'_2
E_0	M_0	DE_2	DE_1	\overline{F}_0	A_2	A_1	F_0	B_2	B_1	A'_0	E_2	E_1	DE_0	Ed_2	De_1
E_1	DE_2	M_1	DE_0	A_2	\overline{F}_1	A_0	B_2	F_1	B_0	E_2	A'_1	E_0	De_2	DE_1	Ed_0
E_2	DE_1	DE_0	M_2	A_1	A_0	\overline{F}_2	B_1	B_0	F_2	E_1	E_0	A'_2	Ed_1	De_0	DE_2
F_0	A_0	$\overline{F}e_2$	$E\overline{f}_1$	AB_0	Dc_2	Cd_1	E_0	P_2	Q_1	$C\overline{F}_0$	Fc_2	Cf_1	$D\overline{F}_0$	\overline{F}_2	\overline{F}_1
F_1	$E\overline{f}_2$	A_1	$\overline{F}e_0$	Cd_2	AB_1	Dc_0	Q_2	E_1	P_0	Cf_2	$C\overline{F}_1$	Fc_0	\overline{F}_2	$D\overline{F}_1$	\overline{F}_0
F_2	$\overline{F}e_1$	$E\overline{f}_0$	A_2	Dc_1	Cd_0	AB_2	P_1	Q_0	E_2	Fc_1	Cf_0	$C\overline{F}_2$	\overline{F}_1	\overline{F}_0	$D\overline{F}_2$
\overline{F}_0	B_0	Fe_2	Ef_1	E_0	P_2	Q_1	AB_0	Dc_2	Cd_1	$C\overline{F}_0$	$\overline{F}c_2$	$C\overline{f}_1$	$D\overline{F}_0$	F_2	F_1
\overline{F}_1	Ef_2	B_1	Fe_0	Q_2	E_1	P_0	Cd_2	AB_1	Dc_0	$C\overline{f}_2$	$C\overline{F}_1$	$\overline{F}c_0$	F_2	$D\overline{F}_1$	F_0
\overline{F}_2	Fe_1	Ef_0	B_2	P_1	Q_0	E_2	Dc_1	Cd_0	AB_2	$\overline{F}c_1$	$C\overline{f}_0$	$C\overline{F}_2$	F_1	F_0	$D\overline{F}_2$
\star	E_0	E_1	E_2	F_0	F_1	F_2	\overline{F}_0	\overline{F}_1	\overline{F}_2						
E_0	AB'_0	C_2	C_1	B_0	$E\overline{f}_2$	Fe_1	A_0	$E\overline{f}_2$	$\overline{F}e_1$						
E_1	C_2	AB'_1	C_0	Fe_2	B_1	$E\overline{f}_0$	$\overline{F}e_2$	A_1	$E\overline{f}_0$						
E_2	C_1	C_0	AB'_2	$E\overline{f}_1$	Fe_0	B_2	$E\overline{f}_1$	$\overline{F}e_0$	A_2						
F_0	B_0	Fe_2	$E\overline{f}_1$	F'_0	A'_2	A'_1	FF_0	D_2	D_1						
F_1	$E\overline{f}_2$	B_1	Fe_0	A'_2	F'_1	A'_0	D_2	FF_1	D_0						
F_2	Fe_1	$E\overline{f}_0$	B_2	A'_1	A'_0	F'_2	D_1	D_0	FF_2						
\overline{F}_0	A_0	$\overline{F}e_2$	$E\overline{f}_1$	FF_0	D_2	D_1	F'_0	A'_2	A'_1						
\overline{F}_1	$E\overline{f}_2$	A_1	$\overline{F}e_0$	D_2	FF_1	D_0	A'_2	F'_1	A'_0						
\overline{F}_2	$\overline{F}e_1$	$E\overline{f}_0$	A_2	D_1	D_0	FF_2	A'_1	A'_0	F'_2						

Proof:

α_0	$D9(C_0$	D_0	B_0	A_1	B_2	AB_1	; AB_0	A_0	$AB_2)$
$\rho\alpha_0$	$D9(E_2$	F_2	A_2	AB_0	A_1	B_0	; B_2	AB_2	$B_1)$
$\rho^2\alpha_0$	$C9(E_1$	\overline{F}_1	AB_1	B_2	AB_0	A_2	; A_1	B_1	$A_0)$
α_1	$C9(E_1$	E_2	B_0	AB_1	AB_2	A_0	; C_0	B_1	$A_2)$
$\beta\alpha_1$	$C9(F_2$	\overline{F}_1	AB_1	B_0	A_0	AB_2	; D_0	B_1	$A_2)$
$\sigma\beta\alpha_1$	$C9(\overline{F}_2$	F_1	AB_1	A_0	B_0	AB_2	; D_0	A_1	$B_2)$
α_2	$C9(C_1$	D_2	A_2	F_2	A_1	AB_0	; Cd_0	B_2	$AB_2)$
$\sigma\alpha_2$	$C9(C_1$	D_2	B_2	\overline{F}_2	B_1	AB_0	; Cd_0	A_2	$AB_2)$
$021021\alpha_2$	$C9(C_2$	D_1	B_1	\overline{F}_1	B_2	AB_0	; Dc_0	A_1	$AB_1)$
$\sigma 021021\alpha_2$	$C9(C_2$	D_1	A_1	F_1	A_2	AB_0	; Dc_0	B_1	$AB_1)$
α_3	$C9(C_0$	F_0	AB_0	C_1	B_2	AB_1	; CF_0	A_0	$AB_2)$
$\sigma\alpha_3$	$C9(C_0$	\overline{F}_0	AB_0	C_1	A_2	AB_1	; $C\overline{F}_0$	B_0	$AB_2)$
$021021\alpha_3$	$C9(C_0$	\overline{F}_0	AB_0	C_2	A_1	AB_2	; $C\overline{F}_0$	B_0	$AB_1)$
$\sigma 021021\alpha_3$	$C9(C_0$	F_0	AB_0	C_2	B_1	AB_2	; CF_0	A_0	$AB_1)$
α_4	$C9(D_0$	E_0	A_1	E_2	AB_1	B_0	; DE_0	A_2	$A_0)$
$021021\alpha_4$	$C9(D_0$	E_0	B_2	E_1	AB_2	A_0	; DE_0	B_1	$B_0)$
α_5	$C9(E_0$	F_0	A_0	E_2	B_1	A_2	; B_0	AB_0	$A_1)$
$\sigma\alpha_5$	$C9(E_0$	\overline{F}_0	B_0	E_2	A_1	B_2	; A_0	AB_0	$B_1)$
$021021\alpha_5$	$C9(E_0$	\overline{F}_0	B_0	E_1	A_2	B_1	; A_0	AB_0	$B_2)$
$\sigma 021021\alpha_5$	$C9(E_0$	F_0	A_0	E_1	B_2	A_1	; B_0	AB_0	$A_2)$
α_6	$C9(E_1$	\overline{F}_2	AB_2	F_2	AB_1	A_0	; $E\overline{f}_0$	B_2	$A_2)$
$\sigma\alpha_6$	$C9(E_1$	F_2	AB_2	\overline{F}_2	AB_1	B_0	; Ef_0	A_2	$B_2)$
α_7	$C9(F_1$	E_2	B_1	\overline{F}_1	AB_2	A_1	; Fe_0	B_0	$AB_1)$
$\sigma\alpha_7$	$C9(\overline{F}_1$	E_2	A_1	F_1	AB_2	B_1	; $\overline{F}e_0$	A_0	$AB_1)$
$\sigma\alpha_8$	$C9(C_0$	E_0	B_1	A_0	A_0	AB_1	; A'_0	B_2	$AB_2)$
α'_8	$C9(A_0$	A_0	B_1	B_0	B_0	A_1	; A'_0	AB_2	$E_1)$
$012210\alpha_8$	$C9(F_1$	F_2	AB_2	B_0	B_0	AB_1	; A'_0	A_2	$A_1)$
$\sigma\alpha_8$	$C9(\overline{F}_1$	\overline{F}_2	AB_2	A_0	A_0	AB_1	; A'_0	B_2	$B_1)$
$210102\alpha_8$	$C9(E_0$	E_0	A_2	AB_0	AB_0	B_2	; AB'_0	A_1	$B_1)$
$120102\alpha_8$	$C9(D_2$	D_1	A_2	AB_0	AB_0	A_1	; AB'_0	B_2	$B_1)$
$210012\alpha_9$	$C9(D_1$	B_2	AB_1	F_1	AB_2	B_1	; $\overline{F}e_0$	A_0	$A_1)$
$\sigma 210012\alpha_9$	$C9(D_1$	A_2	AB_1	\overline{F}_1	AB_2	A_1	; Fe_0	B_0	$B_1)$
$012102\alpha_9$	$C9(F_2$	AB_1	B_2	D_2	B_1	AB_2	; $E\overline{f}_0$	A_0	$A_2)$
$\sigma 012102\alpha_9$	$C9(\overline{F}_2$	AB_1	A_2	D_2	A_1	AB_2	; Ef_0	B_0	$B_2)$
$120201\alpha_9$	$C9(E_1$	AB_2	A_1	E_2	AB_1	A_2	; DE_0	B_0	$A_0)$
α_{10}	$C9(AB_0$	E_0	A_2	D_2	A'_1	A_1	; M_0	A_1	$B_2)$
α_{11}	$C9(AB_2$	D_1	B_1	A'_1	E_2	A_0	; L_0	A_1	$B_1)$
$? \alpha_{11}$	$C9(AB_1$	D_2	B_2	A'_2	E_1	A_0	; \overline{L}_0	A_2	$B_2)$
α_{12}	$C9(F_1$	B_2	B_0	A_2	\overline{F}_1	A_1	; P_0	E_1	$AB_1)$
$? \alpha_{12}$	$C9(F_2$	B_1	B_0	A_1	\overline{F}_2	A_2	; Q_0	E_2	$AB_2)$
α_{13}	$C9(C_0$	C_0	AB_0	C_1	L_2	AB_1	; C'_0	D_0	$AB_2)$
$? \alpha_{13}$	$C9(C_0$	C_0	AB_0	C_2	\overline{L}_1	AB_2	; C'_0	D_0	$AB_1)$
α_{14}	$C9(F_0$	F_0	B_0	\overline{F}_0	\overline{F}_0	A_0	; F'_0	E_0	$AB_0)$
α_{15}	$C9(A_0$	C_0	E_0	DE_0	B_0	B_0	; K_0	A'_0	$D_0)$
$? \alpha_{15}$	$C9(B_0$	C_0	E_0	DE_0	A_0	A_0	; \overline{K}_0	A'_0	$D_0)$
α_{16}	$C9(AB_0$	AB_0	AB_1	L_2	Cc_1	C_0	; AB'_0	C_2	$D_0)$
$? \alpha_{16}$	$C9(AB_0$	AB_0	AB_2	\overline{L}_1	Cc_2	C_0	; AB'_0	C_1	$D_0)$
α_{17}	$C9(AB_0$	AB_0	C_1	Cc_0	C_0	AB_1	; AB'_0	AB_2	$C_2)$
α_{18}	$C9(C_1$	C_2	AB_2	L_0	\overline{L}_0	AB_1	; Cc_0	D_2	$D_1)$
α_{19}	$C9(F_0$	F_0	D_1	\overline{L}_2	P_1	A_0	; F'_0	\overline{F}_2	$AB_0)$
α_{20}	$C9(D_0$	F_0	E_0	\overline{F}_0	A'_0	B_0	; DF_0	B_0	$A_0)$
$? \alpha_{20}$	$C9(D_0$	\overline{F}_0	E_0	F_0	A'_0	A_0	; $D\overline{F}_0$	A_0	$B_0)$

α_{21}	$C9(F_1$	C_2	AB_1	\overline{F}_1	DE_2	E_1	;	Fc_0	AB_0	$B_1)$
$?\alpha_{21}$	$C9(\overline{F}_1$	C_2	AB_1	F_1	DE_2	E_1	;	$\overline{F}c_0$	AB_0	$A_1)$
α_{22}	$C9(C_1$	F_2	E_2	M_2	A_1	AB_0	;	Cf_0	B_2	$AB_2)$
$?\alpha_{22}$	$C9(C_1$	\overline{F}_2	E_2	M_2	B_1	AB_0	;	$C\overline{f}_0$	A_2	$AB_2)$
α_{23}	$C9(F_0$	F_0	D_2	L_1	Q_2	A_0	;	F'_0	\overline{F}_1	$AB_0)$
$?\alpha_{23}$	$C9(F_0$	F_0	D_1	\overline{L}_2	P_1	A_0	;	F'_0	\overline{F}_2	$AB_0)$
α_{24}	$C9(D_0$	D_0	C_0	K_0	\overline{F}_0	B_0	;	D'_0	AB_0	$A_0)$
$?\alpha_{24}$	$C9(D_0$	D_0	C_0	\overline{K}_0	F_0	A_0	;	D'_0	AB_0	$A_0)$
α_{25}	$C9(E_1$	D_2	B_2	B_1	K_2	C_2	;	Ed_0	A_2	$E_0)$
$?\alpha_{25}$	$C9(E_2$	D_1	B_1	B_2	K_1	C_1	;	De_0	A_1	$E_0)$
α_{26}	$C9(C_0$	F_0	A_0	B_0	AB'_0	AB_0	;	CF_0	AB_0	$D_0)$
$?\alpha_{26}$	$C9(C_0$	\overline{F}_0	B_0	A_0	AB'_0	AB_0	;	$C\overline{F}_0$	AB_0	$D_0)$
α_{27}	$C9(F_0$	\overline{F}_0	B_0	D_0	AB'_0	AB_0	;	FF_0	AB_0	$A_0)$

Theorem.

Given a Grassmann configuration $(\{A_i\}, \{B_i\}, \{E_i\})$, The tangential points at A_i and B_i are the same, in the above case A'_i , it will be added to the configuration after a semi colon.

Lemma.

If $(\{A_i\}, \{B_i\}, \{E_i\}, \{A'_i\})$, is a Grassmann configuration so is

$$0. (\{A_i\}, \{B_i\}, \{E_i\}),,$$

where

$$AB_i := A_{i+1} \star B_{i-1}, \text{ and } C_i := AB_{i+1} \star AB_{i-1}.$$

$$1. (\{F_i\}, \{\overline{F}_i\}, \{A'_i\}),,$$

where

$$F_i := AB_i \star A_i, \text{ and } \overline{F}_i := AB_i \star B_i,$$

This follows at once from grom 6.0.2.

Theorem.

Given a Grassmann configuration $(\{A_i\}, \{B_i\}, \{E_i\}; \{AB_i\})$, the following are also Grassmann configurations:

$$0. (\{AB_i\}, \{E_i\}, \{C_i\}; \{AB'_i\}),$$

$$1. (\{F_i\}, \{\overline{F}_i\}, \{A'_i\}; \{F'_i\}),$$

$$2. (\{DE_i\}, \{C_i\}, \{C_i \star AB'_i\}),$$

$$3. (\{D_i\}, \{A'_i\}, \{AB'_i\}; \{d'_i\}).$$

Proof: This follows by repeated applications of the Lemma 3.2.10.

3.2.11 Grassmannian cubics in Involutive Geometry.

Definition.

In involutive geometry I will give the name of Grassmannian cubic to the special case where the 6 lines are m_i and \bar{m}_i .

Theorem.

The correspondence between the elements as given above and those of involutive geometry is as follows

$A_i = CF_i$	$B_i = C\bar{F}_i$	$E_i = DE_i$	$AB_i = C_i = Cc_i$	$F_i = K_i$	$\bar{F}_i = \bar{K}_i$			
MM_i	$\bar{M}M_i$	A_i	AT_i	F_i	\bar{F}_i			
$Ef_i = C\bar{f}_i$	$E\bar{f}_i = Cf_i$	$Fe_i = \bar{F}c_i$	$\bar{F}e_i = Fc_i$	$A'_i = M_i$	$L_i = Cd_i$	$\bar{L}_i = Dc_i$	P_i	Q_i
Ef_i	$E\bar{f}_i$	Fe_i	$\bar{F}e_i$	MM'_i	L_i	\bar{L}_i	P_i	Q_i
a_i	b_i	aB_i	$a\bar{B}_i$	ab_i	e_i	ae_i	be_i	ba_i
mm_i	$\bar{m}m_i$	c_i	\bar{c}_i	a_i	$aeUL_i$	nm_i	$\bar{n}m_i$	eul

Theorem.

0. The Grassmann cubic passes through the points $MM_i, \bar{M}M_i, A_i, D_i$.

1. Its equation is

$$m_0(m_1 + m_2)X_1X_2((m_2 + m_0)X_1 + (m_0 + m_1)X_2)m_1(m_2 + m_0)X_2X_0((m_0 + m_1)X_2 + (m_1 + m_2)X_0)m_2(m_0 + m_1)X_0X_1((m_1 + m_2)X_0 + (m_2 + m_0)X_1) + (s_{21} + 2s_{111})X_0X_1X_2 = 0$$

Proof: Using 3.2.9 on the points A_i and AT_i , we obtain the given form, to determine the coefficients g_i of $X_1X_2((m_2 + m_0)X_1 + (m_0 + m_1)X_2)$, ... and g of $X_0X_1X_2$ we impose the condition that the cubic passes through MM_i , this gives the system of equations

....

Theorem.

Let

$$D2.0. aB_i := A_{i+1} \times B_{i-1}, a\bar{B}_i := A_{i-1} \times B_{i+1},$$

$$D2.1. AB_i := aB_i \times a\bar{B}_i,$$

$$D2.2. abE_i := AB_{i+1} \times E_{i-1}, ab\bar{E}_i := AB_{i-1} \times E_{i+1},$$

$$D2.3. DE_i := abE_i \times ab\bar{E}_i,$$

$$D2.4. de_i := DE_i \times E_i,$$

$$D2.5. ab_i := A_i \times B_i,$$

$$D2.6. D_i := de_i \times ab_i,$$

$$D2.6. ba_i := AB_{i+1} \times AB_{i-1},$$

$$D2.8. abd_i := D_i \times AB_i,$$

$$D2.9. C_i := ba_i \times abd_i,$$

$$D4.0. ae_i := A_i \times E_i, be_i := B_i \times E_i,$$

- $D4.1. ce_i := C_i \times E_i,$
 $D4.2. aab_i := A_i \times AB_i, bab_i := B_i \times AB_i,$
 $D4.3. F_i := be_i \times aab_i, \overline{F}_i := ae_i \times bab_i,$
 $D4.4. f_i := F_{i+1} \times \overline{F}_{i-1}, \overline{f}_i := \overline{F}_{i+1} \times \overline{F}_{i-1},$
 $D4.5. A'_i := ce_i \times \overline{f}_i, B'_i := ce_i \times f_i,$
 $D4.6. aC_i := A_{i+1} \times C_{i-1}, a\overline{C}_i := A_{i-1} \times C_{i+1},$
 $D4.6. bC_i := B_{i+1} \times C_{i-1}, b\overline{C}_i := B_{i-1} \times C_{i+1},$
 $D4.7. CF_i := bC_i \times b\overline{C}_i, C\overline{F}_i := aC_i \times a\overline{C}_i,$
 $D4.8. cD_i := C_{i+1} \times D_{i-1}, c\overline{D}_i := C_{i-1} \times D_{i+1},$
 $D4.9. aF_i := A_{i+1} \times F_{i-1}, a\overline{F}_i := A_{i-1} \times F_{i+1},$
 $D4.10. Cd_i := cD_i \times aF_i, Dc_i := c\overline{D}_i \times a\overline{F}_i,$
 $D4.11. aD_i := A_{i+1} \times D_{i-1}, a\overline{D}_i := A_{i-1} \times D_{i+1},$
 $D4.12. eF_i := E_{i+1} \times F_{i-1}, e\overline{F}_i := E_{i-1} \times F_{i+1},$
 $D4.13. Ef_i := aD_i \times eF_i, Fe_i := a\overline{D}_i \times e\overline{F}_i,$
 $D4.14. bD_i := B_{i+1} \times D_{i-1}, b\overline{D}_i := B_{i-1} \times D_{i+1},$
 $D4.15. \overline{f}E_i := E_{i+1} \times \overline{F}_{i-1}, \overline{f}E_i := E_{i-1} \times \overline{F}_{i+1},$
 $D4.16. E\overline{f}_i := bD_i \times \overline{f}E_i, \overline{F}e_i := b\overline{D}_i \times \overline{f}E_i,$
 $D4.17. ef_i := E_i \times F_i, e\overline{f}_i := E_i \times \overline{F}_i,$
 $D5.0. a'D_i := A'_{i+1} \times D_{i-1}, a'\overline{D}_i := A'_{i-1} \times D_{i+1},$
 $D5.1. abe_i := AB_i \times E_i,$
 $D5.2. M_i := a'D_i \times abe_i,$
 $D5.3. dAB_i := D_{i+1} \times AB_{i-1}, dA\overline{B}_i := D_{i-1} \times AB_{i+1},$
 $D5.4. a'E_i := A'_{i+1} \times E_{i-1}, a'\overline{E}_i := A'_{i-1} \times E_{i+1},$
 $D5.5. L_i := dAB_i \times a'E_i, \overline{L}_i := dA\overline{B}_i \times a'\overline{E}_i,$
 $D5.6. fB_i := F_{i+1} \times B_{i-1}, f\overline{B}_i := F_{i-1} \times B_{i+1},$
 $D5.7. \overline{f}A_i := \overline{F}_{i+1} \times A_{i-1}, \overline{f}A_i := \overline{F}_{i-1} \times A_{i+1},$
 $D5.8. P_i := fB_i \times \overline{f}A_i, Q_i := f\overline{B}_i \times \overline{f}A_i,$
 $D5.9. ac_i := A_i \times C_i, bc_i := B_i \times C_i,$
 $D5.10. bde_i := B_i \times DE_i, ade_i := A_i \times DE_i,$
 $D5.11. K_i := ac_i \times bde_i, \overline{K}_i := bc_i \times ade_i,$
 $D5.12. dE_i := D_{i+1} \times E_{i-1}, eD_i := E_{i+1} \times E_{i-1},$
 $D5.13. bK_i := B_{i+1} \times K_{i-1}, kB_i := B_{i-1} \times K_{i+1},$
 $D5.14. Ed_i := eD_i \times bK_i, De_i := dE_i \times kB_i,$
 $D6.0. cL_i := C_{i+1} \times L_{i-1}, c\overline{L}_i := C_{i-1} \times \overline{L}_{i+1},$
 $D6.1. C'_i := cL_i \times c\overline{L}_i,$
 $D6.2. k\overline{f}_i := K_i \times \overline{F}_i, \overline{k}f_i := \overline{K}_i \times F_i,$
 $D6.3. D'_i := k\overline{f}_i \times \overline{k}f_i,$
 $D6.4. a'f_i := A'_i \times F_i, a'\overline{f}_i := A'_i \times \overline{F}_i,$
 $D6.5. df_i := D_i \times F_i, d\overline{f}_i := D_i \times \overline{F}_i,$
 $D6.6. DF_i := a'\overline{f}_i \times df_i, D\overline{F}_i := a'f_i \times d\overline{f}_i,$
 $D6.7. fC_i := F_{i+1} \times C_{i-1}, f\overline{C}_i := F_{i-1} \times C_{i+1},$
 $D6.8. \overline{f}C_i := \overline{F}_{i+1} \times C_{i-1}, \overline{f}C_i := \overline{F}_{i-1} \times C_{i+1},$
 $D6.9. fDE_i := F_{i+1} \times DE_{i-1}, fD\overline{E}_i := \overline{F}_{i+1} \times DE_{i-1},$
 $D6.10. aM_i := A_{i+1} \times M_{i-1}, bM_i := B_{i+1} \times M_{i-1},$
 $D6.11. Fc_i := fC_i \times fD\overline{E}_i, \overline{F}c_i := \overline{f}C_i \times fDE_i,$

- D6.12. $Cf_i := f\overline{C}_i \times aM_i$, $C\overline{f}_i := \overline{fC}_i \times bM_i$,
 D6.13. $c_i := C_{i+1} \times C_{i-1}$, $ll_i := L_i \times \overline{L}_i$,
 D6.14. $Cc_i := c_i \times ll_i$,
 D6.15. $ccL_i := Cc_{i+1} \times L_{i-1}$, $cc\overline{L}_i := Cc_{i-1} \times \overline{L}_{i+1}$,
 D6.16. $AB'_i := ccL_i \times cc\overline{L}_i$,
 D6.17. $lQ_i := L_{i+1} \times Q_{i-1}$, $p\overline{L}_i := P_{i+1} \times \overline{L}_{i-1}$,
 D6.18. $F'_i := lQ_i \times p\overline{L}_i$,
 D6.19. $f\overline{f}_i := F_i \times \overline{F}_i$, $dab'_i := D_i \times AB'_i$,
 D6.20. $FF_i := f\overline{f}_i \times dab'_i$,
 D7.0. $a'_i := A_i \times A'_i$,
 D7.1. $b'_i := B_i \times A'_i$,
 D7.2. $c'_i := C_i \times C'_i$,
 D7.3. $d'_i := D_i \times D'_i$,
 D7.4. $ab'_i := AB_i \times AB'_i$,
 D7.5. $e'_i := E_i \times AB'_i$,
 D7.6. $f'_i := F_i \times F'_i$,
 D7.7. $\overline{f}'_i := \overline{F}_i \times F'_i$,

then

- C2.0. $C_i \iota e_i$,
 C2.1. $X_i = Y_i$,
 C2.2. $A'_i = B'_i$,
 C2.3. $A_i \iota e\overline{f}_i$, $B_i \iota ef_i$,
 C2.4. $A'_{i+1} \times D_{i-1} = M_i$,
 C2.5. $A'_{i+1} \times E_{i-1} = L_i$,
 C2.6. $E_{i+1} \times A'_{i-1} = M_i$,
 C2.7. $F'_i = \overline{F}'_i$,

- Proof:* H0.0. $m_0 = [0, 1, 1]$, $\overline{m}_0 = [0, m2, m1]$,
 D1.0. $MM_0 = (-1, 1, 1)$, $\overline{M}M_0 = (m0, -m1, -m2)$
 D0.10. $A_0 = (1, 0, 0)$
 D0.10. $a_0 = [1, 0, 0]$
 D.. $ma_0 = [0, 1, -1]$, $\overline{m}a_0 = [0, m2, -m1]$,
 D.. $eul_0 = [m1 - m2, -(m2 - m0), -(m0 - m1)]$,
 D.. $y_0 = [m1 - m2, -(m2 + m0), -(m0 + m1)]$,
 D.. $y_0 = [m1 - m2, m2 + m0, m0 + m1]$,
 D.. $AT_0 = (0, m0 + m1, -(m2 - m0))$,
 D.. $k = [m1 + m2, m2 + m0, m0 + m1]$,
 D.. $\overline{t}AM_0 = [s1 + m0, m2 + m0, m0 + m1]$,
 D.. $tAM_0 = [s11 + m1m2, m0(m2 + m0), m0(m0 + m1)]$,
 D.. $F_0 = (s11 + m1m2, -m1(s1 + m0), -m2(s1 + m0))$,
 D.. $\overline{F}_0 = (m0(s1 + m0), -(s11 + m1m2), -(s11 + m1m2))$,
 D.. $\overline{f}f_0 = [m1(m1 - m2), s11 + m2m0, m1(s1 + m2)]$,
 D.. $D_0 = (m1 + m2)q_0, -m1(m1 - m2)(m2 + m0), m2(m0 + m1)(m1 - m2))$,
 D.. $eul = [m1 - m2, m2 - m0, m0 - m1]$,

$$\begin{aligned}
D.. \ aAT_0 &= [0, m2 + m0, m0 + m1], \\
D.. \ \bar{f}_0 &= [(m1 + m2)q0, -(m2 + m0)(s11 + m2m0), -(m0 + m1)(s11 + m0m1), \\
D.. \ MM'_0 &= (m0(m1 - m2)(m2 + m0)(m0 + m1), -(m0 + m1)(m1 + m2)q0, (m1 + m2)(m2 + \\
&\quad m0)q0), \\
D.. \ 0 &= [(m1 - m2)(s11 + m2m0), m1(m2 - m0)^2, m2q1 - m0q2 + m0m1(m1 - m2)], \\
D.. \ 0 &= [s11 + m2m0, m0(s1 + m1), 0], \\
D.. \ Fe_0 &= (m0(s1 + m1)(m2q1 - m0q2 + m0m1(m1 - m2)), -(s11 + m2m0)(m2q1 - m0q2 + \\
&\quad m0m1(m1 - m2)), (s11 + m2m0)(m1q2 - m0q1 - m2m0(m1 - m2))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ Ef_0 &= (m0(s1 + m2)(m1q2 - m0q1 - m2m0(m1 - m2), (s11 + m0m1)(m2q1 - m0q2 + \\
&\quad m0m1(m1 - m2)), -(s11 + m0m1)(m1q2 - m0q1 - m2m0(m1 - m2))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ \bar{Fe}_0 &= ((s11 + m2m0)(m1q2 - m0q1 - m2m0(m1 - m2), (s11 + m0m1)(m1q2 - m0q1 - \\
&\quad m2m0(m1 - m2), -(s11 + m0m1)(m2q1 - m0q2 + m0m1(m1 - m2))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ E\bar{f}_0 &= ((s11 + m0m1)(m2q1 - m0q2 + m0m1(m1 - m2), m1(s1 + m2)(m1q2 - m0q1 - \\
&\quad m2m0(m1 - m2), -m2(s1 + m2)(m2q1 - m0q2 + m0m1(m1 - m2))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ Ed_0 &= (m0(m1 + m2)^2(m2 + m0)(m0 - m1), -m1q2(2m1(m1 + m2) + (m2 + m0)(m0 + \\
&\quad m1)), s21 + 2s111), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ De_0 &= (m0(m1 + m2)^2(m2 - m0)(m0 + m1), s21 + 2s111, m2q1(2m2(m1 + m2) + (m2 + \\
&\quad m0)(m0 + m1))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ L_0 &= ((m2 + m0)q1(m0^2 + m1m2 + 3m0(m1 + m2), m1(m1 + m2)(m2 - m0)(m0^2 + \\
&\quad m1m2 + 3m0(m1 + m2), -(m1 + m2)(m2 - m0)(s21 + 2s111)), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ \bar{L}_0 &= ((m0 + m1)q2(m0^2 + m1m2 + 3m0(m1 + m2), (m0 - m1)(m1 + m2)(s21 + \\
&\quad 2s111), -m2(m0 - m1)(m1 + m2)(m0^2 + m1m2 + 3m0(m1 + m2))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ P_0 &= (m0(m1 + m2)^2(m2 - m0)(m0 + m1), (s21 + 2s111)q1, -m2q1(m0^2 + m1m2 + \\
&\quad 3m0(m1 + m2))), \\
D.. \ 0 &= \square, \\
D.. \ 0 &= \square, \\
D.. \ Q_0 &= (m0(m1 + m2)^2(m2 + m0)(m0 - m1), -m1q2(m0^2 + m1m2 + 3m0(m1 + m2), -(s21 + \\
&\quad 2s111)q2),
\end{aligned}$$

\star	AT_0	AT_1	AT_2	MM_0	MM_1	MM_2	\overline{MM}_0	\overline{MM}_1	\overline{MM}_2	A_0	A_1	A_2	D_0	D_1
AT_0	D_0	AT_2	AT_1	F_0	\overline{MM}_2	\overline{MM}_1	\overline{F}_0	\overline{MM}_2	\overline{MM}_1	MM'_0	A_2	A_1	AT_0	\overline{L}_2
AT_1	AT_2	D_1	AT_0	\overline{MM}_2	F_1	\overline{MM}_0	MM_2	\overline{F}_1	MM_0	A_2	MM'_1	A_0	L_2	AT_1
AT_2	AT_1	AT_0	D_2	\overline{MM}_1	\overline{MM}_0	F_2	MM_1	MM_0	\overline{F}_2	A_1	A_0	MM'_2	\overline{L}_1	L_0
MM_0	F_0	\overline{MM}_2	\overline{MM}_1	MM'_0	A_2	A_1	D_0	AT_2	AT_1	\overline{F}_0	MM_2	MM_1	\overline{MM}_0	Ef_2
MM_1	\overline{MM}_2	F_1	\overline{MM}_0	A_2	MM'_1	A_0	AT_2	D_1	AT_0	MM_2	\overline{F}_1	MM_0	Fe_2	\overline{MM}_1
MM_2	\overline{MM}_1	\overline{MM}_0	F_2	A_1	A_0	MM'_2	AT_1	AT_0	D_2	MM_1	MM_0	\overline{F}_2	Ef_1	Fe_0
\overline{MM}_0	\overline{F}_0	MM_2	MM_1	D_0	AT_2	AT_1	MM'_0	A_2	A_1	F_0	\overline{MM}_2	\overline{MM}_1	MM_0	Ef_2
\overline{MM}_1	MM_2	\overline{F}_1	MM_0	AT_2	D_1	AT_0	A_2	MM'_1	A_0	\overline{MM}_2	F_1	\overline{MM}_0	\overline{Fe}_2	MM_1
\overline{MM}_2	MM_1	MM_0	\overline{F}_2	AT_1	AT_0	D_2	A_1	A_0	MM'_2	\overline{MM}_1	\overline{MM}_0	F_2	\overline{Ef}_1	\overline{Fe}_0
A_0	MM'_0	A_2	A_1	\overline{F}_0	MM_2	MM_1	\overline{F}_0	\overline{MM}_2	\overline{MM}_1	D_0	AT_2	AT_1	A_0	De_2
A_1	A_2	MM'_1	A_0	MM_2	\overline{F}_1	MM_0	\overline{MM}_2	F_1	\overline{MM}_0	AT_2	D_1	AT_0	Ed_2	A_1
A_2	A_1	A_0	MM'_2	MM_1	MM_0	\overline{F}_2	\overline{MM}_1	\overline{MM}_0	F_2	AT_1	AT_0	D_2	De_1	Ed_0
D_0	AT_0	L_2	\overline{L}_1	\overline{MM}_0	Fe_2	Ef_1	MM_0	\overline{Fe}_2	\overline{Ef}_1	A_0	Ed_2	De_1	D'_0	D_2
D_1	\overline{L}_2	AT_1	L_0	Ef_2	\overline{MM}_1	Fe_0	\overline{Ef}_2	MM_1	\overline{Fe}_0	De_2	A_1	Ed_1	D_2	D'_1
D_2	L_1	\overline{L}_0	AT_2	Fe_1	Ef_0	\overline{MM}_2	\overline{Fe}_1	\overline{Ef}_0	MM_2	Ed_1	De_0	A_2	D_1	D_0
F_0	MM_0	\overline{Fe}_2	\overline{Ef}_1	AT_0	\overline{L}_2	L_1	A_0	P_2	Q_1	\overline{MM}_0	Fe_2	Ef_1	FD_0	\overline{F}_2
F_1	\overline{Ef}_2	MM_1	\overline{Fe}_0	L_2	AT_1	\overline{L}_0	Q_2	A_1	P_0	Ef_2	\overline{MM}_1	Fe_0	\overline{F}_2	FD_1
F_2	\overline{Fe}_1	\overline{Ef}_0	MM_2	\overline{L}_1	L_0	AT_2	P_1	Q_0	A_2	Fe_1	Ef_0	\overline{MM}_2	\overline{F}_1	\overline{F}_0
\overline{F}_0	\overline{MM}_0	Fe_2	Ef_1	A_0	P_2	Q_1	AT_0	\overline{L}_2	L_1	MM_0	\overline{Fe}_2	\overline{Ef}_1	\overline{FD}_0	F_2
\overline{F}_1	Ef_2	\overline{MM}_1	Fe_0	Q_2	A_1	P_0	L_2	AT_1	\overline{L}_0	\overline{Ef}_2	MM_1	\overline{Fe}_0	F_2	\overline{FD}_1
\overline{F}_2	Fe_1	Ef_0	\overline{MM}_2	P_1	Q_0	A_2	\overline{L}_1	L_0	AT_2	\overline{Fe}_1	\overline{Ef}_0	MM_2	F_1	F_0
\star	F_0	F_1	F_2	\overline{F}_0	\overline{F}_1	\overline{F}_2								
F_0	F'_0	MM'_2	MM'_1	D'_0	D_2	D_1								
F_1	MM'_2	F'_1	MM'_0	D_2	D'_1	D_0								
F_2	MM'_1	MM'_0	F'_2	D_1	D_0	D'_2								
\overline{F}_0	D'_0	D_2	D_1	F'_0	MM'_2	MM'_1								
\overline{F}_1	D_2	D'_1	D_0	MM'_2	F'_1	MM'_0								
\overline{F}_2	D_1	D_0	D'_2	MM'_1	MM'_0	F'_2								

Proof:

α_0	$D9(C_0$	D_0	\overline{MM}_0	MM_1	\overline{MM}_2	AT_1	;	AT_0	MM_0	$AT_2)$
$\rho\alpha_0$	$D9(E_2$	F_2	MM_2	AT_0	MM_1	\overline{MM}_0	;	\overline{MM}_2	AT_2	$\overline{MM}_1)$
$\rho^2\alpha_0$	$C9(E_1$	\overline{F}_1	AT_1	\overline{MM}_2	AT_0	MM_2	;	MM_1	\overline{MM}_1	$MM_0)$
α_1	$C9(E_1$	A_2	\overline{MM}_0	AT_1	AT_2	MM_0	;	AT_0	\overline{MM}_1	$MM_2)$
$\beta\alpha_1$	$C9(F_2$	\overline{F}_1	AT_1	\overline{MM}_0	MM_0	AT_2	;	D_0	\overline{MM}_1	$MM_2)$
$\sigma\beta\alpha_1$	$C9(\overline{F}_2$	F_1	AT_1	MM_0	\overline{MM}_0	AT_2	;	D_0	MM_1	$\overline{MM}_2)$
α_2	$C9(C_1$	D_2	MM_2	F_2	MM_1	AT_0	;	L_0	\overline{MM}_2	$AT_2)$
$\sigma\alpha_2$	$C9(C_1$	D_2	\overline{MM}_2	\overline{F}_2	\overline{MM}_1	AT_0	;	L_0	MM_2	$AT_2)$
$021021\alpha_2$	$C9(C_2$	D_1	\overline{MM}_1	\overline{F}_1	\overline{MM}_2	AT_0	;	\overline{L}_0	MM_1	$AT_1)$
$\sigma 021021\alpha_2$	$C9(C_2$	D_1	MM_1	F_1	MM_2	AT_0	;	\overline{L}_0	\overline{MM}_1	$AT_1)$
α_3	$C9(C_0$	F_0	AT_0	AT_1	\overline{MM}_2	AT_1	;	MM_0	MM_0	$AT_2)$
$\sigma\alpha_3$	$C9(C_0$	\overline{F}_0	AT_0	AT_1	MM_2	AT_1	;	\overline{MM}_0	\overline{MM}_0	$AT_2)$
$021021\alpha_3$	$C9(C_0$	\overline{F}_0	AT_0	AT_2	MM_1	AT_2	;	\overline{MM}_0	\overline{MM}_0	$AT_1)$
$\sigma 021021\alpha_3$	$C9(C_0$	F_0	AT_0	AT_2	\overline{MM}_1	AT_2	;	MM_0	MM_0	$AT_1)$
α_4	$C9(D_0$	A_0	MM_1	A_2	AT_1	\overline{MM}_0	;	A_0	MM_2	$MM_0)$
$021021\alpha_4$	$C9(D_0$	A_0	\overline{MM}_2	A_1	AT_2	MM_0	;	A_0	\overline{MM}_1	$\overline{MM}_0)$
α_5	$C9(E_0$	F_0	MM_0	A_2	\overline{MM}_1	MM_2	;	\overline{MM}_0	AT_0	$MM_1)$
$\sigma\alpha_5$	$C9(E_0$	\overline{F}_0	\overline{MM}_0	A_2	MM_1	\overline{MM}_2	;	MM_0	AT_0	$\overline{MM}_1)$
$021021\alpha_5$	$C9(E_0$	\overline{F}_0	\overline{MM}_0	A_1	MM_2	\overline{MM}_1	;	MM_0	AT_0	$\overline{MM}_2)$
$\sigma 021021\alpha_5$	$C9(E_0$	F_0	MM_0	A_1	\overline{MM}_2	MM_1	;	\overline{MM}_0	AT_0	$MM_2)$
α_6	$C9(E_1$	\overline{F}_2	AT_2	F_2	AT_1	MM_0	;	$E\overline{f}_0$	\overline{MM}_2	$MM_2)$
$\sigma\alpha_6$	$C9(E_1$	F_2	AT_2	\overline{F}_2	AT_1	\overline{MM}_0	;	Ef_0	MM_2	$\overline{MM}_2)$
α_7	$C9(F_1$	A_2	\overline{MM}_1	\overline{F}_1	AT_2	MM_1	;	Fe_0	\overline{MM}_0	$AT_1)$
$\sigma\alpha_7$	$C9(\overline{F}_1$	A_2	MM_1	F_1	AT_2	\overline{MM}_1	;	\overline{Fe}_0	MM_0	$AT_1)$
$\sigma\alpha_8$	$C9(C_0$	A_0	\overline{MM}_1	MM_0	MM_0	AT_1	;	A'_0	\overline{MM}_2	$AT_2)$
α'_8	$C9(MM_0$	MM_0	\overline{MM}_1	\overline{MM}_0	\overline{MM}_0	MM_1	;	A'_0	AT_2	$A_1)$
$012210\alpha_8$	$C9(F_1$	F_2	AT_2	\overline{MM}_0	\overline{MM}_0	AT_1	;	A'_0	MM_2	$MM_1)$
$\sigma\alpha_8$	$C9(\overline{F}_1$	\overline{F}_2	AT_2	MM_0	MM_0	AT_1	;	A'_0	\overline{MM}_2	$\overline{MM}_1)$
$210102\alpha_8$	$C9(E_0$	A_0	MM_2	AT_0	AT_0	\overline{MM}_2	;	AB'_0	MM_1	$\overline{MM}_1)$
$120102\alpha_8$	$C9(D_2$	D_1	MM_2	AT_0	AT_0	MM_1	;	AB'_0	\overline{MM}_2	$\overline{MM}_1)$
$210012\alpha_9$	$C9(D_1$	\overline{MM}_2	AT_1	F_1	AT_2	\overline{MM}_1	;	\overline{Fe}_0	MM_0	$MM_1)$
$\sigma 210012\alpha_9$	$C9(D_1$	MM_2	AT_1	\overline{F}_1	AT_2	MM_1	;	Fe_0	\overline{MM}_0	$\overline{MM}_1)$
$012102\alpha_9$	$C9(F_2$	AT_1	\overline{MM}_2	D_2	\overline{MM}_1	AT_2	;	$E\overline{f}_0$	MM_0	$MM_2)$
$\sigma 012102\alpha_9$	$C9(\overline{F}_2$	AT_1	MM_2	D_2	MM_1	AT_2	;	Ef_0	\overline{MM}_0	$\overline{MM}_2)$
$120201\alpha_9$	$C9(E_1$	AT_2	MM_1	A_2	AT_1	MM_2	;	A_0	\overline{MM}_0	$MM_0)$
α_{10}	$C9(AT_0$	A_0	MM_2	D_2	A'_1	MM_1	;	M_0	MM_1	$\overline{MM}_2)$
α_{11}	$C9(AT_2$	D_1	\overline{MM}_1	A'_1	A_2	MM_0	;	L_0	MM_1	$\overline{MM}_1)$
$? \alpha_{11}$	$C9(AT_1$	D_2	\overline{MM}_2	A'_2	A_1	MM_0	;	\overline{L}_0	MM_2	$\overline{MM}_2)$
α_{12}	$C9(F_1$	\overline{MM}_2	\overline{MM}_0	MM_2	\overline{F}_1	MM_1	;	P_0	A_1	$AT_1)$
$? \alpha_{12}$	$C9(F_2$	\overline{MM}_1	\overline{MM}_0	MM_1	\overline{F}_2	MM_2	;	Q_0	A_2	$AT_2)$
α_{13}	$C9(C_0$	AT_0	AT_0	AT_1	L_2	AT_1	;	C'_0	D_0	$AT_2)$
$? \alpha_{13}$	$C9(C_0$	AT_0	AT_0	AT_2	\overline{L}_1	AT_2	;	C'_0	D_0	$AT_1)$
α_{14}	$C9(F_0$	F_0	\overline{MM}_0	\overline{F}_0	\overline{F}_0	MM_0	;	F'_0	A_0	$AT_0)$
α_{15}	$C9(MM_0$	AT_0	A_0	A_0	\overline{MM}_0	\overline{MM}_0	;	F_0	A'_0	$D_0)$
$? \alpha_{15}$	$C9(\overline{MM}_0$	AT_0	A_0	A_0	MM_0	MM_0	;	ovF_0	A'_0	$D_0)$
α_{16}	$C9(AT_0$	AT_0	AT_1	L_2	Cc_1	AT_0	;	AB'_0	AT_2	$D_0)$
$? \alpha_{16}$	$C9(AT_0$	AT_0	AT_2	\overline{L}_1	Cc_2	AT_0	;	AB'_0	AT_1	$D_0)$
α_{17}	$C9(AT_0$	AT_0	AT_1	Cc_0	AT_0	AT_1	;	AB'_0	AT_2	$AT_2)$
α_{18}	$C9(C_1$	AT_2	AT_2	L_0	\overline{L}_0	AT_1	;	Cc_0	D_2	$D_1)$
α_{19}	$C9(F_0$	F_0	D_1	\overline{L}_2	P_1	MM_0	;	F'_0	\overline{F}_2	$AT_0)$
α_{20}	$C9(D_0$	F_0	A_0	\overline{F}_0	A'_0	\overline{MM}_0	;	DF_0	\overline{MM}_0	$MM_0)$
$? \alpha_{20}$	$C9(D_0$	\overline{F}_0	A_0	F_0	A'_0	MM_0	;	$D\overline{F}_0$	MM_0	$\overline{MM}_0)$

α_{21}	$C9(F_1$	AT_2	AT_1	\overline{F}_1	A_2	A_1	;	Fc_0	AT_0	\overline{MM}_1)
$?\alpha_{21}$	$C9(\overline{F}_1$	AT_2	AT_1	F_1	A_2	A_1	;	$\overline{F}c_0$	AT_0	MM_1)
α_{22}	$C9(C_1$	F_2	A_2	M_2	MM_1	AT_0	;	MM_0	\overline{MM}_2	AT_2)
$?\alpha_{22}$	$C9(C_1$	\overline{F}_2	A_2	M_2	\overline{MM}_1	AT_0	;	\overline{MM}_0	MM_2	AT_2)
α_{23}	$C9(F_0$	F_0	D_2	L_1	Q_2	MM_0	;	F'_0	\overline{F}_1	AT_0)
$?\alpha_{23}$	$C9(F_0$	F_0	D_1	\overline{L}_2	P_1	MM_0	;	F'_0	\overline{F}_2	AT_0)
α_{24}	$C9(D_0$	D_0	AT_0	F_0	\overline{F}_0	\overline{MM}_0	;	D'_0	AT_0	MM_0)
$?\alpha_{24}$	$C9(D_0$	D_0	AT_0	ovF_0	F_0	MM_0	;	D'_0	AT_0	MM_0)
α_{25}	$C9(E_1$	D_2	\overline{MM}_2	\overline{MM}_1	F_2	AT_2	;	Ed_0	MM_2	A_0)
$?\alpha_{25}$	$C9(E_2$	D_1	\overline{MM}_1	\overline{MM}_2	F_1	AT_1	;	A_0	MM_1	A_0)
α_{26}	$C9(C_0$	F_0	MM_0	\overline{MM}_0	AB'_0	AT_0	;	MM_0	AT_0	D_0)
$?\alpha_{26}$	$C9(C_0$	\overline{F}_0	\overline{MM}_0	MM_0	AB'_0	AT_0	;	\overline{MM}_0	AT_0	D_0)
α_{27}	$C9(F_0$	\overline{F}_0	\overline{MM}_0	D_0	AB'_0	AT_0	;	FF_0	AT_0	MM_0)

Exercise.

Study the Grassmannian cubic when the 6 lines are mm_i and \overline{mm}_i .

3.2.12 Answer to 3.2.11.

Definition.

In involutive geometry I will give the name of Grassmannian cubic to the special case where the 6 lines are mm_i and $\bar{m}m_i$.

Theorem.

The correspondence between the elements as given above and those of involutive geometry is as follows

A_i	B_i	E_i	AB_i	$C_i = Cc_i$				
M_i	\bar{M}_i	EUL_i	D_i	$Aeul_i$				
a_i	b_i	aB_i	$a\bar{B}_i$	ab_i	e_i	ae_i	be_i	ba_i
mm_i	$\bar{m}m_i$	c_i	\bar{c}_i	a_i	$aeUL_i$	nm_i	$\bar{n}m_i$	eul

Theorem.

0. The Grassmann cubic passes through the points $M_i, \bar{M}_i, EUL_i, D_i$.

1. Its equation is ?

$$\begin{aligned}
 &g_0X_0(-X_0 + X_1 + X_2)(-m_1m_2X_0 + m_2m_0X_1 + m_0m_1X_2) + g_1X_1(X_0 - X_1 + X_2)(m_1m_2X_0 - m_2m_0X_1 + m_0m_1X_2) \\
 &+ g_2X_2(X_0 + X_1 - X_2)(m_1m_2X_0 + m_2m_0X_1 - m_0m_1X_2) = 8m_0m_1m_2(m_2X_0 + m_0X_1 - m_0X_2)(-m_1X_0 + m_0X_1 + m_1X_2)(m_2X_0 - m_2X_1 + m_1X_2) \\
 &\text{where}
 \end{aligned}$$

$$g_0 = (m_1 - m_2)(s_{21} - 2m_0(m_1^2 + m_2^2 - m_1m_2)), \dots$$

Proof: Using 3.2.9 on the points M_i and \bar{M}_i , we obtain the given form, to determine g_i we impose the condition that the cubic passes through EUL_i , with $EUL_0 = (-m_0(m_1 - m_2), m_1(m_2 - m_0), m_2(m_0 - m_1))$, this gives the system of equations

$$4m_1m_2(m_0 - m_1)s_1 + 4m_1m_2(m_2 - m_0)s_2 = (m_0 - m_1)(m_2 - m_0)(m_1 + m_2)^2,$$

$$4m_2m_0(m_0 - m_1)s_0 + 4m_2m_0(m_1 - m_2)s_2 = (m_1 - m_2)(m_0 - m_1)(m_2 + m_0)^2,$$

$$4m_0m_1(m_2 - m_0)s_0 + 4m_0m_1(m_1 - m_2)s_1 = (m_2 - m_0)(m_1 - m_2)(m_0 + m_1)^2,$$

the s_i are proportional to $(m_1 - m_2)(s_{21} - 2m_0(m_1^2 + m_2^2 - m_1m_2))$ and the constant of proportionality is easily determined by substitution into one of the equations.

Verify that $(0, m_0 - m_1, -(m_2 - m_0))$ is on the cubic.

3.2.13 The cubics of Tucker.

Lemma.

0. $m_2(m_0 - m_1)q_1 + m_1(m_2 - m_0)q_2 = (m_1^2 - m_2^2)q_0.$
1. $m_0(m_1 - m_2)q_1q_2 + m_1(m_2 - m_0)q_2q_0 + m_2(m_0 - m_1)q_0q_1$
 $= -s_1s_{11}(m_1 - m_2)(m_2 - m_0)(m_0 - m_1).$
2. $m_1m_2(m_2 - m_0)(m_0 - m_1)q_0 + m_2m_0(m_0 - m_1)(m_1 - m_2)q_1$
 $+ m_0m_1(m_1 - m_2)(m_2 - m_0)q_2 = -(q_0q_1q_2)^2.$

Definition.

Let A_i and Q be a complete quadrilateral, the family of cubics associated to A_i and Q are the cubics through A_i , Q_i and tangent at A_i to aq_i , with q , the polar of Q with respect to $\{A_i\}$,
 $Q_i := a_i \times q$, $aq_i := A_i \times Q_i$.

Theorem.

If $Q = (T_0, T_1, T_2)$, the Tucker family of cubics is
 $(T_0X_1X_2 + T_1X_2X_0 + T_2X_0X_1)(T_1T_2X_0 + T_2T_0X_1 + T_0T_1X_2)$
 $= kT_0T_1T_2X_0X_1X_2.$

Any point R distinct from A_i and Q is on one and only one of these cubics, noted $\text{Tucker}(Q)(R)$.

Theorem.

If $R = (R_0, R_1, R_2)$ is on $\text{Tucker}(M)$, so are
isobaric(R) or (R_0, R_1, R_2) , (R_2, R_0, R_1) , (R_1, R_2, R_0) ,
semi reciprocal(R) or (R_0, R_2, R_1) , (R_2, R_1, R_0) , (R_1, R_0, R_2) ,
reciprocal(R) or (R_1R_2, R_2R_0, R_0R_1) , (R_0R_1, R_1R_2, R_2R_0) , (R_2R_0, R_0R_1, R_1R_2) ,
iso reciprocal(R) or (R_1R_2, R_0R_1, R_2R_0) , (R_0R_1, R_2R_0, R_1R_2) , (R_2R_0, R_1R_2, R_0R_1) .

Theorem.

The following are special cases of Tucker cubics:

$k = 1/0$, for $R \cdot a_i = 0$, $\text{Tucker}(Q)(R) = a_0 \times a_1 \times a_2.$

$k = 0$, for $R \cdot m = 0$ or on $\text{conic}(Q) := \text{conic}(A_1, aq_1, A_2, aq_2, A_0)$,

where $aq_i := A_i \times Q_i$,

$\text{Tucker}(Q)(R) = \text{conic}(Q) \times m$. $k = 1$, for $R \cdot aq_i = 0$, $\text{Tucker}(Q)(R) = aq_0 \times aq_1 \times aq_2.$

$k = 9$, $\text{Tucker}(Q)(Q)$. Finally the constant k is the same for $\text{Tucker}(Q)(R)$ and for $\text{Tucker}(R)(Q)$.

¹Tucker, Messenger of Mathematics, Ser. 2, Vol. 17, 1887-1888, p. 103

Theorem.

0. $\text{conic}(K) = \theta$.
1. $\text{Tucker}(M)(\overline{M})$ is incident to $A_i, MA_i, \overline{M}, PO, P\overline{O}, MAI, P, \overline{P}, \text{Atm}_i$,
2. $\text{Tucker}(\overline{M})(M)$ is incident to $A_i, \overline{MA}_i, M, \overline{\text{Atm}}_i, \overline{Tmm}, Tmm, \overline{Tmm}$.
3. $\text{Tucker}(M)(K)$ is incident to $A_i, MA_i, K, Br1_i, B\overline{r}, B\overline{r}$
4. $\text{Tucker}(\overline{M})(K)$ is incident to $A_i, \overline{Im}_i, K, \overline{Br}1_i$.
5. $\text{Tucker}(\overline{M})(O)$ is incident to $A_i, MA_i, 0, LEM$,
6. $\text{Tucker}(M)(O)$ is incident to ...

Theorem.

In the finite case, there are $p+1$ such cubics, each has besides the 6 vertices A_i and Q_i of the complete quadrilateral, a number of points which is a multiple of 6 except when $k = \frac{1}{0}$ and 1, when it is $3(p-2)$, $k = 0$, when it is $2p-5 - \left(\frac{-3}{p}\right)$, $k = 9$ when it is $p-5 - \left(\frac{-3}{p}\right)$. $\left(\frac{-3}{p}\right)$ is the Jacobi symbol = 1 when $p \equiv 1 \pmod{6}$ and = -1 when $p \equiv 5 \pmod{6}$.

Construction of the cubic of $\text{Tucker}(M)(\overline{M})$ by the ruler only.

H0.0. A_i , See Fig. t and t'

H0.1. M, \overline{M} ,

D0.0 to .5, construct $a_i, ma_i, \overline{ma}_i, M_i, \overline{M}_i, mm_i, MA_i, mm_i, m_i$,

D1.2, D3.0, 3.1, D4.12 and D4.26 construct $Maa_i, \overline{Maa}_i, cc_i, \overline{cc}_i, MMb_i, MM\overline{b}_i, mn_i, m\overline{n}_i, PO, P\overline{O}$.

We then proceed as follows

D80.0. $Aa_i := \overline{M}, P\overline{O}, PO$,

D80.0. $aaA_i := A_{i+1} \times Aa_{i-1}, aa\overline{A}_i := A_{i-1} \times Aa_{i+1}$,

D80.0. $Ad_i := aaA_i \times aa\overline{A}_i$,

D80.0. $maaA_i := MA_{i+1} \times Aa_{i-1}, maa\overline{A}_i := MA_{i-1} \times Aa_{i+1}$,

D80.0. $Ab_i := maaA_i \times maa\overline{A}_i$,

D80.0. $aab_i := A_{i+1} \times Ab_{i-1}, aab\overline{b}_i := A_{i-1} \times Ab_{i+1}$,

D80.0. $Ac_i := aab_i \times aab\overline{b}_i$,

D80.1. $aaaa_i := Aa_{i+1} \times Aa_{i-1}, acac_i := Ac_{i+1} \times Ac_{i-1}$,

D80.1. $Ba_i := aaaa_i \times acac_i$,

D80.1. $aaac_i := Aa_{i+1} \times Ac_{i-1}, aaac\overline{c}_i := Aa_{i-1} \times Ac_{i+1}$,

D80.1. $Bc_i := aaac_i \times aaac\overline{c}_i$,

D80.1. $abA_i := A_{i+1} \times Ba_{i-1}, ab\overline{A}_i := A_{i-1} \times Ba_{i+1}$,

D80.1. $Bd_i := abA_i \times ab\overline{A}_i$,

$$D80.1. \text{ } mabA_i := MA_{i+1} \times Ba_{i-1}, \text{ } mab\bar{A}_i := MA_{i-1} \times Ba_{i+1},$$

$$D80.1. \text{ } Bb_i := mabA_i \times mab\bar{A}_i,$$

$$D80.2. \text{ } baba_i := Ba_{i+1} \times Ba_{i-1}, \text{ } bcbc_i := Bc_{i+1} \times Bc_{i-1},$$

$$D80.2. \text{ } Ca_i := baba_i \times bcbc_i,$$

$$D80.2. \text{ } babc_i := Ba_{i+1} \times Bc_{i-1}, \text{ } bab\bar{c}_i := Ba_{i-1} \times Bc_{i+1},$$

$$D80.2. \text{ } Cc_i := babc_i \times bab\bar{c}_i,$$

$$D80.2. \text{ } acA_i := A_{i+1} \times Ca_{i-1}, \text{ } ac\bar{A}_i := A_{i-1} \times Ca_{i+1},$$

$$D80.2. \text{ } Cd_i := acA_i \times ac\bar{A}_i,$$

$$D80.2. \text{ } macA_i := MA_{i+1} \times Ca_{i-1}, \text{ } mac\bar{A}_i := MA_{i-1} \times Ca_{i+1},$$

$$D80.2. \text{ } Cb_i := macA_i \times mac\bar{A}_i,$$

$$D80.3. \text{ } 'Tucker := cubic(A_i, mm_i, MA_1, MA_2, \bar{M}),$$

$$C80.0. \text{ } MA_0 \cdot 'Tucker = 0,$$

$$C80.0. \text{ } PO \cdot 'Tucker = 0, \text{ } P\bar{O} \cdot 'Tucker = 0,$$

$$C80.0. \text{ } \bar{i}OK \cdot 'Tucker = 0,$$

$$C80.0. \text{ } Ba_0 \cdot \bar{i}OK = 0,$$

$$C80.0. \text{ } (Ba_i \times Aa_i) \cdot 'Tucker = 0, \text{ at } Aa_i?$$

$$C80.0. \text{ } (Bb_i \times Ab_i) \cdot 'Tucker = 0, \text{ at } Ab_i?$$

$$C80.0. \text{ } (Bc_{i-1} \times Ad_i) \cdot 'Tucker = 0, \text{ at } Ad_i?$$

$$C80.0. \text{ } (Bd_{i+1} \times Ac_i) \cdot 'Tucker = 0, \text{ at } Ac_i?$$

$$C80.1. \text{ } Ab_i, Ac_i, Ad_i \cdot 'Tucker = 0,$$

$$C80.1. \text{ } Ba_i, Bb_i, Bc_i, Bd_i \cdot 'Tucker = 0,$$

$$C80.1. \text{ } Ca_i, Cb_i, Cc_i, Cd_i \cdot 'Tucker = 0, \text{ } C80.2. \text{ } Ad_i \cdot tmm_i = 0,$$

$$C80.2. \text{ } Ac_i \cdot mIA_i = 0,$$

$$C80.2. \text{ } Ab_i \cdot mAM_i = 0,$$

$$C80.2. \text{ } Ac_i \cdot (MA_i \times Ad_i) = 0,$$

$$C80.2. \text{ } Ba_i \cdot pOL_i = 0,$$

we can continue indefinitely.

The cubic of Tucker(M)(\bar{M}).

I have determined all the intersections of the following lines with the cubic of Tucker(M)(\bar{M}).

$$mm_i : A_i, A_i, MA_i,$$

$$a_i : A_{i+1}, A_{i-1}, MA_i,$$

$$ma_i : A_i, \bar{M}, MNa_i,$$

$$mn_i : A_i, P\bar{O}, MNa_{i+1},$$

$$m\bar{n}_i : A_i, PO, MNa_{i-1},$$

$$mIA_i : A_i, MAI, Atm_i,$$

$$cc_i : A_i, P, Atm_{i+1},$$

$$\bar{c}c_i : A_i, \bar{P}, Atm_{i+1},$$

$$m : MA_i,$$

$$maM_i : MA_i, \bar{M}, Atm_i,$$

$$aaM_i : MA_{i+1}, PO, Atm_{i-1},$$

$$aa\bar{M}_i : MA_{i-1}, P\bar{O}, Atm_{i+1},$$

$tmm_i : MA_i, \overline{P}, MNa_{i-1},$
 $tm\overline{m}_i : MA_i, \overline{P}, MNa_{i+1},$
 $mpo : \overline{M}, PO, PAM$
 $mp\overline{o} : \overline{M}, P\overline{O}, PAM$
 $\overline{i}POK : \overline{M}, MAI,$
 $: \overline{M}, P,$
 $: \overline{M}, \overline{P},$
 $pOL : PO, P\overline{O}, POL,$
 $: MA_i, MNA_i, MAI,$
 $pmai : P, MAI, PAM$
 $pma\overline{i} : \overline{P}, MAI, PAM$
 $pp : P, \overline{P}, POL,$

Notation.

The correspondance between the notation used here and that used in *EUC.* is as follows:

aaA_i	$aa\overline{A}_i$	$maaA_i$	$maa\overline{A}_i$
$m\overline{n}_1, \overline{m}a_2, mn_0$	$mn_2, m\overline{n}_0, \overline{m}a_1$	$aaM_0, maM_2, aa\overline{M}_1$	$aa\overline{M}_0, aaM_2, maM_1$

3.2.14 NOTES

Vigarié (Mathesis. Série 1, Vol. 9, 1889, Suppl. pp. 1-26 gives the distances to the sides $\delta_a, \delta_b, \delta_c$, the normal coordinates x, y, z which are proportional to these, and or the barycentric coordinates α, β, γ , which are proportional to ax, by, cz , where a, b, c are the lengths of the sides.

These are given in terms of a, b, c and the trigonometric functions of the angles of the triangle. To obtain our barycentric coordinates it is sufficient to replace in α, β and γ ,

a^2 by $m_0(m_1 + m_2),$	or a by $a_0 = j j_0(j_1 + j_2),$
b^2 by $m_1(m_2 + m_0),$	or b by $a_1 = j j_1(j_2 + j_0),$
c^2 by $m_2(m_0 + m_1),$	or c by $a_2 = j j_2(j_0 + j_1),$

and to replace the trigonometric functions as follows:

$\sin A$ by $sa_0,$	$\cos A$ by $c \frac{m_1+m_2}{a_0},$	$\tan A$ by $tm_0,$
$\sin B$ by $sa_1,$	$\cos B$ by $c \frac{m_2+m_0}{a_1},$	$\tan B$ by $tm_1,$
$\sin C$ by $sa_2,$	$\cos C$ by $c \frac{m_0+m_1}{a_2},$	$\tan C$ by $tm_2,$

where

$$\begin{aligned}
 p_{11} &= j_1 j_2 + j_2 j_0 + j_0 j_1, \\
 j^2 &= (p_{11} - j_0^2)(p_{11} - j_1^2)(p_{11} - j_2^2), \\
 s^2 &= \frac{m_0+m_1+m_2}{(m_1+m_2)(m_2+m_0)(m_0+m_1)} = p_{11} \left(\frac{2}{j(j_1+j_2)(j_2+j_0)(j_0+j_1)} \right)^2, \\
 c^2 &= \frac{m_0 m_1 m_2}{(m_1+m_2)(m_2+m_0)(m_0+m_1)}, \quad c = \frac{j}{(j_1+j_2)(j_2+j_0)(j_0+j_1)}, \\
 t &= \frac{s}{c}.
 \end{aligned}$$

(Vigarié's notation is here given between quotes.

Twice the area "2S" by $a_0 a_1 a_2 s$,

$$m_0 + m_1 + m_2 = 4j_0 j_1 j_2 p_{11},$$

$$m_0 m_1 m_2 = j_0 j_1 j_2 p^2,$$

$$("2S")^2 = m_0 m_1 m_2 (m_0 + m_1 + m_2) = (2j_0 j_1 j_2 j p)^2 p_{11},$$

the radius of the inscribed circle “ r ” by $r^2 = (j_0 j_1 j_2)^2 / p_{11}$.

Moreover

$$a + b + c = 2j p_{11},$$

$$b + c - a = j j_0(j_1 + j_2),$$

$$b^2 - c^2 = m_0(m_1 - m_2),$$

$$b + c = j(p_{11} + j_1 j_2),$$

$$b^2 + c^2 - a^2 = 2m_1 m_2.$$

The coordinates are given for the following points, I give first Vigarié’s notation and under

	G	K	H	O	H_o	Ω_1	Ω_2	I	I_a	I_b	I_c
	M	K	$\bar{\{M\}}$	O	MAI	Br	Br	I	I_0	I_1	I_2
	O_9	$I_c(\mathbf{26})$	ν	Γ	ν'_1	ν'_b	ν'_c	Γ'_a	Γ'_b	Γ'_c	
	EE	En	EE	N	J						
	I_o	32	J_δ	J_ρ	N	R	ρ	ρ'	V	W	
					Tar	Ste	$BR\bar{a}$	Bra			
it my notation.	V_2	W_2	P	P_2	D	D_2	Z	A_1	B_1	C_1	
			Tbb			Tnn	Bro	$Br1_0$	$Br1_1$	$Br1_2$	
	A_2	B_2	C_2	A_3	B_3	C_3					
	$Br3_0$	$Br3_1$	$Br3_2$				$Br2_0$	$Br2_1$	$Br2_2$		
	58	59	60	61	62	63	64	δ_0	δ	67	
	mm_i	$m m_i$	j_i	mf_i	\bar{m}	aia	at_i	lem	o	ok	
	68	69	Σ_1	Σ'_1	Σ''_1	Σ_2	IO	KH_o	HH_o		
	bbr	eul									

In our notation we have,

$$”D” = (m_1 m_2 (m_2 + m_0) (m_0 + m_1), \dots),$$

$$”I_0” = (j_1 j_2 (j_2 + j_0) (j_0 + j_1), \dots)$$

$$”J_\delta” = (j_0 j_1 (j_1 + j_2) (j_2 + j_0), j_1 j_2 (j_2 + j_0) (j_0 + j_1), j_2 j_0 (j_0 + j_1) (j_1 + j_2)),$$

$$”J_\rho” = (j_2 j_0 (j_0 + j_1) (j_1 + j_2), j_0 j_1 (j_1 + j_2) (j_2 + j_0), j_1 j_2 (j_2 + j_0) (j_0 + j_1)),$$

$$”P2” = \text{inverse}(”P”)$$

$$”P2” = ((s_{11} + m_2 m_0) (s_{11} + m_0 m_1), \dots)$$

$$”41” = (m_1 m_2 (m_2 + m_0) (m_0 + m_1), \dots).$$

The equations are given for the following lines, m_i , \bar{m}_i , $X_{i+1} \times X_{i-1}$, where $X_i = a_i \times ai_i$, \bar{m}_i , \bar{i} , $I_{i+1} \times I_{i-1}$, at_i , “65”, “66”, ok , “line of Brocard” := $Br1 \times Br2$, e , “70”, “71”, “72”.

The equations of the circles.

$\theta, \iota, \iota_i, \gamma$, “78”, polar circle : $m_1 m_2 X^2 + m_2 m_0 X^2 + m_0 m_1 X^2 = 0$, could only find the obvious I , and $I[i]$ on $(X_0 + X_1 + X_2)(m_0(m_1 + m_2)X_0 + m_1(m_2 + m_0)X_1 + m_2(m_0 + m_1)X_2) - m_0(m_1 + m_2)X_1 X_2 + m_1(m_2 + m_0)X_2 X_0 + m_2(m_0 + m_1)X_0 X_1 = 0$, $m_0(m_1 + m_2)X_0^2 + m_1(m_2 + m_0)X_1^2 + m_2(m_0 + m_1)X_2^2 + 2(m_1 m_2 X_1 X_2 + m_2 m_0 X_2 X_0 + m_0 m_1 X_0 X_1) = 0$ β , “81” family of Circles of Tucker “, λ_1 , λ_2 , “Circle of Taylor ‘Tay?’”, “Circles of Neuberg” (D35.4), “86” “Circles of M’Cay” “87”: “ $\alpha[i]$ ” “Circles of Apollonius”, “88”: family of “Circles of Schoute”,

The equations are given for other curves,

The conic of Brocard (D36.19), the conic of Lemoine (D36.7), also mentioned by Neuberg, *mémoire sur le tétraèdre*, p.5 VI,

$$iM := I \times M, \bar{i}M := \bar{I} \times \bar{M}$$

$$i'M := I' \times M, \bar{i}' := \bar{I}' \times \bar{M}$$

$$\dots^{-1} \cdot iM = \dots^{-1} \cdot i'M = \dots^{-1} \cdot \bar{i} = \dots^{-1} \cdot \bar{i}'M.$$

Hence the foci of \dots are M and K and

the cofoci of \dots are \bar{M} and K .

$$MK = (5s_{11} - 3m_1m_2, 5s_{11} - 3m_2m_0, 5s_{11} - 3m_0m_1),$$

$$\bar{M}K = (m_0(5s_1 - 3m_0), m_1(5s_1 - 3m_1), m_2(5s_1 - 3m_2)),$$

$$\dots^{-1} : (s_{11} + 3m_1m_2)x_1x_2 + (s_{11} + 3m_2m_0)x_2x_0 + (s_{11} + 3m_0m_1)x_0x_1 = 0.$$

$$\dots^{-1} : (5m_1m_2 - m_0^2 + m_1^2 + m_2^2)x_1x_2 + \dots = 0.$$

$$\text{points of contact}_0 = ((s_{11} + 3m_2m_0)(s_{11} + 3m_0m_1), \dots).$$

These are the feet of the symmedians of A_1MA_2 .

$$\text{points of contact}_0 = ((5m_2m_0 + m_0^2 - m_1^2 + m_2^2)(5m_0m_1 + m_0^2 + m_1^2 - m_2^2), \dots).$$

the conic K (D36.2),

the conic of Simmons (92),

the conic of Steiner (S36.3),

the "hyperbola" of Kiepert (D16.19),

the first parabolas of Artzt (D36.8),

The second parabolas of Artzt (96):

Artzt2:

The parabolas of Brocard (97):

Brocard1:

Brocard2:

$$\text{Focus}(\text{Kiepert2}).\text{theta} = 0.$$

The conic of Jerabek (99):

$$\text{Jerabek} = \text{inverse}(e)$$

$$\text{Jerabek: } m_0(m_1^2 - m_2^2)X_1X_2 + m_1(m_2^2 - m_0^2)X_2X_0 + m_2(m_0^2 - m_1^2)X_0X_1 = 0.$$

The conic centrally associated to a point (99'):

$$\text{conic}(X). \text{ Given } X = (X_0, X_1, X_2),$$

$$\text{Let } X_i := a_i \times (A_i \times X),$$

$$\text{conic}(X) := \text{conic}(X_i, \times \text{pole of } i),$$

$$\text{conic}(X): (-X_0 + X_1 + X_2)X_1^2X_2^2X_0^2 + \dots - 2(X_0^3X_1X_2X_1X_2 + \dots) = 0.$$

$$I := \text{conic}(I),$$

"I" no point on it The conic I (100):

$$\text{supplementary}(\theta) = I,$$

$$I: (j_1j_2)^3((j_0 + j_1)(j_2 + j_0))^2X_0^2 + \dots - 2((j_0(j_1 + j_2))^3j_1j_2(j_0 + j_1)(j_2 + j_0)X_1X_2 + \dots) = 0$$

or $(p_{11}^2 + p_1 p_{111})(X_0^2 + X_1^2 + X_2^2) - 2(j_0^2(j_1 + j_2)^2 X_1 X_2 + j_1^2(j_2 + j_0)^2 X_2 X_0 + j_2^2(j_0 + j_1)^2 X_0 X_1) = 0$
the conics of Simson (D16.18),

$$m_1 m_2 X_1 X_2 + m_2 m_0 X_2 X_0 + m_0 m_1 X_0 X_1 = 0 \text{ no point on it}$$

3.2.15 The cubic of 17 points.

Introduction.

The cubic of 17 points is defined without explicit reference by Vigarié. It can be defined as the cubic through the vertices of a triangle, its midpoints and the midpoints Mma_i between the vertices and the feet. The other 8 points are the barycenter, orthocenter, center of the outscribed circle, point of Lemoine, and the 4 centers of the tangent circles. Other points and tangent on it will also be given. In particular, \overline{KLL}_i , \overline{Flor} , \overline{ARTM} , are on the cubic and at_i is the tangent at A_i , mf_i is the tangent at M_i , mk is the tangent at M , ok is the tangent at K .

Definition.

The cubic of 17 points is defined by
"cubic17 := cubic(A_i, M_i, Mma_i).

Theorem.

$$O \cdot \text{"cubic17} = M \cdot \text{"cubic17} = \overline{M} \cdot \text{"cubic17} = K \cdot \text{"cubic17} \\ = I \cdot \text{"cubic17} = I_i \cdot \text{"cubic17} = 0.$$

$$\overline{KLL}_i \cdot \text{"cubic17} = 0.$$

$$\overline{ARTM} \cdot \text{"cubic17} = 0.$$

$$at_i \cdot \text{"cubic17} = 0,$$

Proof.

$$\text{"cubic17: } m_0(m_1 + m_2)X_1 X_2(X_1 - X_2) + m_1(m_2 + m_0)X_2 X_0(X_2 - X_0) \\ + m_2(m_0 + m_1)X_0 X_1(X_0 - X_1) = 0.$$

Theorem.

	M	\overline{M}	O	K	$Flor$	\overline{ARTM}	$C17a$	$C17b$	$C17c$	$C17d$
M	K	O	\overline{M}	M	\overline{ARTM}	$Flor$	$C17b$			
\overline{M}		$C17a$	M	\overline{ARTM}		K	\overline{M}			
O			$Flor$	K	O		$?$			
K				O		\overline{M}				
$Flor$	\overline{ARTM}	$?$	O	$?$	M					
\overline{ARTM}	$Flor$	K	$?$	\overline{M}	M					
$C17a$	$C17b$	\overline{M}	$?$					$?$		
$C17b$	$C17a$									
$C17c$	\overline{ARTM}	$C17d$	$?$	$?$	M	$?$	$?$			
	A_i	M_i	Mma_i	\overline{KLL}_i						
M	M_i	A_i	\overline{KLL}_i	Mma_i						
\overline{M}	Mma_i	$C17d_i$	A_i	$C17b_i$						
O	\overline{KLL}_i	M_i	$C17c_i$	A_i						
K	A_i	Mma_i	M_i	$C17d_i$						
$Flor$	$C17d_i$	$C17b_i$	Mma_i	$C17e_i$						
\overline{ARTM}	$C17c_i$	\overline{KLL}_i	$C17f_i$	M_i						
$C17a$	$C17f_i$	$C17c_i$	$?$	\overline{KLL}_i						
$C17b$	$C17b_i$	$C17e_i$	$C17d_i$	$C17g_i$						
$C17c$	$C17d_i$	$C17b_i$	$?$	$?$						
	A_i	M_i	Mma_i	\overline{KLL}_i						
A_i	K	M	\overline{M}	O						
M_i	M	O	K	\overline{ARTM}						
Mma_i	\overline{M}	K	$C17c_i$	M						
\overline{KLL}_i	O	\overline{ARTM}	M	$C17a$						
	A_{i-1}	M_{i-1}	Mma_{i-1}	\overline{KLL}_{i-1}						
A_{i+1}	M_i	A_i	\overline{KLL}_i	Mma_i						
M_{i+1}	A_i	Mma_i	M_i	$C17d_i$						
Mma_{i+1}	\overline{KLL}_i	M_i	$C17c_i$	A_i						
\overline{KLL}_{i+1}	Mma_i	$C17d_i$	$C17b_i$	M_i						

Exercise.

Construct the tangents to "cubic17 at Mma_i and at \overline{M} .

Exercise.

Give properties of "cubic17 := cubic($A_i, \overline{M}_i, \overline{M}ma_i$).

Partial answer to 3.2.14

The tangent at Mma_0 is

$$[(m1 - m2)(s1 - 2m0), (m1 + m2)(s1 - 2m1), -(m1 + m2)(s1 - 2m2)].$$

The tangent at \overline{M} is

$$[m_1m_2(m_1 - m_2)(s_1 - 2m_0), m_2m_0(m_2 - m_0)(s_1 - 2m_1), \\ m_0m_1(m_0 - m_1)(s_1 - 2m_2)].$$

$$A_0 \oplus A_0 = K, A_1 \oplus A_2 = M_0, A_0 \oplus M_0 = M, A_0 \oplus Mma_0 = \overline{M}, A_1 \oplus Mma_2 = \overline{K}LL_0,$$

$$A_0 \oplus \overline{K}LL_0 = O, M_0 \oplus M_0 = K, M_1 \oplus M_2 = Mma_0,$$

$$M_0 \oplus \overline{K}LL_0 = \overline{ARTM}, M_1 \oplus \overline{K}LL_2 = C17a_0,$$

$O \oplus O = \text{Flor}$, where

$$\text{Flor} = ((m_1 + m_2)(s_1 - 2m_1)(s_1 - 2m_2), (m_2 + m_0)(s_1 - 2m_2)(s_1 - 2m_0), \\ (m_0 + m_1)(s_1 - 2m_0)(s_1 - 2m_1)),$$

tangent at \overline{M} is $[m_1m_2(m_1 - m_2)(s_1 - 2m_0), \dots]$.

$$\overline{M} \times \overline{M} = (m_0(m_1 + m_2)(s_1 - 2m_1)(s_1 - 2m_2)(s_2 - 2m_0^2), \dots),$$

$$M \times \text{Flor} = [(m_1 - m_2)(s_1 - 2m_0), (m_2 - m_0)(s_1 - 2m_1), (m_0 - m_1)(s_1 - 2m_2)],$$

$$\overline{M} \times \overline{ARTM} = [(m_1 - m_2)(s_1 - 2m_0)(s_2 - 2m_0^2), \dots],$$

$$\overline{M} \oplus \overline{ARTM} = K,$$

$$K \times \text{Flor} = [(m_1 - m_2)(m_2 + m_0)(m_0 + m_1)(s_1 - 2m_0)^2, \dots],$$

$$C17a = (m_0(m_1 + m_2)(s_1 - 2m_1)(s_1 - 2m_2)(s_2 - 2m_0^2), \dots), C17b = ((s_1 - 2m_0)(s_2 - 2m_1^2)(s_2 - 2m_2^2), \dots),$$

$$C17c = ((m_1 + m_2)(s_1 - 2m_1)(s_1 - 2m_2), \dots),$$

$$C17d = ((s_2 - 2m_1^2)(s_2 - 2m_2^2)(s_3 - s_{21} - 2s_2m_0), \dots),$$

$$C17b_0 = (2m_0(m_1 + m_2)(s_1 - 2m_1)(s_1 - 2m_2), s_1(s_1 - 2m_1)(s_2 - 2m_2^2), \\ s_1(s_1 - 2m_2)(s_2 - 2m_1^2)),$$

$$C17c_0 = ((m_1 + m_2)(s_1 - 2m_1)(s_1 - 2m_2), m_1s_1(s_1 - 2m_1), m_2s_1(s_1 - 2m_2)),$$

$$C17d_0 = (m_0s_1, (m_2 + m_0)(s_1 - 2m_2), (m_0 + m_1)(s_1 - 2m_1)),$$

$$C17e_0 = ((s_2 - 2m_1^2)(s_2 - 2m_2^2)(s_3 - s_{21} - 2s_{111}),$$

$$-2m_1(m_2 + m_0)(s_2 - 2m_1^2)(s_3 - 2m_2^3 - s_{21} + 2m_2(m_0^2 + m_1^2) + 2s_{111}), -2m_2(m_0 + m_1)(s_2 - 2m_2^2)(s_3 - 2m_1^3 - s_{21} + 2m_1(m_2^2 + m_0^2) + 2s_{111})),$$

$$C17f_0 = (s_1(s_2 - 2m_2^2)(s_2 - 2m_1^2), 2m_1(m_2 + m_0)(s_1 - 2m_2)(s_2 - 2m_1^2), \\ -2m_2(m_0 + m_1)(s_1 - 2m_1)(s_2 - 2m_2^2)),$$

$$C17g_0 = ((m_1 + m_2)s_1(s_1 - 2m_0)(s_1 - 2m_1)(s_1 - 2m_2)(s_3 - s_{21} + 2s_{111} + 2m_2(s_2 - 2m_2^2))((s_3 - s_{21} + 2s_{111} + 2m_1(s_2 - 2m_2^2))), -m_1(s_3 - s_{21} - 2s_{111})(s_3 - s_{21} + 2s_{111} + 2m_1(s_2 - 2m_1^2))(s_4 + 2s_{22} - 4(m_2^4 + m_0^2m_1^2)), -m_2(s_3 - s_{21} - 2s_{111})(s_3 - s_{21} + 2s_{111} + 2m_2(s_2 - 2m_2^2))(s_4 + 2s_{22} - 4(m_1^4 + m_2^2m_0^2))),$$

Answer to

3.2.14

$$\overline{O} \cdot {}^{\overline{\cdot}} \text{cubic17} = M \cdot {}^{\overline{\cdot}} \text{cubic17} = \overline{M} \cdot {}^{\overline{\cdot}} \text{cubic17} = K \cdot {}^{\overline{\cdot}} \text{cubic17} = 0.$$

$$KLL_i \cdot {}^{\overline{\cdot}} \text{cubic17} = 0.$$

$$at_i \cdot {}^{\overline{\cdot}} \text{cubic17} = 0,$$

${}^{\overline{\cdot}} \text{cubic17}$:

$$m_0^2(m_1 + m_2) X_1X_2 (m_2X_1 - m_1X_2) + m_1^2(m_2 + m_0) X_2X_0 (m_0X_2 - m_2X_0) \\ + m_2^2(m_0 + m_1) X_0X_1 (m_1X_0 - m_0X_1) = 0.$$

3.2.16 The cubic of 21 points.*cubic21***3.2.17 The Barbilian Cubics.****Introduction.**

In posthumously published works of Dan Barbilian, also known in his native Roumanian Country as the poet Eon Barbu, the following Theorem is proven. The loci of the pseudo centers of the isotropic cubics which pass through the vertices of a complete quadrilateral and 2 of its diagonal elements is a circle. I observed that in the case where the isotropic points are the fixed points of the involution determined by the 3 pairs of opposite sides of the quadrilateral, the third diagonal point is also on the cubics. It is this family of cubics which will be studied now, to which I will give the name of the Poet-Mathematician Barbilian.

Definition.

An isotropic cubic is a cubic which passes through the isotropic points.

The pseudo center of an isotropic cubic is the intersection of its tangents at the isotropic points.²

Theorem. [Barbilian]

The family of isotropic cubic through the vertices B_j of a complete quadrangle and 2 of its diagonal points $A_1 := (B_0 \times B_2) \times (B_1 \times B_3)$ and $A_2 := (B_0 \times B_1) \times (B_2 \times B_3)$ has a circle as the locus of the pseudo centers. This circle is the Miquel circle of the complete quadrangle and the 2 diagonal points.

I remind the reader that this circle passes through the center of the circumcircles of the triangles $\{B_0, B_1, A_1\}$, $\{B_2, B_3, A_1\}$, $\{B_0, B_2, A_2\}$, $\{B_1, B_3, A_2\}$. See g334

Definition.

The isotropic cubics through the vertices of a triangle, the feet and the orthocenter will be called Barbilian cubics.

Corollary.

The family of Barbilian cubics has a circle as the locus of its pseudo centers.

In this case, $B_0 = A_0$, $B_1 = \overline{M}_1$, $B_2 = \overline{M}_2$, $B_3 = \overline{M}$ and the circles circumscribed to $\{B_2, B_3, A_1\}$, $\{B_1, B_3, A_2\}$ pass through the point of Miquel, \overline{M}_0 .

²The isotropic points are also called circular points. Barbilian calls a pseudo center, a pseudo focus.

Theorem.

The Miquel circle of B_j , A_1 and A_2 is the circle of Brianchon-Poncelet.

Theorem.

The following are degenerate Barbilian cubics.

$$0. \text{ 'Aam}_0 \rtimes \overline{ma}_0, \text{ its equation is}$$

$$(m_1 + m_2) m_0 X_1 X_2 (m_2 X_1 - m_1 X_2) - m_1 m_1 X_2 X_0 (m_0 X_2 - m_2 X_0) \\ - m_2 m_2 X_0 X_1 (m_1 X_0 - m_0 X_1) = 0.$$

$$1. \text{ 'Mma}_0 \rtimes a_0, \text{ its equation is}$$

$$m_1 X_2 X_0 (m_0 X_2 - m_2 X_0) - m_2 X_0 X_1 (m_1 X_0 - m_0 X_1) = 0.$$

Proof: 0 and 1, follow from the definition of the circles 'Aam_i and 'Mma_i given in section D11.1 and .2.

Theorem.

0. The cubics through A_i , \overline{M}_i , \overline{M} , are

$$a_0 m_0 X_1 X_2 (m_2 X_1 - m_1 X_2) + a_1 m_1 X_2 X_0 (m_0 X_2 - m_2 X_0) \\ + a_2 m_2 X_0 X_1 (m_1 X_0 - m_0 X_1) = 0.$$

1. A necessary and condition for the cubics through A_i , \overline{M}_i , \overline{M} , to be Barbilian cubics, is

$$a_0 + a_1 + a_2 = 0.$$

Proof: It is easy to verify 0. For 1, any Barbilian cubic is a linear combination of the degenerate cubics given in the preceding Theorem and this satisfy the given condition.

More details on 3

Recall that the isotropic points are

$$(m_0(m_1 + m_2), -m_0 m_1 - j\tau, -m_2 m_0 + j\tau), \text{ with } j = \pm 1 \text{ and } \tau^2 = -m_0 m_1 m_2 s_1.$$

Theorem.

In homogeneous Cartesian coordinates (X, Y, Z) , with

$A_0 = (0, h, 1)$, $A_1 = (b, 0, 1)$, $A_2 = (c, 0, 1)$ and isotropic points $(\pm j, 1, 0)$, we have the following.

0. The coordinates of the sides, feet, orthocenter and altitudes are

$$a_0 = [0, 1, 0], a_1 = [h, c, -ch], a_2 = [h, b, -bh], \\ \overline{M}_0 = (0, 0, 1), \overline{M}_1 = (c(h^2 + bc), hc(c - b), h^2 + c^2), \overline{M}_2 = (b(h^2 + bc), hb(b -$$

$$c), h^2 + b^2),$$

$$\overline{M} = (0, bc, -h),$$

$$\overline{m}_0 = [1, 0, 0], \overline{m}_1 = [c, -h, -bc], \overline{m}_2 = [b, -h, -bc].$$

1. The circle through $A_1, A_2, \overline{M}_1, \overline{M}_2$ is
 $\alpha m_0 : X^2 + Y^2 + bcZ^2 - (b+c)ZX = 0.$
2. The circle through $A_0, \overline{M}, \overline{M}_1, \overline{M}_2$ is
 $\mu a_0 : h(X^2 + Y^2) - hbcZ^2 + (bc - h^2)XY = 0.$
3. The Barbilian cubics are
 $k\alpha m_0 \rtimes X + l\mu a_0 \rtimes Y = 0.$
4. The pseudo center is, with $d = k(b+c) + l(bc - h^2)$,
 $(kd, -lhd, 2(k^2 + l^2h^2)).$
5. This is a parametric equation of the circle of Brianchon-Poncelet:
 $2h(X^2 + Y^2) - (h^2 - bc)XY - h(b+c)ZX = 0.$
6. The transformation from barycentric to Cartesian coordinates is
 $\begin{pmatrix} 0 & b & c \\ h & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}$ and its inverse is $\frac{1}{h(c-b)} \begin{pmatrix} 0 & c-b & 0 \\ -h & -c & ch \\ h & b & -bh \end{pmatrix}$,
 where the barycentric coordinates of the orthocenter are given by
 $m_0 = \frac{bc(c-b)}{h^2+bc}, m_1 = -c, m_2 = b,$
 provided $h^2 = \frac{m_1 m_2 s_1}{m_0}.$
7. The barycentric coordinates of the pseudo center are easily derived using the value of h and of
 $m_0 d = k m_0 (m_2 - m_1) - l (s_{111} - m_1 m_2 s_1).$

The details of the proof is left to the reader.

Answer to 4

0, is straightforward.

For 1, αm_0 is $u[h, b, -hb] \rtimes [h, c, -hc] = v[c, -h, -bc] \rtimes [b, -h, -bc].$

With $j^2 = -1$, $u = (cj - h)(bj - h)$, $v = (hj + b)(hj + c) = -u.$

After dividing by $h^2 + bc$ we get the equation 1.

For 2, μa_0 is $u[h, b, -hb] \rtimes [c, -h, -bc] = v[h, c, -hc] \rtimes [b, -h, -bc].$

$u = (hj + c)(bj - h)$, $v = (hj + b)(cj - h) = u.$

After dividing by $c - b$ we get the equation 2.

For 4, the tangent at $(j, 1, 0)$, obtained by evaluating the first partial derivatives at that point, is

$$[-2k + 2lhj, 2kj + 2lh, k(b+c) + l(bc - h^2)].$$

The tangent at the other isotropic point is obtained by replacing j by $-j$.

Their intersection is 4, after dividing by $4j$. It is easy to verify that 5, is the equation of a circle through \overline{M}_i , and that the pseudo center is on it for all values of k and l .

For 5, the coordinates of vertices A_i give the coefficients of the matrix. The transform of (m_0, m_1, m_2) is $(m_1b + m_2c, hm_0, s_1)$. Comparing with $(0, bc, -h)$ gives 5. 6, is straightforward. For 7, we need to related the cubics in Cartesian and barycentric coordinates. If we use k' and l' for the barycentric case, comparison of the coefficients of $X_2^2X_0$ in baricentric coordiantes gives

$k'm_1^2m_0 = kc(2bc - bc - c^2) = kc^2(b - c)$, and $l'm_0m_1 = lh(hc^2 - hbc) = lh^2(c - b)$. Using proportionality we can therefore write 7.

The pseudo center will be $(0,0,1)$ if $d = 0$, this gives

$$k = h^2 - bc = \frac{m_1m_2(s_1+m_0)}{m_0}, l = m_2 - m_1.$$

Substituting, we get, after division by $m_1m_2m_0^{-1}$, $k' = s_1 + m_0$, $l' = (m_1 - m_2)s_1$, hence $a_0 = -(m_1 + m_2)(s_1 + m_0)$, $a_1 = (2m_1 - m_2)s_1 + m_0m_1$, $a_2 = (2m_2 - m_1)s_1 + m_0m_2$. To check this independently, we should verify that $M_0 \times I_0$ is tangent to the cubic for these values of k' and l' . $(0, 0, 1) \times (m_0(m_1 + m_2), -m_0m_1 - j\tau, -m_2m_0 + j\tau) = [m_0m_1 + j\tau, m_0(m_1 + m_2), 0]$.

Theorem.

Given an Barbilian cubic Γ , there exists a line l and a circumscribed conic ϕ such that

$$\Gamma = \theta \times l + m \times \phi.$$

More specifically, with l_0 arbitrary,

$$l = [l_0, l_0 - a_2, l_0 + a_1],$$

$$\phi = b_0m_0X_1X_2 + b_1m_1X_2X_0 + b_2m_2X_0X_1 = 0, \text{ with}$$

$$b_0 = -m_2a_1 + m_1a_2 - (m_1 + m_2)l_0, b_1 = -m_2a_1 - (m_2 + m_0)l_0, b_2 = m_1a_2 - (m_0 + m_1)l_0.$$

Proof: Identification of the coefficients of $X_1^2X_2$ and $X_2^2X_1$ gives

$$a_0m_2 = (m_1 + m_2)l_1 + b_0, -a_0m_1 = (m_1 + m_2)l_2 + b_0,$$

subtracting gives, $a_0 = l_1 - l_2$, and similarly $a_1 = l_2 - l_0$, and $a_2 = l_0 - l_1$.

By substitution, we obtain b_0 and similarly b_1 and b_2 , using $a_0 + a_1 + a_2 = 0$.

Definition.

l is called a *radical axis* of Γ , ϕ is called the *corresponding radical conic* of Γ .

θ could be replaced by an other circle.

Theorem.

0. The non trivial ideal point is (a_0, a_1, a_2) .

1. The tangent at the non trivial ideal point, or asymptote is

$$[m_0a_1a_2(m_2a_1 - m_1a_2), m_1a_2a_0(m_0a_2 - m_2a_0), m_2a_0a_1(m_1a_0 - m_0a_1)].$$

Proof: This follows from the fact that the non trivial ideal point is $m \times l$. The tangent is obtain by taking the partial derivatives respectively with respect to X_0 , X_1 and X_2 at (a_0, a_1, a_2) . The first one is

$$m_1a_1a_2(m_0a_2 - 2m_2a_0) - m_2a_1a_2(m_0a_1 - 2m_1a_0) = -m_0a_1a_2(m_2a_1 - m_1a_2).$$

Comment.

Special Barbilian cubics can be obtained by combining the equations of Theorem 3.2.17 For instance,

$\beta a0$ follows from adding the equations 0, for indices 0,1 and 2 respectively multiplied by m_0 , m_1 and m_2 .

$\beta a1$, by using on the equations 0, the multipliers m_1m_2 , m_2m_0 and m_0m_1 .

$\beta a2$, by using on the equations 1, equal multipliers.

Theorem.

The Barbilian cubic $\beta a0$:

$$m_0(m_1 - m_2)X_1X_2(m_2X_1 - m_1X_2) + m_1(m_2 - m_0)X_2X_0(m_0X_2 - m_2X_0) \\ + m_2(m_0 - m_1)X_0X_1(m_1X_0 - m_0X_1) = 0$$

has the following properties:

0. A radical axis is $-mai$, with $mai = [m_0, m_1, m_2]$.

1. The corresponding radical conic has the equation

$$m_0(m_1^2 + m_2^2)X_1X_2 + m_1(m_2^2 + m_0^2)X_2X_0 + m_2(m_0^2 + m_1^2)X_0X_1.$$

2. The non trivial ideal point is $MK = (m_1 - m_2, m_2 - m_0, m_0 - m_1)$.

3. The asymptote is

$$[m_0(m_2 - m_0)(m_0 - m_1)(s_2 - m_0s_1), m_1(m_0 - m_1)(m_1 - m_2)(s_2 - m_1s_1), m_2(m_1 - m_2)(m_2 - m_0)(s_2 - m_2s_1)].$$

4. The tangent at A_i is mka_i , with

$$mka_0 = [0, m_0 - m_1, -(m_2 - m_0)].$$

Theorem.

The Barbilian cubic $\beta a1$:

$$m_0^2(m_1 - m_2)X_1X_2(m_2X_1 - m_1X_2) + m_1^2(m_2 - m_0)X_2X_0(m_0X_2 - m_2X_0) \\ + m_2^2(m_0 - m_1)X_0X_1(m_1X_0 - m_0X_1) = 0$$

has the following properties:

0. A radical axis is $-\overline{m}$.

1. The corresponding radical conic is $2m_0m_1m_2\overline{\text{Steiner}}$, with

$$\overline{\text{Steiner}} = m_0X_1X_2 + m_1X_2X_0 + m_2X_0X_1 = 0,$$

2. The non trivial ideal point is EUL with

$$EUL = (m_0(m_1 - m_2), m_1(m_2 - m_0), m_2(m_0 - m_1)).$$

3. The asymptote is \overline{m} .

4. The tangent at A_i is mka_i , with

$$mka_0 = [0, m_0 - m_1, -(m_2 - m_0)].$$

Theorem.

The Barbilian cubic $\beta a2$:

$$m_0(s_1 - 3m_0)X_1X_2(m_2X_1 - m_1X_2) + m_1(s_1 - 3m_1)X_2X_0(m_0X_2 - m_2X_0) + m_2(s_1 - 3m_2)X_0X_1(m_1X_0 - m_0X_1) = 0$$

has the following properties:

0. A radical axis is eul with $eul = [m_1 - m_2, m_2 - m_0, m_0 - m_1]$.
1. The corresponding radical conic is

$$m_0^2(m_1 - m_2)X_1X_2 + m_1^2(m_2 - m_0)X_2X_0 + m_2^2(m_0 - m_1)X_0X_1 = 0,$$
2. The non trivial ideal point is I_{eul} , where $I_{eul} = (s_1 - 3m_0, s_1 - 3m_1, s_1 - 3m_2)$.
3. The asymptote is $Mkm \times I_{eul}$,

$$[m_0(m_1 - m_2)(s_1 - 3m_1)(s_1 - 3m_2), m_1(m_2 - m_0)(s_1 - 3m_2)(s_1 - 3m_0), m_2(m_0 - m_1)(s_1 - 3m_0)(s_1 - 3m_1)].$$
4. The tangent at A_i is

Several mappings are defined and these allow an algebraic definition of many of the points, these will be given here as theorems for the points already defined and as definition for the others.

reciprocal(X_0, X_1, X_2) := (X_1X_2, X_2X_0, X_0X_1),

reciprocal(x_0, x_1, x_2) := (x_1x_2, x_2x_0, x_0x_1),

inverse(X_0, X_1, X_2) := ($m_0(m_1 + m_2)X_1X_2, m_1(m_2 + m_0)X_2X_0, m_2(m_0 + m_1)X_0X_1$),

complementary(X_0, X_1, X_2) := ($X_1 + X_2, X_2 + X_0, X_0 + X_1$), [Nagel, 1885]

anticomplementary(X_0, X_1, X_2) := ($-X_0 + X_1 + X_2, X_0 - X_1 + X_2, X_0 + X_1 - X_2$), [inverse transformation of de Longchamps, 1886]

supplementary(X_0, X_1, X_2) := ...

algebraically associated(X_0, X_1, X_2) := (($-X_0, X_1, X_2$), ($X_0, -X_1, X_2$), ($X_0, X_1, -X_2$)),

Brocardian(X_0, X_1, X_2) := ((X_0X_1, X_1X_2, X_2X_0), (X_2X_0, X_0X_1, X_1X_2)),

isobaric(X_0, X_1, X_2) := ((X_2, X_0, X_1), (X_1, X_2, X_0)),

semi reciprocal(X_0, X_1, X_2) := ((X_0, X_2, X_1), (X_2, X_1, X_0), (X_1, X_0, X_2)),

associated(X_0, X_1, X_2) := ($X_1 - X_2, X_2 - X_0, X_0 - X_1$).

Theorem.

0. $K = inverse(M)$,
1. $O = inverse(\overline{M}) = complementary(\overline{M})$
2. $(Br2, Br2) = brocardian(K)$,
3. $I_i = algebraically\ associated(I)$,
4. $N = anticomplementary(I)$,
5. $J = reciprocal(N)$,

6. $N_i = \text{algebraically associated}(N)$,
7. $J_i = \text{reciprocal}(N_i)$.

Definition.

The following are the definition of other points.

0. $H_0 := \text{reciprocal}(\overline{M})$
1. $I_c := \text{complementary}(I)$,
2. $I_0 := \text{reciprocal}(I)$,
3. “Center of equal parallels” $:= \text{anticomplementary}(I_0)$,
4. $(\text{”}J_\delta\text{”}, \text{”}J_\rho\text{”}) := \text{Brocardian}(I)$.

Exercise.

Define in terms of the above functions as many points as you can in Theorem

Exercise.

Determine, for many of the points of Definition . . . a linear construction and determine their barycentric coordinates.

3.3 Finite Projective Geometry.

3.3.0 Introduction.

The Theorems given here are deduced from Theorems of Involution Geometry.

Theorem.

Given 6 points A_i and B_i , forming an hexagon inscribed to a conic α and outscribed to an other conic β . Let C be the point common to $A_i \times B_i$. Let T_i be the vertices of the tangents to α at A_i .

0. *The lines $B_i \times T_i$ have a point D in common.*
1. *The line $C \times D$ passes through the pole of with respect to the triangle $\{A_i\}$ of the Desargues line of the perspective triangles $\{T_i\}$ and $\{B_i\}$.*

The Theorem generalizes a Theorem of Kimberling 3.4.6 and 3.4.6 using 3.4.6.

Theorem.

Given the special Desargues configuration with the points A_i on the lines of the triangle $\{MM_0, MM_1, MM_2\}$ with center of perspectivity M . Let \overline{m} be an arbitrary line and \overline{MA}_i be its intersection with the side a_i of the triangle $\{A_0, A_1, A_2\}$, if TMa_i is the intersection of the line MM_{i+1} \overline{MA}_{i-1} and the line MM_{i-1} \overline{MA}_{i+1} , then the lines joining the points A_i to the TMa_i have a point $ARTM$ in common.

The Theorem generalizes a Theorem of Kimberling 3.4.3 assuming that the excenters are replaced by the vertices of the anti complimentary triangle and the direction of the altitudes are replaced by the intersections of the orthic line with the side of the triangle.

Definition.

The point $ARTM$ is called the *point of Luke*.

3.4 Finite Involutive Geometry.

3.4.0 Introduction.

I will now describe the Theorems of involutive Geometry in the traditional way, refering for to proofs of the corresponding sections of the hexal configuration.

Starting with affine geometry, we obtain an involutive geometry, if we choose among all the possible involutions on the ideal line, a particular one, called fundamental involution. We could also start directly from projective geometry and choose among all the possible involutions one involution on one of all the possible lines.

This involution can be given in many ways,

0. by 2 points, the fixed points of the involution,
1. by 2 pairs of corresponding points on a line,
2. by a polarity and a line which does not belong to its line conic,
3. by an hexal complete 5-angle, See II.3.

The definitions will be given in terms of the fundamental involution. Because this involution can be elliptic or hyperbolic, there are 2 distinct types of real involutive geometries, elliptic and hyperbolic. I will study them together and give theorems, in the hyperbolic case, which in some cases can be used as an alternate definition of the concepts. Such theorems will be noted with **(H. D.)**. When the additional notions of measure of distance and angles will have been introduced, the elliptic involutive geometry will become the Euclidean Geometry and the hyperbolic one, will be that of Minkowski. A third geometry which corresponds to the confluence of the 2 fixed points of the involution will be considered later, it is the parabolic (involutive) geometry which becomes the Galilean geometry.

Among the many ways of starting I will give one. It is a good Exercise to ask students to try other approaches.

I will choose one line m as the ideal line and a conic, given by 5 points (again an other set

of 5 elements can be chosen) as the defining circle. Mid points of the side of a triangle can be obtained by the construction of the pole of a line with respect to a triangle, see 3.1.1. Using the mid-points of the sides we can derive the barycenter.

For perpendicularity, we choose one of the point A on the conic, determine its tangent t_A , the parallel tangent t_B , by a construction which is the dual of that of finding the second point of intersection of a line with the conic, and the point of contact B . $A \times B$ is a diameter. Perpendicular directions are obtained as follows. If I_p is an ideal point, we determine the second intersection P of $A \times I_p$ with the conic, the perpendicular direction is then $(P \times B) \times m$. We can therefore construct the altitudes and therefore the orthocenter.

3.4.1 Fundamental involution, perpendicularity, circles.

Definition.

Starting with an affine geometry associated to p , a particular involution on the ideal line will be called the *fundamental involution*.

Definition.

If the fundamental involution is hyperbolic, its fixed points are called *isotropic points*, the other points on the ideal line will be called *ideal points* or *directions*. (In a hyperbolic involutive geometry, the isotropic points are no more called ideal points). The lines through the isotropic points, distinct from the ideal line, are called *isotropic lines*.

The lines which are neither ideal or isotropic are called *ordinary lines*, the points which are not ideal or isotropic points are called *ordinary points*, ordinary lines or points will abbreviated from now on by lines or points. On an ordinary line, there are p ordinary points and one ideal point.

Definition.

Corresponding pairs of points in the fundamental involution are called *perpendicular ideal points* or *perpendicular directions*. 2 lines whose ideal points are perpendicular directions are called *perpendicular lines*.

Some obvious results follow from these definitions and from those of the corresponding affine geometry. For instance:

Theorem.

All the lines perpendicular to a given line are parallel.

Definition.

If the involution defined by a conic on the ideal line is the same as the fundamental involution, the corresponding conic is called a *circle* and the corresponding polarity is called a *circularity*.

Theorem. (H. D)

In a hyperbolic involutive geometry, a necessary and sufficient condition for a conic to be a circle is that it passes through the isotropic points.

Definition.

The *center of a conic* is the pole of the ideal line in the corresponding polarity. (See II.2.3.0).

Theorem. (H. D)

In a hyperbolic geometry, the center of a circle is the intersection of its isotropic tangents.

Definition.

A *diameter of a conic* is a line passing through its center (See II.2.3.1).

Definition.

A *mediatrix of 2 points A and B* on a line l , which is not an isotropic line, is the line perpendicular to l through the mid-point of AB . (See II.6.2.6)

Example.

In the examples of involutive and Euclidean geometry, I will make one of 2 choices for the ideal line and for the defining circle.

0. In the first choice,

0.[1, 1, 1] is the ideal line, as in affine geometry.

1. $X0^2 + X1^2 + k X2^2 = 0$, $k \neq -\frac{1}{2}$, is the defining circle,
 $-(1 + 2k) N p$ for the elliptic case, $-(1 + 2k) R p$ for the hyperbolic case.

2. Let $\delta^2 := -1 - 2k$.

If $k \neq -1$, the isotropic points $(1, y, -1 - y)$ correspond to the roots y_1 and y_2 of

3. $(1 + k)y^2 + 2ky + (1 + k) = 0$.

or with

4. $k' = \frac{2k}{1+k}$,

to the roots of

5. $y^2 + k'y + 1 = 0$.

Therefore

$y_1 = \frac{-k+\delta}{1+k}$ and $y_2 = \frac{-k-\delta}{1+k}$.

If $k = -1$, the isotropic points are $(0,1,-1)$ and $(1,0,-1)$.

The polar of $(X0, X1, X2)$ is $[X0, X1, kX2]$,

The direction perpendicular to $(X0, X1, -X0 - X1)$ is

$(kX0 + (1 + k)X1, -(1 + k)x0 - kX1, X0 - X1)$.

If $k = -\frac{1}{2}$, the conic 0.1. is tangent to the ideal line.

1. In the second choice,
 - 0.[0, 0, 1] is the ideal line, as in Euclidean geometry.
 1. $kX0^2 + X1^2 = X2^2$, $k \neq 0$, the defining circle,
 - $-k \text{ N } p$ for the elliptic case,
 - $-k \text{ R } p$ for the hyperbolic case.
 - $\delta^2 := -k$.
 - If $k = 0$, the conic 1.1. is tangent to the ideal line.
 - The isotropic points are $(1, \delta, 0)$ and $(1, -\delta, 0)$.
 - The polar of $(X0, X1, X2)$ is $[kX0, X1, -X2]$.
 - The direction perpendicular to $(X0, X1, 0)$ is $(X1, -kX0, 0)$.

3.4.2 Altitudes and orthocenter.

Definition.

In a triangle $\{A_i\}$, the *altitude* \overline{ma}_i from A_i is the line through A_i which is perpendicular to the opposite side $a_i := A_{i+1} \times A_{i-1}$ (C0.1,N0.3).

Theorem.

The altitudes \overline{ma}_i of a triangle are concurrent at a point \overline{M} . (D0.12)

Definition.

The point \overline{M} is called the *orthocenter* of the triangle. (N0.2)

Theorem.

The necessary and sufficient condition for a triangle to be a right triangle at A_i is that its orthocenter \overline{M} coincides with A_i .

Theorem.

The necessary and sufficient condition for a triangle to be an isosceles triangle is that the orthocenter be on the altitude from A_i and distinct from the center of mass.

Theorem.

The necessary and sufficient condition for a triangle to be an equilateral triangle is that the orthocenter and the barycenter coincide.

3.4.3 The geometry of the triangle, I.

Introduction.

We are now ready to give a large number of results of finite involutive geometry associated to a scalene triangle whose vertices A_0, A_1, A_2 and whose sides a_0, a_1, a_2 are ordinary.

Theorem II.6.2.7. determines a point M , the center of mass, at the intersection of the *medians* A_0M_0 , A_1M_1 , A_2M_2 , the points M_i being the mid-points of pairs of vertices.

Theorem 3.1. determines a point \overline{M} , the orthocenter, at the intersection of the *altitudes* $A_0\overline{M}_0$, $A_1\overline{M}_1$, $A_2\overline{M}_2$, the points \overline{M}_i being the feet of the altitudes.

In a scalene triangle, M and \overline{M} are distinct, are distinct from the vertices and are not collinear with any of the vertices. A large number of results can therefore be obtained as direct consequences of rephrasing the results of Theorem 3.6. and 4.0.

Similar results can be obtain for right triangles, for isosceles triangle and for equilateral triangles. These will be left as exercises.

These results were in fact the starting point of our study of finite Euclidean geometry, as explained in section

All references will be to Theorems 3.6. and 4.0. unless explicitly indicated.

Definition.

The *ideal points* MA_i of a triangle are the ideal points on its sides.

The *orthic points* \overline{MA}_i of a triangle are the points on the corresponding sides a_i of the triangle and \overline{mm}_i of the orthic triangle (D0.13, N0.6). See Fig. 1.

Theorem.

The orthic points \overline{MA}_i are on the orthic line \overline{m} (D0.14*).

Definition.

The triangle M_i is called the *complementary triangle*. Its sides are denoted mm_i .

The triangle \overline{M}_i is called the *orthic triangle*. Its sides are denoted \overline{mm}_i (D0.18, N0.5).

Definition.

The *orthic line* \overline{m} of a triangle is the polar of its orthocenter with respect to the triangle (N0.8).

Its direction EUL is called the *orthic direction* (N1.1).

Definition.

The line $eul := M \times \overline{M}$ is called the *line of Euler* (D1.0, N1.0).

Theorem.

The mid-points M_i at the intersection of the medians ma_i with the sides a_i and the feet \overline{M}_i of the altitudes \overline{ma}_i are on a circle γ (D1.20, C1.4). See Fig. 2.

Definition.

The circle γ is called the *circle of Brianchon-Poncelet* (N1.11).

Theorem.

If Maa_i ($\overline{Maa_i}$) is the intersection of the median ma_{i+1} ($\overline{ma_{i-1}}$) with the altitude $\overline{ma_{i-1}}$ ($\overline{ma_{i+1}}$), then the lines mMa_i joining Maa_i and $\overline{Maa_i}$ have a point K in common (D1.2, D1.3, D1.4*). See Fig. 3.

Definition.

The point K is called the *point of Lemoine* (N1.2).

Definition.

The *circumcircle* θ of a triangle $\{A_0, A_1, A_2\}$ is the circle passing through the vertices of the triangle (D1.19, H1.1, N1.10).

Theorem.

The line ta_i through the vertex A_i parallel to the side $\overline{m_i}$ of the orthic triangle is the tangent at A_i to the circumcircle (D1.7, D1.19*). See Fig. 4.

Definition.

The triangle with sides ta_i is called the *tangential triangle*. Its vertices are denoted by T_i (D1.8, N1.5).

Definition.

The *mixed triangles* are the triangles with respective sides

$$c_i := M_{i+1} \times \overline{M}_{i-1} \text{ and } \overline{c}_i := \overline{M}_{i+1} \times M_{i-1} \text{ (D1.13, N1.6).}$$

The *mixed feet* are the points CC_i , (\overline{CC}_i) on the side of the given triangle and the corresponding side c_i , (\overline{c}_i) of the mixed triangle (D1.14, N1.7). See Fig. 5.

Theorem.

The mixed feet CC_i , (\overline{CC}_i) of a mixed triangle are collinear on the line p (\overline{p}) (D1.15*).

Definition.

The line p and \overline{p} are called the *mixed lines of a triangle* (N1.8).

Theorem.

The mixed lines p and \overline{p} of a triangle meet at the point PP which is on the line of Euler (D1.16, C1.0).

Definition.

PP is called the *mixed center of the triangle* (N1.9).

Definition.

The intersection $\bar{I}Ma_i$ of a median with the orthic line is called a *medorthic point* (D0.15, N0.9).

Definition.

The intersection of the lines $\bar{m}e_i$ (me_i) joining the medorthic points $\bar{I}Ma_{i+1}$ ($\bar{I}Ma_{i-1}$) to the foot \bar{M}_{i-1} (\bar{M}_{i+1}) are called the *points of Euler* EE_i (*Eulerian points* \bar{E}_i) (D5.0, D5.1). Fig. 6.

Theorem.

The *points of Euler* EE_i are the mid-points of the segment joining the orthocenter \bar{M} to the vertex A_i (D5.1, C5.3).

Theorem.

The points of Euler EE_i are on the circle of Brianchon-Poncelet (C5.5).

The Eulerian point $\bar{E}E_i$ is on the median ma_i as well as on the circle of Brianchon-Poncelet (C5.0, C5.5).

Theorem.

The lines em_i *joining the mid-points* M_i *to the Eulerian points* EE_i *are concurrent at a point* EE .

The lines $\bar{e}m_i$ *joining the feet* \bar{M}_i *to the Eulerian points* $\bar{E}E_i$ *are concurrent at a point* $\bar{E}E$ (D5.2, D5.3*).

EE *is on the line of Euler and is the center of the circle of Brianchon-Poncelet.*

$\bar{E}E$ *is on the line of Euler and is the pole of the orthic line with respect to the circle of Brianchon-Poncelet* (C5.1, C5.4, N5.1).

Definition.

The *mediatrix* mf_i is the line through the mid-point M_i perpendicular to the corresponding side a_i (D6.0, N6.0).

Theorem.

The vertex T_i *of the tangential triangle is on the mediatrix* mf_i (D6.0, C6.8, N6.0).

The mediatrices mf_i *are concurrent at a point* O .

The diameters $\bar{m}f_i$ *of the circle of Brianchon-Poncelet which pass through the feet of the altitudes pass through the same point* \bar{O} (D6.4*, N6.1).

Definition.

O is the *circumcenter* or center of the circumcircle (N6.1).

Theorem.

*The circumcenter O is on the line of Euler.
The point \bar{O} is on the line of Euler (C6.1).*

Definition.

An *equilateral conic* is a conic whose ideal points are harmonic conjugates of the isotropic points.

An *coequilateral conic* is a conic whose points on the orthic line are harmonic conjugates of the coisotropic points.

We leave as an exercise the pproof of the following Theorem and Corollary.

Theorem.

If an conic passes through the vertices of the triangle

0. *it is equilateral if and only if it passes through the orthocenter.
Its center is on the circle of Brianchon-Poncelet.*
1. *it is coequilateral if and only if it passes through the barycenter.
Its cocenter is on the circle of Brianchon-Poncelet.*

Corollary.

A conic

$$a_0X_0^2 + a_1X_1^2 + a_2X_2^2 + b_0X_1X_2 + b_1X_2X_0 + b_2X_0X_1 = 0,$$

0. *is equilateral if and only if*

$$m_1m_2(a_1 + a_2 - b_0) + m_2m_0(a_2 + a_0 - b_1) + m_0m_1(a_0 + a_1 - b_2) = 0.$$
1. *it is coequilateral if and only if*

$$m_0(m_1^2a_1 + m_2^2a_2 - m_1m_2b_0) + m_1(m_2^2a_2 + m_0^2a_0 - m_2m_0b_1) + m_2(m_0^2a_0 + m_1^2a_1 - m_0m_1b_2) = 0.$$

Definition.

The *conic of Kiepert* is the conic circumscribed to the triangle passing through the barycenter and the orthocenter. (D3.8.)

The *conic of Jerabek* is the conic circumscribed to the triangle passing through the orthocenter and the point of Lemoine. (D36.16.)

These are therefore equilateral. (C3.3 and C36.). The center of one conic is the cocenter of the other and these are on the circle of Brianchon-Poncelet (C8.9 and C36.18.)

Definition.

The circle through the vertices T_i of the tangential triangle is the circle of Neff.

Theorem.

0. The circle of Neff is a cocircle.
1. The ortic line is the radical axis of the circle of Neff and both the circumcircle and the circle of Brianchon-Poncelet.

Definition.

A triangle of Neff is a triangle whose orthocenter is on the conic.

Exercise.

Prove that in a triangle of Neff, one of the sides of the tangential triangle is a diameter of the circle of Neff. Determine other conditions for this to happen. *xxx*

Definition.

The points EUL_i at the intersection of the corresponding sides of the complementary triangle and of the orthic triangle are called the complorthic points (D8.0, N8.0).

The lines $aeUL_i$ joining the complorthic points are called complorthic lines (D8.3, N8.1).

The triangle whose vertices are the complorthic points is called the complorthic triangle (N8.2).

Definition.

The intersections of corresponding sides of the mixed triangles are the mixed points D_i (D8.4, N8.4).

Theorem.

0. The mixed points D_i and \overline{D}_i are on the line of Euler (C8.2).
1. The vertex A_i and the mixed point D_i are on the complorthic line $aeUL_i$. (C8.1, C8.3).
2. The lines nm_i joining the mid-points of the sides to corresponding complorthic points EUL_i are concurrent in a point S .
3. The lines $\overline{n}m_i$ joining the feet of the altitudes to the corresponding complorthic points EUL_i are concurrent in a point \overline{S} (D8.1, D8.2*).

Definition.

The points S and \overline{S} are the point and copoint of Schröter (N8.3).

Theorem.

S is the point of Miquel of the quadrangle a_{i+1} , a_{i-1} , $\overline{m}a_{i+1}$, $\overline{m}a_{i-1}$. S is therefore also on the circles through A_i , \overline{M} , \overline{M}_{i+1} , \overline{M}_{i-1} of center E_i and on the circles through A_{i+1} , A_{i-1} , \overline{M}_i of center M_i . (See .)

Theorem.

0. The points of Schröter are on the circle of Brianchon-Poncelet (C8.8).
1. The first point of Schröter S , the Eulerian point $\overline{E}E_i$ and the mixed point D_i are on the same line s_i
2. The second point of Schröter \overline{S} , the point of Euler point EE_i and the mixed point D_i are on the same line \overline{s}_i . (D8.5, C8.4).

Theorem.

The conic through the barycenter M , the orthocenter \overline{M} and the feet Gm_i of the perpendicular iMA_i from M to the corresponding altitude $\overline{m}a_i$ are on a circle ‘omicron (D10.3, D10.4, D10.7, C10.7).

This circle passes also through the perpendiculars $\overline{G}m_i$ which are the feet of the perpendiculars $\overline{g}m_i$ from \overline{M} to the corresponding median ma_i . $\{M, \overline{M}\}$ is a diameter whose mid-point is G (C10.1, C10.8). See Fig. 9.

Definition.

‘omicron is called the orthocentroidal circle (N10.2).

Theorem.

If we join

(D6.1, D10.1, D10.2, D10.3*).

Definition.

The G is the center of the orthocentroidal circle ‘omicron (N10.13).

Theorem.

The line be_i is parallel to the median ma_i (D10.5, N10.0, C10.2).

Theorem.

The 3 circles, the circumcircle θ , the circle γ of Brianchon-Poncelet and the orthocentroidal circle ‘omicron have the same radical axis \overline{m} . (C1.5, C10.9)

Definition.

An orthocentric quadrangle is

An example is provided by the circumcentral orthocentric quadrangle (N10.1).

3.4.4 The geometry of the triangle. II.**Theorem.**

The line tm_i through the mid-point M_i parallel to the side \overline{m}_i of the orthic triangle is tangent at M_i to the circle of Brianchon-Poncelet. (D12.0, C12.11)

Definition.

The line at_i joining the vertex A_i of the triangle to the vertex T_i of the tangential triangle are called the symmedians (D12.1, N12.0).

Theorem.

The symmedians at_i are concurrent at a point K (C12.6).

Theorem.

The point K of Lemoine, the first point S of Schröter and the point G are collinear on the line gk .

The point K of Lemoine, the second point \overline{S} of Schröter and the point \overline{G} are collinear on the line $\overline{g}k$ (D12.2, C12.7).

Definition.

The tangential point AMa_i ($AM\overline{a}_i$) is the intersection of the parallel am_{i+1} ($a\overline{m}_{i-1}$) through A_{i-1} (A_{i+1}) to the altitude $\overline{m}a_i$ and the parallel am_{i-1} ($a\overline{m}_{i+1}$) through A_i to $\overline{m}a_{i+1}$ ($\overline{m}a_{i-1}$) (D6.8, D14.4, N14.0).

Definition.

The tangential circle χa_i ($\chi\overline{a}_i$) is the circle through the vertices A_{i+1} and A_{i-1} tangent at A_{i-1} (A_{i+1}) to the side a_{i+1} (a_{i-1}) (D14.13, C14.8, C14.5).

Theorem.

The tangential circle χa_i ($\chi\overline{a}_i$) passes through the tangential point $AM\overline{a}_{i+1}$ (AMa_{i-1}) (D14.13).

Definition.

The parallels of Lemoine kk_i are the lines through the point K of Lemoine parallel to the sides of the triangle (D15.0, N15.0). See Fig. 13.

Definition.

The vertices $Br1_i$ of the first triangle of Brocard are the intersections of the mediatrices mf_i with the parallels of Lemoine kk_i (D15.1, N15.1).

Theorem.

The lines $br0_i$ joining the vertices of a triangle A_i to the corresponding vertex $Br1_i$ of the first triangle of Brocard are concurrent at a point $BR0$ (D15.2, D15.3*).

Theorem.

The lines br_i ($b\bar{r}_i$) joining the vertices A_{i-1} (A_{i+1}) to the vertices $Br1_{i+1}$ ($Br1_{i-1}$) of the first triangle of Brocard are concurrent at a point Br ($B\bar{r}$) (D15.4, D15.5*).

Definition.

The point Br ($B\bar{r}$) is called the first (second) point of Brocard (N15.4).

Definition.

The points $Br2_i$ at the intersection of the parallel $ok1_i$ to the side a_i through the center O of the circumcircle and the perpendicular km_i to a_i through the point K of Lemoine are the vertices of the second triangle of Brocard (D13.4, D13.3, D15.6, N15.2).

Theorem.

The lines $br3_i$ joining corresponding vertices $Br1_i$ and $Br2_i$ of the first and second triangle of Brocard are concurrent at a point Bro (D15.9, D15.10*).

Definition.

The cross tangential line $mf f_i$ is the line through the tangential points AMa_{i+1} and $AM\bar{a}_{i-1}$ (D15.7, N15.6).

Definition.

The vertices of the third triangle of Brocard $Br3_i$ are the intersections of the cross tangential line $mf f_i$ and the corresponding symmedian at_i (D15.8, N15.3).

Theorem.

The vertices $Br1_i$, $Br2_i$ and $Br3_i$ of the first, second and third triangle of Brocard, the first and second point of Brocard $Br1$ and $Br2$, the center O of the circumcircle and the point K of Lemoine are on a circle β with center Bro , the mid-point of $\{K, O\}$ (D15.18, C15.17, C15.18, C15.12, C15.13, C15.7).

Definition.

The circle β is called the circle of Brocard (N15.6).

Definition.

The conics of Tarry ‘Tarry[i] are the conics through the barycenter M and through 2 vertices, tangent there to the side through the third vertex, A_i . (N19.0.)

Theorem.

Let Apt_0 , (Apt_0) be the intersection of the line through A_0 parallel to the median ma_1 (ma_2) with the line through A_2 (A_1) parallel to the median ma_0 and circularly for Apt_1 , (Apt_1) , Apt_2 , (Apt_2) , then the line $Apt_0 \times (Apt_0)$ is the tangent common to ‘Tarry₁ and ‘Tarry₂ with Apt_0 and Apt_0 as point of contact. (D19.7, C19.0, D33.7, C33.5, C33.6.)

From the coordinates associated with the symmetric Theorem using \overline{M} instead of M , it is easy to solve the problem of C. Bindschelder, *El. Math.* 1990, p. 56.

3.4.5 Geometry of the triangle. III.**Definition.**

The line of Schröter, *pap* is (N4.1) It is tangent to the conics of Steiner, Lemoine and Simmons, (P. de Lepiney, *Math.* 1922-133)(C36.7) !dont have def. of Lemoine and Simmons, these are of the form $b_0x_1x_2 + b_1x_2x_0 + b_2x_0x_1 = 0$, with $b_0m_0(m_1 - m_2) + b_1m_1(m_2 - m_0) + b_2m_2(m_0 - m_1) = 0$. !MK.Center(‘Lemoine) = 0,36.15 no??? MK.Center(‘Simmons) = 0,??

3.4.6 Geometry of the triangle. IV.**Theorem. [Kimberling]**

0. The lines joining the vertices T_i of the tangential triangle to the second intersection B_i of the medians ma_i with the circumcircle θ are concurrent at a point CK . (C47.0.)
1. The lines joining the vertices T_i of the tangential triangle to the second intersection \overline{B}_i of the altitudes \overline{ma}_i with the circumcircle are concurrent at a point $C K$. (C47.0.)

Definition.

The points CK and \overline{CK} just defined is called respectively the point and copoint of Kimberling. (N47.0.)

Theorem. [Kimberling]

The point and copoint of Kimberling are on the line of Euler. (C47.4) See 3.3.0

Theorem.

0. $\text{Desargues}(M, \{A_i\}, \{B_i\}, ee)$. (D47.21)
1. $\text{Desargues}(\overline{M}, \{A_i\}, \{\overline{B}_i\}, \bar{e}e)$. (D47.21)
2. $\text{Desargues}(CK, \{T_i\}, \{B_i\}, \overline{m})$. (C47.6)
3. $\text{Desargues}(\overline{M}, \{A_i\}, \{\overline{B}_i\}, m)$. (C47.6)

Theorem. [Sekigichi]

The set of points on a triangle at which the sum of the distances to the sides is equal to the arithmetic mean of the lengths of the altitudes is a segment of a line through the barycenter. (*Amer. Math. Monthly*, 1981, 349 and 1984, 257.)

Definition.

The line defined in the preceding Theorem is called the line of Sekiguchi.

Theorem.

The line of Sekiguchi is perpendicular to the line ok joining the center O of the circumcircle to the point K of Lemoine.

The segment $[A_0, Sek_0]$ is equal to the segment \overline{M}_1, A_1 , (D18.27), the segment $[\overline{M}_0, Set_1]$ is equal to the segment A_2, \overline{M}_2 , (D18.28), the line sek_2 joining Sek_0 and Set_1 has the direction of $O \times K$ (C18.23).

3.4.7 Geometry of the triangle. V.**Definition.**

The triangle of Nagel, $\{Na_i\}$ has as its vertices the point of contact of the i -th escribed circles with the i -th side. (N21.0.)

Definition.

The conic of Feuerbach is the conic through the vertices of the triangle, the point of Gergonne J and the incenter I . (N20.6.)

Theorem. [Feuerbach]

The conic of Feuerbach is an equilateral hyperbola, it passes through the orthocenter and the point of Nagel, it is tangent at I to the line through I and O (Thébault), it has the point of Feuerbach as its center. (D20.23., C20.14, C20.15, C20.17, C23.8.) See also Neuberg, *Math.* 1922-51-90.

Theorem. [Kimberling]

If Kim_0 is the intersection of the lines from the center I_1 and I_2 of the excribed circles on the exterior bisectrix through A_0 perpendicular respectively to the sides a_2 and a_1 , then the line $kimc_0$ joining Kim_0 to A_0 and the similarly obtained lines $kimc_1$ and $kimc_2$ have a point Kim in common. (D21.30.) See 3.3.0

Definition.

The point Kim is called the *excribed point of Kimberling*. (N21.5.)

Theorem.

The point of Kimberling is on the conic of Feuerbach. (C21.11.)

Theorem.

If Kid_0 is the intersection of the lines from the center I_1 and I_2 of the excribed circles on the exterior bisectrix through A_0 and respectively the points MA_2 and \overline{M}_1 on the orthic line m and the sides a_2 and a_1 , then the line $kidc_0$ joining Kid_0 to A_0 and the similarly obtained lines $kidc_1$ and $kidc_2$ have a point Kid in common. (D21.26.)

Definition.

The point Kid is called the *excribed orthic point*. (N21.4.)

Theorem.

The barycentric coordinates of the incenter I are proportional to the lengths of the sides of the triangle.

Exercise.

Prove that the point En is the centroid of a wire of uniform density forming the sides of the triangle A_i . See C. J. Bradley, Math. Gazette, 1989, p. 44. for the latter.

Definition. [Mandart]

The *conic of Nagel* is the conic tangent at the vertices of the triangle of Nagel to the sides of the triangle. (N27.0)

Theorem. [Mandart and Neuberg]

The center of the conic of Nagel is on the conic of Feuerbach. C27.1. (Math. 1922-125)

Definition. [Mandart]

The *cercle of Nagel* is the circle circumscribed to the triangle of Nagel. (Math. 1922-125)

Theorem.

The complimentary point En of the incenter I is the center of gravity of the perimeter of the triangle. (See Math. 1889, Suppl. p. 8, 26)

3.4.8 Sympathic projectivities.**Introduction.**

This section discusses in some detail the notion of equality of angles in involutive geometry.

Definition.

A *sympathic projectivity* is one which is amicable with the fundamental involution. (II, 1.5.10)

Theorem. (H. D.)

If the involutive geometry is hyperbolic, a sympathic projectivity has 2 fixed points, the isotropic points.

Theorem.

The sympathic projectivities form an Abelian group under composition.

Moreover, using 1.0.10.0.4., if

$$f_b(y) = \frac{-1+by}{b+k'+y},$$

then

$$f_{b_1} \circ f_{b_2} = f_{b_3}, \text{ with } b_3 = \frac{-1+b_1b_2}{k'+b_1b_2}.$$

Proof.

$$f_{b_1}(f_{b_2}(y)) = (-(b_1 + b_2 + k') + \frac{(-1+b_1b_2)y}{(b_1+k')}(b_2 + k') - 1 + (b_1 + b_2 + k')y),$$

dividing numerator and denominator by $b_1 + b_2 + k'$ gives the conclusion of the Theorem.

See also ..., Section 7.

Example.

The method of obtaining sympathic projectivities will be studied in section It will be seen that all are powers of a sympathic projectivity S which is of order $p-1$ in the hyperbolic case and of power $p+1$ in the elliptic case. This generating projectivity is not unique, choosing one of these as fundamental sympathic projectivity will constitute the next step towards Euclidean geometry, the sympathic geometry. The fundamental involution is $S^{(\frac{p-1}{2})}$ or $S^{(\frac{p+1}{2})}$.

With $p = 7$, (elliptic), we will choose $k = 0$, $\delta^2 = 6$,

The sympathic projectivities are S^i , $i = 0$ to 7, with

$$S(1, j, -1 - j) = (2 - 3j, 3 + 2j, -5 + j),$$

$$S(0, 1, 6) = (1, 4, 2), \text{ or}$$

$$\begin{aligned}
S, &= (7, 14, 20, 26, 32, 38, 44, 50) \\
&(38, 44, 26, 14, , 7, 20, 50, 32) = S^7, \\
S^2 &= (7, 14, 20, 26, 32, 38, 44, 50) \\
&(20, 50, 14, 44, 38, 26, 32, , 7) = S^6, \\
S^3 &= (7, 14, 20, 26, 32, 38, 44, 50) \\
&(26, 32, 44, 50, 20, 14, , 7, 38) = S^5.
\end{aligned}$$

The fundamental involution is

$$\begin{aligned}
S^4, &= (7, 14, 20, 26, 32, 38, 44, 50) \\
&(14, 7, 50, 32, 26, 44, 38, 20).
\end{aligned}$$

The isotropic points are $(1, \delta, -1 - \delta)$, $(1, -\delta, -1 + \delta)$

With $p = 7$, (hyperbolic), we will choose $k = 1$, $\delta = 2$,

The sympathic projectivities are S^i , $i = 0$ to 5 , with

$$\begin{aligned}
S &= (26, 38, 7, 14, 20, 32, 44, 50) \\
&(26, 38, 44, 20, 7, 14, 50, 32) = S^5, \\
S^2 &= (26, 38, 7, 14, 20, 32, 44, 50) \\
&(26, 38, 50, 7, 44, 20, 32, 14) = S^4,
\end{aligned}$$

The fundamental involution is

$$\begin{aligned}
S^3 &= (26, 38, 7, 14, 20, 32, 44, 50) \\
&(26, 38, 32, 44, 50, 7, 14, 20).
\end{aligned}$$

The isotropic points are $(26) = (1, 2, 4)$ and $(38) = (1, 4, 2)$.

anti. . . .

3.4.9 Equiangularity.

Definition.

An *angle* is an ordered pair $\{a, b\}$ of ordinary lines a and b .

Definition.

Two angles $\{a, b\}$ and $\{a_1, b_1\}$ are equal and we write

$$\{a, b\} = \{a_1, b_1\},$$

if the ideal points on these lines, A, B, A_1, B_1 are such that there exists a sympathic projectivity which associates A to B and A_1 to B_1 . Compare with Coxeter, p. 9 and p.125).

Notation.

In view of 2.3., we will also use $\{A, B\} = \{A_1, B_1\}$ instead of $\{a, b\} = \{a_1, b_1\}$, where A, B, A_1, B_1 are the ideal points on a, b, a_1, b_1 .

Example.

For $p = 5$, starting with Example II.1.5.12. if ϕ' is used to to define the fundamental involution, then ϕ is a sympathic projectivity. We have the equality of angles $\{(10), (5)\} = \{(5), (26)\} = \{(26), (14)\} = \{(14), (18)\} = \{(18), (22)\} = \{(22), (10)\}$ and of angles $\{(10), (14)\} = \{(5), (18)\} = \{(26), (22)\} = \{(14), (10)\}$.

Theorem.

If a and b are perpendicular, then $\{a, b\} = \{b, a\}$. If c and d are also perpendicular, then $\{a, b\} = \{(c, d)\}$.

Definition.

If a and b are perpendicular, the angle $\{a, b\}$ is called a *right angle*.

Definition.

If a and b are not parallel and c , through $a \times b$, is such that $\{a, c\} = \{c, a\}$, c is called a *bisectrix* of $\{a, b\}$. If a bisectrix exist, we say that the *angle* $\{a, b\}$ can be bisected.

Theorem.

If the ideal points on a and b are $(1, a_1, -1 - a_1)$ and $(1, b_1, -1 - b_1)$, then the ideal point $(1, z, -1 - z)$ on the bisectrix c of $\{a, b\}$ satisfies the second degree equation

$$0. (k' + a_1 + b_1)z^2 - 2(a_1b_1 - 1)z - (a_1 + b_1 + k'a_1b_1) = 0, \text{ with } k' = \frac{2k}{1+k}.$$

1. The discriminant of 0. is

$$t' = (a_1^2 + k'a_1 + 1)(b_1^2 + k'b_1 + 1)$$

2. Moreover,

0. if $t' \neq 0$ is a quadratic residue, the bisectrices are real and perpendicular to each other,

1. if t' is a non residue, there are no real bisectrices,

2. if a or b is an isotropic line, $t' = 0$, the bisectrices coincide with the isotropic line,

3. if both a and b are isotropic, the bisectrices are undefined,

4. if a and b are parallel, the bisectrices do not exist but the directions given by 0. are that of a and of the perpendicular to a .

Proof: Let the sympathetic projectivity which associates to the ideal points on a and c the ideal points on c and b , have the form

$$f(x) = \frac{a' + b'x}{c' + d'x},$$

then

$$z(c' + d'a_1) = a' + b'a_1,$$

$$b_1(c' + d'z) = a' + b'z.$$

Because of 0.0.10., $d' = -a' = 1 + k$, $c' - b' = 2k$.

Substituting and multiplying the first equation by $(c_1 - b_1)$, the second by $(c_1 - a_1)$ and adding, we obtain the equation 0.

If a_1 corresponds to an isotropic point, $a_1^2 + k'a_1 + 1 = 0$, $t' = 0$, the roots of 0. are

$$\frac{a_1b_1-1}{k'+a_1+b_1} = a_1 \frac{a_1b_1-1}{a_1^2+k'a_1+b_1a_1} = a_1.$$

If $a_1 = b_1$, 0. can be written $(z - a)((k' + 2a_1)z + (2 + k'a)) = 0$. The perpendicularity follows from 1.9.6.

Example.

For $p = 7$, hyperbolic case, let the ideal point on “a” be (32) and on “b” be (20), $a_1 = 3$, $b_1 = 1$, $k = k' = 1$, 0. is $5z^2 - 4z = 0$, with roots 0 and 5 giving the points (14) and (44). If $a_1 = b_1 = 0$, one root is 0, the other is 5.

Definition.

The *angle* between distinct non isotropic lines *is even* if and only if the angle can be bisected.

Theorem.

Under the hypothesis of Theorem 0.2.7., an angle is even if $a_1^2 + k'a_1 + 1$ and $b_1^2 + k'b_1 + 1$ are both quadratic residues or both non residues.

The proof follows at once from ...

Theorem.

The relation “even” is a equivalence relation.

Again this follows from

Definition.

The sum of two angles ...

... circle, angle at the center, rotation.

3.4.10 Equidistance, congruence.

congruence (translation composed with rotation)

Theorem.

Any congruence can be written as the composition of a translation rotation and a translation.

Definition.

A *segment* $[A, B]$ is an unordered pair of ordinary points A and B .

... not on the same isotropic line?

Definition.

Two segments are equal iff

Theorem.

If $[A, B] = [B, C]$ and C is on $A \times B$, then either $A = C$ or B is the mid-point of $[A, C]$.

... equality of segments on parallel line iff equal in the affine sense or $AB = CD$ in affine sense or $BA = CD$

Theorem.

$\{A, B\} = \{C, D\}$ implies $[A, B] = [C, D]$.

equal. on non parallel segment using translation and circle may have to use tangent to circle
def. of congruence.

3.4.11 Special triangles.**Definition.**

A *right triangle* is a triangle with 2 perpendicular sides. If a_1 and a_2 are perpendicular we say that the triangle is a *right triangle at A_0* .

Theorem.

A necessary and sufficient condition for a triangle to be a right triangle at A_0 is that $m_1 = m_2 = 0$.

Exercise.

If we start with A_i , M and \overline{M} in involutive geometry, we cannot derive the properties of the right triangles. Other elements have to be preferred. Make an appropriate choice and construct enough elements to determine θ and γ .

Answer to 3.4.11.

To obtain the coordinates, we replace

$$m_0, m_1, m_2 \text{ by } 1, \epsilon m_1, \epsilon m_2,$$

and when the coordinates contain terms of different order of ϵ , we neglect the terms of higher order.

For instance,

$$q_0 = 1, q_1 = -m_2, q_2 = -m_1,$$

$$\theta : m_0(m_1 + m_2)X_1X_2 + m_1(m_2 + m_0)X_2X_0 + m_2(m_0 + m_1)X_0X_1 = 0,$$

becomes

$$\theta : (m_1 + m_2)X_1X_2 + m_1X_2X_0 + m_2X_0X_1 = 0,$$

Of course many points or lines will coincide and some of the construction which are invalid must be replaced by other constructions but the coordinates do not have to be rewritten.

For instance,

$$A_0 = \overline{M}M_0 = \overline{I}Ma_0, \overline{m} = \overline{m}_0 = \overline{m}m_0 = ta_0, \overline{m}a_0 = \overline{m}k, \overline{M}A_0 = TAa_0, eul = ma_0, EUL = Imm_0, ta_0 = \overline{m}, Aat_0 = \overline{M}_0.$$

We can start, for instance, with A_i , M and $K = (m_1 + m_2, m_1, m_2)$, on mm_0 , we construct, as usual, ma_i , M_i , mm_i , MA_i , m_i , MM_i , m . Then

$$mk := M \times K, mk = [m_1 - m_2, -m_1, m_2],$$

$$at_i := K \times A_i, at_0 = [0, m_2, -m_1], at_1 = [m_2, 0, -(m_1 + m_2)],$$

$$Aat_i := at_i \times a_i, Aat_1 = (m_1 + m_2, 0, m_2),$$

$$Iat_i := m \times at_i, Iat_0 = (m_1 + m_2, -(2m_2 + m_1), m_2),$$

$$ta_i := A_i \times Iat_i, ta_0 = [0, m_2, m_1], ta_1 = [m_2, 0, m_1 + m_2],$$

$$TAa_0 := ta_0 \times a_0, TAa[0] = (0, m_1, -m_2).$$

In general, the construction cannot be done for all 3 elements, but can done simultaneously for the elements with index 1 and 2, we can use j for 1 and $-j$ for 2.

$$\theta = \text{conic}(A_0, ta_0, A_1, A_2, MM_0),$$

$$\theta : (m_1 + m_2)X_1X_2 + m_1X_2X_0 + m_2X_0X_1 = 0,$$

$$\gamma := \text{conic}(M_i, Aat_0, A_0),$$

$$\gamma : m_2X_1^2 + m_1X_2^2 - (m_1 + m_2)X_1X_2 - m_1X_2X_0 - m_2X_0X_1 = 0.$$

When we start with J and M , the triangle is a right triangle if $I \times J_1 // a_2$ and $I \times J_2 // a_1$. Moreover, $j_0^2 = p_{11}$, $m_1 = j_1(j_2 + j_0)(j_2 - j_0)$, $m_2 = j_2(j_0 + j_1)(j_0 - j_1)$. The usual construction gives $\overline{M}_0 = Aat_0$, then $at_0 := A_0 \times Aat_0$, $K := at_0 \times mm_0$.

Definition.

An *isosceles triangle* $\{A_i\}$ at A_0 is a triangle whose angles $A_0 A_1 A_2$ and $A_1 A_2 A_0$ are equal. What about right isosceles?

Theorem.

A necessary and sufficient condition for a triangle to be an isosceles triangle at A_0 is that $m_1 = m_2$.

Theorem.

If $\{ABC\}$ is an isosceles triangle at A , then the sides AB and AC are equal.

Theorem.

If $\{ABC\}$ is an isosceles triangle, then the angle $(A \times B, A \times C)$ is even.

Definition.

A triangle $\{ABC\}$ is an *equilateral triangle* iff it is isosceles at B and C .

Theorem.

A necessary and sufficient condition for a triangle to be an equilateral triangle at A_0 is that $m_0 = m_1 = m_2$.

Theorem.

If a triangle is equilateral, then all its angles ABC , BCA and CAB are equal and all its sides are equal.

Definition.

A triangle which is neither a right triangle nor an isosceles triangle, and therefore not an equilateral triangle is called a *scalene triangle*.

Theorem.

A necessary and sufficient condition for a triangle to be a scalene triangle is that m_0 , m_1 and m_2 be distinct.

Definition.

*A triangle which is an isosceles triangle at A but is not an equilateral triangle is called a *proper isosceles triangle*.*

Theorem.

If a triangle is equilateral, then all its angles ABC , BCA and CAB are equal and all its sides are equal.

The following Definitions and Theorem are only meaningful in Minkowskian Geometry.⁵

Definition.

An isotropic triangle is a triangle with one isotropic side.

Definition.

A doubly isotropic triangle is a triangle with 2 isotropic sides

Theorem.

0. *A necessary and sufficient condition for a triangle to be isotropic is that the barycenter be on the complementary triangle.*
1. *A necessary and sufficient condition for a triangle to be doubly isotropic is that the barycenter be one of the vertices of the complementary triangle.*

Theorem.

If $a[0]$ is an isotropic line, then

0. $m_1 + m_2 = 0$,
1. *the circumcircle degenerates into a_0 and the line $[0, m_0 + m_1, -(m_0 - m_1)]$,*

Theorem.

If a_1 and a_2 are isotropic lines, then

0. $m_0 = 1, m_1, m_2 = -1$,
1. *the circumcircle degenerates into a_1 and a_2 .*

⁵4.3.89

3.4.12 Other special triangles.

Introduction.

There are many other types of triangles that can be defined. I will give here 2 examples which allow the constructions of configurations of the type $9 * 3$ & $9 * 3$, distinct from that of Pappus. For the first one, if we choose $B_1 = M_1$, $B_2 = M_2$ and $C_1 = \overline{M}$, the construction of Section 19 gives $C_0 = Mam_2$, $C_2 = Tara_0$, $B_0 = tara_2 \times tarb_2$. from P19.7, follows that $B_0 \cdot a_0 = 0$ iff $q_0 = 0$. This suggest the definition of a triangle of Tarry and the construction of the 1-Pappus configuration.

A similar approach determines the construction of the 2-Pappus configuration.

Definition.

The *1-Pappus configuration* is the set of points

$$1\text{-Pappus}(A_i, B_i, C_i),$$

such that $\{A_i\}$, $\{B_i\}$, $\{C_i\}$ are 3 triangles and $\text{incidence}(A_i, C_i, C_{i-1})$, $\text{incidence}(B_{i+1}, B_{i-1}, C_i)$.

Definition.

The *2-Pappus configuration* is the set of points

$$2\text{-Pappus}(A_i, B_i, C_i),$$

such that $\{A_i\}$, $\{B_i\}$, $\{C_i\}$ are 3 triangles and $\text{incidence}(A_i, B_i, C_i)$, $\text{incidence}(B_i, C_{i+1}, C_{i-1})$.

Definition.

A *triangle of Tarry* is a triangle which is not a right triangle whose point of Tarry is well defined and coincides with one of the vertices of the triangle.

Theorem.

A necessary and sufficient condition for a triangle to be a triangle of Tarry at A_0 is that $q_0 = 0$.

The proof follows at once from $m_i \neq 0$ and from P16.3.

Moreover, if $q_0 = q_1 = 0$, then the point of Tarry is undefined.

Corollary.

A necessary and sufficient condition for a triangle to be a triangle of Tarry at A_0 is that the orthocenter be on the conic of Tarry.

Theorem.

$$\overline{M} \cdot \text{'Tarry}[0] \Rightarrow 1\text{-Pappus}(A_i, Tarb_2 M_1 M_2, Mam_2 \overline{M} Tara_0).$$

Theorem.

In *Involutive Geometry*, $A_0 = (x, y, 1)$, $A_1 = (0, 0, 1)$, $A_2 = (1, 0, 1)$, $M = (1 + x, y, 3)$, $\overline{M} = (xy, x(1 - x), y)$ is a triangle of Tarry iff

$$u^2 - (1 + 2y^2)u + y^4 = 0 \text{ and } x^2 - x + u = 0.$$

Proof: Assuming that $m = [0, 0, 1]$ and $X_0^2 + X_1^2 = X_2^2$ is a circle, a trivial computation determines M and \overline{M} as given. The conic of Tarry is

$$a_0 \times a_0 + ka_1 \times a_2 = 0,$$

where k is determined in such a way that $M \cdot \text{'Tarry} = 0$, this gives $k = 1$. To insure that \overline{M} is on the conic of Tarry gives after division by $u := x(1 - x)$,

$$u + (y^2 - u)(u - y^2) = 0, \text{ a simple discussion determines that } 0 < y \leq \frac{\sqrt{3}}{2}.$$

Definition.

An *Eulerian triangle* is a triangle for which the line of Euler is parallel to one of its sides.

Theorem.

A necessary and sufficient condition for a triangle to be an Eulerian triangle for side a_0 is that $2m_0 = m_1 + m_2$.

The proof follows at once from P1.17.

Theorem.

$$eul // a_0 \Rightarrow 2\text{-Pappus}(A_i, \overline{M}_0 M_1 M_2, \overline{M} \text{ Tar } c_0 \text{ Tar } \bar{c}_0).$$

3.4.13 Geometry of the triangle. V.

(bissectrices)

CHAPTER II

FINITE PROJECTIVE
GEOMETRY**3.90 Answers to problems and miscellaneous notes.**

Answer to **2.2.3.**

Let $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$, $C = (1, 1, 1)$, $B_0 = (b_0, 1, 1)$, $B_1 = (1, b_1, 1)$,

$$B_2 = (1, 1, b_2),$$

by hypothesis, $b_i \neq 1$, $b_2 \neq 0$, $b_1 b_2 \neq 1$ and $2 - b_0 - b_1 - b_2 + b_0 b_1 b_2 \neq 0$ (because of $\{B_i\}$).

$$a_0 = [1, 0, 0], b_0 = [1 - b_1 b_2, -(1 - b_2), -(1 - b_1)],$$

$$c_0 = [0, 1, -1], C_0 = (0, 1 - b_1, -(1 - b_2)),$$

$$c = [(1 - b_1)(1 - b_2), (1 - b_2)(1 - b_0), (1 - b_0)(1 - b_1)], d = [0, b_2, -1],$$

$$D = (b_2, 1, b_2), e = [b_2(1 - b_1), b_2(1 - b_0), -1 + b_0 - b_2 + b_1 b_2],$$

$$E = (1 - b_0 + b_2 b_0 - b_1 b_2 - b_2^2 b_0 + b_2^2 b_0 b_1, 1 - b_0 + b_2 - 2b_1 b_2 - b_2^2 + b_2^2 b_1 + b_0 b_1 b_2, \\ b_2(2 - b_0 - b_1 - b_2 + b_0 b_1 b_2)), f = [1 - b_1 b_2, -b_2(1 - b_2), -b_2(1 - b_1)], F = (b_2(1 - b_1), 0, 1 - b_1 b_2), G = (1 - b_2, 1 - b_1 b_2, 0),$$

$$g = [1 - b_1 b_2, -(1 - b_2), -b_2(1 - b_1)],$$

$$X = (0, 1, b_2), Y = (1 - b_0 - b_2 + b_0 b_1 b_2, -(1 - b_1), -b_2(1 - b_1)),$$

$$Z = (1 - b_2 + b_2^2 - b_2^1 b_1, 1 - b_1 b_2, b_2(1 - b_2)).$$

3.90.1 Answer to exercises.

Exercise. [Pappus]

Define

$$\alpha := (A_0 * A_1) \cdot A_2, \beta := (B_0 * B_1) \cdot B_2, \\ \alpha_{1,2} := (A_1 * A_2) \cdot B_1, \beta_{1,2} := (B_1 * B_2) \cdot A_1, \\ \alpha_{2,0} := (A_2 * A_0) \cdot B_2, \beta_{2,0} := (B_2 * B_0) \cdot A_2, \\ \alpha_{0,1} := (A_0 * A_1) \cdot B_0, \beta_{0,1} := (B_0 * B_1) \cdot A_0,$$

Using 2.3.17.0,

$$C_0 = (A_1 * B_2) * (A_2 * B_1) = ((A_1 * B_2) \cdot B_1) B_2 - ((B_2 * A_2) \cdot B_1) A_1 \\ = \alpha_{1,2} B_2 - \beta_{1,2} A_1,$$

similarly,

$$C_1 = \alpha_{2,0} B_0 - \beta_{2,0} A_2,$$

$$C_2 = \alpha_{0,1} B_1 - \beta_{0,1} A_0, \text{ therefore}$$

$$(C_0 * C_1) \cdot C_2 = \beta \alpha_{1,2} \alpha_{2,0} \alpha_{0,1} - \alpha \beta_{1,2} \beta_{2,0} \beta_{0,1} + \alpha_{2,0} \alpha_{1,2} \beta_{2,0} \beta_{0,1} - \beta_{2,0} \alpha_{1,2} \alpha_{2,0} \beta_{0,1} \\ + \alpha_{0,1} \beta_{1,2} \alpha_{2,0} \beta_{0,1} - \beta_{0,1} \beta_{1,2} \alpha_{2,0} \alpha_{0,1} + \alpha_{1,2} \beta_{1,2} \beta_{2,0} \alpha_{0,1} - \beta_{1,2} \alpha_{1,2} \beta_{2,0} \alpha_{0,1} \\ = \beta \alpha_{1,2} \alpha_{2,0} \alpha_{0,1} - \alpha \beta_{1,2} \beta_{2,0} \beta_{0,1}.$$

Therefore, if the points A_0, A_1, A_2 and the points B_0, B_1, B_2 are collinear, $\alpha = 0$ and $\beta = 0$, therefore $(C_0 * C_1) \cdot C_2 = 0$ and the points C_0, C_1, C_2 are collinear by 2.3.18.

Exercise.

(Harmonic quatern). $a = [0, 0, 1]$, let $A = (0, 0, 1)$, $A \times K = [k, -1, 0]$,

let $B = (1, k, 1)$, $l \neq 0$ and 1.

$$B \times L = [l, -1, k - l], A \times M = [m, -1, 0], D = (l - k, ml - mk, l - m), D \times K = \\ [k(l - m), m - l, (l - k)(m - k)], A \times L = [l, -1, 0], C = (m - k, lm - lk, l - m), B \times C = \\ [2kl - km - lm, 2m - k - l, (k - l)(k - m)], N = (2m - l - k, km + lm - 2kl, 0).$$

Exercise.

(Projectivity). Choose $b = [0, 1, 0]$, $a = [1, 0, 0]$ and $P = (0, 1, 1)$. $c = [0, 0, 1]$, $S = (1, 0, -k)$, $T = (1, 0, -l)$, $Q = (0, m, k)$, $N = [k, ml, 0]$.

Exercise.

(Projectivity with 3 pairs). $C_0 = (1, 0, -1)$, $C_j = (1, a_j, -1 - a_j)$, $j > 0$, with obvious notation,

$D_j = (1, -a_j b_j, -1 - a_j)$, $j = 1, 2$, $t = (a_1 a_2 (b_2 - b_1) + a_2 b_2 - a_1 b_1, a_1 - a_2, a_2 b_2 - a_1 b_1)$,
 $D_j = (a_2 - a_1, a_1 b_1 - a_2 b_2 - a_1 a_2 (b_2 - b_1), (a_1 - a_2)(1 + a_j))$, $j > 2$, hence B_j given above.

Answer to 2.6.14.

In part, the coefficients of A_0 and A_1 in A_l and B_l must be proportional, therefore, $\frac{f_0 t_0 + f_1 t_1}{f_2 t_0 + f_3 t_1} = \frac{t_0}{t_1}$, this gives 1.

Answer to 2.3.7.

For $p = 2$, if $A[] = ((1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1))$, and the diagonal points are B_i ,
 $A_0 \times A_1 = [0, 1, 0]$, $A_2 \times A_3 = [1, 1, 0]$, $B_0 = (0, 0, 1)$. $A_1 \times A_2 = [1, 1, 1]$, $A_3 \times A_0 = [0, 1, 1]$,
 $B_1 = (0, 1, 1)$. $A_0 \times A_2 = [0, 0, 1]$, $A_1 \times A_3 = [1, 0, 1]$, $B_2 = (0, 1, 0)$. The diagonal points are
on $[1, 0, 0]$. For $p = 4$, the coordinates are 0, 1, x , $y = 1 + x$. The addition and multiplication
tables are

+	0	1	x	y	\cdot	0	1	x	y
0	0	1	x	y	0	0	0	0	0
1	1	0	y	x	1	0	1	x	y
x	x	y	0	1	x	0	x	y	1
y	y	x	1	0	y	0	y	1	x

If $A[] = ((1, 0, 0), (1, 0, 1), (1, x, 0), (1, y, 1))$,

$A_0 \times A_1 = [0, 1, 0]$, $A_2 \times A_3 = [x, 1, 1]$, $B_0 = (1, 0, x)$. $A_1 \times A_2 = [x, 1, x]$, $A_3 \times A_0 = [0, 1, y]$,
 $B_1 = (1, 1, x)$. $A_0 \times A_2 = [0, 0, 1]$, $A_1 \times A_3 = [y, 0, y]$, $B_2 = (0, 1, 0)$. The diagonal points are
on $[x, 0, 1]$.

Answer to 2.5.10.

In part,

$C_2 = (c, 1 - c, 1)$, $a_0 = (1, c, -c - 1)$, $b = [1, 0, 0]$, $B_2 = (c^2 - c + 1, -c + 1, 1)$. A geometric
condition is $a_0 \cdot C_2 = 0$ or $b \cdot B_2 = 0$. The configuration is then of type

$$6 * 4 + 3 * 3 + 1 * 2 \& 2 * 4 + 9 * 3.$$

Notes.

On 2.2.2:

Commutativity implies that if

$$J' := (B \times P) \times (E \times Q), J = (b(a - 1), b^2(a - 1), a(b - 1)),$$

$$K' := (A \times P) \times (J' \times M), K = (b(a - 1), ab(a - 1), a(b - 1)),$$

then

$$L \cdot (J' \times K') = 0.$$

The construction

$$D'' := (R \times T') \times a, \text{ with } D'' = (1, b+c)$$

is related to the associative property

$$(a + b) + c = a + (b + c).$$

Before 2.2.9

Theorem.

... describe the degenerate conic, perhaps in 2.10.8 ... determine the collineation which leave a general conic fixed also special case when it is a conic.

Examples.

For $p = 5$,

C0

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
4 4 2 4 4 4 4 4 2 4 4 4 4 1 4 4 4 4 4 2 2 4 4 4 1 4 1 4 4 4

$$N = \begin{pmatrix} 2 & -2 & 0 \\ 2 & 0 & -1 \\ 2 & 0 & 0 \end{pmatrix}, N^I = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & -1 \\ -2 & -2 & 1 \end{pmatrix}.$$

Point conic and its mapping 0 1, 1 6, 10 27, 14 4, 23 8, 27 29,

Line conic and its mapping 1 10, 4 14, 6 0, 8 1, 27 23, 29 27,

Points on line conic and tangent, 0 16, 1 0, 10 22, 14 4, 23 14, 27 29,

Lines on line conic and contact, 1 7, 4 14, 6 5, 8 13, 27 29, 29 27.

The equation of the point conic is $X^2 + 2YZ + ZX = 0$.

The equation of the line conic is $-2z^2 + yz - zx + xy = 0$.

C1

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
6 6 3 6 6 6 6 3 6 6 6 6 6 3 6 6 6 1 6 3 6 6 6 6 3 3 6 6 6 6

$$N = \begin{pmatrix} -2 & 2 & 0 \\ -2 & 0 & -1 \\ -2 & 0 & 0 \end{pmatrix}, N^I = \begin{pmatrix} 0 & -2 & 0 \\ 0 & 0 & -1 \\ 2 & 2 & 1 \end{pmatrix}.$$

Point conic and its mapping 0 1, 1 6, 10 22, 12 5, 18 25, 29 9,

Line conic and its mapping 1 10, 5 18, 6 0, 9 1, 22 12, 25 29,

C2

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
10 5 10 10 2 10 10 10 5 2 10 10 2 5 10 10 10 5 10 2 10 10 11 10 10 11 5 10 10

$$N = \begin{pmatrix} 0 & 1 & -2 \\ 1 & 1 & 0 \\ -1 & 1 & 0 \end{pmatrix}, N^I = \begin{pmatrix} 0 & 0 & 2 \\ -2 & -2 & -1 \\ 2 & -2 & -1 \end{pmatrix}.$$

Point conic and its mapping 0 6, 5 18, 6 5, 15 26, 19 22, 21 25,

22 28, 23 14, 24 17, 25 4, 27 10,

The center is (23), the points are on [21] or [2].

Line conic and its mapping 4 6, 5 24, 6 5, 10 22, 14 23, 17 27,
18 25, 22 21, 25 15, 26 0, 28 19,

The central line is [18], the lines pass through (4) or (12).

The equation of the point conic is $Y^2 + YZ + 2ZX + 2XY = 0$.

The equation of the line conic is $y^2 - 2z^2 - yz - 2zx + xy = 0$.

C3

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
4 4 4 4 4 2 4 4 4 1 4 4 4 2 4 1 4 2 4 4 4 2 4 4 4 4 4 4 4 4 1

Point conic and its mapping 7 10, 9 19, 11 30, 12 18, 29 27, 30 7,

Line conic and its mapping 7 30, 10 12, 18 29, 19 9, 27 11, 30 7,

C4

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 1 5 5 5 5 5 5 5 5 5 5 5 5

Point conic and its mapping 11 29, 14 12, 17 24, 19 28, 26 15, 27 23,

Line conic and its mapping 12 26, 15 19, 23 14, 24 17, 28 11, 29 27,

C5

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5 5 5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

Point conic and its mapping 2 27, 3 3, 8 8, 10 1, 16 19, 18 16,

Line conic and its mapping 1 8, 3 3, 8 18, 16 16, 19 2, 27 10,

C6

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5 5 5 5 5 5 5 5 5 5 5 5 5 5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

Point conic and its mapping 9 14, 10 12, 15 26, 18 29, 23 21, 24 17,

Line conic and its mapping 12 18, 14 23, 17 10, 21 24, 26 15, 29 9,

C7

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5 5 5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

Point conic and its mapping 0 16, 3 3, 8 8, 11 28, 16 0, 28 11,

Line conic and its mapping 0 11, 3 3, 8 28, 11 0, 16 16, 28 8,

C8

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
10 10 10 10 5 1 5 10 10 2 10 10 11 10 10 2 10 10 10 5 10 10 5 10 2

$$N = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}, N^I = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}.$$

Point conic and its mapping 17 24, the center is (17).

Line conic and its mapping 24 17, the central line is [24].

The equation of the point conic is, with $\delta^2 = 2$,

$$(X - (2 + 2\delta)Y - (2 + \delta)Z)(X - (2 - 2\delta)Y - (2 - \delta)Z) = 0.$$

The equation of the line conic is $(x + (2 + 2\delta)y + (1 - 2\delta)z)(x + (2 - 2\delta)y + (1 + 2\delta)z) = 0$.

C9

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5 5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

Point conic and its mapping 2 5, 5 2, 15 25, 20 30, 26 14, 29 11,

Line conic and its mapping 2 15, 5 2, 11 26, 14 20, 25 29, 30 5,

C10

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
1 3 6 6 6 6 3 6 6 6 6 3 6 6 6 6 3 6 6 6 6 3 6 6 6 6 3 6 6 6 6

Point conic and its mapping 3 3, 4 4, 8 28, 9 29, 13 8, 14 9,

Line conic and its mapping 3 13, 4 14, 8 8, 9 9, 28 4, 29 3,

C11

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3

Point conic and its mapping 2 5, 5 2, 12 14, 15 13, 17 24, 20 23,

Line conic and its mapping 2 15, 5 12, 13 17, 14 20, 23 2, 24 5,

C12

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5

$$N = \begin{pmatrix} -2 & -2 & 0 \\ -2 & 0 & 0 \\ -2 & 0 & -1 \end{pmatrix}, N^I = \begin{pmatrix} 0 & 2 & 0 \\ 2 & -2 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Point conic and its mapping 1 6, 7 15, 8 13, 15 25, 16 18, 19 16,

Line conic and its mapping 6 1, 13 15, 15 19, 16 16, 18 8, 25 7,

C13

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
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

$$N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, N^I = \begin{pmatrix} 2 & -2 & -2 \\ -2 & 2 & -2 \\ -2 & -2 & 2 \end{pmatrix}.$$

Point conic and its mapping 0 11, 1 7, 6 2, 13 15, 17 27, 24 30,

Line conic and its mapping 2 6, 7 1, 11 0, 15 13, 27 17, 30 24,

The equation of the point conic is $YZ + ZX + XY = 0$.

The equation of the line conic is $x^2 + y^2 + z^2 - 2yz - 2zx - 2xy = 0$.

C14

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
 2 2 1 2 2 2 2 2 2 1 2 2 2 2 2 1 1 2 2 2 2 2 1 2 2 1 2 2 1 2 2

$$N = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 0 & 2 & -1 \end{pmatrix}, N^I = \begin{pmatrix} 1 & 1 & 2 \\ 0 & -1 & -2 \\ 1 & 1 & 1 \end{pmatrix}.$$

Point conic and its mapping 2 15, 9 29, 15 7, 16 18, 22 21, 28 4,

The points are on [19].

Line conic and its mapping 4 28, 7 15, 15 2, 18 16, 21 22, 29 9,

The lines pass through (25).

C15

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
 2 2 2 2 2 1 2 2 2 2 1 2 1 2 1 2 2 2 1 2 2 2 1 2 2 2 1 2 2 2 2

$$N = N^I = \begin{pmatrix} 1 & -2 & -2 \\ -2 & 1 & -2 \\ -2 & -2 & 1 \end{pmatrix}$$

Point conic and its mapping 19 28, 20 23, 23 20, 25 29, 28 19, 29 25,

Line conic and its mapping 19 28, 20 23, 23 20, 25 29, 28 19, 29 25,

The equation of the point conic is $X^2 + Y^2 + Z^2 + YZ + ZX + XY = 0$.

The equation of the line conic is $x^2 + y^2 + z^2 + yz + zx + xy = 0$.

Answer to 2.2.9.

For $p = 13$, points on the conic are, $(0,1,1) = (2)$, $(0,1,2) = (3)$, $(1,0,1) = (15)$, $(1,0,4) = (18)$, $(1,1,0) = (27)$, $(1,2,0) = (40)$.

The point conic is

2, 3, 15, 18, 27, 35, 40, 51, 133, 135, 146, 151, 158, 168,

the line conic is

111, 83, 156, 121, 179, 22, 98, 148, 112, 129, 86, 25, 165, 166.

The representative matrix is

$$\begin{pmatrix} 1 & -4 & 1 \\ -4 & -6 & -2 \\ 1 & -2 & -3 \end{pmatrix}$$

$(0,1,2) = (13)$ and $(1,0,12) = (26)$ are on $[1,1,1]$, the polars are $[1,6,5] = [97]$ and $[0,1,11] = [12]$. Hence the pole of $[1,1,1]$ is $(1,6,3) = (95)$.

1. $-6 + 3 \cdot 1 - 4 \cdot 5 - 2 \cdot (-3) = -17 = -4$

6. $(-3) + 8 \cdot 6 - 2 \cdot (-6) - (-5) \cdot 5 = 67 = 2$,

2. $5 + 4 \cdot 2 - (-5) \cdot (-3) - 4 \cdot (-6) = 27 = 1$, $(-4, 2, 1) = (1, 6, 3)$.

Answer to 2.2.9.

$A \times B = [1, -1, 1]$, $C \times D = [2, 1, -5]$, $A \times D = [2, -1, 1]$, $B \times C = [1, 1, -3]$, $k_1 = 1.3$, $k_2 = -1.3$, therefore the conic is, after dividing by 3,

$(X_0 - X_1 + X_2)(2X_0 + X_1 - 5X_2) + (2X_0 - X_1 + X_2)(X_0 + X_1 - 3X_2) = 0$,

which gives twice the result of the Example.

Answer to 2.3.2.

0. For $q = 2$, the primitive polynomial giving the selector 0, 1, 3, is $I^3 + I + 1$.

The auto-correlates are 0 11 2 7 8.

The selector function is

i	0	1	2	3	4	5	6	7	8	9	10	11
$f(i)$		0	14	1	0	16	16	14	14	16		
$type$	F_0	V_0	F_4	V_2	T_0	T_2	V_1	F_3	F_1	T_3	E_2	F_2
i	12	13	14	15	16	17	18	19	20			
$f(i)$	4	1	0	1	0	4	4	16	1			
$type$	T_4	E_1	P	V_3	E_0	T_1	E_3	V_4	E_4			

1. The correspondence between the selector notation and the homogeneous coordinates for points and lines is

i	I^i	i^*
0	1	$6^* : 1, 2, 4,$
1	I	$1^* : 0, 2, 6,$
2	I^2	$0^* : 0, 1, 3,$
3	$I + 1$	$5^* : 2, 3, 5,$
4	$I^2 + I$	$3^* : 0, 4, 5,$
5	$I^2 + I + 1$	$4^* : 3, 4, 6,$
6	$I^2 + 1$	$2^* : 1, 5, 6.$

2. The matrix representation is

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

and the equation satisfied by the fixed points is $(X_0 + X_1)^2 = 0$.

3. The degenerate conic through 0, 1, 2 and 5 with tangent 5^* at 5, is represented by the matrix

$$N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

The polar of 0 is 0^* , of 1 is 0^* , of 2 is 5^* , of 4 is 4^* , of 5 is 5^* of 6 is 6^* and of 3 is undefined. The equation in homogeneous coordinates is $X_0(X_1 + X_2) = 0$.

4. A circle with center 14 can be constructed as follows. I first observe that a direction must be orthogonal to itself. Indeed, if 0 is a direction, the others form an angle 1,2,3,4 mod 5, we cannot play favorites and must choose 0. If $A_0 = 1$, $C \times A_0$ and therefore the tangent has direction 0, $A_0 \times A_{i+1}$ has direction $i \pmod{5}$ or are the points 0, 7, 8, 2, 11.

It is natural to choose the pentagonal face-point as 14, and the edge-points on the pentagon as 0, 8, 11, 7, 2. The points on the circle 1, 6, 3, 15, 19 are chosen as the vertex-points opposite the corresponding edge-point, 1 opposite 0, 6 opposite 8, This gives the types, with subscripts indicated in 0. and the definition:

The points are represented on the 5-anti-prism as follows. The pentagonal face-point, P , the 5 triangular face-points, T_i , the 5 vertex-points, V_i , the 5 triangular-triangular edge-points, E_i , the 5 pentagonal-triangular edge-points F_i .

The lines are represented on the 5-anti-prism as follows. The pentagonal face-line, f , which is incident to F_i , the 5 triangular face-lines, t_i , which are incident to F_i , F_i , T_{i+1} , T_{i-1} , E_{i+2} , E_{i-2} . If f is the pentagonal edge of t_i and V , V' are on f , F_i is on it, T_{i+1} (T_{i-1}) share V (V'), E_{i+2} (E_{i-2}) are on an edge through V (V') not on t_i

the 5 vertex-lines, v_i , which are incident to

F_i , V_{i+2} , V_{i-2} , E_{i+1} , E_{i-1} . If t is the face with v_i on its pentagonal edge these are all the vertices, and edge-points on it distinct from v_i .

the 5 triangular-triangular edge-lines, e_i , which are incident to F_i , T_{i+2} , T_{i-2} , V_{i+1} , V_{i-1} . V_{i+1} and V_{i-1} are on the same edge as e_i , the line which joins the center C of the antiprism to E_i is parallel to the edge containing F_i , T_{i+2} and T_{i-2} are the triangular faces which are not adjacent to E_i or F_i .

the 5 pentagonal-triangular edge-lines. f_i , which are incident to P , T_i , V_i , E_i , F_i . T_i is adjacent to f_i , V_i is opposite f_i , E_i joined to the center of the antiprism is parallel to T_i .

Answer to 2.3.3.

For $p = 3$,

0. The primitive polynomial giving the selector 0, 1, 3, 9 is $I^3 - I - 1$.

1. The correspondence between the selector notation and the homogeneous coordinates for points and lines is

i	I^i	i^*
0	1	12^* : 1, 2, 4, 10,
1	I	1^* : 0, 2, 8, 12,
2	I^2	0^* : 0, 1, 3, 9,
3	$I + 1$	7^* : 2, 6, 7, 9,
4	$I^2 + I$	3^* : 0, 6, 10, 11,
5	$I^2 + I + 1$	4^* : 5, 9, 10, 12,
6	$I^2 + 2I + 1$	10^* : 3, 4, 6, 12,
7	$I_2 + I + 2$	6^* : 3, 7, 8, 10,
8	$I^2 + 1$	2^* : 1, 7, 11, 12,
9	$I + 2$	11^* : 2, 3, 5, 11
10	$I_2 + 2I$	9^* : 0, 4, 5, 7,
11	$I^2 + 2I + 2$	5^* : 4, 8, 9, 11,
12	$I^2 + 2$	8^* : 1, 5, 6, 8.

2. The matrix representation of the polarity i to i^* is

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix}.$$

The equation satisfied by the fixed points is $X_0^2 + X_1^2 + 2X_2X_0 = 0$.

3. The degenerate conic through 0, 1, 2 and 5 with tangent 4^* at 5, is obtained by constructing the quadrangle-quadrilateral configuration starting with $P = 5$ and $Q_i = \{0, 1, 2\}$. We obtain $q_i = \{3^*, 2^*, 7^*\}$, which are the tangents at Q_i . The matrix representation is

$$N = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \text{ with equation } X_1X_2 + X_2X_0 + X_0X_1 = 0.$$

We can check that the polar of $10 = 3^* \times 4^*$ is $9^* = 0 \times 5$.

Answer to 2.3.8.

0. For $q = 2^2$, the primitive polynomial giving the selector 0, 1, 4, 14, 16 is $I^3 - I^2 - I - \epsilon$, with

$$\epsilon^2 + \epsilon + 1 = 0.$$

1. The correspondence between the selector notation and the homogeneous coordinates are as follows, i^* has the homogeneous coordinates associated with I^i .

i	I^i	i^*
0	1	20^*
1	I	14^*
2	I^2	0^*
3	$I^2 + I + \epsilon$	10^*
4	$I + \epsilon$	${}^219^*$
5	$I^2 + \epsilon$	${}^2I4^*$
6	$I^2 + \epsilon$	${}^2I + 118^*$
7	$I^2 + 1$	15^*
8	$I^2 + \epsilon$	3^*
9	$I^2 + \epsilon^2 I + \epsilon$	5^*
10	$I^2 + \epsilon I + 1$	9^*
11	$I^2 + \epsilon^2$	13^*
12	$I^2 + \epsilon I + \epsilon$	11^*
13	$I^2 + I + \epsilon^2$	6^*
14	$I + 1$	2^*
15	$I^2 + I$	1^*
16	$I + \epsilon$	12^*
17	$I^2 + \epsilon I$	16^*
18	$I^2 + \epsilon I + \epsilon^2$	17^*
19	$I^2 + \epsilon^2 I + \epsilon^2$	8^*
20	$I^2 + I + 1$	7^*

To obtain the last column, for row 9, $[1, \epsilon^2, \epsilon] = (1, 1, 1) \times (1, \epsilon, 0) = 20 \times 17 = 5^*$.

2. The correspondence i to i^* is a polarity whose fixed points are on a line. The matrix representation is obtained by using the image of 4 points.

$$0 = (0, 0, 1), M(0) = 0^* = [1, 0, 0],$$

$$\begin{aligned} 1 &= (0,1,0), M(1) = 1^* = [1, 1, 0], \\ 2 &= (1,0,0), M(2) = 2^* = [0, 1, 1], \\ 18 &= (1, \epsilon, \epsilon^2), M(18) = 18^* = [1, \epsilon^2, 1]. \end{aligned}$$

The first 3 conditions give the polarity matrix as

The last condition gives $\beta\epsilon + \alpha\epsilon^2 = 1$, $\gamma + \beta\epsilon = \epsilon^2$, $\gamma = 1$. Hence $\gamma = 1$, $\beta = 1$, $\alpha = 1$.

Therefore

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note that M is real and could have been obtained from the reality and non singularity conditions, giving directly $\alpha = \beta = \gamma = 1$.

The polar of (X_0, X_1, X_2) is $[X_1 + X_2, X_0 + X_1, X_0]$.

The fixed points (X_0, X_1, X_2) satisfy $X_1^2 = 0$ corresponding to 14^* .

3. A point conic with no points on 14 is 1, 3, 4, 5,13,
the corresponding line conic is 15,19,10,16, 8.
Projecting from 1 and 3, 1, 3, 5,13, 4,
we get the fundamental projectivity, 8, 2,11, 0, 7 on 14^* .

4. To illustrate Pascal's Theorem, because there are only 5 points on a conic, we need to use the degenerate case. The conic through 0, 1, 2 and the conjugate points 9 and 18 is The last condition gives $\beta\epsilon + \alpha\epsilon^2 = 1$, $\gamma + \beta\epsilon = \epsilon^2$, $\gamma = 1$.

Hence $\gamma = 1$, $\beta = 1$, $\alpha = 1$. Therefore

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, M^{-1} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Note that M is real and could have been obtained from the reality and non singularity conditions, giving directly $\alpha = \beta = \gamma = 1$.

The polar of (X_0, X_1, X_2) is $[X_1 + X_2, X_0 + X_1, X_0]$.

The fixed points (X, X_1, X_2) satisfy $X_1^2 = 0$ corresponding to 14^* .

5. A point conic with no points on 14 is 1, 3, 4, 5,13,

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

The tangents at $(0,0,1)$, $(0,1,0)$, $(1,0,0)$, $(1, \epsilon^2, \epsilon)$, $(1, \epsilon, \epsilon^2)$ are $[1,1,0]$, $[1,0,1]$, $[0,1,1]$, $[1, \epsilon^2, \epsilon)$, $(1, \epsilon, \epsilon^2]$, or 1^* , 15^* , 2^* , 5^* , 17^* . On the other hand, using Pascal's Theorem, the tangent at 0 is given by

$$\begin{aligned} &(((0 \times 1) \times (9 \times 18)) \times ((18 \times 0) \times (1 \times 2))) \times (2 \times 9) \times 0 \\ &= (((0^* \times 7^*) \times (4^* \times 20^*)) \times 12^*) \times 0 \\ &= (((14 \times 17) = 8^*) \times 12^* \text{ or } 13) \times 0 = 1^*. \end{aligned}$$

Answer to

2.3.8.

For $q = 57$, choose the auto-correlates as point on a circle although 0 is on the circle draw as it is the center. With the succession of points X_i ,

$x_i = 0 \times X_i$	36,	1,	52,	43,	3,	32,	13,
X_i	16,	35,	18,	50,	29,	26,	30,
$y_{i+1} = X_{i-1} \times X_{i+1}$	22,	42,	8,	14,	10,	28,	44,
$y_{i+2} = X_{i-2} \times X_{i+2}$	34,	2,	41,	17,	40,	20,	23,
$y_{i+3} = X_{i-3} \times X_{i+3}$	7,	31,	6,	27,	54,	25,	39,
$y_{i+1} \times x_i$	21,	51,	5,	46,	33,	4,	45,
$y_{i+2} \times x_i$	24,	56,	48,	15,	49,	38,	47,
$y_{i+3} \times x_i$	53,	12,	37,	9,	55,	11,	19.

This gives all the points in the projective plane of order 7. We observe

16*	21*	24*	53*	22*	34*	7*
36	36	36	36	36	36	36
16				35, 30	18, 26	50, 29
42, 44	22	8, 28		14, 10		
41, 20		34	17, 40		2, 23	
27, 54	31, 39		7			6, 25
		46, 33	5, 4	21		51, 45
	15, 49		56, 47	48, 38	24	
	37, 11	12, 19			9, 55	53
35*	51*	56*	12*	42*	2*31*	
1	1	1	1	1	1	1
35				16, 18	50, 30	29, 26
22, 8	42	14, 44		10, 28		
17, 23		2	40, 20		34, 41	
54, 25	7, 6		31			27, 39
		33, 4	46, 45	51		21, 5
	49, 38		24, 48	15, 47	56	
	9, 19	53, 37			55, 11	12
18*	5*48*	37*	8*14*	6*		
52	52	52	52	52	52	52
18				35, 50	16, 29	26, 30
42, 14	8	22, 10		28, 44		
34, 40		41	20, 23		2, 17	
25, 39	31, 27		6			7, 54
		4, 45	21, 33	5		51, 46
	38, 47		56, 15	24, 49	48	
	53, 55	12, 9			11, 19	37

Answer to

2.3.8.

For $q = 2^3$,

36 :	0	37	38	40	44	52	18	27	68	1*	3*	7*	2*	4*	5*
$36 \times 0 = 0^*$:	0	1	3	7	15	31	36	54	63	0	0	0	1	3	31
$36 \times 37 = 37^*$:	17	26	36	37	39	43	51	67	72	72	51	67	72	72	26
$36 \times 38 = 38^*$:	16	25	35	36	38	42	50	66	71	35	71	66	71	50	71
$36 \times 40 = 40^*$:	14	23	33	34	36	40	48	64	69	14	33	69	34	69	69
$36 \times 44 = 44^*$:	10	19	29	30	32	36	44	60	65	30	60	29	29	32	10
$36 \times 52 = 52^*$:	2	11	21	22	24	28	36	52	57	2	28	24	52	11	2
$36 \times 18 = 18^*$:	13	18	36	45	55	56	58	62	70	62	70	56	13	70	58
$36 \times 27 = 27^*$:	4	9	27	36	46	47	49	53	61	53	4	47	61	27	49
$36 \times 68 = 68^*$:	5	6	8	12	20	36	41	59	68	6	12	8	5	59	68

Conic with no point on 36: 2, 4, 5, 6, 13, 28, 31, 46, 63

line conic: 29, 59, 31, 9, 18, 43, 28, 35, 64.

Fundamental projectivity: from 2 and 5 on the conic, the points

2, 5, 6, 31, 13, 28, 4, 46, 63 give the points on 36^* :

38, 0, 68, 27, 52, 37, 40, 18, 44.

Chapter 4

FINITE INVOLUTIVE SYMPATHIC AND GALILEAN GEOMETRY

4.0 Introduction.

In part II, I have given a construction of a finite projective geometry associated to a prime p . In it, there is no notion of parallelism, equality of segments or of angles, perpendicularity, etc . I have then obtained the well known finite affine geometry. In it, we have the notion of parallel lines, equality of segments on a given line or on parallel lines, but we have no circles, no notion of equality on non parallel lines, no perpendicularity, etc . It is the purpose of Part III to construct a finite Euclidean geometry in which these notions as well as measure of angles and distances can be obtained.

In the first step, which I will call *involutive geometry*, I choose an involution on the ideal line. This involution either is elliptic, in which case it has no real fixed points or is hyperbolic, in which case it has 2 real fixed points. The elliptic case resembles more the standard Euclidean geometry, while the hyperbolic case is easier to deal with, but the properties of both geometries go hand in hand. In it we define circles and perpendicularity. A principle of compensation, which is not evident in the classical case, makes its appearance. For instance, if we consider the lines through the center of a circle, half of them do not intersect the circle, but the other half do and then at two points. As an other example, not all triangles have an inscribed circle, only roughly one in 4 has, but these have 4 inscribed circles. In the involutive geometry, I also define the equality of angles and the equality of segments.

In the second step, I will introduce the *sympathic geometry*, in which we have the notion of measure of angle. The algebraic development suggests a finite trigonometry. In fact 2 such trigonometries are required for each prime, corresponding to the elliptic and to the hyperbolic case. The trigonometry for the elliptic case is obtained easily from the notion of primitive roots associated to p . The trigonometry for the hyperbolic case, requires a generalization.

In the last step, I introduce the notion of measure of distances and obtain the *finite Euclidean geometry*.

¹G30.TEX [MPAP], September 9, 2019

4.1 Finite involutive geometry.

4.1.9 Theorems in finite involutive Geometry, which do not correspond to known theorems in Euclidean Geometry.

The Theorems in finite Euclidean Geometry fall also in several categories. The first one, ...

The theorems are a direct consequence of ...

The proof follows by assuming like in section ... that m corresponds to the line at infinity and The reference in parenthesis is to the section i_l in Theorem

Theorem.

0. Let $M1 \times H2$ meet $A1 \times A2$ in $C0, \dots$, then the points $C0, C1$ and $C2$ are on the same line p .
1. Let $H1M2$ meet $A1A2$ in $D0, \dots$, then the points $D0, D1$ and $D2$ are on the same line q .
2. The intersection P of p and q is on the line eul of Euler.

Proof: Use AA1, 3.0, 3.1, with $H0 = \overline{M}_0$, $M0 = M_0$, $C0 = C_0$, $D0 = C_0$, $p = p$ and $q = \overline{p}$.

4.1.10 The geometry of the triangle of degree 2.

... Involves problems of the second degree, bisectrices, inscribed circles for even triangles.

4.1.11 Some theorems involving circles.

Introduction.

It is not my intention to develop here the extensive theory on circles for involutive geometry over arbitrary fields. I will simply give an example which illustrates how the problem can be approached effectively.

Definition.

Let θ be a defining circle and m , the ideal line, any circle γ can be written as

$$\gamma = \theta + (m) \times (r),$$

where $(r) = [r_0, r_1, r_2]$ is a given constant times the radical axis with θ . The 3 dimensional representation of the circle γ is defined by the point, with coordinates r_0, r_1 and r_2 . I will write $(\mathbf{r})_3 := (r_0, r_1, r_2)_3$ for that representation. θ is represented by the origin. A degenerate circle $(m) \times (r)$ is represented by the direction of r .

Exercise.

What is the representation of tangent circles.

Lemma.

If γ_0 and γ_1 are circles, represented by $(\mathbf{r}_0)_3$ and $(\mathbf{r}_1)_3$, then the family of circles through their intersections is represented by

$$(\mathbf{r}_0)_3 + k(\mathbf{r}_1)_3,$$

with k an arbitrary element in the field together with ∞ , where ∞ represents γ_1 . The addition is that of vectors in 3 dimensions and the multiplication by k the scalar multiplication.

I will also denote the family by

$$\gamma_0 + k\gamma_1.$$

One can also use the homogeneous representation,

$$k_0\gamma_0 + k_1\gamma_1.$$

Strictly speaking, this is the representation used in the proofs, although I have used the non homogeneous representation to simplify the writing.

Theorem. [Bundle]

Let γ_j , $j = 0$ to 3 , be 4 circles, if there is a circle α which passes through the intersection of the circles γ_0 and γ_1 , as well as the intersection of γ_2 and γ_3 , then there is a circle β passing through the intersections of γ_0 and γ_2 , as well as those of γ_1 and γ_3 .

This is the so called *bundle Theorem*.¹

Proof: If $(\mathbf{r}_j)_3$ is the representation of γ_j . The family through the first 2 circles is represented by $(\mathbf{r}_0)_3 + k(\mathbf{r}_1)_3$ and that through the last 2 circles by

$(\mathbf{r}_2)_3 + l(\mathbf{r}_3)_3$, the hypothesis concerning the circle α implies

$$(\mathbf{r}_0)_3 + k(\mathbf{r}_1)_3 = u((\mathbf{r}_2)_3 + l(\mathbf{r}_3)_3), \text{ which can be rewritten}$$

$$(\mathbf{r}_0)_3 + u(\mathbf{r}_2)_3 = -k((\mathbf{r}_2)_3 + ul(\mathbf{r}_3)_3), \text{ which gives the conclusion concerning the circle}$$

β .

4.1.12 The parabola, ellipse and hyperbola.**Introduction.**

The parabola, ellipse and hyperbola have already be defined in affine geometry. Here we study their properties in involutive geometry.

The parabola.

The ellipse and hyperbola.

If we assume that the isotropic points are $(\delta, 1, 0)$ and $(-\delta, 1, 0)$, where $\delta^2 = d = N p$, we will see that by an appropriate ... transformation, these can be reduced to

$$\frac{X_0^2}{A} + \frac{X_1^2}{B} = X_2^2.$$

Recall also that $i^2 = -1$.

Definition.

The isotropic tangents are isotropic lines tangent to the conic. The foci are the intersection of 2 isotropic tangents through 2 different isotropic points.

¹see Dembosky, p. 256

Theorem.

Given the conic

$$\frac{x_0^2}{A} + \frac{x_1^2}{B} = X^2.$$

D0. $C = A + Bd$,
then

C0. The point polarity is

$$\begin{pmatrix} B & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & -AB \end{pmatrix}$$

C1. The line polarity is

$$\begin{pmatrix} A & 0 & 0 \\ 0 & B & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

C2. The isotropic tangents through $(\delta, 1, 0)$ are
 $(1, -\delta, \sqrt{C})$ and $(1, -\delta, -\sqrt{C})$

C3. The foci are

C3.0. $(-\sqrt{C}, 0, 1), (\sqrt{C}, 0, 1),$

C3.1. $(0, -\sqrt{C}, \delta), (0, \sqrt{C}, \delta),$

C4.0. $C = Rp \Rightarrow$ the foci C3.0. are real, the foci C3.1. are not.

C4.1. $C = Np \Rightarrow$ the foci C3.1. are real, the foci C3.0. are not.

Theorem.

Given the conic

$$D0. \quad \frac{x_0^2}{A} + \frac{x_1^2}{B} = X^2.$$

H1.0. $A = Rp, B = Rp,$

D1.0. $a = \sqrt{A}, b = \sqrt{B},$

H1.1. $A = Np, B = Np,$

D1.1. $a = \sqrt{\frac{A}{d}}, b = \sqrt{\frac{B}{d}},$

H1.2. $A = Rp, B = Np,$

D1.2. $a = \sqrt{A}, b = \sqrt{\frac{B}{d}},$

H1.3. $A = Np, B = Rp,$

D1.3. $a = \sqrt{\frac{A}{d}}$, $b = \sqrt{B}$, then the conic takes the form

C1.0. $\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$,

C1.1. $d\frac{x^2}{a^2} + d\frac{y^2}{b^2} = 1$,

C1.2. $\frac{x^2}{a^2} + d\frac{y^2}{b^2} = 1$,

C1.3. $d\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$,

Theorem.

H0.0. $p \equiv -1 \pmod{4}$ and $AB = Rp$,
or

H0.1. $p \equiv 1 \pmod{4}$ and $AB = Np$,
then

C0. the conic is an ellipse,

Theorem.

H0.0. $p \equiv 1 \pmod{4}$ and $AB = Rp$,
or

H0.1. $p \equiv -1 \pmod{4}$ and $AB = Np$,
then

C0. the conic is a hyperbola.
The ideal points on it are

C1.0. $(\frac{a}{b}i, 1, 0), (-\frac{a}{b}i, 1, 0)$,

C1.1. $(\frac{a}{b}, 1, 0), (-\frac{a}{b}, 1, 0)$.

4.1.13 Cartesian coordinates in involutive Geometry.

Introduction.

Notation.

A pair of reals between parenthesis will denote the Cartesian coordinates of a point. We cannot choose a pair of reals between brackets to denote the x and y intercept of a line in the Cartesian plane, because we have then no way to represent lines through the origin. We will therefore use triplets, with the last non zero coordinate normalized to 1.

Theorem.

If we choose as x axis the line $[0,1,0]$ and as y axis $[1,0,0]$, then we have the correspondence:

$$\begin{aligned} C(i, j, 1) &= (i, j), \\ C[i, j, k] &= [\frac{i}{k}, \frac{j}{k}, 1], k \neq 0, \\ C[i, j, 0] &= [\frac{i}{j}, 1, 0], j \neq 0, \\ C[i, 0, 0] &= [1, 0, 0]. \end{aligned}$$

Theorem.

Given a triangle whose vertices have the Cartesian coordinates

$$(0, a), (b, 0), (c, 0), a \neq 0, b \neq c.$$

0. The point whose barycentric coordinates are (q_0, q_1, q_2) , with $q_0 + q_1 + q_2 \neq 0$, corresponds to the point whose Cartesian coordinates are $(\frac{bq_1 + cq_2}{q_0 + q_1 + q_2}, \frac{aq_0}{q_0 + q_1 + q_2})$.

REDO 1. IN view of the preceding theorem

1. The line, distinct from the ideal line, whose barycentric coordinates are

$$[l_0, l_1, l_2]$$

corresponds to the line whose intercepts are

$$\frac{bl_2 - cl_1}{l_2 - l_1}, \frac{bl_2 - cl_1}{(c-b)l_0 - cl_1 + bl_2},$$

if $bl_2 - cl_1 = 0$

and $((c-b)l_0 - cl_1 + bl_2) \neq 0$, it corresponds to

$$0, \frac{l_2 - l_1}{(c-b)l_0 - cl_1 + bl_2},$$

and $((c-b)l_0 - cl_1 + bl_2) = 0$, it corresponds to

$$1, 0,$$

2. The values of the coordinates of the orthocenter are $m_0 = bc(b-c), m_1 = c(a^2 + bc), m_2 = -b(a^2 + bc)$.

Definition. 3

The following mapping associates to the non ideal points in the finite Euclidean plane associated to p , points in the classical Euclidean plane.

$$T(i, j) = (i + kp, j + lp), \text{ where } k \text{ and } l \text{ are any integers.}$$

Theorem.

Let $d = i_1j_2 - i_2j_1$, then $(i_1, j_1)x(i_2, j_2) = [\frac{j_1 - j_2}{d}, \frac{i_2 - i_1}{d}, 1], d \neq 0,$

$$(i_1, j_1)x(i_2, j_2) = [\frac{j_1 - j_2}{i_2 - i_1}, 1, 0], d = 0, i_2 \neq i_1,$$

$$(i_1, j_1)x(i_2, j_2) = [1, 0, 0], d = 0, i_2 = i_1, j_2 \neq j_1.$$

For the following see ..[1,135]/cartes

Example.

For $p = 13$, let the circles be

$$\text{Cr: } x^2 + y^2 = r^2.$$

The points on the circles are

$$\text{C1: } (1, 0), (-1, 0), (0, 1), (0, -1), (6, 2), (-6, 2), (6, -2), (-6, -2), (2, 6), (-2, 6), (2, -6), (-2, -6),$$

$$\text{C2: } (2, 0), (-2, 0), (0, 2), (0, -2), (4, 1), (-4, 1), (4, -1), (-4, -1), (1, 4), (-1, 4), (1, -4), (-1, -4),$$

$$\text{C3: } (3, 0), (-3, 0), (0, 3), (0, -3), (6, 5), (-6, 5), (6, -5), (-6, -5), (5, 6), (-5, 6), (5, -6), (-5, -6),$$

$$\text{C4: } (4, 0), (-4, 0), (0, 4), (0, -4), (5, 2), (-5, 2), (5, -2), (-5, -2), (2, 5), (-2, 5), (2, -5), (-2, -5),$$

$$\text{C5: } (5, 0), (-5, 0), (0, 5), (0, -5), (4, 3), (-4, 3), (4, -3), (-4, -3), (3, 4), (-3, 4), (3, -4), (-3, -4),$$

$$\text{C6: } (6, 0), (-6, 0), (0, 6), (0, -6), (3, 1), (-3, 1), (3, -1), (-3, -1), (1, 3), (-1, 3), (1, -3), (-1, -3),$$

The isotropic lines through the origin contain the points:

$$\text{i0: } (0, 0), (1, -5), (2, 3), (3, -2), (4, 6), (5, 1), (6, -4), \\ (-1, 5), (-2, -3), (-3, 2), (-4, -6), (-5, -1), (-6, 4),$$

$$\text{i1: } (0, 0), (1, 5), (2, -3), (3, 2), (4, -6), (5, -1), (6, 4), \\ (-1, -5), (-2, 3), (-3, -2), (-4, 6), (-5, 1), (-6, -4),$$

If we join the origin to the points $(1, k)$ and $(1, l)$ we obtain perpendicular directions, with $k, l = 0, \infty; 1, -1; 2, 6; 3, 4; -2, -6; -3, -4$.

For $p = 13$, let the circles be

$$\text{Cr: } x^2 - 6xy + y^2 = r^2.$$

The points on the circles are

$$\text{C1: } (0, 1), (1, 0), (1, 6), (4, 4), (4, -6), (6, 1), (6, -4),$$

$$\text{C2: } (0, 2), (1, -2), (1, -5), (2, 0), (2, -1), (5, 5), (5, -1),$$

$$\text{C3: } (0, 3), (1, 1), (1, 5), (3, 0), (3, 5), (5, 1), (5, 3),$$

$$\text{C4: } (0, 4), (2, 3), (2, -4), (3, 2), (3, 3), (4, 0), (4, -2),$$

$$\text{C5: } (0, 5), (4, 5), (4, 6), (5, 0), (5, 4), (6, 4), (6, 6),$$

$$\text{C6: } (0, 6), (2, 2), (2, -3), (3, -2), (3, -6), (6, 0), (6, -3),$$

as well as the points symmetric with respect to the origin.

If we join the origin to the points $(1, k)$ and $(1, l)$ we obtain perpendicular directions, with $k, l = 0, -4; 1, -1; 2, -5; 3, \infty; 4, -2; 5, -6; 6, -3$.

For $p = 11$, let the circles be

$$\text{Cr: } exx^2 - 4xy + y^2 = r^2.$$

The points on the circles are

$$\text{C1: } (0, 1), (1, 4), (4, 4),$$

C2: $(0, 2), (2, -3), (3, 3),$

C3: $(0, 3), (1, 1), (1, 3),$

C4: $(0, 4), (4, 5), (5, 5),$

C5: $(0, 5), (2, 2), (2, -5),$

as well as the points symmetric with respect to the diagonals, (i, j) here means $(i, j), (j, i), (-i, -j), (-j, -i).$

The isotropic points are

l0: $\text{ex}(0, 0), (1, 3), (1, 4), (2, -3), (2, -5), (3, -2), (3, 1),$
 $(4, 1), (4, 5), (5, -2), (5, 4),$

l1: $\text{ex}(0, 0), (1, -3), (1, -4), (2, 3), (2, 5), (3, 2), (3, -1),$
 $(4, -1), (4, -5), (5, 2), (5, -4),$

If we join the origin to the points $(1, k)$ and $(1, l)$ we obtain perpendicular directions, with $k, l = 0, -5; 1, -1; 2, \infty; 3, 5; 4, -2.$

For $p = 11$, let the circles be

Cr: $\text{ex}x^2 + y^2 = r^2.$

The points on the circles are

C1: $(0, 1), (3, 5),$

C2: $(0, 2), (1, 5),$

C3: $(0, 3), (2, 4),$

C4: $(0, 4), (1, 2),$

C5: $(0, 5), (3, 4),$

as well as the points symmetric with respect to the 2 axis and the diagonals.

(i, j) here means $(i, j), (i, -j), (j, i), (j, -i), (-i, -j), (-i, j), (-j, -i), (-j, i).$

If we join the origin to the points $(1, k)$ and $(1, l)$ we obtain perpendicular directions, with $k, l = 0, \infty; 1, -1; 2, 5; 3, -4; 4, -3; -2, -5.$

4.1.14 Correspondence between circles in finite and classical Euclidean geometry.

Introduction.

Theorem.

To the point (x, y) , in classical geometry, on a circle centered at the origin and of radius r , corresponds, if r is not congruent to 0 modulo p , the point $(x/r \bmod p, y/r \bmod p)$ on a circle of radius 1 in the finite geometry associated to p .

Vice-versa, given a point $P = (x, y)$ on a circle of radius 1 in the finite geometry associated to p , we can always find a point on a circle in the classical geometry which is one of the representatives of P , in the mapping given in

The proof is left to the reader. The first part is trivial, the second part is not trivial. See also [135]FINPYT.BAS

Example.

For $p = 13$,

(2,6) for $r = 1$ is associated to (15,20) for $r = 25$.

For $p = 29$,

(5,11) for $r = 1$ is associated to (24,18) for $r = 30$.

(8,13) for $r = 1$ is associated to (108,45) for $r = 117$.

(6,9) for $r = 1$ is associated to (180,96) for $r = 204$.

Theorem.

There exist a circle of radius u in R^2 which contains all the representatives of a circle in Z_p^2 . Indeed, for the radius 1, for instance, if one of the representatives is on the circle $x^2 + y^2 = r_1^2$ and if $s_1 = 1/r_1$, then

$$u = r_i(s_i + k_i p), \text{ for all } i,$$

by finite induction, if

$$u = r_1(s_1 + p k_1) = r_2(s_2 + p k_2),$$

then

$$r_1 k_1 - r_2 k_2 = (r_2 s_2 - r_1 s_1)/p,$$

this gives

$$k_1 = a_1 + r_2 k'_2 \text{ and with } s'_2 = (s_1 + a_1 p)/r_2,$$

$$u = r_1 r_2 (s'_2 + p k'_2), \dots$$

Example.

For $p = 29$, for $r = 1$, we start with

point in Z_{29}^2 r_i s_i

5,11 5 6

8,13 13 9

6,9 25 7

then

$$5k_1 - 13k_2 = 3, a_1 = -2, s'_2 = -4,$$

$$u = 5.13(-4 + 29k'_2),$$

$$13k'_2 - 5k_3 = 3, a_2 = 1, s'_3 = 5,$$

$$u = 5.13.5(5 + 29k'_3),$$

hence the suitable circle in R^2 with smallest radii has radius $u = 1625$ and contains the points

in R^2 in Z_{29}^2

-1300,-975 5,11;

-1500,-625 8,13;

-1560,-455 6,9.

4.1.15 Answers to problems.

Answer to 1.13.1.

For the second part.

The problem can be restated successively as follows, given a solution of

0. $x^2 + y^2 = z^2$, there exist i, j, k such that $(x + ip)^2 + (y + jp)^2 = (z + kp)^2$, or there exist u and v such that

$$u^2 - v^2 = x, 2uv = y, u^2 + v^2 = z,$$

eliminating v from the first 2 equations and using 0., gives

$$u^2 = \frac{r+x}{2}, v^2 = \frac{r-x}{2},$$

$\frac{r+x}{2}$ need not be a quadratic residue, therefore we use instead

$$u^2 = b\frac{r+x}{2}, v^2 = b\frac{r-x}{2}, c = 1/b,$$

this gives u and v ,

$$x + ip = (u^2 - v^2)c, y + ip = 2uvc, z + ip = (u^2 + v^2)c.$$

A more careful discussion will show that signs may have to be changed and the role of x and y interchanged.

For instance, for $p = 13$ and $2^2 + 6^2 = 1^2$, $b = -2$, $c = 6$, $u^2 = (-5)(-2) = 6^2$, $v^2 = (6)(-2) = 1^2$, hence $x + ip = 35$, $-(y + jp) = 72$, $z + kp = 222$.

For $p = 17$, and $x = 4$, $y = 6$, $z = 1$, $b = 3$, $c = 6$, $u^2 = (6)(3) = 1^2$, $v^2 = (12)(3) = 2^2$, hence after interchange of x and y , $x + ip = 72$, $y + jp = 210$, $z + kp = 222$.

For $p = 19$ and $3^2 + 7^2 = 1^2$, $b = 2$, $c = 10$, $u^2 = (2)(2) = 2^2$, $v^2 = (-1)(2) = 6^2$, hence $-(x + ip) = 320$, $-(y + jp) = 240$, $z + kp = 400$.

(AFTER INVOLUTIVE GEOMETRY)

Comment.

For the following theorem, I will not give a linear construction, although one could be given. The theorem is a generalization of the Theorem of Miquel and can be further generalized in the context of Gaussian geometry.

Notation.

If u and v are 2 lines and ξ is a conic,

$$\xi - u \times v = 0,$$

is equivalent to

$$\xi(X) - (u \cdot X)(v \cdot X) = 0.$$

This should be moved before the definition of circles.

Theorem.

The radical axis of the 2 circles

$$\mu_j := \theta - m \times u_j, j = 0, 1$$

is $u_1 - u_0$.

Indeed, $\mu_1(X) - \mu_0(X) = -(m \cdot X)((u_1 - u_0) \cdot X) = 0$ therefore

$$\mu_1 = \mu_0 - m \times (u_1 - u_0).$$

Theorem.

The radical axis of each pair of 3 circles are concurrent.

Proof: Let the 3 circles be

$$\mu_i := \theta - m \times u_i,$$

u_i are the radical axis of these circles with θ .

the 3 radical axis are $u_2 - u_1$, $u_0 - u_2$, $u_1 - u_0$, but $u_2 - u_1 = (u_0 - u_2) + (u_1 - u_0)$, therefore one of the axis passes through the intersections of the other 2.

Theorem. [Miquel]

$$H0. \quad N_i \cdot a_i = 0,$$

$$H1. \quad N_i \cdot m \neq 0,$$

$$D0. \quad \mu_i := \text{circle}(A_i, N_{i+1}, N_{i-1}),$$

$$D1. \quad \text{Miquel} := (\mu_1 \times \mu_2) - N_0,$$

then

$$C0. \quad \text{Miquel} \times \mu_0 = 0.$$

The nomenclature.

N0. Miquel is called the *point of Miquel associated to N_i* .

Proof. Let

$$N_0 = (0, 1, q_0), N_1 = (q_1, 0, 1), N_2 = (1, q_2, 0).$$

H1. implies that $1 + q_i \neq 0$.

If the equation of μ_0 a circle is

$$\theta - m \times u_0 = 0, \text{ with } u_0 = [u_{0,0}, u_{0,1}, u_{0,2}],$$

$$m = [1, 1, 1]$$

and

$$\theta = m'_0 X_1 X_2 + m'_1 X_2 X_0 + m'_2 X_0 X_1$$

$$m = [1, 1, 1]. \text{ with } m'_0 = m_0(m_1 + m_2), \dots$$

D0. implies, for $i = 0$,

$$u_0 = [0, \frac{m'_2}{1+q_2}, \frac{q_1 m'_1}{1+q_1}].$$

Let $\text{Miquel} = (X_0, X_1, X_2)$. If the 3 circles have a point in common, it is on the intersection of the 3 radical axis u_i , it is therefore necessary that

$$(u_i - u_{i+1}) \cdot \text{Miquel} = 0, i = 0, 1, 2,$$

therefore

$$\text{Miquel} = (u_1 - u_2) \times (u_2 - u_0),$$

this gives after simplification,

$$\text{Miquel} = (\frac{m'_0}{1+q_0} (\frac{-q_0 m'_0}{1+q_0} + \frac{q_0 q_1 m'_1}{1+q_1} + \frac{m'_2}{1+q_2}, \dots).$$

It remains to verify that Miquel belongs to μ_i .

$$\text{First, } u_i \cdot \text{Miquel} = m'_0 m'_1 m'_2 \frac{1+q_0 q_1 q_2}{1+q_0} (1+q_1)(1+q_2),$$

$$\text{second, } m \cdot \text{Miquel} = -\frac{q_0 m'_0 m'_0}{(1+q_0)^2} + \dots + m'_1 m'_2 \frac{1+q_1 q_2}{(1+q_1)(1+q_2)} + \dots$$

It is straightforward to verify that the product of these two expressions is precisely $m'_0 X_1 X_2 + m'_1 X_2 X_0 + m'_2 X_0 X_1$.

Theorem. [Miquel]

$$H0. \quad n := N_1 \times N_2, \quad n \cdot N_0 = 0.$$

$$D0. \quad n = [n_0, n_1, n_2],$$

then

$$C0. \quad Miquel \cdot \theta = 0.$$

$$C1. \quad q_0 = -\frac{n_1}{n_2}, \quad q_1 = -\frac{n_2}{n_0}, \quad q_2 = -\frac{n_0}{n_1}.$$

$$C2. \quad Miquel = \left(\frac{n_1 n_2 m'_0}{n_1 - n_2}, \frac{n_2 n_0 m'_1}{n_2 - n_0}, \frac{n_0 n_1 m'_2}{n_0 - n_1} \right).$$

The condition that the points N_i be collinear is precisely $1 + q_0 q_1 q_2 = 0$, but in this case $\theta = 0$ as follows from the expression $u_i \cdot Miquel$. It is straightforward to verify C1 and C2.

Corollary.

0. The circles μf_i circumscribed to $A_i, \overline{M}A_{i+1}, \overline{M}A_{i-1}$ have a point \overline{Fock} in common.

1. \overline{Fock} is in the circumcircle θ .

$$2. \quad \mu f_i = \theta + m \times \left[0, \frac{m_2 m_0 (m_0 + m_1)}{m_0 - m_1}, -\frac{m_2 m_0 (m_0 + m_1)}{m_0 - m_1} \right].$$

$$3. \quad \overline{Fock} = (m_0(m_1 + m_2)(m_2 - m_0)(m_0 - m_1), m_1(m_2 + m_0)(m_0 - m_1)(m_1 - m_2), m_2(m_0 + m_1)(m_1 - m_2)(m_2 - m_0)).^4$$

This is the special case when n is the orthic line $\overline{m} = [m_0, m_1, m_2]$.

The point \overline{Fock} had been constructed before (D38.9) and proven to be on θ (C38.4).

Theorem. [Miquel]

$$D0. \quad N_{i,j} := \text{midpoint}(A_i, N_j),$$

$$D1. \quad n_{i,j} := \text{mediatrix}(A_i, N_j),$$

$$D2. \quad C_i := n_{i,i+1} \times n_{i,i-1},$$

$$D3. \quad \phi := \text{circle}(C_0, C_1, C_2),$$

then

$$C0. \quad O \cdot \phi = 0.$$

Proof:

$$P0. \quad N_{0,1} = (1 + 2q_1, 0, 1), \quad N_{0,2} = (2 + q_2, q_2, 0).$$

$$P1. \quad n_{0,1} = [m_2 + m_0, m_0 - (1 + 2q_1)m_2, -(1 + 2q_1)(m_2 + m_0)],$$

$$n_{0,2} = [-q_2(m_0 + m_1), (2 + q_2)(m_0 + m_1), (2 + q_2)m_1 - q_2 m_0].$$

$$P2. \quad C_0 = (m_0(1 + 2q_1 + q_1 q_2)m_0 + (2 + q_2)(1 + q_1)m_1 + (1 + 2q_1)(1 + q_2)m_2, \\ (m_2 + m_0)((1 + q_1)m_0 + (q_1 q_2 - 1)m_1), \\ (m_0 + m_1)((1 - q_1 q_2)m_2 + (1 + q_2)m_0).$$

$$P3. \quad \phi : \dots$$

Problem.

The following question suggests itself. Let

$$\nu := \text{circle}(N_0, N_1, N_2).$$

What relation exists between all circles ν having the same point of Miquel?

Same question in the case for which the point of Miquel is on θ .

Theorem . . . states that all the circles are lines and . . . that one of these lines is that of Simson and Wallace. Again what is the relation between these lines?

Theorem. [Simson and Wallace]

- H0. $X \cdot \theta = 0,$
D0. $n_i := X \times Im_i,$
D1. $N_i := n_i \times a_i,$
D2. $n := N_1 \times N_2,$
then
C0. $N_0 \cdot n = 0(*).$
C1. $(W \times N_i) \perp a_i.?$

Proof:

- P0. $n_0 = [m1X_2 - m2X_1, (m1 + m2)X_2 + m2X_0, -m1X_0 - (m1 + m2)X_1].$
P1. $N_0 = (0, m1X_0 + (m1 + m2)X_1, m2X_0 + (m1 + m2)X_2).$
P2. $n = [X_1X_2(-m0X_0 + (m1 + m2)(X_1 + X_2)),$
 $X_2X_0(-m1X_1 + (m2 + m0)(X_2 + X_0)),$
 $X_0X_1(-m2X_2 + (m0 + m1)(X_0 + X_1))].$

To obtain the last expression we use in each coordinate the relation H0,
 $m0(m1 + m2)X_1X_2 + m1(m2 + m0)X_2X_0 + m2(m0 + m1)X_0X_1 = 0.$

MAY WANT TO REFER HERE TO THE FOLLOWING BUT MOVE IT AS APPLICATION OF PARABOLAS.

Theorem.

The set of lines having the same point X of Miquel are on a line parabola⁵:

- C0. $mup^{-1}(X) :$
 $X_0u0(u1 - u2)/m'_0 = X_1u1(u2 - u0)/m'_1 = X_2u2(u0 - u1)/m'_2.$
 $\mu p(X) : (X_1X_2m'_0U_0)^2 + (X_2X_0m'_1U_1)^2 + (X_0X_1m'_2U_2)^2$
 $-2X_0X_1X_2(X_0m'_1m'_2U_1U_2 + X_1m'_2m'_0U_2U_0 + X_2m'_0m'_1U_0U_1).$
C1. $a_i \cdot \mu p(X) = 0.$
C2. *The line of Simson and Wallace is the tangent at the vertex.*
C3. *The point of Miquel is its focus.*

Proof. C2 of Theorem . . . gives C0.

4.1.9 The conic of Kiepert.

Introduction.

The conic of Kiepert has been constructed in 5.4.1.D3.8.⁶

Kiepert showed that, in the classical case, if V_i is a point on the mediatrix mf_i such that

$$\text{angle}(A_1, A_2, V_0) = \text{angle}(A_2, A_0, V_1) = \text{angle}(A_0, A_1, V_2),$$

then $v_i := A_i \times V_i$ have a point V in common which is on a hyperbola, now known as the

⁵30.12.82

⁶13.1.83

hyperbola of Kiepert. After proving this Theorem in the finite case, I will consider several special cases of interest, which can be obtained either by a linear or by a second degree construction. In the latter case, if the angle is $\frac{\pi}{4}$, the point is called the point of Vectem, to which is associated a special chapter of the classical theory of the geometry of the triangle. The cases when the angle is $\frac{\pi}{3}$ and $\frac{\pi}{6}$ are also discussed and a new property is obtained.

Theorem.

*Let*⁷

$$\text{H0.0. } X \cdot \theta = 0.$$

$$\text{G0.0. } X = (X_0, X_1, X_2).$$

$$\text{D1.0. } x1 := A_1 \times X,$$

$$\text{P1.0. } x1 = [X_2, 0, -X_0],$$

$$\text{D1.1. } V_0 := x1 \times mf_0,$$

$$\text{P1.1. } V_0 = ((m1 + m2)X_0, (m1 + m2)X_2 - (m1 - m2)X_0, (m1 + m2)X_0).$$

$$\text{D1.2. } v_0 := A_0 \times V_0,$$

$$\text{P1.2. } v_0 = [0, (m1 + m2)X_2, (m1 - m2)X_0 - (m1 + m2)X_2].$$

$$\text{D1.3. } x2 := A_2 \times V_0,$$

$$\text{P1.3. } x2 = [(m1 + m2)X_2 - (m1 - m2)X_0, -(m1 + m2)X_0, 0].$$

$$\text{D1.4. } x3 := Ma_0 \times X,$$

$$\text{P1.3. } x3 = [-X_1 - X_2, X_0, X_0].$$

$$\text{D1.5. } Y = x2 \times x3.$$

$$\text{P1.4. } Y = ((m1 + m2)X_0, (m1 + m2)X_2 - (m1 - m2)X_0, (m1 - m2)X_0 + (m1 + m2)X_1)$$

$$\text{D2.0. } x4 := A_0 \times X,$$

$$\text{P2.0. } x4 = [0, X_2, -X_1].$$

$$\text{D2.1. } X1 := x4 \times m,$$

$$\text{P2.1. } X1 = (X_1 + X_2, -X_1, -X_2).$$

$$\text{D2.2. } x5 := A_2 \times X1,$$

$$\text{P2.2. } x5 = [X_1, X_1 + X_2, 0].$$

$$\text{D2.3. } V_1 := mf_1 \times x5,$$

$$\text{P2.3. } V_1 = ((m2 + m0)(X_1 + X_2), (m2 + m0)X_1, 2m2X_1 + (m2 + m0)X_2).$$

$$\text{D2.4. } v_1 := A_1 \times v_1,$$

$$\text{P2.4. } v_1 = [2m2X_1 + (m2 + m0)X_2, 0, -(m2 + m0)(X_1 + X_2)].$$

$$\text{D3.0. } y4 := A_0 \times Y,$$

$$\text{P3.0. } y4 = [0, Y_2, -Y_1].$$

$$\text{D3.1. } Y1 := y4 \times m,$$

$$\text{P3.1. } Y1 = (Y_1 + Y_2, -Y_1, -Y_2).$$

$$\text{D3.2. } y5 := A_1 \times Y1,$$

$$\text{P3.2. } y5 = [Y_2, 0, Y_1 + Y_2].$$

$$\text{D3.3. } V_2 := mf_1 \times y5,$$

$$\text{P3.3. } V_2 = ((m0 + m1)(Y_1 + Y_2), (m0 + m1)Y_1 + 2m1Y_2, -(m0 + m1)Y_2).$$

$$\text{D3.4. } v_2 := A_2 \times V_2,$$

$$\text{P3.5. } v_2 = [(m0 + m1)Y_1 + 2m1Y_2, -(m0 + m1)(Y_1 + Y_2), 0].$$

$$\text{D4.0. } V = v_0 \times v_1,$$

$$\begin{aligned} \text{P4.0. } V = & (u(X_1 + X_2), \\ & (m2+m0)((m0-m1)(m1-m2)X_0 - 2m1(m1+m2)X_1 + uX_2, & 2m2(m0+ \\ & m1)(m1+m2)X_1 + uX_2), \\ & \text{where} \\ & u := (m1+m2)(m2+m0)(m0+m1). \\ & \text{then} \end{aligned}$$

$$\text{C0.0. } V \cdot v_2 = 0.$$

$$\text{C0.1. } V \cdot \kappa_{iepert} = 0.$$

The construction is based on

$$\text{angle}(X, A_1, A_2) = \text{angle}(A_1, A_2, Y) = \text{angle}(X, A_0, A_2) = \text{angle}(A_0, A_2, V_1),$$

implying the parallelism of $A_0 \times X$ and $A_2 \times V_1$ and symmetrically for V_2 .

For P4.0., after replacing Y_0 , Y_1 and Y_2 by their values from P1.4., the equation for θ is used to express X_0X_1 in terms of X_2X_0 and X_1X_2 .

Exercise.

To complete the proof of x.x.1., the 2 special case $X = A_0$ and $X = A_1$ should be considered. This is left as an exercise.

In the first case $x4$ should be replaced by the tangent ta_0 at A , in the second case $x1$ should be replaced by the tangent ta_1 at A_1 .

Exercise.

Proceed in the inverse order and construct X from V . Prove that if V is on *Kiepert* then X is on θ .

Exercise.

Study the projectivity which associates to (X_0, X_1, X_2) , the point (V_0, V_1, V_2) , as given by P4.0. without assuming that (X_0, X_1, X_2) is on θ . Determine 4 points and their images and construct any of these points if they have not been constructed in this book.

The following are special cases.

$$X = A_2, \alpha = 0 \text{ gives } V = M.$$

$$\sigma = \frac{\pi}{2} \text{ gives } V = \overline{M}.$$

$$\sigma = \frac{\pi}{4} \text{ gives the point of Vectem (see below).}$$

$$\sigma = \frac{\pi}{3} \text{ gives the equilateral point (see below) } \sigma = \frac{\pi}{6} \text{ gives the hexagonal point (see below)}$$

$$\sigma = \text{angle}(A_{i-1}, A_i, A_{i+1}) \text{ gives } V = A_i.$$

Other angles give $V = Tar.$ (5.4.1.D16.3.), $V = Br0.$ (5.4.1.D15.3.) $V = \overline{Br}0.$ (5.4.1.D15.3.) and $V = En.$ (5.4.1.D21.10)

$$D5.0. \quad Ma\overline{m}_i := ma_{i+1} \times \overline{m}a_{i-1}, \quad \overline{M}a\overline{m}_i := \overline{m}a_{i+1} \times ma_{i-1},$$

$$D5.1. \quad Ae_i := a_i \times e,$$

$$D5.2. \quad mae_i := Ae_{i+1} \times Ma\overline{m}_{i-1}, \quad \overline{m}ae_i := Ae_{i+1} \times \overline{M}a\overline{m}_{i-1},$$

$$D5.3. \quad MMa_i := mae_i \times a_i, \quad \overline{M}Ma_i := \overline{m}ae_i \times a_i,$$

$$D5.4. \quad mm := MMa_1 \times MMa_2, \quad \overline{m}m := \overline{M}Ma_1 \times \overline{M}Ma_2, \\ \text{then}$$

$$C5.0. \quad n_i \cdot Kiepert1 = 0.$$

$$C5.1. \quad mm \cdot Kiepert1 = \overline{m}m \cdot Kiepert1 = 0.$$

$$C5.2. \quad mm \cdot K = \overline{m}m \cdot K = 0.$$

$$C5.3. \quad]S \text{ is the center of Kiepert1, } \overline{S} \text{ is the cocenter}^8.$$

The nomenclature:

Proof.

$$P5.0. \quad Ma\overline{m}_0 = (m0, m1, m0), \quad \overline{M}a\overline{m}_0 = (m0, m0, m2),$$

$$P5.1. \quad Ae_0 = (0, m0 - m1, m0 - m2),$$

$$P5.2. \quad mae_0 = [m2(m1 - m2), m1(m2 - m0), m2(m0 - m1)], \\ \overline{m}ae_0 = [m1(m2 - m1), m2(m0 - m2), m1(m1 - m0)],$$

⁸15.1.83

$$\begin{aligned} \text{P5.3. } MMa_0 &= (0, m2(m0 - m1), m1(m0 - m2)), \\ \overline{M}Ma_0 &= (0, m1(m1 - m0), m2(m2 - m0)), \end{aligned}$$

$$\begin{aligned} \text{P5.4. } mm &= [m0(m1 - m2), m1(m2 - m0), m2(m0 - m1)], \\ \overline{m}m &= [m1m2(m1 - m2), m2m0(m2 - m0), m0m1(m0 - m1)], \end{aligned}$$

The tangent at Tar is

$$[m1m2q0^2(m2 - m1), m2m0q1^2(m0 - m2), m0m1q2^2(m1 - m0)].$$

The tangent at $Br0$ is

$$[m0^3(m1 + m2)^2(m1 - m2), m1^3(m2 + m0)^2(m2 - m0), m2^3(m0 + m1)^2(m0 - m1)].$$

The tangent at $\overline{B}r0$ is

$$[m1m2(m1 + m2)^2(m1 - m2), m2m0(m2 + m0)^2(m2 - m0), m0m1(m0 + m1)^2(m0 - m1)].$$

Example.

With $p = 13$, $A[] = (14, 1, 0)$, $M = (28)$, $\overline{M} = (44)$, $Ma\overline{m}_0 = (41, 29, 70)$, $\overline{M}a\overline{m}_0 = (31, 42, 106)$, $Ae_0 = (4, 25, 79)$, $mae_0 = [138, 81, 145]$, $\overline{m}ae_0 = [151, 84, 141]$, $MMa_0 = (9, 20, 131)$, $\overline{M}Ma_0 = (7, 19, 144)$, $mm = [146]$, $\overline{m}m = [136]$,
 $V = (\frac{a}{\sin(A-\alpha)}, \frac{b}{\sin(B-\alpha)}, \frac{c}{\sin(C-\alpha)})$.

Theorem.

If $V^\sigma = (V_0, V_1, V_2)$ is associated with the angle σ , then

$$\begin{aligned} V^{-\sigma} &= ((m1 - m2)(m2 + m0)(m0 + m1)V_0 + 2m0(m1 + m2)(m2 - m0)V_1 \\ &\quad + 2m0(m0 - m1)(m1 + m2)V_2, \\ &\quad 2m1(m1 - m2)(m2 + m0)V_0 + (m2 - m0)(m0 + m1)(m1 + m2)V_1 \\ &\quad + 2m1(m2 + m0)(m0 - m1)V_2) + 2m2(m0 + m1)(m1 - m2)V_0, \\ &\quad 2m2(m2 - m0)(m0 + m1)V_1 + (m0 - m1)(m1 + m2)(m2 + m0)V_2). \end{aligned}$$

Proof:

$$v_i := V \times A_i, v_0 = [0, V_2, -V_1].$$

$$V_i := v_i \times mf_i,$$

$$V_0 = ((m1 + m2)(V_2 - V_1), (m1 - m2)V_1, (m1 - m2)V_2).$$

$$va_i = A_{i+1} \times V_{i-1},$$

$$va_0 = [(m0 + m1)(V_0 - V_1), 0, (m0 - m1)V_0].$$

$$v\overline{a}_i = A_{i-1} \times V_{i+1},$$

$$v\overline{a}_0 = [(m2 + m0)(V_2 - V_0), (m2 - m0)V_0, 0].$$

$$Va_i = m \times va_i,$$

$$Va_0 = ((m0 - m1)V_0, 2m1V_0 - (m0 + m1)V_1, -(m0 + m1)(V_0 - V_1)).$$

$$V\overline{a}_i = m \times v\overline{a}_i,$$

$$V\overline{a}_0 = ((m2 - m0)V_0, (m2 + m0)(V_2 - V_0), -2m2V_0 + (m2 + m0)V_2).$$

$$vb_i := Va_i \times A_i,$$

$$Vb_0 = [0, (m0 + m1)(V_0 - V_1), 2m1V_0 - (m0 + m1)V_1].$$

$$v\overline{b}_i := V\overline{a}_i \times A_i,$$

$$v\overline{b}_0 = [0, 2m2V_0 - (m2 + m0)V_2, (m2 + m0)(V_2 - V_0)].$$

$$\begin{aligned}
V_i^{-\sigma} &:= vb_{i+1} \times v\bar{b}_{i-1}, \\
V_0^{-\sigma} &= ((m1 + m2)(V_2 - V_1), 2m1V_2 - (m1 + m2)V_1, -2m2V_1 + (m1 + m2)V_2). \\
v_i^{-\sigma} &:= V_i^{-\sigma} \times A_i, \\
v_0^{-\sigma} &= [0, 2m2V_1 - (m1 + m2)V_2, 2m1V_2 - (m1 + m2)V_1]. \\
V^{-\sigma} &= v_1^{-\sigma} \times v_2^{-\sigma}, \\
V^{-\sigma} \cdot v_0^{-\sigma} &= 0(*).
\end{aligned}$$

For the determination of $V^{-\sigma}$, I have multiplied the components by $m1 - m2$ and used the property that V^σ is on *kiepert* to eliminate V_1V_2 . Every component is then divisible by V_0 .

Example.

$$\begin{aligned}
p &= 11, \bar{M} = (1, 2, 4), \\
V^\sigma &= (1, -5, -4), V^{-\sigma} = (1, 4, 3), \\
V_i &= \{(1, -2, 5), (1, 1, -4), (1, -5, -4), \} \\
V_i^- &= \{(1, 5, 1), (1, 4, 3), (1, 4, 2), \} \\
\text{the sides of these triangles are} \\
vv_i &= \{[1, 0, 3], [0, 1, 7], [1, 3, 1], \} \quad vv_i^- = \{[1, -3, 0], [1, -2, -2], [0, 1, -5]\}. \quad vv_i \times vv_i^- = \\
&\{(1, 4, -4), (1, -4, -1), (1, -1, 2), \} \text{ which have } [1, 4, 7] \text{ in common.}
\end{aligned}$$

Exercise

. x.x.x. defines a projectivity which fixes the conic of *kiepert*. Determine other properties of this projectivity.

Exercise.

Construct $V^{\frac{\pi}{2}-\sigma}$ and $V^{\frac{\pi}{2}+\sigma}$ and obtain properties involving these points and V^σ , $V^{-\sigma}$ and lines derived from these.

4.1.10 The Theorem of Vectem and related results.

Introduction.

In classical Euclidean Geometry, the construction of the point of Vectem starts with that of squares on the sides of the triangle, outside of it. In the finite case, there is ambiguity and the squares need not exist. It is easy to determine the intersections of the circle κ_1 with the perpendicular through A_1 to a_0 . This leads to the expression for $X_{1,0}$ given below. To insure the consistency associated to the outside condition of the classical case I have started with that definition for $X_{1,0}$, chosen $X_{2,0}$ on $\bar{\kappa}_2$ and the perpendicular at A_2 to a_0 in such a way that $X_{1,0} \times X_{2,0}$ is parallel to a_0 . $X_{2,1}$, $X_{0,2}$ and $X_{0,1}$, $X_{1,2}$, are defined using the symmetry operation ρ , defined in section ????. Because α is obtained in section ????. using a square root operation the definitions can be repeated using $-\alpha$ instead of α , the corresponding elements are denoted with a superscript -. These have been given explicitly. The conclusions have not been written explicitly. To each conclusion (and

proof) corresponds an other one by exchanging no superscript with the superscript $-$ and α by $-\alpha$.

Explicit expression for distances and area, if needed, are given using the same notation as in the conclusions, replacing C by F.

One could also proceed by first choosing one of the intersections of κ_1 with $A_1 \times I\overline{m}a_0$ as $X_{1,0}$ and constructing all the other points. For instance, $X_{2,0}$ by $(A_2 \times I\overline{m}a_0) \times X_{1,0} \times MA_0$, $X_{0,1}$ by $(A_0 \times I\overline{m}a_1) \times (\overline{m}a_2 \times (A_0 \times X_{1,0}))$, etc.

Theorem.

$$\text{H0.0. } X_{1,0} := (m0(m1 + m2), \alpha - m0m1, -m2m0), X_{1+i,i} := \rho^i X_{1,0}, X_{2,0} := (m0(m1 + m2), -m0m1, \alpha - m2m0), X_{2+i,i} := \rho^i X_{2,0},$$

$$\text{H0.1. } X_{1,0}^- := (m0(m1 + m2), -\alpha - m0m1, -m2m0), X_{1+i,i}^- := \rho^i X_{1,0}^-, X_{2,0}^- := (m0(m1 + m2), -m0m1, -\alpha - m2m0), X_{2+i,i}^- := \rho^i X_{2,0}^-,$$

$$\text{D0.1. } x_{i,j,k} := A_i \times X_{j,k}, i \neq k. x_{i,j,k}^- := A_i \times X_{j,k}^-, i \neq k.$$

$$\text{D0.2. } V_i := x_{i+1,i-1,i} \times x_{i-1,i+1,i}, V_i^- := x_{i+1,i-1,i}^- \times x_{i-1,i+1,i}^-,$$

$$\text{D0.3. } W_i := x_{i+1,i,i+1} \times x_{i-1,i,i-1}, W_i^- := x_{i+1,i,i+1}^- \times x_{i-1,i,i-1}^-,$$

$$\text{D0.4. } U_i := x_{i+1,i-1,i+1} \times x_{i-1,i+1,i-1}, U_i^- := x_{i+1,i-1,i+1}^- \times x_{i-1,i+1,i-1}^-,$$

$$\text{D0.5. } v_i := A_i v V_i, v_i^- := A_i \times V_i^-,$$

$$\text{D0.6. } w_i := X_{i+1,i-1} \times X_{i-1,i+1}, w_i^- := X_{i+1,i-1}^- \times X_{i-1,i+1}^-,$$

$$\text{D0.7. } V := v_1 \times v_2, V^- := v_1^- \times v_2^-,$$

$$\text{D0.8. } v := V \times V^-.$$

$$\text{D1.0. } Ix_{i,j,k} := m \times x_{i,j,k}, j \neq k.$$

$$\text{D1.1. } Iv_i = m \times v_i,$$

$$\text{D1.2. } Iw_i = m \times w_i, \\ \text{then}$$

$$\text{C0.0. } (X_{i+1,i} \times X_{i-1,i}) \cdot MA_i = 0.$$

$$\text{C0.1. } V \cdot v_0 = 0(*).$$

$$\text{C0.2. } U_i \cdot \overline{m}a_i = 0.$$

$$\text{C0.3. } W_i \cdot w_i = 0.$$

$$\text{C0.4. } W_i \cdot v_i = 0.$$

$$\text{C0.5. } V_i^- \cdot w_i = 0.$$

$$\text{C0.6. } x_{i+1,i,i+1} x_{i-1,i,i-1}.$$

$$\text{C0.7. } v_i \cdot w_i.$$

$$\text{C0.8. } \text{dist}^2(A_{i+1}, X_{i+1,i}) = \text{dist}^2(A_{i-1}, X_{i-1,i}) = \text{dist}^2(A_{i+1}, A_{i-1}).$$

$$\text{C0.9. } \text{dist}^2(A_{i+1}, X_{i,i+1}) = \text{dist}^2(A_{i-1}, X_{i,i-1}).$$

$$\text{C0.10. } \text{dist}^2(A_i, V_i) = \text{dist}^2(V_{i+1}, V_{i-1}).$$

$$\text{C0.11. } \text{Area}(A_i, X_{i,i+1}, X_{i,i-1}) = \text{Area}(A_0, A_1, A_2).$$

$$\begin{aligned} \text{P0.1. } x_{0,0,1} &= [0, m2, m2 + m0]. \\ x_{0,0,2} &= [0, m0 + m1, m1]. \\ x_{0,2,0} &= [0, \alpha - m2m0, m0m1]. \\ x_{0,1,0} &= [0, m2m0, \alpha - m0m1]. \\ x_{0,2,1} &= [0, m1m2 - \alpha, m1(m2 + m0)]. \\ x_{0,1,2} &= [0, m2(m0 + m1), m1m2 - \alpha]. \end{aligned}$$

$$\text{P0.2. } V_0 = (m0(m1 + m2), \alpha - m0m1, \alpha - m2m0).$$

$$\text{P0.3. } W_0 = (m0(m1 + m2)\alpha - m0m1m2(s_1 + m0), m1m2(\alpha - m0m1), m1m2(\alpha - m2m0)).$$

$$\text{P0.4. } U_0 = (-m0m1m2, m1(\alpha - m1m2), m2(\alpha - m1m2)).$$

$$\text{P0.5. } v_0 = [0, m2m0 - \alpha, \alpha - m0m1].$$

$$\text{P0.6. } w_0 = [2m1m2\alpha, m2m0(m1s_1 - \alpha), m0m1(m2s_1 - \alpha)].$$

$$\text{P0.7. } V = ((\alpha - m2m0)(\alpha - m0m1), (\alpha - m0m1)(\alpha - m1m2), (\alpha - m1m2)(\alpha - m2m0)).$$

$$\text{P0.8. } v = [(m1 - m2)(m0s_1 - m1m2), (m2 - m0)(m1s_1 - m2m0), (m0 - m1)(m0s_1 - m1m2)].$$

$$\begin{aligned} \text{F0.6. } \text{dist}^2(A_0, X_{2,0}) &= 2\alpha - 2m0m1 - m2(m0 + m1). \\ \text{dist}^2(A_0, X_{1,0}) &= 2\alpha - 2m2m0 - m1(m2 + m0). \end{aligned}$$

$$\begin{aligned} \text{P1.0. } Ix_{0,0,1} &= (m0, -(m2 + m0), m2). \\ Ix_{0,0,2} &= (m0, m1, -(m0 + m1)). \\ Ix_{0,2,0} &= (\alpha - m0(m1 + m2), m0m1, m2m0 - \alpha). \\ Ix_{0,1,0} &= (m0(m1 + m2) - \alpha, \alpha - m0m1, -m2m0). \\ Ix_{0,2,1} &= (\alpha - m1(2m2 + m0), m1(m2 + m0), m1m2 - \alpha). \\ Ix_{0,1,2} &= (m2m0 + \alpha, m1m2 - \alpha, -m2(m0 + m1)). \end{aligned}$$

$$\text{P1.1. } Iv_0 = (m0(m1 + m2) - 2\alpha, \alpha - m0m1, 4 - m2m0).$$

$$\text{P1.2. } Iw_0 = (m0(m1 - m2)\alpha, m1(m2m0s_1 - (2m2 + m0)\alpha, m2((2m1 + m0)\alpha - m0m1s_1)).$$

The nomenclature:

Theorem.

0. $2Area(A_1, A_2, X_{2,1}) = -m_0m_1$.
1. $2Area(A_1, A_2, X_{0,1}) = \alpha - m_0m_1$.
2. $dist^2(V_1, V_2) =$

Comment.

The isotropic points are real if $-\alpha$ is a quadratic residue (5.5.2.) if $p \equiv 1 \pmod{4}$, there are $p - 1$ ordinary points on any circle and $\pi = p - 1$ is divisible by 4, therefore a square can be constructed, the diagonals forming the angle $\frac{\pi}{4}$ with the sides, this is consistent with the fact that $X_{i,j}$ are integers. If α is imaginary and $p \equiv -1 \pmod{4}$, then $\pi = p + 1$ is divisible by 4 and the same situation exist.

The equilateral and hexagonal points.

Let $\beta = \frac{\alpha}{\sqrt{3}}$,

$$\begin{aligned} \text{H0.0. } V_i^e &= \kappa_{i+1} \times \kappa_{i-1}, \\ V_0^e &= (m_0(m_1 + m_2), \beta - m_0m_1, \beta - m_2m_0). \end{aligned}$$

$$\begin{aligned} \text{D0.0. } vea_i &:= V_{i+1} \times A_{i-1}, \\ vea_0 &= [m_1(m_2 + m_0), m_0m_1 - \beta, 0]. \\ ve\bar{a}_i &:= V_{i-1} \times A_{i+1}, \\ ve\bar{a}_0 &= [m_2(m_0 + m_1), 0, m_2m_0 - \beta]. \end{aligned}$$

$$\begin{aligned} \text{D0.1. } Vea_i &:= vea_{i+1} \times MA_{i-1}, \\ Vea_0 &= (\beta - m_0m_1, m_1(m_2 + m_0), m_1m_2 + \beta). \\ Ve\bar{a}_i &:= ve\bar{a}_{i-1} \times MA_{i+1}, \\ Ve\bar{a}_0 &= (\beta - m_2m_0, -m_1m_2 - \beta, m_2(m_0 + m_1)). \end{aligned}$$

$$\begin{aligned} \text{D0.2. } veb_i &:= Vea_{i+1} \times M_{i-1}, \\ veb_0 &= [m_2(m_0 + m_1), -m_2(m_0 + m_1), 2\beta + m_2(m_0 - m_1)]. \\ veb_i &:= Ve\bar{a}_{i-1} \times M_{i+1}, \\ veb_0 &= [m_1(m_2 + m_0), 2\beta - m_1(m_2 - m_0), -m_1(m_2 + m_0)]. \end{aligned}$$

$$\begin{aligned} \text{D0.3. } Veb_i &:= veb_i \times ve\bar{a}_i, \\ Veb_0 &= (\beta - m_2m_0, 3\beta - m_1m_2, m_2(m_0 + m_1)). \\ Ve\bar{b}_i &:= veb_i \times vea_i, \\ Ve\bar{b}_0 &= (\beta - m_0m_1, m_1(m_2 + m_0), 3\beta - m_1m_2). \end{aligned}$$

$$\begin{aligned} \text{D0.4. } vec_i &:= vVeb_i \times A_i, \\ vec_0 &= [0, -m_2(m_0 + m_1), 3\beta - m_1m_2]. \\ ve\bar{c}_i &:= vVe\bar{b}_i \times A_i, \\ ve\bar{c}_0 &= [0, 3\beta - m_1m_2, -m_1(m_2 + m_0)]. \end{aligned}$$

- D0.5. $V_i^h := vec_{i+1} \times ve\bar{c}_{i-}$,
 $V_0^h = (m0(m1 + m2), 3\beta - m0m1, 3\beta - m2m0)$.
- D1.0 $vve_i := V_{i+1}^e \times V_{i-1}^e$,
 $vve_0 = [\beta + m1m2, 2\beta - m2(m0 + m1), 2\beta - m1(m2 + m0)]$.
- D1.1. $vvh_i := V_{i+1}^h \times V_{i-1}^h$,
 $vvh_0 = [m1m2 - \beta, 2\beta - m2(m0 + m1), 2\beta - m1(m2 + m0)]$.
- D1.2. $Veh_i := vve_i \times vvh_i$,
 $Veh_0 = (0, -(2\beta - m1(m2 + m0)), 2\beta - m2 * (m0 + m1))$.
- D1.3. $veh := Veh_1 \times Veh_2$,
 $veh = [(2\beta - m1(m2 + m0))(2\beta - m2(m0 + m1)),$
 $(2\beta - m2(m0 + m1))(2\beta - m0(m1 + m2)),$
 $(2\beta - m0(m1 + m2))(2\beta - m1(m2 + m0))]$.
then

- C0.0. $V_i^e \cdot mf_i = 0$.
- C0.1. $V^e \cdot v_0^e = 0(*)$.
- C0.2. $V^h \cdot \kappa iepert = 0$
- C0.3. $V^h \cdot v_0^h = 0(*)$.
- C0.4. $V^e \cdot \kappa iepert = 0$
- C0.5. $Veh_i \cdot a_i = 0$.
- C0.6. $Veh_0 \cdot veh = 0(*)$.

The nomenclature:

- N0.0. V_i^e are the *equilateral points*, such that
 $angle(V_i^e, A_{i+1}, A_{i-1}) = \frac{\pi}{3}$.
 V_0^e is therefore on κ_{i+1} and κ_{i-1} .
- N0.1. V_i^h are the *hexagonal points*, such that
 $angle(V_i^h, A_{i+1}, A_{i-1}) = \frac{\pi}{6}$.
 V_0^h is therefore the barycenter of the equilateral triangle $(V_i^e, A_{i+1}, A_{i-1})$.

Answer to x.x.4.

- $X = A_0$ gives $V = A_1$,
 $X = A_1$ gives
 $V = ((m2 + m0)(m0 + m1), 2m1(m2 + m0), 2m2(m0 + m1))$,
 $X = A_2$ gives $V = M$.
 $X = (m1 + m2, -(m1 - m2), m1 - m2)$ gives $V = A_2$.

4.1.11 Representation of involutive geometry on the dodecahedron.

Introduction.

When $p = 5$, it is natural to try to represent involutive geometry on the dodecahedron. The most natural choice, for the ideal line, in the hyperbolic case is an edge-line. We can choose two face-points as the isotropic points. In the elliptic case, the simplest choice for the ideal line appears to be a vertex-line. The fundamental involution associates to a vertex-point an edge-point.

Definition.

In the case of hyperbolic involutive geometry, the *isotropic points* are chosen as 2 face-points.

Theorem.

With the chosen fundamental involution, the perpendicular direction of a vertex-point is a vertex point and to an edge-point is an edge-point.

Example.

If the isotropic points are 0 and 4, the perpendicular directions are 10 and 24 as well as 23 and 26.

Theorem.

There are 100 circles in a hyperbolic involutive geometry.

Number of	center	sub – types
2	f	$B, G3; D2, H1.$
2	f	$B, G4; D3, H2.$
2	v	$C1, D4; G1, I3.$
2	v	$C2, D1; G2, I2.$
4	v	$B, H4; G6, G7.$
1	s	$A, E1; E2, I1.$
4	s	$B, I4; F, H3.$
4	s	$C1, D2; D1, G8.$
4	s	$C2, D3; D4, G5.$

Proof: For the type $ffffss$, out of 15 quadruples only 6 contain 2 given ones, therefore the number of conics must be divided by $\frac{15}{6}$.

For the type $fffxxx$, out of 20 triples only 4 contain 2 given ones, hence the number of conics must be divided by $\frac{20}{4} = 5$.

For the type $ffxxxx$, out of 15 pairs, only one is the given one, therefore, the number of conics is to be divided by 15.

As a check there are $25 * 16 * \frac{6}{24} = 100$ conics through 2 given points.

More precisely the conics are

1 of type $ffffff$, sub-type A .

12 of type $ffffss$, sub-type B .

12 of type $fffvvs$, 6 of sub-type $C1$, 6 of sub-type $C2$.

24 of type $fffvss$, 6 each of sub-type $D1$, $D2$, $D3$ and $D4$.

2 of type $ffvvvv$, 1 each of sub-type $E1$, $E2$.

4 of type $ffvvvs$, sub-type F .

24 of type $ffvvss$, 2 each of sub-type $G1$ to $G4$ and 4 each of type $G5$ to $G8$.

12 of type $ffvsss$, 2 each of sub-type $H1$, $H2$ and 4 each of sub-type $H3$, $H4$.

9 of type $ffssss$, 1 of sub-type $I1$, 2 each of sub-type $I2$, $I3$, and 1 of sub-type $I4$.

The centers and their relationship to the conic have been determined using the program [130]DODECA.

Theorem.

In the case of elliptic involutive geometry, if a vertex-line is chosen as the ideal line, there exists an elliptic projectivity which associates, alternately, to a vertex-point, an edge-point and to an edge-point, a vertex-point.

Definition.

The projectivity of Theorem 4.1.11 is chosen as the *fundamental projectivity*.

Example.

We can choose as ideal line 5^* and as fundamental projectivity $(7,13,23,27,29,26)$.

Theorem.

Given a center, there are 4 circles with 6 ordinary points on them. 2 have a diameter in the direction of a ideal face-point and 2 have a diameter in the direction of the other ideal face-point.

Theorem.

There are 100 circles in an elliptic involutive geometry.

Number of	center	sub – types
3	f	$H1, M1; S2, G4$.
3	f	$H2, M4; S1, G3$.
1	v	$A, P; U1, U2$.
6	v	$I4, S5; H3, F$.
3	s	$I2, G1; L1, M3$.
3	s	$I3, G2; L2, M2$.
6	s	$H4, S8; G6, G7$.

Proof: The proof was done using the program [130] EUCLID5 and the interactive program [130] DODECA. The semi colon separates the circles whose diameter have a different ideal face-points.

The details are on G331.PRN.

4.2 Finite Sympathic Geometry.

4.2.0 Introduction.

See Example 1.10 ... Measure of angles, separate from measure of distances,

2 triangles having the same angles are similar, their sides are not equal.

For measure of distances we can do it starting from a unit (2 ordinary distinct points) on all lines which have the same parity (even or odd), the other parity requires an other unit, the two become connected as a subset of sympathic projectivity which is Euclidean geometry.

Although we could have subordinated measure of angles to measure of distance we prefer to do the reverse.

4.2.1 Trigonometry in a Finite Field for p . The Hyperbolic Case.

Introduction.

The trigonometry associated to the finite Euclidean plane with real isotropic points will first be defined and studied in this section for the finite field Z_p . Theorems 1.4. and 1.6. determine $\sin(1)$ and $\cos(1)$ from which all other values can be obtained using the addition formulas. In section 2, definitions and results will be extended, for the finite field associated to p^e , with proofs left as an exercise.

Definition.

Given the sets Z of the integers, Z_p of the integers modulo p , Z_{p-1} of the integers modulo $p-1$, let δ be a square root of a non quadratic residue of p , I define π as follows

$$\pi := p - 1.$$

Therefore $\frac{\pi}{2}$ is an integer.

The problem addressed here is to construct 2 functions *sine* or *sin* and *cosine* or *cos* with domain Z and range $\{Z_p, \delta Z_p\}$ which satisfy:

The Theorem of Pythagoras,

$$0. \sin^2(x) + \cos^2(x) = 1,$$

The addition formulas,

$$1. \sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y),$$

$$2. \cos(x+y) = \cos(x)\cos(y) - \sin(x)\sin(y).$$

The periodicity property

$$1. \sin(2\pi + x) = \sin(x), \cos(2\pi + x) = \cos(x),$$

The symmetry properties

¹G34.TEX [MPAP], September 9, 2019

2. $0. \sin(\pi + x) = -\sin(x), \cos(\pi + x) = -\cos(x),$
 $1. \sin(-x) = -\sin(x), \cos(-x) = \cos(x),$
 $2. \sin(\pi - x) = \sin(x), \cos(\pi - x) = -\cos(x),$
 $3. \sin(\frac{\pi}{2} - x) = \cos(x), \cos(\frac{\pi}{2} - x) = \sin(x),$
 $4. \sin(\frac{\pi}{2} + x) = \cos(x), \cos(\frac{\pi}{2} + x) = -\sin(x),$

and such that

3. $0. \sin(0) = 0, \cos(0) = 1,$
 $1. \sin(\frac{\pi}{2}) = 1, \cos(\frac{\pi}{2}) = 0,$
 $2. \cos(x) \neq 0 \text{ for } 0 < x < \frac{\pi}{2}.$

Theorem.

Let

0. g be a primitive root of p ,
1. $\gamma := \sqrt{g}$,
2. $i := \gamma^{\frac{p-1}{2}}$,
3. $e(j) := \gamma^j$,
4. $\sin(j) = \frac{1}{2i}(e(j) - e(-j)), \cos(j) = \frac{1}{2}(e(j) + e(-j)),$
then
5. $i^2 = -1$ and
satisfy 1.1.0.0. to 1.1.3.2..

Proof. Because g is a primitive root,

$$i^2 = g^{\frac{p-1}{2}} = -1.$$

From the definition of $\sin(j)$ and $\cos(j)$ follows

$$\cos(j) + i\sin(j) = e(j), \cos(j) - i\sin(j) = \frac{1}{e(j)},$$

therefore $\cos(j)^2 + \sin(j)^2 = 1$, hence 1.1.0.0.

From the exponentiation properties follows

$$\begin{aligned} e(j+k) &= \gamma^{j+k} = (\cos(j) + i\sin(j))(\cos(k) + i\sin(k)) \\ &= (\cos(j)\cos(k) - \sin(j)\sin(k)) + i(\cos(j)\sin(k) + \sin(j)\cos(k)), \end{aligned}$$

hence 1.1.0.1. Because of 1. and 5., $e(\frac{\pi}{2}) = \gamma^{\frac{p-1}{2}} = i$, $\frac{1}{e(\frac{\pi}{2})} = -i$, hence 1.1.3.1.

0. implies that $\frac{\pi}{2}$ is the smallest exponent of g which gives -1 ,

hence $\frac{\pi}{2}$ is the smallest exponent of γ which gives $+i$ or $-i$,

therefore 1.1.3.2. The proof of all other properties is left as an exercise.

Theorem.

Assume $p \equiv 1 \pmod{4}$. Let

0. g be a primitive root of p ,

1. $i := g^{\frac{p-1}{4}}, \delta := \gamma = \text{sqr}(g), g' := -g^{\frac{p-3}{2}},$
then
2. $\sin(1) = i^{\frac{g'-1}{2}}\delta, \cos(1) = \frac{g'+1}{2}\delta.$

Proof: $gg' = -g^{\frac{p-1}{2}} = 1, i^2 = g^{\frac{p-1}{2}} = -1.$
 $\delta^{-1} = \delta/g = g'\delta,$

hence

$$\begin{aligned}\sin(1) &= \frac{\delta - \delta^{-1}}{2i} = -i \frac{1 - g'}{2} \delta, \\ \cos(1) &= \frac{\delta + \delta^{-1}}{2} = \frac{1 + g'}{2} \delta.\end{aligned}$$

Theorem.

Assume $p \equiv -1 \pmod{4}$. Let

0. g be a primitive root of p ,
1. $\delta := i$ or $\delta^2 := -1, g' := -g^{\frac{p-3}{4}},$
then
2. $\sin(1) = (g - 1)g'^{\frac{1}{2}}, \cos(1) = (g + 1)g'^{\frac{1}{2}}\delta.$

Proof: $gg'^2 = g^{\frac{p-1}{2}} = -1 = 1/\delta^2$, therefore $\gamma g' = 1/\delta$,
 $\gamma^{-1} = g'\delta$ and $\gamma = gg'\delta$,

hence

$$\begin{aligned}\sin(1) &= \frac{\gamma - \gamma^{-1}}{2i} = \frac{1}{2}(g - 1)g', \\ \cos(1) &= \frac{\gamma + \gamma^{-1}}{2} = \frac{1}{2}(g + 1)g'\delta.\end{aligned}$$

Example.

For $p = 13, g = \delta^2 = 2, i = -5, g' = -6$, then

i	$\sin(i)$	$\cos(i)$	$\tan(i)$
0	0	1	0
1	-2δ	4δ	6
2	-6	-2	3
3	6δ	6δ	1
4	-2	-6	-4
5	4δ	-2δ	-2
6	1	0	∞

For $p = 11, g = 2, g' = -4, \delta^2 = -1$, then

i	$\sin(i)$	$\cos(i)$	$\tan(i)$
0	0	1	0
1	-2	5δ	-4δ
2	2δ	4	-5δ
3	4	2δ	-2δ
4	5δ	-2	3δ
5	1	0	∞

Theorem.

Given a trigonometric table of \sin and \cos , all other $\phi(p-1)$ tables can be obtained by using

$$0. \sin^{(e)}(j) = \sin(je), \cos^{(e)}(j) = \cos(je), (e, p-1) = 1, \\ \text{with } 0 < e < p-1.$$

Proof: We know that there are $\phi(p-1)$ primitive roots. If g^e is an other primitive root, then

$$g^{(e)} = g^e, (e, p-1) = 1, \\ \delta^{(e)} = g^{\frac{e-1}{2}} \delta, \\ \text{for } p \equiv 1 \pmod{4}, i^{(e)} = g^{e\frac{p-1}{4}}, g'^{(e)} = -g^{e\frac{p-3}{2}} \\ \text{for } p \equiv -1 \pmod{4}, g'^{(e)} = -g^{e\frac{p-3}{4}}.$$

Substituting in 2.1.3. and 2.1.4. gives the theorem.

Replacing δ by $-\delta$ gives tables for which $\sin(\frac{\pi}{2}) = -1$.

Example.

For $p = 13$, $g = 2$,

$$e = 5, 7, 11, \\ g^{(e)} = g^e = 6, -2, -6, \\ \delta^{(e)} = 4\delta, -5\delta, 6\delta, \\ i^{(e)} = g^{3e} = -5, 5, 5, \\ g'^{(e)} = -g^{5e} = -2, 6, 2 \\ \sin^{(e)}(1) = 4\delta, -4\delta, 2\delta, \\ \cos^{(e)}(1) = -2\delta, 2\delta, -4\delta.$$

For $e = 5$, $\sin^{(5)}(1) = 5 \cdot \frac{3}{2} \delta^{(e)} = 1\delta^{(e)} = 4\delta$, $\cos^{(5)}(1) = -\frac{1}{2}\delta^{(e)} = 6\delta^{(e)} = -2\delta$.

The tables are:

i	$\sin(i)$	$\cos(i)$	$\tan(i)$
0	0	1	0
1	4δ	-2δ	-2
2	-6	2	-3
3	-6δ	-6δ	1
4	2	-6	4
5	-2δ	4δ	6
6	1	0	∞

4.2.2 Trigonometry in a Finite Field for $q = p^e$. The Hyperbolic Case.

Introduction.

After recalling the definition of Galois fields, for p^2 , I will state the Theorems which generalize 2.1.2., 2.1.3 and 2.1.4.

Definition.

Let n be a non quadratic residue, the *set of elements in the Galois field* p^2 , $GF(p^2)$, are the polynomials of degree 0 or 1, for which addition is performed modulo p and multiplication is performed modulo $I^2 - n$. More specifically

$$(uI + v) + (u'I + v') = (u + u' \bmod p)I + (v + v' \bmod p),$$

$$(uI + v).(u'I + v') = (uv' + u'v \bmod p)I + (vv' + nuu' \bmod p).$$

$$\text{Moreover } (uI + v)^{-1} = \frac{-uI+v}{v^2-nu^2}.$$

More generally, if P is a primitive polynomial of degree n , i.e. a polynomial which has no factors with coefficients in Z_p , the set of elements in the Galois field p^e , $GF(p^e)$, are the polynomials of degree less than e , for which addition is performed modulo p and multiplication is performed modulo P .

Notation.

$uI + v$ will be written $u.v$ or $up + v$.

$tI^2 + uI + v$ will be written $t.u.v$ or $tp^2 + up + v, \dots$

Example.

Let $q = 5^2$, $n = 3$, $g = I + 1 = 1.1 = 6$, then⁹
 $g^{-1} = -2.2 = 3.2 = 17$, $g^2 = 2. - 1 = 2.4 = 14$, $g^4 = 1. - 2 = 1.3 = 8$, $g^6 = 0. - 2 = 0.3 = 3$,
 $g^{12} = 0. - 1 = 0.4 = 4$, hence $-g^{11} = g^{-1}$.

Theorem.

2.1.1. *generalizes for* p^e .

The proof as well as the proof of the other theorems in this section are left as exercises.

Theorem.

Assume $q = p^e \equiv 1 \pmod{4}$. Let

0. g be a primitive root of p^e ,

1. $i := g^{\frac{q-1}{4}}$, $\delta := \text{sqr}(g)$, $g' := -g^{\frac{q-3}{2}}$,
 then

2. $\sin(1) = i(g' - 1)\delta_{\frac{1}{2}}^1$, $\cos(1) = (g' + 1)\delta_{\frac{1}{2}}^1$.

Theorem.

Assume $q = p^e \equiv -1 \pmod{4}$. Let

0. g be a primitive root of p^e ,

⁹26.10.82

1. $g' = -g^{\frac{q-3}{4}}, \delta^2 = -1, g^{-1} = -g^{\frac{q-3}{2}},$
then
2. $\sin(1) = (g-1)g'_{\frac{1}{2}}, \cos(1) = (g+1)g'\delta_{\frac{1}{2}}.$

Example.

For $q = 5^2, n = 3, \delta^2 = g = 6, i = g^6 = 3, g' = -g^{11} = 17,$
 $\sin(1) = 2.4\delta = 14\delta, \cos(1) = 4.4\delta = 24\delta.$
 $\sin(2) = (-1.0).(2.2) - -2. - 1 = 3.4 = 19, \cos^2(1) = (2. - 1).(1.1) = 1.0,$
 $\cos(2) = 2\cos^2(1) - 1 = 2.0 - 0.1 = 2. - 1 = 2.4 = 14.$

This gives the Table:

k	$\sin(k)$	$\cos(k)$
0	0	1
1	14δ	24δ
2	19	14
3	20δ	21δ
4	3	10
5	4δ	12δ
6	20	20
7	12δ	4δ
8	10	3
9	21δ	20δ
10	14	19
11	24δ	14δ
12	1	0

Exercise.

Verify the following and construct the corresponding trigonometric table.

0. For $q = 13^2, n = -2, \delta^2 = g = 15, i = g^{42} = 8, g' = -g^{83} = -147, g^{167} = 35,$
 $\sin(1) = 110\delta, \cos(1) = 18\delta,$
1. For $q = 7^2, n = 3, \delta^2 = -1, g = 8,$
 $\sin(1) = 3.4.\delta = 25\delta, \cos(1) = 2.2\delta = 18\delta,$
2. For $q = 11^2, \delta^2 = 13,$
 $\sin(1) = 0.2\delta = 2\delta, \cos(1) = 8.1\delta = 89\delta,$
3. For $q = 13^2, \delta^2 = 15,$
 $\sin(1) = 11.0\delta = 143\delta, \cos(1) = 3.1\delta = 40\delta,$
4. For $q = 17^2, \delta^2 = 20,$
 $\sin(1) = 11.16\delta = 203\delta, \cos(1) = 7.5\delta = 124\delta,$
5. For $q = 5^3, \delta^2 = 9,$
 $\sin(1) = 3.3.0\delta = 90\delta, \cos(1) = 4.4.1\delta = 121\delta,$
 $\sin(2) = 87, \cos(2) = 110.$

4.2.1 Trigonometry in a Finite Field for p . The Hyperbolic Case.

Introduction.

The trigonometry associated with the finite Euclidean plane with real isotropic points will first be defined and studied in this section for the finite field Z_p . Theorems 4.2.1 and 4.2.1 determine $\sin(1)$ and $\cos(1)$ from which all other values can be obtained using the addition formulas of 4.2.1.

In section 4.2.2, definitions and results will be extended, for the finite field associated with p^e , with proofs left as an exercise.

The trigonometry associated with the finite Euclidean plane with no real isotropic points will be obtained in section 4.2.3, $\sin(1)$ and $\cos(1)$ will be determined, for the general case p^e in 4.2.3 and 4.2.3.

Definition.

Given the sets

Z of the integers,

Z_p of the integers modulo p ,

Z_{p-1} of the integers modulo $p-1$,

let δ be a square root of a non quadratic residue of p .

$$\pi := p - 1.$$

The problem addressed here is to construct 2 functions *sine* or *sin* and *cosine* or *cos* with domain Z and range $\{Z_p \cup \delta Z_p\}$ which satisfy:

The Theorem of Pythagoras,

$$0. \sin^2(x) + \cos^2(x) = 1.$$

The addition formulas,

1. $0. \sin(x + y) = \sin(x)\cos(y) + \cos(x)\sin(y),$
1. $\cos(x + y) = \cos(x)\cos(y) - \sin(x)\sin(y).$

The periodicity property

$$2. \sin(2\pi + x) = \sin(x), \cos(2\pi + x) = \cos(x),$$

The symmetry properties

3. $0. \sin(\pi + x) = -\sin(x), \cos(\pi + x) = -\cos(x),$
1. $\sin(-x) = -\sin(x), \cos(-x) = \cos(x),$
2. $\sin(\pi - x) = \sin(x), \cos(\pi - x) = -\cos(x),$
3. $\sin(\frac{\pi}{2} - x) = \cos(x), \cos(\frac{\pi}{2} - x) = \sin(x),$
4. $\sin(\frac{\pi}{2} + x) = \cos(x), \cos(\frac{\pi}{2} + x) = -\sin(x),$

and such that

¹G35.TEX [MPAP], September 9, 2019

4. 0. $\sin(0) = 0, \cos(0) = 1,$
 1. $\sin(\frac{\pi}{2}) = 1, \cos(\frac{\pi}{2}) = 0,$
 2. $\sin(x) \neq \pm 1$ for $0 < x < \frac{\pi}{2}.$

Theorem.

Let

0. g be a primitive root of $p,$
1. $\gamma := \sqrt{g},$
2. $\iota := \gamma^{\frac{p-1}{2}},$
3. $e(j) := \gamma^j,$
then
4. $\iota^2 = -1$ and
5. $\sin(j) = \frac{e(j)-e(-j)}{2\iota}, \cos(j) = \frac{e(j)+e(-j)}{2},$
satisfy 4.2.1.0 to .4.

Proof. Because g is a primitive root,
 $\iota^2 = g^{\frac{p-1}{2}} = -1.$

From the definition of $\sin(j)$ and $\cos(j)$ follows

$$\cos(j) + \iota \sin(j) = e(j), \cos(j) - \iota \sin(j) = e(j)^{-1},$$

therefore $\cos(j)^2 + \sin(j)^2 = 1,$ hence 4.2.1.0.

From the exponentiation properties follows

$$\begin{aligned} e(j+k) &= \gamma^{(j+k)} = (\cos(j) + \iota \sin(j))(\cos(k) + \iota \sin(k)) \\ &= (\cos(j)\cos(k) - \sin(j)\sin(k)) + \iota(\cos(j)\sin(k) - \sin(j)\cos(k)), \end{aligned}$$

hence 4.2.1.1.

From 5 and 4.2.1.1 follows 4.2.1.3.

0, implies that $\frac{\pi}{2}$ is the smallest exponent of g which gives -1, hence $\frac{\pi}{2}$ is the smallest exponent of γ which gives $+\iota$ or $-\iota$, therefore 4.2.1.4.2. The proof of all other properties is left as an exercise. The next 2 Theorems give $\sin(1)$ and $\cos(1)$ first when $\iota \in Z_p$, then when this is not the case.

Theorem.[Hyperbolic case]

Assume $p \equiv 1 \pmod{4}$. Let

0. g be a primitive root of $p,$
1. $i := \iota := g^{\frac{p-1}{4}}, \delta := \gamma = \sqrt{g}, g' := -g^{\frac{p-3}{2}},$
then
2. $\sin(1) = i^{\frac{g'-1}{2}}\delta,$ and $\cos(1) = \frac{g'+1}{2}\delta.$

Proof: $gg' = -g^{\frac{p-1}{2}} = 1, i^2 = g^{\frac{p-1}{2}} = -1. \delta^{-1} = \delta g^{-1} = g'\delta,$
hence

$$\sin(1) = \frac{\delta - \delta^{-1}}{2i} = -i^{\frac{1-g'}{2}}\delta, \text{ and } \cos(1) = \frac{\delta + \delta^{-1}}{2} = \frac{1+g'}{2}\delta.$$

Theorem.[Hyperbolic case]

Assume $p \equiv -1 \pmod{4}$. Let

0. g be a primitive root of p ,
1. $\delta := \iota$ or $\delta^2 := g^{\frac{p-1}{2}} = -1$, $g' := -g^{\frac{p-3}{4}}$,
then
2. $\sin(1) = \frac{(g-1)g'}{2}$, $\cos(1) = \frac{(g+1)g'}{2}\delta$.

Proof: $gg'^2 = g^{\frac{p-1}{2}} = -1 = \delta^{-2}$. Because $\gamma := \sqrt{g}$, by taking square roots, $\gamma g' = \delta^{-1}$, $\gamma^{-1} = g'\delta$ and $\gamma = gg'\delta$,

hence

$$\sin(1) = \frac{\gamma - \gamma^{-1}}{2\iota} = \frac{(g-1)g'}{2}, \cos(1) = \frac{\gamma + \gamma^{-1}}{2} = \frac{(g+1)g'}{2}\delta.$$

Example.

For $p = 13$, $g = \delta^2 = 2$, $i = -5$, $g' = -6$, then

j	$\sin(j)$	$\cos(j)$	$\tan(j)$
0	0	1	0
1	-2δ	4δ	6
2	-6	-2	3
3	6δ	6δ	1
4	-2	-6	-4
5	4δ	-2δ	-2
6	1	0	∞

For $p = 11$, $g = 2$, $g' = -4$, $\delta^2 = -1$. then

j	$\sin(j)$	$\cos(j)$	$\tan(j)$
0	0	1	0
1	-2	5δ	-4δ
2	2δ	4	-5δ
3	4	2δ	-2δ
4	5δ	-2	3δ
5	1	0	∞

Theorem.

Given a trigonometric table of \sin and \cos , all other $\phi(p-1)$ tables can be obtained by using

0. $\sin^{(e)}(j) = \sin(je)$, $\cos^{(e)}(j) = \cos(je)$, $(e, p-1) = 1$, with $0 < e < p-1$.

Proof: We know that there are $\phi(p-1)$ primitive roots.

If $g^{(e)}$ is an other primitive root, then

$$g^{(e)}e = g^e, (e, p-1) = 1, \delta^{(e)} = g^{\frac{e-1}{2}}\delta,$$

$$\text{for } p \equiv 1 \pmod{4}, i^e = g^{e\frac{p-1}{4}}, g'^e = -g^{e\frac{p-3}{2}},$$

$$\text{for } p \equiv -1 \pmod{4}, g'^e = -g^{e\frac{p-3}{4}}.$$

Substituting in 2.1.3. and 2.1.4. gives the theorem.

Replacing δ by $-\delta$ gives tables for which $\sin(\frac{\pi}{2}) = -1$.

Example.

For $p = 13$, $g = 2$,

e	5	7	11
$g^{(e)} = g^e$	6	-2	-6
δ^e	4δ	-5δ	6δ
$i^e = g^{3e}$	-5	5	5
$g'^e = -g^{5e}$	-2	6	2
$\sin^{(e)}(1)$	4δ	-4δ	2δ
$\cos^{(e)}(1)$	-2δ	2δ	-4δ

For $e = 5$, $\sin^{(5)}(1) = 5 \cdot \frac{3}{2}\delta^e = 1\delta^e = 4\delta$, $\cos^{(5)}(1) = -\frac{1}{2}\delta^e = 6\delta^e = -2\delta$.

The tables are:

j	$\sin(j)$	$\cos(j)$	$\tan(j)$
0	0	1	0
1	4δ	-2δ	-2
2	-6	2	-3
3	-6δ	-6δ	1
4	2	-6	4
5	-2δ	4δ	6
6	1	0	∞

4.2.2 Trigonometry in a Finite Field for $q = p^e$. The Hyperbolic Case.

Introduction.

After recalling the definition of Galois fields, I will generalize Theorems 4.2.1, 4.2.1 and 4.2.1.

Definition.

Let n be a non quadratic residue, the set of elements in the *Galois field* $GF(p^2)$, associated with p^2 , are the polynomials of degree 0 or 1, for which addition is performed modulo p and multiplication is performed modulo $P := I^2 - n$. More specifically

$$\begin{aligned}(uI + v) + (u'I + v') &= (u + u' \bmod p)I + (v + v' \bmod p), \\ (uI + v) \cdot (u'I + v') &= (uv' + u'v \bmod p)I + (vv' + nuu' \bmod p).\end{aligned}$$

Moreover $(uI + v)^{-1} = \frac{-uI+v}{v^2-nu^2}$.

More generally, if P is a primitive polynomial of degree n , i.e. a polynomial which has no factors with coefficients in Z_p , the set of elements in the Galois field $GF(p^e)$, are the polynomials of degree less than e , for which addition and multiplication is performed modulo P .

Notation.

$uI + v$ will be written $u.v$ or $up + v$, $tI^2 + uI + v$ will be written $t.u.v$ or $tp^2 + up + v$.

Example.

Let $q = 5^2$, $n = 3$, $g = I + 1 = 1.1 = 6$, then
 $g^{-1} = -2.2 = 3.2 = 17$, $g^2 = 2. - 1 = 2.4 = 14$, $g^4 = 1. - 2 = 1.3 = 8$, $g^6 = 0. - 2 = 0.3 = 3$,
 $g^{12} = 0. - 1 = 0.4 = 4$, hence $-g^{11} = g^{-1}$.

Theorem.

Theorems 4.2.1, 4.2.1 and 4.2.1 generalize, with p replaced by $q := p^e$.

Example.

For $q = 5^2$, $n = 3$, $\delta^2 = g = 6$, $i = g^6 = 3$, $g' = -g^{11} = 17$,
 $\sin(1) = 2.4\delta = 14\delta$, $\cos(1) = 4.4\delta = 24\delta$.
 $\sin(2) = (-1.0) \cdot (2.2) - -2. - 1 = 3.4 = 19$, $\cos^2(1) = (2. - 1) \cdot (1.1) = 1.0$, $\cos(2) =$
 $2\cos^2(1) - 1 = 2.0 - 0.1 = 2. - 1 = 2.4 = 14$.

This gives the Table:

k	$\sin(k)$	$\cos(k)$
0	0	1
1	14δ	24δ
2	19	14
3	20δ	21δ
4	3	10
5	4δ	12δ
6	20	20
7	12δ	4δ
8	10	3
9	21δ	20δ
10	14	19
11	24δ	14δ
12	1	0

Exercise.

Verify the following and construct the corresponding trigonometric table.

0. For $q = 13^2$, $n = -2$, $\delta^2 = g = 15$, $i = g^{42} = 8$, $g' = -g^{83} = -147$, $g^{167} = 35$,
 $\sin(1) = 110\delta$, $\cos(1) = 18\delta$,
1. For $q = 7^2$, $n = 3$, $\delta^2 = -1$, $g = 8$, $\sin(1) = 3.4\delta = 25\delta$,
 $\cos(1) = 2.2\delta = 18\delta$,
2. For $q = 11^2$, $\delta^2 = 13$, $\sin(1) = 0.2\delta = 2\delta$, $\cos(1) = 8.1\delta = 89\delta$,
3. For $q = 13^2$, $\delta^2 = 15$, $\sin(1) = 11.0\delta = 143\delta$, $\cos(1) = 3.1\delta = 40\delta$,
4. For $q = 17^2$, $\delta^2 = 20$, $\sin(1) = 11.16\delta = 203\delta$, $\cos(1) = 7.5\delta = 124\delta$,

5. For $q = 5^3$, $\delta^2 = 9$, $\sin(1) = 3.3.0\delta = 90\delta$, $\cos(1) = 4.4.1\delta = 121\delta$, $\sin(2) = 87$, $\cos(2) = 110$.

4.2.3 Trigonometry in a Finite Field for $q = p^e$. The Elliptic Case.

Notation.

$(GF(q), +, \cdot)$ is a finite field with $q = p^e$ elements,
 $(GF(q)_b, +, \cdot)$ for the corresponding extension field $GF(q)(\beta)$, with $\beta^2 = b$, where b is a non quadratic residue modulo p .

Convention.

I will heretofore assume that p is a given odd prime. The sets G_b and \overline{G}_b depend on q , we could indicate that dependence by writing $G_{b,q}$ for G_b and $\overline{G}_{b,q}$ for \overline{G}_b .

Definition.

Let $G_b = GF(q) \cup \{\infty\}$.

The operation \circ is defined by

0. $\infty \circ a = a$, $a \in G_b$,
1. $-a \circ a = a \circ -a = \infty$, $a \in GF(q)$,
2. $a \circ a' = \frac{a \cdot a' + b}{a + a'}$, a and $a' \in GF(q)$, $a + a' \neq 0$.
 To avoid confusion with the power notation in $GF(q)$, the k -th power in G_b precedes the exponent with "o". For instance,
3. $a^{o0} = \infty$, $a^{o1} = a$, $a^{ok} = a \circ a^{o(k-1)}$.

Theorem.

If $\left(\frac{b}{p}\right) = -1$, in other words, if b is non quadratic residue modulo p , then

0. $\{G_b, o\}$ is an Abelian group,
1. ∞ is the neutral element,
2. the inverse of $a \in GF(q)$ is $-a$,
3. $r \circ s = t \Rightarrow r \circ (-t) = -s$.

Proof: The associativity property follows from

$$(a \circ a') \circ a'' = \frac{a \cdot a' \cdot a'' + b(a + a' + a'')}{a' \cdot a'' + a'' \cdot a + a \cdot a' + b} = a \circ (a' \circ a''),$$

if $a' \neq -a$ and $a \circ a' \neq -a''$, and from the special cases,

$$(a \circ -a) \circ a' = a' = a \circ (-a \circ a'),$$

$$(\infty \circ a) \circ a' = a \circ a' = \infty \circ (a \circ a').$$

Example.

With $p = 13$,

b	g	g^{o^2}	g^{o^3}	g^{o^4}	g^{o^5}	g^{o^6}	g^{o^7}	g^{o^8}	g^{o^9}	$g^{o^{10}}$	$g^{o^{11}}$	$g^{o^{12}}$	$g^{o^{13}}$	$g^{o^{14}}$
2	2	-5	-6	-4	3	-1	0	1	-3	4	6	5	-2	∞
2	1	-5	4	-4	5	-1	∞							
6	1	-3	5	4	2	-6	0	6	-2	-4	-5	3	-1	∞

Comment.

If $p = 2$, $\left(\frac{b}{p}\right) = -1$ is never satisfied, hence the restriction p odd.

Definition.

If $\left(\frac{b}{p}\right) = -1$ and $\beta = \sqrt{b}$, then

$$\overline{G}_b = \{1\} \cup \left\{ \frac{r+\beta}{r-\beta}, r \in GF(q) \right\}.$$

The elements in \overline{G}_b are distinct and \overline{G}_b is a subset of $GF(q)_b$. The operation of multiplication in $GF(q)_b$ induces one in the set \overline{G}_b .

Theorem.

(\overline{G}_b, \cdot) and (G_b, o) are isomorphic, with the correspondance

0. $1 \in \overline{G}_b$, corresponds to $\infty \in G_b$,

1. $\frac{r+\beta}{r-\beta} \in \overline{G}_b$ corresponds to $r \in G_b$.

Proof: $\frac{r+\beta}{r-\beta} \cdot \frac{s+\beta}{s-\beta} = \frac{(rs+b)+(r+s)\beta}{(rs+b)-(r+s)\beta} = \left(\frac{r+s+\beta}{r+s-\beta}\right)$, if $r + s \neq 0$.

If $s = -r$, $\frac{r+\beta}{r-\beta} \cdot \frac{s+\beta}{s-\beta} = \frac{(r+\beta)(-r+\beta)}{(-r+\beta)(-r-\beta)} = 1$,

Theorem.

0. $\overline{G}_{b,p}$ is an Abelian group, of order $p + 1$.

1. $\left(\frac{r+\beta}{r-\beta}\right)^{p+1} \equiv 1 \pmod{p}$ for any $r \in G_{b,p}$.

Lemma.

If A is a cyclic group of order $q + 1$, the number of elements of order d , where $d|q + 1$, is $\phi(d)$ and

$$q + 1 = \sum_{d|q+1} \phi(d).$$

Lemma. [Gauss]

10

If A is an abelian group of order q which is not cyclic then there exists a divisor d of q such that the number of solutions of $x^d = e$ is larger than d .

¹⁰Herstein, p. 76, 39

Lemma.

The polynomial

$$R_d := (r + \beta)^d - (r - \beta)^d$$

has at most d roots in G_d .

Proof: Dividing by β , we obtain a polynomial in Z_p of degree $d - 1$, which has therefore at most $d - 1$ roots for $z \in Z_p$ or d roots in G_d (∞ being a root).

Example.

With $p = 13$, $b = 2$, if S_d is the set of roots of R_d

$$d = 1, S_1 = \{\infty\}.$$

$$d = 2, S_2 = \{0\} \cup S_1,$$

$$d = 7, S_7 = \{\pm 1, \pm 4, \pm 5\} \cup S_1,$$

$$d = 14, S_{14} = \{\pm 2, \pm 3, \pm 6\} \cup S_7 \cup S_2.$$

Theorem.

$(\overline{G}_{b,p}, \cdot)$ is a cyclic group of order $p + 1$.

$(G_{b,p}, o)$ is a cyclic group of order $p + 1$.

Example.

2 is a generator of $G_{13,2}$, 1 is a generator of $G_{13,6}$.

Theorem.[Elliptic case]

Given $q = p^e \equiv 1 \pmod{4}$. Let

0. b be a non quadratic residue,

1. r_b be a generator of G_b ,

2. $i^2 := -1$,

3. $\beta^2 := b$,

4. $r := r_b^{o \frac{p-1}{4}}$,
then

5. $\sin(1) = \frac{r^2+b}{r^2-b}$, $\cos(1) = \frac{-2ri}{r^2-b}\beta$.

Proof: Let $\sigma = \frac{r+b\beta}{r-b\beta}$, then $\sigma^{p+1} = 1$ and $0 < i < p + 1 \Rightarrow \sigma^i \neq 1$.

$\rho^2 = \sigma \Rightarrow \rho^{2(p+1)} = 1$ and $0 < i < 2(p + 1) \Rightarrow \rho^i \neq 1$.

If we take square roots twice, $\rho^{\frac{p+1}{2}} = \pm i$, we want $\rho^{\frac{p+1}{2}} = \sigma^{\frac{p+1}{4}} = i$, then $\rho = \cos(1) + i \sin(1)$, and $\rho^{2(p+1)} = \cos(2(p + 1)) + i \sin(2(p + 1)) = 1$.

If $r = r_b^{o \frac{p-1}{4}}$, then $\rho^{\frac{p-1}{2}} = \sigma^{\frac{p-1}{4}} = \frac{r+\beta}{r-\beta}$, or $i = \rho^{\frac{p+1}{2}} = \rho \rho^{\frac{p-1}{2}} = \rho \frac{r+\beta}{r-\beta}$, or $\cos(1) + i \sin(1) = \rho = i \frac{r-\beta}{r+\beta}$, $\cos(1) - i \sin(1) = \rho^{-1} = -i \frac{r+\beta}{r-\beta}$,

therefore

$$\cos(1) = -2i r \beta \frac{1}{r^2 - \beta^2}, \sin(1) = \frac{r^2 + \beta^2}{r^2 - \beta^2}.$$

Example.

$$q = 13, i = 5, b = \beta^2 = 6, r_b = 1, r = 5, r^2 = -1, \sin(1) = 3, \cos(1) = -4\beta.$$

k	$\sin(k)$	$\cos(k)$	$\tan(k)$	$\text{atan}(k\beta)$
0	0	1	0β	0
1	3	-4β	-5β	-3
2	2β	-4	6β	4
3	5	-3β	-1β	6
4	-3β	5	2β	5
5	-4	2β	4β	-1
6	-4β	3	3β	2
7	1	0β	∞	-2

q	b	i	r	$\sin(1)$	$\cos(1)$
5	2	2	2	-2	$-\beta$
17	4	3	6	-5	-3β
29	12	2	7	-2	-10β
37	6	2	5	6	$-\beta$
41	9	2	-17	-5	-19β

Theorem.[Elliptic case]

Given $q = p^e \equiv -1 \pmod{4}$. Let

0. b be a non quadratic residue,

1. r_b be a generator of G_b ,

2. $\iota^2 := -1, \delta := \iota$,

3. $\beta^2 := b$,

4. $r := r_b^{o \frac{p+1}{4}}$,

then

5. $\cos(1) = \frac{r_b}{\sqrt{b-r_b^2}}\delta, \sin(1) = \frac{r\cos(1)}{r_b}$.

Proof: The proof proceeds at first as in 4.2.3. $\frac{r+\beta}{r-\beta} = i$, therefore $r = -\beta i$, this establishes the relationship between the sign for the square root of -1 and b .

$$\cos(2) = \frac{1}{2}(\sigma + \sigma^{-1}) = \frac{r_b^2 + b}{r_b^2 - b} \text{ and } \sin(2) = \frac{1}{2i}(\sigma - \sigma^{-1}) = \frac{2r_b}{r_b^2 - b}.$$

$$2\cos^2(1) = 1 + \cos(2) \Rightarrow \cos(1) = \frac{r_b}{\sqrt{r_b^2 - b}},$$

moreover

$\frac{r_b}{b-r_b} = -\cos^2(1)$, $\sin(1)$ follows from $2\sin(1)\cos(1) = \sin(2) = \frac{2r\cos^2(1)}{r_b}$, insuring the consistency between the signs of $\sin(1)$ and $\cos(1)$ to insure that $\sin(\frac{\pi}{2}) = 1$.

Example.

$q = 11$, $\delta^2 = -1$, $b = 2$, $r_b = 1$, $r = -3$, $\cos(1) = \delta$, $\sin(1) = -3\delta$.

k	$\sin(k)$	$\cos(k)$	$\tan(k)$	$\text{atan}(k\beta)$
1	-3δ	1δ	-3	3
2	-5	-3	-2	-2
3	4δ	4δ	1	-1
4	-3	-5	5	-5
5	1δ	-3δ	-4	4
6	1	0	∞	-4

q	b	r_b	r	$\sin(1)$	$\cos(1)$
3	2	1	1	δ	δ
7	3	1	2	3δ	-2δ
19	2	1	6	6δ	δ
23	5	1	8	4δ	-11δ
31	3	1	-11	-13δ	4δ
43	3	5	-13	-7δ	6δ
47	5	4	18	3δ	-15δ

Theorem.

If as usual, $\pi := p + 1$ in the elliptic case or $\pi := p - 1$ in the hyperbolic case, then

0. $3 \mid \pi \Rightarrow \sin(\frac{\pi}{6}) = \frac{1}{2}$, $\cos(\frac{\pi}{6}) = \frac{\sqrt{3}}{2}$.
1. $4 \mid \pi \Rightarrow \cos(\frac{\pi}{4}) = \frac{\sqrt{2}}{2}$.
2. $5 \mid \pi \Rightarrow \cos(\frac{\pi}{5}) = \frac{\sqrt{5}+1}{4}$, $\cos(\frac{2\pi}{5}) = \frac{\sqrt{5}-1}{4}$,
 $\sin(\frac{\pi}{5}) = \frac{\sqrt{10-2\sqrt{5}}}{4}$, $\sin(\frac{2\pi}{5}) = \frac{\sqrt{10+2\sqrt{5}}}{4}$.

In the classical case, there is no ambiguity of sign, because $0 < x < \frac{\pi}{2} \Rightarrow \sin(x), \cos(x) > 0$. This is not the case in a finite field, the formulas can only give the trigonometric functions up to the sign, or alternately one of the values of $\sqrt{3}$, $\sqrt{2}$, $\sqrt{5}$, $\sqrt{10 \pm 2\sqrt{5}}$ can be derived from $\cos(\frac{\pi}{6})$, $\cos(\frac{\pi}{4})$, $\cos(\frac{\pi}{5})$, $\sin(\frac{\pi}{5})$ and $\sin(\frac{2\pi}{5})$.

Example.

$p = 11$, elliptic case, $\sin(2) = -5$, $\cos(2) = -3 \Rightarrow \sqrt{3} = 5$,
 with $\delta^2 = -1$, $\cos(3) = 4\delta \Rightarrow \sqrt{2} = -3\delta$.

$p = 11$, hyperbolic case, $\cos(2) = 4$, $\cos(4) = -2 \Rightarrow \sqrt{5} = 4$,
 with $\gamma^2 = -3$, $\sin(2) = -4\gamma \Rightarrow \sqrt{2} = -5\gamma$, $\sin(4) = \gamma \Rightarrow \sqrt{-4} = 4\gamma$.

$p = 19$, elliptic case, $\cos(5) = -9\delta \Rightarrow \sqrt{2} = \delta$,
 with $\delta^2 = 2$, $\cos(4) = -2 \Rightarrow \cos(8) = 7 \Rightarrow \sqrt{5} = -9$,
 $\sin(4) = 4 \Rightarrow \sqrt{9} = -3$, $\sin(8) = 3 \Rightarrow \sqrt{-8} = -7$.

Definition.

Lemma.

If r_b is a generator of G_b and $b' := \frac{b}{r_b^2}$, then

0. kr_b is a generator of G_{bk^2} ,

1. 1 is a generator of $G_{b'}$.

Theorem.

0. There exists always fundamental roots.

1. There exist $\frac{1}{2}\phi(p+1)$ fundamental roots associated with p .

Example.

6, 7 and 8 are the fundamental roots for $p = 13$,

6, 7 and 12 are the fundamental roots for $p = 17$,

3, 11, 18 and 27 are the fundamental roots for $p = 29$,

6, 14, 15, 18, 19, 20, 23, 24 and 32 are the fundamental roots for $p = 37$,

12, 13, 28, 29, 30 and 35 are the fundamental roots for $p = 41$.

Theorem.

Given an involution, $I(x) = \frac{ax+b}{cx-a}$, $aa + bc \neq 0$, an amicable projectivity, in other words a projectivity with the same fixed points, real or complex, is given by

$$T(x) = \left(\frac{a+f)x+b}{cx-a+f} \right),$$

where $f = \pm \sqrt{(aa + bc)/d}$.

Proof: If $\left(\frac{d}{p} \right) = -1$ then F_d is a fundamental projectivity:

$$F_d = \frac{y+d}{y+1}.$$

In view of 4.2.3, we have $F_d = y \circ 1$.

Comment.

$$\left(\frac{r+\beta}{r-\beta} \right)^e \equiv 1, \text{ for } e|p+1 \implies (r+\beta)^e - (r-\beta)^e \equiv 0,$$

dividing by β , we obtain a polynomial in Z_p of degree $e-1$, which has therefore at most $e-1$ roots for z in Z_p or e roots in G (∞ being a root). We want to show that $(G, .)$ and therefore (G, ∞) are cyclic groups.

Theorem.

Let

0. $r_0 = 1, r_1 = r, r_{i+1} = r_i \circ r,$

1. $x_i \equiv 1/r_i (\in G)$,
2. $u_{i+1} \equiv ru_i + su_{i-1}, u_0 = 0, u_1 = 1,$
 $v_{i+1} \equiv rv_i + sv_{i-1}, v_0 = 2, v_1 = r,$
3. $4s \equiv d - r^2,$
4. $\alpha = \frac{r+\sqrt{d}}{2}$ and $\beta = \frac{r-\sqrt{d}}{2},$
then
5. $x_{i+1} \equiv \frac{rx_i+1}{dx_i+r} \pmod{p}, x_0 = 0,$
6. $r = \alpha + \beta, \sqrt{d} = \alpha - \beta, s = -\alpha\beta.$
7. $u_i = (\alpha^i - \beta^i)/\sqrt{d}, v_i = \alpha^i + \beta^i,$
8. $2u_{i+j} = u_i v_j + v_i u_j, 2v_{i+j} = v_i v_j + bu_i u_j,$
9. $u_{i+1}(bu_i + rv_i) - v_{i+1}(ru_i + v_i) = 0,$
10. $x_i v_i = u_i.$

Proof: $(ru_i + su_{i-1}) = \frac{(\alpha+\beta)(\alpha^i-\beta^i)-\alpha\beta(\alpha^{i-1}-\beta^{i-1})}{\sqrt{d}} = \frac{\alpha^{i+1}-\beta^{i+1}}{\sqrt{d}} = u_{i+1}.$

Substituting in 2. with $j = 1$ after multiplication by \sqrt{d} gives

$$((u_i v_1 + v_i u_1)(bu_i + rv_i) - (v_i v_1 + bu_i u_1)(ru_i + v_i)) \\ = u_i^2(bv_1 - rbu_1) + u_i v_i(bu_1 + rv_1 - rv_1 - bu_1) + v_i^2(ru_1 - v_1) = 0.$$

Moreover,

$$\frac{ru_i + v_i}{du_i + rv_i} = \frac{(\alpha+\beta)(\alpha^i-\beta^i) + (\alpha-\beta)(\alpha^i+\beta^i)}{((\alpha-\beta)(\alpha^i-\beta^i) + (\alpha+\beta)(\alpha^i+\beta^i))\sqrt{d}} = \frac{u_{i+1}}{v_{i+1}} = x_{i+1}.$$

Example.

For $p = 7$, elliptic case, $\iota^2 = -1$,

$$A_k = (\cos(k), \sin(k), 1)$$

are points on the conic

$$x^2 + y^2 = z^2.$$

If we define it as a circle and $z = 0$ as the ideal line, the isotropic points are not real and we have a Euclidean geometry.

The center of the circle, which is the pole of $z = 0$ is $(0,0,1)$. There are 8 real points on the circle,

$$A_0 = (1, 0, 1), A_2 = (-2, -2, 1), A_4 = (0, 1, 1), A_6 = (2, -2, 1), \\ A_8 = (-1, 0, 1), A_{10} = (2, 2, 1), A_{12} = (0, -1, 1), A_{14} = (-2, 2, 1).$$

The distances on the lines $a_{2k} = O \times A_{2k}, k = 0, 1, 2, 3$, are real.

$$a_0 = [0, 1, 0], a_2 = [2, -2, 0], a_4 = [1, 0, 0], a_6 = [1, 1, 0].$$

The other lines through O intersect the circle at complex points:

$$A_1 = (2\iota, 4\iota, 1), A_3 = (4\iota, 2\iota, 1), A_5 = (-4\iota, 2\iota, 1), \\ A_7 = (-2\iota, 4\iota, 1), A_9 = (-2\iota, -4\iota, 1), A_{11} = (-4\iota, -2\iota, 1), \\ A_{13} = (4\iota, -2\iota, 1), A_{15} = (2\iota, -4\iota, 1).$$

These are on the lines $a_{2k+1} = O \times A_{2k+1}$, $k = 0, 1, 2, 3$,

$$a_1 = [-2, 1, 0], a_3 = [1, -2, 0], a_5 = [1, 2, 0], a_7 = [2, 1, 0].$$

If $B_1 = (1, 2, 1)$ is a real point on a_1 , B_1 is on a circle

$$x^2 + y^2 = 5z^2.$$

this circle intersects a_{2k+1} at real points and a_{2k} at complex points. The distances between points on a_1 are multiples of ι , because $\sqrt{5} = 3\iota$. The same is true on the lines a_3, a_5, a_7 .

Definition.

The smallest j such that $u_j \equiv 0 \pmod{p}$ is called the *rank of apparition* of p . Hence

Theorem.

For a fixed r there are $\frac{1}{2}\phi(p+1)$ values of s in $[1, p-1]$ for which the rank of apparition is $p+1$. More generally, there are $\phi(\frac{e}{2})$ values of s in $[1, p-1]$ for which the rank of apparition is e , e divides $p+1$, $e > 2$.

Theorem.

If b is a fundamental root modulo p , then

$$b = \mathbf{N}p, 1 - b = \mathbf{N}p.$$

Comment.

For $p = 17$, $11\mathbf{N}p$, $7\mathbf{N}p$, but 7 is not a fundamental root.

Theorem.

For a given p , the sets

$S_h = \{\cos^2(j), j = 1, \dots, \frac{p-3}{2}\}$, in the hyperbolic case and

$S_e = \{\cos^2(j), j = 1, \dots, \frac{p-1}{2}\}$, in the elliptic case are

independent of the choice of the primitive root or of the fundamental root.

Example.

$$p = 11, S_h = \{4, 5, 7, 8\}, S_e = \{2, 3, 6, 9, 10\}$$

$$p = 29, S_h = \{3, 5, 6, 7, 11, 12, 15, 18, 19, 23, 24, 25, 27\},$$

$$S_e = \{2, 4, 8, 9, 10, 13, 14, 16, 17, 20, 21, 22, 26, 28\}.$$

Theorem.

0. Let $\sin(j) \in \{Z_p - \{0\} - \{1\}\}$,

if $p \equiv -1 \pmod{4}$, then $\sin(j)\sin(k) \neq 1$, for all k ,

if $p \equiv 1 \pmod{4}$, then $\sin(j)\sin(k) = 1$ for some k .

1. $\frac{\sin(j)}{\gamma} \in \{Z_p - \{0\}\}$
if $p \equiv 1 \pmod{4}$, then $\sin(j)\sin(k) \neq 1$, for all k ,
if $p \equiv -1 \pmod{4}$, then $\sin(j)\sin(k) = 1$, for some k .

Example.

... Give examples of associated fundamental symplectic projectivities, see 1.10.

If $T(r) = \frac{r+d}{r+1}$. For $p = 7$, $d = 3$, (5 is the other choice)

$$\begin{array}{cccccccc} r & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ T(r) & 1 & 3 & 2 & 4 & 5 & 0 & 6 & \infty \end{array}$$

... talk about transformations such as $r = 2s$ leading to the form used in 1.10

$$S(s) = \frac{2s+b}{2-3s}.$$

Example.

For $p = 13$, (see g35.bas .5.)

$A = (0, 1, 0)$, $A_j = (1, j, 0)$, $j = 0, \dots, q-1$, $A \times A_j = [0, 0, 1]$, $d_j = \text{dist}(A, A_j)$:

$$\cos(d_j) = \frac{j}{\sqrt{1+j^2}}, \sin(d_j) = \frac{1}{\sqrt{1+j^2}},$$

$$\begin{array}{ccccc} j & \sqrt{1+j^2} & \sin(d_j) & \cos(d_j) & d_j \\ 0 & 1 & 1 & 0 & \frac{1}{2} \\ 1 & \dots & & & \end{array}$$

$$\tan(\text{dist}(A_j, A_k)) = \frac{k-j}{1+jk} \tan(\text{dist}(A, A_k)) = -\frac{1}{k} \tan(\text{dist}(A_j, A_l)) = \tan(\text{dist}(A_j, A_k) + \text{dist}(A_k, A_l)).$$

Indeed, the second member is

$$\frac{(k-j)(1+lk)+(l-k)(1+jk)}{(1+jk)(1+lk)-(k-j)(l-k)} = \frac{(l-j)(1+k^2)}{(1+lj)(1+k^2)} = \tan(\text{dist}(A_j, A_l)).$$

and

$$\tan(\text{dist}(A_j, A_l)) = \tan(\text{dist}(A_j, A) + \text{dist}(A, A_l))$$

Indeed, the second member is

$$\frac{\frac{1}{j} - \frac{1}{l}}{1 + \frac{1}{kl}} = \frac{l-j}{1+kl} = \tan(\text{dist}(A_j, A_l)).$$

$j \setminus k$	0	1	2	3	4	5	6
0		$\frac{3}{12}$	$\frac{11}{12}$	$\frac{10}{12}$	$\frac{4}{12}$		$\frac{5}{12}$
1	$\frac{9}{12}$		$\frac{8}{12}$	$\frac{7}{12}$	$\frac{1}{12}$		$\frac{2}{12}$
2	$\frac{1}{12}$	$\frac{4}{12}$		$\frac{11}{12}$	$\frac{5}{12}$		$\frac{6}{12}$
3	$\frac{2}{12}$	$\frac{5}{12}$	$\frac{1}{12}$		$\frac{6}{12}$		$\frac{7}{12}$
4	$\frac{8}{12}$	$\frac{11}{12}$	$\frac{7}{12}$	$\frac{6}{12}$		$\frac{1}{12}$	
5							
6	$\frac{7}{12}$	$\frac{10}{12}$	$\frac{6}{12}$	$\frac{5}{12}$	$\frac{11}{12}$		
A	$\frac{6}{12}$	$\frac{9}{12}$	$\frac{5}{12}$	$\frac{4}{12}$	$\frac{10}{12}$		$\frac{11}{12}$

Example.

$p = 13$, h , the correspondence between the point $A_j = (1, j, 0)$ and $d(j)$ is

$$\begin{array}{cccccccccccc} j & 0 & -2 & -3 & 1 & 4 & 6 & \infty & -6 & -4 & -1 & 3 & 2 \\ 12d(j) & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \end{array}$$

$i = \pm 5$ corresponds to the ideal point, $d(5) = d(-5) = \infty$.

elliptic case:

$$\begin{array}{cccccccccccc} j\delta & 0 & 3 & -1 & -2 & 4 & -5 & 6 & \infty & -6 & 5 & -4 & 2 & 1 & -3 \\ d(j) & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \end{array}$$

$$\tan(\text{dist}(A_j, A_k)) = \frac{d(k)-d(j)}{1+d(j)d(k)}.$$

4.2.4 Periodicity.

Definition.

Let f be a function, $g(0)$ is arbitrary,

$$g(i+1) = ai + g(i) + f(i) + f(i+1),$$

where a is such that

$$g(T) = g(0),$$

and we write

$$g = Tf.$$

Theorem.

If f is a periodic function with period T , then

0. g is periodic.
1. f odd \Rightarrow even.

Example.

i	0	1	2	3	4	5	6	7	8	9	10
$f(i)$	1	-3	-1	1	3	-1	3	1	-1	-3	1
$g(i)$	0	-2	-6	-6	-2	0	2	6	6	2	0

In this example $a = 0$.

Example.

i	0	1	2	3	4	5
$f(i)$	0	4	7	7	4	0
$g(i + \frac{1}{2})$	0	9	-8	9	0	
$h(i) - ai$	0	0	9	1	-9	-9
$h(i)$	0	-2	5	-5	2	0

In this example $a = -\frac{9}{5}$.

Definition.

Let f be a function. Let g be defined by

$$g(i + \frac{1}{2}) = u(f_i, f_{i+1}),$$

where u is symmetric in its arguments,

we write

$$g = Uf.$$

Let h be defined by

$h(0)$ is arbitrary,

$$h(i+1) = ai + h(i) + g(i + \frac{1}{2}),$$

$$h(T) = h(0).$$

we write

$$h = MUf.$$

Theorem.

If be a periodic function with period T , then

0. *h is a periodic function with period T .*

1.

4.2.5 Orthogonality.

Theorem.

If $p \equiv -1 \pmod{4}$, choose the elliptic case and $q = \frac{p+1}{2}$,

If $p \equiv 1 \pmod{4}$, choose the hyperbolic case and $q = \frac{p-1}{2}$,

0. *The trigonometric functions \sin and \cos are orthogonal.*

1. $(\dots \dots \dots)$
 $(\dots \sin(ij) \dots), i, j = 1 \text{ to } q-1$
 $(\dots \dots \dots)$
is orthogonal, symmetric and $SS = \frac{q}{2}I$.

2. $(\frac{1}{2} \dots \dots s \dots \dots \frac{1}{2})$
 $C = (s \cos(ij)(-1)^i s), i, j = 0 \text{ to } q+1,$
 $(\frac{1}{2} \dots \dots (-1)^j s \dots \frac{1}{2})$

with $s^2 = \frac{1}{2}$,

is orthogonal, symmetric and $CC = \frac{q}{2}I$.

Example.

$p = 7$, Elliptic case, $q = 4$,

$$\begin{array}{ll} & (-3 - 2 - 2 - 2 - 3) \\ & (-21 - 2), \quad (-2 - 2022) \\ S = (10 - 1), C = & (-20 - 10 - 2) \\ & (-2 - 1 - 2), \quad (-220 - 22) \\ & (-32 - 22 - 3) \end{array}$$

$p = 13$, hyperbolic case, $q = 6$,

$$\begin{array}{ll} & (-6sssss - 6) \\ & (-6212 - 6) \quad (s2 - 606 - 2 - s) \\ & (220 - 2 - 2) \quad (s - 66 - 16 - 6s) \\ S = (10 - 101), C = & (s0 - 1010 - s) \\ & (2 - 202 - 2) \quad (s66166s) \\ & (-6 - 21 - 2 - 6) \quad (s - 2 - 6062 - s) \\ & (-6 - ss - ss - s - 6) \end{array}$$

with $s = 2\delta, \delta^2 = 5$.

4.2.6 Conics in sympathic geometry.

Theorem.

$$\begin{aligned} X0_i &= a\cos(2i), X1_i = b\sin(2i), X2_i = 1. \\ X0_i &= \frac{a}{\delta}\cos(2i+1), X1_i = \frac{b}{\delta}\sin(2i+1), X2_i = 1. \\ X0_i &= a\cos(2i), X1_i = \frac{b}{\delta}\sin(2i), X2_i = 1. \\ X0_i &= \frac{a}{\delta}\cos(2i+1), X1_i = b\sin(2i+1), X2_i = 1. \end{aligned}$$

Example.

Let $p = 11$, $a = 1$, $b = 2$, $\delta = i$, $i^2 = -1$.
 In the elliptic case, ... gives $X0^2 + X1^2 \frac{2}{4} = 1$:
 $(1, 0), (-3, 1), (-5, 5), (0, 2), (5, 5), (3, 1),$
 $(-1, 0), (3, -1), (5, -5), (0, -2), (-5, -5), (-3, -1).$
 ... gives
 $-X0^2 - X1^2 \frac{2}{4} = 1$:
 $(1, 5), (4, -3), (-3, 2), (3, 2), (-4, -3), (-1, 5),$
 $(-1, -5), (-4, 3), (3, -2), (-3, -2), (4, 3), (1, -5).$
 In the hyperbolic case, ... gives
 $X0^2 - \frac{1}{4}X1^2 = 1$:
 $(1, 0), (4, 4), (-2, -1), (2, -1), (-4, 4),$
 $(-1, 0), (-4, -4), (2, 1), (-2, 1), (4, -4).$
 The asymptotic directions are $(5, 1, 0)$ and $(-5, 1, 0).$
 ... gives
 $-X0^2 + \frac{1}{4}X1^2 = 1$:
 $(5, -4), (2, -3), (0, 2), (-2, -3), (-5, -4),$
 $(-5, 4), (-2, 3), (0, -2), (2, 3), (5, 4).$
 The asymptotic directions are $(5, 1, 0)$ and $(-5, 1, 0).$

Example.

Let $p = 13$, $a = 1$, $b = 2$, $\delta = 2$, $i = 5$.
 In the elliptic case, ... gives
 $X0^2 + \frac{1}{2}X1^2 = 1$:
 $(1, 0), (-4, -3), (5, -2), (3, 6), (-3, 6), (-5, -2), (4, -3),$
 $(-1, -0), (4, 3), (-5, 2), (-3, -6), (3, -6), (5, 2), (-4, 3).$
 ... gives
 $2X0^2 + \frac{1}{4}X1^2 = 1$:
 $(3, 6), (-1, -3), (5, 5), (0, 2), (-5, 5), (1, -3), (-3, 6),$
 $(-3, -6), (1, 3), (-5, -5), (0, -2), (5, -5), (-1, 3), (3, -6).$
 In the hyperbolic case, ... gives
 $X0^2 + \frac{1}{4}X1^2 = 1$:
 $(1, 0), (-2, 1), (-6, -4), (0, 2), (6, -4), (2, 1),$
 $(-1, 0), (2, -1), (6, 4), (0, -2), (-6, 4), (-2, -1),$
 the asymptotic directions are $(4, 1, 0)$ and $(-4, 1, 0).$

... gives

$$2X0^2 + \frac{1}{2}X1^2 = 1 :$$

$$(4, -4), (6, -1), (-2, -5), (2, -5), (-6, -1), (-4, -4),$$

$$(-4, 4), (-6, 1), (2, 5), (-2, 5), (6, 1), (4, 4),$$

the asymptotic directions are $(4, 1, 0)$ and $(-4, 1, 0)$.

4.2.7 Regular polygons and Constructibility.

Definition.

A regular polygon ...

because the angles are multiples of $\frac{2r}{p-1}$ or $\frac{2r}{p+1}$.

The only regular polygons are those whose number of sides is a divisor of $p-1$ or $p+1$. If we give the unit angle then we can define “convex polygons” and “star polygons”, find appropriate names.

The constructibility by rule and compass in Euclidean geometry corresponds here to those which demand the solution of equations of the first and second degree.

The work of Gauss on cyclotomic polynomials extend immediately to the finite case because of Theorem ... on trigonometric functions.

Theorem.

0. For a regular polygon of n sides to exist, n must divide ...

1. For a regular polygon to be constructible using only equations of the second degree, n must have the form $2^{i_0} p_1^{i_1} p_2^{i_2} \dots p_k^{i_k}$, where i_0 is a non negative integer, i_1, i_2, \dots, i_k , are 0 or 1 and p_j are primes of the form $2^k + 1$, namely, 3, 5, 17, 257, 65537,

All square roots are integers except perhaps the last one.

Theorem.

For triangles.

$$\cos\left(\frac{2r}{3}\right) = \frac{1}{2}, \sin\left(\frac{2r}{3}\right) = \sqrt{\frac{3}{2}}.$$

Example.

$p = 5$, elliptic case,

$$\cos\left(\frac{2r}{3}\right) = 3, \sin\left(\frac{2r}{3}\right) = \sqrt{2}.$$

$p = 7$, hyperbolic case,

$$\cos\left(\frac{2r}{3}\right) = 4, \sin\left(\frac{2r}{3}\right) = \sqrt{6},$$

$p = 23$, elliptic case,

$$\cos\left(\frac{2r}{3}\right) = 12, \sin\left(\frac{2r}{3}\right) = 8.$$

Theorem.

For hexagons, we first obtain the triangle and then use

$$\cos\left(\frac{2r}{6}\right) = \sin\left(\frac{2r}{3}\right), \sin\left(\frac{2r}{6}\right) = \cos\left(\frac{2r}{3}\right).$$

Example.

$p = 23$, elliptic case,
 $\cos(\frac{2r}{6}) = 8$, $\sin(\frac{2r}{6}) = 12$.

Theorem.

For pentagons. The polynomial to solve is

$$x^2 - x + 1 = 0,$$

$$\cos(\frac{2r}{5}) = \frac{x}{2}, \sin(\frac{2r}{5}) = \sqrt{1 - \frac{x^2}{4}}.$$

Example.

$p = 11$, hyperbolic case, $\gamma^2 = 8$.

$$x_1 = (1 + \sqrt{\frac{5}{2}} = \frac{1+7}{2} = 4, x_2 = \frac{1-7}{2} = -3,$$

$$\cos 1(\frac{2r}{5}) = 2, \cos 2(\frac{2r}{5}) = 4,$$

$$\sin 1(\frac{2r}{5}) = \sqrt{-3} = \gamma, \sin 2(\frac{2r}{5}) = \sqrt{-4} = -4\gamma.$$

The choice of 1 or 2 is arbitrary as is the choice of the sign of the coefficient of γ . The second case corresponds to $\sin(\frac{2r}{5})$ of the trigonometric table, trig.tab.

The first, corresponds to $\sin(\frac{6r}{5})$ of the same table.

$p = 19$, elliptic case, $\delta^2 = 10$. $x = \frac{1+9}{2} = 5$,

$$\cos 1(\frac{2r}{5}) = \frac{5}{2} = -7 = \cos(\frac{6r}{5}) \text{ of trig.tab.}$$

$$\sin 1(\frac{2r}{5}) = \sqrt{9} = 3 = \sin(\frac{6r}{5}).$$

Theorem.

For decagons, we first obtain the pentagon and then use $\cos(\frac{2r}{10}) = \sqrt{\frac{(1+\cos \frac{2r}{5})}{2}}$, $\sin(\frac{2r}{10}) = \sin \frac{\frac{2r}{5}}{2\cos(\frac{2r}{10})}$.

Example.

$p = 19$, elliptic case,

$$\cos 1(\frac{2r}{10}) = \sqrt{-3} = 4 = \cos(\frac{6r}{10}), \sin 1(\frac{2r}{10}) = \frac{3}{8} = -2.$$

Theorem.

For 17 sided polygons. The polynomials to solve are in succession:

$$u^2 + u + 4 = 0, \text{ of which we choose 1 root,}$$

$$v^2 - uv - 1 = 0,$$

$$v' = \frac{-3+6v-v^3}{2},$$

$$w^2 - vw + v' = 0,$$

$$\cos(\frac{2r}{p+j}) = \frac{w}{2}, \sin(\frac{2r}{p+j}) = \sqrt{1 - (\frac{w}{2})^2}.$$

Example.

$p = 67$, elliptic case.

$$u = \frac{-1+\sqrt{17}}{2} = 16,$$

$$v = \frac{u+\sqrt{u^2+4}}{2} = \left(\frac{16+\sqrt{59}}{2} = \frac{16+40}{2} = 28,\right.$$

$$v' = 61 = -6,$$

$$w = \frac{v+\sqrt{v^2-4v'}}{2} = \frac{(28+\sqrt{4}}{2} = 15,$$

$$\cos 1\left(\frac{2r}{17}\right) = \frac{15}{2} = -26 = \cos\left(\frac{16r}{17}\right)$$

of the table obtained using the program trig.bas.

$$\sin 1\left(\frac{2r}{17}\right) = \sqrt{1-6} = -14.$$

The other choices for the roots of the above equations lead, with the right choice of sign, to $\cos\left(\frac{2kr}{17}\right)$, $k = 1, 2, 3, 4, 5, 6, 7$. From these all the other angles can be obtained using the trigonometry identities

$p = 137$, hyperbolic case,

$$u = \frac{-1+47}{2} = 23, v = \frac{23+81}{2} = 52,$$

$$v' = \frac{-3+312-46}{2} = 63, w = \frac{52+64}{2} = 58,$$

$\cos 1\left(\frac{2r}{17}\right) = 29 = \cos\left(\frac{12r}{17}\right)$ of the table obtained using the program trig.bas.

4.2.8 Constructibility of the second degree.**Introduction.**

In this section we examine the problems which correspond or require the intersection of a conic or of a circle with a line when one of the intersections is not known.

4.4 Contrast with classical Euclidean Geometry.**4.4.0 Introduction.**

To contrast the notions within finite Euclidean geometry with those of Euclidean geometry, we have the following summary:

In finite Euclidean geometry (of the elliptic type),

The following properties are different in finite Euclidean geometry:

0. There are p points on each line.
1. There are $p + 1$ lines through every point.
2. There are $p + 1$ points and $p + 1$ tangents for each circle.
3. There are even and odd angles, the even ones can be bisected, the odd ones cannot.
4. There are even triangles, for which there are 4 inscribed circles, the others have no inscribed circles.
5. Angles can be expressed as integers, addition of angles is done modulo $p + 1$.

6. line through the center of a circle does not necessarily have an intersection with the circle. The angle between any two lines, through the center, which have an intersection is even.
7. Regular polygons exist only if the number of vertices is a divisor of $p + 1$.
8. Distances can be expressed either as integers or as integers times an irrational, the addition of distances on the same line is done by adding the integers modulo p . The square of the irrational is an integer which is not a square. For instance, for $p = 7$, the irrational can be chosen to be $\sqrt{3}$.
9. Trigonometric functions *sin* and *cos* can expressed like the distances. The cosine of an even angle is always an integer. The cosine of an odd angle is an integer times an irrational. If $p \equiv 1 \pmod{4}$, the sine of an even angle is an integer that of an odd angles is an integer times an irrational, the reverse is true if $p \equiv -1 \pmod{4}$.
10. Ordering cannot be introduced. This is replaced by partial ordering.

Among the properties which are similar, we have the following: Incidence, parallelism, equiangularity, equidistance, perpendicularity, congruence (of figures), similarity, the barycenter, the orthocenter, the circumcircle, the theorem of Pythagoras.

The constructibility of regular polygons (if they exist in the finite case), for instance if we replace the field Z_p by the field $(Z_p, \sqrt{2})$, we always have regular octagons, if we replace by the field $(Z_p, \sqrt{p_i})$, p_i being all the primes, the constructible polygons always exist. If we replace the field Z_p by the field of algebraic numbers, it is those which are roots of some polynomial, then all regular polygons exist.

A similar discussion can be made if we start from the field Q of the rationals. With Q we can only construct squares, extended using

If A is the field of algebraic numbers,

The length of the circle as a limit of the length of polygons only make sense if we start with Q . The implication of the transcendence of ... in A is not a number in A .

... The field of algebraic numbers, the rational case and the existence or non existence of regular polygons.

4.3 Parabolic-Euclidean or Cartesian Geometry.

4.3.0 Introduction.

The Euclidean geometry can be obtained from the projective geometry by choosing an appropriate set of elements, namely the ideal line and 2 complex conjugate points on the line, the isotropic points. Similarly, for the hyperbolic geometry, one choose one real conic as the ideal. In the Cartesian geometry, we choose a line, the ideal line and a point on that line, the isotropic point. Definitions and properties in this geometry will be stated. A construction,

¹G39.TEX [MPAP], September 9, 2019

which allows an elementary algebraic proof of the properties, will be given. The transformations leaving invariant the equality of angles and distances will be studied in a model of the geometry in the Euclidean plane, giving a justification for the name of the geometry.

We start with a projective plane associated to an arbitrary field. A specific line, i , in that plane is chosen, called the ideal line. A specific point, I , on that line is also chosen, called the isotropic point. Because a line is chosen, we can use all the concepts of affine geometry. In particular, 2 lines are called parallel if they have the same ideal point. The mid-point of 2 points A, B is the harmonic conjugate with respect to A, B of the ideal point on $A \times B$. A parabola is a conic tangent to the ideal line.

I now will define new concepts in the Cartesian geometry. To focus the attention on a specific set of properties, I have chosen properties which have been inspired by those associated to the geometry of the triangle. Because we want properties which are true in any field, it is not appropriate to derive them by a limiting procedure. I have therefore stated and proven them independently from the corresponding properties in Euclidean geometry and have indicated the correspondence by giving the same name as that of the corresponding element in Euclidean geometry, but without giving the justification.

The configuration should give theorems in 2 ways ¹¹, using

The equality of angles is associated with a parabolic projectivity (with 2 coincident fixed points).

Recall the construction of a parabolic projectivity on i , let $I1, I2$ be a pair, the point $I4$, corresponding to $I3$, is obtained as follows,

given A , choose B on $A \times I$,

$C := (A \times I2) \times (B \times I1)$, $c := I \times C$,

$D := (B \times I3) \times c$, $a := A \times D$, then

$I4 := a \times i$.

Measure of distances and of angles.

The measure of angles and distances play a fundamental role in the geometry of Euclid and in the study of non Euclidean geometry by de Tilly. On the other hand, starting from projective geometry, these notions are derived notions. The appropriate definitions for the measure of distances and of angles will be given first in the case of a real field using a model on the Euclidean plane with given perpendicular axis x and y through a point O and the line l with equation $y = 1$. This will justify the name of Cartesian geometry.¹²

4.3.1 Fundamental Definitions.

Definition.

In affine geometry let us choose one point on the ideal line as a double isotropic point. This point will be called the *isotropic point* or *sun*. The associated geometry will be called *parabolic-euclidean* or *Cartesian*.

¹¹2.3.83

¹²6.3.83

Definition.

Any line through the sun is called an *isotropic line* or *solar axis*. A parabola with the sun as ideal point is called a *parcircle*.

Comment.

There is a configuration which is a special case of the hexal configuration which allows the study of the geometry of the triangle in the Cartesian geometry. Indeed it is sufficient to choose \overline{M} to be the isotropic point.

Example.

$x_{i+1} := x_i + 1 \pmod{p}$ is such a projectivity.

With $p = 5$,

$$X = \{0, 1, 2, 3, 4, 0, \dots\}$$

. Hence both angles and distances can be represented by an integer modulo p .

The circle is replaced by a parcircle,

Notation.

Let π be the parabolic projectivity with the ideal point as fixed point:

$$0. \quad \pi i = \{(x, x + 1)\}.$$

Theorem.

$$\pi^i = \{(x, x + i)\}, i \in R,$$

therefore, if the coordinates of the point P are x_P and y_P and if the parallels to the lines a and b through O meet l at A and B , we are justified to give the following

Definition.

$$\text{dist}(P, Q) = y_Q - y_P.$$

$$\text{angle}(a, b) := x_B - x_A.$$

We have

Theorem.

Given any 3 points A, B and C and any 3 lines a, b and c ,

$$\text{dist}(A, C) + \text{dist}(C, B) + \text{dist}(B, A) = 0,$$

$$\text{angle}(a, c) + \text{angle}(c, b) + \text{angle}(b, a) = 0.$$

Comment.

Because, in both instances, the notion of measure are associated with the coordinates of a 1 dimensional set of points, both measure of distances and of angles can be given a sign. Of course what we obtain is not a metric but a semi metric because

$|dist(A, B)| \leq |dist(A, C)| + |dist(C, B)|$,
 but $dist(P, Q) = 0$ does not imply $P = Q$ but only $y_P = y_Q$.

In the case of a Gaussian field, if $[0,0,1]$ is the ideal line and $(0,1,0)$ is the isotropic point, we can give

Definition.

$$\begin{aligned} dist((A0, A1, 1), (B0, B1, 1)) &:= B1 - A1 \pmod{p^k}, \\ angle([a0, -1, a2], [b0, -1, b2]) &:= b0 - a0 \pmod{p^k}, \end{aligned}$$

Theorem.

The set of points Q such that angle AQB is constant is a parcircle¹³.

Theorem.

The set of points Q such that angle $QA0 = \text{angle } AQO$ (isosceles triangle) is a set of 2 lines (which can coincide), $A \times S$ and $B \times S$, such that O is equidistant in the Euclidean sense from these 2 lines.

Proof:

$$\begin{aligned} A' &:= (B \times O) \times (A \times S), \quad B' := (A \times O) \times (B \times S), \\ I1 &:= i \times (B \times O), \quad I2 := i \times (A \times B) = i \times (A' \times B'), \\ I3 &:= i \times (A \times O), \end{aligned}$$

then $(I1, I2) = (I2, I3)$ and ABO is an isosceles triangle. (Ii, Ij) denotes the angle of any pair of lines through Ii and Ij on i .

Any other point D on $B \times S$ is such that ADO is an isosceles triangle.

Definition.

$AO = BO$ either if A, B and I are collinear, or if $A'B'$ is parallel to AB where $A' = (B \times O) \times (A \times S)$ and $B' = (A \times O) \times (B \times S)$.

Definition.

Two lines are *antiparallel* if

4.3.2 The Geometry of the Triangle in Galilean Geometry.

Definition.

A line in a triangle is a *symmedian* if

¹³3.3.83

Comment.

We could also define measure of distance and angles dually¹⁴.

$(A, B) = (C, D)$ if $((I \times A), (I \times B))$ and $((I \times C), (I \times D))$ are corresponding pairs in an parabolic projectivity with fixed line i .

If we use as model in the Euclidean plane the line at infinity as the ideal line and the point in the direction of the x axis as the sun all points on a line through the sun are equidistant from points on another line through the sun the measure of distances between the points can be chosen as the measure of the distances between the lines. Therefore, the distance between $A := (a_0, a_1, 1)$ and $B := (b_0, b_1, 1)$ is $b_1 - a_1$.

The angle between $a := [1, -a_1, 0]$ and $b := [1, -a_2, 0]$ is $a_2 - a_1$. a corresponds to $X = a_1 Y$, if α is the angle with the y axis in the clockwise direction, $\tan(\alpha) = a_1$, the “sun” angle is doubled if the tangent is doubled.

Definition.

The *line of Euler* is

Definition.

The *circumparcircle*

Definition.

The *first circle of Lemoine*.

Definition.

The *second circle of Lemoine*.

Definition.

The *circle of Brocard*.

The Brianchon-Poncelet-Feurbach theorem becomes¹⁵

Theorem.

Given a triangle $\{A_i, a_i\}$ and the parcircle ι tangent to a_i . Let M be any point not on the side of the triangle or on i , Let $M_i := (M \times A_i) \times a_i$, the parcircle γ through M_i is tangent to the parcircle ι .

By duality, let m be a line not through A_i or I , let $m_i := (m \times a_i) \times A_i$, the parcircle tangent to m_i is tangent to the parcircle ι .

¹⁴4.3.83

¹⁵3.3.83

4.3.3 The symmetric functions.

Theorem.

The symmetric functions can be expressed in terms of s_{11} and s_{111} . More precisely

$$\text{H0. } s_1 = 0, b := s_{11}, c := s_{111}, \\ \text{then}$$

$$\text{C2. } s_2 = -2b,$$

$$\text{C3 } s_{21} = -3c, s_3 = 3c,$$

$$\text{C4 } s_{22} = b^2, s_{31} = -2b^2, s_4 = 2b^2, s_{211} = 0,$$

$$\text{C5 } s_{221} = bc, s_{32} = -bc, s_{311} = -2bc, s_{41} = 5bc, s_5 = -5bc,$$

$$\text{C6 } s_{222} = c^2, s_{33} = b^3 + 3c^2, s_{321} = -3c^2, s_{411} = 3c^2, s_{42} = -2b^3 - 3c^2, s_{51} = 2b^3 - 3c^2, \\ s_6 = -2b^3 + 3c^2.$$

$$\text{C7 } s_{322} = 0, s_{331} = b^2c, s_{421} = -2b^2c, s_{43} = -b^2c, s_{511} = 2b^2c, s_{52} = 3b^2c, s_{61} = -7b^2c, \\ s_7 = 7b^2c.$$

$$\text{C8 } s_{332} = bc^2, s_{422} = -2bc^2, s_{431} = -bc^2, s_{44} = b^4 + 4bc^2, \\ s_{521} = 5bc^2, s_{53} = -2b^4 - 7bc^2, s_{611} = -5bc^2, s_{62} = 2b^4 + 2bc^2, s_{71} = -2b^4 + 8bc^2, \\ s_8 = 2b^4 - 8bc^2,$$

$$\text{C9 } s_{333} = c^3, s_{432} = -3c^3, s_{441} = b^3c + 3c^3, s_{522} = 3c^3, s_{531} = -2b^3c - 3c^3, s_{54} = -b^3c - 3c^3, \\ s_{63} = 3b^3c + 6c^3, s_{621} = 2b^3c - 3c^3, s_{72} = -5b^3c - 3c^3, s_{711} = -2b^3c + 3c^3, s_{81} = 9b^3c - 3c^3, \\ s_9 = -9b^3c + 3c^3,$$

$$\text{C10 } s_{433} = 0, s_{442} = b^2c^2, s_{532} = -2b^2c^2, s_{541} = -b^2c^2, \\ s_{55} = b^5 + 5b^2c^2, s_{622} = 2b^2c^2, s_{631} = 3b^2c^2, s_{64} = -2b^5 - 9b^2c^2, s_{721} = -7b^2c^2, \\ s_{73} = 2b^5 + 6b^2c^2, s_{811} = 7b^2c^2, s_{82} = -2b^5 + b^2c^2, s_{91} = 2b^5 - 15b^2c^2, s_{10} = -2b^5 + 6b^2c^2,$$

$$\text{C11 } s_{443} = bc^3, s_{533} = -2bc^3, s_{542} = -bc^3, s_{551} = bc^4 + 4bc^3, s_{632} = 5bc^3, s_{641} = -2bc^4 - 7bc^3, \\ s_{65} = -bc^4 - 4bc^3, s_{722} = -5bc^3, s_{731} = 2bc^4 + 2bc^3, s_{74} = 3bc^4 + 11bc^3, s_{821} = -2bc^4 + 8bc^3, \\ s_{83} = -5bc^4 - 13bc^3, s_{911} = 2bc^4 - 8bc^3, s_{92} = 7bc^4 + 5bc^3, s_{10,1} = -11bc^4 + 11bc^3, \\ s_{11} = 11bc^4 - 11bc^3,$$

$$\text{C12 } s_{444} = c^4, s_{543} = -3c^4, s_{552} = b^3c^2 + 3c^4, s_{633} = 3c^4, s_{642} = -2b^3c^2 - 3c^4, s_{651} = -b^3c^2 - 3c^4, \\ s_{66} = b^6 + 6b^3c^2 + 3c^4, s_{732} = 2b^3c^2 - 3c^4, s_{741} = 3b^3c^2 + 6c^4, s_{75} = -2b^6 - 11b^3c^2 - 3c^4, \\ s_{822} = -2b^3c^2 + 3c^4, s_{831} = -5b^3c^2 - 3c^4, s_{84} = 2b^6 + 8b^3c^2 - 3c^4, s_{921} = 9b^3c^2 - 3c^4, \\ s_{93} = -2b^6 - 3b^3c^2 + 6c^4, s_{10,1,1} = -9b^3c^2 + 3c^4, s_{10,2} = 2b^6 - 6b^3c^2 - 3c^4, \\ s_{11,1} = -2b^6 + 24b^3c^2 - 3c^4, s_{12} = 2b^6 - 24b^3c^2 + 3c^4.$$

Theorem.

Given a triangle A_i a point M not on the sides of the triangle and a point \bar{M} on the polar m of M with respect to the triangle.

0. γ is a parcircle,
1. θ is a parcircle,
2. χ_{1i} and χ_{2i} are parcircles.

Proof: We will use the abbreviation

$$\begin{aligned} s_{11} &= m_1m_2 + m_2m_0 + m_0m_1 \text{ and we have} \\ m_0^2 - m_1m_2 &= m_1^2 - m_2m_0 = m_2^2 - m_0m_1 \\ &= m_1^2 + m_2^2 + m_1m_2 = -s_{11}. \end{aligned}$$

$$\begin{aligned} s_{11} + m_1m_2 &= -(m_1^2 + m_2^2), \dots & s_{11} + m_0^2 &= m_1m_2, \dots \\ 2s_{11} - m_1m_2 &= m_1m_2 - 2m_0^2, (m_1 - m_2)^2 &= -(s_{11} + 3m_1m_2). \end{aligned}$$

COMPARE Mmm and $j\bar{a}$, $Mm\bar{m}$ and jia .

Theorem.

The conic

$$m_0X_1X_2 + m_1X_2X_0 + m_2X_0X_1 = 0$$

passes through M , A_i , and

$$ZZ_i = (m_0, -(m_1 - m_2), m_1 - m_2),$$

the tangent at A_i is $\bar{a}c_i$,

the tangent at M is $mai = [m_0, m_1, m_2]$,

the tangent at ZZ_i is $[(m_1 - m_2)^2, m_0m_1, m_2m_0]^{16}$.

4.5 Transformation associated to the Cartesian geometry.

4.5.0 Introduction.

Such transformation must preserve measure of angles and distances.

Theorem.

The transformations associated to the Cartesian geometry are represented by unit upper triangular matrices in the Euclidean The following are subgroups of these transformation

The translations

$$\begin{pmatrix} 1 & 0 & v \\ 0 & 1 & w \\ 0 & 0 & 1 \end{pmatrix}.$$

The shears

$$\begin{pmatrix} 1 & u & v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
 and the special shears

$$\begin{pmatrix} 1 & u & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$
 Indeed,

Definition.

Theorem.

Given a point P , the set of points whose polars with respect to a triangle pass through P are on a conic through the vertices of the triangle and vice-versa.

Proof. The pole of $[q_0, q_1, q_2]$ is (q_1q_2, q_2q_0, q_0q_1) . It is on line (a_0, a_1, a_2) if $a_0q_1q_2 + a_1q_2q_0 + a_2q_0q_1 = 0$.

Definition.

Given a triangle, the point of Lemoine of a conic through the vertices of the triangle is the point P of the preceding Theorem.

Definition.

Given a triangle, the line of Lemoine of a conic tangent to the triangle is the set of points whose polars with respect to the triangle are tangent to the conic.

Corollary.

The point of Lemoine of the circumcircle is the classical point of Lemoine. The point of Lemoine of the conic of Simson $m_0m_1X_1X_2 + \dots = 0$ is $T^{mm} = (m_0m_1, m_1m_2, m_2m_0)$. The line of Lemoine of the inscribed conic is $[j_1j_2, j_2j_0, j_0j_1]$, it is the line through Ja_i .

4.5.1 The geometry of the triangle, the standard form.

Introduction.

In this section, we do give only a representative set of Theorems using a form similar to that found in works on Geometry since Euclid. Many more Theorems can be deduced from the compact form given in section 9.5. The vertices of the triangle are denoted by A_0, A_1, A_2 , its sides by a_0, a_1, a_2 .

Definition.

A Fano line p of a point P is the line through the diagonal points of the quadrangle A_0, A_1, A_2, P .

Definition.

The cocenter M of a triangle is the Fano point of the ideal line m . (D0.1., .2., .12.)

Construction.

Given a triangle A_i , the ideal line m and the center M , we can obtain a conic as follows. The tangents to the conic θ at the vertices of the triangle are be constructed using $m_i = M \times A_i$. Any point on the conic and on a given line through one of its points, are be obtained using the construction of Pascal.

Definition.

The conic

$$\theta$$

constructed in 9.6.3. is by definition a *circle* the *circumcircle* of the triangle. (D1.12., H1.0.)

Definition.

The Euler line of a triangle is the line *eul* through the cocenter and the center of the triangle. (D1.0.)

Definition.

The central parallels kk_i are the lines parallel to the sides of a triangle passing through the center M . (D1.1.)

Theorem.

The central parallels kk_i intersect the sides a_{i+1} and a_{i-1} at points $K A_{i-1}$ and $K A_{i+1}$ which are on a circle λ . (D1.2., D2.11., C2.1., C2.2.)

Definition.

The circle λ is called central circle.

Theorem.

The circumcircle and the central circle are tangent at a point LO . (C23.0.)

Definition.

The central points M_i of a triangle are the intersection of a tangent at a vertex with the opposite sides. (D0.11.)

Definition.

The central line m of a triangle is the Fano line of its center M . (D0.12.)

Definition.

The associated circles α_i are the circles through the center M of the triangle and its vertices A_{i+1} and A_{i-1} . (D3.6., C3.1.)

Definition.

The center-vertex circles κ_i and κ_{-i} are the circles centered at one vertex of a triangle passing through an other vertex. (D4.12., C4.0.)

Definition.

The bissectrices i_i of a triangle are the lines through a vertex A_i such that the lines forms equal angles with the sides of the triangle passing through A_i .

Theorem.

The bissectrices have a point I in common. (9.5.5., D0.3.)

Definition.

The bissector is the point I common to the bissectrices i_i . (D.0.3.) The bissector line i is the Fano line of the bissector. (D20.1)

Comment.

The sides of a triangle do not have a point in common, therefore, there is no circle tangent to its sides.

Definition.

The circles of Apollonius α_i are the circles centered at a central point M_i through a opposite vertex A_i . (D5.12., C5.0., C5.1.) They have a common tangent with the circumcircle (C5.3.). The point of contact with the side a_i is on the bissectrix through A_i . (C22.1.)

Theorem.

The circles of Apollonius have the same radical axis, l mm, which is the common tangent of the circumcircle and the central circle. (C6.2., C2.6.)

Definition.

The sun MI is the direction of the bissector line. (D24.0.)

Definition.

Any parabola, i.e. a conic tangent to the ideal line, whose ideal point is the sun MI is called a *sun-parabola*.

Comment.

In the isotropic geometry, the center of a parabola is an ideal point which is not necessarily its ideal point.

Definition.

The center-cocenter conic γ is the conic through the vertices of the triangle, its center and its cocenter. (D7.10.)

Theorem.

The center-cocenter conic is a sun-parabola. (C24.1.)

Definition.

The tangential circles χt_i (χt_i) are the circles tangent to $a_{i+1}(a_{i-1})$ at $A_{i-1}(A_{i+1})$ passing through $A_{i+1}(A_{i-1})$. (D7.8., C7.0.)

Theorem.

The other intersections $K L_i$ and $K L_i$ with the tangential circles and the sides of the triangles are on a conic ξ which is a sun-parabola. (D3.1., D7.9., C7.2., D24.2.)

Theorem.

The cocircumcircle θ is the conic through the vertices of the triangle for which the tangents are parallel to the opposite side. (D1.12., D0.1., C1.0.)

Definition.

Let Eul and Eul be the points of contact of the circumcircle and of the co-circumcircle with the line of Euler, the conic ι through these points and circumscribed to the triangle is called the bissector conic. (D20.19., C20.2., C20.3.)

Theorem.

The center of the bissector conic is the bissector point. (C20.7.)

Comment.

9.6.28. is an alternate definition from that given in D20.19.

4.5.2 The cubic γ a of Gabrielle.

Introduction.

This section and the related section 11. was conceived after my daughter asked when I would name a Theorem for her. It concerns a general construction which starts from a parabola and constructs points on a cubic of which several are associated to the geometry of the triangle.

Definition.

Let $x = (x_0, x_1, x_2)$ be any line of the dual of the sun-parabola Γ , 0. $(m_1 + m_2)x_1x_2 + (m_2 + m_0)x_2x_0 + (m_0 + m_1)x_0x_1 = 0$.

Let k $k_i = [m_1 + m_2, m_2, m_1]$. The following constructs points $X = (X_0, X_1, X_2)$ of the curve γ a called the cubic of Gabrielle: D1. $X_i := x x k$ k_i ,

D2. $x_i := X_i x A_i$,

D3. $X := x_1 x x_2$.

D4. $\gamma a := \{X\}$.

Definition.

A parametric representation of a curve, with constraint arbitrary point are given in terms of 3 homogeneous parameters subjected to an homogeneous relation R between these 3 parameters.

Theorem.

The curve γ a is a point cubic, with axis 0. $df = [m_0^3(m_1 + m_2)^2, m_1^3(m_2 + m_0)^2, m_2^3(m_0 + m_1)^2]$.

It contains the points A_i , M_i , M , M , LM . A parametric representation, with constraint 9.7.1.0., is 1. $(x_1x_2(m_0(m_1 + m_2)(x_1 + x_2) + m_1m_2x_0),$

$x_2x_0(m_1(m_2 + m_0)(x_2 + x_0) + m_2m_0x_1),$

$x_0x_1(m_2(m_0 + m_1)(x_0 + x_1) + m_0m_1x_2)),$

Its equation in homogeneous coordinates is P4. $\gamma a : m_0X_0(X_1^2 + X_2^2) + m_1X_1(X_2^2 + X_0^2) + m_2X_2(X_0^2 + X_1^2) = 0$.

Proof: Definition 9.7.1. gives P1. $X_0 = (m_1x_1 + m_2x_2, m_1x_0 + (m_1 + m_2)x_2, m_2x_0 + (m_1 + m_2)x_1),$

P2. $x_0 = [0, m_2x_0 + (m_1 + m_2)x_1, m_1x_0 + (m_1 + m_2)x_2],$

P3. $X = ((m_2x_0 + (m_1 + m_2)x_1)(m_0x_1 + (m_2 + m_0)x_2),$

$(m_1x_0 + (m_1 + m_2)x_2)(m_2x_1 + (m_2 + m_0)x_0),$

$(m_2x_0 + (m_1 + m_2)x_1)(m_2x_1 + (m_2 + m_0)x_0)),$

if we multiply all coordinates by x_2 and use 9.7.1.0. we get 9.7.3.1. By a long algebraic verification it can be shown that the equation P4. is satisfied by 1.

Theorem.

- A parametric representation, with constraint 0. $x_0 + x_1 + x_2 = 0$
 is 1. $(x_1x_2(m_1x_1 + m_2x_2), x_2x_0(m_2x_2 + m_0x_0), x_0x_1(m_0x_0 + m_1x_1))$.
 2. *The point 1. is the point on the cubic γ and the line*
 $[x_0, x_1, x_2]$ *through M distinct from M.*
 3. *There is one line m_i where M is a triple point.*

Proof: Let (X_0, X_1, X_2) be any point on the line $[x_0, x_1, x_2]$ passing through M , eliminating X_0 between the equation of the cubic γ and $X_0x_0 + X_1x_1 + X_2x_2 = 0$ gives
 $(X_1 + X_2)^2(X_1(m_0x_1(x_1 + x_2) + m_1x_1^2) + X_2(m_0x_2(x_1 + x_2) + m_2x_2^2)) = 0$
 or $X_1 = x_0x_2(m_0x_0 + m_2x_2), X_2 = x_0x_1(m_0x_0 + m_1x_1)$,
 because of 0., by symmetry we get 1. $X_1 + X_2 = 0$, gives the point M and because $(X_1 + X_2)$
 is a double factor this point has to be counted twice, hence 2., the point M is a *node*. The
 point 1. coincides with M iff the 3 coordinates are equal, the first 2 give after elimination
 of x_0 , $(m_0 + m_1)x_1^2 = (m_2 + m_0)x_2^2$, hence $x_1 = i_2 + i_0, x_2 = i_0 + i_1$, by symmetry $x_0 =$
 $i_1 + i_2$, hence 3.

Theorem.

If the point of contact of a line $[x_0, x_1, x_2]$ through LM with the cubic γ is (X_0, X_1, X_2) ,
 then 0. $X_0^2 = m_0x_1x_2(m_1x_1 + m_2x_2), X_1^2 = m_1x_2x_0(m_2x_2 + m_0x_0),$

$$X_2^2 = m_2x_0x_1(m_0x_0 + m_1x_1).$$

We have 1. $m_0m_1x_1 + m_2m_0x_1 + m_0m_1x_2 = 0$

and 2. $x_0X_0 + x_1X_1 + x_2X_2 = 0$.

Eliminating X_0 between 2. and the equation of the cubic gives $(m_2X_2 + m_1X_1)(m_2x_1(m_0x_0 +$
 $m_1x_1)X_1^2 + m_1x_2(m_0x_0 + m_2x_2)X_2^2) = 0$, because of 1.

The first factor corresponds to the point LM , the other factor has a double root which gives
 0.

Definition.

The cubic χ of Charles is the cubic through the points M_i, M_i, LM_i .

Theorem.

Let 0. $a := m_0m_1m_2,$

1. $a_0 := m_0(m_1^2 + m_2^2 + m_1m_2), a_1 := m_1(m_2^2 + m_0^2 + m_2m_0),$
 $a_2 := m_2(m_0^2 + m_1^2 + m_0m_1),$

then 2. $\chi : a(X_0^3 + X_1^3 + X_2^3)$
 $+ a_0X_1X_2(X_1 + X_2) + a_1X_2X_0(X_2 + X_0) + a_2X_0X_1(X_0 + X_1) = 0$.

3. *The tangent at (X_0, X_1, X_2) is*
 $[aX_0^2 + a_2X_1^2 + a_1X_2^2, aX_1^2 + a_0X_2^2 + a_2X_0^2,$
 $aX_2^2 + a_1X_0^2 + a_0X_1^2],$

4. *The other point (Y_0, Y_1, Y_2) on the tangent $[x_0, x_1, x_2]$ at*
 (X_0, X_1, X_2) , *is obtained by eliminating Z_0 from 2., where*

$(X0, X1, X2)$ is replaced by $(Z0, Z1, Z2)$ and
 $x0Z0 + x1Z1 + x2Z2 = 0$. The coefficient of Z^3 is
 $Y1X1^2$ and that of $Z1^3$ is $Y2X2^2$.

Proof: For 4. we observe that the elimination should lead to the equation $(X2Z1 + X1Z2)^2(Y2Z1 + Y1Z2) = 0$.

An illustration of 4. is given by 12.4.

Conjecture.

Given 9 points A_i, B_i, C_i , on a cubic such that A_i, B_i, C_i and $(A_0, B_0, C_0), (A_1, B_1, C_1)$ are collinear, then (A_2, B_2, C_2) are collinear.

Corollary.

If 3 points A_i are on a cubic, the third point C_i on the tangent to the cubic at A_i are also collinear.

Example.

For $q = 16$, $i0 = 1$, $i1 = \epsilon^8$, $i2 = \epsilon^3$, $m0 = 1, m1 = \epsilon, m2 = \epsilon^6$,
H0.0. $M = 253$, E0.10. $M = 184$, H0.1. $A_i = 2, 1, 0$,
H0.2. $I = 130$,

E0.0. $a_i = 0^*, 1^*, 272^*$,
E0.1. $m_i = 253^*, 2^*, 136^*$, E0.9. $m_i = 179^*, 89^*, 90^*$,
E0.2. $M_i = 136, 272, 137$, E0.11. $M_i = 15, 115, 91$,
E0.3. $i_i = 125^*, 6^*, 233^*$,
E0.4. $I_i = 238, 232, 234$,
E0.5. $im_i = 44^*, 102^*, 339^*$,
 $im_i = 4^*, 151^*, 168^*$,
E0.6. $Tm_i = 194, 14, 16$,
 $Tm_i = 3, 30, 195$,
E0.7. $tm_i = 61^*, 180^*, 15^*$,
 $tm_i = 271^*, 203^*, 194^*$,
E0.8. $IA_i = 94, 240, 133$,
 $IA_i = 101, 215, 183$,
E0.12. $m = 137^*, m = 189^*$,

E1.0. $eul = 20$,
E1.1. $kk_i = 152^*, 205^*, 96^*$, $kk_i = 258^*, 21^*, 147^*$,
E1.2. $KA_i = 234, 127, 30$, $KA_i = 195, 31, 237$,
 $KA_i = 126, 16, 255$, $KA_i = 180, 128, 204$,
E1.3. $kl_i = 203^*, 233^*, 236^*$, $kl_i = 126^*, 194^*, 202^*$,
 $kl_i = 15^*, 134^*, 237^*$, $kl_i = 127^*, 29^*, 14^*$,
E1.4. $B_i = 147, 61, 102$, $B_i = 101, 47, 37$,

$$\text{E1.5. } bb_i =$$

$$\text{E1.6. } Eul_i = 116, 254, 256,$$

$$\text{E1.7. } Ba_i =$$

$$Ba_i =$$

$$\text{E1.8. } tB_i =$$

$$\text{E1.9. } KK_i = 147, 5, 200, K K_i = 101, 199, 143,$$

$$\text{E1.10. } eul_i = 88^*, 135^*, 255^*,$$

$$\text{E1.11. } TT =$$

$$\text{E1.12. } \theta = 0, 1, 2, 40, 61, 102, 123, 145, 147,$$

$$90^*, 89^*, 179^*, 96^*, 120^*, 92^*, 71^*, 49^*, 216^*,$$

$$172, 197, 211, 223, 229, 235, 249, 250,$$

$$104^*, 270^*, 152^*, 10^*, 225^*, 20^*, 205^*, 54^*,$$

$$\text{E2.0. } tim_i = 118^*, 45^*, 16^*, tim_i = 182^*, 101^*, 140^*,$$

$$\text{E2.1. } LI_i = 63, 193, 239, L I_i = 181, 203, 64,$$

$$\text{E2.2. } li_i = 192^*, 62^*, 238^*, l i_i = 13^*, 30^*, 63^*,$$

$$\text{E2.3. } Atm_i = 211, 50, 208, A tm_i = 151, 217, 242,$$

$$\text{E2.4. } lt_i = 125^*, 254^*, 181^*, l t_i = 125^*, 237^*, 31^*,$$

$$\text{E2.5. } LM = 155, L M = 163,$$

$$\text{E2.6. } LT_i = 238, 135, 182, L T_i = 238, 232, 32,$$

$$\text{E2.7. } lm = 98^*, l m = 162^*,$$

$$\text{E2.8. } LMM = 96, L MM = 174,$$

$$LM M = 118, L M M = 265,$$

$$\text{E2.9. } tKKL_i =$$

$$tKKL_i =$$

$$\text{E2.10. } lmm = 83^*, l mm = 92^*,$$

$$lm m = 49^*, l m m = 110^*,$$

$$\text{E3.0. } ka_i = 255^*, 61^*, 203^*, k a_i = 233^*, 88^*, 126^*,$$

$$ka_i = 193^*, 15^*, 5^*, ka_i = 254^*, 127^*, 271^*,$$

$$\text{E6.13. } \Gamma = 0, 1, 33, 41, 51, 93, 105, 111, 129,$$

$$116^*, 254^*, 161^*, 235^*, 253^*, 43^*, 11^*, 70^*, 260^*,$$

$$137, 169, 171, 186, 189, 241, 270, 272,$$

$$96^*, 107^*, 218^*, 268^*, 174^*, 213^*, 184^*, 256^*,$$

$$\text{E7.1. } TMi = 171, T mi = 225,$$

$$\text{E8.0. } dt_i = 139^*, 227^*, 239^*,$$

$$dt_i = 91^*, 151^*, 138^*,$$

$$\text{E8.1. } Du_i = 116, 6, 16,$$

$$Du_i = 90, 30, 117,$$

$$\text{E9.0. } Eb_i = 133, 251, 212, E b_i = 150, 55, 167,$$

- $E b_i = 189, 111, 261, E b_i = 9, 257, 146,$
 E9.2. $ed_i = 226^*, 68^*, 256^*, e d_i = 183^*, 121^*, 123^*,$
 $ed_i = 128^*, 44^*, 144^*, e d_i = 158^*, 185^*, 16^*,$
- E11.19. $Dh_i = 177, 103, 75, D h_i = 133, 253, 183,$
 $Dh_i = 83, 159, 122, D h_i = 253, 34, 22,$
 E11.20. $di_i = 180, 127, 13, d i_i = 180, 3, 253,$
 $di_i = 204, 5, 193, d i_i = 204, 114, 2,$
 E11.21. $Dj_i = 100, 111, 261, D j_i = 100, 124, 253,$
- E11.22. $dk_i = 27^*, 83^*, 35^*, d k_i = 92^*, 71^*, 216^*,$
 $dk_i = 23^*, 35^*, 224^*,$
 E11.23. $du_i = 88^*, 232^*, 15^*,$
 $du_i = 114^*, 203^*, 116^*,$
 E11.24. $Dl_i = 101, 185, 104,$
 $Dl_i = 101, 247, 190,$
 E11.25. $Dm_i = 204, 134, 203,$
 $Dm_i = 14, 15, 29,$
 E11.26. $Dn_i = 30, 205, 255,$
 $Dn_i = 16, 204, 180,$
 E11.27. $dn = 33^*,$
 $dn = 100^*,$
 E11.28. $Do = 200,$
 $Do = 174,$
 E11.29. $dp = 102^*,$
 $dp = 55^*,$
 E11.30. $Dq = 178,$
 E11.31. $dr = 26^*,$
- E11.32. $\gamma a = 0, 1, 2, 15, 40, 80, 91, 100, 103,$
 $181^*, 254^*, 125^*, 121^*, 234^*, 208^*, 245^*, 133^*, 78^*,$
 $115, 124, 155, 169, 178, 184, 253, 263,$
 $118^*, 149^*, 39^*, 119^*, 26^*, 49^*, 83^*, 100^*,$
- $\gamma a = 0, 1, 2, 53, 100, 111, 136, 137, 153,$
 $31^*, 237^*, 125^*, 141^*, 173^*, 70^*, 200^*, 226^*, 41^*,$
 $163, 184, 225, 250, 253, 261, 265, 272,$
 $18^*, 92^*, 111^*, 113^*, 110^*, 75^*, 246^*, 117^*,$
- E12.0. $Na_i = 89, 8, 194, N a_i = 272, 205, 204,$
 E12.1. $na_i = 7^*, 61^*, 115^*, n a_i = 204^*, 29^*, 2^*,$
 E12.2. $Nb_i = 248, 129, 55, N b_i = 29, 70, 251,$
 E12.3. $nc_i = 8^*, 263^*, 144^*, n c_i = 158^*, 245^*, 218^*,$
 E12.4. $lMM_i = 192^*, 180^*, 31^*, l MM_i = 114^*, 30^*, 7^*,$
 E12.5. $nd_i = 263^*, 58^*, 239^*, n d_i = 103^*, 18^*, 66^*,$

- E12.6. $Ne_i = 124, 243, 197, N e_i = 208, 24, 249,$
 E12.7. $nf_i = 80^*, 157^*, 257^*,$
 E12.8. $ng_i = 182^*, 101^*, 140^*, n g_i = 118^*, 45^*, 16^*,$
 E12.9. $Nh_i = 106, 103, 134, N h_i = 186, 228, 222,$
 E12.10. $lI = 170^*, l I = 52^*,$
 E12.11. $Ni_i = 98, 262, 54, N i_i = 170, 18, 258,$
 $Ni_i = 86, 210, 260, N i_i = 218, 35, 41,$
 E12.12. $nj_i = 179^*, 140^*, 147^*, n j_i = 253^*, 239^*, 118^*,$
 E12.13. $nk_i = 32^*, 139^*, 200^*, n k_i = 221^*, 164^*, 223^*,$
 $nk_i = 252^*, 144^*, 117^*, n k_i = 213^*, 48^*, 158^*,$
 E12.14. $Nl_i = 95, 134, 189, N l_i = 83, 124, 186,$
 $Nl_i = 157, 136, 157, N l_i = 20, 228, 115,$
 E12.15. $nl = 99^*, n l = 150^*,$
 $nl = 119^*, n l = 161^*,$
 E12.16. $nm_i = 268^*, 60^*, 66^*, n m_i = 98^*, 152^*, 47^*,$
 E12.17. $np_i = 47^*, 44^*, 109^*, n p_i = 265^*, 268^*, 121^*,$
 $np_i = 76^*, 123^*, 253^*, n p_i = 140^*, 116^*, 76^*,$
 E12.18. $nq_i = 24^*, 139^*, 257^*, n q_i = 48^*, 11^*, 223^*,$
 $nq_i = 146^*, 198^*, 78^*, n q_i = 82^*, 18^*, 172^*,$
 E12.19. $Nr_i = 157, 137, 254, N r_i = 15, 20, 15,$
 $Nr_i = 134, 78, 198, N r_i = 198, 13, 83,$
 E12.20. $nr = 252^*, n r = 218^*,$
 $nr = 202^*, n r = 191^*,$

 E12. $.ND_i = 256, 186, 13,$
 E12. $.$
 $\chi = 13, 15, 20, 78, 83, 91, 95, 103, 106, 115, 116, 124, 131,$
 $261^*, 218^*, 96^*, 195^*, 197^*, 245^*, 193^*, 1^*, 10^*, 158^*, 157^*, 131^*, 269^*,$
 $15, 20, 137, 272, 91, 222, 83, 103, 228, 116, 131, 157, 198,$

 $134, 136, 137, 157, 186, 189, 198, 222, 228, 254, 256, 272,$
 $146^*, 144^*, 263^*, 119^*, 87^*, 49^*, 165^*, 178^*, 60^*, 257^*, 80^*, 8^*,$
 $254, 256, 13, 136, 189, 78, 115, 95, 134, 106, 124, 186,$
(these are the tangents and the other point on the tangent)

 E19.4. $lI = 170^*, l I = 52^*,$
 E19.5. $LJ = 11,$

 E22.0. $iA_i = 179^*, 237^*, 3^*,$
 E22.1. $IA = 230,$
 E22.2. $ab = 224^*,$
 E22.6. $Ia_i = 15, 126, 4,$
 E22.7. $ia = 112^*,$

 E25.0. $Dk = 176,$

E25.1. $dl = 100^*$,

Given the center C of a circle and one of its points A , the point X on any line x through A (or y through C) can be obtained by construction y through C (or x through A) such that the angle $XAC = \text{angle } BCX$. The above as to be reviewed. A construction of a point on a given tangent (or radius) follows. There must be a simpler way. Let the given points be A_0, A_1, A_2 , let the center be C , let the radius-tangent be t , $Mt := t \times m$, find A_4 on the circle and $A_0 \times Mt$, find A_5 on the circle and $A_1 \times Mt$, let $Y := (A_0 \times A_1) \times (A_4 \times A_5)$, $(C \times Y) \times t$ is the point of contact with the circle. To find the bissectrix of an angle $A_{-1} A_0 A_1$ we use the above construction with the tangent-radius $Cx(mx(A_{-1}xA_1))$ the ?? point X on the circle is also on the bissectrix.

Notation.

Angles and directions will be denoted by an upper case letter and a lower case letter underlined.

Theorem.

If the angle of the direction of the sides b_i is nb_i , then the angle of the direction of the tangent is $d_{i+1} + d_{i+2} - d_i \bmod q + 1$.

Theorem.

If the direction of a_i is a_i , the angles at A_i are $A_i = a_{i+1} - a_{i-1} \bmod q + 1$.

Theorem.

0. The angle of the direction of the center of $\chi 1_i$ is

$$c1_i = a_i + A_{i-1},$$

that of the center of $\chi 2_i$ is

$$c2_i = a_i - A_{i+1}.$$

1. The center of $\chi 1_i$ is $(A_{i+1} \times M) \times a_{i+1}$,

$$c1_i$$

that of $\chi 2_i$ is $(A_{i-1} \times M) \times a_{i-1}$,

$$c2_i$$

4.6 Problems

.

4.6.1 Problems for Affine Geometry.

Theorem.

If m is the ideal line, and $A = (A_0, A_1, A_2)$, $B = (B_0, B_1, B_2)$ then

0. the mid-point $A + B$ of A and B is

$$A + B = (m \cdot B)A + (m \cdot A)B.$$
1. the symmetric $2B - A$ of A with respect to B is

$$2B - A = 2(m \cdot A)B - (m \cdot B)A.$$

Theorem.

The mid-points of the diagonals of a complete quadrilateral are collinear. *D37.5, C37.15. (020, Chou and Schelter 1986, p. 18)*

Definition.

The line of the preceding Theorem is called the mid-line of the complete quadrilateral.

Theorem.

Given a complete 5-lines, the mid-lines of the 5 complete quadrilaterals obtained by suppressing any of the 5 lines have a point in common. *(025, Chou and Schelter 1986, p. 19)*

Theorem.

Given a triangle A_i , and a point M_0 , let M_j be the symmetric of M_{j-1} with respect to $A_{j-1 \pmod{3}}$, then

0. M_{i+3} is the symmetric of M_i with respect to MM_{i+1} , vertex of the anticomplementary triangle of A_i .
1. $M_6 = M_0$.
2. $M_i, M_{i+3}, M_{i+1}, M_{i+4}$ are parallelograms.

4.6.2 Problems for Involution Geometry.

Theorem.

The perpendicular direction to (IX_0, IX_1, IX_2) is $(m_0(m_1 - m_2)I_0 + m_0(m_1 + m_2)(I_1 - I_2), m_1(m_2 - m_0)I_1 + m_1(m_2 + m_0)(I_2 - I_0), m_2(m_0 - m_1)I_2 + m_2(m_0 + m_1)(I_0 - I_1))$.

Theorem. [Butterfly Theorem]

If a quadrangle is inscribed in a circle with cent O , then a diagonal point, D , is the midpoint of the intersection with the other sides of a perpendicular through D to $O \times D$. (041, Chou (1984), p.269.)

4.90 Answers to problems and miscellaneous notes.

Answer to 4.6.1.

Let the lines be a_i, \overline{m} and $\overline{m}' = [m'_0, m'_1, m'_2]$.

The midlines are

$$l_4 = [s_1 - 2m_0, s_1 - 2m_1, s_1 - 2m_2],$$

$$l_3 = [s'_1 - 2m'_0, s'_1 - 2m'_1, s'_1 - 2m'_2], \text{ with } s'_1 = m'_0 + m'_1 + m'_2,$$

$$\overline{MA}_1 + \overline{M'A}_2 = (m'_0(m_2 - m_0) - m_0(m'_0 - m'_1), m'_1(m_0 - m_2), m_2(m'_0 - m'_1)).$$

$$\overline{M'A}_1 + \overline{MA}_2 = (m_0(m'_2 - m'_0) - m'_0(m_0 - m_1), m_1(m'_0 - m'_2), m'_2(m_0 - m_1)).$$

$$l_0 = [m_1 m_2 m'_0 (s'_1 - 2m'_0) - m'_1 m'_2 m_0 (s_2 - 2m_0), m'_2 m_0 (2m'_0 (m_0 - m_1) - m'_1 (s_1 - 2m_1)) - m_2 m'_0 (2m_0 (m'_0 - m'_1) - m_1 (s'_1 - 2m'_1)), m'_1 m_0 (2m'_0 (m_2 - m_0) + m'_2 (s_1 - 2m_2)) - m_1 m'_0 (2m_0 (m'_2 - m'_0) + m_1 (s'_1 - 2m'_2))],$$

The common point is

$$P = (m'_0(m_1 - m_2) - m_0(m'_1 - m'_2), m'_1(m_2 - m_0) - m_1(m'_2 - m'_0), m'_2(m_0 - m_1) - m_2(m'_0 - m'_1)).$$

Answer to 4.6.1.

Let $M_0 = (m_0, m_1, m_2)$, with $m_0 + m_1 + m_2 = 1$.

$$M_1 = 2A_0 - M_0 = (2 - m_0, -m_1, -m_2),$$

$$M_2 = 2A_1 - M_1 = (-2 + m_0, 2 + m_1, m_2),$$

$$M_3 = 2A_2 - M_2 = (2 - m_0, -2 - m_1, 2 - m_2),$$

$$M_4 = 2A_0 - M_3 = (m_0, 2 + m_1, -2 + m_2),$$

$$M_5 = 2A_1 - M_4 = (-m_0, -m_1, 2 - m_2),$$

$$M_6 = 2A_2 - M_5 = (m_0, m_1, m_2).$$

Answer to 4.6.2.

Let 3 of the points be A_i , let $D := (0, 1, x)$, be on a_0 , then the 4-th point is $(y, 1, x)$, with

$$y = -\frac{m_0(m_1 + m_2)x}{m_2(m_0 + m_1) + m_1(m_2 + m_0)x}. \quad O = (m_1 + m_2, m_2 + m_0, m_0 + m_1),$$

$$D \times O = [(m_2 + m_0)x - (m_0 + m_1), -(m_1 + m_2)x, (m_1 + m_2)],$$

its direction is $((m_1 + m_2)(m_2x + m_1), m_2(m_2 + m_0)x - s_{11} - m_2m_0, m_1(m_0 + m_1) + x(s_{11} + m_0m_1))$.

The direction perpendicular to $D \times O$ is

$$(m_0(m_1 - m_2)(m_1 + m_2)(m_2x + m_1) + m_0(m_1 + m_2)(m_2(m_2 + m_0)x - s_{11} - m_2m_0) - m_1(m_0 + m_1) + x(s_{11} + m_0m_1)), m_1(m_2 - m_0)m_2(m_2 + m_0)x - s_{11} - m_2m_0 + m_1(m_2 + m_0)(m_1(m_0 + m_1) + x(s_{11} + m_0m_1) - (m_1 + m_2)(m_2x + m_1)), m_2(m_0 - m_1)m_1(m_0 + m_1) + x(s_{11} + m_0m_1) + m_2(m_0 + m_1)((m_1 + m_2)(m_2x + m_1) - m_2(m_2 + m_0)x - s_{11} - m_2m_0)).$$

....

Maybe Chapt. III

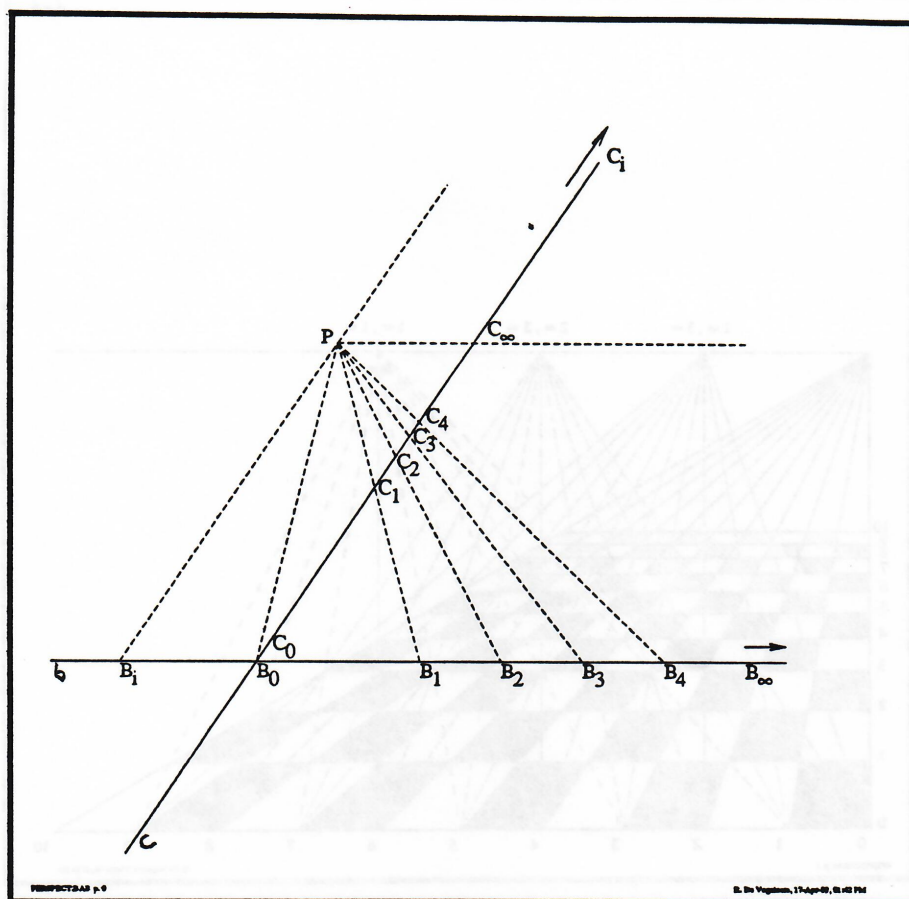


Fig. Pl , Perspectivity of a line onto an other line

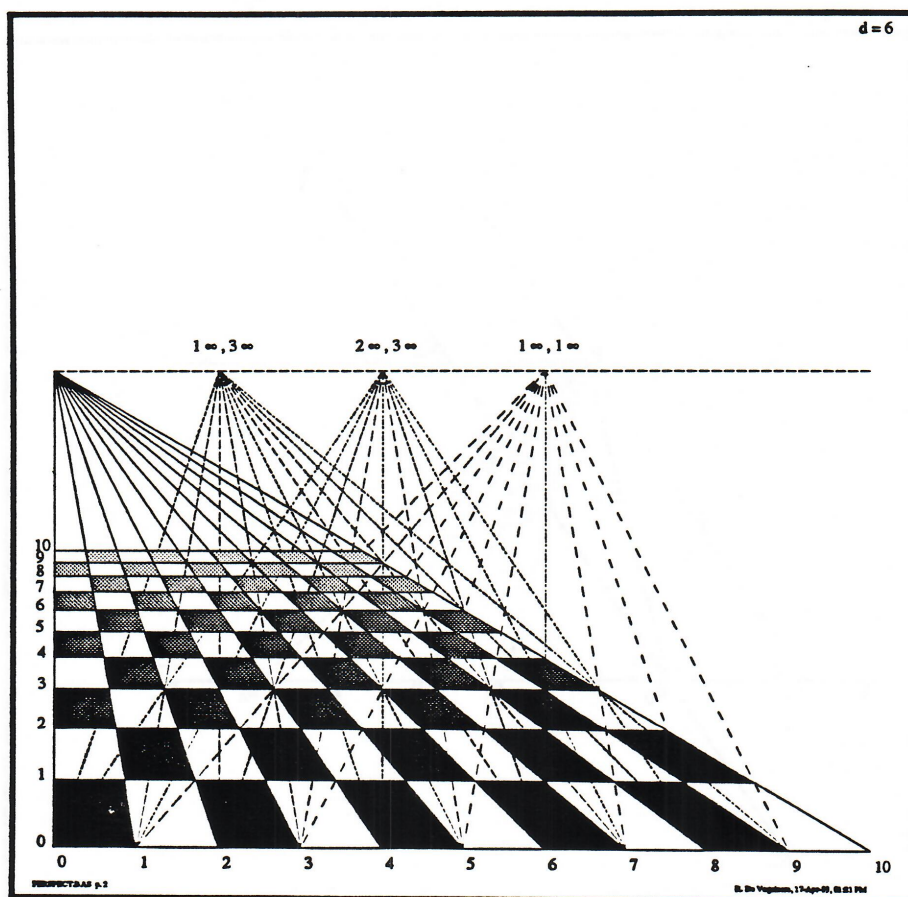


Fig. 5t, Square Tiling

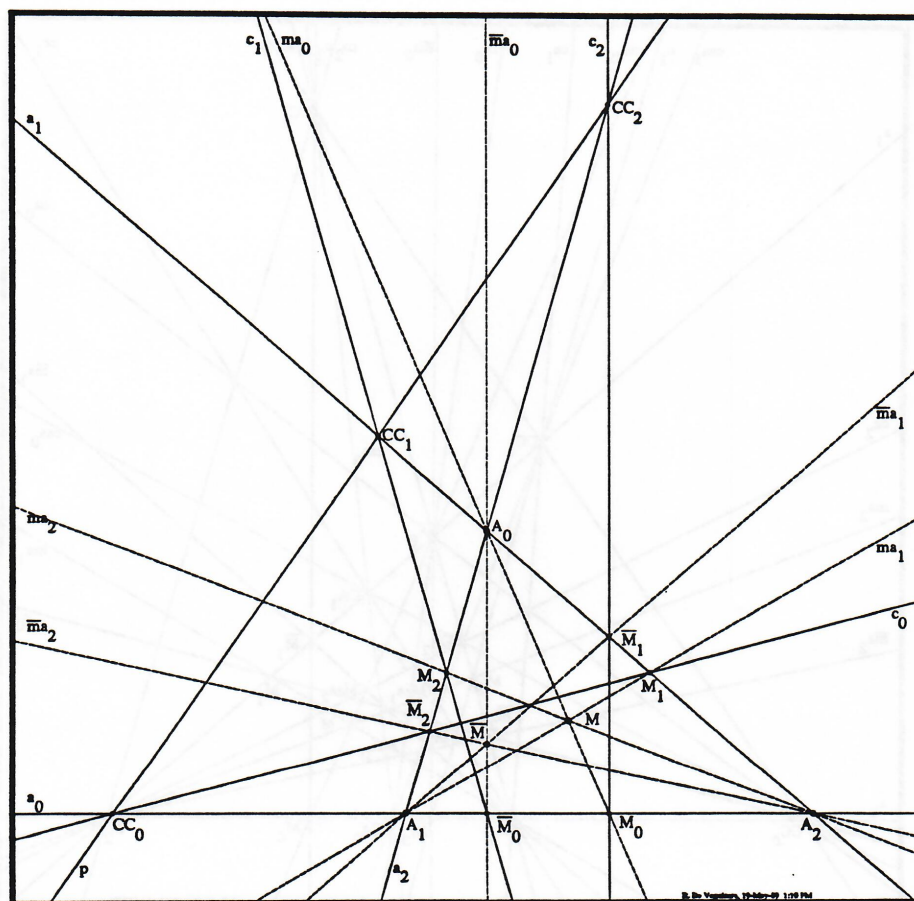


Fig. 0, The Fundamental Configuration.



Fig. 0', Proof of the Fundamental Configuration.

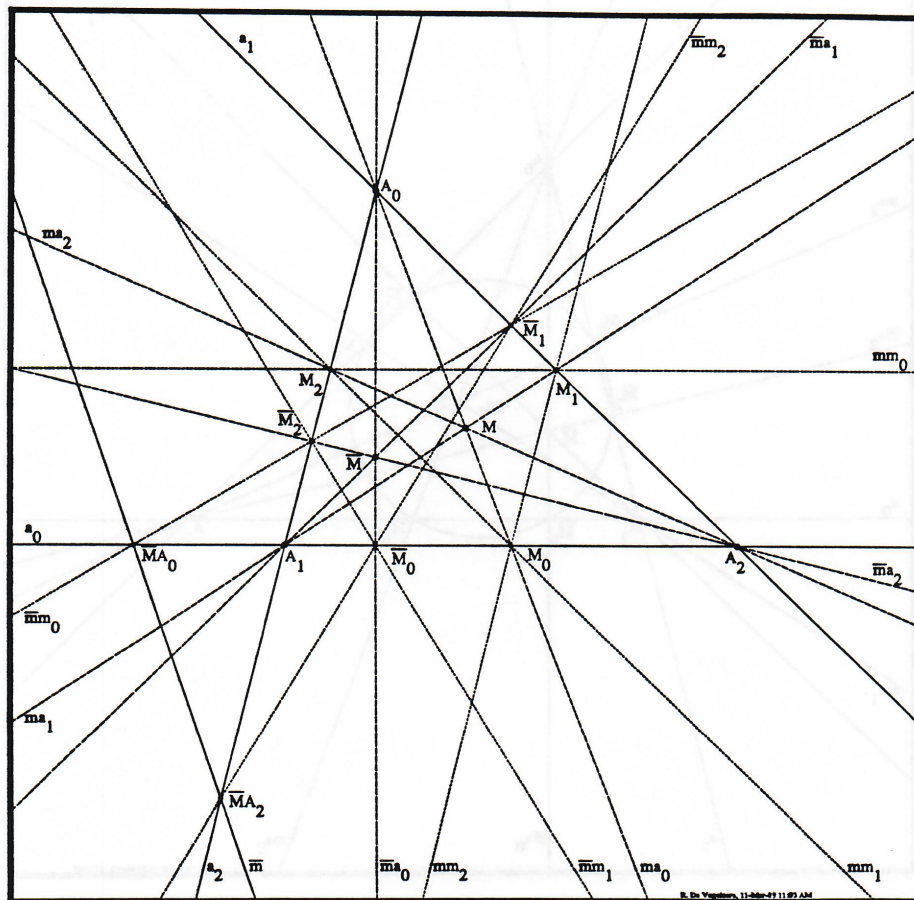


Fig. 1, The Hexal Configuration.

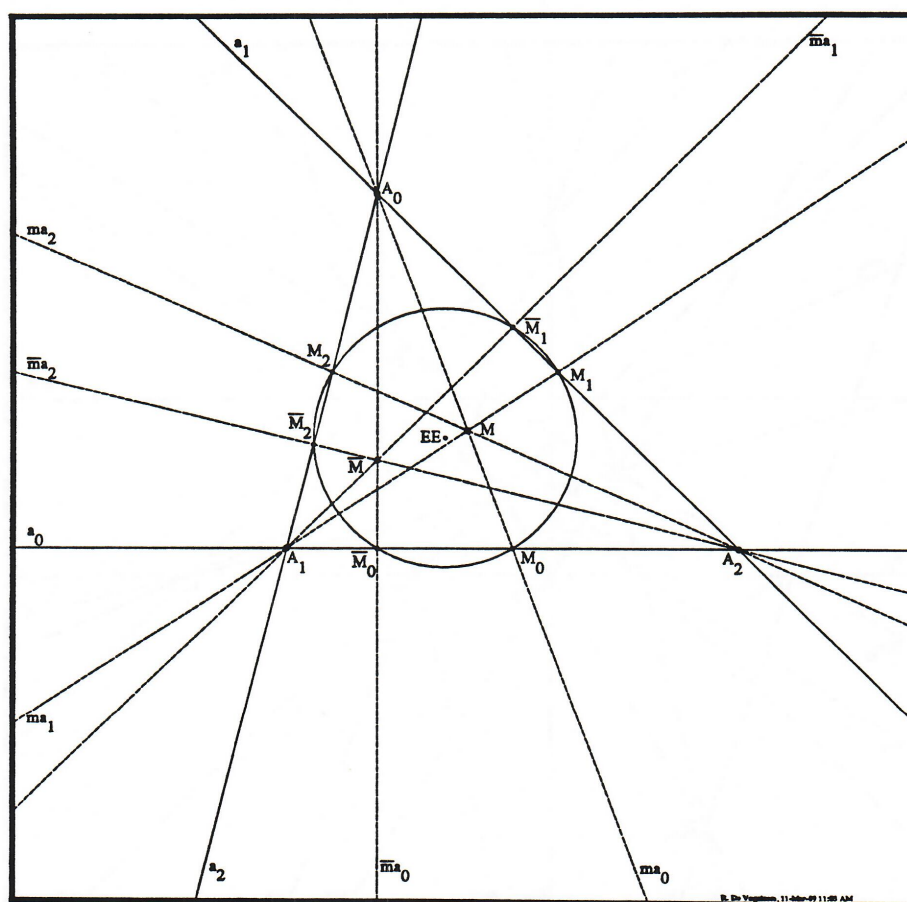


Fig. 2, The circle of Brianchon-Poncelet.

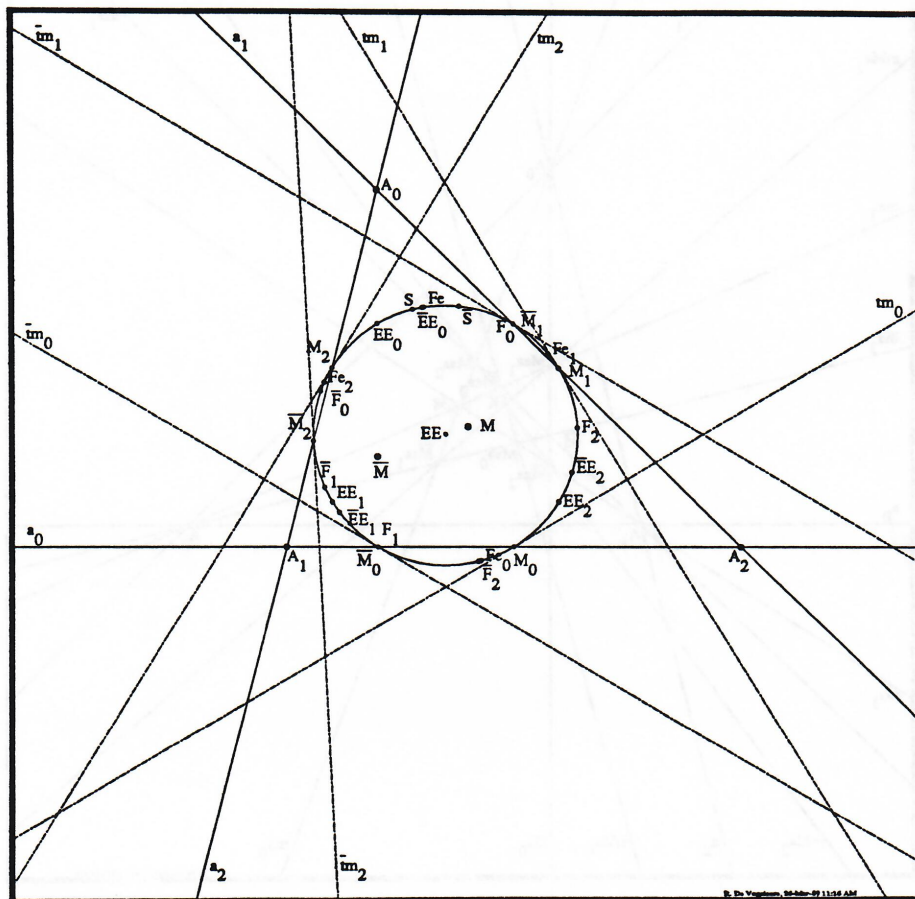


Fig. 2b, The circle of Brianchon-Poncelet.

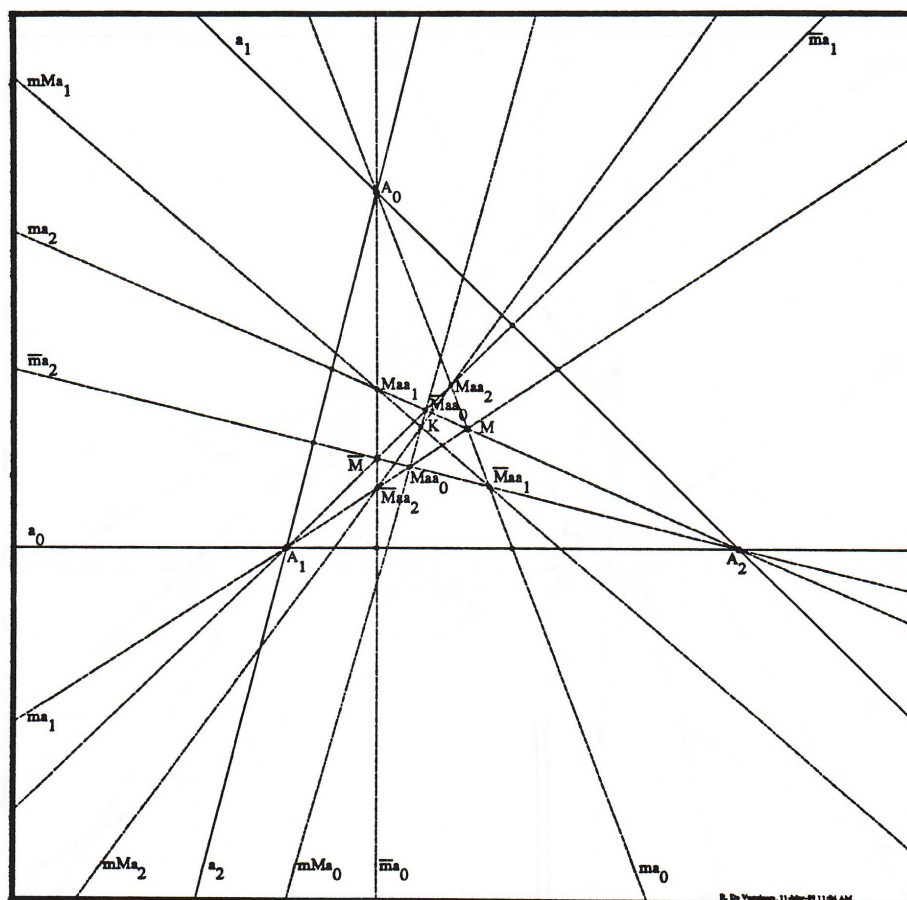


Fig. 3, The Point of Lemoine.

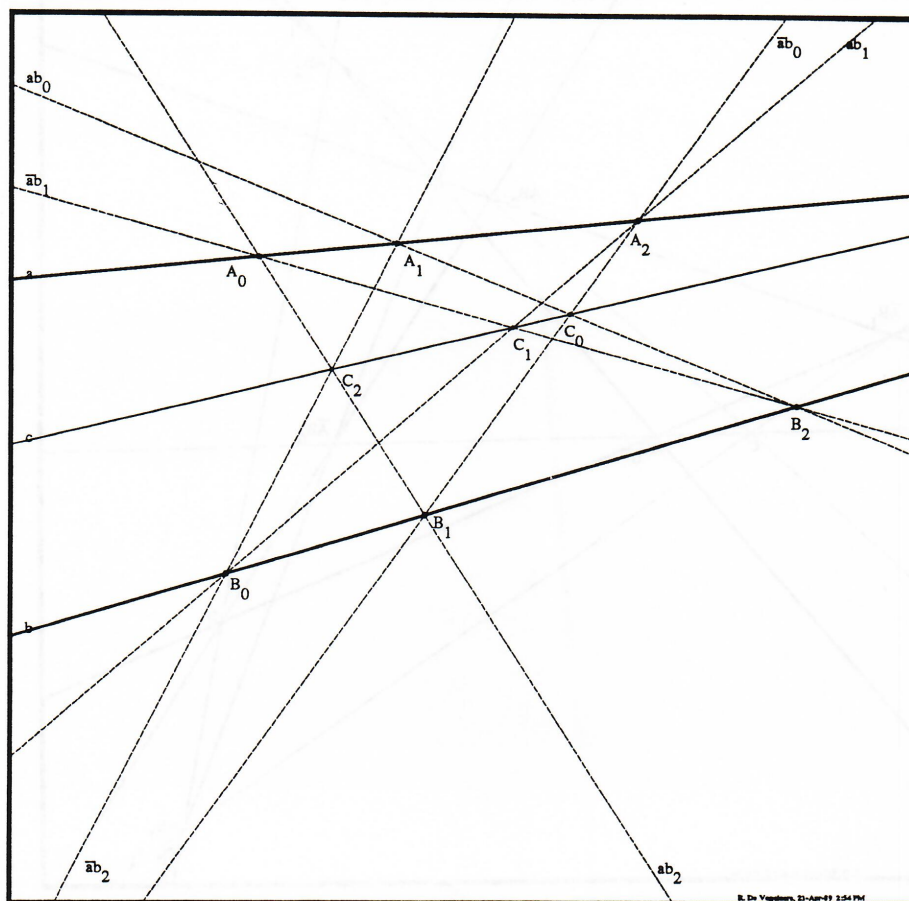


Fig. 1a, Pappus' Configuration.

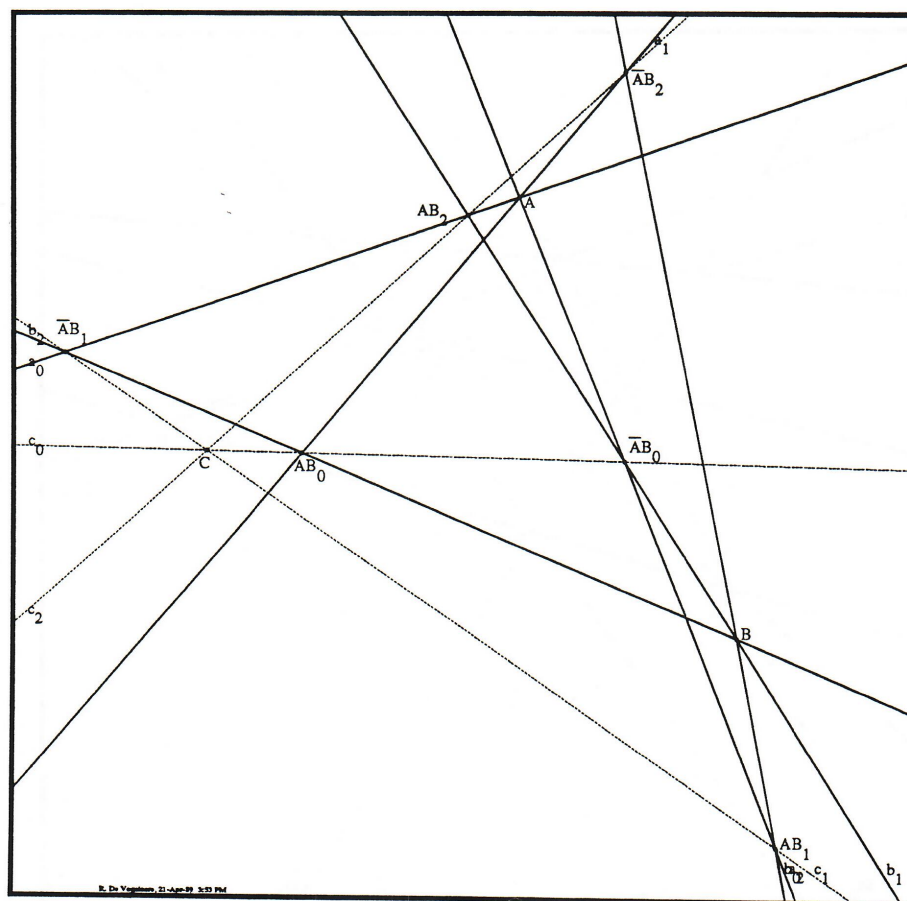


Fig. 1b, Pappus' Dual Configuration.

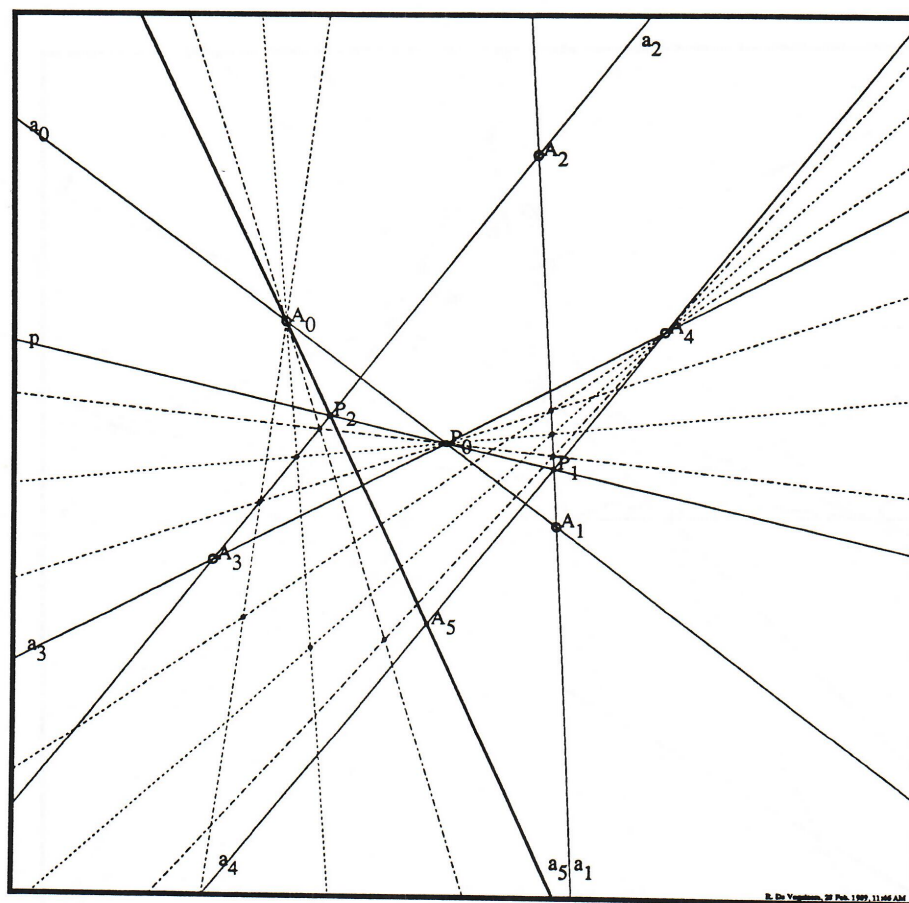
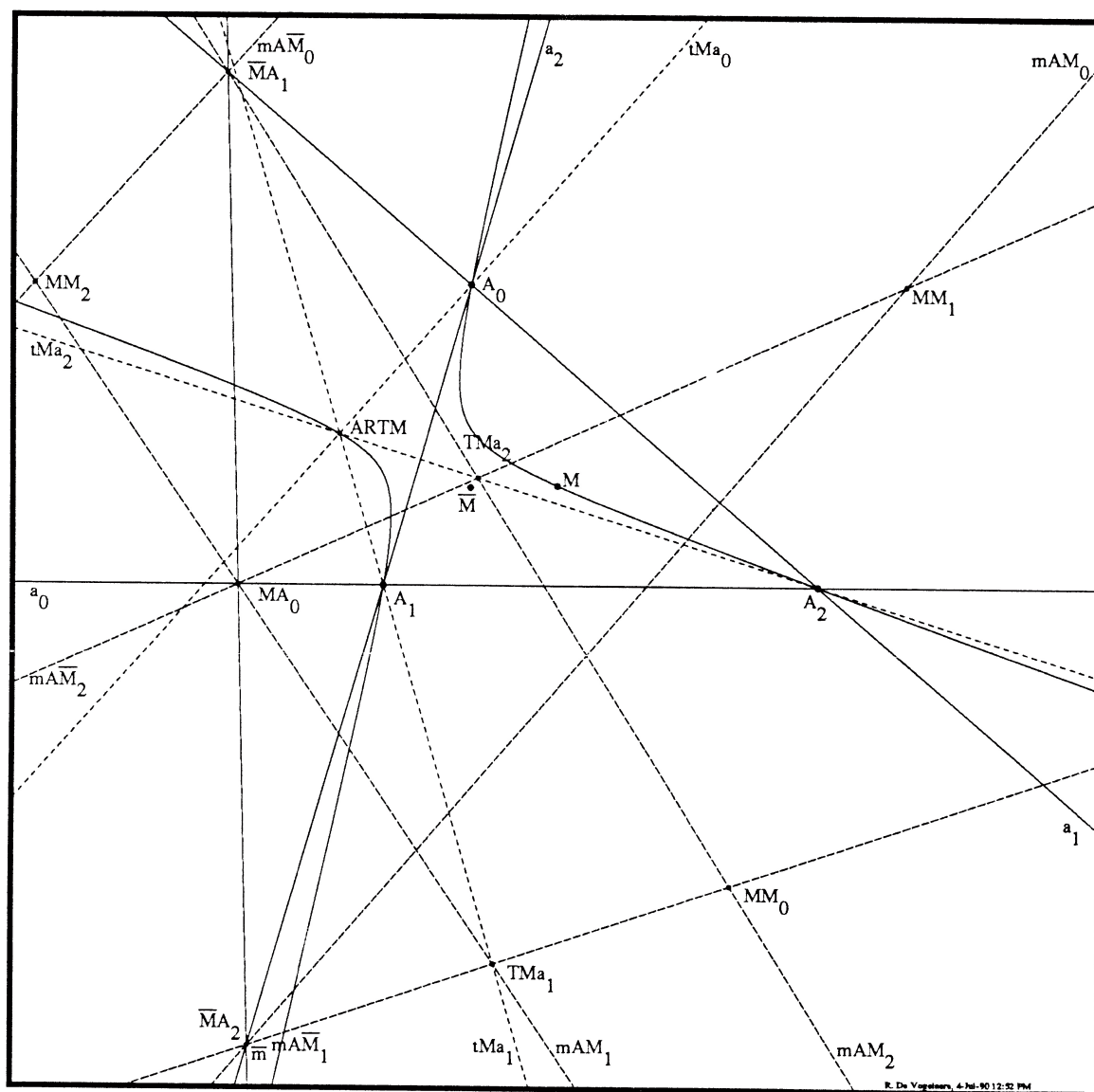


Fig. 200, Pascal's Construction



The point and conic of Luke.

Chapter 5

FINITE NON-EUCLIDEAN GEOMETRY

5.0 Introduction.

In Chapter IV, Finite Euclidean geometry was constructed. In it, we have seen that the angles can be given as integers. In the finite hyperbolic Euclidean geometry, the angles can be represented by elements in Z_{p-1} and in finite elliptic Euclidean geometry by elements in Z_{p+1} . The distances can, in either case, be represented elements in Z_p or by δ times an element in Z_p , where δ is such that δ^2 is a non quadratic residue in Z_p .

I made many attempts to define angles and distances for a geometry which can be considered as the finite form of non-Euclidean geometry. The clue was finely provided by the work of Laguerre. I will show that using this definition, both angles and distances can be treated symmetrically, or to use a mathematical terminology, that we have duality between the notions of angle of 2 lines and distance of 2 points.

For those familiar with non-Euclidean geometry, in the classical case, there is a distinction between the hyperbolic non-Euclidean geometry of Lobatchevski and the elliptic non-Euclidean geometry of Bolyai. The axioms, in a form already familiar to Saccheri, are: there exists a triangle whose sum of interior angles is equal to (Euclidean), smaller than (Lobatchevski) or greater than (Bolyai) 180 degrees.

In the hyperbolic case, the set of lines through a point P not on a line l is subdivided into 2 sets, those which intersect l and those who do not. If we assume continuity, there are 2 lines which form the boundary of either set and are called parallels. The simplest model is obtained by starting with the 2 dimensional projective plane and choosing a given conic as ideal. We define as points those inside the conic and as lines the portion of the lines of the projective plane inside the conic. The parallels to l from a point P not on l are those which pass through the intersection of l with the conic.

In the elliptic case, there are no parallels, the lines always intersect. The simplest model is obtained by choosing a sphere in 3 dimensional Euclidean geometry. We define as lines the great circles of a sphere and as points the points of the sphere, identifying each point with its antipode.

In the finite case, there is no distinction between the elliptic and the hyperbolic case.

Indeed in finite projective geometry, the inside or the outside of a conic cannot be defined. Instead, for some lines there are no parallels and for others the situation is analogous to that described in the classical hyperbolic case. For those who like to refer to some geometric picture, the image of the geometry on the sphere will be useful although imperfect. I will refer to it from time to time. Again, although I would find it more satisfactory to proceed synthetically, I will proceed algebraically to reach the goal more quickly.

In finite Euclidean geometry, I proceeded from projective geometry in 3 steps, affine geometry, involutive geometry and Euclidean geometry. Here I will proceed in 2 steps, polar geometry and non Euclidean geometry.

In the involutive geometry, an involution on the ideal line is chosen, from which the notions of perpendicularity and circles are derived. In finite projective geometry, no conic can be distinguished from any other. To define finite non-Euclidean geometry, I proceed in 2 steps. In the first step, I define the finite polar geometry by choosing, or better still, preferring a specific polarity, or equivalently a specific conic. From it, the notions of parallelism, circles, equality of segments, \dots , are derived. In the second step, I introduce the notions of measure of distances and measure of angles, in this case also, the ideal conic plays again an essential role.

5.1 Finite Polar geometry.

5.1.0 Introduction.

After defining the geometry starting from a finite projective geometry in which a given polarity is preferred, I define elliptic, parabolic and hyperbolic points and lines. I then define circles without using the notion of distance, equidistance and the dual notion of equiangularity are, as in finite Euclidean geometry derived notion. After defining perpendicularity, I define special triangles using equidistance and right angles. I then proceed to define mid-points, medians and mediatrices and finally the circumcircles of a triangle. A new point, which I call the center of a triangle is defined using 2 independent methods. This point also exists in classical non-Euclidean geometry, but I have not found any reference in the literature. The intersection of the circumcircles of a triangle are obtained and constructed. Various results obtained while studying the center of a triangle are derived. The circumcircle for the special case of a triangle with an ideal vertex is studied and finally the properties of the parabola are given in detail.

5.1.1 The ideal conic, elliptic, parabolic and hyperbolic points and lines.

Definition.

Among all the conics in the plane, the chosen one is called the ideal conic or the ideal. The points on the conic are called ideal points or parabolic points. The lines tangent to the conic are called ideal lines or parabolic lines. They could also be called isotropic, by analogy with the Euclidean case, but I will not use this terminology.

A line which intersects the ideal in 2 real points is called a hyperbolic line, a point which is

incident to 2 ideal lines is called a hyperbolic point.

A line which does not contain ideal points or a point which is not on an ideal line is called elliptic.

A point or a line is said to be an ordinary point if the point or the line is either elliptic or hyperbolic.

Two points or two lines are said to be of the same type if they are both either elliptic or hyperbolic. Points of the same type are necessarily ordinary.

Convention.

By convention, the conic chosen for the algebraic derivation is

$$X \cdot X = 0 \text{ or } X_0^2 + X_1^2 + X_2^2 = 0.$$

Example.

For $p = 13$, the ideal points are 6, 9, 19, 22, 57, 62, 69, 76, 79, 118, 134, 141, 148, 153.

Theorem.

The polar of $A = (A_0, A_1, A_2)$ with respect to the ideal conic is $\bar{a} = [A_0, A_1, A_2]$.

Notation.

The polar of A will be denoted \bar{a} , the pole of a , \bar{A} .

This notation should not be confused with the notation in section ... on finite projective geometry.

Theorem.

With $j = +1$ or -1 , the ideal points on the line $a = [a_0, a_1, a_2]$ are

0. if $a_1^2 + a_2^2 \neq 0$,
 $(a_1^2 + a_2^2, -a_0a_1 + ja_2\sqrt{d}, -a_0a_2 - ja_1\sqrt{d})$, where
 $d = -(a_0^2 + a_1^2 + a_2^2)$,
1. if $a_1^2 + a_2^2 = 0$ and $a_1.a_2 \neq 0$,
 $(0, a_1 + ja_2\sqrt{-1}, a_2 - ja_1\sqrt{-1})$,
2. if $a_1 = a_2 = 0$,
 $(0, 1, j\sqrt{-1})$.

Example.

For $p = 13$, let $a = [124] = [1, 8, 6]$, then $d = 3$, $\sqrt{d} = 4$, the ideal points on a are $(-4, -8 - 2, -6 - 6) = (1, 9, 3) = (134)$ and $(-4, -8 + 2, -6 + 6) = (1, 8, 0) = (118)$.

Theorem.

The point $A = (A_0, A_1, A_2)$ and the line $\bar{a} = [A_0, A_1, A_2]$ are

- 0. parabolic, iff $A \cdot A = 0$,
- 1. elliptic, iff $-A \cdot A$ is a non quadratic residue modulo p ,
in other words, if there is no integer x such that
$$x^2 = -A \cdot A,$$
- 2. hyperbolic, iff $-A \cdot A$ is a quadratic residue modulo p .

Example.

For $p = 13$, $(6) = (0, 1, 5)$ is parabolic, $(172) = (1, 12, 2)$ is elliptic and $(124) = (1, 8, 6)$ is hyperbolic.

Theorem.

- 0. There are $p + 1$ parabolic or ideal points,
- 1. There are $\frac{p(p-1)}{2}$ elliptic points,
- 2. There are $\frac{p(p+1)}{2}$ hyperbolic points.

Proof: Each of the $p + 1$ parabolic line meets the other p parabolic lines in a hyperbolic point.

Definition.

Two lines are parallel if they have an ideal point in common.

Two points are parallel if they have an ideal line in common.

Example.

For $p = 13$, $(61) = (1, 3, 8)$ and $(71) = (1, 4, 5)$ are parallel, they are on $[134] = [1, 9, 3]$.

Theorem.

The intersections of the sides of a triangle with the polars of the opposite vertex with respect to any conic are collinear.

This follows at once from II.2.2.4.7 if we choose the coordinates in such a way that the conic is the ideal conic.

5.1.2 Circles in finite polar geometry.

Introduction.

There are 3 kinds of circles in polar geometry.

A hyperbolic circle is a conic tangent to the ideal conic at 2 distinct points. Its center is the intersection of these tangents.

An elliptic circle is a conic tangent to the ideal conic at 2 distinct complex conjugate points.

A parabolic circle is one for which the two points of tangency coincide.

I will give now the corresponding algebraic definition, when convention 5.1.1 is used.

Having introduced the notion of circles, it is natural to define the notion of equidistance between points and equiangularity between lines. When measure of angles and distances will be introduced, the compatibility of the 2 concepts equivalence and measure will be made clear.

Definition.

The circles of center $C = (C_0, C_1, C_2)$ are the conics with equation

$$X \cdot X + k(X \cdot C)^2 = 0.$$

Definition.

The line $c = [C_0, C_1, C_2]$ is called the central line of the circle.

Theorem.

The central line is the polar of the center in the polarity associated to the circle as well as in the polarity associated to the ideal conic.

Definition.

A circle is called hyperbolic if its center is hyperbolic, elliptic, if its center is elliptic and parabolic if its center is a parabolic or ideal point.

Theorem.

The ordinary points on a circle are all either hyperbolic or elliptic.

Proof: If k is a quadratic residue modulo p , then $-X \cdot X$ is a quadratic residue and X is necessarily hyperbolic. If k is a non residue, then $-X \cdot X$ is a non residue and X is necessarily elliptic.

Theorem.

If a circle is hyperbolic, the lines through the center and the ideal points on the central line are tangent to both the ideal conic and the circle. If the circle is parabolic, the center C is an ideal point and its polar is the tangent at the ideal point to both the ideal conic and the circle.

All hyperbolic circles can be constructed using the degenerate form of Pascal's construction. The following Theorem allows the construction of parabolic circles and of many elliptic circles.

Theorem.

For any circle of center C and central line c through a point X_1 not on c , if I_1 is an ideal point on $C \times X_1$ and I_2 is a distinct ideal point not on c and $I_1 \times I_2$ meets c in X_0 then $X_2 := (X_0 \times X_1) \times (C \times I_2)$ is also on the circle.

Theorem.

If a circle of center C is not parabolic, let A and B be arbitrary points on the circle, let M and N be the other ideal points on $C \times A$ and $C \times B$, then the central line, $A \times B$ and $M \times N$ pass through the same point.

Example.

For $p = 13$, (see *g13.tab*)

0. One of the hyperbolic circles of center (124) has the equation

$$6(x^2 + y^2 + z^2) + (x + 8y + 6z)^2 = 0,$$

$$\text{or } 7x^2 + 5y^2 + 3z^2 + 5yz - zx + 3xy = 0.$$

It contains the ideal points 118 and 134 and the elliptic points 2, 7, 44, 46, 54, 56, 105, 111, 135, 151, 158, 164.

1. One of the elliptic circles with center (172) has equation

$$2(x^2 + y^2 + z^2) + (x - y + 2z)^2 = 0,$$

$$\text{or } 3x^2 + 3y^2 + 6z^2 - 4yz + 4zx - 2xy = 0.$$

It contains the elliptic points 7, 13, 15, 21, 41, 44, 70, 77, 98, 111, 116, 151, 156, 169.

2. One of the parabolic circles with center (6) has the equation

$$(x^2 + y^2 + z^2) - (y + 5z)^2 = 0,$$

$$\text{or } x^2 + 2z^2 + 3yz = 0.$$

It contains the ideal point 6 and the hyperbolic points 1, 33, 39, 81, 89, 100, 101, 109, 110, 121, 129, 171, 177.

Definition.

Two circles are parallel if they have one ideal point in common. Two circles are concentric if they have the same center.

Theorem.

Two concentric circles have all their ideal points in common. One for the parabolic circles, 2 for the hyperbolic circles.

Definition.

The points A and B are equidistant from the point C iff there exists a circle of center C passing through both A and B .

Theorem.

A and B are equidistant from C iff

$$(A \cdot C)^2 (B \cdot B) = (B \cdot C)^2 (A \cdot A).$$

This suggest the more general definition:

Definition.

The distance between the points A and B is the same as the distance between the points C and D iff

$$(A \cdot B)^2 (C \cdot C)(D \cdot D) = (C \cdot D)^2 (A \cdot A)(B \cdot B).$$

The angle between the lines a and b is the same as the angle between the lines c and d iff

$$(a \cdot b)^2 (c \cdot c)(d \cdot d) = (c \cdot d)^2 (a \cdot a)(b \cdot b).$$

Definition.

The angle between a and b is a right angle iff $a \cdot b = 0$ and the distance between A and B is a right distance iff $A \cdot B = 0$.

Comment.

Although the distance between 2 points A and B has not yet been defined, I will by convention use the notation $d(A, B)$. This will be acceptable, in polar geometry, as long as the notation appears in both sides of an equality. I will later define the distance between 2 points and show that it is consistent with 5.1.2.

Theorem.

The notion of equidistance between pairs of points and the notion of equiangularity between pairs of lines is an equivalence relation, in other words, the relation is

reflexive: $d(A, B) = d(B, A)$,

symmetric: $d(A, B) = d(C, D) \implies d(C, D) = d(A, B)$,

transitive: $d(A, B) = d(C, D)$ and $d(C, D) = d(E, F) \implies d(A, B) = d(E, F)$.

5.1.3 Perpendicularity.**Definition.**

The line b is perpendicular to the line a iff b passes through the pole A of a with respect to the ideal conic, in other words, when a and b are conjugates with respect to the ideal conic.

Theorem.

If the line b is perpendicular to a , then

$$b \cdot a = 0.$$

In other words, the angle between a and b is a right angle.

This follows at once from 5.1.2.

Theorem.

The perpendicular h_0, h_1, h_2 from the vertices A_0, A_1, A_2 of a triangle to the opposite sides have a point H in common. Moreover,

$$h_0 = (A_2 \cdot A_0) A_1 - (A_0 \cdot A_1) A_2,$$

$$h_1 = (A_0 \cdot A_1) A_2 - (A_1 \cdot A_2) A_0,$$

$$h_2 = (A_1 \cdot A_2) A_0 - (A_2 \cdot A_0) A_1.$$

$$H = (A_2 \cdot A_0)(A_0 \cdot A_1) A_1 * A_2 + (A_0 \cdot A_1)(A_1 \cdot A_2) A_2 * A_0 \\ + (A_1 \cdot A_2)(A_2 \cdot A_0) A_0 * A_1.$$

Proof: $h_0 := A_0 * (A_1 * A_2)$, is indeed a line through A_0 perpendicular to $A_1 * A_2$. The results follow easily from II.2.2.4. Related results are obtained in 5.1.4.

Definition.

h_i are called the altitudes of the triangle. The point H is called the orthocenter.

Example.

For $p = 13$, if $A_0 = (0) = (0, 0, 1)$, $A_1 = (18) = (1, 0, 4)$, $A_2 = (67) = (1, 4, 1)$, then $h_0 = (27) = [1, 1, 0]$, $h_1 = [1, 4, 3]$, $h_2 = [1, 0, 12]$ and $H = (171) = (1, 12, 1)$.

Comment.

Section 7 could be placed here, but then the motivation would be absent.

5.1.4 Special triangles.**Definition.**

A right, double right, polar triangle is a triangle which has one, two or three right angles.

A right sided or double right sided triangle is a triangle for which the distance between one pair or two pairs of vertices is a right distance.

Examples.

For $p = 13$: The triangle $A = (8) = (0, 1, 7)$, $B = (17) = (1, 0, 3)$, $C = (36) = (1, 1, 9)$, with sides $[44] = [1, 2, 4]$, $[150] = [1, 10, 6]$, $[161] = [1, 11, 4]$ is a right triangle at B .

The triangle $A = (44)$, $B = (17)$, $C = (36)$, with sides $[44]$, $[130] = [1, 8, 12]$, $[161]$ is a double right triangle at B and C . The triangle $A = (44)$, $B = (17)$, $C = (161)$, with sides $[44]$, $[17]$ $[161]$ is a polar triangle.

Exchanging vertices and sides, we obtain, by duality, examples of right sided and double right sided triangles.

Definition.

A triangle is isosceles if 2 pairs of vertices are equidistant.

A triangle is equilateral if all 3 pairs of vertices are equidistant.

Theorem.

0. If a triangle $\{ABC\}$ is such that $d(A, B) = d(A, C)$, then

$$d(a, b) = d(a, c).$$

1. If a triangle $\{ABC\}$ is such that $d(A, B) = d(B, C) = d(A, C)$, then

$$d(a, b) = d(a, c) = d(b, c).$$

Proof: The second part follows, by transitivity, from the first part. For the first part, let us set $p = A \cdot A$, $q = B \cdot B$, $r = C \cdot C$, $t = B \cdot C$, $u = C \cdot A$, $v = A \cdot B$. The hypothesis implies

$$v^2 r = u^2 q = s.$$

We want to prove that

$$w = (a \cdot b)^2 c \cdot c$$

does not change when we exchange b and c or q and r as well as u and v . Using II.2.2.4.2 and .3, $a \cdot b = ut - vr$ and $c \cdot c = pq - v^2$,

therefore

$$\begin{aligned} w &= (u^2 t^2 + v^2 r^2 - 2tuvr)(pq - v^2) \\ &= pt^2 s - t^2 u^2 v^2 + psqr - s^2 - 2ptgruv - 2tsuv. \end{aligned}$$

Example.

For $p = 13$: The triangle $A = (172) = (1, 12, 2)$, $B = (7) = (0, 1, 6)$, $C = (13) = (0, 1, 12)$, with sides $a = [14] = [1, 0, 0]$, $b = [182] = [1, 12, 12]$, $c = [74] = [1, 4, 8]$ is an isosceles triangle. The triangle $A = (172)$, $B = (7)$, $C = (15) = (1, 0, 1)$, with sides $a = [104] = [1, 6, 12]$, $b = [182]$, $c = [74]$ is an equilateral triangle.

Theorem.

In a polar triangle, each vertex is the pole of the opposite side and the distance between the vertices is a right distance.

Definition.

Two triangles are dual of each other iff the sides of one are the polar of the vertices of the other.

Example.

The dual of the triangle of example 5.1.3 is, with $p = 13$, $A_0 = (173) = (1, 12, 3)$, $A_1 = (53) = (1, 3, 0)$, $A_2 = (1) = (0, 1, 0)$.

Theorem.

A polar triangle is its own dual.

Theorem.

The altitudes of a triangle and of its dual coincide. The orthocenter of a triangle and of its dual coincide.

The proof is left as an exercise.

5.1.5 Mid-points, medians, mediatrices, circumcircles.

Introduction.

For this section, the analogy with the model of the non-Euclidean geometry on the sphere is useful. We recall that each point has 2 representations on the sphere, which are antipodes of each other. If we take 2 points A and B , let A' and B' be their antipodes, there are 2 points on the great circle, (in the plane through the center of the sphere) which are equidistant from A and B , namely a point on the arc AB and a point on the arc $A'B$, which is the antipode of the mid-point on the arc AB' . But the analogy is not complete, in the finite case, it is only when the points are of the same type that mid-points exist. There is about 1 chance in 2 that the points are not of the same type, there are then no mid-points, there is about 1 chance in 2 that they are of the same type, there are then 2 mid-points, this is an other example of what I call the law of compensation.

To simplify the algebra, I will introduce a scaling in 5.1.5. The scaling contains an arbitrary sign, which may be thought as corresponding to the 2 representations on the sphere. The systematic way which is chosen could be replaced by some other one. The choice is influenced by the choice of a primitive root of p and the sign of the square root and depends on the rule Having the concept of mid-points, we can consider those of the vertices of a triangle, if the vertices are scaled, we can define interior and exterior mid-points. Again, the choice is arbitrary and depends on the rule

To each side correspond 2 medians, these meet 3 by 3 in 4 points corresponding to the barycenter. Again the analogy with the geometry on the sphere is useful, the 4 barycenters can be considered as corresponding to the triangles $\{ABC\}$, $\{A'BC\}$, $\{AB'C\}$, $\{ABC'\}$.

A similar treatment can be made for the mediatrices which meet 3 by 3 in 4 points, each is the center of a circumcircle of the triangle $\{ABC\}$.

But, again, the analogy with the geometry on the sphere is not complete. Given a triangle, there are about 3 chances in 4 that the 3 vertices are not all of the same type, in this case there is no barycenter and no circumcircle. In about 1 chance out of 4, the 3 points are of the same type, and there are 4 barycenters and 4 circumcircles. Again this is the compensation. If the vertices of the triangle are of the same type, the 4 lines joining a barycenter to the corresponding center of a circumcircle can be considered as generalizations of the line of Euler. It is natural to conjecture that these four lines are concurrent. This is indeed the case. The surprise is that this point V is not the orthocenter. The coordinates of V are real even if the vertices of the triangle are not of the same type. V must therefore be obtainable in an independent way. One such method is described in section 7.

I first recall the convention of I.??.

Convention.

Given δ a specific square root of a specific non quadratic residue of p , we choose the square root a of a quadratic residue or the square root $a\delta$, of a non residue in such a way that $0 \leq a < \frac{p-1}{2}$.

Notation.

Using the preceding convention, a square root is uniquely defined. It is convenient to introduce an other scaling for points and lines different from that given in II.2.2.1.

If $A = (A_0, A_1, A_2)$ and A is not an ideal point,

$$A' = \frac{A}{\sqrt{-A \cdot A}}.$$

$|A| = \sqrt{-A \cdot A}$ is called the length of A . Either each component is an integer, or each component is an integer divided by δ , in this last case we say that A' is pure imaginary.

Theorem.

If A is hyperbolic, A' is real, if A is elliptic, A' is pure imaginary. Moreover $A' \cdot A' = -1$.

Definition.

Given 2 points A and B of the same type, M on $A \times B$ is called a mid-point of $[A, B]$ iff the distances MA and MB are equal.

Theorem.

The mid-points of $[A, B]$ are $M = A' + B'$ and $M^- = A' - B'$.

Proof: Because of 5.1.2, $d(M, A) = d(M, B)$ if

$$(M \cdot A')^2 = (M \cdot B')^2,$$

or if $(A' \cdot A')^2 + (A' \cdot B')^2 + 2(A' \cdot A')(A' \cdot B')$

$$= (B' \cdot B')^2 + (B' \cdot A')^2 + 2(B' \cdot B')(B' \cdot A'),$$

which is satisfied because of $A' \cdot A' = B' \cdot B' = -1$ and

$$A' \cdot B' = B' \cdot A'.$$

The proof is similar for M^- .

Definition.

M is called the interior mid-point, M^- is called the exterior mid-point.

Example.

For $p = 13$, the mid-points of $(44) = (1, 2, 4)$ and $(164) = (1, 11, 7)$ are $(115) = (1, 7, 10)$ and $(124) = (1, 8, 6)$. Indeed $|44| = \sqrt{5}$, $|164| = \sqrt{11}$, hence, $\frac{|44|}{|164|} = \sqrt{\frac{-8}{-2}} = \sqrt{4} = 2$, therefore the mid-points are $(1, 2, 4) + 2(1, 11, 7) = (3, 24, 18) = (1, 8, 6)$ and $(1, 2, 4) - 2(1, 11, 7) =$

$(-1, -20, -10) = (1, 7, 10)$.

With $\delta^2 = 8$, $A' = \frac{A}{\delta}$, $B' = \frac{B}{(6\delta)}$, therefore the interior mid-point is $A + \frac{1}{6}B = A - 2B = (1, 7, 10)$ and the exterior mid-point is $A - \frac{1}{6}B = A + 2B = (1, 8, 6)$.

Definition.

m is called a mediatrix of $[A, B]$ iff m is perpendicular to $A \times B$ and passes through a mid-point of $[A, B]$.

Theorem.

$m := A' - B'$ passes through $M = A' + B'$ and

$m^- := A' + B'$ passes through $M^- = A' - B'$.

Proof: m is perpendicular to $A \times B$ because

$$m \cdot (A * B) = m \cdot (A' * B') = A' \cdot (A' * B') - B' \cdot (A' * B') = 0.$$

m passes through M , because $m \cdot M = (A' - B') \cdot (A' + B') = A' \cdot A' - B' \cdot B' = -1 - (-1) = 0$.

Theorem.

The set of points equidistant from A and B are on m or m' .

Definition.

In a triangle, the line joining a vertex to the interior (exterior) mid-points of the opposite side is called an interior (exterior) median.

Theorem.

If a triangle is isosceles, with $d(A_0, A_1) = d(A_0, A_2)$, then a median through A_0 is also a mediatrix.

5.1.6 The center V of a triangle.

Theorem.

Let M_i and M_i^- be the interior and exterior mid-points of A_{i-1} and A_{i+1} , let n_i and n_i^- be the interior and exterior medians associated to A_i .

$$0. G_3 := n_0 \times n_1 \Rightarrow G_3 \cdot n_2 = 0. (*)$$

$$1. G_i := n_i \times n_{i+1}^- \Rightarrow G_i \cdot n_{i-1}^- = 0 (*).$$

Let m_i and m_i^- be the interior and exterior mediatrices of $A_{i+1}A_{i-1}$.

$$2. O_3 := m_0 \times m_1 \Rightarrow O_3 \cdot m_2 = 0. (*)$$

$$3. O_i := m_i \times m_{i+1}^- \Rightarrow O_i \cdot m_{i-1}^- = 0. (*)$$

$$4. e_j := O_j \times G_j \text{ and } V := e_0 \times e_1 \Rightarrow V \cdot e_2 = V \cdot e_3 = 0. (*)$$

The proof follows from Theorem 4.4.12. As in finite Euclidean geometry “*” indicates that there are equivalent definitions, for instance 0 could be written $G_3 := n_1 \times n_2$ and $G_3 \cdot n_0 = 0$.

Definition.

By analogy with Euclidean geometry, the points G_j are called the barycenters of the triangle. The points O_j are called the centers of the circumcircles of the triangle. The lines e_j are called the lines of Euler of the triangle.

Definition.

V is called the center of the triangle.

Theorem.

Let A'_i be the normalized coordinates of the vertices of a triangle¹.

0. The mid points are $A'_{i-1} + j_i A'_{i+1}$, $j_i = +1$ or -1 .
1. The mediatrices are $A'_{i-1} - j_i A'_{i+1}$.
2. The medians n_i are $A'_i \times (A'_{i-1} + j_i A'_{i+1})$.
3. Choosing $j_0 j_1 j_2 = 1$, the medians meet 3 by 3 at the 4 barycenters which are $A'_0 + j_2 A'_1 + j_1 A'_2$.
4. The mediatrices meet 3 by 3 at the 4 centers of circumcircles, which are $A'_1 * A'_2 + j_2 A'_2 * A'_0 + j_1 A'_0 * A'_1$.
5. The Euler lines, joining G_j to O_j are, with $d'_i = A'_{i-1} \cdot A'_{i+1}$, $(j_0 d'_1 - d'_2) A'_0 + (j_2 d'_2 - j_0 d'_0) A'_1 + (d'_0 - j'_2 d'_1) A'_2$.
6. The Euler lines intersect at V and $V = d'_0 A'_1 * A'_2 + d'_1 A'_2 * A'_0 + d'_2 A'_0 * A'_1$.
7. Moreover, $V = A_0 \cdot A_0 A_1 \cdot A_2 A_1 * A_2 + A_1 \cdot A_1 A_2 \cdot A_0 A_2 * A_0 + A_2 \cdot A_2 A_0 \cdot A_1 A_0 * A_1$.
8. V exists when the triangle is not a polar triangle.

Proof: 0. and 1. follow from For 2., the intersection of n_1 and n_2 is

$$\begin{aligned} n_1 * n_2 &= -A'_0 (A'_2 \cdot (A'_1 * A'_0)) \\ &\quad + j_1 A'_2 (A'_0 \cdot (A'_1 * A'_2)) \\ &\quad + j_0 j_1 A'_1 (A'_0 \cdot (A'_1 * A'_2)) \\ &= A'_0 + j_0 j_1 A'_1 + j_1 A'_2. \end{aligned}$$

The same point is obtained if $j_0 j_1 = j_2$ or if $j_0 j_1 j_2 = 1$. There are 4 points corresponding to $j_0 = +\text{or} -1$ and $j_1 = +\text{or} -1$.

The proof of 3. is similar. The proof of 4. to 8. is left as exercises.

¹21.9.81

Comment.

Reality requires, because $A'_i = \frac{A_i}{|A_i|}$ that the lengths $|A_i|$ be either all real or all imaginary, hence:

Theorem.

The mid-points, mediatrices, medians, barycenter and center of circumcircles are real if and only if the vertices are either all elliptic or all hyperbolic. V is always real.

Example.

For $p = 13$, the triangle $A_0 = (58) = (1, 3, 5)$, $A_1 = (51) = (1, 2, 11)$, $A_2 = (159) = (1, 11, 2)$, has all its vertices hyperbolic.

Let $A'_0 = (6, 5, 4)$, $A'_1 = (6, -1, 1)$, $A'_2 = (6, 1, -1)$. The mid-points of A_1 and A_2 are $(14) = (1, 0, 0)$ and $(13) = (0, 1, 12)$. All the mid-points are (14) , (13) ; (115) , (12) ; (139) , (8) .

The mediatrices are $[13]$, $[14]$; $[12]$, $[115]$; $[8]$, $[139]$.

The medians are $[3]$, $[126]$; $[91]$, $[176]$; $[76]$, $[161]$.

The interior mediatrices $[13]$, $[12]$, $[8]$ meet at $O_3 = (14)$.

The centers of the circumcircles are (56) , (8) , (12) and (14) .

The interior medians $[3]$, $[91]$, $[76]$ meet at $G_3 = (33)$.

The barycenters are (152) , (179) , (106) , and (33) .

The center of the triangle is $V = (152)$.

5.1.7 An alternate definition of the center V of a triangle.**Notation.**

From here on, the following notation will be used systematically:

$$0. a_i := A_{i+1} \times A_{i-1}$$

$$1. n_i := \frac{A_{i+1} * A_{i-1}}{a_i} \text{ which means that } A_{i+1} * A_{i-1} = n_i a_i, \text{ defines } n_i, \\ n_i \text{ is the normalization factor, see 2.3.2. and 2.3.11.}$$

$$2. l_i := A_i \cdot A_i,$$

$$3. d_i := A_{i+1} \cdot A_{i-1},$$

$$4. t := (A_0 * A_1) \cdot A_2. \\ \text{Similarly,}$$

$$5. N_i := \frac{a_{i+1} * a_{i-1}}{A_i} \text{ which means that } a_{i+1} * a_{i-1} = N_i A_i, \text{ defines } N_i,$$

$$6. L_i := a_i \cdot a_i,$$

$$7. D_i := a_{i+1} \cdot a_{i-1},$$

$$8. T := (a_0 * a_1) \cdot a_2.$$

Theorem.

$$0. \ t = n_1 n_2 N_0 = n_2 n_0 N_1 = n_0 n_1 N_2.$$

$$1. \ n_i^2 L_i = n_i^2 a_i \cdot a_i = l_{i+1} l_{i-1} - d_i^2.$$

$$2. \ n_{i+1} n_{i-1} D_i = n_{i+1} n_{i-1} a_{i+1} \cdot a_{i-1} \\ = d_{i+1} d_{i-1} - d_i l_i.$$

$$3. \ n_0 n_1 n_2 T = t^2.$$

and the dual relations

$$4. \ T = N_1 N_2 n_0 = N_2 N_0 n_1 = N_0 N_1 n_2.$$

$$5. \ N_i^2 l_i = N_i^2 A_i \cdot A_i \\ = L_{i+1} L_{i-1} - D_i^2.$$

$$6. \ N_{i+1} N_{i-1} d_i = N_{i+1} N_{i-1} A_{i+1} \cdot A_{i-1} \\ = D_{i+1} D_{i-1} - D_i L_i.$$

$$7. \ N_0 N_1 N_2 t = T^2.$$

Theorem.

$$0. \ a_{i+1} * a_{i-1} = t A_i,$$

$$1. \ n_i a_i * A_i = d_{i-1} A_{i-1} - d_{i+1} A_{i+1}.$$

$$2. \ n_i a_i * A_{i+1} = l_{i+1} A_{i-1} - d_i A_{i+1}.$$

$$3. \ n_i a_i * A_{i-1} = d_i A_{i-1} - l_{i-1} A_{i+1}.$$

The proof follows easily from 2.3.17. and from 4.6.0.

Example.

For $p = 13$, with

$A[] = \{(0) = (0, 0, 1), (18) = (1, 0, 4), (67) = (1, 4, 1)\}$, then

$a[] = \{[173] = [1, 12, 3], [53] = [1, 3, 0], [1] = [0, 1, 0]\}$.

$l[] = [1, 4, 5], d[] = [5, 1, 4], n[] = [10, 4, 1],$

$L[] = (11, 10, 1), D[] = (3, 12, 11), N[] = (1, 3, 4),$

$t = [4], T = (3).$

Theorem.

Let h be the polar of H with respect to the triangle. Let K_i be the intersection of h and a_i ,

let v_i be the perpendicular at A_i to $A[i] \times K_i$.

Then v_i have a point in common V^3 .

Moreover, if we define

$$0. \quad u_i := d_{i+1}d_{i-1} - d_i l_i, \\ \text{we have}$$

$$1. \quad h = u_0 a_0 + u_1 a_1 + u_2 a_2.$$

$$2. \quad K_i = u_{i-1} A_{i+1} - u_{i+1} A_{i-1}.$$

$$3. \quad v_i = (d_{i+1}^2 l_{i+1} - d_{i-1}^2 l_{i-1}) A_i - (d_i d_{i+1} l_i - d_{i-1} l_{i-1} l_i) A_{i+1} + (d_i d_{i-1} l_i - d_{i+1} l_{i+1} l_i) A_{i-1}.$$

$$4. \quad V = d_0 l_0 A_1 * A_2 + d_1 l_1 A_2 * A_0 + d_2 l_2 A_0 * A_1.$$

Proof: Because of 5.1.3,

$$H = d_1 d_2 a_0 + d_2 d_0 a_1 + d_0 d_1 a_2,$$

after simplification,

$$H \cdot a_0 = (d_0 d_1 - d_2 l_2)(d_2 d_0 - d_1 l_1),$$

using the definition 0, $H \cdot a_0 = u_2 u_1$, and because of 2.3.20, after multiplication by $u_0 u_1 u_2$, we obtain 1.

$K_i := H * a_i$, gives 2, after division by t .

$$A_i * K_i = u_{i+1} a_{i+1} + u_{i-1} a_{i-1},$$

therefore,

$$V_i = A_i * (A_i * K_i),$$

substituting and using 2.3.17.0., we get

$$V_i = (u_{i-1} d_{i-1} - u_{i+1} d_{i+1}) A_i - u_{i-1} l_i A_{i+1} + u_{i+1} l_i A_{i-1},$$

replacing u_i by its value, we get, 3, from which we obtain

$$v_1 * v_2 = d_0 l_0 A_1 * A_2 + d_1 l_1 A_2 * A_0 + d_2 l_2 A_0 * A_1,$$

after dividing each term by

$$(d_2^2 d_1 l_2 + d_1^2 d_0 l_1 + d_0 l_0 l_1 l_2 - d_0^3 l_0 - 2d_1 d_2 l_1 l_2).$$

5.1.8 Intersections of the 4 circumcircles.

Introduction.

In this section we study the 4-th point of intersection of the 4 circumcircles of a triangle. The expression for these 6 points is given in 5.1.8. A construction in the case where the centers of the 2 circles are given is described in 5.1.8.

²13.10.81

³19.10.81

Notation.

\mathcal{C}_i denotes the circumcircle with center C_i .

$X_{j,k}$ denotes the intersection of \mathcal{C}_j and \mathcal{C}_k distinct from the vertices of the triangle A_i , normalized to A'_i .

$$\begin{aligned} a_i &:= A'_i \cdot A'_2, \\ d &:= A'_0 * (A'_1 * A'_2). \end{aligned}$$

Theorem.

4

The intersections of the circumcircles of a triangle A_i are given, using 5.1.8.

$$\begin{aligned} X_{0,3} &= (1 + a_0) A'_0 + (a_2 - a_1) (A'_1 - A'_2), \\ X_{1,3} &= (1 + a_1) A'_1 + (a_0 - a_2) (A'_2 - A'_0), \\ X_{2,3} &= (1 + a_2) A'_2 + (a_1 - a_0) (A'_0 - A'_1), \\ X_{1,2} &= (1 - a_0) A'_0 + (a_1 + a_2) (A'_1 + A'_2), \\ X_{2,0} &= (1 - a_1) A'_1 + (a_2 + a_0) (A'_2 + A'_0), \\ X_{0,1} &= (1 - a_2) A'_2 + (a_0 + a_1) (A'_0 + A'_1). \end{aligned}$$

Proof: Let $B_i := A'_{i+1} * A'_{i-1}$, then

$$\begin{aligned} C_0 &= -B_0 + B_1 + B_2, \\ C_3 &= B_0 + B_1 + B_2, \end{aligned}$$

the circles with these centers are

$$kX^2 = (X \cdot C_3)^2 \text{ and } kX^2 = (X \cdot C_0)^2,$$

they pass through the vertex A_0 of the triangle if

$$k - 1 = (A_0 \cdot B_0)^2 = d^2$$

and therefore also through the vertices A_1 and A_2 if $k = -d^2$. X is common to the 2 circles if $X \cdot C_0 = jX \cdot C_3$ ($j = +1$ or -1),

$j = +1$ leads to the vertices A'_1 or A'_2 , $j = -1$ gives

$$\begin{aligned} X \cdot (C_0 + C_3) &= 2X \cdot (B_1 + B_2) = \\ 2X \cdot (A'_0 * (A'_1 - A'_2)) &= 0. \end{aligned}$$

therefore, for some l , and with $M_0^- = A'_1 - A'_2$,

$$X = lA'_0 + M_0^-,$$

hence

$$\begin{aligned} X^2 &= -l^2 + (M_0^-)^2 + 2lA'_0 \cdot M_0^-, \text{ and} \\ X \cdot C_3 &= (lA'_0 + M_0^-) \cdot (B_0 + A_0 * M_0^-) = lA'_0 \cdot B_0 = ld. \end{aligned}$$

X is on the circles \mathcal{C}_3 if

$$-d^{2(-l^2)} + (M_0^-)^2 + 2lA'_0 \cdot M_0^- = l^2d^2,$$

therefore

$$l = -\frac{(M_0^-)^2}{2A'_0 \cdot M_0^-} = -\frac{-2(1+a_0)}{2(a_2-a_1)}$$

hence the expression for $X_{0,3}$. The other points are derived similarly.

Corollary.

The intersections $X_{1,3}$ and $X_{2,3}$ coincide if

$$1 - a_0 + a_1 + a_2 = 0$$

⁴Salzburg-Innsbruck 29-30.9.83

and

$$X_{1,3} = X_{2,3} = -A'_0 + A'_1 + A'_2,$$

with similar expressions for other pairs.

The proof is straightforward.

Example.

With the triangle of 5.1.6, $a_i = 5$,

$$X_{0,3} =$$

$$X_{1,3} =$$

$$X_{2,3} =$$

$$X_{1,2} =$$

$$X_{2,0} =$$

$$X_{0,1} =$$

Theorem.

Let $M_{0,0}$, $M_{0,1}$ be the mid-points of a_0, \dots , in the algebraic order defined above, then

0. the dual lines are the mediatrices,
the dual of $M_{0,1}$ passes through $M_{0,1}$, \dots
1. the points $M_{0,1}$, $M_{1,0}$, $M_{2,0}$ are on o_0 ,
the points $M_{0,0}$, $M_{1,1}$, $M_{2,0}$ are on o_1 ,
the points $M_{0,0}$, $M_{1,0}$, $M_{2,1}$ are on o_2 ,
the points $M_{0,1}$, $M_{1,1}$, $M_{2,1}$ are on o_3 .
2. the dual of o_i is the center O_i of one of the 4 circumcircles of the triangle A_i .
3. By duality, the mediatrices $m_{0,0}$, $m_{1,1}$, $m_{2,1}$ are on O_0, \dots .

Let $m'_{0,0}$, $m'_{0,1}$, \dots be the medians $A_0 \cdot M_{0,0}$, $A_0 \cdot M_{0,1}$, \dots then

4. the medians $m'_{0,0}$, $m'_{1,1}$, $m'_{2,1}$ are on G_0 ,
the medians $m'_{0,1}$, $m'_{1,0}$, $m'_{2,1}$ are on G_1 ,
the medians $m'_{0,1}$, $m'_{1,1}$, $m'_{2,0}$ are on G_2 ,
the medians $m'_{0,0}$, $m'_{1,0}$, $m'_{2,0}$ are on G_3 .

Notation.

$u * v$ is the vector $(u_1v_2 - u_2v_1, u_2v_0 - u_0v_2, u_0v_1 - u_1v_0)$

$u \rtimes v$ is the vector $(u_1v_2 + u_2v_1, u_2v_0 + u_0v_2,$
 $u_0v_1 + u_1v_0)$

$u O v$ is the vector (u_0v_0, u_1v_1, u_2v_2)

Algorithm.

Given two circles through the points A_i , with centers C_0 and C_1 , With j in the set $\{0, 1\}$ and i in the set $\{0, 1, 2\}$, and addition within the indices done modulo 2,

$$\begin{aligned} d_j &:= C_j O C_j, \\ B_i &:= a_{i+1} X a_{i+2}, \\ L &:= d_0 * d_1, \\ f_i &:= B_i \cdot L, \\ G &:= f O f, \\ s_i &:= \frac{a_{i+1} a_{i+2}}{A_i}, \\ O &:= \sum_{i=0}^3 (s_i G_i A_i). \end{aligned}$$

Theorem.

O is the 4-th point common to the two circles.

5.1.9 Other results in the geometry of the triangle.**Introduction.**

The following results were obtained while searching for a construction of V , independent from the centers of mass and center of circumcircles.

Theorem.

Let I be an ideal point on the line $I \times B$. Let

$$J := (B \cdot B) I - 2(I \cdot B) B,$$

then J is the other ideal point on $I \times B$.

Example.

For $p = 13$,

Let $I = (22) = (1, 0, 8)$ and $B = (4) = (0, 1, 3)$, then

$$J = -3(1, 0, 8) + 4(0, 1, 3) = (1, 3, 4) = (57).$$

The line $I \times J$ is $[48] = [1, 2, 8]$.

Theorem.

Let a be an ordinary line and B an ordinary point not on a .

Let I and K be the ideal points on a and J and L be the other ideal points on $I \times B$ and $K \times B$, let $c := J * J J$, then

$$c = (B \cdot B) a - 2(a \cdot B) \overline{B}.$$

Proof: With $a = I * K$,

$$J = (B \cdot B) I - 2(I \cdot B) B, \quad L = (B \cdot B) K - 2(K \cdot B) B, \quad \text{hence}$$

$$L * J = (B \cdot B)^2 K * I + 2(B \cdot B)((K \cdot B) I - (I \cdot B) K) * B,$$

$$= (B \cdot B)(-(B \cdot B) a + 2((K * I) * B) * B)$$

because of 2.3.17.0.,

$$\begin{aligned}
&= (B \cdot B)(-(B \cdot B) a - 2(a * B) * B), \\
&= (B \cdot B)(-(B \cdot B) a + 2(B \cdot B) a - 2(a \cdot B) B)
\end{aligned}$$

because of 2.3.17.0., hence the Theorem.

Example.

For $p = 13$, let $a = [139] = [1, 9, 8]$ and $B = (4)$, then $c = -3[1, 9, 8] - 1[0, 1, 3] = [1, 5, 9] = [88]$.

The ideal points are $I = 22$, $J = 57$, $K = 76$, $L = 79$.

Definition.

c as defined in the preceding theorem is called the conjugate of a with respect to B .

Theorem.

The lines

$$x_{i+1}A_{i+1} - x_{i-1}A_{i-1} + y_{i-1}n_{i-1}a_{i-1} - y_{i+1}a_{i+1}$$

are concurrent at the point

$$\begin{aligned}
&\sum_i (y_{i+1}y_{i-1}t + (x_id_{i+1} - x_{i-1}l_{i-1})y_{i+1} + (x_id_{i-1} - x_{i+1}l_{i+1})y_{i-1}) A_i \\
&\quad + \sum_i (x_{i+1}x_{i-1}n_i) a_i.
\end{aligned}$$

Theorem.

Given a triangle A_i with sides a_i , let b_i be the conjugate of a_i with respect to A_i . Assume that the b_i are not collinear. Let B_i be the vertices of the triangle b_i , then

0. $A_i \times B_i$ are concurrent at W_0 .

1. $A_i \times \bar{b}_i$ are concurrent at H .

2. $B_i \times \bar{b}_i$ are concurrent at W_1 .

Moreover,

3. $b_i = l_i A_{i+1} * A_{i-1} - 2t A_i$.

4. $B_i = -3l_{i-1}l_{i+1}A_i + 2l_{i-1}d_{i-1}A_{i+1} + 2l_{i+1}d_{i+1}A_{i-1} + 4tA_{i+1} * A_{i-1}$.

5. $A_i * B_i = l_{i+1}d_{i+1}A_i * A_{i-1} - l_{i-1}d_{i-1}A_{i+1} * A_i + 2td_{i+1}A_{i+1} - 2td_{i-1}A_{i-1}$.

6. $W_0 = \sum_i ((-3l_{i-1}l_{i+1}d_{i-1}d_{i+1})A_i + 2d_i(l_{i-1}d_{i-1}^2 + l_{i+1}d_{i+1}^2)A_i + 4td_{i+1}d_{i-1}A_{i+1} * A_{i-1})$.

7. $A_i \times \bar{b}_i = d_{i+1}A_{i+1} - d_{i-1}A_{i-1}$.

8. $H = d_1d_2A_1 * A_2 + d_2d_0A_2 * A_0 + d_0d_1A_0 * A_1$.

9. With

$$\begin{aligned} x_i &= 8t^2d_i + 2l_{i+1}l_{i-1}d_{i+1}d_{i-1} - l_0l_1l_2d_i \text{ and} \\ y_i &= 4tl_id_i, \\ B_i \times \bar{b}_i &= x_{i+1}A_{i+1} - x_{i-1}A_{i-1} + y_{i-1}A_i * A_{i+1} - y_{i+1}A_{i-1} * A_i. \end{aligned}$$

10. $W_1 =$

Proof: 3., is immediate,

Using 2.3.17.0 and 1.7.2., we obtain .4 after division by t ,

5. and 6. after division by t , 7. after division by l_i .

8. is immediate and is indeed the same as 1.3.3.

Example.

For $p = 13$, using the same triangle as Example 1.7.4.

$$B_i = \{9 = (0, 1, 8), 137 = (1, 9, 6), 61 = (1, 3, 8)\},$$

$$b_i = \{180 = [1, 12, 10], 101 = [1, 6, 9], 80 = [1, 5, 1]\},$$

$$W_0 = 7 = (0, 1, 6), H = 171 = (1, 12, 1), W_1 = 77 = (1, 4, 11).$$

Exercise.

Using the dual triangle, $A_i = \{175, 53, 1\}$, determine B_i , b_i and W_0 , H and W_1 .

5.1.10 Circumcircle of a triangle with at least one ideal vertex.

Introduction.

In the preceding section I have dealt with circumcircles through 3 ordinary points. I will now discuss the case when 1 or more points are ideal points.

Theorem.

The only circle through 3 distinct ideal points is the ideal conic, $X^2 = 0$.

Theorem.

The only circle through 2 distinct ideal points A and B and through an ordinary point C is $(c \cdot C)^2X^2 - (c \cdot X)^2C^2 = 0$, where

$$c := A \times B.$$

Example.

$$p = 11, A = (31) = (1, 3, 2), B = (26) = (1, 2, 4),$$

$C = 54 = (1, 6, 4)$. The circumcircle through A , B and C is

$$X_0^2 + X_1^2 + X_2^2 = 4(X_0 - 2X_1 - X_2)^2.$$

Theorem.

There are 2 circles through 1 ideal point A and through two distinct ordinary points B and C not collinear with A .

Theorem.

Let X be a point not on the sides of a triangle A_i . Let X_i be the intersection with a_i of the line $A_i \times X$, or

$$X_i := (A_i \times X) \times a_i,$$

Let ξ be a circle through X_i .

Let Y_i be the other intersection of a_i with ξ ,

let $y_i := A_i \times Y_i$,

then the lines y_i have a point Y in common.

Comment.

The theorem 5.1.10 is analogous to theorem ... in Euclidean geometry. It follows from its generalization ... to projective geometry.

Because of the clear connection with the Theorem of Ceva, I have the following:

Definition.

The correspondence X to the various points Y associated to the several circumcircles through X_i , is called the Ceva correspondence. I will ignore those points Y which happen to coincide with a vertex of the triangle.

Comment.

Clearly if Y is associated to X , X is associated to Y in a Ceva correspondence. But we cannot call this an involution because the correspondence is not one to one or bijective.

Program.

The program NETR1.BAS determines the Ceva correspondence. It is illustrated in NETR1.HOM.

5.1.11 The parabola in polar geometry.**Introduction.**

In this section I have defined a parabola for non Euclidean geometry and many of the related elements of the parabola, by analogy with the definitions of Euclidean geometry. By duality we essentially double the number of these elements, for instance to the focus in Euclidean geometry corresponds the focal point and the focal line. The basic equation is given by 5.1.11.0.

Definition.

A parabola is a conic which is tangent at one point to the ideal conic and at one point only. This point is called the isotropic point of the parabola, the tangent is called the isotropic line of the parabola.

Definition.

A focal tangent t_1 of a parabola is an ideal tangent to the parabola which is not isotropic. A focal point F_1 is an ideal point which is not isotropic. There are 2 focal points F_1 and F_2 which are either real or complex conjugate.

Definition.

The focus F of a parabola is the intersection of the focal tangents. The focal line f of a parabola is the line through the focal points.

Theorem.

The focus is not on the isotropic line. The focus is not an ideal point.

Proof: In the first case, through the focus we could draw 3 tangents to the parabola. In the second case, the parabola would be tangent at a second point to the ideal conic and would therefore be a circle.

Definition.

The director D of a parabola is the pole of its focal line with respect to the parabola.

Definition.

The axis a of a parabola is the line through its focus and its isotropic point. The axial point A of a parabola is the point on the focal line and on the isotropic line.

Definition.

The vertex V of a parabola is the ordinary point on the parabola and its axis. The vertical line v of a parabola is the ordinary tangent through the axial point.

Theorem.

A parabola with isotropic point I and focal tangent f is

$$0. \quad 2(I \cdot X)(f \cdot X) = t(X \cdot X), \quad f \cdot I \neq 0, \quad f \cdot f \neq 0, \quad t \neq 0, \quad t \neq f \cdot I.$$

The polar of X_0 is

$$1. \quad (I \cdot X_0)f + (f \cdot X_0)I - tX_0.$$

The pole of a is

$$2. (f * I) \cdot aI * f + t(a \cdot f)I + t(a \cdot I)f + (t^2 - 2tI \cdot f)a.$$

Proof: 0, follows from the general equation of a conic through the intersections of the ideal and the lines \bar{I} and f , see ... and from 5.1.11.11.4.

0, represents a degenerate conic corresponding to the lines \bar{I} and f if $t = 0$ and to the lines $I \times F1$ and $I \times F2$ if $t = f \cdot I$.

The proof of the last fact is left as an exercise. 1 follows from 0. See 2 is obtained by choosing 2 points on a , $a * I$ and $f * a$, and determining the intersection of the polars of these lines.

$(f * I) \cdot a$ is a factor of each term.

Example.

For $p = 13$, $I = (1, 5, 0)$, $f = [1, 1, 4]$, $t = 4$,

The parabola is

$$2(x + 5y)(x + y + 4z) = 4(x^2 + y^2 + z^2).$$

The polar of $X0 = (x0, y0, z0)$ is

$$[-x0 + 3y0 + 2z0, 3x0 + 3y0 - 3z0, 2x0 - 3y0 - 2z0].$$

The pole of $a = [a0, b0, c0]$ is

$$[a0 + c0, b0 + 5c0, a0 + 5b0 + 6c0].$$

The director D is $(1, -1, 6)$.

The axial point A is $I * f = (1, 5, 5)$.

With $v^2 = -2$, the ideal points on the parabola are I and

$$F1 = (1, 3 + 3v, -1 - 4v), F2 = (1, 3 - 3v, -1 + 4v).$$

The tangent at $F1$ is

$$f1 = (v - 6)[6 + v, 2 - 5v, -5 - v] = [1, -2 + 6v, 6 + v]$$

The ideal lines $t1 = [1, 3, 4]$ and $t2 = [1, -5, 0]$ are tangent to the parabola at $T1 = (1, 2, -5)$ and $T2 = (2, -5, 2)$, they meet at the focus $F = (1, -5, -3)$.

The directrix is $[1, 4, 4]$.

The axis a is $I * F = [1, 5, 5]$.

The vertex V is $(1, -2, -6)$.

The tangent at the vertex is $[1, 4, 1]$.

The vertical line v is $[1, 4, 1]$.

Theorem.

The polar of X is $\sum_j A_{i,j} X_j$, with

$$A_{j,j} = 2I_j f_j - t,$$

$$A_{j,k} = I_j f_k + I_k f_j, j \neq k,$$

The pole of a is $\sum_k B_{j,k} a_k$, with

$$B_{j,j} = t^2 - 2t(I \cdot f - I_j f_j) - (I * f)_j^2,$$

$$B_{j,k} = t(I_j f_k + I_k f_j) - (I * f)_j (I * f)_k.$$

The dual equation of the conic is

$$2(I \cdot x)(F \cdot x) = u(x \cdot x),$$

The pole of x is $(I \cdot x)F + (F \cdot x)I - ux$ and F and u follow from ...

if $I_j \neq \text{frac}10$, $u = (I_0 B_{0,0} + I_1 B_{1,1} - 2I_0 I_1 B_{0,1})$,

$$\begin{aligned}
& F_j = \frac{u+B_{j,j}}{2I_j}, \\
& \text{if } I_2 = 0, \text{ and } I_1 \neq 0, u = -B_{2,2}, \\
& F_0 = \frac{B_{0,0}-B_{2,2}}{2I_0}, \\
& F_1 = \frac{B_{1,1}-B_{2,2}}{2I_1}, \\
& F_2 = \frac{B_{0,2}}{I_0}, \\
& \text{if } I = (1, 0, 0), u = -B_{1,1}, \\
& F_0 = \frac{B_{0,0}-B_{1,1}}{2}, F_1 = B_{0,1}, F_2 = B_{0,2}.
\end{aligned}$$

Proof: The matrix A follow from (1), the matrix B is its adjoint divided by 2.

Theorem.

The director is

$$D = (f \cdot f)I + (t - f \cdot I)f.$$

Proof: Replace a by f in 5.1.11.2.

Exercise.

Complete the following sentences, for the parabola 5.1.11.0:

0. The axis a is .
1. The axial point A is .
2. The vertex V is .
3. The vertical line v is .
4. The ideal point J is .

Theorem.

0. The vertical line v passes trough the vertex V .
1. The director D , the pole \bar{f} of the focal line f , the pole \bar{d} of the directrix d are all on the axis a .
2. The directrix d , the polar \bar{F} of the focus F , the polar \bar{D} of the director D all pass through the axial point A .
3. The other ideal point J on the axis and the other ideal line j through the axial point are incident.

Answer

5.1.9.

$$\begin{aligned}
& B_i = \{144, 64, 88\}, b_i = \{182, 136, 132\}, \\
& W_0 = (62), H = (171), W_1 = (88).
\end{aligned}$$

5.1.12 Representation of polar geometry on the dodecahedron.

Introduction.

When $p = 5$, the representation of polar geometry on the dodecahedron is suggested by the fact that the 6 faces form a conic which can be chosen as the ideal.

Definition.

Using the dodecahedral representation, the conic which consists of the 6 face-points is the ideal conic.

Theorem.

The 15 side-points are hyperbolic and the 10 vertex-points are elliptic.

This follows at once from the incidence definitions, II.2.3.4.

Theorem.

With the ideal conic of type A ,
 the 3 . 15 conics of type $I3$, $E1$ and $E2$ are hyperbolic circles,
 the 4 . 6 conics of type $J1$, $J2$, $O1$, $O2$ are parabolic circles and
 the 3 . 10 conics of type P , $U1$ and $U2$ are elliptic circles.

Although this should be placed in the Chapter on non-Euclidean geometry, we have.

Theorem.

With a particular choice of unit, the radii of the various sub-types are as follows,
 $U1$ and $E2$ are $\frac{\pi}{6}$, $U2$ and $E1$ are $\frac{\pi}{3}$, P and $I3$ are $\frac{\pi}{3}$.

Example.

Computations relating to $g_434.PRN$:

If we use as primitive polynomial $I^3 - I - 2$, we obtain the correspondence:

x	(y_0, y_1, y_2)	(y)	$[z]$
0	(0, 0, 1)	(0)	[6]
1	(0, 1, 0)	(1)	[1]
2	(1, 0, 0)	(6)	[11]
3	(0, 1, 2)	(3)	[21]
4	(1, 2, 0)	(16)	[16]
5	(1, 3, 1)	(22)	[26]
6	(1, 4, 4)	(30)	[7]
7	(1, 0, 3)	(9)	[9]
8	(0, 1, 3)	(4)	[8]
9	(1, 3, 0)	(21)	[10]
10	(1, 2, 4)	(20)	[0]
11	(1, 0, 1)	(7)	[12]
12	(0, 1, 1)	(2)	[24]
13	(1, 1, 0)	(11)	[18]
14	(1, 1, 2)	(13)	[30]
15	(1, 3, 2)	(23)	[2]
16	(1, 1, 4)	(15)	[17]
17	(1, 0, 2)	(8)	[14]
18	(0, 1, 4)	(5)	[28]
19	(1, 4, 0)	(26)	[25]
20	(1, 4, 3)	(29)	[4]
21	(1, 1, 3)	(14)	[22]
22	(1, 4, 2)	(28)	[29]
23	(1, 2, 3)	(19)	[13]
24	(1, 2, 1)	(17)	[20]
25	(1, 1, 1)	(12)	[3]
26	(1, 2, 2)	(18)	[27]
27	(1, 4, 1)	(27)	[19]
28	(1, 3, 3)	(24)	[23]
29	(1, 3, 4)	(25)	[15]
30	(1, 0, 4)	(10)	[5]

The second column is $I^x \pmod{P}$, the third column is the representation of Chapter II, the fourth column is obtained as follows.

The ideal conic passes through 0,4,6,9,16 and 17 and is therefore represented by the matrix

$$Q = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

or the quadratic form $Q(x, y) = x_0y_0 + x_1y_1 + x_0y_2 + x_2y_0$.

This determines the polar of (y_0, y_1, y_2) as $[y_0 + y_2, y_1, y_0]$, but the polar of x is x^* , therefore if $x = (y_0, y_1, y_2)$ and $[z] = [y_0 + y_2, y_1, y_0]$ then $x^* = [z]$.

For instance, if $x = 7$, $(y) = (1, 0, 3)$, $[z] = [-1, 0, 1] = [10]$.

Example.

The hyperbolic circles have as center a edge-point.

Those with center $8 = 0^ \times 8^*$ and through the point u can be constructed as follows, let $up = 0 \times (4 \times u)$, given any line v through 0 , such that $u \cdot v \neq 0$, the Pascal construction gives the other point on the conic and v using*

$$(((v \times 4) \times up) \times 8) \times u) \times v.$$

This gives, with the radii determined below:

$0,4;;2,15,22,25$ of type fs and sub-type $I3$, radius $\frac{\pi}{3}$.

$0,4;;5,11,13,20$ of type fv and sub-type $E1$, radius $\frac{\pi}{4}$.

$0,4;;7,19,21,29$ of type fv and sub-type $E2$, radius $\frac{\pi}{6}$.

Before having obtained a synthetic construction of the parabolic and elliptic circles we have used the algebraic definition.

The algebraic definition is

$$kx^T Qx - (x^T Q C)^2 = 0,$$

with C on the ideal conic, for parabolic circles and C a vertex-point for elliptic circles.

For $k = 0$, the circle degenerates in (a double) line, consisting of the points at distance $\frac{\pi}{2}$ from C .

Let $C = 0$, the polar $0^ = [1, 0, 0]$, hence the parabolic circles are*

$$k(x_0^2 - x_1^2 + 2x_2x_0) + x_0^2 = 0.$$

With $k' = \frac{1}{k}$, the points are $(0, 0, 1) = 0$, and $(1, x_1, 2(1 - k' + x_1)^2)$. This gives for, $k = -1$, $(1, 0, 4) = 30$, $(1, 1, 1) = 25$, $(1, 4, 1) = 27$, $(1, 2, 2) = 26$, $(1, 3, 2) = 15$, in view of the table above. Hence

$k = 4$, $\{0, 30, 25, 27, 26, 15\}$ of type fs and sub-type $O1$.

$k = 2$, $\{0, 11, 21, 20, 10, 29\}$ of type fv and sub-type $J2$.

$k = 3$, $\{0, 7, 13, 19, 24, 5\}$ of type fv and sub-type $J1$.

$k = 1$, $\{0, 2, 14, 22, 23, 28\}$ of type fs and sub-type $O2$.

Let $C = 5$, the polar $5^ = [1, -1, -2]$, hence the circles are*

$$k(x_0^2 + x_1^2 + 2x_2x_0) - (x_0 - x_1 - 2x_2)^2 = 0.$$

The points are,

$$(0, 1, 2 \pm \sqrt{-k} \text{ and } (1, x_1, -k + 2(x_1 - 1) \pm \sqrt{k^2 - k(x_1^2 - x_1 + 2)}).$$

This gives, for $k = -1$,

$$(0, 1, 3) = 8, (0, 1, 1) = 12, (1, 4, 2) = 22, (1, 2, 3) = 23, (1, 3, 2) = 15, \\ (1, 3, 3) = 22, \text{ in view of the table above.}$$

Hence, with the radii determined below:

$k = 4$, $\{8, 12, 22, 23, 15, 28\}$ of type ss and sub-type $U2$, radius $\frac{\pi}{4}$.

$k = 2$, $\{11, 21, 24, 10, 19, 20\}$ of type vv and sub-type P , radius $\frac{\pi}{3}$.

$k = 3$, $\{5\}$, radius 0 .

$k = 1$, $\{1, 18, 2, 30, 14, 25\}$ of type ss and sub-type $U1$, radius $\frac{\pi}{6}$.

*To summarize, we see that, with the ideal conic of type A ,
the 3 . 15 conics of type $I3$, $E1$ and $E2$ are hyperbolic circles,
the 4 . 6 conics of type $J1$, $J2$, $O1$, $O2$ are parabolic circles and
the 3 . 10 conics of type P , $U1$ and $U2$ are elliptic circles.*

Exercise.

For a synthetic construction of the parabolic circles and some elliptic ones, we can use IV.1.2.7. This is a good exercise.

Example of Distances.

We recall the trigonometric tables for $p = 5$:

With $\delta = 2$,

x	$\sin(x)$	$\cos(x)$	x	$\sin(x)$	$\cos(x)$
0	0	1	0	0	1
1	2δ	2δ	1	-2	δ
2	1	0	2	δ	-2
			3	1	0

$\cos^2(d)$	0	1	2	3	4
$\frac{d}{\pi}$	$\frac{1}{2}$	0	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{3}$

where $\cos(d(C, X)) = \frac{Q(X, C)^2}{Q(X, X)} = \frac{k}{Q(C, C)}$.

Hence the distances, recorded above. For instance, in the case of elliptic circles, for $C = 5 = (1, 3, 1)$ and $X = 8 = (0, 1, 3)$, $Q(C, C) = 2$, $Q(X, X) = 1$, $Q(X, C) = 1$, $\cos^2(d(C, X)) = 3$, $d(C, X) = \frac{\pi}{4}$. Hence

for $k = -1$, the radius is $\frac{\pi}{4}$,

for $k = 2$, $\cos^2(d(C, X)) = -1$, $d(C, X) = \frac{\pi}{3}$,

for $k = 3$, $d(C, X) = 0$,

for $k = 1$, $d(C, X) = \frac{\pi}{6}$.

In the case of hyperbolic circles with $C = 8$ and $X = 5$, we have $d(8, 5) = \frac{\pi}{4}$, the other radii are obtained directly,

$\cos^2(d(8, 2)) = \frac{(-2)^2}{1.1} = -1$, hence $d(8, 2) = \frac{\pi}{4}$,

$\cos^2(d(8, 7)) = \frac{(-2)^2}{1.2} = 2$, hence $d(8, 7) = \frac{\pi}{6}$.

Example.

Computations relating to g_434 .PRN: If we use as primitive polynomial $I^3 - I - 2$, we obtain the correspondence:

x	(y_0, y_1, y_2)	(y)	$[z]$
0	(0, 0, 1)	(0)	[6]
1	(0, 1, 0)	(1)	[1]
2	(1, 0, 0)	(6)	[11]
3	(0, 1, 2)	(3)	[21]
4	(1, 2, 0)	(16)	[16]
5	(1, 3, 1)	(22)	[26]
6	(1, 4, 4)	(30)	[7]
7	(1, 0, 3)	(9)	[9]
8	(0, 1, 3)	(4)	[8]
9	(1, 3, 0)	(21)	[10]
10	(1, 2, 4)	(20)	[0]
11	(1, 0, 1)	(7)	[12]
12	(0, 1, 1)	(2)	[24]
13	(1, 1, 0)	(11)	[18]
14	(1, 1, 2)	(13)	[30]
15	(1, 3, 2)	(23)	[2]
16	(1, 1, 4)	(15)	[17]
17	(1, 0, 2)	(8)	[14]
18	(0, 1, 4)	(5)	[28]
19	(1, 4, 0)	(26)	[25]
20	(1, 4, 3)	(29)	[4]
21	(1, 1, 3)	(14)	[22]
22	(1, 4, 2)	(28)	[29]
23	(1, 2, 3)	(19)	[13]
24	(1, 2, 1)	(17)	[20]
25	(1, 1, 1)	(12)	[3]
26	(1, 2, 2)	(18)	[27]
27	(1, 4, 1)	(27)	[19]
28	(1, 3, 3)	(24)	[23]
29	(1, 3, 4)	(25)	[15]
30	(1, 0, 4)	(10)	[5]

The second column is $I^x \pmod{P}$, the third column is the representation of Chapter II, the fourth column is obtained as follows.

The ideal conic passes through 0,4,6,9,16 and 17 and is therefore represented by the matrix

$$Q = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

or the quadratic form $Q(x, y) = x_0y_0 + x_1y_1 + x_0y_2 + x_2y_0$.

This determines the polar of (y_0, y_1, y_2) as $[y_0 + y_2, y_1, y_0]$, but the polar of x is x^* , therefore if $x = (y_0, y_1, y_2)$ and $[z] = [y_0 + y_2, y_1, y_0]$ then $x^* = [z]$.

For instance, if $x = 7$, $(y) = (1, 0, 3)$, $[z] = [-1, 0, 1] = [10]$.

Example.

The hyperbolic circles have as center a edge-point.

Those with center $8 = 0^ \times 8^*$ and through the point u can be constructed as follows, let $up = 0 \times (4 \times u)$, given any line v through 0 , such that $u \cdot v \neq 0$, the Pascal construction gives the other point on the conic and v using*

$$(((v \times 4) \times up) \times 8) \times u) \times v.$$

This gives, with the radii determined below:

$0,4;;2,15,22,25$ of type fs and sub-type $I3$, radius $\frac{\pi}{3}$.

$0,4;;5,11,13,20$ of type fv and sub-type $E1$, radius $\frac{\pi}{4}$.

$0,4;;7,19,21,29$ of type fv and sub-type $E2$, radius $\frac{\pi}{6}$.

Before having obtained a synthetic construction of the parabolic and elliptic circles we have used the algebraic definition.

The algebraic definition is

$$kx^T Qx - (x^T Q C)^2 = 0,$$

with C on the ideal conic, for parabolic circles and C a vertex-point for elliptic circles.

For $k = 0$, the circle degenerates in (a double) line, consisting of the points at distance $\frac{\pi}{2}$ from C .

Let $C = 0$, the polar $0^ = [1, 0, 0]$, hence the parabolic circles are*

$$k(x_0^2 - x_1^2 + 2x_2x_0) + x_0^2 = 0.$$

With $k' = \frac{1}{k}$, the points are $(0, 0, 1) = 0$, and $(1, x_1, 2(1 - k' + x_1)^2)$. This gives for,

$k = -1$, $(1, 0, 4) = 30$, $(1, 1, 1) = 25$, $(1, 4, 1) = 27$, $(1, 2, 2) = 26$, $(1, 3, 2) = 15$, in view of the table above. Hence

$k = 4$, $\{0, 30, 25, 27, 26, 15\}$ of type fs and sub-type $O1$.

$k = 2$, $\{0, 11, 21, 20, 10, 29\}$ of type fv and sub-type $J2$.

$k = 3$, $\{0, 7, 13, 19, 24, 5\}$ of type fv and sub-type $J1$.

$k = 1$, $\{0, 2, 14, 22, 23, 28\}$ of type fs and sub-type $O2$.

Let $C = 5$, the polar $5^ = [1, -1, -2]$, hence the circles are*

$$k(x_0^2 + x_1^2 + 2x_2x_0) - (x_0 - x_1 - 2x_2)^2 = 0.$$

The points are,

$$(0, 1, 2 \pm \sqrt{-k} \text{ and } (1, x_1, -k + 2(x_1 - 1) \pm \sqrt{k^2 - k(x_1^2 - x_1 + 2)}).$$

This gives, for $k = -1$,

$$(0, 1, 3) = 8, (0, 1, 1) = 12, (1, 4, 2) = 22, (1, 2, 3) = 23, (1, 3, 2) = 15,$$

$$(1, 3, 3) = 22, \text{ in view of the table above.}$$

Hence, with the radii determined below:

$k = 4$, $\{8, 12, 22, 23, 15, 28\}$ of type ss and sub-type $U2$, radius $\frac{\pi}{4}$.

$k = 2$, $\{11, 21, 24, 10, 19, 20\}$ of type vv and sub-type P , radius $\frac{\pi}{3}$.

$k = 3$, $\{5\}$, radius 0 .

$k = 1$, $\{1, 18, 2, 30, 14, 25\}$ of type ss and sub-type $U1$, radius $\frac{\pi}{6}$.

*To summarize, we see that, with the ideal conic of type A ,
the 3 . 15 conics of type $I3$, $E1$ and $E2$ are hyperbolic circles,
the 4 . 6 conics of type $J1$, $J2$, $O1$, $O2$ are parabolic circles and
the 3 . 10 conics of type P , $U1$ and $U2$ are elliptic circles.*

Exercise.

For a synthetic construction of the parabolic circles and some elliptic ones, we can use IV.1.2.7. This is a good exercise.

Example of Distances.

We recall the trigonometric tables for $p = 5$:

With $\delta = 2$,

x	$\sin(x)$	$\cos(x)$	x	$\sin(x)$	$\cos(x)$
0	0	1	0	0	1
1	2δ	2δ	1	-2	δ
2	1	0	2	δ	-2
			3	1	0

$\cos^2(d)$	0	1	2	3	4
$\frac{d}{\pi}$	$\frac{1}{2}$	0	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{3}$

where $\cos(d(C, X)) = \frac{Q(X, C)^2}{Q(X, X)} = \frac{k}{Q(C, C)}$.

Hence the distances, recorded above. For instance, in the case of elliptic circles, for $C = 5 = (1, 3, 1)$ and $X = 8 = (0, 1, 3)$, $Q(C, C) = 2$, $Q(X, X) = 1$, $Q(X, C) = 1$, $\cos^2(d(C, X)) = 3$, $d(C, X) = \frac{\pi}{4}$. Hence

for $k = -1$, the radius is $\frac{\pi}{4}$,

for $k = 2$, $\cos^2(d(C, X)) = -1$, $d(C, X) = \frac{\pi}{3}$,

for $k = 3$, $d(C, X) = 0$,

for $k = 1$, $d(C, X) = \frac{\pi}{6}$.

In the case of hyperbolic circles with $C = 8$ and $X = 5$, we have $d(8, 5) = \frac{\pi}{4}$, the other radii are obtained directly,

$\cos^2(d(8, 2)) = \frac{(-2)^2}{1.1} = -1$, hence $d(8, 2) = \frac{\pi}{4}$,

$\cos^2(d(8, 7)) = \frac{(-2)^2}{1.2} = 2$, hence $d(8, 7) = \frac{\pi}{6}$.

5.2 Finite Non-Euclidean Geometry.**5.2.0 Introduction.****5.2.1 Trigonometry for the general triangle.****Introduction.**

Spherical trigonometry refers to the relation between the measure of angles and arcs of a triangle on a sphere.

The formulas of al-Battani (Albategnius, about 920 A.D.) and of Jabir ibn Aflah (Geber, about 1130 A.D.) have to be adapted to the finite case in which the sine of an angle in the first 2 quadrants cannot be considered as positive. There are several possible solutions. One of these will be given in Theorem 5.2.1.

Let A, B, C be the vertices of a triangle, a, b, c be its sides.

The measure of the angle between b and c will be denoted A, \dots .

The distance between the points B and C will be denoted a, \dots .

Definition.

Let A, B, C be 3 points on the sphere

$$x^2 + y^2 + z^2 = 1,$$

of center $O = (0, 0, 0, 1)$.

The direction DA of A is the ideal point on OA .

The side $a = \{B, C\}$ is a section of the circle \mathcal{C}_a which is the intersection of the sphere and the plane $O \times B \times C$. The spherical distance of the side a , also denoted a is the angle between the directions DB and DC .

The angle BAC , also denoted A is the angle of the directions of the tangents at A to the circles \mathcal{C}_b and \mathcal{C}_c .

Theorem.

Between the trigonometric functions of the angles and sides of a general triangle we have the relations:

0. $\frac{|sina|}{sinA} = \frac{|sinb|}{sinB} = \frac{|sinc|}{sinC} = r.$
1. 0. $\cos A = \cos B \cos C + \sin B \sin C \cos a,$
 1. $\cos B = \cos C \cos A + \sin C \sin A \cos b,$
 2. $\cos C = \cos A \cos B + \sin A \sin B \cos c.$
2. 0. $\cos a = \cos b \cos c + |sinb||sinc|\cos A,$
 1. $\cos b = \cos c \cos a + |sinc||sina|\cos B,$
 2. $\cos c = \cos a \cos b + |sina||sinb|\cos C.$
3. 0. $\sin A = \frac{\cos^2 B - \cos^2 C}{\sin B \cos C \cos c - \sin C \cos B \cos b},$
 1. $\sin B = \frac{(\cos^2 C - \cos^2 A)}{\sin C \cos A \cos a - \sin A \cos C \cos c},$
 2. $\sin C = \frac{(\cos^2 A - \cos^2 B)}{\sin A \cos B \cos b - \sin B \cos A \cos a}.$
4. 0. $|sina| = \frac{\cos^2 b - \cos^2 c}{|sinb|\cos c \cos C - |sinc|\cos b \cos B},$
 1. $|sinb| = \frac{\cos^2 c - \cos^2 a}{|sinc|\cos a \cos A - |sina|\cos c \cos C},$
 2. $|sinc| = \frac{\cos^2 a - \cos^2 b}{|sina|\cos b \cos B - |sinb|\cos a \cos A}.$
5. 0. $\cos A = \frac{\sin B \cos B \cos c - \sin C \cos C \cos b}{\sin B \cos C \cos c - \sin C \cos B \cos b},$
 1. $\cos B = \frac{\sin C \cos C \cos a - \sin A \cos A \cos c}{\sin C \cos A \cos a - \sin A \cos C \cos c},$
 2. $\cos C = \frac{\sin A \cos A \cos b - \sin B \cos B \cos a}{\sin A \cos B \cos b - \sin B \cos A \cos a}.$
6. 0. $\cos a = \frac{|sinb|\cos b \cos C - |sinc|\cos c \cos B}{|sinb|\cos c \cos C - |sinc|\cos b \cos B},$
 1. $\cos b = \frac{|sinc|\cos a \cos A - |sina|\cos c \cos C}{|sinc|\cos a \cos A - |sina|\cos c \cos C},$
 2. $\cos c = \frac{|sina|\cos a \cos B - |sinb|\cos b \cos A}{|sina|\cos b \cos B - |sinb|\cos a \cos A}.$

Proof⁵:

Let the coordinates of the points A, B, C be $(A_0, A_1, A_2, 1), (B_0, B_1, B_2, 1), (C_0, C_1, C_2, 1)$.

Those of DA, DB and DC are $(A_0, A_1, A_2, 0), (B_0, B_1, B_2, 0), (C_0, C_1, C_2, 0)$.

if $A \cdot B := A_0B_0 + A_1B_1 + A_2B_2$ and $A \cdot A := A_0A_0 + A_1A_1 + A_2A_2$, by definition (see ...)

$$\cos a = B \cdot C$$

because $B \cdot B = C \cdot C = 1$.

The plane $A \times B \times O$ is $\{A_1B_2 - A_2B_1, A_2B_0 - A_0B_2, A_0B_1 - A_1B_0, 0\}$

the tangent to the sphere at A is

$$\{A_0, A_1, A_2, -1\}$$

and the ideal plane is

$$\{0, 0, 0, 1\}$$

therefore the direction of $A \times B$ is

$$DAB = A \cdot AB_0 - A \cdot BA_0, A \cdot AB_1 - A \cdot BA_1, A \cdot AB_2 - A \cdot BA_2, 0).$$

Similarly the direction of $A \times C$ is

$$DAC = A \cdot AC_0 - A \cdot CA_0, A \cdot AC_1 - A \cdot CA_1, A \cdot AC_2 - A \cdot CA_2, 0).$$

$DAB \cdot DAB = 1 - (A \cdot B)^2 = 1 - \cos^2 c = \sin^2 c$, and $DAC \cdot DAC = \sin^2 b$.

Therefore

$$\cos A = \frac{B \cdot C + A \cdot BA \cdot C - A \cdot BA \cdot C - A \cdot CA \cdot B}{|sin b| |sin c|} = \frac{\cos a - \cos c \cos b}{|sin b| |sin c|},$$

hence 2.0.

$$\begin{aligned} \sin^2 A \sin^2 b \sin^2 c &= (1 - \cos^2 A) \sin^2 b \sin^2 c \\ &= \sin^2 b \sin^2 c - \cos^2 a - \cos^2 b \cos^2 c + 2 \cos a \cos b \cos c \\ &= 1 - \cos^2 a - \cos^2 b - \cos^2 c + 2 \cos a \cos b \cos c \end{aligned}$$

Therefore, if

$$r := \sqrt{\frac{1 - \cos^2 a - \cos^2 b - \cos^2 c + 2 \cos a \cos b \cos c}{\sin^2 a \sin^2 b \sin^2 c}}$$

then

$$\frac{\sin A}{|sin a|} = \frac{\sin B}{|sin b|} = \frac{\sin C}{|sin c|} = r.$$

Simple algebraic manipulations give 3 to 6.

If we eliminate $\cos B$ and $\cos C$ from 1.1 and 1.2,

$$\begin{aligned} \cos B &= -\frac{\sin C \cos b + \cos A \sin B \cos c}{\sin A}, \\ \cos C &= -\frac{\sin B \cos c + \cos A \sin C \cos b}{\sin A}, \end{aligned}$$

substituting in 1.0. gives

$$\begin{aligned} \cos A &= (\sin C \cos b + \cos A \sin B \cos c)(\sin B \cos c + \cos A \sin C \cos b) / \sin^2 A \\ &\quad - \sin B \sin C \cos a \\ \cos A &= (\sin c \cos b + \cos A \sin b \cos c)(\sin b \cos c + \cos A \sin c \cos b) / \sin^2 a \\ &\quad - \sin b \sin c \cos a \\ \cos B \cos C - \cos A &= \frac{(\cos b - \cos c \cos a)(\cos c - \cos b \cos a) - \sin^2 a (\cos a - \cos b \cos c)}{\sin^2 a |sin b| |sin c|} \\ &= \frac{\cos a (-\cos^2 b - \cos^2 c + 2 \cos a \cos b \cos c + 1 - \cos^2 a)}{\sin^2 a |sin b| |sin c|} \\ &= \cos a \sin B \sin C. \end{aligned}$$

Hence 1.0.

⁵Echo Lake 22.7.84

Example.

For $p = 13$, with $\delta^2 = 2$,

let $A = (0, 0, 1, 1)$, $B = (1, 2, 3, 1)$, $C = (6, 1, 4, 1)$.

$\cos a = 7$, $\cos b = 4$, $\cos c = 3$, $|\sin a| = 2$, $|\sin b| = 5\delta$, $|\sin c| = 3\delta$.

$\cos A = 2$, $\cos B = 4\delta$, $\cos C = 2\delta$, $\sin A = 6$, $\sin B = 2\delta$, $\sin C = -4\delta$.

5.2.2 Trigonometry for the right triangle.**Theorem.**

For a triangle with a right angle at A , let $\sin A = 1$, $\cos A = 0$, then we have the relations:

$$0.1. |\sin b| = |\sin a| \sin B,$$

$$2. |\sin c| = |\sin a| \sin C,$$

$$1.0. \cos B \cos C = \sin B \sin C \cos a,$$

$$1. \cos B = \sin C \cos b,$$

$$2. \cos C = \sin B \cos c.$$

$$2. \cos a = \cos b \cos c,$$

Proof: 1 and 0.2 follow from 5.2.1.0.

0 follows from 5.2.1.2.0.

1 and 1.2 follow from 5.2.1.1 which gives 1.0, using 2.0.

5.2.3 Trigonometry for other triangles .**Definition.**

An auto-dual triangle is a triangle such that

$$A = a, B = b, C = c.$$

Theorem.

If a triangle is auto dual, then

$$0. \cos A = \frac{\cos B \cos C}{1 + \sin B \sin C},$$

$$1. \sin A = -\frac{\sin B + \sin C}{1 + \sin B \sin C}.$$

Proof: 0 follows from Theorem 5.2.1. If we substitute $\cos A$ using 0 in $\sin^2 A + \cos^2 A = 1$, we get $\sin A = +j \frac{\sin B + \sin C}{1 + \sin B \sin C}$, $j = +1$ or -1 . replacing $\sin A$ and $\cos A$ by their expression in 1.1, gives after multiplication by $1 + \sin B \sin C$,

$$1 + \sin B \sin C = \cos^2 C - i(\sin B \sin C + \sin^2 C),$$

therefore $j = -1$.

Notation.

$A = (s, c)$, is an abbreviation for $\sin A = s$, $\cos A = c$.

Example.

For $p = 13$, let $a = A = (-4, -4\delta)$, $b = B = (-6, -2)$, $c = C = (3, 5\delta)$, we easily verify 5.2.3.0 and .1:

$$\cos A = -4\delta = -\frac{2.5\delta}{1+3.-6}, \sin A = -4 = -\frac{3-6}{1+3.-6}.$$

5.3 Tri-Geometry

5.3.1 The primitive case.

Introduction.

To a given polynomial P_3 of the third degree, we can associate a selector. The first case I will consider is that when the polynomial has no integer roots or is primitive. To a given such polynomial corresponds a selector called the fundamental selector and a tri-geometry with non-integer isotropic points and lines. To this fundamental selector we can associate others, see g25.prn, The semi-selector gives conics associated to the auto-polars, the co-selector and the bi-selector are associated to the point-conics⁶ and line-conics through the isotropic points, the bi-selector and the co-selector to the point-conics and line-conics tangent to the isotropic lines. Examples indicated that the other selectors do not give lines or conics or, in general, cubics. It is an open question if they have any geometrical significance.

Definition.

If s is the selector, the selector function is a function from Z_{p^2+p+1} to Z_{p^2+p+1} given by

$$0. f(s_j - s_i) := s_i, i \neq j, f(0) = -1.$$

Theorem.

The selector for the c -lines is the co-selector of the lines. More precisely,

$$0. s^c(i) = 1 - s(i).$$

The selector function for c -lines is given by

$$1. f^c(i) = 1 - f(-i).$$

Theorem.

$$0. a \times b = (f(b - a) - a)^*.$$

$$1. a^* \times b^* = f(b - a) - a.$$

⁶17.3.86

2. a is on b^* iff $f(a+b) = 0$ or $f(a+b) = -1$.
3. the points on a^* are $s(i) - a$, $i = 0$ to p .
4. $acb = (1 - f(b-a) - b)^c$.
5. $a^c b^c = 1 - f(b-a) - b$.
6. a is on b^c iff $f(-a-b) = 1$.
7. the points on a^c are $1 - a - s(i)$, $i = 0$ to p .

Definition.

Let $c^* := a \times b$. Let $a = s(i) - c$, let $b = s(j) - c$, the gap of a and b , written
 $gap(b, a) := j - i \pmod{p+1}$.

Let $c := a^* \times b^*$. Let $a^* = s(i) - c$, let $b^* = s(j) - c$, the gap of a^* and b^* , written
 $gap(b^*, a^*) := j - i \pmod{p+1}$.

Theorem.

Let a_0 be a point on b_0 , let let a_i be on b_i , such that

$$gap(a_i, a_0) + gap(b_i, b_0) = 0,$$

the points a_i are on a c -line through a_0 tangent to b_0 .

Table.

The selector for some values of p and equivalent ones which are not complementary (obtained by reversing the order are

- $p = 3$, 0: 0,1,3,9. 1: 0,1,4,6.
 $p = 5$, 0: 0,1,3,8,12,18. 1: 0,1,3,10,14,26. 2: 0,1,4,6,13,21.
 3: 0,1,4,10,12,17. 4: 0,1,8,11,13,17.
 $p = 7$, 0: 0,1,3,13,32,36,43,52. 1: 0,1,4,9,20,22,34,51.
 2: 0,1,4,12,14,30,37,52. 3: 0,1,5,7,17,35,38,49.
 4: 0,1,5,27,34,37,43,45. 5: 0,1,7,19,23,44,47,49.
 $p = 11$, 0: 0,1,3,12,20,34,38,81,88,94,104,109.
 1: 0,1,3,15,46,71,75,84,94,101,112,128.
 2: 0,1,3,17,21,58,65,73,100,105,111.
 3: 0,1,3,17,29,61,80,86,91,95,113,126.
 4: 0,1,4,12,21,26,45,+68,84,97,99,127.
 5: 0,1,4,16,50,71,73,81,90,95,101,108.
 6: 0,1,4,27,51,57,79,89,100,118,120,125.
 7: 0,1,5,12,15,31,33,39,56,76,85,98.
 8: 0,1,5,21,24,39,49,61,75,92,125,127.
 9: 0,1,5,24,44,71,74,80,105,112,120,122.
 10: 0,1,5,25,28,68,78,87,89,104,120,126.
 11: 0,1,6,18,39,68,79,82,98,102,124,126.

- 12: 0,1,8,21,33,36,47,52,70,74,76,124.
 13: 0,1,9,19,24,31,52,56,58,69,72,98.
 14: 0,1,15,18,20,24,31,52,60,85,95,107.
 15: 0,1,15,25,45,52,58,61,63,80,84,92.
 16: 0,1,16,21,24,49,51,58,62,68,80,94.
 17: 0,1,23,37,57,62,75,83,86,90,92,102.

Example.

Let $p = 3$. If we use the selector 0,1,3,9 and use the representation on the cube (g25.prn), the complementary selector 0,1,5,11 gives the c -lines which can be classified as follows: 3 of type $VVSS$, 2 vertex-points and 1 side-point through each.

More precisely, two of 2 adjacent vertex-points and 1 side-point through each, such that no 2 are in the same face, one of 2 opposite vertex-points and 2 adjacent side-points one through each.

3 of type $FSSS$, 1 face-point, 1 side-point in it and 2 opposite side-points in an other face.

3 of type $FVSS$, 1 face-point, two adjacent side-points in it and a vertex point on one of the side-points.

3 of type $FSVV$, 1 face-point, two adjacent vertex-points in it and a side-point through one of the vertex-points.

1 of type $VFFF$, 1 vertex-point and the 3 face-points.

Clearly the converse is not true. For instance, only one of the 4 vertex-points can serve for the last case given.

Example.

Let $p = 7$, $P_3 = I^3 + 2$,

The powers of $I + 3$ are:

0	0	0	1,	0	1	3,	1	-1	2,	1	3	2,	1	3	3,
5	1	2	0,	1	-3	1,	0	1	-1,	1	2	-3,	1	2	2,
10	1	3	-2,	1	0	1,	1	-2	-2,	1	-1	-1,	1	-2	1,
15	1	2	1,	1	0	3,	1	1	0,	1	-1	3,	1	0	0,
20	1	0	-3,	1	-1	1,	1	-1	-3,	1	-3	-2,	0	1	2,
25	1	-2	-1,	1	0	2,	1	3	-1,	1	-1	-2,	1	1	3,
30	1	-2	0,	1	1	-2,	1	2	-2,	1	-2	-3,	1	-2	3,
35	1	-3	0,	0	1	1,	1	-3	3,	0	1	0,	1	3	0,
40	1	-2	2,	1	3	-3,	1	1	-3,	1	0	-1,	1	2	3,
45	1	-1	0,	1	2	-1,	1	1	-1,	1	-3	-3,	0	1	-2,
50	1	1	1,	1	1	2,	1	3	1,	1	-3	-1,	0	1	-3,
55	1	0	-2,	1	-3	2,									

Example,

$p = 7$, $P_3 = I^3 + 2$,

0^* : 0 1 7 24 36 38 49 54

1^* : 0 6 23 35 37 48 53 56

$7^*: 0 \ 17 \ 29 \ 31 \ 42 \ 47 \ 50 \ 51$

$24^*: 0 \ 12 \ 14 \ 25 \ 30 \ 33 \ 34 \ 40$

$36^*: 0 \ 2 \ 13 \ 18 \ 21 \ 22 \ 28 \ 45$

$38^*: 0 \ 11 \ 16 \ 19 \ 20 \ 26 \ 43 \ 55$

$49^*: 0 \ 5 \ 8 \ 9 \ 15 \ 32 \ 44 \ 46$

$54^*: 0 \ 3 \ 4 \ 10 \ 27 \ 39 \ 41 \ 52$

The points $0, 3, 8, 19, 21, 33, 50, 56$ are on a c -line through 0 .

The points $0, 5, 16, 18, 30, 47, 53, 54$ are on a c -line through 0 .

The part proving that co-, bi- and semi-selectors are conics was proven before this date⁷. The equation of the conics through 2 coordinate points was also obtained earlier. It remains to prove that the 2 are identical.

Lemma.

0. If i is an element of the co-selector, the tangent is $(1 - 2i)^*$.
1. If i is an element of the bi-selector, the tangent is $(a - \frac{i}{2})^*$, for some a .

Proof:

For 0, $(1 - 2i)^*$ is on i because $f(1 - i) = 0$ if i is an element of the co-selector. It remains to prove that it is the only point on $(1 - 2i)^*$. For 2, by duality?

Theorem.

Let S be a selector⁸.

0. The points associated to the co-selector are on a conic which passes through the isotropic points.
1. The points associated to the bi-selector are on a conic which is tangent to the isotropic lines.
2. The points associated to the semi-selector are on a conic for which the isotropic triangle is a polar triangle.
3. The conics of the same family are such that 2 distinct points determine a conic and 2 distinct conics have exactly one point in common.

Proof: Let $P_3 = I^3 + bI - c^9$.

For 0. Consider the selector associated to the line through $0 = G^0$ and $1 = G = I + g$. Let $G^i = I + h$. The corresponding point on the co-selector is G^{-i+1} . We obtain

$$G^{-i+1} = (g - h)I^2 - h(g - h)I + (g(b + h^2) + c)$$

It is easy to check that that point is on the conic

$$(bg + c)X_0^2 + gX_1^2 - gX_0X_1 - X_1X_2$$

and that the isotropic points are on this conic.

⁷31.3.86

⁸17.3.86

⁹2.4.86

Part 1, follows by duality in view of Lemma 3.2.10.1.

For 2, because the line i^* is on the point i , the correspondance which associates i^* to i is a polarity and the points on their polars is a conic, the auto-polar conic. These points are such that $f(2i) = 0$, where f is the selector function and therefore the solutions i are points corresponding to the semi-selector¹⁰. In view of g142.prn, the symmetric matrix M_2 which represents the auto-conic satisfies for some values of u, v, w

$$\begin{pmatrix} u & gv & (g^2 - b)w \\ 0 & v & 2gw \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} a_0 & b_2 & b_1 \\ b_2 & a_1 & b_0 \\ b_1 & b_0 & a_2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 2g \\ 1 & g & g^2 \end{pmatrix}.$$

The inverse of the last matrix is

$$\begin{pmatrix} g^2 & -g & 1 \\ -2g & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Multiplying the first matrix by this last matrix gives, because of the symmetry, $u = 1, v = 1, w = 1$ and with $b = s_{11}$,

$$M_2 = \begin{pmatrix} -s_{11} & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

This matrix clearly associates to the pole $(1, -(\pi_1 + \rho_2), \rho_1\rho_2)$ the polar, $[\rho_0^2, \rho_0, 1]$, because $s_1 = 0$.

Answer to 5.3.1.0.

I fill in here some of the details:

If $(I + g) * (I + h)^{-1} = uI^2 + vI + w$,

then $((v + uh)I^2 + (w + vh - ub) + (wh + uc) = k(I + g)$,

therefore

$$\begin{aligned} v &= -uh, \quad wh + uc = g(w - uh^2 - ub) \quad \text{or} \\ u &= g - h, \quad v = -h(g - h), \quad w = g(b + h^2) + c. \end{aligned}$$

The conic through the isotropic points and through the points 0 and 1 is of the form $a_0X_0^2 + gX_1^2 - X_1X_2 + b_1X_2X_0 + b_2X_0X_1$.

To insure that it passes through the isotropic points gives 3 linear equations for a_0, b_0 and b_2 . It is easiest to check a posteriori that

$$(bg + c)X_0^2 + gX_1^2 - gX_2X_0 - X_1X_2$$

passes through the isotropic points, for instance through $(1, \rho_0, r_1\rho_2)$:

$$g(\rho_1\rho_2 + \rho_2\rho_0 + \rho_0\rho_1 + \rho_0^2 - \rho_1\rho_2) + (c - \rho_0\rho_1\rho_2) = 0.$$

The point (u, v, w) is on the conic because

$$\begin{aligned} &(bg + c)(g - h)^2 + gh^2(g - h)^2 - g(g - h)w + h(g - h)w \\ &= (g - h)^2(bg + c + gh^2 - g(b + h^2) - c) = 0. \end{aligned}$$

Definition.

The mapping which associates to a point P corresponding to G^k , the point Q corresponding to G^{-k} is called the inversion mapping.

¹⁰31.3.86

Theorem.

If $P_3 = I^3 + bI - c$,

0. The inversion mapping T associates to (x, y, z) , (X, Y, Z) with

$$X = bx^2 + y^2 - xz,$$

$$Y = cx^2 - yz,$$

$$Z = (bx - z)^2 + by^2 - cxy.$$

$$T \circ T(x, y, z)$$

$$= (c^2x^3 + bcx^2y + b^2x^2z - 3cxyz - 2bxz^2 + cy^3 + by^2z + z^3).(x, y, z) ?$$

Example.

$p = 7$, $P_3 = I^3 + 2$,

selector: 0 1 7 24 36 38 49 54

selector function:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

-1 0 36 54 54 49 1 0 49 49 54 38 24 36 24 49 38 7 36 38 38 36 36 1

24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

0 24 38 54 36 7 24 7 49 24 24 1 0 1 0 54 24 54 7 38 49 36 49 7

48 49 50 51 52 53 54 55 56

1 0 7 7 54 1 0 38 1

c-selector: 0 1 4 9 20 22 34 51

c-selector fuction:

0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

-1 0 20 1 0 4 51 51 1 0 51 9 22 9 20 51 4 34 4 1 0 1 0 34

24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47

34 9 51 34 51 22 4 20 34 1 0 22 22 20 20 22 51 20 9 34 22 34 20 4

48 49 50 51 52 53 54 55 56

9 9 1 0 9 4 4 22 1

$12 \times 22 = 42^*$, $12c22 = 39^c$, 52^* is tangent at 12 to 39^c , 32^* is tangent at 22 to 39^c , 49^c is tangent at 12 to 42^* , 29^c is tangent at 22 to 42^* , $32^* \times 52^* = 6$, $29^c c 49^c = 28$. $6 \times 28 = 30^*$, $6c28 = 51^c$, 52^* is tangent at 6 to 51^c , 8^* is tangent at 28 to 51^c , 16^c is tangent at 6 to 30^* , 29^c is tangent at 28 to 30^* , $8^* \times 52^* = 14$, $29^c c 16^c = 50$. There appears to be no connection.

the c-lines (conics through the isotropic points) are

$$-2mX_0^2 + lX_1^2 + 3kX_2^2 - mX_1X_2 - lX_2X_0 - kX_0X_1 = 0.$$

the c-line with $l = m = 0$ is

$$0, 1, 0; 1, 0, 0; 1, 3, 1; 1, 3, 6; 1, 5, 2; 1, 5, 5; 1, 6, 3; 1, 6, 4 \text{ or } 12, 18, 19, 22, 27, 38, 40,$$

52,

the 57 others are all obtained by adding a constant, for instance, if we add 38 we get 50, 56,

0, 3, 8, 19, 21, 33 or 1,1,1; 0,0,1; 1,4,5; 1,3,2; 1,2,4; 1,0,0; 1,6,1; 1,5,4

which corresponds to $k = m = 0$,

if we add 19 we get 31, 37, 38, 41,46, 0, 2, 14, ($k = l = 0$)

if we add 33 we get 45, 51, 52, 55, 3, 14, 16, 28, ($k = l = m = 1$)

Is there any significance to the fact that 19, 38 are $\frac{57}{3}$, and $\frac{2 \cdot 57}{3}$?

the c -points (conics tangent to isotropic lines) are

$$3kx_0^2 + lx_1^2 - 2kx_2^2 - kx_1x_2 - lx_2x_0 - kx_0x_1 = 0.$$

Example.

$p = 7$, $P_3 = I^3 + 2$, selector, 0,1,7,24,36,38,49,54,

$3x_0^2 - x_1x_2$: 18,19,22,27,38,40,52,12, (0,1,4,9,20,22,34,51)

40,38,32,22,0,53,29,52, (0,1,5,27,34,37,43,45)

$x_1^2 - x_2x_0$: 56, 0, 3, 8,19,21,33,50, $-2x_2^2 - x_0x_1$: 37,38,41,46, 0, 2,14,31,

If we replace I by $I + 1$ we obtain $P_3 = I^3 + 3I^2 + 3I + 3$,

this gives the same selectors,

$P_3 = I^3 + 1$, and $P_3 = I^3 + I - 1$ give the selectors

(0,1,6,15,22,26,45,55), (0,1,3,13,32,36,43,52) and (0,1,5,7,17,35,38,49).

Example.

For $p = 3$ and $P_3 = I^3 + 2$, the auto-polar conics through two of the points $(0,0,1)$, $(0,1,0)$ and $(1,0,0)$ are

$$X_0^2 - X_1X_2 = 0 \text{ or } x_0^2 + 3x_1x_2 = 0,$$

$$X_1^2 - X_2X_0 = 0 \text{ or } x_1^2 + 2x_2x_0 = 0,$$

$$X_2^2 - X_0X_1 = 0 \text{ or } x_2^2 - x_0x_1 = 0.$$

All 3 do not have 3 points or 3 lines in common.

Comment.

If 2 conics are in the same family and we known the tangents corresponding to the points of one we can obtain those of the other. The sum of the corresponding representation of points and lines is a constant.

Program.

Examples can be studied using 130\ TWODIM.BAS.

5.3.2 The case of 1 root. Inverse geometry.

Introduction.

Let $P_3 = (I^2 + aI + b)(I + c)$, $a^2 - 4b \neq 0$.

There is one isotropic point $(1, a, b)$ and one isotropic line $[c^2, -c, 1]$.

The isotropic point is not on the line otherwise, $-c$ would be a root of $I^2 + aI + b$. The $p+1$ ideal points are $(0, 1, c)$ and $(1, x, c(x - c))$.

The $p+1$ ideal lines are $[0, b, -a]$ and $[1, x, -\frac{1+ax}{b}]$.

In the case of the complex field, if $P_3 = (I^2 + 1)I$, the c -lines are the circles through the origin, it is therefore natural to call this geometry inverse geometry.

Definition.

The pseudo-bi-selector is the set $\{2s_i\}$,

The pseudo-semi-selector is the set $\{\frac{1}{2}s_i\}$,

Example.

$p = 5$. With $P_3 = I^3 - I^2 - 2I - 3$, a generator is $I + 2$, its powers are

0, 0, 1	0, 1, 2	1, 4, 4	1, 2, 3	0, 1, 1	1, 3, 2	1, 0, 2	1, 3, 4	1, 2, 1	0, 1, 0
1, 2, 0	0, 1, 3	1, 0, 1	1, 1, 0	1, 1, 2	1, 4, 3	1, 4, 2	1, 1, 1	1, 0, 0	1, 4, 1
1, 3, 0	1, 3, 3	1, 1, 4	1, 2, 4						

The lines are

0 $[1, 0, 0]$: $\{0, 1, 4, 9, 11\}$ and $(0, 1, 4)$

1 $[1, 2, 4]$: $\{1, 2, 5, 10, 12\}$ and $(1, 1, 3)$

The selector function is

i	1	2	3	4	5	7	8	9	10	11	13	14	15	16	17	19	20	21	22	23
$f(i)$	0	9	1	0	4	4	1	0	1	0	11	11	9	9	11	9	4	4	11	1

The isotropic line $[1, 1, 1]$, the isotropic point is $(1, 0, 3)$. The ideal lines are $[j] = \{j, j + 6, j + 12, j + 18\}$, for $j = 0$ to 5.

I will now examine the case when Z_p is replace by an infinite field R , for instance.

$p = 7$, $P_3 = I^3 + I$, $G = I + 3$,

0, 0, 1	0, 1, 0	0, 1, 1	0, 1, 2	0, 1, 3	0, 1, 4	0, 1, 5	0, 1, 6	1, 0, 0	1, 0, 1
0, i	$0^I, 0^i$	46, 12*	29, 28*	1, 20*	7, 44*	11, 4*	34, 36*	$4^I, 0^*$	$I, 16^*$
1, 0, 2	1, 0, 3	1, 0, 4	1, 0, 5	1, 0, 6	1, 1, 0	1, 1, 1	1, 1, 2	1, 1, 3	1, 1, 4
16, 8*	40, 32*	24, 40*	8, 24*	32, 4*	$6^I, 46^*$	12, 14*	14, 6*	21, 30*	25, 38*
1, 1, 5	1, 1, 6	1, 2, 0	1, 2, 1	1, 2, 2	1, 2, 3	1, 2, 4	1, 2, 5	1, 2, 6	1, 3, 0
15, 22*	43, 2^i	$5^I, 7^*$	44, 23*	23, 15*	38, 39*	35, 47*	37, 31*	18, 3^i	$1^I, 11^*$
1, 3, 1	1, 3, 2	1, 3, 3	1, 3, 4	1, 3, 5	1, 3, 6	1, 4, 0	1, 4, 1	1, 4, 2	1, 4, 3
4, 27*	27, 19*	41, 43*	22, 3*	42, 35*	39, 7^i	$7^I, 29^*$	28, 45*	45, 37*	47, 13*
1, 4, 4	1, 4, 5	1, 4, 6	1, 5, 0	1, 5, 1	1, 5, 2	1, 5, 3	1, 5, 4	1, 5, 5	1, 5, 6
10, 21*	6, 5^*	33, 1^i	$3^I, 1^*$	20, 17*	17, 9*	26, 33*	5, 41*	19, 25*	30, 5^i
1, 6, 0	1, 6, 1	1, 6, 2	1, 6, 3	1, 6, 4	1, 6, 5	1, 6, 6			
$2^I, 34^*$	36, 2^*	2, 42*	3, 18*	31, 26*	9, 10*	13, 6^i			

The real isotropic point is denoted by I , the real isotropic line by i . $1 \times 9 = (-1) - 1 = 7^i$, $(0, 1, 3) \times (1, 6, 5) = [1, 3, 6]$. $9^* \times 17^* = (-1) - 1 = 7^I$, $[1, 5, 2] \times [1, 5, 1] = (1, 4, 0)$ ¹¹. Observe that k^I corresponds to IG'^I , with $G' = I + 3 \pmod{I_2 + 1}$.

The selector is 0, 1, 7, 11, 29, 34, 46.

The co-selector is 0, 1, 3, 15, 20, 38, 42.

The pseudo-bi-selector is $\{0, 2, 14, 22, 10, 20, 44, 4^I\}$.

The corresponding tangents to the bi-conic are $\{i, 47^*, 41^*, 37^*, 19^*, 2^*, 14^*, 0^*\}$

which is a member of the dual of the co-selector family¹².

The pseudo-semi-selector is $\{0, 17, 23, 24, 41, 47, 2^I, 6^I\}$.

The corresponding tangents to the semi-conic are $\{0^*, 17^*, 23^*, 24^*, 41^*, 47^*, 2^i, 6^i\}$.

¹¹7.4.86

¹²9.4.86

The points $2^I, 6^I$, are obtained from the ideal tangents $2^i, 6^i$.

The same can be checked if we add 1, ... , to the values above, we get in this way 24 hyperbolas, e.g.

$$\{1, 18, 24, 25, 42, 0, 3^I, 7^I\}$$

$$\{47^*, 16^*, 22^*, 23^*, 40^*, 46^*, 1^i, 5^i\},$$

and 24 ellipses, e.g.

$$\{1, 4, 6, 15, 25, 28, 30, 39\},$$

$$\{0^*, 3^*, 5^*, 14^*, 24^*, 27^*, 29^*, 38^*\}.$$

Hence, do we also have therefore the Theorem that a selector has $\frac{p-1}{2}$ even values and $\frac{p+1}{2}$ odd values?

Comment.

In the case of the field R , every polynomial of degree 3 has necessarily one root. There is no restriction in assuming that it is $P_3 := I^3 + I$. In this case the isotropic points are $(1, 0, 1)$, and the Euclidean isotropic points $(1, i, 0)$, $(1, -i, 0)$.

Theorem.

If the field is R and $P_3 := I^3 + I$, the transformation associated

0. to $k = -1$, transforms the lines into circles through the point $(1, 0, 1)$.
1. to $k = 2$, transforms the lines into parabolas with focus $(1, 0, 1)$.
2. to $k = \frac{1}{2}$, transforms the lines into equilateral hyperbolas with center $(1, 0, 1)$.

Proof:

For 0, the conics which pass through $(1, i, 0)$ and $(1, -i, 0)$ are circles. $(1, 0, 1)$ is the third isotropic point.

For 1, the conics are tangent to the isotropic line through $(1, i, 0)$ and $(1, -i, 0)$ which is the ideal line. Because the focus of a parabola is at the intersection of the tangent through the Euclidean isotropic point, we have 1.

For 2, because $(1, 0, 1)$ is the pole of the opposite isotropic line which is the ideal line, $(1, 0, 1)$ is the center of the conic. Because the points on the conic and the ideal line form a harmonic quatern with the pole $(1, i, 0)$ and the intersection $(1, -i, 0)$ with its polar, the corresponding directions, which are those of the asymptotes to the hyperbola and therefore perpendicular.

More explicitly:

Theorem.

The transformation associated to the case $k = -1$ associates to the point $(x, y, 1)$ or (x, y) , the point $(X, Y, 1)$ or (X, Y) , with

$$0. (xI^2 + yI + 1)(XI^2 + YI + 1) = 1 \pmod{P_3}. \text{ this gives}$$

$$1. X - 1 = \frac{x-1}{(x-1)^2 + y^2}, Y = -\frac{y}{(x-1)^2 + y^2}.$$

2. The point $Q = (X, Y)$ and the point $P = (x, y)$ are on a line through $(1, 0)$, the product of the distances to that point is 1, and the points P and Q are separated by $(1, 0)$.

Proof:

0, gives with I^3 replaced by $-I$ and I^4 replaced by $-I^2$,

$$-xX + x + X + yY = 0,$$

$$-xY - yX + y + Y = 0.$$

solving for X and Y gives easily 1.

Moreover,

$$\frac{X-1}{Y} = -\frac{x-1}{y},$$

Theorem.

The transformation associated to the case $k = 2$ associates to the point $(x, y, 1)$ or (x, y) , the point $(X, Y, 1)$ or (X, Y) , with

$$0. (XI^2 + YI + 1) = (xI^2 + yI + 1)^2 \pmod{P_3}.$$

this gives

$$1. X - 1 = y^2 - (x - 1)^2,$$

$$Y = -2y(x - 1).$$

2. The line associated to $a(x - 1) + by + c$ is the parabola

$$(-2ab^2(X - 1) + b(a^2 - b^2)Y - 2ac^2)^2 = 4(a^2 + b^2)c^2(c^2 - b^2(X - 1) - abY).$$

Proof: 0, gives with I^3 replaced by $-I$ and I^4 replaced by $-I^2$, we obtain at once 1. For 2, to simplify let us write the line as $y = mx' + d$, with $x' := x - 1$, $m = -\frac{a}{b}$ and $d = -\frac{c}{b}$.

Expressing y in terms of x' gives, with $X' := X - 1$,

$$2mX' + (m^2 - 1)Y = 2(m^2 + 1)dx' + 2md^2 \text{ and}$$

$$X' + mY = -(m^2 + 1)x'^2 + d^2$$

eliminating x' gives 2.

Theorem.

The transformation associated to the case $k = \frac{1}{2}$ associates to the point $(x, y, 1)$ or (x, y) , the point $(X, Y, 1)$ or (X, Y) , with

$$0. (XI^2 + YI + 1)^2 = (xI^2 + yI + 1) \pmod{P_3}.$$

this gives

$$1. x - 1 = Y^2 - (X - 1)^2, y = -2Y(X - 1).$$

2. The line associated to $a(x - 1) + by + c$ is the hyperbola

$$a(Y^2 - (X - 1)^2) - 2bY(X - 1) + c = 0.$$

Proof: 0, gives with I^3 replaced by $-I$ and I^4 replaced by $-I^2$, we obtain at once 1.

Theorem.

0. The lines joining the points associated to the selector and their inverse are tangent to a conic.

$$2y^2 + bz^2 + xz = 0 \text{ or } 2bX^2 - Y^2 - 8XZ = 0.$$

1. The lines joining the points associated to the co-selector and their inverse are tangent to a conic.

Proof: The points of the selector are $I - h$, their inverse is $I^2 + hI + h^2 + b$. The line through these points is $[-2h^2 - b, h, 1]$.

Problem.

Complete a set of axioms of inverse geometry using an appropriate form of the axiom of Pappus:

0. Given 2 distinct points, there exist one and only one line incident to, or passing through, the 2 points, or the points are parallel.
1. Given 2 distinct lines, there exists one and only one point incident to, or on, the 2 lines, or the lines are parallel.
2. There exists at least one line l and two distinct points P and Q not incident to l .
3. On the line l there are exactly p points, p an odd prime.
4. Given a line l and a point P not on the line, there exists one and only one line parallel to l through P .
5. Given a point P and a line l not through the point, there exists one and only one point parallel to P on l .

5.3.4 The case of a double root and a single root.

13

14

Introduction.

There is no ambiguity to call this also the case of 2 roots.

Definition.

The selector function is a function from the set $Z_{p(p-1)} - \{0 \pmod{p}\} - \{0 \pmod{p-1}\}$ into $Z_{p(p-1)}$, with

$$f(i - j) = i - j \pmod{p(p-1)}, \text{ for all } i \text{ and } j \text{ on } [1, 0, 0].$$

¹³16.5.85

¹⁴28.2.86

Example.

$p = 5$ The cyclic group is

0,0,1 0,1,1 1,2,1 1,2,4 1,4,1 1,0,1 1,3,3 0,1,3 1,4,3 1,2,3
1,0,2 1,1,1 1,4,2 1,1,2 1,1,4 1,0,3 1,4,4 1,3,2 0,1,2 1,3,2.

The lines are

0 [1,0,0]: {0,1,7,18 and (0,1,0), (0,1,4)}

19 [1,4,1]: {1,2,8,19 and (1,1,0), (1,0,4)}

18 [1,2,0]: {2,3,9,0 and (1,2,0), (1,2,2)}

17 [1,3,2]: {3,4,10,1 and (1,3,0), (1,1,3)}

....

The selector is

i	1	2	3	6	7	9	11	13	14	17	18	19
$f(i)$	0	18	18	1	0	18	7	7	7	1	0	1

If $f(j-i)$ does not exist, then if $j-i \equiv (\text{mod } 4)$, the points are on a line through (1,4,0).
If $f(j-i)$ does not exist, then if $j-i \equiv (\text{mod } 5)$, the points are on a line through (1,0,0).
Otherwise, the line is $f(j-i) - i (\text{mod } 20)$.

There is no restriction in assuming that $P_3 := I^3 - I^2$.

Definition.

The bi-isotropic point is $I_0 := (1, -1, 0)$,

the isotropic point is $I_1 := (1, 0, 0)$.

The bi-isotropic line is $i_0 := [0, 0, 1]$,

the isotropic line is $i_1 := [1, 1, 1]$.

Theorem.

0. The points associated to the co-selector are on a conic, the co-conic, which passes through the isotropic point I_1 and is tangent to the isotropic line i_1 at the co-isotropic point I_0 .
1. The points associated to the bi-selector are on a conic, the bi-conic, which is tangent to the co-isotropic line i_1 and is tangent to the isotropic line i_0 at the isotropic point I_1 .
2. The points associated to the semi-selector are on a conic, the semi-conic, which is tangent to the isotropic line i_0 at the co-isotropic point I_0 and is such that the polar of the isotropic point I_1 is the co-isotropic line i_1 .

Proof:

For 0, The conic of 3.1.8.0. reduces to

$$(k-l)Y^2 + mZ^2 + (m-l)YZ + (m-k)ZX + (k-l)XY = 0,$$

which passes through I_1 and for which $[1, 1, 1]$ is the polar of $(1, -1, 0)$.

For 1,

For 2,

5.3.5 The case of a triple root. Solar geometry.

Introduction.

In this case the ... There is one special point and a line belonging to each other. The special point and the special lines are called respectively the isotropic point and the isotropic line. The other points on the isotropic line are called ideal points. The other lines through the isotropic point are called ideal line. The other points and lines are called ordinary.

Theorem.

0. There are p ideal points, p ideal lines.
1. There are p^2 ordinary points, p^2 ordinary lines.
2. The isotropic line belongs to 1 isotropic point and p ideal points.
3. The isotropic point belongs to 1 isotropic line and p ideal lines.
4. The ideal lines belong to
5. The ordinary lines belong to

Comment.

In the parabolic-Euclidean or sun-geometry, among all points and lines of projective geometry, one point and a line through it are preferred, in this case this is also true, but if we represent this geometry in the Cartesian plane and choose the isotropic line as the line at infinity and the isotropic point as the direction of the x axis, the c -lines are parabolas which have It is therefore natural, by analogy to choose the names solar geometry and bi-solar geometry, for the geometry in question.

Lemma.

$$0. X_1^2 - 2X_2(X_0 + aX_1) = 0$$

and

$$1. Y_1^2 - 2Y_2(Y_0 + aY_1) = 0$$

implies

$$2. (X_1Y_2 + X_2Y_1)^2 - 2X_2Y_2(X_0Y_2 + X_2Y_0 + X_1Y_1 + a(X_1Y_2 + X_2Y_1)) = 0.$$

Proof: The first member of 2. is the sum of the first member of 0 and 1 multiplied respectively by Y_2^2 and X_2^2 .

Theorem.

Let $a = 0$, generators of T are $I + 1$ and $I + 2$. The cyclic group of order p generated by $I + b$ corresponds to points on the conic

$$X_1^2 - 2X_2(X_0 + aX_1) = 0$$

where $a := \frac{1}{2b}$. The cyclic group of order p generated by $I^2 + I + \frac{1}{2}$ corresponds to points on the conic

$$X_1^2 - 2X_2X_0 = 0.$$

Proof:

The point (X_0, X_1, X_2) corresponds to the polynomial $X_0I^2 + X_1I + X_2$.

The product of $(X_0I^2 + X_1I + X_2)$ and $(Y_0I^2 + Y_1I + Y_2)$ is $(X_0Y_2 + X_2Y_0 + X_1Y_1, X_1Y_2 + X_2Y_1, X_2Y_2)$. The Theorem follows at once from Lemma

Definition.

The selector function is a function from $Z_p \times Z_p$ to $Z_p \times Z_p \dots$

Definition.

The ideal lines can be represented by $[i]$, $i \in Z_p$.

The points on $[i]$ are $(j, i + j \bmod p)$.

Theorem.

$$0. (x, y) \times (x', y') = (f(x' - x, y' - y) - (x, y) \bmod Z_p \times Z_p).$$

$$1. [x, y] \times [x', y'] = [f(x' - x, y' - y) - (x, y) \bmod Z_p \times Z_p].$$

$$2. (x, y) \cdot [x', y'] \text{ iff } f(x' - x, y' - y) = (0, 0).$$

Example.

For $p = 3$, the selector function is

$$\begin{array}{c|cccccc} x & 0,1 & 0,2 & 1,0 & 1,2 & 2,0 & 2,1 \\ f(x) & 0,0 & 0,1 & 0,0 & 0,1 & 1,0 & 1,0 \end{array}$$

With the exponents in the order exponent of b then exponent of a ,

points			line
0,0	0,1	1,0	0,0
0,1	0,2	1,1	0,2
0,2	0,0	1,2	0,1
1,0	1,1	2,0	2,0
1,1	1,2	2,1	2,2
1,2	1,0	2,2	2,1
2,0	2,1	0,0	1,0
2,1	2,2	0,1	1,2
2,2	2,0	0,2	1,1

The points on the 3 ideal lines are

$$\begin{aligned}
[0] &= \{0,0 \ 1,1 \ 2,2\} \\
[1] &= \{0,1 \ 1,2 \ 2,0\} \\
[2] &= \{0,2 \ 1,0 \ 2,1\}
\end{aligned}$$

Example.

If $p = 7$ and $P^3 = I^3$ then the group T is

$0,0,1 \ 0,1,2 \ 1,4,4 \ 1,2,6 \ 1,6,3 \ 1,1,6 \ 1,5,4$
 $0,1,1 \ 1,3,2 \ 1,3,5 \ 1,5,2 \ 0,1,5 \ 1,0,3 \ 1,5,3$
 $1,2,1 \ 1,3,4 \ 1,2,3 \ 1,0,5 \ 1,6,5 \ 1,3,3 \ 1,6,4$
 $1,1,5 \ 1,0,1 \ 1,4,1 \ 1,5,5 \ 0,1,3 \ 1,5,6 \ 0,1,6$
 $1,3,6 \ 1,1,1 \ 1,1,3 \ 1,4,2 \ 1,4,3 \ 1,3,1 \ 1,0,6$
 $1,4,5 \ 1,1,4 \ 1,2,5 \ 1,4,6 \ 1,0,2 \ 1,1,2 \ 1,6,6$
 $1,6,1 \ 1,6,2 \ 1,0,4 \ 1,2,4 \ 1,2,2 \ 1,5,1 \ 0,1,4$

A selector is

$e, a, b, ab^4, a^3b^4, a^3b^6, a^6b^6$. points on $[1,0,0]$.

The conics are

$0,0,1 \ 0,1,1 \ 1,2,1 \ 1,1,5 \ 1,3,6 \ 1,4,5 \ 1,6,1$
 $0,0,1 \ 0,1,2 \ 1,4,4 \ 1,2,6 \ 1,6,3 \ 1,1,6 \ 1,5,5$
 $0,0,1 \ 0,1,3 \ 1,6,2 \ 1,3,3 \ 1,2,5 \ 1,5,3 \ 1,4,2$
 $0,0,1 \ 0,1,4 \ 1,1,2 \ 1,4,3 \ 1,5,5 \ 1,2,3 \ 1,3,2$
 $0,0,1 \ 0,1,5 \ 1,3,4 \ 1,5,6 \ 1,1,3 \ 1,6,6 \ 1,2,4$
 $0,0,1 \ 0,1,6 \ 1,5,1 \ 1,6,5 \ 1,4,6 \ 1,3,5 \ 1,1,1$
 $0,0,1 \ 1,1,4 \ 1,4,1 \ 1,5,2 \ 1,2,2 \ 1,3,1 \ 1,6,4$

The line is $[0,1,0]$ with points $(1,0,1) \cdot (1,0,c) = (1,0, \frac{c}{1+c})$

$0,0,1 \ 1,0,1 \ 1,0,4 \ 1,0,5 \ 1,0,2 \ 1,0,3 \ 1,0,6$.

Other points are on $[0,0,1]$.

They all have a contact of order 2 at $(0,0,1)$ with tangent $[1,0,0]$.

5.3.6 The case of 3 distinct roots.

Definition.

If the roots are a, b, c ,

0. The polynomial which has 2 of the roots corresponds to a point called isotropic point.
1. The 3 lines through 2 of the 3 isotropic points are called isotropic lines.
2. Any non isotropic line through an isotropic point is called an ideal line.
3. Any non isotropic point on an isotropic line is called an ideal point.

Example.

$p = 7$, $a = 1$, $b = 2$, $c = 4^{17}$.

0. The isotropic points are $A_0 = (1, 1, 1)$, $A_1 = (1, 2, 4)$, $A_2 = (1, 4, 2)$.

1. The isotropic lines are $a_0 = [1, 1, 1]$, $a_1 = [1, 4, 2]$, $a_2 = [1, 2, 4]$.

2. The generators of the group are $\alpha = (0, 1, 2)$ and $\beta = (0, 1, 1)$.

3. The ideal lines through A_0 are

$$\begin{aligned} [1, 3, 0] &= S_0 = \{e, b^2, b^4, a^3, a^3b^2, a^3b^4\}, \\ [1, 4, 3] &= bS_0, \\ [0, 1, 3] &= aS_0, \\ [1, 5, 6] &= abS_0, \\ [1, 0, 5] &= a^2S_0, \\ [1, 6, 2] &= a^2bS_0. \end{aligned}$$

4. The ideal lines through A_1 are

$$\begin{aligned} [1, 5, 0] &= S_1 = \{e, a^2, a^4, ab^3, a^3b^3, a^5b^3\}, \\ [1, 2, 6] &= aS_1, \\ [1, 3, 4] &= bS_1, \\ [1, 0, 3] &= abS_1, \\ [0, 1, 5] &= b^2S_1, \\ [1, 6, 5] &= b^2aS_1. \end{aligned}$$

5. The ideal lines through A_2 are

$$\begin{aligned} [1, 6, 0] &= S_2 = \{e, a^2, a^2b^2, a^4b^4, a^4b, b^3, a^2b^5\}, \\ [1, 1, 5] &= abS_2, \\ [1, 5, 1] &= aS_2, \\ [1, 0, 6] &= a^2bS_2, \\ [0, 1, 6] &= bS_2, \\ [1, 3, 3] &= ab^2S_2. \end{aligned}$$

6. A selector is $(e, b^5, ab^5, a^2b^3, a^5b^3)$ giving the points

$$(0, 0, 1), (1, 6, 1), (1, 6, 3), (1, 6, 6), (1, 6, 4) \text{ on } [110],$$

the ideal points on this line are $(1, 6, 0)$, $(1, 6, 5)$, $(1, 6, 2)$.

The 36 other lines are obtained by multiplication by any of the elements in the group, e.g. if we multiply to the left by a^5b^5 , the points are $(0, 1, 4)$, $(1, 6, 4)$, $(1, 2, 2)$, $(1, 3, 6)$, $(1, 0, 1)$, and the ideal points are $(1, 1, 5)$, $(1, 5, 0)$, $(1, 4, 3)$.

Notes.

We have therefore the following operations:

$$l := P \times Q, L := p \times q$$

$$R := P \bullet Q, r := p \bullet q?$$

¹⁷earlier version

where \bullet is done modulo a polynomial of degree 3. If the polynomial is primitive the properties are well known, what is probably new is what happens when the polynomial is not primitive. If it has 3 roots it makes sense to normalize to have the isotropic points at $(1,0,0)$, $(0,1,0)$ and $(0,0,1)$, but I do not see how this can be done in view of the fact that an isotropic point corresponds to $(I - a)(I - b)$.

Definition.

Given a polynomial of the third degree with 3 distinct roots, a line generator is a generator of a cyclic group of order $p - 1$ whose elements correspond to $p - 1$ points of a line through one of the isotropic points, the last point is an ideal point on the isotropic line which does not belong to the isotropic point.

Definition.

Two line generators are said to be independent if they are associated to lines through distinct isotropic points.

Why did I not worry about this when constructing an example and use simply distinct lines?

5.3.7 Conjecture.

Given a polynomial of the third degree with 3 distinct roots, there exists 2 independent line generators.

Comment.

I will choose the roots to be 0, 1 and -1. $P_3 = I^3 - I$.

The isotropic points are $A_0 = (1, 0, -1)$, $A_1 = (1, 1, 0)$, $A_2 = (1, -1, 0)$.

The isotropic lines are $a_0 = [0, 0, 1]$, $a_1 = [1, 1, 1]$, $a_2 = [1, -1, 1]$.

Conjecture.

With the choice just given, there exist an x such that

if $y = -2(x + 1)$, $(1, 0, x)$, $(1, 1, 1y)$, $(x + y + 1, x + 1, xy)$ are line generators corresponding to lines $[0, 1, 0]$, $[1, -1, 0]$, $[1, 1, -\frac{2x+y+2}{xy}]$ through A_0 , A_1 and A_2 .

Example.

$p = 3,$	0, 0, 1	1, 1, 2							
	1, 0, 1	1, 2, 2							
$p = 5,$	0, 0, 1	1, 1, 1	1, 1, 4	1, 1, 2					
	1, 0, 1	1, 4, 2	1, 2, 4	1, 3, 3					
	1, 0, 2	1, 2, 3	1, 4, 4	0, 1, 3					
	1, 0, 3	0, 1, 2	1, 3, 4	1, 4, 1					
$p = 7,$	roots	1, 2, 4,							$I^3 - 1 = 0$
	0, 0, 1	1, 2, 0	1, 2, 1	1, 2, 5	1, 2, 2	1, 2, 3			
	1, 0, 1	1, 3, 2	1, 5, 5	1, 4, 0	1, 1, 6	1, 6, 3			
	1, 4, 4	0, 6, 4	1, 1, 4	1, 5, 4	0, 1, 0	1, 0, 4			
	1, 1, 3	1, 0, 2	1, 6, 1	1, 4, 1	0, 1, 1	1, 3, 5			
	1, 4, 1	1, 5, 3	1, 0, 0	0, 1, 2	1, 1, 2	1, 3, 6			
	1, 6, 6	1, 5, 2	1, 1, 0	1, 4, 5	1, 3, 1	0, 1, 4			

The lines are obtained from

$$(0, 0, 1), (0, 1, 2), (0, 1, 0), (0, 1, 1), (0, 1, 4)$$

or 0,0 4,3 2,4 3,4 5,5

for instance, adding 2,3 modulo 6,6

$$2, 30, 0, 4, 15, 11, 2$$

or (1,5,4), (0,0,1), (1,5,3), (1,5,2), (1,5,5) on [1,4,0].

The c-lines are all obtained from

$$(0, 0, 1), (0, 1, 4), (1, 0, 2), (1, 5, 5), (1, 6, 4)$$

or 0,0 5,5 3,1 1,2 2,1

for instance, adding 3,2 modulo 6,6 gives

$$3, 2 \quad 2, 1 \quad 0, 3 \quad 4, 4 \quad 5, 3$$

or (1,6,1), (1,6,4), (1,2,5), (1,1,2), (1,4,5).

$p = 11$, line generators: (1,0,1), (1,1,7), (1,10,2).

$p = 13$, line generators: (1,0,1), (1,1,9), (1,12,2).

$p = 17$, line generators: (1,0,2), (1,1,11), (1,16,4).

Definition.

A selector is a set of $p - 2$ elements $P_k^i Q_k^j$ which are on an ordinary line.

Theorem.

Given 2 independent line generators P and Q , the isotropic lines are obtained as cosets of the cyclic groups generated by P , Q and $P \bullet Q$.

The ordinary lines are obtained by multiplication modulo P_3 , $P^l Q^m$ by the elements of a selector.

We may want to put this in a section on triangular geometry.

In this geometry we have ordinary, ideal and isotropic points, ordinary, ideal and isotropic lines, and c-lines. These are represented by conics through the isotropic points, the ideal c-lines are the degenerate conics consisting of an isotropic line and an ideal line to the opposite isotropic point. The isotropic c-lines are the degenerate conics consisting of two isotropic

lines. The lines and the c -lines can be interchanged. If the c -lines are considered as lines, then the lines are c -lines, in other words if we start with a geometry where we define the conics through 3 given points as lines, the conics are represented by lines. Pascal's Theorem gives the following, consider a line l , with points P_{2i} on a_i , and 3 other points P_1, P_3, P_5 , this line can be considered a c -conic, indeed, the c -lines through successive points are the degenerate c -lines or ideal c -lines, $a_0 = (A_0 \times P_1) + a_0$, $a_1 = (A_2 \times P_1) + a_2$, $a_2 = (A_2 \times P_3) + a_2$, $a_3 = (A_1 \times P_3) + a_1$, $a_4 = (A_1 \times P_5) + a_1$, $a_5 = (A_0 \times P_5) + a_0$.

The c -Pascal points are $Q_0 = (A_1 \times P_3) \times (A_0 \times P_1)$, $Q_1 = (A_2 \times P_1) \times (A_1 \times P_5)$, $Q_2 = (A_0 \times P_5) \times (A_2 \times P_3)$.

These points are on a conic, with A_0, A_1, A_2 because the Pascal line for the sequence $A_0, Q_0, A_1, Q_1, A_2, Q_2$, gives the Pascal points P_1, P_3, P_5 . This can be used to study what could be called a bi-triangular geometry.

Comment.

The c -lines can be deduced from the line by the transformation which associates, in general, to (X_0, X_1, X_2) , (X_1X_2, X_2X_0, X_0X_1) , a conic becomes then a quadric with double points, isolated or not in the case of a real field. A conic through A_1, A_2 , but not through A_0 , becomes a quadric which degenerates in a_1, a_2 and a conic through A_1, A_2 but not A_0 .

Comment.

We could choose as isotropic points, in a model of this geometry in the Euclidean plane, with Cartesian coordinates, by choosing one of them at the origin, and the 2 others at the direction of the axis. The c -lines are then hyperbolas passing through the origin, with asymptotes in the direction of the axis.

Problem.

Study the axiomatic of the triangular geometry and obtain Theorems in it. Circles could be conics through 2 of the isotropic points.

Problem.

Study the axiomatic of the triangular bi-geometry and obtain Theorems in it.

Comment.

The analysis can be repeated in the form of Euclidean geometry by considering the non-homogeneous points (x, y) and the homogeneous lines $[a, b, c]$. This can be done directly or inferred from the cases 1, 2 and 4 above, with one of the isotropic lines playing the role of the line at infinity in Euclidean geometry.

5.3.8 Notes.

In G45, I give a special case of the following Theorem valid when $s_1 = a = 0$, this generalizes the Theorem, with $b = s_{11}$ and $c = s_{111}$.

It was obtained earlier.

Theorem.

The symmetric functions of the roots are

$$\begin{aligned}
 s_1 &:= \rho_0 + \rho_1 + \rho_2 = a, \\
 s_{11} &:= \rho_1\rho_2 + \rho_2\rho_0 + \rho_0\rho_1 = b, \\
 s_{111} &:= \rho_0\rho_1\rho_2 = c, \\
 s_2 &:= \rho_0^2 + \rho_1^2 + \rho_2^2 = a^2 - 2b, \\
 s_{21} &:= \rho_0^2(\rho_1 + \rho_2) + \rho_1^2(\rho_2 + \rho_0) + \rho_2^2(\rho_0 + \rho_1) = ab - 3c, \\
 s_3 &:= \rho_0^3 + \rho_1^3 + \rho_2^3 = a(a^2 - 3b) + 3c, \\
 s_{211} &:= ac, \\
 s_{22} &:= b^2 - 2ac, \\
 s_{31} &:= a(ab - c) - 2b^2, \\
 s_4 &:= a(a^3 - 4ab + 4c) + 2b^2.
 \end{aligned}$$

Theorem.

0. The conic which pass through the isotropic points is

$$\begin{aligned}
 &k((b^2 - 2ac)X_0^2 + bX_1^2 + 3X_2^2 \\
 &+ 2aX_1X_2 + 2(a^2 - 2b)X_2X_0 - (3c - ab)X_0X_1) \\
 &+ l(bcX_0^2 + 3cX_1^2 + aX_2^2 \\
 &+ 2bX_1X_2 - (3c - ab)X_2X_0 + 2acX_0X_1) \\
 &+ m(3c^2X_0^2 + acX_1^2 + (a^2 - 2b)X_2^2 \\
 &- (3c - ab)X_1X_2 + 2(b^2 - 2ac)X_2X_0 + 2bcX_0X_1) = 0,
 \end{aligned}$$

1. which is tangent to the isotropic lines is

$$\begin{aligned}
 &k(3x_0^2 + (a^2 + b)x_1^2 + acx_2^2 \\
 &- (3c + ab)x_1x_2 + 2bx_2x_0 - 4ax_0x_1) \\
 &+ l(ax_0^2 + a(a^2 - 2b) + 3c)x_1^2 + (a^2 - 2b)cx_2^2 \\
 &- (a(ab + c) - 2b^2)x_1x_2 - (3c - ab)x_2x_0 - 2(a^2 - b)x_0x_1) \\
 &+ m((a^2 - 2b)x_0^2 + a(a^3 - 3ab + 4c)x_1^2 + (a(a^2 - 3b) + 3c)cx_2^2 \\
 &+ (a(-a^2b + 3b^2 - ac) - bc)x_1x_2 + (a(ab - c) - 2b^2)x_2x_0 \\
 &- (a(2a^2 - 5b) + 3c)x_0x_1) = 0.
 \end{aligned}$$

Proof:

The degenerate conics through the isotropic points are

$$\begin{aligned}
 &\alpha_0(\rho_1^2X_0 + \rho_1X_1 + X_2)(\rho_2^2X_0 + \rho_2X_1 + X_2)) \\
 &+ \alpha_1(\rho_2^2X_0 + \rho_2X_1 + X_2)(\rho_0^2X_0 + \rho_0X_1 + X_2)) \\
 &+ \alpha_2(\rho_0^2X_0 + \rho_0X_1 + X_2)(\rho_1^2X_0 + \rho_1X_1 + X_2)) = 0.
 \end{aligned}$$

If we choose, in succession, $\alpha_0 = \alpha_1 = \alpha_2 = 1$, $\alpha_0 = \rho_0$, $\alpha_1 = \rho_1$, $\alpha_2 = \rho_2$, and $\alpha_0 = \rho_0^2$, $\alpha_1 = \rho_1^2$, $\alpha_2 = \rho_2^2$,

we obtain respectively the expressions whose coefficients are k , l and m . Similarly for the c -points we start with the degenerate conics tangent to the isotropic lines, which are

$$\begin{aligned} & \alpha_0(x_0 - (\rho_2 + \rho_0)x_1 + \rho_2\rho_0x_2)(x_0 - (\rho_0 + \rho_1)x_1 + \rho_0\rho_1x_2) \\ & + \alpha_1(x_0 - (\rho_0 + \rho_1)x_1 + \rho_0\rho_1x_2)(x_0 - (\rho_1 + \rho_2)x_1 + \rho_1\rho_2x_2) \\ & + \alpha_2(x_0 - (\rho_1 + \rho_2)x_1 + \rho_1\rho_2x_2)(x_0 - (\rho_2 + \rho_0)x_1 + \rho_2\rho_0x_2) = 0. \end{aligned}$$

The following Theorem was developed to prove the relation between the conics associated to the co, bi and semi-selectors but were found not to be needed. It is now an answer to an exercise.

Answer to exercise .

Let $s_1 = 0$, the conic through $(0,1,0)$, $(0,0,1)$

0. which passes through the isotropic points is

$$s_{111}X_0^2 - X_1X_2 = 0.$$

1. which is tangent to the isotropic lines is

$$x_0^2 - s_{111}x_1x_2 + s_{11}x_2x_0 = 0.$$

or

$$(s_{111}X_0 + s_{11}X_1)^2 - 4s_{111}X_1X_2 = 0,$$

2. which has the isotropic triangle as polar triangle is

$$s_{111}X_0^2 - 2s_{11}X_0X_1 + 2X_1X_2 = 0.$$

Proof: Using

3. $\rho_1 + \rho_2 = -\rho_0$, we can check

$$\begin{aligned} & \text{for } 0, \rho_0\rho_1\rho_2 - (\rho_1 + \rho_2)\rho_1\rho_2 = 0, \\ & \text{for } 1, \rho_0^4 - \rho_0\rho_1\rho_2\rho_0 + (\rho_1\rho_2 + \rho_2\rho_0 + \rho_0\rho_1)\rho_0^2 = 0, \\ & \text{for } 2, \begin{pmatrix} \rho_0^3 \\ \rho_0^2 \\ \rho_0 \end{pmatrix} = \begin{pmatrix} s_{111} & -s_{11} & 0 \\ -s_{11} & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ -\rho_1 - \rho_2 \\ \rho_1\rho_2 \end{pmatrix}. \end{aligned}$$

Exercise.

Let $s_1 = 0$. Determine the conic through $(0,1,0)$, $(0,0,1)$,

0. which passes through the isotropic points,

1. which is tangent to the isotropic lines,

2. which has the isotropic triangle as polar triangle.

Comment.

To obtain the statements of the preceding Theorem, I will illustrate for the case 2. If the conic is represented by the symmetric matrix

$$\begin{pmatrix} 1 & \gamma & \beta \\ \gamma & 0 & \alpha \\ \beta & \alpha & 0 \end{pmatrix}.$$

The condition that I_0 is the pole of i_0 gives

$$\mu \rho_0^2 = 1 - \gamma(\rho_1 + \rho_2) + \beta \rho_1 \rho_2,$$

$$\mu \rho_0 = \gamma + \alpha \rho_1 \rho_2,$$

$$\mu = \beta - \alpha(\rho_1 + \rho_2).$$

Eliminating μ from the first 2 and the last 2 equations gives

$$1 - \gamma(\rho_1 + \rho_2) + \beta \rho_1 \rho_2 - \gamma \rho_0 - \alpha \rho_0 \rho_1 \rho_2 = 0,$$

$$\gamma + \alpha \rho_1 \rho_2 - \beta \rho_0 + \alpha(\rho_0 \rho_1 + \rho_0 \rho_2) = 0,$$

or using 3,

$$1 + \beta \rho_1 \rho_2 - \alpha s_{111} = 0,$$

$$\gamma + \alpha s_{11} - \beta \rho_0 = 0.$$

Because the conic cannot depend on individual values of $\rho_0, \rho_1, \rho_2, \beta = 0$ and then $\alpha = \frac{1}{s_{111}}$ and $\gamma = -\alpha s_{11}$.

5.3.9 On the tetrahedron.**Example.**

Let the roots be 0,1,2,3 and $p = 5$,

the isotropic points are $(1,-1,1,-1), (1,0,1,0), (1,1,-2,0), (1,2,2,0)$.

$P_4 = I^4 - I^3 + I^2 - I$, therefore, $I^5 = I \pmod{P_4}$ and $I^6 = I^2 \pmod{P_3}$.

The cubic surface is given by

$$\begin{vmatrix} k & l & m & n \\ Z+T & Y+Z & X+Y & X \\ X-Z & T-Y & Z-x & Y \\ Y+Z & X+Y & X+T & Z \end{vmatrix} = 0.$$

For instance, a point on $I_0 \times I_1$ is $(u+v, -u, u+v, -u)$ and

$$\begin{vmatrix} k & l & m & n \\ v & v & v & u+v \\ 0 & 0 & 0 & -u \\ v & v & v & u+v \end{vmatrix} = 0,$$

because 2 rows are equal.

Similarly for a point on $I_2 \times I_3$, $(u+v, 2u+v, 2u-2v, 0)$,

$$\begin{vmatrix} k & l & m & n \\ 2u-2v & 4u-v & 3u+2v & u+v \\ -u+3v & -2u-v & u-3v & 2u+v \\ 4u-v & 3u+2v & u+v & 2u-2v \end{vmatrix} = 0, \text{ because the sum of the last 3 rows is equal to}$$

$0 \pmod{5}$.

No other conditions are needed to obtain a family of cubics with 3 parameters because if the isotropic points are chosen as $(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)$ the cubic is

$$d_0X_1X_2X_3 + d_1X_2X_3X_0 + d_2X_3X_0X_1 + d_3X_0X_1X_2 = 0.$$

Example.

¹⁹ For the semi-transformation, let $p = 5$ and $P_4 = I^4 - I^3 + I^2 - I$, $(X, Y, Z, T)^2 = (x, y, z, t)$ gives

$$\begin{aligned} x &= 2XT + 2YZ + (2XZ + Y^2) \\ y &= 2YT + Z^2 - (2XZ + Y^2) + X^2, \\ z &= 2ZT + (2XZ + Y^2) + 2XY, \\ t &= T^2. \end{aligned}$$

A plane $\{k, l, m, n\}$ is therefore transformed in the quadric represented by the symmetric matrix

$$\begin{pmatrix} l & m & k-l+m & k \\ m & k-l+m & k & l \\ k-l+m & k & l & m \\ k & l & m & n \end{pmatrix}. \text{ The isotropic points are } (1, -1, 1, -1), (1, 0, 1, 0), (1, 1, -2, 0), (1, 2, 2, 0),$$

and the corresponding isotropic planes are $\{0, 0, 0, 1\}$, $\{1, 1, 1, 1\}$, $\{-2, -1, 2, 1\}$, $\{2, -1, -2, 1\}$.

It is easy to check the latter are the polar of the former, independently from k, l, m, n . It is easy to verify that the quadric which have the isotropic tetrahedron as polar tetrahedron form a 3 parameter family and that this generalizes to n dimensions.

Exercise.

Study the relation which exist between the correspondance between a pair of points and the pair obtained at the intersection of the tangents at the 2 points to the c -line through these points and the intersection of the c -lines tangent to the line through the 2 points at the two points.

Hint: Study first how to obtain from the point on any other line through a point and the c -line that line through the point which is tangent to the c -line.

Definition.

Let l^c be a line through P ,

Chapter 6

GENERALIZATION TO 3 DIMENSIONS

6.0 Introduction.

I will sketch here part of the generalization to 3 dimensions of what has been presented in the preceding parts. It will be obvious how to generalize further to n dimensions. After a brief look at the history, I will review the application of Grassmann algebra to the incidence properties of the fundamental objects in 3 dimensions, the points, the lines and the planes.

The finite polar geometry will be introduced in section 6.2. It is obtained by preferring a plane, the ideal plane, to which correspond the notions of affine geometry, parallelism, mid-points, equality of segments on parallel lines, and a quadric, the fundamental quadric, which, together with the ideal plane, allow for the definition of spheres and therefore equality of distances between unordered pairs of points as well as orthogonality or more generally equality of angles between ordered pair of lines.

To illustrate properties in 3 dimensions, the geometry of the triangle in involutive geometry will be generalized, in section 6.2.3 to the study of the general tetrahedron in finite polar geometry. In the classical case, the first work on the subject is that of Prouhet, this was followed by important memoirs of Intrigila and Neuberg.

We will see that a special case occurs very naturally, that of the orthogonal tetrahedron, studied in section 6.2.4. We will see that the success of the theory of this special case is explained by the generalization to 3 dimension of the symmetry which exists in 2 dimensions when we exchange the barycenter and the orthocenter.

The isodynamic tetrahedron is studied in section 6.2.5.

The generalization of many other 3 dimensional and n dimensional concepts is left to the reader.

This part ends with an introduction to the anti-polar geometry 6.1.5.

6.0.1 Relevant historical background.

Introduction.

In the classical case, the extension to 3 dimensions is already given by Euclid. The earlier definitions of conics derives from the circular cone in 3 dimensions. Of note is also the fact that the 2-dimensional Desargues' theorem derives directly from the incidence properties in 3 dimensions. Although the algebraic notation of analytic geometry, introduced by Descartes immediately extends and at once suggests to go beyond the observable to 4 and to n dimensions, it is not suitable if we progress from finite polar geometry - where equality of distance and angles are defined and are not primary notions - to finite 3 dimensional Euclidean geometry. Instead, I will use the notation of exterior algebra introduced by Grassmann.

6.0.2 Grassmann algebra applied to incidence properties of points, lines and planes

Introduction.

After introducing in 6.0.2 the algebraic representation of points, lines and planes in Z_p^3 , I recall the basic concepts and properties of the exterior algebra of Grassmann (6.0.2 to 6.0.2), I define the incidence relations (6.0.2) and derive the associated properties (6.0.2, 6.0.2 to 6.0.2).

Definition.

The points and planes in 3 dimensions will be represented using 4 homogeneous coordinates. (Not all coordinates are 0, and if all coordinates are multiplied modulo p by the same non zero element in Z_p , we obtain the same point or plane.)

Points will be denoted by a capital letter and the coordinates will be placed between parenthesis. Planes will be denoted by a capital letter preceded by the symbol “|” or by a calligraphic letter and the coordinates will be placed between braces.

The lines will be represented by 6 homogeneous coordinates $[l_0, l_1, l_2, l_3, l_4, l_5]$, such that $l_0l_5 + l_1l_4 + l_2l_3 = 0$.

This part of the definition will be justified in 6.0.2.4 and 6.0.2.

The normalization will again be such that the leftmost non zero coordinate is 1.

Example.

Let $p = 7$,

$P := (2, 4, 6, 1) = (1, 2, 3, 4)$, $l := [3, 3, 1, 4, 3, 5] = [1, 1, 5, 6, 1, 4]$,

$\mathcal{Q} := \{5, 1, 1, 1\} = \{1, 3, 3, 3\}$ are respectively a point, a line and a plane.

Notation.

To define algebraically the incidence properties, I will use Grassmann algebra with exterior product multiplication. If e_0, e_1, e_2, e_3 are “unit” vectors, we write

$$0. P := (P_0, P_1, P_2, P_3) := P_0 e_0 + P_1 e_1 + P_2 e_2 + P_3 e_3.$$

$$1. l := [l_0, l_1, l_2, l_3, l_4, l_5] \\ := l_0 e_0 \vee e_1 + l_1 e_0 \vee e_2 + l_2 e_0 \vee e_3 + l_3 e_1 \vee e_2 + l_4 e_3 \vee e_1 + l_5 e_2 \vee e_3, \\ \text{with}$$

$$2. l_0 l_5 + l_1 l_4 + l_2 l_3 = 0.$$

$$3. Q := \{Q_0, Q_1, Q_2, Q_3\} \\ := Q_0 e_1 \vee e_2 \vee e_3 + Q_1 e_3 \vee e_2 \vee e_0 + Q_2 e_3 \vee e_0 \vee e_1 + Q_3 e_1 \vee e_0 \vee e_2.$$

In each case not all coefficients are zero.

The specific notation for l and Q will be justified in 6.0.2. For Q the order of the unit vectors is chosen in such a way that the last ones are consecutive, e_3, e_0, e_1, e_2 . If condition 2 is not satisfied, the 2-form will be denoted using an identifier starting with a lower case letter and followed by “ ”. If an identity is satisfied for the general 2-form l' as well as for the line l , I will use the notation l' (see for instance 6.0.2).

I recall:

Definition.

The exterior product is defined by using the usual rules of algebra, namely, commutativity, associativity, neutral element property and distributivity with the exception

$$e_i \vee e_j = -e_j \vee e_i \text{ which gives, in particular, } e_i \vee e_i = 0.$$

Lemma.

$$(e_i \vee e_j) \vee (e_k \vee e_l) = (e_k \vee e_l) \vee (e_i \vee e_j).$$

Theorem.

$$P \vee Q = -Q \vee P, l' \vee m' = m' \vee l'.$$

Corollary.

$$P \vee P = 0.$$

Definition.

Given any expression involving points, lines or planes using the Grassmann representation, the dual of an expression is obtained by replacing the coefficient by itself and

$$e_{i_0} \vee \dots \vee e_{i_{k-1}} \text{ by } j e_{i_k} \vee \dots \vee e_{i_3}$$

where $i_0, \dots, i_{k-1}, i_k, \dots, i_3$ is a permutation of $0, 1, 2, 3$ and $j = 1$ if the permutation is even, -1 if the permutation is odd.

Theorem.

0. $dual(P) = P_0 e_1 \vee e_2 \vee e_3 + P_1 e_3 \vee e_2 \vee e_0 + P_2 e_3 \vee e_0 \vee e_1 + P_3 e_1 \vee e_0 \vee e_2.$
1. $dual(l') = l_0 e_2 \vee e_3 + l_1 e_3 \vee e_1 + l_2 e_1 \vee e_2 + l_3 e_0 \vee e_3 + l_4 e_0 \vee e_2 + l_5 e_0 \vee e_1.$

Because of the notation 6.0.2.1, duality, for a line, simply reverses the order of the components of l .

Notation.

0. $P \cdot Q := Q \cdot P := dual(P \vee Q),$
1. $l' \wedge P := P \wedge l' := dual(dual(P) \vee dual(l')).$
2. $P \wedge Q := Q \wedge P := dual(dual(P) \vee dual(Q)).$

Definition.

A point P is incident to a line l iff

$$P \vee l = 0.$$

A point P is incident to a plane Q iff

$$P \vee Q = 0.$$

A line l is incident to a plane Q iff

$$l \wedge Q = 0.$$

Theorem.

0. $P \vee Q = (P_0 Q_1 - P_1 Q_0) e_0 \vee e_1 + (P_0 Q_2 - P_2 Q_0) e_0 \vee e_2$
 $+ (P_0 Q_3 - P_3 Q_0) e_0 \vee e_3 + (P_1 Q_2 - P_2 Q_1) e_1 \vee e_2$
 $+ (P_3 Q_1 - P_1 Q_3) e_3 \vee e_1 + (P_2 Q_3 - P_3 Q_2) e_2 \vee e_3.$
1. $P \vee Q = (P_2 Q_3 - P_3 Q_2) e_0 \vee e_1 + (P_3 Q_1 - P_1 Q_3) e_0 \vee e_2$
 $+ (P_1 Q_2 - P_2 Q_1) e_0 \vee e_3 + (P_0 Q_3 - P_3 Q_0) e_1 \vee e_2$
 $+ (P_0 Q_2 - P_2 Q_0) e_3 \vee e_1 + (P_0 Q_1 - P_1 Q_0) e_2 \vee e_3.$
2. $P \vee l' = (P_1 l_5 + P_2 l_4 + P_3 l_3) e_1 \vee e_2 \vee e_3$
 $+ (-P_0 l_5 + P_2 l_2 - P_3 l_1) e_3 \vee e_2 \vee e_0$
 $+ (-P_0 l_4 - P_1 l_2 + P_3 l_0) e_3 \vee e_0 \vee e_1$
 $+ (-P_0 l_3 + P_1 l_1 - P_2 l_0) e_1 \vee e_0 \vee e_2.$
3. $P \vee l' = (P_1 l_0 + P_2 l_1 + P_3 l_2) e_1 \vee e_2 \vee e_3$
 $+ (-P_0 l_0 + P_2 l_3 - P_3 l_4) e_3 \vee e_2 \vee e_0$
 $+ (-P_0 l_1 - P_1 l_3 + P_3 l_5) e_3 \vee e_0 \vee e_1$
 $+ (-P_0 l_2 + P_1 l_4 - P_2 l_5) e_1 \vee e_0 \vee e_2.$
4. $l' \vee m' = (l_0 m_5 + l_1 m_4 + l_2 m_3 + l_3 m_2 + l_4 m_1 + l_5 m_0) e_0 \vee e_1 \vee e_2 \vee e_3.$
5. $P \vee Q = (P_0 Q_0 + P_1 Q_1 + P_2 Q_2 + P_3 Q_3) e_0 \vee e_1 \vee e_2 \vee e_3.$

6. $P \vee (P \vee l') = 0.$
7. $\mathcal{Q} \vee (\mathcal{Q} \wedge l') = 0.$
8. $0. (P \vee l') \wedge l' = -(l_0 l_5 + l_1 l_4 + l_2 l_3)P.$
 1. $(P \vee l) \wedge l = 0.$
9. $0. (\mathcal{Q} \wedge l') \vee l' = -(l_0 l_5 + l_1 l_4 + l_2 l_3)\mathcal{Q}.$
 1. $(\mathcal{Q} \wedge l) \vee l = 0.$

The proof is straightforward or follows from duality.

The condition 6.0.2.2 that a sextuple be a line is precisely chosen to insure 8.1 and 9.1.

Example.

For $p = 7$, given $P_0 := (1, 2, 3, 4)$, $P_1 := (1, 0, 1, 1)$, $P_2 := (1, 1, 0, 1)$, $P_3 := (1, 0, 0, 1)$,
 $l_0 := [1, 1, 5, 6, 1, 4]$, $l_1 := [1, 6, 0, 6, 1, 1]$, $\mathcal{Q}_0 := \{1, 3, 3, 3\}$,
 $\mathcal{Q}_1 := \{1, 5, 0, 6\}$, we can easily verify
 P_0 and P_1 are incident to l_0 , P_1 and P_2 are incident to l_1 ,
 P_0, P_1, P_2, l_0 and l_1 are incident to \mathcal{Q}_0 , P_3 and l_0 are incident to \mathcal{Q}_1 .

Notation.

As for 2 dimensional finite projective geometry, we will make use of a compact notation, assuming that the elements are ordered as if the 4 or 6 normalized coordinates were forming an integer in base p . We have the correspondence

$$\begin{array}{ll}
 (0) := (0, 0, 0, 1), & [0] := [0, 0, 0, 0, 0, 1], \\
 (1) := (0, 0, 1, 0), & [1] := [0, 0, 0, 0, 1, 0], \\
 (p+1) := (0, 1, 0, 0), & [p+1] := [0, 0, 0, 1, 0, 0], \\
 (p^2 + p + 1) := (1, 0, 0, 0), & [p^2 + p + 1] := [0, 0, 1, 0, 0, 0], \\
 & [p^3 + p^2 + p + 1] := [0, 1, 0, 0, 0, 0], \\
 & [p^4 + p^3 + p^2 + p + 1] := [1, 0, 0, 0, 0, 0].
 \end{array}$$

Example.

Continuing Example 6.0.2,

$P_0 = (180)$, $P_1 = (65)$, $P_2 = (107)$, $P_3 = (58)$, $l_0 = [7222]$, $l_1 = [17509]$, $\mathcal{Q}_0 = \{228\}$,
 $\mathcal{Q}_1 = \{308\}$.

Theorem.

P and Q are distinct iff $P \vee Q \neq 0$.

Proof: By Corollary 6.0.2, if P and Q are not distinct, $Q = kP$, $k \neq 0$ and $P \vee Q = P \vee kP = 0$. If $P \vee Q = 0$, let P_0 be a coefficient of P different from 0, 6.0.2.0 gives $P_0 Q_1 = P_1 Q_0$, $P_0 Q_2 = P_2 Q_0$, $P_0 Q_3 = P_3 Q_0$, therefore if $Q_0 = 0$ then $Q_1 = Q_2 = Q_3 = 0$, and Q is not a point.

If $Q_0 \neq 0$, I can, by homogeneity choose $Q_0 = P_0$ and then $Q_1 = P_1$, $Q_2 = P_2$ and $Q_3 = P_3$ or $Q = P$.

Theorem.

Given 2 distinct points P and Q , there exist one and only one line $l = P \vee Q$ incident to P and Q .

Proof: Because of associativity, $P \vee (P \vee Q) = 0$ and $(P \vee Q) \vee Q = 0$, therefore $l = P \vee Q$ is incident to both P and Q and $l \neq 0$ because P and Q are distinct.

The line is unique. Let $P \vee Q \neq 0$, $P \vee l = Q \vee l = 0$, $l \neq 0$.

Because $P \vee Q \neq 0$, one of the coordinates is different from 0, let it be

$P_0Q_1 - P_1Q_0$. Theorem 6.0.2.1 gives 4 equations associated to $P \vee l = 0$ and 4 equations associated to $Q \vee l = 0$, the last equations are

$$-P_0l_3 + P_1l_1 - P_2l_0 = 0$$

$$-Q_0l_3 + Q_1l_1 - Q_2l_0 = 0.$$

Multiplying the first by $-Q_0$ and the second by P_0 gives

$$0. (P_0Q_1 - P_1Q_0)l_1 = (P_0Q_2 - P_2Q_0)l_0,$$

Similarly multiplying by $-Q_1$ and P_1 gives

$$1. (P_0Q_1 - P_1Q_0)l_3 = (P_1Q_2 - P_2Q_1)l_0,$$

The third equation of each set gives similarly

$$2. (P_0Q_1 - P_1Q_0)l_2 = (P_0Q_3 - P_3Q_0)l_0,$$

$$3. (P_0Q_1 - P_1Q_0)l_4 = (P_3Q_1 - P_1Q_3)l_0,$$

If we add the first equations for $P \vee l = 0$ multiplied by $-Q_0$ and $-Q_1$, we get

$$4. (P_0Q_1 - P_1Q_0)l_5 = -Q_1P_3l_1 + Q_1P_2l_2 + Q_0P_3l_3 + Q_0P_2l_4 = 0.$$

Because $l_0 \neq 0$, the first parenthesis is different from 0, otherwise, it follows from 0, 1, 2 and 3 then $l_1 = l_3 = l_2 = l_4 = 0$, and from 4 that $l_5 = 0$. We can, because of homogeneity write

$$l_0 = P_0Q_1 - P_1Q_0,$$

it follows that

$$l_1 = P_0Q_2 - P_2Q_0.$$

$$l_3 = P_1Q_2 - P_2Q_1.$$

and from 2 and 3,

$$l_2 = P_0Q_3 - P_3Q_0,$$

$$l_4 = P_3Q_1 - P_1Q_3,$$

Replacing in 4, gives

$$\begin{aligned} (P_0Q_1 - P_1Q_0)l_5 &= Q_1P_2(P_0Q_3 - P_3Q_0) - Q_1P_3(P_0Q_2 - P_2Q_0) \\ &\quad + Q_0P_2(P_3Q_1 - P_1Q_3) + Q_0P_3(P_1Q_2 - P_2Q_1) \\ &= (P_0Q_1 - P_1Q_0)(P_2Q_3 - P_3Q_2). \end{aligned}$$

hence

$$l_5 = P_2Q_3 - P_3Q_2.$$

Therefore $l = P \vee Q$.

Theorem.

Given a point P and a line l , not incident to P , there exists one and only one plane $\mathcal{Q} = P \vee l$ incident to P and l .

Proof: Because of associativity, 6.0.2 and 6.0.2.4.1, $P \vee (P \vee l) = (P \vee l) \wedge l = 0$, therefore $\mathcal{Q} = P \vee l$ is incident to both P and l and $\mathcal{Q} \neq 0$ because P and l are not incident.

The plane is unique, if $P \vee \mathcal{Q} = l \vee \mathcal{Q} = 0$ and $\mathcal{Q} \neq 0$, let \mathcal{Q}_0 be a coefficient of $\mathcal{Q} \neq 0$. $P \vee \mathcal{Q} = 0$ and $l \vee \mathcal{Q} = 0$ give

$$P_0 \mathcal{Q}_0 + P_1 \mathcal{Q}_1 + P_2 \mathcal{Q}_2 + P_3 \mathcal{Q}_3 = 0,$$

$$\mathcal{Q}_1 l_0 + \mathcal{Q}_2 l_1 + \mathcal{Q}_3 l_2 = 0,$$

$$-\mathcal{Q}_0 l_0 + \mathcal{Q}_2 l_3 - \mathcal{Q}_3 l_4 = 0,$$

$$-\mathcal{Q}_0 l_1 - \mathcal{Q}_1 l_3 + \mathcal{Q}_3 l_5 = 0,$$

$$-\mathcal{Q}_0 l_2 + \mathcal{Q}_1 l_4 - \mathcal{Q}_2 l_5 = 0.$$

Multiplying the equations respectively by l_5 , 0 , 0 , $-P_3$ and P_2 and adding gives using homogeneity, and the same argument used in the preceding Theorem,

$$\mathcal{Q}_0 = P_1 l_5 + P_2 l_4 + P_3 l_3,$$

$$\mathcal{Q}_1 = -P_0 l_5 - P_3 l_1 + P_2 l_2.$$

Similarly, if we multiply respectively by l_4 , 0 , P_3 , 0 and $-P_1$ and then add,

$$\mathcal{Q}_2 = -P_0 l_4 + P_3 l_0 - P_1 l_2,$$

and if we multiply respectively by l_3 , 0 , $-P_2$, P_1 and 0 and then add,

$$\mathcal{Q}_3 = -P_0 l_3 - P_2 l_0 + P_1 l_2.$$

Therefore $\mathcal{Q} = P \vee l$.

Using duality, it is easy to deduce from 6.0.2 and 6.0.2.

Theorem.

Given 2 distinct planes \mathcal{P} and \mathcal{Q} , there exist one and only one line $l = \mathcal{P} \wedge \mathcal{Q}$ incident to \mathcal{P} and \mathcal{Q} .

Theorem.

Given a plane \mathcal{Q} and a line l , not incident to \mathcal{Q} , there exists one and only one point $P = \mathcal{Q} \wedge l$ incident to \mathcal{Q} and l .

Lemma.

If l and m are lines, then

$$\begin{aligned} & (l_1 m_5 - l_5 m_1)(l_0 m_5 + l_1 m_4 + l_2 m_3) + (l_1 m_2 - l_2 m_1)(l_3 m_5 - l_5 m_3) \\ & = l_1 m_5(l_0 m_5 + l_1 m_4 + l_2 m_3 + l_3 m_2 + l_4 m_1 + l_5 m_0). \end{aligned}$$

Lemma.

If $l = [0, 0, 0, l_3, l_4, l_5]$ and $m = [m_0, m_1, m_2, 0, 0, 0]$, then l and m have a point P in common iff $l \vee m = 0$ and $P = (0, m_0, m_1, m_2)$.

Proof: The 4 conditions associated with $P \vee l = 0$ give, because not all l_3 , l_4 and l_5 can be 0, $P_0 = 0$ and $P_1 l_5 + P_2 l_4 + P_3 l_3 = 0$. The 4 conditions associated with $P \vee m = 0$ give,

because not all m_0, m_1 and m_2 can be 0, $P_1 = m_0, P_2 = m_1, P_3 = m_2$, substituting in the remaining equation gives the equivalence with $l \vee m = 0$.

Lemma.

If $l_5m_5 \neq 0$ and $l_1m_5 \neq l_5m_1$, if P is on l and m , then l and m have a point P in common iff $l \vee m = 0$ and

$$P = (l_0m_5 + l_1m_4 + l_2m_3, l_3m_4 - l_4m_3, l_5m_3 - l_3m_5, l_4m_5 - l_5m_4).$$

Proof: The first component of $P \vee l = 0$ and of $P \vee m = 0$ implies $P_1 = k_0(l_4m_3 - l_3m_4)$, $P_2 = k_0(l_3m_5 - l_5m_3)$ and $P_3 = k_0(l_5m_4 - l_4m_5)$. Similarly, the second components implies $P_0 = k_1(l_1m_2 - l_2m_1)$, $P_2 = k_1(l_1m_5 - l_5m_1)$ and $P_3 = k_1(l_2m_5 - l_5m_2)$. Consistency implies $(l_1m_5 - l_5m_1)(l_5m_4 - l_4m_5) = (l_3m_5 - l_5m_3)(l_2m_5 - l_5m_2)$.

or

$$\begin{aligned} & l_5m_5(l_3m_2 + l_2m_3 + l_1m_4 + l_4m_1) + m_5^2(-l_1l_4 - l_2l_3) \\ & + l_5^2(-m_1m_4 - m_2m_3) \\ & = l_5m_5(l_3m_2 + l_2m_3 + l_1m_4 + l_4m_1 + l_0m_5 + l_5m_0), \end{aligned}$$

because l and m are lines. Choosing $k_1 = (l_3m_5 - l_5m_3)/(l_1m_5 - l_5m_1)$ and $k_0 = -1$ gives the expression for P using Lemma 6.0.2.

Theorem.

If 2 distinct lines l and m are such that $l \vee m = 0$, they are incident to a point noted $l \rtimes m$ and to a plane noted $l \mathcal{X} m$. Vice-versa, if 2 distinct lines are incident to the same point or the same plane then $l \vee m = 0$. Moreover, if $l = [l_0, l_1, l_2, l_3, l_4, l_5]$ and $m = [m_0, m_1, m_2, m_3, m_4, m_5]$, then one of the following will give the point $l \rtimes m$

0. $(l_0m_5 + l_1m_4 + l_2m_3, l_3m_4 - l_4m_3, l_5m_3 - l_3m_5, l_4m_5 - l_5m_4)$.
1. $(l_1m_2 - l_2m_1, l_4m_1 + l_3m_2 + l_0m_5, l_1m_5 - l_5m_1, l_2m_5 - l_5m_2)$,
2. $(l_2m_0 - l_0m_2, l_0m_4 - l_4m_0, l_5m_0 + l_3m_2 + l_1m_4, l_2m_4 - l_4m_2)$.
3. $(l_0m_1 - l_1m_0, l_0m_3 - l_3m_0, l_1m_3 - l_3m_1, l_5m_0 + l_4m_1 + l_2m_3)$.

and the plane $l \mathcal{X} m$

4. $\{l_5m_0 + l_4m_1 + l_3m_2, l_2m_1 - l_1m_2, l_0m_2 - l_2m_0, l_1m_0 - l_0m_1\}$.
5. $\{l_4m_3 - l_3m_4, l_5m_0 + l_2m_3 + l_1m_4, l_4m_0 - l_0m_4, l_3m_0 - l_0m_3\}$.
6. $\{l_3m_5 - l_5m_3, l_5m_1 - l_1m_5, l_4m_1 + l_2m_3 + l_0m_5, l_3m_1 - l_1m_3\}$.
7. $\{l_5m_4 - l_4m_5, l_5m_2 - l_2m_5, l_4m_2 - l_2m_4, l_3m_2 + l_1m_4 + l_0m_5\}$.

The proof follows by a judicious application of the Lemmas.

Exercise.

If l and m are lines and $l \vee m = 0$ then $l \vee (l \rtimes m) = (l \rtimes m) \vee m = 0$.

Exercise.

If $l \times m$ and $l \mathcal{X} m$ are defined by 6.0.2.0 and .4, then $(l \times m) \vee (l \mathcal{X} m) = 0$.

6.1 Affine Geometry in 3 Dimensions.

6.1.0 Introduction.

To define a 3 dimensional Euclidean geometry, I will start with a preferred plane \mathcal{I} to which are associated the notions of affine geometry. Just as in the case of the Pappian plane, we can define the notions of parallelism, mid-point, equality of segments (ordered pair of points) on parallel lines. It is convenient to introduce a matrix notation to express parallelism and in later sections polarity and orthogonality. Bold faced letters will be used for matrices. The coordinates of points, lines and planes will have associated with them vectors which will be considered as row vectors.

6.1.1 The ideal plane and parallelism.

Definition.

The preferred plane is called the ideal plane. There is no restriction in choosing the ideal plane $\mathcal{I} = \{1, 1, 1, 1\}$ because the coordinates of \mathcal{I} simply corresponds to those of the unit point $(1, 1, 1, 1)$ and can be considered as the polar of the unit point with respect to the tetrahedron of the coordinate system $(1, 0, 0, 0)$, $(0, 1, 0, 0)$, $(0, 0, 1, 0)$, $(0, 0, 0, 1)$.

Definition.

The points in the ideal plane are called the ideal points, the lines in the ideal plane are called the ideal lines.

Definition.

Two lines are parallel iff they are incident to \mathcal{I} at the same point.

Two planes are parallel iff they are incident to \mathcal{I} on the same line.

A plane \mathcal{Q} and a line l are parallel iff the line $\mathcal{Q} \wedge \mathcal{I}$ is incident to the point $\mathcal{I} \wedge l$.

Definition.

$$\mathbf{L} := \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 & 1 & -1 \end{pmatrix}, \mathbf{P} := \left\{ \begin{pmatrix} 0 & 0 & 1 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix} \right\}.$$

Theorem.

If l is a line then $\mathbf{L}l^T$ is the direction of the line l .

If \mathcal{P} is a plane then $\mathbf{P}\mathcal{P}^T$ is the direction of the plane \mathcal{P} .

The proof follows from 6.0.2.3 and 1. Notice that \mathbf{P} is obtained from the transpose of \mathbf{L} by exchanging row i with row $5 - i$, $i = 0, 1, 2$.

Theorem.

Let $\mathcal{Q} := \{Q_0, Q_1, Q_2, Q_3\}$ and $l := [l_0, l_1, l_2, l_3, l_4, l_5]$,

The plane \mathcal{Q} is parallel to the line l iff

$$0. \quad \mathcal{Q}\mathbf{L}l^T = 0, \text{ or} \\ -Q_0(l_0 + l_1 + l_2) + Q_1(l_0 - l_3 + l_4) + Q_2(l_1 + l_3 - l_5) + Q_3(l_2 - l_4 + l_5) = 0.$$

The proof follows from the property that the direction $\mathbf{L}l^T$ of the line l is incident to the plane \mathcal{Q} . Alternately, we can obtain the Theorem by introducing first, directional correspondence.

Definition.

Let $P := (P_0, P_1, P_2, -(P_0 + P_1 + P_2))$ be an ideal point. Let

$m := [m_0, m_1, m_2, m_3, m_4, m_5]$ be an ideal line. These point and line can also be determined by 3 well chosen coordinates. The coordinates of points are placed between double parenthesis and that of lines, between double brackets, while the point P as viewed as a point in the plane is denoted (P) and the line as $[m]$.

One of the good choices is $[[m_3, -m_1, m_0]]$, indeed, in the ideal plane, $m_0 e_0 + m_1 e_1 + m_2 e_2$ is the dual of $m_0 e_1 \vee e_2 + m_1 e_2 \vee e_0 + m_2 e_0 \vee e_1$, while the 3 chosen components give $m_3 e_1 \vee e_2 - m_1 e_0 \vee e_2 + m_0 e_0 \vee e_1$. The other components are $m_2 = -m_0 - m_1$, $m_4 = m_3 - m_0$, $m_5 = m_1 + m_3$.

We have $P^T = \mathbf{U} (P)^T$ and $[m]^T = \mathbf{V} m^T$, with

$$\mathbf{U} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -1 & -1 \end{pmatrix} \text{ and } \mathbf{V} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The correspondence which associates to $P = (P_0, P_1, P_2, P_3)$ in the 3 dimensional space the point $(P) = (P_0, P_1, P_2)$ in the 2 dimensional plane \mathcal{I} , and which associates to the line $m = [m_0, m_1, m_2, m_3, m_4, m_5]$, in the 3 dimensional space the line $[m] = [[m_3, -m_1, m_0]]$, in the 2 dimensional plane \mathcal{I} , is called the directional correspondence.

Theorem.

The directional correspondence is a homomorphism from the 3 dimensional space onto the ideal plane.

Theorem.

$$\mathbf{V} \mathbf{P} = \mathbf{U}^T.$$

Theorem.

If P and m are in the ideal plane, P is on m , iff (P) is on $[m]$, iff

$$(P) \cdot (m) = ((P_0, P_1, P_2)) \cdot [[m_3, -m_1, m_0]] = P_0m_3 - P_1m_1 + P_2m_0 = 0.$$

Alternate Proof of

6.1.1.

For instance, to the point I_l and line i_Q of Theorem 6.1.1, correspond, the point (I_l) and the line $[i_Q]$ in \mathcal{I} .

$$(I_l) = ((l_0 + l_1 + l_2, -l_0 + l_3 - l_4, -l_1 - l_3 + l_5)),$$

$$[i_Q] = [[Q_0 - Q_3, Q_1 - Q_3, Q_2 - Q_3]],$$

Q is parallel to l iff

$$-(l_0 + l_1 + l_2)(Q_0 - Q_3) + (-l_0 + l_3 - l_4)(Q_3 - Q_1) - (-l_1 - l_3 + l_5)(Q_2 - Q_3) = 0$$

which is 6.1.1.0.

Theorem.

The mid-point of two points $A = (a_0, a_1, a_2, a_3)$ and $B = (b_0, b_1, b_2, b_3)$ is

$$(b_0 + b_1 + b_2 + b_3)A + (a_0 + a_1 + a_2 + a_3)B.$$

Notation.

The mid-point of A and B is denoted by $A + B$.

Exercise.

Generalize the construction of the polar p of a point P with respect to a triangle to that of the polar P of a point P with respect to a tetrahedron and prove that if $P = (p_0, p_1, p_2, p_3)$ then $\mathcal{P} = \{\mathcal{P}_1\mathcal{P}_2\mathcal{P}_3, \mathcal{P}_2\mathcal{P}_3\mathcal{P}_0, \mathcal{P}_3\mathcal{P}_0\mathcal{P}_1, \mathcal{P}_0\mathcal{P}_1\mathcal{P}_2\}$.

6.2 Polar Geometry in 3 Dimensions.

6.2.0 Introduction.

To define a polar geometry in 3 dimensions, I will start with an affine Geometry in 3 dimensions and a preferred non degenerate quadric θ which is not tangent to the ideal plane \mathcal{I} . Using the ideal plane and the preferred quadric we can define orthogonality, spheres, centers, equality of pairs of points and lines,

The preferred quadric is represented by a symmetric 4 by 4 matrix \mathbf{F} , which associates to a 4-vector representing a point (pole), a 4-vector representing a plane (polar). Its adjoint \mathbf{G} gives the correspondance from polar to pole. From \mathbf{F} , we can derive a 6 by 6 matrix \mathbf{H} which gives the correspondance between a line and its polar. From \mathbf{F} we can also derive a polarity in the ideal plane represented by a 3 by 3 matrix \mathbf{J}_3 , giving the correspondance from pole to polar and its adjoint \mathbf{K}_3 , giving the correspondance from polar to pole from which we can derive perpendicularity between a line and a plane, the direction of the line giving the pole and the direction of the plane giving the polar. The 6 by 6 matrix \mathbf{J} , derived from \mathbf{J}_3 , allows

for a direct check of the orthogonality of 2 lines and the 4 by 4 matrix \mathbf{K} , derived from \mathbf{K}_3 , allows for a direct check of the orthogonality of 2 planes.

6.2.1 The fundamental quadric, poles and polars.

Introduction.

The properties of pole and polar are properties in Pappian Geometry. They are easily generalized by using a 4 dimension collinearity which transforms the fundamental quadric into an arbitrary quadric or by choosing a coordinate system with the four base points on the quadric.

Definition.

The preferred quadric is called the fundamental quadric. There is no restriction in choosing the fundamental quadric θ as follows, because it simply assumes that the quadric passes through the base points $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$. Let

$$0. \mathbf{F} := \begin{pmatrix} 0 & n_0 & n_1 & n_2 \\ n_0 & 0 & n_3 & n_4 \\ n_1 & n_3 & 0 & n_5 \\ n_2 & n_4 & n_5 & 0 \end{pmatrix},$$

$$1. \Theta := (X_0, X_1, X_2, X_3)\mathbf{F}(X_0, X_1, X_2, X_3)^T \\ = n_0X_0X_1 + n_1X_0X_2 + n_2X_0X_3 + n_3X_1X_2 + n_4X_3X_1 + n_5X_2X_3 = 0.$$

The condition of non degeneracy and non tangency are

$$2. d := \det(\mathbf{F}) = \\ n_0^2n_5^2 + n_1^2n_4^2 + n_2^2n_3^2 - 2(n_0n_1n_4n_5 + n_1n_2n_3n_4 + n_2n_0n_3n_5) \neq 0, \\ 3. t := n_3n_4n_5 + n_1n_2n_5 + n_0n_2n_4 + n_0n_1n_3 + 2n_0n_5(n_0 + n_5) \\ + 2n_1n_4(n_1 + n_4) + 2n_2n_3(n_2 + n_3) - (n_0n_5 + n_1n_4 + n_2n_3)n \neq 0, \\ \text{where} \\ n := n_0 + n_1 + n_2 + n_3 + n_4 + n_5.$$

The condition $t \neq 0$ will be verified in 6.2.1.

Definition.

In polar geometry, the points in the ideal plane which are not on the quadric are called the ideal points, all lines in the ideal plane which are not tangent to the quadric are the ideal lines.

Definition.

The points in the ideal plane and the quadric are the isotropic points. The lines in the ideal plane tangent to the quadric are the isotropic lines.

If the isotropic points are real, the polar geometry is said to be hyperbolic, if there are no

real isotropic points, it is said to be elliptic, if there is exactly one isotropic point, the quadric being tangent to the plane, the geometry is said to be parabolic.

Again as for the involutive geometry, I will not study the parabolic case and will study together the elliptic and hyperbolic case.

Definition.

The polar of the point $P = (P_0, P_1, P_2, P_3)$, is the plane

$$\mathcal{Q}^T := \mathbf{F}P^T = \{n_0P_1 + n_1P_2 + n_2P_3, n_0P_0 + n_3P_2 + n_4P_3, \\ n_1P_0 + n_3P_1 + n_5P_3, n_2P_0 + n_4P_1 + n_5P_2\}.$$

P is called the pole of the plane \mathcal{Q} .

Theorem.

$$P^T = \mathbf{G}\mathcal{Q}^T$$

where \mathbf{G} is the adjoint of \mathbf{F} :

$$\mathbf{G} = \begin{pmatrix} 2n_3n_4n_5 & n_5(n_0n_5 - n_2n_3 - n_1n_4) & n_4(n_1n_4 - n_0n_5 - n_2n_3) & n_3(n_2n_3 - n_1n_4 - n_0n_5) \\ n_5(n_0n_5 - n_2n_3 - n_1n_4) & 2n_1n_2n_5 & n_2(n_2n_3 - n_1n_4 - n_0n_5) & n_1(n_1n_4 - n_0n_5 - n_2n_3) \\ n_4(n_1n_4 - n_0n_5 - n_2n_3) & n_2(n_2n_3 - n_1n_4 - n_0n_5) & 2n_0n_2n_4 & n_0(n_0n_5 - n_2n_3 - n_1n_4) \\ n_3(n_2n_3 - n_1n_4 - n_0n_5) & n_1(n_1n_4 - n_0n_5 - n_2n_3) & n_0(n_0n_5 - n_2n_3 - n_1n_4) & 2n_0n_1n_3 \end{pmatrix}.$$

Theorem.

\mathcal{I} is tangent to the fundamental quadric iff

$$(1, 1, 1, 1)\mathbf{G}\{1, 1, 1, 1\}^T = 0$$

or

$$t = 0.$$

where t is defined in 6.2.1.

$2t$ is simply the sum of all the elements of \mathbf{G} .

Theorem.

If Q is on the polar \mathcal{P} of P then its polar \mathcal{Q} is incident to P .

The proof is left as an exercise. The theorem justifies the following definition:

Definition.

A line m is a polar of a line l iff it is the line common to all the polars of the points of l .

Theorem.

Let $\mathbf{H} :=$

$$\begin{pmatrix} n_1n_4 - n_2n_3 & n_5n_1 & -n_5n_2 & n_5n_3 & n_5n_4 & -n_5^2 \\ -n_4n_0 & n_2n_3 - n_0n_5 & n_4n_2 & n_4n_3 & -n_4^2 & n_4n_5 \\ n_3n_0 & -n_3n_1 & n_0n_5 - n_1n_4 & -n_3^2 & n_3n_4 & n_3n_5 \\ -n_2n_0 & -n_2n_1 & -n_2^2 & n_0n_5 - n_1n_4 & n_2n_4 & -n_2n_5 \\ -n_1n_0 & -n_1^2 & -n_1n_2 & -n_1n_3 & n_2n_3 - n_0n_5 & n_1n_5 \\ -n_0^2 & -n_0n_1 & -n_0n_2 & n_0n_3 & -n_0n_4 & n_1n_4 - n_2n_3 \end{pmatrix},$$

then the polar m of l is given by

$$m^T = \mathbf{H}l^T.$$

Moreover

$$\mathbf{H}\mathbf{H} = d\mathbf{I},$$

where \mathbf{I} is the identity matrix and d is the determinant of \mathbf{F} given in 6.2.1.3.

The proof is left as an exercise. As a hint, consider 2 points P and Q on $l = P \vee Q$ and their polar $\mathbf{F}P$ and $\mathbf{F}Q$.

Definition.

The center of a quadric is the pole of \mathcal{I} ,

Example.

The pole of $\{1, 0, 0, 0\}$ is

$$(2n_3n_4n_5, n_5(n_0n_5 - n_2n_3 - n_1n_4), n_4(n_1n_4 - n_0n_5 - n_2n_3), n_3(n_2n_3 - n_1n_4 - n_0n_5)).$$

The center of the fundamental quadric is

$$\begin{aligned} & (2n_3n_4n_5 + n_0n_5(n_5 - n_3 - n_4) + n_1n_4(n_4 - n_5 - n_3) + n_2n_3(n_3 - n_4 - n_5), \\ & 2n_5n_1n_2 + n_3n_2(n_2 - n_5 - n_1) + n_4n_1(n_1 - n_2 - n_5) + n_0n_5(n_5 - n_1 - n_2), \\ & 2n_2n_4n_0 + n_5n_0(n_0 - n_2 - n_4) + n_1n_4(n_4 - n_0 - n_2) + n_3n_2(n_2 - n_4 - n_0), \\ & 2n_0n_1n_3 + n_2n_3(n_3 - n_0 - n_1) + n_4n_1(n_1 - n_3 - n_0) + n_5n_0(n_0 - n_1 - n_3). \end{aligned}$$

6.2.2 Orthogonality in space and the ideal polarity.

Introduction.

Preferring both an ideal plane and a fundamental quadric allows us to define orthogonality of lines and planes with lines and planes. After defining the polarity in the ideal plane, induced by the fundamental quadric, we use it to derive the 3 conditions which express the orthogonality of lines and planes and the condition which express the orthogonality of 2 lines or of 2 planes.

Definition.

A line is orthogonal to a plane iff the polar of its ideal point is incident to the ideal line of the plane. A line is orthogonal to a line iff the polar of its ideal point is incident to the ideal

point of the other line. A plane is orthogonal to a plane iff the ideal line of one is the polar of the ideal line of the other.

Definition.

The ideal polarity is the polarity induced in the ideal plane \mathcal{I} by the polarity defined by the quadric θ .

Notation.

It is sometimes convenient to use an other notation for the elements of the fundamental quadric.

$n_{ij} = n_{ji}$ is the coefficient of $X_i X_j$ in the equation of the fundamental quadric, more specifically,

$n_{01} := n_0$, $n_{02} := n_1$, $n_{03} := n_2$, $n_{12} := n_3$, $n_{31} := n_4$ and $n_{23} := n_5$.

The elements of the matrices \mathbf{K}_3 and of \mathbf{K} are more easily expressed in terms of i_{ii} and i_{ij} , using $ijkl$ for permutation of 0123,

$$\begin{aligned} i_{ii} &= -(n_{kl}^2 + n_{lj}^2 + n_{jk}^2 + 2(n_{lj}n_{kl} + n_{kl}n_{jk} + n_{jk}n_{lj})), \\ i_{ij} &= (n_{ik} - n_{il})(n_{jk} - n_{jl}) + n_{kl}(3n_{ij} + 2n_{kl} - n), \end{aligned}$$

with $n := n_{01} + n_{02} + n_{02} + n_{12} + n_{31} + n_{23}$.

For instance,

$$\begin{aligned} i_{00} &= -(n_{12}^2 + n_{31}^2 + n_{23}^2 + 2(n_{31}n_{23} + n_{23}n_{12} + n_{12}n_{31}), \\ i_{01} &= (n_{02} - n_{03})(n_{12} - n_{13}) + n_{23}(3n_{01} + 2n_{23} - n), \end{aligned}$$

Theorem.

The point to line ideal polarity is given by the matrix

$$\mathbf{J}_3 = \mathbf{U}^T \mathbf{F} \mathbf{U} = \begin{pmatrix} -2n_2 & n_0 - n_2 - n_4 & n_1 - n_2 - n_5 \\ n_0 - n_2 - n_4 & -2n_4 & n_3 - n_4 - n_5 \\ n_1 - n_2 - n_5 & n_3 - n_4 - n_5 & -2n_5 \end{pmatrix}.$$

The adjoint matrix \mathbf{K}_3 gives the line to point ideal polarity.

$$\mathbf{K}_3 = \begin{pmatrix} i_{00} & i_{01} & i_{02} \\ i_{01} & i_{11} & i_{12} \\ i_{02} & i_{12} & i_{22} \end{pmatrix}.$$

Indeed given a point (P) in \mathcal{I} , $\mathbf{U}(P)$ gives the coordinates of P in space, multiplication to the left by \mathbf{F} determines the polar plane \mathcal{P} . $\mathbf{P}\mathcal{P}$ gives the direction $i_{\mathcal{P}}$ of \mathcal{P} , multiplication to the left by \mathbf{V} gives the 3 coordinates $(i_{\mathcal{P}})$ of the direction in the ideal plane, using 6.1.1 gives \mathbf{J}_3 .

For the adjoint matrix,

$$\begin{aligned} i_{00} &= 4n_4n_5 - (n_3 - n_4 - n_5)^2 = -(n_3^2 + n_4^2 + n_5^2) + 2(n_4n_5 + n_5n_3 + n_3n_4) \\ &= -(n_{12}^2 + n_{31}^2 + n_{23}^2 + 2(n_{31}n_{23} + n_{23}n_{12} + n_{12}n_{31})). \\ i_{01} &= (n_3 - n_4 - n_5)(n_1 - n_2 - n_5) + 2n_5(n_0 - n_2 - n_4) \\ &= (n_{12} - n_{13} - n_{23})(n_{02} - n_{03} - n_{23}) + 2n_{23}(n_{01} - n_{03} - n_{13}) \\ &= (n_{02} - n_{03})(n_{12} - n_{13}) + n_{23}(3n_{01} + 2n_{23} - n). \end{aligned}$$

Theorem.

$$0. \det(\mathbf{J}_3) = 2t.$$

1. The ideal polarity is not degenerate.

Theorem.

If P is on the conic associated with the idea polarity then P is on the fundamental quadric.

Theorem.

Let

$$l_a := l_0 + l_1 + l_2, l_b := -l_0 - l_4 + l_3, l_c := -l_1 - l_3 + l_5, l_d := -l_2 - l_5 + l_4, \\ i_{\mathcal{P}} := \mathcal{P} \wedge \mathcal{I}, i_{\mathcal{Q}} := \mathcal{Q} \wedge \mathcal{I}, I_l := l \wedge \mathcal{I}, I_m := m \wedge \mathcal{I}. \quad \text{then } [l_a, l_b, l_c, l_d] = I_l = \mathbf{L}l.$$

0. A line $l = [l_0, l_1, l_2, l_3, l_4, l_5]$ is orthogonal to the plane

$$\mathcal{P} = \{P_0, P_1, P_2, P_3\} \text{ iff}$$

0. $[i_{\mathcal{P}}] = \mathbf{J}_3(I_l)$, or if for some $k \neq 0$,

$$1. \begin{aligned} k(P_3 - P_0) &= l_a n_2 + l_b(n_0 - n_4) + l_c(n_1 - n_5) + l_d n_2, \\ k(P_3 - P_1) &= l_a(n_2 - n_0) + l_b(-n_4) + l_c(n_3 - n_5) + l_d n_4, \\ k(P_3 - P_2) &= l_a(n_2 - n_1) + l_b(n_3 - n_4) + l_c(-n_5) + l_d n_5. \end{aligned}$$

Other relations can be derived from these, e.g.

$$2. \begin{aligned} k(P_1 - P_0) &= l_a n_0 + l_b n_0 + l_c(n_1 - n_3) + l_d(n_2 - n_4), \\ k(P_2 - P_0) &= l_a n_1 + l_b(n_0 - n_3) + l_c n_1 + l_d(n_2 - n_5), \end{aligned}$$

1. A line $l = [l_0, l_1, l_2, l_3, l_4, l_5]$ is orthogonal to the line

$$m = [m_0, m_1, m_2, m_3, m_4, m_5] \text{ iff}$$

0. $(I_m)\mathbf{J}_3(I_l) = 0$,

or

$$1. -((l_0 + l_1 + l_2)(m_0 + m_4 - m_3) + (m_0 + m_1 + m_2)(l_0 + l_4 - l_3))n_0 \\ - ((l_0 + l_1 + l_2)(m_1 + m_3 - m_5) + (m_0 + m_1 + m_2)(l_1 + l_3 - l_5))n_1 \\ - ((l_0 + l_1 + l_2)(m_2 + m_5 - m_4) + (m_0 + m_1 + m_2)(l_2 + l_5 - l_4))n_2 \\ + ((l_0 + l_4 - l_3)(m_1 + m_3 - m_5) + (m_0 + m_4 - m_3)(l_1 + l_3 - l_5))n_3 \\ + ((l_0 + l_4 - l_3)(m_2 + m_5 - m_4) + (m_0 + m_4 - m_3)(l_2 + l_5 - l_4))n_4 \\ + ((l_1 + l_3 - l_5)(m_2 + m_5 - m_4) + (m_1 + m_3 - m_5)(l_2 + l_5 - l_4))n_5 = 0.$$

or

$$m\mathbf{J}l = 0, \text{ with } \mathbf{J} =$$

$$\begin{pmatrix} -2n_0 & -n_0 - n_1 + n_3 & -n_0 - n_2 + n_4 & n_0 - n_1 + n_3 & -n_0 + n_2 - n_4 & n_1 - n_2 - n_3 + n_4 \\ -n_0 - n_1 + n_3 & -2n_1 & -n_1 - n_2 + n_5 & n_0 - n_1 - n_3 & -n_0 + n_2 + n_3 - n_5 & n_1 - n_2 + n_5 \\ -n_0 - n_2 + n_4 & -n_1 - n_2 + n_5 & -2n_2 & n_0 - n_1 - n_4 + n_5 & -n_0 + n_2 + n_4 & n_1 - n_2 - n_5 \\ n_0 - n_1 + n_3 & n_0 - n_1 - n_3 & n_0 - n_1 - n_4 + n_5 & -2n_3 & n_3 + n_4 - n_5 & n_3 - n_4 + n_5 \\ -n_0 + n_2 - n_4 & -n_0 + n_2 + n_3 - n_5 & -n_0 + n_2 + n_4 & n_3 + n_4 - n_5 & -2n_4 & -n_3 + n_4 + n_5 \\ n_1 - n_2 - n_3 + n_4 & n_1 - n_2 + n_5 & n_1 - n_2 - n_5 & n_3 - n_4 + n_5 & -n_3 + n_4 + n_5 & -2n_5 \end{pmatrix}.$$

2. A plane $\mathcal{P} = \{P_0, P_1, P_2, P_3\}$ is orthogonal to the plane

$$\mathcal{Q} = \{Q_0, Q_1, Q_2, Q_3\} \text{ iff}$$

$$0. (i_{\mathcal{Q}})\mathbf{K}_3(i_{\mathcal{P}})^T = 0,$$

or

$$1. \mathcal{Q}\mathbf{K}\mathcal{P}^T = 0,$$

where \mathbf{K} is the symmetric matrix

$$\mathbf{K} = \begin{pmatrix} i_{00} & i_{01} & i_{02} & i_{03} \\ i_{10} & i_{11} & i_{12} & i_{13} \\ i_{20} & i_{21} & i_{22} & i_{23} \\ i_{30} & i_{31} & i_{32} & i_{33} \end{pmatrix}.$$

Example.

The pole of the line $\mathcal{I} \wedge A_0 = [[1, 0, 0]]$, is $((i_{00}, i_{01}, i_{02}))$, which gives $I_{Q_0} = (i_{00}, i_{01}, i_{02}, -(i_{00} + i_{01} + i_{02}))$, hence if $foot_0 := (A_0 \vee I_{Q_0}) \wedge \mathcal{A}_0$, then $foot_0 = (0, i_{01}, i_{02}, i_{03})$, with $i_{03} = -(i_{00} + i_{01} + i_{02}) = (n_0 - n_1 - n_3)(n_4 - n_3 - n_5) + 2n_3(n_2 - n_1 - n_5)$.

Definition.

The defining quadric and any other which has the the same ideal polarity is called a sphere.

Theorem.

All spheres degenerate or not are given by

$$\Phi := k_1 \Theta + k_2 \mathcal{I} \times \mathcal{R}.$$

with not both k_1 and k_2 equal to 0 and \mathcal{R} a plane, distinct from the ideal plane.

A sphere can be reduced to a point or be degenerate in the ideal plane and an other plane, when $k_1 = 0$.

Definition.

The plane \mathcal{R} of the preceding Theorem is called the radical plane of the 2 spheres Θ and Φ .

Exercise.

Give an example of a sphere which reduces to a single point.

Theorem.

Given 2 ordinary points A and B , on a sphere and the polar of the ideal point on $A \times B$ is incident to $A \times B$ at C , then C is independent of the sphere. C is called mid-point of (A, B) .

Exercise.

Generalize the construction of the polar p of a point P with respect to a conic to that of the polar \mathcal{P} of a point P with respect to a quadric.

Exercise.

Give a construction of the mid-point of 2 points.

6.2.3 The general tetrahedron.

Introduction.

The study of the geometry of the triangle can be generalized in 3 dimensions to the study of the general tetrahedron. A special case occurs very naturally, that of the orthogonal tetrahedron, studied in section 6.2.4.

Notation.

Let IV be the set $\{0, 1, 2, 3\}$ and VI be the set $\{0, 1, 2, 3, 4, 5\}$, let d be a function from the set $IV \times IV$ to the set VI defined by

$$d_{0,1} = 0, d_{0,2} = 1, d_{0,3} = 2,$$

$$d_{1,2} = 3, d_{3,1} = 4, d_{2,3} = 5,$$

$d_{i,i}$ is undefined, $d_{i,j} = d_{j,i}$. d^{-1} denotes the inverse function.

Similarly, let e be a function from the set $IV \times IV \times IV$ to the set VI defined by

$$e_{1,2,3} = 0, e_{2,3,0} = 1, e_{3,0,1} = 2, e_{0,1,2} = 3,$$

$e_{i,j,k}$ unchanged when we permute indices and $e_{i,j,k}$ undefined if 2 indices are equal. e^{-1} denotes its inverse.

Notation.

$a \times b$ indicates first that the lines a and b have a point P in common and second define P . The plane through the lines a and b is similarly denoted by $a\mathcal{X}b$. See 3.2.D.12. In this section, the indices i, j, k, l are in the set $\{0, 1, 2, 3\}$, the indices u, v are in the set $\{0, 1, 2, 3, 4, 5\}$. Unless indicated explicitly the indices i, j, k, l or u, v in a given statement are distinct.

$l_{i,j}$ or $l_{d_{i,j}}$ represent the same line, the second forms indicates explicitly the mapping used to map the 2 dimensional array into a 1 dimensional array.

The set $I_J := \{(0, 1), (0, 2), (0, 3), (1, 2), (3, 1), (2, 3)\}$.

The set $J_I := \{(1, 0), (2, 0), (3, 0), (2, 1), (1, 3), (3, 2)\}$.

The definitions only define the object $u(i, j)$, $(i, j) \in I_J$ and not that (i, j) is in the set I_J unless indicated explicitly.

If $(j, i) \in J_I$, then $u(i, j) = u(j, i)$.

If a definition is followed by $()$, this means that one of several definitions can be used, those not used are Theorems, for instance in D1.12. O_1 can be defined by $\text{facealtitude}_{0,1} \times \text{facealtitude}_{3,1}$, and $O_1 \vee \text{facealtitude}_{2,1} = 0$. A quadric is denoted by a greek letter, θ say, the point quadric is then denoted by Θ , the plane quadric by $|\Theta$.*

Comment.

In this section, I will only give the expression of one of the points in a set, the others are obtained as follows, if a point P_{nu} is defined symmetrically from A_1, A_2 and A_3 the point P_{nv} is obtained as follows,

$$\text{let } nu = n_{d_{i,j}} \text{ then } nv = n_{d_{i+1,j+1}}.$$

where the addition within the subscripts is done modulo 4.

In particular,

$n_0 = n_{0,1}$ becomes $n_{1,2} = n_3$,

$n_1 = n_{0,2}$ becomes $n_{1,3} = n_4$,

$n_2 = n_{0,3}$ becomes $n_{1,0} = n_0$,

$n_3 = n_{1,2}$ becomes $n_{2,3} = n_5$,

$n_4 = n_{3,1}$ becomes $n_{0,2} = n_1$,

$n_5 = n_{2,3}$ becomes $n_{3,0} = n_2$,

If a line l_u is defined non symmetrically in terms of A_0, A_1, A_2, A_3 then l_v is obtained by means of a permutation P of $\{0,1,2,3\}$.

If $l_0 = f(n_0, n_1, n_2, n_3, n_4, n_5)$, then

$l_1 = f(n_1, n_2, n_0, n_5, n_3, n_4)$, $l_2 = f(n_2, n_0, n_1, n_4, n_5, n_3)$.

$l_5 = f(n_5, n_1, n_3, n_2, n_4, n_0)$,

$l_4 = f(n_4, n_2, n_5, n_0, n_3, n_1)$, $l_3 = f(n_3, n_0, n_4, n_1, n_5, n_2)$.

Notation.

$\{A_i\}$ will denote the tetrahedron with vertices A_i . If we want to indicate explicitly not only the vertices A_i but also the edges a_u and the faces \mathcal{A}_j we will use the more elaborate notation $\{A_i, a_u, \mathcal{A}_j\}$.

Comment.

For the tetrahedron with vertices A_0, A_1, A_2, A_3 , the algebra will be done assuming these have the coordinates to be $(1,0,0,0)$, $(0,1,0,0)$, $(0,0,1,0)$, $(0,0,0,1)$, and that the barycentric point M has coordinates $(1,1,1,1)$.

Theorem.

If the coordinates of a point P are (m_0, m_1, m_2, m_3) , $m_0, m_1, m_2, m_3 \neq 0$, those of the plane \mathcal{P} , which is its polar with respect to the tetrahedron $\{A_i\}$ are $\{m_0^{-1}, m_1^{-1}, m_2^{-1}, m_3^{-1}\}$.

The Euclidean geometry will be defined starting with the ideal plane \mathcal{I} which is the polar of M with respect to the tetrahedron and starting from the quadric

$$\Theta : n_0 X_0 X_1 + n_1 X_0 X_2 + n_2 X_0 X_3 + n_3 X_1 X_2 + n_4 X_3 X_1 + n_5 X_2 X_3 = 0.$$

as one of the spheres. Preferring \mathcal{I} and Θ allows us to define parallelism and orthogonality.

Theorem.

Given

H0.0. A_0, A_1, A_2, A_3 ,

H0.1. M, \overline{M} ,

H0.2. Θ .

Let

D0.0. $a_{i,j} := A_i \vee A_j$,

D0.1. $\mathcal{A}_l := A_i \vee A_j \vee A_k$,

D0.2. $\mathcal{I} := \text{polar}(M)$ with respect to the tetrahedron,

D1.0. $C := \text{pole}(\mathcal{I})$,

D1.1. $\text{euler} := C \vee M$,

- D1.2. $AP_i := pole(\mathcal{A}_i)$,
- D1.3. $med_i := C \vee \mathcal{A}_i$,
- D1.4. $Imed_i := \mathcal{I} \wedge med_i$,
- D1.5. $alt_i := A_i \vee Imed_i$,
- D1.6. $Foot_i := \mathcal{A}_i \wedge alt_i$,
- D1.7. $ipa_{i,j} := Imed_i \vee Imed_j, (i, j) \in I_J$,
- D1.8. $Perp_{i,j} := ipa(i, j) \vee A_i, (i, j) \in I_J$,
 $Perp_{j,i} := ipa(i, j) \vee A_j, (j, i) \in J_I$,
- D1.9. $Facefoot_{i,j} := Perp_{i,j} \wedge a_{k,l}, (i, j) \in I_J \text{ or } J_I$,
- D1.10. $facealtitude_{i,j} := Facefoot_{i,j} \vee A_i, (i, j) \in I_J \text{ or } J_I$,
- D1.11. $O_i := facealtitude_{j,i} \rtimes facealtitude_{k,i}, i, j, k \text{ distinct}(*),$
- D1.12. $Mid_i := Foot_i + O_i$,
- D1.13. $mid_i := Mid_i \vee Imed_i$,
- D1.14. $H := mid_0 \rtimes mid_1, (*)$
- D1.15. $\eta := \text{quadric through } alt_i(*),$

then

- C1.0. $M = C + H$
- C1.1. $H \vee euler = 0.$
- C1.2. $Foot_{i,j} = Foot_{j,i}.$
- C1.3. $O_i \vee \eta = 0.$

The nomenclature or alternate definitions:

- A_i are the vertices,
- M is the barycenter,
- N0.0. a_u are the edges,
- N0.1. \mathcal{A}_i are the faces,
 The tetrahedron is $(A_i, a_u, \mathcal{A}_i)$,
- N0.2. \mathcal{I} is the ideal plane,
- N1.0. C is the center of the circumsphere,
- N1.1. $euler$ is the line of Euler,
- N1.2. AP_i is the pole of the face \mathcal{A}_i ,
- N1.3. med_i is the mediatrix of the face \mathcal{A}_i ,
- N1.4. $Imed_i$ is the ideal point on the mediatrix med_i ,
- N1.5. alt_i is the altitude corresponding to A_0 ,
- N1.6. $Foot_i$ is the foot of alt_i , corresponding to \mathcal{A}_i ,
- N1.7. $ipa_{i,j}$ is the direction of the planes perpendicular to $a_{k,l}$,
- N1.8. $Perp_{i,j}, (i, j) \in I_J$, is the plane perpendicular to $a_{k,l}$ through A_i ,
 $Perp_{j,i}, (j, i) \in J_I$, is the plane perpendicular to $a_{k,l}$ through A_j ,
- N1.9. $Facefoot_{i,j}, (i, j) \in I_J \text{ or } J_I$, is the face-foot in the face \mathcal{A}_j , on the edge opposite A_i , $A_i \vee Facefoot_{i,j}$ is perpendicular to $a_{k,l}$,
- N1.10. $facealtitude_{i,j}, (i, j) \in I_J \text{ or } J_I$, is the face-altitude in the face \mathcal{A}_j through the vertex A_i , perpendicular to $a_{k,l}$,
- N1.11. O_i is the orthocenter of \mathcal{A}_i ,
- N1.12. mid_i is the perpendicular to \mathcal{A}_i through M_i ,
- N1.13. H is the center of the hyperboloid η .
- N1.14. η is the hyperboloid of Neuberg.

Proof:

$$G0.0. \quad A_0 = (1, 0, 0, 0).$$

$$G0.1. \quad M = (1, 1, 1, 1).$$

$$G0.2. \quad \Theta : n_0X_0X_1 + n_1X_0X_2 + n_2X_0X_3 + n_3X_1X_2 + n_4X_3X_1 + n_5X_2X_3 = 0.$$

$$P0.0. \quad a_0 = [1, 0, 0, 0, 0, 0].$$

$$P0.1. \quad \mathcal{A}_0 = \{1, 0, 0, 0\}.$$

$$P0.2. \quad \mathcal{I} = \{1, 1, 1, 1\}.$$

$$P1.0. \quad C = ($$

$$2n_3n_4n_5 + n_0n_5(n_5 - n_3 - n_4) + n_1n_4(n_4 - n_5 - n_3) + n_2n_3(n_3 - n_4 - n_5),$$

$$2n_5n_1n_2 + n_3n_2(n_2 - n_5 - n_1) + n_4n_1(n_1 - n_2 - n_5) + n_0n_5(n_5 - n_1 - n_2),$$

$$2n_2n_4n_0 + n_5n_0(n_0 - n_2 - n_4) + n_1n_4(n_4 - n_0 - n_2) + n_3n_2(n_2 - n_4 - n_0),$$

$$2n_0n_1n_3 + n_2n_3(n_3 - n_0 - n_1) + n_4n_1(n_1 - n_3 - n_0) + n_5n_0(n_0 - n_1 - n_3)).$$

$$P1.1. \quad euler = [2n_5(n_3n_4 - n_1n_2) + (n_1n_4 - n_2n_3)(n_2 + n_4 - n_1 - n_3) + n_0n_5(n_1 + n_2 - n_3 - n_4),$$

$$2n_4(n_5n_3 - n_2n_0) + (n_2n_3 - n_0n_5)(n_0 + n_3 - n_2 - n_5) + n_1n_4(n_2 + n_0 - n_5 - n_3),$$

$$2n_3(n_4n_5 - n_0n_1) + (n_0n_5 - n_1n_4)(n_1 + n_5 - n_0 - n_4) + n_2n_3(n_0 + n_1 - n_4 - n_5),$$

$$2n_2(n_1n_5 - n_0n_4) + (n_0n_5 - n_1n_4)(n_4 + n_5 - n_0 - n_1) + n_2n_3(n_0 + n_4 - n_1 - n_5),$$

$$2n_1(n_0n_3 - n_2n_5) + (n_2n_3 - n_0n_5)(n_5 + n_3 - n_2 - n_0) + n_1n_4(n_2 + n_5 - n_0 - n_3),$$

$$2n_0(n_2n_4 - n_1n_3) + (n_1n_4 - n_2n_3)(n_3 + n_4 - n_1 - n_2) + n_5n_0(n_1 + n_3 - n_2 - n_4),$$

$$P1.2. \quad AP_0 = (2n_3n_4n_5, n_5(n_0n_5 - n_2n_3 - n_1n_4), n_4(n_1n_4 - n_0n_5 - n_2n_3),$$

$$n_3(n_2n_3 - n_1n_4 - n_0n_5)).$$

$$P1.3. \quad med_0 = [n_5(n_5 - n_3 - n_4), n_4(n_4 - n_5 - n_3), n_3(n_3 - n_4 - n_5),$$

$$n_4(n_1 - n_2) - n_5(n_0 - n_2), n_5(n_0 - n_1) - n_3(n_2 - n_1),$$

$$n_3(n_2 - n_0) - n_4(n_1 - n_0)].$$

$$P1.4. \quad Imed_0 = (n_3^2 + n_4^2 + n_5^2 - 2(n_4n_5 + n_5n_3 + n_3n_4),$$

$$-n_5(3n_0 + 2n_5 - n) - (n_1 - n_2)(n_3 - n_4),$$

$$-n_4(3n_1 + 2n_4 - n) - (n_2 - n_0)(n_5 - n_3),$$

$$-n_3(3n_2 + 2n_3 - n) - (n_0 - n_1)(n_4 - n_5)).$$

$$P1.5. \quad alt_0 = [n_5(3n_0 + 2n_5 - n) + (n_1 - n_2)(n_3 - n_4),$$

$$n_4(3n_1 + 2n_4 - n) + (n_2 - n_0)(n_5 - n_3),$$

$$n_3(3n_2 + 2n_3 - n) + (n_0 - n_1)(n_4 - n_5), 0, 0, 0].$$

$$P1.6. \quad Foot_0 = (0, n_5(3n_0 + 2n_5 - n) + (n_1 - n_2)(n_3 - n_4),$$

$$n_4(3n_1 + 2n_4 - n) + (n_2 - n_0)(n_5 - n_3),$$

$$n_3(3n_2 + 2n_3 - n) + (n_0 - n_1)(n_4 - n_5)],$$

$$P1.7. \quad ipa_0 = [2n_5, n_3 - n_4 - n_5, -n_3 + n_4 - n_5, -n_1 + n_2 + n_5, -n_1 + n_2 - n_5,$$

$$-n_1 + n_2 + n_3 - n_4].$$

$$P1.8. \quad Perp_{0,1} = \{0, -n_4 + n_3 + n_2 - n_1, -n_5 + n_2 - n_1, n_5 + n_2 - n_1\},$$

$$Perp_{1,0} = \{n_4 - n_3 - n_2 + n_1, 0, -n_5 + n_4 - n_3, n_5 + n_4 - n_3\}.$$

$$P1.9. \quad Facefoot_{0,1} = (0, 0, -n_1 + n_2 + n_5, n_1 - n_2 + n_5),$$

$$Facefoot_{1,0} = (0, 0, -n_3 + n_4 + n_5, n_3 - n_4 + n_5).$$

$$P1.10. \quad facealtitude_{0,1} = [0, -n_1 + n_2 + n_5, n_1 - n_2 + n_5, 0, 0, 0],$$

$$facealtitude_{1,0} = [0, 0, 0, n_3 - n_4 - n_5, n_3 - n_4 + n_5, 0].$$

$$P1.11. \quad O_0 = (0, n_5^2 - (n_3 - n_4)^2, n_4^2 - (n_5 - n_3)^2, n_3^2 - (n_4 - n_5)^2).$$

$$P1.12. \quad Mid_0 = (0, n_5(3n_0 + n_5 - n) + (n_3 - n_4)(n_1 - n_2 + n_3 - n_4),$$

$$n_4(3n_1 + n_4 - n) + (n_5 - n_3)(n_2 - n_0 + n_5 - n_3),$$

$$n_3(3n_2 + n_3 - n) + (n_4 - n_5)(n_0 - n_1 + n_4 - n_5)),$$

$$\begin{aligned}
P1.13. \quad mid_0 &= [n_5(3n_0 + n_5 - n) + (n_3 - n_4)(n_1 - n_2 + n_3 - n_4), \\
&\quad n_4(3n_1 + n_4 - n) + (n_5 - n_3)(n_2 - n_0 + n_5 - n_3), \\
&\quad n_3(3n_2 + n_3 - n) + (n_4 - n_5)(n_0 - n_1 + n_4 - n_5), \\
&\quad (n_0 - n_1 - n_4 + n_5)(n_5 + n_4 - n_3), \\
&\quad (n_2 - n_0 - n_5 + n_3)(n_3 + n_5 - n_4), (n_1 - n_2 - n_3 + n_4)(n_4 + n_3 + n_5)]. \\
P1.14. \quad H &= (n_3n_4n_5 + n_1n_2n_5 + n_2n_0n_4 + n_0n_1n_3 + n_0n_5(n_0 - n_1 - n_2) \\
&\quad + n_1n_4(n_1 - n_2 - n_0) + n_2n_3(n_2 - n_0 - n_1), \\
&\quad 12n_3n_4n_5 + n_1n_2n_5 + n_2n_0n_4 + n_0n_1n_3 + n_0n_5(n_0 - n_3 - n_4) \\
&\quad + n_1n_4(n_4 - n_0 - n_3) + n_2n_3(n_3 - n_4 - n_0), \\
&\quad 12n_3n_4n_5 + n_1n_2n_5 + n_2n_0n_4 + n_0n_1n_3 + n_0n_5(n_5 - n_1 - n_3) \\
&\quad + n_1n_4(n_1 - n_3 - n_5) + n_2n_3(n_3 - n_1 - n_5), \\
&\quad 12n_3n_4n_5 + n_1n_2n_5 + n_2n_0n_4 + n_0n_1n_3 + n_0n_5(n_5 - n_2 - n_4) \\
&\quad + n_1n_4(n_4 - n_5 - n_2) + n_2n_3(n_2 - n_5 - n_4)). \\
P1.15. \quad \eta : r_0X_0X_1 + r_1X_0X_2 + r_2X_0X_3 + r_3X_1X_2 + r_4X_3X_1 + r_5X_2X_3 &= 0. \\
r_0 &= (n_1 - n_2 - n_3 + n_4)(n_0(3n_5 + 2n_0 - n) + (n_1 - n_3)(n_2 - n_4), \\
r_1 &= (n_2 - n_0 - n_5 + n_3)(n_1(3n_4 + 2n_1 - n) + (n_2 - n_5)(n_0 - n_3), \\
r_2 &= (n_0 - n_1 - n_4 + n_5)(n_2(3n_3 + 2n_2 - n) + (n_0 - n_4)(n_1 - n_5), \\
r_3 &= (n_0 - n_4 - n_1 + n_5)(n_3(3n_2 + 2n_3 - n) + (n_0 - n_1)(n_4 - n_5), \\
r_4 &= (n_2 - n_5 - n_0 + n_3)(n_4(3n_1 + 2n_4 - n) + (n_2 - n_0)(n_5 - n_3), \\
r_5 &= (n_1 - n_3 - n_2 + n_4)(n_5(3n_0 + 2n_5 - n) + (n_1 - n_2)(n_3 - n_4).
\end{aligned}$$

Details for the computation of P.15 are given in 6.2.3.

Comment.

A simple derivation for some of the points in the faces follows from a direct application of the results on the geometry of the triangle. Indeed, the circumcircle in \mathcal{A}_0 is on the one hand

$$n_3 X_1X_2 + n_4 X_3X_1 + n_5 X_2X_3 = 0$$

and on the other hand

$$m_3(m_1 + m_2) X_1X_2 + m_2(m_3 + m_1) X_3X_1 + m_1(m_2 + m_3) X_2X_3 = 0,$$

assuming the coordinates of the orthocenter \mathcal{A}_0 to be $(0, m_1, m_2, m_3)$.

Comparing we get

$$m_1m_2 = n_4 + n_5 - n_3, \quad m_2m_3 = n_3 + n_4 - n_5, \quad m_3m_1 = n_5 + n_3 - n_4.$$

m_1, m_2, m_3 are proportional to $(m_1m_2)(m_3m_1), (m_1m_2)(m_2m_3), (m_2m_3)(m_3m_1)$, therefore using homogeneity

$$\begin{aligned}
m_1 &= n_5^2 - (n_3 - n_4)^2, \\
m_2 &= n_4^2 - (n_5 - n_3)^2, \\
m_3 &= n_3^2 - (n_4 - n_5)^2.
\end{aligned}$$

This can therefore be used to derive all the elements in the plane directly from Theorem 2.6. of Chapter 2. The following are useful,

$$\begin{aligned}
m_2 + m_3 &= n_5(n_3 + n_4 - n_5), \\
m_3 + m_1 &= n_4(n_5 + n_3 - n_4), \\
m_1 + m_2 &= n_3(n_4 + n_5 - n_3)
\end{aligned}$$

(The notation is only valid in \mathcal{A}_0 , to have a notation for all faces, m_5, m_4, m_3 should be replaced by m_{01}, m_{02}, m_{03} .)

For instance, to obtains $Foot_0$,

$ia_0 := |A_0|I = [0, 0, 0, 1, 1, 1] = [[1, 0, 0]],$
 $Pia_0 := pole(ia_0) \in \mathcal{I} = ((i_{00}, i_{01}, i_{02})) = (i_{00}, i_{01}, i_{02}, i_{03}),$
 with $i_{03} = -i_{00} - i_{01} - i_{02} = (n_0 - n_1 - n_3)(n_4 - n_3 - n_5) + 2n_3(n_2 - n_1 - n_5).$
 hence $Foot_0 := (A_0 \vee Pia_0)\mathcal{A}_0 = (0, i_{01}, i_{02}, i_{03}).$ Hence
 $Foot_{i,i} = 0,$
 $f_{I_j} := Foot_{i_j} = Foot_{j_i} = (n_{i,k} - n_{i,l})(n_{j,k} - n_{j,l}) + n_{k,l}(3n_{i,j} + 2n_{k,l} - n)$
 for $i \neq j$, and i, j, k, l a permutation of $0, 1, 2, 3.$
 Hence the Theorem as well as C1.3.
 Similarly the center of the circumcircle $\in \mathcal{A}_0$ is
 $(0, n_5(n_3 + n_4 - n_5), n_4(n_5 + n_3 - n_4), n_3(n_4 + n_5 - n_3)).$

Theorem.

Let $r_{i,j}$ be the coordinate of $X_i X_j$ in η .

Let the coordinates of the feet $Foot_0, Foot_1, Foot_2, Foot_3$ be $(0, f_{01}, f_{02}, f_{03}), (f_{10}, 0, f_{12}, f_{13}), (f_{20}, f_{21}, 0, f_{23}), (f_{30}, f_{31}, f_{32}, 0),$
 then

$$r_{i,j} = f_{k,l}(f_{i,k}f_{j,l} - f_{i,l}f_{j,k}), \text{ where } i, j, k, l \text{ is an even permutation of } 0, 1, 2, 3.$$

Proof: Let the inverse f_{I_i} of f_{I_j} modulo p be denoted $g_{I_j}.$

If all $f_{ij} \neq 0$, expressing the fact that the quadric contains the altitudes gives the equations

$$\begin{array}{ll}
 (0) & f_{01}r_0 + f_{02}r_1 + f_{03}r_2 = 0, & (1) & g_{01}r_5 + g_{02}r_4 + g_{03}r_3 = 0, \\
 (2) & f_{10}r_0 + f_{12}r_3 + f_{13}r_4 = 0, & (3) & g_{10}r_5 + g_{12}r_2 + g_{13}r_1 = 0, \\
 (4) & f_{20}r_1 + f_{21}r_3 + f_{23}r_5 = 0, & (5) & g_{20}r_4 + g_{21}r_2 + g_{23}r_0 = 0, \\
 (6) & f_{30}r_2 + f_{31}r_4 + f_{32}r_5 = 0, & (7) & g_{30}r_3 + g_{31}r_1 + g_{32}r_0 = 0.
 \end{array}$$

Equations (0) and (7) are obtained by substituting in the equation of the quadric, X_i by $kA_i + Foot_i,$

g_{30}, g_{31}, g_{32} are proportional to $f_{01}f_{02}, f_{03}f_{01}, f_{02}f_{03},$ and therefore to $f_{03}^{-1}, f_{02}^{-1}, f_{01}^{-1}.$

We solve (0) with respect to r_0 , and (3) with respect to r_5 , in terms of r_1 and r_2 , (5) gives r_4 , substitution in (6) gives an homogeneous equation in terms of r_1 and r_2 only, hence after division by $f_{01}f_{03} + f_{02}f_{13}$

$$r_{0,2} = r_1 = f_{13}(f_{03}f_{21} - f_{01}f_{23}), r_{0,3} = r_2 = -f_{12}(f_{02}f_{31} - f_{01}f_{32}).$$

equations (0) give r_0 , (5) gives r_4 , (7) gives r_3 and (1) gives r_5 . Hence

$$\begin{aligned}
 r_{0,1} &= r_0 = -f_{23}(f_{03}f_{12} - f_{02}f_{13}), \\
 r_{1,2} &= r_3 = f_{03}(f_{10}f_{23} - f_{13}f_{20}), \\
 r_{3,1} &= r_4 = f_{02}(f_{30}f_{12} - f_{32}f_{10}), \\
 r_{2,3} &= r_5 = f_{01}(f_{20}f_{31} - f_{21}f_{30}),
 \end{aligned}$$

equations (2) and (4) can be used as a check. Summarizing the results gives the Theorem. Simplifying by a common factor, we obtain P1.15.

Theorem.

Let

$$D2.0. \quad Ia_u := a_u \wedge \mathcal{I},$$

$$D2.1. \quad \mathcal{P}olar a_u := polar(Ia_u),$$

then

C2.0. $ipa_u \wedge \mathcal{Polar}_{5-u} = 0$.

Nomenclature:

N2.0. Ia_u are the ideal points on the edges a_u ,

N2.1. $polar_{a_u}$ is the equatorial plane perpendicular to a_u .

Proof.

P2.0. $Ia_0 = (1, -1, 0, 0)$.

P2.1. $\mathcal{Polar}_{a_0} = \{-n_0, n_0, n_1 - n_3, n_2 - n_4\}$.

6.2.4 The orthogonal tetrahedron.

Definition.

A tetrahedron is orthogonal iff the 3 pairs of opposite sides are perpendicular.

Lemma.

$a_0 \cdot a_5 = 0$ iff $n_1 + n_4 = n_2 + n_3$,

$a_0 \cdot a_1 = 0$ iff $n_3 = n_0 + n_1$,

$a_1 \cdot a_2 = 0$ iff $n_5 = n_1 + n_2$,

$a_2 \cdot a_0 = 0$ iff $n_4 = n_2 + n_0$.

The first condition expresses the orthogonality of opposite sides, the other conditions the orthogonality of adjacent sides.

Theorem.

The tetrahedron is orthogonal iff the parameters of the circumsphere satisfy

$$n_0 + n_5 = n_1 + n_4 = n_2 + n_3.$$

Proof. The perpendicularity of $A_0 \vee A_1$ and $A_2 \vee A_3$ implies, because of 6.2.2.1, with $l_j = m_j = 0$, except for $l_0 = m_5 = 1$,

$$n_1 - n_3 = n_2 - n_4 \text{ or } n_1 + n_4 = n_2 + n_3,$$

Similarly that of $A_0 \vee A_2$ and $A_1 \vee A_3$ implies

$$n_0 + n_5 = n_2 + n_3.$$

Theorem.

Given an orthogonal tetrahedron whose adjacent sides are not orthogonal, let

$$\begin{aligned} 0. \quad m_0 &= (n_0 + n_1 - n_3)^{-1}, \quad m_1 = (n_3 + n_4 - n_5)^{-1}, \\ m_2 &= (n_5 + n_1 - n_2)^{-1}, \quad m_3 = (n_2 + n_4 - n_0)^{-1}, \end{aligned}$$

then

$$\begin{aligned} 1. \quad n_0 &= (m_0 + m_1)m_2m_3, \quad n_1 = (m_0 + m_2)m_3m_1, \quad n_2 = (m_0 + m_3)m_1m_2, \\ n_3 &= (m_1 + m_2)m_0m_3, \quad n_4 = (m_3 + m_1)m_0m_2, \quad n_5 = (m_2 + m_3)m_0m_1. \end{aligned}$$

Proof: The non orthogonality of adjacent sides implies that the m_j are well defined. We obtain, because of the orthogonality of opposite sides,

$$m_0^{-1} + m_1^{-1} = 2n_0, \quad m_2^{-1} + m_3^{-1} = 2n_1, \quad m_1^{-1} + m_2^{-1} = 2n_3,$$

we also obtain

$$\begin{aligned} m_0^{-1} + m_3^{-1} &= n_1 - n_3 + n_2 + n_4 = 2n_2, \\ m_1^{-1} + m_3^{-1} &= n_3 - n_1 + n_2 + n_4 = 2n_4, \\ m_2^{-1} + m_3^{-1} &= n_1 + n_2 + n_3 + n_4 - 2n_0 = 2n_5. \end{aligned}$$

If we multiply by $\frac{1}{2}m_0m_1m_2m_3$ we get 1.

Comment.

The indices obey the following rules.

Let $n_{i,j}$ be the coefficient of X_iX_j ,

we have $n_{0,1} = n_0$, $n_{0,2} = n_1$, $n_{0,3} = n_2$, $n_{1,2} = n_3$, $n_{1,3} = n_4$, $n_{2,3} = n_5$.

The orthogonality takes the form,

$$n_{0,1} + n_{2,3} = n_{0,2} + n_{1,3} = n_{0,3} + n_{1,2}.$$

m_i is the inverse of $n_{i,j} + n_{i,k} - n_{j,k}$, where i, j, k are distinct.

For instance, if l is distinct from i, j, k , m_i is also the inverse of $n_{i,j} + n_{i,l} - n_{j,l}$.

Definition.

A orthogonal tetrahedron is called a special orthogonal tetrahedron at A_i if 2 adjacent sides through A_i are also orthogonal.

Theorem.

If $A_0 \vee A_1$ is orthogonal to $A_0 \vee A_2$ and the tetrahedron is orthogonal then these lines are orthogonal to $A_0 \vee A_3$ and

$$n_0 + n_1 - n_3 = n_2 + n_0 - n_4 = n_1 + n_2 - n_5 = 0.$$

Vice versa, if $n_0 + n_1 - n_3 = 0$ and the tetrahedron is orthogonal, then it is special at A_0 .

Exercise.

Discuss the special cases

$$0. \quad n_0 + n_1 - n_3 = 0, \quad n_3 + n_4 - n_5 \neq 0 \dots$$

$$1. \quad n_0 + n_1 - n_3 = 0, \quad n_3 + n_4 - n_5 = 0$$

$$2. \quad n_0 = 0.$$

Theorem.

The coordinates of the points lines and planes defined in 6.2.3 are

$$G0.0. \quad A_0 = (1, 0, 0, 0),$$

$$G0.1. \quad M = (1, 1, 1, 1),$$

$$\begin{aligned} G0.2. \quad \Theta : & (m_0 + m_1)m_2m_3X_0X_1 + (m_0 + m_2)m_1m_3X_0X_2 + (m_0 + m_3)m_1m_2X_0X_3 \\ & + (m_1 + m_2)m_0m_3X_1X_2 + (m_3 + m_1)m_0m_2X_3X_1 + (m_2 + m_3)m_0m_1X_2X_3 = 0. \end{aligned}$$

$$P0.0. \quad a_0 = a_{0,1} = [1, 0, 0, 0, 0, 0],$$

$$P0.1. \quad \mathcal{A}_0 = \{1, 0, 0, 0\},$$

$$P0.2. \quad \mathcal{I} = \{1, 1, 1, 1\},$$

$$P1.0. \quad C = (-m_0 + m_1 + m_2 + m_3, m_0 - m_1 + m_2 + m_3, m_0 + m_1 - m_2 + m_3, \\ m_0 + m_1 + m_2 - m_3),$$

$$P1.1. \quad euler = [m_0 - m_1, m_0 - m_2, m_0 - m_3, m_1 - m_2, m_3 - m_1, m_2 - m_3],$$

$$P1.2. \quad AP_0 = (m_0(m_1 + m_2)(m_3 + m_1)(m_2 + m_3), -m_1(m_2 + m_3)(m_0m_1 + m_2m_3), \\ -m_2(m_3 + m_1)(m_0m_2 + m_3m_1), -m_3(m_1 + m_2)(m_0m_3 + m_1m_2)),$$

$$P1.3. \quad med_0 = [m_2 + m_3, m_3 + m_1, m_1 + m_2, m_2 - m_1, m_1 - m_3, m_3 - m_2],$$

$$P1.4. \quad Imed_0 = (-(m_1 + m_2 + m_3), m_1, m_2, m_3),$$

$$P1.5. \quad alt_0 = [m_1, m_2, m_3, 0, 0, 0],$$

$$P1.6. \quad Foot_0 = (0, m_1, m_2, m_3),$$

$$P1.7. \quad ipa_{0,1} = [m_2 + m_3, -m_2, -m_3, m_2, -m_3, 0]$$

$$P1.8. \quad \mathcal{P}erp_{0,1} = \mathcal{P}erp_{1,0} = \{0, 0, -m_3, m_2\},$$

$$P1.9. \quad Facefoot_{0,1} = Facefoot_{1,0} = (m_0, m_1, 0, 0),$$

$$P1.10. \quad facealtitude_{0,1} = [0, m_2, m_3, 0, 0, 0], \quad facealtitude_{1,0} = [0, 0, m_0, 0, m_1, 0],$$

$$P1.11. \quad O_0 = (0, m_1, m_2, m_3),$$

$$P1.12. \quad Mid_0 = (0, m_1, m_2, m_3),$$

$$P1.13. \quad mid_0 = altitude_0,$$

$$P1.14. \quad H = (m_0, m_1, m_2, m_3),$$

$$P1.15. \quad \text{Hyperboloid :}$$

$$m_2m_3 X_0X_1 - m_1m_3 X_0X_2 - m_0m_2 X_1X_3 + m_0m_1 X_2X_3 = 0$$

or

$$m_2m_3 X_0X_1 - m_1m_2 X_0X_3 - m_0m_3 X_1X_2 + m_0m_1 X_2X_3 = 0.$$

Exercise.

Construct a quadric generalizing the conic of Brianchon-Poncelet, and verify that its equation is

$$m_1m_2m_3 X_0^2 + \dots - m_2m_3(m_0 + m_1) X_0X_1 + \dots = 0.$$

Determine points on this quadric by linear constructions which are in none of the faces.

Exercise.

Construct a quadric which generalizes the sphere of Prouhet, passing through the barycenters and orthocenters of the faces and verify that its equation is

$$\begin{aligned} & 3(m_0 + m_1)m_2m_3X_0X_1 + \dots \\ & -2(X_0 + X_1 + X_2 + X_3)(m_1m_2m_3X_0 + \dots) = 0. \end{aligned}$$

(Coolidge, *Treatise*, p. 237)

6.2.5 The isodynamic tetrahedron.**Definition.**

A symmedian is a line joining a vertex to the point of Lemoine of the opposite face.

Definition.

An isodynamic tetrahedron is a tetrahedron in which 3 of the symmedians are concurrent.

Theorem.

A tetrahedron is isodynamic iff

$$n_0n_5 = n_1n_4 = n_2n_3.$$

Proof:

Let K_i be the symmedian in the plane \mathcal{A}_i , let $k_i := A_i \times K_i$,

$$K_0 = (0, n_5, n_4, n_3), K_1 = (n_5, 0, n_2, n_1),$$

$$K_2 = (n_4, n_2, 0, n_0), K_3 = (n_3, n_1, n_0, 0).$$

$k_0 = [n_5, n_4, n_3, 0, 0, 0]$, $k_1 = [n_5, 0, 0, n_2, n_1, 0]$ and $k_2 = [0, n_4, 0, n_2, 0, n_0]$.

k_0 and k_1 are coplanar if $n_1n_4 = n_2n_3$, k_0 and k_2 are coplanar if $n_0n_5 = n_2n_3$, hence the theorem.

Theorem.

In an isodynamic tetrahedron all 4 symmedians are concurrent.

6.1.3 The orthogonal tetrahedron.**Definition.**

A tetrahedron is orthogonal iff opposite sides are perpendicular.

Lemma.

$$a_0 \cdot a_5 = 0 \text{ iff } n_1 + n_4 = n_2 + n_3,$$

$$a_0 \cdot a_1 = 0 \text{ iff } n_3 = n_0 + n_1,$$

$$a_1 \cdot a_2 = 0 \text{ iff } n_5 = n_1 + n_2,$$

$$a_2 \cdot a_0 = 0 \text{ iff } n_4 = n_2 + n_0.$$

Theorem.

The tetrahedron is orthogonal iff the parameters of the circumsphere satisfy

$$n_0 + n_5 = n_1 + n_4 = n_2 + n_3.$$

Proof: The perpendicularity of $A_0 \vee A_1$ and $A_2 \vee A_3$ implies $(0, 0, 1, -1)\mathbf{F}(1, -1, 0, 0)^T = 0$,
or

$$(n_1 - n_3) - (n_2 - n_4) = 0 \text{ or}$$

$$n_1 + n_4 = n_2 + n_3,$$

Similarly that of $A_0 \vee A_2$ and $A_1 \vee A_3$ implies

$$n_0 + n_5 = n_2 + n_3.$$

Theorem.

If $n_0 + n_1 - n_3 \neq 0$, $n_3 + n_4 - n_5 \neq 0$, $n_5 + n_1 - n_2 \neq 0$, $n_2 + n_4 - n_0 \neq 0$, and the tetrahedron is orthogonal. Let

$$0. \quad m_0 = (n_0 + n_1 - n_3)^{-1}, \quad m_1 = (n_3 + n_4 - n_5)^{-1}, \\ m_2 = (n_5 + n_1 - n_2)^{-1}, \quad m_3 = (n_2 + n_4 - n_0)^{-1},$$

then

$$1. \quad n_0 = (m_0 + m_1)m_2m_3, \quad n_1 = (m_0 + m_2)m_3m_1, \quad n_2 = (m_0 + m_3)m_1m_2, \\ n_3 = (m_1 + m_2)m_0m_3, \quad n_4 = (m_3 + m_1)m_0m_2, \quad n_5 = (m_2 + m_3)m_0m_1.$$

Proof: We obtain at once,

$$m_0^{-1} + m_1^{-1} = 2n_0, \quad m_2^{-1} + m_0^{-1} = 2n_1, \quad m_1^{-1} + m_2^{-1} = 2n_3,$$

using 1.3.3., we also obtain

$$m_0^{-1} + m_3^{-1} = n_1 - n_3 + n_2 + n_4 = 2n_2,$$

$$m_1^{-1} + m_3^{-1} = n_3 - n_1 + n_2 + n_4 = 2n_4,$$

$$m_2^{-1} + m_3^{-1} = n_1 + n_2 + n_3 + n_4 - 2n_0 = 2n_5.$$

If we multiply by $\frac{1}{2}m_0m_1m_2m_3$ we get 1.

Comment.

?? when hyp. of prec theorem replace $\neq 0$ by $= 0$, see Theorem 3.7.

Comment.

The indices obey the following rules.

Let $n_{0,1}$ be the coefficient of X_0X_1, \dots ,

we have $n_{0,1} = n_0$, $n_{0,2} = n_1$, $n_{0,3} = n_2$,

$$n_{1,2} = n_3, \quad n_{1,3} = n_4, \quad n_{2,3} = n_5.$$

The orthogonality takes the form,

$$n_{0,1} + n_{2,3} = n_{0,2} + n_{1,3} = n_{0,3} + n_{1,2}.$$

m_i is the inverse of $n_{i,j} + n_{i,k} - n_{j,k}$, where i, j, k are distinct.

For instance, if l is distinct from i, j, k , m_i is also the inverse of $n_{i,j} + n_{i,l} - n_{j,l}$.

Definition.

A orthogonal tetrahedron is called a special orthogonal tetrahedron at A_i if 2 adjacent sides through A_i are also orthogonal.

Theorem.

If $A_0 \vee A_1$ is orthogonal to $A_0 \vee A_2$ and the tetrahedron is orthogonal then these lines are orthogonal to $A_0 \vee A_3$ and

$$n_0 + n_1 - n_3 = n_2 + n_0 - n_4 = n_1 + n_2 - n_5 = 0.$$

Vice versa, if $n_0 + n_1 - n_3 = 0$ and the tetrahedron is orthogonal, then it is special at A_0 .

Exercise.

Discuss the special cases

$$0. \quad n_0 + n_1 - n_3 = 0, \quad n_3 + n_4 - n_5 \neq 0 \dots$$

$$1. \quad n_0 + n_1 - n_3 = 0, \quad n_3 + n_4 - n_5 = 0$$

$$2. \quad n_0 = 0.$$

Theorem.

The coordinates of the points lines and planes defined in in 1.2.7. are $H0.0.$ $A_0 = (1, 0, 0, 0)$,

$$H0.1. \quad M = (1, 1, 1, 1),$$

$$P0.0. \quad a_0 = a_{0,1} = [1, 0, 0, 0, 0, 0],$$

$$P0.1. \quad |0 = \{1, 0, 0, 0\},$$

$$P0.2. \quad |I = \{1, 1, 1, 1\},$$

$$P1.0. \quad C = (-m_0 + m_1 + m_2 + m_3, m_0 - m_1 + m_2 + m_3, m_0 + m_1 - m_2 + m_3, m_0 + m_1 + m_2 - m_3),$$

$$P1.1. \quad euler = [m_0 - m_1, m_0 - m_2, m_0 - m_3, m_1 - m_2, m_3 - m_1, m_2 - m_3],$$

$$P1.2. \quad AP_0 = (m_0(m_1 + m_2)(m_3 + m_1)(m_2 + m_3), -m_1(m_2 + m_3)(m_0m_1 + m_2m_3), -m_2(m_3 + m_1)(m_0m_2 + m_3m_1), -m_3(m_1 + m_2)(m_0m_3 + m_1m_2)),$$

$$P1.3. \quad med_0 = [m_2 + m_3, m_3 + m_1, m_1 + m_2, m_2 - m_1, m_1 - m_3, m_3 - m_2],$$

$$P1.4. \quad Imed_0 = (-(m_1 + m_2 + m_3), m_1, m_2, m_3),$$

$$P1.5. \quad alt_0 = [m_1, m_2, m_3, 0, 0, 0],$$

$$P1.6. \quad Foot_0 = (0, m_1, m_2, m_3),$$

$$P1.7. \quad ipa_{0,1} = [m_2 + m_3, -m_2, -m_3, m_2, -m_3, 0]$$

$$P1.8. \quad |Perp_{0,1} = \{0, 0, -m_3, m_2\}, \text{ perp. to } a_{0,1} \text{ through } A_2 \times A_3 \\ = \text{same??}$$

$$P1.9. \quad Facefoot_{0,1} = (m_0, m_1, 0, 0), \text{ on } a_{0,1} \\ = \text{same},$$

$$P1.10. \quad facealtitude_{0,1} = [0, m_2, m_3, 0, 0, 0], \text{ Facefoot}_{2,3} \vee A_0 \\ [1, 0] = [0, 0, m_0, 0, m_1, 0], \text{ Facefoot}_{2,3} \vee A_1$$

$$P1.11. \quad O_0 = (0, m_1, m_2, m_3),$$

$$P1.12. \quad Mid_0 = (0, m_1, m_2, m_3),$$

$$P1.13. \quad mid_0 = [m_1, m_2, m_3, 0, 0, 0],$$

$$P1.14. \quad H = (m_0, m_1, m_2, m_3),$$

$$P1.15. \quad Eta : m_2m_3X0X1 - m_1m_3X0X2 - m_0m_2X1X3 + m_0m_1X2X3 = 0$$

$$m_2m_3X0X1 - m_1m_2X0X3 - m_0m_3X1X2 + m_0m_1X2X3 = 0.$$

$$Coideal = \{m_1m_2m_3, m_2m_3m_0, m_3m_0m_1, m_0m_1m_2\},$$

$$Cocenter = Barycenter,$$

Theorem.

If $(0, p_1, p_2, p_3)$ is on the Euler line $eul^{(0)}$ then

$$0. \quad p_1(m_2 - m_3) + p_2(m_3 - m_1) + p_3(m_1 - m_2) = 0,$$

1. $P \vee IC(0)$ intersects the Euler line eu ; at

$$((p_1(m_0 - m_2) + p_2(m_1 - m_0))(m_1 + m_2 + m_3),$$

$$p_1((m_1 - m_2)(m_1 + m_2 + m_3) + m_2(m_1 - m_0)) + p_2m_1(m_0 - m_1),$$

$$p_2((m_1 - m_2)(m_1 + m_2 + m_3) + m_1(m_0 - m_2)) + p_1m_2(m_2 - m_0),$$

$$p_2((m_1 - m_3)(m_1 + m_2 + m_3) + m_1(m_0 - m_3)) + p_1((m_3 - m_2)(m_1 + m_2 + m_3) +$$

$$m_2(m_3 - m_0))),$$

or more symmetrically,

$$(p_1(s_1(m_0 - m_2) + m_0(m_2 - m_0) + p_2(s_1(m_1 - m_0) + m_0(m_0 - m_1)),$$

$$p_1(s_1(m_1 - m_2) + m_1(m_2 - m_0) + p_2(s_1(m_1 - m_1) + m_1(m_0 - m_1)),$$

$$p_1(s_1(m_2 - m_2) + m_2(m_2 - m_0) + p_2(s_1(m_1 - m_2) + m_2(m_0 - m_1)),$$

$$p_1(s_1(m_3 - m_2) + m_3(m_2 - m_0) + p_2(s_1(m_1 - m_3) + m_3(m_0 - m_1))),$$

Moreover if $p_1 = km_1 + s - m_0$, $p_2 = km_2 + s - m_0$, $p_3 = km_3 + s - m_0$, then the point on e is

$$((k-1)m_0 + s, (k-1)m_1 + s, (k-1)m_2 + s, (k-1)m_3 + s).$$

In particular,

$$M = (m_1 + m_2 + m_3, m_2 + m_3 + m_0, m_3 + m_0 + m_1, m_0 + m_1 + m_2), \quad P = (s_1t_0 -$$

$$m_0t_0, s_1(m_1^{2-m_2m_3}-m_1t_0, s_1(m_2^2-m_3m_1)-m_2t_0,$$

$$s_1(m_3^{2-m_1m_2}-m_3t_0),$$

$$with t_0 = m_0m_1 + m_0m_2 + m_0m_3 - m_1m_2 - m_3m_1 - m_2m_3,$$

$$\overline{O} = ($$

$$Am = (s_1 - 3m_0, s_1 - 3m_1, s_1 - 3m_2, s_1 - 3m_3),$$

$$G = (s_1 + 2m_0, s_1 + 2m_1, s_1 + 2m_2, s_1 + 2m_3),$$

$$\overline{Am} = ()$$

$$D_0 = ()$$

$$D_1 = ()$$

$$D_2 = ()$$

$$G = ()$$

$$\overline{G} = ()$$

Answer (partial).

$$\dots ? \quad The \text{ polar } pp_0 = [-2m_1m_2, m_2(m_0 + m_1), m_1(m_2 + m_0),$$

$$\dots ? \quad The \text{ intersection } PP_0 = (0, -m_1(m_2 + m_0), m_2(m_0 + m_1)),$$

... ? $pp = [m_1m_2(m_2+m_0)(m_0+m_1), m_2m_0(m_0+m_1)(m_1+m_2), m_0m_1(m_1+m_2)(m_2+m_0)]$.

Point "O", intersection of perpendicular to faces through their barycenter

(special case of ... with $k = 0$ hence

"O" = $(s_1 - m_0, s_1 - m_1, s_1 - m_2, s_1 - m_3)$.

"Conjugate tetrahedron",

"A'" = $(-2s_1 - 2m_0, s_1 + 2m_1, s_1 + 2m_2, s_1 + 2m_3)$,

barycenter of faces of $[A'[i]]$ are

"M'" = $(0, m_1, m_2, m_3)$, which are the orthocenters of the faces,

Perpendiculars through M'_0 to the faces, (which are parallel to those of $[A[]]$ meet at

"O'" = $(3s_1 - 4m_0, 3s_1 - 4m_1, 3s_1 - 4m_2, 3s_1 - 4m_3)$.

Hence his theorem: Then he generalizes the circle of Brianchon-Poncelet and gives its center as the midpoint of H and "O"

I believe his "O" is my G .

Orthocenter, barycenter and "O" are collinear

6.1.4 The isodynamic tetrahedron.

Definition.

A symmedian is a line joining a vertex to the point of Lemoine of the opposite face.

Definition.

An isodynamic tetrahedron is a tetrahedron in which 3 of the symmedians are concurrent.

Theorem.

A tetrahedron is isodynamic iff

$$n_0n_5 = n_1n_4 = n_2n_3.$$

Proof:

$$K_0 = (0, n_5, n_4, n_3), K_1 = (-n_5, 0, n_2, -n_1),$$

$$K_2 = (-n_4, -n_2, 0, n_0), K_3 = () .$$

k_0 and k_1 are coplanar if $n_1n_2 = n_2n_3$, k_0 and k_2 are coplanar if $n_0n_5 = n_2n_3$, hence the theorem.

Theorem.

In an isodynamic tetrahedron all 4 symmedians are concurrent.

In 3 dimensions start with $A_0 = (1, 0, 0, 0)$, ..., $A_3 = (0, 0, 0, 1)$, and with $M = (1, 1, 1, 1)$ and $\overline{M} = (m_0, m_1, m_2, m_3)$. M corresponds to the barycenter, \overline{M} to the intersection of the lines joining the orthocenter of the faces to the opposite vertex and $A[]$ to the vertices of an orthogonal tetrahedron. See ...

. Theorem. Prove that the tetrahedron is orthogonal.

. Theorem. Prove that the circumscribed quadric is given by

$$(m_0 + m_1)m_2m_3X_0X_1 + \dots = 0.$$

. Theorem. Construct a quadric generalizing the conic of Brianchon- Poncelet, and verify that its equation is

$$m_1 m_2 m_3 X_0^2 + \dots - m_2 m_3 (m_0 + m_1) X_0 X_1 + \dots = 0.$$

Determine points on this quadric by linear constructions which are in none of the faces.

. Theorem. Construct a quadric which generalizes the sphere of Prouhet, passing through the barycenters and orthocenters of the faces and verify that its equation is

$$3(m_0 + m_1) m_2 m_3 X_0 X_1 + \dots \\ -2(X_0 + X_1 + X_2 + X_3)(m_1 m_2 m_3 X_0 + \dots) = 0.$$

(Coolidge, Treatise, p. 237)

Point “O”, intersection of perpendicular to faces through their barycenter (special case of ... with $k = 0$ hence

$$“O” = (s_1 - m_0, s_1 - m_1, s_1 - m_2, s_1 - m_3)$$

“Conjugate tetrahedron”,

$$“A'_0” = (-2s_1 - 2m_0, s_1 + 2m_1, s_1 + 2m_2, s_1 + 2m_3),$$

barycenter of faces of $[A'[i]]$ are

$$“M'_0” = (0, m_1, m_2, m_3),$$

which are the orthocenters of the faces,

Perpendiculars through M'_0 to the faces, (which are parallel to those of $[A[]]$ meet at

$$“O'” = (3s_1 - 4m_0, 3s_1 - 4m_1, 3s_1 - 4m_2, 3s_1 - 4m_3),$$

Hence his theorem:

Then he generalizes the circle of Brianchon-Poncelet and gives its center as the midpoint of H and “O”

I believe his “O” is my G .

Orthocenter, barycenter and “O” are collinear.

6.1.5 The antipolarity.

Definition.

Consider the 2-form $[l_0, l_1, l_2, l_3, l_4, l_5]$ with

$$0. l_0 l_5 + l_1 l_4 + l_2 l_3 \neq 0,$$

the point to plane antipolarity associates to a point P a plane $\mathcal{P} := l' \vee P$,

the plane to point antipolarity associates to a plane \mathcal{P} a point $P := l' \mathcal{P}$.

Theorem.

The point to plane antipolarity can be represented by an antisymmetric matrix

$$\mathbf{P} = \begin{pmatrix} 0 & l_5 & l_4 & l_3 \\ -l_5 & 0 & l_2 & -l_1 \\ -l_4 & -l_2 & 0 & l_0 \\ -l_3 & l_1 & -l_0 & 0 \end{pmatrix}$$

The plane to point antipolarity is represented by the antisymmetric matrix

$$\mathbf{Q} = \begin{pmatrix} 0 & l_0 & l_1 & l_2 \\ -l_0 & 0 & l_3 & -l_4 \\ -l_1 & -l_3 & 0 & l_5 \\ -l_2 & l_4 & -l_5 & 0 \end{pmatrix}$$

both have determinant $(l_0l_5 + l_1l_4 + l_2l_3)^2 \neq 0$.

Theorem.

If \mathcal{P} is associated to P in an antipolarity then P is associated to $|P$ and $|P$ is incident to P .

The proof is left as an exercise.

Theorem.

Let

$$0. \ d := l_0l_5 + l_1l_4 + l_2l_3,$$

the planes associated in the antipolarity 6.1.5 to the points of a line m are all incident to a line q and if

$$1. \ \mathbf{L} := l \, dual(l)^T - d\mathbf{I},$$

then

$$2. \ \mathbf{L} = \begin{pmatrix} -l_1l_4 - l_2l_3 & l_0l_4 & l_0l_3 & l_0l_2 & l_0l_1 & l_0^2 \\ l_1l_5 & -l_0l_5 - l_2l_3 & l_1l_3 & l_1l_2 & l_1^2 & l_0l_1 \\ l_2l_5 & l_2l_4 & -l_0l_5 - l_1l_4 & l_2^2 & l_2l_1 & l_2l_0 \\ l_3l_5 & l_3l_4 & l_3^2 & -l_0l_5 - l_1l_4 & l_3l_1 & l_3l_0 \\ l_4l_5 & l_4^2 & l_4l_3 & l_4l_2 & -l_0l_5 - l_2l_3 & l_4l_0 \\ l_5^2 & l_5l_4 & l_5l_3 & l_5l_2 & l_5l_1 & -l_1l_4 - l_2l_3 \end{pmatrix}$$

$$3. \ q = \mathbf{L}m.$$

$$4. \ det(\mathbf{L}) = -d^6.$$

The proof is left as an exercise.

Example.

Let $p = 29$, $l' = [1, 4, 3, 11, 4, 10] = [3644209]$,

$$E0. \quad d = 1.$$

$$E2. \quad \mathbf{L} = \begin{pmatrix} 9 & 4 & 11 & 3 & 4 & 1 \\ 11 & -14 & -14 & 12 & -13 & 4 \\ 1 & 12 & 3 & 9 & 12 & 3 \\ -6 & -14 & 5 & 3 & -14 & 11 \\ 11 & -13 & -14 & 12 & -14 & 4 \\ 13 & 11 & -6 & 1 & 11 & 9 \end{pmatrix}$$

$$E3. \quad m = 732541, 25620, 871, 30, 1, 0.$$

$$q = 20154561, 8595176, 4156378, 3635799, 3644412, 3644208.$$

Theorem.

The antipolarity of vertices, faces and edges of a tetrahedron follows from what follows.
Given

$$H.0. \quad l' = [l_0, l_1, l_2, l_3, l_4, l_5],$$

$$H.1. \quad A_i,$$

let

$$D0.0. \quad a_{i,j} := A_i \vee A_j,$$

$$D0.1. \quad \mathcal{A}_i := a_{j,k} \vee A_l,$$

$$D1.0. \quad \mathcal{B}_i := l' \vee A_i, B_i := l' \mathcal{A}_i,$$

$$D1.1. \quad ba_i := |B_i|A_i, b\bar{a}_i := B_i \vee A_i,$$

$$D1.2. \quad N_{i,j} := a_{k,l} \mathcal{B}_j, \mathcal{N}_{i,j} := a_{i,j} \vee B_j,$$

$$D1.3. \quad n_{i,j} := B_i \vee A_j,$$

$$D1.4. \quad b_{d(i,j)} := |B_i|B_j,$$

then

$$C1.0. \quad B_i \vee \mathcal{B}_j = 0.$$

$$C1.1. \quad N_{i,j} \vee \mathcal{N}_{j,i} = 0.$$

$$C1.2. \quad N_{i,j} \vee n_{i,j} = 0,$$

$$C1.3. \quad n_{i,j} = |B_j|A_i.$$

$$C1.4. \quad b_{d(i,j)} = B_k \vee B_l.$$

$$C1.5. \quad b_u = \mathbf{L}a_u.$$

Proof.

$$P1.0. \quad \mathcal{B}_0 = \{0, -l_5, -l_4, -l_3\}.$$

$$B_0 = (0, -l_0, -l_1, -l_2).$$

$$P1.1. \quad ba_0 = [0, 0, 0, l_3, l_4, l_5].$$

$$b\bar{a}_0 = [l_0, l_1, l_2, 0, 0, 0].$$

$$P1.2. \quad N_{1,2} = (0, 0, l_1, l_2).$$

$$\bar{N}_{1,2} = \{0, 0, l_4, l_3\}.$$

$$P1.3. \quad n_{1,2} = [0, 0, 0, l_1, -l_2, 0].$$

$$P1.4. \quad b_0 = [-l_1l_4 - l_2l_3, l_1l_5, l_2l_5, l_3l_5, l_4l_5, l_5^2].$$

Corollary.

If l is a line and the definitions of Theorem 6.1.5 hold then all the conclusions of 6.1.5 hold.
Moreover $b_u = l$ for all u .

The mapping is not one to one. The image of a point P is the plane $P \vee l$, the image of the plane \mathcal{Q} is the point $\mathcal{Q} \vee l$.

Example.

Let $p = 29$, $l' = [1, 4, 3, 11, 4, 10] = [3644209]$, $A = (871, 30, 1, 0)$,

$$E0.0. \quad a = [732541, 25260, 871, 30, 1, 0].$$

$$E0.1. \quad \mathcal{A} = \{871, 30, 1, 0\}.$$

$$E1.0. \quad \mathcal{B} = \{382, 1463, 7606, 22969\}.$$

$$B = (149, 1397, 9293, 16386).$$

$$E1.1. \quad ba = [139, 220389, 805824, 3570916],$$

$$\begin{aligned}
& b\bar{a} = [3634832, 741908, 33687, 1203]. \\
E1.2. \quad N &= \begin{pmatrix} -- & 9 & 33 & 146 \\ 27 & -- & 875 & 1393 \\ 37 & 883 & -- & 9281 \\ 378 & 1248 & 16009 & -- \end{pmatrix}. \\
\mathcal{N} &= \left\{ \begin{pmatrix} -- & 11 & 34 & 378 \\ 19 & -- & 883 & 1451 \\ 49 & 878 & -- & 7599 \\ 233 & 1103 & 22737 & -- \end{pmatrix} \right\}. \\
E1.3. \quad n &= \begin{bmatrix} -- & 639 & 56 & 26 \\ 659374 & -- & 25285 & 889 \\ 903264 & 732889 & -- & 1422 \\ 9219913 & 745997 & 40398 & -- \end{bmatrix}. \\
E1.4. \quad b &= [20154561, 8595176, 4156378, 3635799, 3644412, 3644208].
\end{aligned}$$

Example.

Let $p = 29$, $l = [3623186] = [1, 4, 2, -14, 4, 12]$, $A = (871, 30, 1, 0)$,

$$E1.0 \quad \mathcal{B} = \{343, 1577, 13493, 18590\}.$$

$$B = (148, 1281, 10148, 23752).$$

$$E1.1. \quad ba = [286, 391098, 781435, 3574280],$$

$$b\bar{a} = [3610443, 745272, 34514, 935].$$

$$E1.2. \quad N = \begin{pmatrix} -- & 16 & 32 & 146 \\ 22 & -- & 875 & 1277 \\ 35 & 897 & -- & 10122 \\ 784 & 1045 & 23578 & -- \end{pmatrix}.$$

$$\mathcal{N} = \left\{ \begin{pmatrix} -- & 12 & 53 & 320 \\ 28 & -- & 881 & 1567 \\ 44 & 878 & -- & 13486 \\ 233 & 929 & 18532 & -- \end{pmatrix} \right\}.$$

$$E1.3. \quad n = \begin{bmatrix} -- & 436 & 57 & 26 \\ 537429 & -- & 25285 & 885 \\ 854486 & 733295 & -- & 1393 \\ 19121847 & 751884 & 47967 & -- \end{bmatrix}.$$

$$E1.4. \quad b_u = [3623186].$$

Theorem.

An antipolarity can be determined as follows,

Given 4 points A_i , a line $ba_0 \in \mathcal{A}_0 = A_1 \vee A_2 \vee A_3$,

a line $ba_1 \in A_1 := A_2 \vee A_3 \vee A_0$ and a point B_0 on $n_{0,1} = A_1 \vee (ba_1 \rtimes a_5)$ but not on $((ba_0 \rtimes a_4) \vee A_0) \rtimes (ba_1 \rtimes a_2) \vee A_1)) \vee ((ba_0 \rtimes a_3) \vee A_0) \rtimes (ba_1 \rtimes a_1) \vee A_1)) (= B_2 \vee B_3)$.

Proof. Let us choose the A_i as basis for the coordinate system.

$ba_0 = [0, 0, 0, l_3, l_4, l_5]$ determines l_3, l_4, l_5 .

$ba_1 = [0, l_1, l_2, 0, 0, l_5]$ determines after scaling l_1 and l_2 .

$B_0 = (0, l_0, l_1, l_2)$, determines, after scaling l_0 . Scaling the last component should check with l_2 .

Example.

Let $p = 29$, $A = (871, 30, 1, 0)$.

Let $ba_0 = [139] = [0, 0, 0, 1, 3, -7]$, $ba_1 = [220389] = [0, 1, 8, 0, 0, -12]$,

$N_{0,1} = ba_1 \rtimes a_5 = (9)$, $n_{0,1} := N_{0,1} \vee A_1 = [639]$.

Finally let $B_0 = (149) = (0, 1, 4, 3)$ on $[639] = [0, 0, 0, 1, -8, 0]$ but not on $[20154561] = [1, -2, 13, 9, -2, -5]$.

(For the details of the computations see Example 6.1.5.)

ba_0 gives $l_3 = 1$, $l_4 = 3$, $l_5 = -7$,

ba_1 gives $l_1 = t$, $l_2 = 8t$, $l_5 = -12t$, t is the scaling factor,

hence $l_1 = t = \frac{7}{12} = 3$, $l_2 = -5$.

B_0 gives $l_0 = u$, $l_1 = 4u$, $l_2 = 3u$, hence $l_0 = u = \frac{3}{4} = 8$.

$l_2 = 3.8 = -5$ is a check.

Therefore $l' = [8, 3, -5, 1, 3, -7] = [1, 4, 3, 11, 4, 10]$.

The associated construction is as follows.

Construction.

Given A_0, A_1, A_2, A_3 , $ba_0 \in \mathcal{A}_0$, $ba_1 \in \mathcal{A}_1$,

$N_{1,0} := ba_0 \rtimes a_5$, $n_{1,0} := N_{1,0} \vee A_0$,

$N_{2,0} := ba_0 \rtimes a_4$, $n_{2,0} := N_{2,0} \vee A_0$,

$N_{3,0} := ba_0 \rtimes a_3$, $n_{3,0} := N_{3,0} \vee A_0$.

$N_{0,1} := ba_1 \rtimes a_5$, $n_{0,1} := N_{0,1} \vee A_1$,

$N_{2,1} := ba_1 \rtimes a_2$, $n_{2,1} := N_{2,1} \vee A_1$,

$N_{3,1} := ba_1 \rtimes a_1$, $n_{3,1} := N_{3,1} \vee A_1$.

$B_2 := n_{2,0} \rtimes n_{2,1}$, $n_{2,3} := B_2 \vee A_3$,

$N_{2,3} := n_{2,3} \rtimes a_0$,

$B_3 := n_{3,0} \rtimes n_{3,1}$, $n_{3,2} := B_3 \vee A_2$,

$N_{3,2} := n_{3,2} \rtimes a_0$.

Given B_0 on $n_{0,1}$, not on $B_2 \vee B_3$ (otherwise l' is a line),

$n_{0,2} := B_0 \vee A_2$, $N_{0,2} := n_{0,2} \rtimes a_4$,

$n_{0,3} := B_0 \vee A_3$, $N_{0,3} := n_{0,3} \rtimes a_3$.

$ba_2 := N_{0,2} \vee N_{3,2}$,

$N_{1,2} := ba_2 \rtimes a_2$, $n_{1,2} := N_{1,2} \vee A_2$,

$B_1 := n_{1,2} \rtimes n_{1,0}$.

B_i are the antipoles of \mathcal{A}_i .

$ba_3 := N_{0,3} \vee N_{2,3}$.

$\mathcal{B}_i := A_i \vee ba_i$.

\mathcal{B}_i are the antipolars of A_i .

To complete the construction,

$N_{1,3} := ba_3 \rtimes a_1$, $n_{1,3} := B_1 \vee A_3$, we can check

$$0. \quad N_{1,3} \vee n_{1,3} = 0.$$

Theorem.

In the geometry of the triangle if A_3 is \overline{M} , ba_0 is m , and ba_1 is an arbitrary line and B_0 is an arbitrary point on $(ba_1 \times (A_2 \times \overline{M})) \times A_1$, the configuration of 6.1.5 consisting of 20 points A , B and N , and of 22 lines a , ba , n , satisfies 6.1.5.0.

Theorem.

$$D1.0. \quad \mathcal{P}a_r := P \vee a_{5-r},$$

$$D1.1. \quad Pab_r := \mathcal{P}a_r b_{5-r},$$

$$D1.2. \quad \mathcal{P} := Pab_0 \vee Pab_1 \vee Pab_2,$$

then

$$C1.0. \quad \mathcal{P} \vee P = 0,$$

$$C1.1. \quad \mathcal{P} = P \vee l'.$$

Example.

With p , l' and A as in Example 6.1.5.

Let $P = (1742) = (1, 1, 1, 1)$, then $\mathcal{P}a = \{24419, 1683, 899\}$, $Pab = (2357, 3443, 25116)$, $\mathcal{P} = \{9747\}$.

Let $P = (5350) = (1, 5, 9, 13)$,

then $\mathcal{P}a = \{20214, 1335, 891\}$, $Pab = (5356, 5363, 3726)$, $\mathcal{P} = \{2611\}$.

Exercise.

The antipolarity associates to a point quadric *Alpha*, a plane quadric *Beta*, the points of one are on the tangent of the other. Study this correspondance in detail.

6.1.6 Example.**Case 0.**

$p = 13$, *Barycenter* = 366, $n = 1, 3, 6, 7, 10, 12$, $m = 1, 2, 4, 5$,

The tetrahedron is orthogonal.

Barycenter = (366)

Ideal = {366}

$A = (183, 14, 1, 0)$

$a = [30941, 2380, 183, 14, 1, 0]$

Center = (1244)

Pole of A = (1509, 525, 271, 60)

mediatrix = [271483, 148770, 212411, 132416]

IC = (387, 747, 591, 579)

altitude = [107836, 32527, 2726, 330]

Foot = (49, 240, 526, 573)

ipa = [85840, 136570, 110191, 374757, 58939, 29111]

Perp. = {8, 24, 92, 188, 222, 1197}

= {8, 24, 92, 188, 222, 1197}

$$Facefoot = (12, 23, 40, 188, 235, 521)$$

$$= (12, 23, 40, 188, 235, 521)$$

$$facealtitude = [26547, 50714, 88063, 31006, 187, 2718]$$

$$= [40, 18, 12, 2388, 32462, 326]$$

$$Orthocenters = (49, 240, 526, 573)$$

$$Mid = (49, 240, 526, 573)$$

$$mid = [107836, 32527, 2726, 330]$$

$$Orthocenter = (578)$$

$$Coideal = \{1504\}$$

$$Cocenter = (366)$$

$$Barycenter(check) = (366)$$

$$Hyperboloid : 1110035, 4011203$$

The coordinates of IC are $(1,1,2,9)$, $(1,3,4,5)$, $(1,2,5,5)$, $(1,2,4,6)$,

those of Foot are $(0,1,2,9)$, $(1,0,4,5)$, $(1,2,0,5)$, $(1,2,4,0)$,

those of the Center of Hyperboloid are $(1, 2, 4, 5)$,

the hyperboloids are

$$\begin{aligned} &(-2r_1 + 4r_2)X_0X_1 + r_1X_0X_2 + r_2X_0X_3 \\ &-r_2X_1X_2 + 3r_1X_3X_1 + (5r_1 + 3r_2)X_2X_3 = 0. \end{aligned}$$

Case 1.

$$p = 13, Barycenter = 1504, n = 1, 3, 6, 7, 10, 12, m = 1, 2, 4, 5,$$

The tetrahedron is orthogonal.

The Center is an ideal point.

$$Barycenter = (1504)$$

$$Ideal = \{578\}$$

$$A = (183, 14, 1, 0)$$

$$a = [30941, 2380, 183, 14, 1, 0]$$

$$Center = (2368)$$

Case 2.

$$p = 13, Barycenter = 366, n = 1, 5, 2, 6, 4, 10,$$

The Center is an ideal point.

$$Barycenter = (366)$$

$$Ideal = \{366\}$$

$$A = (183, 14, 1, 0)$$

$$a = [30941, 2380, 183, 14, 1, 0]$$

$$Center = (2248)$$

Case 3.

$$p = 13, Barycenter = 366, n = 1, 4, 10, 9, 2, 5, m = 1, 8, 4, 2,$$

The tetrahedron is orthogonal.

$$Barycenter = (366)$$

$$Ideal = \{366\}$$

$A = (183, 14, 1, 0)$
 $a = [30941, 2380, 183, 14, 1, 0]$
 $Center = (94)$
 $Poleof \mathcal{A} = (1156, 2225, 589, 942)$
 $mediatrix = [208070, 207763, 208045, 207684]$
 $IC = (1156, 1251, 1563, 1587)$
 $altitude = [252838, 32488, 3743, 252]$
 $Foot = (115, 237, 1537, 1587)$
 $ipa = [269114, 110205, 242016, 374208, 58939, 30209]$
 $\mathcal{P}erp. = \{12, 23, 157, 189, 222, 1535\}$
 $\quad = \{12, 23, 157, 189, 222, 1535\}$
 $Facefoot = (8, 24, 105, 185, 235, 1535)$
 $\quad = (8, 24, 105, 185, 235, 1535)$
 $facealtitude = [17759, 52911, 230868, 30967, 187, 3732]$
 $\quad = [92, 17, 7, 2391, 32462, 248]$
 $Orthocenters = (115, 237, 1537, 1587)$
 $Mid = (115, 237, 1537, 1587)$
 $mid = [252838, 32488, 3743, -1]$
 $Orthocenter = (1589)$
 $Coideal = \{1165\}$
 $Cocenter = (299)$
 $Barycenter(check) = (366)$
 $Hyperboloid : 6100106, 301903$

Case 4.

$p = 13, Barycenter = 366, n = 1, 4, 4, 9, 2, 5,$
 $Barycenter = (366)$
 $\mathcal{I}deal = \{366\}$
 $A = (183, 14, 1, 0)$
 $a = [30941, 2380, 183, 14, 1, 0]$
 $Center = (1833)$
 $Poleof \mathcal{A} = (281, 150, 2341, 527)$
 $mediatrix = [207817, 330382, 309075, 201913]$
 $IC = (1504, 2092, 1312, 1587)$
 $altitude = [237459, 32774, 3396, 252]$
 $Foot = (108, 233, 1208, 1587)$
 $ipa = [269480, 110754, 242016, 375855, 163118, 348392]$
 $\mathcal{P}erp. = \{63, 110, 157, 190, 2133, 1540\}$
 $\quad = \{330, 2215, 157, 190, 227, 1847\}$
 $Facefoot = (2, 19, 105, 194, 326, 1535)$
 $\quad = (8, 24, 105, 194, 235, 1873)$
 $facealtitude = [4577, 41926, 230868, 31084, 194, 3732]$
 $\quad = [92, 17, 7, 2382, 32462, 222]$
 $Orthocenters = (115, 337, 1884, 1587)$

$Mid = (112, 194, 194, 1587)$

$mid = [246391, 173899, 316701, -1]$

$Centerofhyperb. = (194)$

$Coideal = \{-2\}$

$Cocenter = (-2)$

$Barycenter(check) = (366)$

$Hyperboloid : 9800114$

*The coordinates of Center are (1, 9, 9, 12),
those of IC are (1, 7, 10, 8), (1, 11, 3, 11), (1, 6, 8, 11), (1, 8, 4, 0),
those of Foot are (0, 1, 7, 3), (1, 0, 3, 11), (1, 6, 0, 11), (1, 8, 4, 0),
those of orthocenters are (0, 1, 7, 10), (1, 0, 11, 11), (1, 10, 0, 11), (1, 8, 4, 0),
those of the CenterofHyperboloid are (1, 0, 0, 11),
the hyperboloid is*

$$X_0X_1 - 2X_0X_2 - 6X_3X_1 - X_2X_3 = 0.$$

Case 5.

$p = 17, Barycenter = 614, n = 1, 2, 5, 4, 11, 10,$

$Barycenter = (614)$

$\mathcal{I}deal = 614$

$A = (307, 18, 1, 0)$

$a = [88741, 5220, 307, 18, 1, 0]$

$Center = (2954)$

$Poleof\mathcal{A} = (3872, 3441, 1230, 2256)$

$mediatrix = [174494, 1146461, 1279312, 787119]$

$IC = (4484, 2739, 4436, 1700)$

$altitude = [904299, 91648, 9268, 541]$

$Foot = (184, 427, 4368, 1684)$

$ipa = [170402, 88127, 1190767, 798046, 722183, 136312]$

$\mathcal{P}erp. = \{121, 198, 91, 548, 3911, 1187\}$
 $= \{511, 2041, 3605, 1762, 407, 4829\}$

$Facefoot = (12, 23, 86, 318, 341, 3486)$

$= (0, 0, 239, 312, 477, 2908)$

$facealtitude = [59263, 113306, 422825, 88928, 309, 8399]$

$= [1, 0, 5, 5232, 90764, 443]$

$Orthocenters = (0, 346, 2919, 3656)$

$Mid = (173, 7, 29, 2687)$

$mid = [850281, 37068, 146789, 323376]$

$Centerofhyperb. = (2687)$

$Coideal = \{-2\}$

$Cocenter = (-2)$

$Barycenter(check) = (614)$

$Hyperboloid : 42149113$

*The coordinates of the Center are (1, 9, 2, 12),
those of IC are (1, 14, 7, 12), (1, 8, 7, 1), (1, 14, 4, 15), (1, 4, 13, 16),*

those of *Foot* are $(0, 1, 9, 13), (1, 0, 7, 1), (1, 14, 0, 15), (1, 4, 13, 0)$,
 those of *orthocenters* are $(0, 0, 0, 1), (1, 0, 2, 5), (1, 9, 0, 11), (1, 11, 10, 0)$,
 those of the *Center of Hyperboloid* are $(1, 8, 4, 0)$,
 the *hyperboloid* is

$$2X_0X_1 + X_0X_2 + 7X_0X_3 - 4X_1X_2 - 8X_3X_1 - 2X_2X_3 = 0.$$

Case 6.

$p = 17$, *Barycenter* = 614, $n = 1, 5, 2, 11, 4, 10$,
Barycenter = (614)
Ideal = 614
 $A = (307, 18, 1, 0)$
 $a = [88741, 5220, 307, 18, 1, 0]$
Center = (3114)
Pole of A = (3984, 3313, 2240, 1262)
mediatrix = [95281, 167230, 631754, 493841]
IC = (4564, 2643, 1748, 4612)
altitude = [1218731, 93484, 6380, 373]
Foot = (248, 331, 1476, 4608)
 $ipa = [1427515, 407150, 88127, 875734, 799871, 561605]$
Perp. = {41, 107, 198, 567, 1922, 4653}
 = {319, 3493, 2041, 3783, 372, 1395}
Facefoot = (15, 22, 103, 317, 392, 2908)
 = (1, 31, 1, 309, 494, 3486)
facealtitude = [74002, 108393, 506346, 88911, 312, 7821]
 = [18, 22, 0, 5235, 90475, 409]
Orthocenters = (1, 394, 3496, 3095)
Mid = (61, 4, 2623, 205)
 $mid = [304633, 22454, 1185019, 18414]$
Center of hyperb. = (2623)
Coideal = {-2}
Cocenter = (-2)
Barycenter (check) = (614)
Hyperboloid 321051114

The coordinates of *Center* are $(1, 9, 12, 2)$,
 those of *Center of hyperboloid* are $(1, 8, 0, 4)$.
 Observe that the last 2 coordinates are exchanged.

Case 7.

$p = 17$, *Barycenter* = 614, $n = 1, 2, 5, 4, 6, 10$,
 THE QUADRIC IS DEGENERATE

Case 8.

$p = 13$, $Barycenter = 1165$, $n = 1, 4, 10, 9, 2, 5$, $m = 1, 8, 4, 2$,

The tetrahedron is orthogonal.

The Center is an ideal point.

$Barycenter = (1165)$

$\mathcal{I}deal = \{1589\}$

$A = (183, 14, 1, 0)$

$a = [30941, 2380, 183, 14, 1, 0]$

$Center = (501)$

Case 9.

$p = 19$, $Barycenter = 762$, $n = 1, 5, 3, 11, 15, 10$,

$Barycenter = (762)$

$\mathcal{I}deal = \{762\}$

$A = (381, 20, 1, 0)$

$a = [137561, 7240, 381, 20, 1, 0]$

$Center = (5279)$

$Poleof \mathcal{A} = (2484, 3802, 1813, 6007)$

$mediatrix = [2260013, 884810, 642183, 1463793]$

$IC = (597, 128, 4864, 6754)$

$altitude = [82689, 115, 11573, 431]$

$Foot = (12, 15, 4731, 6746)$

$ipa = [881367, 14830, 1375219, 884015, 884396, 386372]$

$Perp. = \{63, 216, 149, 500, 3383, 3644\}$
 $= \{738, 6887, 2775, 2190, 450, 5872\}$

$Facefoot = (12, 23, 77, 396, 438, 1103)$
 $= (15, 32, 191, 395, 495, 2186)$

$facealtitude = [82689, 158138, 528524, 137846, 384, 7962]$
 $= [115, 27, 11, 7245, 142254, 647]$

$Orthocenters = (203, 452, 2201, 1217)$

$Mid = (296, 541, 2557, 1882)$

$mid = [233678, 882463, 2451610, 1218391]$

$Centerofhyperb. = (2557)$

$Coideal = \{-2\}$

$Cocenter = (-2)$

$Barycenter(check) = (762)$

$Hyperboloid : 10870118$

Case 10.

$p = 29$, $Barycenter = 1742$, $n = 1, 5, 3, 11, 4, 10$,

$Barycenter = (1742)$

$\mathcal{I}deal = \{1742\}$

$A = (871, 30, 1, 0)$

$a = [732541, 25260, 871, 30, 1, 0]$
 $Center = (7629)$
 $Poleof \mathcal{A} = (13904, 3284, 4290, 19705)$
 $mediatrix = [5332964, 18533938, 781117, 7231524]$
 $IC = (11875, 23216, 15207, 13667)$
 $altitude = [13487988, 743909, 39576, 1283]$
 $Foot = (553, 1350, 15178, 13660)$
 $ipa = [8254786, 6197397, 2802094, 15763096, 16443405, 9610961]$
 $Perp. = \{484, 433, 109, 27, 11978, 11805\}$
 $\quad = \{1317, 18560, 11630, 1716, 976, 378\}$
 $Facefoot = (17, 40, 436, 871, 1567, 17691)$
 $\quad = (26, 51, 88, 878, 1422, 871)$
 $facealtitude = [415484, 976431, 10634475, 732541, 895, 42080]$
 $\quad = [146, 38, 28, 25282, 740951, 871]$
 $Orthocenters = (109, 1574, 871, 18242)$
 $Mid = (512, 1462, 34, 24564)$
 $mid = [12490883, 8959529, 853649, 15467561]$
 $Centerofhyperb. = (19403)$
 $Coideal = \{4265\}$
 $Cocenter = (759)$
 $Barycenter(check) = (1742)$
 $Hyperboloid : 5714192025$

Case 11.

$p = 29$, $Barycenter = 19403$, $n = 1, 5, 3, 11, 4, 10$,
 $Barycenter = (19403)$
 $\mathcal{I}deal = \{4265\}$
 $A = (871, 30, 1, 0)$
 $a = [732541, 25260, 871, 30, 1, 0]$
 $Center = (759)$
 $Poleof \mathcal{A} = (13904, 3284, 4290, 19705)$
 $mediatrix = [18523362, 18533938, 18522525, 18526776]$
 $IC = (13904, 18759, 19848, 1960)$
 $altitude = [21121745, 751739, 43780, 1691]$
 $Foot = (866, 1098, 19384, 1944)$
 $ipa = [1759206, 15692546, 12959255, 7495237, 10224187, 21187915]$
 $Perp. = \{399, 566, 324, 1401, 8614, 8443\}$
 $\quad = \{1194, 10989, 10499, 20218, 1650, 14791\}$
 $Facefoot = (17, 32, 784, 889, 1567, 14327)$
 $\quad = (20, 34, 523, 878, 1161, 8440)$
 $facealtitude = [415484, 781319, 19121847, 733063, 895, 38716]$
 $\quad = [320, 55, 13, 25282, 748520, 1451]$
 $Orthocenters = (527, 1574, 8458, 14617)$
 $Mid = (202, 901, 7622, 19518)$

$mid = [4930377, 15804147, 19711544, 3631884]$

$Centerofhyperb. = (6873)$

$Coideal = \{22214\}$

$Cocenter = (17926)$

$Barycenter(check) = (19403)$

$Hyperboloid : 21181812216$

6.90 Answers to problems and miscellaneous notes.

Theorem.

If $(0, p_1, p_2, p_3)$ is on the Euler line eul then

$$0. \quad p_1(m_2 - m_3) + p_2(m_3 - m_1) + p_3(m_1 - m_2) = 0,$$

1. $P \vee IC(0)$ intersects the Euler line eul at

$$\begin{aligned} &((p_1(m_0 - m_2) + p_2(m_1 - m_0))(m_1 + m_2 + m_3), \\ &\quad p_1((m_1 - m_2)(m_1 + m_2 + m_3) + m_2(m_1 - m_0)) + p_2m_1(m_0 - m_1), \\ &\quad p_2((m_1 - m_2)(m_1 + m_2 + m_3) + m_1(m_0 - m_2)) + p_1m_2(m_2 - m_0), \\ &\quad p_2((m_1 - m_3)(m_1 + m_2 + m_3) + m_1(m_0 - m_3)) \\ &\quad + p_1((m_3 - m_2)(m_1 + m_2 + m_3) + m_2(m_3 - m_0))), \end{aligned}$$

or more symmetrically,

$$\begin{aligned} &(p_1(s_1(m_0 - m_2) + m_0(m_2 - m_0) + p_2(s_1(m_1 - m_0) + m_0(m_0 - m_1)), \\ &\quad p_1(s_1(m_1 - m_2) + m_1(m_2 - m_0) + p_2(s_1(m_1 - m_1) + m_1(m_0 - m_1)), \\ &\quad p_1(s_1(m_2 - m_2) + m_2(m_2 - m_0) + p_2(s_1(m_1 - m_2) + m_2(m_0 - m_1)), \\ &\quad p_1(s_1(m_3 - m_2) + m_3(m_2 - m_0) + p_2(s_1(m_1 - m_3) + m_3(m_0 - m_1))). \end{aligned}$$

Moreover, if $p_1 = km_1 + s - m_0$, $p_2 = km_2 + s - m_0$, $p_3 = km_3 + s - m_0$, then the point on eul is

$$((k-1)m_0 + s, (k-1)m_1 + s, (k-1)m_2 + s, (k-1)m_3 + s).$$

In particular,

$$M = (m_1 + m_2 + m_3, m_2 + m_3 + m_0, m_3 + m_0 + m_1, m_0 + m_1 + m_2),$$

$$P = (s_1t_0 - m_0t_0, s_1(m_1^2 - m_2m_3) - m_1t_0, s_1(m_2^2 - m_3m_1) - m_2t_0, \\ s_1(m_3^2 - m_1m_2) - m_3t_0),$$

$$\text{with } t_0 = m_0m_1 + m_0m_2 + m_0m_3 - m_1m_2 - m_3m_1 - m_2m_3,$$

$$\overline{O} = ($$

$$Am = (s_1 - 3m_0, s_1 - 3m_1, s_1 - 3m_2, s_1 - 3m_3),$$

$$G = (s_1 + 2m_0, s_1 + 2m_1, s_1 + 2m_2, s_1 + 2m_3),$$

$$\overline{Am} = ($$

$$D_0 = ($$

$$D_1 = ($$

$$D_2 = ($$

$$G = ($$

$$\overline{G} = ($$

Answer to ??.

Answer (partial).

... ? The polar $pp_0 = [-2m_1m_2, m_2(m_0 + m_1), m_1(m_2 + m_0],$

... ? The intersection $PP_0 = (0, -m_1(m_2 + m_0), m_2(m_0 + m_1)),$

... ? $pp = [m_1m_2(m_2 + m_0)(m_0 + m_1), m_2m_0(m_0 + m_1)(m_1 + m_2), m_0m_1(m_1 + m_2)(m_2 + m_0)].$

Point "O", intersection of perpendicular to faces through their barycenter
(special case of ... with $k = 0$ hence

"O" = $(s_1 - m_0, s_1 - m_1, s_1 - m_2, s_1 - m_3).$

"Conjugate tetrahedron",

"A'" = $(-2s_1 - 2m_0, s_1 + 2m_1, s_1 + 2m_2, s_1 + 2m_3),$

barycenter of faces of $[A'[i]]$ are

"M'" = $(0, m_1, m_2, m_3),$ which are the orthocenters of the faces,

Perpendiculars through M'_0 to the faces, (which are parallel to those of $[A[]]$ meet at

"O'" = $(3s_1 - 4m_0, 3s_1 - 4m_1, 3s_1 - 4m_2, 3s_1 - 4m_3).$

Hence his theorem: Then he generalizes the circle of Brianchon-Poncelet and gives its center as the midpoint of H and "O"

I believe his "O" is my G .

Orthocenter, barycenter and "O" are collinear

Chapter 7

QUATERNIONIAN GEOMETRY

7.0 Introduction.

It is a classical result, (see Artin, Harsthorne) that if the coordinates which are used to define a projective geometry are elements of a non commutative division ring, then Desargues' Theorem is true, but Pappus' Theorem is, in general, not true. More precisely, Pappus' theorem implies that the division ring or skew field is commutative. I will prove here detailed geometric properties which justify the definitions of medians and circumcircular polarity in a quaternionian plane.

The results were conjectured by taking the coordinates in the ring with unity associated with quaternions over the finite field Z_p , p prime. This is not a division ring because a finite division ring is a field. In this geometry, not all points define a line and vice-versa. The situation is similar to that described by Knüppel and Salow, for the case of a commutative ring with unity. This generalization merits to be explored in detail.

In involutive Geometry, we started with the triangle $\{A_i, a_i\}$, the barycenter M and the orthocenter \overline{M} . We constructed the medians ma_i , the altitudes $\overline{m}a_i$, the mid-points M_i , the feet \overline{M}_i , the complementary triangle (M_i, mm_i) , the orthic triangle $\{\overline{M}_i, \overline{m}m_i\}$, the ideal points MA_i , the orthic points $\overline{M}A_i$, the ideal line m , the orthic line \overline{m} , the orthic directions, Imm_i , the tangential triangle $\{T_i, ta_i\}$, the symmedians at_i and the point of Lemoine K . Moreover the same tangential triangle T_i can be obtained if we interchange the role of M and \overline{M} .

I attempted the same construction for the Geometry over the quaternion skew field. In this case, however, the lines at_i are not concurrent, in general, but form a triangle K_i and there exists a polarity in which K_i is the pole of a_i and therefore A_i is the pole of at_i . This polarity degenerates into all the lines through K in the involutive Geometry.

The plane corresponding to the involutive plane is defined by choosing a complete 5-angle in the quaternionian plane. 3 points are the vertices of the basic triangle, 1 is the barycenter, 1 is the cobarycenter. We define the ideal line as the polar of the barycenter with respect to the triangle and as comedians, the lines joining the vertices of the triangle to the cobarycenter. It can be shown that there is a polarity which associates to the vertices of the triangle 3 of the lines through them, corresponding to the tangential lines in Euclidean geometry, but, in

¹22.1.87

general, the involution defined by this polarity on the ideal line, does not have the directions of the sides and the direction of the comedians as corresponding points.

7.1 Quaternionian Geometry over the reals.

7.1.1 Points, Lines and Polarity.

Notation.

Identifiers, starting with a lower case letter, will denote quaternions, \bar{q} denotes the conjugate of q , q' , the conjugate inverse, $q^n := q \bar{q} = \bar{q} q$, $q^{-n} := (q^n)^{-1}$.

Definition.

The elements and incidence in Quaternionian geometry in 2 dimensions are defined as follows.

0. The points are (q_0, q_1, q_2) with right equivalence,

1. The lines are $[l_0, l_1, l_2]$ with right equivalence,

2. A point P is incident to a line l iff

$$P \cdot l := \sum_{i=0}^2 \bar{P}_i l_i = 0.$$

Condition 2 is consistent with equivalence and can also be written

$$l \cdot P = 0.$$

I preferred it, because the usual form $\sum_{i=0}^2 P_i l_i = 0$ implies $\sum_{i=0}^2 \bar{l}_i \bar{P}_i = 0$.

We remind the reader of the following

Theorem.

In any skew field, if a matrix \mathbf{A} has a left inverse and a right inverse, these are equal.

Proof: Let \mathbf{C} be the left inverse of \mathbf{A} and \mathbf{B} be its right inverse, by associativity of matrices,

$$\mathbf{C} = \mathbf{C}(\mathbf{A}\mathbf{B}) = (\mathbf{C}\mathbf{A})\mathbf{B} = \mathbf{B}.$$

Lemma.

$$\begin{aligned} 0. \quad p_i \neq q_i, \quad i = 1, 2 &\implies (1, p_1, p_2) \times (1, q_1, q_2) \\ &= [(p'_1 - q'_1)^{-1}(p'_1 \bar{p}_2 - q'_1 \bar{q}_2)(\bar{p}_2 - \bar{q}_2)^{-1}, (\bar{p}_1 - \bar{q}_1)^{-1}, -(\bar{p}_2 - \bar{q}_2)^{-1}], \end{aligned}$$

$$1. \quad (1, p_1, p_2) \times (1, p_1, q_2) = [\bar{p}_1, -1, 0],$$

$$2. \quad (0, 0, 1) \times (1, p_1, 0) = [\bar{p}_1, -1, 0],$$

$$3. \quad (0, 0, 1) \times (0, 1, 0) = [1, 0, 0].$$

Proof: Let the line be $[x_0, x_1, x_2]$, we must have
 $x_0 + \bar{p}_1 x_1 + \bar{p}_2 x_2 = 0$, and $x_0 + \bar{q}_1 x_1 + \bar{q}_2 x_2 = 0$, subtracting gives
 $(\bar{p}_1 - \bar{q}_1) + x_1(\bar{p}_2 - \bar{q}_2)x_2 = 0$,
hence x_1 and x_2 . x_0 follows from substitution into the second equation.

Theorem.

A quaternionian geometry is a perspective geometry.

Lemma.

Let a_i and b_i be different from 0. The points $P_0 := (0, q_1, r_2)$, $P_1 := (r_0, 0, q_2)$, $P_2 := (q_0, r_1, 0)$ are collinear iff

$$(\bar{q}_2 r'_2)(\bar{q}_1 r'_1)(\bar{q}_0 r'_0) = -1 \text{ and the line is given by any of the triples } [r'_0 \bar{q}_2, q'_1 \bar{r}_2, -1], [-1, r'_1 \bar{q}_0, q'_0 \bar{r}_0]$$

Proof: Let $y := [y_0, y_1, -1] := P_0 \times P_1$, we have
 $\bar{q}_1 y_1 + \bar{r}_2 = 0$ and $\bar{r}_0 y_0 + \bar{q}_2 = 0$, this gives the first form y . To verify that P_2 is on y , we need $q'_0 r'_0 \bar{q}_2 + \bar{r}_1 q'_1 \bar{r}_2 = 0$.

Lemma.

In a quaternionian geometry the Theorem of Desargues is satisfied.

Proof: We can always choose the coordinates of A_i and C as follows

$$A_0 = (1, 0, 0), A_1 = (0, 1, 0), A_2 = (0, 0, 1), C = (1, 1, 1).$$

It follows that

$$a_0 = [1, 0, 0], a_1 = [0, 1, 0], a_2 = [0, 0, 1], \\ c_0 = [0, 1, -1], c_1 = [-1, 0, 1], c_2 = [1, -1, 0],$$

It follows that B_i are

$$B_0 = (q_0, 1, 1), B_1 = (1, q_1, 1), B_2 = (1, 1, q_2),$$

therefore

$$b_0 = [0, \bar{q}_1 - 1, -(\bar{q}_2 - 1)], b_1 = [-(\bar{q}_0 - 1), \bar{q}_2 - 1, 0], \\ b_2 = [\bar{q}_0 - 1, -(\bar{q}_1 - 1), 0], \\ B_0 = (q_0, 1, 1), B_1 = (1, q_1, 1), B_2 = (1, 1, q_2), \\ C_0 = (0, q_1 - 1, q_2 - 1), C_1 = (q_0 - 1, q_2 - 1, 0), \\ C_2 = (q_0 - 1, q_1 - 1, 0),$$

the Theorem follows from Lemma 7.1.1.

Theorem.

A quaternionian geometry is a Desarguesian geometry.

Notation.

To give an explicit way of indicating that a 3 by 3 matrix is a point or line collineation or a correlation from points to lines or from lines to point a parenthesis is used on the side of the point and a bracket on the side of a line. This notation is used when we give the

table of elements. It could also be used in connection with the bold face letter representing collineation or correlation. This notation is only useful when we apply algebra to geometry.

Theorem.

If \mathbf{C} is a point collineation, the line collineation is \mathbf{C}'^T .

In particular, the point collineation which associates to A_i , A_i and to $(1, 1, 1)$, (q_0, q_1, q_2) is

$$\begin{pmatrix} q_0 & 0 & 0 \\ 0 & q_1 & 0 \\ 0 & 0 & q_2 \end{pmatrix},$$

and the line collineation is

$$\begin{bmatrix} q'_0 & 0 & 0 \\ 0 & q'_1 & 0 \\ 0 & 0 & q'_2 \end{bmatrix}.$$

Proof: If Q is the image of P , and m is the image of l , we want

$$0 = P \cdot l = \Sigma \bar{P}_i l_i = \Sigma \bar{\mathbf{C}}_{ij}^{-1} Q_j l_i = \Sigma \bar{Q}_j \mathbf{C}'_{ij} l_i = \Sigma \bar{Q}_j m_j = 0,$$

for all points P and incident lines l . This requires

$$m_j = \Sigma \mathbf{C}_{ji}'^T l_i.$$

Definition. 2

A Hermitian matrix \mathbf{M} is a matrix which is equal to its conjugate transpose.

\mathbf{M} defines a transformation from points to line,

\mathbf{M}^{-1} , the inverse, defines the transformation from lines to points.

Theorem.

If \mathbf{M} is Hermitian and $p = \mathbf{M}P$, $q = \mathbf{M}Q$ and $P \cdot q = 0$ then $Q \cdot p = 0$.

$$\begin{aligned} \text{Proof: } Q \cdot p &= \sum_i \bar{Q}_i p_i \\ &= \sum_i \sum_j \bar{Q}_i M_{i,j} P_j \\ &= \sum_j \sum_i (\bar{Q}_i \overline{M_{j,i}}) P_j \\ &= \sum_j \sum_i \overline{(M_{j,i} Q_i)} P_j \\ &= \sum_j \bar{q}_j P_j = q \cdot P = 0. \end{aligned}$$

Theorem.

0. The transformation defined by a Hermitian matrix is a polarity.

1. The columns of a polarity \mathbf{M} are the polars of the points A_i , with $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$.

2. The columns of an inverse polarity \mathbf{M}^{-1} are the poles of the lines a_i , with $a_0 = [1, 0, 0]$, $a_1 = [0, 1, 0]$, $a_2 = [0, 0, 1]$.

Definition.

Polar points are points incident to their polar. Polar lines are lines incident to their pole.

Comment.

A polar line can contain infinitely many polar points. For instance, let the polarity be $\begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}$. $P := (0, 1, 1)$, has for polar $p = [1, 0, 0]$. A point $Q := (0, 1, q)$, on p has for polar $[1 + q, q, 1]$. Q is a polar point if $\Re(q) = 0$. Therefore all the points $(0, 1, a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})$ are polar points on $[1, 0, 0]$.

Lemma.

Let

$$c_i := q_{i-1}q_iq_{i+1} + \bar{q}_{i+1}\bar{q}_i\bar{q}_{i-1} = 2\operatorname{Re}(q_{i-1}q_iq_{i+1}),$$

if $q_i\bar{q}_i \neq 0$ then

$$c_0 = c_1 = c_2$$

and we define

$$c := c_0.$$

Proof:

$$\begin{aligned} \bar{q}_2q_2c_0 &= \bar{q}_2c_0q_2 = \bar{q}_2(q_2q_0q_1 + \bar{q}_1\bar{q}_0\bar{q}_2)q_2 = \bar{q}_2q_2(q_0q_1q_2) + (\bar{q}_2\bar{q}_1\bar{q}_0)\bar{q}_2q_2 \\ &= \bar{q}_2q_2(q_0q_1q_2 + \bar{q}_2\bar{q}_1\bar{q}_0) = \bar{q}_2q_2c_1. \end{aligned}$$

Theorem.

Let

$$a_i = \bar{a}_i,$$

$$b_i := a_{i+1}a_{i-1} - q_i\bar{q}_i,$$

$$r_i := \bar{q}_{i-1}\bar{q}_{i+1} - a_iq_i,$$

then

$$\begin{pmatrix} a_0 & q_2 & \bar{q}_1 \\ \bar{q}_2 & a_1 & q_0 \\ q_1 & \bar{q}_0 & a_2 \end{pmatrix} \begin{pmatrix} b_0 & r_2 & \bar{r}_1 \\ \bar{r}_2 & b_1 & r_0 \\ r_1 & \bar{r}_0 & b_2 \end{pmatrix} = d \mathbf{E},$$

where \mathbf{E} is the identity matrix and

$$d := a_0a_1a_2 - a_0q_0\bar{q}_0 - a_1q_1\bar{q}_1 - a_2q_2\bar{q}_2 + 2\operatorname{Re}(q_2q_0q_1).$$

Moreover,

$$b_i = \bar{b}_i,$$

$$a_i := b_{i+1}b_{i-1} - r_i\bar{r}_i,$$

$$q_i := \bar{r}_{i-1}\bar{r}_{i+1} - b_ir_i,$$

Proof: For instance,

$$a_0b_0 + q_2\bar{r}_2 + \bar{q}_1r_1 = a_0a_1a_2 - a_0q_0\bar{q}_0 + q_2q_0q_1 - q_2a_2\bar{q}_2 + \bar{q}_1\bar{q}_0\bar{q}_2 - \bar{q}_1a_1q_1 = d$$

and

$$a_0r_2 + q_2b_1 + \bar{q}_1\bar{r}_0 = a_0\bar{q}_1\bar{q}_0 - a_0a_2q_2 + q_2a_2a_0 - q_2q_1\bar{q}_1 + \bar{q}_1q_1q_2 - \bar{q}_1a_0\bar{q}_0 = 0.$$

The second part of the proof is obtained similarly or follows from 7.1.1.1.

The 2 parts of the following Lemma use different approaches to the problem of constructing polarities.

Lemma.

0. If all the components of the lines x_i are non zero and the i -th component of x_i is real, necessary and sufficient conditions for x_i to be polars of A_i are

$$0. \ x_{i+1,i-1}^{-1} \bar{x}_{i-1,i+1} = k_i, \ k_i \text{ real.}$$

$$1. \ k_0 k_1 k_2 = 1.$$

1. Let 3 points have coordinates

$$P_0 = (a_0, q_2, q_1^{-1}), \ P_1 = (q_2^{-1}, a_1, q_0), \ P_2 = (q_1, q_0^{-1}, a_2),$$

where $a_i = \bar{a}_i$, then, if the norm of $q_0 q_1 q_2 = 1$ and if the matrix \mathbf{P} is obtained by multiplying the column vectors P_i respectively by 1, q_2^n , $\frac{1}{q_1^n}$, this matrix defines a polarity which associates the lines a_i to the points P_i .

Proof: For part 0, the condition that the i -th component of x_i is real can always be satisfied by multiplying the components of x_i by \bar{x}_{ii} .

It remains to find real numbers which multiplied by x_i give the columns of an Hermitian matrix. Considering the elements x_{01} and x_{10} requires $\bar{x}_{10} = x_{01} k_2$, k_2 real, or more generally

0. Multiplying the first and second column by k_1 and k_1^{-1} requires condition 1, for the elements in position 12 and 21 to be conjugates of each other.

For the second part, the matrix is then

$$\begin{pmatrix} a_0 & \bar{q}_2 & q'_1 \\ q_2 & q_2^n a_1 & q_2^n \bar{q}_0 \\ q_1^{-1} & q_2^n q_0 & q_1^{-n} a_2 \end{pmatrix}.$$

Exercise.

State and prove the Theorem which extends the preceding Theorem to the case where some of the components of the vectors x_i are 0, or some of the q_i are 0.

Lemma. 3

$$u_j^n \neq 0, \ v_j^n \neq 0, \ j = 1, 2, \text{ and } d_0 := u_1 u_2^{-1} + v_1 v_2^{-1}, \ e_0 := u_2 u_1^{-1} + v_2 v_1^{-1},$$

$$\Rightarrow u_1^{-1} d_0 v_2 = u_2^{-1} e_0 v_1 \text{ and}$$

$$d_0^n v_2^n u_2^n = e_0^n v_1^n u_1^n.$$

$$\text{Proof: } u_1^{-1} d_0 v_2 = u_2^{-1} v_2 + u_1^{-1} v_1 \text{ and } u_2^{-1} e_0 v_1 = u_1^{-1} v_1 + u_2^{-1} v_2.$$

Lemma.

$$(u_0 u_1 u_2 v_0 v_1 v_2)^n \neq 0,$$

$$d_i := u_{i+1} u_{i-1}^{-1} + v_{i+1} v_{i-1}^{-1}, \ d := d_0 d_1 d_2,$$

$$e_i := u_{i-1}u_{i+1}^{-1} + v_{i-1}v_{i+1}^{-1}, \quad e := e_0e_1e_2, \\ \Rightarrow d^n = e^n.$$

Proof: This follows from Lemma 7.1.1, taking norms and using the fact that the norm of a product is the product of the norms.

7.1.2 Quaternionian Geometry of the Hexal Complete 5-Angles.

Notation.

In what follows, I will use the same notation as in involutive Geometry, namely,

$l := P \times Q$, means that the line l is defined as the line incident to P and Q .

If subscripts are used these have the values 0, 1 and 2 and the computation is done modulo 3,

$P \cdot l = 0$ means that the point P is incident to the line l .

When 3 lines intersect, this intersection can be defined in 3 ways, this has been indicated by using () after the definition and implies a Theorem.*

$$\sigma := \text{polarity}((M_i, a_i)).$$

implies that σ is the polarity which associates M_0 to a_0 , M_1 to a_1 and M_2 to a_2 .

$$m = \text{polar}(\sigma, M).$$

implies that in the polarity σ , m is the polar of M .

The labeling used is “H,” for Hypothesis, “D”, for definitions, “C”, for conclusions, “N”, for nomenclature, “P”, for proofs, this labelling being consistent with that of the corresponding definitions. The example given is associated to the quaternions over Z_{19} , the labelling is “E” and is consistent with the corresponding definitions.

Because any 3 pairs of points and lines do not necessarily define a polarity, if a polarity is defined it implies a conclusion (or Theorem) I have therefore replaced “D” by “DC”.

The special configuration of Desargues.

With this notation, the special configuration of Desargues can be defined by

$$a_i := A_{i+1} \times A_{i-1}, \quad qa_i = Q \times A_i, \\ Q_i := a_i \times qa_i, \quad qq_i := Q_{i+1} \times Q_{i-1}, \\ QA_i := a_i \times qq_i, \quad q_i := A_i \times QA_i, \\ QQ_i := q_{i+1} \times q_{i-1}, \quad q := QA_1 \times QA_2(*),$$

and the other conclusion of the special Desargues Theorem can be written,

$$QQ_i \cdot qa_i = 0.$$

Let Q and A_i be

$$Q = (q_0, q_1, q_2), \quad \text{and } A_0 = (1, 0, 0), \quad A_1 = (0, 1, 0), \quad A_2 = (0, 0, 1),$$

then we have the following results, not obtained in the given order,

$$A_0 = (1, 0, 0), \quad a_0 = [1, 0, 0], \\ Q = (q_0, q_1, q_2), \quad q = [q'_0, q'_1, q'_2], \\ QA_0 = (0, q_1, -q_2), \quad qa_0 = [0, q'_1, -q'_2], \\ Q_0 = (0, q_1, q_2), \quad q_0 = [0, q'_1, q'_2], \\ QQ_0 = (-q_0, q_1, q_2), \quad qq_0 = [-q'_0, q'_1, q'_2],$$

The self duality of the configuration corresponds to the replacement of points by lines

where upper case letters are replaced by lower case letters and coordinates by their conjugate inverse.

Fundamental Hypothesis, Definitions and Conclusions.

The ideal line and the coideal line.

Given

H0.0. A_i ,

H0.1. M, \overline{M} ,

Let

D1.0. $a_i := A_{i+1} \times A_{i-1}$,

D1.1. $ma_i := M \times A_i, \overline{ma}_i := \overline{M} \times A_i$,

D1.2. $\overline{M}_i := ma_i \times a_i, \overline{M}_i := \overline{ma}_i \times a_i$,

D1.3. $eul = M \times \overline{M}$,

DC1.4. $\sigma := \text{polarity}((M_i, a_i)), \overline{\sigma} := \text{polarity}((\overline{M}_i, a_i))$,

D2.0. $mm_i := M_{i+1} \times M_{i-1}, \overline{mm}_i := \overline{M}_{i+1} \times \overline{M}_{i-1}$,

D2.1. $MA_i := a_i \times mm_i, \overline{MA}_i := a_i \times \overline{mm}_i$,

D2.2. $m_i := A_i \times MA_i, \overline{m}_i := A_i \times \overline{MA}_i$,

D2.3. $MM_i := m_{i+1} \times m_{i-1}, \overline{MM}_i := \overline{m}_{i+1} \times \overline{m}_{i-1}$,

D2.4. $m := MA_1 \times MA_2 (*), \overline{m} := \overline{MA}_1 \times \overline{MA}_2 (*)$,

D2.5. $Ima_i := m \times ma_i, \overline{Ima}_i := \overline{m} \times \overline{ma}_i$,

D2.6. $IMa_i := m \times \overline{ma}_i, \overline{IMa}_i := \overline{m} \times ma_i$,

D2.7. $iMA_i := M \times MA_i, \overline{iMA}_i := \overline{M} \times \overline{MA}_i$,

then

C2.0. $m = \text{polar}(\sigma, M), \overline{m} = \text{polar}(\overline{\sigma}, \overline{M})$.

C2.1. $mm_i = \text{polar}(\sigma, A_i), \overline{mm}_i = \text{polar}(\overline{\sigma}, A_i)$.

C2.2. $ma_i = \text{polar}(\sigma, MA_i), \overline{ma}_i = \text{polar}(\overline{\sigma}, \overline{MA}_i)$.

C2.3. $iMA_i = \text{polar}(\sigma, Ima_i), \overline{iMA}_i = \text{polar}(\overline{\sigma}, \overline{Ima}_i)$.

Let

D3.0. $mf_i := M_i \times Ima_i, \overline{mf}_i := \overline{M}_i \times \overline{Ima}_i$,

D3.1. $O := mf_1 \times mf_2(*), \overline{O} := \overline{mf}_1 \times \overline{mf}_2(*)$,

D3.2. $Mfa_i := a_{i+1} \times mf_{i-1}, \overline{Mfa}_i := a_{i+1} \times \overline{mf}_{i-1}$,

$Mf\overline{a}_i := a_{i-1} \times mf_{i+1}, \overline{Mf}\overline{a}_i := a_{i-1} \times \overline{mf}_{i+1}$,

D3.3. $mfa_i := Mfa_{i+1} \times A_{i-1}, \overline{mfa}_i := \overline{Mfa}_{i+1} \times A_{i-1}$,

$m\overline{f}\overline{a}_i := Mf\overline{a}_{i-1} \times A_{i+1}, \overline{m}\overline{f}\overline{a}_i := \overline{Mf}\overline{a}_{i-1} \times A_{i+1}$,

D3.4. $Mfm_i := mfa_i \times m_i, \overline{Mfm}_i := \overline{mfa}_i \times \overline{m}_i$,

then

C3.0. $O \cdot eul = \overline{O} \cdot eul = 0$.

C3.1. $Mfm_i \cdot m\overline{f}\overline{a}_i = \overline{Mfm}_i \cdot \overline{m}\overline{f}\overline{a}_i = 0$.

Let

D4.0. $Imm_i := m \times \overline{mm}_i, \overline{Imm}_i := \overline{m} \times mm_i$,

D4.1. $ta_i := A_i \times Imm_i$,

D4.2. $T_i := ta_{i+1} \times ta_{i-1}$,

D4.3. $at_i := A_i \times T_i$,

D4.4. $K_i := at_{i+1} \times at_{i-1}$,

D4.5. $T A a_i := t a_i \times a_i$,

D4.6. $p o K_i := T a a_{i+1} \times T a a_{i-1}$,

DC4.7. $\theta := \text{polarity}((A_i, t a_i))$,

DC4.8. $\lambda := \text{polarity}((A_i, a t_i))$,

then

C4.0. $\bar{I} m m_i \cdot t a_i = 0$.

C4.1. $T_i \cdot m f_i = 0$.

C4.2. $a_i := \text{polar}(\theta, T_i)$.

C4.3. $a_i := \text{polar}(\lambda, K_i)$.

The nomenclature:

N0.0. A_i are the vertices of the triangle,

N0.1. M is the barycenter, \bar{M} is the cobarycenter.

N1.0. a_i are the sides.

N1.1. $m a_i$ are the medians, $\bar{m} a_i$ are the comedians

N1.2. M_i are the mid-points of the sides. \bar{M}_i are the feet of the comedians

N1.3. eul is the line of Euler,

N1.4. σ is the Steiner polarity. $\bar{\sigma}$ is the co-Steiner polarity.

N2.0. $\{M_i, m m_i\}$ is the complementary triangle,

$\{\bar{M}_i, \bar{m} m_i\}$ is the orthic triangle,

N2.1. $M A_i$ are the directions of the sides,

N2.2. $\{M M_i, m_i\}$ is the anticomplementary triangle.

N2.3. m is the ideal line corresponding to the line at infinity,

\bar{m} is the orthic line which is the polar of \bar{M} with respect to the triangle.

N2.4. $I m a_i$ are the directions of the medians.

$I M a_i$ are the directions of the comedians.

N3.0. $m f_i$ are the mediatrices,

N3.1. O is the center,

N3.2. $M f m_i$ are the trapezoidal points,

N4.0. $I m m_i$ are the directions of the antiparallels of a_i with respect to the sides a_{i+1} and a_{i-1} .

N4.1. $(T_i, t a_i)$ is the tangential triangle,

N4.2. $a t_i$ are the symmedians,

N4.3. K_i is the triangle of Lemoine.

N4.4. θ is the circumcircular polarity

N4.5. λ is the Lemoine polarity.

Theorem.

If we derive a point X and a line x by a given construction from A_i , M and \bar{M} , with the coordinates as given in G0.0 and G0.1, below, and the point \bar{X} and line \bar{x} are obtain by the same construction interchange M and \bar{M} ,

$$X = (f_0(m_0, m_1, m_2), f_1(m_0, m_1, m_2), f_2(m_0, m_1, m_2)),$$

$$x = [g_0(m_0, m_1, m_2), g_1(m_0, m_1, m_2), g_2(m_0, m_1, m_2)],$$

\implies

$$\bar{X} = (m_0 f_0(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_1 f_1(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_2 f_2(m_0^{-1}, m_1^{-1}, m_2^{-1})),$$

$$\bar{x} = [m'_0 g_0(m_0^{-1}, m_1^{-1}, m_2^{-1}), m'_1 g_1(m_0^{-1}, m_1^{-1}, m_2^{-1}), m'_2 g_2(m_0^{-1}, m_1^{-1}, m_2^{-1})].$$

Proof: The point collineation $\mathbf{C} = \begin{pmatrix} q_0 & 0 & 0 \\ 0 & q_1 & 0 \\ 0 & 0 & q_2 \end{pmatrix}$, associates to $(1, 1, 1)$, (q_0, q_1, q_2) , and

to (m_0, m_1, m_2) , (r_0, r_1, r_2) , if $r_i = q_i m_i$.

In the new system of coordinates,

$$X = (q_0 f_0(q_0^{-1} r_0, q_1^{-1} r_1, q_2^{-1} r_2), q_1 f_1(q_0^{-1} r_0, q_1^{-1} r_1, q_2^{-1} r_2), q_2 f_2(q_0^{-1} r_0, q_1^{-1} r_1, q_2^{-1} r_2)).$$

Exchanging q_i and r_i and then replacing q_i by 1 and r_i by m_i is equivalent to substituting m_i for q_i and 1 for r_i , which gives \bar{X} . \bar{x} is obtained similarly.

The line collineation is

$$\begin{bmatrix} q'_0 & 0 & 0 \\ 0 & q'_1 & 0 \\ 0 & 0 & q'_2 \end{bmatrix}.$$

Exercise.

Prove that if a point to line polarity $[\mathbf{P}]$ has its i, j -th element

$$\mathbf{P}_{ij} = f(m_0, m_1, m_2),$$

then the i, j -th element of the polarity obtained by the same construction, after exchange of M and \bar{M} , is

$$\bar{\mathbf{P}}_{ij} = m'_i f(m_0^{-1}, m_1^{-1}, m_2^{-1}) m_j^{-1}.$$

Similarly, for a line to point polarity (\mathbf{P}^{-1})

$$(\mathbf{P}^{-1})_{ij} = g(m_0, m_1, m_2), \implies (\bar{\mathbf{P}}^{-1})_{ij} = m_i g(m_0^{-1}, m_1^{-1}, m_2^{-1}) \bar{m}_j.$$

Lemma.

$$m_1^{-1}(m_0 + m_1)(m_0 - m_1)^{-1} = -(m_0^{-1} + m_1^{-1})(m_0^{-1} - m_1^{-1})^{-1} m_1^{-1}.$$

This Lemma is useful in checking equivalent representations of coordinates of points and lines.

Notation.

$$\begin{aligned} r_i &:= (m_{i-1}^{-1} + m_i^{-1})^{-1} (m_{i+1}^{-1} - m_{i-1}^{-1}), \\ s_i &:= -(m_{i-1}^{-1} + m_i^{-1})^{-1} (m_i^{-1} + m_{i+1}^{-1}), \\ t_i &:= s_{i+1}^{-1} s_{i-1}^{-1}, \\ f_i &:= s_i - s_{i+1}^{-1} s_{i-1}^{-1}, \\ g_i &:= t_i - t_{i+1}^{-1} t_{i-1}^{-1}. \end{aligned}$$

Lemma.

$$0. \ s_0 s_1 s_2 = -1.$$

$$1. \ \text{norm}(t_0 t_1 t_2) = 1.$$

$$2. \ s'_2 \bar{f}_2 s_0^{-1} = -f_2 s_1.$$

$$3. \ t'_2 \bar{f}_2 t_0^{-1} = -f_2 t_1.$$

Proof: For 0, we use Lemma 7.1.1 and obtain 1, from the definition of t_i . For 2, we substitute f_2 by its definition and compare the terms of both sides of the equality which have the same sign.

Proof of 7.1.2.

Let

$$G0.0. A_0 = (1, 0, 0), A_1 = (0, 1, 0), A_2 = (0, 0, 1),$$

$$G0.1. M = (1, 1, 1), \bar{M} = (m_0, m_1, m_2),$$

then

$$P1.0. a_0 = (1, 0, 0), a_1 = (0, 1, 0), a_2 = (0, 0, 1),$$

$$P1.1. ma_0 = [0, 1, -1], \bar{m}a_0 = [0, m'_1, -m'_2],$$

$$P1.2. M_0 = (0, 1, 1), \bar{M}_0 = (0, m_1, m_2),$$

$$P1.3. eul = [1, (\bar{m}_1 - \bar{m}_2)^{-1}(\bar{m}_2 - \bar{m}_0), (\bar{m}_1 - \bar{m}_2)^{-1}(\bar{m}_0 - \bar{m}_1)],$$

$$P1.4. \mathbf{S} = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{pmatrix}, \mathbf{S}^{-1} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

$$\bar{\mathbf{S}} = \begin{pmatrix} m_0^{-n} & -m'_0 m_1^{-1} & -m'_0 m_2^{-1} \\ -m'_1 m_0^{-1} & m_1^{-n} & -m'_1 m_2^{-1} \\ -m'_2 m_0^{-1} & -m'_2 m_1^{-1} & m_2^{-n} \end{pmatrix},$$

$$\bar{\mathbf{S}}^{-1} = \begin{pmatrix} 0 & m_0 \bar{m}_1 & m_0 \bar{m}_2 \\ m_1 \bar{m}_0 & 0 & m_1 \bar{m}_2 \\ m_2 \bar{m}_0 & m_2 \bar{m}_1 & 0 \end{pmatrix}.$$

$$P2.0. mm_0 = [1, -1, -1], \bar{m}m_0 = [m'_0, -m'_1, -m'_2],$$

$$P2.1. MA_0 = (0, 1, -1), \bar{M}A_0 = (0, m_1, -m_2),$$

$$P2.2. m_0 = [0, 1, 1], \bar{m}_0 = [0, m'_1, m'_2],$$

$$P2.3. MM_0 = (1, -1, -1), \bar{M}M_0 = (m_0, -m_1, -m_2),$$

$$P2.4. m = [1, 1, 1], \bar{m} = [m'_0, m'_1, m'_2],$$

$$P2.5. Ima_0 = (2, -1, -1), \bar{I}ma_0 = (2m_0, -m_1, -m_2),$$

$$P2.6. IMA_0 = (m_1 + m_2, -m_1, -m_2), \bar{I}MA_0 = (m_0(m_1^{-1} + m_2^{-1}), -1, -1),$$

$$P2.7. iMA_0 = [2, -1, -1], \bar{i}MA_0 = [2m'_0, -m'_1, -m'_2],$$

$$P3.0. mf_0 = [(m_1 + m_2)'(\bar{m}_1 - \bar{m}_2), 1, -1],$$

$$\bar{m}f_0 = [m'_0(m_1^{-1} + m_2^{-1})'(m'_1 - m'_2), m'_1, -m'_2, 1],$$

$$P3.1. O = (m_1 + m_2, m_2 + m_0, m_0, m_1),$$

$$\bar{O} = (m_0(m_1^{-1} + m_2^{-1}), m_1(m_2^{-1} + m_0^{-1}), m_2(m_0^{-1} + m_1^{-1})),$$

$$P3.2. Mfa_0 = (1, 0, -(m_0 + m_1)(m_0 - m_1)^{-1}),$$

$$\bar{M}fa_0 = (m_0, 0, -m_2(m_0^{-1} + m_1^{-1})(m_0^{-1} - m_1^{-1})^{-1}),$$

$$\bar{M}f\bar{a}_0 = (1, m'_2(m_2 + m_0)(m_2 - m_0)^{-1}, 0),$$

$$\bar{M}f\bar{a}_0 = (m_0, m_1(m_2^{-1} + m_0^{-1})(m_2^{-1} - m_0^{-1})^{-1}, 0),$$

$$P3.3. mfa_0 = [(m_1 + m_2)'(\bar{m}_1 - \bar{m}_2), 1, 0],$$

$$\bar{m}fa_0 = [m'_0(m_1^{-1} + m_2^{-1})'(m'_1 - m'_2), m'_1, 0],$$

$$mf\bar{a}_0 = [(m_1 + m_2)'(\bar{m}_1 - \bar{m}_2), 0, -1],$$

$$\bar{m}f\bar{a}_0 = [m'_0(m_1^{-1} + m_2^{-1})'(m'_1 - m'_2), 0, -m'_2],$$

$$P3.4. Mfm_0 = ((m_1 + m_2)(m_1 - m_2)^{-1}, -1, 1),$$

$$\bar{M}fm_0 = (m_0(m_1^{-1} + m_2^{-1})(m_1^{-1} - m_2^{-1})^{-1}, -m_1, m_2),$$

$$P4.0. \text{Imm}_0 = (r_0, 1, s_0), \bar{\text{Imm}}_0 = (-r_0, 1, s_0),$$

$$P4.1. \text{ta}_0 = [0, 1, -s'_0],$$

$$P4.2. T_0 = (1, s_2, s_1^{-1}),$$

$$P4.3. \text{at}_0 = [0, s'_2, -\bar{s}_1] = [0, 1, -t'_0],$$

$$P4.4. K_0 = (1, t_2, t_1^{-1}),$$

$$P4.5. \text{Taa}_0 = (0, 1, s_0),$$

$$P4.6. \text{poK}_0 = [-1, s'_2, \bar{s}_1],$$

$$P4.7. \mathbf{T} = \begin{pmatrix} 0 & \bar{f}_2 & -\bar{f}_2 s_0^{-1} \\ f_2 & 0 & -f_2 s_1 \\ -s'_0 f_2 & -\bar{s}_1 \bar{f}_2 & 0 \end{pmatrix}, \mathbf{T}^{-1} = \begin{pmatrix} 1 & \bar{s}_2 & s'_1 \\ s_2 & s_2^n & s_2^n \bar{s}_0 \\ s_1^{-1} & s_2^n s_0 & s_1^{-n} \end{pmatrix}.$$

$$P4.8. \mathbf{L} = \begin{pmatrix} 0 & \bar{g}_2 & -\bar{g}_2 t_0^{-1} \\ g_2 & 0 & -g_2 t_1 \\ -t'_0 g_2 & -\bar{t}_1 \bar{g}_2 & 0 \end{pmatrix}, \mathbf{L}^{-1} = \begin{pmatrix} 1 & \bar{t}_2 & t'_1 \\ t_2 & t_2^n & t_2^n \bar{t}_0 \\ t_1 & t_1^{-n} t'_0 & t_1^{-n} \end{pmatrix}.$$

Details of proof:

For P4.0, if the coordinates of Imm_0 are x_0 , 1 and x_2 , we have to solve

$$\begin{aligned} x_0 + 1 + x_2 &= 0, \\ -m_0^{-1}x_0 + m_1^{-1} + m_2^{-1}x_2 &= 0. \end{aligned}$$

Multiplying the equations to the left respectively by m_2^{-1} and -1 , or by m_0^{-1} and 1 and adding gives x_0 and x_2 using the notation 7.1.2.

For P4.7, it is easier to obtain \mathbf{T}^{-1} first, the columns are T_0, T_1, T_2 , multiplied to the right by $1, s_2^n, s_1^{-n}$. The matrix \mathbf{T} is then obtained using Theorem 7.1.1, multiplying by $-s_1^{-n}$. The equivalence with the matrix whose columns are ta_i can be verified using Lemma 7.1.2.2. A similar proof gives P4.8. It is trivialize by the notationb used for t .

Theorem.

The product of the diagonal elements of \mathbf{T}^{-1} and of \mathbf{L}^{-1} is the same.

This follows from Lemma 7.1.1.

Exercise.

Prove that the center of the circumcircular polarity is

$$(m'_0(m_1^{-1} + m_2^{-1}), m'_1(m_2^{-1} + m_0^{-1}), m'_2(m_0^{-1} + m_1^{-1})).$$

Therefore, in general, it is distinct from O . From this follows, that, in general, mf_i is not the polar of MA_i in the circumcircular polarity.

7.2 Finite Quaternionian Geometry.

7.2.1 Finite Quaternions.

Definition.

Finite Quaternions over Z_p are associative elements of the form

$$q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k},$$

where q_i are elements of Z_p and $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are such that

$$\mathbf{i}^2 = \mathbf{j}^2 = -1 \text{ and } \mathbf{k} = \mathbf{ij} = -\mathbf{ji}.$$

Theorem.

$\mathbf{i}, \mathbf{j}, \mathbf{k}$ satisfy

$$\mathbf{k}^2 = -1, \mathbf{i} = \mathbf{jk} = -\mathbf{kj}, \mathbf{j} = \mathbf{ki} = -\mathbf{ik}.$$

This follows at once from associativity.

Theorem.

Finite quaternions in Z_p can be represented by 2 by 2 matrices over Z_p .

In particular, if $j_0^2 + j_1^2 = -1$, then we can represent

$$1 \text{ by } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} \text{ by } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{j} \text{ by } \begin{pmatrix} j_0 & j_1 \\ j_1 & -j_0 \end{pmatrix}, \mathbf{k} \text{ by } \begin{pmatrix} j_1 & -j_0 \\ -j_0 & -j_1 \end{pmatrix}.$$

Comment.

If $p \equiv 1 \pmod{4}$, we can find an interger j_0 such that $j_0^2 = -1$, and choose $j_1 = 0$.

Example.

0. $p = 5$, we can represent

$$1 \text{ by } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} \text{ by } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{j} \text{ by } \begin{pmatrix} 2 & 0 \\ 0 & -2 \end{pmatrix}, \mathbf{k} \text{ by } \begin{pmatrix} 0 & -2 \\ -2 & 0 \end{pmatrix}.$$

1. $p = 7$, we can represent

$$1 \text{ by } \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} \text{ by } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{j} \text{ by } \begin{pmatrix} -3 & 2 \\ 2 & 3 \end{pmatrix}, \mathbf{k} \text{ by } \begin{pmatrix} 2 & 3 \\ 3 & -2 \end{pmatrix}.$$

Finite quaternions will be represented by an integer using the following notation.

Notation.

In the example the quaternion over Z_p ,

$$q = q_0 + q_1\mathbf{i} + q_2\mathbf{j} + q_3\mathbf{k}$$

is represented by

$$q = q_0 + q_1p + q_2p^2 + q_3p^3, 0 \leq q_i < p.$$

For instance, when $p = 19$, the representation of $18 + 3\mathbf{i} + 6\mathbf{j}$ is 2222, of $11 + 10\mathbf{i} + 4\mathbf{j} + 3\mathbf{k}$ is 22222, of $16 + 8\mathbf{i} + 18\mathbf{j}$ is 6666 and of $14 + 12\mathbf{i} + 13\mathbf{j} + 9\mathbf{k}$ is 66666.

7.2.2 Example in a finite quaternionian geometry.

Let $p = 19$,

$G0.0.$ $A_0 = (1, 0, 0)$, $A_1 = (0, 1, 0)$, $A_2 = (0, 0, 1)$,

$G0.1.$ $M = (1, 2222, 22222)$, $\overline{M} = (1, 6666, 66666)$,

then

$E1.0.$ $a_0 = [1, 0, 0]$, $a_1 = [0, 1, 0]$, $a_2 = [0, 0, 1]$,

$E1.1.$ $ma_i = [0, 1, 13827]$, $[22219, 0, 1]$, $[1, 6378, 0]$,

$\overline{m}a_i = [0, 1, 41987]$, $[66657, 0, 1]$, $[1, 3333, 0]$,

$E1.2.$ $M_i = (0, 1, 48176)$, $(22219, 0, 1)$, $(1, 2222, 0)$,

$\overline{M}_i = (0, 1, 21174)$, $(70903, 0, 1)$, $(1, 6666, 0)$,

$E1.3.$ $eul = [1, 35222, 126587]$,

$E1.4$ $\mathbf{S} = \begin{pmatrix} 1 & 868 & 115341 \\ 6378 & 13 & 82528 \\ 22222 & 48176 & 18 \end{pmatrix}$, $\mathbf{S}^{-1} = \begin{pmatrix} 0 & 5034 & 115341 \\ 2222 & 0 & 116883 \\ 22222 & 13827 & 0 \end{pmatrix}$,

$\overline{\mathbf{S}} = \begin{pmatrix} 1 & 1835 & 33434 \\ 5407 & 14 & 88952 \\ 104133 & 48615 & 11 \end{pmatrix}$, $\overline{\mathbf{S}}^{-1} = \begin{pmatrix} 0 & 443 & 69658 \\ 6789 & 0 & 92894 \\ 67891 & 44653 & 0 \end{pmatrix}$,

$E2.0.$ $mm_i = [1, 6378, 22222]$, $[2205, 1, 13827]$, $[22219, 48173, 1]$,

$\overline{m}m_i = [1, 3333, 70894]$, $[6653, 1, 41987]$, $[66657, 21177, 1]$,

$E2.1.$ $MA_i = (0, 1, 82525)$, $(115341, 0, 1)$, $(1, 5017, 0)$,

$\overline{M}A_i = (0, 1, 116386)$, $(66657, 0, 1)$, $(1, 573, 0)$,

$E2.2.$ $m_i = [0, 1, 116874]$, $[115341, 0, 1]$, $[1, 861, 0]$,

$\overline{m}_i = [0, 1, 95573]$, $[70903, 0, 1]$, $[1, 3906, 0]$,

$E2.3.$ $MM_i = (1, 5017, 115338)$, $(868, 1, 82525)$, $(115341, 116883, 1)$,

$\overline{M}M_i = (1, 573, 70894)$, $(3903, 1, 116386)$, $(66657, 95586, 1)$,

$E2.4.$ $m = [1, 861, 115338]$, $\overline{m} = [1, 3906, 66666]$,

$E2.5.$ $Ima_i = (1, 6128, 61279)$, $(624, 1, 41443)$, $(61290, 123602, 1)$,

$\overline{I}ma_i = (1, 3906, 35637)$, $(2132, 1, 58383)$, $(101928, 116383, 1)$,

$E2.6.$ $IMa_i = (1, 31398, 82872)$, $(70470, 1, 745)$, $(35569, 2751, 1)$,

$\overline{I}Ma_i = (1, 84862, 112419)$, $(112219, 1, 114203)$, $(4535, 17280, 1)$,

$E2.7.$ $iMA_i = [2, 6378, 22222]$, $[2205, 2, 13827]$, $[22219, 48173, 2]$,

$\overline{i}MA_i = [2, 3333, 70894]$, $[6653, 2, 41987]$, $[66657, 21177, 2]$,

$E3.0.$ $mf_i = [1, 57399, 96485]$, $(22698, 1, 119282)$, $(59539, 116028, 1)$,

$\overline{m}f_i = [1, 17052, 63592]$, $(87814, 1, 43860)$, $(49067, 45624, 1)$,

$E3.1.$ $O = (1, 39571, 2622)$, $\overline{O} = (1, 26376, 18393)$.

$E3.2.$ $Mfa_i = (1, 0, 59534)$, $(57399, 1, 0)$, $(0, 119282, 1)$,

$\overline{M}f\overline{a}_i = (1, 22693, 0)$, $(0, 1, 116019)$, $(96498, 0, 1)$,

$\overline{M}fa_i = (1, 0, 49068)$, $(17053, 1, 0)$, $(0, 43863, 1)$,

$\overline{M}f\overline{a}_i = (1, 87803, 0)$, $(0, 1, 45633)$, $(63575, 0, 1)$,

$E3.3.$ $mfa_i = (1, 57399, 0)$, $[0, 1, 119282]$, $[59539, 0, 1]$,

$\overline{m}f\overline{a}_i = (1, 0, 96485)$, $[22698, 1, 0]$, $[0, 116028, 1]$,

$\overline{m}fa_i = (1, 17052, 0)$, $[0, 1, 43860]$, $[49067, 0, 1]$,

$\overline{m}f\overline{a}_i = (1, 0, 63592)$, $[87814, 1, 0]$, $[0, 45624, 1]$,

$E3.4.$ $Mfm_i = (1, 57399, 57265)$, $(10093, 1, 49647)$, $(92996, 18940, 1)$,

$$\begin{aligned}
& \overline{M} f m_i = (1, 39191, 23604), (90214, 1, 112020), (72715, 69295, 1), \\
E3.5. & i M A_i = [1, 6628, 76281], [1112, 1, 7094], [76270, 89247, 1], \\
& \bar{i} M A_i = [1, 5096, 35637], [3336, 1, 21174], [101928, 79188, 1], \\
E4.0. & Imm_i = (1, 101541, 76547), (91854, 1, 115568), (74057, 64703, 1), \\
& \bar{I} mm_i = (1, 36019, 60652), (45706, 1, 21992), (63503, 72857, 1), \\
E4.1. & ta_i = [0, 1, 19660], [64952, 0, 1], [1, 51999, 0], \\
E4.2. & T_i = (1, 115899, 64951), (51988, 1, 114948), (39743, 19651, 1), \\
E4.3. & at_i = [0, 1, 86571], [100052, 0, 1], [1, 66787, 0], \\
E4.4. & K_i = (1, 52716, 100037), (66802, 1, 11323), (84095, 86576, 1), \\
E4.5. & Taa_i = (0, 1, 114948), (39743, 0, 1), (1, 115899, 0), \\
E4.6. & poK_i = [1, 51999, 39734], [115882, 1, 19660], [64952, 1149331], \\
E4.7. & \mathbf{T} = \begin{pmatrix} 0 & 126353 & 46604 \\ 10833 & 0 & 10388 \\ 90969 & 127181 & 0 \end{pmatrix}, \mathbf{T}^{-1} = \begin{pmatrix} 1 & 21317 & 72608 \\ 115899 & 14 & 32443 \\ 64951 & 105118 & 2 \end{pmatrix}, \\
E4.8. & \mathbf{L} = \begin{pmatrix} 0 & 66802 & 84095 \\ 70412 & 0 & 66737 \\ 53448 & 70833 & 0 \end{pmatrix}, \mathbf{L}^{-1} = \begin{pmatrix} 1 & 84484 & 37508 \\ 52716 & 14 & 35592 \\ 100037 & 101959 & 2 \end{pmatrix}.
\end{aligned}$$

Except for interchanges the computation of \times is done as follows
we normalize l_2 to 1

$$\bar{l}_0.P_0 + \bar{l}_1.P_1 + P_2 = 0,$$

$$\bar{l}_0.Q_0 + \bar{l}_1.Q_1 + Q_2 = 0,$$

Multiplying the first by $P_0^{-1}.Q_0$ to the right and subtract from the second equation gives

$$\bar{l}_1(Q_1 - P_1P_0^{-1}Q_0) + (Q_2 - P_2P_0^{-1}Q_0) = 0,$$

therefore if $r_3 := (Q_1 - P_1P_0^{-1}Q_0)^{-1}$ and $r_4 = -(Q_2 - P_2P_0^{-1}Q_0)$, then

l_1 = the conjugate of $r_4.r_3$ and

$$l_0 = - \text{ the conjugate of } (\bar{l})_1 p_1 + p_2) p_0^{-1}.$$

The interchange is done as follows

if $P_0 = 0$, then we exchange P_i and Q_i ,

if after exchange, $P_0 = 0$, we consider all permutations sub0, sub1, sub2, of the subscripts 0, 1 and 2 .

Correspondance in Z_{19} between representation and quaternion.

representation	r	i	j	k	for
2222	18	2	6	0	M
22222	11	10	4	3	
6666	$16 * 8$	18	0	\overline{M}	
66666	14	12	13	9	
35222	15	10	2	5	eul
126587	9	12	8	18	

7.3 Miniquaternionian Plane Ψ of Veblen-Wedderburn.

7.3.0 Introduction.

Starting with the work of L. E. Dickson of 1905, non-Desarguesian planes of order 9 were discovered by Veblen and Wedderburn in 1907, I will here consider only one of these which is self dual, and for which non trivial polarities exists, and refer to the work of G. Zappa (1957), T. G. Ostrom (1964), D. R. Hughes (1957) and T. G. Room and P. B. Kirkpatrick (1971) for further reading.

The synthetic definition used can be traced to Veblen and Wedderburn, who first consider points obtained by applying a transformation (see p. 383), later generalized by J. Singer. The notation is inspired by Room and Kirkpatrick (see Table 5.5.4) using the same method I used for the finite plane reversing the indices for lines.

An alternate definition, (5.6.1), is given by Room and Kirkpatrick.

7.3.1 Miniquaternion near-field.

Definition.

A near-field $(N, +, \circ)$ is a set N with binary operations such that

0. N is finite,
1. $(N, +)$ is an Abelian group, with neutral element 0 ,
2. $(N - \{0\}, \circ)$ is an group, with neutral element 1 ,
3. \circ is right distributive over $+$, or
 $(\xi + \eta) \circ \zeta = \xi \circ \zeta + \eta \circ \zeta$, for all $\xi, \eta, \zeta \in N$
4. $\xi \circ 0 = 0$, for all $\xi \in N$.

Theorem.

In any near-field,

0. $0 \circ \xi = 0$, for all $\xi \in N$.
1. $\xi \circ \eta = 0 \implies \xi = 0$ or $\eta = 0$.
2. $1, -1 \neq 0$.

Theorem.

In any near-field of order 9,

0. $\{0, 1, -1\} \approx Z_3$.
1. $\xi + \xi + \xi = 0$, for all $\xi \in Q_9$,

2. $-1 \circ \xi = \xi \circ (-1) = \xi$, for all $\xi \in Q_9$,
3. $(-\xi) \circ \eta = \xi \circ (-\eta) = -(\xi \circ \eta)$, for all $\xi, \eta \in Q_9$,
4. $(-\xi) \circ (-\eta) = \xi \circ \eta$, for all $\xi, \eta \in Q_9$,
5. Given $\kappa \in Q_9^*$, $\lambda = s - \kappa r$ determines a one to one correspondance between the elements $\lambda \in Q_9$ and the pairs (r, s) , $r, s \in Z_3$.
6. Q_9 being an other near-field of order 9, the groups $(Q_9, +)$ and $(Q'_9, +)$ are isomorphic.
7. Besides $\text{GF}(3^2)$ there is only one near-field of order 9, which is the smallest near-field which is not a field, (*Zassenhaus, 1936*).

Exercise.

Determine the correspondance of 7.6.2.5.

Definition.

The miniquaternion set $Q_9 := \{0, \pm 1, \pm \alpha, \pm \beta, \pm \gamma\}$ with the operations of addition and multiplications defined from,

$$\xi + \xi + \xi = 0 \text{ for all } \xi \in Q_9,$$

$$\alpha - 1 = \beta, \alpha + 1 = \gamma,$$

$$\alpha^2 = \beta^2 = \gamma^2 = \alpha\beta\gamma = -1.$$

The set $Q_9^* := \{\pm \alpha, \pm \beta, \pm \gamma\}$.

Theorem.

0. $\alpha - \beta = \beta - \gamma = \gamma - \alpha = 1, \alpha + \beta + \gamma = 0$.
1. $\beta\gamma = -\gamma\beta = \alpha, \gamma\alpha = -\alpha\gamma = \beta, \alpha\beta = -\beta\alpha = \gamma$.
2. the multiplication is right distributive, $(\rho + \sigma)\tau = \rho\tau + \sigma\tau$, for all $\rho, \sigma, \tau \in Q_9$.
3. $\{Q_9, +, \cdot\}$ is a near-field.
4. $\{Q_9, +, \cdot\}$ is not a field, e. g.
 $\alpha(\alpha + \beta) = \alpha(-\gamma) = \beta, \alpha\alpha + \alpha\beta = -1 + \gamma = \alpha$.

	+	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
	1	-1	0	γ	$-\beta$	α	$-\gamma$	β	$-\alpha$
	-1	0	1	β	$-\gamma$	γ	$-\alpha$	α	$-\beta$
	α	γ	β	$-\alpha$	0	$-\gamma$	1	$-\beta$	-1
5.	$-\alpha$	$-\beta$	$-\gamma$	0	α	-1	γ	1	β
	β	α	γ	$-\gamma$	-1	$-\beta$	0	$-\alpha$	1
	$-\beta$	$-\gamma$	$-\alpha$	1	γ	0	β	-1	α
	γ	β	α	$-\beta$	1	$-\alpha$	-1	$-\gamma$	0
	$-\gamma$	$-\alpha$	$-\beta$	-1	β	1	α	0	γ

\cdot	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
1	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
-1	-1	1	$-\alpha$	α	$-\beta$	β	$-\gamma$	γ
α	α	$-\alpha$	-1	1	γ	$-\gamma$	$-\beta$	β
$-\alpha$	$-\alpha$	α	1	-1	$-\gamma$	γ	β	$-\beta$
β	β	$-\beta$	$-\gamma$	γ	-1	1	α	$-\alpha$
$-\beta$	$-\beta$	β	γ	$-\gamma$	1	-1	$-\alpha$	α
γ	γ	$-\gamma$	β	$-\beta$	$-\alpha$	α	-1	1
$-\gamma$	$-\gamma$	γ	$-\beta$	β	α	$-\alpha$	1	-1

7.3.2 The miniquaternionian plane Ψ .

Definition.

With $i, i' \in \{0, 1, 2\}$, $j \in \{0, 1, \dots, 12\}$, and the addition being performed modulo 3 for the first element of a pair, and modulo 13, for the second element in the pair or for the element, if single, then the elements and incidence in the miniquaternionian plane Ψ are defined as follows.

0. The points P are $(j), (i, j), (i', j)$,
1. The lines l are $[j], [i, j], [i', j]$,
2. The incidence is defined by

$$[j] := \{(-j), (1-j), (3-j), (9-j), (i, -j), (i', -j)\},$$

$$[i, j] := \{(-j), (i, 2-j), (i, 5-j), (i, 6-j), (i', 3-j), (i', 11-j),$$

$$(i' + 1, 7-j)(i' + 1, 9-j), (i' - 1, 1-j), (i' - 1, 8-j)\},$$

$$[i', j] := \{(-j), (i', 2-j), (i', 5-j), (i', 6-j), (i, 3-j),$$

$$(i, 11-j), (i + 1, 7-j)(i + 1, 9-j), (i - 1, 1-j), (i - 1, 8-j)\}.$$

Exercise.

7.6.4.2 is similar to the use of ordered cosets to determine efficiently operations of finite as well as infinite groups. In this case, $[j]$ is a subplane, $[i, j]$ and $[i', j]$ are copseudoplanes.

0. Perform a similar representation of points, lines and incidence starting with a subplane which is a Fano plane.
1. Determine similar representations for non Desarguesian geometries of order 5^2 , using a subplane of order 4, or of order 5 ($651 = 31 \cdot 21$).
2. Determine other such representation for non Desarguesian geometries of higher order.

Theorem.

The same incidence relations obtain, if we interchange points and lines in 7.6.4.2.

Theorem. [see Room and Kirkpatrick]

0. 0 The correspondance (j) to $[j]$ and (i, j) to $[i, j]$ and (i', j) to $[i', j]$ is a polarity \mathcal{P}_0 (\mathcal{J}^*).
- 1 The 16 auto-poles are $(0), (7), (8), (11), (0, 8), (0, 12), (1, 4), (1, 7), (2, 10), (2, 11), (0', 8), (0', 12), (1', 4), (1', 7), (2', 10), (2', 11)$.
1. 0 The correspondance (j) to $[j]$ and (i, j) to $[i', j]$ and (i', j) to $[i, j]$ is a polarity \mathcal{P}_1 (\mathcal{J}'^*).
- 1 The 22 auto-poles are $(0), (7), (8), (11), (0, 1), (0, 3), (0, 9), (1, 1), (1, 3), (1, 9), (2, 1), (2, 3), (2, 9), (0', 1), (0', 3), (0', 9), (1', 1), (1', 3), (1', 9), (2', 1), (2', 3), (2', 9)$.
- 2 $(0), (7), (8), (11), (0, 1), (1, 9), (2, 3), (0', 9), (1', 3), (2', 1), (0), (7), (8), (11), (1, 1), (2, 9), (0, 3), (2', 9), (0', 3), (1', 1), (0), (7), (8), (11), (2, 1), (0, 9), (1, 3), (1', 9), (2', 3), (0', 1)$ are ovals.

Exercise.

0. Prove that the correspondance (j) to $[j]$ and (i, j) to $[(i+1)', j]$ and (i', j) to $[i-1, j]$ is a polarity \mathcal{P}_2 .
1. Prove that the correspondance (j) to $[j]$ and (i, j) to $[(i-1)', j]$ and (i', j) to $[i+1, j]$ is a polarity \mathcal{P}_3 .

Exercise.

0. Determine a configuration in 7.6.4.0.2, which gives an example where the Theorem of Pascal is satisfied and an other, in which it is not satisfied.
1. Determine ovals which are subsets of 7.6.4.1.1.

Theorem.

The polar m of a point M with respect to a triangle is incident to that point.

Indeed, we can always assume that the triangle consists of the real points $A_0 = (0)$, $A_1 = (1)$, $A_2 = (2)$, and that $M = (5) = (1, 1, 1)$. It follows that $m = [4] = [1, 1, 1]$ which is incident to M .

Exercise.

Check that the other points and lines of the polar construction are $M_i = (4), (8), (3)$, $MA_i = (10), (12), (9)$, $MM_i = (7), (6), (11)$, $a_i = [12], [1], [0]$, $ma_i = [9], [8], [11]$, $m_i = [3], [2], [7]$, $mm_i = [6], [10], [5]$.

Theorem. [see Room and Kirkpatrick]

0. The planes obtained by taking the complete quadrangle associated with 3 real points A_0, A_1, A_2 , and a point \overline{M} which such that none of the lines $\overline{M} \times A_i$ are real are Fano planes associated with Z_2 .
1. There are $(\frac{1}{6}13.12.9).24 = 5616$ Fano planes that contain 3 real points.

Example.

The following is a Fano plane $(0), (1), (2), (0,3), (2,1), (0',12), (1,0), [12], [1], [0], [0',0], [0,12], [2',11], [0',7]$.

Exercise.

Determine the Fano plane associated with $(0), (1), (2), (0,7)$.

Comment.

The correspondance between the notation of Veblen-Wedderburn and Room-Kirkpatrick is

Veblen – Wedderburn	a_j	b_j	c_j	d_j	e_j	f_j	g_j
Room – Kirkpatrick	k_j	a_j	b_j	c_j	a_j	b_j	c_j
De Vogelaere	$[-j]$	$[0, -j]$	$[1, -j]$	$[2, -j]$	$[0', -j]$	$[1', -j]$	$[2', -j]$
Veblen – Wedderburn	A_j	B_j	C_j	D_j	E_j	F_j	G_j
Room – Kirkpatrick	K_j	A_j	C_j	B_j	A_j	C_j	B_j
De Vogelaere	(j)	$(0, j)$	$(1, j)$	$(2, j)$	$(0', j)$	$(1', j)$	$(2', j)$

Example. [Veblen-Wedderburn]

With the notation

$(C\langle c_0, c_1, c_2 \rangle, \{A_0, A_1, A_2\}\{a_0, a_1, a_2\}, \{B_0, B_1, B_2\}\{b_0, b_1, b_2\};$

$\{C_0, C_1, C_2\}\{d_0, d_1, d_2\})$, with $d_i := C_{i+j} \times C_{i-j}$,

the following configuration shows that the Desargues axiom is not satisfied

$((0)\langle [0, 0], [1', 0], [2, 0] \rangle, \{(0, 1), (1, 7), (1', 2)\}\{[1, 1], [0', 8], [0', 9]\}, \{(2, 3), (0'3), (2, 1)\}\{[0, 11], [2', 7], [10]\};$
 $\{(2', 5), (0, 10), (1', 3)\}\{[2, 1], [1, 0], [0, 4]\})$.

Definition.

The Singer matrix $\mathbf{G} := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Its powers \mathbf{G}^k are the columns

$k, k+1, k+2$ of

$k =$	0	1	2	3	4	5	6	7	8	9	10	11	12
	1	0	0	1	0	1	1	1	-1	-1	0	1	-1
	0	1	0	1	1	1	-1	-1	0	1	-1	1	0
	0	0	1	0	1	1	1	-1	-1	0	1	-1	1

Problem.

Can we characterize the plane Ψ using Theorem 7.6.4.0.

move to g6a.tex:

Answer to 7.6.2.

κ	$\lambda =$	0	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
α	r	0	0	0	-1	1	-1	1	-1	1
	s	0	1	-1	0	0	-1	1	1	-1
β	r	0	0	0	-1	1	-1	1	-1	1
	s	0	1	-1	1	-1	0	0	-1	1
γ	r	0	0	0	-1	1	-1	1	-1	1
	s	0	1	-1	-1	1	-1	0	0	0

Definition.

The elements and incidence in the miniquaternionian plane Ψ are defined as follows.

0. The points are (ξ_0, ξ_1, ξ_2) with right equivalence,
- 1.
2. A point P is incident to a line l iff

Definition. [Veblen-Wedderburn]

The points P are $(x, y, 1)$, $(x, 1, 0)$, $(1, 0, 0)$, the lines l are $[1, b, c]$, $[0, 1, c]$, $[0, 0, 1]$, and the incidence is $P \cdot l = 0$.

Theorem. [Veblen-Wedderburn]

0. $[1, b, c] \times [1, b', c'] = (-(yb + c), y, 1)$, with $y(b - b') = -(c - c')$.
1. $[1, b, c] \times [0, 1, c'] = (c'b - c, -c', 1)$,
2. $[1, b, c] \times [0, 0, 1] = (-b, 1, 0)$,
3. $[0, 1, c] \times [0, 1, c'] = (1, 0, 0)$,
4. $[0, 1, c] \times [0, 0, 1] = (1, 0, 0)$,

Theorem. [Veblen-Wedderburn]

Let $(a(b+c) = ab+ac)$

$$0. \mathbf{M} := \begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix}.$$

1. $A_0 := (-1, 0, 1)$, $B_0 := (-\gamma, \alpha, 1)$, $C_0 := (\beta, -\alpha, 1)$, $D_0 := (-\beta, \gamma, 1)$, $E_0 := (\alpha, -\gamma, 1)$,
 $F_0 := (\gamma, -\beta, 1)$, $G_0 := (-\alpha, \beta, 1)$,

2. $A_j := \mathbf{M}^j A_0, B_j := \mathbf{M}^j B_0, \dots$, for $j = 0$ to 12 ,

3. $a_0 := [1, 1, 1], b_0 := [1, \alpha, 1], c_0 := [1, -\alpha, 1], d_0 := [1, \gamma, 1], e_0 := [1, -\gamma, 1], f_0 := [1, -\beta, 1], g_0 := [1, \beta, 1]$,

then

4. $a_0 = \{A_0, A_1, A_3, A_9, B_0, C_0, D_0, E_0, F_0, G_0\}$,
 $b_0 = \{A_0, B_1, B_8, D_3, D_{11}, E_2, E_5, E_6, G_7, G_9\}$,
 $c_0 = \{A_0, C_1, C_8, E_7, E_9, F_3, F_{11}, G_2, G_5, G_6\}$,
 $d_0 = \{A_0, B_7, B_9, D_1, D_8, F_2, F_5, F_6, G_3, G_{11}\}$,
 $e_0 = \{A_0, B_2, B_5, B_6, C_3, C_{11}, E_1, E_8, F_7, F_9\}$,
 $f_0 = \{A_0, C_7, C_9, D_2, D_5, D_6, E_3, E_{11}, F_1, F_8\}$,
 $g_0 = \{A_0, B_3, B_{11}, C_2, C_5, C_6, D_7, D_9, G_1, G_8\}$,

5. $A_0 = \{a_0, a_4, a_{10}, a_{12}, b_0, c_0, d_0, e_0, f_0, g_0\}$,
 $B_0 = \{a_0, b_5, b_{12}, d_4, d_6, e_7, e_8, e_{11}, g_2, g_{10}\}$,
 $C_0 = \{a_0, c_5, c_{12}, e_2, e_{10}, f_4, f_6, g_7, g_8, g_{11}\}$,
 $D_0 = \{a_0, b_2, b_{10}, d_5, d_{12}, f_7, f_8, f_{11}, g_4, g_6\}$,
 $E_0 = \{a_0, b_7, b_8, b_{11}, c_4, c_6, e_5, e_{12}, f_2, f_{10}\}$,
 $F_0 = \{a_0, c_1, c_{10}, d_7, d_8, d_{11}, e_4, e_6, f_5, f_{12}\}$,
 $G_0 = \{a_0, b_4, b_6, c_7, c_8, c_{11}, d_2, d_{10}, g_5, g_{12}\}$,

6. $X_j \iota x_k \implies X_{j+l \bmod 13} \iota x_{k+l \bmod 13}$.

7. $\mathbf{M}^2 = \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}, \mathbf{M}^3 = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}, \mathbf{M}^4 = \begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, \mathbf{M}^5 = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}$,
 $\mathbf{M}^6 = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}, \mathbf{M}^7 = \begin{pmatrix} -1 & 1 & -1 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}, \mathbf{M}^8 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ -1 & -1 & 1 \end{pmatrix}, \mathbf{M}^9 = \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}$,
 $\mathbf{M}^{10} = \begin{pmatrix} 0 & -1 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & -1 \end{pmatrix}, \mathbf{M}^{11} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}, \mathbf{M}^{12} = \begin{pmatrix} 0 & -1 & 0 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}, \mathbf{M}^{13} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$.

Proof: $[x, y, z] \iota \beta?$ iff $x(\mathbf{M}_{00}^k + \mathbf{M}_{20}^k) + y(\mathbf{M}_{01}^k + \mathbf{M}_{21}^k) + z(\mathbf{M}_{02}^k + \mathbf{M}_{22}^k) + (z\mathbf{M}_{10}^k + y\mathbf{M}_{11}^k + x\mathbf{M}_{12}^k)\beta = 0, \dots$

Example. [Veblen-Wedderburn]

With the notation

$(C\langle c_0, c_1, c_2 \rangle, \{A_0, A_1, A_2\}\{a_0, a_1, a_2\}, \{B_0, B_1, B_2\}\{b_0, b_1, b_2\};$
 $\{C_0, C_1, C_2\}\{d_0, d_1, d_2\})$, with $d_i := C_{i+j} \times C_{i-j}$,

the following configuration shows that the Desargues axiom is not satisfied

$(A_0\langle b_0, f_0, d_0 \rangle, \{B_1, C_7, F_2\}\{c_{12}, e_5, e_4\}, \{D_3, E_3, D_1\}\{b_2, g_6, a_3\};$
 $\{G_5, B_{10}, F_3\}\{d_{12}, c_0, b_9\})$.

Partial answer to 7.6.4.

For $n = 7^2$, $2451 = 57.43$, for $n = 9^2$, $6643 = 91.73$, for $n = 11^2$, $14763 = 57.259$, For $n = 13^2$, $28731 = 3.9577$.

Answer to 7.6.4.

The other points are $(1,1)$, $(0',12)$, $(0',0)$, the lines are $[12]$, $[1]$, $[0]$, $[1',0]$, $[0,12]$, $[0,11]$ and the polar of $(0,7)$ is $[0',6]$.

Answer to 7.6.4.

$(7) \times (8) = [6]$, $[6] \times [0] = (3)$, $(8) \times (0) = [1]$, $[1] \times [7] = (2)$, $(0) \times (7) = [9]$, $[9] \times [8] = (5)$, $\langle (3), (2), (5); [11] \rangle$.

$(7) \times (8) = [6]$, $[6] \times [0,1] = (1',7)$, $(8) \times (0,1) = [0,5]$, $[0,5] \times [7] = (0',6)$, $(0,1) \times (7) = [2',6]$, $[2',6] \times [8] = (2,5)$, $(2,5)$ is not incident to $(1',7) \times (0'6) = [2,2]$.

This has not been checked.

From Dembowski, p. 129

Definition.

A linear ternary ring $(\Sigma, +, \cdot)$ is called a cartesian field iff $(\Sigma, +)$ is associative and is therefore a group.

Definition.

A cartesian field is called a quasifield iff the right distributivity law holds:

$$(x + y)z = xz + yz.$$

Artzy adds that $xa = xb + c$ has a unique solution, but this is a property (28). This is Veblen-Wedderburn.

Definition.

A quasifield is called a semifield iff the left distributivity law holds:

$$z(x + y) = zx + zy.$$

Definition.

A quasifield is called a nearfield iff (Σ, \cdot) is associative and is therefore a group.

Definition.

A semifield is called a alternative field iff $x^2y = x(xy)$ and $xy^2 = (xy)y$.

Theorem.

P is (p, L) transitive iff P is (p, L) Desarguesian. p is point, L is a line. *Dembowski p.123, 16*

Let $Q_0 = (79)$, $Q_1 = (80)$, $Q_2 = (90)$, and $U = (81)$ then $q_2 = [79]$, $q_0 = [90]$, $q_1 = [80]$, $v = [88]$, $i = [78]$, $V = (78)$, $I = (82)$, $j = [89]$, $W = (89)$,

Points on q_2 : 86, 12, 25, 38, 51, 64, 77

Points on q_1 : 85, 11, 24, 37, 50, 63, 76

$11 \times 12 = [7] : 84(78, 86), 8(51, 25), 43(77, 64), 48(86, 38), 52(12, 12), 54(25, 78), 66(64, 80), 72(38, 51),$
 $11 \times 25 = [61] : 82(78, 80), 0(64, 64), 18(12, 51), 28(51, 78), 33(77, 12), 58(38, 86), 61(86, 25), 62(25, 38),$
 $11 \times 38 = [75] : 81(78, 78), 4(38, 25), 14(12, 80), 19(77, 86), 36(51, 64), 70(64, 38), 73(25, 51), 74(86, 12),$
 $11 \times 51 = [4] : 87(86, 86), 1(38, 80), 2(77, 78), 46(25, 64), 55(78, 38), 57(51, 12), 69(64, 51), 75(12, 25),$
 $11 \times 64 = [8] : 83(86, 78), 7(64, 25), 10(77, 51), 42(78, 12), 47(12, 64), 53(51, 80), 65(38, 38), 71(25, 86),$
 $11 \times 77 = [68] : 88(86, 80), 5(38, 64), 13(51, 51), 21(77, 38), 30(25, 12), 32(64, 86), 67(12, 78), 68(78, 25),$

Coordinates of points:

(0)	64, 64	38, 80	77, 78	78, 51	38, 25	38, 64	51, 86	64, 25
(8)	51, 25	86, 77	77, 51	80, 77	12	51, 51	12, 80	64, 78
(16)	78, 77	12, 38	12, 51	77, 86	51, 38	77, 38	86, 64	64, 77
(24)	80, 64	25	77, 77	25, 80	51, 78	78, 64	25, 12	25, 77
(32)	64, 86	77, 12	64, 12	86, 51	51, 64	80, 51	38	25, 25
(40)	77, 80	38, 78	78, 12	77, 64	77, 25	12, 86	25, 64	12, 64
(48)	86, 38	38, 12	80, 38	51	12, 12	51, 80	25, 78	78, 38
(56)	51, 77	51, 12	38, 86	12, 77	38, 77	86, 25	25, 38	80, 25
(64)	64	38, 38	64, 80	12, 78	78, 25	64, 51	64, 38	25, 86
(72)	38, 51	25, 51	86, 12	12, 25	80, 12	77	78	80, 80
(80)	0	78, 78	78, 80	86, 78	78, 86	80, 86	86	86, 86
(88)	86, 80	80, 78	∞					

Coordinates of lines:

[0]	78, 38	38	77, 78	12, 12	51, 77	86, 38	12, 86	12, 77
[8]	64, 77	77, 25	64, 12	80, 25	51, 80	78, 12	12	64, 78
[16]	25, 25	77, 64	86, 12	25, 86	25, 64	51, 64	64, 38	51, 25
[24]	80, 38	77, 80	78, 25	25	51, 78	38, 38	64, 51	86, 25
[32]	38, 86	38, 51	77, 51	51, 12	77, 38	80, 12	64, 80	78, 77
[40]	77	38, 78	51, 51	12, 38	86, 77	51, 86	51, 38	25, 38
[48]	38, 64	25, 51	80, 64	12, 80	78, 51	51	25, 78	64, 64
[56]	38, 25	86, 51	64, 86	64, 25	12, 25	25, 77	12, 64	80, 77
[64]	38, 80	78, 64	64	12, 78	77, 77	25, 12	86, 64	77, 86
[72]	77, 12	38, 12	12, 51	38, 77	80, 51	25, 80	78, 80	∞
[80]	80	78, 78	86	86, 78	86, 86	80, 86	86, 80	78, 86
[88]	78	80, 78	80, 80					

[80] : 11(80, 77), 24(80, 64), 37(80, 51), 50(80, 38), 63(80, 25), 76(80, 12), 79(80, 80), 85(80, 86), 89(80, 78), 92(80, 88)

$B = A + \alpha$, $(A, B) \iota [V, Y]$, $V = (78)$, $(76) = (80, 12) = (\underline{0}, \alpha)$, $Y \times V = (78) \times (76) = [13]$.

[13] : 78(78), 15(64, 78), 18(12, 51), 19(77, 86), 68(78, 25), 76(80, 12), 46(25, 64), 48(86, 38), 53(51, 80), 60(38, 77), 62(25, 38), 64(78, 86), 66(64, 80), 69(64, 51), 70(64, 38), 72(38, 51), 73(25, 51), 74(86, 12), 75(12, 25), 77(77, 78), 79(80, 80), 81(78, 78), 82(78, 80), 83(86, 78), 84(78, 86), 85(80, 86), 86(86, 86), 87(86, 86), 88(86, 80), 89(80, 78), 90(90, 90), 91(86, 86), 92(80, 88)

hence $12 = 80 + \alpha$, $51 = \alpha + \alpha = -\alpha$, $25 = 78 + \alpha = 1 + \alpha = \gamma$, $64 = 25 + \gamma = \gamma + \gamma = -\beta$,

$38 = 86 + \alpha = -1 + \alpha = \beta$, $77 = 38 + \alpha = \beta + \alpha = -\gamma$.

$$\begin{array}{cccccccccc} \infty & 0 & 1 & -1 & \alpha & -\alpha & \beta & -\beta & \gamma & -\gamma \\ 90 & 80 & 78 & 86 & 12 & 51 & 38 & 64 & 25 & 77 \end{array}$$

$$[\alpha, 0] = (12) \times (80, 80) = (12) \times (79) = [51], (a, b) \iota [51] \implies b = a \cdot \alpha.$$

$$(42) = (78, 12) = (\underline{1}, \alpha) \implies \alpha = 1 \times \alpha,$$

$$(45) = (12, 86) = (\alpha, \underline{-1}) \implies -1 = \alpha \times \alpha,$$

$$(23) = (64, 77) = (-\beta, -\gamma) \implies -\gamma = -\beta \times \alpha,$$

$$(28) = (51, 78) = (-\alpha, \underline{1}) \implies 1 = -\alpha \times \alpha,$$

$$(35) = (86, 51) = (\underline{-1}, -\alpha) \implies -\alpha = \underline{-1} \times \alpha,$$

Using DATA 6,0, 6,4, 6,10, 6,12, 0,0, 1,0, 2,0, 3,0, 4,0, 5,0 DATA 6,0, 0,7, 0,8, 0,11, 3,2, 3,10, 4,4, 4,6, 5,5, 5,12 gives the same multiplication table give left not right distributive law with $Q_i = 79, 81, 87$, $U = (83)$, $\alpha = (12)$, $q_0 = [87] = \{79, 81, 82, 86, 4, 17, \dots\}$,

$$q_1 = [81] = \{79, 85, 87, 88, 10, 23, \dots\},$$

$$q_2 = [79] = \{81, 87, 89, 90, 12, 25, \dots\},$$

with case 7, data 79,81,87,83,12:

$$\infty = 87, \underline{0} = 81, \underline{1} = 89, \underline{-1} = 90, \alpha = 12, -\alpha = 77, \beta = 38, -\beta = 51, \gamma = 25, -\gamma = 64.$$

This is a try for a section to be included in g19.tex between Moufang and Desargues.

7.4 Axiomatic.

7.4.1 Veblen-MacLagan planes.

Introduction.

The first example of a Veblen-Wedderburn plane was given in 1907 by Veblen and MacLagan-Wedderburn. It is associated to the algebraic structure of a nearfield, which is a skew field which lacks the left distributive law, hence is an other plane between the Veblen-Wedderburn plane and the Desarguesian plane.

Axiom. [Da] ⁴

Given a Veblen-Wedderburn plane, 2 points Q_1 and Q_2 on the ideal line and an other point Q_0 not on it, any 2 parallelograms A_i and B_i with directions Q_1 and Q_2 , with no sides in common $\dots, ???$, such that A_j and B_j are perspective from Q_0 for $j = 0$ To 2, imply that A_3 and B_3 are perspective from Q_0 .

Notation.

$$Da(\{Q_0, Q_1, Q_2\}, \{A_j\}, \{B_j\}).$$

Definition.

A Veblen-MacLagan plane is a Veblen-Wedderburn plane in which the axiom Da is satisfied.

⁴Da for Desargues leading to associativity of multiplication.

Lemma. [For Associativity]

H1.0. A_0, a_{12}, x , (See Fig. 2?.)

D1.0. $a_{01} := Q_1 \times A_0, a_{02} := Q_2 \times A_0,$

D1.1. $A_1 := a_{01} \times a_{12}, A_2 := a_{02} \times a_{12},$

D1.2. $a_{13} := Q_2 \times A_1, a_{23} := Q_1 \times A_2, A_3 := a_{13} \times a_{23},$

D2.0. $a_0 := Q_0 \times A_0, a_1 := Q_0 \times A_1, a_2 := Q_0 \times A_2, a_3 := Q_0 \times A_3, D2.1.$ $B_0 := a_0 \times y,$
 $b_{01} := Q_1 \times B_0, b_{02} := Q_2 \times B_0,$

D2.1. $B_1 := b_1 \times b_{01}, B_2 := b_2 \times b_{02}, D2.2.$ $b_{13} := Q_2 \times B_1, b_{23} := Q_1 \times B_2, B_3 := b_{13} \times b_{23},$

C1.0. $B_3 \iota b_3,$

Moreover

$A_0 = (A, B), A_1 = (A', B), A_2 = (A, B'), A_3 = (A', B'), B_0 =$

Proof: $Da(\{Q_0, Q_1, Q_2\}, \{A_j\}, \{B_j\}).$

Theorem.

In a Veblen-MacLagan plane, the ternary ring $(\Sigma, *)$ is a nearfield.:

0. $(\Sigma, +)$ is an Abelian group,
1. $(\Sigma - \{0\}, \cdot)$ is a group,
2. $(\Sigma, *) = (\Sigma, +, \cdot)$ is right distributive, $(a + b) \cdot c = a \cdot c + b \cdot c.$

7.4.2 Examples of Perspective planes.

Theorem.

0. The Cayleyan plane is not a Veblen-MacLagan plane.

Definition.

A miniquaternion plane

Theorem.

0. A miniquaternion plane is a Veblen-MacLagan plane.
1. A miniquaternion plane is not a Moufang plane.

Tables.

The following are in an alternate notation the known table for $p = 3$ and a new table for $p = 5$. The other incidence are obtained by adding one to the subscripts of the lines and subtracting one for the subscript of the points.

Selectors for Ψ plane, when $p = 3$:

$(0_0^0) : [0_2^0], [0_5^0], [0_6^0], [1_1^0], [1_8^0], [1_7^1], [1_9^1], [1_3^2], [1_{11}^3],$

$(0_0^1) : [0_2^1], [0_5^1], [0_6^1], [1_3^1], [1_{11}^1], [1_1^2], [1_8^3], [1_7^0], [1_9^0],$

$$\begin{aligned}
(0_6^2) &: [0_2^2], [0_5^2], [0_6^2], [1_7^2], [1_3^3], [1_3^0], [1_{11}^0], [1_1^1], [1_8^1], \\
(1_9^0) &: [1_2^0], [1_5^0], [1_6^0], [0_1^0], [0_8^0], [0_7^1], [0_9^1], [0_3^1], [0_{11}^1], \\
(1_0^1) &: [1_2^1], [1_5^1], [1_6^1], [0_3^1], [0_{11}^1], [0_1^2], [0_8^3], [0_7^0], [0_9^0], \\
(1_2^0) &: [1_2^2], [1_5^2], [1_6^2], [0_7^2], [0_9^3], [0_3^0], [0_{11}^0], [0_1^1], [0_8^1],
\end{aligned}$$

Selectors for Ψ plane, when $p = 5$:

$$\begin{aligned}
(0_0^0) &: [0_6^0], [0_{21}^0], [0_{16}^0], [1_{18}^2], [1_{25}^2], [1_5^3], [1_{13}^3], [0_4^3], [1_{22}^0], [0_{28}^2], \\
&\quad [2_{12}^0], [2_{23}^0], [2_{24}^0], [2_{26}^0], [2_1^1], [2_{10}^1], [2_{14}^4], [2_8^4], [3_9^1], [3_{27}^1], [3_{15}^4], [3_{19}^4], [2_{29}^2], [2_{20}^3], [3_3^0], \\
(0_1^0) &: [0_{25}^0], [0_{19}^0], [0_6^1], [1_{12}^1], [1_{26}^3], [1_{18}^4], [1_{21}^4], [0_{22}^4], [1_{28}^1], [0_{27}^3], \\
&\quad [2_3^1], [2_5^1], [2_{29}^1], [2_{13}^1], [2_{20}^2], [2_9^2], [2_1^0], [2_{10}^0], [3_{16}^2], [3_{15}^2], [3_4^0], [3_8^0], [2_{14}^3], [2_{24}^4], [3_{23}^1], \\
(0_2^0) &: [0_{26}^2], [0_8^2], [0_{25}^2], [1_3^4], [1_{13}^4], [1_{12}^0], [1_6^0], [0_{28}^0], [1_{27}^2], [0_{15}^4], \\
&\quad [2_{23}^2], [2_{18}^2], [2_{14}^2], [2_{21}^2], [2_{24}^2], [2_{16}^3], [2_{20}^1], [2_9^1], [3_{19}^3], [3_4^3], [3_{22}^1], [3_{10}^1], [2_1^4], [2_{29}^0], [3_5^2], \\
(0_3^0) &: [0_{13}^3], [0_{10}^3], [0_{26}^3], [1_{23}^0], [1_{21}^1], [1_3^1], [1_{25}^1], [0_{27}^1], [1_{15}^3], [0_4^0], \\
&\quad [2_5^3], [2_{12}^3], [2_3^3], [2_6^3], [2_{29}^4], [2_{19}^4], [2_{24}^4], [2_{16}^2], [3_8^4], [3_{22}^4], [3_{28}^2], [3_9^2], [2_{20}^0], [2_{14}^1], [3_{18}^3], \\
(0_4^0) &: [0_{21}^4], [0_9^4], [0_{13}^4], [1_5^1], [1_6^1], [1_{23}^2], [1_{26}^2], [0_{15}^2], [1_4^4], [0_{22}^1], \\
&\quad [2_{18}^4], [2_3^4], [2_{20}^4], [2_{25}^4], [2_{14}^0], [2_8^0], [2_{29}^2], [2_{19}^3], [3_{10}^0], [3_{28}^0], [3_{27}^3], [3_{16}^3], [2_{24}^1], [2_1^2], [3_{12}^4], \\
(1_9^0) &: [1_9^0], [1_{19}^0], [1_{26}^0], [0_6^2], [0_{12}^2], [0_{21}^3], [0_{23}^3], [1_{18}^1], [1_5^4], [0_{22}^0], \\
&\quad [3_{27}^0], [3_{15}^0], [3_{24}^0], [3_{16}^0], [2_4^1], [2_8^1], [2_{28}^2], [2_{10}^4], [3_{20}^3], [3_{25}^3], [3_{29}^2], [3_{13}^2], [3_1^1], [3_{14}^4], [2_3^0], \\
(1_1^0) &: [1_{16}^1], [1_8^1], [1_{13}^1], [0_{25}^3], [0_3^3], [0_6^4], [0_5^4], [1_{12}^0], [1_{18}^0], [0_{28}^2], \\
&\quad [3_{15}^1], [3_4^1], [3_{29}^1], [3_{19}^1], [2_{22}^2], [2_{10}^2], [2_{27}^2], [2_9^0], [3_{24}^4], [3_{26}^4], [3_{14}^3], [3_{21}^1], [3_{20}^2], [3_1^0], [2_{23}^1], \\
(1_2^0) &: [1_{19}^2], [1_{10}^2], [1_{21}^2], [0_{26}^4], [0_{23}^4], [0_{25}^0], [0_{18}^0], [1_3^3], [1_{12}^1], [0_{27}^2], \\
&\quad [3_4^2], [3_{22}^2], [3_{14}^2], [3_8^2], [2_{28}^3], [2_9^3], [2_{15}^1], [2_{16}^1], [3_{29}^0], [3_{13}^0], [3_1^4], [3_6^4], [3_4^3], [3_{20}^1], [2_5^2], \\
(1_3^0) &: [1_8^3], [1_9^3], [1_6^3], [0_{13}^0], [0_5^0], [0_{26}^1], [0_{12}^1], [1_{23}^4], [1_3^2], [0_{15}^3], \\
&\quad [3_{22}^3], [3_{28}^3], [3_1^3], [3_{10}^3], [2_{27}^4], [2_{16}^4], [2_4^2], [2_{19}^2], [3_{14}^1], [3_{21}^1], [3_{20}^0], [3_{25}^0], [3_{29}^4], [3_{24}^2], [2_{18}^3], \\
(1_4^0) &: [1_{10}^4], [1_{16}^4], [1_{25}^4], [0_{21}^1], [0_{18}^1], [0_{13}^2], [0_2^3], [1_5^0], [1_{23}^3], [0_4^4], \\
&\quad [3_{28}^4], [3_{27}^4], [3_{20}^4], [3_9^4], [2_{15}^0], [2_{19}^0], [2_{22}^2], [2_8^3], [3_1^2], [3_6^2], [3_{24}^1], [3_{26}^1], [3_{14}^0], [3_{29}^3], [2_{12}^4], \\
(2_0^0) &: [2_6^0], [2_{21}^0], [2_{16}^0], [3_{18}^2], [3_{25}^2], [3_5^3], [3_{13}^3], [2_4^3], [3_{22}^0], [2_{28}^2], \\
&\quad [0_{12}^0], [0_{23}^0], [0_{24}^0], [0_{26}^0], [0_1^1], [0_{10}^1], [0_{14}^4], [0_8^4], [1_9^1], [1_{27}^1], [1_{15}^4], [1_{19}^4], [0_{29}^2], [0_{20}^3], [1_3^0], \\
(2_1^0) &: [2_{25}^1], [2_{19}^1], [2_6^1], [3_{12}^3], [3_{26}^3], [3_{18}^4], [3_{21}^4], [2_{22}^2], [3_{28}^1], [2_{27}^3], \\
&\quad [0_5^1], [0_5^1], [0_{29}^1], [0_{13}^1], [0_{20}^2], [0_9^2], [0_1^0], [0_{10}^0], [1_{16}^2], [1_{15}^2], [1_9^0], [1_8^0], [0_{14}^3], [0_{24}^4], [1_{23}^1], \\
(2_2^0) &: [2_{26}^2], [2_8^2], [2_{25}^2], [3_3^4], [3_{13}^4], [3_{12}^0], [3_6^0], [2_{28}^2], [3_{27}^2], [2_{15}^4], \\
&\quad [0_{23}^2], [0_{18}^2], [0_{14}^2], [0_{21}^2], [0_{24}^3], [0_{16}^3], [0_{20}^1], [0_9^1], [1_{19}^3], [1_4^3], [1_{22}^1], [1_{10}^1], [0_1^4], [0_{29}^0], [1_5^2], \\
(2_3^0) &: [2_{13}^3], [2_{10}^3], [2_{26}^3], [3_{23}^0], [3_{21}^0], [3_3^1], [3_{25}^1], [2_{27}^1], [3_{15}^3], [2_4^0], \\
&\quad [0_5^3], [0_{12}^3], [0_1^3], [0_6^3], [0_{29}^4], [0_{19}^4], [0_{24}^2], [0_{16}^2], [1_8^4], [1_{22}^4], [1_{28}^2], [1_9^2], [0_{20}^0], [0_{14}^1], [1_{18}^3], \\
(2_4^0) &: [2_{21}^4], [2_9^4], [2_{13}^4], [3_5^1], [3_6^1], [3_{23}^3], [3_{26}^2], [2_{15}^2], [3_4^4], [2_{22}^2], \\
&\quad [0_{18}^4], [0_3^4], [0_{20}^4], [0_{25}^4], [0_{14}^0], [0_8^0], [0_{29}^3], [0_{19}^3], [1_{10}^0], [1_{28}^0], [1_{27}^3], [1_{16}^3], [0_{24}^1], [0_1^2], [1_{12}^4], \\
(3_0^0) &: [3_9^0], [3_{19}^0], [3_{26}^0], [2_{12}^2], [2_{21}^2], [2_{21}^3], [2_{23}^3], [3_{18}^1], [3_5^4], [2_{22}^0], \\
&\quad [1_{27}^0], [1_{15}^0], [1_{24}^0], [1_{16}^0], [0_4^1], [0_8^1], [0_{28}^4], [0_{10}^4], [1_{20}^3], [1_{25}^3], [1_{29}^2], [1_{13}^2], [1_1^1], [1_{14}^4], [0_3^0], \\
(3_1^0) &: [3_{16}^1], [3_8^1], [3_{13}^1], [2_{25}^3], [2_3^3], [2_6^4], [2_5^4], [3_{12}^0], [3_{18}^0], [2_{28}^2], \\
&\quad [1_{15}^1], [1_{14}^1], [1_{29}^1], [1_{19}^1], [0_{22}^2], [0_{10}^2], [0_{27}^0], [0_9^0], [1_{24}^4], [1_{26}^4], [1_{14}^3], [1_{21}^3], [1_{20}^2], [1_1^0], [0_{23}^1], \\
(3_2^0) &: [3_{19}^2], [3_{10}^2], [3_{21}^2], [2_{26}^4], [2_{23}^4], [2_{25}^2], [2_{18}^0], [3_3^3], [3_{12}^1], [2_{27}^2], \\
&\quad [1_4^2], [1_{22}^2], [1_{14}^2], [1_8^2], [0_{28}^3], [0_9^3], [0_{15}^1], [0_{16}^1], [1_{29}^0], [1_{13}^0], [1_4^4], [1_6^4], [1_{20}^1], [0_5^2], \\
(3_3^0) &: [3_8^3], [3_9^3], [3_6^3], [2_{13}^0], [2_5^0], [2_{26}^1], [2_{12}^1], [3_{23}^4], [3_3^2], [2_{15}^3],
\end{aligned}$$

$[1_{22}^3], [1_{28}^3], [1_{11}^3], [1_{10}^3], [0_{27}^4], [0_{16}^4], [0_4^2], [0_{19}^2], [1_{14}^1], [1_{21}^1], [1_{20}^0], [1_{25}^0], [1_{29}^4], [1_{24}^2], [0_{18}^3],$
 $(3_0^4) : [3_{10}^4], [3_{16}^4], [3_{25}^4], [2_{21}^1], [2_{18}^1], [2_{13}^2], [2_3^2], [3_5^0], [3_{23}^3], [2_4^4],$
 $[1_{28}^4], [1_{27}^4], [1_{20}^4], [1_9^4], [0_{15}^0], [0_{19}^0], [0_{22}^0], [0_8^3], [1_1^2], [1_6^2], [1_{24}^1], [1_{26}^1], [1_{14}^0], [1_{29}^3], [0_{12}^4],$

An abbreviated form is as follows:

The array for the indices:

i	0	1	2	3	4
a_i	24	29	14	1	20
b_i	3	23	5	18	12
c_i	22	28	27	15	4
d_i	16	19	8	10	9
e_i	26	13	21	6	25

Selectors for the Ψ plane, when $p = 5$:

$(0_0^0) : [0_{e_2}^0], [0_{e_3}^0], [0_{d_0}^0], [1_{e_1}^3], [1_{b_2}^3], [1_{e_4}^2], [1_{b_3}^2], [0_{c_1}^2], [0_{c_4}^3], [1_{c_1}^0],$
 $[2_{b_1}^0], [2_{b_4}^0], [2_{a_0}^0], [2_{e_0}^0], [2_{a_2}^4], [2_{d_2}^4], [2_{a_3}^1], [2_{d_3}^1],$
 $[3_{d_1}^4], [3_{c_3}^4], [3_{d_4}^1], [3_{c_2}^1], [2_{a_1}^2], [2_{a_4}^3], [3_{b_0}^0],$
 $(1_0^0) : [1_{d_1}^0], [1_{d_4}^0], [1_{e_0}^0], [0_{b_1}^3], [0_{e_2}^3], [0_{b_4}^2], [0_{e_3}^2], [1_{b_2}^4], [1_{b_3}^1], [0_{c_0}^0],$
 $[3_{c_2}^0], [3_{c_3}^0], [3_{a_0}^0], [3_{d_0}^0], [3_{a_1}^2], [3_{e_1}^2], [3_{a_4}^3], [3_{e_4}^3],$
 $[2_{c_1}^4], [2_{d_3}^4], [2_{c_4}^1], [2_{d_2}^1], [3_{a_2}^4], [3_{a_3}^1], [2_{b_0}^0],$
 $(2_0^0) : [2_{e_2}^0], [2_{e_3}^0], [2_{d_0}^0], [3_{e_1}^3], [3_{b_2}^3], [3_{e_4}^2], [3_{b_3}^2], [2_{c_1}^2], [2_{c_4}^3], [3_{c_1}^0],$
 $[0_{b_1}^0], [0_{b_4}^0], [0_{a_0}^0], [0_{e_0}^0], [0_{a_2}^4], [0_{d_2}^4], [0_{a_3}^1], [0_{d_3}^1],$
 $[1_{d_1}^4], [1_{c_3}^4], [1_{d_4}^1], [1_{c_2}^1], [0_{a_1}^2], [0_{a_4}^3], [1_{b_0}^0],$
 $(3_0^0) : [3_{d_1}^0], [3_{d_4}^0], [3_{e_0}^0], [2_{b_1}^3], [2_{e_2}^3], [2_{b_4}^2], [2_{e_3}^2], [3_{b_2}^4], [3_{b_3}^1], [2_{c_0}^0],$
 $[1_{c_2}^0], [1_{c_3}^0], [1_{a_0}^0], [1_{d_0}^0], [1_{a_1}^2], [1_{e_1}^2], [1_{a_4}^3], [1_{e_4}^3],$
 $[0_{c_1}^4], [0_{d_3}^4], [0_{c_4}^1], [0_{d_2}^1], [1_{a_2}^4], [1_{a_3}^1], [0_{b_0}^0],$

7.5 Desarguesian Geometry.

I will attempt to generalize the results of quaternionian geometry to Desarguesian geometry. It is not clear to me now that polarities exist in general. Indded, we have seen that we can construct a system of homogeneous coordinates over a skew field, for which the incidence property is $\Sigma P_i l_i = 0$, with right equivalence for the lines l and left equivalence for the points P . A line collineation can be represented by a matrix, $m = \mathbf{C}_l l$ while a point collineation requires, $P^T = Q^T \mathbf{C}_P$, to allow for right and left equivalence. For a polarity, these equivalences do not appear to be compatible with a matrix transformation.

It should be kept in mind that every skew field which is not a field has a non trivial subfield

generated by 1, which can be finite (Ore) or not. This implies that given 4 points forming a complete quadrangle, there exist a Pappian subgeometry through these 4 points, the elements of which are obtained from the linear constructions which start from these 4 points.

Theorem.

In any skew field, if a matrix \mathbf{A} has a left inverse and a right inverse, these are equal.

Proof: Let \mathbf{C} be the left inverse of \mathbf{A} and \mathbf{B} be its right inverse, by associativity of matrices,

$$\mathbf{C} = \mathbf{C}(\mathbf{A}\mathbf{B}) = (\mathbf{C}\mathbf{A})\mathbf{B} = \mathbf{B}.$$

Theorem.

IF \mathbf{C}_p is a point collineation, the line collineation \mathbf{C}_l is \mathbf{C}_p^{-1} .

In particular, the point collineation which associates to A_i , A_i and to $(1, 1, 1)$, (q_0, q_1, q_2) is

$$\begin{pmatrix} q_0 & 0 & 0 \\ 0 & q_1 & 0 \\ 0 & 0 & q_2 \end{pmatrix},$$

and the line collineation is

$$\begin{pmatrix} q_0^{-1} & 0 & 0 \\ 0 & q_1^{-1} & 0 \\ 0 & 0 & q_2^{-1} \end{pmatrix}.$$

Proof: If Q is the image of P , and m is the image of l , we want

$0 = P \cdot l = \Sigma P_i l_i = \Sigma Q_i \mathbf{C}_{p_{ij}} \mathbf{C}_{l_{jk}} m_k = \Sigma Q_i m_i = 0$, for all points P and incident lines l iff $\mathbf{C}_l = \mathbf{C}_p^{-1}$.

7.5.1 Desarguesian Geometry of the Hexal Complete 5-Angles.

Notation.

In what follows, I will use the same notation as in involutive Geometry, namely,

$l := P \times Q$, means that the line l is defined as the line incident to P and Q .

If subscripts are used these have the values 0, 1 and 2 and the computation is done modulo 3,

$P \cdot l = 0$ means that the point P is incident to the line l .

When 3 lines intersect, this intersection can be defined in 3 ways, this has been indicated by using (*) after the definition and implies a Theorem.

The labeling used is “H,” for Hypothesis, “D”, for definitions, “C”, for conclusions, “N”, for nomenclature, “P”, for proofs, this labelling being consistent with that of the corresponding definitions.

The special configuration of Desargues.

With this notation, the special configuration of Desargues can be defined by

$$\begin{aligned} a_i &:= A_{i+1} \times A_{i-1}, \quad qa_i = Q \times A_i, \\ Q_i &:= a_i \times qa_i, \quad qq_i := Q_{i+1} \times Q_{i-1}, \end{aligned}$$

$$QA_i := a_i \times qq_i, \quad q_i := A_i \times QA_i,$$

$$QQ_i := q_{i+1} \times q_{i-1}, \quad q := QA_1 \times QA_2(*),$$

and the other conclusion of the special Desargues Theorem can be written,

$$QQ_i \cdot qa_i = 0.$$

Let Q and A_i be

$$Q = (q_0, q_1, q_2), \text{ and } A_0 = (1, 0, 0), \quad A_1 = (0, 1, 0), \quad A_2 = (0, 0, 1),$$

then we have the following results, not obtained in the given order,

$$A_0 = (1, 0, 0), \quad a_0 = [1, 0, 0],$$

$$Q = (q_0, q_1, q_2), \quad q = [q_0^{-1}, q_1^{-1}, q_2^{-1}],$$

$$QA_0 = (0, q_1, -q_2), \quad qa_0 = [0, q_1^{-1}, -q_2^{-1}],$$

$$Q_0 = (0, q_1, q_2), \quad q_0 = [0, q_1^{-1}, q_2^{-1}],$$

$$QQ_0 = (-q_0, q_1, q_2), \quad qq_0 = [-q_0^{-1}, q_1^{-1}, q_2^{-1}],$$

The self duality of the configuration corresponds to the replacement of points by lines where upper case letters are replaced by lower case letters and coordinates by their inverse.

Fundamental Hypothesis, Definitions and Conclusions.

The ideal line and the coideal line.

Given

H0.0. A_i ,

H0.1. M, \overline{M} ,

Let

D1.0. $a_i := A_{i+1} \times A_{i-1}$,

D1.1. $ma_i := M \times A_i, \quad \overline{ma}_i := \overline{M} \times A_i$,

D1.2. $M_i := ma_i \times a_i, \quad \overline{M}_i := \overline{ma}_i \times a_i$,

D1.3. $eul = M \times \overline{M}$,

D2.0. $mm_i := M_{i+1} \times M_{i-1}, \quad \overline{mm}_i := \overline{M}_{i+1} \times \overline{M}_{i-1}$,

D2.1. $MA_i := a_i \times mm_i, \quad \overline{MA}_i := a_i \times \overline{mm}_i$,

D2.2. $m_i := A_i \times MA_i, \quad \overline{m}_i := A_i \times \overline{MA}_i$,

D2.3. $MM_i := m_{i+1} \times m_{i-1}, \quad \overline{MM}_i := \overline{m}_{i+1} \times \overline{m}_{i-1}$,

D2.4. $m := MA_1 \times MA_2(*), \quad \overline{m} := \overline{MA}_1 \times \overline{MA}_2(*)$,

D2.5. $Ima_i := m \times ma_i, \quad \overline{Ima}_i := \overline{m} \times \overline{ma}_i$,

D2.6. $IMa_i := m \times \overline{ma}_i, \quad \overline{IMa}_i := \overline{m} \times ma_i$,

D2.7. $iMA_i := M \times MA_i, \quad \overline{iMA}_i := \overline{M} \times \overline{MA}_i$,

Let

D3.0. $mf_i := M_i \times IMa_i, \quad \overline{mf}_i := \overline{M}_i \times \overline{IMa}_i$,

D3.1. $O := mf_1 \times mf_2(*), \quad \overline{O} := \overline{mf}_1 \times \overline{mf}_2(*)$,

D3.2. $Mfa_i := a_{i+1} \times mf_{i-1}, \quad \overline{Mfa}_i := a_{i+1} \times \overline{mf}_{i-1}$,

$$Mf\overline{a}_i := a_{i-1} \times mf_{i+1}, \quad \overline{Mf}\overline{a}_i := a_{i-1} \times \overline{mf}_{i+1},$$

D3.3. $mf\overline{a}_i := Mfa_{i+1} \times A_{i-1}, \quad \overline{mf}\overline{a}_i := \overline{Mfa}_{i+1} \times A_{i-1}$,

$$mf\overline{a}_i := Mf\overline{a}_{i-1} \times A_{i+1}, \quad \overline{mf}\overline{a}_i := \overline{Mf}\overline{a}_{i-1} \times A_{i+1},$$

D3.4. $Mfm_i := mf\overline{a}_i \times m_i, \quad \overline{Mfm}_i := \overline{mf}\overline{a}_i \times \overline{m}_i$,

then

C3.0. $O \cdot eul = \overline{O} \cdot eul = 0$.

C3.1. $Mfm_i \cdot mf\overline{a}_i = \overline{Mfm}_i \cdot \overline{mf}\overline{a}_i = 0$.

Let

$$D4.0. \text{ } Imm_i := m \times \overline{m}m_i, \overline{Imm}_i := \overline{m} \times mm_i,$$

$$D4.1. \text{ } ta_i := A_i \times Imm_i,$$

$$D4.2. \text{ } T_i := ta_{i+1} \times ta_{i-1},$$

$$D4.3. \text{ } at_i := A_i \times T_i,$$

$$D4.4. \text{ } K_i := at_{i+1} \times at_{i-1},$$

$$D4.5. \text{ } T Aa_i := ta_i \times a_i,$$

$$D4.6. \text{ } poK_i := Taa_{i+1} \times Taa_{i-1},$$

then

$$C4.0. \text{ } \overline{Imm}_i \cdot ta_i = 0.$$

$$C4.1. \text{ } T_i \cdot mf_i = 0.$$

The nomenclature:

N0.0. A_i are the vertices of the triangle,

N0.1. M is the barycenter, \overline{M} is the orthocenter.

N1.0. a_i are the sides.

N1.1. ma_i are the medians, \overline{ma}_i are the altitudes

N1.2. M_i are the mid-points of the sides. \overline{M}_i are the feet of the altitudes

N1.3. eul is the line of Euler,

N2.0. $\{M_i, mm_i\}$ is the complementary triangle,

$\{\overline{M}_i, \overline{m}m_i\}$ is the orthic triangle,

N2.1. MA_i are the directions of the sides,

N2.2. $\{MM_i, m_i\}$ is the anticomplementary triangle.

N2.3. m is the ideal line corresponding to the line at infinity,

\overline{m} is the orthic line which is the polar of \overline{M} with respect to the triangle.

N2.4. Ima_i are the directions of the medians.

IMa_i are the directions of the altitudes.

N3.0. mf_i are the mediatrices,

N3.1. O is the center,

N3.2. Mfm_i are the trapezoidal points,

N4.0. Imm_i are the directions of the antiparallels of a_i with respect to the sides a_{i+1} and a_{i-1} .

N4.1. (T_i, ta_i) is the tangential triangle,

N4.2. at_i are the symmedians,

N4.3. K_i is the triangle of Lemoine.

Theorem.

If we derive a point X and a line x by a given construction from A_i , M and \overline{M} , with the coordinates as given in G0.0 and G0.1, below, and the point \overline{X} and line \overline{x} are obtain by the same construction interchange M and \overline{M} ,

$$X = (f_0(m_0, m_1, m_2), f_1(m_0, m_1, m_2), f_2(m_0, m_1, m_2)),$$

$$x = [g_0(m_0, m_1, m_2), g_1(m_0, m_1, m_2), g_2(m_0, m_1, m_2)],$$

\implies

$$\overline{X} = (f_0(m_0^{-1}, m_1^{-1}, m_2^{-1})m_0, f_1(m_0^{-1}, m_1^{-1}, m_2^{-1})m_1, f_2(m_0^{-1}, m_1^{-1}, m_2^{-1})m_2),$$

$$\overline{x} = [m_0^{-1}g_0(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_1^{-1}g_1(m_0^{-1}, m_1^{-1}, m_2^{-1}), m_2^{-1}g_2(m_0^{-1}, m_1^{-1}, m_2^{-1})].$$

Proof: The point collineation $\mathbf{C}_P = \begin{pmatrix} q_0 & 0 & 0 \\ 0 & q_1 & 0 \\ 0 & 0 & q_2 \end{pmatrix}$, associates to $(1,1,1)$, (q_0, q_1, q_2) ,

and to (m_0, m_1, m_2) , (r_0, r_1, r_2) , if $r_i = m_i q_i$.

In the new system of coordinates,

$$X = (f_0(q_0^{-1}r_0, q_1^{-1}r_1, q_2^{-1}r_2)q_0, f_1(q_0^{-1}r_0, q_1^{-1}r_1, q_2^{-1}r_2)q_1, f_2(q_0^{-1}r_0, q_1^{-1}r_1, q_2^{-1}r_2)q_2).$$

Exchanging q_i and r_i and then replacing q_i by 1 and r_i by m_i is equivalent to substituting m_i for q_i and 1 for r_i , which gives \bar{X} . \bar{x} is obtained similarly.

The line collineation is

$$\begin{pmatrix} q_0^{-1} & 0 & 0 \\ 0 & q_1^{-1} & 0 \\ 0 & 0 & q_2^{-1} \end{pmatrix}.$$

Notation.

$$\begin{aligned} a_i &:= (m_{i+1}^{-1} - m_{i-1}^{-1})(m_{i-1}^{-1} + m_i^{-1})^{-1}, \\ s_i &:= -(m_i^{-1} + m_{i+1}^{-1})(m_i^{-1} + m_{i-1}^{-1})^{-1}, \\ t_i &:= s_{i+2}s_{i+1}, \\ f_i &:= s_i - s_{i+1}^{-1}s_{i-1}^{-1}, \\ g_i &:= t_i^{-1} - t_{i+1}t_{i-1}. \end{aligned}$$

Proof of 7.5.1.

Let

$$G0.0. A_0 = (1, 0, 0), A_1 = (0, 1, 0), A_2 = (0, 0, 1),$$

$$G0.1. M = (1, 1, 1), \bar{M} = (m_0, m_1, m_2),$$

then

$$P1.0. a_0 = (1, 0, 0), a_1 = (0, 1, 0), a_2 = (0, 0, 1),$$

$$P1.1. ma_0 = [0, 1, -1], \bar{m}a_0 = [0, m_1^{-1}, -m_2^{-1}],$$

$$P1.2. M_0 = (0, 1, 1), \bar{M}_0 = (0, m_1, m_2),$$

$$P1.3. eul = [1, (m_1 - m_2)^{-1}(m_2 - m_0), (m_1 - m_2)^{-1}(m_0 - m_1)],$$

$$P2.0. mm_0 = [1, -1, -1], \bar{m}m_0 = [m_0^{-1}, -m_1^{-1}, -m_2^{-1}],$$

$$P2.1. MA_0 = (0, 1, -1), \bar{M}A_0 = (0, m_1, -m_2),$$

$$P2.2. m_0 = [0, 1, 1], \bar{m}_0 = [0, m_1^{-1}, m_2^{-1}],$$

$$P2.3. MM_0 = (1, -1, -1), \bar{M}M_0 = (m_0, -m_1, -m_2),$$

$$P2.4. m = [1, 1, 1], \bar{m} = [m_0^{-1}, m_1^{-1}, m_2^{-1}],$$

$$P2.5. Ima_0 = (2, -1, -1), \bar{I}ma_0 = (2m_0, -m_1, -m_2),$$

$$P2.6. IMa_0 = (m_1 + m_2, -m_1, -m_2), \bar{I}Ma_0 = ((m_1^{-1} + m_2^{-1})m_0, -1, -1),$$

$$P2.7. iMA_0 = [2, -1, -1], \bar{i}MA_0 = [2m_0^{-1}, -m_1^{-1}, -m_2^{-1}],$$

$$P3.0. mf_0 = [(m_1 + m_2)^{-1}(m_1 - m_2), 1, -1],$$

$$\bar{m}f_0 = [m_0^{-1}(m_1^{-1} + m_2^{-1})^{-1}(m_1^{-1} - m_2^{-1}), m_1^{-1}, -m_2^{-1}, 1],$$

$$P3.1. O = (m_1 + m_2, m_2 + m_0, m_0 + m_1),$$

$$\bar{O} = ((m_1^{-1} + m_2^{-1})m_0, (m_2^{-1} + m_0^{-1})m_1, (m_0^{-1} + m_1^{-1})m_2),$$

$$P3.2. Mfa_0 = (1, 0, -(m_0 - m_1)^{-1}(m_0 + m_1)),$$

$$\bar{M}fa_0 = (m_0, 0, (m_0^{-1} - m_1^{-1})(m_0^{-1} + m_1^{-1})^{-1}m_2),$$

$$Mf\bar{a}_0 = (1, (m_2 - m_0)^{-1}(m_2 + m_0), 0),$$

$$\bar{M}f\bar{a}_0 = (m_0, (m_2^{-1} - m_0^{-1})^{-1}(m_2^{-1} + m_0^{-1})m_1, 0),$$

$$P3.3. mfa_0 = [(m_1 + m_2)^{-1}(m_1 - m_2), 1, 0],$$

$$\begin{aligned}
\overline{m}fa_0 &= [m_0^{-1}(m_1^{-1} + m_2^{-1})^{-1}(m_1^{-1} - m_2^{-1}), m_1^{-1}, 0], \\
mf\overline{a}_0 &= [(m_1 + m_2)^{-1}(m_1 - m_2), 0, -1], \\
\overline{m}f\overline{a}_0 &= [m_0^{-1}(m_1^{-1} + m_2^{-1})^{-1}(m_1^{-1} - m_2^{-1}), 0, m_2^{-1}], \\
P3.4. \quad Mfm_0 &= ((m_1 + m_2)(m_1 - m_2)^{-1}, -1, 1), \\
\overline{M}fm_0 &= ((m_1^{-1} - m_2^{-1})^{-1}(m_1^{-1} + m_2^{-1})m_0, -m_1, m_2), \\
P4.0. \quad Imm_0 &= (a_0, 1, s_0), \quad \overline{I}mm_0 = (-a_0, 1, s_0), \\
P4.1. \quad ta_0 &= [0, 1, -s_0^{-1}], \\
P4.2. \quad T_0 &= (1, s_2, s_1^{-1}), \\
P4.3. \quad at_0 &= [0, s_2^{-1}, -s_1] = [0, 1, -t_0], \\
P4.4. \quad K_0 &= (1, t_2^{-1}, t_1), \\
P4.5. \quad Taa_0 &= (0, 1, s_0), \\
P4.6. \quad poK_0 &= [-1, s_2^{-1}, s_1],
\end{aligned}$$

Details of proof:

For P4.0, if the coordinates of Imm_0 are x_0 , 1 and x_2 , we have to solve

$$x_0 + 1 + x_2 = 0, \quad -x_0m_0^{-1} + m_1^{-1} + x_2m_2^{-1} = 0.$$

Multiplying the equations to the right respectively by m_2^{-1} , and -1 or by m_0^{-1} and 1 and adding gives x_0 and x_2 using the notation 7.5.1.

7.5.2 Perpendicularity mapping.

Definition.

Given \overline{M} and a direction I_x , the perpendicular direction I_y is defined by the following construction

$$\begin{aligned}
D5.0. \quad b &:= A_0 \times I_x, \\
D5.1. \quad B &:= b \times a_0, \\
D5.2. \quad c &:= B \times IMa_2, \\
D5.3. \quad C &:= c \times \overline{m}a_0, \\
D5.4. \quad d &:= C \times A_1, \\
D5.5. \quad I_y &:= d \times m,
\end{aligned}$$

Theorem.

If $I_x = (-1 - q, q, 1)$ and $I_y = (1 - r, r, 1)$ then

$r = .$

Proof:

$$\begin{aligned}
P5.0. \quad b &= [0, -q^{-1}, 1], \\
P5.1. \quad B &= (0, q, 1), \\
P5.2. \quad c &= [x, -q^{-1}, 1], \text{ with } x = m_0^{-1}(m_0 + m_1 + m_1q^{-1}), \\
P5.3. \quad C &= (y, m_1, m_2), \text{ with } y = (m_1q^{-1} - m_2)x^{-1}, \\
P5.4. \quad d &= [y^{-1}, 0, -m_2^{-1}], \\
P5.5. \quad I_y &= (y, z, m_2), \text{ with } z = -y - m_2, \\
\text{Therefore } r &= -m_2^{-1}(y + m_2) = -m_2^{-1}(m_2 + (m_1q^{-1} - m_2)(m_0 + m_1 + m_1q^{-1})^{-1}m_0).
\end{aligned}$$

If the skew field we therefore have

$$\begin{aligned}
&-m_2(r + 1)m_0^{-1}((m_0 + m_1)q + m_1) = m_1 - m_2q. \\
&-rm_0^{-1}(m_0 + m_1)q - rm_0^{-1}m_1 - m_0^{-1}m_1q - m_2^{-1}m_1 = 0.
\end{aligned}$$

which is, in general, not an involution.

7.6 The Hughes Planes.

7.6.0 Introduction.

There are essentially 2 methods to algebraize a plane. The first one which start with the work of Desargues coordinatized the plane using 2 coordinates, the difficulty of representing the ideal points or points at infinity can be dealt with by using 3 homogeneous coordinates. This approach has been generalized to perspective planes, for which the only axioms are those of incidence, by using as coordinates, elements of a ternary ring instead of elements in a field. This generalization was given by Marshall Hall in 1943, but its origin can be found, for the case of nearfields, introduced by Dickson (1905), in the most remarkable paper of Veblen and MacLagan-Wedderburn in 1907 (p. 380-382).

In this paper they give, independently from Vahlen the first example of non Pappian Geometry. The independent result consisted in showing that quaternions could be used as coordinates for such a geometry.

The second approach, which can be used in finite planes, is to construct a difference set, of $q = p^k$ integers as a subset $\{0, \dots, q^2 + q\}$ from which the points incident to each line, and the lines incident to every point can be completely derived. This approach was fully examined for the finite Pappian planes by J. Singer in 1938, but it again can be traced in the paper of 1907 (p. 383 and 385). Moreover, the generalization to non Desarguesian planes is given explicitly for a plane of order 9, called Ψ plane by Room and Kirkpatrick.

I do prefer, when applying the notion of difference sets to geometry, to use, instead of it, the terminology of selector introduced by Fernand Lemay, in 1979. (See his most accessible paper of 1983.)

It is the second approach, that I am exploring in this paper, gives many of the results in the form of conjectures.

We will see that to give the incidence properties for planes of the Ψ type and order p^2 we have to give p selectors of p elements, and in a particular notation the points which are incident to $\frac{p-1}{2}$ lines from which all other incidences can be derived. The notation is such that the same incidence tables are valid for the points on any line, giving rise to a fundamental polarity.

One of the advantages of the selector approach is to eliminate the need of addition and multiplication tables in the particular nearfield which greatly simplifies the exploration of new properties with a computer. Many of the planes are special case of Hughes planes, hence the title of the section.

I will assume that p is an odd prime.

7.6.1 Nearfield and coordinatization of the plane.

Definition. [Dickson]

A left nearfield $(N, +, \circ)$ is a set N with binary operations such that

0. N is finite,
1. $(N, +)$ is an Abelian group, with neutral element 0 ,
2. $(N - \{0\}, \circ)$ is an group, with neutral element 1 ,
3. \circ is left distributive over $+$, or

$$\zeta \circ (\xi + \eta) = \zeta \circ \xi + \zeta \circ \eta, \text{ for all } \xi, \eta, \zeta \in N$$

4. $0 \circ \xi = 0$, for all $\xi \in N$.

For a right nearfield, the left distributive law is replaced by the right one and $0 \circ \xi = 0$, is replaced by $\xi \circ 0 = 0$.

Theorem.

In any left nearfield,

0. $\xi \circ 0 = 0$ for all $\xi \in N$.

1. $\xi \circ \eta = 0 \implies \xi = 0$ or $\eta = 0$.

2. $1, -1 \neq 0$.

Definition. [Dickson]

Let n be a non residue of p . A Dickson left nearfield $(N, +, \circ)$ is a set N with the operations

$$(a_0 + b_0\alpha) + (a_1 + b_1\alpha) := ((a_0 + a_1) + (b_0 + b_1)\alpha),$$

$$(a_0 + b_0\alpha) \cdot (a_1 + b_1\alpha) := ((a_0a_1 + e n b_0b_1) + (a_1b_0 + e a_0b_1)\alpha),$$

where $e = +1$ if $a_1^2 - n b_1^2$ is a quadratic residue of p and $e = -1$ otherwise.

A Dickson right nearfield is obtained by the replacement of $(a_1b_0 + e a_0b_1)\alpha$, by $(a_0b_1 + e a_1b_0)\alpha$.

Theorem.

A Dickson left nearfield is a left nearfield.

Definition.

Let β, γ, ξ and η are elements of a Dickson nearfield. In a Hughes plane, the points are the triples

$$(1, \beta, \gamma), (0, 1, \gamma), (0, 0, 1),$$

and the lines are the triples

$$[\eta, \xi, -1], [\eta, -1, 0], [1, 0, 0]$$

A point (P_0, P_1, P_2) is incident to a line $[l_0, l_1, l_2]$ if and only if

$$P_0l_0 + P_1l_1 + P_2l_2 = 0.$$

A point or a line is real if the coefficient of α in its coordinates are 0. A point or line is complex, otherwise.

The notation is used to indicate the close relationship with the corresponding coordinates in a ternary ring, see for instance Artzy, p. 203-203,

for the points: $(b, c) = (1, b, c)$, $(c) = (0, 1, c)$, $(\infty) = (0, 0, 1)$,

for the lines: $[x, y] = [y, x, -1]$, $[y] = [y, 1, 0]$, $[\infty] = [1, 0, 0]$

indeed $1 \cdot y + b \cdot x - c = 0$ corresponds to $c = b \cdot x + y$, giving the ternary ring conditions of incidence.

Theorem. [Hughes]

A Hughes plane is of Lenz-Barlotti type I.1

See Hughes, Rosati and Dembowski, p. 247. The simplest case $p = 3$, is given by Veblen and MacLagan-Wedderburn p. 383, it is called in this case a Ψ plane by Room and Kirkpatrick.

Theorem.

A real line has $p + 1$ real and $p^2 - p$ complex points incident to it.
 A complex line has 1 real and p^2 complex points incident to it.

See, for instance, Room and Kirkpatrick.

Theorem.

The p selectors and the negative inverses of the fundamental selector modulo $p^2 + p + 1$ form a partition of the set $\{1, \dots, p^2 + p\}$.

Theorem.

The $p^4 + p^2 + 1$ points are partitioned into $p^2 + p + 1$ real points and $p - 1$ phyla of complex points. Each phylum consists of p classes. Each class consists of $p^2 + p + 1$ points, which form by definition a coplane.

Starting with the work of L. E. Dickson of 1905, non-Desarguesian planes of order 9 were discovered by Veblen and Wedderburn in 1907, I will here consider only one of these which is self dual, and for which non trivial polarities exists, and refer to the work of G. Zappa (1957), T. G. Ostrom (1964), D. R. Hughes (1957) and T. G. Room and P. B. Kirkpatrick (1971) for further reading.

The synthetic definition used can be traced to Veblen and Wedderburn, who first consider points obtained by applying a transformation (see p. 383), later generalized by J. Singer. The notation is inspired by Room and Kirkpatrick (see Table 5.5.4) using the same method I used for the finite plane reversing the indices for lines.

An alternate definition, (5.6.1), is given by Room and Kirkpatrick.

7.6.2 Miniquaternion nearfield.**Theorem.**

In any left nearfield Q_9 , of order 9,

0. $\{0, 1, -1\} \approx Z_3$.
1. $\xi + \xi + \xi = 0$, for all $\xi \in Q_9$,
2. $-1 \circ \xi = \xi \circ (-1) = \xi$, for all $\xi \in Q_9$,
3. $(-\xi) \circ \eta = \xi \circ (-\eta) = -(\xi \circ \eta)$, for all $\xi, \eta \in Q_9$,
4. $(-\xi) \circ (-\eta) = \xi \circ \eta$, for all $\xi, \eta \in Q_9$,
5. Given $\kappa \in Q_9^* := Q_9 - 0$, $\lambda = s - \kappa r$ determines a one to one correspondance between the elements $\lambda \in Q_9$ and the pairs (r, s) , $r, s \in Z_3$.
6. Q_9 being an other nearfield of order 9, the groups $(Q_9, +)$ and $(Q'_9, +)$ are isomorphic.
7. Besides $GF(3^2)$ there is only one nearfield of order 9, which is the smallest nearfield which is not a field, (Zassenhaus, 1936).

Exercise.

Determine the correspondance of 7.6.2.5.

Definition.

The left miniquaternions is the set $Q_9 := \{0, \pm 1, \pm \alpha, \pm \beta, \pm \gamma\}$ with the operations of addition and multiplications defined from,

$$\begin{aligned}\xi + \xi + \xi &= 0 \text{ for all } \xi \in Q_9, \\ \alpha - 1 &= \beta, \alpha + 1 = \gamma, \\ \alpha^2 &= \beta^2 = \gamma^2 = -\alpha\beta\gamma = -1.\end{aligned}$$

The set $Q_9^* := \{\pm \alpha, \pm \beta, \pm \gamma\}$.

For the right miniquaternions, we replace $\alpha\beta\gamma = 1$ by $\alpha\beta\gamma = -1$.

Theorem.

0. $\alpha - \beta = \beta - \gamma = \gamma - \alpha = 1, \alpha + \beta + \gamma = 0$.
1. $-\beta\gamma = \gamma\beta = \alpha, -\gamma\alpha = \alpha\gamma = \beta, -\alpha\beta = \beta\alpha = \gamma$.
2. the multiplication is left distributive, $\tau(\rho + \sigma) = \tau\rho + \tau\sigma$,
for all $\rho, \sigma, \tau \in Q_9$.
3. $\{Q_9, +, \cdot\}$ is a left nearfield.
4. $\{Q_9, +, \cdot\}$ is not a field, e. g.
 $\alpha(\alpha + \beta) = \alpha(-\gamma) = \beta, \alpha\alpha + \alpha\beta = -1 + \gamma = \alpha$.

+	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
1	-1	0	γ	$-\beta$	α	$-\gamma$	β	$-\alpha$
-1	0	1	β	$-\gamma$	γ	$-\alpha$	α	$-\beta$
α	γ	β	$-\alpha$	0	$-\gamma$	1	$-\beta$	-1
5. $-\alpha$	$-\beta$	$-\gamma$	0	α	-1	γ	1	β
β	α	γ	$-\gamma$	-1	$-\beta$	0	$-\alpha$	1
$-\beta$	$-\gamma$	$-\alpha$	1	γ	0	β	-1	α
γ	β	α	$-\beta$	1	$-\alpha$	-1	$-\gamma$	0
$-\gamma$	$-\alpha$	$-\beta$	-1	β	1	α	0	γ
·	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
1	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
-1	-1	1	$-\alpha$	α	$-\beta$	β	$-\gamma$	γ
α	α	$-\alpha$	-1	1	$-\gamma$	γ	β	$-\beta$
$-\alpha$	$-\alpha$	α	1	-1	γ	$-\gamma$	$-\beta$	β
β	β	$-\beta$	γ	$-\gamma$	-1	1	$-\alpha$	α
$-\beta$	$-\beta$	β	$-\gamma$	γ	1	-1	α	$-\alpha$
γ	γ	$-\gamma$	$-\beta$	β	α	$-\alpha$	-1	1
$-\gamma$	$-\gamma$	γ	β	$-\beta$	$-\alpha$	α	1	-1

For the right miniquaternions, we change the sign of the products in 1. and exchange rows and columns for the multiplication table, e.g. $\alpha\beta = \gamma$.

7.6.3 The first non-Pappian plane, by Veblen and Wedderburn.

Definition. [Veblen-Wedderburn]

The points P are $(x, y, 1)$, $(x, 1, 0)$, $(1, 0, 0)$, the lines l are $[1, b, c]$, $[0, 1, c]$, $[0, 0, 1]$, and the incidence is $P \cdot l = 0$, where x, y, b and c are elements of a left nearfield.

Theorem. [Veblen-Wedderburn]

With b, c, b', c' in Q_9 ,

0. $[1, b, c] \times [1, b', c'] = (-(yb + c), y, 1)$, with $y(b - b') = -(c - c')$.
1. $[1, b, c] \times [0, 1, c'] = (c'b - c, -c', 1)$,
2. $[1, b, c] \times [0, 0, 1] = (-b, 1, 0)$,
3. $[0, 1, c] \times [0, 1, c'] = (1, 0, 0)$,
4. $[0, 1, c] \times [0, 0, 1] = (1, 0, 0)$,

Theorem. [Veblen-Wedderburn]

Let $(a(b + c) = a b + a c)$

$$0. \mathbf{M} := \begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & -1 \end{pmatrix},$$

1. $A_0 := (-1, 0, 1)$, $B_0 := (-\gamma, \alpha, 1)$, $C_0 := (\beta, -\alpha, 1)$, $D_0 := (-\beta, \gamma, 1)$, $E_0 := (\alpha, -\gamma, 1)$,
 $F_0 := (\gamma, -\beta, 1)$, $G_0 := (-\alpha, \beta, 1)$,
2. $A_j := \mathbf{M}^j A_0$, $B_j := \mathbf{M}^j B_0$, \dots , for $j = 1$ to 12 ,
3. $a_j := \{M^j X_i\}$, $X_i \in a_0$, and similarly for b_j to g_j .
4. $a_0 := [1, 1, 1]$, $b_0 := [1, \alpha, 1]$, $c_0 := [1, -\alpha, 1]$, $d_0 := [1, \gamma, 1]$, $e_0 := [1, -\gamma, 1]$, $f_0 := [1, -\beta, 1]$,
 $g_0 := [1, \beta, 1]$,
then
5. M is of order 13.
6. $a_0 = \{A_0, A_1, A_3, A_9, B_0, C_0, D_0, E_0, F_0, G_0\}$,
 $b_0 = \{A_0, B_1, B_8, D_3, D_{11}, E_2, E_5, E_6, G_7, G_9\}$,
 $c_0 = \{A_0, C_1, C_8, E_7, E_9, F_3, F_{11}, G_2, G_5, G_6\}$,
 $d_0 = \{A_0, B_7, B_9, D_1, D_8, F_2, F_5, F_6, G_3, G_{11}\}$,
 $e_0 = \{A_0, B_2, B_5, B_6, C_3, C_{11}, E_1, E_8, F_7, F_9\}$,
 $f_0 = \{A_0, C_7, C_9, D_2, D_5, D_6, E_3, E_{11}, F_1, F_8\}$,
 $g_0 = \{A_0, B_3, B_{11}, C_2, C_5, C_6, D_7, D_9, G_1, G_8\}$,
7. $A_0 = \{a_0, a_4, a_{10}, a_{12}, b_0, c_0, d_0, e_0, f_0, g_0\}$,
 $B_0 = \{a_0, b_5, b_{12}, d_4, d_6, e_7, e_8, e_{11}, g_2, g_{10}\}$,
 $C_0 = \{a_0, c_5, c_{12}, e_2, e_{10}, f_4, f_6, g_7, g_8, g_{11}\}$,
 $D_0 = \{a_0, b_2, b_{10}, d_5, d_{12}, f_7, f_8, f_{11}, g_4, g_6\}$,

$$\begin{aligned} E_0 &= \{a_0, b_7, b_8, b_{11}, c_4, c_6, e_5, e_{12}, f_2, f_{10}\}, \\ F_0 &= \{a_0, c_2, c_{10}, d_7, d_8, d_{11}, e_4, e_6, f_5, f_{12}\}, \\ G_0 &= \{a_0, b_4, b_6, c_7, c_8, c_{11}, d_2, d_{10}, g_5, g_{12}\}, \end{aligned}$$

$$8. \quad X_j \iota x_k \implies X_{j+l \bmod 13} \iota x_{k+l \bmod 13}.$$

Given a_0 , to g_0 , it is easy to verify that A_0 is on all these lines and determine B_0 to G_0 all on a_0 and B_0 on b_0 , C_0 on c_0 ,

Having determined, the other points using 2, it is easy to verify which points are on b_0 ,

The notation helps greatly in justifying that 2 points have one and only one line in common and 2 lines have only one point in common. The notation can be made even more compact. See 7.6.4.

The following are the powers of M .

$$\begin{aligned} M^2 &= \begin{pmatrix} 1 & -1 & 0 \\ -1 & 0 & -1 \\ 1 & 1 & 1 \end{pmatrix}, M^3 = \begin{pmatrix} -1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & -1 & 0 \end{pmatrix}, M^4 = \begin{pmatrix} -1 & -1 & 1 \\ 1 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, M^5 = \begin{pmatrix} 0 & -1 & 1 \\ 1 & 1 & -1 \\ 1 & 0 & 1 \end{pmatrix}, \\ M^6 &= \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 1 & -1 & 0 \end{pmatrix}, M^7 = \begin{pmatrix} -1 & 1 & -1 \\ -1 & 1 & 1 \\ -1 & 0 & 1 \end{pmatrix}, M^8 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -1 & 1 \\ -1 & -1 & 1 \end{pmatrix}, M^9 = \begin{pmatrix} 0 & 0 & 1 \\ -1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}, \\ M^{10} &= \begin{pmatrix} 0 & -1 & -1 \\ 0 & 0 & -1 \\ 1 & -1 & -1 \end{pmatrix}, M^{11} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ -1 & 1 & 1 \end{pmatrix}, M^{12} = \begin{pmatrix} 0 & -1 & 0 \\ -1 & -1 & -1 \\ 1 & 1 & 0 \end{pmatrix}, M^{13} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \end{aligned}$$

Example. [Veblen-Wedderburn]

With the notation

non-Desargues($C\langle c_0, c_1, c_2 \rangle, \{A_0, A_1, A_2\}\{a_0, a_1, a_2\}, \{B_0, B_1, B_2\}\{b_0, b_1, b_2\};$
 $\{C_0, C_1, C_2\}\{d_0, d_1, d_2\}$), with $d_i := C_{i+j} \times C_{i-j}$,

the following configuration shows that the Desargues axiom is not satisfied

non-Desargues($A_0\langle b_0, f_0, d_0 \rangle, \{B_1, C_7, F_2\}\{c_{12}, e_8, e_9\}, \{D_3, E_3, D_1\}\{b_{11}g_7, a_3\};$
 $\{G_5, B_{10}, F_3\}\{d_1, c_0, b_9\}$).

7.6.4 The miniquaternionian plane Ψ .

Definition.

With $i \in \{0, 1, 2\}$, $i' \in \{0', 1', 2'\}$, $j \in \{0, 1, \dots, 12\}$, and the addition being performed modulo 3 for the first element of a pair, and modulo 13, for the second element in the pair or for the element, if single, then the elements and incidence in the miniquaternionian plane Ψ are defined as follows. (See 7.6.4

0. The 91 points P are $(j), (i, j), (i', j),$

1. The 91 lines l are $[j], [i, j], [i', j],$

2. The incidence is defined by

$$\begin{aligned} [j] &:= \{(-j), (1-j), (3-j), (9-j), (i, -j), (i', -j)\}, \\ [i, j] &:= \{(-j), (i, 2-j), (i, 5-j), (i, 6-j), (i' + 1, 3-j), (i' + 1, 11-j), \\ &\quad (i' - 1, 7-j), (i' - 1, 9-j), (i', 1-j), (i', 8-j)\}, \\ [i', j] &:= \{(-j), (i', 2-j), (i', 5-j), (i', 6-j), (i - 1, 3-j), (i - 1, 11-j), \\ &\quad (i + 1, 7-j), (i + 1, 9-j), (i, 1-j), (i, 8-j)\}. \end{aligned}$$

giving the 10 points on each line. i and i' in the same definition correspond to the same integer, 0, 03-' or 1, 1'

Exercise.

7.6.4.2 is similar to the use of ordered cosets to determine efficiently operations of finite as well as infinite groups. In this case, $[j]$ is a subplane, $[i, j]$ and $[i', j]$ are copseudoplanes.

0. Perform a similar representation of points, lines and incidence starting with a subplane which is a Fano plane.
1. Determine similar representations for non Desarguesian geometries of order 5^2 , using a subplane of order 4, or of order 5 ($651 = 31 \cdot 21$).
2. Determine other such representation for non Desarguesian geometries of higher order.

Theorem.

The same incidence relations obtain, if we interchange points and lines in 7.6.4.2.

Theorem. [see Room and Kirkpatrick]

0. 0 The correspondance (j) to $[j]$ and (i, j) to $[i, j]$ and (i', j) to $[i', j]$ is a polarity \mathcal{P}_0 (\mathcal{J}^*).
- 1 The 16 auto-poles are (0) , (7) , (8) , (11) , $(0, 8)$, $(0, 12)$, $(1, 4)$, $(1, 7)$, $(2, 10)$, $(2, 11)$, $(0', 8)$, $(0', 12)$, $(1', 4)$, $(1', 7)$, $(2', 10)$, $(2', 11)$.
1. 0 The correspondance (j) to $[j]$ and (i, j) to $[i', j]$ and (i', j) to $[i, j]$ is a polarity \mathcal{P}_1 (\mathcal{J}'^*).
- 1 The 22 auto-poles are (0) , (7) , (8) , (11) , $(0, 1)$, $(0, 3)$, $(0, 9)$, $(1, 1)$, $(1, 3)$, $(1, 9)$, $(2, 1)$, $(2, 3)$, $(2, 9)$, $(0', 1)$, $(0', 3)$, $(0', 9)$, $(1', 1)$, $(1', 3)$, $(1', 9)$, $(2', 1)$, $(2', 3)$, $(2', 9)$.
- 2 (0) , (7) , (8) , (11) , $(0, 1)$, $(1, 9)$, $(2, 3)$, $(0', 9)$, $(1', 3)$, $(2', 1)$, (0) , (7) , (8) , (11) , $(1, 1)$, $(2, 9)$, $(0, 3)$, $(2', 9)$, $(0', 3)$, $(1', 1)$, (0) , (7) , (8) , (11) , $(2, 1)$, $(0, 9)$, $(1, 3)$, $(1', 9)$, $(2', 3)$, $(0', 1)$ are ovals.

Exercise.

0. Prove that the correspondance (j) to $[j]$ and (i, j) to $[(i + 1)', j]$ and (i', j) to $[i - 1, j]$ is a polarity \mathcal{P}_2 .
1. Prove that the correspondance (j) to $[j]$ and (i, j) to $[(i - 1)', j]$ and (i', j) to $[i + 1, j]$ is a polarity \mathcal{P}_3 .

Exercise.

0. Determine a configuration in 7.6.4.0.2, which gives an example where the Theorem of Pascal is satisfied and an other, in which it is not satisfied.
1. Determine ovals which are subsets of 7.6.4.1.1.

Theorem.

The polar m of a point M with respect to a triangle is incident to that point.

Indeed, we can always assume that the triangle consists of the real points $A_0 = (0)$, $A_1 = (1)$, $A_2 = (2)$, and that $M = (5) = (1, 1, 1)$. It follows that $m = [4] = [1, 1, 1]$ which is incident to M .

Exercise.

Check that the other points and lines of the polar construction are $M_i = (4), (8), (3)$, $MA_i = (10), (12), (9)$, $MM_i = (7), (6), (11)$, $a_i = [12], [1], [0]$, $ma_i = [9], [8], [11]$, $m_i = [3], [2], [7]$, $mm_i = [6], [10], [5]$.

Theorem. [see Room and Kirkpatrick]

0. The planes obtained by taking the complete quadrangle associated with 3 real points A_0, A_1, A_2 , and a point \overline{M} which such that none of the lines $\overline{M} \times A_i$ are real are Fano planes associated with Z_2 .
1. There are $(\frac{1}{6}13.12.9).24 = 5616$ Fano planes that contain 3 real points.

Notation.

For a Fano subplane with 7 elements, I will use the notation associated with the selector 0, 1, 3 and construction:

Given a complete quadrangle 0, 1, 2, 5,

$0^* := 0 \times 1$, $6^* := 1 \times 2$, $1^* := 2 \times 0$, $5^* := 2 \times 5$, $3^* := 0 \times 5$, $2^* := 1 \times 5$,

$3 := 0^* \times 5^*$, $4 := 6^* \times 3^*$, $6 := 1^* \times 2^*$, $4^* := 3 \times 6$. The Fano plane property implies $4 \times 4^*$.

The configuration is denoted by $\text{Fano}(0, 1, 2, 3, 4, 5, 6, 0^*, 1^*, 2^*, 3^*, 4^*, 5^*, 6^*)$.

Example.

The following is a Fano plane configuration: $\text{Fano}((0), (1), (2), (2, 0), (1, 1), (0, 3), (1', 12), [0], [1], [0, 12], [1', 0], [1', 6], [0', 11], [12])$.

Exercise.

Determine the Fano plane associated with $(0), (1), (2), (0, 7)$.

Comment.

The correspondance between the notation of Veblen-Wedderburn and Room-Kirkpatrick is

Veblen – Wedderburn	a_j	b_j	c_j	d_j	e_j	f_j	g_j
Room – Kirkpatrick	k_j	a_j	b_j	c_j	a_j	b_j	c_j
De Vogelaere	$[-j]$	$[0, -j]$	$[2', -j]$	$[1, -j]$	$[0', -j]$	$[1', -j]$	$[2, -j]$
Veblen – Wedderburn	A_j	B_j	C_j	D_j	E_j	F_j	G_j
Room – Kirkpatrick	K_j	A_j	C_j	B_j	A_j	C_j	B_j
De Vogelaere	(j)	$(0', j)$	$(2, j)$	$(1', j)$	$(0, j)$	$(1, j)$	$(2', j)$

Example. [Veblen-Wedderburn]

The example 7.6.3 becomes with the above notation

$((0)\langle[0, 0], [1', 0], [2, 0]\rangle, \{(0, 1), (1, 7), (1', 2)\}\{[1, 1], [0', 8], [0', 9]\}, \{(2, 3), (0'3), (2, 1)\}\{[0, 11], [2', 7], [10]\};$
 $\{(2', 5), (0, 10), (1', 3)\}\{[2, 1], [1, 0], [0, 4]\}$.

Problem.

Can we characterize the plane Ψ using Theorem 7.6.4.0.

Definition.

The Singer matrix $\mathbf{G} := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$. Its powers \mathbf{G}^k are the columns

$k, k+1, k+2$ of

$k =$	0	1	2	3	4	5	6	7	8	9	10	11	12
	1	0	0	1	0	1	1	1	-1	-1	0	1	-1
	0	1	0	1	1	1	-1	-1	0	1	-1	1	0
	0	0	1	0	1	1	1	-1	-1	0	1	-1	1

move to g6a.tex:

Answer to 7.6.2.

$\kappa =$	$\lambda =$	0	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
α	r	0	0	0	-1	1	-1	1	-1	1
s		0	1	-1	0	0	-1	1	1	-1
β	r	0	0	0	-1	1	-1	1	-1	1
s		0	1	-1	1	-1	0	0	-1	1
γ	r	0	0	0	-1	1	-1	1	-1	1
s		0	1	-1	-1	1	1	-1	0	0

of r .

For $-\alpha, -\beta, -\gamma$, change the sign

Definition.

The elements and incidence in the miniquaternionian plane Ψ are defined as follows.

0. The points are (ξ_0, ξ_1, ξ_2) with right equivalence,
- 1.
2. A point P is incident to a line l iff

Partial answer to 7.6.4.

For $n = 7^2$, $2451 = 57.43$, for $n = 9^2$, $6643 = 91.73$, for $n = 11^2$, $14763 = 57.259$, For $n = 13^2$, $28731 = 3.9577$.

Answer to 7.6.4.

We have $\text{Fano}((0), (1), (2), (1'0), (2, 1), (0, 7), (1', 12), [0], [1], [0, 12], [2', 0], [1', 6], [0, -2], [12])$.

Answer to 7.6.4.

$(7) \times (8) = [6], [6] \times [0] = (3), (8) \times (0) = [1], [1] \times [7] = (2), (0) \times (7) = [9], [9] \times [8] = (5), \langle (3), (2), (5); [11] \rangle$.

$(7) \times (8) = [6], [6] \times [0, 1] = (1', 7), (8) \times (0, 1) = [0, 5], [0, 5] \times [7] = (0', 6), (0, 1) \times (7) = [2', 6], [2', 6] \times [8] = (2, 5), (2, 5)$ is not incident to $(1', 7) \times (0'6) = [2, 2]$.

This has not been checked.

From Dembowski, p. 129

Definition.

A linear ternary ring $(\Sigma, +, \cdot)$ is called a cartesian field iff $(\Sigma, +)$ is associative and is therefore a group.

Definition.

A cartesian field is called a quasifield iff the right distributivity law holds:

$$(x + y)z = xz + yz.$$

Artzy adds that $xa = xb + c$ has a unique solution, but this is a property (28). This is Veblen-Wedderburn.

Definition.

A quasifield is called a semifield iff the left distributivity law holds:

$$z(x + y) = zx + zy.$$

Definition.

A quasifield is called a nearfield iff (Σ, \cdot) is associative and is therefore a group.

Definition.

A semifield is called a alternative field iff $x^2y = x(xy)$ and $xy^2 = (xy)y$.

Theorem.

P is (p, L) transitive iff P is (p, L) Desarguesian. p is point, L is a line. Dembowski p.123, 16

Let $Q_0 = (79), Q_1 = (80), Q_2 = (90)$, and $U = (81)$ then $q_2 = [79], q_0 = [90], q_1 = [80], v = [88], i = [78], V = (78), I = (82), j = [89], W = (89)$,

Points on q_2 : 86,12,25,38,51,64,77

Points on q_1 : 85,11,24,37,50,63,76

$11 \times 12 = [7] : 84(78, 86), 8(51, 25), 43(77, 64), 48(86, 38), 52(12, 12), 54(25, 78), 66(64, 80), 72(38, 51),$
 $11 \times 25 = [61] : 82(78, 80), 0(64, 64), 18(12, 51), 28(51, 78), 33(77, 12), 58(38, 86), 61(86, 25), 62(25, 38),$
 $11 \times 38 = [75] : 81(78, 78), 4(38, 25), 14(12, 80), 19(77, 86), 36(51, 64), 70(64, 38), 73(25, 51), 74(86, 12),$
 $11 \times 51 = [4] : 87(86, 86), 1(38, 80), 2(77, 78), 46(25, 64), 55(78, 38), 57(51, 12), 69(64, 51), 75(12, 25),$
 $11 \times 64 = [8] : 83(86, 78), 7(64, 25), 10(77, 51), 42(78, 12), 47(12, 64), 53(51, 80), 65(38, 38), 71(25, 86),$
 $11 \times 77 = [68] : 88(86, 80), 5(38, 64), 13(51, 51), 21(77, 38), 30(25, 12), 32(64, 86), 67(12, 78), 68(78, 25),$

Coordinates of points:

(0)	64, 64	38, 80	77, 78	78, 51	38, 25	38, 64	51, 86	64, 25
(8)	51, 25	86, 77	77, 51	80, 77	12	51, 51	12, 80	64, 78
(16)	78, 77	12, 38	12, 51	77, 86	51, 38	77, 38	86, 64	64, 77
(24)	80, 64	25	77, 77	25, 80	51, 78	78, 64	25, 12	25, 77
(32)	64, 86	77, 12	64, 12	86, 51	51, 64	80, 51	38	25, 25
(40)	77, 80	38, 78	78, 12	77, 64	77, 25	12, 86	25, 64	12, 64
(48)	86, 38	38, 12	80, 38	51	12, 12	51, 80	25, 78	78, 38
(56)	51, 77	51, 12	38, 86	12, 77	38, 77	86, 25	25, 38	80, 25
(64)	64	38, 38	64, 80	12, 78	78, 25	64, 51	64, 38	25, 86
(72)	38, 51	25, 51	86, 12	12, 25	80, 12	77	78	80, 80
(80)	0	78, 78	78, 80	86, 78	78, 86	80, 86	86	86, 86
(88)	86, 80	80, 78	∞					

Coordinates of lines:

[0]	78, 38	38	77, 78	12, 12	51, 77	86, 38	12, 86	12, 77
[8]	64, 77	77, 25	64, 12	80, 25	51, 80	78, 12	12	64, 78
[16]	25, 25	77, 64	86, 12	25, 86	25, 64	51, 64	64, 38	51, 25
[24]	80, 38	77, 80	78, 25	25	51, 78	38, 38	64, 51	86, 25
[32]	38, 86	38, 51	77, 51	51, 12	77, 38	80, 12	64, 80	78, 77
[40]	77	38, 78	51, 51	12, 38	86, 77	51, 86	51, 38	25, 38
[48]	38, 64	25, 51	80, 64	12, 80	78, 51	51	25, 78	64, 64
[56]	38, 25	86, 51	64, 86	64, 25	12, 25	25, 77	12, 64	80, 77
[64]	38, 80	78, 64	64	12, 78	77, 77	25, 12	86, 64	77, 86
[72]	77, 12	38, 12	12, 51	38, 77	80, 51	25, 80	78, 80	∞
[80]	80	78, 78	86	86, 78	86, 86	80, 86	86, 80	78, 86
[88]	78	80, 78	80, 80					

$[80] : 11(80, 77), 24(80, 64), 37(80, 51), 50(80, 38), 63(80, 25), 76(80, 12), 79(80, 80), 85(80, 86), 89(80, 78), 90(/inf$
 $B = A + \alpha, (A, B) \iota [V, Y], V = (78), (76) = (80, 12) = (0, \alpha), Y \times V = (78) \times (76) = [13].$

$[13] : 78(78), 15(64, 78), 18(12, 51), 19(77, 86), 68(78, 25), 76(80, 12), 46(25, 64), 48(86, 38), 53(51, 80), 60(38, 77)$

hence $12 = 80 + \alpha, 51 = \alpha + \alpha = -\alpha, 25 = 78 + \alpha = 1 + \alpha = \gamma, 64 = 25 + \gamma = \gamma + \gamma = -\beta,$

$38 = 86 + \alpha = -1 + \alpha = \beta, 77 = 38 + \alpha = \beta + \alpha = -\gamma.$

∞	0	1	-1	α	$-\alpha$	β	$-\beta$	γ	$-\gamma$
90	80	78	86	12	51	38	64	25	77

$[\alpha, 0] = (12) \times (80, 80) = (12) \times (79) = [51], (a, b) \iota [51] \implies b = a \cdot \alpha.$

$(42) = (78, 12) = (\underline{1}, \alpha) \implies \alpha = 1 \times \alpha,$

$(45) = (12, 86) = (\alpha, \underline{-1}) \implies -1 = \alpha \times \alpha,$

$(23) = (64, 77) = (-\beta, -\gamma) \implies -\gamma = -\beta \times \alpha,$

$(28) = (51, 78) = (-\alpha, \underline{1}) \implies 1 = -\alpha \times \alpha,$

$(35) = (86, 51) = (\underline{-1}, -\alpha) \implies -\alpha = \underline{-1} \times \alpha,$

Using DATA 6,0, 6,4, 6,10, 6,12, 0,0, 1,0, 2,0, 3,0, 4,0, 5,0 DATA 6,0, 0,7, 0,8, 0,11, 3,2, 3,10, 4,4, 4,6, 5,5, 5,12 gives the same multiplication table give left not right distributive law with $Q_i = 79, 81, 87, U = (83), \alpha = (12), q_0 = [87] = \{79, 81, 82, 86, 4, 17, \dots\},$

$q_1 = [81] = \{79, 85, 87, 88, 10, 23, \dots\},$

$q_2 = [79] = \{81, 87, 89, 90, 12, 25, \dots\},$

with case 7, data 79,81,87,83,12:

$\infty = 87, \underline{0} = 81, \underline{1} = 89, \underline{-1} = 90, \alpha = 12, -\alpha = 77, \beta = 38, -\beta = 51, \gamma = 25, -\gamma = 64.$

This is a try for a section to be included in g19.tex between Moufang and Desargues.

7.7 Axiomatic.

7.7.1 Veblen-MacLagan planes.

Introduction.

The first example of a Veblen-Wedderburn plane was given in 1907 by Veblen and MacLagan-Wedderburn. It is associated to the algebraic structure of a nearfield, which is a skew field which lacks the left distributive law, hence is an other plane between the Veblen-Wedderburn plane and the Desarguesian plane.

Axiom. [Da] ⁶

Given a Veblen-Wedderburn plane, 2 points Q_1 and Q_2 on the ideal line and an other point Q_0 not on it, any 2 parallelograms A_i and B_i with directions Q_1 and Q_2 , with no sides in common $\dots, ???$, such that A_j and B_j are perspective from Q_0 for $j = 0$ To 2, imply that A_3 and B_3 are perspective from Q_0 .

Notation.

$Da(\{Q_0, Q_1, Q_2\}, \{A_j\}, \{B_j\}).$

Definition.

A Veblen-MacLagan plane is a Veblen-Wedderburn plane in which the axiom Da is satisfied.

Lemma. [For Associativity]

H1.0. A_0, a_{12}, x , (See Fig. 2?.)

D1.0. $a_{01} := Q_1 \times A_0, a_{02} := Q_2 \times A_0,$

D1.1. $A_1 := a_{01} \times a_{12}, A_2 := a_{02} \times a_{12},$

D1.2. $a_{13} := Q_2 \times A_1, a_{23} := Q_1 \times A_2, A_3 := a_{13} \times a_{23},$

D2.0. $a_0 := Q_0 \times A_0, a_1 := Q_0 \times A_1, a_2 := Q_0 \times A_2, a_3 := Q_0 \times A_3, D2.1. B_0 := a_0 \times y,$
 $b_{01} := Q_1 \times B_0, b_{02} := Q_2 \times B_0,$

D2.1. $B_1 := b_1 \times b_{01}, B_2 := b_2 \times b_{02}, D2.2. b_{13} := Q_2 \times B_1, b_{23} := Q_1 \times B_2, B_3 := b_{13} \times b_{23},$

C1.0. $B_3 \iota b_3,$

Moreover

$A_0 = (A, B), A_1 = (A', B), A_2 = (A, B'), A_3 = (A', B'), B_0 =$

Proof: $Da(\{Q_0, Q_1, Q_2\}, \{A_j\}, \{B_j\}).$

⁶Da for Desargues leading to associativity of multiplication.

Theorem.

In a Veblen-MacLagan plane, the ternary ring $(\Sigma, *)$ is a nearfield.:

0. $(\Sigma, +)$ is an Abelian group,
1. $(\Sigma - \{0\}, \cdot)$ is a group,
2. $(\Sigma, *) = (\Sigma, +, \cdot)$ is right distributive, $(a + b) \cdot c = a \cdot c + b \cdot c$.

7.7.2 Examples of Perspective planes.**Theorem.**

e Desarg.?

0. The Cayleyian plane is not a Veblen-MacLagan plane.

Definition.

A miniquaternion plane

Theorem.

0. A miniquaternion plane is a Veblen-MacLagan plane.
1. A miniquaternion plane is not a Moufang plane.

Tables.

The following are in an alternate notation the known table for $p = 3$ and a new table for $p = 5$. The other incidence are obtained by adding one to the subscripts of the lines and subtracting one for the subscript of the points.

7.8 Bibliography.

1. Artzy, Rafael, *Linear Geometry*, Reading Mass., Addison-Wesley, 1965, 273 pp.
2. Baumert, Leonard D., *Cyclic Difference Sets*, N. Y., Springer, 1971.
3. Dembowski, Peter, *Finite Geometries*, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Band 44, Springer, New-York, 1968, 375 pp.
4. Dickson, *Göttingen Nachrichten*, 1905, 358-394.
5. Hall, Marshall, *Projective Planes*, *Trans. Amer. Math. Soc.*, Vol. 54, 1943, 229-277.
6. Hughes, D. R., *A class of non-Desarguesian projective planes*, *Canad. J. of Math.*, Vol. 9, 1957, 378-388. (I,9.p.1)
7. Lemay, Fernand, *Le dodécaèdre et la géométrie projective d'ordre 5*, p. 279-306 of Johnson, Norman L., Kallaher, Michael J., Long Calvin T., Edit., *Finite Geometries*, N. Y., Marcel Dekker Inc. 1983.

8. MacLagan-Wedderburn, J. H., A theorem on finite algebras, *Trans. Amer. Math. Soc.*, Vol. 6, 1905, 349. (*A finite skew-field is a field*)
9. Moore, E. H., *Mathematical Papers, Chicago Congress, 1893*, 210-226. (*Def. of Galois Fields.*)
10. Room, Thomas Gerald and Kirkpatrick P. B., *Miniquaternion geometry; an introduction to the study of projective planes*, Cambridge [Eng.] University Press, 1971.
11. Rosati, L. A., *I gruppi di collineazioni dei piani di Hughes*. *Boll. Un. Mat. Ital.* Vol. 13, 505-513.
12. Singer, James, *A Theorem in Finite Projective Geometry and some applications to number Theory*, *Trans. Amer. Math. Soc.*, Vol. 43, 1938, 377-385
13. Vahlen, Karl Theodor, *Abstrakte Geometrie, Untersuchungen über die Grundlagen der Euklidischen und nicht-Euklidischen Geometrie, Mit 92 abbildungen im text*, 2., neubearb. Aufl. Leipzig, S. Hirzel, 1940, *Series title: Deutsche mathematik, im auftrage der Deutschen forschungsgemeinschaft*, 2. beiheft.
14. Veblen, Oswald & Bussey, W. H., *Finite Projective Geometries*, *Trans. Amer. Math. Soc.*, Vol. 7, 1906, 241-259. (*On $PG(n, p^k)$*)
15. Veblen, Oswald, and Wedderburn, Josph H. MacLagan, *Non-Desarguesian and non-Pascalian geometries*, *Trans. Amer. Math. Soc.*, Vol. 8, 1907, 379-388.
16. Zappa, G. *Sui gruppi di collineazioni dei piani di Hughes*, *Boll. Un. Mat. Ital.* (3), Vol. 12, 1957, p. 507-516.

7.90 Answer to problems and Comments.

Notation.

$$\begin{aligned}
 u_{ij} &:= q_i q_j^{-1} - r_i r_j^{-1}, \\
 v_{ij} &:= q_i q_j^{-1} + r_i r_j^{-1}, \\
 s_i &:= -v_{i,i-1}^{-1} v_{i,i+1}, \\
 a_i &:= -v_{i-1,i}^{-1} u_{i-1,i+1}, \\
 t_i &:= s_{i+2} s_{i+1}, \\
 f_i &:= s_i - s_{i+1}^{-1} s_{i-1}^{-1}, \\
 g_i &:= t_i^{-1} - t_{i+1} t_{i-1}, \\
 k_i &:= q'_{i-1} \bar{q}_{i+1}, \\
 l_i &:= r'_{i-1} \bar{r}_{i+1}.
 \end{aligned}$$

Exercise.

Prove $q_1^{-1} u_{12} r_2 + q_2^{-1} u_{20} r_0 + q_0^{-1} u_{01} r_1 = 0$,
associated with $M \cdot eul = 0$.

The proof follows from substitution of u_{ij} by their definition.

Exercise.

Prove $u_{12} u_{02}^{-1} u_{01} = -u_{10} u_{20}^{-1} u_{21}$, associated with 2 equivalent forms of eul one for which the first coordinate is one and the other obtain by “rotation”, the second coordinate being one.

Form the definition of u_{02} it follows by multiplication to the right or left by u_{02}^{-1} , that

$$\begin{aligned}
 q_0 q_2^{-1} u_{02}^{-1} - r_0 r_2^{-1} u_{02}^{-1} &= 1, \\
 u_{02}^{-1} q_0 q_2^{-1} - u_{02}^{-1} r_0 r_2^{-1} &= 1.
 \end{aligned}$$

Moreover,

$$u_{20} = q_2 q_0^{-1} - r_2 r_0^{-1} = -q_2 q_0^{-1} u_{02} r_2 r_0^{-1}$$

or

$$u_{20}^{-1} = r_0 r_2^{-1} u_{02}^{-1} q_0 q_2^{-1}.$$

If we substitute in the identity to prove, with both terms in the second member, u_{12} , u_{01} , u_{10} and u_{21} , by their definition, we get

$$\begin{aligned}
 &q_1 q_2^{-1} u_{02}^{-1} q_0 q_1^{-1} - q_1 q_2^{-1} u_{02}^{-1} r_0 r_1^{-1} \\
 &- r_0 r_1^{-1} u_{02}^{-1} q_1 q_2^{-1} + r_0 r_1^{-1} u_{02}^{-1} r_1 r_2^{-1} \\
 &- q_1 q_0^{-1} r_0 r_2^{-1} u_{02}^{-1} q_0 q_2^{-1} q_2 q_1^{-1} + q_1 q_0^{-1} r_0 r_2^{-1} u_{02}^{-1} q_0 q_2^{-1} r_2 r_1^{-1} \\
 &+ r_1 r_0^{-1} r_0 r_2^{-1} u_{02}^{-1} q_0 q_2^{-1} q_2 q_1^{-1} - r_1 r_0^{-1} r_0 r_2^{-1} u_{02}^{-1} q_0 q_2^{-1} r_2 r_1^{-1} = 0,
 \end{aligned}$$

because terms 3 and 7 cancel, terms 1 and 5 as well as 4 and 8 give 1 and -1, terms 2 and 6 give 0 by application of the identities given at the beginning of the proof.

Lemma.

$$0. \text{ norm}(s_0 s_1 s_2) = 1.$$

$$1. \text{ norm}(t_0 t_1 t_2) = 1.$$

$$2. s_2' \bar{f}_2 s_0^{-1} = -f_2 s_1.$$

$$3. \bar{t}_2 \bar{g}_2 t_0 = -g_2 t_1^{-1}.$$

Proof: For 0, we use Lemma 7.1.1 and obtain 1, from the definition of t_i . For 2, we substitute f_2 by its definition and compare the terms of both sides of the equality which have the same sign.

Proof of 7.1.2.

Let

$$G0.0. A_0 = (1, 0, 0), A_1 = (0, 1, 0), A_2 = (0, 0, 1),$$

$$G0.1. M = (q_0, q_1, q_2), \bar{M} = (r_0, r_1, r_2),$$

then

$$P1.0. a_0 = (1, 0, 0), a_1 = (0, 1, 0), a_2 = (0, 0, 1),$$

$$P1.1. ma_0 = [0, q'_1, -q'_2], \bar{m}a_0 = [0, r'_1, -r'_2],$$

$$P1.2. M_0 = (0, q_1, q_2), \bar{M}_0 = (0, r_1, r_2),$$

$$P1.3. eul = [1, -u'_{12}\bar{u}_{02}, -u'_{21}\bar{u}_{01}],$$

$$P1.4. \mathbf{S} = \begin{pmatrix} q_0^{-n} & -q'_0 q_1^{-1} & -q'_0 q_2^{-1} \\ -q'_1 q_0^{-1} & q_1^{-n} & -q'_1 q_2^{-1} \\ -q'_2 q_0^{-1} & -q'_2 q_1^{-1} & q_2^{-n} \end{pmatrix}, \mathbf{S}^{-1} = \begin{pmatrix} 0 & q_0 \bar{q}_1 & q_0 \bar{q}_2 \\ q_1 \bar{q}_0 & 0 & q_1 \bar{q}_2 \\ q_2 \bar{q}_0 & q_2 \bar{q}_1 & 0 \end{pmatrix}.$$

$$\bar{\mathbf{S}} = \begin{pmatrix} r_0^{-n} & -r'_0 r_1^{-1} & -r'_0 r_2^{-1} \\ -r'_1 r_0^{-1} & r_1^{-n} & -r'_1 r_2^{-1} \\ -r'_2 r_0^{-1} & -r'_2 r_1^{-1} & r_2^{-n} \end{pmatrix}, \bar{\mathbf{S}}^{-1} = \begin{pmatrix} 0 & r_0 \bar{r}_1 & r_0 \bar{r}_2 \\ r_1 \bar{r}_0 & 0 & r_1 \bar{r}_2 \\ r_2 \bar{r}_0 & r_2 \bar{r}_1 & 0 \end{pmatrix}.$$

$$P2.0. mm_0 = [-q'_0, q'_1, q'_2], \bar{m}m_0 = [-r'_0, r'_1, r'_2],$$

$$P2.1. MA_0 = (0, q_1, -q_2), \bar{M}A_0 = (0, r_1, -r_2),$$

$$P2.2. m_0 = [0, q'_1, q'_2], \bar{m}_0 = [0, r'_1, r'_2],$$

$$P2.3. MM_0 = (-q_0, q_1, q_2), \bar{M}M_0 = (-r_0, r_1, r_2),$$

$$P2.4. m = [q'_0, q'_1, q'_2], \bar{m} = [r'_0, r'_1, r'_2],$$

$$P2.5. Ima_0 = (-2q_0, q_1, q_2), \bar{I}ma_0 = (-2r_0, r_1, r_2),$$

$$I\bar{m}a_0 = (-q_0(q_1^{-1}r_1 + q_2^{-1}r_2), r_1, r_2), \bar{I}ma_0 = (-r_0(r_1^{-1}q_1 + r_2^{-1}q_2), q_1, q_2),$$

$$P2.6. iMA_0 = [2q'_0, -q'_1, -q'_2], \bar{i}MA_0 = [2r'_0, -r'_1, -r'_2],$$

$$P3.0. mf_0 = [k_1 v'_{21} \bar{u}_{21}, k_0^{-1}, -1], \bar{m}f_0 = [l_1 v'_{21} \bar{u}_{21}, -l_0^{-1}, 1],$$

$$P3.1. O = \square, \bar{O} = \square,$$

$$P3.2. Mfa_0 = (\bar{k}_2, 0, -k'_0 v_{10} u_{10}^{-1}), \bar{M}fa_0 = (\bar{l}_2, 0, l'_0 v_{10} u_{10}^{-1}),$$

$$Mf\bar{a}_0 = (1, k'_2 \bar{v}_{02} u'_{02}, 0), \bar{M}f\bar{a}_0 = (1, -l'_2 \bar{v}_{02} u'_{02}, 0),$$

$$P3.3. mfa_0 = (\bar{k}_1 v'_{21} \bar{u}_{21}, k_0^{-1}, 0), \bar{m}fa_0 = (\bar{l}_1 v'_{21} \bar{u}_{21}, -l_0^{-1}, 0),$$

$$mf\bar{a}_0 = (\bar{k}_1 v_{21}^{-1} \bar{u}_{21}, 0, -1), \bar{m}f\bar{a}_0 = (\bar{l}_1 v_{21}^{-1} \bar{u}_{21}, 0, 1),$$

$$P3.4. Mfm_0 = (k_1^{-1} v_{21} u_{21}^{-1}, -\bar{k}_0, 1), \bar{M}fm_0 = (l_1^{-1} v_{21} u_{21}^{-1}, \bar{l}_0, -1),$$

$$P4.0. Imm_0 = (a_0, 1, s_0), \bar{I}mm_0 = (-a_0, 1, s_0),$$

$$P4.1. ta_0 = [0, 1, -s'_0],$$

$$P4.2. T_0 = (1, s_2, s_1^{-1}),$$

$$P4.3. at_0 = [0, s'_2, -\bar{s}_1] = [0, 1, -\bar{t}_0],$$

$$P4.4. K_0 = (1, t_2^{-1}, t_1),$$

$$P4.5. Taa_0 = (0, 1, s_0),$$

$$P4.6. poK_0 = [-1, s'_2, \bar{s}_1],$$

$$P4.7. \mathbf{T} = \begin{pmatrix} 0 & \bar{f}_2 & -\bar{f}_2 s_0^{-1} \\ f_2 & 0 & -f_2 s_1 \\ -s'_0 f_2 & -\bar{s}_1 \bar{f}_2 & 0 \end{pmatrix}, \mathbf{T}^{-1} = \begin{pmatrix} 1 & \bar{s}_2 & s'_1 \\ s_2 & s_2^n & s_1^{-n} s_0^{-1} \\ s_1^{-1} & s_2^n s_0 & s_1^{-n} \end{pmatrix}.$$

$$P4.8. \mathbf{L} = \begin{pmatrix} 0 & \bar{g}_2 & -\bar{g}_2 t_0 \\ g_2 & 0 & -g_2 t_1^{-1} \\ -\bar{t}_0 g_2 & -t'_1 \bar{g}_2 & 0 \end{pmatrix}, \mathbf{L}^{-1} = \begin{pmatrix} 1 & t'_2 & \bar{t}_1 \\ t_2^{-1} & t_2^n & t_1^n t_0 \\ t_1 & t_1^n \bar{t}_0 & t_1^n \end{pmatrix}.$$

Proof:

For P4.0, if the coordinates of Imm_0 are $x_0, 1$ and x_2 , we have to solve

$$\begin{aligned} q_0^{-1}x_0 + q_1^{-1} + q_2^{-1}x_2 &= 0, \\ -r_0^{-1}x_0 + r_1^{-1} + r_2^{-1}x_2 &= 0. \end{aligned}$$

Multiplying the equations to the left respectively by q_2 and $-r_2$, or by q_0 and r_0 and adding gives x_0 and x_2 using the notation 7.90.

For P4.7, it is easier to obtain \mathbf{T}^{-1} first, the columns are T_0, T_1, T_2 , multiplied to the right by $1, s_2^n, s_1^{-n}$. The matrix \mathbf{T} is then obtained using Theorem 7.1.1, multiplying by $-s_1^{-n}$. The equivalence with the matrix whose columns are ta_i can be verified using Lemma 7.90.2. A similar proof gives P4.8.

Theorem.

The product of the diagonal elements of \mathbf{T}^{-1} and of \mathbf{L}^{-1} is the same.

This follows from Lemma 7.1.1.

The correspondance between the definitions in EUC and here is as follows

D0.0	D1.0	D0.1	D1.1	D0.2	D1.2	D1.0	D1.3	D36.12	DC1.4
D0.3	D2.0	D0.4	D2.1	D0.5	D2.2	D0.6	D2.3	D0.7	D2.4
D10.3	D2.5	D0.25	D2.6	D10.3	D2.7	D6.0	D3.0	D6.4	D3.1
?	D3.2	?	D3.3	D14.0	D3.4	D1.6	D4.0	D1.7	D4.1
D1.8	D4.2	D12.1	D4.3	D1.2	D4.4	D1.4	D4.4	D1.9	D4.5
D15.12	D4.6	D1.19	DC4.7		DC4.8				

Chapter 8

FUNCTIONS OVER FINITE FIELDS

8.0 Introduction.

Notation.

The first notation is standard, the second is useful for Theorem 8.2.1.2.1.

$$(a)_i := \prod_0^{i-1} (a+i) = a(a+1) \dots (a+i-1). \\ [a]_i := \prod_0^{i-1} (a+2i) = a(a+2) \dots (a+2i-2).$$

Notation.

The following notation, favored on the European continent, but seldom used elsewhere, is quite useful:

$$0!! := 1 \\ 2n!! := 2.4. \dots 2n. \\ (2n+1)!! := 1.3. \dots (2n+1).$$

8.1 Polynomials over Finite Fields.

8.1.1 Definition and basic properties.

Introduction.

In a finite field, we can define polynomials of degree up to $p-1$. These are determined by their values at i in Z_p . If these are defined in the real field with rational coefficients, the definition and properties automatically extend to the finite field.

Definition.

A polynomial is a function $a_0I^{p-1} + a_1I^{p-2} + \dots + a_{p-1}$ which associates to $x \in Z_p$ the integer

$$a_0x^{p-1} + a_1x^{p-2} + \dots + a_{p-1}.$$

The polynomial is of degree k iff $a_0 \dots a_{p-k-1}$ are congruent to 0 modulo p and a_{p-k} is not.

Theorem. [Lagrange]

Given $k + 1$ distinct integers x_i (modulo p), $k < p$, and given $k + 1$ integers f_i , \exists a polynomial P of degree k \ni

$$P(x_i) = f_i, i = 0 \text{ to } k.$$

8.1.2 Derivatives of polynomials.**Definition.**

The derivative of the polynomial 8.1.1.0 is $(p-1)a_0I^{p-2} + (p-2)a_1I^{p-3} + \dots + a_{p-2}$.

8.2 Orthogonal Polynomials over Finite Fields.**8.2.0 Introduction.**

The main purpose of writing this Chapter is connected with interesting symmetry properties of the orthogonal polynomials, in Z_p . In the classical theory there is a scaling factor which is arbitrarily chosen for each of the families of orthogonal polynomials. For some time now, the same scaling factor, in each case, is universally used. When determining values of the Chebyshev polynomials for some small values of p , I was struck by the symmetry properties given in 8.2.2 and 8.2.2. These properties are dependent on the scaling factors and it turns out that the unanimously accepted ones are essentially the only ones giving this property. The same property has been found for the polynomials of Legendre and of Laguerre. For the polynomial of Hermite this is not the case. I have succeeded in obtaining some scaling, given in 8.2.5 for which a symmetry can be obtained. This scaling is given by expressions which are different for the even and for the odd Hermite polynomials, therefore the recurrence relation has a constant whose expression differs for even and odd indices. It is therefore possible to give an a-posteriori justification of the scaling factor for the classical polynomial, and there is some reason to introduce a different scaling for the Hermite polynomials. The case of the Jacobi polynomials with 2 parameters a and b is left as an exercise. With $a = b$, again a scaling is required to obtain symmetry.

8.2.1 Basic Definitions and Theorems.**Introduction.**

For orthogonal polynomials, recurrence relations, differential equations and values of the coefficients generalize automatically, from the classical case. Therefore, we have the definitions 8.2.1 and the theorems 8.2.1 to 8.2.1.

Definition.

The polynomials of Chebyshev of the first (T_n) and of the second kind (U_n), of Legendre (P_n), of Laguerre (L_n) and of Hermite (H_n) are defined by the recurrence relations:

$$0. \quad T_0 := 1, T_1 := I, T_{n+1} := 2(2I-1)T_n - T_{n-1},$$

$$1. \quad U_0 := 1, U_1 := 2I, U_{n+1} := 2(2I-1)U_n - U_{n-1},$$

$$2. \quad P_0^{(a)} := 1, P_1^{(a)} := I, \\ (n+2a+1)P_{n+1}^{(a)} := (2n+2a+1)IP_n^{(a)} - nP_{n-1}^{(a)}, \quad a \geq 0, n < p-1-2a,$$

$$3.0. \quad L_0 := 1, L_1 := 1 - I, \\ (n+1)L_{n+1} := (2n+1-I)IL_n - nL_{n-1}, \quad n < p-1,$$

$$1. \quad L_0^{(a)} := 1, L_1^{(a)} := a+1-I, \\ (n+1)L_{n+1}^{(a)} := (2n+a+1-I)L_n^{(a)} - (n+a)L_{n-1}^{(a)}, \quad n < p-1,$$

$$4. \quad H_0 := 1, H_1 := 2I, H_{n+1} := 2IH_n - 2nH_{n-1}.$$

The Legendre polynomial is $P_n := P_n^{(0)}$ and $P_n^{(a)} := \frac{n!a!}{(n+a)!} P_n^{(a,b)}$, where $P_n^{(a,b)}$, are the polynomials of Jacobi, scaled so that $P_n^{(a)}(1) = 1$.

$L_n^{(a)}$ are the generalized Laguerre polynomials and $L_n = L_n^{(0)}$.

See for instance *Handbook of Mathematical functions*, p. 782.

Theorem.

If $X_{n,j}$ denotes the coefficient of I^j in the polynomial X_n ,

$$0. \quad T_{n,n-2j} = \frac{1}{2}n2^{(n-2j)}(-1)^j \frac{(n-j-1)!}{j!(n-2j)!},$$

$$1. \quad U_{n,n-2j} = \frac{1}{2}n2^{(n-2j)}(-1)^j \frac{(n-j)!}{j!(n-2j)!},$$

$$2.0. \quad P_{n,n-2j} = 2^{(-n)}(-1)^j \frac{(2n-2j)!}{j!(n-j!(n-2j)!)},$$

$$1. \quad P_{2n,2j}^{(a)} = (-1)^{(n-j)} \binom{n}{j} \frac{[2a+2n+1]_j [2j+1]_{n-j}}{[2a+2]_n}, \\ P_{2n,2j}^{(a)} = (-1)^{(n-j)} \binom{n}{j} \frac{[2a+2n+3]_j [2j+3]_{n-j}}{[2a+2]_n},$$

$$3.0. \quad L_{n,j} = (-1)^j \frac{n!}{(n-j)!j!^2},$$

$$1. \quad L_{n,j}^{(a)} = (-1)^j \frac{(n+a)!}{(n-j)!(a+j)!j!},$$

$$4. \quad H_{n,n-2j} = n!2^{(n-2j)}(-1)^j \frac{1}{j!(n-2j)!},$$

See for instance *Handbook of Mathematical functions*, p. 775.

Theorem.

The polynomials of Chebyshev, of the first (T_n) and of the second kind (U_n), of Legendre (P_n), of Laguerre (L_n) and of Hermite (H_n) satisfy by the differential equations

$$0. \quad (1-I^2)D^2T_n - IDT_n + n^2T_n = 0,$$

$$1. \quad (1-I^2)D^2U_n - 3IDU_n + n(n+2)U_n = 0,$$

$$2. \quad (1 - I^2) D^2 P_n^{(a)} - 2(a+1)I DP_n^{(a)} + n(n+2a+1) P_n^{(a)} = 0,$$

$$3.0. \quad ID^2 L_n + (1 - I)DL_n + nL_n = 0.$$

$$1. \quad ID^2 L_n^{(a)} + (a+1 - I)DL_n^{(a)} + nL_n^{(a)} = 0.$$

$$4. \quad D^2 H_n - 2IDH_n + 2nH_n = 0.$$

See for instance *Handbook of Mathematical functions*, p. 781.

Theorem.

$$0. \quad T_n(1) = 1, DT_n(1) = n^2.$$

$$1. \quad U_n(1) = n+1, DU_n(1) = \frac{n(n+1)(n+2)}{3}.$$

$$2. \quad P_n^{(a)}(1) = 1, DP_n^{(a)}(1) = -\frac{n(n+2a+1)}{2(a+1)}.$$

$$3.0. \quad L_n(0) = 1, DL_n(0) = -n.$$

$$1. \quad L_n^{(a)} = \binom{n+a}{n}, DL_n^{(a)} = -\binom{n+a}{n-1}.$$

$$4. \quad H_{2n}(0) = (-1)^n \frac{(2n)!}{n!}, DH_{2n}(0) = 0. \quad H_{2n+1}(0) = 0, DH_{2n+1}(0) = (-1)^{n+1} \frac{(2n)!}{n!}.$$

Comment.

It is easy to verify that, contrary to the classical case, the roots of the orthogonal polynomials are not necessarily in Z_p . For instance, T_2 has a root in Z_p iff $2 \nmid p$ or $p \equiv \pm 1 \pmod{8}$.

Program.

[m130]FIN_ORTHOG.HOM illustrates the use of the program [m130]FIN_ORTHOG.BAS, which determines these various orthogonal polynomials. [m130]FIN_ORTHOG.NOT are notes tracing some of the steps leading to the conjectures proven here.

8.2.2 Symmetry properties for the Polynomials of Chebyshev of the first and second kind.

Theorem.

$$0. \quad T_{p+i,j} = T_{p-i,j}.$$

$$1. \quad T_{i+2pk,j} = -T_{i+pk,j} = T_{i,j}, \quad j < p.$$

Proof:

$$\begin{aligned} T_{p+i,j} &= (-1)^{\frac{1}{2}(p+i-j)} 2^j \frac{(\frac{1}{2}(p+i+j)-1)! \frac{1}{2}(p+i)}{(\frac{1}{2}(p+i-j))! j!} \\ &= (-1)^{\frac{1}{2}(p+i-j)} (-1)^{\frac{1}{2}(p-i-j)} (-1)^{\frac{1}{2}(p-i+j+i)} \frac{2^j (\frac{1}{2}(p-i+j-2))! \frac{1}{2}(p-i)}{(\frac{1}{2}(p-i-j))! j!} \end{aligned}$$

$$\begin{aligned}
&= (-1)^{\frac{1}{2}(p-i-j)} 2^j \frac{(\frac{1}{2}(p-i+j-2))! \frac{1}{2}(p-i)}{(\frac{1}{2}(p-i-j))! j!} \\
&= T_{p-i,j}.
\end{aligned}$$

Example.

For $p = 5$,

$$\begin{aligned}
T_0 &= -T_{10} = T_{20} = 1. \\
T_1 &= -T_9 = -T_{11} = T_{19} = +I. \\
T_2 &= -T_8 = -T_{12} = T_{18} = -1 + 2I^2. \\
T_3 &= -T_7 = -T_{13} = T_{17} = +2I - I^3. \\
T_4 &= -T_6 = -T_{14} = T_{16} = 1 + 2I^2 - 2I^4. \\
T_5 &= T_{15} = 0.
\end{aligned}$$

Theorem.

0. $U_{p-1+i,j} = U_{p-1-i,j}$.
1. $U_{i+2pk,j} = -U_{i+pk,j} = U_{i,j}$, $j < p$.

Proof:

$$\begin{aligned}
U_{p-1+i,j} &= (-1)^{(\frac{1}{2}(p-1+i-j))} \frac{(\frac{1}{2}(p-1+i+j))! 2^j}{(\frac{1}{2}(p-1+i-j))! j!} \\
&= (-1)^{(\frac{1}{2}(p-1+i-j))} (-1)^{(\frac{1}{2}(p-i-j-1))} \\
&\quad \frac{(-1)^{(\frac{1}{2}(p-i+j-1))} (\frac{1}{2}(p-i+j-1))! 2^j}{(\frac{1}{2}(p-1+i-j))! j!} \\
&= (-1)^{(\frac{1}{2}(p-1+i-j))} 2^j \frac{(\frac{1}{2}(p-1-i+j))!}{\frac{1}{2}((p-1-i-j))! j!} \\
&= U_{p-1-i,j}.
\end{aligned}$$

Example.

For $p = 5$,

$$\begin{aligned}
U_0 &= U_8 = -U_{10} = -U_{18} = 1. \\
U_1 &= U_7 = -U_{11} = -U_{17} = 2I. \\
U_2 &= U_6 = -U_{12} = -U_{16} = -1 - I^2. \\
U_3 &= U_5 = -U_{13} = -U_{15} = I - 2I^3. \\
U_4 &= -U_{14} = 1 - 2I^2 + I^4. \\
U_9 &= -U_{19} = 0.
\end{aligned}$$

8.2.3 Symmetry properties for the Polynomials of Legendre.

Introduction.

Theorem.

1

$$P_{p-1-2a-n}^{(a)} = P_n^{(a)}, \quad n \leq \frac{p-1}{2} - a.$$

Proof:

Let $p' = \frac{1}{2}(p-1)$. The recurrence relations 8.2.1.2 imply

¹24.11.83 and 17.2.89

$$(p' + 1)P_{p'+1} = -p'P_{p'-1},$$

hence $P_{p'+1} = P_{p'-1}$.

They can also be written,

$$(n + 1)P_{p-n-2} = -(2n + 1)P_{p-n-1} - nP_{p-n}.$$

Therefore, starting from $P_{p'}$ and from $P_{p'-1}$ and $P_{p'+1}$, we obtain by induction $P_{p-1-n} = P_n$.

Example.

For $p = 11$,

$$\begin{aligned} P_0 &= P_{10} = 1, \\ P_1 &= P_9 = I, \\ P_2 &= P_8 = 5 - 4I^2, \\ P_3 &= P_7 = 4I - 3I^3, \\ P_4 &= P_6 = -1 - I^2 + 3I^4, \\ P_5 &= -5I + 5I^3 + I^5, \end{aligned}$$

For $p = 13$,

$$\begin{aligned} P_0 &= P_{12} = 1, \\ P_1 &= P_{11} = I, \\ P_2 &= P_{10} = 6 - 5I^2, \\ P_3 &= P_9 = 5I - 4I^3, \\ P_4 &= P_8 = 2 + 6I^2 + 6I^4, \\ P_5 &= P_7 = -3I + I^3 + 3I^5, \\ P_6 &= -6 - 4I^2 - I^4 - I^6, \end{aligned}$$

Theorem.

² $P_{p-1-n} = P_n$, $n < p$?

$$\begin{aligned} P_0^{(a)} &= 1, \\ P_1^{(a)} &= I, \\ P_2^{(a)} &= \frac{-1+(2a+3)I^2}{2(a+1)}, \\ P_3^{(a)} &= -\frac{3I+(2a+5)I^3}{2^2(a+1)(a+2)}, \\ P_4^{(a)} &= \frac{3-6(2a+5)I^2+(2a+5)(2a+7)I^4}{2^2(a+1)(a+2)}, \\ P_5^{(a)} &= \frac{15I-10(2a+7)I^3+(2a+7)(2a+9)I^5}{2^2(a+1)(a+2)}, \end{aligned}$$

Example.

For $p = 11, a = 2$

$$\begin{aligned} P_0^{(2)} &= 1, \\ P_1^{(2)} &= I, \\ P_2^{(2)} &= -2 + 3I^2, \\ P_3^{(2)} &= 5I - I^3, \\ P_4^{(2)} &= -2 + 3I^2, \\ P_5^{(2)} &= I, \\ P_6^{(2)} &= 1, \end{aligned}$$

For $p = 13, a = 2$

$$\begin{aligned} P_0^{(2)} &= 1, \\ P_1^{(2)} &= I, \\ P_2^{(2)} &= 2 - I^2, \\ P_3^{(2)} &= 6I - 5I^3, \\ P_4^{(2)} &= -4 - 6I^2 - 2I^4, \\ P_5^{(2)} &= 6I - 5I^3, \\ P_6^{(2)} &= 2 - I^2, \\ P_7^{(2)} &= I, \\ P_8^{(2)} &= 1, \end{aligned}$$

8.2.4 Symmetry properties for the Polynomials of Laguerre.

Theorem (La).

$$0. L_{p-1-i,j} = (-1)^j L_{i+j,j}, \quad 0 \leq i, j, \quad i+j < p.$$

Proof:

$$1. L_{n,j} = (-1)^j \frac{1}{j!} \binom{n}{j}.$$

See for instance, Handbook p.775.

Example.

For $p = 7$,

$$L_0 = 1.$$

$$L_1 = 1 - I.$$

$$L_2 = 1 - 2I - 3I^2.$$

$$L_3 = 1 - 3I - 2I^2 + I^3.$$

$$L_4 = 1 + 3I + 3I^2 - 3I^3 - 2I^4.$$

$$L_5 = 1 + 2I - 2I^2 + 3I^3 - 3I^4 - I^5.$$

$$L_6 = 1 + I - 3I^2 + I^3 - 2I^4 + I^5 - I^6.$$

Theorem (La).

$$0. L_{p-a-1-i,j}^{(a)} = (-1)^{j+a} L_{i+j,j}^{(a)}, \quad 0 \leq i, j, \quad i+j < p-a.$$

$$1. L_{j,j}^{(a)} = -(a-1)! I^{p-a}, \quad 0 < a, \quad p-a \leq j < p.$$

$$2. L_{i,j}^{(a)} = 0, \quad a > 0, \quad j < p-a \leq i < p.$$

The proof is left to the reader.

Example.

For $p = 13$, $a = 5$

$$L_0^{(5)} = 1.$$

$$L_1^{(5)} = 6 - I.$$

$$L_2^{(5)} = -5 + 6I - 6I^2.$$

$$L_3^{(5)} = 4 - 2I + 4I^2 + 2I^3.$$

$$L_4^{(5)} = -4 - 6I + 5I^2 + 5I^3 + 6I^4.$$

$$L_5^{(5)} = 5 - 2I - 5I^2 - I^3 - 5I^4 + 4I^5.$$

$$L_6^{(5)} = -6 + 6I - 4I^2 + 5I^3 + 5I^4 + 5I^5 - 5I^6.$$

$$L_7^{(5)} = -1 - I + 6I^2 + 2I^3 - 6I^4 + 4I^5 + 5I^6 - 3I^7.$$

$$L_8^{(5)} = 2I^8.$$

$$L_9^{(5)} = 2I^8 - 6I^9.$$

$$L_{10}^{(5)} = 2I^8 + I^9 - 2I^{10}.$$

$$L_{11}^{(5)} = 2I^8 - 5I^9 - 6I^{10} - I^{11}.$$

$$L_{12}^{(5)} = 2I^8 + 2I^9 + I^{10} - 4I^{11} - I^{12}.$$

8.2.5 Symmetry properties for the Polynomials of Hermite.

Definition.

The scaled Hermite polynomials are defined by

0. $H_0^s = 1$,
1. $H_1^s = I$,
2. $[\frac{1}{2}n]H_n^s = a_n I H_{n-1}^s - \frac{1}{2}(n-1)H_{n-2}^s$,
where $a_n = 1$ if n is even and $a_n = [\frac{1}{2}n]$, the largest integer in $\frac{1}{2}n$ if n is odd.

Example.

In the fields Q or R ,

$$\begin{aligned} H_2^s &= -\frac{1}{2} + I^2, \\ H_3^s &= -\frac{3}{2}I + I^3, \\ H_4^s &= \frac{3}{8} - \frac{3}{2}I^2 + \frac{1}{2}I^4, \\ H_5^s &= \frac{15}{8}I - \frac{5}{2}I^3 + \frac{1}{2}I^5, \\ H_6^s &= -\frac{5}{16} + \frac{15}{8}I^2 - \frac{5}{4}I^4 + \frac{1}{6}I^6, \\ H_7^s &= -\frac{35}{16}I + \frac{35}{8}I^3 - \frac{7}{4}I^5 + \frac{1}{6}I^7. \end{aligned}$$

Theorem.

$$\begin{aligned} H_{2n}^s(0) &= (-1)^n \frac{(2n-1)!!}{(2n)!!}, \quad DH_{2n}^s(0) = 0. \\ H_{2n+1}^s(0) &= 0, \quad DH_{2n+1}^s(0) = (-1)^n \frac{(2n+1)!!}{(2n)!!}. \end{aligned}$$

Lemma.

In Z_p , $p > 2$,

0. $(p-1)! = -1$.
1. $(p-1-i)! = (-1)^{(i+1)} \frac{1}{i!}$, $0 \leq i < p$.
2. $\binom{p-1-i}{j} = (-1)^j \binom{i+j}{j}$, $0 \leq i, j, i+j < p$.
3. $\binom{kp+i}{j} = \binom{i}{j}$, $j < p$.
4. $(p-2-i)!! i!! = (-1)^{\frac{1}{2}k} (p-1-k-i)!! (k+i-1)!!$, $0 \leq i < p-1$, $0 < k+i < p$.

Proof: 0, is the well known Theorem of Wilson. 1, can be considered as a generalization.

$$\begin{aligned} (p-1-i)! &= (-1)^i (p-1) \dots (i+1) \\ &= (-1)^i \frac{(p-1)!}{i!} \\ &= (-1)^{(i+1)} \frac{1}{i!}. \end{aligned}$$

For 2, $\frac{(p-1-i)!}{(p-1-i-j)!j!} = (-1)^{(i+1)} \frac{(i+j)!}{(-1)^{i+j+1}i!j!} = (-1)^j \binom{i+j}{j}$.

Lemma.

Modulo p , $p > 2$,

$$0. \quad ((p-2)!!)^2 = (-1)^{\frac{1}{2}(p-1)}$$

$$1. \quad (p-1)!!(p-2)!! = -1.$$

$$0.0. \quad (p-2-i)!!i!! = (-1)^s (p-2)!!, \\ \text{where } s = \frac{1}{2}i \text{ when } i \text{ is even and } s = \frac{1}{2}(p-2-i) \text{ when } i \text{ is odd.}$$

$$1. \text{ or where } s = [\frac{1}{2}([\frac{1}{2}p] + 1 + i)] + [\frac{1}{4}(p+1)].$$

0 and 1 are well known and are given for completeness. for 2, if i is even,

$$(p-2-i)!!i!! = (p-i)!!(i-2)!!(\frac{i}{p-i} \text{ or } -1) \\ = (-1)^{(\frac{1}{2}i)}(p-2)!!0!!.$$

if i is odd,

$$(p-2-i)!!i!! = (p-4-i)!!(i+2)!!(\frac{p-2-i}{i+2} \text{ or } -1) \\ = (-1)^{\frac{1}{2}(p-2-i)}(0)!!p-2!!.$$

2.1, can be verified by choosing $p = 1, 3, 5, 7$ and $i = 0, 1, 2, 3, 4$.

Theorem.

For scaled Hermite

$$0. \quad H_{i+j,j}^s = 0, \quad 0 \leq i, j, \quad i \text{ odd.}$$

$$1. \quad H_{p-1-i,j}^s = H_{i+j,j}^s, \quad 0 \leq i, j, \quad i \text{ even, } j \text{ even, } i+j < p.$$

$$2. \quad H_{p-2-i,j}^s = H_{i+j,j}^s, \quad 0 \leq i, j, \quad i \text{ even, } j \text{ odd, } i+j < p.$$

The proof is left as an exercise.

Example.

For $p = 11$,

$$H_0^s = 1.$$

$$H_1^s = I.$$

$$H_2^s = 5 + I^2$$

$$H_3^s = 4I + I^3$$

$$H_4^s = -1 + 4I^2 - 5I^4$$

$$H_5^s = -5I + 3I^3 - 5I^5$$

$$H_6^s = -1 - 5I^2 - 4I^4 + 2I^6$$

$$H_7^s = 4I + 3I^3 + I^5 + 2I^7$$

$$H_8^s = 54I^2 - 4I^4 + 4I^6 - 5I^8$$

$$H_9^s = I + I^3 - 5I^5 + 2I^7 - 5I^9.$$

$$H_{10}^s = 1 + I^2 - 5I^4 + 2I^6 - 5I^8 - I^{10}.$$

Problem.

The Jacobi polynomials can be defined by

$$Ps_0^{(a,b)} := 1, P_1^{(a,b)} := \frac{a-b+(a+b+2)I}{2(a+1)},$$

$$2(n+1)(n+a+b+1)(2n+a+b) P_{n+1}^{(a,b)} :=$$

$$((2n+a+b+1)(a^2-b^2)$$

$$+ (2n+a+b)(2n+a+b+1)(2n+a+b+2)I) P_n^{(a,b)}$$

$$- 2(n+a)(n+b)(2n+a+b+2) P_{n-1}^{(a,b)}.$$

Determine an appropriate scaling for the Jacobi polynomials that gives symmetry properties which generalize those of the special case where $a = b$.

8.3 Addition Formulas for Functions on a Finite Fields.

8.3.0 Introduction.

Ungar, gave recently the addition formulas associated with a generalization of the trigonometric and hyperbolic functions by Ricatti. This suggested the extension to the finite case. Section 1, is the Theorem of Ungar, the special case for 3 functions is given in 8.3.2, with the associated invariant 8.3.2.2. The invariant defines the distances, addition, which in fact corresponds to the multiplication of associated Toeplitz matrices gives the angles. For 3 dimensions we have 2 special cases, $p \equiv 1 \pmod{3}$ and $p \equiv -1 \pmod{3}$. In the latter case all non isotropic direction form a cycle. In the former case, we can consider that the set of $(p-1)^2$ non isotropic directions corresponds to a direct product of 2 cyclic groups of order $p-1$, I conjecture (14) that there are always pairs of generators which are closely related called special generators (13). This is extended to more than 3 functions in 8.3.3. The connection with difference sets is given at the end of that chapter.

8.3.1 The Theorem of Ungar.

Theorem. [Ungar]

If f is a solution of

$$0. D^{n+1}f + a_n D^n f + \dots + a_0 f = 0, a_{n+1} = 1,$$

$$1. D^n f(0) = 1, D^k f(0) = 0, 0 \leq k < n,$$

then

$$2. f(x+y) = \sum_{m=0}^n a_{m+1} \sum_{k=0}^m D^k f(x) D^{m-k} f(y).$$

More generally, if

$$3. D^k f(0) = d_k, 0 \leq k \leq n,$$

then

$$4. \sum_{m=0}^n a_{m+1} \sum_{k=0}^m D^k f(x) D^{m-k} f(y)$$

$$= \sum_{m=0}^n a_{m+1} \sum_{k=0}^m d_k D^{m-k} f(x+y).$$

Proof: See Abraham Ungar, 1987.

Example.

$$0.0. \ a_m = 0, \ 0 \leq m \leq n, \ f = \frac{I^n}{n!},$$

$$1. \ (x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$

$$1.0. \ n = 0, \ a_1 = 1, \ a_{-1} = 0, \ f = e^I,$$

$$1. \ e^{x+y} = e^x e^y.$$

$$2.0. \ n = 1, \ a_2 = 1, \ a_1 = 0, \ a_0 = 1, \ f = \sin,$$

$$1. \ \sin(x+y) = \sin(x)\cos(y) + \cos(x)\sin(y).$$

$$3.0. \ n = 1, \ a_2 = 1, \ a_1 = 0, \ a_0 = -1, \ f = \sinh,$$

$$1. \ \sinh(x+y) = \sinh(x)\cosh(y) + \cosh(x)\sinh(y).$$

$$4. \ a_{n+1} = 1, \ a_k = 0, \ 0 < k \leq n, \ a_0 = -j, \ \text{where } j = \pm 1,$$

$$D^i f = R^{(jn,0)} = \sum_{k=0}^{\infty} \frac{I^{rk-i}}{(rk-i)!}, \ \text{where } r = n+1,$$

$$(j = -1?)$$

$$1. \ R^{(-n,0)}(x+y) = R^{(-n,0)}(x)R^{(-n,n)}(y) \\ + R^{(-n,1)}(x)R^{(-n,n-1)}(y) + \dots \\ + R^{(-n,0)}(x)R^{(-n,n)}(y).$$

$$(j = -1?)$$

These are, with my notation, the functions of Vincenzo Ricatti. In particular, when $n = 2$,? we have the following Theorem.

Theorem.

If n is odd, then

$$0. \ R^{(-n,0)} = R^{(n,0)}(-I).$$

$$1. \ R^{(-n,j)} = (-1)^j R^{(n,j)}(-I).$$

8.3.2 The case of 3 functions.

Theorem.

Let

$$0. \ f = R^{(2,0)}, \ g = R^{(2,1)}h = R^{(2,2)},$$

then

$$1. \ f(x+y) = f(x)h(y) + g(x)g(y) + h(x)f(y), \\ g(x+y) = g(x)h(y) + h(x)g(y) + f(x)f(y), \\ h(x+y) = h(x)h(y) + f(x)g(y) + g(x)f(y),$$

$$2. \ f^3 + g^3 + h^3 - 3fgh = 1.$$

$$\begin{aligned}
3. & (f(x)h(y) + g(x)g(y) + h(x)f(y))^3 \\
& + (g(x)h(y) + h(x)g(y) + f(x)f(y))^3 \\
& + (h(x)h(y) + f(x)g(y) + g(x)f(y))^3 \\
& - 3(f(x)h(y) + g(x)g(y) + h(x)f(y)) \\
& \quad (g(x)h(y) + h(x)g(y) + f(x)f(y)) \\
& \quad (h(x)h(y) + f(x)g(y) + g(x)f(y)) \\
& = (f(x)^3 + g(x)^3 + h(x)^3 - 3f(x)g(x)h(x)) \\
& \quad (f(y)^3 + g(y)^3 + h(y)^3 - 3f(y)g(y)h(y)).
\end{aligned}$$

Proof:

$$g = Df, h = Dg = D^2f, f = Dh = D^2g = D^3f,$$

f, g and h satisfy the same differential equation, whose Wronskian is constant this gives

$$\det \begin{vmatrix} f & g & h \\ g & h & f \\ h & f & g \end{vmatrix} = -1.$$

Theorem.

The solution of 8.3.2, f, g, h is given by

0. $f = Ae^I + Be^{\beta I} + Ce^{\beta^{-1}I},$
1. $g = Ae^I + B\beta e^{\beta I} + C\beta^{-1}e^{\beta I},$
2. $h = Ae^I + B\beta^{-1}e^{\beta I} + C\beta^{-1}e^{\beta I},$
where
3. $\beta^2 + \beta + 1 = 0,$
4. $A = \frac{1}{3}, B = \frac{1}{3}\beta, C = \frac{1}{3}\beta^{-1}.$

Corollary.

$$\begin{aligned}
f &= e^{-\frac{1}{2}I} \cos\left(\frac{\sqrt{3}}{2}I\right), \\
g &= e^{-\frac{1}{2}I} \cos\left(\left(\frac{\sqrt{3}}{2} + \frac{\pi}{3}\right)I\right), \\
h &= e^{-\frac{1}{2}I} \cos\left(\left(\frac{\sqrt{3}}{2} - \frac{\pi}{3}\right)I\right),
\end{aligned}$$

is a solution of $D^3f = f$.

I examined the more general case³ starting from f_1, g_1, h_1 and using the addition formulas, it appears that the period is always $p-1$ and that if

$$f^3 + g^3 + h^3 - 3fgh = 1 \text{ then we have}$$

$$f\left(\frac{\pi}{3}\right) = g\left(\frac{2\pi}{3}\right) = 0 \text{ when } p \equiv 1 \pmod{6}.$$

Application to the case of 3 dimensional Affine geometry associated to p^4 .

Lemma.

Let

³7.12.87

⁴8.12.87

$$0. \quad T(x, y, z) := x^3 + y^3 + z^3 - 3xyz, \quad L(x, y, z) := x + y + z, \\ S(x, y, z) := x^2 + y^2 + z^2 - yz - zx - xy,$$

then

$$T(x, y, z) = L(x, y, z)S(x, y, z).$$

0.0. If $-3Np$ or $p \equiv 2 \pmod{3}$, then the only points of $S = 0$ are (a, a, a) .

1. If $-3Rp$ or $p \equiv 1 \pmod{3}$, then

$$S(x, y, z) = (x + \tau y + \tau' z)(x + \tau' y + \tau z), \text{ with} \\ \tau := \frac{1}{2}(-1 + \sqrt{-3}\tau') := \frac{1}{2}(-1 - \sqrt{-3}).$$

2. The number of lines through the origin on $T(x, y, z) = 0$ is $3p$ if $p \equiv 1 \pmod{3}$

and

$$p + 2 \text{ if } p \equiv -1 \pmod{3}.$$

Proof: The number of lines through the origin is the same as the number of points in a plane not through the origin which are on the ideal line or on S .

If $p \equiv 1 \pmod{3}$, this gives $(p + 1) + 1$,

if $p \equiv -1 \pmod{3}$, this gives $3(p + 1) - 3$.

Definition.

Let \mathcal{T} be the set of points $(x, y, z) \ni$

$$0. \quad x^3 + y^3 + z^3 - 3xyz = 1.$$

Let the addition in T be defined by

$$1. \quad (x, y, z) + (x', y', z') := (yy' + xz' + zx', xx' + yz' + zy', zz' + xy' + yx')$$

Theorem.

0. $(\mathcal{T}, +)$ is an Abelian group with neutral element $(0, 0, 1)$.

$$1. \quad (x, y, z) + (x', y', z') + (x'', y'', z'') \\ = (x(x'y'' + y'x'' + z'z'') + y(x'x'' + y'z'' + z'y'') + z(x'z'' + y'y'' + z'x''), \\ x(x'z'' + y'y'' + z'x'') + y(x'y'' + y'x'' + z'z'') + z(x'x'' + y'z'' + z'y''), \\ x(x'x'' + y'z'' + z'y'') + y(x'z'' + y'y'' + z'x'') + z(x'y'' + y'x'' + z'z'')).$$

$$2. \quad (x, y, z) + (y^2 - zx, x^2 - yz, z^2 - xy) = (0, 0, 1).$$

Corollary.

$$0. \quad 2(x, y, z) = (y^2 + 2zx, x^2 + 2yz, z^2 + 2xy).$$

$$1. \quad 3(x, y, z) = (3(x^2y + y^2z + z^2x), 3(x^2z + y^2x + z^2y), 1 + 9xyz).$$

Theorem.

If

- 0. $(x_n, y_n, z_n) := n(x, y, z)$ then
- 1. $x_n + y_n + z_n = (x + y + z)^n$.
- 2. $x_{k(p-1)+i} + y_{k(p-1)+i} + z_{k(p-1)+i} = x_i + y_i + z_i$.

Theorem.

Let

- 0. $u^2 = -3x^2 + 2sx - \frac{s^2}{3} + \frac{4}{3s}$
- 1. $y = \frac{1}{2}(s - x \pm u)$,
- 2. $z = s - x - y$, then $(x, y, z) \in \mathcal{T}$.

Proof:

Substitute z by $s - x - y \in x^3 + y^3 + z^3 - 3xyz - 1 = 0$ gives
 $3s y^2 - 3s(s - x)y + (3s x^2 - 3s^2 x + s^3 - 1) = 0$,
 dividing by $3s$, the discriminant is the second member of 0. \square

Definition.

- 0. The distance d between 2 points (x, y, z) and (x', y', z') is given by

$$d^3(x, x') := (x' - x)^3 + (y' - y)^3 + (z' - z)^3 - 3(x' - x)(y' - y)(z' - z).$$
- 1. If the distance between 2 distinct points is 0, the line incident to the 2 points is called isotropic.

Theorem.

The isotropic lines are those on the surface $T(x, y, z) = 0$.

Lemma.

$$d^3(x, x') = d^3(0, x) - d^3(0, x') - 3(x(x'^2 - y'z') + y(y'^2 - z'x') + z(z'^2 - x'y')) \\ + 3(x'(x^2 - yz) + y'(y^2 - zx) + z'(z^2 - xy)).$$

Theorem.

- 0. $d(P, Q) = -d(Q, P)$.
- 1. If $P = (0, 0, 0, 1)$, then $P \times Q$ is isotropic iff Q is on the line l joining P to $(1, 1, 1, 1)$ or on a line through P perpendicular to l .

The ideal points on the surface satisfy⁵

$$x^3 + y^3 + z^3 - 3xyz = 0.$$

⁵11.12.87

Definition.

The normal to the surface \mathcal{T} at (a, b, c) is
 $[a^2 - bc, b^2 - ca, c^2 - ab].$

Notation.

If $p \equiv 1 \pmod{6}$, $\delta := \frac{p-1}{3}$.

Theorem.

If $p \equiv 1 \pmod{6}$, $(\mathcal{T}, +) \sim C_{p-1} \rtimes C_{p-1}$.

Proof: The order of the group follows from Lemma 8.3.2?

Lemma.

If an Abelian group is isomorphic to $C_q \rtimes C_q$ if u and v are of order p and $u^i \neq v^j$ for all i and j between 1 and q , u and v are generators of the group.

Lemma.

If $p \equiv 1 \pmod{6}$, g is a primitive root of p and (a, b, c) and (a', b', c') are obtained using

0. $b, c = \frac{g^{-a} \pm \sqrt{\frac{-g^2 + 6ag - 9a^2 + 4g^{-1}}{3}}}{2}$
 if their i -th iterates are distinct, $0 < i < p-1$, then (a, b, c) and (a', b', c') are generators.
 In particular, if $h^3 = 1$ then

1. $b, c = \frac{h^{-a} \pm \sqrt{(h+3a)(h-a)}}{2}$

Proof: the fact that g is primitive insures that the sum of the components of the i -th iterate of (a, b, c) is g^i , because these are distinct for $i = 1$ to $p-2$, the Lemma follows.

Definition.

If the pair (a, b, c) and (b, a, c) are pairs of generators of $(T, +)$ then (a, b, c) is called a special generator of T .

Conjecture.

Given a primitive root of $p \equiv 1 \pmod{6}$, there exists always special generators $(a, b, c) \ni a+b+c = g \pmod{p}$ ⁶.

Theorem.

If (a_1, b_1, c_1) is a special generator, the period is

0 1 2 ... δ $\delta+1$ $\delta+2$... 2δ $2\delta+1$ $2\delta+2$...

0 a_1 a_2 ... 1 c_1 c_2 ... 0 b_1 b_2 ...

0 b_1 b_2 ... 0 a_1 a_2 ... 1 c_1 c_2 ...

1 c_1 c_2 ... 0 b_1 b_2 ... 0 a_1 a_2 ...

For (b_1, a_1, c_1) the period, scaled again is

0 1 2 ... δ $\delta + 1$ $\delta + 2$... 2δ $2\delta + 1$ $2\delta + 2$...

0 b_1 b_2 ... 0 a_1 a_2 ... 1 c_1 c_2 ...

0 a_1 a_2 ... 1 c_1 c_2 ... 0 b_1 b_2 ...

1 c_1 c_2 ... 0 b_1 b_2 ... 0 a_1 a_2 ...

Algorithm.

For a given p , we determine the smallest positive primitive root g , then for increasing values of a , we determine b and c using 8.3.2.0, if $c(\delta) = 1$ we permute a, b, c , in the order

$b, a, c, c, b, a, a, c, b, c, a, b, b, c, a,$

unless $p \equiv 1 \pmod{9}$, in which case we try a new p , if $c(\delta) = 0$, we save the period and permute, if $c(\delta) = 0$ and the values of $a(i), b(i), c(i)$ are not distinct from some i , from the corresponding saved values, we permute again, if we exhaust the permutations, we ignore this value of a . When we have obtained (a, b, c) such that the first $a(\delta) = -1$ and the second $= 1$ we exchange.

Example.

0. $p = 7, g^i = 1, 3, 2, 6, 4, 5, \mathcal{T} =$

0	1	2	3	4	5	6	7	8
(0, 0, 1)	(0, 0, 2)	(0, 0, 4)	(0, 1, 0)	(0, 2, 0)	(0, 4, 0)	(1, 0, 0)	(1, 3, 6)	(1, 5, 5)
(0, 0, 1)	(0, 0, 1)	(0, 0, 1)	(0, 1, 0)	(0, 1, 0)	(0, 1, 0)	(1, 0, 0)	(5, 1, 2)	(2, 3, 3)
9	10	11	12	13	14	15	16	17
(1, 6, 3)	(2, 0, 0)	(2, 3, 3)	(2, 5, 6)	(2, 6, 5)	(3, 1, 6)	(3, 2, 3)	(3, 3, 2)	(3, 4, 5)
(5, 2, 1)	(1, 0, 0)	(2, 3, 3)	(5, 2, 1)	(5, 1, 2)	(1, 5, 2)	(3, 2, 3)	(3, 3, 2)	(2, 5, 1)
18	19	20	21	22	23	24	25	26
(3, 5, 4)	(3, 6, 1)	(4, 0, 0)	(4, 3, 5)	(4, 5, 3)	(4, 6, 6)	(5, 1, 5)	(5, 2, 6)	(5, 3, 4)
(2, 1, 5)	(1, 2, 5)	(1, 0, 0)	(5, 2, 1)	(5, 1, 2)	(2, 3, 3)	(3, 2, 3)	(2, 5, 1)	(1, 2, 5)
27	28	29	30	31	32	33	34	35
(5, 4, 3)	(5, 5, 1)	(5, 6, 2)	(6, 1, 3)	(6, 2, 5)	(6, 3, 1)	(6, 4, 6)	(6, 5, 2)	(6, 6, 4)
(1, 5, 2)	(3, 3, 2)	(2, 1, 5)	(2, 5, 1)	(1, 5, 2)	(2, 1, 5)	(3, 2, 3)	(1, 2, 5)	(3, 3, 2)
+	0	9	4	29	20	27		
0	0	9	4	29	20	27		
30	30	35	13	24	26	11		
10	10	31	2	21	3	32		
34	34	8	17	16	7	33		
5	5	18	6	14	1	12		
22	22	15	19	23	25	28		

When scaled the group is isomorphic to $C_6 \rtimes C_2$, we have the equivalences,

0,1,2; 3,4,5; 6,10,20; 7,13,22; 8,11,23; 9,12,21; 14,27,3; 15,24,33; 16,28,35; 17,25,30; 18,29,32; 19,26,34.

We have the table

+	0	9	3	18	6	14
0	0	9	3	18	6	14
16	16	7	15	19	8	17

1. $p = 13, g^i = 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7$, the scaled period is

(0, 0, 1) (7, 1, 6) (7, 9, 11) (11, 10, 6),
 (1, 0, 0) (6, 7, 1) (11, 7, 9) (6, 11, 10),
 (0, 1, 0) (1, 6, 7) (9, 11, 7) (10, 6, 11),

2. $p = 19$, $g^i = 1, 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10$, the scaled period is
 (0, 0, 1), (3, 9, 8), (15, 1, 4), (8, 13, 18), (7, 5, 8), (11, 0, 9)
 (1, 0, 0), (8, 3, 9), (4, 15, 1), (18, 8, 13), (8, 7, 5), (9, 11, 0)
 (0, 1, 0), (9, 8, 3), (1, 4, 15), (13, 18, 8), (5, 8, 7), (0, 9, 11)

Example.

The following are special generators, for the given primitive root, which is the smallest positive one:

p	g	$sp.gen.$	p	g	$sp.gen.$	p	g	$sp.gen.$
7	3	(6, 1, 3)	283	3	(3, 158, 125)	631	3	(324, 4, 306)
13	2	(1, 2, 12)	307	5	(4, 192, 116)	643	11	(152, 0, 502)
19	2	(6, 18, 16)	313	10	(5, 21, 297)	661	2	(2, 134, 527)
31	3	(30, 4, 0)	331	3	(0, 237, 97)	673	5	(3, 52, 623)
37	2	(18, 7, 14)	337	10	(180, 0, 167)	691	3	(425, 0, 269)
43	3	(8, 35, 3)	349	2	(50, 299, 2)	709	2	(424, 3, 284)
61	2	(3, 2, 58)	367	6	(22, 346, 5)	727	5	(377, 352, 3)
67	2	(2, 12, 55)	373	2	(53, 6, 316)	733	6	(1, 541, 197)
73	5	(4, 12, 62)	379	2	(5, 200, 176)	739	3	(0, 400, 342)
79	3	(5, 42, 35)	397	5	(8, 22, 372)	751	3	(4, 426, 324)
97	5	(24, 3, 75)	409	21	(390, 38, 2)	757	3	(5, 122, 632)
103	5	(79, 25, 4)	421	2	(6, 5, 412)	769	11	(1, 404, 375)
109	6	(13, 0, 102)	433	5	(3, 273, 162)	787	2	(411, 3, 375)
127	3	(77, 0, 53)	439	15	(0, 264, 190)	811	3	(0, 188, 626)
139	2	(107, 31, 3)	457	13	(14, 456, 0)	823	3	(15, 0, 811)
151	6	(106, 51, 0)	463	3	(0, 335, 331)	829	2	(7, 572, 252)
157	5	(4, 39, 119)	487	3	(39, 0, 551)	853	2	(155, 698, 2)
163	2	(2, 29, 134)	499	7	(1, 87, 418)	859	2	(228, 625, 8)
181	2	(2, 36, 145)	523	2	(310, 6, 209)	877	2	(10, 5, 864)
193	5	(122, 3, 73)	541	2	(93, 3, 447)	883	2	(147, 6, 732)
199	5	(30, 5, 167)	547	2	(335, 2, 212)	907	2	(553, 2, 354)
211	2	(33, 2, 178)	571	3	(7, 8, 559)	919	7	(129, 0, 727)
223	3	(138, 0, 88)	577	5	(4, 300, 278)	937	5	(7, 493, 442)
229	6	(1, 168, 66)	601	7	(138, 463, 7)	967	5	(3, 661, 308)
241	7	(20, 4, 224)	607	3	(0, 441, 169)	991	6	(8, 228, 761)
271	6	(159, 7, 111)	613	2	(3, 50, 562)	997	7	(0, 625, 379)
277	5	(11, 5, 266)	619	2	(5, 65, 551)			

Lemma.

If $p \equiv -1 \pmod{6}$,

$$0. \ s_i := P_{i0} + P_{i1} + P_{i2} \Rightarrow s_i = s_1^i.$$

$$1. \ f_i := P_{i0}^2 + P_{i1}^2 + P_{i2}^2 - (P_{i1}P_{i2} + P_{i2}P_{i0} + P_{i0}P_{i1}) \Rightarrow f_i = f_1^i.$$

Lemma.

If $p \equiv -1 \pmod{6}$, if g is a primitive root of p ,

Proof: Let ...

To determine what happens for the solutions for $i = 1, 2, \dots, p-1$:

let g be a generator for p , we want To determine what happens for the solutions for $i \equiv 0 \pmod{p-1}$:

$$a + b + c = 1, a^2 + b^2 + c^2 - (bc + ca + ab) = 1, \Rightarrow$$

$$(a + b + c)^2 = 1, bc + ca + ab = 0,$$

given $a, b + c = 1 - a, bc = a(a - 1)$,

$$b, c = \frac{1-a \pm \sqrt{(a-1)(1-3a)}}{2}$$

special solutions $(1, 0, 0), (-\frac{1}{3}, \frac{2}{3}, \frac{2}{3}), 2(-\frac{1}{3}, \frac{2}{3}, \frac{2}{3}) = (0, 1, 0), 2(\frac{2}{3}, -\frac{1}{3}, \frac{2}{3}) = (1, 0, 0)$, there should be $\frac{p+1-3-3}{2} = \frac{p-5}{2}$ possible values of a .

Notation.

$\epsilon := (0, 0, 1), \alpha := (1, 0, 0), \beta := (0, 1, 0)$.

Theorem.

If $p \equiv -1 \pmod{6}$, and $3\delta = p^2 - 1$, then

$$0. (\mathcal{T}, +) \sim C_{3\delta}.$$

1. If h is a generator of this group then $h^\delta = (0, 1, 0)$ or $(1, 0, 0)$, in the former case, we will choose $g = h^{-1}$ otherwise we will choose $g = h$.

2. If $g^i = (a, b, c)$, then $g^{i+\delta} = (c, a, b), g^{i+2\delta} = (b, c, a), g^{pi} = (b, a, c), g^{pi+\delta} = (c, b, a), g^{pi+2\delta} = (a, c, b)^7$.

$$3. d(P_i, P_{p+(p+1)l+(p-1)kj+i}) = d(P_i, P_{1+(p+1)l-(p-1)kj+i}).$$

$$4. d(P_i, P_{(p+1)l+(p-1)kj+i}) = d(P_i, P_{(p+1)l-(p-1)kj+i}).$$

Proof:

If $p \equiv -1 \pmod{6}$, to any of the $p^2 - 1$ line through the origin which does not pass through $(1, 1, 1)$ and is not in the plane perpendicular to this last line, associate a point $a, b, c, 1$ say let $u := a^3 + b^3 + c^3 - 3abc, u \neq 0$ and u has a unique cube root v in Z_p , therefore the point $(\frac{a}{v}, \frac{b}{v}, \frac{c}{v}) \in \mathcal{T}$.

$$(a, b, c) + (1, 0, 0) = (c, a, b), (a, b, c) + (0, 1, 0) = (b, c, a).$$

Lemma.

Proof: $\phi(p^2 - 1) = 2 \phi(p-1) \phi(p+1)$,

Example.

$p = 11, g = 7$,

Lemma.

$$0. (a + b + c)(a^2 + b^2 + c^2 - bc - ca - ab) = a^3 + b^3 + c^3 - 3abc.$$

1. Given a and g , a primitive root of p , then

$$b, c = \frac{g-a \pm \sqrt{\frac{-g^2+6ag-9a^2+4g^{-1}}{3}}}{2}$$

Proof: $a+b+c = g$ and $a^2+b^2+c^2-bc-ca-ab = g^{-1} \Rightarrow (a+b+c)^2 = g^2$ and $bc+ca+ab = 0$, therefore $b+c = g-a$ and $bc = \frac{g^2-g^{-1}}{3} - a(g-a)$, hence b and c are roots of a quadratic equations, this gives 1.

Theorem.

If $p \equiv -1 \pmod{6}$,

0. A necessary condition for (a, b, c) in \mathcal{T} to be a generator is that $a + b + c$ be a primitive root for p .

1. If (a, b, c) is a generator such that $(a, b, c)^\delta = (1, 0, 0)$,

2.0. $p \equiv 2 \pmod{9}$, or $p \equiv 11 \pmod{18} \Rightarrow$
 $(b, c, a)^\delta = \epsilon, (c, a, b)^\delta = \beta, (c, b, a)^\delta = \epsilon, (a, c, b)^\delta = \alpha, (b, a, c)^\delta = \beta,$

0. $p \equiv 5 \pmod{9}$, or $p \equiv 5 \pmod{18} \Rightarrow$
 $(b, c, a)^\delta = \beta, (c, a, b)^\delta = \epsilon, (c, b, a)^\delta = \alpha, (a, c, b)^\delta = \epsilon, (b, a, c)^\delta = \beta,$

1. $p \equiv 8 \pmod{9}$, or $p \equiv 17 \pmod{18} \Rightarrow$
 $(b, c, a)^\delta = \alpha, (c, a, b)^\delta = \alpha, (c, b, a)^\delta = \beta, (a, c, b)^\delta = \beta, (b, a, c)^\delta = \beta,$

1. $p(u, v, w) = (v, u, w).$

Definition.

Given a generator (a, b, c) and a non isotropic scaled direction (u, v, w) the corresponding angular direction is the multiplier i such that $i(a, b, c) = (u, v, w).$

Conjecture. 8

0. angular direction(P_{i+k}, P_i) = $i + \text{angular direction}(P_k, P_0)$
 $\pmod{p^2 - 1}.$

1. angular direction(O, M_i) = $i + \text{angular direction}(0, M_0)$, where M_i is the mid-point of $(P_i, P_{i+1}).$

2. angular direction(O, N_i) = $i + \text{angular direction}(0, N_0)$, where N_i is the mid-point of $(P_{i-1}, P_{i+1}).$

3. angular direction(P_i, N_i) = $i + \text{angular direction}(P_0, N_0).$

Example.

$p = 17$, generator $(13, 4, 3)$,
 $\text{angular direction}((0, 0, 1), (13, 4, 3)) = 164$,
 $\text{angular direction}((0, 0, 1), (9, 6, 1)) = 224$,
 $M_0 = (15, 2, 2)$, $\text{angular direction}(O, M_0) = 60$,
 $N_1 = (13, 3, 6)$, $\text{angular direction}(O, N_0) = 33$,
 $\text{angular direction}(P_1, N_1) = 40$.

Corollary.

The coordinates of the normal to the surface \mathcal{T} are those of $-p(a, b, c)^9$.

Lemma.

If (a, b, c) is a generator and g^i is a primitive root of p , then

$$0. \ i, \text{ prime}, \equiv 1 \pmod{3} \Rightarrow (g^i)^\delta = \alpha.?$$

$$1. \ i, \text{ prime}, \equiv 2 \pmod{3} \Rightarrow (g^i)^\delta = \beta.?$$

$$2. \ i \text{ is not a prime} \Rightarrow (g^i)^\delta = \epsilon.$$

Example.

The following table gives generators (a, b, c) for the given values of p and g ,
 $\alpha, \epsilon, \beta, -\epsilon, \alpha, \beta, \alpha, \beta, \epsilon, -\alpha, \epsilon, \beta, \alpha, \alpha, -\beta, \beta, \beta$

$p = 11,$	4, 9, 0	$p = 5,$	0, 4, 3	$p = 17,$	13, 4, 3
$g = 2,$	1, 7, 5	$g = 2,$		$g = 3,$	15, 16, 6
$p = 29,$	0, 17, 14	$p = 23,$	11, 1, 16	$p = 53,$	17, 38, 0
$g = 2,$	4, 24, 3	$g = 5,$	5, 21, 2	$g = 2,$	2, 34, 19
	7, 16, 8		6, 13, 9		23, 25, 7
	11, 26, 23		18, 10, 0		48, 52, 8
$p = 47,$	0, 30, 22	$p = 41,$	36, 1, 10		11, 24, 20
$g = 5,$	1, 12, 39	$g = 6,$	35, 3, 9		12, 49, 47
	2, 4, 46		30, 12, 5	$p = 71,$	69, 7, 2
	6, 25, 21		17, 16, 14	$g = 7,$	36, 39, 3
	18, 7, 27		40, 33, 15		4, 43, 31
	13, 45, 41		31, 29, 28		21, 48, 9
	17, 15, 20	$p = 59,$	53, 0, 8		13, 49, 16
	19, 44, 36	$g = 2,$	44, 15, 2		17, 67, 65
$p = 83,$	62, 23, 0		30, 28, 3		56, 58, 35
$g = 2,$	2, 20, 63		48, 4, 9		50, 54, 45
	4, 11, 70		19, 6, 36	$p = 89,$	39, 48, 5
	50, 29, 6		32, 17, 12	$g = 3,$	8, 13, 71
	8, 16, 61		27, 21, 13		37, 45, 10
	27, 9, 49		18, 52, 50		29, 44, 19
	77, 10, 81				20, 83, 78
	21, 13, 51				43, 86, 52
	25, 18, 42				46, 81, 54
	35, 31, 19				47, 72, 62
	45, 64, 59				
	67, 53, 48				

Example.

0. $p = 5, \mathcal{T} =$

0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	-1	-1	-1	2	-1	1	-2	-1	1
0	-1	-1	-2	-2	0	2	1	0	0	1	-1
1	-2	-1	1	-1	-2	0	-2	0	-1	-1	-2
12	13	14	15	16	17	18	19	20	21	22	23
-1	-2	0	-2	0	-1	-1	-2	-2	0	2	1
-1	-1	2	-1	1	-2	-1	1	-1	-2	0	-2
-2	0	2	1	0	0	1	-1	-1	-1	2	-1

The ideal points are (last coord. 0), A, B, C, D, E, F, G (0,1,-1), (1,0,-1), (1,-1,0), (1,1,1), (1,1,-2), (1,2,2), (1,-2,1).

successive powers, $A, G, E, F, B, C, 0$; $B, F, E, G, A, C, 0$; C, C ; D, D ; E, D, E ; F, G, D, F .

1. $p = 11, g = 2, \mathcal{T} =$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	1	-5	0	-2	4	5	1	-3	-4	4	3	-3	5	4	4	-4
0	3	3	-4	3	-3	-3	-4	0	-1	-5	1	-3	-3	5	-2	-2
1	4	0	-1	3	-2	1	5	-3	1	2	4	4	4	-5	-3	-2
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
-2	4	1	-3	-5	3	-3	-4	-5	5	-2	-4	2	2	-3	-2	-4
4	3	-1	-4	5	-5	5	-4	5	1	0	-1	0	-5	5	2	0
0	-2	-4	-3	-3	0	4	1	-1	-3	4	-1	5	4	-5	-2	-1
34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
5	5	4	1	4	2	1	4	0	-1	3	-2	1	5	-3	1	2
4	-5	4	5	-2	5	0	1	-5	0	-2	4	5	1	-3	-4	4
-5	-1	-5	-4	3	0	0	3	3	-4	3	-3	-3	-4	0	-1	-5
...																

2. $p = 17, g = 3, \mathcal{T} = \{$
 $(0, 0, 1), (1, 2, 3), (10, 13, 13), (1, 7, 4), (4, 13, 4), (8, 0, 16),$
 $(6, 6, 13), (9, 16, 6), (14, 1, 1), (11, 2, 15), (1, 13, 1), (13, 8, 1),$
 $(5, 5, 3), (11, 9, 7), (7, 1, 1), (7, 12, 1), (12, 11, 12), (2, 1, 3),$
 $(11, 11, 14), (1, 4, 7), (1, 10, 10), (16, 0, 8), (5, 15, 5), (16, 9, 6),$
 $(4, 4, 8), (11, 15, 2), (14, 9, 9), (1, 8, 13), (15, 0, 15), (9, 11, 7),$
 $(5, 5, 16), (7, 1, 12), (1, 0, 0), (3, 1, 2), (13, 10, 13), (4, 1, 7),$
 $\dots\}$

Example.

A generator associated to the given primitive root is such that $(a, b, c)^\delta = \alpha = (1, 0, 0)$, with $\delta := \frac{p^2-1}{3}$.

p	g	generator
5	2	(0, 4, 3)
11	2	(1, 3, 4)
17	3	(3, 4, 13)
23	5	(0, 7, 12)
29	2	(0, 4, 7)
41	6	(0, 2, 17)
47	5	(0, 7, 37)
53	2	(0, 6, 20)
59	2	(0, 3, 11)
71	7	(0, 8, 54)
83	2	(0, 6, 60)
89	3	(0, 6, 77)
101	2	(0, 7, 60)
107	2	(0, 2, 29)
113	3	(0, 3, -12)???
131	2	(0, 4, 18)
137	3	(0, 2, -25)
149	2	(0, 3, -53)
167	5	(0, 7, -2)
173	2	(0, 3, 71)
179	2	(0, 4, 36)
191	19	(0, 5, -83)
197	2	(0, 19, 61)

See [M130] RICATTI. for more.

8.3.3 The case of 4 Functions.

Definition.

The set R_4 is the set of elements

$$0. (x, y, z, t) \ni x, y, z, t \in \mathbb{Z}_p \text{ and} \\ -(x^2 - z^2)^2 + (y^2 - t^2)^2 + 4((x^2 + z^2)yt - (y^2 + t^2)xz) = 1, \\ \text{with addition}$$

$$1. (x, y, z, t) + (x', y', z', t') = (xt' + tx' + yz' + zy', xx' + zz' + yt' + ty', \\ xy' + yx' + zt' + tz', yy' + tt' + xz' + zx').$$

Theorem.

$(R^4, +)$ is an Abelian group.

Conjecture.

0. If $p \equiv 1 \pmod{4}$ then the maximum period is $p - 1$.

1. If $p \equiv -1 \pmod{4}$ then the maximum period is $p^2 - 1$ ¹⁰.

Example.

0. If $p = 3$, $(1, 2, 0, 1)$, is of period 8.
1. If $p = 5$, $(1, 2, 0, 1)$, is of period 4.
2. If $p = 7$, $(3, 3, 0, 4)$, is of period 48.
3. If $p = 11$, $(3, 2, 6, 3)$, is of period 120.
4. If $p = 13$, $(1, 2, 3, 9)$, is of period 12.
5. If $p = 17$, $(15, 13, 4, 8)$, is of period 16.
6. If $p = 19$, $(12, 13, 14, 1)$, is of period 360.
7. If $p = 23$, $(2, 3, 6, 17)$, is of period 528.
8. If $p = 29$, $(15, 16, 11, 18)$, is of period 28.

Lemma.

$$\begin{aligned}
\begin{vmatrix} z & y & x \\ x & z & y \\ y & x & z \end{vmatrix} &= \begin{vmatrix} x+y+z & y & x \\ x+y+z & z & y \\ x+y+z & x & z \end{vmatrix} = (x+y+z) \begin{vmatrix} 1 & y & x \\ 1 & z & y \\ 1 & x & z \end{vmatrix} \\
&= (x+y+z) \begin{vmatrix} 1 & y & x \\ 0 & z-y & y-x \\ 0 & x-z & z-y \end{vmatrix} = (x+y+z)((z-y)^2 - (x-z)(y-x)).
\end{aligned}$$

Lemma.

$$\begin{aligned}
\begin{vmatrix} t & z & y & x \\ x & t & z & y \\ y & x & t & z \\ z & y & x & t \end{vmatrix} &= (x+y+z+t) \begin{vmatrix} 1 & z & y & x \\ 1 & t & z & y \\ 1 & x & t & z \\ 1 & y & x & t \end{vmatrix} \\
&= (x+y+z+t) \begin{vmatrix} t-z & z-y & y-x \\ x-t & t-z & z-y \\ y-x & x-t & t-z \end{vmatrix} \\
&= (x+y+z+t) \begin{vmatrix} t-z+y-x & z-y & y-x \\ x-t+z-y & t-z & z-y \\ y-x+t-z & x-t & t-z \end{vmatrix} \\
&= (x+y+z+t)(-x+y-z-t) \begin{vmatrix} 1 & z-y & y-x \\ -1 & t-z & z-y \\ 1 & x-t & t-z \end{vmatrix} \\
&= (x+y+z+t)(-x+y-z+t) \begin{vmatrix} 1 & z-y & y-x \\ 0 & t-y & z-x \\ x-z & t-y & \end{vmatrix} \\
&= (x+y+z+t)(-x+y-z+t)((t-y)^2 + (x-z)^2).
\end{aligned}$$

8.3.4 The case of 5 functions.

Definition.

$$\det(x, y, z, t, u) = \begin{vmatrix} u & t & z & y & x \\ x & u & t & z & y \\ y & x & u & t & z \\ z & y & x & u & t \\ t & z & y & x & u \end{vmatrix}$$

Definition.

The set R_5 is the set of elements

$$0. \quad (x, y, z, t, u) \ni x, y, z, t, u \in Z_p \text{ and} \\ \det(x, y, z, t, u) = 1 \\ \text{with addition}$$

$$1. \quad (x, y, z, t, u) + (x', y', z', t', u') \\ = (xt' + yu' + zt' + tz' + uy', xy' + yx' + zu' + tt' + uz', \\ xz' + yy' + zx' + tu' + ut', xt' + yz' + zy' + tx' + uu', xu' + yt' + zz' + ty' + ux').$$

Lemma.

$$\begin{vmatrix} u & t & z & y \\ x & u & t & z \\ y & x & u & t \\ z & y & x & u \end{vmatrix} \\ = (u^2 - xt)^2 - (tu - xz) * (xu - yt) \\ + (zu - xy) * (x^2 - yu) + (t^2 - zu) * (yu - zt) \\ - (zt - yu) * (xy - zu) + (z^2 - yt)(y^2 - xz) \\ = u^4 - x^3y - y^3t - z^3x - t^3z + x^2t^2 + y^2z^2 \\ + 2x^2zu + 2y^2xu + 2z^2tu + 2t^2uy - 3u^2xt - 3u^2yz - xyzt$$

Theorem.

$$\det(x, y, z, t, u) = s(2(x^4 + y^4 + z^4 + t^4 + u^4) - s(x^3 + y^3 + z^3 + t^3 + u^3) \\ + x^2(y(2z + 2t - 3u) - 3zt + 2tu + 2uz) + \dots \\ - yztu - ztux - tuxy - uxyz - xyzt),$$

with $s = x + y + z + t + u$.

Proof: We use

$$\begin{vmatrix} u & t & z & y & x \\ x & u & t & z & y \\ y & x & u & t & z \\ z & y & x & u & t \\ t & z & y & x & u \end{vmatrix} = s \begin{vmatrix} 1 & t & z & y & x \\ 1 & u & t & z & y \\ 1 & x & u & t & z \\ 1 & y & x & u & t \\ 1 & z & y & x & u \end{vmatrix}$$

and then the Lemma.

Theorem.

$(R^5, +)$ is an Abelian group.

Conjecture.

0. If $p \equiv 1 \pmod{10}$ then the maximum period is $p - 1$.
1. If $p \equiv 9 \pmod{10}$ then the maximum period is $p^2 - 1$ ¹¹.
2. If $p \equiv \pm 3 \pmod{10}$ then the maximum period is $p^4 - 1$ ¹².

For examples see 8.4.1.

8.4 Application to geometry.

8.4.0 Introduction.

To define distances in a sub geometry of affine k -dimensional geometry, we have to define a homogeneous function $f(P)$ of degree k . We can then either define the distance between 2 points P and Q by the k -th root of $f(Q - P)$ or the hypercube between 2 points P and Q by $f(Q, P)$. I will not discuss here the extension of a 2-dimensional distance to n -dimension as is done in Euclidean geometry.

To define angles, we can associate to a point P , a k by k matrix by a bijection, if the set of these matrices, which are of determinant 1, form a subset of an Abelian group under matrix multiplication, with generator G_0, \dots, G_l , we can define then angular direction of a point associated to the matrix $G_0^{i_0} \dots G_l^{i_l}$ by (i_0, \dots, i_l) .

We can also define $f(P)$ as the determinant of the associated matrix. If in the 2 dimensional real affine geometry, we associate to (x, y) the matrix

$$\begin{pmatrix} y & x \\ -x & y \end{pmatrix},$$

then $f(x, y) = x^2 + y^2$, the matrices of determinant 1 for an Abelian group with generator $x = \sin(1)$, $y = \cos(1)$, and we obtain the 2-dimensional Euclidean distance and angle.

If in the 2-dimensional real affine geometry, we associate to (x, y) the matrix

$$\begin{pmatrix} y & x \\ x & y \end{pmatrix},$$

then $f(x, y) = y^2 - x^2$, the matrices of determinant 1 for an Abelian group with generator $x = \sinh(1)$, $y = \cosh(1)$, and we obtain the 2-dimensional Minkowskian distance and angle.

This will now be extended using the generalization of the hyperbolic functions by Ricatti.

8.4.1 k -Dimensional Affine Geometry.

Definition.

In k -dimensional affine geometry we define the Ricatti function as the function which associates to the point $P = (P_0, \dots, P_{k-1})$, the Toeplitz matrix \mathbf{T} , defined by $\mathbf{T}_{i,j} = P_{k-1-i+j}$, $0 \leq i, j < k$,

where the subscripts computation is done modulo k .

¹¹24.12.87

¹²22.12.87

Theorem.

The matrix multiplication defines an addition (which is a convolution) for the points as follows, if \mathbf{T} is associated to P and \mathbf{U} , to Q , \mathbf{TU} is associated to R with

$$P \circ Q := R_i = \sum_j P_j Q_{i-1-j}.$$

For instance,

0. $k = 3$,

$$\begin{aligned}(P \circ Q)_0 &= P_0 Q_2 + P_1 Q_1 + P_2 Q_0, \\ (P \circ Q)_1 &= P_0 Q_0 + P_1 Q_2 + P_2 Q_1, \\ (P \circ Q)_2 &= P_0 Q_1 + P_1 Q_0 + P_2 Q_2.\end{aligned}$$

1. $k = 4$,

$$\begin{aligned}(P \circ Q)_0 &= P_0 Q_3 + P_1 Q_2 + P_2 Q_1 + P_3 Q_0, \\ (P \circ Q)_1 &= P_0 Q_0 + P_1 Q_3 + P_2 Q_2 + P_3 Q_1, \\ (P \circ Q)_2 &= P_0 Q_1 + P_1 Q_0 + P_2 Q_3 + P_3 Q_2, \\ (P \circ Q)_3 &= P_0 Q_2 + P_1 Q_1 + P_2 Q_0 + P_3 Q_3.\end{aligned}$$

Corollary.

The set of matrices, associated to all the non ideal points of k -dimensional affine geometry with determinant 1, form an abelian group under matrix multiplication.

Theorem.

If $p = k$ then $P_i = \delta_{i,0}$ has period p . Moreover, the j -th iterate $P^{(j)}$ is such that $P_i^{(j)} = \delta_{j,i}$.

Theorem.

Let $\det(\dots, z, y, x)$ denote the determinant of the Toeplitz matrix associated with $P = (x, y, z, \dots)$, let s be the sum of the components of P , then

0. $k = 3$,

$$\det(zyx) = x^3 + y^3 + z^3 - 3xyz = s((z - y)^2 - (x - z)(y - x)).$$

1. $k = 4$,

$$\det(tzyx) = s(-x + y - z + t)((t - y)^2 + (x - z)^2).$$

2. $k = 5$,

$$\begin{aligned}\det(x, y, z, t, u) &= s(2(x^4 + y^4 + z^4 + t^4 + u^4) - s(x^3 + y^3 + z^3 + t^3 + u^3) \\ &\quad + x^2(y(2z + 2t - 3u) - 3zt + 2tu + 2uz) + \dots \\ &\quad - yztu - ztux - tuxy - uxyz - xyzt).\end{aligned}$$

In the following examples we have obtained what a cyclic generator of what appears to be the longest period, without examining the details of the structure of the solution.

Example.

0. $k = 4$.

p	<i>period</i>	<i>cyclic generator</i>
3	8	(1, 2, 0, 1),
5	4	(1, 2, 0, 1),
7	48	(3, 3, 0, 4),
11	120	(3, 2, 6, 3),
13	12	(1, 2, 3, 9),
17	16	(15, 13, 4, 8),
19	360	(12, 13, 14, 1),
23	528	(2, 3, 6, 17),
29	28	(15, 16, 11, 18).

1. $k = 5$.

p	<i>period</i>	<i>cyclic generator</i>
3	80	(1, 1, 0, 1, 2),
5	5	(1, 0, 0, 0, 0),
7	2400	(1, 2, 4, 1, 4),
11	10	(4, 2, 1, 4, 2).
13	28560	(3, 5, 1, 11, 8)
17	83520	(9, 7, 8, 2, 11),
19	18	(7, 16, 15, 2, 0),
23	279840	(14, 12, 4, 7, 14),
29	840	(13, 8, 25, 5, 9),
31	30	(26, 30, 11, 2, 27).

2. $k = 6$,

p	<i>period</i>	<i>cyclic generator</i>
3	6	(0, 1, 1, 2, 1, 0),
5	24	(0, 2, 4, 1, 0, 0),
7	6	(3, 5, 0, 6, 1, 2),
11	120	(5, 9, 2, 4, 2, 2),
13	12	(3, 8, 4, 2, 1, 10)
17	288	(2, 12, 5, 14, 4, 3),
19	18	(2, 12, 5, 14, 4, 3),
23	528	(3, 16, 20, 4, 13, 18),
29	840	(10, 2, 8, 22, 14, 4),
31	30	(1, 11, 7, 4, 29, 13),

3. $k = 7$,

p	<i>period</i>	<i>cyclic generator</i>
3		728 (1, 2, 2, 1, 0, 1, 1, 1),
5		15624 (0, 0, 4, 3, 0, 0, 0),
7		7 (1, 0, 0, 0, 0, 0, 0),
11		1330 (0, 1, 8, 4, 3, 4, 4),
13		168 (6, 3, 11, 2, 4, 2, 0),
17		24137568 (3, 10, 13, 16, 3, 4, 5),
19		47045880 (18, 10, 17, 5, 14, 9, 5),
23		12166 (0, 17, 4, 7, 3, 15, 5),
29		28 (26, 7, 9, 10, 15, 7, 15),
31	(6)	887503680 (26, 26, 15, 18, 26, 22, 19),
37	(3)	50652 (9, 9, 18, 31, 0, 27, 25),
41	(2)	1680 (7, 10, 22, 32, 27, 2, 27).

4. $k = 8$,

p	<i>period</i>	<i>cyclic generator</i>
3	8	(1, 2, 2, 1, 0, 1, 1, 1),
5	24	(2, 0, 3, 3, 1, 4, 4, 0),
7	48	(1, 3, 0, 0, 3, 3, 4, 3),
11	120	(5, 1, 9, 9, 4, 8, 2, 8),
13	168	(7, 11, 5, 4, 12, 9, 5, 1),
17	16	(9, 13, 7, 10, 0, 15, 4, 3),
19	360	(18, 11, 4, 13, 8, 1, 7, 16),
23	528	(9, 10, 22, 4, 8, 17, 16, 11),
29	840	(28, 1, 14, 21, 9, 26, 14, 5),
31	960	(28, 6, 30, 20, 25, 1, 30, 18),
37	1368	(0, 21, 5, 5, 28, 36, 9, 9),
41	40	(16, 30, 30, 27, 14, 18, 18, 17),

5. $k = 9$,

p	<i>period</i>	<i>cyclic generator</i>	
3	18	(0, 2, 2, 1, 2, 2, 0, 1, 1),	
5	15624	(1, 1, 2, 0, 1, 1, 4, 1, 1),	<i>may not be largest period</i>
7			
11			
13			
17	288	(15, 8, 16, 15, 9, 13, 7, 10, 12),	
19	18	(2, 4, 15, 11, 6, 11, 4, 0, 6),	
23			
29			
31			
37	36	(5, 27, 14, 9, 28, 24, 20, 12, 11)	

Example.

Here we have written j when the maximum period is $p^j - 1$, unless the number is underlined in which case the period is given.

$k \setminus p$	3	5	7	11	13	17	19	23	29	31	37	41
3	\underline{k}	2	1	2	1	2	1	2	2	1	1	2
4	2	1	2	2	1	1	2	2	1	2	1	1
5	4	\underline{k}	4	1	4	4	2	4	2	1	4	1
6	\underline{k}	2	1	2	1	2	1	2	2	1	1	2
7	6	6	\underline{k}	3	2	6	6	3	1	6	3	2
8	2	2	2	2	2	1	2	2	2	2	2	1
9	\underline{k}	6	3	6	3	2	1	6	6	3	1	6
10	4	$\underline{2k}$	4	1	4	4	2	4	2	1	4	1
11	5	5	10	\underline{k}	10	10	10	1	10	5	5	≥ 10
12	$\underline{2k}$	2	2	2	1	2	2	2	2	2	1	2
13	3	4	12	12	\underline{k}	6	≥ 12	6	3	4	≥ 10	≥ 10
14	6	6	$\underline{3k}$	3	2	6	6	3	1	6	3	2
15	$\underline{16k}$	$\underline{8k}$	4	2	4	4	2	4	2	1	4	2
16	4	4	2	4	4	1	4	2	4	2	4	2
17	16	16	16	≥ 16	4	—	8	≥ 16	≥ 16	≥ 16	?	?
19	18	5	3	3	≥ 18	9	—	9	≥ 18	6	2	?
$k \setminus p$	43	47	53	59	61	67	71	73	79	83	89	97
3	1	2	2	2	1	1	2	1	1	2	2	1
4	2	2	1	2	1	2	2	1	2	2	1	1
5	4	4	4	2	1	4	1	4	2	4	2	4
6	1	2	2	2	1	1	2	1	1	2	2	1
7	1	6	3	6	6	3	1	6	3	2	6	2
8	2	2	2	2	2	2	2	1	2	2	1	1
9	3	6	2	6	3	3	2	1	3	6	2	3
10	4	4	4	2	1	4	1	4	2	4	2	4
11	2	5	5	5	≥ 10	1	5	≥ 10	≥ 10	≥ 10	1	5
12	2	2	2	2	1	2	2	1	2	2	2	1
13	6	4	1	≥ 8	3	≥ 8	≥ 8	4	1	4	≥ 7	≥ 7
14	1	6	3	6	6	3	1	6	3	2	6	2
15	4	4	4	2	1	4	2	4	2	4	2	4
16	4	2	4	4	4	4	2	2	2	4	2	1
17	8	?	?	8	≥ 16	2	?	?	?	≥ 8	4	?
19	?	9	≥ 9	≥ 9	?	?	?	≥ 9	101	≥ 9	103	≥ 9

Moreover it appears that

$\{\em k \mid$	18	\mid	20	\mid	21	\mid	22	\mid	24	\mid	25	\mid
26	\mid	27	$\}$									
\mid	3	$k \mid$	5	$k \mid$	3	104	$k \mid$	11	5	$k \mid$	3	$k \mid$
13	2	$k \mid$	3	k								
\mid		\mid		7	6	$k \mid$		\mid		\mid		\mid
$\{\em k \mid$	28	\mid	30	\mid	33	\mid	34	\mid	35	\mid	36	\mid
38	\mid	39	$\}$									
\mid	7	12	$k \mid$	3	8	$k \mid$	3	22	$k \mid$	17	$\$8kL\backslash\mathrm{hti}\{-1\}/\$$	\mid
5	.k	\mid	3	.k	\mid	19	9	$k \mid$	3	.k		
\mid		\mid	5	4	$k \mid$	11	40	$k \mid$		7	560	$k \mid$
		\mid	13	.k								

{\em k	40	42	44	45	46	48
49	50}					
5 3k	3 .k	11 15k	3 .k	23 11k	3 5k	
7 .k	5 k					
	7 .k		5 .k			
{\em k	51	52	54	55	56	57
58	60}					
\$3\geq\$ 200k	13 3k	3		11 5k	7 8k	3 .k
29 .k	3 .k					
17 .k				19 .k		
5 .k						

Conjecture.

If $k = 4$, then

0. if $p \equiv 1 \pmod{4}$ then the maximum period is $p - 1$.
1. if $p \equiv -1 \pmod{4}$ then the maximum period is $p^2 - 1$ ¹³.

Conjecture.

If $k = 5$,

0. if $p \equiv 1 \pmod{10}$ then the maximum period is $p - 1$,
1. if $p \equiv 9 \pmod{10}$ then the maximum period is $p^2 - 1$ ¹⁴,
2. if $p \equiv \pm 3 \pmod{10}$ then the maximum period is $p^4 - 1$ ¹⁵.

The above examples may lead to other conjectures perhaps for all k .

Conjecture.

Let $p \nmid k$. The maximum period is $p^e - 1$, where e depends on p and k ,¹⁶

0. $e(p^i, p') = e(p^i, p'')$ if $p' \equiv p'' \pmod{p^i}$.
1. $(q_1, q_2) = 1 \Rightarrow e(k, q_1 q_2) = \text{lcm}(e(k, p_1), e(k, p_2))$.
2. $e(p^i, p') = \text{order}(p') \in Z_{p^i, \cdot}$.
In view of 0, we can define $e_u := e(p^i, u)$ for $u \in Z_{p^i, \cdot}$.

¹³22.12.87

¹⁴24.12.87

¹⁵24.12.87

¹⁶2.2.88

3. $e(p^i, 1) = 1$, $e(p^i, p^i - 1) = 2$, $k = 5$, $e_2 = e_3 = 4$,
 $k = 7$, $e_2, e_4 = 3$, $e_3, e_5 = 6$,
 $k = 2^3$, $e_3, e_5 = 2$,
 $k = 3^2$, $e_4, e_7 = 3$, $e_2, e_5 = 6$,
 $k = 11$, $e_3, e_4, e_5, e_9 = 5$, $e_2, e_6, e_7, e_8 = 10$,
 $k = 13$, $e_3, e_9 = 3$, $e_5, e_8 = 4$, $e_4, e_{10} = 6$, $e_2, e_6, e_7, e_{11} = 12$, $k = 17$, $e_3, e_4, e_5, e_9 = 5$,
 $e_2, e_6, e_7, e_8 = 10$, ?

Theorem.

If, for $k = 3$, $p \equiv 5 \pmod{6}$, we construct a period associated to a generator and determine the coplanar directions to the directions associated to 0 and 1, we obtain a difference sets For the set $Z_{p^2, \cdot}$ of the numbers from 0 to p^2 relatively prime to p .
The sets have $p(p - 1)$ elements.

Proof: The proof is similar to that of Singer. In this case, the directions are the non isotropic ones and 2 non isotropic directions determine exactly one plane, through the origin, which contains $p + 1$ directions.

This Theorem extends to any dimension. We should check if these difference sets are also obtained by some other method.

Example.

$k = 3$, ($[130 \backslash RIC.BAS]$ p , then diff. set then generator)

p	gen.	difference set (mod $p^2 - 1$) of $p(p - 1)$ elements
5	(0, 4, 3)	0, 1, 14, 16, 21
11	(1, 3, 4)	0, 1, 9, 28, 30, 34, 41, 44, 83, 98, 103
17	(3, 4, 13)	0, 1, 10, 13, 34, 45, 59, 86, 112, 114, 129, 134, 191, 195, 251, 259, 282
23	(0, 7, 12)	0, 1, 60, 91, 134, 142, 148, 203, 249, 253, 266, 269, 271, 298, 305, 333, 342, 352, 363, 375, 450, 488, 503
29	(0, 4, 7)	0, 1, 134, 147, 153, 228, 246, 316, 326, 328, 373, 411, 432, 435, 452, 457, 484, 488, 521, 549, 560, 575, 589, 623, 719, 774, 790, 797, 832
41	(0, 2, 17)	0, 1, 24, 199, 208, 230, 424, 470, 522, 525, 533, 604, 682, 684, 694, 698, 748, 775, 805, 823, 872, 879, 915, 941, 975, 1014, 1061, 1120, 1133, 1161, 1178, 1248, 1263, 1283, 1316, 1527, 1548, 1567, 1592, 1643, 1675,
47	(0, 7, 37)	0, 1, 8, 115, 147, 253, 373, 401, 412, 447, 693, 714, 716, 765, 889, 923, 964, 982, 994, 1095, 1124, 1182, 1185, 1258, 1303, 1308, 1322, 1339, 1419, 1472, 1519, 1655, 1744, 1757, 1782, 1822, 1826, 1842, 1848, 1910, 1925, 1934, 1967, 1977, 2004, 2099, 2153,
53	(0, 6, 20)	0, 1, 28, 42, 59, 133, 183, 194, 218, 239, 339, 385, 404, 497, 499, 548, 695, 721, 773, 783, 805, 820, 843, 849, 922, 958, 962, 1048, 1056, 1226, 1251, 1256, 1290, 1333, 1623, 1680, 1854, 1872, 1925, 1941, 2022, 2102, 2191, 2194, 2203, 2266, 2314, 2321, 2334, 2417, 2450, 2554, 2621,
59	(0, 3, 11)	0, 1, 243, 331, 362, 386, 448, 469, 488, 598, 625, 734, 814, 816, 825, 839, 912, 915, 969, 1012, 1134, 1227, 1484, 1626, 1633, 1667, 1744, 1761, 1773, 1819, 2083, 2151, 2275, 2320, 2364, 2379, 2435, 2527, 2543, 2549, 2596, 2717, 2737, 2798, 2802, 2840, 2850, 2868, 2876, 3022, 3071, 3101, 3106, 3138, 3233, 3272, 3305, 3417, 3430,

p	$gen.$	$difference\ set\ (\bmod\ p^2 - 1)\ of\ p(p - 1)\ elements$
71	(0, 8, 54)	0, 1, 339, 345, 406, 542, 687, 821, 907, 989, 1171, 1294, 1429, 1443, 1502, 1522, 1553, 1617, 1628, 1650, 1691, 1737, 1792, 1828, 1946, 2108, 2125, 2229, 2237, 2247, 2266, 2281, 2461, 2500, 2503, 2550, 2655, 2743, 2768, 2966, 2970, 3019, 3028, 3035, 3127, 3195, 3280, 3328, 3360, 3405, 3426, 3431, 3617, 3912, 3996, 4019, 4031, 4162, 4273, 4343, 4400, 4460, 4490, 4514, 4590, 4592, 4630, 4673, 4686, 4836, 5013,
83	(0, 6, 60)	0, 1, 182, 187, 214, 255, 500, 503, 565, 590, 596, 827, 1353, 1389, 1406, 1456, 1501, 1555, 1577, 1629, 1690, 1720, 1900, 2039, 2067, 2136, 2250, 2261, 2265, 2336, 2645, 2704, 2737, 2783, 2785, 2792, 2984, 3250, 3271, 3479, 3641, 3711, 3723, 3746, 3760, 3868, 3902, 3953, 4053, 4063, 4071, 4194, 4296, 4309, 4353, 4459, 4568, 4592, 4611, 4675, 4722, 4738, 4764, 4896, 4973, 5013, 5093, 5191, 5230, 5346, 5366, 5490, 5550, 5616, 5654, 5710, 5844, 5922, 6279, 6337, 6611, 6683, 6712,
89	(0, 6, 77)	0, 1, 11, 323, 584, 613, 697, 739, 804, 940, 1052, 1256, 1273, 1430, 1535, 1816, 1820, 1871, 1896, 2030, 2280, 2347, 2566, 2598, 2648, 2743, 2781, 3096, 3352, 3496, 3624, 3790, 3831, 3868, 3887, 3922, 3927, 3953, 3974, 4115, 4179, 4293, 4397, 4445, 4478, 4561, 4736, 4815, 4885, 4971, 5074, 5082, 5098, 5268, 5280, 5369, 5426, 5479, 5556, 5679, 5830, 5858, 6067, 6135, 6138, 6184, 6259, 6303, 6683, 6783, 6822, 6852, 7024, 7047, 7195, 7197, 7255, 7269, 7289, 7501, 7544, 7562, 7589, 7682, 7691, 7697, 7704, 7822, 7858,
101	(0, 7, 60)	0, 1, 40, 354, 640, 885, 888, 1015, 1031, 1072, 1120, 1125, 1217, 1273, 1361, 1461, 1487, 1569, 1580, 1634, 1638, 1683, 1754, 1993, 2069, 2128, 2223, 2321, 2656, 2773, 2837, 2872, 3052, 3180, 3383, 3458, 3548, 3830, 3987, 4019, 4093, 4385, 4676, 4688, 4719, 4942, 4957, 4975, 5449, 5477, 5647, 5765, 5874, 5947, 5970, 6030, 6142, 6194, 6264, 6349, 6489, 6621, 6790, 6800, 6901, 6923, 7064, 7315, 7317, 7528, 7657, 7665, 7686, 7695, 7720, 7737, 7799, 7886, 7970, 8148, 8198, 8225, 8408, 8474, 8598, 8634, 8795, 8931, 9038, 9052, 9099, 9177, 9190, 9214, 9258, 9389, 9408, 9475, 9856, 9876, 10194
107	(0, 2, 29)	0, 1, 29, 224, 230, 300, 471, 497, 538, 789, 1049, 1190, 1193, 1276, 1467, 1509, 1566, 1709, 1774, 1919, 2067, 2598, 2834, 2859, 3009, 3023, 3028, 3230, 3334, 3395, 3450, 3474, 3571, 3732, 3856, 3941, 4166, 4292, 4329, 4369, 4381, 4449, 4561, 4595, 4615, 4713, 5053, 5388, 5395, 5743, 5747, 6086, 6276, 6298, 6345, 6752, 6788, 6848, 6901, 6922, 7031, 7033, 7327, 7602, 7632, 7696, 7704, 7739, 7958, 8096, 8211, 8238, 8249, 8366, 8688, 8704, 8779, 8823, 8872, 8956, 9001, 9019, 9034, 9051, 9107, 9173, 9232, 9346, 9355, 9436, 9482, 9802, 9850, 9860, 9873, 9960, 10247, 10446, 10549, 10735, 10827, 10866, 10928, 11033, 11084, 11115, 11289

p	$gen.$	$difference\ set\ (\bmod\ p^2 - 1)\ of\ p(p - 1)\ elements$
131	(0, 4, 18)	0, 1, 8, 49, 136, 674, 699, 811, 843, 954, 1044, 1198, 1217, 1338, 1376, 1615, 1753, 2201, 2215, 2225, 2309, 2321, 2443, 2635, 2662, 2702, 2704, 2843, 2936, 3284, 3782, 4495, 4881, 4947, 5006, 5039, 5042, 5304, 5386, 5433, 5513, 5623, 5629, 5794, 6032, 6133, 6183, 6198, 6353, 6611, 6648, 6828, 6954, 7168, 7365, 7417, 7437, 7468, 7567, 7621, 8051, 8160, 8343, 8389, 8411, 9030, 9048, 9242, 9300, 9323, 9339, 9885, 10100, 10173, 10330, 10642, 10924, 10959, 11195, 11266, 11295, 11380, 11440, 11526, 11571, 11628, 11792, 12096, 12159, 12272, 12488, 12644, 12688, 12923, 12934, 13220, 13425, 13446, 13588, 13649, 13934, 13938, 14393, 14511, 14704, 14721, 14819, 14893, 14971, 15041, 15118, 15146, 15295, 15325, 15359, 15414, 15582, 15744, 15749, 15931, 16022, 16294, 16401, 16427, 16480, 16489, 16802, 16845, 16858, 16962, 17085
137	(0, 2, 112)	0, 1, 61, 213, 288, 306, 353, 531, 568, 652, 686, 755, 900, 1118, 1175, 1185, 1763, 2101, 2179, 2322, 2473, 2489, 2578, 2763, 2785, 2920, 3102, 3142, 3155, 3339, 3468, 3509, 3538, 3776, 4101, 4157, 4320, 4403, 4436, 4479, 4569, 4575, 4601, 4737, 4829, 5239, 5250, 5277, 5486, 5822, 5881, 5945, 6056, 6339, 6430, 6791, 7095, 7107, 7278, 7366, 7535, 7636, 7996, 8116, 8182, 8226, 8262, 8491, 8591, 9106, 9164, 9250, 9295, 9577, 9703, 10031, 10034, 10059, 10138, 10187, 10235, 10524, 10747, 10801, 11185, 11302, 11309, 11326, 11570, 11781, 11790, 11820, 12163, 12461, 12512, 12567, 12586, 12649, 12654, 13083, 13168, 13374, 13394, 13489, 13694, 14017, 14432, 14800, 14894, 15147, 15256, 15386, 15534, 15681, 15683, 15923, 16392, 16695, 16875, 16890, 16898, 17071, 17092, 17106, 17205, 17627, 17804, 17978, 18264, 18326, 18378, 18424, 18428, 18505, 18536, 18578, 18697

8.4.2 Ricatti geometry.

Introduction.

It occurred to me that just like in 3 dimensional Euclidean geometry, the geometry on the sphere can be used as a model for the non euclidean geometry of elliptic type, in the same way the geometry on the surface $T : x^3 + y^3 + z^3 - 3xyz = 1$, can be used as a model for an other geometry, if $p \equiv -1 \pmod{6}$. I will call this geometry, Ricatti geometry. It turns out that this geometry is more akin to an Euclidean geometry. It can be considered as starting from a dual affine geometry in which we prefer a line (the ideal line) and a point (the ideal point) which is not on the line. The line corresponds to the intersection with $t = 0$ of the plane $x + y + z = 0$, the point to the direction of the line through the origin and the point $(1, 1, 1)$.

Definition.

Given $p \equiv -1 \pmod{6}$, the group $(\mathcal{T}, +)$ is cyclic (8.3.2). We determine a generator (a, b, c) of the group using in part 8.3.2. The points on \mathcal{T} are labelled according to $i(a, b, c)$ from 0 to $p^2 - 2$. The lines are the set of points on \mathcal{T} and a plane through the origin distinct from $[1, 1, 1, 1]$ and which does not contain the line from the origin to $(1, 1, 1, 1)$. The line through i and $i + 1$ is labelled $-i^$.*

Notation.

Points are denoted by a lower case letter or integer $\text{mod } p^2 - 1$, lines by the same followed by a * .

Definition.

If 2 points do not determine a line they are called parallel.

If 2 lines are not incident to a point they are called parallel.

Definition.

There is a correspondence between the point i and the line i^* , called polarity.

Theorem.

0. There are $p^2 - 1$ points and lines.
1. A line is incident to p points and a point to p lines.
2. A point is parallel to $p - 2$ points and a line is parallel to $p - 2$ lines.
3. There is duality in this geometry.

Theorem.

If i^* is incident to i_0, i_1, i_2, i_3 and i_4 , then $(i + j)^*$ is incident to $i_0 - j, i_1 - j, i_2 - j, i_3 - j$ and $i_4 - j$.

Definition.

Let D be a difference set associated to the integers in Z_{p^2-1} , between 0 and $p^2 - 1$, relatively prime to p , $D = \{d_0, d_1, \dots, d_{p-1}\}$.

0. The selector function is defined as follows,

$$f(k(p+1)) = -1,$$

$$f(d_j - d_i) = d_i.$$
1. With points represented by elements in Z_{p^2-1} and lines similarly represented but followed by * , the incidence relation is defined by

$$i \text{ is on } j^* \text{ iff } f(i + j) = 0.$$

Theorem.

0. i is parallel to j or i^* is parallel to j^* iff $f(i - j) = -1$,
1. the line $(i \times j)^*$ incident to i and j , not parallel, is $(f(i - j) - j)^*$.
2. the line k^* incident to i parallel to j^* is ...

Proof: For 2, we want k to be $\equiv j \pmod{p+1}$ such that $f(k + i) = 0, \dots$

Example.

$p = 5$, $D = \{0, 1, 14, 16, 21\}$,

i	0	1	2	3	4	5	6	7	8	9	10	11
$f(i)$	-1	0	14	21	21	16	-1	14	16	16	14	14
i	12	13	14	15	16	17	18	19	20	21	22	23
$f(i)$	-1	1	0	1	0	21	-1	21	1	0	16	1

Examples of such differences sets are given in 8.4.1.

Example.

$p = 5$, the computations are done mod 24.

0. The coordinates of the i -th point on \mathcal{T} are a_i, b_i, c_i , the distance between j and $j + i$ is

$$d_i = \sqrt[3]{a_i^3 + b_i^3 + (c_i - 1)^3 - 3a_i b_i (c_i - 1)}.$$

i	0	1	2	3	4	5	6	7	8	9	10	11
a_i	0	0	1	-1	-1	-1	2	-1	1	-2	-1	1
b_i	0	-1	-1	-2	-2	0	2	1	0	0	1	-1
c_i	1	-2	-1	1	-1	-2	0	-2	0	-1	-1	-2
d_i	0	3	1	1	0	3	3	4	0	4	1	4
i	12	13	14	15	16	17	18	19	20	21	22	23
a_i	-1	-2	0	-2	0	-1	-1	-2	-2	0	2	1
b_i	-1	-1	2	-1	1	-2	-1	1	-1	-2	0	-2
c_i	-2	0	2	1	0	0	1	-1	-1	-1	2	-1
d_i	0	2	4	1	0	1	2	2	0	4	4	2

1. The line i^* is incident to the points $-i, 1 - i, 14 - i, 16 - i, 21 - i$.

2. The point i is parallel to $i + 6, i + 12$ and $i - 6$.

3. The angle between lines j^* and $(j + i)^*$ is d_i .

In particular,

$0^* : 0, 1, 14, 16, 21$, is parallel to $6^*, 12^*, 18^*$,

$1^* : 23, 0, 13, 15, 20$, is parallel to $7^*, 13^*, 19^*$,

$14^* : 10, 11, 0, 2, 7$,

$16^* : 8, 9, 22, 0, 5$,

$21^* : 3, 4, 17, 19, 0$,

$23^* : 1, 2, 15, 17, 22$.

on 0^* , the distances are

	0	1	14	16	21
0	0	3	4	0	4
1	2	0	1	1	0
14	1	4	0	1	4
16	0	4	4	0	3
21	1	0	1	2	0

The “circles” of radius r and center 0 are

r	points on
1	2, 3, 10, 13, 15, 17
4	7, 9, 11, 14, 21, 22
2	18, 19, 23
3	1, 5, 6
0	0, 4, 8, 12, 16, 20

Example

Let $p = 11$,

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a_i	0	1	6	0	9	4	5	1	8	7	4	3	8	5	4	4
b_i	0	3	3	7	3	8	8	7	0	10	6	1	8	8	5	9
c_i	1	4	0	10	3	9	1	5	8	1	2	4	4	4	6	8
d_i	0	8	10	3	2	1	10	3	2	1	0	8	7	6	9	8
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
a_i	7	9	4	1	8	6	3	8	7	6	5	9	7	2	2	8
b_i	9	4	3	10	7	5	6	5	7	5	1	0	10	0	6	5
c_i	9	0	9	7	8	8	0	4	1	10	8	4	10	5	4	6
d_i	8	4	6	9	0	10	10	6	5	6	1	2	8	8	0	2
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
a_i	9	7	5	5	4	1	4	2	1	4	0	10	3	9	1	5
b_i	2	0	4	6	4	5	9	5	0	1	6	0	9	4	5	1
c_i	9	10	6	10	6	7	3	0	0	3	3	7	3	8	8	7
d_i	9	3	9	6	7	10	7	2	0	3	5	8	2	8	1	10

i	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
a_i	8	1	2	4	4	4	6	8	9	0	9	7	8	8	0	4
b_i	8	7	4	3	8	5	4	4	7	9	4	1	8	6	3	8
c_i	0	10	6	1	8	8	5	9	9	4	3	10	7	5	6	5
d_i	3	5	0	9	3	7	1	1	8	2	7	5	0	6	4	9
i	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79
a_i	1	10	8	4	10	5	4	6	9	10	6	10	6	7	3	0
b_i	7	6	5	9	7	2	2	8	9	7	5	5	4	1	4	2
c_i	7	5	1	0	10	0	6	5	2	0	4	6	4	5	9	5
d_i	3	10	10	4	8	2	0	6	8	1	10	3	9	3	6	8
i	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
a_i	0	3	3	7	3	8	8	7	0	10	6	1	8	8	5	9
b_i	1	4	0	10	3	9	1	5	8	1	2	4	4	4	6	8
c_i	0	1	6	0	9	4	5	1	8	7	4	3	8	5	4	4
d_i	0	9	4	1	4	5	2	8	2	9	0	3	3	9	10	5
i	96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111
a_i	9	4	3	10	7	5	6	5	7	5	1	0	10	0	6	5
b_i	9	0	9	7	8	8	0	4	1	10	8	4	10	5	4	6
c_i	7	9	4	1	8	6	3	8	7	6	5	9	7	2	2	8
d_i	6	5	1	1	0	2	5	7	3	3	2	5	4	3	0	10
i	112	113	114	115	116	117	118	119	120							
a_i	2	0	4	6	4	5	9	5	0							
b_i	9	10	6	10	6	7	3	0	0							
c_i	9	7	5	5	4	1	4	2	1							
d_i	9	8	1	10	9	8	1	3	0							

The “circles” of radius r and center 0 are

r	points on	
1	5, 9, 26, 46, 54, 55, 73, 83, 98, 99, 114, 118	(12)
10	2, 6, 21, 22, 37, 47, 65, 66, 74, 94, 111, 115	(12)
2	4, 8, 27, 31, 39, 44, 57, 69, 86, 88, 101, 106	(12)
9	14, 19, 32, 34, 51, 63, 76, 81, 89, 93, 112, 116	(12)
3	3, 7, 33, 41, 48, 52, 64, 75, 77, 91, 92, 104, 105, 109, 119	(15)
8	1, 11, 15, 16, 28, 29, 43, 45, 56, 68, 72, 79, 87, 113, 117	(15)
4	17, 62, 67, 82, 84, 108	(6)
7	12, 36, 38, 53, 58, 103	(6)
5	24, 42, 49, 59, 85, 95, 97, 102, 107	(9)
6	13, 18, 23, 25, 35, 61, 71, 78, 96	(9)
0	0, 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110	(12)

$p = 17$; circles of center 0 with given radius:

0 :	0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 256, 272	(18)
1 :	29, 60, 62, 73, 89, 111, 118, 133, 145, 147, 156, 159, 161, 162, 190, 195, 202, 205, 216, 235, 245, 251, 266, 278	(24)
2 :	24, 47, 67, 120, 151, 186, 223, 253, 263, 269, 275, 282	(12)
3 :	1, 8, 17, 38, 66, 70, 136, 219, 236, 258, 267, 268	(12)
4 :	18, 39, 74, 78, 87, 100, 106, 109, 113, 125, 134, 174, 193, 260, 262	(15)
5 :	23, 59, 92, 103, 110, 124, 139, 142, 165, 180, 213, 234	(12)
6 :	3, 33, 36, 41, 42, 44, 50, 51, 55, 56, 71, 77, 88, 101, 121, 138, 157, 172, 273, 274, 277	(21)
7 :	2, 4, 7, 9, 34, 61, 63, 68, 91, 107, 119, 153, 173, 198, 207	(15)
8 :	5, 27, 31, 40, 45, 46, 57, 58, 76, 84, 85, 97, 104, 105, 122, 130, 140, 171, 189, 194, 206, 209, 239, 276	(24)
9 :	12, 49, 79, 82, 94, 99, 117, 148, 158, 166, 183, 184, 191, 203, 204, 212, 230, 231, 242, 243, 248, 257, 261, 283	(24)
10 :	81, 90, 115, 135, 169, 181, 197, 220, 225, 227, 254, 279, 281, 284, 286	(15)
11 :	11, 14, 15, 116, 131, 150, 167, 187, 200, 211, 217, 232, 233, 237, 238, 244, 246, 247, 252, 255, 285	(21)
12 :	54, 75, 108, 123, 146, 149, 164, 178, 185, 196, 229, 265	(12)
13 :	26, 28, 95, 114, 154, 163, 175, 179, 182, 188, 201, 210, 214, 249, 270	(15)
14 :	20, 21, 30, 52, 69, 152, 218, 222, 250, 271, 280, 287	(12)
15 :	6, 13, 19, 25, 35, 65, 102, 137, 168, 221, 241, 264	(12)
16 :	10, 22, 37, 43, 53, 72, 83, 86, 93, 98, 126, 127, 129, 132, 141, 143, 155, 170, 177, 199, 215, 226, 228, 259	(24)

The points common to the circles given above and noted i : if the radius is i are given below if there are points which are common with

center 1, radius 1: 30,61,63,74,90,112,119,134,146,148,157,160,162,
163,191,196,203,206,217,236,246,252,267,279
0: 112,160; 1: 162; 3: 236,267; 4: 74,134; 6: 157;
7: 61,63,119; 8: 206; 9: 148,191,203; 10: 90,279;
11: 217,246,252; 12: 146,196; 13: 163; 14: 30;
center 1, radius 2: 25,48,68,121,152,187,224,254,264,270,276,283
0: 48,224; 6: 121; 7: 68; 8: 276; 9: 283; 10: 254; 11: 187;
13: 270; 14: 152; 15: 25,264;
center 1, radius 3: 2,9,18,39,67,71,137,220,237,259,268,269
2: 67,269; 3: 268; 4: 18,39; 6: 71; 7: 2,9; 10: 220; 11: 237;
15: 137; 16: 259;
center 1, radius 4: 19,40,75,79,88,101,107,110,114,126,135,175,194,261,
263
2: 263; 5: 110; 6: 88,101; 7: 107; 8: 40,194; 9: 79,261; 10: 135;
12: 75; 13: 114,175; 15: 19; 16: 126;
center 1, radius 5: 24,60,93,104,111,125,140,143,166,181,214,235
1: 60,111,235; 2: 24; 4: 125; 8: 104,140; 9: 166; 10: 181;
13: 214; 16: 93,143;
center 1, radius 6: 4,34,37,42,43,45,51,52,56,57,72,78,89,102,122,139,
158,173,274,275,278
1: 89,278; 2: 275; 4: 78; 5: 139; 6: 42,51,56,274; 7: 4,34,173;
8: 45,57,122; 9: 158; 14: 52; 15: 102; 16: 37,43,72;
center 1, radius 7: 3,5,8,10,35,62,64,69,92,108,120,154,174,199,208
0: 64,208; 1: 62; 2: 120; 3: 8; 4: 174; 5: 92; 6: 3; 8: 5; 12: 108;
13: 154; 14: 69; 15: 35; 16: 10,199;
center 1, radius 8: 6,28,32,41,46,47,58,59,77,85,86,98,105,106,123,131,
141,172,190,195,207,210,240,277
0: 32,240; 1: 190,195; 2: 47; 4: 106; 5: 59; 6: 41,77,172,277;
7: 207; 8: 46,58,85,105; 11: 131; 12: 123; 13: 28,210; 15: 6;
16: 86,98,141;

center 1, radius 9: 13,50,80,83,95,100,118,149,159,167,184,185,192,204,
205,213,231,232,243,244,249,258,262,284
0: 80,192; 1: 118,159,205; 3: 258; 4: 100,262; 5: 213; 6: 50;
9: 184,204,231,243; 10: 284; 11: 167,232,244; 12: 149,185;
13: 95,249; 15: 13; 16: 83;
center 1, radius 10: 82,91,116,136,170,182,198,221,226,228,255,280,282,
285,287
2: 282; 3: 136; 7: 91,198; 9: 82; 11: 116,255,285; 13: 182;
14: 280,287; 15: 221; 16: 170,226,228;

center 1, radius 11: 12,15,16,117,132,151,168,188,201,212,218,233,234,
238,239,245,247,248,253,256,286
0: 16,256; 1: 245; 2: 151,253; 5: 234; 8: 239; 9: 12,117,212,248;
10: 286; 11: 15,233,238,247; 13: 188,201; 14: 218; 15: 168; 16: 132;
center 1, radius 12: 55,76,109,124,147,150,165,179,186,197,230,266
1: 147,266; 2: 186; 4: 109; 5: 124,165; 6: 55; 8: 76; 9: 230;
10: 197; 11: 150; 13: 179;
center 1, radius 13: 27,29,96,115,155,164,176,180,183,189,202,211,215,
250,271
0: 96,176; 1: 29,202; 5: 180; 8: 27,189; 9: 183; 10: 115; 11: 211;
12: 164; 14: 250,271; 16: 155,215;
center 1, radius 14: 21,22,31,53,70,153,219,223,251,272,281,0
0: 0,272; 1: 251; 2: 223; 3: 70,219; 7: 153; 8: 31; 10: 281;
14: 21; 16: 22,53;
center 1, radius 15: 7,14,20,26,36,66,103,138,169,222,242,265
3: 66; 5: 103; 6: 36,138; 7: 7; 9: 242; 10: 169; 11: 14; 12: 265;
13: 26; 14: 20,222;
center 1, radius 16: 11,23,38,44,54,73,84,87,94,99,127,128,130,133,142,
144,156,171,178,200,216,227,229,260
0: 128,144; 1: 73,133,156,216; 3: 38; 4: 87,260; 5: 23,142; 6: 44;
8: 84,130,171; 9: 94,99; 10: 227; 11: 11,200; 12: 54,178,229;
16: 127;

center 2, radius 1: 31,62,64,75,91,113,120,135,147,149,158,161,163,164,
192,197,204,207,218,237,247,253,268,280
0: 64,192; 1: 62,147,161; 2: 120,253; 3: 268; 4: 113; 7: 91,207;
8: 31; 9: 158,204; 10: 135,197; 11: 237,247; 12: 75,149,164;
13: 163; 14: 218,280;
center 2, radius 2: 26,49,69,122,153,188,225,255,265,271,277,284
6: 277; 7: 153; 8: 122; 9: 49; 10: 225,284; 11: 255; 12: 265;
13: 26,188; 14: 69,271;
center 2, radius 3: 3,10,19,40,68,72,138,221,238,260,269,270
2: 269; 4: 260; 6: 3,138; 7: 68; 8: 40; 11: 238; 13: 270;
15: 19,221; 16: 10,72;
center 2, radius 4: 20,41,76,80,89,102,108,111,115,127,136,176,195,262,
264
0: 80,176; 1: 89,111,195; 3: 136; 4: 262; 6: 41; 8: 76; 10: 115;
12: 108; 14: 20; 15: 102,264; 16: 127;
center 2, radius 5: 25,61,94,105,112,126,141,144,167,182,215,236
0: 112,144; 3: 236; 7: 61; 8: 105; 9: 94; 11: 167; 13: 182; 15: 25;
16: 126,141,215;

center 2, radius 6: 5,35,38,43,44,46,52,53,57,58,73,79,90,103,123,140,
159,174,275,276,279
1: 73,159; 2: 275; 3: 38; 4: 174; 5: 103; 6: 44;
8: 5,46,57,58,140,276; 9: 79; 10: 90,279; 12: 123; 14: 52; 15: 35;
16: 43,53;
center 2, radius 7: 4,6,9,11,36,63,65,70,93,109,121,155,175,200,209
3: 70; 4: 109; 6: 36,121; 7: 4,9,63; 8: 209; 11: 11,200; 13: 175;
15: 6,65; 16: 93,155;
center 2, radius 8: 7,29,33,42,47,48,59,60,78,86,87,99,106,107,124,132,
142,173,191,196,208,211,241,278
0: 48,208; 1: 29,60,278; 2: 47; 4: 78,87,106; 5: 59,124,142;
6: 33,42; 7: 7,107,173; 9: 99,191; 11: 211; 12: 196; 15: 241;
16: 86,132;

center 2, radius 9: 14,51,81,84,96,101,119,150,160,168,185,186,193,205,
206,214,232,233,244,245,250,259,263,285
0: 96,160; 1: 205,245; 2: 186,263; 4: 193; 6: 51,101; 7: 119;
8: 84,206; 10: 81; 11: 14,150,232,233,244,285; 12: 185; 13: 214;
14: 250; 15: 168; 16: 259;
center 2, radius 10: 83,92,117,137,171,183,199,222,227,229,256,281,283,
286,0
0: 0,256; 5: 92; 8: 171; 9: 117,183,283; 10: 227,281,286; 12: 229;
14: 222; 15: 137; 16: 83,199;
center 2, radius 11: 13,16,17,118,133,152,169,189,202,213,219,234,235,
239,240,246,248,249,254,257,287
0: 16,240; 1: 118,133,202,235; 3: 17,219; 5: 213,234; 8: 189,239;
9: 248,257; 10: 169,254; 11: 246; 13: 249; 14: 152,287; 15: 13;
center 2, radius 12: 56,77,110,125,148,151,166,180,187,198,231,267
2: 151; 3: 267; 4: 125; 5: 110,180; 6: 56,77; 7: 198;
9: 148,166,231; 11: 187;
center 2, radius 13: 28,30,97,116,156,165,177,181,184,190,203,212,216,
251,272
0: 272; 1: 156,190,216,251; 5: 165; 8: 97; 9: 184,203,212; 10: 181;
11: 116; 13: 28; 14: 30; 16: 177;
center 2, radius 14: 22,23,32,54,71,154,220,224,252,273,282,1
0: 32,224; 2: 282; 3: 1; 5: 23; 6: 71,273; 10: 220; 11: 252;
12: 54; 13: 154; 16: 22;
center 2, radius 15: 8,15,21,27,37,67,104,139,170,223,243,266
1: 266; 2: 67,223; 3: 8; 5: 139; 8: 27,104; 9: 243; 11: 15; 14: 21;
16: 37,170;
center 2, radius 16: 12,24,39,45,55,74,85,88,95,100,128,129,131,134,
143,145,157,172,179,201,217,228,230,261
0: 128; 1: 145; 2: 24; 4: 39,74,100,134; 6: 55,88,157,172;
8: 45,85; 9: 12,230,261; 11: 131,217; 13: 95,179,201;
16: 129,143,228;

8.4.3 3 - Dimensional Equidistance Curves.

Introduction.

On the surface T , for $p \equiv -1 \pmod{5}$, we can define besides lines (intersection with a plane through the origin), circles (pts equidistant using the cubic function from a given point), line-circle (set of tangents in space to the circles), podars (set of points where tangents in space intersect T), mediatrices (set of points equidistant from 2 points). This section describes those curves.

Definition.

The circles are the set of points on T such that the cubic distance from a given point on T , called the center of the circle, is a given integer r , called the radius of the circle.

Theorem.

The circles of radius r and center $(0, 0, 1)$, are the points (x, y, z) which satisfy 0. and 1. or 0. and 2.

$$0. \quad x^3 + y^3 + z^3 - 3xyz = 1.$$

$$1. \quad x^3 + y^3 + z^3 - 3z^2 + 3z - 1 - 3xyz + 3xy = r^3.$$

$$2. \quad 3z^2 - 3z - 3xy = -r^3.$$

Definition.

A line-circle is the set of lines tangent in space to a circle.

Theorem.

The line-circle associated to the circles in 8.4.3 have at (x, y, z) the direction $(\Delta x, \Delta y, \Delta z)$ given by

$$0. \quad \Delta x = xz_2 + z'y_2, \Delta y = -yz_2 - z'x_2, \Delta z = -xx_2 + yy_2, \\ \text{where}$$

$$1. \quad x_2 = x^2 - yz, y_2 = y^2 - zx, z_2 = z^2 - xy, z' = 2z - 1.$$

Proof: the component of the direction satisfy

$$(x^2 - yz)\Delta x + (y^2 - zx)\Delta y + (z^2 - xy)\Delta z = 0, \\ -y\Delta x - x\Delta y + (2z - 1)\Delta z = 0,$$

hence 0.

Definition.

A podar is set of points where tangents in space intersect T .

Theorem.

The coordinates of points on the podar associated to the circle in 8.4.3 are the points $(x + t\Delta x, y + t\Delta y, z + t\Delta z)$ where t satisfies

$$0. \quad t = -3 \frac{x\Delta x_2 + y\Delta y_2 + z\Delta z_2}{(\Delta x + \Delta y + \Delta z)} (\Delta x_2 + \Delta y_2 + \Delta z_2).$$

where

$$1. \quad \Delta x_2 = \Delta x^2 - \Delta y\Delta z, \Delta y_2 = \Delta y^2 - \Delta z\Delta x, \Delta z_2 = \Delta z^2 - \Delta x\Delta y.$$

Proof. A point $(x + t\Delta x, y + t\Delta y, z + t\Delta z)$ on the line (x, y, z) with direction $(\Delta x, \Delta y, \Delta z)$ is on T if t satisfies the cubic equation,

$$(\Delta x + \Delta y + \Delta z)(\Delta x_2 + \Delta y_2 + \Delta z_2)t^3 + 3(x\Delta x_2 + y\Delta y_2 + z\Delta z_2)t^2 + 3(x_2\Delta x + y_2\Delta y + z_2\Delta z)t + (x^3 + y^3 + z^3 - 3xyz - 1) + 1 = 0,$$

the coefficient of t^0 is 0 because (x, y, z) is on T , that of t is 0 because it is $x_2(xz_2 + z'y_2) + y_2(-yz_2 - z'x_2) + z_2(-xx_2 + yy_2) = 0$.

Theorem.

0. If the tangent k^* at i to the circle, centered at 0 of radius r , meets T at j , then the tangent $(k^{+2i})^*$ at $-i$ to the circle, centered at 0 of radius $-r \pmod{p}$, meets T at $j - 2i$.

1. If the tangent at i to the circle, centered at 0 of radius r , meets T at j parallel to i , then the tangent at $-i$ to the circle, centered at 0 of radius $-r \pmod{p}$, meets T at $j - 2i$ parallel to $-i$.

Example.Let $p = 11$, $r = 1$,*circle**podar**line-circle*

5	9	26	46	54	55	73	83	98	99	114	118
92	15	113	43	51	52	4	44	107	45	81	97
29*	19*	8*	118*	110*	109*	30*	0*	22*	119*	40*	32*

 $r = 10$,*circle**podar**line-circle*

2	6	21	22	37	47	65	66	74	94	111	115
101	93	87	31	118	98	62	63	71	61	117	82
28*	28*	77*	98*	46*	56*	99*	98*	90*	60*	37*	39*

 $r = 2$ *circle**podar**line-circle*

4	8	27	31	39	44	57	69	86	88	101	106
28	59	36	118	6	68	36	66	95	49	98	85
—	95*	93*	3*	115*	—	93*	95*	34*	115*	63*	44*

 $r = 9$ *circle**podar**line-circle*

14	19	32	34	51	63	76	81	89	93	112	116
113	16	113	43	48	42	100	48	56	102	43	20
16*	25*	51*	86*	113*	87	—	73*	65*	27*	111*	—

 $r = 3$ *circle**podar**line-circle*

3	7	33	41	48	52	64	75	77	91	104	105	109	119
9	88	99	107	48	58	73	84	8	97				
25*	76*	65*	57*	—	96*	56*	45*	26*	57*				

 $r = 3$ *circle**podar**line-circle*

	92	104	105	109	119
	38	83	84	40	80
	6*	46*	45*	114*	84*

 $r = 8$ *circle**podar**line-circle*

1	11	15	16	28	29	43	45	56	68
82	62	114	115	94	35	94	54	65	74
82*	92*	15*	14*	70*	119*	60*	75*	64*	80*

 $r = 8$ *circle**podar**line-circle*

	72	79	87	113	117
	72	25	33	74	3
	—	19*	11*	90*	31*

 $r = 4$ *circle**podar**line-circle*

17	62	67	82	84	108
41	113	91	43	84	108
—	41*	—	1*	—	—

 $r = 7$ *circle**podar**line-circle*

12	36	38	53	58	103
12	36	119	77	109	7
—	—	45*	—	45*	—

 $r = 5$ *circle**podar**line-circle*

24	42	49	59	85	95	97	102	107
24	21	73	83	16	56	103	111	53
—	108*	—	—	18*	108*	51*	18*	111*

 $r = 6$ *circle**podar*

13	18	23	25	35	61	71	78	96
79	27	29	106	86	85	95	57	96

Definition.

A mediatrix of 2 points is the set of points equidistant from them.

Conjecture.

The number of points on the mediatrix is $\equiv 0 \pmod{4}$, unless the points are i and $i + k(p - 1)$ in which case it is \dots namely these points are for 0 and $p - 1$, $(p - 1)k$ and $(p + 1)k - 1$. When $p = 11$, the multiples are 8, 12 and 16; when $p = 17$, 12, 16, 20 and 24; when $p = 23$, 0, 16, 20, 24, 28, 32.

Example

of mediatrices for $p = 11$:

For 0 and 3, 0 and 6, 0 and 9, no points.

For 0 and 1: 16, 22, 29, 55, 66, 92, 99, 105.

For 0 and 2: 25, 34, 38, 45, 77, 84, 88, 97.

For 0 and 4: 1, 3, 6, 7, 8, 9, 15, 31, 52, 72, 93, 109, 115, 116, 117, 118.

For 0 and 5: 16, 18, 19, 23, 44, 58, 67, 81, 102, 106, 107, 109.

For 0 and 7: 2, 5, 25, 48, 49, 78, 79, 102.

For 0 and 8: 1, 7, 39, 41, 54, 74, 87, 89.

For 0 and 10: $10i$ and $12i - 1$.

For 0 and 11: 2, 5, 6, 9, 52, 56, 75, 79.

For 0 and 12: 25, 28, 35, 39, 63, 64, 68, 69, 93, 97, 104, 107.

For 0 and 13: 28, 29, 32, 44, 56, 57, 76, 77, 89, 101, 404, 105.

For 0 and 14: 3, 11, 15, 29, 43, 91, 105, 119.

For 0 and 15: 6, 9, 16, 21, 34, 37, 43, 48, 53, 82, 87, 92, 98, 101, 114, 119.

For 0 and 16: 22, 37, 45, 64, 72, 91, 99, 114.

For 0 and 17: 26, 28, 35, 44, 45, 51, 53, 59.

For 0 and 18: 3, 4, 7, 11, 14, 15, 29, 32, 42, 57, 65, 73, 81, 96, 106, 109.

For 0 and 19: 3, 16, 21, 27, 51, 52, 66, 73, 87, 88, 112, 118.

Definition.

The horizon of a point P on T is the set of points on T and the tangent plane through P .

Theorem.

The coordinates of points on the tangent at $P = (x, y, z)$ in the plane P through O and $Q = (x', y', z')$ which is also on T is

$(x + t\Delta x, y + t\Delta y, z + t\Delta z)$, where t satisfies

$$0. \quad t = -3 \frac{x\Delta x_2 + y\Delta y_2 + z\Delta z_2}{(\Delta x + \Delta y + \Delta z)} (\Delta x_2 + \Delta y_2 + \Delta z_2).$$

where

$$1. \quad \Delta x_2 = \Delta x^2 - \Delta y \Delta z, \Delta y_2 = \Delta y^2 - \Delta z \Delta x, \Delta z_2 = \Delta z^2 - \Delta x \Delta y.$$

Proof. The direction of the normal to P at P is $(a := yz' - zy', b := zx' - xz', c := xy' - yx')$. The direction $(\Delta x, \Delta y, \Delta z)$ satisfies $a\Delta x + b\Delta y + c\Delta z = 0$ and $x_2\Delta x + y_2\Delta y + z_2\Delta z = 0$, where

$$x_2 = x^2 - yz, y_2 = y^2 - zx, z_2 = z^2 - xy,$$

therefore $\Delta x = y_2c - z_2b$, $\Delta y = z_2a - x_2c$, $\Delta z = x_2b - y_2a$.

A point $(x + t\Delta x, y + t\Delta y, z + t\Delta z)$ on the line (x, y, z) with direction $(\Delta x, \Delta y, \Delta z)$ is on T if t satisfies the cubic equation,

$$(\Delta x + \Delta y + \Delta z)(\Delta x_2 + \Delta y_2 + \Delta z_2)t^3 + 3(x\Delta x_2 + y\Delta y_2 + z\Delta z_2)t^2 + 3(x_2\Delta x + y_2\Delta y + z_2\Delta z)t + (x^3 + y^3 + z^3 - 3xyz - 1) + 1 = 0,$$

the coefficient of t^0 is 0 because (x, y, z) is on T , that of t is 0 because it is $x_2(y_2c - z_2b) + y_2(z_2a - x_2c) + z_2(x_2b - y_2a) = 0$.

Algorithm.

To determine the horizon as 0 we determine for each point with $z = 1$, on which the line $0 \times \text{sel}(i)$ it is located, if $x + y = 0$, the point is the ideal point, if $x = 0$ or $y = 0$, 0 is a triple contact, if it is on no line $0 \times \text{sel}(i)$, then it corresponds to points parallel to it. This is implement in $\wedge 130 \backslash \text{RIC.BAS}$ option 12.

Proof: The horizon of P of 0 are the points on T and $z = 1$ or $x^3 + y^3 - 3xy = 0$, those in the plane $x = kt$, $y = lt$ satisfy $(k^3 + l^3)t - 3kl = 0$ and $t = 0$, twice. If $k = 0$ or $l = 0$ then $t = 0$ is a triple root, if $k = -l$, or $x + y = 0$, then the point is an ideal point. In all other cases, $t = \frac{3kl}{k^3 + l^3}$.

Example.

For $p = 11$, the points H on the horizon of 0 have their tangent t and the points Q on T for which the tangent is t^* given by

H	t^*	Q
0	1*	8, 27, 29, 33, 40, 43, 82, 97, 102, 119($y = 0$)
	41*	3, 42, 57, 62, 79, 80, 88, 107, 109, 113($x = 0$)
6	28*	2, 6, 13, 16, 55, 70, 75, 92, 93, 101
9	0*	1, 9, 28, 30, 34, 41, 44, 83, 98, 103
24	—	12, 24, 36, 48, 60, 72, 84, 96, 108
51	103*	17, 18, 26, 45, 47, 51, 58, 61, 100, 115
66	98*	5, 22, 23, 31, 50, 52, 56, 63, 66, 105
81	83*	15, 20, 37, 38, 46, 65, 67, 71, 78, 81
87	34*	7, 10, 49, 64, 69, 86, 87, 95, 114, 116
99	30*	4, 11, 14, 53, 68, 73, 90, 91, 99, 118
117	44*	39, 54, 59, 76, 77, 85, 104, 106, 110, 117
∞	9*	19, 21, 25, 32, 35, 74, 89, 94, 111, 112

Conjecture.

The points on the horizon of 0 are multiples of 3.

Example.

The horizon of 0 is for

0. $p = 5$,

selector	0	1	14	16	21	—
horizon	0	15	∞	0	3	18

1. $p = 11$,

selector	0	1	9	28	30	34	41	44	83	98	103	—
horizon	9	0	∞	6	99	87	0117	81	66	51	24	

2. $p = 17$,

<i>selector</i>	0	1	10	13	34	45	59	86	112	114	129	134
<i>horizon</i>	114	111	24	246	225	150	0	165	210	81	159	213
<i>selector</i>	191	195	251	259	282	—	—					
<i>horizon</i>	∞	93	0	141	120	108						

3. $p = 23$,

<i>selector</i>	0	1	60	91	134	142	148	203	249	253	266	269
<i>horizon</i>	0	270	273	180	69	387	471	285	279	366	3	219
<i>selector</i>	271	298	305	333	342	352	363	375	450	488	503	—
<i>horizon</i>	81	231	426	444	33	0	498	402	453	∞	294	408

8.4.4 Generalization of the Selector Function.

Introduction.

The selector function was introduced by Fernand Lemay to determine easily from the selector, points on 2 lines, lines incident to 2 points, points on lines or lines incident to points. This notion is generalized to 3 and more? dimensions.

Definition.

defining polynomial

Theorem.

If the P_i denotes a primitive polynomial of degree i , for $k = 3$, the defining polynomials P can have the following form,

$$P_4, P_1P_3, P_1^2P_2,$$

there are $p^4 + p^3 + p^2 + p + 1$, $p^4 - 1$, $p^4 - p$ polynomials relatively prime to P , in these respective cases.

For $k = 4$, the defining polynomials P can have the following form,

$$P_5, P_1P_4, P_1^2P_3, P_2P_3.$$

there are $p^5 + p^4 + p^3 + p^2 + p + 1$, $(p^3 - 1)(p + 1)$, $p^5 - 1$, $p^5 - p$ polynomials relatively prime to P , in these respective cases.

Proof: The polynomials in the sets are those which are relatively prime to the defining polynomial. There are p^k homogeneous polynomials of degree k . If, for instance, $k = 4$ and the defining polynomial P is P_2P_3 , there are $p^2 + p + 1$ polynomials which are multiple of P^2 and $p + 1$, which are multiples of P_3 , hence $p^4 + p^3 + p^2 + p + 1 - (p^2 + p + 1) - (p - 1)$ polynomials relatively prime to P .

Example.

a_0, a_1, \dots represents $I^{k+1} - a_0 I^k - a_1 I^{k-1} - \dots$.

k	p	period	def.pol.	sel.	roots of def.pol. or prim.pol.
3	3	40	2, 1, 1, 1	13	—
		26	1, 1, 1, 1	9	1
		24	0, 1, 1, 1	8	2, 2
5		156	1, 2, 0, 2	31	—
		124	1, 0, 0, 2	25	4
		120	0, 0, 1, 2	24	4, 4
4	3	121	2, 0, 0, 0, 1	40	—
		104	0, 1, 0, 0, 1	35	$(I^2 + I - 1)(I^3 - I^2 + I + 1)$
		80	0, 2, 0, 0, 1	27	2
5		78	1, 0, 0, 0, 1	26	2, 2
		781	4, 0, 0, 0, 1	156	—
		744	2, 2, 0, 0, 1	149	$(I^2 + I + 2)(I^3 + 2I^2 - I + 2)$
7		624	2, 0, 0, 0, 1	125	3
		620	3, 0, 1, 0, 1	124	3, 3
		2801	3, 0, 0, 0, 1	400	—
11		2736	6, 0, 0, 0, 1	391	$(I^2 + 2I - 2)(I^3 - I^2 - 3I - 3)$
		2400	3, 1, 0, 0, 1	343	3
		2394	0, 3, 3, 0, 1	342	5, 5
13		30941	8, 0, 0, 0, 1	2380	—
		30744	5, 0, 0, 0, 1	2365	$(I^2 - 3I + 6)(I^3 - 2I^2 + I + 2)$
		28560	2, 0, 0, 0, 1	2197	11
5	3	28548			
		364	1, 0, 0, 0, 0, 1	121	—
		242	1, 1, 0, 0, 0, 1	81	2
5		240	1, 2, 1, 0, 0, 1	80	2, 2

Definition.

Given a selector s , the selector function associates to the integers in the set Z_n a set of $p+1$ integers or p integers obtained as follows,

$$s(j) \in f_i \text{ iff } sel(l) - sel(j) = i \text{ for some } l.$$

Theorem.

0. $f(i)$ is the set of points on the line $i^* \times 0^*$.
1. $0.f(i) - j$, where we subtract j to each element in the set, is the set of points in $(i+j)^* \times j^*$, equivalently
2. $1.f(i-j) - j$, is the set of points in $i^* \times j^*$.
3. $a^* \times b^* \times c^* = ((a-i)^* \times (b-i)^* \times (c-i)^*) - i$.

Definition.

Theorem.

Theorem.

0. If the defining polynomial is primitive, then

1. 0. $|s| = \frac{p^k-1}{p-1}$,

2. 1. if $i \neq 0$, $|f(i)| = p+1$

3. If the defining polynomial has one root, then

4. 0. $|s| = p^k$,

5. 1. if $i \neq 0$, $|f(i)| = p$,

6. If the defining polynomial has one root, then

7. 0. $|s| = p^k - 1$,

8. 1. if $i \neq 0$, $|f(i)| = p$,

9. 2. if $i \neq 0$, $|f(i)| = p-1$,

10. If the defining polynomial has one quadratic factor, then

11. 0. $|s| = (p^k - 1)(p+1)?$,

12. 1. if $i \neq 0$, $|f(i)| = p$,

Example.

0. $k = 3$, $p = 3$, defining polynomial $I^4 - 2I^3 - I^2 - I - 1$.

selector: 0 1 2 9 10 13 15 16 18 20 24 30 37

selector function:

0	-1	-1	-1	-1	14	1	2	10	16	28	2	9	13	30
1	0	1	9	15	15	0	1	9	15	29	1	13	20	24
2	0	13	16	18	16	0	2	24	37	30	0	10	20	30
3	10	13	15	37	17	1	13	20	24	31	9	10	18	24
4	9	16	20	37	18	0	2	24	37	32	9	10	18	24
5	10	13	15	37	19	1	18	30	37	33	9	16	20	37
6	9	10	18	24	20	0	10	20	30	34	15	16	24	30
7	2	9	13	30	21	9	16	20	37	35	2	15	18	20
8	1	2	10	16	22	2	15	18	20	36	1	13	20	24
9	0	1	9	15	23	1	18	30	37	37	0	13	16	18
10	0	10	20	30	24	0	13	16	18	38	2	15	18	20
11	2	9	13	30	25	15	16	24	30	39	1	2	10	16
12	1	18	30	37	26	15	16	24	30					
13	0	2	24	37	27	10	13	15	37					

1. $k = 3, p = 3, \text{defining polynomial } I^4 - I^3 - I^2 - I - 1.$

selector: 0 1 2 8 11 18 20 22 23

selector function:

0	-1	-1	-1	7	1	11	20	14	8	20	23	21	1	2	23
1	0	1	22	8	0	18	20	15	8	11	22	22	0	1	22
2	0	18	20	9	2	11	18	16	2	11	18	23	0	11	23
3	8	20	23	10	1	8	18	17	1	11	20	24	2	20	22
4	18	22	23	11	0	11	23	18	0	2	8	25	1	2	23
5	18	22	23	12	8	11	22	19	1	8	18				
6	2	20	22	13	-1	-1	-1	20	0	2	8				

2. $k = 3, p = 3, \text{defining polynomial } I^4 - I^2 - I - 1.$

selector: 0 1 2 4 14 15 19 21

selector function:

0	-1	-1	-1	6	15	19	-1	12	2	14	-1	18	1	21	-1
1	0	1	14	7	14	19	21	13	1	2	15	19	0	2	19
2	0	2	19	8	-1	-1	-1	14	0	1	14	20	1	4	19
3	1	21	-1	9	15	19	-1	15	0	4	-1	21	0	4	-1
4	0	15	21	10	4	14	15	16	-1	-1	-1	22	2	4	21
5	14	19	21	11	4	14	15	17	2	4	21	23	1	2	15

Example.

In the case of Example 3.6.x.0. if we denote by $i^\%$, the lines $0^* \times i^*$, these lines, which are sets of 4 points can all be obtained from

$1^\% = \{0, 1, 9, 15\}$, $2^\% = \{0, 13, 16, 18\}$, $4^\% = \{9, 16, 20, 37\}$ and

$10^\% = \{0, 10, 20, 30\}$ by adding an integer modulo n .

$1^\% + 0 = 1^\%$, $9^\%$, $15^\%$, $1^\% + 1 = 39^\%$, $8^\%$, $14^\%$, $1^\% + 9 = 6^\%$, $31^\%$, $32^\%$, $1^\% + 15 = 34^\%$, $25^\%$, $26^\%$,
 $2^\% + 0 = 2^\%$, $24^\%$, $37^\%$, $2^\% + 2 = 22^\%$, $35^\%$, $38^\%$, $2^\% + 37 = 3^\%$, $5^\%$, $27^\%$, $2^\% + 24 = 13^\%$, $16^\%$, $18^\%$,
 $4^\% + 0 = 4^\%$, $21^\%$, $33^\%$, $4^\% + 4 = 17^\%$, $29^\%$, $36^\%$, $4^\% + 21 = 12^\%$, $19^\%$, $23^\%$,
 $4^\% + 33 = 7^\%$, $11^\%$, $28^\%$,
 $10^\% + 0 = 10^\%$, $20^\%$, $30^\%$.

Definition.

Conjecture.

8.5 Generalization of the Spheres in Riccati Geometry.

8.5.1 Dimension k .

Introduction.

If we choose the “sphere“ $x^3 + y^3 + z^3 - 3xyz = 1$ in 3 dimension we do not obtain for a given prime all periods as we do with the selector. We have to generalize using what is derived from differential equations with constant coefficients in which the coefficient of the $k - 1$ -th derivative is zero to obtain a constant Wronskian. But, just as in the case of 2 dimensions, to obtain all sets of trigonometric functions, corresponding to the circular and hyperbolic functions, for all p , we have

to introduce in 3 dimension a cubic non residue if there is any, ... I will first recall some well known definitions and Theorems of linear differential equations.

Definition.

Given a linear differential equation $D^k x = C_0 x + C_1 D x + \dots C_{k-2} D^{k-2} x$, and k solutions y_i of these equations, the Wronskian is the matrix of functions whose j -th row are the j -th derivatives of y_i , for $i = 0$ to $k - 1$.

Theorem.

0. The functions y_i are independent solution iff the determinant of the Wronskian is different from 0 for a particular value of the independent variable.
1. The determinant of the Wronskian is a constant function.
2. If $W(0) = E$, then $W(x + y) = W(x)W(y)$.

Theorem.

If the linear differential equation 8.5.1.0. is such that C_i are constant functions then any linear combination of x and its derivatives is also a solution of 8.5.1.0.

Comment.

If we choose x such that its derivatives are 0 except the $k - 1$ -th, chosen equal to 1, it is easy to obtain independent solutions using linear combination of x and its derivatives to insure $W(0) = E$. If $\det(W(t)) = 1$, then $\det(W(nt)) = 1$ and the surface $D^i x(nt)$, $i = 0$ to $k - 1$, can be chosen as a "sphere" in k -dimension and n as the angle between the directions joining the origin to the points $(D^i x((n + a)t))$ and $(D^i x(at))$.

Notation.

Given 2 solutions x and x' of 8.5.1.0. and a parameter t let $x_i := \{D^j x(it)\}$ and $x'_i := \{D^j x'(it)\}$,
 $y_{i,j} := x_i x'_j + x_j x'_i$, $i \neq j$
 $y_{i,i} := x_i x'_i$,

8.5.2 Dimension 3.

Theorem.

For $k = 3$, let

$$0.0. \quad D^3 x_0 = C_0 x_0 + C_1 D x_0,$$

with

$$0.1. \quad D x_0(0) = 0, \quad D x_0 = x_1(0) = 0, \quad D^2 x_0(0) = x^2(0) = 1,$$

then

1.0. the set of functions $x_2 - C_1 x_0$, x_1 , x_0 are independent

1. their Wronskian is

$$W = \begin{vmatrix} x_2 - C_1x_0 & x_1 & x_0 \\ C_0x_0 & x_2 & x_1 \\ C_0x_1 & C_0x_0 + C_1x_1 & x_2 \end{vmatrix}$$

3. $W(0) = E$.

2. The distance from $(0, 0, 0)$ to (x_0, x_1, x_2) is

$$C_0^2x_0^3 + C_0x_1^3 + x_2^3 - 3x_0x_1x_2 - C_1x_1^2x_2 - C_1x_2^2x_0 + 2C_0C_1x_0^2x_1 \\ + C_1^2x_0x_1^2.$$

3. The addition formulas are

$$x_0'' = y_{0,2} + y_{1,1} - C_1y_{0,0}, \\ x_1'' = y_{1,2} + C_0y_{0,0}, \\ x_2'' = y_{2,2} + C_0y_{0,1} + C_1y_{1,1}.$$

4. The tangent plane at (x_0, x_1, x_2) is

$$[3C_0^2x_0^2 - 3C_0x_1x_2 - C_1x_2^2 + 4C_0C_1x_0x_1 + C_1^2x_1^2, \\ 3C_0x_1^2 - 3C_0x_2x_0 + 2C_0C_1x_0^2 - 2C_1x_1x_2 + 2C_1^2x_0x_1, \\ 3x_2^2 - 3C_0x_0x_1 - 2C_1x_2x_0 - C_1x_1^2].$$

Definition.

If

0. $p \equiv 1 \pmod{6}$, then $\nu^3 = n$ is a non cubic residue and the functions are not necessary real, we therefore denote then by ξ_i instead of x_i and express ξ_i in terms of a power of ν and an integer x_i as follows,

1. $x_0(3i) = x_0(3i)$, $\xi_1(3i) = x_1(3i)\nu$, $\xi_2(3i) = x_2(3i)\nu^2$, $\xi_0(3i+1) = x_0(3i)\nu^2$, $\xi_1(3i+1) = x_1(3i+1)$, $\xi_2(3i) = x_2(3i)\nu$, $\xi_0(3i+2) = x_0(3i)\nu$, $\xi_1(3i+2) = x_1(3i+2)\nu^2$, $\xi_2(3i) = x_2(3i)$. Moreover C_1 is replaced by $C_1\nu^2$.

The addition formulas become, for instance,

2. $x_0(3i) = x_0(1)x_2(3i-1) + x_2(1)x_0(3i-1)n + x_1(1)x_1(3i-1) \\ - C_1x_0(1)x_0(3i-1)n, \\ x_1(3i) = x_1(1)x_2(3i-1) + x_2(1)x_1(3i-1) + C_0x_0(1)x_0(3i-1), \\ x_2(3i) = x_2(1)x_2(3i-1)n + C_0(x_0(1)x_1(3i-1) + x_1(1)x_0(3i-1)n) \\ + C_1x_1(1)x_1(3i-1)n.$
3. $x_0(3i+1) = x_0(1)x_2(3i) + x_2(1)x_0(3i)n + x_1(1)x_1(3i)n \\ - C_1x_0(1)x_0(3i)n, \\ x_1(3i+1) = x_1(1)x_2(3i) + x_2(1)x_1(3i)n + C_0x_0(1)x_0(3i), \\ x_2(3i+1) = x_2(1)x_2(3i) + C_0(x_0(1)x_1(3i) + x_1(1)x_0(3i)) \\ + C_1x_1(1)x_1(3i)n.$
4. $x_0(3i+2) = x_0(1)x_2(3i+1) + x_2(1)x_0(3i+1) + x_1(1)x_1(3i+1) \\ - C_1x_0(1)x_0(3i+1), \\ x_1(3i+2) = (x_1(1)x_2(3i+1) + x_2(1)x_1(3i+1)n) + C_0x_0(1)x_0(3i+1), \\ x_2(3i+2) = x_2(1)x_2(3i+1)n + C_0(x_0(1)x_1(3i+1) + x_1(1)x_0(3i+1)) \\ + C_1x_1(1)x_1(3i+1)n.$

Theorem.

(on the period special case for type 1 and 2 and $p \equiv 1 \pmod{6}$)

The period for type 0, 1 and 2 is respectively $p^2 + p + 1$, $p^2 - 1$, $p^2 - p$.

Notation.

The period in k -dimension, which depends on the type is denoted by π_k .

Theorem.

(on the selector)

Example.

For $k = 3$, (See \130 RIC.BAS)

0. $p = 5$,

type	period	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	31	1, 3	0, 3, 1
1	24	1, 0	0, 4, 3
2	20	1, 2	0, 2, 1

1. $p = 7, \nu = 2$,

type	period	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	57	1, 0	0, 5, 6
1	48	1, 1	0, 5, 4
2	42	3, 3	0, 3, 0

2. $p = 11$,

type	period	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	133	1, 3	0, 1, 6
1	120	1, 0	0, 2, 5
2	110	1, 5	0, 1, 4

3. $p = 13, \nu = 2$,

type	period	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	183	1, 0	0, 7, 3
1	168	1, 1	1, 1, 10
2	156	4, 1	0, 7, 0

4. $p = 17$,

type	period	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	307	1, 4	0, 1, 2
1	288	1, 0	0, 2, 3
2	272	1, 12	0, 2, 10

5. $p = 19, \nu = 2$,

type	period	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	381	1, 0	0, 3, 7
1	360	1, 1	0, 5, 6
2	342	4, 2	0, 2, 11

6. $p = 23$,

<i>type</i>	<i>period</i>	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	553	1, 3	0, 1, 16
1	528	1, 0	0, 2, 9
2	506	1, 1	0, 1, 1

7. $p = 29$,

<i>type</i>	<i>period</i>	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	871	1, 1	0, 1, 1
1	840	1, 0	0, 2, 13
2	812	1, 10	0, 3, 7

8. $p = 31, \nu = 3$,

<i>type</i>	<i>period</i>	C_0, C_1	$x_0(1), x_1(1), x_2(1)$
0	993	2, 0	0, 3, 24
1	960	1, 2	0, 4, 5
2	930	6, 3	0, 3, 29

Example.For $k = 3$, (See [m130] WRONSKI.BAS)

The table also includes the coordinates of a line,

e.g., for $p = 5$, type 0, $3^* = [2, 0, 3]$.0. $p = 5$, type 0, $C_0 = 1, C_1 = 3$,

<i>i</i>	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_0	0	0	4	2	2	3	4	1	2	4	1	1	1	3	4	0
x_1	0	3	1	0	2	2	4	2	4	4	0	0	4	2	2	3
x_2	1	1	3	4	0	4	1	4	0	2	0	3	1	0	2	2
l^*	11	14	28	29	19	20	2	23	24	8	0	10	27	15	4	5
<i>i</i>	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
x_0	4	1	4	0	2	0	3	1	0	2	2	4	2	4	4	
x_1	4	1	2	4	1	1	1	3	4	0	4	1	4	0	2	
x_2	4	2	4	4	0	0	4	2	2	3	4	1	2	4	1	
l^*	6	18	30	94	1	21	13	12	22	3	16	17	7	25	26	

selector: $\{0, 1, 15, 19, 21, 24\}$ *selector function*:

−1	0	19	21	15	19	15	24	24	15	21	21	19	19	1	0
15	15	1	0	1	0	24	1	0	21	24	19	24	21	1	

1. $p = 5$, type 1, $C_0 = 1, C_1 = 0$,

<i>i</i>	0	1	2	3	4	5	6	7	8	9	10	11
x_0	0	0	1	4	4	4	2	4	1	3	4	1
x_1	0	4	4	3	3	0	2	1	0	0	1	4
x_2	1	3	4	1	4	3	0	3	0	4	4	3
<i>i</i>	12	13	14	15	16	17	18	19	20	21	22	23
x_0	4	3	0	3	0	4	4	3	3	0	2	1
x_1	4	4	2	4	1	3	4	1	4	3	0	3
x_2	3	0	2	1	0	0	1	4	4	4	2	4

selector: $\{0, 1, 14, 16, 21, --\}$

selector function:

−1	0	14	21	21	16	−1	14	16	16	14	14
−1	1	0	1	0	21	−1	21	1	0	16	1

2. $p = 5$, type 2, $C_0 = 1$, $C_1 = 2$,

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x_0	0	0	4	2	1	2	3	0	2	4	2	3	3	1	1	1	4	3	0	4
x_1	0	2	4	2	3	3	1	1	1	4	3	0	4	0	0	4	2	1	2	3
x_2	1	1	4	3	0	4	0	0	4	2	1	2	3	0	2	4	2	3	3	1

selector: $\{0, 1, 7, 18, --, --\}$

selector function:

−1	0	18	18	−1	−1	1	0	−1	18	−1	7	−1	7	7	−1	−1	1	0	1
----	---	----	----	----	----	---	---	----	----	----	---	----	---	---	----	----	---	---	---

3. $p = 7$, type 0, $n = 5$, $C_0 = 1$, $C_1 = 0$,

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
x_0	0	0	4	3	5	2	1	0	2	3	1	4	3	3	1	4	6	4	3	0
x_1	0	5	6	5	0	5	3	6	4	4	1	6	1	5	6	3	2	6	2	2
x_2	1	6	5	5	3	3	0	5	3	0	1	0	2	6	6	2	4	3	1	0
i	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
x_0	3	5	1	0	3	2	5	1	5	2	5	3	3	5	2	4	5	6	4	1
x_1	4	3	3	2	6	0	1	6	0	3	0	4	4	5	4	5	6	2	0	0
x_2	0	5	6	3	6	2	0	6	6	2	5	6	6	3	1	5	5	6	0	2
i	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56			
x_0	2	6	4	4	0	2	4	0	6	0	1	1	1	1	3	4	4			
x_1	3	4	6	5	6	0	5	4	4	3	4	5	6	3	3	3	4			
x_2	3	2	0	6	4	1	2	3	6	3	6	2	3	4	5	3	5			

selector: $\{0, 1, 7, 19, 23, 44, 47, 49\}$

selector function:

−1	0	47	44	19	44	1	0	49	49	47	47	7	44	44	49	7	47	1	0
44	23	1	0	23	19	23	49	19	47	19	49	44	47	23	23	44	7	19	19
7	23	7	1	0	19	1	0	1	0	7	7	49	23	47	49	1			

4. $p = 7$, type 1, $n = 2$, $C_0 = 1$, $C_1 = 1$,

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15				
x_0	0	0	4	5	4	4	1	3	1	6	6	0	3	1	0	6				
x_1	0	5	3	2	6	5	3	2	1	0	5	2	4	2	4	2				
x_2	1	4	5	5	2	5	4	2	2	1	6	2	1	3	0	5				
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
x_0	5	1	3	6	5	1	4	0	6	1	2	1	2	1	3	3				
x_1	6	6	1	6	2	1	1	4	3	1	4	5	0	6	0	4				
x_2	0	1	1	1	0	0	1	3	1	1	2	6	2	5	5	0				
i	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47				
x_0	4	3	1	4	4	2	5	4	2	6	0	3	0	2	2	2				
x_1	4	4	0	0	4	5	4	4	1	3	1	6	6	0	3	1				
x_2	6	2	0	5	3	2	6	5	3	2	1	0	5	2	4	2				

selector: $\{0, 1, 11, 14, 23, 42, 44, --\}$

selector function:

−1	0	42	11	44	44	42	42	−1	14	1	0	11	1	0	44
−1	42	44	23	42	23	1	0	−1	23	23	44	14	42	14	11
−1	11	14	14	23	11	11	23	−1	1	0	1	0	14	44	1

5. $p = 7$, type 2, $n = 5$, $C_0 = 3$, $C_1 = 3$,

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
x_0	0	0	2	0	6	5	5	2	5	6	6	0	6	1	5	3
x_1	0	3	0	6	4	4	2	4	2	6	0	2	1	4	1	0
x_2	1	0	2	6	4	3	6	2	2	0	2	5	6	1	0	4
i	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
x_0	0	1	4	3	0	2	4	4	6	1	1	3	2	5	1	6
x_1	5	6	3	0	3	4	6	2	1	5	1	2	4	5	6	6
x_2	6	1	0	3	6	2	2	5	4	1	3	6	5	2	2	6
i	32	33	34	35	36	37	38	39	40	41						
x_0	4	4	6	4	1	6	5	4	2	3						
x_1	6	6	6	5	6	4	6	2	1	0						
x_2	2	2	5	2	6	6	3	5	0	0						

selector: $\{0, 1, 3, 11, 16, 20, --, --\}$

selector function:

−1	0	1	0	16	11	−1	−1	3	11	1	0	−1	3	−1	1
0	3	−1	1	−1	20	20	−1	20	16	16	−1	16	−1	11	11
20	11	−1	−1	16	20	3	3	1							

Definition.

0. The direction $dir(i, j)$ of 2 points i and j on the “sphere“ is the direction of the line associated to the 2 points.
1. A triangle (i, j, k) is isosceles iff $j - i = k - j$.
2. The planar direction $pl(i, j)$ of 2 points i and j on the “sphere“ is when $C_0 = 1$ and $C_1 = 0$ that of the normal to the plane passing through the origin, i and j .
3. The t plane $t^*(i)$ at the point i is the plane through the origin parallel to the tangent plane at i .

Theorem.

17

0. $dir(i, j) = dir(i + k, j + k) - k$.
1. if $c_0 = 1$ and $c_1 = 0$ then $pl(i, j) = pl(i + k, j + k) + pk$.
2. if $c_0 = 1$ and $c_1 = 0$ then $n(i) = -pi$,
- 3.0 For types 0 and 1, the correspondance $i, n(i)$ is a bijection.
 1. For type 2, there are $2p - 3$ values of n which are undefined because the length of the normal is 0 (ideal point).
4. For types 0 and 1, $t^*(i) + i = t^*(j) + j$.

Corollary.

If a triangle (i, j, k) is isosceles, then

$$\text{dir}(j, k) = \text{dir}(i, j) + k - i$$

Example.

$p = 5$, type 0, $\text{dir}(0, 1) = 21$, $\text{dir}(1, 2) = 22$, $\text{dir}(0, 2) = 5$, $\text{dir}(0, 3) = 25$, $\text{dir}(0, 4) = 17$.
 $t^*(0) = 3^*$, $t^*(1) = 2^*$.

In the triangle $\{0, 2, 4\}$, $\text{dir}(2, 4) = 5$, $\text{dir}(4, 0) = 17$, $\text{dir}(2, 4) = 7 = 5 + 2$.

$p = 5$, type 1, $\text{pl}(0, 1) = 8$, $\text{pl}(1, 2) = 3$, $\text{pl}(2, 3) = 22$, $\text{pl}(0, 2) = 6$, $\text{pl}(1, 2) = 1$.

$t^*(0) = 8^*$, $t^*(1) = 7^*$.

$p = 11$, type 1, $\text{pl}(0, 1) = 40$, $\text{pl}(1, 2) = 29$, $\text{pl}(2, 3) = 18$.

8.5.3 Dimension 4.**Theorem.**

For $k = 4$, let

$$0.0. \quad D^4x_0 = C_0x_0 + C_1Dx_0 + C_2D^2x_0,$$

with

$$0.1. \quad Dx_0(0) = 0, \quad Dx_0 = x_1(0) = 0, \quad D^2x_0(0) = x_2(0) = 0, \quad D^3x_0(0) = x_3(0) = 1,$$

then

1.0. the functions $x_3 - C_2x_1 - C_1x_0$, $x_2 - C_2x_0$, x_1 and x_0 are independent

1. their Wronskian is

$$W = \begin{vmatrix} x_3 - C_2x_1 - C_1x_0 & x_2 - C_2x_0 & x_1 & x_0 \\ C_0x_0 & x_3 - C_2x_1 & x_2 & x_1 \\ C_0x_1 & C_0x_0 + C_1x_1 & x_3 & x_2 \\ C_0x_2 & C_0x_1 + C_1x_2 & C_0x_0 + C_1x_1 + C_2x_2 & x_3 \end{vmatrix}$$

2. $W(0) = E$.

2. The addition formulas are

$$\begin{aligned} x_0'' &= y_{0,3} + y_{1,2} - C_1y_{0,0} - C_2y_{0,1} \\ x_1'' &= y_{1,3} + y_{2,2} - C_0y_{0,0} - C_2y_{1,1} \\ x_2'' &= y_{2,3} + C_0y_{0,1} + C_1y_{1,1} \\ x_3'' &= y_{3,3} + C_0(y_{0,2} + y_{1,1}) + C_1y_{1,2} + C_2y_{2,2} \end{aligned}$$

Example.

Chapter 9

FINITE ELLIPTIC FUNCTIONS

9.0 Introduction.

The success of the study of the harmonic polygons of Casey (II.6.1), suggested the study of the polygons of Poncelet. After having conjectured that the Theorem of Poncelet, as given in I.2.2. generalized to the finite case, and because one of the proof of this Theorem, in the classical case, is by means of elliptic functions, this suggested that these too could be generalized to the finite case. Just as the additions properties were used to define the trigonometric functions, the same properties were generalized to the finite case. It was soon realized that the poles of the elliptic functions correspond to values, which in the finite case are outside of the finite field. The basic definitions and properties of section 1 do not give directly functions but an abelian group structure on a set E , whose elements are, in general, triplets of integers modulo p . In section 2, this structure will be described as the direct product of the Klein 4-group and an abelian group which can be used as seen in section 3 to define 3 functions which generalize, in the finite case, the functions sn , cn and dn of Jacobi.

In this Chapter, j and j' will denote $+1$ or -1 .

9.1 The Jacobi functions.

9.1.1 Definitions and basic properties of the Jacobian elliptic group.

Introduction.

Given p and m different from 0 and 1, we will define in 3.1.1, the set $E = E(p, m)$ and, in 3.1.7., an operation “ $+$ ” from $E \times E$ into E . The basic result that $(E, +)$ is an abelian group is given in 3.1.15.

Definition.

Given $s, c, d \in Z_p$. The elements of E are

$$(s, c, d)$$

such that

$$D0. \quad s^2 + c^2 = 1 \text{ and } d^2 + m s^2 = 1.$$

as well as, when -1 and $-m$ are quadratic residues,

$$(\infty, c \infty, d \infty), \text{ where } c^2 = -1 \text{ and } d^2 = -m.$$

Notation.

$$i := \sqrt{-1}, m_1 := 1 - m, k := \sqrt{m}, k_1 := \sqrt{m_1}.$$

Theorem.

$$H0. \quad (s, c, d), (s_1, c_1, d_1), (s_2, c_2, d_2) \in E,$$

$$H1. \quad j = +1 \text{ or } -1,$$

then

$$C0. \quad d^2 - m c^2 = m_1.$$

$$C1. \quad c^2 + m_1 s^2 = d^2.$$

$$C2. \quad c^2 + s^2 d^2 = d^2 + m s^2 c^2 = 1 - m s^4.$$

$$C3. \quad m(1 - c)(1 + c) = (1 - d)(1 + d).$$

$$C4. \quad (c + d)(1 + j d) = (1 + j c)(j m_1 + d + m c).$$

$$C5. \quad m(c + d)(1 - j c) = (1 - j d)(j m_1 + d + m c)$$

$$C6. \quad d^2 - m s^2 c^2 = d^2 + c^2(d^2 - 1).$$

$$C7. \quad d_1^2 d_2^2 + m m_1 s_1^2 s_2^2 = m_1 - m c_1^2 c_2^2.$$

$$C8. \quad (d_1 s_1 c_2 + d_2 s_2 c_1)(d_1 d_2 - m s_1 s_2 c_1 c_2) = (s_1 c_2 d_2 + s_2 c_1 d_1)(d_1^2 d_2^2 + m m_1 s_1^2 s_2^2).$$

Proof: Each of the identities can easily be verified using Definition 1.1. If C3, is written

$$C3' \quad m(1 - j c)(1 + j c) = (1 - j d)(1 + j d),$$

then C5, follows from C4.

Lemma.

$$H0. \quad m s_0^2 s_1^2 = 1,$$

then

$$C0. \quad d_0^2 = -m s_0^2 c_1^2, d_1^2 = -m s_1^2 c_0^2,$$

$$C1. \quad (s_0 c_1 d_1)^2 = (s_1 c_0 d_0)^2,$$

$$C2. \quad (c_0 c_1)^2 = (d_0 s_0 d_1 s_1)^2,$$

$$C3. \quad (d_0 d_1)^2 = (m s_0 c_0 s_1 c_1)^2,$$

$$C4. \quad s_0 s_1 \neq 0.$$

Lemma.

$$H0. \quad m s_0^2 s_1^2 = 1,$$

$$H1. \quad s_0 c_1 d_1 = -j s_1 c_0 d_0,$$

then

$$C0. \quad c_0 c_1 = j d_0 s_0 d_1 s_1,$$

$$C1. \quad d_0 d_1 = j m s_0 c_0 s_1 c_1.$$

$$C2. \quad c_0 = 0 \Rightarrow d_1 = 0 \text{ and } c_1 \neq 0.$$

$$c_1 = 0 \Rightarrow d_0 = 0 \text{ and } c_0 \neq 0.$$

Proof: If $c_0 = c_1 = 0$ then $s_0^2 = s_1^2 = 1$ hence $m = 1$, which is excluded.

Lemma.

$$H0. \quad (s_0 c_1 d_1)^2 = (s_1 c_0 d_0)^2,$$

then

$$C0. \quad s_0 = j s_1 \text{ or } m s_0^2 s_1^2 = 1.$$

Definition.

The addition is defined as follows:

Let $D = 1 - m s_0^2 s_1^2$.

If $D \neq 0$, then

$$D0. \quad (s_0, c_0, d_0) + (s_1, c_1, d_1) = \left(\frac{s_0 c_1 d_1 + s_1 c_0 d_0}{D}, \frac{c_0 c_1 - d_0 s_0 d_1 s_1}{D}, \frac{d_0 d_1 - m s_0 c_0 s_1 c_1}{D} \right),$$

If $D = 0$, $s_0 c_1 d_1 = s_1 c_0 d_0$, $c_0 \neq 0$ and $c_1 \neq 0$, then

$$D1. \quad (s_0, c_0, d_0) + (s_1, c_1, d_1) = (\infty, c \infty, d \infty),$$

where $c = \frac{c_1}{s_1 d_0}$ and $d = \frac{d_1}{s_1 c_0}$,

If $D = 0$, $s_0 c_1 d_1 = -s_1 c_0 d_0$, $c_0 \neq 0$ and $c_1 \neq 0$, then

$$D2.0. \quad (s_0, c_0, d_0) + (s_1, c_1, d_1) = \left(\frac{s_0^2 - s_1^2}{2 s_0 c_1 d_1}, \frac{c_0^2 + c_1^2}{2 c_0 c_1}, \frac{d_0^2 + d_1^2}{2 d_0 d_1} \right),$$

If $D = 0$, $s_0 c_1 d_1 = j s_1 c_0 d_0$, $c_0 = 0$ and $c_1 \neq 0$, then

$$D2.1. \quad (s_0, c_0, d_0) + (s_1, c_1, d_1) = (\infty, c \infty, d \infty),$$

where $c = \frac{-d_0 s_1}{c_1}$ and $d = \frac{d_0^3}{m s_0 c_1^3}$.

If $D = 0$, $s_0 c_1 d_1 = j s_1 c_0 d_0$, $c_0 \neq 0$ and $c_1 = 0$, then

$$D2.2. \quad (s_0, c_0, d_0) + (s_1, c_1, d_1) = (\infty, c \infty, d \infty),$$

where $c = \frac{-d_1 s_0}{c_0}$ and $d = \frac{d_1^3}{m s_1 c_0^3}$.

If $s_0 \neq 0$, then

$$D3.0. \quad (\infty, c \infty, d \infty) + (s_0, c_0, d_0) \\ = (s_0, c_0, d_0) + (\infty, c \infty, d \infty) = \left(\frac{-cd}{m s_0}, \frac{dd_0}{m s_0}, \frac{cc_0}{m s_0} \right).$$

If $s_0 = 0$, then

$$D3.1. \quad (\infty, c \infty, d \infty) + (0, c_0, d_0) \\ = (0, c_0, d_0) + (\infty, c \infty, d \infty) = (\infty, c d_0 \infty, d c_0 \infty).$$

$$D4. \quad (\infty, c_0 \infty, d_0 \infty) + (\infty, c_1 \infty, d_1 \infty) = \left(0, \frac{d_0 d_1}{m}, c_0 c_1 \right).$$

Example.

With $p = 11$, $m = 3$, $(-\frac{1}{11}) = (-\frac{3}{11}) = -1$,

$$E = \{(0, 1, 1), (0, 1, -1), (0, -1, 1), (0, -1, -1), \\ (1, 0, 3), (1, 0, -3), (-1, 0, 3), (-1, 0, -3), \\ (5, 3, 5), (5, 3, -5), (5, -3, 5), (5, -3, -5), \\ (-5, 3, 5), (-5, 3, -5), (-5, -3, 5), (-5, -3, -5)\}.$$

If the elements of E in the above order are abbreviated $0, 1, 2, \dots, 15$, then the addition table is

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	7	6	5	4	13	12	15	14	9	8	11	10
2	2	3	0	1	6	7	4	5	14	15	12	13	10	11	8	9
3	3	2	1	0	5	4	7	6	11	10	9	8	15	14	13	12
4	4	7	6	5	2	1	0	3	10	13	14	9	8	15	12	11
5	5	6	7	4	1	2	3	0	9	14	13	10	11	12	15	8
6	6	5	4	7	0	3	2	1	12	11	8	15	14	9	10	13
7	7	4	5	6	3	0	1	2	15	8	11	12	13	10	9	14
8	8	13	14	11	10	9	12	15	4	1	2	5	0	7	6	3
9	9	12	15	10	13	14	11	8	1	6	7	2	5	0	3	4
10	10	15	12	9	14	13	8	11	2	7	6	1	4	3	0	5
11	11	14	13	8	9	10	15	12	5	2	1	4	3	6	7	0
12	12	9	10	15	8	11	14	13	0	5	4	3	6	1	2	7
13	13	8	11	14	15	12	9	10	7	0	3	6	1	4	5	2
14	14	11	8	13	12	15	10	9	6	3	0	7	2	5	4	1
15	15	10	9	12	11	8	13	14	3	4	5	0	7	2	1	6

Example.

With $p = 13$, $m = 3$, $(-\frac{1}{13}) = (-\frac{3}{13}) = 1$,

$$E = \{(0, 1, 1), (0, 1, -1), (0, -1, 1), (0, -1, -1),$$

$$(\infty, 5\infty, 6\infty), (\infty, 5\infty, -6\infty), (\infty, -5\infty, 6\infty), (\infty, -5\infty, -6\infty),$$

$$(6, 2, 6), (6, 2, -6), (6, -2, 6), (6, -2, -6),$$

$$(-6, 2, 6), (-6, 2, -6), (-6, -2, 6), (-6, -2, -6)\}.$$

If the elements of E in the above order are abbreviated $0, 1, 2, \dots, 15$, then the addition table is

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	6	7	4	5	13	12	15	14	9	8	11	10
2	2	3	0	1	5	4	7	6	14	15	12	13	10	11	8	9
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	6	5	7	3	1	2	0	12	14	13	15	11	9	10	8
5	5	7	4	6	1	3	0	2	10	8	11	9	13	15	12	14
6	6	4	7	5	2	0	3	1	9	11	8	10	14	12	15	13
7	7	5	6	4	0	2	1	3	15	13	14	12	8	10	9	11
8	8	13	14	11	12	10	9	15	7	1	2	4	0	5	6	3
9	9	12	15	10	14	8	11	13	1	4	7	2	6	0	3	5
10	10	15	12	9	13	11	8	14	2	7	4	1	5	3	0	6
11	11	14	13	8	15	9	10	12	4	2	1	7	3	6	5	0
12	12	9	10	15	11	13	14	8	0	6	5	3	4	1	2	7
13	13	8	11	14	9	15	12	10	5	0	3	6	1	7	4	2
14	14	11	8	13	10	12	15	9	6	3	0	5	2	4	7	1
15	15	10	9	12	8	14	13	11	3	5	6	0	7	2	1	4

Theorem.

- C0. $(s_0, c_0, d_0) + (j's_0, jc_0, j'j'd_0) = (0, j, j'j').$
C1. $(\infty, c\infty, d\infty) + (\infty, jc\infty, j'd\infty) = (0, -j', -j).$
C2. $-(s_0, c_0, d_0) = (-s_0, c_0, d_0).$

- C3. $-(\infty, c \infty, d \infty) = (\infty, -c \infty, -d \infty).$
 C4. $(s_0, c_0, d_0) + (0, j, j') = (js_0, j'c_0, j j'd_0).$
 C5. $(\infty, c \infty, d \infty) + (0, j', j) = (\infty, jc \infty, j'd \infty).$

Theorem.

- H0. $(s_0, c_0, d_0) + (s_1, c_1, d_1) = (s_2, c_2, d_2),$
 then
 C0. $(s_0, c_0, d_0) + (-s_1, -c_1, d_1) = (-s_2, -c_2, d_2).$
 C1. $(s_0, c_0, d_0) + (s_1, -c_1, -d_1) = (s_2, -c_2, -d_2).$
 C2. $(s_0, c_0, d_0) + (-s_1, c_1, -d_1) = (-s_2, c_2, -d_2).$

Notation.

We will use the notation, which is customary in abelian groups with addition as operation symbol,
 $n(s_0, c_0, d_0) = (n-1)(s_0, c_0, d_0) + (s_0, c_0, d_0), n \in \mathbb{Z}$
 using induction starting with $n = 0$ or $n = -1$.

Theorem.

- C0. $n(-s_0, -c_0, -d_0) = j n(s_0, c_0, d_0),$ with $j = (-1)^n$.

Theorem.

- D0. $D_2 := 1 - m s^4,$
 then
 C0. $2(s, c, d) = (\frac{2scd}{D_2}, \frac{c^2 - s^2 d^2}{D_2}, \frac{d^2 - m s^2 c^2}{D_2}).$

Theorem.

$(E, +)$ is an abelian group. Its order is divisible by 4.

The proof, although tedious, is straightforward. The closure follows from the definition .6. Associativity follows, non trivially from .6. The neutral element is $(0, 1, 1)$. The additive inverse element of (s, c, d) is given by 1.10. C2. and C3.

Definition.

The group $(E, +)$ is called the *Jacobian elliptic group* associated to the prime p and the integer $m \in \mathbb{Z}_p$.

Corollary.

The following constitute special cases.

0. For $m = 0$, the elements of the group are
 $(\text{sink}, \text{cosk}, 1)$ and $(\text{sink}, \text{cosk}, -1),$
 and the addition formulas reduce to
 $(\text{sink}, \text{cosk}, j_1) + (\text{sinl}, \text{cosl}, j_2) =$
 $(\text{sin}(j_1 k + j_2 l), \text{cos}(j_2 k + j_2 l), j_1 j_2),$ j_1 and j_2 are $+1$ or -1 .

1. For $m = 1$, the elements of the group are
 $(\tanh k, \operatorname{cosech} k, \operatorname{cosech} k), (\tanh k, \operatorname{cosech} k, -\operatorname{cosech} k)$
and if $c^2 = -1$,
 $(\infty, c \infty, c \infty), (\infty, -c \infty, c \infty), (\infty, c \infty, -c \infty), (\infty, -c \infty, -c \infty)$.
and the addition formulas correspond to
 $\tanh k_0 + \tanh k_1 = \frac{\tanh k_0 + \tanh k_1}{1 + \tanh k_0 \tanh k_1}$.
 $\operatorname{cosech}(k_0 + k_1) = \frac{\operatorname{cosech} k_0 \operatorname{cosech} k_1}{1 + \tanh k_0 \tanh k_1}$.

Comment.

To remove some of the mystery associated with some of the formulas just given, assume that the finite field is replaced by the field of reals. For instance, D4, is obtained by replacing in D0, c by $i s$, d by $i k s$, c_1 by $i s_1$, d_1 by $i k s_1$ and letting s and s_1 tend to infinity.

9.1.2 Finite Jacobian elliptic groups for small p .

Introduction.

It can be shown that $(E, +)$ is isomorphic to the direct product of the Klein 4-group and the group E associated to the finite Weierstrass p function introduced by Professor Tate and that the kernel of a homomorphism between the 2 groups is the subgroup of $(E, +)$ of elements with $s = 0$. A less precise form of this Theorem is given in 2.1. and is illustrated by the examples given in this section and prepares for the definition of finite Jacobi elliptic functions. In many cases the generator of the larger group allows the inclusion of one of the generators of the Klein 4-group.

Theorem.

$(E, +)$ is isomorphic to $Z_2 \rtimes Z_{2n}$ or to $Z_4 \rtimes Z_{4n}$.

Example.

In the example the generators of the factor groups will be given. The additional information in the second column will be explained in the Chapter on isomorphisms and homomorphisms.

p	m	E is isomorphic to $Z_i \rtimes Z_n$	generator of Z_i and Z_n
3	2	$Z_2 \rtimes Z_2$	$(0, 1, -1), (0, -1, 1)$
5	3	$Z_2 \rtimes Z_2$	$(0, 1, -1), (0, -1, 1)$
	$2 = m'(2)Z_2 \rtimes Z_4$	$(0, 1, -1), (1, 0, 2)$	
	$4 = m_j(2)$	"	$(0, 1, -1), (\infty, 2\infty, \infty)$
7	3	$Z_2 \rtimes Z_2$	$(0, 1, -1), (0, -1, 1)$
	2	$Z_2 \rtimes Z_4$	$(0, -1, 1), (2, 2, 0)$
	$4 = m''(2)$	"	$(0, 1, -1), (1, 0, 2)$
	$6 = m'(4)$	"	$(0, 1, -1), (1, 0, 3)$
	5	$Z_2 \rtimes Z_6$	$(0, 1, -1), (2, -2, 3)$
11	5	$Z_2 \rtimes Z_4$	$(0, -1, 1), (3, 5, 0)$
	$8 = m'(9)$	"	$(0, 1, -1), (1, 0, 2)$
	$9 = m''(5)$	"	$(0, 1, -1), (1, 0, 5)$
	2	$Z_2 \rtimes Z_6$	$(0, 1, -1), (3, 5, 4)$
	6	"	$(0, 1, -1), (5, 3, 4)$
	10	"	$(0, -1, 1), (5, 3, -2)$
	3	$Z_2 \rtimes Z_8$	$(0, 1, -1), (5, 3, 5)$
	$4 = m''(3)$	"	$(0, -1, 1), (3, 5, 3)$
	$7 = m'(3)$	"	$(0, 1, -1), (3, 5, 2)$
13	$2 = m'(2)$	$Z_2 \rtimes Z_4$	$(0, 1, -1), (1, 0, 5)$
	$12 = m_j(2) = m''(12)$	"	$(0, 1, -1), (\infty, 5\infty, \infty)$
	$4 = m'(10) = m''(10)$	$Z_4 \rtimes Z_4$	$(\infty, 5\infty, 3\infty), (1, 0, 6)$
	$10 = m_j(4)$	"	$(\infty, 5\infty, 4\infty), (1, 0, 2)$
	6	$Z_2 \rtimes Z_6$	$(0, 1, -1), (2, 6, 4)$
	$8 = m_j(6)$	"	$(0, -1, 1), (6, 2, 5)$
	$3 = m_j(11)$	$Z_2 \rtimes Z_8$	$(0, 1, -1), (6, 2, 6)$
	$5 = m_j(9)$	"	$(0, 1, -1), (6, 2, 4)$
	$9 = m''(3)$	"	$(0, 1, -1), (2, 6, 2)$
	$11 = m'(5)$	"	$(0, 1, -1), (2, 6, 3)$
	$7 = m_j(7)$	$Z_2 \rtimes Z_{10}$	$(0, -1, 1), (2, 6, -5)$
17	$2 = m'(2)$	$Z_4 \rtimes Z_4$	$(\infty, 4\infty, 7\infty), (1, 0, 4)$
	$9 = m''(2) = m_j(9)$	"	$(\infty, 4\infty, 5\infty), (1, 0, 3)$
	$16 = m_j(2) = m''(16)$	"	$(\infty, 4\infty, 1\infty), (1, 0, 6)$
	6	$Z_2 \rtimes Z_6$	$(0, 1, -1), (3, 3, 7)$
	$12 = m_j(6)$	"	$(0, 1, -1), (4, 6, 8)$
	4	$Z_2 \rtimes Z_8$	$(0, 1, -1), (3, 3, 4)$
	$5 = m_j(13)$	"	$(0, 1, -1), (6, 4, 5)$
	$13 = m''(4) = m_j(5)$	"	$(0, 1, -1), (6, 4, 3)$
	$14 = m_j(4) = m'(5)$	"	$(0, 1, -1), (4, 6, 7)$
	7	$Z_2 \rtimes Z_{10}$	$(0, 1, -1), (4, -6, 5)$
	$11 = m_j(7)$	"	$(0, 1, -1), (3, 3, -2)$
	3	$Z_2 \rtimes Z_{12}$	$(0, 1, -1), (4, 6, 2)$
	8	"	$(0, 1, -1), (4, 6, 3)$
	$10 = m'(3) = m_j(8)$	"	$(0, 1, -1), (3, 3, 8)$
	$15 = m_j(3) = m''(8)$	"	$(0, 1, -1), (3, 3, 6)$

p	m	E is isomorphic to $Z_i \rtimes Z_n$	generator of Z_i and Z_n
19	12	$Z_2 \rtimes Z_6$	$(0, 1, -1), (3, 7, -8)$
	3	$Z_2 \rtimes Z_8$	$(0, 1, -1), (7, 3, 5)$
	$11 = m'(3)$	"	$(0, 1, -1), (3, 7, 4)$
	$7 = m''(11)$	"	$(0, -1, 1), (2, 4, 7)$
	4	"	$(0, 1, -1), (2, 4, 2)$
	$5 = m''(4)$	"	$(0, -1, 1), (4, 2, 4)$
	$14 = m'(4)$	"	$(0, 1, -1), (4, 2, 9)$
	2	$Z_2 \rtimes Z_{10}$	$(0, 1, -1), (4, -2, 8)$
	10	"	$(0, 1, -1), (3, -7, 5)$
	18	"	$(0, 1, -1), (2, 4, 9)$
	6	$Z_2 \rtimes Z_{12}$	$(0, -1, 1), (7, 3, 7)$
	$15 = m'(16)$	"	$(0, 1, -1), (2, 4, 6)$
	$16 = m''(6)$	"	$(0, 1, -1), (3, 7, 3)$
	9	"	$(0, 1, -1), (4, 2, 3)$
	$13 = m'(9)$	"	$(0, 1, -1), (3, 7, 6)$
	$17 = m''(9)$	"	$(0, -1, 1), (7, 3, 2)$
	8	$Z_2 \rtimes Z_{14}$	$(0, 1, -1), (2, 4, 8)$
23	4	$Z_2 \rtimes Z_8$	$(0, -1, 1), (4, 10, 11)$
	$6 = m''(4)$	"	$(0, 1, -1), (8, 11, 10)$
	$15 = m'(6)$	"	$(0, 1, -1), (11, 8, 7)$
	5	$Z_2 \rtimes Z_{10}$	$(0, 1, -1), (4, 10, 6)$
	10	"	$(0, 1, -1), (4, -10, 5)$
	17	"	$(0, 1, -1), (9, -9, 2)$
	2	$Z_2 \rtimes Z_{12}$	$(0, -1, 1), (11, 8, 9)$
	$12 = m''(2)$	"	$(0, 1, -1), (9, 9, 8)$
	$22 = m'(12)$	"	$(0, 1, -1), (10, 4, 3)$
	3	"	$(0, -1, 1), (8, 11, 4)$
	$8 = m''(3)$	"	$(0, 1, -1), (10, 4, 11)$
	$11 = m'(8)$	"	$(0, 1, -1), (11, 8, 2)$
	13	"	$(0, -1, 1), (9, 9, 11)$
	$16 = m''(13)$	"	$(0, 1, -1), (8, 11, 9)$
	$21 = m'(16)$	"	$(0, 1, -1), (9, 9, 5)$
	7	$Z_2 \rtimes Z_{14}$	$(0, 1, -1), (4, 10, 2)$
	14	"	$(0, 1, -1), (8, -11, 5)$
	19	"	$(0, 1, -1), (8, -11, 2)$
	9	$Z_2 \rtimes Z_{16}$	$(0, -1, 1), (4, 10, 8)$
	$18 = m''(9)$	"	$(0, 1, -1), (10, 4, 8)$
	$20 = m'(18)$	"	$(0, 1, -1), (4, 10, 7)$

9.1.3 Finite Jacobian Elliptic Function.

Definition.

Given a prime p and an integer m in Z_p , 3.2.1. defines an cyclic group of order $2n$ and $4n$. If we choose a generator $g := (s_1, c_1, d_1)$ of this group, we obtain by successive addition $ng = n(s_1, c_1, d_1) = (s_n, c_n, d_n)$. The *finite Jacobi elliptic functions* sn , cn and dn , scd are defined by

$$sn(n) := s_n, cn(n) := c_n, dn(n) := d_n, scd(n) := (s_n, c_n, d_n).$$

The *period* is denoted by $4K$.

Example.

For $p = 11, m = 3, K = 2$, — For $p = 13, m = 3, K = 2$,

i	$sn(i)$	$cn(i)$	$dn(i)$	i	$sn(i)$	$cn(i)$	$dn(i)$
0	0	1	1	0	0	1	1
1	-5	3	-5	1	6	2	6
2	1	0	3	2	∞	-5∞	-6∞
3	-5	-3	-5	3	-6	-2	-6
4	0	-1	1	4	0	-1	-1
5	5	-3	-5	5	6	-2	-6
6	-1	0	3	6	∞	5∞	6∞
7	5	3	-5	7	-6	2	6
8	0	1	1	8	0	1	1

Definition.

0. $ns := \frac{1}{sn}, nc := \frac{1}{cn}, nd := \frac{1}{dn},$
1. $sc := \frac{sn}{cn}, cd := \frac{cn}{dn}, ds := \frac{dn}{sn},$
2. $cs := \frac{cn}{sn}, dc := \frac{dn}{cn}, sd := \frac{sn}{dn}.$

The notation is due to Glaisher, Glaisher, J.W.L., On elliptic functions, Messenger of Mathematics, Vol. 11, 1881, 81-95.

9.1.4 Identities and addition formulas for finite elliptic functions.

Introduction.

The formulas given in this section are for the most part the same as in the real case. Theorem 9.1.4 gives the addition formulas. Theorem 9.1.4, which may be new is needed to prove the addition formula for the Jacobi *Zeta function*. Theorem 9.1.4 is given for sake of completeness. It is clearly less elegant than 9.1.4.

Lemma.

$$1 - ms_0^2 s_1^2 = c_1^2 + d_0^2 s_1^2 = d_0^2 + ms_0^2 c_1^2.$$

Theorem.

0. $sn^2(u)cn^2(v)dn^2(v) - sn^2(v)cn^2(u)dn^2(u)$
 $= (1 - msn^2(u)sn^2v)(sn^2(u) - sn^2(v)).$
1. $cn^2(u)cn^2(v) - sn^2(u)sn^2(v)dn^2(u)dn^2(v)$
 $= (1 - msn^2(u)sn^2v)(1 - sn^2(u) - sn^2(v)).$
2. $dn^2(u)dn^2(v) - m^2sn^2(u)sn^2(v)cn^2(u)cn^2(v)$
 $= (1 - msn^2(u)sn^2v)(1 - msn^2(u) - msn^2(v) + msn^2(u)sn^2(v)).$

Theorem.

0. $sn(u+v) = \frac{sn^2(u) - sn^2(v)}{sn(u)cn(v)dn(v) - sn(v)cn(u)dn(u)}.$
1. $cn(u+v) = \frac{1 - sn^2(u) - sn^2(v)}{cn(u)cn(v) + sn(u)sn(v)dn(u)dn(v)}.$
2. $dn(u+v) = \frac{1 - msn^2(u) - msn^2(v) + msn^2(u)sn^2(v)}{dn(u)dn(v) + msn(u)sn(v)cn(u)cn(v)}.$
3. $cn(u+v) = \frac{sn(u)cn(u)dn(v) - sn(v)cn(v)dn(u)}{sn(u)cn(v)dn(v) - sn(v)cn(u)dn(u)},$ for $u \neq (v).$
4. $dn(u+v) = \frac{sn(u)dn(u)cn(v) - sn(v)dn(v)cn(u)}{sn(u)cn(v)dn(v) - sn(v)cn(u)dn(u)},$ for $u \neq (v).$

Formulas 0., 3. and 4. are due to Cayley (1884).

Theorem.

0. $-mcn(u)cn(v)cn(u+v) + dn(u)dn(v)dn(u+v) = 1 - m.$
1. $dn(v)dn(u+v) + mcn(u)sn(v)sn(u+v) = dn(u).$
2. $sn(v)dn(u)sn(u+v) + cn(v)cn(u+v) = cn(u).$

Theorem.

0. $sn(u+v+w)(sn(v)sn(u+w) - sn(w)sn(u+v))$
 $= sn(u)(sn(v)sn(u+v) - sn(w)sn(u+w)).$
1. $sn(a_0 - a_1)sn(a_1 - a_2)sn(a_2 - a_0)$
 $- sn(a_1 - a_2)sn(a_2 - a_3)sn(a_3 - a_1)$
 $+ sn(a_2 - a_3)sn(a_3 - a_0)sn(a_0 - a_2)$
 $- sn(a_3 - a_0)sn(a_0 - a_1)sn(a_1 - a_3) = 0$ ¹.

Proof: If we write $u = a_0 - a_1$, $v = a_1 - a_2$, $w = a_3 - a_0$, then $u + v = a_0 - a_2$, $u + w = a_3 - a_1$, $u + v + w = a_3 - a_2$ and we obtain 0, from 1. To prove 1, let us introduce the notation

$$s_0 := sna_0, s_1 := sna_1, s_2 := sna_2, s_3 := sna_3.$$

and similarly for c_i and d_i . Let

$$B_0 := (s_1^2 - s_2^2)(s_2^2 - s_3^2)(s_3^2 - s_1^2)$$

$$(s_0c_1d_1 + s_1c_0d_0)(s_0c_2d_2 + s_2c_0d_0)$$

$$(s_0c_3d_3 + s_3c_0d_0).$$

Let B_1, B_2, B_3 be obtained by adding 1, 2, 3 modulo 4 to each digit, using 9.1.4.0 in 1. and reducing to the same denominator, we have to prove that

$$B_0 - B_1 + B_2 - B_3 = 0.$$

Using .0.D0.,

$$B_0 = (s_1^4(s_3^2 - s_2^2) + s_2^4(s_1^2 - s_3^2) + s_3^4(s_2^2 - s_1^2))$$

$$(s_1s_2s_3c_0d_0(1 - s_0^2)(1 - ms_0^2)$$

$$+ s_2s_3s_0c_1d_1(1 - s_0^2)(1 - ms_0^2))$$

¹3.11.83

$$\begin{aligned}
& +s_3s_0s_1c_2d_2(1-s_0^2)(1-ms_0^2) \\
& +s_0s_1s_2c_3d_3(1-s_0^2)(1-ms_0^2) \\
& +s_0^3c_1d_1c_2d_2c_3d_3 \\
& +s_0^2s_1c_2d_2c_3d_3c_0d_0 \\
& +s_0^2s_2c_3d_3c_0d_0c_1d_1 \\
& +s_0^2s_3c_0d_0c_1d_1c_2d_2)
\end{aligned}$$

therefore

$$\begin{aligned}
B_0 - B_1 + B_2 - B_3 = & (s_1s_2s_3c_0d_0(s_0^4s_1^4(s_3^2 - s_2^2)(m - m) + \dots \\
& + s_0^4s_1^2s_2^2(1 + m - 1 - m) + \dots \\
& + s_0^4s_1^2(1 - 1) + \dots) + \dots) \\
& + (s_0c_1d_1c_2d_2c_3d_3(s_0^4s_1^2s_2^2(1 - 1) + \dots \\
& + s_0^2s_1^4s_2^2(-1 + 1) + \dots \\
& + s_1^4s_2^2s_3^2(-1 + 1) + \dots) + \dots) = 0.
\end{aligned}$$

The given terms come from

$$\begin{aligned}
& s_1^4(s_3^2 - s_2^2)s_1s_2s_3c_0d_0ms_0^4 \text{ in } B_0 \text{ and from the term in } B_1 \\
& \text{corresponding to the term } s_3^4(s_2^2 - s_1^2)s_0s_1s_2c_3d_3ms_0^4 \text{ in } B_0,
\end{aligned}$$

the term in B_2 corresponding to $-s_2^4s_3^2s_3s_0s_1c_2d_2(-1-m)s_0^2$ in B_0 and the term in B_1 , to $-s_3^4s_1^2s_0s_1s_2c_3d_3(-1-m)s_0^2$ in B_0 , the term in B_2 corresponding to $-s_2^4s_3^2s_3s_0s_1c_2d_2$ in B_0 and the term in B_3 , to $-s_1^4s_2^2s_2s_3s_0c_1d_1$ in B_0 , the term in B_2 corresponding to $-s_2^4s_3^2s_0^2s_2c_3d_3c_0d_0c_1d_1$ in B_0 and the term in B_1 , to $-s_3^4s_1^2s_0^2s_3c_0d_0c_1d_1c_2d_2$ in B_0 , the term $-s_1^4s_2^2s_0^3c_1d_1c_2d_2c_3d_3$ in B_0 and the term in B_2 , to $s_3^4s_2^2s_0^2s_2c_3d_3c_0d_0c_1d_1$ in B_0 and the term in B_2 corresponding to $-s_3^4s_1^2s_0^2s_2c_3d_3c_0d_0c_1d_1$ in B_0 and the term in B_3 , to $-s_2^4s_3^2s_0^2s_1c_2d_2c_3d_3c_0d_0$ in B_0 , The reduction involves $4(6.2.2 + 4.3.4 + 4.3.2) + 4(3 + 6 + 3)2$ terms, which exhausts the list of $4(6(4.4 + 4)) = 480$ terms in $B_0 - B_1 + B_2 - B_3$.

Comment.

Formula 9.1.4.0, should be compared with the formula of Jacobi, (Crelle Vol. 15)

$$\begin{aligned}
& sn(u + v + w)sn(u)(1 - msn(v)sn(w)sn(u + v)sn(u + w)) \\
& = sn(u + v)sn(u + w) - sn(v)sn(w).
\end{aligned}$$

Formulas 9.1.4.0. to 1. should also be compared with the formulas of Glaisher (1881) and of Cayley (Crelle Vol. 41),

Corollary.

$$0. \quad sn(u + 1) = \frac{sn(1)(sn(1)sn(2) - sn(u-1)sn(u))}{sn(1)sn(u) - sn(2)sn(u-1)}, \quad u = 3, \dots$$

Proof: Use 9.1.4.0. with $u = v = 1$ and $w = u - 1$,

Theorem.

$$0. \quad cn(u + v + w) = \frac{sn(u)dn(v)dn(w)(cn(v)cn(u + v) - cn(w)cn(u + w)) - dn(u)(sn(v)cn(v)dn(w) - sn(w)cn(w)dn(v))}{dn(u)(sn(v)dn(w)cn(u + w) - sn(w)dn(v)cn(u + v))}.$$

$$\begin{aligned}
1. \quad & sd(a_1 - a_2)cn(a_1 - a_2) - sd(a_3 - a_0)cn(a_3 - a_0) \\
& = sd(a_0 - a_1)(cn(a_0 - a_2)cn(a_2 - a_1) - cn(a_0 - a_3)cn(a_3 - a_1)) \\
& \quad - cn(a_2 - a_3)(cn(a_2 - a_0)sd(a_0 - a_3) - sd(a_2 - a_1)cn(a_1 - a_3))
\end{aligned}$$

Proof: One proof is to derive first 9.1.4.1. using the same method as in 9.1.4, the other is to set $a_3 = 0$ and derive the corresponding formula using 9.1.4.

9.1.5 Double and half arguments.

Theorem.

$$\begin{aligned}
 0. \quad sn(2u) &= \frac{2sn(u)cn(u)dn(u)}{1-msn^4(u)}. \\
 1. \quad cn(2u) &= \frac{cn^2(u)-sn^2(u)dn^2(u)}{1-msn^4(u)} \\
 &= \frac{cn^2(u)-sn^2(u)dn^2(u)}{cn^2(u)+sn^2(u)dn^2(u)}. \\
 2. \quad dn(2u) &= \frac{dn^2(u)-msn^2(u)cn^2(u)}{1-msn^4(u)} \\
 &= \frac{dn^2(u)+cn^2(u)(dn^2(u)-1)-msn^4(u)}{dn^2(u)-cn^2(u)(dn^2(u)-1)}.
 \end{aligned}$$

Theorem.

$$D0. \quad s_1 := \sqrt{\frac{1-c}{1+d}},$$

$$D1. \quad c_1 := \sqrt{\frac{1+d}{1+c}},$$

$$D2. \quad d_1 := \frac{s(c+d)}{(1+c)(1+d)s_1c_1},$$

then

$$C0. \quad d_1^2 = \frac{c+d}{1+c},$$

$$C1. \quad 2(s_1, c_1, d_1) = (s, c, d).$$

Proof. C0. follows directly from D0. to D1. It is not used to define d_1 to insure that $2(s_1, c_1, d_1)$ is (s, c, d) not $(-s, c, d)$.

The formulas can be derived starting from

$$d_1^2 - ms_1^2c_1^2 = d(1 - ms_1^4).$$

Expressing c_1^2 and d_1^2 in terms of s_1^2 gives

$$m(1+d)s_1^4 - 2ms_1^2 + 1 - d = 0, \text{ hence}$$

$$s_1^2 = \frac{m+j\sqrt{m^2-m(1-d^2)}}{m(1+d)},$$

where $j = +1$ or -1 , hence

$$s_1^2 = \frac{1-jc}{1+d}.$$

therefore

$$c_1^2 = \frac{jc+d}{1+d} \text{ and } d_1^2 = \frac{m1+d+jmc}{1+d} = \frac{jc+d}{1+jc}.$$

It remains to verify, by substitution, for c and s .

For c ,

$$c_1^2 - s_1^2d_1^2 = \frac{2jc(jc+d)}{(1+d)(1+jc)}, \text{ therefore } j = 1.$$

For s ,

$$1 + ms_1^4 = 1 + \frac{m(1-c)^2}{(1+d)^2} = 1 + \frac{1-c}{1+d} \frac{1-d}{1+c}$$

$$= \frac{2(c+d)}{(1+d)(1+c)} = \frac{2s_1c_1d_1}{s},$$

$$2s_1c_1d_1 = \sqrt{\frac{1-j}{1+j} \frac{c}{c} \frac{j}{j} \frac{c+d}{1+d}} = \frac{2s(c+d)}{(1+c)(1+d)}$$

$$= \frac{2j_1 s (jc+d)}{(1+jc)(1+d)},$$

$j_1 = +1$ or -1 has to be determined once the square roots have been chosen unambiguously.

Example.

$p = 19, m = 2, \delta^2 = 2,$
 Let $(s, c, d) = (4, 2, 8),$
 $s_1^2 = 2, c_1^2 = -1, d_1^2 = -3,$ therefore
 $s_1 = \delta, c_1 = 3\delta$ or $-3\delta, d_1 = 4$ or $-4.$

Theorem.

If $dn(u) \neq -1,$ then at $u,$

$$0. \quad sn \circ \frac{1}{2}I = \sqrt{\frac{1-cn}{1+dn}}.$$

$$1. \quad cn \circ \frac{1}{2}I = \sqrt{\frac{cn+dn}{1+dn}}.$$

$$2. \quad dn \circ \frac{1}{2}I = \sqrt{\frac{1-m+mcn+dn}{1+dn}}.$$

Theorem.

If $sn(u) = 0, cn(u) = 1$ and $dn(u) = -1,$ then

$$0. \quad sn\left(\frac{u}{2}\right) = \sqrt{\frac{1}{m}}$$

$$1. \quad cn\left(\frac{u}{2}\right) = \sqrt{\frac{m-1}{m}}.$$

$$2. \quad dn\left(\frac{u}{2}\right) = 0.$$

Theorem.

If $sn(u) = 0, cn(u) = -1$ and $dn(u) = -1,$ then

$$0. \quad sn\left(\frac{u}{2}\right) = \infty.$$

$$1. \quad cn\left(\frac{u}{2}\right) = \sqrt{-1}\infty.$$

$$2. \quad dn\left(\frac{u}{2}\right) = \sqrt{-m}\infty.$$

Conjecture.

$$0. \quad (1-m) \mid p \Rightarrow scd(2K) = (1, 0, \sqrt{1-m}).$$

$$1. \quad -1 \mid p \text{ and } -m \mid p \Rightarrow scd(K) = (\sqrt{-1}\infty, \sqrt{-m}\infty, \infty) \text{ and } scd(2K) = (0, -1, -1).$$

$$2. \quad m \mid p \text{ and } (m-1) \mid p \Rightarrow scd(K) = \left(\sqrt{\frac{1}{m}}, \sqrt{1-\frac{1}{m}}, 0\right) \text{ and } scd(2K) = (0, 1, -1).$$

Conjecture.

If $(1-m) \mid p$ then $sn(K-u) = cd(u).$

9.1.6 The Jacobi Zeta function.

Introduction.

Definitions 9.1.6 are inspired by the relation which exist, in the real case, between the Jacobi *Zeta function*, the θ functions and the Weierstrass ζ function. See Handbook p.578, 16.34 and p.650, 18.10.7.

Definition.

The *function* u is defined by:

$$\begin{aligned} u(1) &:= 0, \\ u(i+1) &:= u(i) - msn(1)sn(i)sn(i+1). \end{aligned}$$

Definition.

The *Jacobi Zeta function* Z is defined by

$$\begin{aligned} Z(1) &:= -\frac{u(K)}{K}. \\ Z(i) &:= u(i) + Z(1)i, \quad i \neq 1. \end{aligned}$$

Theorem.

0. $Z(u+v) = Z(u) + Z(v) - msn(u)sn(v)sn(u+v).$
1. $Z(u+v) = Z(u) + Z(v) + msd(u)(cn(v)cn(u+v) - cn(u))$
2. $Z(u+v) = Z(u) + Z(v) + sc(u)(dn(v)dn(u+v) - dn(u))$

Proof of 0. The formula is true, by definition, for $v = 1$. It follows by induction on v and from ... 9.1.4 Indeed,

$$\begin{aligned} Z(u+v+1) &= Z(u+v) + Z(1) - msn(1)sn(u+v)sn(u+v+1) \\ &= Z(u) + Z(v) + Z(1) - msn(u)sn(v)sn(u+v) - msn(1)sn(u+v)sn(u+v+1) \\ &= Z(u) + Z(v+1) + msn(1)sn(v)sn(v+1) - msn(u)sn(v)sn(u+v) - msn(1)sn(u+v)sn(u+v+1) \\ &= Z(u) + Z(v+1) - msn(u)sn(v+1)sn(u+v+1). \end{aligned}$$

The proof of 1. and 2. is left as an exercise. Hint: Use 9.1.4.

Theorem.

0. $Z(K-u) = -Z(u) + msn(u)cd(u).$
1. $Z(\frac{1}{2}K) = \frac{m}{2}sn(\frac{K}{2})cd(\frac{K}{2}),$ if K is even.
2. $Z(K) = 0.$
3. $Z(K+u) = -Z(K-u).$
4. $Z(2K-u) = -Z(2K+u).$
5. $Z(2K+u) = Z(u).$

Proof: 0, follows from the additional formula for *Zeta*($K-u$) and from ... 9.1.5 See Example 3.1.1. and \130 elliptic.bas

Definition.

0. $z_1(u) := Z(u) + cn(u)ds(u)$
1. $z_2(u) := Z(u) - dn(u)sc(u)$.
2. $z_3(u) := Z(u) + msn(u)cd(u)$.
3. $z_4(u) := Z(u)$.

9.1.7 Example.

Several examples of Jacobian elliptic functions follow.

$p = 5$	$m = 3$	$\delta^2 = 2$	$p = 5$	$m = 2$	$\delta^2 = 2$	$p = 5$	$m = 4$	$\delta^2 = 2$
.5	(1, -1, 2 δ)		.5	(1 δ , 2, 1 δ)		.5	(1 δ , 1 δ , 1)	
1	(0, -1, 1)		1	(1, 0, 2)		1	(∞ , 2 ∞ , 1 ∞)	
	2K = 1		2	(0, -1, 1)		2	(0, -1, -1)	
			3	(-1, 0, 2)		3	(∞ , -2 ∞ , -1 ∞)	
				2K = 2			2K = 2	
$p = 7$	$m = 3$	$\delta^2 = 3$	$p = 7$	$m = 2$	$\delta^2 = 3$	$p = 7$	$m = 4$	$\delta^2 = 3$
.5	(1, -1, 2 δ)		.5	(3 δ , 3, 1 δ)		.5	(2 δ , 1 δ , 3)	
1	(0, -1, 1)		1	(2, 2, 0)		1	(1, 0, 2)	
	2K = 1		2	(0, 1, -1)		2	(0, -1, 1)	
			3	(-2, 2, 0)		3	(-1, 0, 2)	
				2K = 2			2K = 2	
$p = 7$	$m = 6$	$\delta^2 = 3$	$p = 7$	$m = 5$	$\delta^2 = 3$			
.5	(3, 3 δ , 1 δ)		.5	(3 δ , 3, 3 δ)				
1	(1, 0, 3)		1	(2, -2, 3)				
2	(0, -1, 1)		2	(-2, 2, -3)				
3	(-1, 0, 3)		3	(0, -1, -1)				
	2K = 2		4	(2, 2, -3)				
			5	(-2, -2, 3)				
				2K = 3				
$p = 11$	$m = 5$	$\delta^2 = 2$	$p = 11$	$m = 8$	$\delta^2 = 2$	$p = 11$	$m = 9$	$\delta^2 = 2$
.5	(-3 δ , 4, 4 δ)		.5	(2, 2 δ , 1 δ)		.5	(1 δ , 4 δ , 4)	
1	(3, 5, 0)		1	(1, 0, 2)		1	(1, 0, 5)	
2	(0, 1, -1)		2	(0, -1, 1)		2	(0, -1, 1)	
3	(-3, 5, 0)		3	(-1, 0, 2)		3	(-1, 0, 5)	
	2K = 2			2K = 2			2K = 2	
$p = 11$	$m = 2$	$\delta^2 = 2$	$p = 11$	$m = 6$	$\delta^2 = 2$	$p = 11$	$m = 10$	$\delta^2 = 2$
.5	(2 δ , 2, -3 δ)		.5	(2, 2 δ , 4 δ)		.5	(1 δ , 4 δ , 5)	
1	(3, 5, 4)		1	(5, 3, 4)		1	(5, 3, -2)	
2	(-3, -5, -4)		2	(5, -3, 4)		2	(5, 3, 2)	
3	(0, -1, -1)		3	(0, -1, 1)		3	(0, 1, -1)	
4	(3, -5, -4)		4	(-5, -3, 4)		4	(-5, 3, 2)	
5	(-3, 5, 4)		5	(-5, 3, 4)		5	(-5, 3, -2)	
	2K = 3			2K = 3			2K = 3	

$p = 11$	$m = 3 \delta^2 = 2$	$p = 11$	$m = 4 \delta^2 = 2$	$p = 11$	$m = 7 \delta^2 = 2$
.5	$(5\delta, 5\delta, 4)$.5	$(4\delta, 1\delta, 4)$.5	$(5\delta, 5\delta, 5)$
1	$(-5, 3, -5)$	1	$(3, 5, 3)$	1	$(-3, 5, 2)$
2	$(1, 0, 3)$	2	$(5, 3, 0)$	2	$(1, 0, 4)$
3	$(-5, -3, -5)$	3	$(3, 5, -3)$	3	$(-3, -5, 2)$
4	$(0, -1, 1)$	4	$(0, 1, -1)$	4	$(0, -1, 1)$
5	$(5, -3, -5)$	5	$(-3, 5, -3)$	5	$(3, -5, 2)$
6	$(-1, 0, 3)$	6	$(-5, 3, 0)$	6	$(-1, 0, 4)$
7	$(5, 3, -5)$	7	$(-3, 5, 3)$	7	$(3, 5, 2)$
	$2K = 4$		$2K = 4$		$2K = 4$
$p = 13$	$m = 2 \delta^2 = 2$	$p = 13$	$m = 12 \delta^2 = 2$	$p = 13$	$m = 4 \delta^2 = 2$
.5	$(-5\delta, 4, 3\delta)$.5	$(3\delta, 6\delta, 2)$.5	$(1\delta, -5, 4\delta)$
1	$(1, 0, 5)$	1	$(\infty, 5\infty, 1\infty)$	1	$(1, 0, 6)$
2	$(0, -1, 1)$	2	$(0, -1, -1)$	2	$(0, -1, 1)$
3	$(-1, 0, 5)$	3	$(\infty, -5\infty, -1\infty)$	3	$(-1, 0, 6)$
	$2K = 2$		$2K = 2$		$2K = 2$
$p = 13$	$m = 10 \delta^2 = 2$	$p = 13$	$m = 6 \delta^2 = 2$	$p = 13$	$m = 8 \delta^2 = 2$
.5	$(3, 3\delta, 1\delta)$.5	$(-5, 1\delta, 6\delta)$.5	$(1\delta, -5, -5\delta)$
1	$(1, 0, 2)$	1	$(2, 6, 4)$	1	$(6, 2, 5)$
2	$(0, -1, 1)$	2	$(2, -6, 4)$	2	$(6, 2, -5)$
3	$(-1, 0, 2)$	3	$(0, -1, 1)$	3	$(0, 1, -1)$
	$2K = 2$	4	$(-2, -6, 4)$	4	$(-6, 2, -5)$
		5	$(-2, 6, 4)$	5	$(-6, 2, 5)$
			$2K = 3$		$2K = 3$
$p = 13$	$m = 3 \delta^2 = 2$	$p = 13$	$m = 5 \delta^2 = 2$	$p = 13$	$m = 9 \delta^2 = 2$
.5	$(-5\delta, 4, 6\delta)$.5	$(3\delta, 3, 1\delta)$.5	$(6\delta, 6\delta, 4)$
1	$(6, 2, 6)$	1	$(-6, 2, 4)$	1	$(2, 6, 2)$
2	$(\infty, -5\infty, -6\infty)$	2	$(1, 0, 3)2$		
3	$(-6, -2, -6)$	3	$(-6, -2, 4)$	3	$(-2, -6, -2)$
4	$(0, -1, -1)$	4	$(0, -1, 1)$	4	$(0, -1, -1)$
5	$(6, -2, -6)$	5	$(6, -2, 4)$	5	$(2, -6, -2)$
6	$(\infty, 5\infty, 6\infty)$	6	$(-1, 0, 3)6$		
7	$(-6, 2, 6)$	7	$(6, 2, 4)$	7	$(-2, 6, 2)$
	$2K = 4$		$2K = 4$		$2K = 4$
$p = 13$	$m = 11 \delta^2 = 2$	$p = 13$	$m = 7 \delta^2 = 2$		
.5	$(1\delta, -5, 3\delta)$.5	$(-5\delta, 4, 1\delta)$		
1	$(2, 6, 3)$	1	$(2, 6, -5)$		
2	$(1, 0, -4)$	2	$(6, -2, 3)$		
3	$(2, -6, 3)$	3	$(6, -2, -3)$		
4	$(0, -1, 1)$	4	$(2, 6, 5)$		
5	$(-2, -6, 3)$	5	$(0, 1, -1)$		
6	$(-1, 0, -4)$	6	$(-2, 6, 5)$		
7	$(-2, 6, 3)$	7	$(-6, -2, -3)$		
	$2K = 4$	8	$(-6, -2, 3)$		
		9	$(-2, 6, -5)$		
			$2K = 5$		

9.1.8 Other results.

Theorem.

$$\begin{aligned} \text{H0.} \quad & \left(\frac{1-m}{p} \right) = 1, \\ \text{then C0.} \quad & (1, 0, k_1) \in E, \\ \text{C1.} \quad & (1, 0, k_1) + (1, 0, k_1) = (0, -1, 1). \end{aligned}$$

Definition.

$$\begin{aligned} \text{Let } e = (s, c, d), \quad & s \neq \infty, \\ & \sin(2e) := 2s c, \quad \cos(2e) := c^2 - s^2. \end{aligned}$$

Can this be justified?

This is done better using $sn = \sin \circ am$, $cn = \cos \circ am$.

Theorem?.

$$\sin(2e_0 + 2e_1) = \dots$$

Theorem. [Landen]

$$\begin{aligned} \text{Let H0.} \quad & e_0 := (s_0, c_0, d_0) \in E, \\ \text{H1.} \quad & s_0 c_0 d_0 \neq 0, \quad s_0 \neq \infty, \\ \text{H2.} \quad & e_1 := (s_1, c_1, d_1) := (s_0, c_0, d_0) + (1, 0, k_1), \\ \text{H3.} \quad & l(2e_0) := \frac{\sin(2e_1) \cos(2e_0) - \cos(2e_1) \sin(2e_0)}{\sin(2e_0) - \sin(2e_1)}, \\ \text{then C0.} \quad & l(e_0) = \frac{1-k_1}{1+k_1}. \end{aligned}$$

l or $l(p, m)$ is the Landen constant associated to p and m .

Proof.

$$\begin{aligned} \text{P0.} \quad & e_1 = \left(\frac{c}{d}, -\frac{k_1 s}{d}, \frac{k_1}{d} \right). \\ \text{P1.} \quad & l(e_0) = \frac{k_1(s^2 - c^2) + c^2 - k_1^2 s^2}{d^2 + k_1} = \frac{1-k_1}{1+k_1}. \end{aligned}$$

Comment.

We can replace in the above Theorem $(1, 0, k_1)$ by $(-1, 0, k_1)$, this gives the same constant l .

We can also replace k_1 by $-k_1$, this gives the constant

$$l_1 = \frac{1}{l}.$$

9.1.9 Isomorphisms and homomorphisms.

Theorem.

If k_1 is real, there exists an isomorphism ϕ' between the elliptic group associated to m and that associated to

$$\begin{aligned} m' &= \frac{m}{m-1}, \\ \phi'(s, c, d) &:= \left(\frac{k_1 s}{d}, \frac{c}{d}, \frac{1}{d} \right) \\ \phi'(s, c, 0) &:= \left(\infty, \frac{c}{k_1 s}, \infty, \frac{1}{k_1 s}, \infty \right), \\ \phi'(\infty, c, \infty, d, \infty) &:= \left(\frac{k_1}{d}, \frac{c}{d}, 0 \right). \end{aligned}$$

Corollary.

If k_1 is real the order of the group associated to m and to $\frac{m}{m-1}$ are the same.

Theorem. [Jacobi]

If k is real, there exists an isomorphism ϕ'' between the elliptic group associated to m and that associated to

$$\begin{aligned} m'' &= \frac{1}{m}, \\ \phi''(s, c, d) &:= (k s, d, c) \\ \phi''(\infty, c \infty, d \infty) &:= (\infty, \frac{d}{k} \infty, \frac{c}{k} \infty). \end{aligned}$$

Corollary.

If k is real the order of the group associated to m and to $\frac{1}{m}$ are the same.

Theorem. [Jacobi]

If $p \equiv 1 \pmod{4}$, there exists an isomorphism ϕ_1 between the elliptic group associated to m and that associated to

$$\begin{aligned} m_j &= m_1, \\ \phi_1(s, c, d) &:= (\sqrt{-1} \frac{s}{c}, \frac{1}{c}, \frac{d}{c}), \\ \phi_1(s, 0, d) &:= (\infty, \frac{c}{\sqrt{-1}} s \infty, \frac{d}{\sqrt{-1}} s \infty), \\ \phi_1(\infty, c \infty, d \infty) &:= (\frac{\sqrt{-1}}{c}, 0, \frac{d}{c}). \end{aligned}$$

Corollary.

If $p \equiv 1 \pmod{4}$, the order of the group associated to m and to m_1 are the same.

Theorem. [Gauss]

If k is real, there exist a homomorphism ϕ_G from the elliptic group associated to m and that associated to

$$\begin{aligned} m_G &= \frac{4k}{(1+k)^2}, \\ \phi_G(s, c, d) &:= (\frac{(1+k)s}{D}, \frac{cd}{D}, \frac{2}{D} - 1), \text{ where } D = 1 + k s^2, \\ \phi_G(s, c, d) &:= (\infty, \frac{cd}{(1+k)s} \infty, \frac{2}{(1+k)s} \infty), \text{ if } 1 + k s^2 = 0. \\ \phi_G(\infty, c \infty, d \infty) &:= (0, cd, -1). \text{ CHECK } cd \end{aligned}$$

The kernel of the homomorphism is $\{(0, 1, 1), (0, -1, -1)\}$.

The image of the homomorphism is a subgroup of index 2.

Corollary.

If k is real the order of the group associated to m and to $\frac{4k}{(1+k)^2}$ are the same.

Theorem. [Landen]

If k_1 is real, there exist a homomorphism ϕ_L from the elliptic group associated to m and that associated to

$$m_L = (\frac{1-k_1}{1+k_1})^2,$$

$$\phi_L(s, c, d) := \left(\frac{(1+k_1)s}{d} c, \frac{1+k_1}{m} \frac{(d^2-k_1)}{d}, \frac{1-k_1}{m} \frac{d^2+k_1}{d} \right),$$

$$\phi_L(s, c, 0) := \left(\infty, -\frac{k}{m s c} \infty, \frac{k}{(1+k_1)^2} s c \infty \right),$$

$$\phi_L(\infty, c \infty, d \infty) := \left(\infty, \frac{d^2}{m c} \infty, \frac{d^2}{(1+k_1)^2} c \infty \right),$$

The kernel of the homomorphism is $\{(0, 1, 1), (0, -1, 1)\}$.

The image of the homomorphism is a subgroup of index 2.

Corollary.

If k_1 is real the order of the group associated to m and $+o(\frac{1-k_1}{1+k_1})^2$ are the same.

Definition.

The *amplitude function* is defined by

$$\sin \circ am = sn, \cos \circ am = cn.$$

The example below gives $\sin(2k)$, $\cos(2k)$ under \sin and \cos .

Theorem.

$$C0. \quad D am = dn,$$

$$C1. \quad D \sin = \cos, D \cos = -\sin.$$

$$C2. \quad D sn = cn dn, D cn = -sn dn, D dn = -m sn cn.$$

$$C3. \quad D^2(2am) = -m \sin \circ (2am)$$

Proof: Using the derivative of composition of functions,

$$D sn = D(\sin \circ am) = \cos \circ am D am = cn dn.$$

The other relations in C2, follow from $sn^2 + cn^2 = 1$ and $dn^2 + m sn^2 = 1$. C3, follows from $D^2(2am) = 2D dn = -2m sn cn = -m 2 \sin \circ am \cos \circ am = -m \sin \circ (2am)$.

Comment.

The derivatives will have to be defined in a separate section. Somehow the connection with p -adic functions will have to be involved.

If $|h| < 1$, then

$$\sin(x+h) = \sin(x) \cos(h) + \cos(x) \sin(h),$$

$$\sin(x+h) - \sin(x) = \sin(x) (\cos(h) - 1) + \cos(x) \sin(h),$$

but

$$\sin(h) = h + o(h) \text{ and } \cos(h) - 1 = h^2 + o(h),$$

hence

$$\frac{\sin(x+h) - \sin(x)}{h} = \cos(x) + o(1) \text{ and } D \sin = \cos.$$

For the elliptic functions, we have, see for instance Handbook, l. c., p. 575, 16.22.1 to .3 and

$$am(h) = h - \frac{h^3}{3!} m + \frac{h^5}{5!} m(4+m) - \dots,$$

$$sn(h) = h + o(h),$$

$$cn(h) = 1 + o(h),$$

$$dn(h) = 1 + o(h),$$

$$am(h) = h + o(h).$$

Hence $sn(x+h) - sn(x) = sn(x)(cn(h) dn(h) - 1) + cn(x) dn(x) sn(h) = h(cn(x) dn(x)) + o(h)$, therefore

$$D sn = cn dn.$$

$$D(\sin \circ am) = \cos \circ am D am = cn dn, \text{ therefore } D am = dn.$$

9.2 Applications.

9.2.1 The polygons of Poncelet.

Definition.

Let us associated to $e = (s, c, d)$ the point $P(e) = (\sin(e), \cos(e), 1)$.

The set of points $P(e_0 + j e)$, $j = 0, 1, \dots$ are the vertices of a polygon called the *polygon of Poncelet*.

Theorem. [Poncelet]

The sides $P(e_0 + j e) \times P(e_0 + j e + e)$ are tangent to a circle.

Proof. Let

$$\begin{aligned} e_1 &:= e_0 + j e, e_2 := e_1 + e, \\ P_1 &:= P(e_1), P_2 := P(e_2), \text{ then} \\ P_1 &= (2s_1c_1, c_1^2 - s_1^2, 1), \\ e_1 &= (s_1, c_1, d_1), \\ e_2 &= \left(\frac{s c_1 d_1 + s_1 c d}{D}, \frac{c c_1 - d s d_1 s_1}{D}, \frac{d d_1 - m s c s_1 c_1}{D} \right), \\ \text{with } D &= 1 - m s^2 s_1^2, \\ P_2 &= \left(2 \frac{(s c_1 d_1 + s_1 c d)(c c_1 - d s d_1 s_1)}{D^2}, \right. \\ &\quad \left. \frac{(c c_1 - d s d_1 s_1)^2 - (s c_1 d_1 + s_1 c d)^2}{D^2}, 1 \right), \\ P_1 \times P_2 &= [\dots]. \end{aligned}$$

Corollary. [Landen]

The lines $P_{\dots} \times P_{\dots}$ pass through a fixed point $L := (0, l, 1)$ called the point of Landen.

This is a special case of the Theorem of Poncelet, when

$$(s_0, c_0, d_0) = (1, 0, k_1).$$

Construction.

Determination of Poncelet's polygons.

Let the outscribed circle θ be

$$X_0^2 + (X_1 - d_1)^2 = S^2,$$

let the inscribed circle γ be

$$R^2(t_0^2 + t_1^2) = (c_1 t_1 + t_2)^2,$$

Given a point $P = (P_0, P_1, P_2)$ on θ and a tangent $t = (t_0, t_1, t_2)$ to γ through P , the other tangent $u = (u_0, u_1, u_2)$ is given by

$$u_1 = t_2(P_0^2 - R^2 P_2^2), u_2 = t_1(P_0^2 c_1^2 - R^2(P_0^2 + P_1^2)), u_0 = -\frac{P_1 u_1 + P_2 u_2}{P_0}.$$

Given a tangent t to γ and a point on it and θ , the other point $Q = (Q_0, Q_1, Q_2)$ common to t and θ is given by

$$Q_2 = 1, Q_1 = 2 \frac{t_0^2 d_1 - t_1 t_2}{t_0^2 + t_1^2}, Q_0 = -\frac{Q_1 t_1 + t_2}{t_0}.$$

9.3 The Weierstrass functions.

9.3.1 Complex elliptic functions.

Definition.

Given g , a non residue of p , or $\left(\frac{g}{p}\right) = -1$, then

$C_{p,g} = C_p$ is the set of pairs (a, b) , $a, b \in Z_p$ such that

$$(a, b) + (c, d) = (a + b, c + d),$$

$$(a, b) \cdot (c, d) = (ac + bdg, ad + bc).$$

We could also write (a, b) as $a + b\gamma$, with $\gamma^2 = g$.

Definition.

Given $s, c, d \in C_p$, we can repeat definition

Definition.

2 of the functions are pure imaginary, the third is real,
3 types S, C, D .

Theorem.

$$H0. \quad \delta^2 = d,$$

$$D0. \quad e_1 := (s_1\delta, c_1\delta, d_1), \quad e_2 := (s_2, c_2, d_2),$$

$$e_3 := (s_3\delta, c_3\delta, d_3),$$

$$D1. \quad D_4 := 1 - m d s_1^2 s_2^2,$$

$$D2. \quad s_4 := \frac{s_1 c_2 d_2 + s_2 c_1 d_1}{D_4}, \quad c_4 := \frac{c_1 c_2 - s_1 s_2 d_1 d_2}{D_4},$$

$$d_4 := \frac{d_1 d_2 - m d s_1 s_2 c_1 c_2}{D_4},$$

Hence replace md by m'

$$D3. \quad D_5 := 1 - m d^2 s_1^3 s_3^2,$$

$$s_5 := \frac{(s_1 c_3 d_3 + s_3 c_1 d_1)d}{D_5}, \quad c_5 := \frac{(c_1 c_3 s_1 + s_3 d_1 d_3)d}{D_5},$$

$$d_5 := \frac{d_1 d_3 - m d^2 s_1 s_3 c_1 c_3}{D_5},$$

$$H1. \quad D_4 \neq 0, \quad D_5 \neq 0,$$

then

$$C0. \quad e_1 + e_2 = (s_4\delta, c_4\delta, d_4),$$

$$C1. \quad e_1 + e_3 = (s_5, c_5, d_5).$$

$$C2. \quad 2n e_1 \in E, \quad (2n + 1)e_1 \in S.$$

Definition.

$(a, b) > 0$ if $b = 0$ and $0 < a < \frac{p}{2}$
or if $0 < b < \frac{p}{2}$.

Comment.

All that has been said above can be repeated.

9.3.2 Weierstrass' elliptic curves and the Weierstrass elliptic functions.

Introduction.

The modern work on elliptic curves starts and ends with the elliptic curves of Weierstrass. I refer the reader to Lang S.

Theorem.

- Let D0. $e_3 := -\frac{1+m}{3}$,
 D1. $g_2 = 4\frac{m^2-m+1}{3}$, $g_3 = \frac{4}{27}(m+1)(m-2)(2m-1)$.
 D2. $\Delta := g_2^3 - 27g_3^2$, $J := \frac{g_2^3}{\Delta}$,
 D3. $pn := e_3 + \frac{1}{s^2}$, $Dpn := -2\frac{cd}{s^3}$,
 D4. $e_2 := \frac{2-4m}{3}$,
 D5. $g'_2 := \frac{4}{3}16m^2 - 16m + 1$, $g'_3 := \frac{8}{27}(2m-1)(32m^2 - 32m - 1)$,
 D6. $\Delta' := g_2'^3 - 27g_3'^2$, $J' = \frac{g_2'^3}{\Delta'}$,
 D7. $qn := e_2 + \frac{1+c}{1-c}$, $Dqn := -4\frac{d(1+c)^2}{s^3}$,
 then
 C0. $Dpn^2 = 4pn^3 - g_2pn - g_3$.
 C1. $Dqn^2 = 4qn^3 - g'_2qn - g'_3$.
 C2. $\Delta = 3(12m(m-1))^2$, $J = (m^2 - m + 1)^3(\frac{2}{27m(m-1)})^2$.
 C3. $\Delta' = 256m(m-1)$, $J' = (16m^2 - 16m + 1)^3\frac{1}{108m(m-1)}$.

The proof is straihforward. Substituting D2 in C0, multiplying by s^4 and expressing c^2 and d^2 in terms of s^2 gives a polynomial of the second degree in s^2 . The coefficients of 1, s^2 and s^4 give in turn, e_3 , g_2 and g_3 .

Substituting D5 in C1, multiplying by $(1-c)^2$ gives similarly a polynomial of the second degree in $x := 1-c$. The coefficients of 1, x and x^3 give in turn e_2 , g'_2 and g'_3 .

pn corresponds to the Weierstrass P function and Dpn to its derivative.

The formulas correspond to those of real elliptic functions with the ratio of the period ω and the complete elliptic integral K set to 1.

(See for instance Handbook for Mathematical functions, p649, 18.9.1, 2,3,4,5,8,9 and 11).

Example.

With $p = 7$, $m = 2$, then $e_3 = -1$, $g_2 = 3$, $g_3 = -1$,

with $p = 7$, $m = 6$, then $e_3 = 0$, $g_2 = 3$, $g_3 = 0$.

with $p = 19$, $k^2 = 2$, then $e_3 = 18$, $g_2 = 4$, $g_3 = 0$,

$$e_2 = 17, g'_2 = 6, g'_3 = -1,$$

	sn	cn	dn	sin	cos	am	pn	Dpn	qn	Dqn
0	0	1	1	0	1	0	∞	∞	∞	∞
1	4	2	8	7	3	8	5	9	-5	5
2	7	3	6	4	-2	1	6	2	-6	-8
3	7	3	-6	-2	4	1	6	-2	-6	8
4	4	2	-8	3	7	8	5	-9	-5	-5
5	0	1	-1	1	0	0	∞	∞	∞	∞

Jacobi Z function = 0, -3, -2, 2, 3, 0

Weierstrass ζ function = ∞ , 1, 6, -6, -1, ∞ .

with $p = 19$, $k^2 = 3$, then $e_3 = 5$, $g_2 = 3$, $g_3 = -9$,

$e_2 = 3$, $g'_2 = 9$, $g'_3 = 5$,

	sn	cn	dn	sin	cos	am	pn	Dpn	qn	Dqn
0	0	1	1	0	1	0	∞	∞	∞	∞
1	7	3	5	7	3	1	-7	8	1	3
2	-1	0	6	4	-2	-4	6	0	-7	7
3	7	-3	5	-2	4	9	-7	-8	4	8
4	0	-1	1	3	7	-9	-19	-19	3	-19
5	-7	-3	5	1	0	-8	-7	8	4	-8
6	1	0	6	3	-7	5	6	0	-7	-7
7	-7	3	5	-2	-4	0	-7	-8	1	-3
8	0	1	1	4	2	0	∞	∞	∞	∞

Jacobi Z function = 0, -7, 0, 7, 0, -7, 0, 7, 0.

Weierstrass ζ function = ∞ , 6, 0, -6, ∞ , 6, 0, -6, ∞ .

If $2T$ is the period for the Jacobi functions, T is the period of pn , which is even and of Dpn which is odd. See the next section for the last 2 columns.

RERUN LAST EXAMPLE using `..[130]/ELLIPT`

Theorem.

Let $a := e_3$.

D0. $(pn3, Dpn3) := (pn1, Dpn1) + (pn2, Dpn2)$,

D1. $Q := (pn1 - a)(pn2 - 1)$, $Q' := (pn1 - a - 1)(pn2 - a - 1)$,

then

C0. $pn3 - a = 4(pn1 - a)(pn2 - a)$

C1. $pn3 - a = \left(\frac{(pn1-a)(pn2-a)-m}{(pn1-a)Dpn2+(pn2-a)Dpn1} \right)^2$

C2. $Dpn3 = \frac{Q(Q-m)(Dpn1Dpn2-4QQ')(Dpn1Dpn2-4mQ)}{Q(pn0-a)Dpn1+(pn1-a)Dpn0}$.

RECHECK THIS (the line above)

If $pn1 \neq pn2$ then

C3.0. $pn3 = \left(\frac{Dpn1-Dpn2}{2(pn1-pn2)} \right)^2 - (pn1 + pn2)$.

C4.0. $Dpn3 = \frac{pn3(Dpn1-Dpn2)+(pn1Dpn2-pn2Dpn1)}{pn2-pn1}$.

If $pn1 = pn2$ and $Dpn1 = -Dpn2$ then

C3.1. $pn3 = \infty$.

C4.1. $Dpn3 = \infty$.

If $pn1 = pn2$ and $Dpn1 = Dpn2$ then

C3.2. $pn3 = -2pn1 + \left(\frac{3pn1^2 - g_2 \frac{1}{4}}{Dpn1} \right)^2$,

C4.2. $Dpn3 = \frac{(3pn1^2 - \frac{1}{4}g_2)(pn1-pn3)}{Dpn1} - Dpn1$.

If $pn1 = pn2$ and $Dpn1 = Dpn2 = 0$ then

C3.3. $pn3 = \infty$.

C4.3. $Dpn3 = \infty$.

The proof of C3 and C4 follow from the addition formulas for the Jacobi functions. That of C2 and C3 is analogous of the formulas for the real case (Handbook p.635, 18.4.1, 18.4.2)

Theorem.

If H0. $(pn1, Dpn1) + (pn2, Dpn2) = (pn3, Dpn3)$,
then

C0. $(pn1, Dpn1), (pn2, Dpn2), (pn3, -Dpn3)$ are collinear.

This follows at once from 3.10.3. and is the geometric interpretation of C3.

Theorem.

If D0. $pn(ti, t) := t^{-2}pn(i)$,

D1. $Dpn(ti, t) := t^{-3}Dpn(i)$,

D2. $g_2(t) := t^{-4}g_2$,

D3. $g_3(t) := t^{-6}g_3$,

then

C0. $Dpn(ti, t)^2 = 4pn(ti, t)^3 - g_2(t)pn(ti, t) - g_3(t)$.

The proof follows at once from

ellinv.tab gives a table of the invariants $g_2(t)$ and $g_3(t)$ for $p = 19$ and $m = 2$ to 18.

Theorem.

Making explicit the dependence of g_2 and g_3 on m , C0. $g_2(m+1, t) = g_2(-m, t) = g_2(m+1, -t) = g_2(-m, -t)$.

C1. $g_3(m+1, t) = -g_3(-m, t) = -g_3(m+1, -t) = g_3(-m, -t)$.

C2. $g_2'(m+1, t) = g_2'(-m, t) = g_2'(m+1, -t) = g_2'(-m, -t)$.

C3. $g_3'(m+1, t) = -g_3'(-m, t) = -g_3'(m+1, -t) = g_3'(-m, -t)$.

The sections 3.10.7. to 10.12. were inspired from the formulas on complex elliptic functions.

(See for instance, Handbook, p.635 18.4.3., 18.4.8)

In the classical case, the Weierstrass p function is defined in such a way that the constant term in the Maclaurin expansion is 0. The Weierstrass ζ function is defined as its integral and the constant term is again chosen as zero, which is natural if we want ζ to be an odd function. ζ is not periodic. In the finite case, we have chosen pn and ζ using the same definition in terms of the Jacobi functions as in the real case, but now ζ as an odd periodic function. This should be contrasted with the classical case in which the Weierstrass function is not periodic. Theorem 3.10.9. gives an interesting property of $\zeta(1)$.

Definition. 2

The Weierstrass ζ function is defined by

$$\zeta(u) = Z(u) + \frac{cn(u)dn(u)}{sn(u)}.$$

Definition. 3

The function u is defined as follows:

Given $u(1) = 0$,

D0.0. $pn(i) \neq pn(j)$,

$$u(i+j) := u(i) + u(j) + \frac{Dpn(i) - Dpn(j)}{2(pn(i) - pn(j))}.$$

²5.12.83

³15.11.82

D0.1. $pn(i) = pn(j)$ and $Dpn(i) \neq Dpn(j)$, $u(i+j) = \infty$.

D1.0. $Dpn(i) \neq 0$, $u(2i) := 2u(i) + \frac{3pn(i)^2 - \frac{1}{4}g_2}{Dpn(i)}$.

D1.1. $Dpn(i) = 0$, $12pn(i)^2 = g(2)$, $u(2i) = \infty$.

D2.0. $u(0) = u(T) = \infty$.

T is the period

Theorem.

There exist a constant $\zeta(1)$ such that

$$u(j) + j \zeta(1) = u(T-j) + (T-j)\zeta(1), \quad j = 1 \text{ to } \frac{T}{2} - 1.$$

Proof. ... ?

Theorem.

The Weierstrass ζ function is related to the u function by

$$\zeta(j) := u(j) + j \zeta(1).$$

Comment.

The definitions and theorems can be repeated replacing respectively pn , Dpn , u , ζ by qn , Dqn , v , ζ' , but we have the additional property of the next Theorem.

Theorem.

$$\zeta'\left(\frac{T}{2}\right) = 0.$$

Proof. ... ?

Theorem.

ζ and ζ' are odd functions and their period is either $\frac{T}{2}$ or T .

Notation.

$\text{card}(X)$ denotes the cardinality of the set X .

Theorem.

If $p \equiv -1 \pmod{4}$, then

$$0. \quad \text{card}(g2, g3) + \text{card}(g2, -g3) = 2(p+1).$$

If $p \equiv 1 \pmod{4}$, then

$$1. \quad \text{card}(g2, g3) = \text{card}(g2, -g3).$$

Corollary.

If $p \equiv -1 \pmod{4}$, then $\text{card}(g2, 0) = p+1$.

Comment.

Examples can be obtained using P.BAS see P.HOM.

Definition.

The function Ke is defined by

$$-p < Ke(m) \equiv K(m) < p, Ke(m) \text{ is even.}$$

Theorem. [Hasse conjectured by Artin]

$$-2\sqrt{p} < Ke(m) < 2\sqrt{p}.$$

Conjecture. 4

0. Given an integer x in the range

$$-2\sqrt{p} < x < 2\sqrt{p}.$$

then there exist a pair $(g2, g3)$ such that the corresponding Weierstrass elliptic curve $W2$ has card $p + 1 + x$ and the corresponding group is abelian.

This has been verified up to $p = 47^5$.

1. If the cardinality of $W2$ is divisible by 4 and $W2$ is not abelian, then there exist a $J2$ or a $J3$ isomorphic to $W2^6$.

2. If $e_1 + e_2 + e_3 = 0$, $e_i - e_k$ are all non quadratic residue, and $j' \neq 0$, then the elliptic group is isomorphic to

$$C_{4l+2} \rtimes C_2 \text{ for some } 4l.$$

This has been verified up to $p = 97$. See g7622, Example.

Comment.

If for a given m we obtain $J3(m)$ and $J2(m)$ and the corresponding $W2$ and $W2'$, $\text{card}(W2) = \text{card}(W2')$ but $W2$ and $W2'$ are not necessarily isomorphic. E.g. $p = 17$, $J3(-2) = C_2 \rtimes C_{12}$, $J2(-2) = C_{24}$.

Comment 7

Excluding $(g2, g3) = (0, 0)$, if $j' \neq 0, 1$ there exists 2 sets of elliptic curves, corresponding to $(g2, g3)$ and $(g2, -g3)$. What is the connection between the structure if any?

None except that concerning cardinality. E.g. $p = 31$, $W2(1, 5) \sim C_{37}$, $W2(1, -5) \sim C_9 \rtimes C_3$, $W2(3, 11) \sim C_{28}$, $W2(3, -11) \sim C_{12} \rtimes C_3$.

9.3.3 The isomorphism between the elliptic curves in 3 and 2 dimensions.

This should be integrated with 3.1.

⁴4.1.84

⁵4.1.84

⁶6.1.84

⁷6.1.84

Introduction.

The usual correspondance in the real field between the functions sn , cn and dn of Jacobi and P , DP of Weierstrass should be modified to insure an isomorphism between the 3 dimensional elliptic curve associated to (sn, cn, dn) and the 2 dimensional elliptic curve associated to (P, DP) . This requires in fact to associate, in the real case to $sn(t)$, $P(2t)$.

Theorem.

The curve (P, P') has a singularity when $m = 0$ and $m = 1$, When $m = 0$, the singularity is $(-\frac{1}{3}, 0)$, because $-\frac{1}{3}$ is a double root of $4p^3 - g_2 p - g_3$, the regular solution when $P' = 0$ is $(\frac{2}{3}, 0)$. When $m = 1$, the singularity is $(\frac{1}{3}, 0)$, because $\frac{1}{3}$ is a double root of $4p^3 - g_2 p - g_3$, the regular solution when $P' = 0$ is $(-\frac{2}{3}, 0)$.

Definition.

Let (s, c, d) in E , if $m = 0$ we add the restriction $d = 1$, if $m = 1$, we add the restriction $c = d$. Let $e_3 := -\frac{1+m}{3}$, $e_2 := e_3 + 1$, $e_1 := e_3 + m$,

0. $T(s, c, d) := (e_3 + \frac{1+d}{1-c}, 2\frac{(c+d)(1+d)}{s(c-1)})$,
if $s \neq \frac{1}{c-1}$, ∞ .
1. $0.T(0, 1, 1) := (\infty, \infty)$, $1.T(0, 1, -1) := (e_1, 0)$, $m \neq 0, 1$, item $2.T(0, -1, 1) := (e_2, 0)$, item $3.T(0, -1, -1) := (e_3, 0)$,
(when $m = 0$, $d = 1$, when $m = 1$, $d = -1$),
2. $T(\infty, c\infty, d\infty) := (e_3 - \frac{d}{c}, 2\frac{(c+d)d}{c})$,
($m \neq 0$, for $m = 1$ and $c = \sqrt{-1}$, $T(\infty, c\infty, c\infty) = (-\frac{5}{3}, 4c)$).
3. $e_1 = \frac{2m-1}{3}$, $e_2 = \frac{2-m}{3}$.
... D0. gives $s_1 = \frac{1-c}{1+d}$, $c_1 = \sqrt{\frac{c+d}{1+d}}$,
 $d_1 = \frac{s(c+d)}{(1+c)(1+d)s_1 c_1}$.

Theorem.

Let $a := \frac{p'}{2(p-e_3)(p-e_3-1)}$, then

0. $a^2 \neq 0, -1 \Rightarrow T^{-1}(p, p') = (s, c, d)$, where
 $c := \frac{1-a^2}{1+a^2}$, $s := \frac{c-1}{a}$, $d := (1-c)(p-e_3)-1$.
1. $a^2 = -1 \Rightarrow T^{-1}(p, p') = (\infty, a\infty, a(e_3-p)\infty)$.
2. $0.T^{-1}(e[3], 0) = (0, -1, -1)$, for $m \neq 0$. $1.T^{-1}(e[3]+1, 0) = (0, -1, 1)$, for $m \neq 1$. $2.T^{-1}(e[3]+m, 0) = (0, 1, -1)$, for $m \neq 0, 1$.
3. $T^{-1}(\infty, \infty) = (0, 1, 1)$.

Proof: If $a^2 \neq 0, -1$, solving $(1-c)(p-3e_3) = 1+d$ and $sp' = -2(c+d)(p-e_3)$ for c gives $c-1 = a s$. Hence $(c-1)^2 = a^2(1-c)^2$, but $c \neq 1$, $1-c = a^2(1+c)$, hence $c, s = \frac{c-1}{a} = -2\frac{a}{1+a^2}$ and d .

Theorem.

Let $g_2 := 4\frac{m^2-m+1}{3}$ and $g_3 := \frac{4}{27}(m-2)(2m-1)(m+1)$, let $T(s, cd) = (p, p')$, then

$$0. \quad p'^2 = 4p^3 - g_2p - g_3.$$

Definition.

The bijection defined by 9.3.3 and justified by 9.3.3 defines an isomorphism between the 3 dimensional elliptic curve of ... and the 2 dimensional elliptic curve 9.3.3.0.

Definition.

The invariant j of sec-tell32a.0. is

$$j := 2^6 3^3 j', \text{ with}$$

$$j' := \frac{g_2^3}{g_2^3 - g_3^2}.$$

Theorem.

$$0. \quad g_2^3 - g_3^2 = (m(m-1))^2.$$

$$1. \quad j = 2^6 3^3 \frac{(m^2-m+1)^3}{(m(m-1))^2}.$$

$$2. \quad \text{If } j \text{ is given and } M \text{ is a solution of 1, the other solutions are } 1-m, \frac{1}{m}, 1-\frac{1}{m}, \frac{1}{1-m}, \frac{m}{1-m}.$$

Example.

For $p = 11$, let $u := m(m-1)$, $j' = -3$ corresponds to $u = 1, -2, -5$ or $m = -3, 4, 3, -2, -4, 5$ giving

$$K(j) = 4 \text{ or } -4.$$

$j' = 4$ corresponds to $u = 2, -3$ or $m = 2, -1, -5$ giving $K(j) = 0$.

$j' = \infty$ corresponds to $u = 0$ or $m = 0, 1$ giving $K(j) = 1$ or -1 .

$j' = 0$ corresponds to $u = -1$ or $m = -5 + 2\delta$, giving $K(j) = 0$.

Theorem.

Given e_1, e_2 and e_3 such that

$$H.0. \quad e_1 + e_2 + e_3 = 0,$$

$$H.1. \quad e_i \text{ are distinct,}$$

$$\text{Let } m := \frac{e_1 - e_3}{e_2 - e_3},$$

$$e_2 - e_3 = d,$$

$$g2 := 4(e_3^2 - e_1 e_2),$$

$$g3 := 4e_1 e_2 e_3.$$

then

$$C.0. \quad (d_p) = 1 \Rightarrow J3(m) \sim W2(g2, g3).$$

$$C.1. \quad (d_p) = -1 \Rightarrow (p+1 - |J3(m)|) - (-1_p)(p+1 - |W2(g2, g3)|) = 0.$$

Proof: Let $c^2 = \frac{1}{d}$, $e'_i = c^2 e_i$, then $e'_1 = e'_3 + m$ and $e'_2 = e'_3 + 1 \dots$

9.3.4 Correspondance between the Jacobi elliptic curve (cn, sd) and the Weierstrass elliptic curve

Definition.

Let $m_1 := 1 - m$, $e_2 := 2\frac{1-2m}{3}$.

$$0. \quad T(cn, sd) := (e_2 + \frac{1+cn}{1-cn}, -4sd\frac{m_1+mcn^2}{(1-cn)^2}),$$

if $cn \neq 1$.

$$1. \quad T(1, 0) := (\infty, \infty),$$

$$2. \quad T(\infty, sd) := (e_2 - 1, -4msd),$$

$$3. \quad \text{If } -\frac{m_1}{m} = b^2 \text{ then}$$

$$T(b, \infty) = (e_2 + \frac{1+b}{1-b}, 0).$$

Theorem.

Let $a := p - e_2 + 1$, then

$$0. \quad a \neq 0, \quad cn := \frac{a-2}{a},$$

$$m_1 + mcn^2 \neq 0 \text{ then } T^{-1}(p, p') = (cn, sd),$$

$$\text{where } sd := P' \frac{(1-cn)^2}{-4(m_1+mcn^2)},$$

$$m_1 + mcn^2 = 0 \text{ then } T^{-1}(p, p') = (cn, \infty),$$

$$1. \quad T^{-1}(\infty, \infty) = (1, 0).$$

$$2. \quad a = 0 \Rightarrow T^{-1}(p, p') = (\infty, \frac{p'}{-4m}).$$

$$3. \quad T(-1, 0) = (e_2, 0).$$

$$4. \quad \text{If } T^{-1}(x, 0) = (y, \infty) \text{ and } x \neq e_2 \text{ then}$$

$$m(m-1) = d^2 \text{ and}$$

$$x = e_1 \text{ or } e_3 = -\frac{e_2}{2} \pm 2d.$$

Theorem.

Let $g_2 := \frac{4}{3}(16m^2 - 16m + 1)$ and

$$g_3 := \frac{8}{27}(2m-1)(32m^2 - 32m - 1),$$

let $T(cn, sd) = (P, P')$, then

$$0. \quad P'^2 = 4P^3 - g_2P - g_3.$$

Definition.

The bijection defined by 9.3.4 and justified by 9.3.4 defines an *isomorphism between the 2 dimensional elliptic curve of ... and the 2 dimensional elliptic curve sec-tell32a.0.*

Theorem.

Using 9.3.3,

$$0. \quad g_2^3 - g_3^2 = 256m(m-1).$$

$$1. \quad j = 16 \frac{(16m^2 - 16m + 1)^3}{m(m-1)}.$$

Corollary.

Let $c := \sqrt{1 - \frac{1}{m}}$, $p = e_2 + \frac{1+c}{1-c}$, using e_2 from 9.3.4 and g_2, g_3 from sec-tjacweia, then
 $p^3 - g_2p - g_3 = -1$.
 ... DOUBLE CHECK THIS.

The proof follows from the fact that the denominator $m_1 + m \, cn$ in 9.3.4.0. cannot be zero.

Theorem.

Given e_1, e_2 and e_3 such that H.0. $e_1 + e_2 + e_3 = 0$,

$$H.1. \quad 1 - \left(\frac{e_1 - e_3}{3e_2}\right)^2 = f^2,$$

H.2. e_i are distinct,

$$\text{Let } m := \frac{1}{2}\left(1 + \frac{1}{d}\right),$$

$$d = 2 \frac{1-2m}{3e_2},$$

$$g_2 := 4(e_3^2 - e_1e_2),$$

$$g_3 := 4e_1e_2e_3.$$

then

$$C.0. \quad (d_p) = 1 \Rightarrow J3(m) \sim W2(g_2, g_3).$$

$$C.1. \quad (d_p) = -1 \Rightarrow (p+1 - |J3(m)|) - (-1-p)(p+1 - |W2(g_2, g_3)|) = 0.$$

Proof: Let $e'_i = c^2 e_i$. We have a $J2(m)$ if $e'_2 = 2 \frac{1-2m}{3}$ and $e'_1 - e'_3 = 4d = 4\sqrt{m(m_1-1)}$ because of ...

Example.

p	e_1, e_2, e_3	g_2, g_3	j'	m'	$structure$
13	1, 3, 9	0, 4	0	-5	$C_6 \rtimes C_2$
29	1, 9, 19	-13, -12	13	3	$C_{14} \rtimes C_2$
37	1, 6, 30	-13, 17	-6	-14	$C_{22} \rtimes C_2$
	2, 15, 20	0, -5	0	-5	$C_{14} \rtimes C_2$
41	1, 13, 27	-6, 10	-6	-12	$C_{18} \rtimes C_2$
53	1, 19, 33	-13, 17	-17	-22	$C_{30} \rtimes C_2$
	1, 20, 32	-12, 16	-21	3	$C_{22} \rtimes C_2$
61	1, 8, 52	-13, 17	15	-23	$C_{30} \rtimes C_2$
	1, 29, 31	7, -3	26	11	$C_{30} \rtimes C_2$
	2, 26, 33	0, -29	0	-28	$C_{38} \rtimes C_2$
73	1, 8, 64	0, 4	0	$C_{42} \rtimes C_2$	
	1, 15, 57	15, -11	13	-21	$C_{42} \rtimes C_2$
	1, 29, 43	-20, 24	-7	-29	$C_{34} \rtimes C_2$
89	1, 13, 75	20, -16	44	-26	$C_{50} \rtimes C_2$
	1, 25, 63	23, -19	-12	-30	$C_{42} \rtimes C_2$
	1, 29, 59	13, -9	15	24	$C_{42} \rtimes C_2$
97	1, 8, 88	1, 3	2	-39	$C_{50} \rtimes C_2$
	1, 18, 78	14, -10	-17	-20	$C_{50} \rtimes C_2$
	1, 35, 61	0, 4	0	$C_{42} \rtimes C_2$	
	1, 38, 58	15, -11	7	-19	$C_{42} \rtimes C_2$
				
113	...				
	1, 22, 90	-6, 10	21	$C_{58} \rtimes C_2$	
	...				

9.4 Complete elliptic integrals of the first and second kind.

Introduction.

Several conjectures appear to justify the terminology of complete elliptic integrals of the first and second kind for the functions K and E defined below. The definitions are inspired from the definitions in the real and complex fields. Their importance is associated with Conjecture 9.4. By convention in this section I will use

$$q := \left[\frac{p}{2}\right] = \frac{p-1}{2}.$$

Again I denotes the identity function ($I(i) = i$), D denotes the derivative operator and $f \circ g$ denotes the function which is obtained by composition from the functions f and g .

Definition. 8

$$0. \ K_j := \left(\frac{(2j-1)!!}{2^j}\right)^2, \pmod{p}, \ 0 \leq j \leq q.$$

1. $E'_j := K_j \frac{2j}{2j-1}$, $j = 0$ to q ,
2. $E_0 := 1$, $E_j := -\frac{K_j}{2j-1}$, $j = 1$ to q ,

Definition.

0. $K := \sum_{j=0}^q (K_j I^j)$,
1. $E' := \sum_{j=0}^q (E'_j I^j)$,
2. $E := \sum_{j=0}^q (E_j I^j)$,

Example.

For $p = 11$,

j	K	E'	E	D	B	C	K''	$all[j]$
0	1	0	1	-5	-5	-4	(1)	
1	3	-5	-3	5	-2	-3	1	
2	1	5	-4	-1	2	-2	(-5)	
3	1	-1	2	5	-4	-2	-4	
4	3	5	-2	-5	-3	-1	(-4)	
5	1	-5	-5	0	1	0	-1	

For $p = 13$,

j	K	E'	E	D	B	C	K''	$all[j]$
0	1	0	1	-6	-6	5	1	
1	-3	-6	3	1	-4	-6	(1)	
2	4	1	3	-1	5	1	-6	
3	-3	-1	-2	-1	-2	-2	(-5)	
4	4	-1	5	1	3	4	-6	
5	-3	1	-4	-6	3	-1	(4)	
6	1	-6	-6	0	1	0	2	

See 9.4 and 9.4.

Lemma.

0. $K_j = K_{q-j}$, $0 \leq j \leq q$.
1. $E'_j = E'_{q+1-j}$, $0 < j \leq q$.
2. $E'_j = \frac{2j-1}{2j} K_{j-1}$, $0 < j \leq q$.
3. $E_{j+1} = \frac{(2j-1)(2j-3)}{4j^2} E_j$, $0 < j \leq q$.
4. $2jK_j - (2j+1)K_{j-1} = 2jE_j$, $0 < j \leq q$.
5. $2jE_j + E'_j = 0$, $0 \leq j \leq q$.
6. $2(j+1)E'_{j+1} - 2jE'_j - E_j = 0$, $0 \leq j < q$.

The proof⁹ follows at once from Lemma 3.0.8.4 (g730) and from 9.4.

Theorem.

(see KE.NOT)

$$K\left(\frac{1}{m}\right) = (m_p)K(m), 0 < m < p.$$

Proof.

$K\left(\frac{1}{m}\right) = m^q K(m)$, because of 9.4.0 and $m^q = (m_p)$ by the Theorem of Euler. See for instance Adams and Goldstein, p. 107.

Corollary.

$$p \equiv 1 \pmod{4} \Rightarrow K(-1) = 0.$$

Theorem.

$$0. \ 2IDK + K - 2DE' = 0.$$

$$1. \ 2(1 - I)DK - K - 2DE = 0.$$

$$2. \ 2IDE + E' = 0.$$

$$3. \ 2(1 - I)DE' - E = 0.$$

Proof: This follow immediately from the definitions, for instance, the coefficient of I^j is

$$2jK_j + K_j - 2(j+1)E'_{j+1} = 0 \text{ for } 0 \leq j < q,$$

and that of $I^q = 0$ because $2q + 1 = p = 0$.

Corollary.

$$0. \ K(0) = 2DE'(0) = E(0) = 1.$$

$$1. \ DK(0) - DE(0) = \frac{1}{2}.$$

$$2. \ E'(0) = 0.$$

$$3. \ K(1) = -2DE(1) = 2DE'(1) - 2DK(1) = -E'(1).$$

$$4. \ E(1) = 0.$$

Theorem.

$$0. \ 4D(I(1 - I)DK) - K := 0.$$

$$1. \ 4ID((1 - I)DE') + E' := 0.$$

$$2. \ 4(1 - I)D(IDE) + E := 0.$$

$$3. \ K = E + E'.$$

This derives from 9.4 by elimination, for instance, eliminating E' from 2 and 3 gives

$$4(1 - I)D(IDE) = -2(1 - I)DE' = -E$$

$$4ID((1 - I)DE') = 2IDE = -E'.$$

1, times I gives

$$4I(1 - I)DK - 2IK - 4IDE = 0,$$

using 2 and 0 gives

$$\begin{aligned} 4I(1-I)DK - 2IK + 2E' &= 0, \\ 4D(I(1-I)DK) - 2D(IK) + 2IDK + K &= 0. \end{aligned}$$

Finally, it follows from 9.4.0 and 1 that $D(K - E - E') = 0$, but $K(0) = E(0) + E'(0) = 1$, hence 3.

Definition.

0. $K_j'' := \frac{((2j-3)(2j-7)\dots)^2}{j!} \pmod{p}$,
1. $K'' := \sum_{j=0}^{\frac{q}{2}} (K_{q-2j} I^{(q-2j)})$.

Lemma.

- 0.0. $p \equiv 1 \pmod{4} \Rightarrow K'' \text{ is even,}$
1. $p \equiv -1 \pmod{4} \Rightarrow K'' \text{ is odd.}$
1. $(q-j+2)(q-j+3)K_{q-j+2}'' = (2q-4j+1)^2 K_{q-j}''$, $1 < j \leq q$.
2. $D((1-4I^2)DK'') - K'' = 0$.
3. cK'' are, for arbitrary constant c , the only solutions of 2.

To prove 3., we substitute

$$\sum_{j=0}^q (X_{q-j} I^{(q-j)}),$$

in 2, this gives

$$\begin{aligned} &-(2q+1)^2 X_q I^{(q)} - (2q-1)^2 X_{q-1} I^{(q-1)} \\ &+ \sum_{j=2}^q ((q-j+2)(q-j+3)X_{q-j+2} - (2q-4j+1)^2 X_{q-j}) I^{q-j} = 0. \end{aligned}$$

The coefficient of I^q is zero because $2q+1=0$, hence X_q is arbitrary. The coefficient of $I^{(q-1)}$ must be zero, therefore $X_{q-1} = X_{q-3} = \dots = 0$.

Lemma.

0. $K \circ (1-I)$ satisfies 9.4.0.
1. $E \circ (1-I)$ satisfies 9.4.1.
2. $K \circ (I + \frac{1}{2})$ satisfies 9.4.2.
3. $K'' = sK'' \circ (-I)$.
4. $K = sK \circ (1-I)$.
5. $E = sE' \circ (1-I)$.

For instance,

$$\begin{aligned} K \circ (1-I) &= 4(D(I(1-I)DK) \circ (1-I)) \\ &= -4D((1-I)IDK \circ (1-I)) \end{aligned}$$

$= 4D((1-I)ID(K \circ (1-I)))$. Hence 0. 3, from 9.4.0 and $s = (-1)^{\frac{p-1}{2}}$. $K = cK'' \circ (I - \frac{1}{2}) = scK'' \circ (\frac{1}{2} - I) = sK \circ (1-I)$, hence 4. Finally, $E \circ (1-I)$ and E' satisfy the same differential equation, of second order, moreover $E(1) = sE'(0) = 0$ and $DE(1) = -sDE'(0)$ because of ... and of $K(1) = sK(0)$ hence 5.

Corollary.

0. $K(m) = sK(1-m)$, with $s = (-1)^q$.
 1. $K(\frac{m}{m-1}) = (\frac{m^2}{1-m})K(m)$, $2 < m < p-1$.
 2. $E(m) + sE(1-m) = K(m)$
 3. $\frac{E(m)}{K(m)} + \frac{E(1-m)}{K(1-m)} = 1$.
 4. $mRp, k^2 = m \Rightarrow K(\frac{4k}{1+k}{}^2) = K(m)$, $2 < m < p-1$.
 5. $1-mRp, k^2 = 1-m \Rightarrow K(((1-k)(1+k))^2) = K(m)$, $2 < m < p-1$.
- 4 and 5 are still conjectures.

Corollary.

$$(-1)^k \sum_{j=0}^j \left(\frac{(2j-1)!!}{(2j)!!} \right)^2 \binom{j}{k} = (-1)^q \left(\frac{(2k-1)!!}{(2k)!!} \right)^2.$$

Exchanging k and j , 1. follows from Lemma 3.0.x. of g730. Theorem 7.

Corollary.

0. $p \equiv -1 \pmod{4} \Rightarrow K(\frac{p+1}{2}) = 0$,
1. $p \equiv 1 \pmod{4} \Rightarrow K(\frac{p+1}{2}) = 2E(\frac{p+1}{2})$.

Conjecture.

With the exception of $p = 7$, $K(3) = 3(= -4)$,
 $m \neq 0, 1, |K(m)| < \frac{p}{2} \Rightarrow K(m) \equiv p+1 \pmod{4}$.

Corollary.

$$p \equiv 1 \pmod{4}, \Rightarrow K(m) \neq 0.$$

Example.

For $p = 11$,

m	K	E'	E	D	B	C	K''	$\frac{E}{K}$	$all(m)$
0	1	0	1	1	1	1	0	1	
1	-1	-1	0	5	-5	5	-4	0	
2	0	-1	1	-4	-5	-4	4	∞	
3	4	-4	-3	2	3	2	4	2	
4	4	-5	-2	3	4	3	0	5	
5	-4	4	3	-3	-2	-3	-1	2	
6	0	-5	5	0	-1	0	1	∞	
7	4	-3	-4	2	1	2	0	-1	
8	-4	2	5	0	-1	0	-4	-4	
9	-4	3	4	-2	-1	-2	-4	-1	
10	0	-1	1	-4	-5	-4	4	∞	

For $p = 13$,									
m	K	E'	E	D	B	C	K''	$\frac{E}{K}$	$all(m)$
0	1	0	1	1	1	1	1	1	
1	1	1	0	6	-6	6	4	0	
2	6	6	0	-6	6	-6	-4	0	
3	-2	3	-5	1	2	1	-4	-4	
4	-2	1	-3	3	4	3	-4	-5	
5	-2	-3	1	-5	-6	-5	-1	6	
6	2	4	-2	5	4	5	2	-1	
7	-6	-3	-3	4	3	4	2	-6	
8	2	-2	4	-2	-3	-2	-1	2	
9	-2	1	-3	3	4	3	-4	-5	
10	-2	-3	1	-6	-5	-6	-4	6	
11	-2	-5	3	-3	-4	-3	-4	5	
12	6	0	6	-1	0	-1	4	1	

Definition.

By analogy with the case of the real or complex field,

$$0. D_j := K_{j+1} - E_{j+1}, 0 \leq j < q, D_q := 0.$$

$$1. B_j := K_j - D_j, 0 \leq j \leq q.$$

$$2. C_j := D_{j+1} - B_{j+1}, 0 \leq j < q, C_q := 0.$$

$$3. D := \sum_{j=0}^q (D_j I^j),$$

$$4. B := \sum_{j=0}^q (B_j I^j),$$

$$5. C := \sum_{j=0}^{\frac{q}{2}} (C_j I^j).$$

Theorem.

$$0. D_j = E_{j+1}, 0 \leq j < q.$$

$$1. B_j = E_{q-j}, 0 \leq j \leq q.$$

$$2. D = \frac{E'}{I}.$$

$$3. IB = IE + (I - 1)E'.$$

$$4. I^2 C = (2 - I)E' - IE.$$

$$5. I^2 C = 2E' - IK. ?$$

9.5 P-adic functions, polynomials, orthogonal polynomials.

Comment.

In a p -adic field, we can define polynomials of degree up to $p - 1$. These are determined by their values at i in Z_p . If these are defined in the real field with rational coefficient, the definition and properties are automatically extended to the p -adic field. For orthogonal polynomials, recurrence relations, differential equations and values of the coefficients generalize automatically. Therefore, we have the definitions 1. and the theorems 2. and 3.

Definition.

The *polynomials of Chebyshev of the first* (T_n) *and of the second kind* (U_n), *of Legendre* (P_n), *of Laguerre* (L_n) *and of Hermite* (H_n) are defined by the differential equations:

0. $(1 - I^2)D^2T_n - IDT_n + n^2T_n \equiv 0$,
 $T_n(0) \equiv 1, DT_n(0) \equiv .$
1. $(1 - I^2)D^2U_n - 3IDU_n + n(n + 2)U_n \equiv 0$,
 $U_n(0) \equiv 1, DU_n(0) \equiv .$
2. $(1 - I^2)D^2P_n - 2IDP_n + n(n + 1)P_n \equiv 0$,
 $P_n(0) \equiv 1, DP_n(0) \equiv .$
3. $ID^2L_n + (1 - I)DL_n + n \equiv 0$.
4. $D^2H_n - 2IH_n + 2n \equiv 0$.

Theorem.

If $X_{n,j}$ denotes the coefficient of I^j in the polynomial X_n , then

0. $T_{n,n-2j} \equiv \frac{n}{2} 2^{(n-2j)} (-1)^j \frac{(n-j-1)!}{j!(n-2j)!}$,
1. $U_{n,n-2j} \equiv \frac{n}{2} 2^{(n-2j)} (-1)^j \frac{(n-j)!}{j!(n-2j)!}$,
2. $P_{n,n-2j} \equiv 2^{(-n)} (-1)^j \frac{(2n-2j)!}{j!(n-j)!(n-2j)!}$,
3. $L_{n,j} \equiv (-1)^j \frac{n!}{(n-m)!(m!)^2}$,
4. $H_{n,n-2j} \equiv n! 2^{(n-2j)} (-1)^j \frac{1}{j!(n-2j)!}$,

See for instance Handbook of Mathematical functions, p. 775.

Theorem.

0. $T_0 1, T_1 \equiv I, T_{n+1} \equiv 2(2I - 1)T_n - T_{n-1}$,
1. $U_0 \equiv 1, U_1 \equiv 2I, U_{n+1} \equiv 2(2I - 1)U_n - U_{n-1}$,
2. $P_0 \equiv 1, P_1 \equiv I, (n + 1)P_{n+1} \equiv -(2n + 1)IP_n - nP_{n-1}$,

3. $P_0 \equiv 1, P_1 \equiv I, (n+1)P_{n+1} \equiv (2n+1-I)P_n - nP_{n-1},$
4. $H_0 \equiv 1, H_1 \equiv 2I, H_{n+1} \equiv 2IH_n - 2nH_{n-1}.$

See for instance Handbook of Mathematical functions, p. 782.

Theorem (T).

$$T_{i+2pk,j} = -T_{i+pk,j} = T_{i,j}, j < p.$$

Proof:

$$\begin{aligned} T_{p+i,j} &\equiv (-1)^{\frac{p+i-j}{2}} 2^j \frac{(\frac{p+i-j}{2}-1)! \frac{p+i}{2}}{(\frac{p+i-j}{2})! j!} \\ &\equiv (-1)^{\frac{p+i-j}{2}} (-1)^{\frac{p-i-j}{2}} (-1)^{\frac{p-i+j+i}{2}} 2^j \frac{(\frac{p-i+j-2}{2})! \frac{p-i}{2}}{(\frac{p-i-j}{2})! j!} \\ &\equiv (-1)^{\frac{p-i-j}{2}} 2^j \frac{(\frac{p-i+j-2}{2})! \frac{p-i}{2}}{(\frac{p-i-j}{2})! j!} \\ &\equiv T_{p-i,j}. \end{aligned}$$

Theorem (U).

0. $U_{i+2pk,j} = -U_{i+pk,j} = U_{i,j}, j < p.$
1. $U_{p-1+i,j} \equiv (-1)^{\frac{p-1+i-j}{2}} \frac{(\frac{p-1+i+j}{2})! 2^j}{(\frac{p-1+i-j}{2})! j!}$
2. $U_{p-1+i,j} \equiv (-1)^{\frac{p-1+i-j}{2}} (-1)^{\frac{p-i-j-1}{2}}$
3. $(-1)^{\frac{p-i+j-1}{2}} \frac{(\frac{p-i+j-1}{2})! 2^j}{(\frac{p-1+i-j}{2})! j!}$
4. $U_{p-1-i,j} \equiv (-1)^{\frac{p-1+i-j}{2}} 2^j \frac{(\frac{p-1-i+j}{2})!}{(\frac{p-1-i-j}{2})! j!} \equiv U_{p-1-i,j}.$

Theorem (Le). 10

$$P_{p-1-n} = P_n, n < p.$$

Proof: The polynomials can be defined by the recurrence relations,

$$P_0 = 1, P_1 = I, (n+1)P_{n+1} = (2n+1)IP_n - nP_{n-1}, n < p-1.$$

The last equation is valid for $n+1 = p$ and therefore P_p can be considered as 0 as far as the proof of the theorem is concerned. They satisfy the Rodrigues' formula

$$P_n = \frac{1}{2^n n!} D^n (I^{2-1})^n$$

Therefore

$$\begin{aligned} P_{p-1} &= \frac{1}{(2^{p-1}(\frac{p-1}{2})!)^2} D^{(p-1)} (-I^2)^{(\frac{p-1}{2})} \\ &= (-1)^{\frac{p-1}{2}} \frac{(p-1)!}{2^{p-1}(\frac{p-1}{2})!^2}, \end{aligned}$$

but $2^{(p-1)} = 1, (p-1)! = -1$, and

$$(\frac{p-1}{2})!^2 = (-1)^{(\frac{p-1}{2})} (p-1)!$$

because $\frac{p-i}{2} = -\frac{p+i}{2}$, hence

$$P_{p-1} = 1.$$

By convention we can write $P_p = P_{-1} = 0$, if we replace in the recurrence relation n by $p - n - 1$ we obtain

$$(n+1)P_{p-n-2} = (2n+1)P_{p-n-1} - nP_{p-n},$$

and therefore, by induction,

$$P_{p-1-n} = P_n.$$

Example.

$p = 11$, see orthog, 120.

$$P_0 = 1,$$

$$P_1 = I,$$

$$P_2 = 5 - 4I^2,$$

$$P_3 = 4I - 3I^3,$$

$$P_4 = -1 - I^2 + 3I^4,$$

$$P_5 = -5I + 5I^3 + I^5,$$

$$P_6 = -1 - I^2 + 3I^4,$$

$$P_7 = 4I - 3I^3$$

$$P_8 = 5 - 4I^2,$$

$$P_9 = I,$$

$$P_{10} = 1.$$

For $p = 13$,

$$P_0 = P_{12} = 1,$$

$$P_1 = P_{11} = I,$$

$$P_2 = P_{10} = 6 - 5I^2,$$

$$P_3 = P_9 = 5I - 4I^3,$$

$$P_4 = P_8 = 2 + 6I^2 + 6I^4,$$

$$P_5 = P_7 = -3I + I^3 + 3I^5,$$

$$P_6 = -6 - 4I^2 - I^4 - I^6,$$

Theorem (La).

Theorem (H).

Definition.

The *scaled Hermite polynomials* are defined by

$$0. \ H_0 = 1,$$

$$1. \ H_1 = I,$$

$$2. \ \begin{aligned} \left[\frac{n}{2} \right] H_n &= a_n H_{n-1} - \frac{n-1}{2} H_{n-2}, \\ \text{where } a_n &= 1 \text{ if } n \text{ is even and } a_n = \left[n \frac{1}{2} \right], \text{ the largest integer in } \frac{n}{2} \text{ if } n \text{ is odd.} \end{aligned}$$

Example.

$$H_2 = -\frac{1}{2} + I^2,$$

$$H_3 = -\frac{3}{2}I + I^3,$$

$$H_4 = \frac{3}{8} - \frac{3}{2}I^2 + \frac{1}{2}I^4,$$

$$H_5 = \frac{15}{8}I - \frac{5}{2}I^3 + \frac{1}{2}I^5,$$

$$\begin{aligned} H_6 &= -\frac{5}{16} + \frac{15}{8}I^2 - \frac{5}{4}I^4 + \frac{1}{6}I^6, \\ H_7 &= -\frac{35}{16}I + \frac{35}{8}I^3 - \frac{7}{4}I^5 + \frac{1}{6}I^7. \end{aligned}$$

Lemma.

Modulo p , $p > 2$,

0. $(p-1)! \equiv -1$.
1. $(p-1-i)! \equiv (-1)^{(i+1)} \frac{1}{i!}$, $0 \leq i < p$.
2. $\binom{p-1-i}{j} \equiv (-1)^j \binom{i+j}{j}$, $0 \leq i, j, i+j < p$.
3. $\binom{kp+i}{j} \equiv \binom{i}{j}$, $j < p$.
4. $(p-2-i)!!i!! \equiv (-1)^{k\frac{1}{2}}(p-1-k-i)!!(k+i-1)!!$
 $0 \leq i < p-1, 0 < k+i < p$.

Proof: 0. is the well known Theorem of Wilson. 1. can be considered as a generalization.

$$\begin{aligned} (p-1-i) &\equiv (-1)^i(p-1) \dots (i+1) \\ &\equiv (-1)^i \frac{(p-1)!}{i!} \\ &\equiv (-1)^{i+1} \frac{1}{i!}. \end{aligned}$$

For 2. $\frac{(p-1-i)!}{(p-1-i-j)!j!}$

$$\equiv (-1)^{(i+1)} \frac{(i+j)!}{(-1)^{i+j+1}i!j!} \equiv (-1)^j \binom{i+j}{j}.$$

Lemma.

Modulo p , $p > 2$,

0. $((p-2)!!)^2 \equiv (-1)^{\frac{p-1}{2}}$
1. $(p-1)!!(p-2)!! \equiv -1$.
2. $0.(p-2-i)!!i!!(-1)^s(p-2)!!$,
where $s = i\frac{1}{2}w \equiv n$ i is even
and $s = \frac{p-2-i}{2}$ when i is odd. 1. or where $s = [\frac{[\frac{p}{2}]+1+i}{2}] + [\frac{p+1}{4}]$.

0, and 1 are well known and given for completeness. 2, if i is even,

$$\begin{aligned} (p-2-i)!!i!!(p-i)!!(i-2)!!(i\frac{1}{p-i}) &\text{ or } -1 \\ (-1)^{(i\frac{1}{2})}(p-2)!!0!! & \end{aligned}$$

if i is odd,

$$\begin{aligned} (p-2-i)!!i!!(p-4-i)!!(i+2)!!(i\frac{p-2-i}{i+2}) &\text{ or } -1 \\ \equiv (-1)^{(\frac{p-2-i}{2})}(0)!!p-2!! & \end{aligned}$$

2.1, can be verified by choosing $p = 1, 3, 5, 7$ and $i = 0, 1, 2, 3, 4$.

Theorem (La).

$$0. \quad L_{p-1-i,j} \equiv (-1)^j L_{i+j,j}, \quad 0 \leq i, j, \quad i+j < p.$$

Proof:

For $0, L_{n,j} = (-1)^j \binom{n}{j} \frac{1}{j!}$. See for instance, Handbook p.775.

Lemma.

11

$$\begin{aligned} & \sum ((2j-1)!!(2k)!! \frac{1}{(2j)}!!(2k-1)!!)^2 j! \frac{1}{k!(j-k)!} \\ & = (-1)^{([p\frac{1}{2}] - k)}, \quad j = k \text{ to } [p\frac{1}{2}]. \end{aligned}$$

This is needed for g761, Not yet proven.

The expression which is summed in the first member can be replaced by

$$\frac{(\frac{(2j)!}{(2k)!})^2 k!}{j!(j-k)! 2^{2(j-k)}}.$$

9.5.1 Trigonometric Functions.**Introduction.**

. Connection with p -adic fields. In p -adic fields, introduced by Kurt Hensel, trigonometric functions are defined. The connection between these and those obtained in finite fields has to be explored. To that effect, 2 programs have been written, padic.bas and sin.bas. The first program obtains the functions sin and cos for arguments which are congruent to 0 modulo p . For instance to 7^4

Example.

x	$\sin(x)$	$\cos(x)$	
$\frac{1}{2}$	0.4333	0.4343	1.0605
0.1	0.1011	1.0331	
0.2	0.2012	1.0562	
0.3	0.3062	1.0622	
0.4	0.4013	1.0655	
0.5	0.5062	1.0516	
0.6	0.6061	1.0344	
0.01	0.0100	1.0003	

Example.

In base 7 and 7^4 , we have for the elliptic case

y	$\sin(y)$	$\cos(y)$	$\sin(y)$	$\cos(y)$		
0	0	1	0.000	1.000	0.000	1.000
2	2	2	2.126	2.406	2.653	2.653
4	1	0	1.053	0.514	1.000	0.000
6	2	5	2.054	5.143	2.653	5.013
8	0	6	0.332	6.606	0.000	6.000
10	5	5	5.444	5.352	
12	6	0	6.631	0.614		
14	5	2	5.030	2.601		
16	0	1	0.101	1.033		

If we observe that

$$0.332 = -0.434 \text{ and } 6.606 = -1.060,$$

we get the first clue for the relation between the functions in the p -adic field and in base 7^4 .

For 13^n ,																	
x		$\sin(x)$								$\cos(x)$							
0.	0	0.	0	0	0	0	0	0	0	1.	0	0	0	0	0	0	0
0.	1	0.	1	0	2	2	11	9	10	1.	0	6	61	2	5	4	0
0.	2	0.	2	0	3	4	6	3	4	1.	0	11	12	4	4	12	8
0.	3	0.	3	0	2	6	9	3	6	1.	0	2	6	11	1	0	3
0.	4	0.	4	0	11	7	7	7	10	1.	0	5	12	1	5	9	0
0.	5	0.	5	0	3	9	3	12	5	1.	0	7	5	12	7	7	2
0.	6	0.	6	0	3	10	4	2	0	1.	0	8	11	1	4	8	10
0.	7	0.	7	0	10	10	9	1	1	1.	0	8	4	8	0	8	8
0.	$\frac{1}{2}$	0.	7	6	3					1.	0	8	11				
0.	8	0.	8	0	10	10	10	8	5	1.	0	7	10	5	4	0	7
0.	9	0.	9	0	2	10	6	9	8	1.	0	5	3	8	9	1	10
0.	10	0.	10	0	11	8	4	3	5	1.	0	2	9	4	10	11	8
0.	11	0.	11	0	10	6	7	3	10	1.	0	11	1	11	0	11	12
0.	12	0.	12	0	11	3	2	11	4	1.	0	6	7	5	1	10	3
0.	0 1	0.	0	1	0	0	0	2	2	1.	0	0	0	6	6	6	6
	$\frac{\pi}{6}$	7.	6	6	6	6	6	6	6	2.	4	3	4	6	1	7	5
	$\frac{\pi}{3}$	2.	4	3	4	6	1	7	5	7.	6	6	6	6	6	6	6
	$\frac{\pi}{2}$	1.	0	0	0	0	0	0	0	0.	0	0	0	0	0	0	0

Example.

p,first e,s%? 13,2,7

c% = 2

1	7	2	7.	0	2.	0
2	2	7	2.	0	7.	0
3	1	0	1.	0	0.	0
4	2	6	2.	0	6.	0

p,first e,s%? 169,2,137

c% = 41

1	137	41	137.	0	41.	0
2	80	150	80.	0	150.	0
3	1	91	1.	0	91.	0
4	2	45	2.	0	45.	0
5	163	50	163.	0	50.	0
6	13	168	13.	0	168.	0
7	58	37	58.	0	37.	0
8	11	162	11.	0	162.	0
9	168	65	168.	0	65.	0
10	76	98	76.	0	98.	0
11	149	28	149.	0	28.	0
12	143	1	143.	0	1.	0
13	85	54	85.	0	54.	0
14	67	33	67.	0	33.	0
15	1	117	1.	0	117.	0
16	15	97	15.	0	97.	0
17	46	63	46.	0	63.	0

18	39	168	39.	0	168.	0
19	110	24	110.	0	24.	0
20	24	110	24.	0	110.	0
21	168	39	168.	0	39.	0
22	63	46	63.	0	46.	0
23	97	15	97.	0	15.	0
24	117	1	117.	0	1.	0
25	33	67	33.	0	67.	0
26	54	85	54.	0	85.	0
27	1	143	1.	0	143.	0
28	28	149	28.	0	149.	0
29	98	76	98.	0	76.	0
30	65	168	65.	0	168.	0
31	162	11	162.	0	11.	0
32	37	58	37.	0	58.	0
33	168	13	168.	0	13.	0
34	50	163	50.	0	163.	0
35	45	2	45.	0	2.	0
36	91	1	91.	0	1.	0
37	150	80	150.	0	80.	0
38	41	137	41.	0	137.	0
39	1	0	1.	0	0.	0
40	41	32	41.	0	32.	0

Comment.

Using $s_1 = x$, $s_{2i+1} = s_i x^{2 \frac{(2i-1)^2}{2i(2i+1)}}$,

and $\arcsin(x) = s_1 + s_3 + \dots$,

$\arcsin(.7, 6, 6, 6, 6, 6, 6) = .7, 6, 9, 12, 9, 6, 5$

and

$\sin(.7, 6, 9, 12, 9, 6, 5) = .7, 6, 6, 6, 6, 6, 6 = (.1, 0, 0, 0, 0, 0, 0)$

modulo 169, at 13 we read 85 and 54 corresponding to

.76 and .24

hence $\frac{\pi}{6}$ correspond to $\arcsin(.7, 6, 6) = .7, 6, 9$ and p to .3, 0, 5, 11, 7, 1, 7

If we use the program `padic.bas` we can, given $\sin(\alpha)$ and $\cos(\alpha)$, obtained using 115a `n2adic`, determine $\sin(i\alpha)$ and $\cos(i\alpha)$.

For $p = 13$, using $\sin(\alpha) \equiv 7 \pmod{13}$, we get $(\pmod{p^3})$ all distinct values except $(0, 2, 5, 6, 7, 8, 11) \pmod{169 \pm 1}$.

The non zero numbers in the parenthesis are the non residues.

This indicates that the connection is tenuous.

Theorem.

12

If $s(1) \equiv g \pmod{p^n}$, where g is a primitive root of p , then ...

Let $s1 = c2 = \frac{1}{2} = 6.666\dots$, $c1 = s2 = \sqrt{\frac{3}{2}} = 2.12\dots$,

given ξ , determine $s = \sin(\xi)$, $c = \cos(\xi)$, in the p -adic field, $(\xi \equiv 0 \pmod{p})$,

determine,

$$s(i) = \sin(i\xi)cp(i) + \cos(i\xi)sp(i), \quad c(i) = \cos(i\xi)cp(i) - \sin(i\xi)sp(i).$$

(ξ was { control H - }?)

9.5.2 Integration.

Definition. 13

1. $Int_{2i}^{2j} \sin = \cos(2j) - \cos(2i).$
2. $Mid_{2i}^{2j} \sin = \sin(2i+1) + \sin(2i+3) + \dots + \sin(2j-1).$
3. $Trap_{2i}^{2j} \sin = \frac{1}{2}\sin(2i) + \sin(2i+2) + \dots + \sin(2j-2) + \frac{1}{2}\sin(2j).$
4. $Simpson_{2i}^{2j} \sin = \sin(2i) + 4\sin(2i+2) + 2\sin(2i+4) + 4\sin(2i+6) + \dots + 4\sin(2j-2) + \sin(2j).$

Theorem.

$$\begin{aligned} Int_{2i}^{2j} \sin &= -2\sin(1) Mid_{2i}^{2j} \sin \\ &= -2\tan(1) Trap_{2i}^{2j} \sin \\ &= -2\frac{\sin(2)}{2+\cos(2)} Simpson_{2i}^{2j} \sin. \end{aligned}$$

9.6 P-adic field.

9.6.1 Generalities.

Notation.

Writing $x = x_0 + x_1p + x_2p^2 + x_3p^3 + \dots$ in the form $x = x_0.x_1x_2x_3\dots$, we will also write

$$x \equiv x_0 \pmod{p}, \quad x \equiv x_0.x_1 \pmod{p^2}, \quad \dots$$

We have, for instance,

$$0.\frac{1}{2} = 0.7666666\dots$$

Example.

$p = 5$, up to p^6 ,

$$\frac{1}{2} = 3.22222, \text{ indeed, } 2 \cdot 3 = 6 \equiv 1 \pmod{5},$$

$$2(3.2) = 2.13 = 26 \equiv 1 \pmod{5^2}, \dots$$

$$-1/2 = 2.22222, \quad -1/2 = .22222, \quad -.01/2 = .02222.$$

Definition.

In the p -adic field, the *exponential, logarithmic and trigonometric functions* are defined by:

$$\exp(x) := 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \dots, \text{ for } |x| < \dots$$

$$\log(x) := x - \frac{1}{2}x^2 + \frac{1}{3}x^3 + \dots, \text{ for } |x| < \dots$$

$$\sin(x) := x - \frac{1}{3!}x^3 + \frac{1}{5!}x^5 - \dots, \text{ for } |x| \leq p^{-1}$$

$$\cos(x) := 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4 - \dots, \text{ for } |x| \leq p^{-1}.$$

Example.

$p = 5, x = 0.1,$	1	= 1.00000	00		x	= 0.10000	00
	x	= 0.10000	00		$-x^2/2$	= 0.02222	22
	$x^2/2$	= 0.03222	22		$x^3/3$	= 0.00231	31
	$x^3/1.1$	= 0.00140	40		$-x^4/4$	= 0.00011	11
	$x^4/4.4$	= 0.00044	34		$x^5/1$	= 0.00010	00
	$x^5/44$	= 0.00044	34		$-x^6/1.1$	= 0.00000	40
	$x^6/4301$	= 0.00004	03		$x^7/2.1$	= 0.00000	03
	$x^7/31031$	= 0.00000	24				
	$x^8/422422$	= 0.00000	04				
	$\exp(0.1)$	= 1.13341	24		$\log(1.1)$	= 0.12320	14
	x	= 0.10000	00		1	= 1.00000	00
	$-x^3/1.1$	= 0.00404	04		$-x^2/2$	= 0.02222	22
	$x^5/44$	= 0.00044	34		$x^4/4$	= 0.00044	34
	$-x^7/31031$	= 0.00000	30		$-x^6/1.1$	= 0.00001	41
	$\sin(0.1)$	= 0.10443	24		$x^8/422422$	= 0.00000	04
					$\cos(1.1)$	= 1.02213	03

Example.

For $p = 13$,

x	$\sin(x)$	$\cos(x)$
0. 1	0. 1 0 2 2 11 9 10,	1. 0 6 6 12 5 4 0
0. 2	0. 2 0 3 4 6 3 4,	1. 0 11 12 4 4 12 8
0. 3	0. 3 0 2 6 9 3 6,	1. 0 2 6 11 1 0 3
0. 4	0. 4 0 11 7 7 7 10,	1. 0 5 12 1 5 9 0
0. 5	0. 5 0 3 9 3 12 5,	1. 0 7 5 12 7 7 2
0. 6	0. 6 0 3 10 4 2 0,	1. 0 8 11 1 4 8 10
0. 7	0. 7 0 10 10 9 1 1,	1. 0 8 4 8 0 8 8
0. $\frac{1}{2}$	0. 7 6 3 0 5 5 7,	1. 0 8 1 10 0 1 0
0. 8	0. 8 0 10 10 10 8 5,	1. 0 7 10 5 4 0 7
0. 9	0. 9 0 2 10 6 9 8,	1. 0 5 3 8 9 1 10
0. 10	0. 10 0 11 8 4 3 5,	1. 0 2 9 4 10 11 8
0. 11	0. 11 0 10 6 7 3 10,	1. 0 11 1 11 0 11 12
0. 12	0. 12 0 11 3 2 11 4,	1. 0 6 7 5 1 10 3
0. 0 1	0. 0 1 0 0 0 2 2,	1. 0 0 0 6 6 6 6
0. 11 1	0. 11 1 10 4 10 9 1,	1. 0 11 3 3 10 11 1
0. 0 2	0. 0 2 0 0 0 3 4,	1. 0 0 0 11 12 12 12
0. 10 2	0. 10 2 11 12 2 1 8,	1. 0 2 2 1 1 3 3
0. 0 3	0. 0 3 0 0 0 2 6,	1. 0 0 0 2 6 6 6

Definition.

The *Chebyshev polynomials* are defined by the recurrence relation

$$T_{i+1}(x) := -T_{i-1}(x) + 2xT_i(x), i = 1, 2, \dots, \text{ with}$$

$$T_0(x) := 1, T_1(x) := x.$$

Definition.

For $p \equiv 1 \pmod{4}$, a root c_1 of T_i is called a *primitive root modulo p* , if all the roots of T_i ,

$$c_1, c_3, \dots, c_{2i-1}$$

can be obtained from it using the addition formulas,

$$c_1 := c_1, c_3 := 4c_1^3 - 3c_1, \quad c_{2i+1} := -c_{2i-3} + 2c_{2i-1}(2c_1^2 - 1), i = 2, \dots, i-1.$$

Example.

For $p = 13$, the roots of $T_3 = 4x^3 - 3x$ are 0, 2 and -2 . 2 and -2 are primitive roots.

If $c_1 = c_1 = 2$ then $c_3 = 0$, $c_5 = -2$.

For $p = 17$, $T_4(x) = 8x^4 - 8x^2 + 1$, which has the primitive roots 4, -4 , 6, -6 .

Notation.

For $p \equiv 1 \pmod{4}$, the roots of $T_{\frac{p-1}{4}}$ will be denoted,

$$\cos(\alpha), \cos(3\alpha), \dots, \cos\left(\frac{p-3}{2}\alpha\right).$$

with $\alpha = \frac{\pi}{\frac{p-1}{2}}$.

We will also define

$$\begin{aligned} \cos(0\alpha) &:= 1, \\ \cos(2k\alpha) &:= -\cos((2k-2)\alpha) + 2c_1\cos((2k-1)\alpha), \\ k &= 1, \dots, \frac{p-1}{4}. \\ \sin(k\alpha) &= \cos\left(\left(\frac{p-1}{4} - k\right)\alpha\right). \end{aligned}$$

Example.

For $p = 13$, $\alpha = \frac{\pi}{6}$, $\delta^2 = 2$,

(the lines $k = \frac{1}{2}, \frac{3}{2}, \dots$ will be explained in 1.1, 1.2),

$$k \quad \sin(k\alpha) \quad \cos(k\alpha)$$

0	0.	0	0	0	0	0	0	0	1.	0	0	0	0	0	0	0	
$\frac{1}{2}$	9.	7	1	1	0	9	12	0	δ	2.	1	8	7	6	2	6	7 δ
1	7.	6	6	6	6	6	6	6	2.	4	3	4	6	1	7	4	
$\frac{3}{2}$	6.	6	6	6	6	6	6	6	δ	6.	6	6	6	6	6	6	6 δ
2	2.	4	3	4	6	1	7	4	7.	6	6	6	6	6	6	6	
$\frac{5}{2}$	2.	1	8	7	6	2	6	7	δ	9.	7	1	1	0	9	12	0 δ
3	1.	0	0	0	0	0	0	0	0.	0	0	0	0	0	0	0	
$\frac{7}{2}$	2.	1	8	7	6	2	6	7	δ	4.	5	11	11	12	3	0	12 δ
4	2.	4	3	4	6	1	7	4	6.	6	6	6	6	6	6	6	
$\frac{9}{2}$	6.	6	6	6	6	6	6	6	δ	7.	6	6	6	6	6	6	6 δ
$\frac{5}{2}$	7.	6	6	6	6	6	6	6									
$\frac{11}{2}$	11.	11	4	5	6	10	6	5	δ								
6	0.	0	0	0	0	0	0	0									
$\frac{13}{2}$	12.	12	12	12	12	12	12	12	12								
7	4.	5	11	11	12	3	0	12	δ								
$\frac{15}{2}$	11.	11	4	5	6	10	6	5	δ								
8	6.	6	6	6	6	6	6	6									
$\frac{17}{2}$	11.	8	9	8	6	11	5	8	δ	7.	6	6	6	6	6	6	6 δ
9	11.	8	9	8	6	11	5	8	6.	6	6	6	6	6	6	6	
$\frac{19}{2}$	11.	11	4	5	6	10	6	5	δ	4.	5	11	11	12	3	0	12 δ
10	12.	12	12	12	12	12	12	12	0.	0	0	0	0	0	0	0	
$\frac{21}{2}$	11.	11	4	5	6	10	6	5	δ	9.	7	1	1	0	9	12	0 δ
11	11.	8	9	8	6	11	5	8	7.	6	6	6	6	6	6	6	
$\frac{23}{2}$	7.	6	6	6	6	6	6	6	δ	6.	6	6	6	6	6	6	6 δ
12	6.	6	6	6	6	6	6	6	2.	4	3	4	6	1	7	4	
	4.	5	11	11	12	3	0	12	δ	2.	1	8	7	6	2	6	7 δ
	0.	0	0	0	0	0	0	0	1.	0	0	0	0	0	0	0	

In this particular case, $\sin(\alpha) = \frac{1}{2}$, $\cos(\alpha) = \frac{\sqrt{3}}{2}$, are sufficient to obtain the entries 0, 1, 2, ..., 12, in the table.

We have therefore a first method of obtaining tables of trigonometric functions in a finite field¹⁴. We choose x , such that $|x| = p^{-1}$, therefore $|kx| \leq p^{-1}$. (If $|x| < p^{-1}$, primitivity is not insured. See 1.3.)

We compute $\sin(kx)$ and $\cos(kx)$ by Maclaurin series, (see 0.1.) and use the addition formulas $\sin(k(\alpha+x)) = \sin(kp\alpha)\cos(kx) + \cos(kp\alpha)\sin(kx)$, $\cos(k(\alpha+x)) = \cos(kp\alpha)\cos(kx) - \sin(kp\alpha)\sin(kx)$, where kp is $k \pmod{p}$.

Example.

For $p = 13$, and $x = 0.1$,

(The lines $k = \frac{1}{2}, \frac{3}{2}, \dots$ will be explained in 1.3).

k $\sin(k(\alpha+x))$

$\cos(k(\alpha+x))$

¹⁴12.10.82

$\frac{1}{2}$		9.	8	2	11	7	1	5	9	δ	2.	3	7	12	12	12	11	1	δ	
1		7.	8	0	4	3	7	4	5		2.	10	8	7	2	10	10	6		
$\frac{3}{2}$		6.	2	6	10	8	11	2	2	δ	6.	10	12	0	3	3	5	7	δ	
2		2.	5	12	3	5	5	1	0		7.	2	10	6	12	2	11	4		
$\frac{5}{2}$		2.	4	11	4	4	7	6	4	δ	9.	2	11	4	4	2	10	1	δ	
3		1.	0	2	6	11	1	0	3		0.	10	12	10	6	3	9	6		
$\frac{7}{2}$		2.	2	11	4	2	8	8	2	δ	4.	11	8	8	0	12	4	5	δ	
4		2.	2	0	11	5	1	11	10		6.	11	6	10	6	9	12	0		
$\frac{9}{2}$		6.	5	4	1	7	4	9	2	δ	7.	5	2	2	7	5	9	0	δ	
5		7.	9	8	12	12	9	1	1		11.	12	1	7	5	3	7	5		
$\frac{11}{2}$			9.	9	3	0	3	0	5	5	δ	11.	7	2	1	8	7	3	3	δ
6		0.	7	12	9	2	8	10	12		12.	12	4	1	11	8	4	2		
	0.	$\frac{1}{2}$	4.	5	10	4	8	7	1	10	δ	11.	11	2	9	10	12	1	2	δ
	7		6.	5	12	12	1	12	6	5		11.	5	0	5	11	0	7	5	
	2.	$\frac{1}{2}$	7.	0	0	4	6	1	11	11	δ	7.	12	5	8	7	11	2	6	δ
	8		11.	4	8	6	4	5	11	6		6.	9	3	2	8	6	8	1	
	4.	$\frac{1}{2}$	11.	6	8	1	3	6	3	2	δ	4.	9	6	0	7	10	12	2	δ
	9		12.	12	7	9	4	3	11	2		0.	9	0	2	10	6	9	8	
	6.	$\frac{1}{2}$	11.	12	8	7	3	11	6	6	δ	9.	0	11	7	11	0	9	2	δ
	10		11.	0	6	7	4	10	9	1		7.	0	10	7	2	3	6	0	
	8.	$\frac{1}{2}$	7.	4	5	9	12	6	4	3	δ	6.	4	0	12	2	12	2	12	δ
	11		6.	2	1	10	3	11	10	1		2.	3	6	11	0	10	4	12	
	10.	$\frac{1}{2}$	4.	2	7	8	9	4	10	4	δ	2.	7	6	7	7	12	9	11	
	12		0.	12	0	11	3	2	11	4		1.	0	6	7	5	1	10	3	
	11.	$\frac{1}{2}$	9.	6	3	1	9	11	1	4	δ	2.	12	5	5	0	2	9	11	
	0.		7.	6	8	10	12	0	7	10		2.	4	9	10	11	5	4	1	
	1.	$\frac{1}{2}$	6.	9	11	0	4	6	7	5	δ	6.	3	6	4	12	2	2	1	δ
	1.		2.	11	2	1	9	11	6	8		7.	4	3	4	3	6	1	11	
	3.	$\frac{1}{2}$	2.	8	3	4	5	2	3	6	δ	9.	4	2	4	12	3	0	9	δ
	2.		1.	0	11	10	10	7	2	5		0.	11	11	9	10	7	2	10	
	5.	$\frac{1}{2}$	2.	11	2	0	10	2	0	5	δ	4.	0	7	0	0	12	5	9	δ
	3.		2.	9	6	4	3	12	4	7		6.	0	4	6	9	10	2	9	
	7.	$\frac{1}{2}$	6.	11	2	0	2	12	9	0	δ	7.	11	4	4	1	12	8	3	δ
	4.		7.	11	9	3	11	12	4	10		11.	6	5	5	1	10	10	2	
	9.	$\frac{1}{2}$	9.	11	8	0	12	9	2	12	δ	11.	3	4	7	9	10	3	7	δ
	5.		0.	8	11	9	9	12	5	11		12.	12	5	12	7	1	5	7	
	11.	$\frac{1}{2}$	4.	7	7	12	11	6	6	4	δ	11.	2	5	1	12	10	10	3	δ
	6.		6.	7	1	6	3	1	8	4		11.	11	0	6	6	2	8	6	
	0.	$\frac{1}{2}$	7.	6	10	9	6	10	5	4	δ	7.	6	2	3	0	4	2	10	δ

A second method to obtain trigonometric tables in finite fields is to start with $\sin(\alpha)$ such that $x_0.x_1$ is a primitive root for p^2 and $\cos(\alpha) = \sqrt{1 - \sin^2(\alpha)}$ and use the addition formulas to obtain in succession

$\sin(k\alpha)$ and $\cos(k\alpha)$ for $k = 2, 3, \dots$. For instance, we have the following

Example.

For $q = 13^4$ and $\sin(\alpha) = 7.804$, then
 $\cos(\alpha) = 2.1087$, the period is 12.13^3 and

k	$\sin(k\alpha)$	$\cos(k\alpha)$							
1	7.	8	0	4	2.	10	8	7	
2	2.	5	12	3	7.	2	10	6	
3	1.	0	2	6	0.	10	12	10	
4	2.	2	0	11	6.	11	6	10	
5	7.	9	8	12	11.	12	1	7	
6	0.	7	12	9	12.	12	4	1	
7	6.	5	12	12	11.	5	0	5	
8	11.	4	8	6	6.	9	3	2	
9	12.	12	7	9	0.	9	0	2	
10	11.	0	6	7	7.	0	10	7	
11	6.	2	1	10	2.	3	6	11	
12	0.	12	0	11	1.	0	6	7	
0. 1	7.	6	8	10	2.	4	9	10	
11. 1	0.	11	1	10	1.	0	11	3	
0. 2	2.	4	4	4	7.	6	2	11	
10. 2	0.	10	2	11	1.	0	2	2	
0. 3	1.	0	0	0	0.	0	10	12	

Theorem.

If $\sinh(x) = x + \frac{1}{3!}x^3 + \frac{1}{5!}x^5 + \dots$, $|x| \leq p^{-1}$,
and $\cosh(x) = 1 + \frac{1}{2!}x^2 + \frac{1}{4!}x^4 + \dots$, $|x| \leq p^{-1}$,
then

$$\sin(xi) = i\sinh(x), \cos(xi) = \cosh(x),$$

Example.

With $p = 11$,

$$\sin(0. \frac{1}{2}i) = 0. 6 5 810 3 8 0 i, \cos(0. \frac{1}{2}i) = 1. 0 7 9 5 7 0 2.$$

$$\sin(0.1i) = 0. 1 0 2 9 0 9 6 i, \cos(0.1i) = 1. 0 6 5 0 5 9 6.$$

Example.

For $p = 11$ and $x = . 1$, Using 6.1.13 and

$$\sin(\frac{\alpha}{2}) = 9. 3 5 9 2 2 410 \text{ and } \cos(\frac{\alpha}{2}) = 5. 7 6 3 0 4 6 9 i,$$

$$\sin(\alpha) = 2.10 5 5 6 5 6 6 i \text{ and } \cos(\alpha) = 4. 919 3 8 7 9 4$$

of 1.6, we obtain

$$\sin((\frac{\alpha+1}{2})i) = 9. 6 910 9 2 1 0 i, \cos((\frac{\alpha+1}{2})i) = 5. 8 610 0 0 7 2, \sin((\alpha+1)i) = 2. 3 5 7 8 5 5 2 i,$$

$$\cos((\alpha+1)i) = 4. 0 1 210 6 810.$$

The table can be computed from the first values the second are used here as a check:

$$k \qquad \sin(k(\alpha+x)/2) \qquad \cos(k(\alpha+x)/2)$$

0. 0	0. 0	0 0 0 0 0 0 0 0	1. 0	0 0 0 0 0 0 0
1. 0	9. 6	9 10 9 2 1 0	5. 8	6 10 0 0 7 2 <i>i</i>
2. 0	2. 3	5 7 8 5 5 2 <i>i</i>	4. 0	1 2 10 6 8 10
3. 0	4. 6	5 4 8 0 9 8	2. 4	2 1 0 3 3 1 <i>i</i>
4. 0	5. 3	2 8 0 5 3 7 <i>i</i>	9. 2	5 0 0 9 10 5
5. 0	1. 0	10 9 8 0 6 4	0. 3	5 4 6 0 0 9 <i>i</i>
6. 0	5. 2	1 8 5 2 4 9 <i>i</i>	2. 0	4 10 4 9 10 0
7. 0	4. 5	10 1 4 2 6 8	9. 8	6 7 7 3 4 1 <i>i</i>
8. 0	2. 5	6 4 3 2 10 4 <i>i</i>	7. 9	8 2 0 10 10 8
9. 0	9. 9	4 10 3 10 1 9	6. 1	1 0 9 3 4 1 <i>i</i>
10. 0	0. 6	10 2 7 2 7 10 <i>i</i>	10. 10	3 4 6 3 9 9
0. 1	2. 7	2 5 3 7 0 2	6. 3	3 9 5 2 10 4 <i>i</i>
1. 1	9. 9	0 9 0 0 5 0 <i>i</i>	7. 0	10 5 5 7 2 7
2. 1	7. 3	9 9 9 5 4 8	9. 4	4 6 2 4 1 7 <i>i</i>
3. 1	6. 6	3 4 0 5 9 8 <i>i</i>	2. 5	2 6 2 7 4 1
4. 1	10. 10	8 9 6 0 8 7	0. 2	6 10 2 2 3 3 <i>i</i>
5. 1	6. 9	6 7 1 2 5 7 <i>i</i>	9. 7	2 7 3 2 10 8
6. 1	7. 6	5 9 9 7 0 2	2. 0	1 5 8 0 0 1 <i>i</i>
7. 1	9. 3	8 0 9 9 6 8 <i>i</i>	4. 2	4 4 1 4 9 10
8. 1	2. 9	5 8 7 1 7 6	5. 10	5 5 8 1 1 10 <i>i</i>
9. 1	0. 10	0 9 7 9 9 0 <i>i</i>	1. 0	6 4 6 8 8 6
10. 1	9. 0	1 8 8 0 2 7	5. 6	1 3 4 9 9 5 <i>i</i>
0. 2	2. 10	9 3 7 3 9 5 <i>i</i>	4. 9	1 3 5 1 9 6
1. 2	4. 8	9 5 5 6 3 4	2. 8	5 8 0 0 2 6 <i>i</i>
2. 2	5. 5	5 6 8 8 7 9 <i>i</i>	9. 8	5 0 3 10 3 2
3. 2	1. 0	8 5 3 9 2 5	0. 4	4 1 9 9 0 6 <i>i</i>
4. 2	5. 0	0 2 7 6 10 0 <i>i</i>	2. 6	7 10 3 4 0 6
5. 2	4. 3	1 0 4 4 6 5	9. 1	7 10 8 2 10 0 <i>i</i>
6. 2	2. 9	4 8 7 7 9 0 <i>i</i>	7. 7	3 6 9 3 10 7
7. 2	9. 4	10 6 3 3 0 7	6. 10	4 2 0 9 10 0 <i>i</i>
8. 2	0. 7	9 3 9 1 3 4 <i>i</i>	10. 10	2 6 8 4 8 8
9. 2	2. 2	1 2 3 7 1 10	6. 5	0 10 10 2 1 5 <i>i</i>
10. 2	9. 2	6 3 4 6 7 5 <i>i</i>	7. 2	7 6 0 1 10 3
0. 3	7. 1	3 0 7 10 10 1	9. 0	0 3 10 10 2 10 <i>i</i>
1. 3	6. 4	3 0 9 3 9 2 <i>i</i>	2. 10	2 3 7 6 3 0
2. 3	10. 10	4 9 7 9 9 0	0. 1	7 7 1 6 1 9 <i>i</i>
3. 3	6. 0	0 10 3 3 8 3 <i>i</i>	9. 1	9 3 1 1 6 3
4. 3	7. 8	1 5 1 4 6 8	2. 7	1 5 10 2 10 5 <i>i</i>
5. 3	9. 10	8 5 1 5 10 4 <i>i</i>	4. 4	0 1 0 4 5 2
6. 3	2. 3	1 0 6 0 8 0	5. 1	10 0 0 4 9 0 <i>i</i>
7. 3	0. 9	1 6 7 2 5 2 <i>i</i>	1. 0	2 7 9 4 0 2

9.6.2 Extension to the half argument.

Introduction.

The tables of trigonometric functions can be extended to the half arguments. These are required for the angles in finite Euclidean geometry.

Theorem.

If g is a primitive root of p , and $\delta^2 = g$, then $c1' = \cos(\alpha\frac{1}{2})\delta-1$ is a primitive root of

$$S'_{\frac{p-1}{2}} = T_{\frac{p-1}{2}} \circ (\delta I),$$

where I is the identity function.

Indeed, $T_{2n} = T_n \circ (2I^2 - 1)$. The other roots are denoted by $c2', c3', \dots$

Example.

For $p = 13$, $g = 2$,

$$S'_6 = 256I^6 - 192I^4 + 36I^2 - 1,$$

$c1' = \cos(\alpha\frac{1}{2})\delta-1 = 2.1876267$, from which we derive the values in 0.6. for $i = \frac{1}{2}, \frac{3}{2}, \dots, \frac{11}{2}$.

Comment.

The method given at the end of section 0.6. enables to complete the table of Example 0.7. Alternately, if g is a primitive root for p^2 , $p \equiv 1 \pmod{4}$, we know that g is a primitive root for p^e , $e = 3, 4, \dots$

If $\delta^2 = g$, $\sin(\alpha/2) = \delta\sqrt{\frac{1-\cos(\alpha)}{2g}}$ and $\cos(\alpha\frac{1}{2}) = \delta\sqrt{\frac{1+\cos(\alpha)}{2g}}$.

Example.

For $p = 13$,

$\sin(\alpha\frac{1}{2})\delta-1 = \sqrt{(3.774123104)} = 9.82117159\delta$, $\cos(\alpha\frac{1}{2})\delta-1 = \sqrt{(4.121117291)} = 2.371212111\delta$.

One of the signs of the square roots can be chosen arbitrarily, the other must be chosen in such a way that

$$\sin(\alpha) = 2g \sin(\alpha\frac{1}{2})\cos(\alpha\frac{1}{2}).$$

Theorem.

For $p \equiv -1 \pmod{4}$, with $\delta^2 = -1$,

$\cos(\alpha/2)\delta-1$ is a primitive root of

$$V_{\frac{p-3}{2}} = (T_{\frac{p-1}{2}} I^{-1}) \circ (\delta I).$$

$\sin(\alpha/2)$ is a primitive root of

$$U_{\frac{p-3}{2}} = (T_{\frac{p-1}{2}} I^{-1}) \circ \sqrt{1 - I^2}.$$

Example.

For $p = 11$, $\delta^2 = -1$, $\alpha = \frac{\pi}{5}$,

$$V_4 = 16I^4 + 20I^2 + 5,$$

with roots 5.7630469 and 2.10556566,

$$U_4 = 16I^4 - 12I^2 + 1,$$

with roots 9.35922410 and 4.91038794. Hence, k

$\sin(k\alpha)$

$\cos(k\alpha)$

0	0.	0	0	0	0	0	0	0	1.	0	0	0	0	0	0	0
$\frac{1}{2}$	9.	3	5	9	2	2	4	10	5.	7	6	3	0	4	6	9 δ
1	2.	10	5	5	6	5	6	6 δ	4.	9	10	3	8	7	9	4
$\frac{3}{2}$	4.	9	10	3	8	7	9	4	2.	10	5	5	6	5	6	6 δ
2	5.	7	6	3	0	4	6	9 δ	9.	3	5	9	2	2	4	10
$\frac{5}{2}$	1.	0	0	0	0	0	0	0	0.	0	0	0	0	0	0	0
3	5.	7	6	3	0	4	6	9 δ	2.	7	5	1	8	8	6	0
$\frac{7}{2}$	4.	9	10	3	8	7	9	4	9.	0	5	5	4	5	4	4 δ
4	2.	10	5	5	6	5	6	6 δ	7.	1	0	7	2	3	1	6
$\frac{9}{2}$	9.	3	5	9	2	2	4	10	6.	3	4	7	10	6	4	1 δ
5	0.	0	0	0	0	0	0	0,	10.	10	10	10	10	10	10	10,

Tables.

These can be found in the Handbook for Mathematical functions. Table 22.3 gives T and V and, by a simple transformation, S' . Table 22.5 gives U .

U and V can be obtained by recurrence:

$$U_0 = 1, U_2 = 4I^2 - 1, U_{2i+2} = 2(2I^2 - 1)U_{2i} - U_{2i-2}.$$

$$V_0 = 1, V_2 = 4I^2 + 3, V_{2i+2} = 2(2I^2 + 1)V_{2i} - V_{2i-2}.$$

We have

$$p = 5, g = 2, S'_2 = 4I^2 - 1,$$

$$c_2 = s_1 = 2. \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2, c_1 = 2. \ 2 \ 2 \ 2 \ 2 \ 2 \ 2 \ 2.$$

$$p = 7, U_2 = 4I^2 - 1, s_1 = 4. \ 3 \ 3 \ 3 \ 3 \ 3 \ 3 \ 3,$$

$$V_2 = 4I^2 + 3, c_1 = 1. \ 6 \ 3 \ 6 \ 2 \ 1 \ 4 \ 0.$$

$$p = 11, U_4 = 16I^4 - 12I^2 + 1, s_1 = 9. \ 3 \ 5 \ 9 \ 2 \ 2 \ 4 \ 10.$$

$$V_4 = 16I^4 + 20I^2 + 5, c_1 = 5. \ 7 \ 6 \ 3 \ 0 \ 4 \ 6 \ 9.$$

$$p = 13, g = 2, S'_6 = 256I^6 - 192I^4 + 36I^2 - 1,$$

$$c_3' = s_1 = 9. \ 7 \ 1 \ 1 \ 0 \ 9 \ 12 \ 0, c_1' = c_1 = 2. \ 1 \ 8 \ 7 \ 6 \ 2 \ 6 \ 7.$$

$$p = 17, g = 3, S'_8 = 10368I^8 - 6912I^6 + 1440I^4 - 96I + 1,$$

$$c_5' = s_1 = 10. \ 8 \ 8 \ 4 \ 3 \ 5 \ 14 \ 1, c_1' = c_1 = 5.15151513 \ 2 \ 3 \ 9.$$

$$p = 19, U_8 = 256I^8 - 448I^6 + 240I^4 - 40I^2 + 1,$$

$$s_1 = 14.13 \ 0 \ 6 \ 18 \ 9 \ 118,$$

$$V_8 = 256I^8 + 576I^6 + 432I^4 + 120I^2 + 9,$$

$$c_1 = 9.101611 \ 6 \ 15 \ 12 \ 1.$$

Comment.

The following values may be useful,

$$\sqrt{-1}_5 = 2. \ 1 \ 2 \ 1 \ 3 \ 4 \ 2 \ 3 \ 0 \ 3 \ 2$$

$$\sqrt{-1}_{13} = 5. \ 5 \ 1 \ 0 \ 5 \ 5 \ 1 \ 0 \ 1 \ 8 \ 8,$$

$$\sqrt{-1}_{17} = 4. \ 2 \ 10 \ 5 \ 12 \ 16 \ 12 \ 8 \ 13 \ 3 \ 14,$$

$$\sqrt{-1}_{29} = 12. \ 1 \ 12 \ 118 \ 16 \ 15 \ 3 \ 92 \ 425.$$

9.6.3 The logarithm.**Definition.**

The *exponentiaonal function* and the *logarithmic function* are defined by the following p -adic expansion.

$$\text{D.0.} \quad \exp(x) = 1 + x + \dots + \frac{1}{n!}x^n + \dots, |x| < 1.$$

$$\text{D.1.} \quad \log(1+x) = x - \frac{1}{2}x^2 + \dots + (-1)^n \frac{1}{n}x^n + \dots, |x| < 1.$$

The classical theorem is (See for instance Koblitz, 1977.)

Theorem.

...

Motivation.

For $p = 5$,

$$\log(-4) = \log(1-5) = 0.41041,$$

$$\log(1.1) = \log(1+5) = 0.12420,$$

$$\log(-4.1) = \log(1-10) = 0.32314.$$

If we want $\log(xy) = \log(x) + \log(y)$ to hold, we have 3 equations to determine $\log(-1)$, $\log(2)$ and $\log(3)$. $\log(1.3)$ and $\log(-4.4)$ can be used as check. This gives

$$\log(-1) = 0,$$

$$\log(2) = 0.23240,$$

$$\log(3) = 0.43134.$$

Clearly we now have a function which is not a bijection, for instance,

$$\log(1.20230) = 0.23420.$$

This suggest that we can extend the range of definition of the logarithm function. The equation $x^{p-1} \equiv 1 \pmod{p}$ has $p-1$ roots, $1, 2, \dots, p-1$, therefore the equation $x^{p-1} = 1$ has $p-1$ roots in the p -adic field, with first digit $1, 2, \dots, p-1$.

In general the roots are $1, x1, x2, \dots, -x2, -x1, -1$.

Algorithm.

If g is a primitive root in Z_p , the corresponding primitive root $g' \in \dots$ can be obtained by Newton's method:

$$y := g,$$

$$y = y - \frac{1}{\frac{p-1}{2}} \left(y + \frac{1}{y} \right)^{\frac{p-3}{2}} \text{ for } i = 1 \text{ to } n.$$

Theorem.

Algorithm 9.6.3 determines the first $2n$ digits of g' .

Theorem.

Given a prime p , a primitive root $g \in Z_p$ and x , H0. $|x| = 1$,

$$\text{D0.} \quad x0 = \text{ind}(\text{int}(x)),$$

where ind is the index function in Z_p associated to g ,

$$\text{D1.} \quad y := x/g^{x0} - 1$$

$$\text{D2.} \quad z := y - \frac{1}{2}y^2 + \dots + \frac{1}{n}(-y)^n$$

then

$$\text{C0.} \quad |z| < 1.$$

$$\text{C1.} \quad \log_{p,g}(x) = \{x0, z\}$$

Example.

For $p = 5$, $x1 = 2.1213423$.

(All the roots are 1, 2 .1213423, $-2.1213423 = 3.3231021$, $-1 = 4.4444444$)

For $p = 7$, $x1 = 2.4630262$, $x2 = 3.4630262$.

For $p = 11$, $x1 = 2.10\ 4\ 9\ 1\ 2\ 3\ 9$, $x2 = 3.\ 0\ 1\ 2\ 3\ 610\ 8$,
 $x3 = 4.\ 7\ 9\ 5\ 2\ 9\ 8\ 0$, $x4 = 5.\ 2\ 5\ 1\ 7\ 8\ 510$.

For $p = 13$, $x1 = 2.\ 6\ 2\ 2\ 4\ 2\ 5\ 8$, $x2 = 3.11\ 6\ 9\ 7\ 2\ 4\ 4$,
 $x3 = 4.11\ 6\ 9\ 7\ 2\ 4\ 4$, $x5 = 5.\ 5\ 1\ 0\ 5\ 5\ 1\ 0$
 $x6 = 6.\ 1\ 910\ 3\ 5\ 6\ 4$.

For $p = 17$, $x1 = 2.\ 9\ 312\ 914\ 1\ 5$, $x2 = 3.13\ 2\ 3\ 011\ 4\ 0$,
 $x3 = 4.\ 210\ 5121612\ 8$, $x4 = 5.\ 9\ 0\ 516\ 9\ 1\ 5$,
 $x5 = 6.\ 214\ 4\ 1\ 6\ 2\ 3$, $x6 = 7.\ 4\ 216\ 11514\ 2$,
 $x7 = 8.\ 6\ 1\ 415\ 116\ 2$.

For $p = 19$, $x1 = 2.\ 614\ 414131014$, $x2 = 3.16\ 7\ 8161815\ 1$,
 $x3 = 4.\ 51717\ 5\ 614\ 0$, $x4 = 5.\ 3\ 3131113\ 716$,
 $x5 = 6.12\ 21714181716$, $x6 = 7.15\ 7\ 0\ 118\ 0\ 4$,
 $x7 = 8.15\ 7\ 0\ 118\ 0\ 4$, $x8 = 9.\ 118\ 21712\ 5\ 1$.

For $p = 23$, $x1 = 2.11211015\ 2\ 912$, $x2 = 3.\ 51717\ 71821\ 7$,
 $x3 = 4.2122\ 4\ 7\ 81622$, $x4 = 5.\ 1\ 219\ 8\ 2\ 919$,
 $x5 = 6.201517\ 114\ 720$, $x6 = 7.1519\ 5\ 8\ 81519$,
 $x7 = 8.171710171911\ 3$, $x8 = 9.\ 713\ 1\ 7191512$,
 $x9 = 10.11\ 72112221517$, $x10 = 11.\ 81017\ 3\ 31922$.

The logarithmic functions as defined is not one to one. $p - 1$ arguments give the same value. To make it one to one we give the following

Definition.

Given a primitive root g ,

$$\log_{p,g}(x) = \{i0, x0, \log_p(x)\},$$

$$i0 \in (Z, +), x0 \in (Z_{p-1}, +), \log_p(x) \in \dots$$

where

$|x| = p^{-i0}$, $g^{x0} = \text{int}(x)$, and $\log_p(x)$ is the p -adic logarithm.

$i0$ is called the *characteristic*, $x0$, the *index* and $\log_p(x)$, the *mantissa*.

Example.

For $p = 5$ and $g = 2$,

$$\log_{5,2}(1.0000000) = \{0, 0\}, \log_{5,2}(2.1213423) = \{1, 0\},$$

$$\log_{5,2}(3.3231021) = \{3, 0\}, \log_{5,2}(4.4444444) = \{2, 0\}.$$

Theorem.

H0. $|x|, |y| = 1$.

C0. $\log_{p,g}(x * y) = \log_{p,g}(x) + \log_{p,g}(y)$.

Problem.

Extend the definition to allow $|x|$, $|y|$ to be anything using the relation C.0. and the idea of mantissa.

9.6.4 P-adic Geometry and Related Finite Geometries.**Introduction.**

Some thought on finite geometry for different powers of p and the p -adic geometry.

Given p , if we take the points on a line, with coordinates of the form $x0. \dots$ these are indistinguishable if we use the p -adic valuation to the precision 1.

If we consider the points $x0.x1$, these are distinguishable to the precision 1 but not to the precision $\frac{1}{p}$.

They can be considered, if p is 5 say, to have a color associated to the various digits of $x0$ the colors “purple, blue, green, yellow, orange, red.” As we proceed to the next digit all yellows become sub-colours proceeding from yellow to orange.

We can with more discrimination distinguish them. We can proceed further \dots

We observe also that, in this scheme of things, what is a shade of yellow for one is a shade of green for some one else. This is associated to a change of origin.

When this is transfered to angles this will give different trigonometric tables associated to different values of x .

Comment.

15

The trigonometric functions work as follows.

In the hyperbolic case,

for p , the period is $2(p-1)$,

for p^2 , the period is $2p(p-1)$, \dots

The factor 2 corresponds to the fact, that just as in Euclidean geometry the total angle is 2π , lines which form an angle π correspond to the same direction.

For the hyperbolic case, there are 2 real isotropic points,

There are on the ideal line

$p+1$ points,

$p-1$ ideal (non isotropic) points for the p -geometry,

p^2-1 ideal points for the p^2 -geometry, of which p^2-p are not included in the preceding set.

The hyperbolic trigonometry associated to p^2 is presumably for these p^2-p directions \dots

For the elliptic case, the period is $2(p+1)$ as one would expect for the p -geometry.

For the p^2 case, the period of the trigonometric functions is p^2+p . I do not yet understand how this comes into the picture.

Definition.

16

 p -ADIC GEOMETRY

Let $p \equiv -1 \pmod{4}$, let $z=0$ be the ideal line, let $x^2+y^2=z^2$ be a circle. There are no solutions of $x^2+y^2=0$, therefore the isotropic points are not real.

¹⁵19.10.82

¹⁶21.10.82

If $z \neq 0$, then we can normalize using $z = 1$, consider
 Let $|x| \geq |y|$. If $|x| > 1$ then there are no solutions.
 (Hint: divide by $p^{|x|}$ and work modulo p)

$$x^2 + y^2 = 1.$$

Lemma.

If $s = \sin(\alpha)$ is a root of ... then
 $\sin(p\alpha) = \sin(\alpha)$, $\cos(p\alpha) = \cos(\alpha)$.

Theorem.

Let $s = \sin(\alpha)$ be a root of

If $|\sin(\beta) - \sin(\alpha)| < 1$ then

$$\lim_{n \rightarrow \infty} \sin(p^n \beta) = \sin(\alpha).$$

If $|x| = 1$, there are solutions, $x = x_0.x_1x_2 \dots$. Let $|x_0|$ be a primitive solution of the polynomial

let x_1 . be

To x corresponds the pair $(x, y) = (\sin(\alpha), \cos(\alpha))$,

Let $X(x) = \sin(p\alpha)$, then the sequence $x, X(x), X^2(x), \dots$ converges to x' . Moreover x' is a root of ...

Example.

$p = 11$, let $x = \sin(\alpha) = 3$, $X(3.0000000) = 3.02801146$,

$$\cos(p\alpha) = 10.103125741,$$

$$X(3.0200000) = 3.026071212,$$

$$X(3.0260000) = 3.02676122,$$

$$X(3.0267000) = 3.026712112,$$

$$X(3.02671200) = 3.026712121,$$

$$X(3.026712120) = 3.026712122.$$

$p = 11$, elliptic case, $g = -1$

The following is a table of \sin , with $\sin(k = (2l + 1)\alpha)\delta^{-1}$, $\sin(k = 2l\alpha)$

[illegible]

Chapter 10

DIFFERENTIAL EQUATIONS AND FINITE MECHANICS

10.0 Introduction.

In the context of Finite Geometry, we should examine the subject of Differential Equations, their approximation and the application to finite mechanics.

I will describe the first success associated with the harmonic polygonal motion, then . . .

10.1 The first Examples of discrete motions.

10.1.1 The harmonic polygonal motion.

Introduction.

In classical Euclidean geometry as well as in finite Euclidean geometry I define the harmonic polygonal motion as the motion which associates to linearly increasing time successive points of the harmonic polygon. I will determine, for the classical case, the differential equation of the motion, by considering first points which are close to each other 10.1.1. I will then prove that this equation is satisfied when points are not close to each other 10.1.1. The equation bears resemblance with the equation of Kepler. Because the method uses derivatives of functions of the trigonometric functions only and in view of the method of Hensel for p -adic functions, the result extend automatically to the finite case.

Definition.

Given a conic

0. $A(E) = (a\cos(E), b\sin(E), 1)$,
and the point of Lemoine $K = (q, 0)$, given the correspond harmonic polygon of Casey (g2734, p.5 . . .), A_i , we define the *harmonic polygonal motion* by
1. $A(E(t_0 + i h)) = A_i$.

Theorem.

Let

0. $r = \frac{q}{a}$,
if h is small, the motion satisfies the differential equation

1. $C DE = 1 - r \cos(E)$,
for some constant of integration C .

Proof: The polar k of K is

2. $k = [\frac{q}{a^2}, 0, -1]$,

the polar $a(E)$ of $A(E)$ is

3. $a(E) = [\frac{\cos(E)}{a}, \frac{\sin(E)}{b}, -1]$,

it meets k at

4. $B(E) = (a^2 \sin(E), b(q - a \cos(E)), q \sin(E))$.

the condition that $A_{i-1} \times A_{i+1}$ passes through $B(E(t))$ gives

$$5. \begin{vmatrix} a^2 \sin(E(t)) & b(q - a \cos(E(t))) & q \sin(E(t)) \\ a \cos(E(t-h)) & b \sin(E(t-h)) & 1 \\ a \cos(E(t+h)) & b \sin(E(t+h)) & 1 \end{vmatrix} = 0.$$

Let

6. $s(t) = \frac{1}{2}(E(t+h) + E(t-h))$, $d(t) = \frac{1}{2}(E(t+h) - E(t-h))$, then to the second order in h ,
with $k = \frac{1}{2}h^2$,
 $s = E + kD^2E$, $d = hDE$,

7. $\cos(s) = \cos(E) - k \sin(E)D^2E$, $\sin(s) = \sin(E) + k \cos(E)D^2E$, $\cos(d) = 1 - k(DE)^2$.

Replacing the determinant by that obtained by using instead of the last 2 lines their half sum and their half difference, gives after division of the first row and first column by a and the second column by b ,

$$\begin{vmatrix} \sin(E) & r - \cos(E) & r \sin(E) \\ \cos(s)\cos(d) & \sin(s)\cos(d) & 1 \\ -\sin(s)\sin(d) & \cos(s)\sin(d) & 0 \end{vmatrix} = 0.$$

Dividing the last row by $\sin(d)$ and expanding with respect to the first row gives, after changing sign,

8. $\sin(E)\cos(s) + (r - \cos(E))\sin(s) - r\sin(E)\cos(d) = 0$,

or, after using 7 and dividing by k ,

9. $(1 - r\cos(E))D^2E = r\sin(E)(DE)^2$,

integrating gives 1, with some appropriate constant C ,

10. $(1 - e\cos(E))DE = C$. This is tantalizing close to Kepler's equation.

Theorem.

The harmonic polygonal motion associated to the point of Lemoine $(r, a, 0, 1)$ is described on the ellipse by the differential equation

$$0. \quad CDE = 1 - r \cos(E).$$

Proof: We have to show that if we take the derivative of the relation between 3 points equidistant in time, namely 10.1.1.8, this derivative is 0 if the differential equation 0. is satisfied. We can assume that $C = 1$.

From 0 and from 10.1.1.6. follows

$$1. \quad Ds = 1 - \frac{1}{2}r(\cos(E(t+h)) + \cos(E(t-h))) \\ = 1 - r\cos(s)\cos(d),$$

$$2. \quad Dd = -\frac{1}{2}r(\cos(E(t+h)) - \cos(E(t-h))) \\ = r\sin(s)\sin(d).$$

Taking the derivative of 10.1.1.8, gives

$$\cos(s)\cos(E)(1 - r\cos(E)) - \sin(s)\sin(E)(1 - r\cos(s)\cos(d)) \\ + \sin(s)\sin(E)(1 - r\cos(E)) + \cos(s)(r - \cos(E))(1 - r\cos(s)\cos(d)) \\ - r\cos(d)\cos(E)(1 - r\cos(E)) + r^2\sin(s)\sin(E)\sin(d)^2.$$

We would like to prove that this expression is identically zero. 0, gives

$$3. \quad r\cos(d) = \cos(s) + \sin(s)\frac{r - \cos(E)}{\sin(E)}, \text{ substituting in the expression gives} \\ \cos(s)\cos(E)(1 - r\cos(E)) \\ - r\sin(s)\sin(E)\cos(E) + \cos(s)(r - \cos(E)) \\ + r^2\sin(s)\sin(E) \\ + (\sin(s)\cos(s)\sin(E) - r\cos^2(s) + \cos^2(s)\cos(E) - \cos(E) \\ + r\cos^2(E))(\cos(s) + \sin(s)\frac{r - \cos(E)}{\sin(E)}) \\ - \sin(s)\sin(E)(\cos(s) + \sin(s)(r - \cos(E)))/\sin(E)^2.$$

$$\text{The coefficient of } r^2 \text{ is} \\ \sin(s)\sin(E) + \frac{(\cos^2(E) - \cos^2(s))\sin(s)}{\sin(E)} - \frac{\sin^3(s)}{\sin(E)} \\ = \frac{\sin(s)(\sin^2(E) + \cos^2(E) - \cos^2(s) - \sin^2(s))}{\sin(E)} = 0.$$

The coefficient of r is

$$-\cos(s)\cos^2(E) - \sin(s)\sin(E)\cos(E) + \cos(s) \\ + (\cos(s) - \sin(s)\frac{\cos(E)}{\sin(E)})(\cos^2(E) - \cos^2(s)) \\ + \sin(s)(\sin(s)\cos(s)\sin(E) + \cos^2(s)\cos(E) - \cos(E))/\sin(E) \\ - 2\sin(s)\sin(E)(\cos(s) - \sin(s)\cos(E)/\sin(E))\sin(s)/\sin(E) \\ = \sin(s)(-\cos^3(E) + \cos(E)\cos^2(s) - \cos(E) + \sin(s)\cos(s)\sin(E) \\ + \cos^2(s)\cos(E) - 2\cos(s)\sin(s)\sin(E) + 2\sin^2(s)\cos(E))/\sin(E) \\ - \cos(s)\cos^2(E) - \sin(s)\sin(E)\cos(E) + \cos(s) + \cos(s)\cos^2(E) - \cos^3(s) \\ = \sin(s)(\cos(E)(-\cos^2(E) + \cos^2(s) - 1 + \cos^2(s) + 2\sin^2(s))/\sin(E) \\ - \sin(s)\sin(E)\cos(E) - \sin(s)\sin(E)\cos(E) + \cos(s)\sin^2(s) \\ = \sin(s)\cos(E)\sin(E) - \sin^2(s)\cos(s) - \sin(s)\sin(E)\cos(E) + \cos(s)\sin^2(s) = 0.$$

The term independent of r is

$$\cos(s)\cos(E) - \cos(s)\cos(E) \\ + (\sin(s)\cos(s)\sin(E) + \cos^2(s)\cos(E) - \cos(E)) \\ (\cos(s) - \sin(s)\cos(E)/\sin(E)) \\ - \sin(s)\sin(E)(\cos(s) - \sin(s)\cos(E)/\sin(E))^2$$

$$\begin{aligned}
&= (\cos(s) - \sin(s)\cos(E)/\sin(E)) \\
&\quad (\sin(s)\cos(s)\sin(E) + \cos^2(s)\cos(E) - \cos(E) - \sin(s)\cos(s)\sin(E) \\
&\quad + \sin^2(s)\cos(E)) = 0.
\end{aligned}$$

Theorem. 1

Let $e'^2 = 1 - e^2$, then

$$0. \quad e' \tan(\tfrac{1}{2}e'M) = (1 + e) \tan(\tfrac{1}{2}E).$$

Theorem.

$$0. \quad \text{If } t(M) = \tan(\tfrac{1}{2}E) \text{ and }^2$$

$$1. \quad k = \frac{e+1}{e-1},$$

$$2. \quad t'_i = \sqrt{-kt}(M_i),$$

then

$$3. \quad t'_{1+2} = \frac{t'_1 + t'_2}{1 - t'_1 t'_2}.$$

Example.

For $p = 13$ and $e = 2$, $k = 3$ and

M	0	1	2	3	4	5	6	7	8	9	10	11	12
$t(M)$	0	1	7	11	8	4	∞	9	5	2	6	12	0
t'_M	0	6	3	1	-4	-2	∞	2	4	-1	-3	-6	0
$\frac{1}{2}E$	0	3	7	1	4	6	8	11	5	9			

For $p = 13$ and $e = 3$, $k = 2$ and

M	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$t(M)$	0	2	12	4	8	7	3	∞	10	6	5	9	1	11
$\frac{1}{2}E$	0													

Programs.

The programs pl.bas and planet.bas ...

Exercise.

Prove that the acceleration is

$$\frac{1-r \cos E}{C^2} (-(a \cos E, b \sin E, 0) + r(a \cos(2E), b \sin(2E), 0))$$

10.1.2 The Parabolic Motion.

Introduction.

The parabola has been studied in g33. Galileo Galilei was the first to show that the motion of a particle in a uniform gravitational field is a parabola. (Love, p.45) The result extend to the finite case.

¹26.6.83

²29.6.83

Theorem.

In both the infinite and finite cases, the solution of

$$mD^2x = 0 \text{ and } mD^2y = -mg$$

is

$$\begin{aligned} x(t) &= v_0 t, \quad y(t) = -\frac{1}{2}gt^2 + v_1 t, \text{ or} \\ y &= ax^2 + bx, \text{ with} \\ a &:= -\frac{g}{2v_0^2}, \quad b := \frac{v_1}{v_0}. \end{aligned}$$

Proof: Comparing the equation in the form

$$(x + \frac{b}{2a})^2 = \frac{y}{a} + (\frac{b}{2a})^2.$$

with the standard equation $y^2 = 4cx$ shows that the vertex V and the directrix d are

$$V = (\frac{b}{2a}, (\frac{b}{2a})^2),$$

$$d: y = \frac{v_0^2 + v_1^2}{2g} = \frac{v^2}{2g}$$

corresponding to the Torricelli law.

Example.

For $p = 7$, $g = 1$ and $v_0 = v_1 = 4$, then $a = -2$, $b = 1$,

$$y(x) = -2x^2 + x = 1 - 2(x - 2)^2,$$

x	0	1	2	3	-3	-2	-1	0
y	0	-1	1	-1	0	-3	-3	1
z	1	1	1	1	1	1	1	0
t	0	2	-3	-1	1	3	-2	

10.1.3 Attempts to Generalize Kepler's Equation.**Introduction.**

I have made many attempts to generalize Kepler's equation or the simple planetary motion to the finite case. In section ... , I examine the use of p -adic function to obtain a solution in the neighbourhood of a circular motion.

10.1.4 The circular motion.**Definition.**

The *circular motion* is defined by

$$x(t) = \cos(t), \quad y(t) = \sin(t),$$

$$Dx(t) = -\sin(t), \quad Dy(t) = \cos(t).$$

This assumes that the unit of distance is chosen as the radius of the circle and the unit of time is chosen in such a way that the period is 2π .

10.2 Approximation to the Solution of Differential Equations.

10.2.0 Introduction.

To approximate the solution of differential equations it is important to insure that essential properties are preserved. In particular, for conservative systems, the same should hold. In this connection, I developed in 1956 a method of first order and a method of second order which are contact transformations and therefore preserve the essential properties of conservative systems. These will be applied to the finite case.

10.2.1 Some Algorithms.

Algorithm.

The first order algorithm is defined by

Theorem.

Algorithm.

The second order algorithm for the solution of the differential equation

$$D^2\mathbf{x} = \mathbf{f} \circ \mathbf{x}, \mathbf{x}(0) = \mathbf{x}_0, D\mathbf{x}(0) = D\mathbf{x}_0,$$

is defined by

$$\mathbf{x}_{i+1} = \mathbf{x}_i + hD\mathbf{x}_i + \frac{1}{2}h^2\mathbf{f}_i, D\mathbf{x}_{i+1} = D\mathbf{x}_i + \frac{1}{2}h(\mathbf{f}_{i+1} + \mathbf{f}_i),$$

where

$$\mathbf{f}_i := \mathbf{f}(\mathbf{x}_i).$$

Definition.

A mapping is reversible iff

Theorem.

Given the Algorithm 10.2.1, the mapping is reversible.

Proof: If we solve for \mathbf{x}_i and $D\mathbf{x}_i$, we get

$$\begin{aligned} D\mathbf{x}_i &= D\mathbf{x}_{i+1} - \frac{h}{2}(\mathbf{f}_{i+1} + \mathbf{f}_i), \\ \mathbf{x}_i &= \mathbf{x}_{i+1} - hD\mathbf{x}_i - \frac{1}{2}h^2\mathbf{f}_i, \\ &= \mathbf{x}_{i+1} - hD\mathbf{x}_{i+1} + \frac{1}{2}h^2(\mathbf{f}_i + \mathbf{f}_{i+1}). \end{aligned}$$

Definition.

A mapping is symplectic iff

Theorem.

The mapping defined in algorithm 10.2.1 is symplectic.

Proof:

Example.

Let x and f be one dimensional, let

$$f(x) = -x - 2x^3,$$

let $Dx_0 = 0$, we have the following solutions, for $h = 1$ and various initial conditions $(x(0), Dx(0) = 0)$.

$p = 11,$									
i	0	1	2	3	4	5	6	7	8
$(x, Dx)_i$	1, 0	5, 3	-4, 2	-2, 0	-4, -2	5, -3	1, 0		
	3, 0	2, 1	5, 2	-5, 2	-2, 1	-3, 0	-2, -1	-5, -2	5, -2
	4, 0	4, 0							
	5, 0	4, -1	3, -2	0, -3	-3, -2	-4, -1	-5, 0	-4, 1	-3, 2
$p = 13,$									
i	0	1	2	3	4	5	6	7	8
$(x, Dx)_i$	1, 0	6, -6	2, 0	6, 6	1, 0				
	3, 0	-6, 2	-6, -2	3, 0					
	4, 0	3, 3	-3, 3	-4, 0	-3, -3	3, -3	4, 0		
	5, 0	1, 1	-6, 4	-4, 3	0, 4	4, 3	6, 4	-1, 1	-5, 0
	6, 0	-5, 6	5, 6	-6, 0	5, -6	-5, -6	6, 0		

Theorem.

If we apply the mapping 10.2.1 to

$$D^2x = -x, x(0) = 0, Dx(0) = 1,$$

we obtain, up to a scaling factor the trigonometric functions.

Example.

With $p = 13$ and $h = 1$,

i	0	1	2	3	4	5	6	7	
		8	9	10	11	12	13	14	
$(x, Dx)_i$	0, 1	1, -5	3, -3	-5, -4	-5, 4	3, 3	1, 5	0, -1	
$?(\delta x, Dx)((i) = (sin, cos)(-10i), \text{ if } sin(1) = 3 \text{ and } cos(1) = 3\delta, \text{ with } \delta^2 = 2.$									

Program.

[130] PENDUL(um)

10.3 The Parabolic Motion.

10.3.0 Introduction.

The parabola has been studied in g33. Galileo Galilei was the first to show that the motion of a particle in a uniform gravitational field is a parabola. (Love, p.45) The result extend to the finite case.

Theorem.

In both the infinite and finite cases, the solution of

$$mD^2x = 0 \text{ and } mD^2y = -mg$$

is

$$x(t) = v_0 t, \quad y(t) = -\frac{1}{2}gt^2 + v_1 t, \text{ or}$$

$$y(x) = ax^2 + bx, \text{ with}$$

$$a := \frac{g}{2v_0^2}, \quad b := \frac{v_1}{v_0}.$$

Proof: Comparing the equation in the form

$$(x - \frac{b}{2a})^2 = -\frac{(y - \frac{b^2}{4a})}{a}$$

with the standard equation $y^2 = 4cx$ shows that the vertex V and the directrix d are

$$V = (\frac{b}{2a}, \frac{b^2}{4a}),$$

$$d : y = \frac{v_0^2 + v_1^2}{2g} = \frac{v^2}{2g}$$

corresponding to the Torricelli law.

Example.

For $p = 7$, $g = 1$ and $v_0 = v_1 = 4$,

$$y(x) = -2x^2 + x,$$

x	0	1	2	3	-3	-2	-1	0
y	0	-1	1	-1	0	-3	-3	1
z	1	1	1	1	1	1	1	0
t	0	2	-3	-1	1	3	-2	

10.4 Attempts to Generalize Kepler's Equation.

Introduction.

I have made many attempts to generalize Kepler's equation or the simple planetary motion to the finite case. In section ... , I examine the use of p -adic function to obtain a solution in the neighbourhood of a circular motion.

10.4.1 The circular motion.

Definition.

The *circular motion* is defined by

$$x(t) = \cos(t), \quad y(t) = \sin(t),$$

$$Dx(t) = -\sin(t), \quad Dy(t) = \cos(t).$$

This assumes that the unit of distance is chosen as the radius of the circle and the unit of time is chosen in such a way that the period is 2π .

10.5 Approximation to the Solution of Differential Equations.

Introduction.

To approximate the solution of differential equations it is important to insure that essential properties are preserved. In particular, for conservative systems, the same should hold. In this connection, I developed in 1956 a method of first order and a method of second order which are contact transformations and therefore preserve the essential properties of conservative systems. These will be applied to the finite case.

Algorithm.

The first order algorithm is defined by

Theorem.

Algorithm.

The second order algorithm for the solution of the differential equation

$$D^2\mathbf{x} = \mathbf{f} \circ \mathbf{x}, \mathbf{x}(0) = \mathbf{x}_0, \mathbf{D}\mathbf{x}(0) = \mathbf{D}\mathbf{x}_0,$$

is defined by

$$\mathbf{x}_{i+1} = \mathbf{x}_i + h\mathbf{D}\mathbf{x}_i + \frac{1}{2}h^2\mathbf{f}_i, \mathbf{D}\mathbf{x}_{i+1} = \mathbf{D}\mathbf{x}_i + \frac{1}{2}h(\mathbf{f}_{i+1} + \mathbf{f}_i),$$

where

$$\mathbf{f}_i := \mathbf{f}(\mathbf{x}_i).$$

Definition.

A mapping is reversible iff

Theorem.

Given the Algorithm 4.1.3., the mapping is reversible.

Proof: If we solve for \mathbf{x}_i and $\mathbf{D}\mathbf{x}_i$, we get

$$\begin{aligned} \mathbf{D}\mathbf{x}_i &= \mathbf{D}\mathbf{x}_{i+1} - \frac{h}{2}(\mathbf{f}_{i+1} + \mathbf{f}_i), \\ \mathbf{x}_i &= \mathbf{x}_{i+1} - h\mathbf{D}\mathbf{x}_i - \frac{1}{2}h^2\mathbf{f}_i, \end{aligned} \quad = \mathbf{x}_{i+1} - h\mathbf{D}\mathbf{x}_{i+1} + \frac{1}{2}h^2(\mathbf{f}_i + \mathbf{f}_{i+1}).$$

Definition.

A mapping is iff

Theorem.

The mapping defined in algorithm 4.1.3. is

Proof:

Example.

Let x and f be one dimensional, let

$$f(x) = -x - 2x^3,$$

let $Dx_0 = 0$, we have the following solutions

$p = 11$,

i	0	1	2	3	4	5	6	7
	8	9	10	11				
$(x, Dx)_i$	1, 0	5, 3	-4, 2	-2, 0	-4, -2	5, -3		
	3, 0	2, 1	5, 2	-2, 1	-3, 0	-2, -1	-5, -2	5, -2
		2, -1						
	4, 0							
	5, 0	4, -1	3, -2	0, -3	-3, -2	-4, -1	-5, 0	-4, 1
		-3, 2	0, 3	3, 2	4, 1			

$p = 13$,

i	0	1	2	3	4	5	6	7
		8	9	10	11	12	13	14
		15						
$(x, Dx)_i$	1, 0	6, -6	2, 0	6, 6				
	3, 0	-6, 2	-6, -2					
	4, 0	3, 3	-3, 3	-4, 0	-3, -3	3, -3		
	5, 0	1, 1	-6, 4	-4, 3	0, 4	4, 3	6, 4	-1, 1
		-5, 0	-1, -1	6, -4	4, -3	0, -4	-4, -3	-6, -4
		1, -1						
	6, 0	-5, 6	5, 6	-6, 0	5, -6	-5, -6		

Theorem.

If we apply the mapping 0.3. to $D^2x = -x$, $x(0) = 0$, $Dx(0) = 1$, we obtain, up to a scaling factor the trigonometric functions.

Example.

With $p = 13$ and $h = 1$,

i	0	1	2	3	4	5	6	7
		8	9	10	11	12	13	14
$(x, Dx)_i$	0, 1	1, -5	3, -3	-5, -4	-5, 4	3, 3	1, 5	0, -1

$(\delta x, Dx)((i) = (\sin, \cos)(-10i)$, if $\sin(1) = 3$ and $\cos(1) = 3\delta$, with $\delta^2 = 2$.

Program.

[130] PENDUL(um)

10.5.1 On the existence of primitive roots.**Introduction.**

I will first give a non constructive proof of the existence of primitive roots and then give a construction. The first proof insures that the construction is always successful.

Theorem.

0. $d = \text{ord}_p(x)$, $(d, p) = g$, $0 < l < d \Rightarrow \text{ord}_p(x^l) = \frac{d}{g}$,
1. $d = \text{ord}_p(x)$, $0 \leq i, j < d$, $x^i \equiv x^j \pmod{p} \Rightarrow i = j$.
2. If $d|p-1$ then $x^d \equiv 1 \pmod{p}$ has $\phi(d)$ solutions of order d . Hint 2.25.
3. In particular, there are $\phi(p-1)$ primitive roots of p .
4. $d = \text{ord}_p(z)$, $e = \text{ord}_p(y)$, $(d, e) = 1 \Rightarrow \text{ord}_p(z.y) = d.e$.

What follows is a Theorem which gives a constructive method of determining primitive roots or more generally of solutions of

$$d = \text{ord}(x), \text{ where } d|p-1.$$

The construction is inspired by Gauss, 1801, section 55.

Theorem.

Let $\Pi_{j=1}^n p_j^{i_j}$ be a prime factorization of $q-1$.

Let $\frac{a_j^{(q-1)}}{p_j} \not\equiv 1 \pmod{q}$ and $a_j^{(q-1)} \equiv 1 \pmod{q}$, for $j = 1, 2, \dots, n$, then

0. $p_j^k = \text{ord}_q(a_j^{\frac{q-1}{p_j^{i_j}}})$, $0 \leq k_j \leq i_j$.
Let $P_j = p_j^{i_j}$, let $h_j \equiv a_j^{\frac{q-1}{P_j}} \pmod{q}$, then,

1. in particular, $p_j = \text{ord}_q(h_j)$.

Let $h_j^{k_j} = a_j^{\frac{q-1}{i_j^{k_j}}} \pmod{q}$, $0 \leq k_j < i_j$, then

2. $\Pi_{j=1}^n h_j^{k_j} = \text{ord}_q(\Pi_{j=1}^n h_j^{k_j})$.
Let $h = \Pi_{j=1}^n h_j \pmod{q}$, then,

3. in particular, $q-1 = \text{ord}_q(h)$,

4. q is prime,

5. h is a primitive root of q .

Chapter 11

COMPUTER IMPLEMENTATION

11.0 Introduction.

One of the tradition of Mathematicians is to discover properties by working on special cases or examples, this is especially so at the beginning of many branches of Mathematics, geometry, number theory, algebra, This was certainly the tradition kept up by Euler, see ..., by Gauss, see In Euclidean geometry, the special cases were obtained by drawing a reasonably accurate figure, in number theory by numerical computation, and in algebra by algebraic manipulations. All three can now be done accurately and with great speed using computers and these are now becoming more and more available to every one.

Depending on our training or, I believe, on the structure of our individual brain, such experimentation is almost essential for many to obtain a thorough understanding of basic concepts.

To help in the understanding of the material given above and, I hope, to help the reader in the discovery of new properties, it is becoming essential to provide him with the tools to realize quickly computer programs.

When the subject matter is well settled and the experimentation is not at the basic level, a higher level non interactive language such as FORTRAN, ALGOL, PASCAL, PL1, ADA, is an excellent choice. When this is not the case, an interactive language such as BASIC or APL is by far preferable. BASIC, BASIC+, BASIC+ extended.

Hardware, operating system, files, interaction, language, compiler, interpreter.

REFERENCES

1. Adobe Systems, Postscript Language, Tutorial and Cookbook, N. Y., Addison- Wesley, 1985, 243 pp.
2. Adobe Systems, Postscript Language, Reference Manual, N. Y., Addison-Wesley, 1985, 319 pp.
3. Apollonius, A treatise on Conic Sections, ed. Th. L. Heath, Cambridge, 1896.
4. Apollonius, Les Coniques d'Apollonius de Pergé, trans. P. ver Eecke, Bruges, Belgique, 1923.
5. Artin, E., Geometric Algebra, N. Y., Interscience, 1957.
6. Artzy, Rafael, Linear Geometry, Reading Mass., Addison-Wesley, 1965, 273 pp.
7. Aryabhata I, The Aryabhatiya of Aryabhata, Tranlated with notes by Walter Eugen Clark, Chicago, Ill. Univ. of Chicago Press, 1930.
8. Aryabhata I, Aryabhatiya, Ed. by Kripa Shandar Shukla, New Delhi, Indian Nat. Sc. Acad.,1976. 219 pp.
9. Baker, Henry, Frederick, Principles of Geometry, Vol. 1 to 4, Cambridge Univ. Press 1, 1929, 195 pp. 2, 1930, 259 pp.
10. Barbilian, Dan, (or Barbu, Ion), Pagini Inedite, Vol. 2, Bucarest, Ed. Albatros, 1984, 292 pp.
11. Baumert, Leonard D., Cyclic Difference Sets, N. Y., Springer, 1971.
12. Bézier, P., Definition numérique des courbes et surfaces, I, II, Automatismes, Vol. 11, 1966, 625-632 and 12, 1967, 17-21. Also Vol. 13, 1968 and Thesis, Univ. of Paris VI, 1977.

13. Bézier, P., The Mathematical Basis of UNISURF CAD System. London, Butterworths, 1986.
14. Bézier, P., Numerical Control; Mathematics and Applications (transl. by R. Forrest). New-York, John Wiley, 1972.
15. Bolyai, Farkas, Tentamen Juventutem Studiosam ein Elementa Mathiseos Parae introducendi, Maros-Vasarhely, 1829, see Smith D. E. p. 375.
16. Bolyai, Janos, Appendix of Bolyai, Farkas.
17. Bolyai, Janos, The science absolute of space independent of the truth and falsity of Euclid's Axiom XI, translated by Dr. George Brus Halstead, Austin, Texas, The Neomon, Vol. 3, 71 pp, 1886.
18. Borsuk, Karol and Szmielew Wanda, Foundations of Geometry, Amsterdam, North-Holland, 1960, 444 pp.
19. Boubals, J. de Math. Elem. (de Longchamps et Bourget), 1891, p.218. (points of, on the circle of Brianchon-Poncelet)
20. Brahme Gupta and Bhascara, Algebra with Arithmetic and Mensuration, from the Sanscript of Brahme Gupta and Bhascara, translated by Henry Thomas Cole-brooke, London, John Murray, 1817.
21. Braikenridge, William, Exercitatio geometrica, London, 1733.
22. Brianchon, Charles, Poncelet, Jean, Recherches sur la détermination d'une hyperboie équilatre au moyen de quatre conditions données, Ann. de Math., Vol. 11, 1820-1821 , p. 205-220, see Smith, D. E., p. 337.
23. Buchheim Arthur, An extension of Pascal's theorem to space of three dimensions. Messenger of Mathematics, Ser. 2, Vol. 14, 1984, 74-75.
24. Casey John, Sequel to Euclid, London, 1881, p.101 for III.4.4.0.
25. Charles, Michel, Apperçu historique sur l'origine et le developement des méthodes en géométrie, 2e Edition, Paris, 1875.
26. Ch'in, Chiu-Shao, see Libbrecht, Ulrich.

27. Chou, Shang-Ching, Proving Elementary Geometry Theorems using Wu's Algorithm. Contemporary Mathematics, Bledsoe, W. W., and Loveland, D. W. Ed., Amer. Math. Soc. Vol. 29, 1984 243-286.
28. Clebsch, Rudolf Frederick Alfred, Vorlesungen uber Geometrie, p.312
29. Coolidge, Julian, The Elements of non-Euclidean Geometry. Oxford Clarendon Press, 1909, 291 pp.
30. Coolidge, Julian, A treatise on the Circle and the Sphere, Oxford, Clarendon Press, 1916. 603 pp., III.4.4.0.
31. Coolidge, Julian, A History of geometrical methods. Oxford Clarendon Press, 1940, 451 pp.
32. Coolidge, Julian, A History of the Conic Sections and Quadric Surfaces. Oxford Clarendon Press, 1945, 214 pp.
33. Coxeter, H. S. M., The Real projective Plane, New-York, McGraw-Hill, 1949, 196 pp.
34. Coxeter H. S. M. and Greitzer, S. L., Geometry Revisited, N. Y. Random House, 1967, 193 pp.
35. Coxeter H. S. M. and Moser, W. O. J., Generators and relations for discrete groups. Springer, 1957.
36. Dalle A. et De Waele C., Géométrie plane. Namur, Belgique, Wesmael-Charlier, 1936, 408 pp.
37. David Antoine, 2000 Théormes et Problmes de Géométrie avec Solutions. Namur, Belgique, Wesmael-Charlier, 1956, 1055 pp.
38. de Casteljau, P., Outillages méthodes calcul. Technical Report, Citron, Paris 1959, See also 1963.
39. de Casteljau, P., Shapes Mathematics and CAD. Kogan Page, London, 1986.
40. Dembowski, Peter, Finite Geometries, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44, Springer, New-York, 1968, 375 pp.

41. Desargues, Gérard, Brouillon d'un projet d'une atteinte aux évènements des rencontres d'un cne avec un plan, Paris, 1639. See Smith D. E., p. 307.
42. Descartes, René, La Géométrie, Nouv. Ed., Paris Hermann, 1886, 91 pp.
43. De Vogelaere, R., Finite Euclidean and non-Euclidean Geometry with application to the finite Pendulum and the polygonal harmonic motion. A first step to finite Cosmology. The Big Bang and Georges Lemaitre, Proc. Symp. in honor of 50 years after his initiation of Big-Bang Cosmology, Louvain-la-Neuve, Belgium, October 1983., D. Reidel Publ. Co, Leyden, the Netherlands. 341-355.
44. De Vogelaere, R., Géométrie Euclidienne finie. Le cas p premier impair. La Gazette des Sciences Mathématiques du Québec, Vol. 10, Mai 1986.
45. Dieudonné, Jean, La géométrie des groupes classiques, Berlin, Springer, Ergebnisse Der Math. und ihrer Grenzgebiete, 1963, 125 pp.
46. Donath, E. Die merkwürdigen Punkte und linien des Dreiecks, Berlin, VEB Deutscher Verlag der Wissenschaften, 1968.
47. Emmerich A., Die Brocarsschen Gebilde, Berlin, Verlag Georg Reimer, 1891,
48. Engle and Staeckel, Theorie der Parallellinien von Euklid bis auf Gauss, Leipzig, 1895. (See Mathesis, Sér. 2, Vol. 6, 1896, Suppl. pp. 1-11 or Rev. des quest. scient. Sér. 2, Vol. 8, 1895, pp. 603-612)
49. Enriques, Frederigo, Lezioni di geometria proiettiva, Bologna, 1904, French Translation, Paris 1930
50. Euclides, Les oeuvres en grec, en latin et en français, par Peyrard, Paris, Patris, 1814, 519 pp.
51. Evans, Anthony B., On planes of prime order with translations and homologies, J. of Geometry, 34, 1989, 36-41. (Desarguesian planes)
52. Eves, Howard, An Introduction to the History of Mathematics, New-York, Holt, Reinehart and Winston, 1953, 588 pp.
53. Fano, Sui postulati fondamentali della geometria proiettiva, Giorn. di mat., Vol. 30, 1892, 106-132. (PG(n,p))

54. Farin, Gerald, Curves and Surfaces for Computer Aided and Geometric Design, New-York, Acad. Press, 1988, 334 pp..
55. Feuerbach, Karl, Grundriss zu analytischen Untersuchungen der dreyeckigen Pyramide, Nuremberg, 1827.
56. Feuerbach, Karl, Eigenschaften einiger merkwürdigen Punkte des geradlinigen Dreiecks. Nürnberg, Riegel und Wiessner, 1822, 16+62 pp.
57. Fontené, G., Extension du Théorme de Feuerbach. Nouv. Ann. de Math., Sér.4, Vol. 5, 1905.
58. Forder, Henry, George, The Foundations of Euclidean Geometry, Cambridge Univ. P., 1927, repr. N. Y. Dover P., 1958, 349 pp.
59. Forder, Henry, George, Higher Course Geometry, Cambridge Univ. P., 1931, 264 pp.
60. Forder, Henry, George, The Calculus of Extension, New-York, Chelsea Pub. Co., 1960.
61. Freudenthal, Oktaven, Ausnahmen gruppen und Oktavengeometrie, Uttrecht, Utrecht Univ. 1960.
62. Fritz, Kurt von, The discovery of incommensurability by Hippasus of Metapontum, Annals of Math., Vol. 46, 1945, 242-264. Also Studies in Presocratic Philosophy, Furley David and Allen R. E. Rdit. New-York, Humanities P., 1970, pp.382-412.
63. Gauss, Carl, Disquisitiones Arithmeticae, Lipsiae, Fleicher, 1801. Translated by Clarke, Arthur, S.J., New Haven, Yale Univ. P. 1966, 473 pp.
64. Gergonne, Joseph, Diaz, circle inscrit Nagel cerele exinscrit.
65. Gergonne, Joseph, Diaz, Annales de Mathématiques, 1827, Vol. 17, p. 220 and 1829, Vol. 19, p. 97 and 129.
66. Greenberg, M., Euclidean and Non-Euclidean Geometries, San Francisco, Freeman, 1974.
67. Hagge, Der Fuhrmannsche Kreis und der Brocardsche Kreis, Zeitschrift für rnathematische Urnterricht, vol. 38, 1907.

68. Hall, Marshall, Projective Planes , Trans. Amer. Math. Soc., Vol. 54, 1943, 229-277
69. Hall, Marshall, Jr, Projective Planes and related Topics, Calif. Inst. of Technology, April 1954, 77 pp.
70. Hartshorne, Robin C., Foundation of Projective Geometry, N. Y. Benjamin, 1967, 161 pp.
71. Heath, Sir Thomas, The thirteen books of Euclid's elements, Vol. 1, Cambridge University Press, 1908. 424 pp. Other Edition, "The Classics of the St John's program," Annapolis, The St. John's College Press, 1947.
72. Heath, Sir Thomas, Diophantus of Alexandria, 2nd Edition, Cambridge University Press, 1910.
73. Heath, Sir Thomas, A Manual of Greek Mathematics, Oxford Univ. P., 1931, 551 pp.
74. Heidel, W. A . The Pythagoreans and Greek Mathematics, Amer. J. of Philology, Vol. 61, 1940, 1-33. Also Studies in Presocratic Philosophy, Furley David and Allen R. E. Edit. New York, Humanities P., 1970, pp. 350-381.
75. Hensel, Kurt Theorie der algebraischen Zahlen, Berlin, Teubner, 1908, 349 pp.
76. Hensel, Kurt, Zahlentheorie, Berlin, Goeschens'sche Verslaghandlung, 1913, 356 pp.
77. Hessenberg G., Math. Ann., Vol. 61, 1905, pp. 161-172.
78. Hilbert D., Grudlagen der Geometrie, 1899, tr. by E. J. Townsend, La Salle, Ill., Open Court Publ. Cp., 1962, 143 pp.
79. Hilbert D. und Cohn-Vossen S., Auschauliche Geometrie, Berlin, Springer, 1932, 310 pp.
80. Hirschfeld, J. W. P., Projective geometries over finite fields, Oxford, Clarendon Press, 1979. 474 pp.
81. Hughes, D. R., A class of non-Desargesian projective planes, Canad. J. of Math., 1957, Vol. 9, 378-388. (I.9.p.1)

82. Intrigila, Carmelo, Sul Tetraedro, Rend. della R. Accad. delle Scienze di Napoli, Vol. 22, 1883, pp. 69-92.
83. Iversen, Birger, An Invitation to Geometry, Math. Inst. Aarhus Univ. Lect. Notes Series, No 59, 1989, 186 pp.
84. Jacobi, Karl Gustav, Crelle J. für Reine und Angewandte Mathematik, Vol. 15, 199-204, Werke, I, p.336, (4)).
85. Järnefelt G. and Kustaanheimo Paul, An Observation on Finite Geometries. Den II. Skandinavische matematikerkongress, Trondheim, August 1949, 166-182.
86. Järnefelt G. , Reflections on a finite Approximation to Euclidean Geometry. Physical and Astronomical Prospects. Suomalaisen Tiedekatemia Toimituksia, Ser. A, 1951, No 96.
87. Johnson, Norman L., Kallaher, Michael J., Long Calvin T., Edit. Finite Geometries, N. Y., Marcel Dekker Inc. 1983.
88. Johnson, Roger A., Modern Geometry, Houghton Mifflin Co, 1929, 319 pp.
89. Karteszi, F. Introduction to finite geometries. Amsterdam, North Holland Publ. Co., 1976, 266 pp.
90. Kirk, G. S., Popper on Science and the Presocratics. Mind, Vol 69, 1960, 318- 339. Also Studies in Presocratic Philosophy, Furley David and Allen P. E. Edit. New-York, Humanities P., 1970, pp.154-177.
91. Klein Felix, Geometry, N.Y. MacMillan, 1939.
92. Klein, Felix, Famous Problems of Elementary Geometry, tr. by W.W. Beman and D. E. Smith, 1897, N.Y. Ginn, Reprinted in Famous Problems and other Monographs. New York, Chelsea, 1955.
93. Knüppel, Frieder and Salow, Edzard, Plane elliptic geometry over rings. Pacific Journal of Mathematics. Vol. 123, (1986), 337-384.
94. Koblitz Neal, A Short Course on Some Current Research in p-adic Analysis (Talks at Hanoi Math. Inst., July 1978), 66 pp. (Prof. Ogus)

95. Koblitz Neal, *p-adic Numbers, p-adic Analysis and Zeta-Functions*, Springer- Verlag, N.Y., 1977, 124 pp.
96. Lachlan, On Poristic Systems of Circles, *Messenger of Mathematics*, vol. 16, 1887.
97. Laguerre, Edmond Nicolas, *Oeuvres*, 2 Vol. Paris, Gauthier-Villars, 1898-1905. (I,9.,p1)
98. Lebesgue, Henri, *Leçons sur les constructions géométriques*, Paris, Gauthier- Villars, 1950, 304 pp.
99. Lehmer, D. H., *An elementary course in synthetic projective geometry*. Boston, 1917 and Berkeley, California, Univ. of Calif. Pr., 1933, 123 pp.
100. Lemaître Georges. *l'Hygrothse de l'Atome Primitif, Essai de Cosmogonie*, Neucgatel, Ed. du Griffon, 1946, 201 pp.
101. Lemaître Georges. *The Primeval Atom, A Hypothesis of the Origin of the Universe*. Trans. by Betty and Serge Korff, van Nostran, N. Y., 1950, 186 pp.
102. Lemay, Fernand, *Imagination dissidente*, Bull. de l'APAME mars 1979.
103. Lemay, Fernand, *Motivation intrinsque*, Bull. de l'APAME, novembre 1979.
104. Lemay, Fernand, *Le dodécadre et la géométrie projective d'ordre 5*, see Johnson N. L., 279-306
105. Lemoine, Emile, *Propriétés relatives a deux points du plan d'un triangle qui se déduisent d'un point K quelconque du plan comme les points de Brocard se déduisent du point de Lemoine*. *Mathesis*, Sér.1, Vol. 6, 1886, Suppl. 1-27.
106. Lemoine, Emile, 1902, *Géométrographie*, C. Naud, Paris
107. Lemoine, Emile, *J. de Math. Elem. (de Longchamps et Bourget)*, 1889, p.93 1890, p.118, (point of, on the circle of Brianchon-Poncelet)
108. Libbrecht, Ulrich, *Chinese Mathematics in the Thirteenth Century, The Shu- Shu-Chiui-Chang of Ch'in*, Chiu-Shao, Cambridge, MIT Press, 1973, 555 pages.

109. Lobachevskii, Nikolai, Ivanovich, see Nolden. A., *Elementare Einfuhrung in die Lobachewskische Geometrie*, Berlin, VEB Deutscher Verlag der Wissenschaften, 1958, 259 pp.
110. MacLaurin, Colin, *Phil. Trans. Roy. Soc. London*, 1735. (On Pascal Constr)
111. Mansion, Paul, *Premiers Principes de la Métagéométrie ou Géométrie générale*, Mathesis, Ser. 2, Vol. 6, 1896, Suppl. 1-46.
112. Mascheroni L. *Géométrie du Compas*, translated in French Carette A.M., Paris 1798
113. Maxwell, E. A., *The methods of plane projective geometry based on the use of general homogeneous coordinates*. Cambridge Univ. Press, 1952. 230 pp.
114. Menger, K., *Untersuchungen über allgemeine Metrik*, Math. Ann. Vol. 100, 1928, 75-163.
115. Michel, Charles, *Compléments de géométrie moderne*, Paris, Vuibert, 1926. harmonic polygons, p. 272.
116. Michel, Paul-Henri, *De Pythagorea Euclide*, Paris, Les Belles Lettres, 1950, 699 pp.
117. Miquel, Auguste, *Théorèmes de géométrie*, J. de Liouville, Vol. 3, 1838, p.486.
118. Miquel, Auguste, *Mémoires de Géométrie*, J. de Mathématiques Pures et Appliquées, (J. de Liouville), Vol. 9, 1844, p.24.
119. Möbius August, *Werke*, (Calculus Barycentrique)
120. Moise, Edwin E., *Elementary Geometry from an advanced standpoint*, Palo Alto, Addison-Wesley, 1963, 419 pp.
121. Moufang, Ruth, *Alternativkörper und der Satz vom vollständigen Vierseit*, Abh. Math. Sem. Hamburg, Vol. 9, 1933, 207-222.
122. Moulton, F. R., *A simple non-Desarguesian plane Geometry*, Trans. Amer. Math. Soc. Vol. 3, 1902, 192-195.
123. Nagel, Chretien Henry, *Untersuchungen über die wichtigsten zum Dreieck gehörende Kreise*, 1836.

124. Neuberg, Joeeph, Mémoire sur le tétradre, Mémoires couronnés de l'Académie de Belgique, Vol. .37, 1886, pp. 3-72.
125. O'Hara, C. W. and Ward, D. R., An introduction to Projective Geometry, London, Oxford Uni, P., 1937, 298 pp.
126. Ostrom, T, G., Finite translation planes, Lecture Notes in Math., Number 158, Berlin, Springer, 1970.
127. Ostrom, T. G., Some translation planes that are not well known, Technical Report, N. 13, Department of Math. Washington State Univ., 1968, 49 pp.
128. Pascal, Blaise, Pensées, Nouv. Ed., Philippe Sellier, 1976, 543 pp.
129. Pascal, Blaise, Essay sur les couiques, 1639, see Smith, D. E., p, 326.
130. Pascal, Blaise, Oeuvres, Ed. Brunschvig et Boutroux, I, p. 252, (on Pascal, Constr.)
131. Pasch, Moritz, Vorlesungen uber neuere Geometrie, Leipzig, Teubner, 1882, 202 pp.
132. Pasch, Moritz und Dehn, Max, Vorlesungen uber neuere Geouetrie, Berlin,
133. Pickert. G., Projektive Ebenen, Berlin, Springer, 1955, 343 pp.
134. Pieri, Un sistema di postulati per la geometria proeitiva, Rev. Mathém. Torino, Vol 6, 1896. See also Atti Torino, 1904, 1906.
135. Pieri, I principii della geornetria di posizione, composti in sistema logico deduttivo, Mem. della Reale Acad. delle Scienze di Torino, serie 2, Vol.48, 1899, pp 1-62.
136. Playfair, John, Elements of Geometry, Philadelphia, Lippincoot & Co, 1864, 318 pp
137. Plücker, Julius, Analitische geometrie Entwicklungen, Voi 1 and 2 1828-1831 Crelle, Vol.5, 1830, Vol.12 (1834). Springer, 1976, 275 pp.
138. Plücker, Julius, Theorie der algebraischen Curven 1839

139. Poncelet, Jean, Victor, Application d'Analyse et de Géométrie, Paris, Mallet- Bachelier, I, 1862, 563 pp., II, 1864, 602 pp.
140. Poncelet, Jean. Victor, Traité des propriétés projectives des figures, Paris, Gauthier- Villars, I, 1865, 428+xii pp. II, 1866, 452+vi pp.
141. Popper, Sir Karl, Back to the Presocratics, Proc. of the Aristotelian Society, Vol. 59, 1958-9, 1-24, also Studies in Presocratic Philosophy, Furley David and Allen R. E. Edit. New York, Humanities P., 1970, pp.130-153.
142. Prouhet, , Analogies du triangle et du tétradre, Nouv. Ann. de Math., Série 2, Vol. 2, 1863, p.138.
143. Reidemeister, K., Grundlagen der Geometrie, Berlin, Springer, Grundl, der math,Wissens in Einz., Vol. 32, 1968,
144. Robert, Alain; Elliptic curves, Lecture Notes in Mathematics, Berlin, Springer, Vol. 326, 1973, 264 pp.
145. Roberts, Michael, On the analogues of the Nine-Point Circle in the Space of Three Dimensions, Proc. London Math. Soc., Vol. 19, 1878.
146. Roberts, Samuel, Proc. London Math Soc., Vol 12, 117. (Generalization of Miquel to tetrahedron)
147. Robinson, A., Non-standard Analysis, North-Holland, Amsterdam, 1974, 293 pp.
148. Robinson, G. de B., The foundations of Geometry, Toronto, 1940.
149. Saccheri, Giovanni Girolamo, Euclides ab omni naevo vindicatus Milan, 1732. Tr. George Halstead, London Open Court Pr. 1920, 246 pp. See Engel and Stäckel.
150. Salmon, George, A treatise on Conic. Sections, 6-th ed. London 1879.
151. Salmon, George, A treatise on the higher plane curves, 3d ed. Dublin, Hodges, Foster and Figgis, 1879, 395 pp.
152. Schwabhuser W., Szmielew W., Tarski.A, Metamathdmatiscche Methoden in der Geometrie, N. Y, Springer, 1980, 482 pp.

153. Segre, B, Lectures on modern Geometry. Rome, Cremonese, 1961, 479 pp.
154. Segre, C, Un,nuovo campo di ricerche geometriche, Atti R. Acad. Sc. Torino, Vol 25, 1889, 430-457.
155. Seidenberg, Lectures in Projective Geometry, Princeton N. J., van Nostrand, 1962, 230 pp.
156. Shively, Levi S., An Introduction to Modern Geometry, N. Y., John Wiley, 1939. 167 pp.
157. Smith, David, Eugene, History of Mathematics, Vol. I, II.
158. Smith, David, Eugene, A Source Book of Mathematics, N. Y. McGraw Hill, 1929, 701 pp.
159. Smogorzhevskii, A. S., The ruler in Geometrical Constructions, tr. by Halina Moss, New York, Blaisdell, 1961.
160. Sommerville, Duncan, Bibliography of non-Euclidean Geometry, London, Harrison, 1911, 403 pp.
161. Spieker, Ein merkwürdiger Kreis um der Schwerpunkt des Perimeters des geradlinigen Dreiecks als Analogon des Kreises der neun. Punkte, Grunert's Archiv, Vol. 51, 1870.
162. Staudt, K. G. C. von, Geometrie der Lage, Nuremberg 1847
163. Staudt, K. G. C. von, Beitrage zur Geometrie der Lage, Nuremberg 1857.
164. Steiner, Jacob, Geometrical Constructions with a Ruler, tr. by M. E. Stark, ed. by R. C. Archibald, New York Scripta Mathematica, 1950.
165. Steiner, Jakob, Collected. Works; Vol. I., pp. 43 and 135 for III.4.4.0.
166. Stevenson, F.W., Projective Planes, W.E. Freeman and Co, 1972, 416 pp.
167. Stroeker, R. J., Brocard Points, Circulant Matrices, and Descates' Folium; Math. Magazine, Vol. 61, 1988, 172-187

168. Tarski, Alfred, What is Elementary Geometry, The axiomatic method with special reference to Geometry and Physics, Studies in Logic and the Foundation of Mathematics, North-Holland, Amsterdam, 1959, 16-29, Collected. Works, IV, 17-32.
169. Taurinus, Theorie der Pallellinien. 1825, 102pp.
170. Taurinus, Geometriae primia Elementa, 1826, 76pp.
171. Taylor, H. M., On a six point circle connected with a triangle, Messenger of Mathematics, Vol 11, 177-179. (Circle of Taylor).
172. Taylor, H. M., The Porism of the ring of circles touching two circles, Messenger of Mathematics, Vol. 7, 1878. III.4.4.0.
173. Taylor, W. W., On the ring of circles touching two circles, Messenger of Mathematics, Vol. 7, 1878. III.4.4.0.
174. Terquem, Orly, Consideration sur le triangle rectiligne, Nouv. Ann. de Math., Serie 1, Vol. 1, 1842, 196-200
175. Thomas, Ivor, Greek Mathematics, Cambridge, Mass., Harvard Univ. P., Vol. 1. 1939, 505 pp.
176. Thureau-Dangin, F. Textes Mathematiques Babylonien, Leiden 1938.
177. Tilly, Joseph Marie de, Essai sur les Principes fondamentaux de Géométrie et de Mecanique, Bruxelles, Mayolez, 1879 192 pp. Also, Mem. Soc. scinc. phys. et natur. de Bordeaux, Vol III Ser. 2, cahier 1.
178. Tilly, Joseph Marie de, Essai de Géométrie analytique générale, Bruxelles 1892. Blumenthal considers than in this paper Tilly makes a fundamental contribution by introducing n-point relations to characterize a space metrically.
179. Tucker, R., The “cosine” orthocenters of a triangle and a cubic through them Messenger of Mathematics, Ser 2, Vol. 17, pp. 97-103. (10 distances between 5 points!)
180. Vahlen, Ueber Steinersche Kugelketten, Zeitschrift für Mathematik und Physik, Vol. 41, 1896, III.4.4.0.

181. van der Waerden, Mathematics and Astronomy in Mesopotamia, Dict. of Scientific Bibliography, Vol 15.
182. Veblen, Oswald, and Bussey, W. H., Trans. Amer. Math. Soc., Vol. 7, 1906, 241-259. (PG(n,pk))
183. Veblen, Oswald, and Young, John, Projective Geometry, Wesley, Boston, I, 1910, II, 1918
184. Ver Eecke, Paul, Proclus de Lycie, Les commentaires sur le premier livre des éléments d'Euclide, Bruges, Desclee De Brouwer, 1948, 372 pp.
185. Verriest, Gustave, Eléments de Géométrie Projective, Louvain, Feyaerts, 1930, 412 pp.
186. Vigarié, Emile, Premier inventaire de la géométrie du triangle, Mathesis, Sér. 1, Vol. 9, 1889, Suppl. pp. 1-26.
187. Vigarié, Emile, La bibliographie de la géométrie du triangle, Mathesis, Sér. 2, Vol. 6, 1896, Suppl. 1-14. (603 articles)
188. Vuibert, Sur la Géométrie classique du Triangle.
189. Walker, R., Cartesian and Projective Geometry., London, Edward Arnold and Co, 1953, 320 pp.
190. Whitehead, Alfred, The Axioms of Projective Geometry, Cambridge, 1906.
191. Wu, Wen-Tsun, On the Decision Problem and the Mechanization of Theorem-Proving in Elementary Geometry, Contemporary Mathematics, Bledsoe, W. W., and Loveland, D. W. Ed., Amer. Math. Soc. Vol. 29, 1984 213-234.
192. Wu, Wen-Tsun, Some Recent Advances in Mechanical Theorem-Proving of Geometries. Contemporary Mathematics, Bledsoe, W. W., and Loveland, D.W. Ed., Amer. Math. Soc. Vol. 29, 1984 215-242.
193. Young, John, Projective geometry, 4th Carus Monograph, Chicago, 1930.