

TEKST NR 280

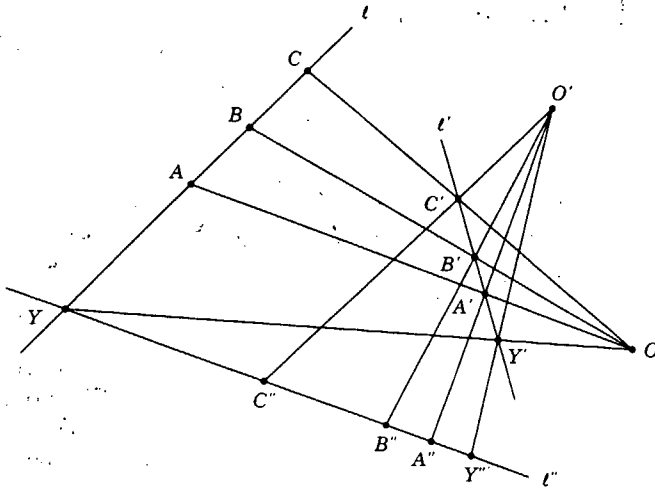
1994

A Course in Projective Geometry

by Lars Kadison

and

Matthias T. Kromann



TEKSTER fra

IMFUFA

ROSkilde UNIVERSITETSCENTER
INSTITUT FOR STUDIET AF MATEMATIK OG FYSIK SAMT DERES
FUNKTIONER I UNDERVISNING, FORSKNING OG ANVENDELSER

IMFUFA, Roskilde Universitetscenter, Postbox 260, DK-4000 Roskilde.
"A Course in Projective Geometry" by Lars Kadison and Matthias T. Kromann.
IMFUFA tekst nr. 280/94, 210 pages, ISSN 0106-6242.

Abstract

This book gives a self-contained account of the synthetic and analytic developments of basic projective geometry. A chapter on elementary group theory provides the necessary background to study the interplay of projectivities and collineations with the geometry of the projective line and plane. A chapter on division rings and related ring theory provides the background for generalizing our analytic development over the field of real numbers to division rings, and then to coordinatize the synthetic projective plane having Desargues' Theorem. One theme of this text is the equivalence of geometric axioms for affine and projective planes with algebraic axioms for the corresponding automorphism groups or division ring coordinates.

This is a draft of a forthcoming volume intended for undergraduates who have a background in linear algebra and the calculus of several variables and wish to major in mathematics. The volume is intended for a one-semester geometry course, which will serve as an effective complement and motivation for a course in modern algebra (on groups, rings and fields). The book is composed of 11 chapters, 97 figures and 162 exercises. A set of four appendices on additional topics is designed to provide students with further reading for independent study or accredited projects in geometry.

© 1994 by Lars Kadison. All rights reserved. This book may not be reproduced or distributed in any form or by any means, without the prior written permission of Lars Kadison.

This book was set in Computer Modern, using AMS-LATEX . Figures were programmed in PostScript, using psMath , a PostScript library developed by M.T. Kromann.

Preface

In this book we study the synthetic and analytic aspects of basic projective geometry. On the one hand, we develop a postulational system, beginning with only four postulates. One of these is a particular departure from Euclid's parallel postulate: two distinct lines of a projective plane are assumed to always meet in one point. On the other hand we introduce and study our basic example, the real projective plane. The real projective plane is approached in either of two equivalent ways. First, it is an extension by ideal points and the line-at-infinity of the Euclidean plane. Second, it is a system of homogeneous points, in which lines and higher degree algebraic curves, such as

$$X^n + Y^n = Z^n, \quad n \geq 3,$$

intersect in the "right" number of points (see Bezout's Theorem, appendix B).

In chapters 3, 5 and 6, we develop the analytic theory of the real projective plane. We prove Desargues' Theorem and Fano's Theorem by direct computation with homogeneous coordinates. Then we prove the Fundamental Theorem (FT) of one-dimensional projectivity by using linear fractional transformations. At the same time, we develop the synthetic theory by the addition of three axioms, which correspond to the three major theorems above: their statements are added as axioms since they cannot be proven by synthetic means. As axioms are added, we define and study complete quadrangles, harmonic points, projectivities, cross ratio, projective collineation and Pappus' configuration in chapters 5 and 6. Early in chapter 5, we establish the Principle of Duality, which will imply that our theory correctly dualizes to a theory of complete quadrilaterals, harmonic lines, etc. The dualization is obtained very simply by exchanging pairs of words in definitions and propositions: "point" and "line," "on" and "through," "collinear" and "concurrent." The Principle of Duality has been a marvel to new generations of mathematicians since its discovery in the early 19th century.

In chapter 8 we leave the analytic development of the projective plane over the real numbers, and go to a greater generality — viz., projective planes over division rings. Having introduced division rings,

fields, and many examples in the previous chapter, we replace the reals with division ring elements in the homogeneous coordinate model. It is at this stage that the reader will be enlightened to the meaning of the somewhat exotic examples of the synthetic theory, the finite projective planes: they are but projective planes over finite fields. Armed with many new examples of projective planes, we then establish the independence of the axioms of Desargues, Fano and FT — and a useful redundancy in one case — with the help of quaternions and a skew field of characteristic two. Pappus' Theorem is shown to be equivalent to commutativity of multiplication in the underlying division ring; Fano's Axiom to $1 + 1 \neq 0$ in the symbols of division ring theory. Desargues' Theorem is shown to be valid in projective planes over division rings. In chapter 9, the converse is established: a Desarguesian plane is isomorphic to a projective plane over a division ring.

Throughout the book, a good deal of attention is focussed on the automorphism groups of projective and affine planes. For the projective planes of order p , these are finite groups of order $p^3(p^3 - 1)(p^2 - 1)$. For the projective plane over the reals, these are continuous groups of 3×3 nonsingular matrices of reals up to a scalar multiple: their geometric classification into elations, homologies, etc., leads us in chapter 11 to some interesting corollaries in linear algebra. In order to better study these and other automorphism groups, we have provided in chapter 4 the basics of group theory with many exercises. In chapter 8, we prove a fundamental theorem about the automorphism group of a Desarguesian plane: it is generated by two subgroups, a subgroup of linear automorphisms and a subgroup of automorphisms fixing four points in general position. In a later chapter, we show the former subgroup is generated by elations and homologies, which correspond to translations and central dilatations (homotheties) of the affine plane, respectively. The latter subgroup is isomorphic to the group of division ring automorphisms. In chapter 9, we apply our knowledge of the dilatation group of a Desarguesian plane in defining the operations of addition and multiplication on the points of an arbitrary line — and proving that these form a division ring. In chapter 11, the group of linear automorphisms is shown to be identical with the group of projective collineations: then we apply that to prove Ceva's Theorem in

advanced Euclidean geometry.

This is a draft of a forthcoming volume. In writing this book, we intended it to serve the student as a self-contained textbook for an undergraduate course. However, it is equally suitable to the general reader with a background in linear algebra and the calculus of several variables. Our book does not presuppose any background in abstract algebra. On the contrary, it is intended to provide both background and motivation for a later study of groups, rings and fields. Based on several experiences giving a university course on roughly the contents of this book, we found that the students absorbed the necessary abstract algebra with alacrity.

There are four appendices on additional topics: conics, algebraic curves and Bezout's Theorem, elliptic geometry and ternary rings. They are partly intended to develop several themes in the book. For the most part though, they are intended to lead the reader through some independent study among the references, or to lead the student through an accredited project. Each appendix proposes a central problem that the reader may take up on his own, or pursue in the literature of algebraic geometry, metric geometry or foundations of geometry.

The authors

Roskilde, Denmark

September 13, 1994

Acknowledgements. We thank R. Hartshorne, J. Gonzalo and B. Booß-Bavnbek for helpful discussions about our book.

Historical Foreword

The motivation for the modern theory of projective geometry came from the fine arts. By 1300 artists like Duccio and Giotto were no longer content with the highly stylized medieval art and sought to revive Graeco-Roman standards: they made the first experiments in foreshortening and the use of converging lines to give an impression of depth in a scene painting. Their intuitive theory of perspective culminated in the work of Lorenzetti in the 1340's.



Figure 0.1. Drawing from Jan Vredeman de Vries, "Perspective" (1604).

At this stage, further progress in the realistic representation of three-dimensional scenes on a two-dimensional canvas had to await the development of a mathematical theory of perspective. The Italian painter and architect Brunelleschi was teaching such a theory in 1425. In 1435, L. B. Alberti had written the first treatise of perspective. Later, the gifted mathematician and painter Piero della Francesca (c. 1418–1492) considerably extended the work of Alberti. Still later, both Leonardo da Vinci (1452–1519) and Albrecht Dürer (1471–1528) wrote treatises which not only presented the mathematical theory of

perspective but insisted on its fundamental importance in all of painting.

In a separate development pre-dating the theory of perspective by a couple of millenia, Appollonius, Archimedes, Euclid and Menaechmus, in the period from 400 until 200 B.C., had introduced and studied the subject of conics. However, the first truly projective theorems were discovered by Pappus in Alexandria around 250 A.D. (see chapter 6) and proven by him using complicated Euclidean argumentation.

The German astronomer Johann Kepler (1571–1630) elevated the ellipse of Apollonius to center stage in scientific history with his first law of planetary motion. In 1639 the sixteen year old Blaise Pascal wrote *Essai pour les Coniques*¹, in which he deduced 400 propositions on conics, including the work of Appollonius and others, from the theorem that now bears his name.

The proof of Pascal's Theorem used the method of projection, which he had learnt from Girard Desargues (1591–1661). The architect and gifted mathematician Desargues added a great body of work to projective geometry, including his two truly great theorems (in chapter 3 and appendix A). His work was not well received in his lifetime, which perhaps was due to his obscure style: of seventy terms he introduced, but one (involution) survives today. However, E.T. Bell, in his unforgettable biographical style, notes the following irony of history and the passage of time: Bell traces the mathematics of Einstein's general theory of relativity back to Desargues [Bell, p. 213], who was unknown to Isaac Newton (1642–1728).

Newtonian mechanics and calculus had dominated mathematics, physics and philosophy for a century, when a young engineering officer J. V. Poncelet (1788–1867) was facing internment in a prisoner-of-war camp for prisoners taken from Napoleon's Grand Army. He had a solid education in geometry from Monge and the elder Carnot, and set about trying to recall what he had learnt from them. Finding that he could recreate the general principles but could not recall the barren details of the eighteenth century masters, he proceeded to invent projective geometry as we know it today. Among many things, he

¹Now lost but apparently Leibniz had read it.

is the first to have applied the principle of duality in a treatise on projective geometry: his habit of writing about projective geometry in two columned pages, one column for the new theory, the other for its dual, continued into the twentieth century.

Projective geometry came into its own as a research field of mathematics after the publication of Poncelet's work. K. G. C. von Staudt (1798–1867) studied conics, polarities and emancipated the ideal points from their special status. The Swiss Jakob Steiner (1796–1863) studied conics from the point of view of one-dimensional projectivities. The French M. Chasles (1793–1880) discovered facts about cross ratio and conics, facts like those of von Staudt and Steiner which had escaped men for close to two thousand years. Arthur Cayley derived in 1859 (perhaps with a hint from Laguerre's earlier book) the three geometries of Euclid, Bolyai and Lobatchevsky from cross ratio, a fixed conic and region in the real projective plane. Matrix multiplication itself seems to have grown out of Cayley's investigations of the projective invariants of A. F. Möbius (1790–1868). To Möbius and Feuerbach we owe homogeneous coordinates in 1827, but it was left to Felix Klein in 1871 to remove the last vestiges of Euclidean geometry and provide the algebraic foundations of projective geometry that is evident in chapter 8 of the present book.

In 1899 David Hilbert (1862–1943) published his *Grundlagen der Geometrie* in which the fruit of about twenty years intellectual labor of himself, Pasch and others were recorded. This book can be viewed as the work that set Euclid straight after 2000 years unquestioned intellectual hegemony. Six primitive notions and twenty axioms were given for three-dimensional Euclidean geometry in an almost flawless postulational system. Hilbert showed his postulational system to be as consistent as the arithmetic of real numbers (in analogy with the reasoning in chapter 9). Later, Hilbert was emboldened to formulate his doctrine of formalism. It is presumably at this time that insights into the foundations of projective geometry were made as well.

As we come into the twentieth-century the present authors approach a tangle of events they are not able to sort through. So we quote a memorable phrase from Bell, writing in the 30's, and note him right about being wrong.

*“The conspicuous beauty of projective geometry and the supple elegance of its demonstrations made it a favorite study with the geometers of the nineteenth century. Able men swarmed into the new goldfield and quickly stripped it of its more accessible treasures. Today the majority of experts seem to agree that the subject is worked out so far as it is of interest to professional mathematicians. However, it is conceivable that there may be something in it as obvious as the principle of duality which has been overlooked.”*²

Indeed Marshall Hall’s 1943 article where he coordinatizes projective planes with ternary rings — and the subsequent charting of non-Desarguesian geometry, finite or not — would probably qualify in Bell’s own opinion as a brilliantly obvious development.

Before we leave the history of our subject, and take up its close study, we would like to identify our text and its place in this large mosaic. According to Philip Davis a course very similar to ours was taught for many years at Harvard University by Oscar Zariski, a well-known algebraic geometer who emphasized the role of commutative rings in this subject. Robin Hartshorne gave a similar course at Harvard in the 60’s and wrote up his lecture notes in [Hartshorne]. We are indebted to [Hartshorne], from which we learned the present subject ourselves before teaching it in the same tradition. Our hearty thanks to Gestur Olafsson for recommending these notes to us.

Lars Kadison
Roskilde University
DK-4000 Roskilde, Denmark
kadison@fatou.ruc.dk

Matthias T. Kromann
Roskilde University
DK-4000 Roskilde, Denmark
kromann@euler.ruc.dk

²*Bell continues encouragingly “In any event it is an easy subject to acquire and one of fascinating delight to amateurs and even to professionals at some stage of their careers.”*

Contents

Preface	i
Historical Foreword	v
1 Affine Planes	1
1.1 Affine Geometry	2
1.2 Transformations of the Affine Plane	5
2 Projective Planes	13
2.1 Completion of the Affine Plane	13
2.2 Homogeneous Coordinates for the Real Projective Plane	15
3 Desargues' Theorem	23
3.1 Moulton's Example	26
3.2 Axioms for Projective Space	28
4 A Brief Introduction to Groups	31
4.1 Elements of Group Theory	31
4.2 Automorphisms of the Projective Plane of Seven Points	36
5 Elementary Synthetic Projective Geometry	43
5.1 Principle of Duality	43
5.2 Fano's Axiom	47
5.3 Harmonic Points	49
5.4 Perspectivities and Projectivities	55

6	The Fundamental Theorem for Projectivities on a Line	65
6.1	Geometry of Complex Numbers	68
6.2	Pappus' Theorem	71
7	A Brief Introduction to Division Rings	79
7.1	The Quaternions \mathbb{H}	82
7.2	A Noncommutative Division Ring with Characteristic p .	85
8	Projective Planes over Division Rings	93
8.1	The Automorphism Group of $\mathbb{P}^2(R)$	95
8.2	The Algebraic Meaning of Axioms P6 and P7	107
8.3	Independence of Axioms	110
9	Introduction of Coordinates in a Projective Plane	113
9.1	The Major and Minor Desargues' Axioms	115
9.2	Division Ring Number Lines	121
9.3	Introducing Coordinates in \mathbb{A}	125
10	Möbius Transformations and Cross Ratio	133
10.1	Assessment	133
10.2	The Group of Möbius Transformations of the Extended Field	134
10.3	$PJ(\ell) \cong PGL(1, \mathbb{F})$	137
10.4	Cross Ratio: a Projective Invariant	140
11	Projective Collineations	147
11.1	Elations and Homologies	149
11.2	The Fundamental Theorem of Projective Collineation . .	151
11.3	$PC(\pi) \cong PGL(2, \mathbb{F})$	154
11.4	Ceva's Theorem	157

Independent Studies in Projective Geometry	165
A Conics	169
B Algebraic Curves and Bezout's Theorem	175
B.1 Intersection Theory of Algebraic Curves	178
C Elliptic Geometry	185
C.1 The Incidence Geometry of the Hyperbolic Plane	189
D Ternary Rings	193
D.1 Addition	197
D.2 Multiplication	198
 Annotated Bibliography	 203
 Index	 206

Chapter 1

Affine Planes

Projective geometry developed from considerations of geometric properties invariant under central projection. Properties of incidence such as "collinearity of points", "concurrency of lines" and "triangle" are invariants under central projection, while ordinary notions of distance, angle, and parallelism are noninvariants, as they are visibly distorted under central projection. Thus in the axiomatic development of the theory our focus is on properties of incidence without parallelism.

However, one of the most important examples of the theory is the real projective plane. There we will use all techniques available to us from Euclidean geometry and analytic geometry in order to see what is true or not true.

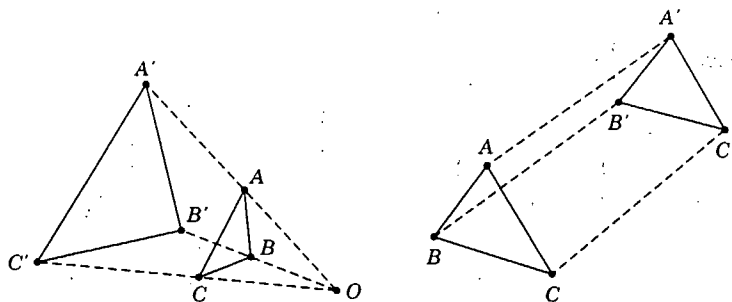


Figure 1.1. Central and parallel projection.

1.1 Affine Geometry

As the center of projection of one plane to another moves far enough away we become concerned with invariants of figures under parallel projection. In this limiting case, parallel lines project to parallel lines as one may see by taking different sections of two parallel planes. Let us then start out on our path toward projective geometry with some of the most elementary facts of ordinary plane geometry, which we take as axioms for our synthetic development.

DEFINITION. An *affine plane* is a set, whose elements are called *points*, and a set of subsets, called *lines*, satisfying the following three axioms, A1–A3. We will use the terminology “ P lies on ℓ ” or “ ℓ passes through P ” to mean the point P is an element of the line ℓ .

- A1.** Given two distinct points P and Q , there is one and only one line containing both P and Q .
- A2.** Given a line ℓ and a point P , not on ℓ , there is one and only one line m , having no point in common with ℓ , and passing through P .
- A3.** There exist three non-collinear points.

A set of points P_1, \dots, P_n is said to be *collinear* if there exists a line ℓ containing them all. We say that two lines are *parallel* if they are equal, or if they have no points in common.

Notation

$P \neq Q$	P is not equal to Q
$P \in \ell$	P lies on ℓ
$\ell \cap m$, $\ell.m$	the intersection of ℓ and m
$\ell \parallel m$	ℓ is parallel to m
PQ , $P \cup Q$	line through P and Q
$\#(S)$	number of elements in a finite set S
$X - B$	the complement of B in X

EXAMPLE. The ordinary plane, known to us from Euclidean geometry, satisfies the axioms A1–A3, and therefore is an affine plane, the *real affine plane*.

A convenient way of representing this plane is by introducing Cartesian coordinates, as in analytic geometry. Thus a point P is represented as an ordered pair (x, y) of real numbers. A line is the solutions (x, y) of linear equations $y = mx + b$ or $x = a$.

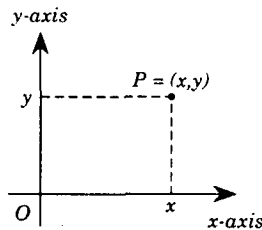


Figure 1.2. The ordinary plane.

DEFINITION. A relation \sim on a set $S = \{a, b, c, \dots\}$ is an *equivalence relation* if it has the following three properties:

- 1) *Reflexive*: $a \sim a$
- 2) *Symmetric*: $a \sim b \implies b \sim a$
- 3) *Transitive*: $a \sim b$ and $b \sim c \implies a \sim c$

The *equivalence class* $[a]$ of a is the subset of elements equivalent to a : $[a] = \{b \in S \mid b \sim a\}$.

PROPOSITION 1.1. *Parallelism is an equivalence relation.*

Proof. We must check the three properties

- 1) Any line is parallel to itself, by definition.
- 2) $\ell \parallel m \implies m \parallel \ell$ by definition.
- 3) If $\ell \parallel m$ and $m \parallel n$, we wish to prove $\ell \parallel n$. If $\ell = n$, there is nothing to prove. If $\ell \neq n$, and there is a point $P \in \ell \cap n$, then ℓ, n are both $\parallel m$, and pass through P , which is impossible, by Axiom A2. We conclude that $\ell \cap n = \emptyset$, and so $\ell \parallel n$. \square

PROPOSITION 1.2. *Two distinct lines have at most one point in common.*

Proof. For if ℓ and m both pass through two distinct points P and Q , then $\ell = m$ by Axiom A1. \square

EXAMPLE. There is an affine plane with four points.

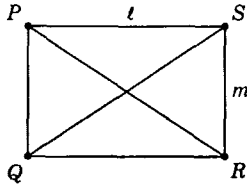


Figure 1.3. The affine plane of 4 points.

Indeed, by A3 there are three non-collinear points. Call them P , Q , R . By A2 there is a line ℓ through P , parallel to the line QR , which exists by A1. Similarly, there is a line $m \parallel PQ$, passing through R .

Now, ℓ is not parallel to m ($\ell \not\parallel m$). For if it were, then we would have $PQ \parallel m \parallel \ell \parallel QR$ and hence $PQ \parallel QR$ by Proposition 1.1. This is impossible, however, because $PQ \neq QR$, and both contain Q .

Hence ℓ must meet m in some point S . Since S lies on m , which is parallel to PQ , and different from PQ , S does not lie on PQ , so $S \neq P$, and $S \neq Q$. Similarly $S \neq R$. Thus S is indeed a fourth point.

Now consider the lines PR and QS . It may happen that they meet (for example in the Euclidean plane they will). On the other hand, it is consistent with the axioms to assume that they do not meet.

In that case we have an affine plane consisting of four points P , Q , R , S , and six lines PQ , PR , PS , QR , QS , RS , and one can verify easily the axioms A1–A3. This is the smallest affine plane.

DEFINITION. A *pencil of lines* is either

- 1) the set of all lines passing through some point P ,
- or
- 2) the set of all lines parallel to some line ℓ .

In the second case we speak of a *pencil of lines*!of parallel lines.

DEFINITION. A *one-to-one correspondence* between two sets X and Y is a mapping $T: X \rightarrow Y$ (i.e. a rule T , which associates to each element x of the set X one element $T(x) = y \in Y$) such that $x_1 \neq x_2$ implies that $Tx_1 \neq Tx_2$, and such that for all $y \in Y$ there exists $x \in X$ such that $T(x) = y$. A one-to-one correspondence of a set X with itself is called a *permutation* of X .

1.2 Transformations of the Affine Plane

Notice that any other labelling of the 4 points in Figure 1.3 with the letters P, Q, R , and S would induce a permutation of $\{P, Q, R, S\}$ that sends lines to lines and preserves parallelism. For example, exchanging P and Q sends lines PR and QS to lines QR and PS , respectively. However, the resulting sets of points and lines is the same as before. In addition, a new labelling of points in the real affine plane coming from a change in coordinate axes is itself a permutation of \mathbb{R}^2 , given by

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$$

where $a_{11}a_{22} - a_{12}a_{21} \neq 0$; or in more compact matrix and vector notation we could write $v' = Av + b$ where $\det A \neq 0$. A is the transition matrix between old and new bases.

Now, true affine invariants should not depend on the labelling of points in an affine plane. In the next definition we give the precise meaning of "relabelling a geometry."

DEFINITION. Let \mathbb{A} be an affine plane. An *automorphism* ϕ of \mathbb{A} is a permutation of \mathbb{A} sending collinear points to collinear points.

CONVENTION. We will often say an automorphism ϕ transforms a point P to P' , point Q to Q' , line ℓ to ℓ' , i.e. $\phi(P) = P'$, $\phi(Q) = Q'$, $\phi(\ell) = \ell'$, so priming a lettered point or line is used to denote the image point or line under ϕ . In addition, different notations stand for distinct elements: $P, Q \in \mathbb{A}$ will mean $P \neq Q$ unless stated otherwise.

REMARK. It follows from elementary considerations that given a line $\ell = PQ$, ϕ is a one-to-one correspondence between the sets of points ℓ and ℓ' .

We observe that an automorphism satisfies the two "algebraic" conditions

- 1) $\phi(P \cup Q) = \phi(P) \cup \phi(Q)$ ($\forall P, Q$)
- 2) $\phi(\ell.m) = \phi(\ell).o(m)$ ($\forall \ell, m: \ell \nparallel m$)

PROPOSITION 1.3. *An automorphism transforms parallel lines to parallel lines.*

Proof. Suppose $PQ \parallel RS$ in an affine plane \mathbb{A} . If $B' \in P'Q' \cap R'S'$, then by the remark $B' \in PQ \cap RS$, so $PQ = RS$. Hence $P'Q' = R'S'$. If $P'Q'$ and $R'S'$ had no point in common they would be parallel, leaving no more to prove. \square

PROPOSITION 1.4. *The set of automorphisms $\text{Aut } \mathbb{A}$ is closed under composition and inversion.*

Proof. We would like see that $\phi, \psi \in \text{Aut } \mathbb{A}$ imply $\phi \circ \psi \in \text{Aut } \mathbb{A}$ and $\phi^{-1} \in \text{Aut } \mathbb{A}$. Now both $\phi \circ \psi$ and ϕ^{-1} are permutations of \mathbb{A} . We check lines go to lines.

If P, Q , and R are collinear, then $\psi(P), \psi(Q)$, and $\psi(R)$ are collinear and so is $\phi(\psi(P)), \phi(\psi(Q))$, and $\phi(\psi(R))$. Also, $P = \phi(A)$, $Q = \phi(B)$, and $R = \phi(C)$ for three points $A, B, C \in \mathbb{A}$ and A, B , and C are collinear (otherwise $AB \neq BC$ so $PQ \neq QR$ as lines). But $A = \phi^{-1}(P)$, $B = \phi^{-1}(Q)$, and $C = \phi^{-1}(R)$ so ϕ^{-1} also takes lines to lines. \square

We now study some special automorphisms in affine geometry that are needed later.

DEFINITION. Let \mathbb{A} be an affine plane. A *dilatation* is an automorphism $\phi: x \mapsto x'$ of \mathbb{A} , such that for any two distinct points P, Q ,

$$PQ \parallel P'Q'.$$

In other words, ϕ takes each line into a parallel line.

EXAMPLES. In the real affine plane $\mathbb{A}^2(\mathbb{R}) = \{(x, y) \mid x, y \in \mathbb{R}\}$, a stretching in the ratio k , given by equations

$$(x, y) \mapsto (x', y'): \begin{cases} x' = kx \\ y' = ky \end{cases}$$

is a dilatation. Indeed, let O be the point $(0, 0)$ then ϕ stretches points away from O k -times, and if P, Q are any two points, clearly $PQ \parallel P'Q'$, by similar triangles.

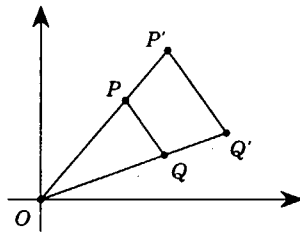


Figure 1.4. Stretching.

Another example of a dilatation of $\mathbb{A}^2(\mathbb{R})$ is given by a translation

$$\begin{cases} x' = x + a \\ y' = y + b \end{cases}$$

In this case, any point P is translated by the vector (a, b) , so $PQ \parallel P'Q'$ again, for any P, Q .

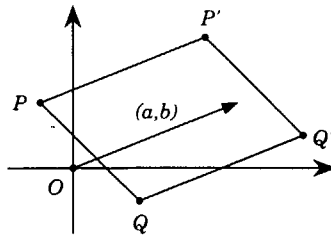


Figure 1.5. Translation.

Without asking for the moment whether there *are* any non-trivial dilatations in a given affine plane \mathbb{A} , let us study some of their properties.

PROPOSITION 1.5. *Let \mathbb{A} be an affine plane. Then the set of dilatations, $\text{Dil } \mathbb{A}$, is closed under composition and inversion.*

Proof. Indeed, we must see that the product of two dilatations is a dilatation, and that the inverse of a dilatation is a dilatation. This follows immediately from the fact that parallelism is an equivalence relation. \square

PROPOSITION 1.6. *A dilatation which leaves two distinct points fixed is the identity.*

Proof. Let ϕ be a dilatation, let P, Q be fixed, and let R be any point not on PQ . Let $\phi(R) = R'$. Then we have $PR \parallel PR'$ and $QR \parallel QR'$ since ϕ is a dilatation. Hence $R' \in PR$ and $R' \in QR$. But $PR \neq QR$ since $R \notin PQ$. Hence $PR \cdot QR = R$, and so $R = R'$, i.e. R is also fixed. But R was an arbitrary point not on PQ . Applying the same argument to P and R , we see that every point of PQ is also fixed. so ϕ is the identity. \square

COROLLARY 1.7. *A dilatation is determined by the images of two points, i.e. any two dilatations ϕ, ψ , which behave the same way on two distinct points P, Q , are equal.*

Proof. Indeed, $\psi^{-1}\phi$ leaves P, Q fixed, so is the identity. \square

So we see that a dilatation different from the identity can have at most one fixed point. We have a special name for those dilatations with no fixed points:

DEFINITION. A *translation* is a dilatation with no fixed points, or the identity.

PROPOSITION 1.8. *If ϕ is a translation, different from the identity, then for any two points P, Q , we have $PP' \parallel QQ'$, where $\phi(P) = P'$, $\phi(Q) = Q'$.*

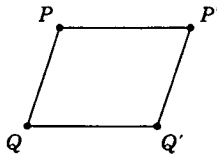
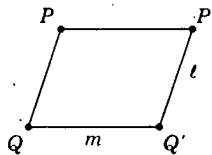


Figure 1.6. Translation.

Proof. Suppose $PP' \nparallel QQ'$. Then these two lines intersect in a point O . But the fact that ϕ is a dilatation implies that ϕ sends the line PP' into itself, and ϕ sends QQ' into itself. (For example, let $R \in PP'$. Then $PR \parallel P'R'$, but $PR = PP'$, so $R' \in PP'$). Hence $\phi(O) = O$, a contradiction. \square

PROPOSITION 1.9. *The translations of \mathbb{A} form a subset $\text{Tran } \mathbb{A}$ of the set of dilatations of \mathbb{A} , which is closed under composition and inversion. Furthermore, for any $\tau \in \text{Tran } \mathbb{A}$, and $\sigma \in \text{Dil } \mathbb{A}$, $\sigma\tau\sigma^{-1} \in \text{Tran } \mathbb{A}$.*

Proof. First we must check that the product of two translations is a translation, and the inverse of a translation is a translation. Let τ_1, τ_2 be translations, then $\tau_1\tau_2$ is a dilatation. Suppose it has a fixed point P . Then $\tau_2(P) = P'$, $\tau_1(P') = P$. If Q is any point not on PP' , then let $Q' = \tau_2(Q)$.

Figure 1.7. Q' is the intersection of ℓ and m .

We have by the previous Proposition $PQ \parallel P'Q'$ and $PP' \parallel QQ'$. Hence Q' is determined as the intersection of the line $\ell \parallel PQ$ through P' , and the line $m \parallel PP'$ through Q .

For a similar reason, $\tau_1(Q') = Q$. Hence $\tau_1\tau_2$ leave P and Q fixed, so by our proposition $\tau_1\tau_2 = \text{id}$. Hence $\tau_1\tau_2$ is a translation. Clearly

the inverse of a translation is a translation, so the translations form a subset of $\text{Dil } \mathbb{A}$, which is closed under composition and inverse.

Now let $\tau \in \text{Tran } \mathbb{A}$, $\sigma \in \text{Dil } \mathbb{A}$. Then $\sigma\tau\sigma^{-1}$ is certainly a dilatation. If it has no fixed points, it is a translation. If it has a fixed point P , then $\sigma\tau\sigma^{-1}(P) = P$ implies $\tau\sigma^{-1}(P) = \sigma^{-1}(P)$, so τ has a fixed point. Hence $\tau = \text{id}$, and $\sigma\tau\sigma^{-1} = \text{id}$. \square

The question of existence of translations and central dilatations between arbitrary pairs of points is taken up in chapter 9.

EXERCISES

EXERCISE 1.1. Given a 2×2 real matrix \mathbf{A} with nonzero determinant and 2×1 real column vector \mathbf{b} , define an *affine transformation* T to be the bijection of \mathbb{R}^2 with itself given by $T(\mathbf{x}) = \mathbf{A}\mathbf{x} + \mathbf{b}$. Show that T is an automorphism of the real affine plane.

EXERCISE 1.2. A *shear* T is an affine transformation taking Q to R , fixing every point on another line parallel to QR . By translating and changing basis, find a matrix \mathbf{A} and vector \mathbf{b} such that $T(\mathbf{x}) = \mathbf{A}\mathbf{x} + \mathbf{b}$.

EXERCISE 1.3. An *affine reflection* is an affine transformation T that interchanges two points Q and R and fixes a third point P not on QR . Show that T fixes every point on PM , where M is the midpoint of the line segment QR .

EXERCISE 1.4. An *isometry* T of the Euclidean plane is a mapping of \mathbb{R}^2 onto itself that preserves distance: i.e. if $d(P, Q)$ denotes the Euclidean distance from P to Q , then

$$d(T(P), T(Q)) = d(P, Q) \quad (\forall P, Q).$$

Show that T sends lines to lines.

EXERCISE 1.5. Show that any two pencils of parallel lines in an affine plane have the same cardinality (i.e. that one can establish a one-to-one correspondence between them). Show that this is also the cardinality of the set of points on any line.

EXERCISE 1.6. If there is a line with exactly n points, show that the number of points in the whole affine plane is n^2 .

EXERCISE 1.7. Construct an affine plane with 16 points.

Hint. We know from Exercise 1.5 that each pencil of parallel lines has four lines in it. Let a, b, c, d be one pencil of parallel lines, and let 1, 2, 3, 4 be another. Then label the intersections $A_1 = a \cap 1$, etc. To construct the plane, you must choose other subsets of four points to be the lines in the three other pencils of parallel lines. Write out each line explicitly, by naming its four points, e.g. the line 2 = $\{A_2, B_2, C_2, D_2\}$.

EXERCISE 1.8. Euler in 1782 posed the following problem: "A meeting of 36 officers of six different ranks and from six different regiments must be arranged in a square in such a manner that each row and each column contains 6 officers from different regiments and of different ranks." G. Tarry in 1901 confirmed Euler's prediction that this problem has no solution. Deduce from Tarry's fact that there is no affine plane with 36 points.

EXERCISE 1.9. How many ways are there to label the points in Figure 1.3 with the letters P, Q, R , and S ? How many automorphisms of this affine plane are there?

EXERCISE 1.10. A *partition* of a set S is a set of subsets of S , $\{X_1, \dots, X_n, \dots\}$, such that $\bigcup X_i = S$ and $X_i \cap X_j = \emptyset$ whenever $i \neq j$.

a) Show that the set of equivalence classes of a set S is a partition of S .

b) Conversely, show that a partition of S naturally determines an equivalence relation on S .

EXERCISE 1.11. Suppose τ is a translation of an affine plane \mathbb{A} such that $\tau(P) = P'$. Suppose Q is a point not on the line PP' . Show that $Q' := \tau(Q)$ may be obtained by the following parallelogram construction:

Let $\ell \parallel PP'$ such that $Q \in \ell$. Let $m \parallel PQ$ such that $P' \in m$. Then $Q' \in \ell m$.

Chapter 2

Projective Planes

There are two points of view as to why we should avoid parallel lines in planar geometry. One is that lines and indeed higher degree polynomial curves should intersect in the “right” number of points: two lines, for instance, usually intersect in one point and should therefore do so at all times. This leads to the introduction of a common “ideal point” to each line in a pencil of parallels.

The second point of view stems from the art of perspective which holds that a two or three dimensional figure should be united with the eye of the observer O by lines to produce a “cone” over the figure. A drawing of the figure corresponds to a planar cross section of this cone. The cone over parallel lines is two planes intersecting in a line through O , cross sections of which generally are two intersecting lines. This point of view leads to homogeneous coordinates for the real projective plane.

We will show in Proposition 2.2 that the two points of view on the real projective plane are equivalent in a certain strictly defined sense.

2.1 Completion of the Affine Plane

We will now complete the affine plane by adding certain “points at infinity” and thus arrive at the notion of the projective plane.

Let \mathbb{A} be the affine plane. For each line $\ell \in \mathbb{A}$, we will denote by $[\ell]$ the pencil of lines parallel to ℓ . To each pencil of parallels $[\ell]$ we add to \mathbb{A} an *ideal point*, or *point at infinity in the direction of ℓ* , which we denote by $P_{[\ell]}$.

We define the *completion* \mathbb{S} of \mathbb{A} as follows. The *points* of \mathbb{S} are the points of \mathbb{A} , plus all the ideal points of \mathbb{A} . A *line* in \mathbb{S} is either

- a) An ordinary line ℓ of \mathbb{A} , plus the ideal point $P_{[\ell]}$ of ℓ , or
- b) the "line at infinity", consisting of all the ideal points of \mathbb{A} .

We will see shortly that \mathbb{S} is a projective plane, in the sense of the following definition.

DEFINITION. A *projective plane* \mathbb{S} is a set, whose elements are called points, and a set of subsets, called lines, satisfying the following four axioms.

- P1.** Two distinct points P, Q of \mathbb{S} lie on one and only one line.
- P2.** Two distinct lines meet in precisely one point.
- P3.** There exist three non-collinear points.
- P4.** Every line contains at least three points.

PROPOSITION 2.1. *The completion \mathbb{S} of an affine plane \mathbb{A} , as described above, is a projective plane.*

Proof. We must verify the four axioms P1–P4 of the definition.

P1. Let $P, Q \in \mathbb{S}$. 1) If P, Q are ordinary points of \mathbb{A} , then P and Q lie on only one line of \mathbb{A} . They do not lie on the line at infinity of \mathbb{S} , hence they lie on only one line of \mathbb{S} . 2) If Q is an ordinary point, and $P_{[\ell]}$ is an ideal point, we can find by A2 a line m such that $Q \in m$, and $m \parallel \ell$, i.e. $m \in [\ell]$, so that $P_{[\ell]}$ lies on the extension of m to \mathbb{S} . This is clearly the only line of \mathbb{S} containing P and Q . 3) If P, Q are both ideal points, then they both lie on the line "at infinity", the only line of \mathbb{S} containing them.

P2. Let ℓ, m be lines. 1) If they are both ordinary lines, and $\ell \nparallel m$, then they meet in a point of \mathbb{A} . If $\ell \parallel m$, then the ideal point $P_{[\ell]}$ lies on both ℓ and m in \mathbb{S} . 2) If ℓ is an ordinary line, and $m = \ell_\infty$ is the line at infinity, then $P_{[\ell]}$ lies on both ℓ and m .

P3. Follows immediately from A3. One must check only that if P, Q, R are non-collinear in \mathbb{A} , then they are also non-collinear in \mathbb{S} . Indeed, the only new line is the line at infinity, which contains none of them.

P4. It is easy to see that each line of \mathbb{A} contains at least two points. But in \mathbb{S} it has also an ideal point, so any line has at least three points. (It follows from Exercise 1.5 that ℓ_∞ has at least three points). \square

EXAMPLE 1. By completing the real affine plane of Euclidean geometry, we obtain the real projective plane.

EXAMPLE 2. By completing the affine plane of 4 points, we obtain a projective plane with 7 points.

EXAMPLE 3. Another example of a projective plane can be constructed as follows: let \mathbb{R}^3 be ordinary Euclidean 3-space, and let O be a point of \mathbb{R}^3 . Let S be the set of lines through O . We define a *point* of S to be a line through O in \mathbb{R}^3 . We define a *line* of S to be the collection of lines through O which all lie in some plane through O . Then S satisfies the axioms P1-P4 (Exercise 2.7), and so it is a projective plane.

2.2 Homogeneous Coordinates for the Real Projective Plane

We can give an analytic definition of the real projective plane as follows. We consider Example 3 given above of lines in \mathbb{R}^3 . A point of \mathbb{S} is a line through the origin O . We will represent the point P of \mathbb{S} corresponding to ℓ by choosing any point (x_1, x_2, x_3) on ℓ different from the point $(0, 0, 0)$. The numbers x_1, x_2, x_3 are *homogeneous coordinates* of P . Any other point of ℓ has the coordinates $(\lambda x_1, \lambda x_2, \lambda x_3)$, where $\lambda \in \mathbb{R}$, $\lambda \neq 0$. Thus \mathbb{S} is the collection of triples (x_1, x_2, x_3) of real numbers,

not all zero, and two triples (x_1, x_2, x_3) and (x'_1, x'_2, x'_3) represent the same point if and only if there exists $\lambda \in \mathbb{R}$ such that $x'_i = \lambda x_i$ for $i = 1, 2, 3$. Since the equation of a plane in \mathbb{R}^3 passing through O is of the form

$$a_1x_1 + a_2x_2 + a_3x_3 = 0 \quad (\text{not all } a_i = 0)$$

we see that this is also the equation of a line of \mathbb{S} , in terms of the homogeneous coordinates.

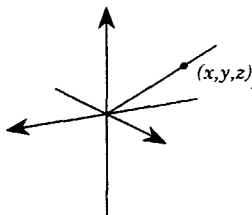


Figure 2.1. Homogeneous coordinates.

DEFINITION. Two projective planes \mathbb{S} and \mathbb{S}' are *isomorphic* if there exists a one-to-one correspondence $T: \mathbb{S} \rightarrow \mathbb{S}'$ which takes collinear points into collinear points. T is referred to as an *isomorphism*; or as an *automorphism* if $\mathbb{S}' = \mathbb{S}$.

PROPOSITION 2.2. *The projective plane \mathbb{S} defined by homogeneous coordinates which are real numbers, as above, is isomorphic to the projective plane obtained by completing the ordinary affine plane of Euclidean geometry.*

Proof. On the one hand, we have \mathbb{S} , whose points are given by homogeneous coordinates (x_1, x_2, x_3) , $x_i \in \mathbb{R}$, not all zero. On the other hand, we have the Euclidean plane \mathbb{A} , with Cartesian coordinates (x, y) . Let us call the completion \mathbb{S}' . Thus the points of \mathbb{S}' are the points (x, y) of \mathbb{A} (with $x, y \in \mathbb{R}$), plus the ideal points. Now a pencil of parallel lines is uniquely determined by its slope m , which may be any real number, or ∞ . Thus the ideal points are described by coordinate m .

Now we will define a mapping $T: \mathbb{S} \rightarrow \mathbb{S}'$ which will exhibit the isomorphism of \mathbb{S} and \mathbb{S}' . Let $(x_1, x_2, x_3) = P$ be a point of \mathbb{S} .

1) If $x_3 \neq 0$, we define $T(P)$ to be the point of \mathbb{A} with coordinates $x = x_1/x_3$, $y = x_2/x_3$. Note that this is uniquely determined, because if we replace (x_1, x_2, x_3) by $(\lambda x_1, \lambda x_2, \lambda x_3)$, then x and y do not change. Note also that every point of \mathbb{A} can be obtained in this way. Indeed, the point with coordinates (x, y) is the image of the point of \mathbb{S} with homogeneous coordinates $(x, y, 1)$.

2) If $x_3 = 0$, then we define $T(P)$ to be the ideal point of \mathbb{S}' with slope $m = x_2/x_1$. Note that this makes sense if we set $x_2/0 = \infty$, because x_1 and x_2 cannot both be zero. Again replacing $(x_1, x_2, 0)$ by $(\lambda x_1, \lambda x_2, 0)$ does not change m . Also each value of m occurs: If $m \neq \infty$, we take $T(1, m, 0)$, and if $m = \infty$, we take $T(0, 1, 0)$.

Thus T is a one-to-one mapping of \mathbb{S} into \mathbb{S}' . We must check that T takes collinear points into collinear points. A line ℓ in \mathbb{S} is given by an equation

$$a_1x_1 + a_2x_2 + a_3x_3 = 0$$

1) Suppose that a_1 and a_2 are not both zero. Then for those points with $x_3 = 0$, namely the point given by $x_1 = \lambda a_2$, $x_2 = -\lambda a_1$, T of this point is the ideal point given by the slope $m = -a_1/a_2$, which indeed is on a line in \mathbb{S}' with the finite points.

2) If $a_1 = a_2 = 0$, ℓ has the equation $x_3 = 0$. Any point of \mathbb{S} with $x_3 = 0$ goes to an ideal point of \mathbb{S}' , and these form a line. \square

REMARK. From now on, we will not distinguish between the two isomorphic planes of Proposition 2.2: we will call it the *real projective plane* and denote it by $\mathbb{P}^2(\mathbb{R})$. It will be the most important example of the axiomatic theory we are going to develop, and we will often check results of the axiomatic theory in this plane by way of example. Similarly, theorems in the real projective plane can give motivation for results in the axiomatic theory. However, to establish a theorem in our theory, *we must derive it from the axioms and from previous theorems*. If we find that it is true in the real projective plane, that is evidence in favor of the theorem, but does not constitute a proof in our set-up.

Also note that if we remove any line from the real projective plane, we obtain the Euclidean plane. Here is a nice application of that idea. Consider the *conic* in the real projective plane given by $\{(x, y, z) \mid x^2 + y^2 - z^2 = 0\}$. Removing the lines $z = 0$, $y = 0$, or $z - y = 0$, we

obtain a circle, hyperbola, or parabola (respectively) in the Euclidean plane: these are the “conic sections” of the planes $z = 1$, $y = 1$, and $z - y = 1$, respectively.

THE SPHERE MODEL

Consider some basic facts about the standard sphere

$$S^2 = \{ (x_1, x_2, x_3) \mid x_1^2 + x_2^2 + x_3^2 = 1 \}.$$

Lines in \mathbb{R}^3 through the origin intersect S^2 in antipodal points, and planes through the origin intersect S^2 in the great circles. Conversely, antipodal points on S^2 , $\pm(x_1, x_2, x_3)$, lie on one line through the origin; and a great circle on S^2 is coplanar with the origin.

Now define a projective plane \mathbb{S}'' as follows: a point is a pair of antipodal points on S^2 , and a line is a set of points lying on a great circle on S^2 . We have just set up an isomorphism between the projective plane of homogeneous coordinates \mathbb{S} and \mathbb{S}'' . (What is it?) \mathbb{S}'' is a third model for the real projective plane.

NOTE. The sphere model \mathbb{S}'' of the real projective plane is a topological favorite. By considering a hemisphere and pinching antipodal points together on the boundary, one can see how exotic the real projective plane is topologically. It is a nonorientable surface, embeddable in \mathbb{R}^4 but not in \mathbb{R}^3 . It is topologically equivalent to a Möbius strip with a disk attached to its boundary: to see this, remove a cap around the pole of the upper hemisphere, remove the image of cap under the antipode map $v \mapsto -v$ from the lower hemisphere, and visualize the rest of \mathbb{S}'' as a circular band with antipodal points identified — now half of this circular band is a straight band whose ends are placed together with the well-known Möbius twist.

EXERCISES

EXERCISE 2.1. Discuss the possible systems of points and lines which satisfy P1, P2, P3, but not P4.

EXERCISE 2.2. Let \mathbb{S} be a projective plane, and let ℓ be a line of \mathbb{S} . Define \mathbb{S}_0 to be the points of \mathbb{S} not on ℓ , and define lines in \mathbb{S}_0 to be the restrictions of lines in \mathbb{S} . Prove (using P1–P4) that \mathbb{S}_0 is an affine plane. Prove also that \mathbb{S} is isomorphic to the completion of the affine plane \mathbb{S}_0 .

EXERCISE 2.3. a) Prove that the projective plane of 7 points, obtained by completing the affine plane of four points, is the smallest possible projective plane.

b) Show that two projective planes of 7 points are isomorphic.

EXERCISE 2.4. If one line in a projective plane has n points, find the number of points in the projective plane.

EXERCISE 2.5. a) Give a proof that the axioms P1, P2, P3, and P4 of a projective plane imply the statement

Q: "There are four points, no three of which are col-linear"

b) Prove also that P1, P2, and Q imply P3 and P4.

EXERCISE 2.6. A) In the real projective plane, what is the equation of the line

a) joining the points $(1, 0, 1)$ and $(1, 2, 3)$?

b) joining the points $(0, 3, 9)$ and $(0, 25, 43)$?

c) joining the points (a_1, a_2, a_3) and (b_1, b_2, b_3) ?

B) What is the point of intersection

a) of the lines

$$\begin{aligned}x_1 - x_2 + 2x_3 &= 0 \\3x_1 + x_2 + x_3 &= 0 \quad ?\end{aligned}$$

b) of the lines

$$\begin{aligned}x_1 \quad \quad + x_3 &= 0 \\x_1 + 2x_2 + 3x_3 &= 0 \quad ?\end{aligned}$$

c) of the lines

$$\begin{aligned}A_1x_1 + A_2x_2 + A_3x_3 &= 0 \\B_1x_1 + B_2x_2 + B_3x_3 &= 0 \quad ?\end{aligned}$$

EXERCISE 2.7. Let \mathcal{S} denote the set of lines through some point O in \mathbb{R}^3 . Define points of \mathcal{S} to be lines through O in \mathbb{R}^3 , and define a line of \mathcal{S} to be the set of lines through O which all lie in some plane through O . Prove that \mathcal{S} satisfies P1–P4.

EXERCISE 2.8. Let \mathbf{v} denote a nonzero vector in \mathbb{R}^3 , and think of it as a column vector, or 3×1 matrix, with coordinates v_1, v_2 , and v_3 . Now \mathbf{v} represents a point in $\mathbb{P}^2(\mathbb{R})$ with homogeneous coordinates (v_1, v_2, v_3) .

a) Given a 3×3 matrix \mathbf{A} with real coefficients $a_{11}, \dots, a_{ij}, \dots, a_{33}$, and nonzero determinant, show that the linear transformation of \mathbb{R}^3 , $\mathbf{v} \mapsto \mathbf{A}\mathbf{v}$, determines a mapping $T_{\mathbf{A}}: \mathbb{P}^2(\mathbb{R}) \rightarrow \mathbb{P}^2(\mathbb{R})$ of points given by

$$(v_1, v_2, v_3) \mapsto \left(\sum_{i=1}^3 a_{1i}v_i, \sum_{i=1}^3 a_{2i}v_i, \sum_{i=1}^3 a_{3i}v_i \right).$$

b) Show that if $\lambda \in \mathbb{R} - \{0\}$ then $T_{\mathbf{A}} = T_{\lambda\mathbf{A}}$.

c) Prove that $T_{\mathbf{A}}$ is an automorphism of the projective plane $\mathbb{P}^2(\mathbb{R})$.

Hint. If \mathcal{L} denotes the solution set of $c_1x_1 + c_2x_2 + c_3x_3 = 0$, show that $T_{\mathbf{A}}(\mathcal{L})$ is the solution set of $\sum_{i=1}^3 c'_i x'_i = 0$ where $c'_i = \sum_{j=1}^3 b_{ji}c_j$ and $\mathbf{A}^{-1} = (b_{ij})$. In other words, $T_{\mathbf{A}}$ transforms points by $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ and lines by $\mathbf{c} \mapsto (\mathbf{A}^{-1})^T \mathbf{c}$, where \mathbf{X}^T denotes the transpose of a matrix \mathbf{X} .

EXERCISE 2.9. Refer to Exercise 2.2. Does every automorphism of \mathcal{S} that takes ℓ to ℓ restrict to an automorphism of the affine plane \mathcal{S}_0 ? Conversely, does every automorphism of \mathcal{S}_0 extend to one of the projective plane \mathcal{S} ?

EXERCISE 2.10. Let π be a projective plane of order n , i.e. it has $N := n^2 + n + 1$ points.

a) Show that π has N lines.

Label the points P_1, \dots, P_N and lines ℓ_1, \dots, ℓ_N . Let $a_{ij} = 1$ if point P_i is incident with ℓ_j , and $a_{ij} = 0$ if $P_i \notin \ell_j$. This will define an $N \times N$ matrix $\mathbf{A} = (a_{ij})$ of 0's and 1's called the *incidence matrix* of π .

b) Show that $\mathbf{B} = \mathbf{A}\mathbf{A}^T$ is an $N \times N$ matrix with each diagonal element $b_{ii} = n + 1$ and each off-diagonal element $b_{ij} = 1$.

c) Show the converse of b): Let n be an integer ≥ 2 , let $N := n^2 + n + 1$, and let $\mathbf{A} = (a_{ij})$ be a $N \times N$ matrix with $a_{ij} \in \mathbb{Z}_+ \cup \{0\}$ for all $i, j = 1, \dots, N$. If \mathbf{A} satisfies the equations $\mathbf{A}\mathbf{A}^T = \mathbf{A}^T\mathbf{A} = \mathbf{B}$ (where \mathbf{B} is the matrix defined in b)), then \mathbf{A} is a matrix consisting of 0's and 1's and the incidence matrix of a projective plane.

Chapter 3

Desargues' Theorem

The first main result of projective geometry that we shall study is the theorem of Desargues about triangles in perspective. A *triangle* in an abstract projective plane is determined by three noncollinear points (or equally well by three nonconcurrent lines) — Axiom P3 states the existence of a triangle. Consider the truth value of the following simple statement in an abstract projective plane.

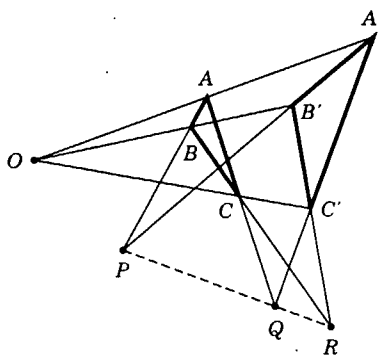


Figure 3.1. Desargues' Axiom.

- P5. (DESARGUES' AXIOM) Let ABC and $A'B'C'$ be two triangles such that the lines joining corresponding vertices, namely AA' , BB' and CC' , meet at a

point O . (We say the two triangles are perspective from O .) Then the three pairs of corresponding sides intersect in three points $P = AB.A'B'$, $Q = AC.A'C'$, and $R = BC.B'C'$ which lie on a line. (We say that triangles ABC and $A'B'C'$ are perspective from the line PQR .)

Now it would not be quite right for us to call this a theorem, because it cannot be proved from our axioms P1–P4. However, we will show that it is true in the real projective plane (and this is the content of “Desargues’ Theorem”). Then we will take this statement as a further axiom, P5, or Desargues’ Axiom, of our abstract projective geometry. We will show by an example that P5 is not a consequence of P1–P4: namely, we will exhibit a geometry that satisfies P1–P4 but not P5. We will sometimes refer to projective planes satisfying Axiom P5 as *Desarguesian*¹ planes.

THEOREM 3.1 (DESARGUES). *In the real projective plane two triangles perspective from a point are perspective from a line.*

Proof. A straightforward computation using homogeneous coordinates follows.² Let triangles ABC and $A'B'C'$ be perspective from the point O , and define the points $P = AB.A'B'$, $Q = AC.A'C'$ and $R = BC.B'C'$ (see Figure 3.1). We must show that P , Q and R are collinear.

Note that no three points of A , B , C and O are collinear; in other words, the coordinates of three of these points will form a linearly independent set of vectors in \mathbb{R}^3 , while the fourth point has coordinates a linear combination of these with no coefficient zero. A simple linear change of coordinates followed by a scaling on the axes allows us with no loss of generality to assume $A = (1, 0, 0)$, $B = (0, 1, 0)$, $C = (0, 0, 1)$ and $O = (1, 1, 1)$. (This can equally well be said using an automorphism of the real projective plane: cf. Exercise 2.8.)

¹Day-sargz-ian

²The student need not view triangles in perspective in the homogeneous coordinate model, which involves visualizations in solid geometry: just take a planar section away from the origin as done in Proposition 2.2. Section 3.2 provides a second, synthetic proof based on viewing Figure 3.1 spatially.

Now $A' \in OA$ which has the parametric equation

$$\lambda(1, 0, 0) + \mu(1, 1, 1) = (\lambda + \mu, \mu, \mu)$$

which is equivalent to $(1 + \frac{\lambda}{\mu}, 1, 1)$ or $(a', 1, 1)$ in homogeneous coordinates. Similarly, $B' = (1, b', 1)$ and $C' = (1, 1, c')$ for some $b', c' \in \mathbb{R}$.

Now we determine coordinates for P , Q and R . The line AB has equation $x_3 = 0$, while $A'B'$ has equation

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ a' & 1 & 1 \\ 1 & b' & 1 \end{vmatrix} = (1 - b')x_1 + (1 - a')x_2 + (a'b' - 1)x_3 = 0.$$

P has homogeneous coordinates satisfying both equations: namely,

$$P = (1 - a', b' - 1, 0).$$

Similarly, we compute AC : $x_2 = 0$, and $A'C'$: $(c' - 1)x_1 + (1 - a'c')x_2 + (a' - 1)x_3 = 0$ with point of intersection

$$Q = (a' - 1, 0, 1 - c').$$

Finally, BC : $x_1 = 0$, and $B'C'$: $(b'c' - 1)x_1 + (1 - c')x_2 + (1 - b')x_3 = 0$ so

$$R = (0, 1 - b', c' - 1).$$

We conclude by noting that P , Q , and R collinear, since the three representative vectors \mathbf{P} , \mathbf{Q} , and \mathbf{R} form a linearly dependent set: using the particular coordinates given above, $\mathbf{P} + \mathbf{Q} + \mathbf{R} = (0, 0, 0)$. Hence \mathbf{P} , \mathbf{Q} , and \mathbf{R} lie on a plane through the origin. \square

DEFINITION. A *configuration* is a set, whose elements are called *points*, and a collection of subsets, called *lines*, which satisfies the following axiom:

C1. Two distinct points lie on at most one line.

It follows that two distinct lines have at most one point in common. Note however that two points may have no line joining them. Projective planes, affine planes, and the next example are configurations.

EXAMPLE. Desargues' configuration has a lot of symmetry: refer to Figure 3.1. It consists of 10 points and 10 lines. Each point lies on three lines, and each line contains 3 points. Thus it may be given the symbol (10_3) . Also, the role of the various points is not fixed. Any one of the ten points can be taken as the center of perspectivity of two triangles (Exercise 3.7). In Exercises 4.10, 4.11, and 4.12, we will see that the "automorphism group" is the full group of permutations on five letters, which is related to viewing Figure 3.1 spatially and noting five planes.

3.1 Moulton's Example

We now give an example of a non-Desarguesian projective plane, that is, a plane satisfying P1-P4, but not P5. This will show that P5 is not a logical consequence of P1-P4.

A very simple idea for making Desargues' Axiom fail in a projective plane is to let the line QR in Desargues' configuration (Figure 3.1) veer away from P ; and this simple idea can be made to work! At the level of axioms P1-P4, lines are still, with few restrictions, the things we define them to be, and need not look much like the "shortest path between points."

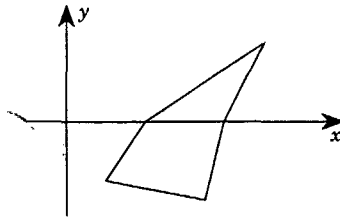


Figure 3.2. A Moulton triangle.

We define on \mathbb{R}^2 an alternative affine plane A' . Points, vertical lines, and lines of negative slope are the same in A' as in the Euclidean affine plane. However, lines of positive slope are not admitted in A' . Rather a line of slope $m > 0$ in the lower half-plane is pasted together at the

x -axis with a line of slope $m/2$ in the upper half-plane. Analytically these Moulton lines are given by

$$f(x) = \begin{cases} m(x - x_0) & \text{if } x \leq x_0 \\ \frac{m}{2}(x - x_0) & \text{if } x > x_0 \end{cases} \quad (\forall x_0 \in \mathbb{R}).$$

It is easy to see that two points in \mathbb{A}' are joined by lines if they give a negative slope or lie vertically; in Exercise 3.1 you will be asked to check the existence of a Moulton line if the two points give a positive slope. Axiom A2 is verified by taking any line ℓ of \mathbb{A}' , a point P off ℓ , and drawing a line m through P with the same slope as ℓ in the upper and lower halfplanes: so, clearly $m \parallel \ell$ in \mathbb{A}' . A3 is a triviality.

Now complete \mathbb{A}' to \mathbb{P}' , a projective plane (cf. Proposition 2.1). Arrange Desargues' configuration in \mathbb{R}^2 so that all points but P lie below the x -axis and so that QR has positive slope. By the ordinary Desargues' Theorem the Moulton line QR does not contain P .

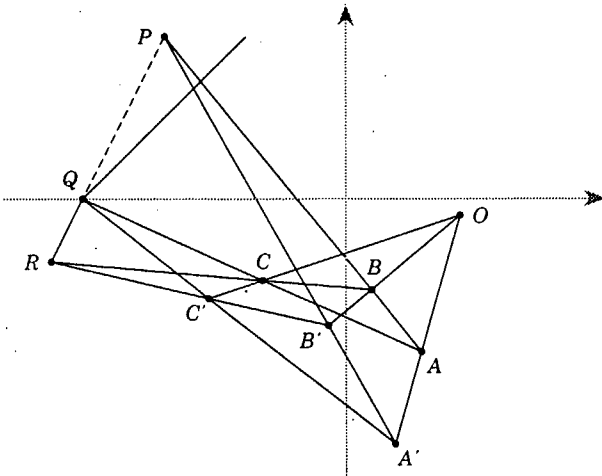


Figure 3.3. The Desargues configuration in the Moulton plane.

3.2 Axioms for Projective Space

DEFINITION. A *projective 3-space* is a set whose elements are called *points*, together with certain subsets called *lines*, and certain other subsets called *planes*, which satisfy the following axioms:

- S1. Two distinct points P, Q lie on one and only one line ℓ .
- S2. Three non-collinear points P, Q, R lie on a unique plane.
- S3. A line meets a plane in at least one point.
- S4. Two planes have at least a line in common.
- S5. There exist four non-coplanar points, no three of which are collinear.
- S6. Every line has at least three points.

EXAMPLE. By a process analogous to that of completing an affine plane to a projective plane, the ordinary Euclidean 3-space can be completed to a projective 3-space, which we call *real projective 3-space* (Exercise 3.6). Alternatively, this same real projective 3-space can be described by homogenous coordinates, as follows. A point is described by a quadruple (x_1, x_2, x_3, x_4) of real numbers, not all zero, where we agree that (x_1, x_2, x_3, x_4) and $(\lambda x_1, \lambda x_2, \lambda x_3, \lambda x_4)$ represent the same point, for any $\lambda \in \mathbb{R} - \{0\}$. A plane is defined by a linear equation $\sum_{i=1}^4 a_i x_i = 0$, not all $a_i = 0$, $a_i \in \mathbb{R}$, and a line is defined as the intersection of two distinct planes. The details of verification of the axioms are left to the reader in Exercise 3.7, and the reader should also check that the lines and points contained in the plane $x_1 = 0$ form the real projective plane defined in section 2.2.

The remarkable fact is that although P5 is not a consequence of P1–P4 in the projective plane, it is a consequence of the seemingly equally simple axioms for projective 3-space. In Exercise 3.5 you will be asked to prove that a plane in projective 3-space is a projective plane. As a consequence the next theorem provides a second proof that Desargues' Axiom is true in the real projective plane.

THEOREM 3.2. *Desargues' Axiom holds in projective 3-space, where we do not necessarily assume that all the points lie in a plane. In particular, Desargues' Axiom holds for any plane that lies in a projective 3-space.*

Proof. We work with the points in Figure 3.1. There are two cases to consider.

Case 1. Let us assume that the plane Σ containing the points A, B, C is different from the plane Σ' containing the points A', B', C' . The lines AB and $A'B'$ both lie in the plane determined by O, A, B , and so they meet in a point P . Similarly we see that AC and $A'C'$ meet, and that BC and $B'C'$ meet. Now the points P, Q, R lie in the plane Σ , and also in the plane Σ' . Hence they lie in the intersection $\Sigma \cap \Sigma'$, which is a line (Exercise 3.3c).

Case 2. Suppose that $\Sigma = \Sigma'$, so that the whole configuration lies in one plane (call it Σ). Pick a point X which does not lie in Σ . Draw lines joining X to all the points in the diagram. Choose D on XB , different from B , and let $D' = OD \cdot XB'$. (Why do they meet?) Then the triangles ADC and $A'D'C'$ are perspective from O , and do not lie in the same plane. We conclude from Case 1 that the points $P' = AD \cdot A'D'$, $Q = AC \cdot A'C'$, and $R' = DC \cdot D'C'$ lie in a line. But these points are projected from X onto P, Q , and R , hence P, Q, R are collinear. \square

EXERCISES

EXERCISE 3.1. Establish the existence of a Moulton line through two points giving positive slope.

EXERCISE 3.2. Draw a figure for Theorem 3.2, case 2, and check the details.

EXERCISE 3.3. Using the axioms S1–S6 of projective 3-space, prove the following statements. Be very careful not to assume anything except what is stated by the axioms. Refer to the axioms explicitly by number.

- a) If two distinct points P, Q lie in a plane Σ then the line joining them is contained in Σ .
- b) A plane and a line not contained in the plane meet in exactly one point.
- c) Two distinct planes meet in exactly one line.
- d) A line and a point not on it lie in a unique plane.

EXERCISE 3.4. Given two lines ℓ and m intersecting "off the paper", and a point P not on either line, use Desargues' Theorem to construct a line through P and $\ell \cap m$.

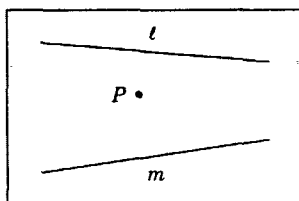


Figure 3.4. Two lines intersecting "off the paper".

EXERCISE 3.5. Prove that any plane Σ in a projective 3-space is a projective plane, i.e. satisfies the axioms P1–P4. (You may use the results of Exercise 3.3).

EXERCISE 3.6. Propose axioms for affine 3-space and show how one may complete this to obtain a projective 3-space. Check carefully that axioms S1–S6 are satisfied. State and prove a 3-dimensional analog of Proposition 2.2.

EXERCISE 3.7. Verify that the projective space $\mathbb{P}^3(\mathbb{R})$ does indeed satisfy Axioms S1–S6.

EXERCISE 3.8. Find the two triangles in Figure 3.1 which are in perspective from center P . What is their *axis* (i.e. the line in which their corresponding sides meet)?

Chapter 4

A Brief Introduction to Groups

The sets of automorphisms with their compositions. Tran \mathbb{A} and Dil \mathbb{A} , which we encountered when studying the affine plane \mathbb{A} , are examples of an important algebraic concept, the group. Groups got their real start with Galois as finite invariants of polynomial equations, which could resolve questions of solvability by radicals. In Galois theory, difficult questions about polynomial equations are converted to easier questions about groups, which can be answered with a small amount of group theory. Group theory and projective geometry have a somewhat similar relation.

4.1 Elements of Group Theory

DEFINITION. A *group* is a set G , together with a function (or binary operation) $G \times G \rightarrow G$, $(a, b) \mapsto ab$, such that

- G1.** (ASSOCIATIVITY) For all $a, b, c \in G$, $(ab)c = a(bc)$.
- G2.** There exists an element $1 \in G$ such that $a \cdot 1 = 1 \cdot a = a$ for all a .
- G3.** For each $a \in G$, there exists an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$.

The element 1 is called the *identity, unit, or neutral element*. The element a^{-1} is called the *inverse of a* . (Both 1 and a^{-1} are easily shown to be unique.) The cancellation law holds in groups: $ax = ay$ or $xa = ya \implies x = y$ ($a, x, y \in G$). A set with binary operation satisfying only G1 is called a *semigroup*.

Note that in general the product ab may be different from ba . However, we say the group G is *abelian, or commutative* if

G4. For all $a, b \in G$, $ab = ba$.

The multiplicative notation for a group is often changed to an additive notation for abelian groups: $a + b$, 0 the neutral element, $-a$ the inverse of a . E.g. the common integers \mathbb{Z} under addition is an abelian group. Another example is a vector space; forgetting all about scalar multiplication, one notes that the vectors form an abelian group under addition.

EXAMPLE 1. Let S be any set, and let $G = \text{Perm } S$ be the set of permutations of the set S . (Recall that a permutation is a one-to-one mapping of S onto S .) If $g_1, g_2 \in G$ are two permutations, define $g_1g_2 \in G$ to be the permutation obtained by performing first g_2 , then g_1 : $g_1g_2(x) = g_1(g_2(x))$ for all $x \in S$.

EXAMPLE 2. Let C be a configuration, and let G be the set of *automorphisms* of C , i.e. the set of those permutations of C which send lines onto lines. Again we define the product g_1g_2 of two automorphisms g_1, g_2 , by performing g_2 first, and then g_1 . This group is written $\text{Aut } C$.

DEFINITION. A *homomorphism* $\phi: G_1 \rightarrow G_2$ of one group to another, is a mapping of the set G_1 to the set G_2 such that

$$\phi(ab) = \phi(a)\phi(b)$$

for each $a, b \in G_1$.

An *isomorphism* of one group with another, is a homomorphism which is one-to-one and onto. It follows easily that a homomorphism sends unit to unit. Linear transformations of vector spaces provide examples of homomorphisms between (abelian) groups.

DEFINITION. Let G be a group. A *subgroup* of G is a nonempty subset $H \subseteq G$, such that for any $a, b \in H$, $ab \in H$, and $a^{-1} \in H$.

Note this condition implies $1 \in H$. Then H (with the binary operation restricted to H) is itself a group.

EXAMPLE 3. Let G be the group of permutations of a set S . Let $x \in S$, and let $H_x = \{g \in G \mid g(x) = x\}$. Then H_x is a subgroup of G , called the *stabilizer subgroup* of x . Check it! (Exercise 4.7).

EXAMPLE 4. The even integers under addition form a subgroup of \mathbb{Z} . More generally, the multiples of n form a subgroup $n\mathbb{Z}$ under addition.

EXAMPLE 5. $\text{Aut } C$ is a subgroup of $\text{Perm } C$, where C denotes both a configuration and its underlying set of points.

DEFINITION. Let G be a group, and H a subgroup of G . The *left coset* of H generated by $g \in G$ is the subset of G given by $gH = \{gh \mid h \in H\}$. The *right coset* Hg is similarly defined to be the subset $\{hg \mid h \in H\}$.

LEMMA 4.1. Let H be a subgroup of G , and let gH be a left coset. Then there is a one-to-one correspondence between the elements of H and the elements of gH . (In particular, if H is finite, they have the same number of elements.)

Proof. Map $H \rightarrow gH$ by $h \mapsto gh$. By definition of gH , this map is onto. So suppose $h_1, h_2 \in H$ have the same image. Then $gh_1 = gh_2$. Multiplying on the left by g^{-1} , we deduce $h_1 = h_2$. \square

THEOREM 4.2 (LAGRANGE'S THEOREM). Let G be a finite group, and let H be a subgroup. Then

$$\#(G) = \#(H) \cdot (\text{number of left cosets of } H).$$

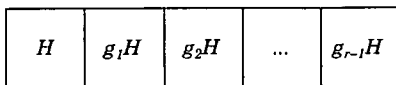


Figure 4.1. Division of G into r left cosets of equal size.

Proof. Indeed, all the left cosets of H have the same number of elements as H , by the lemma. If $g \in G$, then $g \in gH$, since $g = g \cdot 1$, and $1 \in H$. Thus G is the union of the left cosets of H . Finally, if we show that two cosets gH , and $g'H$ are either equal, or disjoint, then we have the set G partitioned into subsets of size $\#(H)$ each, which proves the theorem.

Indeed, suppose gH and $g'H$ have an element in common, namely x . Then $xH \subseteq gH$ and $xH \subseteq g'H$, but the lemma tells us that cosets have the same cardinality. Hence $gH = xH = g'H$. \square

Thus the subgroup H has *order*, i.e. number of elements, a divisor of the order of G .¹ Let's see a good application of Lagrange's Theorem to the first step towards classification of finite groups up to isomorphism.

In any group G an element g generates a subgroup $\langle g \rangle$ consisting of the powers of g : $g^2 = gg$, $g^3 = g^2g$, etc. (also g^{-1} , $g^{-2} = g^{-1}g^{-1}$ if necessary). In a finite group the order of $\langle g \rangle$ is called the *order of g* , and equals the least positive integer n such that $g^n = 1$. Since a group G having prime order has no proper divisors, Lagrange informs us that there are no nontrivial subgroups (different from $\{1\}$ or G). Hence, every nonunit in G generates all of G . Hence every group of prime order is generated by one element (such groups are called *cyclic groups*), and any cyclic groups of the same order are isomorphic (an easy exercise, Exercise 4.8).

DEFINITION. Suppose G is a subgroup of some Perm S . The *orbit* of x is the set of points

$$\beta_x = \{g(x) : g \in G\}$$

COROLLARY 4.3. *If G is a finite group in Perm S , then*

$$\#(G) = \#(H_x) \cdot \#(\beta_x).$$

Proof. In order to apply Lagrange's Theorem we need only show the orbit β_x in one-to-one correspondence with the number of distinct left cosets of H_x in G .

¹Beware though that it is not necessarily true that every divisor of $\#(G)$ corresponds to $\#(H)$ for some subgroup H in G : there is no eight element subgroup in the 24 element group S_4 whose acquaintance we make below.

Given $y \in \beta_x$, there exists $g \in G$ such that $y = g(x)$, so map $\beta_x \rightarrow \{\text{left cosets}\}$ with the function $T: y \mapsto gH_x$.

We claim T is a one-to-one correspondence. T is well-defined: if $g'(x) = y = g(x)$, then $g^{-1}g'(x) = x$, so $g^{-1}g' \in H_x$, so $g'H_x = gH_x$, i.e. T is one-valued at y . T is onto: given a coset gH_x , $T(g(x)) = gH_x$. T is one-to-one: if $T(y_1) = gH_x = T(y_2)$, it follows that $y_1 = g(x) = y_2$. Hence, T is the desired one-to-one correspondence. \square

DEFINITION. A group $G \subseteq \text{Perm } S$ of permutations of a set S is *transitive* if the orbit of some element is the whole of S . It follows that the orbit of every element is all of S .

So in the above corollary, if G is transitive, $\#(G) = \#(H_x) \cdot \#(S)$.

COROLLARY 4.4. Let S be a set with n elements, and let $S_n = \text{Perm } S$. Then $\#(S_n) = n!$.

Proof on induction by n . If $n = 1$, there is only the identity permutation, so $\#(S_1) = 1$. So let S have $n + 1$ elements, and let $x \in S$. Let H_x be the subgroup of permutations leaving x fixed. S_{n+1} is transitive, since one can permute x with any other element of S . Hence

$$\#(S_{n+1}) = \#(S) \cdot \#(H_x) = (n + 1) \cdot \#(H_x).$$

But H_x is just the group of permutations of the remaining n elements of S different from x , so $\#(H_x) = n!$ by the evident induction hypothesis. Hence $\#(S_{n+1}) = (n + 1)!$ \square

GENERATORS

A subset A of a group G is said to *generate* the subgroup H , denoted by $H = \langle A \rangle$, if H is the smallest subgroup containing A . H is in fact the subgroup $\{a_1^{n_1} \dots a_q^{n_q} \mid a_1, \dots, a_q \in A; n_1, \dots, n_q \in \mathbb{Z}\}$ of products of powers of elements in A (Exercise 4.15).

Later in the course, we will have much to do with the group of automorphisms of a projective plane, and certain of its subgroups. In particular, we will show that the Axiom P5 of Desargues is equivalent to the statement that the group of automorphisms has enough (of the

projective equivalents of) translations and stretchings. For the moment, we will content ourselves with calculating the automorphisms of a few simple configurations.

4.2 Automorphisms of the Projective Plane of Seven Points

Call the plane π and name its seven points A, B, C, D, P, Q , and R . π may be obtained by completing the affine plane of four points A, B, C , and D . Its lines are shown in Figure 4.2.

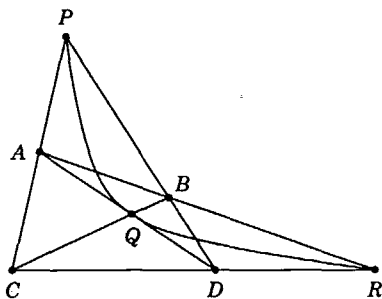


Figure 4.2. The projective plane of seven points.

PROPOSITION 4.5. $G = \text{Aut } \pi$ is transitive.

Proof. We will write down some elements of G explicitly.

$$a = (AC)(BD)$$

for example. This notation means “interchange A and C , and interchange B and D ”. More generally a symbol $(A_1 A_2 \dots A_r)$ means “send A_1 to A_2 , A_2 to A_3 , \dots , A_{r-1} to A_r , and A_r to A_1 ”, and is referred to as an r -cycle. Multiplication of two such symbols is defined by performing the one on the right first, then the next on the right and so on.

$$b = (AB)(CD)$$

Thus we see already that A can be sent to B or to C . We calculate

$$ab = (AC)(BD)(AB)(CD) = (AD)(BC),$$

and

$$ba = (AB)(CD)(AC)(BD) = (AD)(BC) = ab.$$

Thus we can also send A to D .

Another automorphism is

$$c = (BQ)(DR).$$

Since the orbit of A already contains B, C, D , we see that it also contains Q and R . Finally

$$d = (PA)(BQ)$$

shows that the orbit of A is all of π , so G is transitive. \square

PROPOSITION 4.6. *Let $H_P \subseteq G$ be the subgroup of automorphisms of π leaving P fixed. Then H_P is transitive on the set $\pi - \{P\}$.*

Proof. Note that a, b, c above are all in H , so that the orbit of A under H_P is

$$\{A, B, C, D, Q, R\} = \pi - \{P\}. \quad \square$$

THEOREM 4.7. *G has 168 elements.*

Proof. We carry the above analysis a step farther as follows. Let $K \subseteq H_P$ be the subgroup leaving Q fixed. Therefore since elements of K leave P and Q fixed, they also leave R fixed. K is transitive on the set $\{A, B, C, D\}$, since $a, b \in K$. On the other hand, an element of K is uniquely determined by where it sends the point A , since lines go to lines and two of the three points per line are determined. Since A may only go to four points, K is just the group consisting of the four elements $1, a, b, ab$. We conclude from the previous discussion that

$$\begin{aligned} \#(G) &= \#(H_P) \cdot \#(\pi) = 7 \cdot \#(H_P) \\ \#(H_P) &= \#(K) \cdot \#(\pi - \{P\}) = 4 \cdot 6 \end{aligned}$$

whence $\#(G) = 7 \cdot 6 \cdot 4 = 168$. \square

COROLLARY 4.8. *Given triangles $A_1A_2A_3$ and $A'_1A'_2A'_3$ in π , there is one, and only one, automorphism sending $A_i \mapsto A'_i$ ($i = 1, 2, 3$).*

Proof. For each triangle $\Delta B_1B_2B_3$ we show that there is an automorphism $\alpha_{B_1B_2B_3}$ sending P, Q, A onto B_1, B_2, B_3 , respectively. Then $\alpha_{A'_1A'_2A'_3} \circ \alpha_{A_1A_2A_3}^{-1}$ proves the existence part of our statement.

Since G is transitive, we can find $g \in G$ such that $g(P) = B_1$. Since $B_1 \neq B_2$ it follows that $g^{-1}(B_2) \neq P$. But H_P is transitive on $\pi - P$, so there is an element $h \in H_P$ such that $h(Q) = g^{-1}(B_2)$. Then $gh(P) = B_1$ and $gh(Q) = B_2$. Now $(gh)^{-1}(B_3) \notin \{P, Q, R\}$ since B_3 is not on the line B_1B_2 . Hence there is $k \in K$ such that $k(A) = (gh)^{-1}(B_3)$. Then $(ghk)(P) = B_1$, $(ghk)(Q) = B_2$, and $(ghk)(A) = B_3$. This completes the existence argument.

For uniqueness of this element, let us count the number of triples of non-collinear points in π . The first can be chosen in 7 ways, the second in 6 ways, and the last in 4 ways. Thus there are 168 such triples. Since the order of G is 168, there must be exactly one automorphism sending a given triangle into another triangle. \square

EXERCISES

EXERCISE 4.1. Show that the identity of a group G is unique. Next, show that inverses are unique: if b and c satisfy $ab = ba = 1$, $ac = ca = 1$, then $b = c$.

EXERCISE 4.2. Given a semigroup G , a *left identity* is an element e satisfying $ea = a$ (for all $a \in G$). Given $a \in G$, a *left inverse* b satisfies $ba = e$. Show that a semigroup with left identity, in which each element has a left inverse, is a group. Is something similar true where right replaces left?

EXERCISE 4.3. Let G be a group. If $a^2 = 1$ for all $a \in G$, prove that G is abelian.

EXERCISE 4.4. Let n be a positive integer > 1 . Consider the additive group \mathbb{Z} of integers, and subgroup $n\mathbb{Z}$. Show that the left cosets $\{x + n\mathbb{Z} \mid x = 0, \dots, n-1\}$ form a group under $+$, call it \mathbb{Z}_n .

EXERCISE 4.5. If $\phi: G \rightarrow H$ is a homomorphism, prove that the kernel of ϕ , $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = 1\}$, is a subgroup of G .

EXERCISE 4.6. Show that the natural map $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ given by $x \mapsto x + n\mathbb{Z}$ is a homomorphism with kernel $n\mathbb{Z}$.

EXERCISE 4.7. If $G = \text{Perm } S$, prove that $H_x = \{g \in G \mid g(x) = x\}$ is a subgroup of G for every $x \in S$. If $x = g(y)$ for some $g \in G$ and $x, y \in S$, show that $H_x = gH_yg^{-1}$; whence H_x and H_y are isomorphic.

EXERCISE 4.8. Show that \mathbb{Z}_n is a cyclic group, i.e. generated by one element. Prove that cyclic groups of same order n are isomorphic, whence all are isomorphic to \mathbb{Z}_n .

EXERCISE 4.9. Prove in a manner similar to Corollary 4.8 that the affine plane of 9 points has automorphism group of order $9 \cdot 8 \cdot 6 = 432$, and any three non-collinear points can be taken into any three non-collinear points by a unique element of the group.

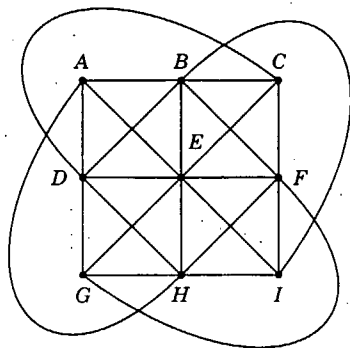


Figure 4.3. The affine plane of 9 points.

EXERCISES 4.10–4.12. We will consider the Desargues configuration, which is a set of 10 elements,

$$\Sigma = \{O, A, B, C, A', B', C', P, Q, R\},$$

and 10 lines, which are the subsets $\{O, A, A'\}$, $\{O, B, B'\}$, $\{O, C, C'\}$, $\{A, B, P\}$, $\{A', B', P\}$, $\{A, C, Q\}$, $\{A', C', Q\}$, $\{B, C, R\}$, $\{B', C', R\}$, and $\{P, Q, R\}$. Let $G = \text{Aut } \Sigma$ be the set of automorphisms of Σ in Exercise 4.10, 4.11, and 4.12.

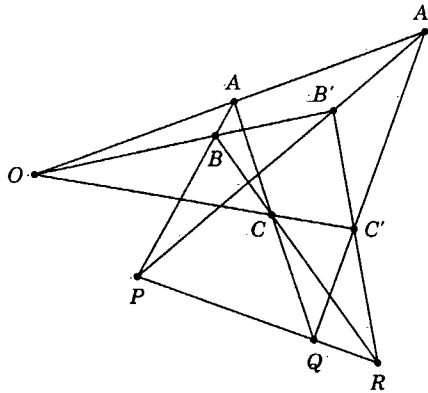


Figure 4.4. The Desargues configuration.

EXERCISE 4.10. Show that G is transitive on Σ .

EXERCISE 4.11. a) Show that the subgroup of G leaving a point fixed is transitive on a set of six letters.

b) Show that the subgroup of G leaving two collinear points fixed has order 2.

c) Deduce the order of G from the previous results.

Now we consider some further subsets of Σ , which we will call planes, namely

$$\begin{aligned} 1 &= \{O, A, B, A', B', P\} \\ 2 &= \{O, A, C, A', C', Q\} \\ 3 &= \{O, B, C, B', C', R\} \\ 4 &= \{A, B, C, P, Q, R\} \\ 5 &= \{A', B', C', P, Q, R\} \end{aligned}$$

EXERCISE 4.12. Show that each element of G induces a permutation of the set of five planes $\{1, 2, 3, 4, 5\}$, and that the resulting map-

ping $\phi: G \rightarrow \text{Perm}\{1, 2, 3, 4, 5\}$ is an isomorphism of groups. Thus G is isomorphic to the permutation group on five letters.

EXERCISE 4.13. Let S_4 be the group of permutations of the four symbols 1, 2, 3, 4.

a) Let $G \subseteq S_4$ be the subgroup generated by the permutation (1234). What is the order of G ?

b) Let $H \subseteq S_4$ be the subgroup generated by the permutations (12) and (34). What is the order of H ?

c) Is there an isomorphism (of abstract groups) $\phi: G \rightarrow H$? If so, write it explicitly. If not, explain why not.

EXERCISE 4.14. The *Pappus configuration* Σ is the configuration of 9 points and 9 lines as shown in the diagram.

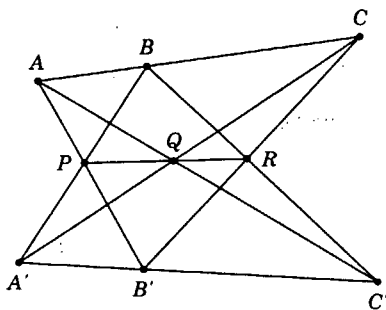


Figure 4.5. The Pappus configuration.

a) What is the order of the group of automorphisms of Σ ?

b) Explain *briefly* how you arrived at the answer to a).

EXERCISE 4.15. Let A be a subset of a group G .

a) Show that the set $K = \{a_1^{n_1} \dots a_q^{n_q} \mid a_1, \dots, a_q \in A; n_1, \dots, n_q \in \mathbb{Z}\}$ is a subgroup of G .

b) Show that $K = \langle A \rangle$, the subgroup generated by A .

EXERCISE 4.16. Show that the number of right cosets of a subgroup in a finite group is equal to the number of left cosets:

Chapter 5

Elementary Synthetic Projective Geometry

We will now define what we mean by central projection or perspectivity in our axiomatic development, and meet some of the basic invariants of projective geometry like cross ratio. But first we cut in half our labors by noting the principle of duality.

5.1 Principle of Duality

Before reading the next proposition it will be helpful to recall that a projective plane is a set where elements are called “points” together with a set of subsets of those “points”, each of which is called a “line”: the “points” and “lines”, though, must satisfy P1–P4. To facilitate understanding we write point and line in different script from time to time in our discussion of duality.

PROPOSITION 5.1. Let π be a projective plane. Let π^ be the set of lines in π , and define a line in π^* to be a pencil of lines in π . Then π^* is a projective plane. Furthermore, if π satisfies P5, so does π^* .*

REMARK. We call π^* the *dual projective plane* of π .

Proof. We must verify the axioms P1–P4 for π^* . These translate into statements D1, D2, D3, and D4, respectively, which we show to be simple consequences of P1–P4. We also show $P5 \implies D5$.

P1. If p, q are two distinct points of π^* ; then there is a unique line of π^* containing p and q . If we translate this into a statement for π , it says

D1. If p, q are two distinct lines of π , then there is a unique pencil of lines containing p, q .

I.e. p, q have a unique point in common. Thus D1 is equivalent to P2.

P2. If L and M are two lines in π^* , they have exactly one point in common. In π , this says that

D2. Two pencils of lines have exactly one line in common.

This is equivalent to P1.

P3. There are three non-collinear points in π^* .

D3. There are three non-concurrent lines in π .

(We say three or more lines are *concurrent* if they all pass through some point, i.e. if they are contained in a pencil of lines.) By P3 there are three non-collinear points A, B, C . Then one sees easily that the lines AB, AC, BC are not concurrent: these correspond to three non-collinear points in π^* . (Conversely, three non-concurrent lines implies the existence of three non-collinear points.)

P4. Every line in π^* has at least three points. This says that

D4. Every pencil in π has at least three lines.

Let the pencil be centered at P , and let ℓ be some line not passing through P . Then by P4, ℓ has at least three points A, B, C . Hence the pencil of lines through P has at least three lines $a = PA, b = PB, c = PC$. (Conversely, assuming D4 we easily show P4.)

Now we will assume P5, Desargues' Axiom, is true in π and prove it in π^* .

P5. Let o, a, b, c, a', b', c' be seven distinct points of π^* , such that oaa', obb', occ' are collinear, and $abc, a'b'c'$ are triangles. Then the points $p = ab.a'b', q = ac.a'c',$ and $r = bc.b'c'$ are collinear.

Translated into π , this says the following

D5. Let o, a, b, c, a', b', c' be seven lines, such that $o, a, a'; o, b, b'; o, c, c'$ are concurrent and such that abc and $a'b'c'$ form two triangles. Then the lines $p = (a.b) \cup (a'.b'), q = (a.c) \cup (a'.c'),$ and $r = (b.c) \cup (b'.c')$ are concurrent.

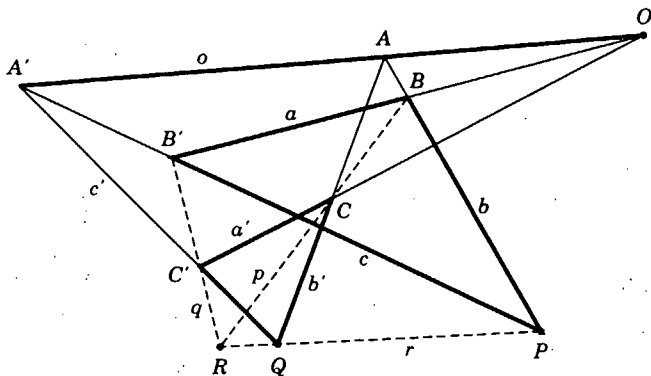


Figure 5.1. Proof of the converse of Desargues' Axiom.

To prove this statement, we will label the points of the diagram in such a way as to be able to apply P5. So let $O = o.a.a', A = o.b.b', A' = o.c.c', B = a.b, B' = a.c, C = a'.b',$ and $C' = a'.c'.$ Then O, A, B, C, A', B', C' satisfy the hypothesis of P5, so we conclude that $P = AB.A'B' = b.c, Q = AC.A'C' = b'.c',$ and $R = BC.B'C' = p.q$ are collinear. But $PQ = r,$ so $p, q,$ and r are concurrent at $R.$ \square

We have in fact nearly proven that π is a projective plane if and only if (iff) π^* is a projective plane: indeed, π Desarguesian iff π^*

Desarguesian (Exercise 5.15).

The converse of Desargues' Theorem. Notice that statement D5 is in fact the converse of Desargues' Theorem: two axially perspective triangles are centrally perspective. What we have proved then is that if Desargues' Theorem holds in a projective plane then so does its converse.¹ \square

METATHEOREM 5.2 (PRINCIPLE OF DUALITY). *Let S be any statement about a projective plane π , which can be proved from the axioms $P1$ – $P4$ (respectively $P1$ – $P5$). Then the "dual" statement D , obtained from S by interchanging the words*

point	\longleftrightarrow	line
lies on	\longleftrightarrow	passes through
collinear	\longleftrightarrow	concurrent
intersection	\longleftrightarrow	join
etc.		

is a true statement as well about projective planes (resp. Desarguesian planes).

Metaproof. The statement S is true for projective planes, so it holds in particular for the dual projective planes, which are themselves projective planes as we have just seen. Now if S is true for π^* , then D is true for π , since D is just the application to S of the definition of *point*, *line*, *point on line*, etc. in π^* . π being arbitrary, D is a true statement about projective planes. \square

REMARK. Consider the dual of the dual projective plane π^* ; denote it by π^{**} . Is it something new? There is a natural map $\pi \rightarrow \pi^{**}$ given by sending a point P of π into the pencil of lines through P , which is a point of π^{**} . This turns out to be an isomorphism of the two projective planes π and π^{**} (Exercise 5.4). Hence π^{**} is not anything new.

¹That the dual of statement P5 is its converse is by no means usual for statements about projective planes.

For the real projective plane π the dual projective plane π^* is isomorphic with π (in notation, $\pi \cong \pi^*$). Given a line ℓ through the origin O , send this to the plane through O perpendicular to ℓ : check that this defines an isomorphism. It is also true that $\pi \cong \pi^*$ for the finite projective planes π of $p^{2n} + p^n + 1$ points (p a prime, n a positive integer). Isomorphisms between π and π^* are called *polarities* in the literature. However, there are non-Desarguesian projective planes where $\pi \not\cong \pi^*$.

5.2 Fano's Axiom

DEFINITION. Suppose A, B, C , and D are four points in a projective plane such that no three of these points are collinear. Then the *complete quadrangle* $ABCD$ is the configuration of seven points and six lines obtained by taking all six lines determined by A, B, C , and D , and then taking the intersection of opposite sides: $P = AB \cdot CD$, $Q = AC \cdot BD$, and $R = AD \cdot BC$. The points P, Q, R are called *diagonal points* of the complete quadrangle.

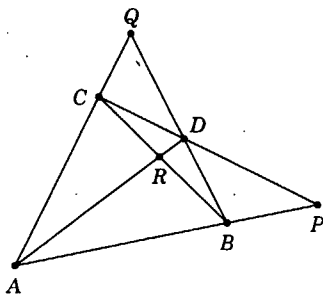


Figure 5.2. Complete quadrangle.

It may happen that the diagonal points P, Q, R of a complete quadrangle are collinear (as for example in the projective plane of seven points). However, this never happens in the real projective plane (as we will see below), and in general, it is to be regarded as a pathological phenomenon, hence we will make an axiom saying this should not happen.

P6. (FANO'S AXIOM). The diagonal points of a complete quadrangle are not collinear.

PROPOSITION 5.3. *The real projective plane satisfies P6.*

Proof. Given a complete quadrangle $ABCD$, no three of A, B, C, D are collinear, so in the homogeneous coordinate model any three representative vectors (representing $A, B, \dots =$ lines through the origin) are linearly independent. Choosing these as a basis and rescaling, we may assume A, B, C, D to be the points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, and $(1, 1, 1)$ respectively. You are asked to compute that the diagonal points of this complete quadrangle are $(1, 1, 0)$, $(1, 0, 1)$, and $(0, 1, 1)$ in Exercise 5.1b. To see if they are collinear, we calculate the determinant:

$$\begin{vmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{vmatrix} = -2$$

Hence the rows are linearly independent, so the lines they represent are not coplanar, and we conclude that the points are not collinear. \square

Let's temporarily call a projective plane satisfying P6 a Fano plane. In a later chapter we shall see P6 independent of P1–P4 and P5, so we had better consider the question of whether a Fano plane π has dual plane π^* also a Fano plane. We will obviously need to dualize the notion of complete quadrangle.

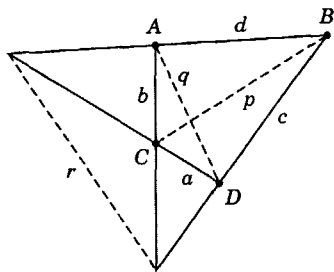


Figure 5.3. Complete quadrilateral.

DEFINITION. A *complete quadrilateral* $abcd$ is the configuration of seven lines and six points, obtained by taking four lines a, b, c, d , of which we require that no three are concurrent, their six points-of-intersection, and the three lines $p = (a.b) \cup (c.d)$, $q = (a.c) \cup (b.d)$, $r = (a.d) \cup (b.c)$ joining opposite pairs of points. The lines p, q , and r are called the *diagonal lines* of the complete quadrilateral.

PROPOSITION 5.4. *If π satisfies Axiom P6, then so does π^* .*

Proof. Clearly, the negation of the dual of P6 states: there exists a complete quadrilateral $abcd$ such that the three diagonal lines p, q, r are concurrent. Then this implies that the diagonal points of the complete quadrangle $ABCD$, where $A = b.d$, $B = c.d$, $C = a.b$, and $D = a.c$, are collinear, which contradicts P6. \square

REMARK. The reader is urged to construct the duals of definitions, theorems, and proofs. For example, in the next section try developing the theory of harmonic lines, dual to harmonic points.

5.3 Harmonic Points

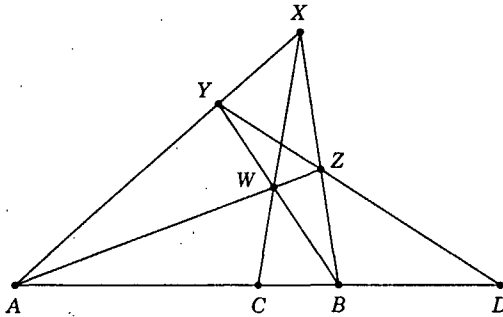


Figure 5.4. Harmonic points.

DEFINITION. An ordered quadruple of distinct points A, B, C, D on a line is called a *harmonic quadruple* if there is a complete quadrangle $XYZW$ such that A and B are diagonal points of the complete

quadrangle (say $A = XYZW$ and $B = XZYW$), and C, D lie on the remaining two sides of the quadrangle (say $C \in XW$ and $D \in YZ$).

In symbols, we write $H(A, B; C, D)$ if A, B, C, D form a harmonic quadruple. Note that we equally well have $H(B, A; C, D)$, $H(A, B; D, C)$, and $H(B, A; D, C)$.

Note that if A, B, C, D is a harmonic quadruple, then the fact that A, B, C, D are distinct implies that the diagonal points of a defining quadrangle $XYZW$ are not collinear. In fact, the notion of four harmonic points does not make much sense unless Fano's Axiom P6 is satisfied, hence we will always assume this axiom when we speak of harmonic points.

PROPOSITION 5.5. *Let A, B, C be three distinct points on a line. Then (assuming P6) there is a point D such that $H(A, B; C, D)$. Furthermore, if P5 is assumed, this point is unique. (D is called the fourth harmonic point of A, B, C , or the harmonic conjugate of C with respect to A and B .)*

Proof. We construct a complete quadrangle having A and B as diagonal points and with C on one of the two remaining lines.

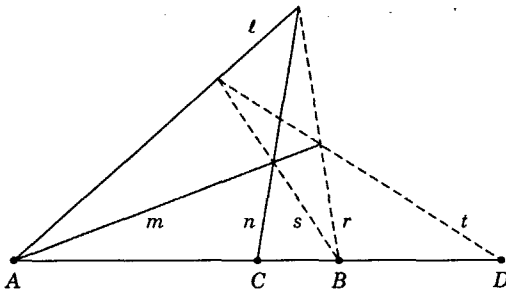


Figure 5.5. Harmonic conjugate.

By D3 we find two lines ℓ and m through A , different from the line ABC . Find a line n through C , different from ABC .

Then let r denote $B \cup (\ell, n)$, and let s denote $B \cup (m, n)$. Then $r \cdot m$ and $s \cdot \ell$ join to form a line, call it t . Let t intersect ABC at D . By P6

we see that D is distinct from A, B, C . Then by construction we have $H(A, B; C; D)$.

Now we assume P5, and will prove the uniqueness of the fourth harmonic point. Given A, B, C construct D as above. Suppose D' is another point such that $H(A, B; C; D')$. Then by definition, there is a complete quadrangle $XYZW$ such that $A = XY.ZW$, $B = XZ.YW$, $C \in XW$, $D' \in YZ$. Call $\ell' = AX$, $m' = AZ$, and $n' = CX$. Then we see that the above construction, applied to ℓ', m', n' , will give D' .

Thus it is sufficient to show that our construction of D is independent of the choice of ℓ, m, n . We do this in three steps, by showing that if we vary one of ℓ, m, n , the point D remains the same.

Step 1. If we replace ℓ by a line ℓ' , we get the same D .

Let D be defined by ℓ, m, n as above, and label the resulting complete quadrangle $XYZW$. Let ℓ' be another line through A , distinct from ℓ , and label the quadrangle obtained from ℓ', m, n , $X'Y'Z'W$. (Note the point $W = m.n$ belongs to both quadrangles).

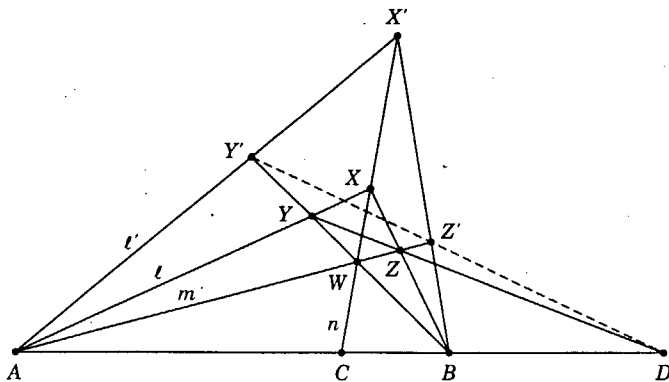


Figure 5.6. Harmonic points, ℓ varies.

We must show that the line $Y'Z'$ passes through D , i.e. that $Y'Z'.AB = D$. Indeed, observe that the two triangles XYZ and $X'Y'Z'$ are perspective from W . Two pairs of corresponding sides meet in A and B respectively: $A = XY.X'Y'$ and $B = XZ.X'Z'$.

Hence by P5, the third pair of corresponding sides, namely YZ and $Y'Z'$, must meet on AB , so that $Y'Z' \cdot AB = D$.

Step 2. If we replace m by m' , we get the same D . The proof in this case is identical with that of Step 1, interchanging the roles of l and m .

Step 3. If we replace n by n' we get the same D .

The proof in this case is more difficult, since all four points of the corresponding complete quadrangle change. So let $XYZW$ be the quadrangle formed by l, m, n , which defines D . Let $X'Y'Z'W'$ be the quadrangle formed by l, m, n' . We must show that $Y'Z'$ also meets ABC at D .

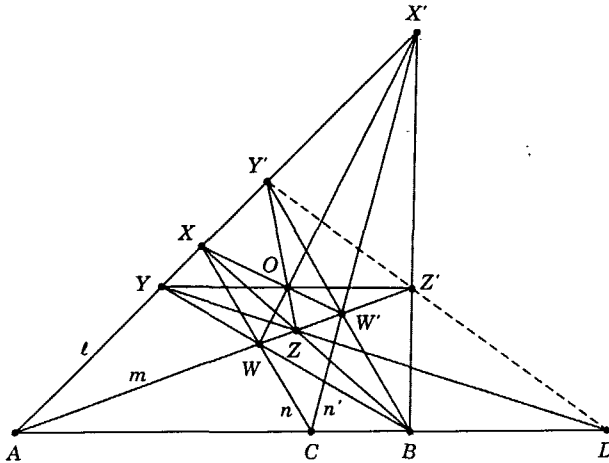


Figure 5.7. Harmonic points, n varies.

Consider the triangles XYW and $W'Z'X'$. Corresponding sides meet in the collinear points A, B , and C , respectively. By D5 the two triangles must be perspective from a point O . In other words, the lines XW' , $Y'Z'$, and WX' meet in a point O .

Similarly, by considering the ordered triangles ZWX and $Y'X'W'$, and applying D5 once more, we deduce that the lines ZY' , WX' , and XW' are concurrent. Since two of these lines are among the three

above, and $XW' \neq X'W$, we conclude that their point of intersection is also O .

In other words, the quadrangles $XYZW$ and $W'Z'Y'X'$ are perspective from O , in that order. In particular, the triangles XYZ and $W'Z'Y'$ are perspective from O . Two pairs of corresponding sides meet in A and B , respectively. Hence the third pair of sides, YZ and $Z'Y'$, must meet on the line AB , i.e. $D \in Z'Y'$. \square

PROPOSITION 5.6. Let AB, CD be four harmonic points. Then (assuming P5) also CD, AB are four harmonic points. Combining with an earlier observation (p. 50), we find therefore

$$\begin{aligned} H(A, B; C, D) &\Leftrightarrow H(B, A; C, D) \Leftrightarrow H(A, B; D, C) \Leftrightarrow H(B, A; D, C) \\ &\Downarrow \\ H(C, D; A, B) &\Leftrightarrow H(D, C; A, B) \Leftrightarrow H(C, D; B, A) \Leftrightarrow H(D, C; B, A). \end{aligned}$$

Proof. We assume $H(A, B; C, D)$, and let $XYZW$ be a complete quadrangle as in the definition of harmonic quadruple.

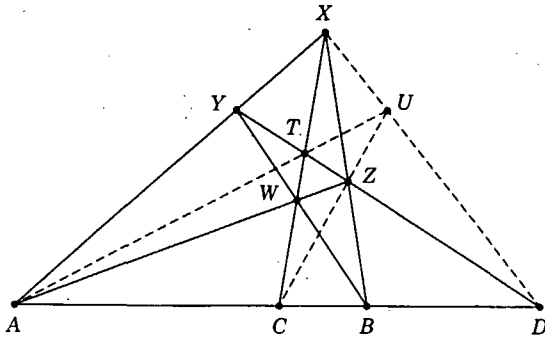


Figure 5.8. Proof of $H(C, D; A, B)$.

Draw DX and CZ , and let them meet in U . Let $XW.YZ = T$. Then $XTUZ$ is a complete quadrangle with C, D as two of its diagonal points: B lies on XZ , so it will be sufficient to prove that TU passes through A . For then we will have $H(C, D; A, B)$.

Consider the two triangles XUZ and YTW . Their corresponding sides meet in D, B, C respectively, which are collinear. Hence by D5,

the lines joining corresponding vertices, namely XY , TU , WZ , are concurrent, which is what we wanted to prove. \square

EXAMPLES: 1) In the projective plane of thirteen points, there are four points on any line: These four points always form a harmonic quadruple, in any order.

To prove this, it will be sufficient to show that P6 holds in this plane. For then there will always be a fourth harmonic point to any three points; and it must be *the* fourth point on the line. We will prove this later: The plane of 13 points is the projective plane over the field of three elements, which is of characteristic 3. But P6 holds in the projective plane over any field of characteristic $\neq 2$.

2) In the real Euclidean plane, three collinear points A, B, C may be assigned the following simple invariant under parallel projection:

$$(A, B; C) = \frac{AC}{BC},$$

the ratio of signed segment lengths that C is said to divide AB . For example, C is the midpoint of line segment \overline{AB} if and only if $(A, B; C) = -1$. Now midpoint is clearly not an invariant under central projection, but it turns out that cross ratio of four collinear points is such an invariant.

Four collinear points A, B, C, D are assigned a *cross ratio* defined by

$$R_x(A, B; C, D) = \frac{AC}{AD} \bigg/ \frac{BC}{BD}.$$

Then A, B, C and D form a harmonic quadruple if and only if $R_x(A, B; C, D) = -1$ (Exercise 5.2).

3) The cross ratio of four concurrent lines ℓ, m, n, o in the Euclidean plane is best dualized as follows:

$$R_x(\ell, m; n, o) = \frac{\sin \angle \ell n}{\sin \angle \ell o} \cdot \frac{\sin \angle m o}{\sin \angle m n}.$$

In this way the cross ratio of 4 lines equals the cross ratio of four points of intersection with any transversal (Exercise 5.8). $\angle \ell n$ denotes the signed angle between ℓ and n .

5.4 Perspectivities and Projectivities

DEFINITION. A *perspectivity* is a mapping of one line ℓ into another line ℓ' (both considered as sets of points in any projective plane), which can be obtained in the following way. Let O be a point not on either ℓ or ℓ' . For each point $A \in \ell$, let OA meet ℓ' in A' . Then map $A \mapsto A'$. This is a perspectivity. In symbols we write $\ell \stackrel{O}{\sim} \ell'$, and we say " ℓ is mapped into ℓ' by a perspectivity with center at O ", or $ABC \dots \stackrel{O}{\sim} A'B'C' \dots$, which says "the points A, B, C (of the line ℓ) are mapped into the points A', B', C' , respectively (of the line ℓ')".

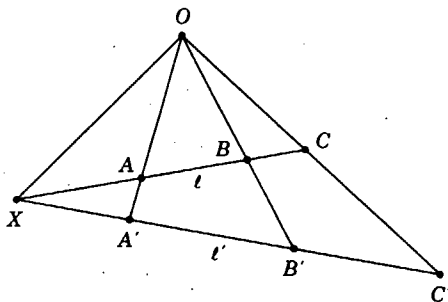


Figure 5.9. A perspectivity between ℓ and ℓ' .

A perspectivity is always one-to-one and onto, and its inverse is also a perspectivity. Note that if $X = \ell \cdot \ell'$, then X as a point of ℓ is sent to itself as a point of ℓ' .

One can see easily that a composition of two or more perspectivities need not be a perspectivity. For example, in Figure 5.10 we have $\ell \stackrel{O}{\sim} \ell'$ and $ABCY \stackrel{O'}{\sim} A'B'C'Y'$ and $A'B'C'Y' \stackrel{O''}{\sim} A''B''C''Y''$. Now if the composed map from ℓ to ℓ'' were a perspectivity, it would have to send $\ell \cdot \ell'' = Y$ to itself. However, Y goes into Y'' . Therefore we make the following

DEFINITION. A *projectivity* is a mapping of one line ℓ into another ℓ' (which may be equal to ℓ), which can be expressed as a composition

of a finite number of perspectivities:

$$\ell \stackrel{O_1}{\bar{\wedge}} \ell_1 \stackrel{O_2}{\bar{\wedge}} \dots \stackrel{O_{n-1}}{\bar{\wedge}} \ell_n \stackrel{O_n}{\bar{\wedge}} \ell'$$

We abbreviate this to $\ell \bar{\wedge} \ell'$, and write $A_1 A_2 \dots A_n \bar{\wedge} A'_1 A'_2 \dots A'_n$, if the projectivity takes points A_1, A_2, \dots, A_n into A'_1, A'_2, \dots, A'_n respectively.

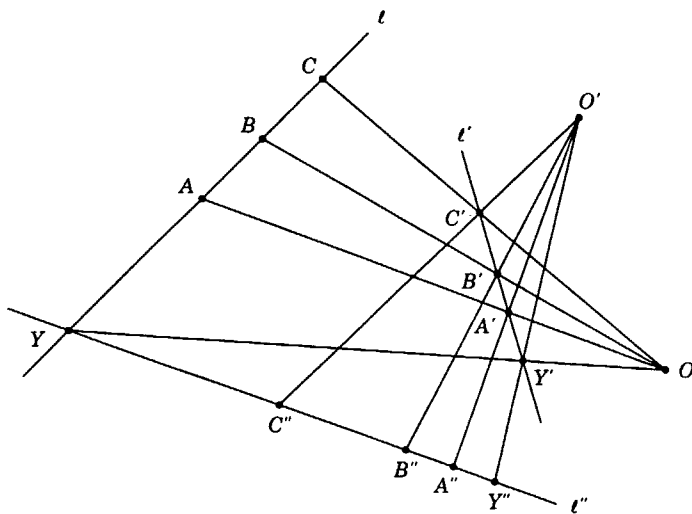


Figure 5.10. A projectivity that is not a perspectivity.

Note that a projectivity also is always one-to-one and onto.

PROPOSITION 5.7. *Let ℓ be a line. Then the set of projectivities of ℓ into itself forms a group, which we will call $PJ(\ell)$.*

Proof. The composition of two projectivities is a projectivity, because the result of performing one chain of perspectivities followed by another is still a chain of perspectivities. The identity map of ℓ into itself is a projectivity (in fact a perspectivity), and acts as the identity element in $PJ(\ell)$. The inverse of a projectivity is a projectivity, since we need only reverse the chain of perspectivities. \square

Naturally, we would like to study this group, and in particular, we would like to know how many times transitive it is: it is clearly 2-transitive, i.e. there exists a group element, a projectivity, sending two arbitrary points A and B into two arbitrary points A' and B' (Exercise 5.5). We will see in the next proposition that it is three times transitive, and in the proposition after, that it cannot be four times transitive.

PROPOSITION 5.8. *In a projective plane π , let A, B, C and A', B', C' be two triples of collinear points. Then there is a projectivity of ℓ into itself which sends A, B, C into A', B', C' .*

Proof. If all six points lie on a line ℓ , we can start arguing as follows. Let ℓ' be a line different from ℓ , which does not pass through A or A' . Let O be any point not on ℓ, ℓ' , and project A', B', C' from ℓ to ℓ' , giving A'', B'', C'' , so we have

$$A'B'C' \stackrel{O}{\underset{\wedge}{\cong}} A''B''C''$$

and $A \notin \ell', A'' \notin \ell$. Now it is sufficient to construct a projectivity from ℓ to ℓ' , taking ABC into $A''B''C''$ (why?). Drop double primes, and forget the original points $A', B', C' \in \ell$. What remains is to do the following problem:

Let ℓ, ℓ' be two distinct lines, let A, B, C be three distinct points on ℓ , and let A', B', C' be three distinct points on ℓ' ; assume furthermore that $A \notin \ell'$ and $A' \notin \ell$. Construct a projectivity from ℓ to ℓ' which carries A, B, C into A', B', C' , respectively.

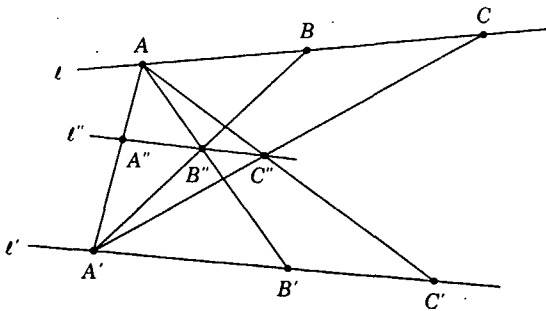


Figure 5.11. A projectivity sending ABC into $A'B'C'$.

Consider lines AA' , AB' , AC' , $A'B$, $A'C$, and let $B'' = AB'.A'B$ and $C'' = AC'.A'C$. Let ℓ'' denote $B''C''$ and meet AA' at A'' . Then $\ell \stackrel{A'}{\wedge} \ell'' \stackrel{A}{\wedge} \ell'$ sends

$$ABC \stackrel{A'}{\wedge} A''B''C'' \stackrel{A}{\wedge} A'B'C'.$$

Thus we have found the required projectivity as a composition of two perspectivities.

The case where one or both of A and A' is the point $\ell.\ell'$ is disposed of by relabelling points. \square

REMARK. In the presence of Axiom P7, introduced in the next chapter, the line ℓ'' is called the *cross axis* of the projectivity $ABC \bar{\wedge} A'B'C'$. In fact, it does not depend on which three points A, B, C are chosen in the domain of the projectivity (Exercise 6.12).

PROPOSITION 5.9. *A projectivity takes harmonic quadruples into harmonic quadruples (assuming P5).*

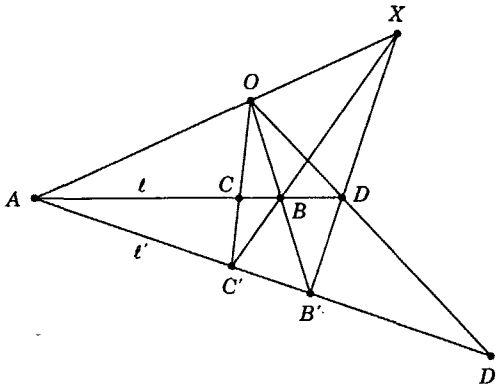


Figure 5.12. Harmonic points under perspectivity.

Proof. Since a projectivity is a composition of perspectivities, it will be sufficient to show that a perspectivity takes harmonic quadruples into harmonic quadruples.

So suppose $\ell \stackrel{\circ}{\lambda} \ell'$, and $H(A, B; C, D)$, where $A, B, C, D \in \ell$. Let A', B', C', D' be their images. Let $\ell'' = AB'$. Then $\ell \stackrel{\circ}{\lambda} \ell'' \stackrel{\circ}{\lambda} \ell'$ is the same mapping, so it is sufficient to consider $\ell \stackrel{\circ}{\lambda} \ell''$ and $\ell'' \stackrel{\circ}{\lambda} \ell'$ separately. Here one has the advantage that the intersection of the two lines is one of the four points considered. By relabeling, we may assume it is A in each case. Hence it is sufficient to solve the following problem:

Let $\ell \stackrel{\circ}{\lambda} \ell'$, and let $A = \ell \cdot \ell', B, C, D$ be four points on ℓ such that $H(A, B; C, D)$. Prove that $H(A, B'; C', D')$, where B', C', D' are the images of B, C, D .

Let X denote $BC' \cdot OA$. Consider the complete quadrangle $OXB'C'$. Two of its diagonal points are A, B ; C lies on the side OC' . Hence the intersection of XB' with ℓ must be the fourth harmonic point of ABC ; i.e. $XB' \cdot \ell = D$. (Here we use the uniqueness of the fourth harmonic point).

Now consider the complete quadrangle $OXBD$. Two of its diagonal points are A and B' ; The other two sides meet ℓ' in C' and D' . Hence $H(A, B'; C', D')$, as we wished to prove. \square

So we see that the group $PJ(\ell)$ is three times transitive, but it is not four times transitive, because it must take quadruples of harmonic points into quadruples of harmonic points.

EXERCISES

EXERCISE 5.1. Find the diagonal points of the complete quadrangle

- on the four points $(\pm 1, \pm 1, 1)$,
- and on the four points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, and $(1, 1, 1)$.

EXERCISE 5.2. Let π be the real projective plane, and let $A = (a, 0, 1)$, $B = (b, 0, 1)$, $C = (c, 0, 1)$, $D = (d, 0, 1)$, $a, b, c, d \in \mathbb{R}$, be four points on the " x_1 -axis". Prove that AB, CD are four harmonic points

if and only if the product

$$R_x(A, B; C, D) := \frac{a-c}{a-d} \cdot \frac{b-d}{b-c}$$

is equal to -1 . You may use methods of Euclidean geometry in the affine plane $x_3 \neq 0$.

EXERCISE 5.3. If P and Q are points in the real projective plane represented by the vectors v and w , respectively, in \mathbb{R}^3 , find an expression for the harmonic conjugate with respect to P and Q of the point R represented by $\alpha v + \beta w$.

EXERCISE 5.4. Prove that the map $T: \pi \rightarrow \pi^{**}$ defined by $T(P) = [P]$ ($=$ pencil of lines through P) is an isomorphism of projective planes.

EXERCISE 5.5. Give a simple demonstration that $\text{PJ}(\ell)$ is 2-transitive on the set of points constituting ℓ . I.e. given A, B and A', B' on ℓ find a projectivity $\ell \bar{\wedge} \ell$ taking $A \mapsto A', B \mapsto B'$.

EXERCISE 5.6. Consider the hyperbola $xy = 1$ in \mathbb{R}^2 : its tangent lines give a means of associating points on the x -axis with points on the y -axis. Show that this mapping sends x on the x -axis to $4/x$ on the y -axis, and is naturally extended to the projectivity in the real projective plane given by

$$(y = 0) \stackrel{(4,1)}{\bar{\wedge}} \ell_\infty \stackrel{(1,0)}{\bar{\wedge}} (y = 4x) \stackrel{Z}{\bar{\wedge}} (x = 0)$$

where Z is the ideal point on all lines with slope 0. If we denote this projectivity by $ABC \bar{\wedge} A'B'C'$, show that the cross-joins AB' and $A'B$ are parallel.²

EXERCISE 5.7. Pick a line ℓ in the seven point plane and compute $\text{PJ}(\ell)$. You should arrive at a subgroup of S_3 .

²It is in general true that conics (of which the hyperbola in the exercise is a special affine case) determine a projectivity between each pair of its tangent lines. See the appendix for more information.

EXERCISE 5.8. Refer to Figure 5.13.

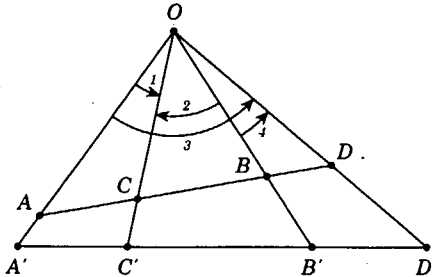


Figure 5.13. Cross ratio is invariant under central projection.

a) Apply the Law of Sines in the Euclidean plane to show that

$$R_X(A, B; C, D) = \frac{\sin \angle 1}{\sin \angle 2} \div \frac{\sin \angle 3}{\sin \angle 4}$$

b) Show that $R_X(A, B; C, D) = R_X(\overline{OA}, \overline{OB}; \overline{OC}, \overline{OD}) = R_X(A', B'; C', D')$.

c) Deduce that cross ratio is invariant under central projection. Cf. Example 3, p. 54.

EXERCISE 5.9. In the Euclidean plane define the cross ratio of four points on a circle as the cross ratio of the four lines determined by these and concurrent in a fifth point on the circle. Which well-known theorem of Euclidean geometry assures us that this definition is independent of the choice of fifth point? Apply Exercise 5.8 to obtain a good definition of the cross ratio of four points on any conic section. (You may use this exercise to demonstrate Pascal's Theorem in Exercise 6.17.)

EXERCISE 5.10. Let ℓ, ℓ' be two distinct lines in a projective plane π . Let $X = \ell \cdot \ell'$. Let A, B be two distinct points on ℓ , different from X . Let C, D be two distinct points on ℓ' , different from X . Construct a projectivity $\phi: \ell \rightarrow \ell'$ which sends A, X, B into X, C, D , respectively.

EXERCISE 5.11. Establish the following: given two harmonic quadruples A, B, C, D and A', B', C', D' , there exists a projectivity $ABCD \bar{\lambda} A'B'C'D'$. Identify the propositions used in your proof.

EXERCISE 5.12. In the ordinary Euclidean plane (considered as being contained in the real projective plane), let C be a circle with center O ; let P be a point outside C , and let t_1 and t_2 be the tangents from P to C , meeting C at A_1 and A_2 . Draw A_1A_2 to meet OP at B , and let OP meet C at X and Y .

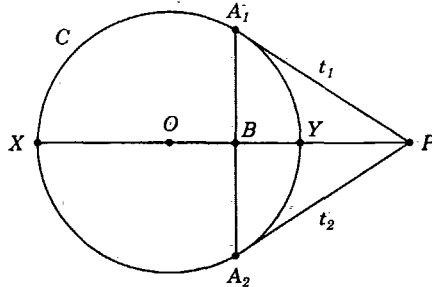


Figure 5.14. Construction of harmonic points using a circle.

a) Prove (by any method) that X, Y, B, P are four harmonic points.

b) What is the harmonic conjugate of the midpoint of a line segment with respect to its endpoints?

EXERCISE 5.13. Given a complete quadrangle $ABCD$ with diagonal points P, Q , and R , choose any three points of A, B, C, D , say ABC . Show that the harmonic conjugates of P, Q , and R with respect to AB, AC , and BC lie on a line.³

EXERCISE 5.14. Use Exercise 5.13 to prove the following Euclidean theorem: the medians of a triangle are concurrent.

EXERCISE 5.15. Show that the Desargues' Axiom converse implies Desargues' Axiom.

EXERCISE 5.16. Refer to Proposition 5.6. What are the permutations in S_4 under which an ordered 4-tuple of harmonic points remains harmonic? Do they form a group?

³Poncelet called this line the *trilinear polar* of D . Much of the theory in this chapter is due to him.

EXERCISE 5.17. Suppose⁴ that there exist points A, B, C, D , and E on a line such that

$$R_x(A, B; C, D) = R_x(A, B; C, E).$$

Show that $D = E$.

EXERCISE 5.18. Convince yourself that statements D1–D4 in Proposition 5.1 are an alternative and equivalent set of axioms for a projective plane.

EXERCISE 5.19. In the Euclidean plane one can define X to be between A and B if $d(A, B) = d(A, X) + d(X, B)$. This corresponds to our intuitive idea about betweenness. Suppose $AXB \bar{\wedge} A'X'B'$. Is X' between A' and B' ?

⁴This exercise extends Proposition 5.5 in the case of the real projective plane. In addition, you should obtain a simpler proof.

Chapter 6

The Fundamental Theorem for Projectivities on a Line

In Proposition 5.8 we saw that, having specified three collinear points A, B, C , and another three collinear points A', B', C' , we can find at least one projectivity $ABC \bar{\lambda} A'B'C'$. In this chapter, we come to the "Fundamental Theorem", which states that there is only one projectivity $ABC \bar{\lambda} A'B'C'$. Hence the image of a fourth point on ABC may be constructed by drawing a line through A, A' and a line through A and the point of intersection on the cross axis as in Proposition 5.8.

It turns out that the Fundamental Theorem cannot be proven from P1-P6, so we introduce it as an additional axiom P7, on the grounds that it is true in the real projective plane (Theorem 6.5). Then we examine the key role P7 plays in projective geometry: we prove both Pappus' Theorem and Desargues' Theorem in the presence of P7.

P7. FUNDAMENTAL THEOREM FOR PROJECTIVITIES ON A LINE. Let ℓ be a line in a projective plane. Let A, B, C and A', B', C' be two triples of three distinct points on ℓ . Then there is one and only one projectivity of ℓ into ℓ such that $ABC \bar{\lambda} A'B'C'$.

Since two lines are in one-to-one correspondence by some perspectivity, P7 holds on every line if it holds on a single line. As a simple

consequence of P7, $ABC \bar{\wedge} ABC$ must be the identity. Then a projectivity not equal to the identity has at most 2 fixed points. Next we consider how P7 may be reformulated in several ways.

PROPOSITION 6.1. *P7 is equivalent to:*

- P7'. Let ℓ and ℓ' be two distinct lines in a projective plane. Let $A, B, C \in \ell$ and $A', B', C' \in \ell'$. Then there is one and only one projectivity of ℓ onto ℓ' such that $ABC \bar{\wedge} A'B'C'$.
- P7''. Let ℓ and ℓ' be distinct lines in a projective plane and $X = \ell.\ell'$. Then every projectivity $\ell \bar{\wedge} \ell'$ sending X to itself is a perspectivity.

Proof. P7 \implies P7'. Suppose two distinct projectivities $\phi: ABC \bar{\wedge} A'B'C'$ and $\psi: ABC \bar{\wedge} A'B'C'$ exist mapping ℓ onto ℓ' . Then there is $X \in \ell$ such that $\phi(X) \neq \psi(X)$. Let O be a point not on either ℓ or ℓ' . Denote the perspectivity with center O between ℓ' and ℓ by $\tau: A'B'C' \stackrel{O}{\bar{\wedge}} A''B''C''$ where $A'' = OA'.\ell$, etc. Then $\tau\phi$ and $\tau\psi$ are two projectivities $ABC \bar{\wedge} A''B''C''$ of ℓ onto itself, but $\tau(\phi(X)) \neq \tau(\psi(X))$ since τ is a one-to-one correspondence. This contradicts P7.

P7' \implies P7''. Let A, B be two points on ℓ different from $X = \ell.\ell'$, and A', B' their images under a projectivity ϕ , which sends X to itself. Let $O = AA'.BB'$. Then ϕ must equal the perspectivity $ABX \stackrel{O}{\bar{\wedge}} A'B'X$ by P7'.

P7'' \implies P7. Suppose we have two projectivities on a line ℓ'' with the same effect on a triple of points: $\psi_1, \psi_2: PQR \bar{\wedge} P'Q'R'$. Given distinct lines ℓ and ℓ' we construct projectivities $\phi_1: PQR \bar{\wedge} XAB$ and $\phi_2: P'Q'R' \bar{\wedge} XA'B'$ where $X = \ell.\ell'$, $A, B \in \ell$ and $A', B' \in \ell'$. Then $\phi_2\psi_1\phi_1^{-1}$ and $\phi_2\psi_2\phi_1^{-1}$ both send $XAB \bar{\wedge} XA'B'$, so by P7'', $\phi_2\psi_1\phi_1^{-1} = \phi_2\psi_2\phi_1^{-1}$. Multiplying by ϕ_2^{-1} from the left and ϕ_1 from the right it follows that $\psi_1 = \psi_2$.¹ \square

¹With the same sort of argument one establishes the following principle: if in a projective plane π there exist collinear points A, B, C and A', B', C' such that $\psi_1, \psi_2: ABC \bar{\wedge} A'B'C' \implies \psi_1 = \psi_2$, then π satisfies P7 (Exercise 6.3). In other words, the Fundamental Theorem is equivalent to any of its special cases.

In chapter five the Principle of Duality would-naturally provide us with perspectivities between pencils of lines via a line as axis. We extend the Principle of Duality with the next proposition.

PROPOSITION 6.2. *P7 implies its dual statement:*

D7. *Let P be a point in a projective plane. Let a, b, c and a', b', c' be two triples of lines through P . Then there exists one and only one projectivity $abc \bar{\wedge} a'b'c'$.*

Proof. An elementary correspondence τ gives a one-to-one correspondence from a pencil of lines through Q , to the set of points, or *range* of points, on a line ℓ not passing through Q by associating a line m through P with the point $\ell.m$. (τ^{-1} is the same elementary correspondence, but the inverse mapping, from a range of points to a pencil of lines. Then a perspectivity is the application of two elementary correspondences.)

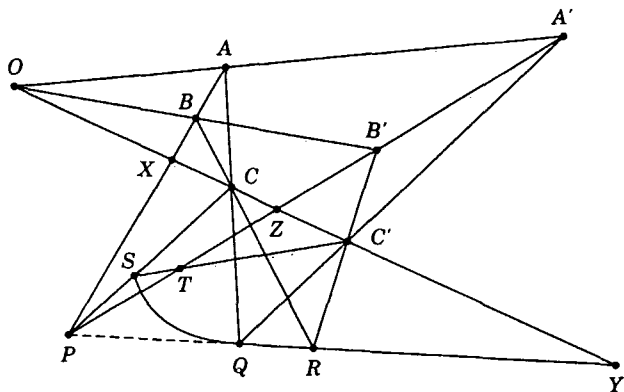
Now let P be the point in the hypothesis with ℓ a line not passing through P . Consider the elementary correspondence τ from the pencil of lines at P to the range of points on ℓ . Denote straightforwardly $\tau(a) = A, \tau(b) = B, \dots, \tau(c') = C'$. If $\psi_1, \psi_2: abc \bar{\wedge} a'b'c'$ are two projectivities, then $\tau\psi_1\tau^{-1}, \tau\psi_2\tau^{-1}: ABC \bar{\wedge} A'B'C'$ are two projectivities between ranges of points. (Why are $\tau\psi_i\tau^{-1}$ projectivities? Exercise 6.9). We have $\tau\psi_1\tau^{-1} = \tau\psi_2\tau^{-1}$ by P7, whence $\psi_1 = \psi_2$ as mappings, which establishes D7. \square

The next theorem says that *the Fundamental Theorem implies Desargues' Theorem*.

THEOREM 6.3. *If P7 holds in a projective plane π , then P5 holds in π .*

Proof. Given lines $OAA', OBB', OCC', ABP, ACQ, BCR, A'B'P, A'C'Q, B'C'R$, we have to show that PQR is a line. So we should prove P is on QR .

Let $S = CP.QR, T = A'B'.C'S, X = AB.OC, Y = OC.QR$, and $Z = OC'.A'B'$. We consider first the projectivity $ABXP \stackrel{Q}{\bar{\wedge}} A'B'ZP$. Second, consider the projectivity $ABXP \stackrel{C}{\bar{\wedge}} QRS \stackrel{C'}{\bar{\wedge}} A'B'ZT$.

Figure 6.1. Proof of Desargues' Theorem: $P = T = S$.

By the Fundamental Theorem, the two projectivities must be identical, hence $T = P$. This implies that $P \in C'S$. Since $S \in CP$, we get $S \in C'P.CP$. So $S = P$, which implies that $P \in QR$. \square

6.1 Geometry of Complex Numbers

In this section we wish to check P7 in the real projective plane. In order to do this we introduce Möbius transformations of the complex numbers and prove a lemma, all of which will be useful also in later chapters.

Recall that \mathbb{R}^2 may be identified with \mathbb{C} via the mapping $(a, b) \mapsto a+bi$, thereby giving \mathbb{R}^2 multiplication and division operations $(a, b)(c, d) = (ac - bd, bc + ad)$ and $(a, b) \div (c, d) = \left(\frac{ac+bd}{c^2+d^2}, \frac{bc-ad}{c^2+d^2}\right)$ so long as $c^2 + d^2 \neq 0$. These formulas are usually remembered by using the complex number notation and the relation $i^2 = -1$.

DEFINITION. Let \mathbb{C}_∞ denote the extended complex numbers $\mathbb{C} \cup \{\infty\}$. Define for all $a, b, c, d \in \mathbb{C}$ such that $ad - bc \neq 0$ a mapping $f: \mathbb{C}_\infty \rightarrow \mathbb{C}_\infty$ by $x \mapsto \frac{ax+b}{cx+d}$, $\infty \mapsto \begin{cases} a/c, & c \neq 0 \\ \infty, & c = 0 \end{cases}$, and $-d/c \mapsto \infty$ if $c \neq 0$. f is called a *Möbius transformation*, or *fractional linear transformation*.

LEMMA 6.4. *The set of Möbius transformations form a group under composition; in particular, each Möbius transformation is a one-to-one correspondence of \mathbb{C}_∞ with itself. Furthermore, a Möbius transformation is determined by its value on three elements in \mathbb{C}_∞ .*

Proof. Given a Möbius transformation denoted by $f(x) = \frac{ax+b}{cx+d}$, and another $g(x) = \frac{a'x+b'}{c'x+d'}$, their composite is

$$f \circ g(x) = \frac{(aa' + bc')x + (ab' + bd')}{(ca' + dc')x + (cb' + dd')}$$

as can be obtained by direct computation. Note that the coefficients in the composite correspond from left to right, up to down, with the coefficients in the matrix product

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix},$$

while the condition $ad - bc \neq 0$ is equivalent to $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$. Since determinant of square matrices \mathbf{A}, \mathbf{B} satisfies $\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$, it follows that $f \circ g$ is a Möbius transformation.

The identity $f(x) = x$ is obtained when $a = d = 1, b = c = 0$. Moreover, a Möbius transformation $\frac{ax+b}{cx+d}$ has inverse function $\frac{dx-b}{-cx+a}$ corresponding to the adjugate matrix: whence it is a one-to-one correspondence of \mathbb{C}_∞ with itself.

To prove the last statement in the lemma it suffices to check that there is one and only one Möbius transformation $f_{\alpha,\beta,\gamma}$ taking $0, 1, \infty$ to an arbitrary triple α, β, γ in \mathbb{C}_∞ . For then $f_{\alpha',\beta',\gamma'} \circ f_{\alpha,\beta,\gamma}^{-1}$ is clearly the unique Möbius transformation sending an arbitrary triple α, β, γ to α', β', γ' in \mathbb{C}_∞ .

First suppose $\alpha, \beta, \gamma \in \mathbb{C}$ and $f(x) = \frac{ax+b}{cx+d}$. Then

- (1) $f(0) = b/d = \alpha,$
- (2) $f(1) = \frac{a+b}{c+d} = \beta,$ and
- (3) $f(\infty) = a/c = \gamma.$

Clearly, one parameter of a Möbius transformation is freely chosen, so take $d = 1$. This forces $b = \alpha$, $a = c\gamma$, and $\beta = \frac{a+b}{c+1}$, so $\beta = \frac{c\gamma+\alpha}{c+1}$, forcing $c = \frac{\alpha-\beta}{\beta-\gamma}$ and $a = \gamma \frac{\alpha-\beta}{\beta-\gamma}$. Then

$$ad - bc = \frac{(\alpha - \beta)(\gamma - \alpha)}{\beta - \gamma} \neq 0;$$

after multiplication through by the factor $\beta - \gamma$, we get

$$f(x) = \frac{\gamma(\alpha - \beta)x + \alpha(\beta - \gamma)}{(\alpha - \beta)x + (\beta - \gamma)}$$

to be the Möbius transformation determined by equations (1), (2), and (3). If one of $\alpha, \beta, \gamma = \infty$, a similar computation determines a unique Möbius transformation (Exercise 6.13). \square

THEOREM 6.5. *The Fundamental Theorem (Axiom P7) holds in the real projective plane.*

Proof. We first show that a perspectivity $\ell \stackrel{O}{\sim} \ell'$ is given by a Möbius transformation if the ideal points on ℓ and ℓ' are both identified with ∞ . Suppose ℓ is parametrized by $(a + ib)t + c + id = ut + v$, ℓ' by $(a' + ib')s + c' + id' = u's + v'$, and O has coordinates (p, q) .

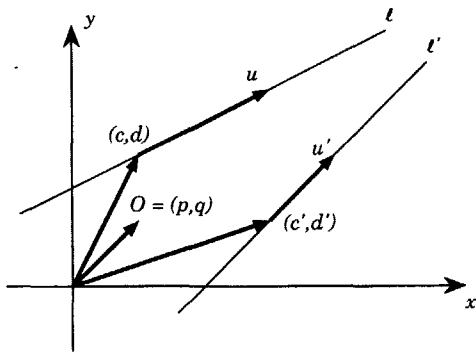


Figure 6.2.

We claim that $\ell \stackrel{O}{\wedge} \ell'$ is the Möbius transformation $M_4 M_3^{-1} M_2 M_1(t)$ of \mathbb{C}_∞ , where M_1, M_2, M_3 and M_4 are given by

$$\begin{aligned} M_1(x) &= u^{-1}x - u^{-1}v, & M_2(x) &= \frac{ax+c-p}{bx+d-q} \\ M_3(x) &= \frac{a'x+c'-p}{b'x+d'-q}, & M_4(x) &= u'x + v'. \end{aligned}$$

Note that $M_4 M_3^{-1} M_2 M_1(ut+v) = u' M_3^{-1} M_2(t) + v'$ so we must show that $ut+v, p+iq$, and $u' M_3^{-1} M_2(t) + v'$ are collinear. Let $M = M_3^{-1} M_2$. We must show that the slope of the line through points $ut+v$ and $p+iq$ equals the slope of the line through the points $u'M(t) + v'$ and $p+iq$: i.e. show that

$$\frac{bt+d-q}{at+c-p} = \frac{b'M(t)+d'-q}{a'M(t)+c'-p}.$$

Now, the left hand side is equal to $1/M_2(t)$, the right hand side equal to

$$\frac{1}{M_3(M(t))} = \frac{1}{M_3 \circ M_3^{-1} \circ M_2(t)} = \frac{1}{M_2(t)}.$$

This proves the identity.

Thus a perspectivity $\ell \stackrel{O}{\wedge} \ell'$ with center O in \mathbb{R}^2 is a Möbius transformation of the line ℓ in \mathbb{C}_∞ onto ℓ' in \mathbb{C}_∞ . It is left as an easy exercise to check the same if O is an ideal point (giving parallel projection of ℓ onto ℓ' — this implies $M_3^{-1} M_2(t) = kt$ for some stretching constant k). It follows that any projectivity $\ell \stackrel{\lambda}{\wedge} \ell'$ is similarly a complex Möbius transformation restricted to $\ell \cup \{\infty\}$. By Lemma 6.4, a Möbius transformation is determined by its effect on three points. Hence, any projectivity is uniquely determined by its values on three points, which is the Fundamental Theorem. \square

6.2 Pappus' Theorem

We now come to one of the oldest of projective theorems, which states that if six vertices of a hexagon lie alternately on two lines, then the three pairs of opposite sides meet in collinear points. The theorem was discovered by Pappus of Alexandria, living in the fourth century A.D., and demonstrated with laborious Euclidean methods.

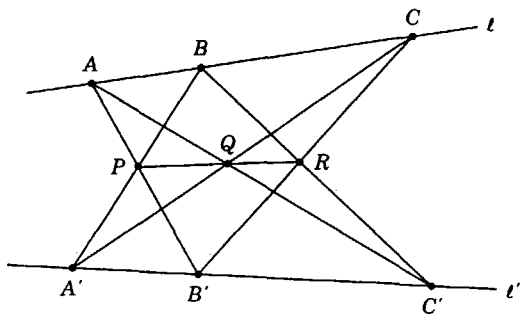


Figure 6.3. Pappus' Theorem: if hexagon $AB'CA'B'C'$ is inscribed on two lines, then the pairs of opposite sides meet in three collinear points.

THEOREM 6.6 (PAPPUS' THEOREM). *Let ℓ and ℓ' be two distinct lines. Let A, B, C be three distinct points on ℓ , different from $Y = \ell.\ell'$. Let A', B', C' be three distinct points on ℓ' , different from Y . Define $P = AB'.A'B$, $Q = AC'.A'C$, and $R = BC'.B'C$. Then P, Q , and R are collinear.*

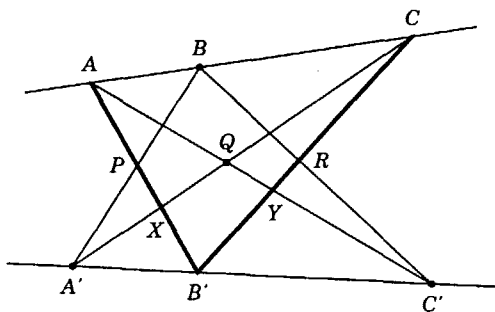


Figure 6.4. Proof of Pappus' Theorem.

Proof. Refer to Figure 6.4. We will construct a projectivity from line AB' into line $B'C$. Let σ be the elementary correspondence from AB' into the pencil of lines through A' , and τ the elementary correspondence from the pencil of lines through C' into the range of points on $B'C$. Finally let η be the perspectivity from the pencil of lines through

A' into the pencil of lines through C' having ℓ as an axis:

$$\eta: A'X \mapsto C'X \quad (\forall X \in \ell).$$

Consider the projectivity $\phi_1: AB' \bar{\wedge} B'C$ defined as

$$\phi: AXB' \bar{\wedge} ZCB'.$$

Since B' is fixed ϕ is a perspectivity by Axiom P7: indeed ϕ is the perspectivity with center Q .

Clearly $\phi(P) = \tau(BC') = R$, whence P, Q and R are collinear. \square

In a Desarguesian plane, Pappus' Theorem is in fact equivalent to statement P7, or any one of its variants. You may work out the implication Pappus \implies P7 in Exercises 6.14–6.16 below. For this reason we will follow tradition and occasionally refer to projective planes that satisfy P7 as *Pappian planes*.

EXERCISES

EXERCISE 6.1. If A, B, C and A', B', C' are two triples on the same line, construct the image X' of a fourth collinear point X under the projectivity $ABC \bar{\wedge} A'B'C'$ (assuming the Fundamental Theorem).

EXERCISE 6.2. Let π be a finite Pappian plane having $p^2 + p + 1$ points in all. If ℓ is a line in π , then what is the order of the group $PJ(\ell)$?

EXERCISE 6.3. Suppose that the following statement is true in π : there exist collinear triples A, B, C and A', B', C' such that if ψ_1, ψ_2 both send $ABC \bar{\wedge} A'B'C'$, then $\psi_1 = \psi_2$ as mappings. Show that Axiom P7 holds in π : i.e. if P, Q, R and P', Q', R' are any two triples of points on a line ℓ , then there is a unique projectivity $PQR \bar{\wedge} P'Q'R'$.

EXERCISE 6.4. If A, B, C and A', B', C' are triples of points on a line ℓ in a projective plane π , show that if there are two different projectivities $ABC \bar{\wedge} A'B'C'$, then there exist two different projectivities $ABC \bar{\wedge} A''B''C''$ between distinct lines of π .

EXERCISE 6.5. (Together with Exercises 5.8 and 5.17, this exercise will provide an alternative proof that P7 holds in the real projective plane.) Suppose ψ_1 and ψ_2 are projectivities on a real projective line both sending $ABC \bar{\wedge} A'B'C'$. Choose a fourth point X , different from A , B , or C and show that $\psi_1(X) = \psi_2(X)$ by using cross ratios.

EXERCISE 6.6. For each of the following projective planes, state which of the axioms P5, P6, P7 holds in it, and explain why each axiom does or does not hold. (Please refer to results proved earlier, and give *brief* outlines of their proofs.)

- The projective plane of seven points.
- The real projective plane.
- The Moulton plane.

EXERCISE 6.7. Let π be a projective plane satisfying P5, P6, and P7, and let ℓ be a line in π .

a) Prove that if ϕ is a projectivity of ℓ onto ℓ which interchanges two distinct points A, B of ℓ (i.e. $\phi(A) = B$ and $\phi(B) = A$), then ϕ^2 is the identity.²

b) Conclude that $A'B'C'D' \bar{\wedge} B'A'D'C'$ for any 4 points A', B', C', D' on a line.

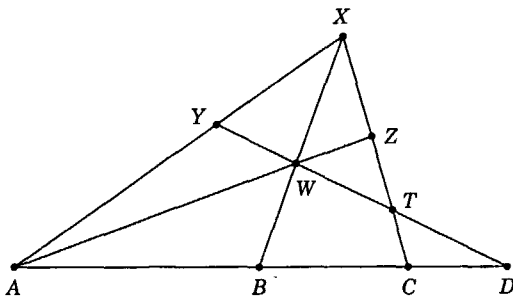


Figure 6.5. Existence of involution $ABCD \bar{\wedge} BADC$.

²A projectivity $\phi: \ell \bar{\wedge} \ell$ such that $\phi^2 = \text{id}_\ell$ is called an involution. You are asked to prove that a projectivity interchanging a pair of points is an involution.

Hint. Let C be another point of ℓ and let $\phi(C) = D$. Construct a projectivity $\phi': \ell \rightarrow \ell$ which interchanges A and B , and interchanges C and D , using Figure 6.5; justify. Then apply the Fundamental Theorem.

EXERCISE 6.8 (G. HESSENBERG, 1905). Prove that Pappus' Theorem implies Desargues' Theorem.

Hint. Using the labelling in Figure 3.1, define $S = A'C'.AB$ and apply Pappus' Theorem to the triad $(\begin{smallmatrix} O & C & C' \\ B & S & A \end{smallmatrix})$, label the new points, and apply Pappus' Theorem again to the triad $(\begin{smallmatrix} O & B & B' \\ C' & A & S \end{smallmatrix})$. Label the new point and apply Pappus' Theorem again to conclude that P, Q, R are collinear.

EXERCISE 6.9. Suppose τ is the elementary correspondence between the pencil $[P]$ of lines through P and range of points on ℓ . Show that if ϕ is a projectivity between the pencil of lines, $[P] \xrightarrow{\lambda} [P_1] \xrightarrow{\mu} \dots \xrightarrow{\nu} [P]$, then $\tau\phi\tau^{-1}$ is a projectivity between the range of points $\ell \xrightarrow{\lambda} \ell_1 \xrightarrow{\mu} \ell_2 \xrightarrow{\nu} \dots \xrightarrow{\lambda} \ell_n \xrightarrow{\mu} \ell$.

EXERCISE 6.10. Let T be a complex Möbius transformation sending three points Z, Z_1, Z_2 on a line ℓ in \mathbb{R}^2 into three points Z, W_1, W_2 , respectively, on a line $m = Z$.

- Is T restricted to ℓ a perspectivity from ℓ to m ?
- If so, where does the center lie?
- How many fixed points does T have?

EXERCISE 6.11. Establish by direct means Pappus' Theorem in the real projective plane: Let $\ell, \ell', A, B, C, A', B', C'$ be as in the statement of Pappus' Theorem, and take ℓ to be the line at infinity. Then prove by Euclidean methods that $P = A'B.AB'$, $Q = A'C.AC'$, and $R = B'C.BC'$ are collinear.

EXERCISE 6.12. Prove that the cross axis does not depend on which three points A, B, C are chosen in the domain of the projectivity.

EXERCISE 6.13. Prove the existence and uniqueness of a Möbius transformation sending $0, 1, \infty$ to α, β, γ in each case where one of α, β, γ is ∞ .

Suppose π is a projective plane where Desargues' Theorem and Pappus' Theorem are true. The next three exercises will guide you through to a proof that π satisfies P7. Thus Pappus' Theorem is equivalent to the Fundamental Theorem.

As pointed out in the text it will suffice to show that any projectivity between distinct lines, $\tau: \ell \rightarrow \ell'$, which fixes $X = \ell.\ell'$, i.e. $\tau(X) = X$, is a perspectivity.

EXERCISE 6.14. Suppose ℓ_1, ℓ_2 , and ℓ_3 are distinct concurrent lines. Suppose the projectivity τ is given by $\ell_1 \xrightarrow{P_1} \ell_2 \xrightarrow{P_2} \ell_3$. Let the effect of τ on points be given by $A_1X_1 \xrightarrow{P_1} A_2X_2 \xrightarrow{P_2} A_3X_3$. Use Desargues' Theorem to prove that ϕ is the perspectivity $\ell_1 \xrightarrow{Q} \ell_3$ where $Q = A_1A_2.P_1P_2$.

EXERCISE 6.15. Suppose τ is the projectivity given by $\ell \xrightarrow{P_1} \ell_1 \xrightarrow{P_2} \ell_2 \xrightarrow{P_3} \ell'$, where $\ell, \ell_1, \ell_2, \ell'$ are distinct lines, no three being concurrent. Consider the line m joining $\ell.\ell_1$ and $\ell_2.\ell'$. Aside from the case where $P_2 \in m, \ell.\ell_1$, τ is equal to the projectivity, $\ell \xrightarrow{P_1} \ell_1 \xrightarrow{P_2} m \xrightarrow{P_3} \ell_2 \xrightarrow{P_3} \ell'$.

a) Show that points Q and R may be found such that τ is the projectivity $\ell \xrightarrow{Q} m \xrightarrow{R} \ell'$.

b) Show that the chain of perspectivities defining τ may also be shortened by one perspectivity in the exceptional case where $P_3 \in m$.

c) Assume that ℓ, ℓ_1 , and ℓ' are concurrent. By inserting a line through ℓ_1, ℓ_2 and avoiding P_3 , reduce to the case we started with (four lines, no three concurrent).

d) Conclude that any projectivity between distinct lines may be given as a chain of only two perspectivities.

EXERCISE 6.16. By Exercise 6.15, we may find points $P_1, P_2 \in \pi$ and line m , such that τ is the projectivity $\ell \xrightarrow{P_1} m \xrightarrow{P_2} \ell'$. If m is concurrent with ℓ and ℓ' , we are done by Exercise 6.14. Suppose m is not concurrent with ℓ and ℓ' . Recall that $X = \ell.\ell'$ and $\tau(X) = X$. Let $\ell.m = V, \ell'.m = U$, and $XP_1.m = T$.

a) Show that P_1, P_2 , and X are collinear.

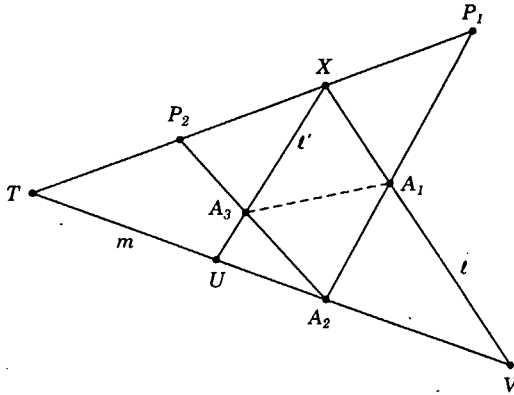


Figure 6.6.

b) Let τ map $A_1 \mapsto A_2 \mapsto A_3$ as pictured. Applying Pappus, show that A_1A_3 passes through the point $Q = P_1U.P_2V$ for all $A_1 \in \ell$ with image $A_3 \in \ell'$ under τ . Conclude that $\tau: \ell \xrightarrow{Q} \ell'$, and that π satisfies Axiom P7.

EXERCISE 6.17. Prove PASCAL'S THEOREM in $\mathbb{P}^2(\mathbb{R})$: If hexagon $ABCDEF$ is inscribed in a conic section, then the three pairs of opposite sides meet in three collinear points.

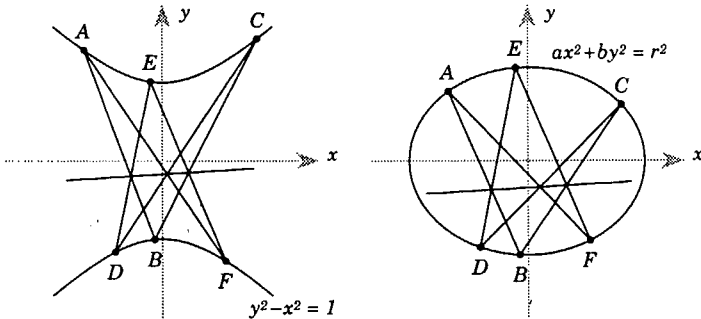


Figure 6.7. Pascal's Theorem.

Hint. Apply cross ratio of 4 points on a conic section (defined in Exercise 5.9) and uniqueness of the fourth point in fixed cross ratio (Exercise

5.17 and its dual). You should set out to prove that lines PR and QR are equal by drawing some helping lines and projecting cross ratio about the figure.

EXERCISE 6.18. Show that complex Möbius transformations map circles and lines into circles and lines.

EXERCISE 6.19. Answer Castillon's Problem: given a circle Γ in the Euclidean plane and points $A, B, C \notin \Gamma$, is there a triangle inscribed on Γ whose sides pass through A, B , and C ?

Chapter 7

A Brief Introduction to Division Rings

In this chapter we introduce the notions of ring, division ring and field. We give basic examples of each: polynomial and Laurent series rings, quaternions and the finite fields of integers modulo p . Replacing \mathbb{R} in $\mathbb{P}^2(\mathbb{R})$ with general division rings will provide us with many examples of projective planes in Chapter 8.

DEFINITION. A *ring* is a set R together with two binary operations $+$ and \cdot on R , denoted by $(a, b) \mapsto a + b$ and $(a, b) \mapsto ab$, such that

R1. $(R, +)$ is an abelian group, whose neutral element we denote by 0 .

R2. (R, \cdot) is a semigroup¹ possessing a unit element 1 .

R3. \cdot is left and right distributive over $+$: $a(b + c) = ab + ac$, and $(a + b)c = ac + bc$ (for all $a, b, c \in R$).

A *division ring* is a ring R such that

DR1. $(R - \{0\}, \cdot, 1)$ is a group.

¹We have followed tradition and dropped the dot in $a \cdot b$.

I.e. every nonzero element has a multiplicative inverse. A *field* is a division ring F such that

$$\text{F1. } ab = ba \text{ (for all } a, b \in F)$$

I.e. multiplication is a commutative operation.

EXAMPLE 1. The set of integers \mathbb{Z} under addition and multiplication is clearly a ring. Since multiplication is a commutative operation, we can express this by saying \mathbb{Z} is a *commutative ring*.

EXAMPLE 2. The set of all $n \times n$ matrices ($n > 1$) with real coefficients, $M_n(\mathbb{R})$, is a ring under the usual matrix addition and matrix multiplication. In this example multiplication is noncommutative, and not every nonzero matrix has an inverse. Other examples of rings are obtained by replacing \mathbb{R} in $M_n(\mathbb{R})$ with \mathbb{Q} , \mathbb{C} , any field or indeed any ring (Exercise 7.17).

EXAMPLE 3. Familiar examples of fields are the rationals \mathbb{Q} , \mathbb{R} , \mathbb{C} under ordinary addition and multiplication.

A *subfield* is straightforwardly defined as a subset of a field closed under addition and multiplication, containing 0 and 1, and itself a field. For example, \mathbb{Q} is a subfield of \mathbb{R} , which in turn is a subfield of \mathbb{C} .

EXAMPLE 4. THE INTEGERS MODULO n . Let n be an integer greater than 1. We say integers a and b are *congruent modulo n* , writing $a \equiv b \pmod{n}$, if $a - b$ is a multiple of n . Check that this is an equivalence relation on \mathbb{Z} (Exercise 7.18).

Denote the equivalence class of a by $[a]$, i.e. $[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{n}\}$, and the set of all equivalence classes by $\mathbb{Z}_n (= \{[0], [1], \dots, [n-1]\})$. Note that $[a]$ is the left coset $a + n\mathbb{Z}$ of the subgroup $n\mathbb{Z}$ of \mathbb{Z} under addition; according to Exercise 4.4, \mathbb{Z}_n is a group with addition given by

$$[a] + [b] = [a + b].$$

By Exercise 4.6 the map $\pi: a \mapsto [a]$ is a surjective group homomorphism. Define a *ring homomorphism* to be a mapping between rings $f: R_1 \rightarrow R_2$ satisfying $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$

(for all $x, y \in R_1$). Now you might guess that decreasing π a ring homomorphism would carry over to \mathbb{Z}_n the multiplication making it a ring, and you would be right. Indeed, define a multiplication in \mathbb{Z}_n by

$$[a][b] = [ab].$$

This definition is independent of the representatives a and b of their respective equivalence classes, since

$$(a + kn)(b + rn) = ab + (kb + ra + krn)n.$$

It is a rather simple exercise (Exercise 7.19) to check distributivity of multiplication over addition in \mathbb{Z}_n . Then \mathbb{Z}_n is a commutative ring \mathbb{P} . Let $n = 6$: observe that $[2][3] = [0]$ in \mathbb{Z}_6 , so clearly \mathbb{Z}_6 is not a field. (In a general ring R , a is called a *zero divisor* if $a \neq 0$ and there exists $b \in R - \{0\}$ such that $ab = 0$).

Suppose n is a prime p . We claim that \mathbb{Z}_p is a field. I.e. if $[a] \neq [0]$, then $[a]$ is *invertible*. Here is why: since a and p are relatively prime, there exist integers b and k such that $ab + pk = 1$ (Exercise 7.20). Then $[a][b] = [1]$, so $[a]$ has an inverse as claimed.

Note that in \mathbb{Z}_p , adding $[1]$ together p times gives 0: $p[1] = [0]$. We say that \mathbb{Z}_p is a field of characteristic p , and make the following definition.

DEFINITION. Let F be a division ring. The *characteristic* of F is the smallest integer $p \geq 2$ such that

$$\underbrace{1 + \cdots + 1}_{p \text{ times}} = 0$$

or, if there is no such integer, the characteristic of F is defined to be 0.

PROPOSITION 7.1. *The characteristic p of a division ring F is always 0 or a prime number.*

Proof. If $p \neq 0$, suppose $p = m \cdot n$ where $m, n > 1$. Then

$$(m1)(n1) = \underbrace{(1 + \cdots + 1)}_{m \text{ times}} \underbrace{(1 + \cdots + 1)}_{n \text{ times}} = p1 = 0.$$

Hence one of $m1$ or $n1$ must be 0, which contradicts the choice of p . Hence, p is prime. \square

EXAMPLES OF CHARACTERISTIC. The fields \mathbb{Q} , \mathbb{R} , and \mathbb{C} have characteristic 0. We have seen that there exists a field of each prime characteristic. The quaternions described below form a noncommutative division ring of characteristic 0. Later we construct a skew Laurent series ring over $\mathbb{Z}_p(x)$, providing lots of examples of polynomials and an example of a noncommutative division ring of characteristic p .

7.1 The Quaternions \mathbb{H}

We define on \mathbb{R}^4 , the set of ordered 4-tuples of reals, an addition and multiplication that yields a division ring we denote² by \mathbb{H} . Addition is just coordinatewise addition familiar from linear algebra:

$$(x_1, x_2, x_3, x_4) + (y_1, y_2, y_3, y_4) = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4).$$

Multiplication is given by the complicated but interesting formula;

$$(7.1) \quad (x_1, x_2, x_3, x_4) \cdot (y_1, y_2, y_3, y_4) = \\ (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4, x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3, \\ x_1y_3 + x_3y_1 + x_4y_2 - x_2y_4, x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2).$$

The formula does lend itself to four quick insights.

- 1) $(1, 0, 0, 0)$ is the unit element.
- 2) Multiplication is distributive over addition.
- 3) We have

$$(cx_1, cx_2, cx_3, cx_4) \cdot (y_1, y_2, y_3, y_4) = \\ (x_1, x_2, x_3, x_4) \cdot (cy_1, cy_2, cy_3, cy_4) \quad (\forall c \in \mathbb{R}).$$

Using ordinary scalar multiplication of \mathbb{R} in \mathbb{R}^4 , we write at times $c(x_1, x_2, x_3, x_4)$ in place of (cx_1, cx_2, cx_3, cx_4) .

- 4) If

$$\|(x_1, x_2, x_3, x_4)\| = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}$$

²After their discoverer, W. R. Hamilton (1805–1865)

denotes the Euclidean norm on \mathbb{R}^4 , then

$$\begin{aligned}(x_1, x_2, x_3, x_4) \cdot (x_1, -x_2, -x_3, -x_4) &= (\|(x_1, x_2, x_3, x_4)\|^2, 0, 0, 0) \\ &= (x_1, -x_2, -x_3, -x_4) \cdot (x_1, x_2, x_3, x_4)\end{aligned}$$

so each nonzero 4-tuple is invertible.

Define \mathbb{H} to be \mathbb{R}^4 equipped with $+$ and \cdot as above and call its elements *quaternions*. We must only check associativity to see that \mathbb{H} is a division ring. There are two approaches that avoid direct computation. First, we assign certain key quaternions their standard notations: $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$, $k = (0, 0, 0, 1)$, and the unit $\mathbf{1} = (1, 0, 0, 0)$. Since $\{\mathbf{1}, i, j, k\}$ is a basis of \mathbb{R}^4 , any quaternion is a linear combination of these: $q = x_1\mathbf{1} + x_2i + x_3j + x_4k$. Note that $G = \{\pm\mathbf{1}, \pm i, \pm j, \pm k\}$ is closed under multiplication: $i^2 = -\mathbf{1} = j^2 = k^2$, $ij = k = -ji$, $jk = i = -kj$, $ik = -j = -ki$. We could check somewhat laboriously that G is a group and deduce an associative multiplication on \mathbb{H} from this (Exercise 7.11).

REMARK. If we identify the space of *pure quaternions* $\{a_1i + a_2j + a_3k \mid a_1, a_2, a_3 \in \mathbb{R}\}$ with the space of 3-vectors $\mathbb{R}^3 = \{v \mid v = v_1i + v_2j + v_3k\}$ equipped with dot product and cross product, the multiplication of quaternions is given by

$$(7.2) \quad (x_1\mathbf{1} + v) \cdot (y_1\mathbf{1} + w) = (x_1y_1 - v \cdot w)\mathbf{1} + y_1v + x_1w + v \times w$$

Check this formula against Formula 7.1 above using your knowledge of vector analysis (Exercise 7.10).³

A second method for establishing associativity on the quaternions uses 2×2 matrices of complex numbers. We define a mapping $T: \mathbb{H} \rightarrow M_2(\mathbb{C})$: first break down a quaternion $q = x_1\mathbf{1} + x_2i + x_3j + x_4k$ into two complex numbers $\alpha = x_1 + x_2\sqrt{-1}$ and $\beta = x_3 + x_4\sqrt{-1}$. Define

$$T(q) = \begin{pmatrix} x_1 + x_2\sqrt{-1} & x_3 + x_4\sqrt{-1} \\ -x_3 + x_4\sqrt{-1} & x_1 - x_2\sqrt{-1} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}.$$

We note that:

³Historically, the quaternions led to the cross product on vectors.

T is an *injective* mapping clearly since $q_1 \neq q_2 \implies T(q_1) \neq T(q_2)$.

T is *multiplicative*, i.e. $T(qw) = T(q)T(w)$ (for all $q, w \in \mathbb{H}$), since taking q above and letting $w = y_1\mathbf{1} + y_2i + y_3j + y_4k$, $\gamma = y_1 + y_2\sqrt{-1}$, and $\delta = y_3 + y_4\sqrt{-1}$, we compute

$$(7.3) \quad T(q)T(w) = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\bar{\beta}\gamma - \bar{\alpha}\bar{\delta} & -\bar{\beta}\delta + \bar{\alpha}\bar{\gamma} \end{pmatrix}.$$

Now page back to Formula 7.1 where the quaternion product qw is given. Break the quaternion qw into two complex numbers ρ and σ , i.e. $T(qw) = \begin{pmatrix} \rho & \sigma \\ -\bar{\sigma} & \bar{\rho} \end{pmatrix}$. It is easily checked by hand that $\rho = \alpha\gamma - \beta\bar{\delta}$ and $\sigma = \alpha\delta + \beta\bar{\gamma}$ (cf. Exercise 7.12). Hence T is multiplicative.

We must show $(q_1q_2)q_3 = q_1(q_2q_3)$ (for all $q_1, q_2, q_3 \in \mathbb{H}$). Since matrix multiplication is associative, it follows that

$$\begin{aligned} T((q_1q_2)q_3) &= T(q_1q_2)T(q_3) = (T(q_1)(T(q_2))T(q_3)) \\ &= T(q_1)(T(q_2)T(q_3)) = T(q_1)T(q_2q_3) = T(q_1(q_2q_3)), \end{aligned}$$

so $(q_1q_2)q_3 = q_1(q_2q_3)$ by injectivity of T .⁴

Certain elements q in \mathbb{H} *commute* with all other quaternions: $qq' = q'q$ (for all $q' \in \mathbb{H}$). For example $(x\mathbf{1})q = q(x\mathbf{1})$ (for all $x \in \mathbb{R}$ by using one of Equations 7.1, 7.2, or 7.3). You will be asked to provide a proof that $\{x\mathbf{1} \mid x \in \mathbb{R}\}$ is the full set of quaternions that commute with all quaternions (Exercise 7.14).

DEFINITION. Let F be a division ring. Let $Z(F)$ be the set of $a \in F$ such that $ab = ba$ for all $b \in F$. $Z(F)$ is called the *center* of F .

PROPOSITION 7.2. *The center $Z(F)$ of a division ring is a field.*

Proof. Suppose $a, b \in Z(F)$. Then for all $c \in F$

$$(a + b)c = ac + bc = ca + cb = c(a + b)$$

⁴There is a principle involved here that could be formulated as follows for sets A and B with one or more binary operations: If $T: A \rightarrow B$ is a one-to-one correspondence preserving the binary operations, then whatever laws that hold on A must also hold on B .

and

$$(ab)c = a(bc) = a(cb) = \cdots = c(ab)$$

(fill in the missing steps). It follows that $Z(F)$ is closed under addition and multiplication. Also, $(-a)c = -(ac) = -(ca) = c(-a)$, so $-a \in Z(F)$. Moreover, $ab = ba$, so $Z(F)$ is a commutative ring. Finally, if $b \in Z(F) - \{0\}$

$$cb^{-1} = b^{-1}(bc)b^{-1} = b^{-1}(cb)b^{-1} = b^{-1}c \quad (\forall c \in F).$$

Hence $b^{-1} \in Z(F)$. This completes the proof. \square

We will find both center and automorphism of division rings crucial to our analytic development of projective geometry in the next chapter.

DEFINITION. An *automorphism* of a division ring F is a one-to-one correspondence $\sigma: F \rightarrow F$ such that

$$\begin{aligned} \sigma(a + b) &= \sigma(a) + \sigma(b) \\ \sigma(ab) &= \sigma(a)\sigma(b) \end{aligned} \quad (\forall a, b \in F).$$

It follows that $\sigma(0) = 0$ and $\sigma(1) = 1$. Note that the automorphisms of F form a group under composition, which we denote by $\text{Aut } F$.

EXAMPLE. In Exercise 7.7 you are invited to show that $\sigma_\lambda(x) = \lambda x \lambda^{-1}$ defines an automorphism of F for any $\lambda \neq 0$, called an *inner automorphism*. If $\lambda \in Z(F)$, then $\sigma_\lambda = \text{id}_F$. If $F = \mathbb{H}$, it can be shown that every automorphism is an inner automorphism.

7.2 A Noncommutative Division Ring with Characteristic p

PROPOSITION 7.3. *There exists a noncommutative division ring with arbitrary characteristic p .*

Proof. We sketch the construction of an example due to Hilbert. Certain details will be left to the exercises.

Given a field F with automorphism σ we show how to form the *skew Laurent series ring in one indeterminate* $F((z; \sigma))$, or D . Elements in D are formal sums with possibly infinitely many nonzero coefficients $a_j \in F$ having a lower bound in index:

$$\frac{a_{-m}}{z^m} + \frac{a_{-(m-1)}}{z^{m-1}} + \cdots + \frac{a_{-1}}{z} + a_0 z^0 + a_1 z + \cdots + a_n z^n + \cdots$$

or equivalently $\sum_{i=-m}^{\infty} a_i z^i$. The lower bound $-m$ will vary from element to element, and might be any integer. We can of course write the element $\sum_{i=-m}^{\infty} a_i z^i$ as $\sum_{i=-\infty}^{\infty} a_i z^i$ by assigning $a_i = 0$ to each $i < -m$. Define an addition on D by

$$\sum_{i=-\infty}^{\infty} a_i z^i + \sum_{i=-\infty}^{\infty} b_i z^i = \sum_{i=-\infty}^{\infty} (a_i + b_i) z^i.$$

Define multiplication on D by

$$\sum_{i=-n}^{\infty} a_i z^i \sum_{j=-m}^{\infty} b_j z^j = \sum_{k=-n-m}^{\infty} c_k z^k$$

where $c_k = \sum_{i+j=k} a_i \sigma^i(b_j)$. Note that multiplication is arrived at in three steps:

- 1) Enforcing the distributive law.
- 2) $z^i b = \sigma^i(b) z^i$ (i is zero, positive or negative, so σ^i stands for i successive applications of σ or its inverse, while $\sigma^0 = \text{id}$).
- 3) $z^i z^j = z^{i+j}$.

Multiplication is associative since

$$\begin{aligned} (a_i z^i b_j z^j) c_k z^k &= a_i \sigma^i(b_j) z^{i+j} c_k z^k = a_i \sigma^i(b_j) \sigma^{i+j}(c_k) z^{i+j+k} \\ &= a_i \sigma^i(b_j \sigma^j(c_k)) z^i z^{j+k} = a_i z^i (b_j z^j c_k z^k) \end{aligned}$$

It is now rather easy to see that D is a ring (Exercise 7.15).

The extraordinary fact is that D is a division ring. Since the unit element is z^0 , each z^i is invertible. By Exercise 4.2 it will suffice to show

that an arbitrary nonzero *Laurent series* $\sum_{i=-m}^{\infty} a_i z^i = f_1$ ($a_{-m} \neq 0$) has a right inverse. Since z^m is invertible, it will suffice to show how to find a right inverse of $f = f_1 z^m = \sum_{i=0}^{\infty} b_i z^i$ where $b_i = a_{i-m}$. Suppose $g = \sum_{k=0}^{\infty} c_k z^k$ satisfies $fg = 1$, then

$$\begin{aligned} b_0 c_0 &= 1 \\ b_1 \sigma(c_0) + b_0 c_1 &= 0 \\ b_2 \sigma^2(c_0) + b_1 \sigma(c_1) + b_0 c_2 &= 0 \\ &\vdots \end{aligned}$$

Taking $c_0 = b_0^{-1}$, $c_1 = -b_0^{-1} b_1 \sigma(b_0^{-1})$, and defining c_n inductively in terms of the first $n-1$ coefficients of f , it is clear that g above satisfies $fg = 1$. (For example, the student might recall the formula for the sum of a geometric series $\frac{1}{1-z} = \sum_{k=0}^{\infty} z^k$.)

So far we have built a division ring D for each field F and automorphism $\sigma: F \rightarrow F$. D will only be noncommutative if we can find a $\sigma \neq \text{id}$. In Exercise 7.7 you will show that taking $F = \mathbb{Z}_p$ won't do for completing the proof since \mathbb{Z}_p has no nontrivial automorphisms. We must therefore build a bigger field over \mathbb{Z}_p . One idea is to let $\sigma = \text{id}$ and $F = \mathbb{Z}_p$ in our general construction $F((z; \text{id})) = \mathbb{Z}_p((z))$, which is called the Laurent series ring in one indeterminate over \mathbb{Z}_p .

Now within the ring $\mathbb{Z}_p((z))$ restrict attention to the subring $\mathbb{Z}_p[z]$ of *polynomials*, elements of the form $\sum_{i=0}^n a_i z^i$, having no negative powers of z and whose nonnegative coefficients end at a power n of z (called the *degree* of the polynomial). Now each nonzero polynomial has an inverse in $\mathbb{Z}_p((z))$, so we might consider the set $\mathbb{Z}_p(z) = \{fg^{-1} \mid f, g \in \mathbb{Z}_p[z], g \neq 0\}$. Indeed $\mathbb{Z}_p(z)$ is a subfield of $\mathbb{Z}_p((z))$, called the *field of rational functions in one indeterminate* over \mathbb{Z}_p . (See Exercise 7.14 for another, equivalent construction of any field of rational functions in one indeterminate.) On the field $\mathbb{Z}_p(z)$ induce an automorphism by sending $z \mapsto z^{-1}$. Thus $z^2 \mapsto z^{-2}$, $p(z) = \sum_{i=0}^n a_i z^i \mapsto p(z^{-1}) = a_0 + \sum_{i=1}^n a_i z^{-i}$. Since $\sigma^2 = \text{id}$, σ is a bijection; it is clear that σ is linear and multiplicative, whence an automorphism.

Now consider $F((x; \sigma))$ where F is the field $\mathbb{Z}_p(z)$, and σ is the automorphism induced by $z \mapsto z^{-1}$. Written side by side $\mathbb{Z}_p(z)((x; \sigma))$ is a two variable skew Laurent series, but this needn't bother us. We

have shown that $\mathbb{Z}_p(z)((x; \sigma))$ is a noncommutative division ring. Note (carefully) that

$$\underbrace{1 + \cdots + 1}_p = 0$$

in this ring. Hence we have constructed a noncommutative division ring with characteristic p . \square

EXERCISES

EXERCISE 7.1. Let R be a ring. Show that

- a) $a0 = 0a = 0$ (for all $a \in R$).
 b) $(-a)c = -(ac) = a(-c)$ (for all $a, c \in R$).

EXERCISE 7.2. Suppose R is a ring with no zero divisors, i.e. $ab = 0 \implies a = 0$ or $b = 0$ (for all $a, b \in R$). Then multiplication satisfies left (and right) cancellation: $x \neq 0$ and $xy_1 = xy_2 \implies y_1 = y_2$. Prove.

EXERCISE 7.3. Show that conjugation is an automorphism of \mathbb{C} . Why is it not an inner automorphism?

EXERCISE 7.4. Define an operation on \mathbb{H} called *conjugation* (or *involution*): this is a mapping $\mathbb{H} \rightarrow \mathbb{H}$ defined by $q \mapsto q^* = x_1\mathbf{1} - x_2i - x_3j - x_4k$ where $q = x_1\mathbf{1} + x_2i + x_3j + x_4k$. Show that

- a) $q^{-1} = \frac{q^*}{\|q\|^2}$.
 b) $(q_1 + q_2)^* = q_1^* + q_2^*$.
 c) $(q_1 q_2)^* = q_2^* q_1^*$.
 d) EULERS' FORMULA (apply a)-c) to establish it):

$$\begin{aligned} (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = \\ (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4)^2 + (x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3)^2 \\ + (x_1y_3 + x_2y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

EXERCISE 7.5. An *isomorphism* of rings R_1 and R_2 is a one-to-one correspondence $\psi: R_1 \rightarrow R_2$ that satisfies

- 1) $\psi(x + y) = \psi(x) + \psi(y)$,
- 2) $\psi(xy) = \psi(x)\psi(y)$ (for all $x, y \in R_1$).

Show that

- a) $\psi(1) = 1$.
- b) If $u \in R_1$ is invertible, then $\psi(u)$ is invertible in R_2 .
- c) \mathbb{H} is not isomorphic with $M_2(\mathbb{R})$.

EXERCISE 7.6. Show that the subset $\{x1 + yi \mid x, y \in \mathbb{R}\}$ of \mathbb{H} forms a subring isomorphic with \mathbb{C} . Note the same for $\{x1 \mid x \in \mathbb{R}\}$ and \mathbb{R} . This is why the quaternions are considered to be an extension of the complex numbers and the reals.

EXERCISE 7.7. a) Let F be a division ring, and let λ be a fixed nonzero element of F . Prove that the map $\phi: F \rightarrow F$, defined by $\phi(x) = \lambda x \lambda^{-1}$ for all $x \in F$, is an automorphism of F .

b) Let p be a prime number. Prove that the field \mathbb{Z}_p of p elements has no automorphisms other than the identity.

EXERCISE 7.8. Let $k = \{0, 1, 2\}$ be the field of 3 elements, with addition and multiplication modulo 3. Let $F = \{a + bj \mid a, b \in k\}$, where j is a symbol.

a) Define addition and multiplication in F , using the relation $j^2 = -1$. Check that F is then a field.

b) Prove that the multiplicative group F^* of non-zero elements of F is cyclic of order 8.

c) Find a nontrivial automorphism of F .

EXERCISE 7.9. A commutative ring R with no zero divisors is called an *integral domain*. Define its *field of fractions* F and embed R in F as follows.

a) On $R \times (R - \{0\})$ introduce the relation $(a, b) \sim (c, d)$ if $ad = bc$. Show that \sim is an equivalence relation. Let $\frac{a}{b}$ denote the equivalence class of (a, b) .

b) Define addition by $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Check that this formula is not dependent on choice of representative $\frac{a}{b}$ or $\frac{c}{d}$. Show that $F = \{\frac{a}{b} \mid a \in R, b \in R - \{0\}\}$ is an abelian group under $+$.

c) Define multiplication by $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ and check that $(F, +, \cdot)$ is a field. If R is the ring of integers, which field is F (up to isomorphism).

d) Show that the mapping $R \rightarrow F$ given by $x \mapsto \frac{x}{1}$ is a ring homomorphism.

e) If $\phi: R \rightarrow F_1$ is a ring homomorphism of R into a field F_1 and ι is the map in d), show that there is a uniquely determined ring homomorphism $\alpha: F \rightarrow F_1$ such that $\phi = \alpha \circ \iota$.

EXERCISE 7.10. Define on $\mathbb{R} \times \mathbb{R}^3 = \{(x, \mathbf{v}) \mid x \in \mathbb{R}, \mathbf{v} \in \mathbb{R}^3\}$ an addition $(x, \mathbf{v}) + (y, \mathbf{w}) = (x + y, \mathbf{v} + \mathbf{w})$ and multiplication

$$(x, \mathbf{v}) \cdot (y, \mathbf{w}) = (xy - \mathbf{v} \cdot \mathbf{w}, x\mathbf{w} + y\mathbf{v} + \mathbf{v} \times \mathbf{w})$$

where we have used vector addition, dot product, cross product, and scalar multiplication familiar from vector geometry.

Let $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ denote the standard basis of units in \mathbb{R}^3 . Show that the mapping $\psi: \mathbb{H} \rightarrow \mathbb{R} \times \mathbb{R}^3$ given by $x_1\mathbf{1} + x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k} \mapsto (x_1, x_2\mathbf{i} + x_3\mathbf{j} + x_4\mathbf{k})$ is a one-to-one correspondence that is linear ($\psi(x + y) = \psi(x) + \psi(y)$ for all $x, y \in \mathbb{H}$) and multiplicative ($\psi(xy) = \psi(x)\psi(y)$). Using the fact that \mathbb{H} is a division ring, show that $\mathbb{R} \times \mathbb{R}^3$ is a division ring isomorphic to \mathbb{H} . (You should establish symbolically that ψ carries associativity, etc., over to $\mathbb{R} \times \mathbb{R}^3$. What is the principle applicable to sets with one or more binary operations?)

EXERCISE 7.11. Verify the associative law on the set $G = \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ of quaternions using formula 7.1. Show that G is a non-abelian group.

EXERCISE 7.12. a) Check that the subset

$$D = \left\{ \begin{pmatrix} \alpha & \beta \\ -\beta & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}$$

of $M_2(\mathbb{C})$ is a division ring.

b) Show that the mapping $T: \mathbb{H} \rightarrow D$ given by

$$T(x_1\mathbf{1} + x_2i + x_3j + x_4k) = \begin{pmatrix} x_1 + x_2\sqrt{-1} & x_3 + x_1\sqrt{-1} \\ -x_3 + x_4\sqrt{-1} & x_1 - x_2\sqrt{-1} \end{pmatrix}$$

is a ring isomorphism.

c) Show that $\det T(q) = \|q\|$ and $T(q^*) = \overline{T(q)}^T$ where \bar{A}^T denotes the complex transpose of matrix A .

EXERCISE 7.13. Prove that the center of \mathbb{H} is isomorphic with the field \mathbb{R} .

EXERCISE 7.14. Let F be a field. Define the ring of *polynomials* in one indeterminate $F[x]$ as follows.

a) Let $x^0, x^1, x^2, \dots, x^n, \dots$ denote the basis elements of an infinite dimensional vector space V over F . Let $F[x]$ be the set of all finite linear combinations of these denoted by $\sum_{i=0}^n a_i x^i$, if $a_n \neq 0$ and possibly one or more $a_i = 0$ ($i < n$), or 0. An element $a_0 x^0 + \dots + a_n x^n$ in $F[x]$ is called a polynomial of *degree* n . Show that $F[x]$ inherits an addition from V such that $F[x]$ is an abelian group and $\deg(f + g) = \max\{\deg(f), \deg(g)\}$ where $\deg(f)$ denotes the degree of a polynomial f .

b) Define a multiplication first on the basis elements: $x^i x^j = x^{i+j}$. Extend this multiplication to $F[x]$ distributively and letting coefficients commute past the powers of x . Show that this gives

$$\sum_{i=0}^m a_i x^i \sum_{j=0}^n b_j x^j = \sum_{k=0}^{m+n} c_k x^k$$

where $c_k = \sum_{i=0}^k a_i b_{k-i}$ ($c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0$, ...). Show that $\deg(fg) = \deg(f) + \deg(g)$ (for all $f, g \in F[x]$).

c) Show that $F[x]$ is an integral domain and identifiable via an isomorphism with the polynomial in the Laurent series ring $F((x; \text{id})) := F((x))$. Applying Exercise 7.9, its field of fractions is denoted by $F(x)$ and called the *field of rational functions*. Show that the field of fractions $F(x)$ is isomorphic with the subfield $\{fg^{-1} \mid f, g \in F[x], g \neq 0\}$ in the field $F((x))$.

EXERCISE 7.15. Use an infinite vector space with basis as in Exercise 7.14 to define the skew Laurent series ring $F((z; \sigma))$ over field F and automorphism $\sigma: F \rightarrow F$ (cf. Proposition 7.3). Prove that $F((z; \sigma))$ is a ring without zero divisors.

EXERCISE 7.16. Given a ring R , associate the set $U(R) = \{x \in R \mid \exists y \in R: xy = 1 = yx\}$. Show that $U(R)$ is a group (called the group of units of R).

EXERCISE 7.17. Let $M_n(R)$ denote the set of $n \times n$ matrices over an arbitrary ring R , and show that $M_n(R)$ is a ring.

EXERCISE 7.18. Check that congruence modulo n is an equivalence relation on \mathbb{Z} .

EXERCISE 7.19. Check the distributivity of multiplication over addition in \mathbb{Z}_n .

EXERCISE 7.20. Prove that if a and b are relatively prime, then there exists m and n such that $am + bn = 1$.

EXERCISE 7.21. Let σ be an automorphism of the division ring R , and x a nonzero number in R . Show that $\sigma(x^{-1}) = \sigma(x)^{-1}$.

Chapter 8

Projective Planes over Division Rings

In this chapter we introduce the projective plane over a division ring. This will give us many examples of projective planes aside from the ones we know already. Then we will also discuss various properties of the projective plane corresponding to properties of the division ring.

Recall from Chapter 7 that a division ring has all the properties of the real numbers except for commutativity of multiplication, ordering and completeness. Now we define the projective plane over a division ring, mimicking the analytic definition of the real projective plane (p. 15).

DEFINITION. Let R be a division ring. We define the *projective plane over R* , written $\mathbb{P}^2(R)$, as follows. A *point* of the projective plane is an equivalence class of triples $P = (x_1, x_2, x_3)$ where $x_1, x_2, x_3 \in R$ are not all zero, and where the two triples are equivalent, $(x_1, x_2, x_3) \sim (x'_1, x'_2, x'_3)$ if and only if there is an element $\lambda \in R$, $\lambda \neq 0$, such that $x'_i = x_i \lambda$ for $i = 1, 2, 3$. (Note that we multiply by λ on the *right*. It is important to keep this in mind, since the multiplication may not be commutative.)

A *line* in $\mathbb{P}^2(R)$ is the set of all points satisfying a linear equation of the form $c_1 x_1 + c_2 x_2 + c_3 x_3 = 0$ where $c_1, c_2, c_3 \in R$ are not all zero. Note that we multiply here on the left, so that this equation actually

has equivalence classes of triples instead of triples in its solution set.

Now one can check that the axioms P1-P4 are satisfied, and so $\mathbb{P}^2(R)$ is a projective plane (Exercise 8.10).

EXAMPLE 1. If $R = \mathbb{Z}_2$ is the field of two elements, then $\mathbb{P}^2(R)$ is the projective plane of seven points.

EXAMPLE 2. More generally, if $R = \mathbb{Z}_p$ for any prime number p , then $\mathbb{P}^2(R)$ is a projective plane with $p^2 + p + 1$ points. Indeed, any line has $p + 1$ points, so this follows from Exercise 2.4.

EXAMPLE 3. If $R = \mathbb{R}$ we get back the real projective plane.

THEOREM 8.1. *The plane $\mathbb{P}^2(R)$ over a division ring always satisfies Desargues' Axiom P5.*

Proof. One could argue the same way as in the proof of Theorem 3.1 if R is a field. For the general case we apply Theorem 3.2. One defines projective 3-space $\mathbb{P}^3(R)$ by taking points to be equivalence classes (x_1, x_2, x_3, x_4) , $x_i \in R$ not all zero, and where this is equivalent of $(x_1\lambda, x_2\lambda, x_3\lambda, x_4\lambda)$. Planes are defined by left linear equations, $\sum_{i=1}^4 c_i x_i = 0$, and lines as intersections of distinct planes. Now it is an exercise to check that the axioms S1-S6 are satisfied, so $\mathbb{P}^3(R)$ is a projective space (Exercise 8.7).

Then $\mathbb{P}^2(R)$ is embedded as the plane $x_4 = 0$ in this projective 3-space. and so P5 holds there by Theorem 3.2. \square

n-DIMENSIONAL PROJECTIVE GEOMETRY

Define $\mathbb{P}^n(R)$, n -dimensional projective space over an arbitrary division ring R , as the set of points (x_1, \dots, x_{n+1}) in R^{n+1} subject to the equivalence relation $(x_1, \dots, x_{n+1}) \sim (x_1, \dots, x_{n+1})\lambda = (x_1\lambda, \dots, x_{n+1}\lambda)$. n -planes or hyperplanes are the points satisfying left linear equations like $\sum_{i=1}^{n+1} c_i x_i = 0$. k -planes are sets of points satisfying simultaneously a system of $n + 1 - k$ different left linear equations.

Notice that 1-planes are points, and 2-planes may be called lines. Axioms for n -space are not hard to give: see [Seidenberg]. One can also work analytically with $\mathbb{P}^n(R)$. See [Samuel] or [Yale]. It is a relatively

easy project to generalize section all the results in the next section to $\text{Aut } \mathbb{P}^n(R)$.

8.1 The Automorphism Group of $\mathbb{P}^2(R)$

Now we will study the group $\text{Aut } \mathbb{P}^2(R)$ of automorphisms of our projective plane. It may be helpful to read this section first to see what it says for the real numbers, and secondly for what it says in the more general case of division rings.

DEFINITION. An $n \times n$ matrix $A = (a_{ij})$ of elements of R is *invertible* if there is an $n \times n$ matrix B , such that $AB = BA = I$, the identity matrix. B is called an inverse of A and denoted A^{-1} . Note that, if we are working over a field F , the invertible matrices are just the matrices with determinant $\neq 0$. Over general division rings, determinants do not make sense.

PROPOSITION 8.2. Let $A = (a_{ij})$ be an invertible 3×3 matrix of elements of R . Then the equations $x'_i = \sum_{j=1}^3 a_{ij}x_j$ for $i = 1, 2, 3$ define an automorphism T_A of $\mathbb{P}^2(R)$.

Proof. We must observe several things.

1) If we replace (x_1, x_2, x_3) by $(x_1\lambda, x_2\lambda, x_3\lambda)$, then (x'_1, x'_2, x'_3) is replaced by $(x'_1\lambda, x'_2\lambda, x'_3\lambda)$, so the mapping is well-defined. We must also check that x'_1, x'_2, x'_3 are not all zero. Indeed, in matrix notation

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix}$$

or in compact notation, $Ax = x'$. But since A has inverse A^{-1} , we can multiply on the left by A^{-1} , and get $x = A^{-1}x'$. Here we can appeal to associativity of the ring $M_n(R)$ of square matrices over R (Exercise 7.17) by letting a column vector $\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$ stand for the matrix $\begin{pmatrix} y_1 & 0 & 0 \\ y_2 & 0 & 0 \\ y_3 & 0 & 0 \end{pmatrix}$. So if the x'_i are all zero, the x_i are also all zero, which is not possible for a point of $\mathbb{P}^2(R)$. Thus T_A is a well-defined map of $\mathbb{P}^2(R)$ into $\mathbb{P}^2(R)$.

2) The expression $x = A^{-1}x'$ shows that $T_{A^{-1}}$ is the inverse mapping to T_A , hence T_A must be one-to-one and surjective.

3) Finally, we must check that T_A takes lines into lines. Indeed, let

$$(8.1) \quad c_1x_1 + c_2x_2 + c_3x_3 = 0$$

be the equation of a line. We must find a new line, such that whenever (x_1, x_2, x_3) satisfy this equation 8.1, its image (x'_1, x'_2, x'_3) lies on the new line. Let $A^{-1} = (b_{ij})$. Then we have $x_i = \sum_{j=1}^3 b_{ij}x'_j$ for each i . Thus if (x_1, x_2, x_3) satisfy 8.1, then (x'_1, x'_2, x'_3) will satisfy the equation

$$c_1 \sum_{j=1}^3 b_{1j}x'_j + c_2 \sum_{j=1}^3 b_{2j}x'_j + c_3 \sum_{j=1}^3 b_{3j}x'_j = 0$$

which is

$$\left(\sum_{i=1}^3 c_i b_{i1} \right) x'_1 + \left(\sum_{i=1}^3 c_i b_{i2} \right) x'_2 + \left(\sum_{i=1}^3 c_i b_{i3} \right) x'_3 = 0.$$

This is the equation of the required line. We have only to check that the three coefficients

$$(8.2) \quad c'_j = \sum_{i=1}^3 c_i b_{ij} \quad (j = 1, 2, 3)$$

are not all zero. But this argument is analogous to the argument in (1) above: The equation 8.2 represents the fact that

$$(c_1, c_2, c_3) \cdot A^{-1} = (c'_1, c'_2, c'_3)$$

where $(c_1, c_2, c_3) = \begin{pmatrix} c_1 & c_2 & c_3 \\ 0 & 0 & 0 \end{pmatrix}$. Multiplying by A on the right shows that the c_i can be expressed in terms of the c'_i . Hence if the c'_i were all zero, the c_i would all be zero, which contradicts the definition of line in $\mathbb{P}^2(R)$.

Hence T_A is an automorphism of $\mathbb{P}^2(R)$. \square

LEMMA 8.3. *Let A and A' be two invertible matrices. Then T_A and $T_{A'}$ have the same effect on the four points $P_1 = (1, 0, 0)$, $P_2 = (0, 1, 0)$, $P_3 = (0, 0, 1)$, and $P_4 = (1, 1, 1)$ if and only if there is a $\mu \in R$, $\mu \neq 0$, such that $A' = A\mu$.*

Proof. Clearly if there is such a μ , $T_A(P_i) = T_{A'}(P_i)$ for $i = 1, 2, 3$, and 4, by a direct computation.

Conversely, suppose $T_A = T_{A'}$. We will then study the action of T_A and $T_{A'}$ on four specific points of $\mathbb{P}^2(R)$, namely $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, and $(1, 1, 1)$, i.e. P_1 , P_2 , P_3 , and P_4 respectively. Give A and A' the usual coefficients a_{ij} and a'_{ij} , respectively. Now

$$T_A(P_1) = A \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ a_{21} \\ a_{31} \end{pmatrix}$$

and

$$T_{A'}(P_1) = A' \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a'_{11} \\ a'_{21} \\ a'_{31} \end{pmatrix}.$$

Now these two sets of coordinates are supposed to represent the same points of $\mathbb{P}^2(R)$, so there must exist a $\lambda_1 \in R$, $\lambda_1 \neq 0$, such that $a'_{11} = a_{11}\lambda_1$, $a'_{21} = a_{21}\lambda_1$, and $a'_{31} = a_{31}\lambda_1$. Similarly, applying T_A and $T_{A'}$, to the points P_2 and P_3 , we find the numbers $\lambda_2 \in R$ and $\lambda_3 \in R$, both $\neq 0$, such that

$$\begin{aligned} a'_{12} &= a_{12}\lambda_2 & a'_{13} &= a_{13}\lambda_3 \\ a'_{22} &= a_{22}\lambda_2 & a'_{23} &= a_{23}\lambda_3 \\ a'_{32} &= a_{32}\lambda_2 & a'_{33} &= a_{33}\lambda_3 \end{aligned}$$

Now apply T_A to the point P_4 . We find

$$A \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} + a_{12} + a_{13} \\ a_{21} + a_{22} + a_{23} \\ a_{31} + a_{32} + a_{33} \end{pmatrix}$$

Similarly for $T_{A'}$. Again, $T_A(P_4) = T_{A'}(P_4)$, so there is a number $\mu \neq 0$ such that $T_{A'}(P_4) = T_A(P_4)\mu$. Now using all our equations we find

$$\begin{aligned} a_{11}(\lambda_1 - \mu) + a_{12}(\lambda_2 - \mu) + a_{13}(\lambda_3 - \mu) &= 0 \\ a_{21}(\lambda_1 - \mu) + a_{22}(\lambda_2 - \mu) + a_{23}(\lambda_3 - \mu) &= 0 \\ a_{31}(\lambda_1 - \mu) + a_{32}(\lambda_2 - \mu) + a_{33}(\lambda_3 - \mu) &= 0. \end{aligned}$$

In other words, the vector $(\lambda_1 - \mu, \lambda_2 - \mu, \lambda_3 - \mu)$ is sent into $(0, 0, 0)$ under the mapping A . Hence $\lambda_1 = \lambda_2 = \lambda_3 = \mu$. (We saw this in the

proof of Proposition 8.1: an ordered triple of numbers, not all zero, cannot be sent into $(0, 0, 0)$ by \mathbf{A} . Hence $\lambda_1 - \mu = 0$, $\lambda_2 - \mu = 0$, and $\lambda_3 - \mu = 0$.)

So $\mathbf{A}' = \mathbf{A}\mu$, and we are done. \square

LEMMA 8.4. *Let $\lambda \in R$, $\lambda \neq 0$, and consider the matrix $\lambda\mathbf{I}$. Then $T_{\lambda\mathbf{I}}$ is the identity transformation of $\mathbb{P}^2(R)$ if and only if λ is in the center of R . Otherwise, $T_{\lambda\mathbf{I}}$ is the automorphism given by $(x_1, x_2, x_3) \mapsto (\sigma(x_1), \sigma(x_2), \sigma(x_3))$ where σ is the automorphism of R given by $x \mapsto \lambda x \lambda^{-1}$. I.e. σ is an inner automorphism.*

Proof. In general, $T_{\lambda\mathbf{I}}$ takes (x_1, x_2, x_3) to the point $(\lambda x_1, \lambda x_2, \lambda x_3)$. This latter point also has homogeneous coordinates $(\lambda x_1 \lambda^{-1}, \lambda x_2 \lambda^{-1}, \lambda x_3 \lambda^{-1})$, which proves the second assertion. Take $x_1 = x$, $x_2 = 1$, $x_3 = 1$. Then it is clear that $\lambda\mathbf{I}$ is the identity automorphism of $\mathbb{P}^2(R)$ if and only if $\lambda x = x \lambda$ for all x , i.e. λ is in the center of R . \square

DEFINITION. We denote by $\text{PGL}(2, R)$ the group of automorphisms of $\mathbb{P}^2(R)$ of the form $T_{\mathbf{A}}$ for some invertible 3×3 matrix \mathbf{A} . (Note that if \mathbf{B} is another invertible 3×3 matrix, then $T_{\mathbf{A}\mathbf{B}} = T_{\mathbf{A}}T_{\mathbf{B}}$. Also, $T_{\mathbf{I}} = \text{id}$ and $T_{\mathbf{A}^{-1}} = T_{\mathbf{A}}^{-1}$, so that $\text{PGL}(2, R)$ is indeed a group.)

PROPOSITION 8.5. *Let \mathbf{A} and \mathbf{A}' be invertible matrices. Then $T_{\mathbf{A}} = T_{\mathbf{A}'}$ if and only if there exists a non-zero λ in the center of R such that $\mathbf{A}' = \mathbf{A}\lambda$.*

Proof. \Leftarrow is clear. Conversely, if $T_{\mathbf{A}} = T_{\mathbf{A}'}$, then by Lemma 8.3, $\mathbf{A}' = \mathbf{A}\lambda = \mathbf{A} \cdot (\lambda\mathbf{I})$. So $T_{\mathbf{A}'} = T_{\mathbf{A} \cdot \lambda\mathbf{I}}$, whence $T_{\lambda\mathbf{I}}$ is the identity. By Lemma 8.4, λ lies in the center of R . \square

The next theorem is fundamental to projective geometry. It says the automorphisms of $\mathbb{P}^2(R)$ are transitive on complete quadrangles.

THEOREM 8.6. *Let A, B, C, D and A', B', C', D' be two quadruples of points, no 3 collinear. Then there is an element $T \in \text{PGL}(2, R)$ such that $T(A) = A'$, $T(B) = B'$, $T(C) = C'$, and $T(D) = D'$. If R is a field, T is unique.*

Proof. Let P_1, P_2, P_3, P_4 be the four points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$, and $(1, 1, 1)$ considered above. Then it will be sufficient to prove the theorem in the case $A, B, C, D = P_1, P_2, P_3, P_4$. Indeed, suppose we can send the quadruple P_1, P_2, P_3, P_4 into any other. Let ϕ send it to A, B, C, D , and let ψ send it to A', B', C', D' . Then $\psi\phi^{-1}$ sends A, B, C, D into A', B', C', D' .

Let A, B, C, D have homogeneous coordinates (a_1, a_2, a_3) , (b_1, b_2, b_3) , (c_1, c_2, c_3) , and (d_1, d_2, d_3) , respectively. Then we must find an invertible 3×3 matrix (t_{ij}) and numbers λ, μ, ν, ρ such that

$$T(P_1) = A, \text{ i.e. } a_i\lambda = t_{i1} \quad (i = 1, 2, 3)$$

$$T(P_2) = B, \text{ i.e. } b_i\mu = t_{i2} \quad (i = 1, 2, 3)$$

$$T(P_3) = C, \text{ i.e. } c_i\nu = t_{i3} \quad (i = 1, 2, 3)$$

$$T(P_4) = D, \text{ i.e. } d_i\rho = t_{i1} + t_{i2} + t_{i3} \quad (i = 1, 2, 3).$$

Clearly it will be sufficient to take $\rho = 1$, and find $\lambda, \mu, \nu \neq 0$ such that

$$a_1\lambda + b_1\mu + c_1\nu = d_1$$

$$a_2\lambda + b_2\mu + c_2\nu = d_2$$

$$a_3\lambda + b_3\mu + c_3\nu = d_3$$

LEMMA 8.7. *Let A, B, C be three points in $\mathbb{P}^2(R)$, with coordinates (a_1, a_2, a_3) , (b_1, b_2, b_3) , and (c_1, c_2, c_3) , respectively. Then A, B, C are not collinear if and only if $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$ is invertible.*

Proof of lemma. The points A, B, C are collinear if and only if there is a line, with equation say $h_1x_1 + h_2x_2 + h_3x_3 = 0$, h_i not all zero, such that this equation is satisfied by the coordinates of A, B, C . We have seen that the matrix $\mathbf{A} = (a_{ij})$ is invertible if and only if for each set of numbers $\mathbf{b} = (b_i)$, the set of linear equations corresponding to $\mathbf{A}\mathbf{x} = \mathbf{b}$ have a unique solution $\mathbf{x} = \mathbf{A}^{-1}\mathbf{b}$. It follows that \mathbf{A} is invertible if and only if for $b_i = 0$, the set of equations $\sum a_{ij}x_j = b_i$ has only a trivial solution, i.e. $\mathbf{x} = 0$ (\Leftarrow is Exercise 8.3). Now our h_i are solutions of such a set of equations. Indeed

$$(h_1, h_2, h_3) \cdot \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} = (0, 0, 0).$$

Therefore solutions h_i don't exist if and only if the matrix above is invertible.

Proof of theorem, continued. In our case, A, B, C are non-collinear, hence by the lemma, $\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}$ is invertible. Hence we can solve the equations above for λ, μ, ν not all zero. Now we claim that λ, μ, ν are all $\neq 0$. Indeed, suppose with no loss of generality that $\lambda = 0$. Then our equations say that

$$\begin{aligned} b_1\mu + c_1\nu - d_1 &= 0 \\ b_2\mu + c_2\nu - d_2 &= 0 \\ b_3\mu + c_3\nu - d_3 &= 0 \end{aligned}$$

and hence $\begin{pmatrix} b_1 & c_1 & d_1 \\ b_2 & c_2 & d_2 \\ b_3 & c_3 & d_3 \end{pmatrix}$ is non-invertible, which is impossible, by the lemma, since B, C, D are not collinear.

So we have found non-zero λ, μ, ν which satisfy the equations above. We define t_{ij} by the equations $a_i\lambda = t_{i1}$, $b_i\mu = t_{i2}$, and $c_i\nu = t_{i3}$. Then (t_{ij}) is a matrix, which is invertible (again by the lemma, since A, B, C are non-collinear!), so T , given by the matrix (t_{ij}) , is an element of $\text{PGL}(2, R)$ which sends P_1, P_2, P_3, P_4 to A, B, C, D .

For the uniqueness in the case of a field F , suppose that T and T' are two elements of $\text{PGL}(2, F)$ which accomplish our task. Then by Proposition 8.3, $T' = T\mu$ for some $\mu \in F - \{0\}$, and hence give the same element of $\text{PGL}(2, F)$. \square

Note that in general the transformation T is not unique. For example, over the quaternions \mathbb{H} there are many nontrivial inner automorphisms (Exercise 7.7); each will induce automorphisms fixing P_1, P_2, P_3 , and P_4 !

PROPOSITION 8.8. *Let ϕ be any automorphism of $\mathbb{P}^2(R)$ which leaves fixed the four points P_1, P_2, P_3, P_4 mentioned above. Then there is an automorphism $\sigma \in \text{Aut } R$, such that $\phi(x_1, x_2, x_3) = (\sigma(x_1), \sigma(x_2), \sigma(x_3))$.*

Proof. We note that ϕ must leave the line $x_3 = 0$ fixed since it contains P_2 and P_1 . We will take this line as the line at infinity, and

consider the affine plane $x_3 \neq 0: \mathbb{A} = \mathbb{P}^2(R) - \{x_3 = 0\}$. (Refer to Exercise 2.2.)

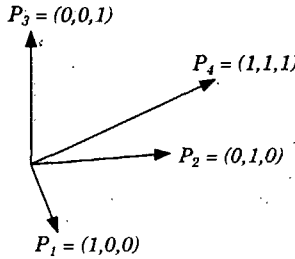


Figure 8.1. The points P_1 - P_4 of the standard quadrangle.

Our automorphism ϕ then sends \mathbb{A} into itself, and so is an automorphism of the affine plane. We will use affine coordinates $x = x_1x_3^{-1}$, $y = x_2x_3^{-1}$. Then P_1 and P_2 refer to ideal points on lines of slope 0 and ∞ , respectively, while P_3 and P_4 receive affine coordinates $(0,0)$ and $(1,1)$, respectively. Since ϕ leaves fixed P_1 and P_2 , it will send horizontal lines into horizontal lines, vertical lines into vertical lines. Since ϕ leaves fixed $(0,0)$ and $(1,1)$, it leaves fixed the x -axis and the y -axis.

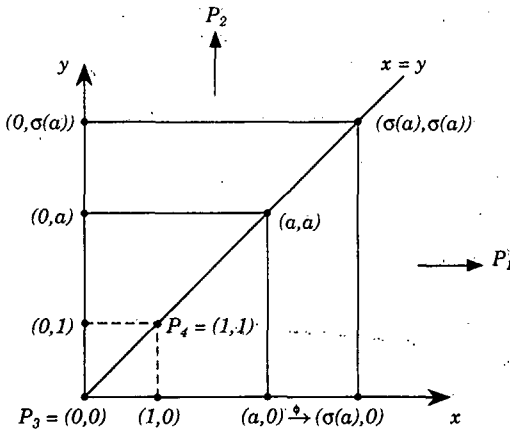


Figure 8.2. Definition of ϕ .

Let $(a, 0)$ be a point on the x -axis. Then $\phi(a, 0)$ is also on the x -axis, so it can be written as $(\sigma(a), 0)$ for a suitable element $\sigma(a) \in R$. Thus we define a mapping $\sigma: R \rightarrow R$, and we see immediately that $\sigma(0) = 0$. Also $\sigma(1) = 1$ since ϕ fixes the horizontal line $y = 0$ and vertical line $x = 1$, therefore their intersection $(1, 0)$.

The line $x = y$ is sent into itself, because P_3 and P_4 are fixed. Since vertical lines go into vertical lines, the point

$$(a, a) = (\text{line } x = y) \cap (\text{line } x = a)$$

is sent into

$$(\sigma(a), \sigma(a)) = (\text{line } x = y) \cap (\text{line } x = \sigma(a)).$$

Similarly, horizontal lines go into horizontal lines, and the y -axis goes into itself, so we deduce that $\phi(0, a) = (0, \sigma(a))$. Finally, if (a, b) is any point, we deduce by drawing lines $x = a$ and $y = b$ that $\phi(a, b) = (\sigma(a), \sigma(b))$.

Hence the action of ϕ on the affine plane is completely expressed by the mapping $\sigma: R \rightarrow R$ which we have constructed.

Of course, since ϕ is an automorphism of \mathbb{A} , it must send the x -axis onto itself in a one-to-one manner, so σ is one-to-one and onto.

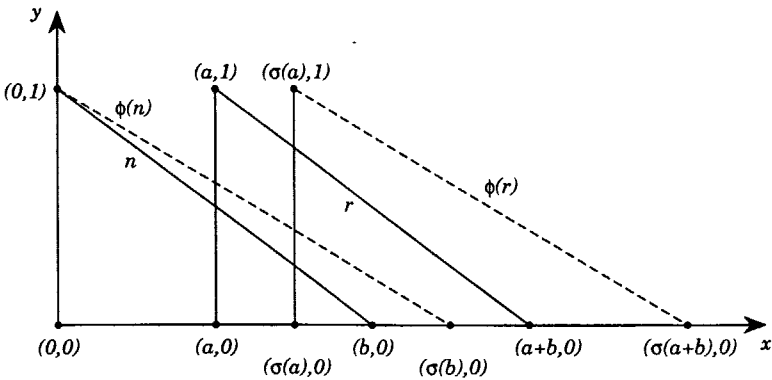


Figure 8.3. $\sigma(a) + \sigma(b) = \sigma(a + b)$.

Now we will show that σ is an automorphism of R . Let $a, b \in R - \{0\}$, and consider the points $(a, 0)$, $(b, 0)$ on the x -axis. We can construct the point $(a + b, 0)$ geometrically as follows:

- 1) Draw the line n joining $(0, 1)$ and $(b, 0)$.
- 2) Draw the line r parallel to n through $(a, 1)$.
- 3) Intersect r with the x -axis. This is the point $(a + b, 0)$ since r clearly has equation $y = -b^{-1}x + 1 + b^{-1}a$.

Now ϕ preserves joins, intersections and parallelism. Then $\phi(r) \parallel \phi(n)$, $\phi(r)$ a line through $(\sigma(a), 1)$, and $\phi(n)$ the line through $(0, 1)$ and $(\sigma(b), 0)$. Hence, intersecting $\phi(r)$ with the x -axis gives via construction the point $(\sigma(a) + \sigma(b), 0)$. On the other hand, $(a + b, 0)$ is r intersected with the x -axis, so $\phi(a + b, 0) = (\sigma(a + b), 0)$ is $\phi(r)$ intersected with the x -axis (fixed under ϕ). Hence,

$$\sigma(a) + \sigma(b) = \sigma(a + b).$$

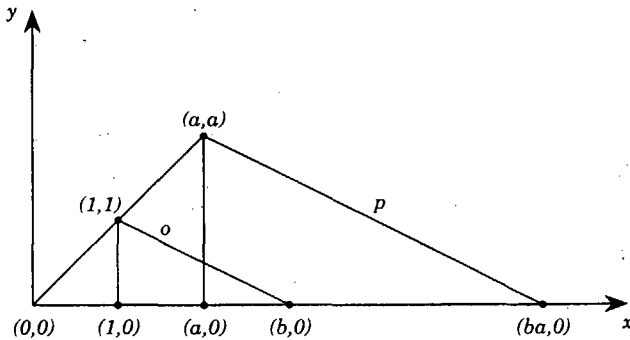


Figure 8.4. $\sigma(b)\sigma(a) = \sigma(ba)$.

By another construction, we can obtain the point $(ba, 0)$ geometrically from the point $(a, 0)$ and $(b, 0)$.

Assume $a \neq 1$ and $b \neq 1$.

- 1) Join $(1, 1)$ to $(b, 0)$, call it o .
- 2) Draw a line p parallel to o through (a, a) .
- 3) Intersect p with the x -axis. This is the point $(ba, 0)$ since p has equation $y = -(b-1)^{-1}x + (b-1)^{-1}a + a$.

ϕ leaves $(1, 1)$ fixed, so by considering $\phi(o)$ and $\phi(p)$ we can argue as before (Exercise 8.5):

$$\sigma(ba) = \sigma(b)\sigma(a).$$

Hence σ is an automorphism of the division ring R .

Now we return to the projective plane $\mathbb{P}^2(R)$, and show that the effect of ϕ on a point with homogeneous coordinates (x_1, x_2, x_3) , is to send it into $(\sigma(x_1), \sigma(x_2), \sigma(x_3))$ as claimed.

Case 1. If $x_3 = 0$, we write this point as the intersection of the line $x_3 = 0$ (which is left fixed by ϕ) and the line joining $(0, 0, 1)$ with $(x_1, x_2, 1)$. Now the latter point is in \mathbb{A} , and has affine coordinates (x_1, x_2) . Hence ϕ transforms it to $(\sigma(x_1), \sigma(x_2))$, whose homogeneous coordinates are $(\sigma(x_1), \sigma(x_2), 1)$. Therefore by intersecting the transformed lines, we find

$$\phi(x_1, x_2, 0) = (\sigma(x_1), \sigma(x_2), 0).$$

Case 2. $x_3 \neq 0$. Then the point (x_1, x_2, x_3) is in \mathbb{A} , and has affine coordinates $x = x_1x_3^{-1}$, $y = x_2x_3^{-1}$. So $\phi(x, y) = (\sigma(x), \sigma(y)) = (\sigma(x_1)\sigma(x_3)^{-1}, \sigma(x_2)\sigma(x_3)^{-1})$. (σ takes inverses to inverses by Exercise 7.5.) Therefore $\phi(x, y)$ has homogeneous coordinates $(\sigma(x_1), \sigma(x_2), \sigma(x_3))$ and we are done. \square

Since the automorphism ϕ which fixes the standard quadrangle, turns out to depend on the division ring automorphism σ , let us rename it S_σ for the next proposition and thereafter.

PROPOSITION 8.9. *The mapping $\text{Aut } R \rightarrow \mathbb{P}^2(R)$ given by $\sigma \mapsto S_\sigma$, where S_σ is described in the previous proposition, is an isomorphism of $\text{Aut } R$ onto the subgroup H of $\text{Aut } \mathbb{P}^2(R)$ consisting of those automorphisms which leave P_1, P_2, P_3, P_4 fixed.*

Proof. It is onto by the previous proposition. To see it is one-to-one, let σ and $\sigma' \in \text{Aut } R$ and apply $S_\sigma, S_{\sigma'}$ to $(x, 1, 0)$. Suppose $(\sigma(x), 1, 0)$ is the same point as $(\sigma'(x), 1, 0)$, then $\sigma(x) = \sigma'(x)$, and $\sigma = \sigma'$. Clearly it preserves the group law. \square

GENERATORS. Recall that a subset A_i of a group G is said to generate the subgroup H if H is the smallest subgroup containing A_i . Then H consists only of products of powers of elements in A_i (Exercise 4.15). In particular, two subgroups H_1, H_2 are said to generate G if their set-theoretic union $H_1 \cup H_2$ generates G .

THEOREM 8.10. *The two subgroups $\text{PGL}(2, R)$ and H generate $\text{Aut } \mathbb{P}^2(R)$. The intersection K of $\text{PGL}(2, R)$ and H is isomorphic to the group of inner automorphisms of R , $\text{InAut } R$.*

Proof. Given an element $T \in \text{Aut } \mathbb{P}^2(R)$, we can find an element $T_A \in \text{PGL}(2, R)$ such that $T_A(P_i) = T(P_i)$ for $i = 1, 2, 3, 4$ by the Fundamental Theorem. Then $T_{A^{-1}} \circ T$ fixes P_i so there exists $S_\sigma \in H$ such that $T_{A^{-1}} \circ T = S_\sigma$. Then $T = T_A \circ S_\sigma$ which shows (most strongly) that the subgroups H and $\text{PGL}(2, R)$ generate $\text{Aut } \mathbb{P}^2(R)$.

An element $T \in \text{PGL}(2, R) \cap H$ fixes the points P_1, \dots, P_4 and is induced by an invertible matrix A : i.e. $T = T_A$. By Lemma 8.3, $A = \lambda I$ for some $\lambda \in R$ and, by Lemma 8.4, $T = S_\sigma$ where σ is the inner automorphism given by $\sigma(x) = \lambda x \lambda^{-1}$. \square

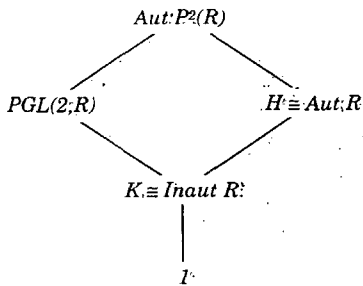


Figure 8.5. Lattice diagram of key subgroups in $\text{Aut } \mathbb{P}^2(R)$. This is presumably a theorem of von Staudt and the Basque Ancochea.

We are now in a position to determine the automorphism group of the real projective plane.

PROPOSITION 8.11. *The identity automorphism is the only automorphism of the field of real numbers.*

Proof. Let σ be an automorphism of the real numbers. We proceed in several steps.

1) $\sigma(1) = 1$ and $\sigma(a + b) = \sigma(a) + \sigma(b)$. Hence, by induction, we can prove that $\sigma(n) = n$ for any positive integer n .

2) $n + (-n) = 0$, so $\sigma(n) + \sigma(-n) = 0$, so $\sigma(-n) = -n$. Hence σ leaves all the integers fixed.

3) If $b \neq 0$, then $\sigma(a/b) = \sigma(a)/\sigma(b)$. Hence σ leaves all the rational numbers fixed.

4) If $x \in \mathbb{R}$, then $x > 0$ if and only if there is an $a \neq 0$ such that $x = a^2$. Then $\sigma(x) = \sigma(a)^2$, so $x > 0 \implies \sigma(x) > 0$: Therefore $x < y \implies \sigma(x) < \sigma(y)$: σ is order-preserving.

5) Let $x \in \mathbb{R} - \mathbb{Q}$ and suppose $\sigma(x) \neq x$, so either $x < \sigma(x)$ or $x > \sigma(x)$. Suppose $x < \sigma(x)$. By the Archimedean principle there exists a rational number r such that $x < r < \sigma(x)$. Then $r - x > 0$, which implies that $\sigma(r) - \sigma(x) = r - \sigma(x) > 0$ by 4), or $r > \sigma(x)$, a contradiction of the choice of r . Assuming $\sigma(x) < x$ leads to a similar contradiction. Hence $\sigma(x) = x$.

Thus σ is the identity. \square

THEOREM 8.12. $\text{PGL}(2, \mathbb{R}) = \text{Aut } \mathbb{P}^2(\mathbb{R})$

Proof. By Proposition 8.11, $H = \{1\}$. By Theorem 8.10 the subgroup $\text{PGL}(2, \mathbb{R})$ is then the whole automorphism group. \square

THE FUNDAMENTAL THEOREM IN TWO DIMENSIONS

As a consequence of Theorems 8.6 and 8.12 we have the following important theorem for the real projective plane:

THEOREM 8.13. *Let $ABCD$ and $PQRS$ be two complete quadrangles in $\mathbb{P}^2(\mathbb{R})$. Then there exists a unique automorphism of $\mathbb{P}^2(\mathbb{R})$ such that $T(A) = P$, $T(B) = Q$, $T(C) = R$ and $T(D) = S$.*

You will show in Exercise 8.9 that this theorem is not true in $\mathbb{P}^2(\mathbb{C})$. The problem with \mathbb{C} is that it possesses a nontrivial field automorphism, given by $z \mapsto \bar{z}$.

The Fundamental Theorems of chapters 5 and 8 are generalized to n -dimensional real projective spaces in more advanced textbooks (such as [Samuel]) as follows:

Given two ordered sets, X_1 and X_2 , of $n + 2$ points of $\mathbb{P}^n(\mathbb{R})$ in general position¹ there is a unique automorphism of $\mathbb{P}^n(\mathbb{R})$ sending X_1 into X_2 .

8.2 The Algebraic Meaning of Axioms P6 and P7

Now we obtain precise answers for when the axioms P6 and P7 hold in a projective plane $\mathbb{P}^2(R)$.

THEOREM 8.14. *Fano's Axiom P6 holds in $\mathbb{P}^2(R)$ if and only if the characteristic of R is not 2.*

Proof. Using an automorphism of $\mathbb{P}^2(R)$, we reduce to the question of whether the diagonal points of the standard quadrangle $P_1P_2P_3P_4$, $(1, 1, 0)$, $(1, 0, 1)$, and $(0, 1, 1)$, are collinear (cf. Proposition 5.3). Since R may not be commutative, we may not use determinants, but must give a hands-on proof.

Suppose they are collinear. Then they all satisfy an equation $c_1x_1 + c_2x_2 + c_3x_3 = 0$, with the c_i not all zero. Hence $c_1 + c_2 = 0$, $c_1 + c_3 = 0$, and $c_2 + c_3 = 0$. Thus $c_1 = -c_2$, $c_1 = -c_3$, $c_2 = -c_3$, so $2c_2 = 0$. So either $c_2 = 0$, in which case $c_3 = 0$, $c_1 = 0$, a contradiction, or $2 = 0$, in which case the characteristic of R is 2.

Now suppose the characteristic of R is 2. Then $(1, 1, 0)$, $(1, 0, 1)$, and $(0, 1, 1)$ satisfy the equation $x_1 + x_2 + x_3 = 0$ of a projective line. \square

¹No $n + 1$ are co- $(n - 1)$ -planar.

THEOREM 8.15 (HILBERT). *The Fundamental Theorem P7 holds in the projective plane $\mathbb{P}^2(R)$ over a division ring R if and only if R is commutative.*

Proof. First let us suppose that P7 holds. We take $x_3 = 0$ to be the line at infinity, and represent an element $a \in R$ as the point $(a, 0)$ on the x -axis. If $(a, 0)$ and $(b, 0)$ are two points, we construct the product of a and **b** as in the proof of Proposition 8.8, then reverse the order, and apply Pappus' Theorem.

Suppose with no loss of generality that $a \neq 0, 1$ and $b \neq 0, 1$. By inspection, one finds that the equation of the line joining $(1, 1)$ and $(b, 0)$ is $x + (b - 1)y = b$. Hence the equation of the line parallel to this one, through (a, a) is $x + (b - 1)y = ba$, so that the point we have constructed is $(ba, 0)$.

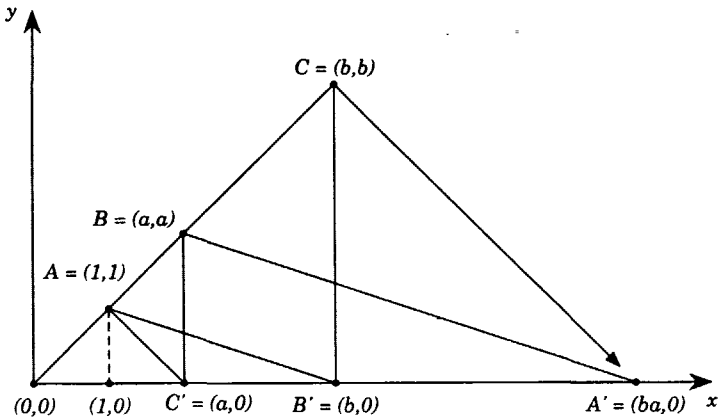


Figure 8.6. Geometric construction of multiplication.

To get the product in the other order, we reverse the process, by drawing the line through $(1, 1)$ and $(a, 0)$, and the line parallel to this through (b, b) . This line has equation $x + (a - 1)y = ab$. Refer to the point labels above! $AB' \parallel BA'$ and $BC' \parallel B'C$. Now the affine version of Pappus' Theorem implies that $AC' \parallel A'C$ (why?). Whence $A'C$ has equation $x + (a - 1)y = ab$. Then $A' = (ba, 0)$ satisfies this equation, whence $ab = ba$, and R is commutative.

Before proving the converse, we give a lemma.

LEMMA 8.16. *Let ℓ, A, B, C , and ℓ', A', B', C' be two sets, each consisting of a line, and three non-collinear points, not on the line, in $\mathbb{P}^2(R)$. Then there is an automorphism ϕ of $\mathbb{P}^2(R)$ such that $\phi(\ell) = \ell'$, and $\phi(A) = A', \phi(B) = B', \phi(C) = C'$.*

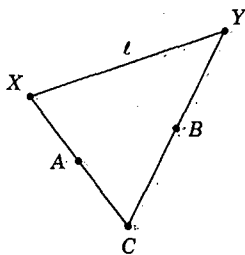


Figure 8.7.

Proof. Let $X = \ell.AC$ and $Y = \ell.BC$, and define similarly $X' = \ell'.A'C'$, $Y' = \ell'.B'C'$, then A, B, X, Y are four points, no three collinear, and similarly for A', B', X', Y' , so by Theorem 8.6 there is an automorphism ϕ of $\mathbb{P}^2(R)$ sending A, B, X, Y into A', B', X', Y' . Then clearly ϕ sends ℓ into ℓ' and C into C' .

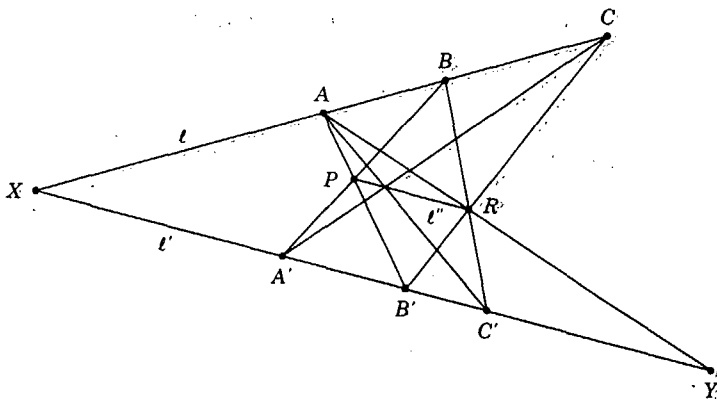


Figure 8.8.

Proof of theorem, continued. Now assume we have a field F . It will suffice to prove that Pappus' Theorem holds in $\mathbb{P}^2(F)$. Indeed, Pappus' Theorem implies the Fundamental Theorem (P7) as we saw in Exercises 6.14–6.16.

With the usual notation let $P = AB'.A'B$, $R = BC'.B'C$, and let ℓ'' be the line PR . We may assume that $X = \ell.\ell'$ does not lie on ℓ'' . (If it did, take a different pair P, Q or Q, R . If all these three pairs lie on lines through X , then P, Q, R are already collinear, and there is nothing to prove.) Let $Y = AR.\ell'$. Then Y is not on ℓ'' , and A, X, Y are non-collinear. Hence by the lemma, we can find an automorphism ϕ of $\mathbb{P}^2(F)$ taking ℓ'' to the line $x_3 = 0$, and taking A, X, Y to the points $(1, 1)$, $(0, 0)$, $(1, 0)$, respectively.

Then we have the situation of Figure 8.6 again (why are BC' and CB' vertical lines?), where we wish to prove $AC' \parallel A'C$. But this follows from the commutativity of F . \square

8.3 Independence of Axioms

We are now in a position to show that among the axioms P5, P6, P7, the only implication is $P7 \implies P5$ (Theorem 6.3). We prove this by giving examples of projective planes which have all relevant combinations of axioms holding or not.

EXPLANATIONS

- 1) The projective plane of seven points π_7 has P5, not P6, P7.
- 2) The real projective plane $\mathbb{P}^2(\mathbb{R})$ has P5, P6, P7.
- 3) The Moulton plane has not P5, P6 (Exercise 6.6), not P7.
- 4) Let \mathbb{H} be the division ring of quaternions. Then $\mathbb{P}^2(\mathbb{H})$ has P5, P6, not P7 (because $\text{char. } \mathbb{H} = 0 \implies P6$, and \mathbb{H} noncommutative \implies not P7).
- 5) Let K be a noncommutative division ring of characteristic 2. Then $\mathbb{P}^2(K)$ has P5, not P6, P7.

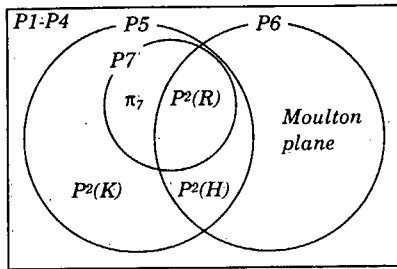


Figure 8.9: Projective planes and axioms P5–P7.

Notice a couple of things from the diagram. Axioms P5 and P6 are independent: this means that neither of the implications $P5 \implies P6$ or $P6 \implies P5$ are true. Axioms P6 and P7 are independent as well. There is an example of a projective plane that is neither Fano nor Desarguesian: it is called the free projective plane on the π_7 configuration with one extra point (see [Hartshorne, p. 17–19]).

EXERCISES

EXERCISE 8.1. In the real projective plane, we know that there is an automorphism which will send any four points, no three collinear, into any four points, no three collinear. Find the coefficients a_{ij} of an automorphism with equations

$$x'_i = a_{i1}x_1 + a_{i2}x_2 + a_{i3}x_3 \quad i = 1, 2, 3,$$

which sends the points $A = (0, 0, 1)$, $B = (0, 1, 0)$, $C = (1, 0, 0)$, $D = (1, 1, 1)$ into $A' = (1, 0, 0)$, $B' = (0, 1, 1)$, $C' = (0, 0, 1)$, $D' = (1, 2, 3)$, respectively.

EXERCISE 8.2: a) Let R be a division ring. Show that the Cartesian product R^2 with lines of form $\{(x, y) \mid y = mx + b\}$ and $\{(x, y) \mid x = a\}$ (for each $a, m, b \in R$) is an affine plane we denote by $A^2(R)$.

b) Complete $A^2(A)$ to obtain a projective plane S .

c) Adapt Proposition 2.2 and its proof to show that $\mathbb{P}^2(R)$ is the projective plane S .

Hint. Why does a collinearity-preserving one-to-one correspondence (a *collineation*) force one geometry to be a projective plane if the other is so?

EXERCISE 8.3. Let R be a division ring and $A \in M_n(R)$. Let \mathbf{x} denote the $n \times n$ matrix

$$\begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & & & \\ x_n & 0 & \cdots & 0 \end{pmatrix}.$$

Suppose that $A\mathbf{x} = \mathbf{0} \implies \mathbf{x} = \mathbf{0}$ where $\mathbf{0}$ denotes the zero $n \times n$ matrix. Show that A is invertible.

EXERCISE 8.4. Let σ be an automorphism of a division ring R . Check that the mapping $S_\sigma: \mathbb{P}^2(R) \rightarrow \mathbb{P}^2(R)$ defined by $S_\sigma: (x_1, x_2, x_3) \mapsto (\sigma(x_1), \sigma(x_2), \sigma(x_3))$ is an automorphism of projective planes.

EXERCISE 8.5. Provide the details in the proof that $\sigma(ba) = \sigma(b)\sigma(a)$ on p. 103.

EXERCISE 8.6. Complete the details of $\mathbb{P}^2(F) \implies$ Pappus' Theorem in Hilbert's Theorem.

EXERCISE 8.7. Prove that $\mathbb{P}^3(R)$ as defined on page 94 is a projective 3-space, i.e. satisfies S1–S6.

EXERCISE 8.8. If F is a field, re-do Exercise 5.2 in the projective plane $\mathbb{P}^2(F)$. You will now have defined cross ratio for Pappian planes.

EXERCISE 8.9. In $\mathbb{P}^2(\mathbb{C})$ consider the standard quadrangle $P_1P_2P_3P_4$. Find two automorphisms of the projective plane $\mathbb{P}^2(\mathbb{C})$ fixing the standard quadrangle (sending $P_i \mapsto P_i$, $i = 1, 2, 3, 4$). Compare with Theorem 8.14.

EXERCISE 8.10. Prove that axioms P1–P4 are satisfied in $\mathbb{P}^2(\mathbb{R})$, the real projective plane defined by homogeneous coordinates.

Chapter 9

Introduction of Coordinates in a Projective Plane

In this chapter we ask the question, when is a projective plane π isomorphic to a projective plane of the form $\mathbb{P}^2(R)$, for some division ring R ? Stated in other words, given π can we find a division ring R , and assign homogeneous coordinates (x_1, x_2, x_3) , $x_i \in R$, to points of π , such that the lines are given by linear equations?

A necessary condition for this to be possible is that π should satisfy Desargues' Axiom, P5, since we have seen that $\mathbb{P}^2(R)$ always satisfies P5 (Theorem 8.1). And in fact we will see that Desargues' Axiom is a sufficient condition that π is coordinatizable on the basis of a division ring.

We will begin with a simpler problem, namely the introduction of coordinates in an affine plane \mathbb{A} . One approach to this problem¹ would be the following: Choose three non-collinear points in \mathbb{A} , and call them $(1, 0)$, $(0, 0)$, $(0, 1)$. Let ℓ be the line through $(0, 0)$ and $(1, 0)$. Now take R to be the set of points on ℓ , and define addition and multiplication in R via the geometrical constructions given in the proof of Proposition 8.8. Then one would have to verify that R is a division ring, i.e. prove that addition is commutative and associative, that multiplication is associative and distributive, etc. The proofs involve some rather messy

¹done in [Seidenberg], chapter 3.

diagrams. Finally one coordinatizes the plane using these coordinates on ℓ , and prove that lines are given by linear equations.

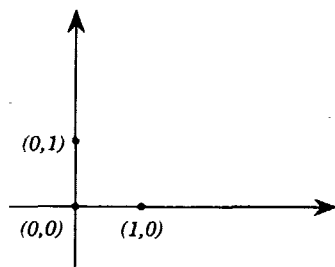


Figure 9.1. One method of coordinatizing.

However, we will use slightly more high-powered techniques, in the hope that our work becomes less onerous. Recall our work with central dilatations and translations in chapter 1: we will begin by studying the group theory of dilatations and what implications Desargues' Theorem has.

Let A be an affine plane. Recall that a dilatation of A is an automorphism sending each line onto a parallel line. A dilatation different from the identity map on A could have either 0 or 1 fixed point (Proposition 1.6): if it has no fixed points, it is called a translation, if it has one fixed point, a central dilatation. However, the identity is considered a translation for practical reasons.

We have proved in chapter 1 that the set of dilatations, as well as the subset of translations, is closed under composition of maps, contains all inverses, and possesses the identity element, or mapping. The next two propositions are just re-statements of Proposition 1.5 and 1.9 in group-theoretic terms — with one group-theoretic definition intervening.

PROPOSITION 9.1. *The set of dilatations, $\text{Dil } A$, is a group under composition. (And $\text{Dil } A$ is a subgroup of $\text{Aut } A$.)*

DEFINITION. Let G be a group. A subgroup N is said to be *normal* if

$$xNx^{-1} \subseteq N \quad (\forall x \in G),$$

i.e. $x \in G$ and $y \in N$ implies $xyx^{-1} \in N$.

The kernel of a homomorphism is a normal subgroup (Exercise 9.1). Every subgroup of an abelian group is normal. A normal subgroup N of any group G has equal right and left cosets, and the set of cosets gets a natural group structure (Exercise 9.2)

PROPOSITION 9.2. *The set of translations, $\text{Tran } \mathbb{A}$, is a normal subgroup of $\text{Dil } \mathbb{A}$.*

9.1 The Major and Minor Desargues' Axioms

Now we come to the question of existence of translations and dilations, and for this we will need Desargues' Axiom. In fact, we will find that these two existence problems are equivalent to two affine forms of Desargues' Axiom. In this we see yet another example where an axiom about some configuration is equivalent to a geometric property of the plane. Desargues' Axiom is equivalent to saying that our geometry has enough automorphisms in a sense which will become clear from the theorems.

- A4. (THE MINOR DESARGUES' AXIOM)** Let ℓ, m, n be three distinct parallel lines. Let $A, A' \in \ell$, $B, B' \in m$, and $C, C' \in n$. Assume $AB \parallel A'B'$ and $AC \parallel A'C'$. Then $BC \parallel B'C'$.

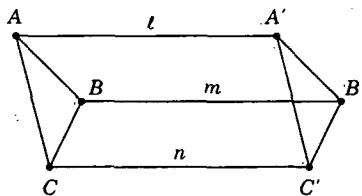


Figure 9.2. Two triangles in the affine plane that are perspective from an ideal point.

REMARK. If our affine plane \mathbb{A} is contained in a projective plane π , then A4 follows from P5 in π . Indeed, ℓ, m, n meet in a point O on the line at infinity ℓ_∞ . Our hypotheses state that $P = AB.A'B' \in \ell_\infty$, and $Q = AC.A'C' \in \ell_\infty$. So P5 says that $R = BC.B'C' \in \ell_\infty$, i.e. $BC \parallel B'C'$ in \mathbb{A} .

THEOREM 9.3. *Let \mathbb{A} be an affine plane. Then the following statements are equivalent:*

- i) *The axiom A4 holds in \mathbb{A} .*
- ii) *Given any points $P, P' \in \mathbb{A}$, there exists a unique translation τ such that $\tau(P) = P'$.*

Proof. i) \implies ii). We assume A4. If $P = P'$, then the identity is the only translation taking P to P' , so there is nothing to prove.

Now suppose $P \neq P'$. We will set out to construct a translation τ sending P to P' .

Step 1. For any pair of distinct points X and X' in \mathbb{A} , we define a translation $\tau_{XX'}$ of $\mathbb{A} - \ell$, where ℓ is the line XX' , as follows: for $Y \notin \ell$, Y' is the fourth corner of the parallelogram on X, X', Y , and we set $\tau_{XX'}(Y) = Y'$.

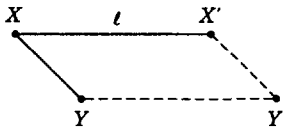


Figure 9.3. Parallelogram construction of Y' .

Step 2. Consider the effect of two parallel transformations $\tau_{PP'}$ and $\tau_{QQ'}$. Suppose $Q \notin PP'$. If $\tau_{PP'}(Q) = Q'$, then for any $R \notin PP'$, and $R \notin QQ'$, we have $\tau_{PP'}(R) = \tau_{QQ'}(R)$. Indeed, define $R' = \tau_{PP'}(R)$. Then by A4, $QR \parallel Q'R'$, so by the parallelogram construction $R' = \tau_{QQ'}(R)$.

Step 3. Starting with our two distinct points, P and P' and $Q \notin PP'$, take $Q' = \tau_{PP'}(Q)$. We can now define τ to be $\tau_{PP'}$ or $\tau_{QQ'}$, whichever happens to be defined at a given point, since we have seen that they agree where they are both defined.

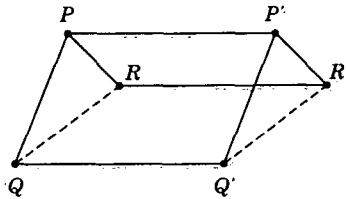


Figure 9.4.

Step 4. Note that if R is any point, and $\tau(R) = R'$, then $\tau = \tau_{RR'}$ whenever they are both defined. This follows as before.

Step 5. Clearly τ is one-to-one and onto (Exercise 9.3). If X, Y, Z are collinear points and sent into X', Y', Z' by τ , then $Y' = \tau_{XX'}(Y)$ and $Z' = \tau_{XX'}(Z)$. So it follows immediately from the definition of $\tau_{XX'}$ that X', Y', Z' are collinear. Hence τ is an automorphism of \mathbb{A} . One sees immediately from the construction that it is a dilatation with no fixed points, hence is a translation, and it takes P to P' .

The uniqueness of τ : if τ' is any translation sending P to P' , then $\tau'\tau^{-1}$ has a fixed point and is the identity. So $\tau = \tau'$.

(ii) \implies (i). We assume the existence of translations, and must deduce A4. Suppose we are given $\ell, m, n, A, A', B, B', C, C'$, as in the statement of A4. Let τ be a translation taking A into A' . Then $\tau(B) = B'$ since $AB \parallel A'B'$ and $AA' \parallel BB'$ (Exercise 1.11). Similarly $\tau(C) = C'$. Hence $BC \parallel B'C'$ since τ is a dilatation. \square

PROPOSITION 9.4. (Assuming A4) *Tran \mathbb{A} is an abelian group.*

Proof. Let τ, τ' be translations. We must show that $\tau\tau' = \tau'\tau$.

Case 1. τ and τ' translate in different directions. Let P be a point. Let $\tau(P) = P', \tau'(P) = Q$. We are assuming $P, P',$ and Q are not collinear. Then $\tau(Q) = \tau\tau'(P)$ and $\tau'(P') = \tau'\tau(P)$ are both found as the fourth vertex of the parallelogram on P, P', Q , hence are equal, so $\tau\tau' = \tau'\tau$. (So far we have not used Axiom A4.)

Case 2. τ and τ' are in the same direction. By Theorem 9.3 there exists a translation σ in a different direction (Axiom A3 ensures that there is another direction). Then

$$\tau\tau' = \tau(\tau'\sigma)\sigma^{-1} = (\tau'\sigma)\tau\sigma^{-1} = \tau'(\sigma\tau)\sigma^{-1}$$

by an application of case 1, since τ and $\tau'\sigma$ are in different directions. Then since τ and σ are in different directions we may transpose the symbols within parentheses, so

$$\tau\tau' = \tau'\tau\sigma\sigma^{-1} = \tau'\tau. \quad \square$$

DEFINITION. We say a group G is the *semi-direct product* of two subgroups H and K , and write $G = H \rtimes K$, if

SD1. H is a normal subgroup of G .

SD2. $H \cap K = \{1\}$.

SD3. H and K together generate G .

PROPOSITION 9.5. $G = H \rtimes K \implies$ that every element $g \in G$ can be written uniquely as a product $g = hk$, $h \in H$, $k \in K$.

Proof. Note that $hkh_1k_1 = h(kh_1k^{-1})kk_1$ is of the form $h'k'$ ($h \in H, k' \in K$) since H is a normal subgroup of G . Any element in G may be written as a product of elements from H and K by Axiom SD3, which can be thus put in the form $h'k'$.

Uniqueness follows from the observation: $hk = h_1k_1 \implies h_1^{-1}h = k_1k^{-1} \implies h_1^{-1}h = 1 = k_1k^{-1}$ by SD2, so $h = h_1$ and $k = k_1$. \square

DEFINITION. Let O be a point in \mathbb{A} , and define $\text{Dil}_O(\mathbb{A})$ to be the subset of $\text{Dil } \mathbb{A}$ consisting of those dilatations ϕ such that $\phi(O) = O$. It is trivial to see that $\text{Dil}_O(\mathbb{A})$, the set of central dilatations fixing O , is a group.

PROPOSITION 9.6. (Assuming A4) $\text{Dil } \mathbb{A}$ is the semi-direct product of $\text{Tran } \mathbb{A}$ and $\text{Dil}_O(\mathbb{A})$.

Proof. We agree that $\text{Tran } \mathbb{A}$ and $\text{Dil}_O(\mathbb{A})$ are subgroups of the group $\text{Dil } \mathbb{A}$. We need to check the three axioms SD1–SD3.

- 1) We have seen that $\text{Tran } \mathbb{A}$ is a normal subgroup of $\text{Dil } \mathbb{A}$.
- 2) If $\tau \in \text{Tran } \mathbb{A} \cap \text{Dil}_O(\mathbb{A})$, then τ has the fixed point O and must be the identity.

3) Let $\phi \in \text{Dil } \mathbb{A}$. Let Q denote $\phi(O)$. By Theorem 9.3 there is a translation τ such that $\tau(O) = Q$. Then $\tau^{-1}\phi \in \text{Dil}_O(\mathbb{A})$, so $\phi = \tau(\tau^{-1}\phi)$ shows that $\text{Tran } \mathbb{A}$ and $\text{Dil}_O(\mathbb{A})$ generate $\text{Dil } \mathbb{A}$. \square

A5. (THE MAJOR DESARGUES' AXIOM). Let O, A, B, C, A', B', C' be distinct points in the affine plane \mathbb{A} , and assume that O, A, A' are collinear, O, B, B' are collinear, O, C, C' are collinear, $AB \parallel A'B'$, and $AC \parallel A'C'$. Then $BC \parallel B'C'$.

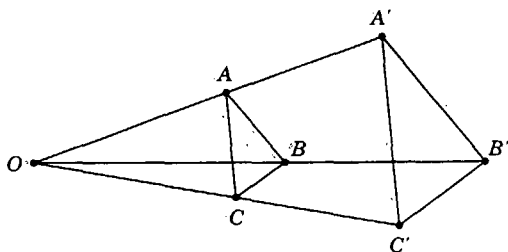


Figure 9.5. Major Desargues' Axiom.

Note that this statement follows from P5, if \mathbb{A} is embedded in a projective plane π .

THEOREM 9.7. *The following two statements are equivalent in the affine plane \mathbb{A} .*

- i) *The axiom A5 holds in \mathbb{A} .*
- ii) *Given any three points O, P, P' , with $P \neq O$, $P' \neq O$, and O, P, P' collinear, there exists a unique dilatation σ of \mathbb{A} , such that $\sigma(O) = O$ and $\sigma(P) = P'$.*

Proof. The proof is entirely analogous to the proof of Theorem 9.3, so the details will be left to the reader. Here is an outline:

i) \implies ii). Given O, P, P' , as above, define a transformation $\phi_{O, P, P'}$, for points Q not on the line ℓ containing O, P, P' as follows:

$\phi_{O,P,P'}(Q) = Q'$, where Q' is the intersection of the line OQ with the line through P , parallel to PQ .

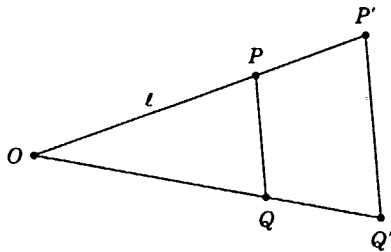


Figure 9.6. Dilatation.

Now, if $\phi_{O,P,P'}(Q) = Q'$, one proves using A5 that $\phi_{O,P,P'}$ agrees with $\phi_{O,Q,Q'}$ (defined similarly) whenever both are defined. Hence one can define σ by

$$\sigma(X) = \begin{cases} \phi_{O,P,P'}(X) & \text{if } X \in OP \\ \phi_{O,Q,Q'} & \text{if } X \in OQ. \end{cases}$$

Then $\sigma(O) = O$ and σ is well-defined everywhere. Next show that if $\sigma(R) = R'$, $R \neq O$, then $\sigma = \phi_{O,R,R'}$, wherever both maps are defined. Now clearly σ is one-to-one and onto. One can show easily that it takes lines into lines, so is an automorphism, and that $XY \parallel \sigma(X)\sigma(Y)$ for any X, Y , so σ is a dilatation. The uniqueness follows from Corollary 1.7.

ii) \implies i). Let O, A, B, C, A', B', C' be given satisfying the hypothesis of A5. Let σ be a dilatation which leaves O fixed and sends A into A' . Then by the hypotheses, $\sigma(B) = B'$, and $\sigma(C) = C'$. It follows from the fact that σ is a dilatation that $BC \parallel B'C'$. \square

We make a little diversion into the relationship of axioms A4 and A5 with the next proposition.

PROPOSITION 9.8. $A5 \implies A4$.

Proof. Indeed, let us assume we have an affine plane \mathbb{A} satisfying A5. Let P, P' be two points. We will construct a translation sending

P into P' , which by Theorem 9.3 shows that A4 holds, since P, P' are arbitrary. If $P = P'$, we can take the identity, so assume from the start that $P \neq P'$.

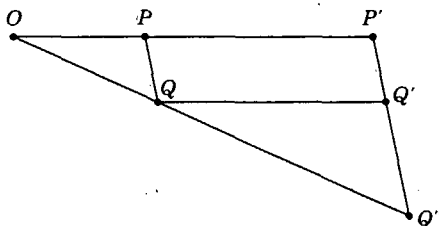


Figure 9.7. A5 \implies A4.

Let Q be a point not on PP' , and let Q' be the fourth vertex of the parallelogram on P, P', Q . Let O be a point on PP' , not equal to P or P' . Let σ_1 be a dilatation which leaves O fixed, and sends P to P' (which exists by Theorem 9.7). Let $\sigma_1(Q) = Q''$. Then P', Q', Q'' are collinear. Again, by Theorem 9.7 there exists a dilatation σ_2 leaving P' fixed, and sending Q'' to Q' .

Now consider $\tau = \sigma_2\sigma_1$. Being a product of dilatations, it is itself a dilatation. One sees easily that $\tau(P) = P'$ and $\tau(Q) = Q'$. Now any fixed point of τ must lie on PP' and on QQ' (because if X is a fixed point $XP \parallel XP' \implies X, P, P'$ collinear, and similarly for Q). But $PP' \not\parallel QQ'$, so τ has no fixed points. Hence τ is a translation sending P into P' . \square

REMARK. A projective plane is called a *translation plane* if, upon removing any line, the resulting affine plane satisfies the Desargues' Axiom!minor. Translation planes have been an active area of research in recent memory.

9.2 Division Ring Number Lines

Now we come to the construction!of coordinates in an affine plane A satisfying axioms A4 and A5. Our program is to construct the following objects:

- 1) a division ring R ;
- 2) coordinates for the points of \mathbb{A} so that \mathbb{A} is in one-to-one correspondence with the set of ordered pairs of elements of R ;
- 3) equations for an arbitrary translation and an arbitrary dilatation of \mathbb{A} in terms of coordinates;
- 4) linear equations for the lines in \mathbb{A} .

This will prove that \mathbb{A} is isomorphic to the affine plane $\mathbb{A}^2(R)$ (with (3) a convenient bonus).

In the course of these constructions, there will be about a hundred details to verify, so we will not attempt to do them all, but will give indications, and leave the trivial verifications to the reader.

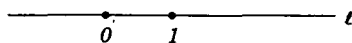


Figure 9.8. The number line.

Fix a line ℓ in \mathbb{A} , and fix two points on ℓ , call them 0 and 1. Now let R be the set of points of ℓ .

Let $a \in R$, (i.e. if a is a point of ℓ). By A4 and Theorem 9.3, there is a unique translation that takes 0 into a . Similarly, using A5 and assuming $a \neq 0$, let σ_a be the unique dilatation of \mathbb{A} which leaves 0 fixed, and sends 1 into a .

Now we define addition and multiplication in R as follows. If $a, b \in R$, define

$$(9.1) \quad a + b = \tau_a \tau_b(0) = \tau_a(b).$$

Since the translations form an abelian group, we see immediately that addition is associative and commutative:

$$\begin{aligned} (a + b) + c &= a + (b + c) \\ a + b &= b + a. \end{aligned}$$

Since $\tau_0 = \text{id}$ we see that 0 is the identity element. Let $-a = \tau_a^{-1}(0)$; this is clearly the inverse of a . Thus R is an abelian group under addition.

Translations are equal if they agree on one point, so

$$(9.2) \quad \tau_{a+b} = \tau_a \tau_b \quad \text{for all } a, b \in R.$$

Now we define multiplication as follows: first, 0 times anything is 0. Second, if $a, b \in R$, $b \neq 0$, we define

$$(9.3) \quad ab = \sigma_b(a) = \sigma_b \sigma_a(1).$$

Now since the dilatations form a group, we see immediately that

$$(ab)c = a(bc),$$

that $a \cdot 1 = 1 \cdot a = a$ for all a , and that $\sigma_a^{-1}(1) = a^{-1}$ is a multiplicative inverse. Therefore the non-zero elements of R form a group under multiplication. Furthermore, we have the formulae (for $b \neq 0$)

$$(9.4) \quad \tau_{ab} = \sigma_b \tau_a \sigma_b^{-1}$$

$$(9.5) \quad \sigma_{ab} = \sigma_b \sigma_a,$$

the top equation follows by checking it on 0; the bottom on 0 and 1.

It remains to establish the distributive laws in R . The left distributive law is much harder than the right, perhaps because our definition of multiplication is asymmetric. First consider $(a+b)c$. If $c = 0$, $(a+b)c = 0 = ac + bc$. If $c \neq 0$, we use formulas 9.4 and 9.2, and find $\tau_{(a+b)c} = \sigma_c \tau_{a+b} \sigma_c^{-1} = \sigma_c \tau_a \tau_b \sigma_c^{-1} = \sigma_c \tau_a \sigma_c^{-1} \sigma_c \tau_b \sigma_c^{-1} = \tau_{ac} \tau_{bc} = \tau_{ac+bc}$. Now applying both ends of this equality to the point 0, we have

$$(a+b)c = ac + bc.$$

Before proving the left distributive law, we must establish a lemma. For any line m in \mathbb{A} , denote the group of translations in the direction of m by $\text{Tran}_m(\mathbb{A})$, i.e. those translations $\tau \in \text{Tran } \mathbb{A}$ such that either $\tau = \text{id}$ or $PP' \parallel m$ for all P (where $\tau(P) = P'$).

Let m, n be lines in \mathbb{A} (which may be the same). Let $\tau' \in \text{Tran}_m(\mathbb{A})$ and $\tau'' \in \text{Tran}_n(\mathbb{A})$ be fixed translations, different from the identity, and let o be a fixed point of \mathbb{A} . We define a mapping $\phi: \text{Tran}_m(\mathbb{A}) \rightarrow$

$\text{Tran}_n(\mathbb{A})$ as follows. For each $\tau \in \text{Tran}_m(\mathbb{A})$, $\tau \neq \text{id}$, there exists by Theorem 9.7 a unique central dilatation σ leaving o fixed such that $\sigma(\tau'(o)) = \tau(o)$. Then $\tau = \sigma\tau'\sigma^{-1}$ since both τ and $\sigma\tau'\sigma^{-1}$ are translations that agree on o . Now using σ define ϕ by

$$(9.6) \quad \phi(\tau) = \sigma\tau''\sigma^{-1}.$$

Check that $\sigma\tau''\sigma^{-1}$ is a translation in the direction of n (Exercise 9.5).

LEMMA 9.9. $\phi: \text{Tran}_m(\mathbb{A}) \rightarrow \text{Tran}_n(\mathbb{A})$ is a homomorphism of groups.

Proof. We need to show that $\phi(\tau_1\tau_2) = \phi(\tau_1)\phi(\tau_2)$ for all $\tau_1, \tau_2 \in \text{Tran}_m(\mathbb{A})$. There is a subtlety in this since σ depends on the argument. We distinguish two cases.

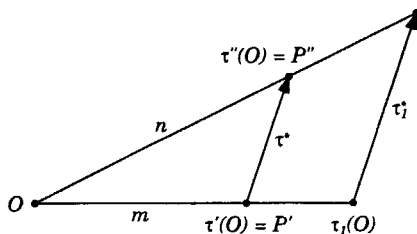


Figure 9.9. σ_1 stretches P' into $\tau_1(o)$.

Case 1. $m \nparallel n$. Replacing m and n by lines parallel to them, if necessary, we may assume that m and n pass through o . Let $\tau'(o) = P'$ and $\tau''(o) = P''$. Let τ^* be the unique translation which takes P' into P'' . Then

$$\tau'' = \tau'\tau^*.$$

If $\tau_1, \tau_2 \in \text{Tran}_m(\mathbb{A})$, let σ_1, σ_2 be the corresponding central dilatations, i.e. $\tau_i = \sigma_i\tau'\sigma_i^{-1}$ ($i = 1, 2$). Then $\phi(\tau_1) = \sigma_1\tau''\sigma_1^{-1} = \sigma_1\tau'\tau^*\sigma_1^{-1} = \sigma_1\tau'\sigma_1^{-1}\sigma_1\tau^*\sigma_1^{-1} = \tau_1 \circ \sigma_1\tau^*\sigma_1^{-1} = \tau_1\tau_1^*$, where we define $\tau_1^* = \sigma_1\tau^*\sigma_1^{-1}$. Similarly, $\phi(\tau_2) = \tau_2\tau_2^*$, where $\tau_2^* = \sigma_2\tau^*\sigma_2^{-1}$. If σ_3 is the dilatation with center O such that $\tau_1\tau_2 = \sigma_3\tau'\sigma_3^{-1}$, we get by a similar calculation that $\phi(\tau_1\tau_2) = \tau_1\tau_2 \circ \tau_3^*$, where $\tau_3^* = \sigma_3\tau^*\sigma_3^{-1}$.

So we have

$$\phi(\tau_1\tau_2) = \tau_1\tau_2 \circ \tau_3^* \quad \text{and} \quad \phi(\tau_1)\phi(\tau_2) = \tau_1\tau_2 \circ \tau_1^*\tau_2^*.$$

Let $Q := \phi(\tau_1\tau_2)(o)$ and $R := \phi(\tau_1)\phi(\tau_2)(o)$. Now $\phi(\tau_1\tau_2)$ and $\phi(\tau_1)\phi(\tau_2)$ are both translations in the m direction. Then o , Q and R are collinear. But τ_3^* and $\tau_1^*\tau_2^*$ are both translations in the τ^* direction, so $\tau_1\tau_2(o)$, Q , and R are collinear. Hence $Q = R$. It follows that $\phi(\tau_1\tau_2) = \phi(\tau_1)\phi(\tau_2)$.

Case 2. $m \parallel n$. Let $\tau', \tau'' \in \text{Tran}_m(\mathbb{A})$. Take another line p not parallel to m , and take $\tau''' \in \text{Tran}_p(\mathbb{A})$. Define $\psi_1: \text{Tran}_m(\mathbb{A}) \rightarrow \text{Tran}_p(\mathbb{A})$ using τ' and τ''' , and define $\psi_2: \text{Tran}_p(\mathbb{A}) \rightarrow \text{Tran}_m(\mathbb{A})$ using τ''' and τ'' .

Then $\phi = \psi_2\psi_1$ (Exercise 9.6). But ψ_1, ψ_2 are homomorphisms by Case 1. Hence, ϕ is a homomorphism. \square

Now we can prove the left distributivity law as follows. Consider $\lambda(a + b)$. In the lemma, take $m = n = \ell$, $o = 0$, $\tau' = \tau_1$, $\tau'' = \tau_\lambda$. Then ϕ is the map of $\text{Tran}_\ell(\mathbb{A}) \rightarrow \text{Tran}_\ell(\mathbb{A})$ which sends τ_a into $\tau_{\lambda a}$, for any a . Indeed, by equation (9.4) $\tau_a = \sigma_a\tau_1\sigma_a^{-1}$, so $\phi(\tau_a) = \sigma_a\tau_\lambda\sigma_a^{-1} = \tau_{\lambda a}$. By the lemma $\phi(\tau_a\tau_b) = \phi(\tau_a)\phi(\tau_b)$ (for all $a, b \in R$), whence $\phi(\tau_{a+b}) = \phi(\tau_a)\phi(\tau_b)$ by equation (9.2). Hence $\tau_{\lambda(a+b)} = \tau_{\lambda a}\tau_{\lambda b} = \tau_{\lambda a + \lambda b}$. Evaluating both translations at 0, we get by equation (9.2)

$$\lambda(a + b) = \lambda a + \lambda b.$$

This completes the proof of

THEOREM 9.10: *Let \mathbb{A} be an affine plane satisfying axioms A4 and A5. Let ℓ be a line of \mathbb{A} , let $0, 1$ be two points of ℓ , let R be the set of points of ℓ , and define $+$ and \cdot in R as given in Equations 9.1 and 9.3 above. Then R is a division ring.*

9.3 Introducing Coordinates in \mathbb{A}

We are now ready to introduce coordinates in \mathbb{A} . We have already fixed a line ℓ in \mathbb{A} , and two points $0, 1$ on ℓ . On the basis of these choices we

defined our division ring R . Choose another line, m , passing through 0 , and fix a point $1'$ on m .

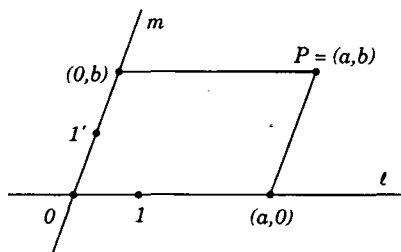


Figure 9.10.

For each point $P \in \ell$, if P corresponds to the element $a \in R$, we give P the coordinates affine coordinates $(a, 0)$. Thus 0 and 1 have coordinates $(0, 0)$ and $(1, 0)$, respectively.

If $P \in m$, $P \neq 0$, then there is a unique dilatation σ leaving 0 fixed and sending $1'$ into P . σ is of the form σ_a where $a = \sigma(1) \in R$. So we give P coordinates $(0, a)$.

Finally, if P is a point not on ℓ or m , we draw lines through P , parallel to ℓ and m , to intersect m in $(0, b)$ and ℓ in $(a, 0)$. Then we give P the coordinates (a, b) .

One sees easily that in this way \mathbb{A} is put into one-to-one correspondence with the set of ordered pairs of elements of R . We have yet to see that lines are given by — this will come after we find the equations of translations and dilatations.

We investigate the equations of translations and dilatations. First some notation. For any $a \in R$, denote by τ'_a the translation which takes 0 into $(0, a)$. Thus τ'_1 is the translation which takes 0 into $1'$, and for any $a \in R$, $a \neq 0$,

$$(9.7) \quad \tau'_a = \sigma_a \tau'_1 \sigma_a^{-1}.$$

This follows from the definition of the point $(0, a)$. Furthermore, it follows from equation (9.7) and Lemma 9.9 that the mapping $\phi: \text{Tran}_\ell(\mathbb{A}) \rightarrow \text{Tran}_m(\mathbb{A})$ defined by $\tau_a \mapsto \tau'_a$ is a homomorphism, and hence we

have the formulae, for any $a, b \in \mathbb{R}$,

$$(9.8) \quad \tau'_{a+b} = \tau'_a \tau'_b$$

$$(9.9) \quad \tau'_{ab} = \sigma_b \tau'_a \sigma_b^{-1},$$

the bottom formula (9.9) coming from applying σ_b on the left, and σ_b^{-1} on the right of Equation 9.7 and recalling (9.5).

PROPOSITION 9.11. *Let τ be a translation of \mathbb{A} , and suppose that $\tau(0) = (a, b)$. Then τ takes an arbitrary point $Q = (x, y)$ into $Q' = (x', y')$ where*

$$\begin{cases} x' = x + a \\ y' = y + b. \end{cases}$$

Proof. Indeed, let τ_{0Q} be the translation taking 0 into Q . Then $\tau_{0Q} = \tau_x \tau'_y$. Also $\tau = \tau_a \tau'_b$. So $\tau(Q) = \tau \tau_{0Q}(0) = \tau_a \tau'_b \tau_x \tau'_y(0) = \tau_a \tau_x \tau'_b \tau'_y(0) = \tau_{a+x} \tau'_{b+y}(0) = (x + a, y + b)$. \square

PROPOSITION 9.12. *Let σ be any dilatation of \mathbb{A} leaving 0 fixed. Then $\sigma = \sigma_a$ for some $a \in \mathbb{R}$, and σ takes the point $Q = (x, y)$ into $Q' = (x', y')$, where*

$$\begin{cases} x' = xa \\ y' = ya. \end{cases}$$

Proof. Again write $\tau_{0Q} = \tau_x \tau'_y$. Then, using equations (9.2) and (9.9),

$$\begin{aligned} \sigma(Q) &= \sigma_a \tau_x \tau'_y(0) = \sigma_a \tau_x \tau'_y \sigma_a^{-1}(0) \\ &= \sigma_a \tau_x \sigma_a^{-1} \cdot \sigma_a \tau'_y \sigma_a^{-1}(0) = \tau_{xa} \cdot \tau'_{ya}(0) = (xa, ya). \quad \square \end{aligned}$$

THEOREM 9.13. *Let \mathbb{A} be an affine plane satisfying A4 and A5. Fix two nonparallel lines ℓ, m in \mathbb{A} , and fix points $1 \in \ell$ and $1' \in m$, different from $0 := \ell \cdot m$. Then assigning coordinates as above, the lines in \mathbb{A} are all linear equations of the form $y = mx + b$, $m, b \in \mathbb{R}$, or $x = a$, $a \in \mathbb{R}$. Thus \mathbb{A} is isomorphic to the affine plane $\mathbb{A}^2(\mathbb{R})$.*

Proof. By construction of the coordinates, a line parallel to ℓ will have an equation of the form $y = b$, and a line parallel to m will have an equation of the form $x = a$.

Now let r be any line through 0 , different from ℓ and m . Then r must intersect the line $x = 1$, say in the point $Q = (1, a)$ ($a \in R$).

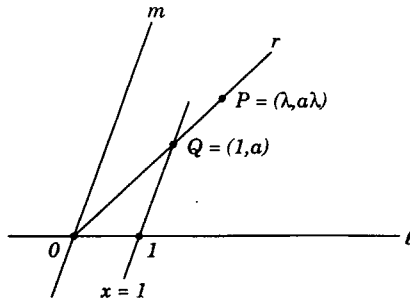


Figure 9.11. Assigning a linear equation to r .

Now if P is any other point on r , different from 0 , there is a unique dilatation σ_λ leaving 0 fixed and sending Q into P . Hence P will have coordinates $x = 1 \cdot \lambda$, $y = a \cdot \lambda$. Substituting x for λ , we find the equation of r is $y = ax$.

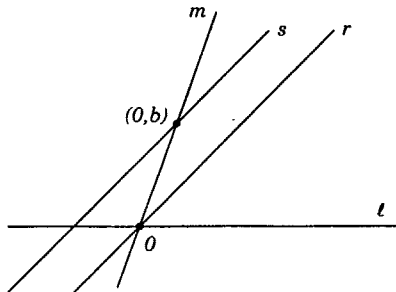


Figure 9.12. Assigning an equation to s .

Finally, let s be a line not passing through 0 , and not parallel to ℓ or m . Let r be the line parallel to s , passing through 0 . Let s intersect m in $(0, b)$. Then it is clear that the points of s are obtained by applying

the translation τ'_b to the points of r . So if $(\lambda, a\lambda)$ is a point of r (for $x = \lambda$), the corresponding point of s will be $x = \lambda + 0 = \lambda$, $y = a\lambda + b$, by Proposition 9.11. So the equation of r is $y = ax + b$. \square

REMARK. If σ is an arbitrary dilatation of \mathbb{A} , then σ can be written as $\tau\sigma'$, where τ is a translation, and σ' is a dilatation leaving 0 fixed (cf. Proposition 9.6). So if τ has equations $x' = x + c$, $y' = y + d$, and σ' has equations $x' = xa$, $y' = ya$, we find that σ has equations

$$\begin{cases} x' = xa + c \\ y' = ya + d \end{cases}$$

THEOREM 9.14. *Let π be a projective plane satisfying P1-P5. Then there is a division ring R such that π is isomorphic to $\mathbb{P}^2(R)$, the projective plane over R .*

Proof. Let ℓ_0 be any line in π , and consider the affine plane $\mathbb{A} = \pi - \ell_0$. Then \mathbb{A} satisfies A4 and A5, hence $\mathbb{A} \cong \mathbb{A}^2(R)$, by the previous theorem. But π is the projective plane obtained by completing the affine plane \mathbb{A} , and $\mathbb{P}^2(R)$ is the projective plane that completes the affine plane $\mathbb{A}^2(R)$ (Exercise 8.2), so the isomorphism above extends to show $\pi \cong \mathbb{P}^2(R)$. \square

REMARK. This is a good point at which to clear up a question left hanging from the early chapters, about the correspondence between affine planes and projective planes. We saw that an affine plane \mathbb{A} could be completed to a projective plane $S(\mathbb{A})$ by adding ideal points and an ideal line. Conversely, if π is a projective plane, and ℓ_0 a line in π then $\pi - \ell_0$ is an affine plane, by Exercise 2.2.

What happens if we perform first one process and then the other? Do we get back to where we started? There are two cases to consider.

1) If π is a projective plane, ℓ a line in π , and $\pi - \ell$ the corresponding affine plane, then one can see easily (Exercise 2.2) that $S(\pi - \ell)$ is isomorphic to π in a natural way.

2) Let \mathbb{A} be an affine plane, and let $S(\mathbb{A}) = \mathbb{A} \cup \ell_\infty$ be the corresponding projective plane. Then clearly $S(\mathbb{A}) - \ell_\infty \cong \mathbb{A}$. But what if ℓ_1 is a line in $S(\mathbb{A})$ different from ℓ_∞ ? Then in general one cannot expect $S(\mathbb{A}) - \ell_1$ isomorphic to \mathbb{A} .

However, if we assume that \mathbb{A} satisfies A4 and A5, then $S(\mathbb{A}) - \ell_1 \cong \mathbb{A}$. Indeed, $S(\mathbb{A}) \cong \mathbb{P}^2(R)$, for some division ring R , and we can always find an automorphism $\phi \in \text{Aut } \mathbb{P}^2(R)$, taking ℓ to ℓ_∞ (see Proposition 8.2). Then ϕ gives an isomorphism of $S(\mathbb{A}) - \ell_1$ and \mathbb{A} .

EXERCISES

EXERCISE 9.1. Prove that the kernel of a homomorphism of groups is a normal subgroup.

EXERCISE 9.2. In this exercise you will assist in the definition of factor group G/N obtained from a group G and normal subgroup N . As a set $G/N = \{gN \mid g \in G\}$, the set of left cosets of N in G . (Beware that the same coset may go under different names: $gN = g'N$ so long as $g^{-1}g' \in N$.)

a) Show that for each g in G the right coset g equals the left coset of g : i.e. $gN = Ng$.

b) Show that the following formula defines a group operation on G/N :

$$(gN)(g'N) = gg'N.$$

Where must you use normality of N ?

c) If G is a semidirect product of N with another subgroup K , i.e. $G = N \rtimes K$, find an isomorphism showing $G/N \cong K$.

EXERCISE 9.3. Let \mathbb{A} be an affine plane in which A4 holds, and let P, P' be two distinct points in \mathbb{A} . Define the mapping $\tau: \mathbb{A} \rightarrow \mathbb{A}$ taking P into P' by the parallelogram construction. Refer to the proof of Theorem 9.3. Prove that τ is an automorphism of \mathbb{A} .

EXERCISE 9.4. Give a rigorous proof of case 2 in the proof of Proposition 9.4.

EXERCISE 9.5. Prove that $\sigma\tau''\sigma^{-1}$ in equation (9.6) is a translation in the direction of n .

EXERCISE 9.6. Prove that $\phi = \psi_2\psi_1$ in case 2 of the proof of Lemma 9.9.

EXERCISE 9.7. Let π be a Desarguesian plane. Theorem 9.14 tells us that we may coordinatize points in π by selecting a line ℓ_0 , and coordinatizing the affine plane $\mathbb{A} = \pi - \ell_0$. \mathbb{A} may be coordinatized by selecting nonparallel lines ℓ_1 and ℓ_2 in \mathbb{A} , $O \in \ell_1, \ell_2$, $1 \in \ell_1, 1' \in \ell_2$, $R = \{\text{points on } \ell_1\}$, $+$ and \cdot defined in section 9.2, and proceeding as in section 9.3.

a) Show how to assign coordinates (x_1, x_2, x_3) to each point of π .

b) Show how to assign a linear equation $\sum_{i=1}^3 c_i x_i = 0$ to each line in π .

EXERCISE 9.8. Is the homomorphism $\phi: \text{Tran}_m(\mathbb{A}) \rightarrow \text{Tran}_n(\mathbb{A})$ actually an isomorphism of groups?

EXERCISE 9.9. In section 9.2 we let R be the set of points on a line ℓ in \mathbb{A} , where two points are designated 0 and 1. Addition and multiplication are defined by means of translation along ℓ and central dilatation fixing O (cf. equations (9.1) and (9.3)). Suppose m is a line in \mathbb{A} intersecting ℓ in O . Take R' to be the set of points with 0 and a point $1'$ to be chosen in $R' - \{0\}$. Define addition by translations along m and equation (9.1), multiplication by central dilatations fixing 0 and equation (9.3). Then R and R' are division rings.

a) Show that they are isomorphic rings: $R \cong R'$.

b) If m were parallel to ℓ , $0'$ and $1'$ arbitrary points in m , show that $R \cong R'$.

c) Show that $R \cong R'$ with no restriction on m .

Chapter 10

Möbius Transformations and Cross Ratio

10.1 Assessment

Let us pause for a moment to see what we have done and where we are going. We have been studying the subject of projective geometry from two points of view, the synthetic and the analytic.

The synthetic approach to planar projective geometry starts with points and lines satisfying axioms P1–P4. We make definitions like automorphism and complete quadrangle, proceeding in logical steps and proving theorems. Eventually we add axioms P5, P6, and P7 as we need them. For example, we add P6 when we need harmonic points, and P5 when we need to show the well-definedness of the harmonic conjugate. We added P7 in order to make the group $PJ(\ell)$ of projective projectivities precisely 3-transitive, and prove Pappus' Theorem.

The analytic approach to projective geometry starts from an algebraic object like the reals, complex numbers or any division ring R or field \mathbb{F} . Then we defined $\mathbb{P}^2(\mathbb{F})$ as nonzero ordered triples of \mathbb{F} -elements with the equivalence relation $(x_1, x_2, x_3) \sim (x_1, x_2, x_3)\lambda$, and lines as linear equations. We defined cross ratio,¹ a certain group of automorphisms, viz. $PGL(2, \mathbb{F})$, using 3×3 matrices, another group using field

¹cf. Section 5.3, Exercises 5.2, 5.8, 8.8

automorphisms of \mathbb{F} , and proved a fundamental theorem telling that these two subgroups together generate $\text{Aut } \mathbb{P}^2(\mathbb{F})$. In addition, two ordered sets, \mathcal{Q}_1 and \mathcal{Q}_2 , of four points in general position have a unique automorphism of $\text{PGL}(2, \mathbb{F})$ transforming \mathcal{Q}_1 into \mathcal{Q}_2 .

In the last two chapters we have tied these two approaches together, by showing that a Desarguesian projective plane is isomorphic to $\mathbb{P}^2(R)$ for a division ring we can construct, and conversely a $\mathbb{P}^2(R)$ satisfies Axiom P5. Additionally, we showed that axioms P6 and P7 in our synthetic development are equivalent to algebraic statements about R in our analytic development on $\mathbb{P}^2(R)$. For example, every Pappian plane is of the form $\mathbb{P}^2(\mathbb{F})$, and is Fano iff $\text{Char } (\mathbb{F}) \neq 2$.

In this chapter and the next, we continue to tie up our two approaches. Among the loose ends that are left are to give an analytic interpretation of the group of conjunctive projectivities $\text{PJ}(\ell)$, which we have so far studied only from the synthetic point of view. This is what we do in this chapter. In the next chapter, we give a synthetic interpretation of the subgroup $\text{PGL}(2, \mathbb{F})$ of automorphisms of a Pappian plane, which so far we have only studied from the analytic point of view. As a bonus of this interpretation, we prove Ceva's Theorem, a basic theorem in advanced Euclidean geometry.

10.2 The Group of Möbius Transformations of the Extended Field

Let \mathbb{F} be a field, and let $\pi = \mathbb{P}^2(\mathbb{F})$ be the projective plane over \mathbb{F} . Then π is a Pappian plane (which, you will recall, has Desargues' Axiom).² Let ℓ be the line $x_3 = 0$: simplify the homogeneous coordinates for points on ℓ , $(x_1, x_2, 0)$, by writing just (x_1, x_2) .

We have studied in our synthetic development in chapter 5 and 6 the group $\text{PJ}(\ell)$ of conjunctive projectivities on ℓ . Now we will define another group $\text{PGL}(2, \mathbb{F})$ of transformations of ℓ into itself, and will prove it is equal to $\text{PJ}(\ell)$.

²We stick to the commutative case for simplicity. Much of this section is valid over division rings — with a great deal of effort.

In the same spirit as section 8.1, we define a transformation T_A of ℓ onto itself for each nonsingular matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Recall that nonsingularity of A is equivalent to the condition $\det A = ad - bc \neq 0$. Now $T_A(x_1, x_2) = (x'_1, x'_2)$ where

$$\begin{aligned} x'_1 &= ax_1 + bx_2 \\ x'_2 &= cx_1 + dx_2, \end{aligned}$$

or in vector notation $T_A(\mathbf{x}) = \mathbf{A}\mathbf{x} = \mathbf{x}'$.

Clearly, for each nonzero scalar λ in \mathbb{F} , $T_{\lambda A} = T_A$ since $T_{\lambda A}(\mathbf{x}) = \lambda \mathbf{x}' = \mathbf{x}'$ because we are working in homogeneous coordinates. Now if we wanted, we could work our way through a 2×2 variant of section 8.1, proving that T_A is a one-to-one correspondence of ℓ with itself, whose inverse is $T_{A^{-1}}$ (Exercise 10.1). Moreover the set $\{T_X: \ell \rightarrow \ell \mid X \text{ is a } 2 \times 2 \text{ nonsingular matrix}\}$ forms a group (Exercise 10.2). Two matrices A and B define the same transformation, i.e. $T_A = T_B$, if and only if there is a nonzero $\lambda \in \mathbb{F}$: $B = \lambda A$ (Exercise 10.3). In addition, given three distinct points X_1, X_2, X_3 and another triple Y_1, Y_2, Y_3 we may find one and only one matrix system $\{\lambda A \mid \lambda \in \mathbb{F} - \{0\}\}$ such that $T_A(X_i) = Y_i$ ($i = 1, 2, 3$): this you may do in Exercise 10.4. In analogy with section 8.1, we have

DEFINITION. The group of transformations of ℓ into itself of the form T_A defined above, where A is a 2×2 nonsingular matrix over \mathbb{F} , is denoted by $\text{PGL}(1, \mathbb{F})$.

In carrying out our program of proving $\text{PGL}(1, \mathbb{F}) = \text{PJ}(\ell)$, we find it more convenient to introduce the inhomogeneous coordinate $x = x_1/x_2$ on ℓ . Note that x puts the points (x_1, x_2) of ℓ in one-to-one correspondence with the extended field $\mathbb{F} \cup \{\infty\}$, which we denote by \mathbb{F}_∞ : the notation ∞ corresponds to the single point $(x_1, 0)$, i.e. " $\infty = x_1/0$ ". (No special meaning should be given to ∞ here.)

By dividing the expressions for x'_1 with that for x'_2 above it is apparent that the group $\text{PGL}(1, \mathbb{F})$ is the set of transformations $T_A: x \mapsto x'$ where

$$x' = \frac{ax + b}{cx + d} \quad (a, b, c, d \in \mathbb{F}, ad - bc \neq 0).$$

In addition $T_A(\infty) = \frac{a}{c}$ and $T_A(-\frac{d}{c}) = \infty$ if $c \neq 0$, and $T_A(\infty) = \infty$ if $c = 0$. Such transformations of the extended field are called *Möbius transformations* or *fractional linear transformations*, and recur throughout mathematics. You will recall seeing Möbius transformations of \mathbb{C}_∞ in section 6.1. The next proposition is proven just like Lemma 6.4.

PROPOSITION 10.1. *The set of Möbius transformations of \mathbb{F}_∞ form a group under composition: i.e. $\text{PGL}(1, \mathbb{F})$ is a group. Moreover, if a, b, c and α, β, γ are two triples of distinct elements of \mathbb{F}_∞ , then there is a unique transformation T_A in $\text{PGL}(1, \mathbb{F})$ which sends a, b, c into α, β , and γ , respectively.*

Proof. Exercise 10.6. \square

PROPOSITION 10.2. *The group $\text{PGL}(1, \mathbb{F})$ of Möbius transformations is generated by the sets I, J, K of Möbius transformations of three kinds:*

$$\begin{aligned} I &= \left\{ T_A \mid A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F} \right\} \\ J &= \left\{ T_B \mid B = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, a \in \mathbb{F} - \{0\} \right\} \\ K &= \left\{ T_C \mid C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}. \end{aligned}$$

REMARK. In symbols, $\text{PGL}(1, \mathbb{F}) = \langle I \cup J \cup K \rangle$. The transformations in I are translations with equation $x' = x + a$. The transformations in J are central dilatations. Sets I and J are in fact subgroups. The only transformation in K is called inversion, an order 2 element.

Proof. We start with a transformation $T(x) = \frac{ax+b}{cx+d}$ where $ad - bc \neq 0$. There are two cases to consider: $c = 0$ and $c \neq 0$.

If $c = 0$, then $d \neq 0$. Let $T'_1(x) = \frac{a}{d}x$, so $T'_1 \in J$. Let $T'_2(x) = x + \frac{b}{d}$, so $T'_2 \in I$. Then $T'_2(T'_1(x)) = \frac{ax+b}{d} = T(x)$. We have disposed of this case.

If $c \neq 0$, we can in fact work out that

$$T(x) = (T_1 \circ T_2 \circ T_3 \circ T_4)(x)$$

where

$$T_4(x) = x + \frac{d}{c}, \quad T_3(x) = \frac{1}{x}$$

$$T_2(x) = \frac{bc - ad}{c^2}x, \quad T_1(x) = x + \frac{a}{c}.$$

You will be asked to verify this in Exercise 10.2.

Note that $T_1, T_4 \in I$, $T_2, T_5 \in J$ and $T_3 \in K$, so I , J , and K generate the group of Möbius transformations. \square

10.3 $PJ(\ell) \cong PGL(1, \mathbb{F})$

PROPOSITION 10.3. *Each of the translations in I , central dilations in J and the inversion in K in the Möbius transformations of \mathbb{F}_∞ is a projectivity of ℓ ($x_3 = 0$) to itself. Hence, $PGL(1, \mathbb{F}) \subseteq PJ(\ell)$.*

Proof. We must exhibit each of the special Möbius transformations as a composition of perspectivities within $\mathbb{P}^2(\mathbb{F})$. Remove the line $x_2 = 0$ as the line at ∞ of the affine plane with coordinates $x = x_1/x_2$ and $y = x_3/x_2$ (cf. Exercise 2.2 and Proposition 2.2). Then the line ℓ is $y = 0$, i.e. the x -axis.

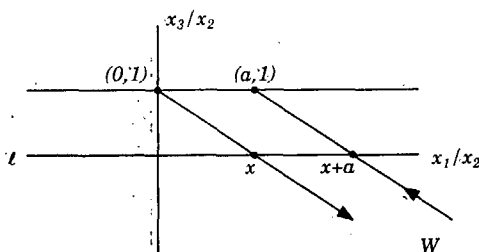


Figure 10.1. $\ell_\infty: x_2 = 0$. $x' = x + a$ as a projectivity.

Case I. We must show the transformation $T_I: x \mapsto x + a$ to be a projectivity.

Consider

$$\ell \stackrel{(0,1)}{\underset{\wedge}{\cong}} \ell_\infty \stackrel{(a,1)}{\underset{\wedge}{\cong}} \ell.$$

This projectivity sends $(x, 0)$ to the ideal point W lying on the line connecting $(0, 1)$ and $(x, 0)$, i.e. of slope $-\frac{1}{x}$. Now the line of slope $-\frac{1}{x}$ through $(a, 1)$ intersects the x -axis, ℓ , at $(x + a, 0)$. Hence x is sent to $x + a$ on ℓ , so T_J is equal to this projectivity.

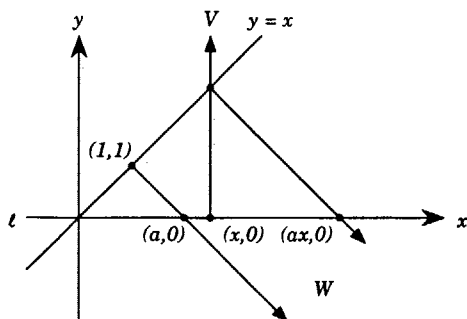


Figure 10.2. $x' = ax$ as a projectivity.

Case J. Consider the transformation $T_J: x \mapsto ax$ ($a \neq 0$). We claim T_J coincides on ℓ with the projectivity

$$\ell \stackrel{V}{\underset{\wedge}{\cong}} (x = y) \stackrel{W}{\underset{\wedge}{\cong}} \ell.$$

where V is ideal point on the vertical lines and W the ideal point on the line through $(1, 1)$ and $(a, 0)$. You will be asked to verify the details of T_J being this projectivity (Exercise 10.7a).

Case K. The transformation $x' = \frac{1}{x}$ is a product of three perspectivities

$$\ell \stackrel{(1,1)}{\underset{\wedge}{\cong}} \ell_\infty \stackrel{(1,0)}{\underset{\wedge}{\cong}} (x = y) \stackrel{V}{\underset{\wedge}{\cong}} \ell$$

You will be asked to check that $(x, 0)$ is sent to $(\frac{1}{x}, 0)$ in Exercise 10.7b.

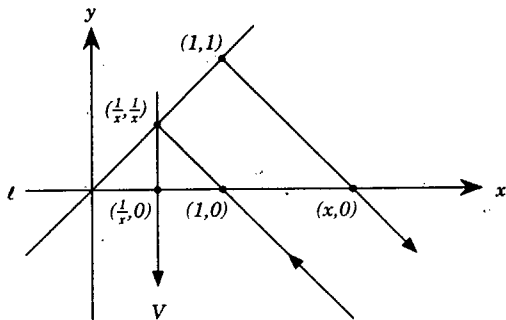


Figure 10.3. Inversion as a projectivity.

In conclusion, every Möbius transformation T is a projectivity of ℓ into itself, since T is a product of transformations in case I , J , and K . \square

THEOREM 10.4. *In a Pappian plane π with line ℓ , the group of projectivities of ℓ into itself is isomorphic to the group of Möbius transformations on the extended field \mathbb{F} associated with π :*

$$PJ(\ell) \cong PGL(1, \mathbb{F}).$$

Proof. We have seen in Proposition 10.3 that $PGL(1, \mathbb{F}) \subseteq PJ(\ell)$, where ℓ is line $x_3 = 0$ in $\mathbb{P}^2(\mathbb{F})$. We establish the reverse inequality.

Let $\psi \in PJ(\ell)$, and suppose ψ takes the points 0 , 1 and ∞ (or $(0, x_2)$, (x_1, x_1) and $(x_1, 0)$ in homogeneous coordinates on ℓ) into X , Y , and Z , respectively (and projectively, of course). Now by Proposition 10.1, there exists a Möbius transformation T taking 0 , 1 , ∞ into X , Y , Z , respectively, and Proposition 10.3 establishes that T is a projectivity. By the Fundamental Theorem, $T = \psi$ since their values on three points agree. This completes our proof for the line ℓ . \square

Now given the lines ℓ and ℓ' , in π it is a general fact that $PJ(\ell)$ and $PJ(\ell')$ are isomorphic as groups. For let ϕ be any perspectivity from ℓ onto ℓ' . Define a map $\psi: PJ(\ell) \rightarrow PJ(\ell')$ by

$$\alpha \mapsto \phi \alpha \phi^{-1}.$$

You will be asked to show in Exercise 10.4 that ψ is a group isomorphism. (Since ϕ is an arbitrary perspectivity, with no clear alternative, $PJ(\ell)$ and $PJ(\ell')$, though isomorphic, are not *canonically* so.) This shows the group of projectivities to be an invariant of the projective plane, and removes the special nature of our computation with $x_3 = 0$.

REMARK. Notice that our assumption of commutative scalars was put to full use in the form of the Fundamental Theorem. [Frankild-Kromann] investigates what is the case over a divisionring R : Möbius transformations (suitably defined) still form a group, they are still generated by translations, dilatations, and inversion, and we still have $PGL(1, R) \cong PJ(\ell)$. However, the Fundamental Theorem is only true up to inner automorphism of R .

10.4 Cross Ratio: a Projective Invariant

We have seen in the exercises that cross ratio is a projective invariant of $\mathbb{P}^2(\mathbb{R})$: however, this was done using special properties of the reals like the existence of trigonometric functions.

Now cross ratio is clearly definable over any field \mathbb{F} (cf. Exercise 8.8), since we need only subtract, divide and multiply in order to compute cross ratio. We will see in this section that cross ratio is also a projective invariant in $\mathbb{P}^2(\mathbb{F})$. Indeed the next theorem states that $PJ(\ell)$ is the group of permutations of points on ℓ that preserve cross ratio.

First, we give the definition of cross ratio in this more general setting. Let a, b, c , and d be four distinct points given in inhomogeneous coordinates for the line $\ell, x_3 = 0$; i.e. $a, b, c, d \in \mathbb{F}_\infty$.

DEFINITION. The cross ratio is defined by

$$R_X(a, b, c, d) = \frac{a - c}{a - d} \cdot \frac{b - d}{b - c},$$

if none of $a, b, c, d = \infty$. In case one of a, b, c , or $d = \infty$ we set $R_X(a, b, c, d) = \frac{b-d}{b-c}$ (if $a = \infty$), $\frac{a-c}{a-d}$ (if $b = \infty$), $\frac{b-d}{a-d}$ (if $c = \infty$), and $\frac{a-c}{b-c}$ (if $d = \infty$).

DEFINITION. By a transformation of ℓ into itself that preserves cross ratio, we mean a one-to-one correspondence $\ell \rightarrow \ell$ sending each $X \in \ell$ into $X' \in \ell$ such that

$$R_x(A, B; C, D) = R_x(A', B'; C', D')$$

for every quadruple of points A, B, C, D in ℓ . It is clear that the set of cross ratio preserving transformations of ℓ into itself is a group under composition of functions, which we denote by $\mathcal{R}(\ell)$.

THEOREM 10.5. Let \mathbb{F} be a field, and ℓ the line $x_3 = 0$ in $\mathbb{P}^2(\mathbb{F})$. Then the group of Möbius transformations (on the inhomogeneous coordinates \mathbb{F}_∞ for ℓ) is equal to the group of permutations of ℓ that preserve cross ratio:

$$PJ(\ell) = \mathcal{R}(\ell).$$

Proof. We first wish to prove that $PJ(\ell) \subseteq \mathcal{R}(\ell)$. Now given a projectivity $T: \ell \bar{\wedge} \ell$ we have shown in Theorem 10.4 and its proof that T is a Möbius transformation of the inhomogeneous coordinates for ℓ . In Proposition 10.2 and its proof we saw how to factor T into a product of translations, central dilatations and inversions of \mathbb{F}_∞ .

It remains to show that $T \in \mathcal{R}(\ell)$ by showing that each of the three types of generating Möbius transformations preserve cross ratio.

Case I. If $T(x) = x + \lambda$, translation by λ (and $T(\infty) = \infty$), we easily compute cross ratio of primed image points:

$$R_x(a', b'; c', d') = \frac{a + \lambda - (c + \lambda)}{a + \lambda - (d + \lambda)} \cdot \frac{b + \lambda - (d + \lambda)}{b + \lambda - (c + \lambda)},$$

which is clearly equal to $R_x(a, b; c, d)$ (also in the case that one point is ∞).

Case J. If $T(x) = \lambda x$ (and $T(\infty) = \infty$) where $\lambda \in \mathbb{F} - \{0\}$, the transformed points satisfy

$$R_x(a', b'; c', d') = \frac{\lambda a - \lambda c}{\lambda a - \lambda d} \cdot \frac{\lambda b - \lambda d}{\lambda b - \lambda c},$$

which again is clearly equal to $R_x(a, b; c, d)$ (also in case one point is ∞).

Case K. If $T(x) = \frac{1}{x}$ ($T(\infty) = 0$, $T(0) = \infty$) we compute cross ratio of $T(a) = a'$, etc. to be

$$\begin{aligned} R_X(a', b'; c', d') &= \frac{\frac{1}{a} - \frac{1}{c}}{\frac{1}{a} - \frac{1}{d}} \cdot \frac{\frac{1}{b} - \frac{1}{d}}{\frac{1}{b} - \frac{1}{c}} \cdot \frac{abcd}{abcd} \\ &= \frac{c-a}{d-a} \cdot \frac{d-b}{c-b} = R_X(a, b; c, d) \end{aligned}$$

if none of a , b , c , or $d = \infty$ or 0 . If $a = \infty$,

$$R_X(a', b'; c', d') = \frac{b}{b} \cdot \frac{d}{c} \cdot \frac{\frac{1}{b} - \frac{1}{d}}{\frac{1}{b} - \frac{1}{c}} = \frac{d-b}{c-b} = R_X(\infty, b; c, d).$$

If $a = 0$,

$$R_X(a', b'; c', d') = \frac{bcd}{bcd} \cdot \frac{\frac{1}{b} - \frac{1}{d}}{\frac{1}{b} - \frac{1}{c}} = \frac{c}{d} \cdot \frac{d-b}{c-b} = R_X(0, b; c, d).$$

The other cases proceed along the same line (Exercise 10.8).

This establishes that $PJ(\ell) \subseteq \mathcal{R}(\ell)$.

Conversely, suppose $\phi \in \mathcal{R}(\ell)$. Let $a = \phi(0)$, $b = \phi(1)$, $c = \phi(\infty)$ and generally $x' = \phi(x)$. By hypothesis $R_X(a, b; c, x') = R_X(0, 1; \infty, x)$, i.e.

$$\frac{a-c}{a-x'} \cdot \frac{b-x'}{b-c} = \frac{1-x}{-x}.$$

Suppose for the moment that a , b , and $c \neq \infty$. Upon solving for x' in three steps we have

$$(1) \quad x(a-c)(b-x') = (x-1)(a-x')(b-c)$$

$$(2) \quad x(a-c)b + x(c-b)a + a(b-c) = axx' - bxx' + (b-c)x'$$

$$(3) \quad x' = \frac{\frac{a-b}{b-c}cx + a}{\frac{a-b}{b-c}x + 1}$$

Since $\frac{a-b}{b-c}c - a\frac{a-b}{b-c} = \frac{(c-a)(a-b)}{b-c} \neq 0$ as \mathbb{F} -elements, we conclude that ϕ is a Möbius transformation. If $a = \infty = \phi(0)$, we get $\frac{b-x'}{b-c} = \frac{x-1}{x}$, so

$x' = -(b-c)\frac{x-1}{x} + b = \frac{cx+c-b}{x}$, which is also a Möbius transformation. You will be asked to check the other cases in Exercise 10.8.

Hence, $\phi \in \text{PJ}(\ell)$ and so $\text{PJ}(\ell) = \mathcal{R}(\ell)$. \square

NOTE. In the spirit of calling \mathbb{F}^{n+1}/\sim projective n -space over \mathbb{F} , where $(x_1, \dots, x_{n+1}) \sim (x_1\lambda, \dots, x_{n+1}\lambda)$, we call \mathbb{F}^2/\sim the *projective line over \mathbb{F}* , denoted by $\mathbb{P}^1(\mathbb{F})$. We saw that the line ℓ with inhomogeneous coordinates could be viewed as the extended "number line" \mathbb{F}_∞ . Note there is nothing special about $x_3 = 0$: in the first instance, we see that $x_2 = 0$ or $x_1 = 0$ may replace ℓ and still be put in a canonical one-to-one correspondence with \mathbb{F}_∞ . Now any line m may be transformed to ℓ by a projective collineation, defined in the next chapter, which puts m in one-to-one correspondence with \mathbb{F}_∞ (only up to a Möbius transformation since there will be more than one projective collineation transforming m into ℓ). This has two consequences. One is that any line in $\mathbb{P}^2(\mathbb{F})$ is projectively equivalent to the projective line over \mathbb{F} . The other is that cross ratio is definable for every line and the last theorem, Theorem 10.5, is valid for any line in $\mathbb{P}^2(\mathbb{F})$.

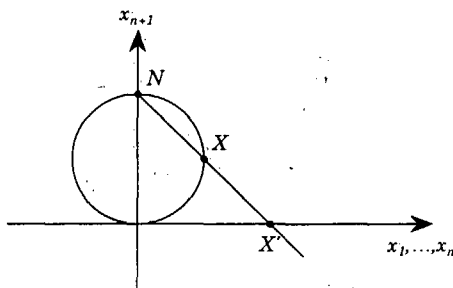


Figure 10.4. Stereographic projection of the n -sphere S^n into $\mathbb{R}^n \cup \{\infty\}$.

In case $\mathbb{F} = \mathbb{R}$ or \mathbb{C} the projective line over \mathbb{F} has certain well-known topological models. The projective line over the reals is a circle and the projective line over the complex numbers is a sphere (or *Riemann sphere*), both of which can be seen by stereographic projection in dimension 2 and 3, respectively, from the "north pole", north pole of sphere. Under this mapping, the "north pole" of the sphere corresponds to ∞ .

These identifications are useful for putting functions on the circle in one-to-one correspondence with functions of two homogeneous variables.

It is shown in a course in complex analysis that the group of Möbius transformations of the Riemann sphere is equal to the group of orientation-preserving, conformal (i.e. angle-preserving) one-to-one transformations of the Riemann sphere onto itself. These are automatically infinitely differentiable at all points except one, where a "simple pole" takes place. This provides a fourth interpretation of the same group $PJ(\ell)$ in the case $\mathbb{F} = \mathbb{C}$.

EXERCISES

EXERCISES 10.1–10.4 provide alternative demonstrations of Proposition 10.1, and may be done by adapting the proofs of Propositions 8.2, 8.5 and Theorem 8.6 to 2×2 nonsingular matrices over a field \mathbb{F} .

EXERCISE 10.1. Let ℓ be the line $x_3 = 0$, \mathbf{A} a nonsingular 2×2 matrix, and $T_{\mathbf{A}}$ the transformation $\mathbf{x}' = \mathbf{A}\mathbf{x}$. Show that $T_{\mathbf{A}}$ is a one-to-one correspondence of ℓ into itself, with inverse given by $T_{\mathbf{A}^{-1}}$.

EXERCISE 10.2. Show that the set $\{T_{\mathbf{A}}: \ell \rightarrow \ell \mid \det \mathbf{A} \neq 0\}$ is a group under composition.

EXERCISE 10.3. Show that $T_{\mathbf{A}} = T_{\mathbf{B}}: \ell \rightarrow \ell$ if and only if there exists $\lambda \in \mathbb{F} - \{0\}$ such that $\mathbf{A} = \lambda\mathbf{B}$.

EXERCISE 10.4. Let X_1, X_2, X_3 and Y_1, Y_2, Y_3 be two triples of points on ℓ , no two of which are equal. Show that there is a unique matrix \mathbf{A} up to scalar such that $T_{\mathbf{A}}(X_i) = Y_i$ for $i = 1, 2$, and 3.

EXERCISE 10.5. In section 8.1 we chose to work with $PGL(2, \mathbb{R})$ using homogeneous coordinates and 3×3 nonsingular matrices. This is in direct contrast to our use of inhomogeneous coordinates \mathbb{F}_{∞} and Möbius transformations in section 10.1. In this exercise you will see what you obtain if you pass to inhomogeneous coordinates in a study of $PGL(2, \mathbb{F})$ for some field \mathbb{F} .

a) Starting with the transformation $T_A \in \text{PGL}(2, \mathbb{F})$ where $A = (a_{ij})$ and $\det A \neq 0$; show that T_A is given by

$$x' = \frac{a_{11}x + a_{12}y + a_{13}}{a_{31}x + a_{32}y + a_{33}}, \quad y' = \frac{a_{21}x + a_{22}y + a_{23}}{a_{31}x + a_{32}y + a_{33}}$$

in the inhomogeneous coordinates $x = x_1/x_3$, $y = x_2/x_3$.

b) Show that the ideal point on the affine plane $x_3 = 1$ corresponding to slope m is sent to

$$x' = \frac{a_{11} + ma_{12}}{a_{31} + ma_{32}}, \quad y' = \frac{a_{21} + ma_{22}}{a_{31} + ma_{32}}$$

How is this to be interpreted if $m = \infty$?

EXERCISE 10.6. Prove that $\text{PGL}(1, \mathbb{F})$ is a 3-transitive group; refer to the statement of Proposition 10.1 and the proof of Lemma 6.4.

EXERCISE 10.7. Let ℓ be the line $x_3 = 0$ in $\mathbb{P}^2(\mathbb{F})$, which is made to correspond to the x -axis in the affine coordinates $y = x_3/x_2$, $x = x_1/x_2$.

a) Consider the projectivity

$$\ell \xrightarrow[V]{\Lambda} (x = y) \xrightarrow[W]{\Lambda} \ell$$

as in the proof of Proposition 10.3; where V is the ideal point on the y -axis and W is the ideal point on the line through $(1, 1)$ and $(a, 0)$ where $a \neq 0$. Show that $(x, 0)$ is sent to $(ax, 0)$.

b) Consider the projectivity

$$\ell \xrightarrow[(1,1)]{\Lambda} \ell_\infty \xrightarrow[(1,0)]{\Lambda} (x = y) \xrightarrow[V]{\Lambda} \ell,$$

where V is the same as in a). Show that the projectivity sends $(x, 0)$ into $(\frac{1}{x}, 0)$.

EXERCISE 10.8. Let ϕ be a cross ratio preserving transformation of \mathbb{F}_∞ . Let $a = \phi(0)$, $b = \phi(1)$, and $c = \phi(\infty)$. Suppose that one of b or c is ∞ . Show that $\phi(x) = x'$ is a Möbius transformation.

EXERCISE 10.9. A linear transformation τ of a vector space V is called an involution if $\tau^2 = \text{id}_V$. Suppose V is a 2-dimensional vector space over a field \mathbb{F} . Show that every invertible linear transformation $T: V \rightarrow V$ is, up to a scalar multiple, either an involution or is the product of two involutions.

Hint. What does Exercise 6.7 say for linear transformations?

EXERCISE 10.10. Show that the set of Möbius transformations of \mathbb{F}_∞ can be mapped injectively to a subset of $\mathbb{P}^3(\mathbb{F})$.

EXERCISE 10.11. Suppose $f: \mathbb{F}_\infty \rightarrow \mathbb{F}_\infty$ sends harmonic quadruples into harmonic quadruples. Moreover, suppose $f(0) = 0$, $f(1) = 1$ and $f(\infty) = \infty$. Prove that f restricted to \mathbb{F} is a field automorphism.

Chapter 11

Projective Collineations

In this chapter we develop the synthetic theory of projective collineation. In general, *collineation* is a synonym for automorphism of a projective plane, because lines are sent into lines.

DEFINITION. Let ℓ be a line of the projective plane π . An automorphism $\phi: \pi \rightarrow \pi$, $\ell \mapsto \ell'$, is called a *projective collineation* if ϕ restricted to ℓ is a projectivity:

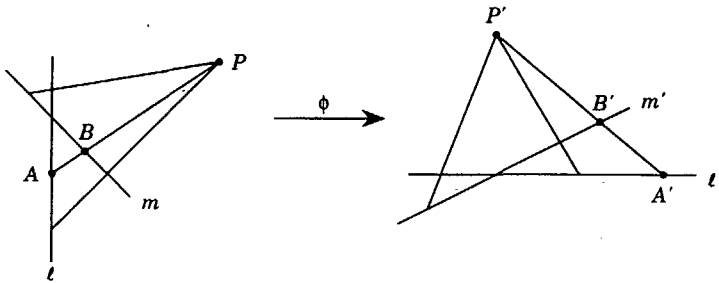
$$\phi|_{\ell}: \ell \xrightarrow{\sim} \ell'.$$

Now this definition will probably seem vague on a first reading, for could not ϕ be projective on ℓ but fail to be on some other line? We will see in the next proposition that this is not the case.

PROPOSITION 11.1. *Let ϕ be a projective collineation of π . Then for any line m , $\phi|_m$ is a projectivity.*

Proof. Assuming $\phi|_{\ell}$ is a projectivity, $\ell \not\bar{\wedge} \ell'$, we wish to show that $\phi|_m: m \rightarrow m'$ is a projectivity as well. Let P be a point not on ℓ or m .

Let $\rho: m \rightarrow \ell$ be the perspectivity $m \stackrel{P}{\bar{\wedge}} \ell$. Let $B \in m$ and $\rho(B) = A$. Then A, B and P are collinear, and so are their image points, A', B' and P' under our automorphism ϕ . Clearly $A' \in \ell'$ and $B' \in m'$.

Figure 11.1. $\phi|_m$ is a projectivity.

Now consider the mapping $\phi|_{\ell'} \circ \rho \circ \phi^{-1}|_{m'}$ of m' into ℓ' . This mapping sends B' into A' and therefore coincides with the perspectivity $\tau: m' \xrightarrow{P'} \ell'$. Then

$$\tau = \phi|_{\ell'} \circ \rho \circ \phi^{-1}|_{m'}.$$

Multiplying both sides of the equation from the right by $\phi|_m$, and from the left by τ^{-1} , we arrive at

$$\phi|_m = \tau^{-1} \circ \phi|_{\ell'} \circ \rho.$$

Since $\phi|_{\ell'}$ is a projectivity and τ^{-1} as well as ρ are perspectivities, this exhibits $\phi|_m$ as a projectivity. \square

The simplest example of a projective collineation is the identity. We will next study two key examples of projective collineations, called elations and homologies. We will prove that if π is a Pappian plane, then any projective collineation is a composition of at most three elations and two homologies. Finally, we will be able to show that if $\pi \cong \mathbb{P}^2(\mathbb{F})$ where \mathbb{F} is a field, then the group of projective collineations is precisely $\text{PGL}(2, \mathbb{F})$.

For now, let us just apply our knowledge gained from chapter 10 to note that an automorphism ϕ that fails to preserve cross ratio will fail to be a projectivity. From chapter 8 we know that an automorphism of \mathbb{F} gives an automorphism of $\mathbb{P}^2(\mathbb{F})$. Since complex conjugation, $z \mapsto \bar{z}$, does not preserve cross ratio, complex conjugation will induce an automorphism of $\mathbb{P}^2(\mathbb{C})$ that is *not* a projective collineation (Exercise 11.1).

11.1 Elations and Homologies

It follows from the fact that projective collineations transform every line projectively that the set of projective collineations form a group, denoted by $PC(\pi)$, within the group of automorphisms of a projective plane π . As promised, we turn to the study of elations and homologies.¹

DEFINITION. An *elation* is an automorphism α of π that leaves fixed each point P of some line ℓ , called the *axis*, but fixes no other points of π :

$$\alpha(P) = P \iff P \in \ell$$

We have seen something like an elation before. If we remove from π the line ℓ , we are left with an affine plane \mathbb{A} as in Exercise 2.2. We will now show that $\alpha|_{\mathbb{A}}$ is a translation different from the identity. Indeed we need only show $\alpha|_{\mathbb{A}}$ is a dilatation since α has no fixed points outside of the removed line ℓ . Then given $P, Q \in \mathbb{A}$ we must show that the transformed points P', Q' lie on a line parallel to PQ . Suppose PQ intersects ℓ in the point W in π . Then P, Q and W are collinear. Since $\alpha(W) = W$, it follows that P', Q' and W are collinear. Since pencils of parallels in \mathbb{A} are pencils of lines on points of ℓ , we arrive at $PQ \parallel P'Q'$. Thus an elation restricts to a dilatation of \mathbb{A} ; indeed, $\alpha|_{\mathbb{A}}$ is a translation since it has no fixed points.

Conversely, it is easy to see that a translation gives an elation α of the completed plane by defining $\alpha(X) = X$ on each ideal point X (Exercise 11.2):

PROPOSITION 11.2. *Let π be any projective plane. The elations with axis ℓ , together with the identity transformation, form a group $\mathcal{E}(\ell)$ under composition, itself a subgroup of $PC(\pi)$. Also, $\mathcal{E}(\ell) \cong \text{Tran } \mathbb{A}$.*

Proof. Since an elation is the identity projectivity on its axis, it is a projective collineation. It is easy to see that if $\alpha, \beta \in \mathcal{E}(\ell)$, then $\alpha \circ \beta^{-1} \in \mathcal{E}(\ell)$, so $\mathcal{E}(\ell)$ is a group (Exercise 11.3). Now the foregoing discussion has shown how to associate a translation to each elation; and vice-versa. This bijection is in fact a group isomorphism (Exercise 11.4). \square

¹This terminology is due to Sophus Lie (1842-1899).

If α is an elation with axis ℓ , then we have noted that $\alpha|_{\mathbb{A}}$ is a translation. Recall that for any $P, Q \in \mathbb{A}$, $PP' \parallel QQ'$. Let $PP'.\ell = X$. We call X the *center* of the elation α . In the real affine plane X would be the direction of the translation $\alpha|_{\mathbb{A}}$.

Although $\mathcal{E}(\ell)$ is a group, one should not suppose that all elations taken together form a group. For if α and β are elations with different axes, ℓ and m , there is no reason to suppose that $\alpha\beta$ is an elation. Exercise 11.5 asks you to find a “counterexample” in the 7 point plane.

However there is something we can say about all elations. It will turn out that, with the addition of Axiom P5, the two subgroups $\mathcal{E}(\ell)$ and $\mathcal{E}(m)$ of $\text{Aut}(\pi)$ are isomorphic in a very special way: they are conjugate subgroups, a group-theoretic concept we now define.

DEFINITION. Let G be a group. Let H and K be subgroups of G . H and K are called *conjugate* subgroups, if there is an element $g \in G$ such that the map

$$h \mapsto ghg^{-1}$$

is an isomorphism of H onto K . This is sometimes denoted by $K = gHg^{-1}$. Note that symmetrically one has $H = g^{-1}Kg$.

PROPOSITION 11.3. *Let π be a Desarguesian plane. Then the groups of elations $\mathcal{E}(\ell)$ and $\mathcal{E}(m)$ are conjugate subgroups in $\text{Aut}(\pi)$.*

Proof. We pick an automorphism ϕ that sends ℓ into m (cf. Theorem 8.6). Then the mapping

$$\alpha \mapsto \phi \circ \alpha \circ \phi^{-1} \quad (\alpha \in \mathcal{E}(\ell))$$

is an isomorphism of $\mathcal{E}(\ell)$ onto $\mathcal{E}(m)$. Indeed, $\phi\alpha\phi^{-1}$ fixes P if and only if $P \in m$, so $\phi\alpha\phi^{-1} \in \mathcal{E}(m)$. That the mapping is a group isomorphism is a routine exercise in group theory (Exercise 11.6). The converse is proved in Exercise 11.7. \square

We now turn to the other type of projective collineation — homology — which turns out to be closely related to central dilatation of the affine plane.

DEFINITION. A *homology* of the projective plane π is a projective collineation α of π leaving a line ℓ pointwise fixed and fixing precisely one other point O in $\pi - \ell$. α is said to be the homology with *axis* ℓ and *center* O . The set of homologies with axis ℓ and center O is a group denoted by $\mathcal{H}(\ell, O)$. The set of homologies together with elations, all with axis ℓ but of arbitrary center on or off ℓ , is a group denoted by $\mathcal{H}(\ell)$.

PROPOSITION 11.4. *Let π be a Desarguesian plane. Then $\mathcal{H}(\ell)$ is a semi-direct product of its subgroups $\mathcal{E}(\ell)$ and $\mathcal{H}(\ell, O)$.*

Proof. Let $\pi - \ell$ be the affine plane \mathbb{A} . \mathbb{A} satisfies the major and minor Desargues' Axioms as noted in chapter 9. The mapping

$$\alpha \mapsto \alpha|_{\mathbb{A}}$$

is an isomorphism of $\mathcal{H}(\ell)$ onto $\text{Dil } \mathbb{A}$ sending $\mathcal{H}(\ell, O)$ onto the group of central dilatations $\text{Dil}_O(\mathbb{A})$ and sending $\mathcal{E}(\ell)$ onto $\text{Tran } \mathbb{A}$; this claim follows from Proposition 11.2 and the preceding discussion. In Proposition 9.6 it was shown that $\text{Dil } \mathbb{A}$ is the semi-direct product of the normal, abelian subgroup $\text{Tran } \mathbb{A}$ and any one of its subgroups $\text{Dil}_O(\mathbb{A})$ for $O \in \mathbb{A}$. But group-isomorphism preserves a semi-direct product structure. You will be asked to check the details in Exercise 11.8. \square

11.2 The Fundamental Theorem of Projective Collineation

PROPOSITION 11.5. *Let π be a Desarguesian plane. Let A, B, C, D and A', B', C', D' be two quadruples of points, no three of which are collinear. Then one can find a product ϕ of elations and homologies such that $\phi(A) = A'$, $\phi(B) = B'$, $\phi(C) = C'$ and $\phi(D) = D'$.*

Proof. The proof proceeds in five steps as we show that, in general, ϕ is a product of three elations and two homologies.

1. Choose a line ℓ not incident with either A or A' . Since π is Desarguesian, it follows from Theorem 9.3 that there is a translation

of the affine plane $\pi - \ell$ which sends A into A' , and as we have seen in the last section this gives an elation $\alpha_1: \pi \rightarrow \pi$ with axis ℓ such that $\alpha_1(A) = A'$. Denote $\alpha_1(B) = B_1$, $\alpha_1(C) = C_1$ and $\alpha_1(D) = D_1$.

2. Since α_1 will be the first in a product of elations and homologies, we now wish to fix A' and send B_1 into B' as a second step. We can do this by choosing a line m incident with A' but not incident with either B_1 or B' .

As before there exists a unique elation α_2 with axis m such that $\alpha_2(B_1) = B'$. Note that $\alpha_2(A') = A'$ since A' is on the axis. Denote $\alpha_2(C_1) = C_2$ and $\alpha_2(D_1) = D_2$.

3. This time apply Theorem 9.3 to transform C_2 into C' by an elation α_3 with axis $A'B'$. Note that there is no problem with this, since $C' \notin A'B'$ and $C \notin AB$ by hypothesis, so

$$\alpha_2\alpha_1(C) = C_2 \notin \alpha_2\alpha_1(A) \cup \alpha_2\alpha_1(B) = A'B',$$

since α_1, α_2 are collineations. So far $\alpha_3 \circ \alpha_2 \circ \alpha_1$ transforms A, B, C into A', B', C' , respectively and, denoting $\alpha_3(D_2) = D_3$, D transforms into D_3 .

4. In the last two steps we will fix A', B', C' and transform D_3 by two homologies into D' .

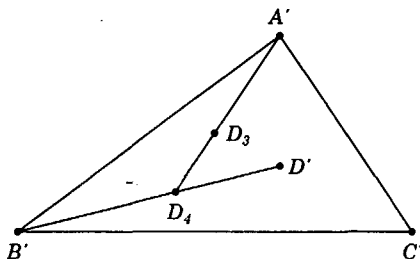


Figure 11.2. Transforming D_3 into D' in two steps.

Let $D_4 = A'D_3.B'D'$. Now in the affine plane $\pi - B'C'$, in which the major Desargues' Axiom holds, we find by Theorem 9.7 a (unique) central dilatation $\hat{\beta}_4$ holding A' fixed and sending D_3 into D_4 , for A', D_3 and D_4 are collinear points, none of which lie on $B'C'$ (why?). So

if β_4 denotes the homology with axis $B'C'$ and center A' corresponding to $\hat{\beta}_4$, then $\beta_4(A') = A'$, $\beta_4(B') = B'$, $\beta_4(C') = C'$ and $\beta_4(D_3) = D_4$.

5. This time apply Theorem 9.7 to get an homology β_5 with axis $A'C'$, center B' , such that $\beta_5(D_4) = D'$. There is no problem doing this, because B' , D_4 and D' are collinear points, none of which lie on $A'C'$ (why?).

In conclusion, $\phi = \beta_5 \circ \beta_4 \circ \alpha_3 \circ \alpha_2 \circ \alpha_1$ transforms A, B, C, D into A', B', C', D' , respectively. \square

LEMMA 11.6. *Let π be a Pappian plane. Let ϕ be a projective collineation of π , which leaves fixed four points A, B, C and D , no three of which are collinear. Then ϕ is the identity transformation.*

Proof. Let ℓ denote the line BC . Since $\phi(B) = B$ and $\phi(C) = C$, ϕ sends ℓ into itself. Indeed, $\phi|_\ell$ is a projectivity of ℓ into itself, since ϕ is a projective collineation.

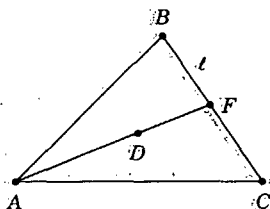


Figure 11.3. Three fixed points on a line.

Since ϕ also fixes A and D , it follows that $F := AD \cap \ell$ is fixed by ϕ . Whence, $\phi|_\ell: BFC \xrightarrow{\sim} BFC$, so $\phi|_\ell = \text{id}_\ell$ by the Fundamental Theorem (cf. chapter 6).

Let \mathbb{A} denote the affine plane $\pi - \ell$. Since ϕ fixes each point on ℓ , we have seen in the discussion preceding Proposition 11.2 that $\phi|_{\mathbb{A}}$ is a dilatation. But $\phi|_{\mathbb{A}}$ has the two fixed points A and D . Hence, $\phi|_{\mathbb{A}} = \text{id}_{\mathbb{A}}$ by Proposition 1.6. Putting $\phi|_{\mathbb{A}} = \text{id}_{\mathbb{A}}$ and $\phi|_\ell = \text{id}_\ell$ together, we conclude that $\phi = \text{id}_\pi$. \square

We now come to the Fundamental Theorem of Projective Collineation.

THEOREM 11.7. FUNDAMENTAL THEOREM OF PROJECTIVE COLLINEATION. *Let π be a Pappian plane. If A, B, C, D and A', B', C', D' are two quadruples of points, no three of which are collinear, then there is a unique projective collineation ϕ such that $\phi(A) = A'$, $\phi(B) = B'$, $\phi(C) = C'$ and $\phi(D) = D'$.*

Moreover, the group $PC(\pi)$ is generated by elations and homologies.

Proof. In Proposition 11.5 we proved that ϕ could be chosen to be a product of elations and homologies. Since each elation and homology is a projective collineation, it follows that $\phi \in PC(\pi)$.

We are left with proving uniqueness. Suppose ϕ, ψ are two projective collineations transforming A, B, C, D into A', B', C', D' , respectively. Then $\phi \circ \psi^{-1} \in PC(\pi)$, and $\phi \circ \psi^{-1}$ fixes A', B', C' and D' . We may apply Lemma 11.6 to get $\phi \circ \psi^{-1} = \text{id}_\pi$, so $\phi = \psi$, which gives uniqueness.

Finally, it is clear that given $\eta \in PC(\pi)$, η will coincide with a product of elations and homologies on four points in general position. By an application of the previous lemma, η is then the product of elations and homologies. Whence, the union of the subset of elations with the subset of homologies generates $PC(\pi)$. \square

11.3 $PC(\pi) \cong \text{PGL}(2, \mathbb{F})$

At this point we are in a position to realize our program of giving a synthetic interpretation to $\text{PGL}(2, \mathbb{F})$.

THEOREM 11.8. *Let \mathbb{F} be a field, and let $\pi = \mathbb{P}^2(\mathbb{F})$, the projective plane over \mathbb{F} . Then*

$$PC(\pi) = \text{PGL}(2, \mathbb{F}).$$

Proof. We first show that elations and homologies are representable by matrices.

Let ℓ be the line $x_3 = 0$, and P the point $(1, 0, 0)$ on ℓ . Then $\pi - \ell$ is the affine plane \mathbb{A} consisting of points with coordinates $x_3 \neq 0$. The

affine coordinates of \mathbb{A} are as usual

$$\begin{aligned}x &= x_1/x_3 \\ y &= x_2/x_3.\end{aligned}$$

Now an elation of π with axis ℓ and center P is a translation of \mathbb{A} , and conversely. Perhaps the simplest example of a translation $\alpha|_{\mathbb{A}}$ is

$$\begin{aligned}x' &= x + a \\ y' &= y,\end{aligned}$$

with homogeneous coordinates

$$\begin{aligned}x'_1 &= x_1 + ax_3 \\ x'_2 &= x_2 \\ x'_3 &= x_3.\end{aligned}$$

Whence the elation $\alpha: \pi \rightarrow \pi$ is represented by the matrix

$$A = \begin{pmatrix} 1 & 0 & a \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

with $a \in \mathbb{F}$; i.e. $x' = \alpha(x) = Ax$ is the equation defining α . Thus $\alpha \in PGL(2, \mathbb{F})$.

If β is any other elation, with axis m and center Q , we can always find a nonsingular 3×3 matrix X such that the induced automorphism T_X of π sends ℓ into m and P into Q (cf. Theorem 8.6). Then β and $T_X \circ \alpha \circ T_X^{-1}$ are two automorphisms both fixing each point on line m . Now the center of $T_X \circ \alpha \circ T_X^{-1}$ may be computed as follows: since

$$T_X^{-1}(R) \cup \alpha(T_X^{-1}(R)) \cdot \ell = P,$$

it follows by applying T_X to both sides of the incidence equation that

$$R \cup T_X \alpha T_X^{-1}(R) \cdot m = Q.$$

Hence, $T_X \circ \alpha \circ T_X^{-1}$ has center Q , so $T_X \circ \alpha \circ T_X^{-1} = \beta$. But $\alpha = T_A$, so $\beta = T_{XAX^{-1}}$ (β is represented by XAX^{-1} with X a transition matrix).

Hence, each elation of π is representable by a matrix that may be obtained from A by a change of basis.

Thus every elation is in $\text{PGL}(2, \mathbb{F})$. Now consider a homology γ with axis $x_1 = 0$ and center $(1, 0, 0)$ off the axis. In the affine plane $x_1 \neq 0$ with affine coordinates $x = x_2/x_1$, $y = x_3/x_1$, $\gamma|_A$ is a central dilatation with center $(0, 0)$, hence a stretching in some ratio $k \neq 0$. It will have equation in homogeneous coordinates

$$\begin{aligned}x'_1 &= x_1 \\x'_2 &= kx_2 \\x'_3 &= kx_3,\end{aligned}$$

i.e. $\gamma = T_C$ where

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & k \end{pmatrix}.$$

As before, any other homology δ has a matrix similar to C , i.e. there exists $Y \in \text{GL}_3(\mathbb{F})$ such that $\delta = T_{YCY^{-1}}$ (Exercise 11.9).

Hence, every elation and homology, and indeed every product of such, are of the form T_A for some 3×3 nonsingular matrix A over \mathbb{F} . So by Theorem 11.7,

$$\text{PC}(\pi) \subseteq \text{PGL}(2, \mathbb{F}).$$

We finish in what is by now a standard way.² Let $T \in \text{PGL}(2, \mathbb{F})$. Let A, B, C, D be a quadruple of points in general position, and suppose $T(A) = A'$, $T(B) = B'$, $T(C) = C'$ and $T(D) = D'$. Now A', B', C', D' is also a quadruple in general position since T is a collineation. By the Fundamental Theorem of Projective Collineation, there exists a unique $\beta \in \text{PC}(\pi)$ such that $\beta(A) = A'$, $\beta(B) = B'$, $\beta(C) = C'$ and $\beta(D) = D'$. But we have shown in the paragraphs above that $\beta \in \text{PGL}(2, \mathbb{F})$. So we have β, T in $\text{PGL}(2, \mathbb{F})$, having the same values on the quadruple A, B, C, D in general position, so by Theorem 8.6 we have $\beta = T$ since \mathbb{F} is a field. So

$$\text{PGL}(2, \mathbb{F}) \subseteq \text{PC}(\pi). \quad \square$$

²You might cover the rest of the paragraph and try it as an exercise.

11.4 Ceva's Theorem

In this section we prove an important theorem in advanced Euclidean geometry known as Ceva's Theorem.³ We will make full use of our projective theory of cross ratio and projective collineation in order to prove a generalization of Ceva's Theorem to Pappian planes. In another direction, the interested reader can see an application of our theory of projective collineation to matrices and determinants in Exercise 11.10.

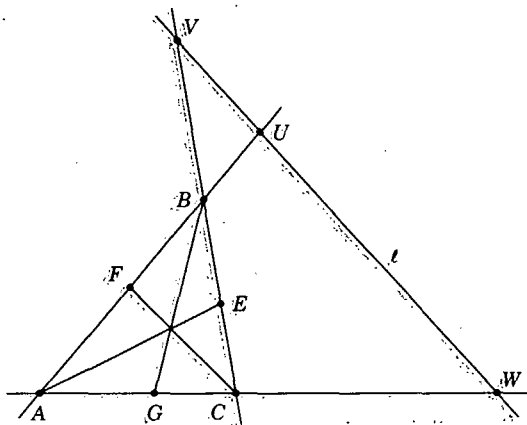


Figure 11.4. Ceva's configuration.

THEOREM 11.9. Let π be the Pappian, Fano plane $\pi = \mathbb{P}^2(\mathbb{F})$, \mathbb{F} a field of characteristic $\neq 2$. Let ABC be a triangle in π , and l a line different from AB , BC , or AC . Denote the points of intersection by

$$\begin{aligned} U &= l \cdot AB \\ V &= l \cdot BC \\ W &= l \cdot CA. \end{aligned}$$

Let E , F and G be arbitrary points on BC , AB , and AC , respectively. Then the lines BG , AE and CF are concurrent if and only if the cross

³After Giovanni Ceva (c. 1647–1736). If we are given a triangle ABC with a point D in general position, the lines AD , BD , and CD are named *cevians* in his honor.

ratios satisfy

$$(11.1) \quad R_x(A, B; F, U)R_x(B, C; E, V)R_x(C, A; G, W) = -1.$$

Proof. By the Fundamental Theorem we can carry A, B, C to the standard points P_1, P_2, P_3 by a projective collineation α : we could even carry a fourth point in general position to P_4 if we needed to. Since α restricted to each line is a projectivity, it follows from Theorem 10.5 (suitably extended in Exercise 11.11) that α preserves cross ratio.

Let $A = (1, 0, 0)$, $B = (0, 1, 0)$ and $C = (0, 0, 1)$ without loss of generality. Assume the line ℓ has equation $ax_1 + bx_2 + cx_3 = 0$. Let $E = (0, a_1, b_1)$, $F = (a_2, b_2, 0)$ and $G = (a_3, 0, b_3)$ be arbitrary points on BC ($x_1 = 0$), AB ($x_3 = 0$), and AC ($x_2 = 0$), respectively. Then

$$\begin{aligned} U &= \ell.AB = (-b, a, 0) \\ V &= \ell.BC = (0, -c, -b) \\ W &= \ell.CA = (-c, 0, a). \end{aligned}$$

Computing cross ratios, we get

$$R_x(A, B; F, U) = R_x(\infty, 0; a_2/b_2, -b/a) = -\frac{b/a}{a_2/b_2}$$

$$R_x(C, A; G, W) = R_x(\infty, 0; b_3/a_3, -a/c) = -\frac{a/c}{b_3/a_3}$$

and

$$R_x(B, C; E, V) = R_x(\infty, 0; a_1/b_1, -c/b) = -\frac{c/b}{a_1/b_1}.$$

Equation 11.1 becomes after simplification

$$b_1b_2a_3 = a_1a_2b_3.$$

The equations of lines BG , AE and CF , the lines we wish to show concurrent, are easily computed as follows. Line BG has the equation

$$\begin{vmatrix} x_1 & x_2 & x_3 \\ 0 & 1 & 0 \\ a_3 & 0 & b_3 \end{vmatrix} = b_3x_1 - a_3x_3 = 0.$$

Line AE has equation $b_1x_2 - a_1x_3 = 0$, and line CF has equation $-b_2x_1 + a_2x_2 = 0$. Now the lines BG , AE and CF are concurrent iff

$$\begin{vmatrix} b_3 & 0 & -a_3 \\ 0 & -b_1 & a_1 \\ -b_2 & a_2 & 0 \end{vmatrix} = b_1b_2a_3 - a_1a_2b_3 = 0.$$

Hence equation 11.1 holds iff the lines BG , AE and CF are concurrent.

The special cases arising from a , b , c , b_1 , b_2 or $a_3 = 0$ are left to the reader (Exercise 11.12). \square

We recall the notation AB for the signed length of the line segment \overline{AB} in the Euclidean plane.

THEOREM 11.10 (CEVA'S THEOREM). *Suppose ABC is a triangle in the Euclidean plane, and E , F and G are points on BC , AB and AC , respectively. Then AE , CF and GB are concurrent iff*

$$(11.2) \quad \frac{AF}{FB} \cdot \frac{BE}{EC} \cdot \frac{CG}{GA} = 1.$$

Proof. Let ℓ be the line at ∞ for the real affine plane in the previous theorem. If W is an ideal point in the completed Euclidean plane, then $R_x(Z, U; V, W) = \frac{ZV}{UV}$ (which is positive if V is between Z and U , and negative if U is between Z and V). Now equation (11.2) follows from equation (11.1). \square

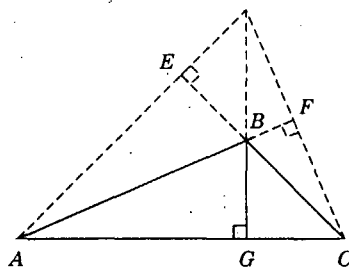


Figure 11.5. The altitudes of a triangle.

COROLLARY 11.11. *The altitudes of a triangle are concurrent.*

Proof. Label the points of a triangle ABC and the base of each altitude E, F, G as in the figure. If \sim denotes similar triangles, then the right triangles

$$\triangle AEC \sim \triangle BGC \quad \text{so} \quad \frac{CG}{EC} = \frac{BC}{CA}$$

$$\triangle AFC \sim \triangle AGB \quad \text{so} \quad \frac{AF}{GA} = \frac{CA}{AB}$$

and

$$\triangle BEA \sim \triangle BFC \quad \text{so} \quad \frac{BE}{FB} = \frac{AB}{BC}$$

Multiplying the three equations above together we obtain equation 11.2. Hence, altitudes BG, AE and CF are concurrent by Ceva. \square

It is rather remarkable that one can prove this Euclidean using projective techniques. In the exercises you may similarly show that medians and angle bisectors of a triangle are concurrent (Exercise 11.13).

EXERCISES

EXERCISE 11.1. Find an example of an automorphism of $\mathbb{P}^2(\mathbb{C})$ which is not a projective collineation. Justify.

EXERCISE 11.2. Let \mathbb{A} be an affine plane, and \mathbb{S} be its completion to a projective plane (chapter 2). Show that a translation τ of \mathbb{A} (chapter 1) may be extended to an elation α of \mathbb{S} by defining

$$\alpha(X) = \begin{cases} X & \text{if } X \in \ell_\infty \\ \tau(X) & \text{if } X \in \mathbb{A}. \end{cases}$$

EXERCISE 11.3. Show that the set $\mathcal{E}(\ell)$ of elations with axis ℓ forms a group under composition of mappings $\pi \rightarrow \pi$.

EXERCISE 11.4. Show that $\text{Tran } \mathbb{A} \cong \mathcal{E}(\ell)$ as groups, if ℓ is a line in a projective plane π , and \mathbb{A} is the affine plane $\pi - \ell$ (cf. Exercise 2.2).

EXERCISE 11.5. Refer to Figure 4.2 and the proof of Proposition 4.5. Find two elations, α and β , of the 7-point plane π_7 such that $\alpha \circ \beta$ is not an elation.

EXERCISE 11.6. Let H be a subgroup of a group G . Show that for an arbitrary g in G

a) the set $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ is a subgroup of G ;

b) the mapping $\phi: h \mapsto ghg^{-1}$ ($h \in H$) is a homomorphism $\phi: H \rightarrow gHg^{-1}$;

c) ϕ is a bijection between H and gHg^{-1} .

Note that gHg^{-1} and H are conjugate subgroups.

EXERCISE 11.7. Suppose π is a projective plane satisfying P5. Given $\phi \in \text{Aut}(\pi)$ and the group of elations $\mathcal{E}(\ell)$ with axis ℓ , show that the conjugate subgroup $\phi\mathcal{E}(\ell)\phi^{-1}$ is the group of elations $\mathcal{E}(\ell')$ with axis $\ell' = \phi(\ell)$.

EXERCISE 11.8. Show in detail that

a) if $G = H \rtimes K$, $\phi: G \xrightarrow{\cong} G'$, $\phi(H) := H'$, $\phi(K) := K'$, then $G' = H' \rtimes K'$ (cf. chapter 9, semi-direct product).

b) $\mathcal{H}(\ell) = \mathcal{E}(\ell) \rtimes \mathcal{H}(\ell; O)$ (cf. Proposition 11.4).

EXERCISE 11.9. Let $\pi = \mathbb{P}^2(\mathbb{F})$, \mathbb{F} a field. Show that any homology $\delta: \pi \rightarrow \pi$ can be represented by a matrix similar (in the technical sense of linear algebra) to the matrix $C = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ ($a \in \mathbb{F}$).

EXERCISE 11.10. Prove that

a) any invertible 3×3 matrix Y over a field \mathbb{F} is a product of five special matrices: $Y = C_5 C_4 A_3 A_2 A_1$, where C_5 and C_4 are similar to C , and A_3, A_2, A_1 are similar to A in the proof of Theorem 11.8.

b) Suppose a function $D: M_3(\mathbb{F}) \rightarrow \mathbb{F}$ mapping the set of 3×3 matrices into \mathbb{F} satisfies the two conditions

D1. If A, B are two 3×3 matrices,

$$D(AB) = D(A)D(B)$$

D2. For each $a \in \mathbb{F}$, let $C(a) = \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Then $D(C(a)) =$
 a .

Show that D is the determinant; i.e. $D(X) = \det(X)$ on every 3×3 matrix X .

EXERCISE 11.11. Let $\pi = \mathbb{P}^2(\mathbb{F})$, \mathbb{F} a field. Settle a question left hanging since Theorem 10.5 by defining cross ratio on any line m in π and extending Theorem 10.5 to arbitrary lines.

EXERCISE 11.12. Let $\pi = \mathbb{P}^2(\mathbb{F})$, \mathbb{F} a field of characteristic $\neq 2$. Let $A = (1, 0, 0)$, $B = (0, 1, 0)$, and $C = (0, 0, 1)$. Assume ℓ is a line with equation $ax_1 + cx_2 = 0$.

a) Show that Theorem 11.9 holds true in this case, too. Why must $a \neq 0$ and $c \neq 0$?

b) If one of a or $b = 0$, show that Theorem 11.9 is still true. Dispose of the outstanding cases in the proof of Theorem 11.9.

c) What can go wrong in characteristic 2?

EXERCISE 11.13. Let ABC be a triangle in the Euclidean plane.

a) Prove that the medians of ABC are concurrent.

b) Prove that the angle bisectors of ABC are concurrent.

EXERCISE 11.14. Prove Menelaus' Theorem:

Given a triangle ABC in the Euclidean plane and points U, V and W on BC, AC , and AB , respectively, then U, V and W are collinear iff

$$\frac{AW}{WB} \cdot \frac{BU}{UC} \cdot \frac{CV}{VA} = -1.$$

EXERCISE 11.15. Suppose ABC is a triangle in the Euclidean plane, and X and Y are midpoints of the sides \overline{AB} and \overline{BC} , respectively. Show that $\overline{XY} \parallel \overline{AC}$.

EXERCISE 11.16. Let \mathbb{F}_q be a finite field with q elements. (It is shown in a full year algebra course that q is necessarily a power of a prime and \mathbb{F}_q is unique up to isomorphism.) The finite projective plane $\mathbb{P}^2(\mathbb{F}_q)$ is called the *projective plane of order q* . Determine the number of projective collineations of the projective plane of order q .

EXERCISE 11.17. A line in general position will intersect a complete quadrangle in six points called an *involution hexad* or a *quadrangular set*. Define a projective invariant of ordered six-tuples on a line such that the six points form a quadrangular set if and only if your invariant is -1 .

Hint. Use equation (11.1) and Figure 11.4 as a starting point.

Appendix

Independent Studies in Projective Geometry

Projective geometry leads naturally to the study of algebraic geometry, non-Euclidean geometry or foundations of geometry. We would like to leave the student with an approach to each of these subjects. Information and references are provided in four appendices which we hope will inform the reader enough to profit from an independent investigation. For example, we believe each of the four topics suitable for a project at Roskilde — that is to say — suitable for a semester's investigation by a group of students, who focus on a suitably broad problem, enjoying the guidance of a professor and writing a joint report at the semester's end.

Appendix A is about conics and B about Bezout's Theorem. Both are topics at the beginning of a typical course in algebraic geometry, and might interest the reader in looking further into algebraic geometry (e.g. [Reid]). We have considered conics in the real projective plane in several places in the text and exercises; in A we then give an easily understood synthetic definition of conic that permits its study in any Pappian plane.

Having Bezout's Theorem in one's geometry is the natural justification for assuming each pair of lines meet in one point. In a projective plane over an algebraically closed field, two algebraic curves of degree m and degree n meet in mn points (with multiplicity).

In appendix C we place a metric on the real projective plane and delve a little into the resulting elliptic geometry. Elliptic and spherical geometries are locally the same, globally different by the presence of axiom P1 in the first. In both these geometries triangles have internal angles that sum to more than 180° . The hyperbolic geometry, where triangles have internal angles summing to less than 180° , has an incidence geometry represented by the Klein model in the projective plane — we will define this, too. Bolyai's Theorem says that the Law of Sines, suitably defined, holds for the Euclidean, spherical and hyperbolic geometries: [Hsiang] gives a unified proof.

In appendix D we take up the evident question after a reading of chapter 9: are there sensible coordinates for a projective plane without Desargues' Theorem? It turns out that any projective plane π is coordinatized by a ternary ring R . The stronger the geometric axioms we put on π , the stronger the algebraic axioms we get on the generalized ring R . For example, suppose a projective plane π satisfies a modified version of P5:

- P5***. Let ABC and $A'B'C'$ be two triangles in π and O a point such that AA' , BB' , and CC' meet at O . Let $P = AB.A'B'$, $Q = AC.A'C'$ and $R = BC.B'C'$. Assume that O lies on PQ . Then R lies on PQ .

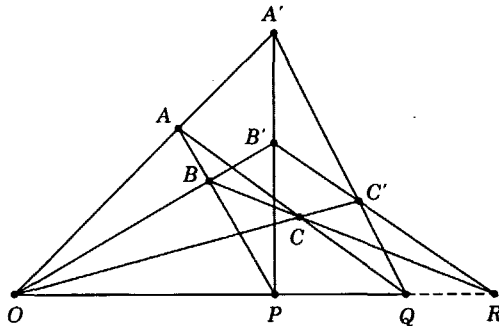


Figure A.1. The configuration of P5*.

Such a π is called an *alternative plane*. Then π is isomorphic to

a projective plane over an alternative division ring, like the Cayley-Graves octonions.

Appendix A

Conics

In this appendix we will give five different definitions of a conic. Each will be a different aspect of the same figures we are all familiar with — the circle, ellipse, parabola and hyperbola. Several of the definitions will lead to generalizations of the ordinary conic to finite geometry, complex geometry, or other specializations of a field F . The challenge for you is to show the equivalence of some or all of the definitions, over the course of several weeks or months. We include a sketch of the proofs of several implications and mention several important projective theorems you should obtain along the way. Finally, a set of exercises at the end will be helpful in illuminating the text.

In the Euclidean plane, a first notion is a circle since it is the locus of all points equidistant (at some fixed radius) from a point. As a second step, conic is naturally defined as a figure obtained from a circle by applying a series of finitely many central or parallel projections in Euclidean space (and ending up in the plane of the original circle):

DEFINITION 1 (DESARGUES). A *conic* is the locus of points in a plane obtained from a circle after a finite number of projections in space.

According to Exercise 5.9 one can deduce from this definition a sensible cross ratio of four coconic points, say points A, B, C, D on conic Γ . $R_x(A, B; C, D)$ is defined to be $R_x(AP, BP; CP, DP)$ for any fifth point P on Γ : Exercise 5.9 shows the choice of P in the cross ratio

of four lines concurrent at P to be irrelevant. Thus

$$R_x(AX, BX; CX, DX) = \text{constant} \quad \text{if } X \in \Gamma - \{A, B, C, D\}.$$

Indeed the converse is not hard to prove, either (cf. Exercise A.2).

DEFINITION 2 (M. CHASLES). Suppose A, B, C, D are points in a plane such that no three are collinear. A conic is the locus of points A, B, C, D and fifth variable point X such that

$$R_x(AX, BX; CX, DX) = k \quad (k \neq 0, 1).$$

Given two points A, B on a conic Γ a projectivity between pencils at A and B , $\tau: [A] \bar{\wedge} [B]$, may be defined as follows: given $X \in \Gamma$,

$$\tau: AX \mapsto BX.$$

That leaves only the small detail of the tangent lines to Γ at A and B (why?). τ sends AB into the tangent line b at B , and sends the tangent a at A into AB . Now why is the one-to-one correspondence a projectivity? Basically because it is a cross ratio preserving transformation of pencils: just apply Definition 2 to four coconic points! It is not hard to prove that Definition 3 below is equivalent to Definition 2 in the Euclidean plane.

DEFINITION 3 (J. STEINER). Let τ be a projectivity between pencils of lines centered at points A and B . Suppose $A \neq B$ and τ is not a perspectivity. A conic Γ is the locus of points ℓ, ℓ' where $\tau: \ell \bar{\wedge} \ell'$.

Definition 3 fits very well into our synthetic development of projective geometry. Thus we have here a natural definition of conic in any projective plane. However, it appears that A and B play some special role on Γ , whereas the truth is that for any two points C and D on Γ in a Pappian plane there is a projectivity $\sigma: [C] \bar{\wedge} [D]$ such that $\Gamma = \{X \mid \sigma: CX \bar{\wedge} DX\}$: we might suggestively summarize this by writing $\Gamma = \Gamma(A, B; \tau) = \Gamma(C, D; \sigma)$. Since three points and their values determine a projectivity in a Pappian plane, we might write this as $\Gamma = \Gamma(A, B; C, D, E)$, where A, B, C, D, E are five distinct points and τ is determined from $AC, AD, AE \bar{\wedge} BC, BD, BE$.

At this point, you should prove

THEOREM A.1 (PASCAL'S THEOREM). *Let Γ be a conic, and A, B, C, D, E points on Γ . Given a sixth point F in the projective plane, consider the hexagon $ABCDEF$. Suppose no three vertices are collinear. Then $F \in \Gamma$ if and only if $AB \cdot DE$, $BC \cdot EF$ and $CD \cdot AF$ are collinear.*

You may essentially copy the proof of Pappus' Theorem in chapter 6 to obtain the proof of \implies , if you assume $\Gamma = \mathbb{R}(A, C; \tau)$.

Now you should attempt to show that you may cyclically permute the points in $\Gamma = \mathbb{R}(A, B; C, D, E)$; thus showing Γ not to be dependent on A and B .

Definition 3 also suffers from the drawback of not being visibly self-dual. If you dualize Definition 3, you would obtain something you could call a line-conic, the envelope of lines through projectively related points on ℓ and ℓ' . You have already seen an instance of the dual of Definition 3 in Exercise 5.6. If you define a point-conic to be a conic with its tangent lines (their definition?), and include the contact points (their definition?) in line-conic, it is possible to prove that point-conics are line-conics, and line-conics are point-conics. This is what is meant when we say conic is a self-dual concept. So dualizing Pascal's Theorem gives a theorem stating roughly:

THEOREM A.2 (BRIANCHON). *Opposite vertices of a hexagon inscribed in a conic join in three concurrent lines.*

This theorem was discovered around 1806 while Pascal's Theorem predated it by as much as 167 years. It was in fact Brianchon's Theorem that gelled the Principle of Duality in the minds of Poncelet, Gergonne and others: see [Bell].

Let us cast about for a self-dual definition of conic. In Exercise A.3 you can associate to a point P , away from a conic Γ , the line p obtained as the locus of the variable point Z on a secant ℓ such that $H(X, Y; Z, P)$, where $\{X, Y\} = \Gamma \cap \ell$.

We call the line p the *polar* of P , and P the *pole* of p . Points on Γ receive their tangent lines as poles.

The assignment of pole to polar, polar to pole, with respect to a conic, is an example of a *polarity*. A polarity is a one-to-one correspondence between points and lines of a projective plane, respecting

incidence: thus a polarity sends ranges into pencils, pencils into ranges, and complete quadrangles into complete quadrilaterals, etc. Moreover, one assumes of a polarity that it sends each range of points into a pencil of lines *projectively*. One generalizes terminology to say that a polarity sends A to its polar a , and sends a line b to its pole B .

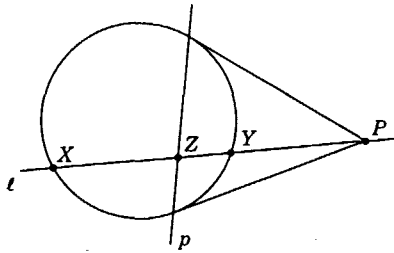


Figure A.1. The pole p of P with respect to a conic Γ .

A polarity has the property that if it sends a into A , then it sends A into a . We say A and B are *conjugate points*, and a, b *conjugate lines* of a polarity T if $B \in a$ and $A \in b$ (and by convention $T(B) = b$, $T(A) = a$). So a point X is *self-conjugate* if $X \in x$. A polarity is termed *hyperbolic* if it has at least one self-conjugate point. Then one can show that every line but one has exactly two self-conjugate points. Self-conjugate lines are similarly defined, and their theory is dually developed.

DEFINITION 4 (VON STAUDT). A *conic* is the locus of self-conjugate points of a hyperbolic polarity.

If we add the envelope of self-conjugate lines to this definition — as we add the lines to the vertices of a projectively defined triangle — we will obtain a self-dual definition of conic. Showing Definitions 3 and 4 equivalent will then complete the program of understanding self-duality of conic within our synthetic development, as well as add much to your understanding of conics. You will want to prove some basic theorems as possible stepping stones to proving Definition 3 equivalent to 4; we list them below (and do Exercises A.4 and A.5 as well).

THEOREM A.3 (VON STAUDT). *Given a polarity, there exists a self-polar triangle and a unique self-polar pentagon. (An odd polygon is said to be self-polar if each vertex is transformed into the opposite side.)*

THEOREM A.4 (CHASLES). *Given a polarity, a triangle and its polar triangle, if distinct, are in perspective.*

THEOREM A.5 (DESARGUES' INVOLUTION THEOREM). *Suppose $PQRS$ is a complete quadrangle in a Pappian plane and ℓ a line not passing through either P, Q, R or S . If a conic through P, Q, R, S meets ℓ , it does so in a pair of points X, X' of an involution τ : i.e., $X, X' \in \ell \cap \Gamma$ implies that $\tau: X \bar{\wedge} X', \tau^2 = \text{id}$.*

We now ask, what happens in field coordinates? You should show that a polarity of $\mathbb{P}^2(\mathbb{F})$ is represented by a symmetric matrix. Then you can establish from Definition 4 the equivalence of the next

DEFINITION 5. A conic is the locus of points $\mathbf{X} = (x_1, x_2, x_3)$ such that

$$\mathbf{X}\mathbf{C}\mathbf{X}^T = 0,$$

$$c_{11}x_1^2 + c_{22}x_2^2 + c_{33}x_3^2 + 2c_{23}x_2x_3 + 2c_{31}x_3x_1 + 2c_{12}x_1x_2 = 0,$$

for some symmetric matrix $\mathbf{C} = (c_{ij})$ with nonzero determinant.

In the real projective plane you should show that every conic transforms under an automorphism to

$$XZ = Y^2.$$

See [Reid] for more on the equivalence of conics, and quadratic forms, their classification, and the fact that a conic is isomorphic with a projective line.

EXERCISES

EXERCISE A.1. Suppose that four concurrent lines ℓ_1, ℓ_2, ℓ_3 and ℓ_4 in the coordinatized Euclidean plane have slopes m_1, m_2, m_3 and m_4 , respectively. Show that the cross ratio

$$R_X(\ell_1, \ell_2; \ell_3, \ell_4) = \frac{m_1 - m_3}{m_2 - m_3} \bigg/ \frac{m_1 - m_4}{m_2 - m_4}.$$

Hint. Use Exercise 5.8.

EXERCISE A.2. Consider the four points $A = (1, 0)$, $B = (-1, 0)$, $C = (0, 1)$, $D = (0, -1)$ in the Euclidean plane, and a variable point $P = (x, y)$ such that

$$R_X(PA, PB; PC, PD) = -1.$$

Compute the locus of points satisfying this equation.

EXERCISE A.3. Refer to Exercise 5.12 and Figure 5.14. Let ℓ be a secant line through P and intersecting circle C at Z and W .

- a) Prove that if $Y = A_1A_2.\ell$, then $H(Z, W; Y, P)$.
- b) Prove that $\angle XBA_1$ is a right angle.

EXERCISE A.4. Let A, B, C be distinct points on a conic Γ . Let a, b, c be tangents of Γ at A, B, C , respectively. Show that $AB.c$, $AC.b$ and $BC.a$ are collinear.

Hint. Apply Chasles' Theorem.

EXERCISE A.5. Given a polarity, a line ℓ , and $A \in \ell$, associate to A the point $A' = a.\ell$. Show that $A \mapsto A'$ defines an involution of ℓ (cf. Exercise 6.7).

EXERCISE A.6. Let π be a finite projective plane of order q . Show that the number of conics is $q^5 - q^2$.

Appendix B

Algebraic Curves and Bezout's Theorem

An *algebraic curve* in the affine plane $\mathbb{A}^2(\mathbb{R})$ is the locus of points (x, y) satisfying a polynomial equation in two variables and real coefficients.

$$f(x, y) = 0.$$

Algebraic curves we have seen so far include points, $(x - a)^2 + (y - b)^2 = 0$; lines, $ax + by + c = 0$; triangles, $(ax + by + c)(a'x + b'y + c')(a''x + b''y + c'') = 0$; and conic sections, $ax^2 + by^2 + cxy + dx + ey + f = 0$ (with certain *degenerate conics* occurring for some choices of a, b, \dots, f).

Algebraic curves we have not yet seen include *elliptic curves*, a cubic curve of the form

$$y^2 = f(x) := x^2 + ax^2 + bx + c,$$

where the roots of $f(x)$ are distinct (complex) numbers. It has recently been shown that Fermat's Last Theorem, which the reader may know to be actually a long-standing conjecture about the triviality of the set of rational solutions to the equation,

$$x^n + y^n = 1,$$

where integer $n \geq 3$, may be reduced to a plausible conjecture about the group of rational points on an elliptic curve with rational coefficients: for further information, see [Silverman-Tate] and [Rubin-Silverberg].

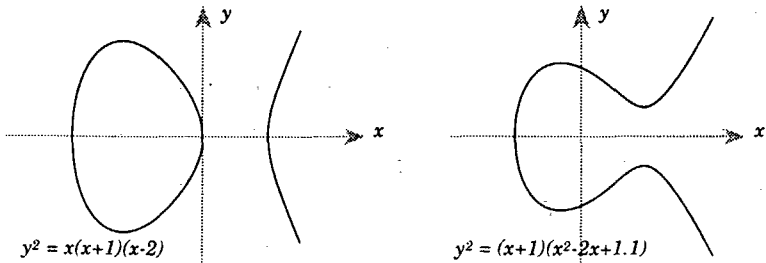


Figure B.1. Two elliptic curves.

Naturally, there are many other algebraic curves, $f(x, y) = 0$, of higher degree, the *degree* being defined to be the highest sum of powers $i + j$ present among the monomial $x^i y^j$ occurring in $f(x, y)$.

In the projective plane $\mathbb{P}^2(\mathbb{R})$ there is the corresponding notion of algebraic curve. These are also the zeros of polynomials like in the affine case, just with the difference that the polynomials be homogeneous polynomials of three variables in order to assume consistency with the definition of point as a line in \mathbb{R}^3 through $(0, 0, 0)$. A polynomial $F(X, Y, Z)$ is called a *homogeneous polynomial of degree d* if and only if F satisfies for each t

$$F(tX, tY, tZ) = t^d F(X, Y, Z).$$

This implies that $F(X, Y, Z)$ be a sum of monomials $X^i Y^j Z^k$ where $i + j + k = d$, d fixed. Define then a *projective algebraic curve of degree d* as the locus of points with homogeneous coordinates (X, Y, Z) such that

$$F(X, Y, Z) = 0.$$

An algebraic curve in $\mathbb{P}^2(\mathbb{R})$, say $F(X, Y, Z) = 0$, corresponds to an affine algebraic curve, $f(x, y) = 0$, by *dehomogenization* (with respect to a variable, say Z), a process you will recognize from switching a line to its affine coordinate equation. One simply sets $Z = 1$, letting $f(x, y) = F(x, y, 1)$. For example, the conic $X^2 + Y^2 - Z^2 = 0$ takes either the form of a circle, $x^2 + y^2 = 1$, or of a hyperbola, $x^2 - z^2 = -1$, if we dehomogenize with respect to Y .

It can happen that much information is lost in dehomogenization. In an extreme example, $F(X, Y, Z) = Z = 0$ should dehomogenize to $1 = 0$, which should be interpreted as the line at infinity of the affine plane $Z \neq 0$. So we need to think of the affine curve corresponding to a projective curve as the curve $F(x, y, 1) = 0$ together with the ideal points $(X, Y, 0)$ satisfying $F(X, Y, 0) = 0$. For example, $F(X, Y, Z) = X^2 - Y^2 + Z^2 = 0$ dehomogenizes to the affine algebraic curve $f(x, y) = x^2 - y^2 + 1$ together with the ideal points $(1, \pm 1, 0)$.

To an affine algebraic curve

$$f(x, y) = \sum a_{ij} x^i y^j = 0$$

of degree d , we make correspond the projective curve

$$F(X, Y, Z) = \sum a_{ij} X^i Y^j Z^{d-i-j} = 0.$$

This correspondence is called *homogenization* and is clearly inverse to dehomogenization in the sense that a one-to-one correspondence is set up between affine and projective algebraic curves that do not contain the line $Z = 0$.

It may be of great value to transform one algebraic curve of degree d to another by a projective collineation. For example, the curve

$$C: X^2 + 2Y^2 + 3Z^2 + 2XY + 2XZ + 4YZ = 0$$

transforms to $(X')^2 + (Y')^2 + (Z')^2 = 0$, which clearly has no solutions: since projective collineations — in fact we used $X' = X + Y + Z$, $Y' = Y + Z$, $Z' = Z$ — are invertible, we conclude there is no solution to the first equation, either.

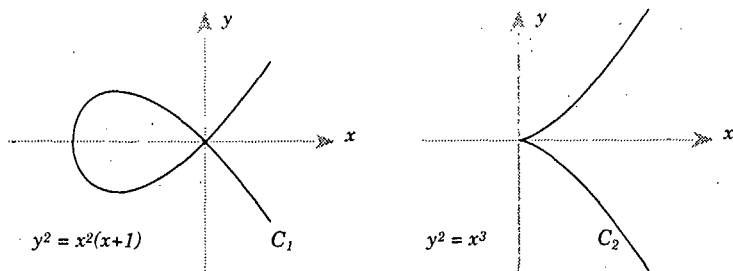


Figure B.2. Singularities at $(0, 0)$.

The curves above, $C_1: y^2 - x^3 - x^2 = 0$ and $C_2: y^2 - x^3 = 0$, as well as their homogenizations $\tilde{C}_1: Y^2Z - X^3 - X^2Z = 0$ and $\tilde{C}_2: Y^2Z - X^3 = 0$, are said to have *singularities* at the point $(0, 0)$ or $(0, 0, 1)$, because all their partial derivatives vanish at these points. For example,

$$\left. \frac{\partial}{\partial Y}(Y^2Z - X^3 - X^2Z) \right|_{(0,0,1)} = 2YZ|_{(0,0,1)} = 0.$$

An algebraic curve with no singularities is said to be *smooth*.

Algebraic curves may be defined in an entirely similar way over a general field. Smoothness carries over, too, in spite of the seeming use of limit and ϵ - δ arguments with a notion of distance implicit. Since we deal only with polynomials, we can define partial differentiation formally by $\frac{\partial}{\partial X} X^n Y^i Z^j = nX^{n-1} Y^i Z^j$, etc.

B.1 Intersection Theory of Algebraic Curves

We can now investigate how many points of intersection there are between two projective algebraic curves of degree m and n . If $m = n = 1$ and the lines are different, we know there is only one answer (unlike the affine case): one point.

If $m = 1$ and $n = 2$, we can run into the following difficulty: if $C_1: X - Y = 0$ and $C_2: X^2 - Y^2 = 0$, then $C_1 \cap C_2$ contains an infinite number of points — in fact, the whole curve C_1 . Indeed C_2 is the union of two lines, one of them being C_1 . The way to circumvent such a nuisance is to remark that, like unique factorization of integers into primes, polynomials may be factored into irreducible polynomials (of degree 1 or more, and homogeneous in the projective case). For example, $X^2 - Y^2 = (X + Y)(X - Y)$. We now insist that we look only at pairs of curves with no common component, i.e., no one polynomial occurs in both factorizations into irreducible polynomials.

Now another obvious occurrence when $m = 2$ and $n = 1$ is that the line and conic might miss one another entirely. For example $C_1: X^2 + Y^2 - Z^2 = 0$ and $C_2: X - 3Z = 0$. Although $C_1 \cap C_2$ contain no real points, if we allow complex solutions, i.e., we consider C_1 and C_2 as curves in $\mathbb{P}^2(\mathbb{C})$, then we get two solutions, viz. $(3, \pm i\sqrt{8}, 1)$.

Yet another sort of example is the following: $C_1: Y - Z = 0$ and $C_2: X^2 + Y^2 - Z^2 = 0$. This is a circle and one of its tangent lines when we homogenize with respect to Z . It is certain that $C_1 \cap C_2 = \{(0, 1, 1)\}$, but perhaps $(0, 1, 1)$ should count twice! After all, if we substitute $Y - Z = 0$ in $X^2 + (Y - Z)(Y + Z) = 0$, we get $X^2 = 0$, and we would say $X = 0$ is a root of multiplicity 2 (i.e., also a root of the derived polynomial). Multiplicity in intersection theory is captured by the notion of intersection multiplicity at a common point P , denoted by $I(C_1 \cap C_2, P)$. Its definition is technical, involving rings called local rings, and postponed until the exercises where we look only at the affine plane: a highly recommended reference for beginners is [Silverman-Tate, appendix A].

Let it suffice to say that $I(C_1 \cap C_2, P) = 1$ if C_1 and C_2 intersect transversally at P . In affine terms, this means that P is a nonsingular point for both curves and their tangents span the plane as in Figure B.3.

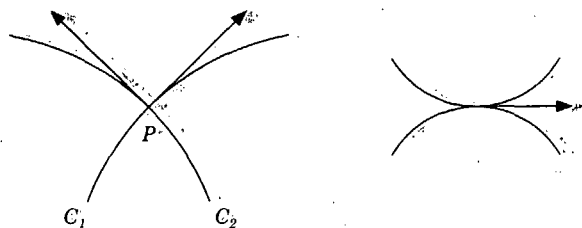


Figure B.3: Left: Transversal intersection. Right: non-transversal intersection.

We are now ready to state the definitive theorem, in the subject, Bezout's Theorem for real algebraic curves viewed in $\mathbb{P}^2(\mathbb{C})$.

THEOREM B.1 (BEZOUT'S THEOREM). *Let C_1 and C_2 be projective algebraic curves with no common components. Then*

$$\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (\deg C_1)(\deg C_2).$$

In particular, if C_1 and C_2 are smooth with only transversal intersections, then $\#(C_1 \cap C_2) = (\deg C_1)(\deg C_2)$. In all other cases,

$$\#(C_1 \cap C_2) \leq (\deg C_1)(\deg C_2).$$

A proof of Bezout's Theorem has been broken into a series of easy exercises in [Silverman-Tate]: we recommend the student focus in this project on the meaning of Bezout's Theorem, its proof, its applications, and its history. The student should see [Reid] for a special proof of Bezout's Theorem in case $\deg C_1 = 2 = \deg C_2$.

Bezout's Theorem is very powerful. For example, let us apply it to two curves C_1 and C_2 both of degree 2. If we moreover suppose that both are conics and have five points in common, no three of which are collinear, then Bezout's Theorem tells us that $C_1 = C_2$. Moreover, it is possible to prove the following theorem when $d_1 = d_2 = 3$ using an argument that identifies the set of cubic curves with $\mathbb{P}^9(\mathbb{R})$ (see [Silverman-Tate]).

THEOREM B.2 (BACHARACH-CAYLEY THEOREM). *Let C_1 and C_2 be projective algebraic curves of degrees d_1 and d_2 , without common components. Suppose that C_1 and C_2 intersect in d_1d_2 points. Let \mathcal{D} be a projective algebraic curve of degree $d_1 + d_2 - 3$. If \mathcal{D} passes through $d_1d_2 - 1$ points of $C_1 \cap C_2$, then it passes also through the remaining point of $C_1 \cap C_2$.*

Let us apply the Bacharach-Cayley Theorem and Bezout's Theorem to prove (one half of) Pascal's Theorem. The following proof would in principle be valid in $\mathbb{P}^2(\mathbb{F})$ for any field \mathbb{F} (of characteristic $\neq 2$) since we can replace \mathbb{R} and \mathbb{C} with \mathbb{F} and its algebraic closure¹ in the statement and proof of Bezout's Theorem and the Bacharach-Cayley Theorem.

THEOREM B.3 (PASCAL'S THEOREM). *Let C be a smooth conic and A, B, C, D, E, F six distinct points on C . Let $A = AB.DE$, $R = BC.EF$ and $S = CD.AF$. Then Q , R and S are collinear.*

Demonstration. Consider the cubic curves (not irreducible!) $C_1 = \overline{AB} \cup \overline{CD} \cup \overline{EF}$ and $C_2 = \overline{BC} \cup \overline{DE} \cup \overline{AF}$. All nine points $A, B, C, D, E, F, Q, R, S$ lie on C_1 and C_2 . Let C_3 be the cubic curve defined by

$$C_3 = C \cup \overline{QR}.$$

¹see [Kaplansky, p. 74-76] for a proof that any field \mathbb{F} has an algebraic closure in which degree n polynomials all factor into linear factors.

Now C_3 contains eight of the points above; viz., A, B, C, D, E, F, Q and R . By the Bacharach-Cayley Theorem, C_3 contains S , too. Where on C_3 is S ? If $S \in C$, the line AF intersects C in three distinct points in contradiction of Bezout's Theorem. We conclude that $S \in QR$, demonstrating collinearity.

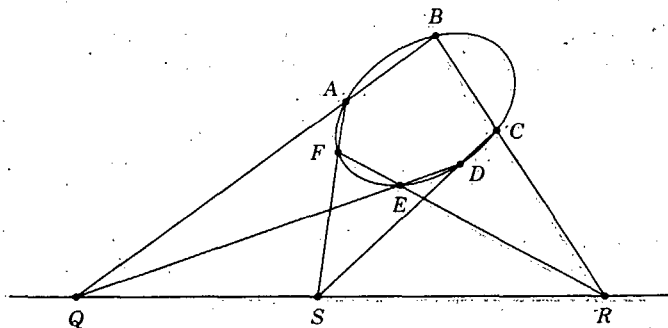


Figure B.4. Pascal's Theorem.

EXERCISES

EXERCISE B.1. Find the well-known formula for solution x of $Ax^2 + Bx + C = 0$ by applying a projective transformation (projectivity) of the projective line.

Hint. Multiply by $4A$ and complete the square.

EXERCISE B.2. Let R be a ring. An ideal I in R is a set such that

$$\text{I1. } x, y \in I \implies x - y \in I.$$

$$\text{I2. } x \in R, y \in I \implies xy \in I \text{ and } yx \in I.$$

Check that

- a) I is a ring in itself, though possibly without 1.
- b) I is a normal subgroup in R under $+$.

c) The set of cosets R/I gets a well-defined multiplication as follows:

$$(a + I)(b + I) = ab + I.$$

d) R/I is a ring.

e) If $f: R \rightarrow S$ is a homomorphism of rings, which is surjective, then $\text{Ker}(f)$ is an ideal in R .

f) $R/\text{Ker}(f) \cong S$.

EXERCISE B.3. Let R be a commutative ring. A subset T of R is said to be *multiplicative* if $1 \in T$ and $a, b \in T$ implies $ab \in T$. An ideal P in R is said to be a *prime ideal* if $ab \in P$ implies $a \in P$ or $b \in P$. Show that

a) P is a prime ideal if and only if $R - P$ is a multiplicative set.

b) If R is the ring of integers, ideals are of the form $(n) = \{nq \mid q \in \mathbb{Z}\}$, and prime ideals of the form (p) , p a prime number.

EXERCISE B.4. This exercise generalizes an earlier exercise on forming the field of fractions. Given a multiplicative subset T of a ring R , we form the *ring of fractions* of R by T as follows. In $R \times T$ define a relation by

$$(r, t) \sim (r', t')$$

if there exists an element t_1 in T such that

$$t_1(t'r - tr') = 0.$$

a) Check that \sim is an equivalence relation.

b) Denote the equivalence class of (r, t) by $\frac{r}{t}$, and the set of these by R_T . Define a multiplication in R_T by

$$\left(\frac{r}{t}\right) \left(\frac{r'}{t'}\right) = \frac{rr'}{tt'}.$$

Check that multiplication is independent of representative chosen for the equivalence class.

c) Define addition in R_T by the rule

$$\frac{r}{t} + \frac{r'}{t'} = \frac{t'r + tr'}{tt'}.$$

Check that addition is well-defined and R_T is a ring.

d) Check that the mapping $f: R \rightarrow R_T, r \mapsto r/1$ is a homomorphism.

e) Let S be another multiplicative subset of R and $S \subseteq T$. Define a natural mapping $R_S \rightarrow R_T$.

EXERCISE B.5. An ideal M in a commutative ring R is said to be *maximal* if K ideal, $M \subset K \subset R$ implies $K = M$ or $K = R$.

a) Prove that if M is a maximal ideal, then M is a prime ideal.

b) R/M is a field.

c) P is a prime ideal if and only if R/P has no zero divisors.

d) One can form the ring of fractions of R by $R - M$, which is traditionally denoted by R_M .

e) If $R = \mathbb{F}[X, Y]$, $P = (X) = \{Xf \mid f \in R\}$, $M = (X, Y) = \{Xf_1 + Yf_2 \mid f_1, f_2 \in R\}$, then P is prime but not maximal and M is maximal.

Let $C_1: f_1(x, y) = 0$ and $C_2: f_2(x, y) = 0$ be two affine algebraic curves with no common factor. So $f_1, f_2 \in \mathbb{F}[x, y]$, the polynomial ring over an algebraically closed field \mathbb{F} in two indeterminates. Suppose $P \in C_1 \cap C_2$. Let R be the commutative ring $\mathbb{F}[X, Y]$, which is in fact an integral domain. Form its field of fractions K (denoted by $\mathbb{F}(X, Y)$) and called the *field of rational functions* of X and Y . In R there is a maximal ideal $M(P) = \{f(x, y) \mid f(P) = 0\}$; check this. Then the ring of fractions $R_{M(P)} := \mathcal{O}_P$ is called the *local ring* of P .

Check that \mathcal{O}_P is a subring of K via the map you defined in B.4e. Check that the map

$$\frac{f(x, y)}{g(x, y)} \mapsto \frac{f(P)}{g(P)}$$

defines a homomorphism of \mathcal{O}_P onto \mathbb{F} with kernel

$$M_P := \left\{ \frac{f}{g} \in \mathcal{O}_P \mid \frac{f(P)}{g(P)} = 0 \right\}.$$

Now let (f_1, f_2) be the ideal in \mathcal{O}_P generated by $f_1/1$ and $f_2/1$ in \mathcal{O}_P : i.e.

$$(f_1, f_2) = \left\{ \frac{f_1 f}{g} + \frac{f_2 f'}{g'} \mid f, f' \in R, g, g' \in R - M(P) \right\}.$$

The intersection multiplicity of C_1 and C_2 at P is

$$I(C_1 \cap C_2, P) = \dim \left(\frac{\mathcal{O}_P}{(f_1, f_2)} \right)$$

where the right hand side is just the dimension of a vector space, since the field \mathbb{F} acts like scalars.

EXERCISE B.6. Compute $I(C_1 \cap C_2, P) = 1$ where $C_1: x = 0$, $C_2: y = 0$ and $P = (0, 0)$.

Appendix C

Elliptic Geometry

Euclidean geometry has taught us that planar geometry is especially fertile in the presence of a notion of distance between points and an angle between lines. You will recall some of the important theorems in Euclidean geometry: the Law of Cosines, the Law of Sines, and the theorem which states that the sum of interior angles of a triangle is π radians. For the convenience of the reader we state these theorems in equations (C.1) and (C.2) below:

$$(C.1) \quad \text{Law of Cosines: } a^2 = b^2 + c^2 - 2bc \cos A$$

$$(C.2) \quad \text{Law of Sines: } \frac{\sin A}{a} = \frac{\sin B}{b} = \frac{\sin C}{c}$$

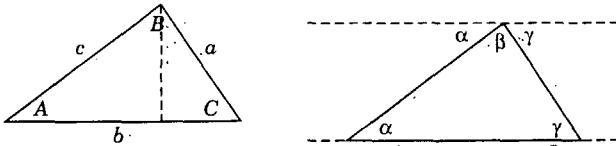


Figure C.1. Left: Angles and lengths of general triangle. Right: $\alpha + \beta + \gamma = \pi$.

The real projective plane has a respectable distance geometry on it as well: it is essentially the spherical geometry of the everyday experience of airline pilots! We use the sphere model of the real projective plane, denoted by P^2 in this appendix. Let S^2 be the unit sphere in

\mathbb{R}^3 centered at the origin O . A point P in P^2 stands for a set of two antipodal points, $\pm P$, in S^2 . A line ℓ in P^2 is a great circle on S^2 .

The distance between two points P and Q in P^2 is defined to be the acute angle in radians between lines OP and OQ :

$$d(P, Q) = \arccos |P \cdot Q|.$$

Angles between lines is convertible to distance between points by a choice of polarity (or what is equivalent, a conic or nondegenerate quadratic form). Now the coordinates suggest a natural choice for the polarity: send point

$$(A, B, C) \mapsto \text{line } \ell: Ax + By + Cz = 0.$$

Inversely, a line or great circle on S^2 is sent to its "north-south pole:" the great circle through P and Q is sent to $P \times Q$. Then the angles between two lines a and b is the distance $d(A, B)$ between its poles. As a consequence the polar of a triangle XYZ with lengths a, b, c and angle measures α, β, γ is the triangle xyz with lengths α, β, γ and angle measures a, b, c .

We are going to derive the Law of Cosines and the Law of Sines for elliptic geometry and indicate in the exercises what the sum of internal angles is in a triangle. We will note the Law of Sines to be one instance of the great theorem of J. Bolyai (1802–1860). In his work on absolute geometry J. Bolyai states the following theorem for a general triangle in the spherical, Euclidean or hyperbolic planes (notation as in Figure C.1, left):

$$\frac{\sin A}{\odot a} = \frac{\sin B}{\odot b} = \frac{\sin C}{\odot c},$$

where $\odot r$ denotes the arclength of a circle of radius r in each geometry ($2\pi \sin r$, $2\pi r$ and $2\pi \sinh r$, respectively).

We suggest the following project: research the statement, history and proof of J. Bolyai's Sine Law, and then look at modern treatments such as the unified proof in [Hsiang]. We recommend [Ryan] for a modern textbook treatment of the basics of the Euclidean, spherical, elliptic and hyperbolic planes.

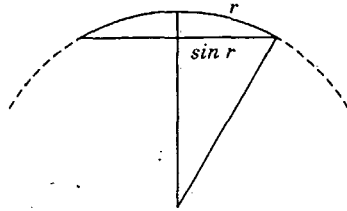


Figure C.2. Arc length $\odot r = 2\pi \sin r$ on sphere.

THEOREM C.1 (LAW OF COSINES). For an elliptic triangle ABC with sides of length a, b, c and angle measures α, β, γ the following equation holds:

$$(C.3) \quad \cos a = \cos b \cos c + \sin b \sin c \cos \alpha$$

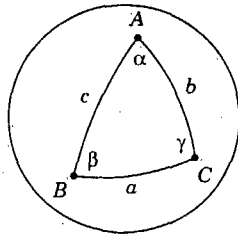


Figure C.3. A geodesic triangle on the sphere.

Proof. Do Exercises C.1, C.2 and C.3 in order to establish the following advanced identity from vector analysis:

$$(C.4) \quad (C \times A) \cdot (A \times B) = (C \cdot A)(A \cdot B) - (C \cdot B)(A \cdot A).$$

The left-hand side of (C.4) simplifies in three steps:

$$\begin{aligned} \|C \times A\|^2 &= -(C \times A) \cdot (A \times C) = -(C \cdot A)^2 + (C \cdot C)(A \cdot A) \\ &= -\cos^2 b + 1 = \sin^2 b, \end{aligned}$$

so

$$\|A \times B\|^2 = \sin^2 c,$$

so

$$(C \times A) \cdot (A \times B) = -\sin b \sin c \cos \alpha.$$

The right-hand side is just

$$(C \cdot A)(A \cdot B) - (C \cdot B)(A \cdot A) = \cos b \cos c - \cos a,$$

whence (C.3) follows from (C.4). \square

The Law of Cosines in Euclidean geometry may be recovered from equation (C.3) by replacing $\cos x$ with $1 - x^2/2$ and $\sin y$ with y , their second degree Taylor polynomials.

COROLLARY C.2. *For the elliptic triangle above with $\gamma = \pi/2$, the following equations hold:*

$$(C.5) \quad \cos c = \cos a \cos b$$

$$(C.6) \quad \cos \alpha = \sin \beta \cos a$$

$$(C.7) \quad \sin b = \sin c \sin \beta$$

Proof. Note that the Law of Cosines gives three equations for one triangle; one of which is

$$\cos c = \cos a \cos b + \sin a \sin b \cos \gamma.$$

But $\cos \gamma = 0$ when $\gamma = \pi/2$, whence (C.5).

The Law of Cosines applied to the polar triangle gives

$$\cos a = \cos \beta \cos \gamma + \sin \beta \sin \gamma \cos a.$$

But $\sin \gamma = 1$ when $\gamma = \pi/2$, whence (C.6).

Now apply (C.5) to (C.3), using $\cos^2 b = 1 - \sin^2 b$: we get

$$(C.8) \quad \cos a \sin b = \sin c \cos \alpha.$$

Apply (C.6) to (C.8) and cancel to get (C.7). \square

THEOREM C.3 (LAW OF SINES). *For an elliptic triangle (Figure C.4),*

$$\frac{\sin \alpha}{\sin a} = \frac{\sin \beta}{\sin b} = \frac{\sin \gamma}{\sin c}.$$

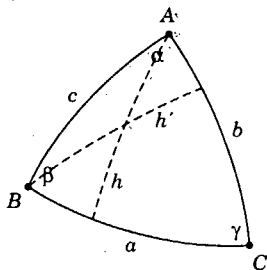


Figure C.4. Elliptic triangle with altitudes.

Proof. Let h be the length of an altitude from A to BC . By the corollary (C.7) we have

$$\sin \gamma \sin b = \sin h = \sin \beta \sin c.$$

Hence,

$$\frac{\sin \gamma}{\sin c} = \frac{\sin \beta}{\sin b}.$$

By dropping an altitude from B of length h' as in Figure C.4, you similarly prove that

$$\frac{\sin \gamma}{\sin c} = \frac{\sin \alpha}{\sin a}. \quad \square$$

C.1 The Incidence Geometry of the Hyperbolic Plane

Already in chapter 2 we saw the incidence geometry of the Euclidean plane embedded in the real projective plane as a subgeometry (cf. Exercise 2.2). In the section just completed we noted that spherical and projective geometry are locally identical — even in their metrical aspect. In this section we will give a simple and brief description of the incidence geometry of the hyperbolic plane as a subgeometry of the real projective plane.¹

¹It was these observations and others in which Arthur Cayley (1821–1895) obtained various metrics from the cross ratio that led him to pronounce with char-

Consider the subgeometry of points and lines within one connected component of a conic in P^2 . One concrete example of such is the set of points $P = (x, y, z) \in P^2$ such that $x^2 + y^2 < 1$ and $z = 1$. Lines in this geometry $\{(x, y, 1) \mid x^2 + y^2 < 1\}$ are simply the line segments satisfying linear equations $ax + by + c = 0$. This is the *Beltrami-Klein model* of the hyperbolic plane H^2 .

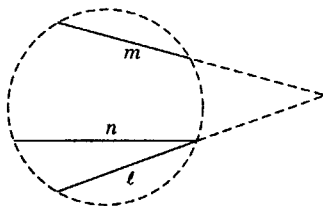


Figure C.5. Klein model: n and ℓ parallel lines; m and ℓ ultraparallel.

It is clear that two points in H^2 determine a unique line through them. Unlike Euclidean and projective geometries, there is not 0 or 1 lines through a point P and parallel to (disjoint with) a line ℓ such that $P \notin \ell$: there are infinitely many lines! We call all such lines $m \ni P$ such that $m \cap \ell = \emptyset$ *ultraparallel* to ℓ , except two; namely, the lines n_1 and n_2 that intersect ℓ on the circle boundary which are said to be *parallel* to ℓ .

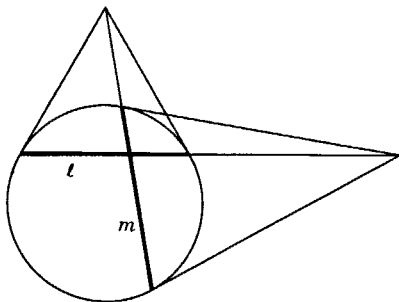


Figure C.6. Perpendicular lines ℓ and m in the Klein model.

acteristic enthusiasm metric geometry to be a part of projective geometry, and projective geometry to be all of geometry.

Figure C.6 below gives a construction for perpendicular lines in H^2 . Otherwise one must exercise caution with the Klein model, since angles and lengths are not faithfully represented. For example, a hyperbolic line has in fact infinite length although it is represented by a finite chord in the Klein model. See [Ryan] for a faithful model of H^2 .

EXERCISES

EXERCISE C.1. Prove that for vectors u, v, w in \mathbb{R}^3 :

$$(u \times v) \times w - u \times (v \times w) = (u \cdot v)w - (v \cdot w)u.$$

Hint. Use Exercise 7.10 and associativity of quaternionic multiplication. Since triple product of vectors is a 3×3 determinant, it follows that $(u \times v) \cdot w = u \cdot (v \times w)$.

EXERCISE C.2. Use the previous exercise to prove that

$$(u \times v) \times w = (u \cdot w)v - (v \cdot w)u.$$

EXERCISE C.3. Use the preceding exercise to prove that

$$(u \times v) \cdot (v \times w) = (u \cdot v)(v \cdot w) - (v \cdot v)(u \cdot w).$$

EXERCISE C.4. Compute the area of a lune of angle α on the sphere, i.e. the shaded region in the figure. Show that the total area of the elliptic plane is 2π .

Hint. Double integration with spherical coordinates.

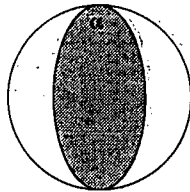


Figure C.7. Lune.

EXERCISE C.5. Show that the area of an elliptic triangle with internal angles α, β, γ is $\alpha + \beta + \gamma - \pi$.

Hint. Use the preceding exercise and the partitioned lunes in the figure below.

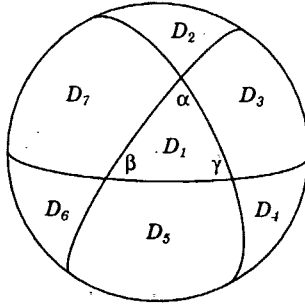


Figure C.8. Partitioned lunes.

EXERCISE C.6. Show that the altitudes of an elliptic triangle are concurrent. Do the same with the medians and angle bisectors of an elliptic triangle.

Hint. Use Theorem 11.9.

Appendix D

Ternary Rings

In chapter 9 we essentially did the following: starting with an affine plane satisfying the minor and major Desargues' Axioms, A4 and A5, respectively, and choosing a line with two preferred points, 0 and 1, we proved the nine axioms of a division ring to be satisfied by the points on ℓ with operations \cdot and $+$. Coordinatizing the projective plane with axiom P5 by a division ring turned out later to be a detail in this campaign.

In this appendix we are going to do the same thing to an affine plane *without* axioms A4 and A5. We can no longer resort to translations and central dilatations for our definitions of addition and multiplication. We will see what algebraic conditions axioms A1–A3 lead to on a ternary ring — an algebraic structure on the set of points on a “diagonal” line, consisting of a ternary operation with several properties and from which limited notions of addition and multiplication may be recovered. Conversely, ordered pairs of coordinates from a ternary ring with lines defined by the ternary operation form an affine plane. Then we take up the interesting question of what extra conditions on the ternary ring of an affine plane axiom A4 alone imposes. Indeed, as we add stronger axioms that converge to A5, we expect to see the ternary ring converge to a division ring.

The project we suggest in this appendix is to expand on what is presented and experiment with geometric axioms and their algebraic conditions on a ternary ring, or the converse. You might add to your

project by doing a small amount of scholarly investigation in the literature. The ternary ring is due to the 20th century American mathematician Marshall Hall: our source is [Blumenthal].

Let \mathbb{A} be an affine plane. (We are assuming only axioms A1, A2, A3 listed in chapter 1.) We proceed to give \mathbb{A} coordinates from a ternary ring in several steps.

1) Select any point in \mathbb{A} and label it O : call O the *origin*.

2) Using axiom A3 and A2, we can show that there exist three distinct lines through O . Choose one and call it the *x-axis*, another to call the *y-axis*, and a third to call the *diagonal*.

3) On the diagonal select a point I different from O . Refer to I as the *unit point*.

4) Let Γ be an abstract set in one-to-one correspondence with the set of points on the diagonal. We adopt the convention that points are given capital letters, and, if the points is on OI , the corresponding element in Γ is the same letter in small case. The two exceptions are O and I to which we make $0, 1 \in \Gamma$ correspond.

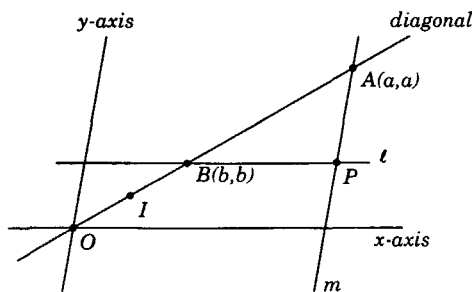


Figure D.1. Assigning coordinates to P . ($\ell \parallel x$ -axis, $m \parallel y$ -axis.)

5) Let A denote any point on the diagonal, OI . We assign to A the coordinates (a, a) : to O and I , we assign $(0, 0)$ and $(1, 1)$, respectively.

6) Let P be a point in \mathbb{A} , not on OI . By A2 there is a unique line through P and parallel to the *x-axis*. This line must intersect OI at some point. let us say B . Again, there is a line through P and parallel to the *y-axis*: this must intersect the diagonal at a point A . Assign to P

the coordinate (a, b) . This is an unequivocal assignment of coordinates in a bijective correspondence between $\Gamma \times \Gamma$ and A .

7) We assign a slope and y -intercept to each line ℓ not parallel to the y -axis. Call the unique line through I and parallel to the y -axis the *line of slopes*. Let ℓ' be parallel to ℓ and passing through O . ℓ' will intersect the line of slopes, say at $(1, m)$. We assign to ℓ the slope $m \in \Gamma$. In addition, ℓ will intersect the y -axis, say at the point $(0, b)$; b is called the *y -intercept* of ℓ . Note that b and m uniquely determine a line through $(0, b)$ and parallel to the join of O and $(1, m)$; indeed, the line of slope m and y -intercept b .

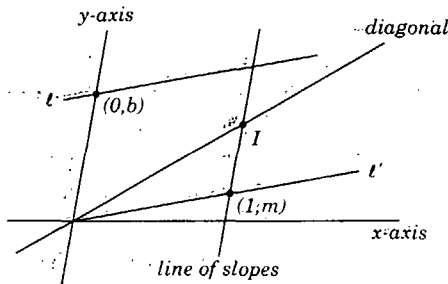
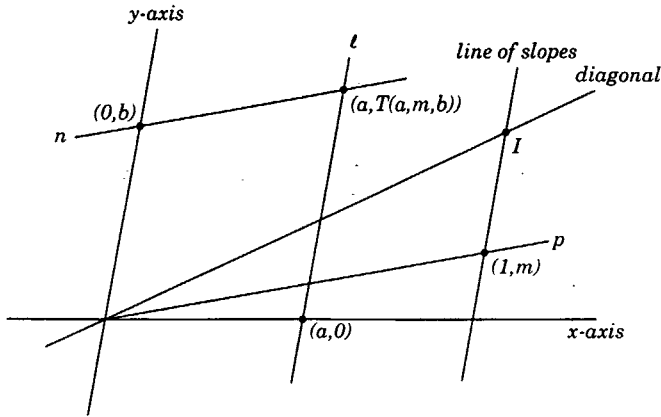


Figure D.2. Slope and y -intercept of a line in A .

8) To each ordered triple, $(a, m, b) \in \Gamma \times \Gamma \times \Gamma$, we are going to assign a unique element $T(a, m, b)$ of Γ . This will define a ternary ring (Γ, T) , i.e. a set Γ with ternary operation $T: \Gamma \times \Gamma \times \Gamma \rightarrow \Gamma$ satisfying five properties, T1-T5 below.

The definition of $T(a, m, b)$ is very simple. Consider the line with slope m and y -intercept b : call it n . Let ℓ be the line through $(a, 0)$ and parallel to the y -axis. Since n has a slope it is not parallel to the y -axis and will intersect ℓ at a point: the point will have coordinates of the form (a, y) . Assign $T(a, m, b) = y$.

Note that an arbitrary point $P(x, y)$ lies on n if and only if the equation $y = T(x, m, b)$ is satisfied. Thus $y = T(x, m, b)$ is an equation of the line with slope m and y -intercept b . (A line parallel to the y -axis has equation of the form $x = a$.)

Figure D.3. Defining the ternary operation. ($p \parallel n$.)

DEFINITION 1. A (planar) *ternary ring* (Γ, T) is a set $\Gamma = \{0, 1, a, b, c, \dots\}$ together with a mapping $T: \Gamma \times \Gamma \times \Gamma \rightarrow \Gamma$ such that T1-T5 are satisfied:

T1. For all $a, b, c \in \Gamma$,

$$T(0, b, c) = T(a, 0, c) = c.$$

T2. For all $a \in \Gamma$,

$$T(a, 1, 0) = T(1, a, 0) = a.$$

T3. If $m, m', b, b' \in \Gamma$ and $m \neq m'$, then the equation

$$T(x, m, b) = T(x, m', b')$$

has a unique solution in Γ .

T4. If $a, a', b, b' \in \Gamma$, $a \neq a'$, the system of equations

$$\begin{aligned} T(a, x, y) &= b \\ T(a', x, y) &= b' \end{aligned}$$

has a unique solution.

T5. For all $a, m, c \in \Gamma$, the equation

$$T(a, m, x) = c$$

has a unique solution.

EXAMPLE 1. The set Γ with ternary operation defined in steps (1)–(8) is a ternary ring. T1 and T2 are special cases for the lines n or ℓ . T3 is equivalent to the proposition that lines are either parallel (and have the same slope) or intersect in precisely one point. T4 is equivalent to Axiom A1: through the distinct points (a, b) and (a', b') there is one and only one line ℓ of slope x and intercept y . T5 is equivalent to Axiom A2: there is a unique line through (a, c) and parallel to OM where $M = M(1, m)$. Our use of the word “equivalent” is not an accident: a ternary ring (Γ, T) defines on $\Gamma \times \Gamma$ an affine plane with lines given by $\{(x, y) \mid x = a\}$ and $\{(x, y) \mid y = T(x, m, b)\}$ ($\forall m, b \in \Gamma$). You will then be able to prove A1–A3 by reversing the reasoning above.

EXAMPLE 2. A division ring $(R, +, \cdot, 0, 1)$ is a ternary ring. Define $T(a, m, b) = a \cdot m + b$. You should now check that properties T1–T5 are satisfied.

We continue by defining some limited notions of addition and multiplication.

D.1 Addition

We define a binary operation $\Gamma \times \Gamma \rightarrow \Gamma$ we call *addition* and denote it simply by $(a, b) \mapsto a + b$. Define $a + b = T(a, 1, b)$. Figure D.4 below indicates how addition works on the diagonal.

DEFINITION 2. A *loop* is a set Λ with preferred element 0 , and binary operation \odot such that properties L1 and L2 are satisfied.

L1. $a \odot 0 = a = 0 \odot a \quad (\forall a \in \Lambda)$

L2. $a \odot b = c$ uniquely determines any one of $a, b, c \in \Lambda$ whenever the other two are given.

REMARK. There is a slight redundancy in the definition of loop: where is it? Examples of a loop are $(\Gamma, +, 0)$ and any group (G, \cdot, e) .

Although $(\Gamma, +, 0)$ is a loop it is generally neither true that it is a group nor that $+$ is a commutative operation. It is a fact that in the presence of the minor Desargues' Axiom $(\Gamma, +, 0)$ is an abelian group.

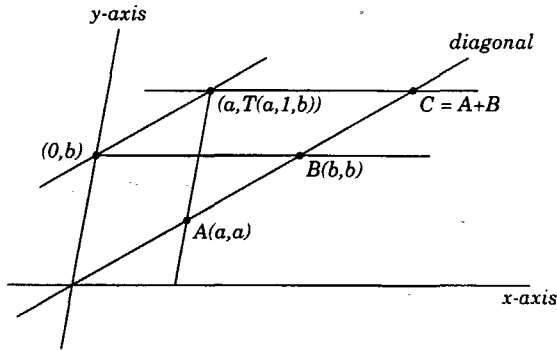


Figure D.4. Addition of diagonal points.

D.2 Multiplication

We define a binary operation on Γ called *multiplication* and denoted by $(a, b) \mapsto a \cdot b$. Define $a \cdot b = T(a, b, 0)$. Figure D.5 below gives the resulting construction of multiplication on the diagonal.

Now show that

- 1) $(\Gamma - \{0\}, \cdot, 1)$ is a loop.
- 2) $A \cdot B = 0$ if and only if $A = 0$ or $B = 0$ ($A, B \in OI$).

REMARK. We now have simple equations for certain lines in \mathbb{A} : $y = x + b$, $y = x \cdot m$, $y = b$, $x = a$. (Notice the change in left-right convention from chapters 8 and 9.) It is in general not true that $T(x, m, b) = x \cdot m + b$. This would be equivalent to the equation

$$T(x \cdot m, 1, b) = T(x, m, b).$$

If such is the case for all ordered triples, T is said to be *linear*. Another outcome of assuming A4 is that T is linear.

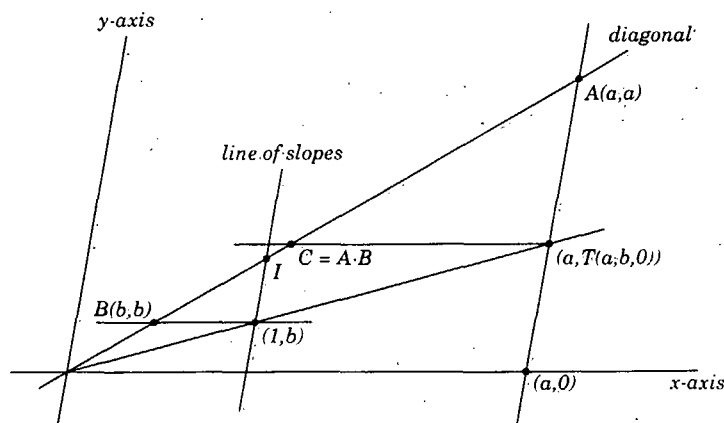


Figure D.5. Multiplication of diagonal points.

The next theorem requires a brief definition and example to precede it. You will be required to supply its proof with the help of the Exercises D.2-D.4.

DEFINITION 3. A ternary ring (Γ, T) is called a *Veblen-Wedderburn system* if and only if

VW1. $(\Gamma, +, 0)$ is an abelian group.

VW2. $(\Gamma - \{0\}, \cdot, 1)$ is a loop.

VW3. $a \cdot 0 = 0 \cdot a = 0$ ($\forall a \in \Gamma$).

VW4. Right distributivity: $(a + b) \cdot c = a \cdot c + b \cdot c$ (for all $a, b, c \in \Gamma$).

EXAMPLE. Consider an 8-dimensional real vector space with basis $\{1 = e_1, e_2, \dots, e_8\}$. We will define the non-associative algebra of octonions \mathcal{O} on this vector space. Introduce multiplication on the basis elements by letting $1e_i = e_i = e_i1$ for $i = 1, \dots, 8$, $e_i^2 = -1$ for $i \geq 2$,

and $e_i e_j = -e_j e_i$ for $1 < i < j \leq 8$. We also define

$$\begin{aligned} e_2 e_3 &= e_4, & e_2 e_5 &= e_6, & e_3 e_5 &= e_7, & e_4 e_5 &= e_8, \\ e_6 e_4 &= e_7, & e_7 e_2 &= e_8, & e_8 e_3 &= e_6, \end{aligned}$$

with 14 more relations gotten by permuting indices, i.e. if $e_i e_j = e_k$ we require $e_j e_k = e_i$ and $e_k e_i = e_j$. Multiplication between general octonions is obtained by using both distributive laws and now letting the real numbers commute. The following is a mnemonic scheme for octonionic multiplication.

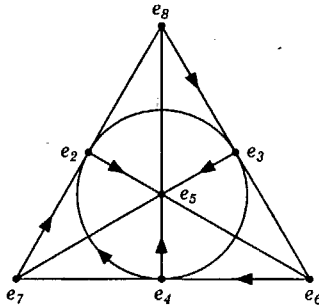


Figure D.6. Diagram for octonionic multiplication.

The octonions are an example of a Veblen-Wedderburn system. (Why?)

THEOREM D.1. *An affine plane \mathbb{A} satisfies A_4 , the minor Desargues' Axiom, if and only if $\mathbb{A} \cong \Gamma \times \Gamma$, where lines are given $x = a$ and $y = T(x, m, b)$, and (Γ, T) is a Veblen-Wedderburn system.*

EXERCISES

EXERCISE D.1. Give a synthetic proof for the existence of an affine plane of nine points $\{A, B, C, \dots, I\}$. Coordinatize with $P = \{0, 1, 2\}$. Assign slopes to each line ABC , etc. Evaluate $T(2, 2, 2)$, $T(1, 2, 1)$ and

$T(2, 1, 1)$. Write equations for several lines. Does $T(x, m, b) = x \cdot m + b$ in this example?

EXERCISE D.2. Does the Moulton plane satisfy A4?

Define a *vector* in \mathbb{A} by an ordered pair \overline{AB} . Line AB is the carrier of the vector \overline{AB} . If $A = B$, \overline{AB} is a *null*. Define a relation \simeq among vectors as follows:

$$\overline{AB} \simeq \overline{CD} \quad \text{iff} \quad \begin{cases} B = A_1 \iff C = D_1, \text{ or} \\ A = C \iff B = D, \text{ or} \\ AB \parallel CD \text{ and } AC \parallel BD. \end{cases}$$

EXERCISE D.3. Show that \simeq is a symmetric and reflexive relation. Show \simeq is a transitive relation if and only if A4 holds in \mathbb{A} .

Let \overline{AB} and \overline{CD} be two vectors (now assumed to be equivalence classes of \simeq). Define an addition as follows: if $B = C$, $\overline{AB} + \overline{CD} = \overline{AD}$. If $B \neq C$, and Q denotes the unique point such that $\overline{BQ} \simeq \overline{CD}$ (in the presence of A4), then $\overline{AB} + \overline{CD} = \overline{AQ}$.

EXERCISE D.4. Show that the set of vectors is an abelian group under $+$. Show by these means, or by means of translations, that $(\Gamma, +, 0)$ is an abelian group.

EXERCISE D.5. Show that, in the presence of A4, the ternary operator T is linear.

EXERCISE D.6. Show that, in the presence of A4, multiplication is right-distributive over addition. Complete the remaining steps in the proof of the (Veblen-Wedderburn) Theorem.

EXERCISE D.7. Let \mathbb{F} be the field of nine elements in Exercise 7.8. Let $\mathbb{A} = \mathbb{F}$ as sets. Prove that \mathbb{A} is a Veblen-Wedderburn system if the ternary operation is defined by

$$T(a, m, b) = \begin{cases} am + b & \text{if } m \text{ is a square in } \mathbb{F} \\ a^3m + b & \text{if } m \text{ is not a square in } \mathbb{F} \end{cases}$$

The right-hand side should be interpreted as operations in the field \mathbb{F} . A square y in \mathbb{F} has $z \in \mathbb{F}$ such that $y = z^2$. Prove that $(\mathbb{A} - \{0\}, \cdot, 1)$ is in fact a group.

EXERCISE D.8. Define a projective plane over \mathbb{A} in the preceding exercise. (denote it by $\mathbb{P}_{\mathbb{A}}^2$) Show that Desargues' Theorem does not hold in $\mathbb{P}_{\mathbb{A}}^2$: an example of a finite non-Desarguesian plane.

EXERCISE D.9. Give coordinates to a general projective plane.

Bibliography

[Bell]

Eric T. Bell. *Men of Mathematics*. Simon and Schuster. New York, 1965.

Biographies of Pascal, Poncelet, Lobatchevsky and others:

[Blumenthal]

L.M. Blumenthal. *A Modern View of Geometry*. Dover Publications, 1980:

Clear exposition of the basic postulational systems in geometry, including ternary rings and non-Euclidean geometry.

[Coxeter]

H.M.S. Coxeter. *Projective Geometry*. Springer Verlag, 1987.

Synthetic projective geometry, with several chapters on polarity and conics.

[Dörrie]

H. Dörrie. *100 Great Problems of Elementary Mathematics*. Dover Publications, New York, 1965:

The development of projective geometry and geometry in general can be traced here from a realistic problem-oriented viewpoint.

[Frankild-Kromann]

Anders Frankild and Matthias T. Kromann. Projektiv geometri og quaterniongeometri. NATBAS Preprint series, Roskilde University, 1993.

In Danish. Account of projective geometry over division rings.

[Hartshorne]

Robin Hartshorne. *Foundations of Projective Geometry*, Lecture Notes, Harvard University. Benjamin Press, 1967.

(See the historical foreword.) *The free projective plane is worked out in chapter 2.*

[Herstein]

I. N. Herstein. *Topics in Algebra*. Wiley and Sons, Inc., 1975.

An excellent undergraduate text on groups, rings, fields, modules, and linear algebra re-done from this viewpoint.

[Heyting]

A. Heyting. *Axiomatic Projective Geometry*. North Holland Publications, 1963.

Achieves categoricity: a complete set of axioms characterizing the real projective plane.

[Hsiang]

Wu-Yi Hsiang. On the laws of trigonometries of two-point homogeneous spaces. *Annals of Global Analysis and Geometry*, 7 (1), 29-45, 1989.

Lays the fundamentals for more research in trigonometry.

[Kaplansky]

Irving Kaplansky. *Fields and Rings*. 2nd ed., University of Chicago Press, 1972.

Galois theory of fields, non-commutative ring theory and homological algebra.

[Kline]

Morris Kline. *Mathematical Thought from Ancient to Modern Times*. Oxford University Press, 1972.

Historical chapters on projective geometry, one on algebraic geometry and one on foundations of geometry.

[Reid]

Miles Reid. *Undergraduate Algebraic Geometry*. London Mathematical Society Student Texts, Cambridge University Press, 1988.

Bezout's theorem for pairs of conics, as well as chapters on cubic curves, varieties and applications.

[Rubin-Silverberg]

K. Rubin and A. Silverberg. A report on Wiles' Cambridge lectures. *Bulletin of American Mathematical Society*, 31 (1), 15-38, 1994.

The recent attack on Fermat's Last Theorem.

[Ryan]

P. Ryan. *Euclidean and Non-euclidean Geometry: an analytic approach*. Cambridge University Press, 1986.

The classical planar geometries and their automorphism groups using only vector analysis and a little matrix theory.

[Samuel]

P. Samuel. *Projective Geometry*. Undergraduate Texts in Mathematics, Readings in Mathematics, translated by S. Levy, Springer Verlag, 1988.

A general n -dimensional treatment of projective geometry including conics, quadrics, polarities and their classification.

[Schwerdtfeger]

Hans Schwerdtfeger. *Geometry of Complex Numbers*. Dover Publications; first edition: University of Toronto Press, 1962.

The geometry of conics and cross ratio via the complex numbers.

[Seidenberg]

A. Seidenberg. *Lectures in Projective Geometry*. University Series in Undergraduate Mathematics, van Nostrand Company, Princeton, 1962.

Well-written book with chapters on projective geometry, axioms for n -space, as well as conics as an extension of a basic course in Euclidean geometry.

[Silverman-Tate]

J. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Undergraduate Texts in Mathematics. Springer Verlag, 1992.

Clear account of elliptic curves and their group of rational points with an application of H. Lenstra to factorization of large integers. Appendix on projective geometry and a proof of Bezout's theorem.

[Wylie]

C.R. Wylie, Jr. *Introduction to Projective Geometry*. McGraw-Hill Book Company, New York, 1970.

Chapters on involutory hexads. the Cayley-Laguerre metrics and subgeometries of the real projective plane. Incidence table for a finite non-Desarguesian geometry.

[Yale]

P. Yale. *Geometry and Symmetry*. Dover Publications, New York, 1988; first edition: Holden-Day, 1968.

The similarities of n -dimensional projective geometry and the planar case is clearly seen in this book. Geometry from the transformation group viewpoint.

Index

- k -plane, 94
 y -intercept, 195
- abelian group, 32, 115
addition, 182, 197
additive notation, 32
affine algebraic curve, 176, 177, 183
affine coordinates, 125-127
affine plane, 2-11, 101, 111, 116, 119,
145, 160, 175
 Desarguesian, 125, 127
 of 16 points, 11
 of 36 points, 11
 of 4 points, 4, 15, 19, 36
 of 9 points, 39, 200
 over division ring, 127
affine reflection, 10
affine transformation, 10
algebraic closure of field, 180
algebraic curve, 175-184
alternative plane, 166
altitude, 189
altitude of triangle, 159, 192
angle, 185, 186
angle bisector of triangle, 160
antipodal point, 186
Archimedean principle, 106
associative law, 31, 90, 122, 191
automorphism of plane
 affine plane, 5-11, 20, 101
 complex projective plane, 112, 160
 configuration, 32
 homogeneous coordinates, 95
 projective plane, 16, 20, 104, 109,
 111, 112, 145, 147
 projective plane of 7 points, 36-
 38
automorphism of ring
 $\mathbb{Z}_p(z)$, 87
 complex numbers, 107
 division ring, 85, 92, 104, 112
 field of 3 elements, 89
 integers modulo p , 87, 89
 real numbers, 106
- Bacharach-Cayley Theorem, 180, 181
Beltrami-Klein model of hyperbolic plane,
190
Bezout's Theorem, 179-181
binary operation, 84
Bolyai's Theorem, 186
Bolyai, J., 186
Brianchon, 171
Brianchon's Theorem, 171
- cancellation law, 88
Cartesian coordinates, 3, 16
Castillon's Problem, 78
Cayley, Arthur, 189
center of division ring, 84, 98
 of quaternions, 84, 91
central dilatation, 114, 118, 136, 137,
141
central projection, 169
Ceva's Theorem, 157-160
cevian, 157
characteristic of field, 54, 81, 107
Chasles, M., 170, 173
circle, 18, 62, 78, 143, 169, 174, 176,
179
coconic points, 169

- collinear points, 2, 99
- collineation, 112, 147
- commutative division ring, 108
- commutative group, 32
- commutative ring, 80, 182, 183
- commutator, 84
- complete quadrangle, 47, 62, 98, 172, 173
 - diagonal point, 47, 59, 62
- complete quadrilateral, 49, 172
 - diagonal line, 49
- completion of affine plane, 13-15, 19, 111, 129, 160
 - real affine plane, 16
- complex conjugation, 88, 107
- complex Möbius transformation, 68-71, 75, 78
- complex numbers, 80, 89, 178
- complex transpose of matrix, 91
- concurrent lines, 44
- configuration, 25, 32
- congruence modulo n , 80, 92
- conic, 17, 169-174, 176, 178, 186, 190
 - and projectivity, 60
 - definition of Desargues, 169
 - definition of J. Steiner, 170
 - definition of M. Chasles, 170
 - definition of von Staudt, 172
 - in finite projective plane, 174
 - section, 18, 77
 - self-dual definition, 172
- conic section, 175
- conjective projectivity, 56-60, 137
- conjugate lines, 172
- conjugate points, 172
- conjugate subgroups, 150
- conjugation of quaternion, 88
- construction
 - of addition, 103, 122
 - of coordinates, 121, 122
 - of dilatations, 122
 - of division ring, 122, 125, 126
 - of lines, 122, 127
 - of multiplication, 103, 122, 123
 - of translations, 122
- contact point of conic, 171
- coordinate axes, 194
- coordinates of projective plane, 113-131
- coset, 182
- cross product, 83, 90
- cross ratio, 74, 112, 140-146, 158, 189
 - of 4 collinear points, 54, 63
 - of 4 concurrent lines, 54, 61
 - of 4 points on conic, 61, 169
 - of coordinates, 60, 140
 - of harmonic quadruple, 59
 - under central dilatation, 141
 - under inversion, 142
 - under Möbius transformation, 141
 - under projectivity, 61
 - under translation, 141
- cross ratio preserving transformation, 141, 142, 145, 170
- cycle, 36
- cyclic group, 34
- degenerate conic, 175
- degree of algebraic curve, 176
- degree of polynomial, 87, 91, 176
- dehomogenization of projective algebraic curve, 176, 177
- Desargues' Axiom, 23-30, 45, 62, 75, 94, 115
 - converse, 46, 62
 - in projective 3-space, 29
 - major, 119
 - minor, 115, 121, 198
- Desargues' configuration, 26, 39
- Desargues' Involution Theorem, 173
- Desargues' Theorem, 24-25, 76
- Desarguesian plane, 24, 111, 129
- determinant, 95
- diagonal of ternary plane, 194
- dilatation, 6-10, 114, 115, 118, 119, 127, 129, 136, 137, 140, 149
- dimension of vector space, 184
- distance, 185, 186

- distance geometry, 185
 distributive law, 79, 123
 division ring, 79-92, 95, 108, 197
 of Desarguesian plane, 129
 dot product, 83, 90
 dual
 of conic, 171
 of cross ratio, 54
 of dual projective plane, 46, 60
 of Fano's Axiom, 49
 of Fundamental Theorem for con-
 junctive projectivities, 67
 dual projective plane, 43-47

 elation, 149-156, 160
 axis, 149
 center, 150

 elementary correspondence, 67, 72
 elliptic curve, 175
 elliptic geometry, 185-192
 elliptic triangle, 187, 188, 192
 envelope, 171
 of self-conjugate lines, 172
 equivalence class, 3, 11, 182
 equivalence relation, 3, 11, 182
 reflexivity, 3
 symmetry, 3
 transitivity, 3
 Euclidean 3-space, 15, 28
 Euclidean geometry, 185, 188
 Euclidean plane, 3, 4, 17, 54, 61, 62,
 159, 169, 170, 189
 Euclidean space, 169
 Euler's officer problem, 11
 Euler, L., 11
 Eulers' formula, 88
 extended complex numbers, 68
 extended field, 135
 extension of field, 89

 factor group, 130
 factorization of polynomial, 178, 180
 Fano plane, 48, 111
 Fano's Axiom, 47-50, 54, 107-111
 Fermat's Last Theorem, 175

 field, 80
 of 3 elements, 89
 of characteristic zero, 82
 of fractions, 89, 91, 182
 of integers modulo p , 81
 of order p^k , 163
 of rational functions, 87, 91, 183
 field of fractions, 183
 finite affine plane, 11
 finite field, 163
 finite non-Desarguesian plane, 202
 finite Pappian plane, 73
 finite projective plane, 19, 20, 47, 163,
 174
 fourth harmonic point, 50
 fractional linear transformation, 68, 136
 free projective plane, 111
 Fundamental Theorem
 for conjunctive projectivities, 70
 in n dimensions, 107
 in 2 dimensions, 106
 of conjunctive projectivities, 65-78,
 107-111, 140
 of projective collineation, 151-154

 Galois, E., 31
 generators of $PC(\pi)$, 154
 generators of group, 35, 105, 118
 geometric series, 87
 Gergonne, 171
 great circle, 186
 group, 31-41
 of conjunctive projectivities, 56, 133-
 146
 of cross ratio preserving permu-
 tations of a line, 140, 141
 of cross ratio preserving permu-
 tations of line, 135
 of dilatations, 114
 of elations with axis ℓ , 149, 160;
 161
 of homologies with axis ℓ and cen-
 ter O , 151

- of Möbius transformations, 69, 133-146
 - of projective collineations, 149, 154
 - of translations, 114, 161
 - of units, 92
- group of automorphisms, 85
 - inner, 105
 - of projective plane over division ring, 95-107
 - of real projective plane, 106
- Hall, Marshall, 194
- Hamilton, W.R., 82
- harmonic conjugate, 50, 60, 62
 - uniqueness, 50, 63
- harmonic quadruple, 49-54, 58, 61, 62
 - construction by circle, 62
- Hessenberg, G., 75
- hexagon, 71, 72, 77, 171
 - inscribed in conic, 171
- Hilbert's Theorem, 112
- Hilbert, D., 85, 108
- homogeneous coordinates, 20
 - of real projective 3-space, 28
 - of real projective plane, 15-20
 - over division ring, 93
- homogeneous polynomial, 176
- homogenization of affine algebraic curve, 177
- homology, 149-156, 161
 - axis, 151
 - center, 151
- homomorphism of groups, 32, 124
- homomorphism of rings, 80, 182
- hyperbola, 18, 60, 176
- hyperbolic line, 191
- hyperbolic plane, 189, 190
- hyperbolic polarity, 172
- hyperplane, 94
- ideal, 181-183
- ideal point, 14, 101, 145
- identity, 32, 38
- incidence geometry, 189
- incidence matrix, 20
- infinite vector space, 92
- inhomogeneous coordinates, 135, 144
- injective mapping, 84
- inner automorphism, 85, 88, 89, 98, 100, 105, 140
- integers, 80, 90, 106, 182
 - modulo n , 38-39, 80
- integral domain, 88, 89, 91, 183
- intersection multiplicity, 179, 184
- intersection of algebraic curves, 178-184
- inverse, 32, 38, 81, 123
- inverse projectivity, 56
- inversion, 136, 137, 140, 142
- invertible matrix, 95, 99
- involution, 74, 174
- involution of quaternion, 88
- involutory hexad, 163
- irreducible polynomial, 178
- isometry, 10
- isomorphism
 - of groups, 32
 - of projective planes, 16
 - of rings, 89
- kernel of homomorphism, 39, 115, 130
- Klein model, 191
- Lagrange's Theorem, 33
- Laurent series, 87
- Law of Cosines, 185-188
- Law of Sines, 185, 186, 188
- left coset, 33, 80
- left distributive law, 123
- left identity, 38
- left inverse, 38
- line at infinity, 14, 177
- line of slopes, 195
- line-conic, 171
- linear ternary operation, 199
- local ring, 179, 183
- loop, 197
- lune, 191

- Möbius transformation, 68, 75, 133–146
 over division ring, 140
 mapping, 5
 maximal ideal, 183
 median of triangle, 62, 160
 Menelaus' Theorem, 162
 metric geometry, 190
 Moulton line, 27, 29
 Moulton plane, 26–27, 74, 110, 201
 multiplication, 198
 multiplicative inverse, 80
 multiplicative mapping, 84
 multiplicative notation, 32
 multiplicative subset of ring, 182
 multiplicity of root, 179
- neutral element, 32
 non-abelian group, 90
 noncommutative division ring, 88
 of characteristic p , 85–88
 of characteristic 2, 110
 norm of quaternions, 83
 normal subgroup, 114, 118, 130, 181
 null, 201
- octonions, 199
 one-to-one correspondence, 5, 84
 orbit of element, 34
 order of element, 34
 order of group, 34
 origin, 194
- Pappian plane, 73, 170, 173
 Pappus of Alexandria, 71
 Pappus' configuration, 41
 Pappus' Theorem, 71–78, 110, 112, 171
 in real projective plane, 75
- parabola, 18
 parallel lines, 2
 in Klein model, 190
 parallel projection, 169
 partial derivative, 178
 partition of set, 11
- Pascal's Theorem, 61, 77, 171, 180
 pencil of lines, 4, 43, 170, 172
 of parallel lines, 5
 permutation, 5, 32
 perspective triangles, 24
 perspectivity, 55–59, 72, 137
 point-conic, 171
 points at infinity, 14
 polar, 171, 172, 186
 polar triangle, 173, 188
 polarity, 47, 171–174, 186
 pole, 171, 172
 polygon, 173
 polynomial, 87, 91, 175, 178
 polynomial ring, 183
 Poncelet, J. V., 62, 171
 prime ideal, 182, 183
 Principle of Duality, 43–47, 67, 171
 projective n -space, 143
 over division ring, 94
 projective 3-space, 28–29, 112
 over division ring, 94
 over field, 146
 projective algebraic curve, 176, 177, 179, 180
 projective collineation, 20, 24, 95, 98, 100, 104, 143, 147–163, 177
 projective geometry, 190
 projective line over field, 143
 projective plane, 13–21, 111, 116, 176
 non-Desarguesian, 26, 47
 of $p^{2k} + p^k + 1$ points, 94, 163
 of 13 points, 54
 of 7 points, 15, 19, 36–38, 47, 60, 74, 94, 110, 161
 over division ring, 93–112, 129, 140
 over quaternions, 110
 projectivity, 55–59, 61, 73, 170, 181
 cross axis, 58, 75
 pure quaternions, 83
- quadrangular set, 163
 quaternions, 82–85, 89, 100, 110, 191

- range of points, 67, 172
- rational numbers, 80, 90, 106
- real affine plane, 3, 5, 7-8, 15, 150, 159
- real numbers, 80, 89, 95
- real projective n -space, 107
- real projective 3-space, 28
- real projective plane, 15-18, 47, 48, 59, 60, 63, 70, 74, 94, 110, 111, 173, 185, 189
- Riemann sphere, 143, 144
- right coset, 33
- ring, 79, 181
 - of polynomials, 91
 - of square matrices, 80, 92, 95
- ring of fractions, 182, 183
- scalar multiplication, 82, 90
- secant, 171, 174
- self-conjugate line, 172
- self-conjugate point, 172
- self-duality of conics, 171
- self-polar odd polygon, 173
- self-polar pentagon, 173
- self-polar triangle, 173
- semi-direct product, 118, 161
- semigroup, 32
- shear, 10
- similar matrices, 161
- similar triangles, 160
- singularity of algebraic curve, 178
- skew Laurent series ring, 86, 87, 91, 92
- slope, 195
- smooth algebraic curve, 178, 179
- sphere, 191
- sphere model of projective plane, 18-21, 185
- spherical geometry, 185, 189
- stabilizer subgroup, 33
- standard quadrangle, 96, 101, 104, 107, 112
- standard sphere, 18
- Steiner, J., 170
- stereographic projection, 143
- stretching, 7
- subfield, 80
- subgroup, 33
- symmetric matrix, 173
- tangent line of conic, 60, 62, 170, 171, 174, 179
- Tarry, G., 11
- Taylor polynomial, 188
- ternary ring, 196
- topology of complex projective line, 143
- topology of real projective line, 143
- topology of real projective plane, 18
- transformation of extended field, 136
- transition matrix, 5
- transitive group, 35
- translation, 7-10, 114-116, 123, 127, 129, 136, 137, 140, 141, 149, 160
- translation plane, 121
- transversal intersection, 179
- triangle, 23, 78, 173, 175, 185
- trilinear polar, 62
- ultraparallel lines, 190
- unit, 32, 79
- unit point, 194
- unit sphere, 185
- Veblen-Wedderburn system, 199
- vector, 201
- von Staudt, K. G. C., 172, 173
- zero divisor, 81, 92, 183

Tekster fra IMFUFA 270-279

Liste over tidligere udkomne tekster tilsendes gerne. Henvendelse herom kan ske til IMFUFA's sekretariat; tlf: 46 75 77 11, lokal: 2263.

- 270/94: "*The Image of the Enveloping Algebra and Irreducibility of Induced Representations of Exponential Lie Groups*" by Jacobi Jacobsen.
- 271/94: "*Matematikken i Fysikken. Opdaget eller opfundet?*". NAT-BAS projekt. Vejleder: Jens Højgaard-Jensen.
- 272/94: "*Tradition og fornyelse. Det praktiske elevarbejde i gymnasiets fysikundervisning, 1907-1988*" af Kristian Hoppe og Jeppe Guldager. Vejledere: Karin Beyer og Nils Hybel.
- 273/94: "*Model for kort- og mellemdistanceløb. Verifikation af model*" af Lise Fabricius Christensen, Helle Pilemann, Bettina Sørensen. Vejleder: Mette Olufsen.
- 274/94: "*Model 10 - en matematisk model af intravenøse anæstetikas farmakokinetik*". 3. modul: matematik, forår 1994. Af Trine Andreassen, Bjørn Christensen, Christina Green, Anja Skjoldborg Hansen, Lisbeth Helmgård. Vejledere: Viggo Andreassen og Jesper Larsen.
- 275/94: "*Perspective on Teichmüller and the Jahresbereich*". 2nd edition; by Bernhelm Booß-Bavnbek.
- 276/94: "*Dispersionsmodellering*", projektrapport 1. modul; af Gitte Andersen, Reannah Borup, Lisbeth Friis, Per Gregersen, Kristina Vejrup. Vejleder: Bernhelm Booß-Bavnbek.
- 277/94: "*Projektarbejds pædagogik - om tre tolkninger af problemorienteret projektarbejde*" af Claus Elensted-Behrens, Frederik Voetmann Christiansen, Jørn Skov Hansen, Thomas Thingstrup. Vejleder: Jens Højgaard-Jensen.
- 278/94: "*The Models Underlying the Anaesthesia Simulator Sophus*" by Mette Olufsen (Måth-Tech), Finn Nielsen (RISO National Laboratory), Per Føge Jensen (Herlev University Hospital), Stig Andur Pedersen (Roskilde University).
- 279/90: "*Description of a Method of Measuring the Shear Modulus of Supercooled Liquids and a Comparison of their Thermal and Mechanical Response Functions*" by Tage Christensen.