

- Abbott:** Understanding Analysis.
- Anglin:** Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
- Anglin/Lambek:** The Heritage of Thales.
Readings in Mathematics.
- Apostol:** Introduction to Analytic Number Theory. Second edition.
- Armstrong:** Basic Topology.
- Armstrong:** Groups and Symmetry.
- Axler:** Linear Algebra Done Right. Second edition.
- Beardon:** Limits: A New Approach to Real Analysis.
- Bak/Newman:** Complex Analysis. Second edition.
- Banchoff/Wermer:** Linear Algebra Through Geometry. Second edition.
- Berberian:** A First Course in Real Analysis.
- Bix:** Conics and Cubics: A Concrete Introduction to Algebraic Curves.
- Brémaud:** An Introduction to Probabilistic Modeling.
- Bressoud:** Factorization and Primality Testing.
- Bressoud:** Second Year Calculus.
Readings in Mathematics.
- Brickman:** Mathematical Introduction to Linear Programming and Game Theory.
- Browder:** Mathematical Analysis: An Introduction.
- Buchmann:** Introduction to Cryptography.
- Buskes/van Rooij:** Topological Spaces: From Distance to Neighborhood.
- Callahan:** The Geometry of Spacetime: An Introduction to Special and General Relativity.
- Carter/van Brunt:** The Lebesgue–Stieltjes Integral: A Practical Introduction.
- Cederberg:** A Course in Modern Geometries. Second edition.
- Childs:** A Concrete Introduction to Higher Algebra. Second edition.
- Chung/AitSahlia:** Elementary Probability Theory: With Stochastic Processes and an Introduction to Mathematical Finance. Fourth edition.
- Cox/Little/O’Shea:** Ideals, Varieties, and Algorithms. Second edition.
- Croom:** Basic Concepts of Algebraic Topology.
- Curtis:** Linear Algebra: An Introductory Approach. Fourth edition.
- Daepf/Gorkin:** Reading, Writing, and Proving: A Closer Look at Mathematics.
- Devlin:** The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
- Dixmier:** General Topology.
- Driver:** Why Math?
- Ebbinghaus/Flum/Thomas:** Mathematical Logic. Second edition.
- Edgar:** Measure, Topology, and Fractal Geometry.
- Elaydi:** An Introduction to Difference Equations. Second edition.
- Erdős/Surányi:** Topics in the Theory of Numbers.
- Estep:** Practical Analysis in One Variable.
- Exner:** An Accompaniment to Higher Mathematics.
- Exner:** Inside Calculus.
- Fine/Rosenberger:** The Fundamental Theory of Algebra.
- Fischer:** Intermediate Real Analysis.
- Flanigan/Kazdan:** Calculus Two: Linear and Nonlinear Functions. Second edition.
- Fleming:** Functions of Several Variables. Second edition.
- Foulds:** Combinatorial Optimization for Undergraduates.
- Foulds:** Optimization Techniques: An Introduction.
- Franklin:** Methods of Mathematical Economics.

(continued after index)

Judith N. Cederberg

A Course in Modern Geometries

Second Edition

With 151 Illustrations



Springer

who used a preliminary version of the text and made helpful suggestions are Thomas Q. Sibley of St. John's University in Collegeville, Minnesota, and Martha L. Wallace of St. Olaf College. I am also indebted to Joseph Malkevitch of York College of the City University of New York for serving as mathematical reader for the text, and to Christina Mikulak for her careful editorial work.

Judith N. Cederberg

Contents

Preface to the Second Edition	v
Preface to the First Edition	xiii
1 Axiomatic Systems and Finite Geometries	1
1.1 Gaining Perspective*	1
1.2 Axiomatic Systems	2
1.3 Finite Projective Planes	9
1.4 An Application to Error-Correcting Codes	18
1.5 Desargues' Configurations	25
1.6 Suggestions for Further Reading	30
2 Non-Euclidean Geometry	33
2.1 Gaining Perspective	33
2.2 Euclid's Geometry	34
2.3 Non-Euclidean Geometry*	47
2.4 Hyperbolic Geometry—Sensed Parallels	51
2.5 Hyperbolic Geometry—Asymptotic Triangles	61
2.6 Hyperbolic Geometry—Saccheri Quadrilaterals	68
2.7 Hyperbolic Geometry—Area of Triangles	74
2.8 Hyperbolic Geometry—Ultraparallels	80
2.9 Elliptic Geometry	84

2.10	Significance of the Discovery of Non-Euclidean Geometries	93
2.11	Suggestions for Further Reading	93
3	Geometric Transformations of the Euclidean Plane	99
3.1	Gaining Perspective	99
3.2	Exploring Line and Point Reflections*	103
3.3	Exploring Rotations and Finite Symmetry Groups*	108
3.4	Exploring Translations and Frieze Pattern Symmetries*	116
3.5	An Analytic Model of the Euclidean Plane	121
3.6	Transformations of the Euclidean Plane	129
3.7	Isometries	136
3.8	Direct Isometries	144
3.9	Indirect Isometries	154
3.10	Frieze and Wallpaper Patterns	165
3.11	Exploring Plane Tilings*	173
3.12	Similarity Transformations	183
3.13	Affine Transformations	190
3.14	Exploring 3-D Isometries	198
3.15	Suggestions for Further Reading	207
4	Projective Geometry	213
4.1	Gaining Perspective	213
4.2	The Axiomatic System and Duality	214
4.3	Perspective Triangles*	221
4.4	Harmonic Sets*	223
4.5	Perspectivities and Projectivities*	229
4.6	Conics in the Projective Plane*	240
4.7	An Analytic Model for the Projective Plane	250
4.8	The Analytic Form of Projectivities	258
4.9	Cross Ratios	264
4.10	Collineations	270
4.11	Correlations and Polarities	283
4.12	Subgeometries of Projective Geometry	298
4.13	Suggestions for Further Reading	311

5	Chaos to Symmetry: An Introduction to Fractal Geometry	315
5.1	A Chaotic Background*	316
5.2	Need for a New Geometric Language	334
5.3	Fractal Dimension	347
5.4	Iterated Function Systems*	360
5.5	Finally—What Is a Fractal?	377
5.6	Applications of Fractal Geometry	380
5.7	Suggestions for Further Reading	382

Appendices	389	
A	Euclid's Definitions, Postulates, and the First 30 Propositions of <i>Elements, Book I</i>	389
B	Hilbert's Axioms for Plane Geometry	395
C	Birkhoff's Postulates for Euclidean Plane Geometry	399
D	The MSG Postulates for Euclidean Geometry	401
E	Some MSG Definitions for Euclidean Geometry	405
F	The ASA Theorem	409

References	413
-------------------	------------

Index	427
--------------	------------

* Supplementary dynamic geometry software activities using *Cabri Geometry II* and *Geometer's Sketchpad* are available at the website:
<http://www.stolaf.edu/people/cederj/geotext/info.htm>.

1

CHAPTER

Axiomatic Systems and Finite Geometries

1.1 Gaining Perspective*

Finite geometries were developed in the late nineteenth century, in part to demonstrate and test the axiomatic properties of *completeness*, *consistency*, and *independence*. They are introduced in this chapter to fulfill this historical role and to develop both an appreciation for and an understanding of the revolution in mathematical and philosophical thought brought about by the development of non-Euclidean geometry. In addition, finite geometries provide relatively simple axiomatic systems in which we can begin to develop the skills and techniques of geometric reasoning. The finite geometries introduced in Sections 1.3 and 1.5 also illustrate some of the fundamental properties of non-Euclidean and projective geometry.

Even though finite geometries were developed as abstract systems, mathematicians have applied these abstract ideas in designing statistical experiments using Latin squares and in developing error-correcting codes in computer science. Section 1.4 develops a simple

*Supplementary dynamic geometry software activities are available at the website: <http://www.stolaf.edu/people/cederj/geotext/info.htm>.

error-correcting code and shows its connection with finite projective geometries. The application of finite affine geometries to the building of Latin squares is equally intriguing. Since Latin squares are clearly described in several readily accessible sources, the reader is encouraged to explore this topic by consulting the resources listed at the end of this chapter.

In studying finite axiomatic systems, you are encouraged to take advantage of the visual nature of geometry by constructing illustrations. These can be drawn using paper and pencil, or built with concrete objects such as yarn and game chips. While working through this first chapter, you are also encouraged to become familiar with dynamic geometry software (DGS). This new tool enables accurate renditions of traditional compass and straightedge constructions that then can be dynamically rearranged by dragging initial objects. Introductions featuring activities that review basic ideas in Euclidean geometry are available for both *Geometer's Sketchpad* and *Cabri Geometry* at the website: <http://www.stolaf.edu/people/cederj/geotext/info.htm>. You are encouraged to become familiar with one or both of these programs so that you can carry out explorations suggested in Chapters 2 through 5.

1.2 Axiomatic Systems

The study of any mathematics requires an understanding of the nature of deductive reasoning; frequently, geometry has been singled out for introducing this methodology to secondary school students. There are important historical reasons for choosing geometry to fulfill this role, but these reasons are seldom revealed to secondary school initiates. This section introduces the terminology essential for a discussion of deductive reasoning so that the extraordinary influence of the history of geometry on the modern understanding of deductive systems will become evident.

Deductive reasoning takes place in the context of an organized logical structure called an *axiomatic* (or *deductive*) system. Such a system consists of the components listed below:

Components of an Axiomatic System

1. Undefined terms.
2. Defined terms.
3. Axioms.
4. A system of logic.
5. Theorems.

Undefined terms are included since it is not possible to define all terms without resorting to circular definitions. In geometrical systems these undefined terms frequently, but not necessarily, include *point*, *line*, *plane* and *on*. *Defined terms* are not actually necessary, but in nearly every axiomatic system certain phrases involving undefined terms are used repeatedly. Thus, it is more efficient to substitute a new term, that is, a defined term, for each of these phrases whenever they occur. For example, in Euclidean geometry we substitute the term "parallel lines" for the phrase "lines that do not intersect." Furthermore, it is impossible to prove all statements constructed from the defined and undefined terms of the system without circular reasoning, just as it is impossible to define all terms. So an initial set of statements is accepted without proof. The statements that are accepted without proof are known as *axioms*. From the axioms, other statements can be deduced or proved using the rules of inference of a *system of logic* (usually Aristotelian). These latter statements are called *theorems*.

As noted earlier, the axioms of a system must be statements constructed using the terms of the system. But they cannot be arbitrarily constructed since an axiom system must be consistent.

Definition 1.1

An axiomatic system is said to be *consistent* if there do not exist in the system any two axioms, any axiom and theorem, or any two theorems that contradict each other.

It should be clear that it is essential that an axiomatic system be consistent, since a system in which both a statement and its negation can be proved is worthless. However, it soon becomes evident that it would be difficult to verify consistency directly from this definition, since all possible theorems would have to be considered.

Instead, models are used for establishing consistency. A *model* of an axiomatic system is obtained by assigning interpretations to the undefined terms so as to convert the axioms into true statements in the interpretations. If the model is obtained by using interpretations that are objects and relations adapted from the real world, we say we have established *absolute consistency*. In this case, statements corresponding to any contradictory theorems would lead to contradictory statements in the model, but contradictions in the real world are supposedly impossible. On the other hand, if the interpretations assigned are taken from another axiomatic system, we have only tested consistency relative to the consistency of the second axiomatic system; that is, the system we are testing is consistent only if the system within which the interpretations are assigned is consistent. In this second case, we say we have demonstrated *relative consistency* of the first axiomatic system. Because of the number of elements in many axiomatic systems, relative consistency is the best we are able to obtain. We illustrate the use of models to determine consistency of the axiomatic system for four-point geometry.

Axioms for Four-Point Geometry

Undefined Terms. Point, line, on.

Axiom 4P.1. There exist exactly four points.

Axiom 4P.2. Two distinct points are on exactly one line.

Axiom 4P.3. Each line is on exactly two points.

Before demonstrating the consistency of this system, it may be helpful to make some observations about these three statements which will also apply to other axioms in this text. Axiom 4P.1 explicitly guarantees the existence of exactly four points. However, even though lines are mentioned in Axioms 4P.2 and 4P.3, we cannot ascertain whether or not lines exist until theorems verifying this are proved, since there is no axiom that explicitly insures their existence. This is true even though in this system the proof of the existence of lines is almost immediate. Axioms 4P.2 and 4P.3, like many mathematical statements, are disguised “if . . . then” statements. Axiom 4P.2 should be interpreted as follows: If two distinct points exist,



FIGURE 1.1 A four-point geometry model.

then these two points are on exactly one line. Similarly, Axiom 4P.3 should be interpreted: If there is a line, then it is on exactly two points. In other axiomatic systems, we will discover that the axioms actually lead to theorems telling us that there are many more points and/or lines than those guaranteed to exist by the axioms.

These observations suggest that the construction of any model for four-point geometry must begin with the objects known to exist, that is, four points. In model 4P.1 these points are interpreted as the letters A, B, C, D whereas in model 4P.2 (see Fig. 1.1) these points are interpreted as dots. In continuing to build either model, we must interpret the remaining undefined terms so as to create a system in which Axioms 4P.2 and 4P.3 become true statements.

Model 4P.1

Undefined Term	Interpretation
Points	Letters A, B, C, D
Lines	Columns of letters given below
On	Contains, or is contained in
<i>Lines</i>	
	$A \ A \ A \ B \ B \ C$
	$B \ C \ D \ C \ D \ D$

Model 4P.2

Undefined Term	Interpretation
Points	Dots denoted 1, 2, 3, 4
Lines	Segments illustrated in Fig. 1.1
On	A dot is an endpoint of a segment or vice versa

There are several other important properties that an axiomatic system *may* possess.

Definition 1.2

An axiom in an axiomatic system is *independent* if it cannot be proved from the other axioms. If each axiom of a system is independent, the system is said to be independent.

Clearly an independent system is more elegant since no unnecessary assumptions are made. However, the increased difficulty of working in an independent system becomes obvious when we merely note that accepting fewer statements without proof leaves more statements to be proved. For this reason the axiomatic systems used in secondary-school geometry are seldom independent.

The verification that an axiomatic system is independent is also done via models. The independence of Axiom A in an axiomatic system S is established by finding a model of the system S' where S' is the system obtained from S by replacing Axiom A with a negation of A. Thus, to demonstrate that a system consisting of n axioms is independent, n models must be exhibited—one for each axiom. The independence of the axiomatic system for four-point geometry is demonstrated by the following three models, all of which interpret points as letters of the alphabet and lines as the columns of letters indicated.

Models Demonstrating Independence of Axioms for Four-Point Geometry

Model 4P I.1

A model in which a negation of Axiom 4P.1 is true (i.e., there do not exist four points):

Points	Lines
A, B	A B

Since this model contains only two points, the negation of Axiom 4P.1 is clearly true and it is easy to show that Axioms 4P.2 and 4P.3 are true statements in this interpretation.

Model 4P I.2

A model in which a negation of Axiom 4P.2 is true (i.e., there are two distinct points not on one line):

Points	Lines
A, B, C, D	A C B D

Note that in this model there is no line on points A and C. What other pairs of points fail to be on a line?

Model 4P I.3

A model in which a negation of Axiom 4P.3 is true (i.e., there are lines not on exactly two points):

Points	Lines
A, B, C, D	A A B C B D D D C

In this model one line is on three points, whereas the remaining lines are each on two points, so the negation of Axiom 4P.3 is true in this interpretation.

Since we have demonstrated the independence of each of the axioms of four-point geometry, we have shown that this axiomatic system is independent.

Another property that an axiomatic system may possess is *completeness*.

Definition 1.3

An axiomatic system is *complete* if every statement containing undefined and defined terms of the system can be proved valid or invalid, or in other words, if it is not possible to add a new independent axiom to the system.

In general, it is impossible to demonstrate directly that a system is complete. However, if a system is complete, there cannot exist two

essentially different models. This means all models of the system must be pairwise *isomorphic*.

Definition 1.4

Two models α and β of an axiomatic system are said to be *isomorphic* if there exists a one-to-one correspondence ϕ from the set of points and lines of α onto the set of points and lines of β that preserves all relations. In particular if the undefined terms of the system consist of the terms "point," "line," and "on," then ϕ must satisfy the following conditions:

1. For each point P and line l in α , $\phi(P)$ and $\phi(l)$ are a point and line in β .
2. If P is on l , then $\phi(P)$ is on $\phi(l)$.

If all models of a system are pairwise isomorphic, it is clear that each model has the same number of points and lines. Furthermore, if a new independent axiom could be added to the system, there would be two distinct models of the system: a model α in which the new axiom would be valid and a model β in which the new axiom would not be valid. The models α and β could not then be isomorphic. Hence, if all models of the system are necessarily isomorphic, it follows that the system is complete.

In the example of the four-point geometry, it is clear that models 4P.1 and 4P.2 are isomorphic. The verification that all models of this system are isomorphic follows readily once the following theorem is verified (see Exercises 5 and 6).

Theorem 4P.1

There are exactly six lines in the four-point geometry.

Finally, any discussion of the properties of axiomatic systems must include mention of the important result contained in Gödel's theorem. Greatly simplified, this result says that any consistent axiomatic system comprehensive enough to contain the results of elementary number theory is not complete.

Exercises

For Exercises 1–4, consider the following axiomatic system:

Axioms for Three-Point Geometry

Undefined Terms. Point, line, on.

Axiom 3P.1. There exist exactly three points.

Axiom 3P.2. Two distinct points are on exactly one line.

Axiom 3P.3. Not all points are on the same line.

Axiom 3P.4. Two distinct lines are on at least one common point.

1. (a) Prove that this system is consistent. (b) Did the proof in part (a) demonstrate absolute consistency or relative consistency? Explain.
2. Prove that this system is independent.
3. Prove the following theorems in this system: (a) Two distinct lines are on exactly one point. (b) Every line is on exactly two points. (c) There are exactly three lines.
4. Is this system complete? Why?
5. Prove Theorem 4P.1.
6. Prove that any two models of four-point geometry are isomorphic.

Use the following definition in Exercises 7 and 8.

Definition

The *dual* of a statement p in four-point geometry is obtained by replacing each occurrence of the term "point" in p by the term "line" and each occurrence of the term "line" in p by the term "point."

7. Obtain an axiomatic system for *four-line geometry* by dualizing the axioms for four-point geometry.
8. Verify that the dual of Theorem 4P.1 will be a theorem of four-line geometry. How would its proof differ from the proof of Theorem 4P.1 in Exercise 5?

1.3 Finite Projective Planes

As indicated by the examples in the previous section, there are geometries consisting of only a finite number of points and lines. In

this section we will consider an axiomatic system for an important collection of finite geometries known as *finite projective planes*. These geometries may, at first glance, look much like finite versions of plane Euclidean geometry. However, there is a very important difference. In a finite projective plane, each pair of lines intersects; that is, there are no parallel lines. This pairwise intersection of lines leads to several other differences between projective planes and Euclidean planes. A few of these differences will become apparent in this section; others will not become evident until we study general plane projective geometry in Chapter 4.

Some of the first results in the study of finite projective geometries were obtained by von Staudt in 1856, but it wasn't until early in this century that finite geometries assumed a prominent role in mathematics. Since then, the study of these geometries has grown considerably and there are still a number of unsolved problems currently engaging researchers in this area.

Axioms for Finite Projective Planes

Undefined Terms. Point, line, incident.

Defined Terms. Points incident with the same line are said to be *collinear*. Lines incident with the same point are said to be *concurrent*.

Axiom P.1. There exist at least four distinct points, no three of which are collinear.

Axiom P.2. There exists at least one line with exactly $n + 1$ ($n > 1$) distinct points incident with it.

Axiom P.3. Given two distinct points, there is exactly one line incident with both of them.

Axiom P.4. Given two distinct lines, there is at least one point incident with both of them.

Any set of points and lines satisfying these axioms is called a *projective plane of order n* . Note that the word "incident" has been used in place of the undefined term "on" in this axiom system, since "incident" is commonly used in the study of general projective planes.

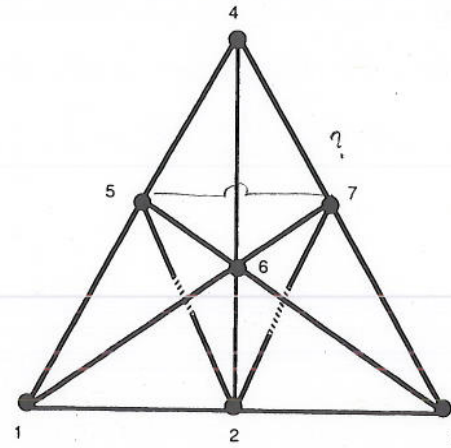


FIGURE 1.2 A finite projective plane model.

The consistency of this axiomatic system is demonstrated by either of the following models which use the same interpretations as models 4P.1 and 4P.2 in Section 1.2.

Model P.1

Points	Lines
A, B, C, D, E, F, G	A A B A B C C B D D F E D E C E F G G G F

Model P.2

Points	Lines
Dots denoted 1, 2, 3, 4, 5, 6, 7	Segments illustrated in Fig. 1.2

Note that Models P.1 and P.2 depict a projective plane of order 2 and both have exactly three points on each line, but there are projective planes with more than three points on a line as shown by the next model.

Model P.3

Points	Lines
A, B, C, D, E,	A A A A B B B C C C D D D
F, G, H, I, J,	B E H K E F G E F G E F G
K, L, M	C F I L H I J I J H J H I D G J M K L M M K L L M K

Whereas models P.1 and P.2 have three points on each line, three lines on each point, and a total of seven points and seven lines, model P.3 has four points on each line, four lines on each point, and a total of thirteen points and thirteen lines. To determine if finite projective planes exist with more points and lines, it is clearly impractical to employ trial-and-error procedures. Instead we develop a series of theorems that lead to a general result regarding the number of points and lines in a finite projective plane of order n .

The proofs of these theorems are simplified by noting that this axiom system satisfies the *principle of duality*, which Coxeter has described as "one of the most elegant properties of projective geometry" (Coxeter, 1969, p. 231). As noted in the exercises in Section 1.2, the *dual* of a statement is obtained by replacing each occurrence of the word "point" by the word "line" and vice versa (consequently, the words "concurrent" and "collinear" must also be interchanged).

Definition 1.5

An axiomatic system in which the dual of any theorem is also a theorem is said to satisfy the *principle of duality*.

Thus, in an axiomatic system that satisfies the principle of duality, the proof of any theorem can be "turned into" a proof of a dual theorem merely by dualizing the original proof. To show that an axiom system has the property of duality it is necessary to prove that the duals of each axiom are theorems of the system. The theorems that are the dual statements of the four axioms of this system are listed here. The proofs of the duals of Axioms P.1, P.3, and P.4 are left to you.

Theorem P.1 (Dual of Axiom P.1)

There exist at least four distinct lines, no three of which are concurrent.

Theorem P.2 (Dual of Axiom P.3)

Given two distinct lines, there is exactly one point incident with both of them.

Theorem P.3 (Dual of Axiom P.4)

Given two distinct points, there is at least one line incident with both of them.

Theorem P.4 (Dual of Axiom P.2)

There exists at least one point with exactly $n + 1$ ($n > 1$) distinct lines incident with it.

Proof

By Axiom P.2 there is a line l with $n + 1$ points P_1, P_2, \dots, P_{n+1} and by Axiom P.1 there is a point P not incident with l . Then by Axiom P.3 there exist lines l_1, l_2, \dots, l_{n+1} joining the point P to points P_1, P_2, \dots, P_{n+1} , respectively (see Fig. 1.3). It is sufficient to show that these lines are all distinct and that there are no other lines through P . If $l_i = l_j$ for $i \neq j$ then the two points P_i and P_j would be incident with both l and $l_i = l_j$, and it would follow by Axiom P.3 that $l = l_i = l_j$. But P is on l_i and *not* on l so we have a contradiction. Thus, $l_i \neq l_j$ for $i \neq j$. Now assume there is an additional line, l_{n+2} through P . This line must also intersect l at a point Q (Axiom P.4). Since l has exactly $n + 1$ points, Q must be one of the points P_1, \dots, P_{n+1} . Assume $Q = P_1$, then, since $Q = P_1$ and P are two distinct points on both l_1 and l_{n+2} , it follows that $l_{n+2} = l_1$. Therefore, the point P is incident with exactly $n + 1$ lines. ■

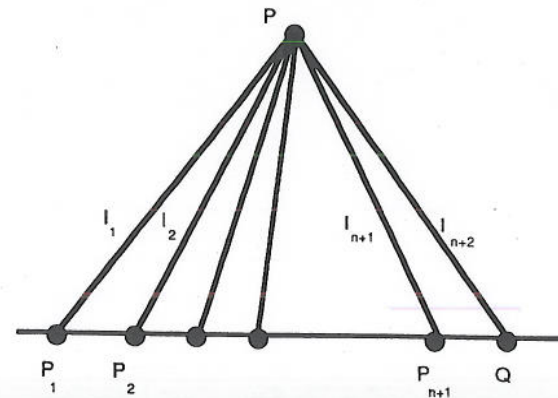


FIGURE 1.3 Proof P.4.

The previous proof demonstrates several geometric conventions. First, to make the proof less awkward, the phrase "is incident with" is frequently replaced by a variety of other familiar terms such as "is on," "contains," and "through." The meanings of these substitute terms should be obvious by their context. Second, uppercase letters are used to designate points while lowercase letters are used for lines. Finally, since diagrams are extremely helpful both in constructing and following a proof, figures are included as part of the proofs whenever appropriate; but the narrative portions of the proofs are constructed so as to be completely independent of the figures.

In models P.1, P.2, and P.3, the number of points on each line and the number of lines on each point is the same for all lines and points in each model. That this must be true in general is verified by the following theorems.

Theorem P.5

In a projective plane of order n , each point is incident with exactly $n + 1$ lines.

Proof

Let P be a point of the plane. Axiom P.2 guarantees the existence of a line l containing $n + 1$ points, P_1, P_2, \dots, P_{n+1} . Then there are

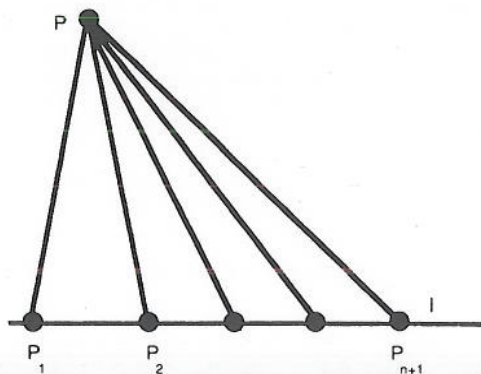


FIGURE 1.4 Proof P.5, P not on l .

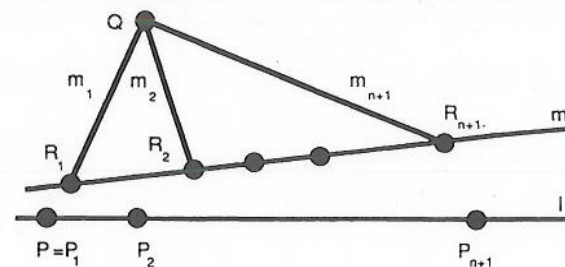


FIGURE 1.5 Proof P.5, P on l .

two cases to consider, depending on whether P is on l or not (see Figs. 1.4 and 1.5).

Case 1 (P is not on l): If P is not on l there are at least $n + 1$ lines through P , namely, the lines joining P to each of the points P_1, P_2, \dots, P_{n+1} . Just as in the proof of the previous theorem, it can be shown that these lines are distinct and there are no other lines through P . So in this case there are exactly $n + 1$ lines through P .

Case 2 (P is on l): Assume $P = P_1$. Axiom P.1 guarantees the existence of a point Q not on l . It is also possible to verify the existence of a line m that contains neither P nor Q (see Exercise 7). By case 1, Q is on exactly $n + 1$ lines m_1, m_2, \dots, m_{n+1} . But each of these lines intersects m in a point R_i for $i = 1, \dots, n + 1$. It can easily be shown that these points are distinct and that these are the only points on line m . Thus, P is not on the line m , which contains exactly $n + 1$ points, so as in case 1, P is incident with exactly $n + 1$ lines. ■

With this theorem in hand, the following theorem follows immediately by duality.

Theorem P.6

In a projective plane of order n , each line is incident with exactly $n + 1$ points.

Using these results, we can now determine the total number of points and lines in a projective plane of order n .

Theorem P.7

A projective plane of order n contains exactly $n^2 + n + 1$ points and $n^2 + n + 1$ lines.

Proof

Let P be a point in a projective plane of order n . Then every other point is on exactly one line joining it with the point P . By Theorem P.5 there are exactly $n + 1$ lines through P and by Theorem P.6 each of these lines contains exactly $n + 1$ points, that is, n points in addition to P . Thus, the total number of points is $(n + 1)n + 1 = n^2 + n + 1$. A dual argument verifies that the total number of lines is also $n^2 + n + 1$. ■

Thus, a finite projective plane of order two must have seven points and seven lines and a projective plane of order three must have thirteen points and thirteen lines. But one of the unresolved questions in the study of finite geometries is the determination of the orders for which finite projective planes exist. A partial answer to this question was given in 1906 when Veblen and Bussey proved that there exist finite projective planes of order n whenever n is a power of a prime. It has long been conjectured that these are the only orders for which finite projective planes exist. In 1949 Bruck and Ryser proved that if n is congruent to 1 or 2 (modulo 4), and if n cannot be written as the sum of two squares, then there are no projective planes of order n . This proved the conjecture for an infinite number of cases including $n = 6, 14, 21$, and 22. However, it also left open an infinite number of cases including $n = 10, 12, 15, 18$, and 20. In late 1988, a group of researchers in the computer science department at Concordia University in Montreal completed a case-by-case computer analysis requiring several thousand hours of computer time. By investigating the implications of the existence of an order 10 projective plane, they concluded that the conjecture is also correct for $n = 10$; that is, finite projective planes of order 10 do not exist. This leaves $n = 12$ as the smallest number for which the conjecture is unproved (Cipra, 1988).

The study of the infinite projective plane from both synthetic and analytic viewpoints yields a wealth of interesting geometric properties which are generalizations of both Euclidean and non-Euclidean properties. We pursue this study in Chapter 4, following an introduc-

tion of non-Euclidean geometry (Chapter 2) and the development of an analytic model for Euclidean geometry (Chapter 3). However, as we shall see in the following section, even one of the simplest projective geometries, namely the finite projective plane of order 2, has an application that demonstrates the relevance of geometry to exciting new areas of mathematics.

Exercises

1. Which axioms for a finite projective plane are also valid in Euclidean geometry? Which are not?
2. Prove that the axiomatic system for finite projective planes is incomplete.
3. Verify that models P.1 and P.2 are isomorphic.
4. Prove Theorem P.1.
5. Prove Theorem P.2.
6. Prove Theorem P.3.
7. Verify the existence of the line m used in case 2 of the proof of Theorem P.5.
8. How many points and lines does a finite projective plane of order 7 have?

The axioms for a *finite affine plane of order n* are given below. The undefined terms and definitions are identical to those for a finite projective plane.

Axioms for Finite Affine Planes

Axiom A.1. There exist at least four distinct points, no three of which are collinear.

Axiom A.2. There exists at least one line with exactly n ($n > 1$) points on it.

Axiom A.3. Given two distinct points, there is exactly one line incident with both of them.

Axiom A.4. Given a line l and a point P not on l , there is exactly one line through P that does not intersect l .

9. How do the axioms for a finite affine plane differ from those for a finite projective plane?
10. Show that a finite affine plane does not satisfy the principle of duality.
11. Find models of affine planes of orders 2 and 3.

The following exercises ask you to prove a series of theorems about finite affine planes. You should prove these in the order indicated since some will require that you use a previous result.

12. Prove: In an affine plane of order n , each point lies on exactly $n + 1$ lines. [Hint: Consider two cases as in the proof of Theorem P.5.]
13. Prove: In an affine plane of order n , each line contains exactly n points.
14. Prove: In an affine plane of order n , each line l has exactly $n - 1$ lines that do not intersect l .
15. Prove: In an affine plane of order n , there are exactly n^2 points and $n^2 + n$ lines.
16. Verify that if one line and its points are deleted from the finite projective plane of order 2 given in model P.1 or P.2, the remaining points and lines form a model of an affine plane. What is its order?

1.4 An Application to Error-Correcting Codes

The finite projective plane of order 2 illustrated in models P.1 and P.2 of the previous section is known as a *Fano plane*. A concise way of representing this and other finite planes is a configuration known as an *incidence table*. The lines of the plane are represented by columns in Table 1.1, while the points of the plane are represented by rows. Entries of 0 and 1 represent nonincidence and incidence, respectively.

This table demonstrates that we can represent each point in a Fano plane uniquely by a vector consisting of the entries in the corresponding row of the incidence table. Thus, point A can be represented by the vector (1, 0, 0, 0, 0, 1, 1). Similarly, every point in a

TABLE 1.1 Incidence Table for a Fano Plane.

	l_1	l_2	l_3	l_4	l_5	l_6	l_7
A	1	0	0	0	0	1	1
B	0	1	0	0	1	0	1
C	0	0	1	0	1	1	0
D	1	0	0	1	1	0	0
E	0	1	0	1	0	1	0
F	0	0	1	1	0	0	1
G	1	1	1	0	0	0	0

Fano plane can be represented by a binary 7-tuple; that is, a vector with seven components, each of which is a 0 or 1. Note that the vector for any given point contains exactly three 1's, so in the language of coding theory, we say that each vector has *weight* 3. Following a brief introduction to the area of coding theory, we shall see that these seven vectors play an important role in an elementary error-correcting code.

Coding theory is devoted to the detection and correction of errors that are introduced when messages are transmitted. Such codes have found application in transmission of pictures from space and in the development of the compact disk. The impetus for developing these codes arose from the frustrations that Richard W. Hamming encountered in 1947 when working with a mechanical relay computer, which dumped his program whenever it detected an error. Having a computer that could detect but not find and correct an error led to the development of error-correcting codes.

Since then, coding theory has become an important research area, using results from projective geometry, group theory, the theory of finite fields, and linear programming. Error-correcting coding has been described as "the art of adding redundancy efficiently so that most messages, if distorted, can be correctly decoded" (Pless, 1982, p. 2).

One of the simplest error-correcting codes is a projective geometry code known as the *Hamming (7,4) code*. This code can be generated by the four rows of the matrix G below, known as the *generator matrix* for the code. In this matrix, the first row vector is the code word for 1000, the binary representation of the decimal

number 8; the second row is the code word for 0100, the binary representation of the decimal number 4; and so on. The first four digits of these code words occupy the so-called *information positions*, since they represent the actual number or message to be transmitted. The remaining three positions are called the *redundancy positions*.

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Other code words are obtained by adding these rows where the addition is the usual componentwise vector addition modulo 2. Note that when we find all possible sums of these rows (see Table 1.2), we obtain in the first four positions all 16 possible strings of 0's and 1's; that is, all binary representations of the decimal numbers 0 through 15.

The redundancy digits in the last three positions allow single error corrections; that is, if a transmitted message contains a single digit error these extra digits allow us to find and correct the error.

TABLE 1.2 Possible Code Words.

0	0	0	0	0	0	0	Adding no words
1	0	0	0	0	1	1	Adding one word
0	1	0	0	1	0	1	
0	0	1	0	1	1	0	
0	0	0	1	1	1	1	
1	1	0	0	1	1	0	Adding two words
1	0	1	0	1	0	1	
1	0	0	1	1	0	0	
0	1	1	0	0	1	1	
0	1	0	1	0	1	0	
0	0	1	1	0	0	1	
1	1	1	0	0	0	0	Adding three words
1	1	0	1	0	0	1	
1	0	1	1	0	1	0	
0	1	1	1	1	0	0	
1	1	1	1	1	1	1	Adding four words

For example, the message $x = 1010010$ does not appear in Table 1.2 as a possible code word. Assuming that a single error has occurred in the transmission of a code word we can locate the error and correct it using the parity check matrix H . This parity check matrix consists of seven column vectors, which give the binary representations of the decimal numbers 1 through 7.

$$Hx = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

Since the result is $(1, 0, 0)$, namely, the binary representation of the decimal number 4, the error occurs in the fourth position; hence the original code word was 1011010. Similarly, we can show that each of the 2^7 possible binary 7-tuples differs from a possible code word in at most one digit; and if there is a difference, the digit in which the "error" occurs can be located with the parity check matrix. However, when an actual code word is multiplied by this parity check matrix, the result is $(0, 0, 0)$ (see Exercises 6 and 7).

The parity check matrix H can be thought of as the defining matrix for this code. Note that the matrix H clearly has rank 3, and since H is a 3×7 matrix it represents a linear transformation from a vector space of dimension 7 to one of dimension 3. As we recall from linear algebra the kernel of this linear transformation is the set of solutions of $Hx = 0$ and the dimension of this kernel is $7 - 3 = 4$. By demonstrating that $Hx = 0$ whenever x is a code word, we can show that the row vectors of the generator matrix G are basis vectors for this kernel. Thus, the code words of the Hamming $(7, 4)$ code form a subspace of a vector space. Any code for which the code words form a subspace is said to be *linear*.

The code words of the Hamming $(7, 4)$ code can be considered to be coordinates of points in a seven-dimensional space where the entire space consists of points corresponding to the 2^7 possible messages, that is, the possible binary 7-tuples. Distance in this space is defined in terms of a function known as the *Hamming distance*.

Definition

The *Hamming distance* $d(x, y)$ between two binary n -tuples x and y is the number of components by which the n -tuples differ.

Thus, if $x = 1001110$ and $y = 1011101$, $d(x, y) = 3$. Clearly, the maximum distance between binary 7-tuples is 7, and, as you can easily verify, the minimum distance between any pair of nonzero code words in the Hamming (7, 4) code is 3. Since the minimum distance is 3 this is also known as the Hamming (7, 4, 3) code. Also note that the distance between 0000000 and any other binary 7-tuple x is just the number of ones in x , that is, the weight of x . Thus the *minimum weight* of this code is said to be 3.

To further illustrate the role of the Hamming distance in the Hamming (7, 4, 3) code, we first consider a more elementary code consisting of just the two code words 000 and 111. These two code words can be identified as opposite vertices in a three-dimensional cube with vertices consisting of all ordered triples of 0 and 1 where edges join pairs of vertices whose Hamming distance is 1, as shown in Fig. 1.6. Notice that the Hamming distance between two vertices in this cube counts the number of edges of the cube that must be traversed to go from one vertex to the other.

Whereas the Hamming distance between the two code words 000 and 111 is 3, the binary 3-tuples that could occur if exactly one error is made in transmitting the code word 000 would be those at distance

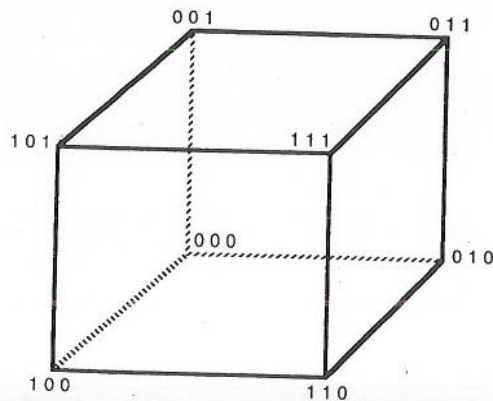


FIGURE 1.6 Cube determined by binary triples.

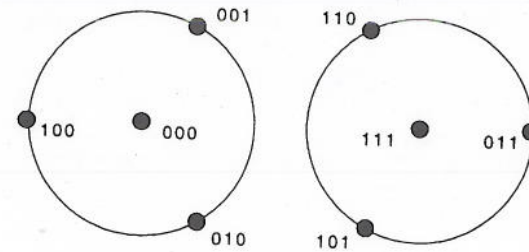


FIGURE 1.7 Spheres of binary 3-tuples.

1 from 000, namely, 001, 010, and 100. The set {001, 010, 100} is said to form a 1-*sphere*, centered at the code word 000. These same binary 3-tuples are located at a distance 2 from the other code word, 111. The vertex 111 is the center of a second 1-sphere consisting of all binary 3-tuples that could occur if exactly one error is made in transmitting 111 (Fig. 1.7). These two spheres partition the set of binary 3-tuples, so that every binary 3-tuple appears in one of these two spheres. Thus, if we assume that a given message contains one or fewer errors, we can decode it by locating the unique nearest code word.

Similarly, we can view the code words in the Hamming (7, 4, 3) code as select vertices in a seven-dimensional cube where edges again join pairs of vertices located a Hamming distance of 1 unit apart. Here the minimum distance between code words is also 3 and all binary 7-tuples lie in a set of nonoverlapping 1-spheres that exhaust the seven-dimensional cube (see Exercise 6). The decoding process we are using is that of locating the nearest code word. Codes with the property that all possible messages lie within or on nonoverlapping spheres of radius t , are called *perfect t -error correcting codes*. Thus, the Hamming (7, 4, 3) code, in addition to being linear, is a perfect 1-error-correcting code.

A result from coding theory (Blake, 1975, p. 185) shows that a perfect linear code is spanned by its minimum weight vectors. This means that the vectors of weight 3 span the Hamming (7, 4, 3) code. As we can easily verify, these are the vectors in the rows of the incidence table for the Fano plane. Furthermore, the rows of the generator matrix G form a basis for this set.

Exercises

1. Show that the points and lines of the incidence table (Table 1.1) satisfy the axioms for a projective plane.
2. Demonstrate that the Fano plane given by the incidence table (Table 1.1) is isomorphic to that given in model P.1 of Section 1.3.
3. Verify that any pair of coordinate vectors in the incidence table (Table 1.1) differ in exactly four components, that is, their Hamming distance is 4.
4. Write out the binary representations of the decimal numbers 1 through 15.
5. Verify that there are exactly $2^7 - 16$ binary 7-tuples that are not code words in the Hamming (7, 4, 3) code.
6. (a) Show that there are exactly seven binary 7-tuples that differ from the code word 1000011 in exactly one digit. (b) Apply the parity check matrix H to one of these seven and verify that it does locate the position in which the digit differs.
7. Show that $Hx = 0$ for each row vector in the generator matrix G .
8. Obtain all possible code words in the linear (5, 3) binary code with generator matrix G' .

$$G' = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

9. Show that the Hamming distance is a metric, that is, that it satisfies each of the following conditions:
 - (i) $d(x, y) = 0$ iff $x = y$.
 - (ii) $d(x, y) = d(y, x)$.
 - (iii) $d(x, z) \leq d(x, y) + d(y, z)$.
10. Verify that the minimum distance between any pair of code words in the Hamming (7, 4, 3) code is 3.
11. Show that the set of code words in the Hamming (7, 4, 3) code can be obtained by adding the two 7-tuples 0000000 and 1111111 to the fourteen 7-tuples that occur either as rows of Table 1.1 or as rows of the incidence table obtained from Table 1.1 by interchanging 0's and 1's.

1.5 Desargues' Configurations

In this section we consider an axiomatic system for one more finite structure. We shall see that this structure not only satisfies the principle of duality but also exhibits an interesting relation between points and lines similar to the *polarity* relation of projective geometry. This relation involves points that do not lie on a line. Since the term "geometry" is usually reserved for structures in which each pair of points determines a unique line, we refer to the structures that satisfy our axioms as Desargues' configurations. Desargues' configurations are so named because they illustrate a theorem in real projective geometry known as *Desargues' theorem*. This theorem is stated in terms of two particular properties of triangles, that is, sets of three noncollinear points. If two triangles ABC and DEF have the

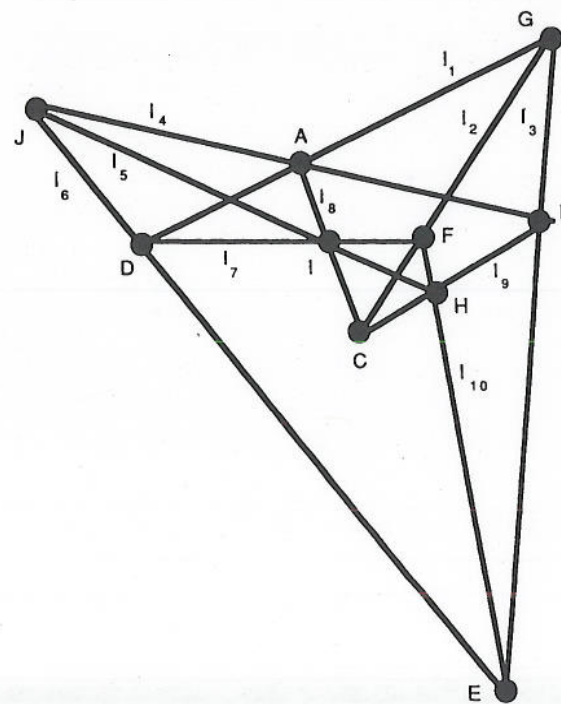


FIGURE 1.8 A Desargues' configuration.

property that lines joining corresponding vertices (i.e., AD , BE , CF) are concurrent, the triangles are said to be *perspective from a point*. Similarly, if the triangles possess the dual property that the intersections of corresponding sides are collinear, they are said to be *perspective from a line*. With these definitions, Desargues' theorem can be stated succinctly.

Desargues' Theorem

If two triangles are perspective from a point, then they are perspective from a line.

An example of a Desargues' configuration and its corresponding incidence table is shown in Fig. 1.8 and Table 1.3 (as in Section 1.4 entries of 0 and 1 represent nonincidence and incidence, respectively). As you can see, either from the configuration or the incidence table, ABC and DEF are triangles that are perspective from point G and line l_5 .

Careful scrutiny of either the structure shown in Fig. 1.8 or the corresponding incidence table (Table 1.3) will lead to the observation that for each point M in the structure there is a line m such that no lines join M with points on m . The point M and line m are referred to as *pole* and *polar*, respectively. This *pole-polar* relation is described in detail by the following definitions and axioms.

TABLE 1.3 Incidence Table for a Desargues' Configuration.

	l_1	l_2	l_3	l_4	l_5	l_6	l_7	l_8	l_9	l_{10}
A	1	0	0	1	0	0	0	1	0	0
B	0	0	1	1	0	0	0	0	1	0
C	0	1	0	0	0	0	0	1	1	0
D	1	0	0	0	0	1	1	0	0	0
E	0	0	1	0	0	1	0	0	0	1
F	0	1	0	0	0	0	1	0	0	1
G	1	1	1	0	0	0	0	0	0	0
H	0	0	0	0	1	0	0	0	1	1
I	0	0	0	0	1	0	1	1	0	0
J	0	0	0	1	1	1	0	0	0	0

Axioms for Desargues' Configurations

Undefined Terms. Point, line, on.

Defined Terms. If there are no lines joining a point M with points on line m (M not on m), m is called a *polar* of M and M is called a *pole* of m .

Axiom DC.1. There exists at least one point.

Axiom DC.2. Each point has at least one polar.

Axiom DC.3. Each line has at most one pole.

Axiom DC.4. Two distinct points are on at most one line.

Axiom DC.5. There are exactly three distinct points on each line.

Axiom DC.6. If line m does not contain point P , then there is a point on both m and any polar of P .

It should be no surprise that the Desargues' configuration shown in Fig. 1.8 provides a model for this axiomatic system. Furthermore, as you can easily verify, this axiomatic system satisfies the principle of duality (see Exercise 3).

Other properties of Desargues' configurations are given by the following theorems. The first of these theorems describes an important property of poles and polars. We encounter this property again when we study the polarity relation in projective geometry in Chapter 4.

Theorem DC.1

If P is on a polar of point Q , then Q is on each polar of P .

Proof

Let P be on q where q is a polar of Q (Fig. 1.9). Thus, since Q is not on q (why?), q must contain two more points, R and S , which are distinct from P and Q (Axiom DC-5). Let p be a polar of P and assume Q is not on p . Then by Axiom DC-6, p and q must intersect at a point, namely, P , R , or S . But P is not on p by definition. And if R or S are on p , then q is a line joining P with a point on its polar, contradicting the definition. Thus, Q is on p . ■

The usefulness of the property described in Theorem DC.1 is illustrated in the proofs of the following two theorems, which verify that the correspondence between poles and polars is one-to-one.

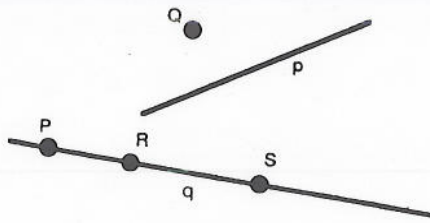


FIGURE 1.9 Proof DC.1.

Theorem DC.2

Each point has exactly one polar.

Proof

Let P be an arbitrary point. By Axiom DC.2, P has at least one polar p . Assume P has a second polar p' . By Axioms DC.4 and DC.5 there is a point T on p' but not on p . Let t be a polar of T . Then by Axiom DC.6, p and t intersect. But since T is on p' , P is on t by the previous theorem, and so line t joins P to a point on p , contradicting the definition of polar. Thus P has exactly one polar. ■

Theorem DC.3

Each line has exactly one pole.

Proof

By Axiom DC.3 each line has at most one pole. Hence, it suffices to show that an arbitrary line p has at least one pole. Let R , S and T be the three points on p , and let r and s be the unique polars of R and S (Theorem DC.2). Clearly, S is not on r (why?). Therefore, by Axiom DC.6, there is a point P on r and s . But P is on the polars of R and S ; hence, by Theorem DC.1, R and S are on the unique polar of P . So p is the polar of P or P is the pole of p . ■

These theorems and the following exercises illustrate that even though a finite structure may involve a limited number of points and lines, the structure may possess "strange" properties such as duality and polarity, which are not valid in Euclidean geometry. Another unexpected property illustrated by the exercises is that in Desargues' configurations, a line has exactly three lines parallel to

it through its pole; that is, there are points through which there are three lines parallel to a given line (see Exercise 6). Because of this latter property, Desargues' configurations can be classified as non-Euclidean.

Exercises

1. In the Desargues' configuration shown in Fig. 1.8 find the pole of line AB and the polar of C .
2. (a) Find two triangles in the Desargues' configuration in Fig. 1.8 that are perspective from point C . From which line are these two triangles perspective? (b) Find two triangles in the Desargues' configuration in Fig. 1.8 that are perspective from line AB . From which point are these two triangles perspective?

The following exercises ask you to verify theorems in the axiom system for Desargues' configurations. This means you must justify your proofs on the basis of the axioms— you cannot verify your reasoning on the basis of the model or incidence table given in this section.

3. Verify the duals of Axioms DC.1 through DC.6.
4. Prove: There is a line through two distinct points iff their polars intersect.
5. Prove: If p and q are two lines both parallel to m (i.e., p and m have no common points, nor do q and m), then p and q intersect at the pole of m .
6. Prove: Through a point P there are exactly three lines parallel to p , the polar of P (i.e., the three lines have no points in common with line p).
7. Prove: There are exactly 10 points and 10 lines in a Desargues' configuration.
8. Prove Desargues' theorem. That is, show that if ABC and $A'B'C'$ are two triangles perspective from a point P , then they are perspective from a line. (Assume that the points A , B , C , A' , B' , C' , and P are all distinct and that no three of the points A , B , C , A' , B' , C' are collinear.)

The following exercises ask you to work in an axiomatic system for finite structures known as *Pappus' configurations*. These axioms are as follows:

Axioms for Pappus' Configurations

Undefined Terms. Point, line, on.

Defined Terms. Two lines without a common point on them are *parallel*.

Two points without a common line on them are *parallel*.

Axiom PC.1. There exists at least one line.

Axiom PC.2. There are exactly three distinct points on every line.

Axiom PC.3. Not all points are on the same line.

Axiom PC.4. There is at most one line on any two distinct points.

Axiom PC.5. If P is a point not on a line m , there is exactly one line on P parallel to m .

Axiom PC.6. If m is a line not on a point P , there is exactly one point on m parallel to P .

9. (a) Construct a model of a Pappus' configuration. (b) Construct an incidence table for this model.
10. Verify that this axiomatic system satisfies the principle of duality.
11. Prove: If m is a line, there are exactly two lines parallel to m .
12. Prove: There are exactly nine points and nine lines in a Pappus' configuration.
13. Prove: If m and n are parallel lines with distinct points A, B, C on m and A', B', C' on n , then the three intersection points of AC' with CA' , AB' with BA' , and BC' with CB' are collinear. (This result, which is valid in some projective planes, is known as the Theorem of Pappus.)

1.6 Suggestions for Further Reading

Albert, A. A., and Sandler, R. (1968). *An Introduction to Finite Projective Planes*. New York: Holt, Rinehart and Winston. (Contains a thorough group theoretic treatment of finite projective planes.)

Anderson, I. (1974). *A First Course in Combinatorial Mathematics*. Oxford, England: Clarendon Press. (Chapter 6 discusses block designs and error-correcting codes.)

Beck, A., Bleicher, M. N., and Crowe, D. W. (1972). *Excursions into Mathematics*. New York: Worth. (Sections 4.9–4.15 give a very readable discussion of finite planes, including the development of analytic models.)

Benedicty, M., and Sledge, F. R. (1987). *Discrete Mathematical Structures*. Orlando, FL: Harcourt Brace Jovanovich. (Chapter 13 gives an elementary presentation of coding theory.)

Cipra, B. A. (1988). Computer search solves old math problem. *Science* 242:1507–1508. (Reports on verification that there is no projective plane of order 10.)

Gallian, J. (1996). Error detection methods. *ACM Computing Surveys*. Vol. 28, No. 3, pp. 504–517.

Gensler, H. J. (1984). *Gödel's Theorem Simplified*. Lanham, MD: University Press of America.

Hofstadter, D. R. (1984). Analogies and metaphors to explain Gödel's theorem. In *Mathematics: People, Problems, Results*. D. M. Campbell and J. C. Higgins (Eds.), Vol. 2, pp. 262–275. Belmont, CA: Wadsworth.

Kolata, G. (1982). Does Gödel's theorem matter to mathematics? *Science* 218: 779–780.

Lam, C. W. H. (1991). The Search for a Projective Plane of Order 10. *The American Mathematical Monthly*. Vol. 98, No. 4, pp. 305–318.

Lockwood, J. R., and Runion, G. E. (1978). *Deductive Systems: Finite and Non-Euclidean Geometries*. Reston, VA: NCTM (Chapter 1 contains an elementary discussion of axiomatic systems.)

Nagel, E. and Newman, J. R. (1956). Gödel's proof. In *The World of Mathematics*. J. R. Newman (Ed.), Vol. 3, pp. 1668–1695. New York: Simon and Schuster.

Pless, V. (1982). *Introduction to the Theory of Error-Correcting Codes*. New York: Wiley. (A well-written explanation of this new discipline and the mathematics involved.)

Smart, J. R. (1998). *Modern Geometries*, 5th ed. Pacific Grove, CA: Brooks/Cole. (Chapter 1 contains an easily readable discussion of axiomatic systems and several finite geometries.)

Thompson, T. M. (1983). *From Error-Correcting Codes Through Sphere Packings to Simple Groups*. The Carus Mathematical Monographs, No. 21. Ithaca, NY: MAA (Incorporates numerous historical anecdotes while tracing 20th century mathematical developments involved in these topics.)

Readings on Latin Squares

Beck, A., Bleicher, M. N. and Crowe, D. W. (1972). *Excursions into Mathematics*, pp. 262–279. New York: Worth.

- Crowe, D. W., and Thompson, T. M. (1987). Some modern uses of geometry. In *Learning and Teaching Geometry, K-12, 1987 Yearbook*, M. M. Lindquist and A. P. Schulte (Eds.), pp. 101–112. Reston, VA: NCTM.
- Gardner, M. (1959). Euler's spoilers: The discovery of an order-10 Graeco-Latin square. *Scientific American* 201: 181–188.
- Sawyer, W. W. (1971). Finite arithmetics and geometries. In *Prelude to Mathematics*, Chap. 13. New York: Penguin Books.

2

Non-Euclidean Geometry

CHAPTER

2.1 Gaining Perspective

Mathematics is not usually considered a source of surprises, but non-Euclidean geometry contains a number of easily obtainable theorems that seem almost “heretical” to anyone grounded in Euclidean geometry. A brief encounter with these “strange” geometries frequently results in initial confusion. Eventually, however, this encounter should not only produce a deeper understanding of Euclidean geometry, but it should also offer convincing support for the necessity of carefully reasoned proofs for results that may have once seemed obvious. These individual experiences mirror the difficulties mathematicians encountered historically in the development of non-Euclidean geometry. An acquaintance with this history and an appreciation for the mathematical and intellectual importance of Euclidean geometry is essential for an understanding of the profound impact of this development on mathematical and philosophical thought. Thus, the study of Euclidean and non-Euclidean geometry as mathematical systems can be greatly enhanced by parallel readings in the history of geometry. Since the mathematics of the ancient Greeks was primarily geometry, such readings provide an introduction to the history of geometry.