Axioms and Proofs

Axioms are the assumptions upon which proofs are based. Axioms are propositions, stated using explicitly defined terms, which are assumed to be true. Axioms need not actually be “true in reality”, but serve to clarify the properties of the definitions. Sometimes, axioms are called postulates. In other contexts, postulates refer to unstated assumptions, such as the laws of logic, arithmetic and set theory.

A collection of axioms or axiom system or formal system is assumed to be true for the purpose of determining what can be deduced from it. Any proposition provable from an axiom system is true of any specific example which satisfies the axioms. This is the principle use of axiom systems. An axiom system usually serves to summarize some properties shared by many specific applications and examples; and by proving propositions about the axiom system, one proves propositions about all the summarized applications and examples. The two sections which follow illustrate this role of axiom systems in algebra and geometry.

In the text, most proofs are based upon the “axioms” often called the Laws of Algebra for the Natural Numbers and the Real Numbers. The standard axiom system for the Natural Numbers is often called “The Peano Axioms” and is based upon the concept of “a successor”, which formalizes the notion of counting. The appendix to the text (Rosen: Discrete Mathematics) contains axiom systems for the natural and real numbers.   All the usual Laws of Algebra can be proven from these axiom systems, but this is a long and time-consuming process and will only be illustrated briefly in class. This is a second use of an axiom system: to explicitly and categorically define a single important example. How successful these systems are in doing this is a question which would take us far beyond the scope of this course.

Axioms and Abstract Algebra

Abstract algebra is the study of sets with operations.

Definition: A (binary) operation on set A is a function: $\circ : A\times A \to A$.
A unary operation on set A is a function: $\sim: A \to A$.
One usually writes "$\circ(a,b)$" as "$a\circ b$", and "$\sim(a)$" as "$\sim a$".

There are five standard sets with the usual arithmetic operations:

$\mathbb{N}$, the Naturals $\mathbb{Z}$, the Integers $\mathbb{Q}$, the Rationals;
$\mathbb{R}$, the Reals $\mathbb{C}$, the Complex Numbers

One usually requires that the operation(s) satisfy certain axioms.

++++++++++++++++++++++++++++++++++++++

Definition: A GROUP is a set, G, with operation, $\circ$, satisfying:

G1: There exists an identity e in G with $e\circ g = g\circ e = g$ for all g in G;
G2: For any g,h,k in G, $g\circ(h\circ k) = (g\circ h)\circ k$ (associative);
G3: For any g in G, there is an inverse $\sim g$ in G with $g\circ\sim g = e = \sim g\circ g$.
(G4: A commutative group also satisfies $g\circ h = h\circ g$ for all g,h in G.)

Remark: May write " $g^n = g\circ g\circ\ldots\circ g$ (n-times) " and " $g^{-1} = \sim g$ ".

Example I: Let A = $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ with "$\circ$, e, $\sim a$" = "+, 0, -a".
Example II: Let A = $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$: A – {0} with "$\circ$, e, $\sim a$" = "•, 1, $^1/_a = a^{-1}$".

The above examples are commutative groups. (Why not $\mathbb{Z}$ in II?)

Exercise: For A = $\mathbb{R}^+$, the positive reals, show that the binary operation of exponentiation is not associative and has no identity.

Example III: X = any set. G = {all 1-1 & onto functions $f: X \rightarrow X$ }, ◦ = usual composition, identity e(x) = x and usual inverse functions. If X is finite, such groups are called Permutation Groups (Chapter 5).

Example IV: The following table defines a finite, non-commutative group called the quaternion 8-group, Q = { 1, -1, i, -i, j, -j, k, -k }, which was once very important in physics.

◦	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

The following is true about any group, G.

Proposition: The group identity, e, is unique.
Proof: Suppose e & f in G are identities, then f = e◦f = e (why?). QED

Exercise: Rewrite the axioms for a group in the notation of formal logic. Answer the “why?” in the above proof and then prove the following proposition.

Proposition: For every g in G, $\sim g = g^{-1}$ is unique.

Exercise: Prove Example III is a non-commutative group for #(X)>2. Hint: Show that the composition of 1-1 functions is 1-1 and the same for onto. We know what are the identity and inverses.

++++++++++++++++++++++++++++++++++++++

Definition: A RING is a set, R, with 2 operations, + (addition) and $\bullet$ (multiplication) satisfying the following axioms:

R0: Under + alone, R is a commutative group with additive identity "0" and additive inverses "$-r$".

R1: There exists a multiplicative identity "1" in R with $1\bullet r = r\bullet 1 = r$ for all r in R . (The additive inverse of "1" is written "-1".)

R2: For all r,s,t in R, $r\bullet (s\bullet t) = (r\bullet s)\bullet t$.

R3: For all r,s,t in R, $r\bullet(s+t) = (r\bullet s)+(r\bullet t)$ and $(s+t)\bullet r = (s\bullet r)+(t\bullet r)$.

(R4: A commutative ring also satisfies $r\bullet s = s\bullet r$ for all r,s in R .)

Example I: Integers, $\mathbb{Z}$, under + and $\bullet$ are a commutative ring.

Example 2: For a non-empty set, X , P(X) , the set of all subsets of X, is a ring with $+ = \cup$, $\bullet = \cap$, $0 = \varnothing$, and $1 = X$.

The following is true about any ring, R.

Proposition: (a) The multiplicative identity is unique.

(b) For all r in R, $r\bullet 0 = 0\bullet r = 0$ and $(-1)\bullet r = r\bullet(-1) = -r$.

Proof: (a) Done. (b) For all r,s: $r\bullet s = r\bullet(s+0) = r\bullet s + r\bullet 0$, hence $r\bullet 0 = 0$.

Exercise: Prove the second part of (b) in the above proposition.

Definition: A commutative ring is a FIELD if it also satisfies:

R5: For all r in R-{0}, there is an r^{-1} in R-{0} with $r\bullet r^{-1} = 1 = r^{-1}\bullet r$.

(So, R-{0} is a commutative group under $\bullet$ alone.)

Example II: $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ under + and $\bullet$ are fields.

Example III: Polynomials (with coefficients in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$) are a commutative ring under polynomial multiplication (FOIL, etc).

Exercise: Why is it not a field when the coefficients are a field?

Example IV: Square matrices (with entries in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$) are a non-commutative ring under matrix multiplication.

Exercise: **Why is it not a field when the entries are a field?**

The axioms for rings and fields resemble the usual Laws of Algebra; indeed, rings and/or fields are sometimes called algebras. Most of the usual laws of algebra hold true for all commutative rings.

Exercise: **Show that the set of all 2-by-2 real matrices under the usual operations of matrix addition and multiplication constitute a non-commutative ring. Show that if both diagonal entries equal the same number, “a” , and the non-diagonal entries equal “± b”, it is a field:**

$$\begin{vmatrix} a & -b \\ b & a \end{vmatrix}$$

Rings and fields may be finite. Consider “clock arithmetic”, which is called “mod 12” arithmetic. Relabel the numbers on a clock-face as “0” through “11”. Do addition and multiplication as usual and then take the remainder after dividing by “12”. For example:

$5+2 = 7$ $\qquad$ $5+9 = 2$ $\qquad$ $5 \cdot 2 = 10$ $\qquad$ $5 \cdot 9 = 9$

For “modular 10” arithmetic, take the units digit after each operation.

Example V: **“Modular n” arithmetic on the set, {0, 1, …, n-1}, defines a commutative ring. If n is a prime, it defines a field.**

Applications

Groups occur frequently in mathematics and physics where they are used to specify symmetries. Consider a regular tetrahedron (four vertices, four faces all equilateral triangles). The twelve rigid motions which transform the tetrahedron back onto itself are a group under composition. Groups are used in chemistry to study crystalline structures. Rings occur in cryptology and quantum mechanics.

Axioms and Plane Geometry

Definitions: Points are elements of a set (called the plane).
Lines are certain subsets of points.

Axioms: G1: Two points determine (elements of) a unique line.
G2: Two lines determine (intersect in) at most one point.
G3: There exist (at least) 3 non-colinear points (3 points not all elements of the same line).

Notice, according to the definitions, lines are subsets containing points as elements. Axiom G3 is needed to ensure we have a “plane”.

Exercise: Rewrite these axioms in the notation of formal logic.

The set of points need not be infinite; indeed, it need not resemble a “normal” set of planar points. This example satisfies the axioms.

Points = { a, b, c, d }
Lines = { ab, ac, ad, bc, bd, cd } , where ab = {a, b}.

Question: Do parallel lines (lines with empty intersection) exist?

They do in the above example:
ab & cd are parallel, as are ac & bd and ad & bc.

Now consider the following example, which also satisfies the axioms.

Points = { a, b, c, d, x, y, z }
Lines = { abz, acy, adx, bcx, bdy, cdz, xyz } , where abc = {a,b,c}.

In this example there are no parallel lines.

Exercise: Verify that each example satisfies the axioms.

The question − "Do parallel lines exist?" − cannot be answered on the basis of these axioms. In such situations, the question is called independent of the axioms. To remedy this situation, one might replace these axioms with one of the following two systems:

Affine:

A1. Two points determine a unique line.
A2: A line, L, and a point p not on L, determine a unique line, M, passing through p and parallel to L ($L \cap M = \varnothing$).
A3: There exist 3 non-colinear points.

Projective:

P1. Two points determine a unique line.
P2: Two lines determine at least one point.
P3: There exist 4 points, no 3 of which are colinear.

The first are the axioms for affine plane geometry and the second are for projective plane geometry. Both are useful. The 4-point example above satisfies A1-A3 and the 7-point example satisfies P1-P3.

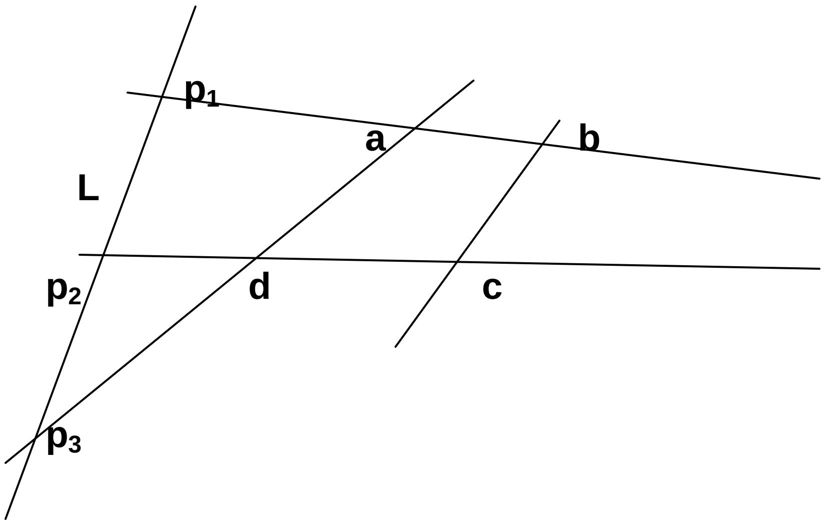
Exercise: Verify the above assertion.

The following propositions are true for projective geometry.

Proposition: Two lines intersect in (determine) a unique point.
Proof: By P2, any two lines intersect in at least one point. Suppose there were two lines, L_1 & L_2 which intersected in (at least) two points, p_1 & p_2 ; then these two points would determine (be elements of) two lines. This would contradict P1, so it can't happen. QED

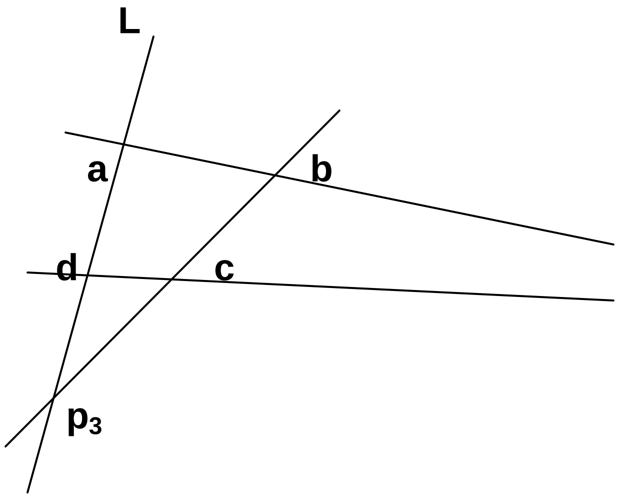
Proposition: Given a line, L, there is a point, q, not on L.
Proof: Follows by contradiction from P3.

Proposition: Any line, L, contains at least 3 points.
Proof: (Use the diagram only to help keep track.)



By P3 there are points, a,b,c,d, no 3 of which are collinear, as shown. There are now three cases: (i) L contains none of a,b,c,d as shown above; (ii) L contains exactly one of a,b,c,d; (iii) L contains exactly two of a,b,c,d. We'll do case (i) and (iii) only.

(i) Line <u>ab</u> must intersect L in a point p_1. Line <u>cd</u> must intersect L in a point p_2. Line <u>ad</u> must intersect L in a point p_3. These points are distinct: if not, , we have two lines containing the same pair of points, which is prohibited by P1. QED (Yes, in this case there is also a p_4…)

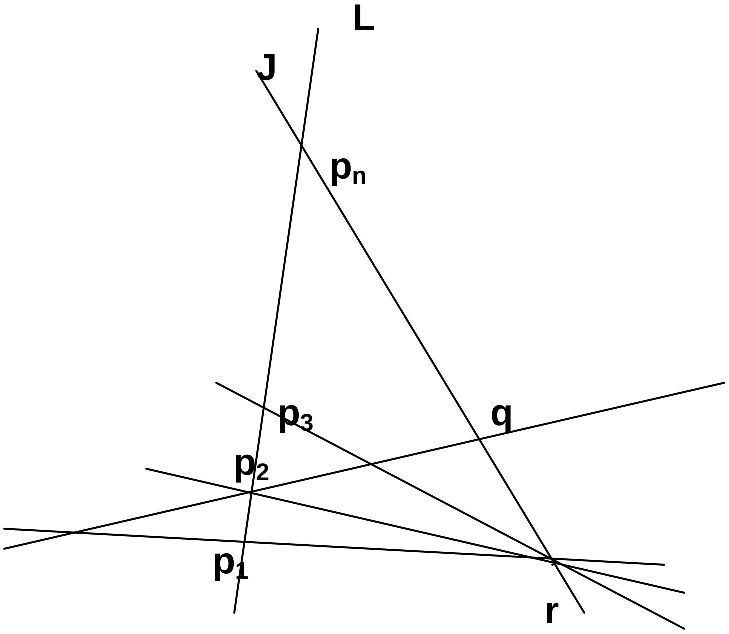


(iii) Let a & d be on L. Line bc must intersect L in a point p_3, distinct from a and d. QED. (No p_4 is guaranteed)

<u>Exercise</u>: Argue case (ii).

These propositions hold true for any “geometry” which satisfies the 3 axioms, whether or not the set of all points is finite or infinite. It clearly holds for the 7 point example given above, where all lines contain precisely 3 points. In general, we also have:

<u>Proposition:</u> If some line, L, has exactly n points, #(L)=n , then every line has exactly n points.
Proof: Let L and K be distinct lines, with L = {p_1,p_2,…,p_n}.



Prove the proposition by justifying the following seven propositions.
(i)L and K intersect in a distinct point, say, L∩K={p_2}.
(ii)There is a point, q, on K but not on L.
(iii)There exists a third line, J=$\underline{qp}_n$, distinct from L and K.
(iv)There exists a point, r, on J but not on L, distinct from q.
(v)There exists n distinct lines determined by the {r, p_i}.
(vi)These n lines determine n distinct points on K (one may be q).
(vii)So #(K)≥#(L). Reverse K and L: #(L)≥#(K), so #(K)=#(L). QED

<u>Exercise:</u> Justify each of the 7 steps above from the Axioms.
The above proposition is often stated as: “In any finite projective geometry, every line has the same number of points.” Other propositions and theorems may be proven from these axioms.

Proposition: In a projective geometry with a finite set of points, the number of points equals the number of lines equals $n^2 - n + 1$, for some integer n>2, where there are n points on each line and n lines intersecting at each point. (In the second example, n=3, and there are $7=3^2-3+1$ points.)

Unsolved Question: For what n does a projective geometry exist? It is conjectured that n-1 must be a prime power.

Optional Exercise: Find a projective geometry for n=4.

Theorem: Given any projective geometry, an affine geometry may be created by removing a line and all its points.

Theorem: Given any affine geometry, a projective geometry may be created by adding, as an additional line, the "points at infinity" for each family (or pencil) of mutually parallel lines.

In terms of the two examples given earlier, removing the line xyz and its points creates the affine example. Adding 3 new "points at infinity", {x,y,z} (z is point at infinity for parallel lines ab and cd) re-creates the projective example.

The complete proofs of these and other propositions and theorems are long. See the text book by Robin Hartshorne, "Foundations of Projective Geometry".

http://books.google.com/books/about/Foundations_of_Projective_Geometry.html?id=EUfRQwAACAAJ

It is interesting to visualize "Points at Infinity" for the usual 2 dimensional, affine geometry we all use intuitively. They were used

by Renaissance painters to render perspective. Two parallel lines, like railroad tracks, appear to intersect in the far distance (at infinity).

The usual geometry we all know requires the concepts of distance and angles and was formalized by Euclid using 5 axioms.

> **E1: Two points determine a unique line.**
> **E2: A line may be extended (or shortened) indefinitely.**
> **E3: Two points determine a unique circle (distance measure).**
> **E4: All flat angles are equal (angle measure).**
> **E5: A line, L, and a point p not on L, determine a unique line, M, passing through p and parallel to L (the famous 5th Axiom).**

E1 and E2 say we have a straight-edge. E3 says we have a compass. Proving theorems via Euclid is closely related to the so-called constructions by straight-edge and compass.

These axioms are not quite sufficient. One also must define circle and angle and other notions, such as:

> **A point is in the <u>interior</u> of a circle or angle if ... .**
>
> **A point is <u>between</u> two other points on a line if … .**

Essentially, Euclid assumed that "drawing pictures" was a valid way to reason without formally defining concepts like the above (a point is in the interior of a circle means any line thru the point intersects the circle).

Euclid probably thought these notions were so obvious that definitions were unnecessary; but a rigorous formulation of geometry does require them. David Hilbert produced a rigorous set of some 20 axioms around 1910; but it is complicated and seldom used. See:

http://userpages.umbc.edu/~rcampbel/Math306/Axioms/Hilbert.html