1

Projective spaces

In this chapter, we describe projective and affine spaces synthetically, in terms of vector spaces, and derive some of their geometric properties.

1.1 Fields and vector spaces

Fields will not necessarily be commutative; in other words, the term "field" will mean "division ring" or "skew field", while the word "commutative" will be used where necessary. Often, though, I will say "skew field", as a reminder. (Of course, this refers to the multiplication only; addition will always be commutative.)

Given a field F, let

$$I = \{n \in \mathbb{N} : (\forall \alpha \in F)\ n \cdot \alpha = 0\} = \{n \in \mathbb{N} : n \cdot 1_F = 0\}.$$

Then I is an ideal in $\mathbb{N}$, hence $I = (c)$ for some non-negative integer c called the *characteristic* of F. The characteristic is either 0 or a prime number. For each value of the characteristic, there is a unique *prime field* which is a subfield of any field of that characteristic: the rational numbers in characteristic zero, and the integers modulo p in prime characteristic p.

Occasionally I will assume rudimentary results about field extensions, degree, and so on.

Much of the time, we will be concerned with finite fields. The main results about these are as follows.

Theorem 1.1 (Wedderburn's Theorem) *A finite field is commutative.*

Theorem 1.2 (Galois' Theorem) *A finite field has prime power order. For any prime power q, there is a unique finite field of order q.*

The unique field of order q is denoted by $\mathrm{GF}(q)$. If $q = p^d$ with p prime, its additive structure is that of a d-dimensional vector space over its prime field $\mathrm{GF}(p)$ (the integers modulo p). Its multiplicative group is cyclic (of order $q-1$), and its automorphism group is cyclic (of order d). If $d = 1$ (that is, if q is prime), then $\mathrm{GF}(q)$ is the ring of integers mod q.

An *anti-automorphism* of a field is a bijection σ with the properties

$$\begin{aligned}(c_1+c_2)^\sigma &= c_1^\sigma + c_2^\sigma,\\ (c_1\cdot c_2)^\sigma &= c_2^\sigma \cdot c_1^\sigma.\end{aligned}$$

The identity (or, indeed, any automorphism) is an anti-automorphism of a commutative field. Some non-commutative fields have anti-automorphisms. A well-known example is the field $\mathbb{H}$ of quaternions, with a basis over $\mathbb{R}$ consisting of elements $1, i, j, k$ satisfying

$$i^2 = j^2 = k^2 = -1, \qquad ij = k, \quad jk = i, \quad ki = j;$$

the anti-automorphism is given by

$$a + bi + cj + dk \mapsto a - bi - cj - dk.$$

Others, however, do not.

The *opposite* of the field $(F, +, \cdot)$ is the field $(F, +, \circ)$, where the binary operation $\circ$ is defined by the rule

$$c_1 \circ c_2 = c_2 \cdot c_1.$$

Thus, an anti-automorphism of F is just an isomorphism between F and its opposite F°.

For non-commutative fields, we have to distinguish between left and right vector spaces. In a left vector space, if we write the product of the scalar c and the vector $\mathbf{v}$ as $c\mathbf{v}$, then $c_1(c_2\mathbf{v}) = (c_1c_2)\mathbf{v}$ holds. In a right vector space, this condition reads $c_1(c_2\mathbf{v}) = (c_2c_1)\mathbf{v}$. It is more natural to write the scalars on the right (thus: $\mathbf{v}c$), so that the condition is $(\mathbf{v}c_2)c_1 = \mathbf{v}(c_2c_1)$). A right vector space over F is a left vector space over F°.

Our vector spaces will almost always be finite dimensional.

For the most part, we will use left vector spaces. In this case, it is natural to represent a vector by the row tuple of its coordinates with respect to some basis; scalar multiplication is a special case of matrix multiplication. If the vector space has dimension n, then vector space endomorphisms are represented by $n \times n$ matrices, acting on the right, in the usual way:

$$(\mathbf{v}A) = \sum_i v_i A_{ij}$$

if $\mathbf{v} = (v_1, \ldots, v_n)$.

The *dual space* V^* of a (left) vector space V is the set of linear maps from V to F, with pointwise addition and with scalar multiplication defined by

$$(\mathbf{f}c)\mathbf{v} = \mathbf{f}(c\mathbf{v}).$$

Note that this definition makes V^* a right vector space.

1.2 Projective spaces

A projective space of dimension n over a field F (not necessarily commutative!) can be constructed in either of two ways: by adding a hyperplane at infinity to an affine space, or by "projection" of an $(n+1)$-dimensional space. Both methods have their importance, but the second is the more natural.

Thus, let V be an $(n+1)$-dimensional left vector space over F. The *projective space* $\mathrm{PG}(n,F)$ is the geometry whose *points, lines, planes,* ... are the vector subspaces of V of dimensions 1, 2, 3, ...

Note that the word "geometry" is not defined here; the properties which are regarded as geometrical will emerge during the discussion.

Note also the dimension shift: a d-dimensional projective subspace (or flat) is a $(d+1)$-dimensional vector subspace. This is done in order to ensure that familiar geometrical properties hold. For example, two points lie on a unique line; two intersecting lines lie in a unique plane; and so on. Moreover, any d-dimensional projective subspace is a d-dimensional projective space in its own right (when equipped with the subspaces it contains).

To avoid confusion (if possible), I will from now on reserve the term *rank* (in symbols, rk) for vector space dimension, so that unqualified "dimension" will be geometric dimension.

A *hyperplane* is a subspace of codimension 1 (that is, of dimension one less than the whole space). If H is a hyperplane and L a line not contained in H, then $H \cap L$ is a point.

A projective plane (that is, $\mathrm{PG}(2,F)$) has the property that any two lines meet in a (unique) point. For, if $\mathrm{rk}(V) = 3$ and $U, W \subseteq V$ with $\mathrm{rk}(U) = \mathrm{rk}(W) = 2$, then $U + W = V$, and so $\mathrm{rk}(U \cap W) = 1$; that is, $U \cap W$ is a point. From this, we deduce:

Proposition 1.3 (Veblen's Axiom) *If a line intersects two sides of a triangle but doesn't contain their intersection, then it intersects the third side also.*

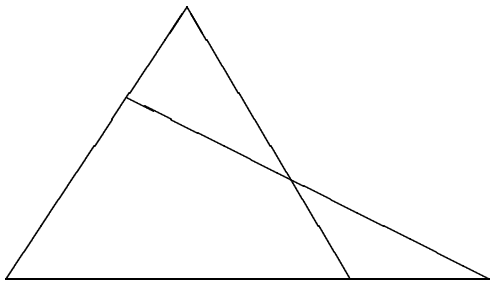

Figure 1.1: Veblen's Axiom

For the triangle is contained in a plane, and the hypotheses guarantee that the line in question is spanned by points in the plane, and hence also lies in the plane.

Veblen's axiom is sometimes called the Veblen-Young Axiom or Pasch's Axiom. The latter name is not strictly accurate: Pasch was concerned with real projective space, and the fact that if two intersections are inside the triangle, the third is outside; this is a property involving order, going beyond the incidence geometry which is our concern here. In Section 3.1 we will see why 1.3 is referred to as an "axiom".

Another general geometric property of projective spaces is the following.

Proposition 1.4 (Desargues' Theorem) *In Figure 1.2, the three points p, q, r are collinear.*

In the case where the figure is not contained in a plane, the result is obvious geometrically. For each of the three points p, q, r lies in both the planes $a_1b_1c_1$ and $a_2b_2c_2$; these planes are distinct, and both lie in the 3-dimensional space spanned by the three lines through o, and so their intersection is a line.

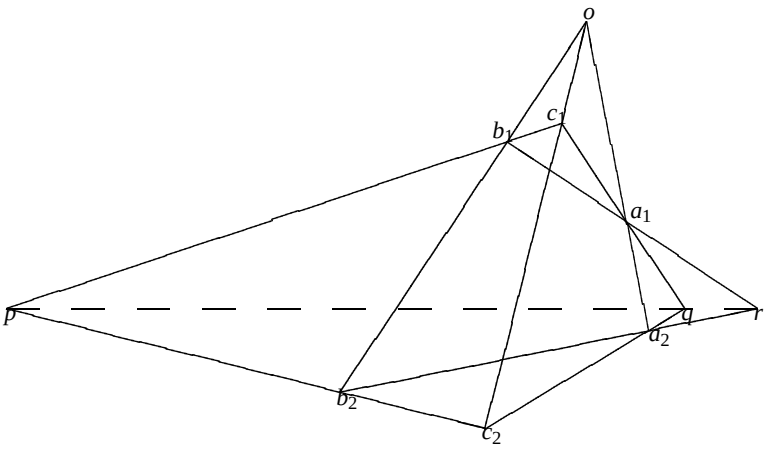

Figure 1.2: Desargues' Theorem

The case where the figure is contained in a plane can be deduced from the "general" case as follows. Given a point o and a hyperplane H,write $aa' \sim bb'$ if oaa', obb' are collinear triples and the lines ab and $a'b'$ intersect in H (but none of the points a, a', b, b' lies in H). Now Desargues' Theorem is the assertion that the relation $\sim$ is transitive. (For p, q, r are collinear if and only if every hyperplane containing p and q also contains r; it is enough to assume this for the hyperplanes not containing the points a, a', etc.) So suppose that $aa' \sim bb' \sim cc'$. The geometric argument of the preceding paragraph shows that $aa' \sim cc'$ if the configuration is not coplanar; so suppose it is. Let od be a line not in this plane, with $d \notin H$, and choose d' such that $aa' \sim dd'$. Then $bb' \sim dd'$, $cc' \sim dd'$, and $aa' \sim cc'$ follow in turn from the non-planar Desargues' Theorem.

(If we are only given a plane initially, the crucial fact is that the plane can be embedded in a 3-dimensional space.)

Remark The case where $|F| = 2$ is not covered by this argument — can you see why? — and, indeed, the projective plane over $\mathrm{GF}(2)$ contains no non-degenerate Desargues configuration: it only contains seven points! Nevertheless, Desargues' Theorem holds, in the sense that any meaningful degeneration of it is true in the projective plane over $\mathrm{GF}(2)$. We will not make an exception of this case.

It is also possible to prove Desargues' Theorem algebraically, by choosing

coordinates (see Exercise 1). However, it is important for later developments to know that a purely geometric proof is possible.

Let V be a vector space of rank $n+1$ over F, and V^* its dual space. As we saw, V^* is a right vector space over F, and so can be regarded as a left vector space over the opposite field F°. It has the same rank as V if this is finite. Thus we have projective spaces $\mathrm{PG}(n,F)$ and $\mathrm{PG}(n,F^\circ)$, standing in a dual relation to one another. More precisely, we have a bijection between the flats of $\mathrm{PG}(n,F)$ and those of $\mathrm{PG}(n,F^\circ)$, given by

$$U \leftrightarrow \mathrm{Ann}(U) = \{\mathbf{f} \in V^* : (\forall \mathbf{u} \in U)\ (\mathbf{fu} = 0)\}.$$

This correspondence preserves incidence and reverses inclusion:

$$\begin{aligned} U_1 \subseteq U_2 &\Rightarrow \mathrm{Ann}(U_2) \subseteq \mathrm{Ann}(U_1), \\ \mathrm{Ann}(U_1 + U_2) &= \mathrm{Ann}(U_1) \cap \mathrm{Ann}(U_2), \\ \mathrm{Ann}(U_1 \cap U_2) &= \mathrm{Ann}(U_1) + \mathrm{Ann}(U_2). \end{aligned}$$

Moreover, the (geometric) dimension of $\mathrm{Ann}(U)$ is $n - 1 - \dim(U)$.

This gives rise to a *duality principle*, where any configuration theorem in projective space translates into another (over the opposite field) in which inclusions are reversed and dimensions suitably modified. For example, in the plane, the dual of the statement that two points lie on a unique line is the statement that two lines meet in a unique point.

We turn briefly to affine spaces. The description closest to that of projective spaces runs as follows. Let V be a vector space of rank n over F. The *points, lines, planes, ...* of the *affine space* $\mathrm{AG}(n,F)$ are the cosets of the vector subspaces of rank 0, 1, 2, ... (No dimension shift this time!) In particular, points are cosets of the zero subspace, in other words, singletons, and we can identify them with the vectors of V. So the affine space is "a vector space with no distinguished origin".

The other description is: $\mathrm{AG}(n,F)$ is obtained from $\mathrm{PG}(n,F)$ by deleting a hyperplane together with all the subspaces it contains.

The two descriptions are matched up as follows. Take the vector space

$$V = F^{n+1} = \{(x_0, x_1, \ldots, x_n) : x_0, \ldots, x_n \in F\}.$$

Let W be the hyperplane defined by the equation $x_0 = 0$. The points remaining are rank 1 subspaces spanned by vectors with $x_0 \neq 0$; each point has a unique spanning vector with $x_0 = 1$. Then the correspondence between points in the two descriptions is given by

$$\langle (1, x_1, \ldots, x_n) \rangle \leftrightarrow (x_1, \ldots, x_n).$$

(See Exercise 2.)

In $\mathrm{AG}(n,F)$, we say that two subspaces are *parallel* if (in the first description) they are cosets of the same vector subspace, or (in the second description) they have the same intersection with the deleted hyperplane. Parallelism is an equivalence relation. Now the projective space can be recovered from the affine space as follows. To each parallel class of d-dimensional subspaces of $\mathrm{AG}(n,F)$ corresponds a unique $(d-1)$-dimensional subspace of $\mathrm{PG}(n-1,F)$. Adjoin to the affine space the points (and subspaces) of $\mathrm{PG}(n-1,F)$, and adjoin to all members of a parallel class all the points in the corresponding subspace. The result is $\mathrm{PG}(n,F)$.

The distinguished hyperplane is called the *hyperplane at infinity* or *ideal hyperplane*. Thus, an affine space can also be regarded as "a projective space with a distinguished hyperplane".

The study of projective geometry is in a sense the outgrowth of the Renaissance theory of perspective. If a painter, with his eye at the origin of Euclidean 3-space, wishes to represent what he sees on a picture plane, then each line through the origin (i.e., each rank 1 subspace) should be represented by a point of the picture plane, viz., the point at which it intersects the picture plane. Of course, lines parallel to the picture plane do not intersect it, and must be regarded as meeting it in ideal "points at infinity". Thus, the physical picture plane is an affine plane, and is extended to a projective plane; and the points of the projective plane are in one-to-one correspondence with the rank 1 subspaces of Euclidean 3-space. It is easily checked that lines of the picture plane correspond to rank 2 subspaces, provided we make the convention that the points at infinity comprise a single line. Not that the picture plane really is affine rather than Euclidean; the ordinary distances in it do not correspond to distances in the real world.

Exercises

1. Prove Desargues' Theorem in coordinates.

2. Show that the correspondence defined in the text between the two descriptions of affine space is a bijection which preserves incidence, dimension, and parallelism.

3. The LaTeX typesetting system provides facilities for drawing diagrams. In a diagram, the slope of a line is restricted to being infinity or a rational number whose numerator and denominator are each at most 6 in absolute value.

(a) What is the relation between the slopes of the six lines of a complete quadrangle (all lines joining four points)? Investigate how such a figure can be

drawn with the above restriction on the slopes.

(b) Investigate similarly how to draw a Desargues configuration.

1.3 The "Fundamental Theorem of Projective Geometry"

An *isomorphism* between two projective spaces is a bijection between the point sets of the spaces which maps any subspace into a subspace (when applied in either direction). A *collineation* of $\mathrm{PG}(n,F)$ is an isomorphism from $\mathrm{PG}(n,F)$ to itself. The theorem of the title of this section has two consequences: first, that isomorphic projective spaces have the same dimension and the same coordinatising field; second, a determination of the group of all collineations.

We must assume that $n > 1$; for the only proper subspaces of a projective line are its points, and so any bijection is an isomorphism, and the collineation group is the full symmetric group. (There are methods for assigning additional structure to a projective line, for example, using cross-ratio; these will be discussed later on, in Section 4.5.)

The *general linear group* $\mathrm{GL}(n+1,F)$ is the group of all non-singular linear transformations of $V = F^{n+1}$; it is isomorphic to the group of invertible $(n+1) \times (n+1)$ matrices over F. (In general, the determinant is not well-defined, so we cannot identify the invertible matrices with those having non-zero determinant.) Any element of $\mathrm{GL}(n+1,F)$ maps subspaces of V into subspaces of the same rank, and preserves inclusion; so it induces a collineation of $\mathrm{PG}(n,F)$. The group $\mathrm{Aut}(F)$ of automorphisms of F has a coordinate-wise action on V^{n+1}; these transformations also induce collineations. The group generated by $\mathrm{GL}(n+1,F)$ and $\mathrm{Aut}(F)$ (which is actually their semi-direct product) is denoted by $\Gamma\mathrm{L}(n+1,F)$; its elements are called *semilinear transformations*. The groups of collineations of $\mathrm{PG}(n,F)$ induced by $\mathrm{GL}(n+1,F)$ and $\Gamma\mathrm{L}(n+1,F)$ are denoted by $\mathrm{PGL}(n+1,F)$ and $\mathrm{P\Gamma L}(n+1,F)$, respectively.

More generally, a semi-linear transformation from one vector space to another is the composition of a linear transformation and a coordinate-wise field automorphism of the target space.

Theorem 1.5 (Fundamental Theorem of Projective Geometry) *Any isomorphism between projective spaces of dimension at least* 2 *is induced by a semilinear transformation between the underlying vector spaces, unique up to scalar multiplication.*

Before outlining the proof, we will see the two important corollaries of this result. Both follow immediately from the theorem (in the second case, by taking the two projective spaces to be the same).

Corollary 1.6 *Isomorphic projective spaces of dimension at least* 2 *have the same dimension and are coordinatised by isomorphic fields.* ■

Corollary 1.7 *(a) For* $n > 1$*, the collineation group of* $\mathrm{PG}(n,F)$ *is the group* $\mathrm{P\Gamma L}(n+1,F)$.

(b) The kernel of the action of $\Gamma\mathrm{L}(n+1,F)$ *on* $\mathrm{PG}(n,F)$ *is the group of non-zero scalars (acting by left multiplication).* ■

Remark The point of the theorem, and the reason for its name, is that the algebraic structure of the underlying vector space can be recovered from the incidence geometry of the projective space. The proof is a good warm-up for the coordinatisation theorems I will be discussing soon. In fact, the proof concentrates on Corollary 1.7, for ease of exposition. The dimension of a projective space is two less than the number of subspaces in a maximal chain (under inclusion); and our argument shows that the geometry determines the coordinatising field up to isomorphism.

Proof We show first that two semi-linear transformations which induce the same collineation differ only by a scalar factor. By following one by the inverse of the other, we see that it suffices to show that a semi-linear transformation which fixes every point of $\mathrm{PG}(n,F)$ is a scalar multiplication. So let $\mathbf{v} \mapsto \mathbf{v}^\sigma A$ fix every point of $\mathrm{PG}(n,F)$, where $\sigma \in \mathrm{Aut}(F)$ and $A \in \mathrm{GL}(n+1,F)$. Then every vector is mapped to a scalar multiple of itself. Let $\mathbf{e}_0,\ldots,\mathbf{e}_n$ be the standard basis for V. Then (since σ fixes the standard basis vectors) we have $\mathbf{e}_i A = \lambda_i \mathbf{e}_i$ for $i = 0,\ldots,n$. Also,

$$\begin{aligned}(\mathbf{e}_0 + \ldots + \mathbf{e}_n)A &= \lambda_0\mathbf{e}_0 + \ldots + \lambda_n\mathbf{e}_n \\ &= \lambda(\mathbf{e}_0 + \ldots + \mathbf{e}_n), \quad \text{say,}\end{aligned}$$

so $\lambda_0 = \ldots = \lambda_n = \lambda$.

Now, for any $\mu \in F$, the vector $(1,\mu,0,\ldots,0)$ is mapped to the vector $(\lambda,\mu^\sigma\lambda,0,\ldots,0)$; so we have $\lambda\mu = \mu^\sigma\lambda$. Thus

$$\mathbf{v}^\sigma A = \mathbf{v}^\sigma\lambda = \lambda\mathbf{v}$$

for any vector $\mathbf{v}$, as required.

Note that the field automorphism σ is conjugation by the element λ (that is, $\mu^\sigma = \lambda\mu\lambda^{-1}$); in other words, an inner automorphism.

Now we prove that any isomorphism is semilinear. The strategy is similar. Call an $(n+2)$ tuple of points *special* if no $n+1$ of them are linearly dependent. We have:

> There is a linear map carrying any special tuple to any other (in the same space, or another space of the same dimension over the same field).

(For, given a special tuple in the first space, spanning vectors for the first $n+1$ points form a basis $\mathbf{e}_0,\ldots,\mathbf{e}_n$, and the last point is spanned by a vector with all coordinates non-zero relative to this basis. Adjusting the basis vectors by scalar factors, we may assume that the last point is spanned by $\mathbf{e}_0+\ldots+\mathbf{e}_n$. Similarly, the points of a special tuple in the second space are spanned by the vectors of a basis $\mathbf{f}_0,\ldots,\mathbf{f}_n$, and $\mathbf{f}_0+\ldots+\mathbf{f}_n$. The unique linear transformation carrying the first basis to the second also carries the first special tuple to the second.)

Let θ be any isomorphism. Then there is a linear map ϕ which mimics the effect of θ on a special $(n+2)$-tuple. Composing θ with the inverse of ϕ, we obtain an automorphism of $\mathrm{PG}(n,F)$ which fixes the $(n+2)$-tuple pointwise. We have to show that such an automorphism is the product of a scalar and a field automorphism. (Note that, as we saw above, left and right multiplications by λ differ by an inner automorphism.)

We assume that $n=2$; this simplifies the argument, while retaining its essential features. So let g be a collineation fixing the spans of $\mathbf{e}_0,\mathbf{e}_1,\mathbf{e}_2$ and $\mathbf{e}_0+\mathbf{e}_1+\mathbf{e}_2$. We use homogeneous coordinates, writing these vectors as $(1,0,0)$, $(0,1,0)$, $(0,0,1)$, and $(1,1,1)$, and denote the general point by (x,y,z).

The points on the line $\{(x_0,0,x_2)\}$, apart from $(1,0,0)$, have the form $(x,0,1)$ for $x\in F$, and so can be identified with elements of F. Now the bijection between this set and the set of points $(0,y,1)$ on the line $\{(0,x_1,x_2)\}$, given by $(x,0,1)\mapsto(0,x,1)$, can be geometrically defined in a way which is invariant under collineations fixing the four reference points (see Fig. 1.3). The figure also shows that the coordinates of all points in the plane are determined.

Furthermore, the operations of addition and multiplication in F can be defined geometrically in the same sense (see Figures 1.4 and 1.6). (The definitions look more familiar if we take the line $\{(x_1,x_2,0)\}$ to be at infinity, and draw the figure in the affine plane with lines through $(1,0,0)$ and $(0,1,0)$ horizontal and vertical respectively. this has been done for addition in Figure 1.5; the reader should draw

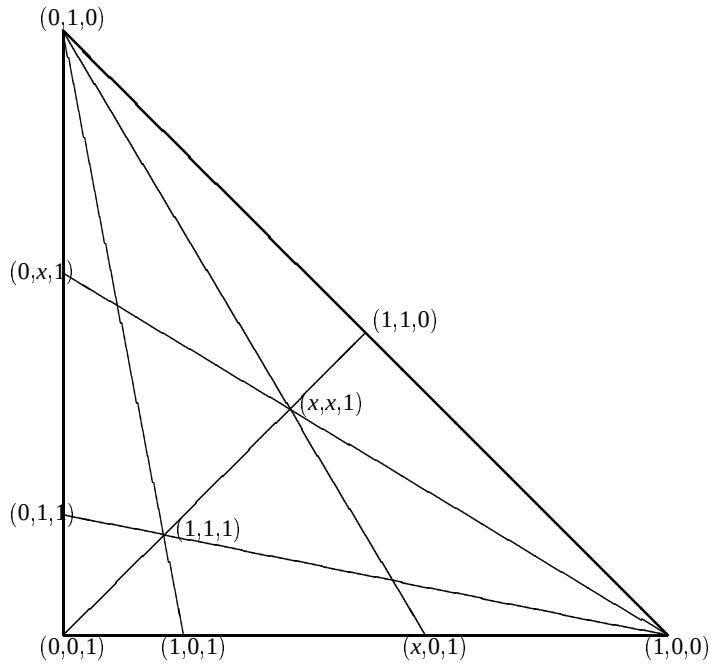

Figure 1.3: Bijection between the axes

the corresponding diagram for multiplication.) It follows that any collineation fixing our four basic points induces an automorphism of the field F, and its actions on the coordinates agree. The theorem is proved. ■

A group G acting on a set Ω is said to be *t-transitive* if, given any two t-tuples $(\alpha_1,\ldots,\alpha_t)$ and $(\beta_1,\ldots,\beta_t)$ of distinct elements of Ω, some element of G carries the first tuple to the second. G is *sharply t-transitive* if there is a unique such element. (If the action is not faithful, it is better to say: two elements of G which agree on t distinct points of Ω agree everywhere.)

Since any two distinct points of $\mathrm{PG}(n,F)$ are linearly independent, we see that $\mathrm{P\Gamma L}(n+1,F)$ (or even $\mathrm{PGL}(n+1,F)$) is 2-transitive on the points of $\mathrm{PG}(n,F)$. It is never 3-transitive (for $n>1$); for some triples of points are collinear and others are not, and no collineation can map one type to the other.

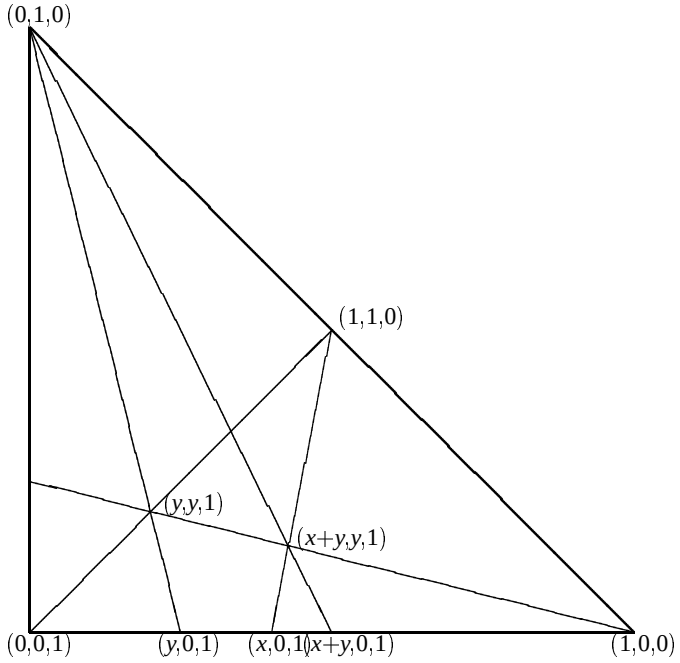

Figure 1.4: Addition

I will digress here to describe the analogous situation for $\mathrm{PG}(1,F)$, even though the FTPG does not apply in this case.

Proposition 1.8 *(a) The group* $\mathrm{PGL}(2,F)$ *is* 3*-transitive on the points of* $\mathrm{PG}(1,F)$*, and is sharply* 3*-transitive if and only if* F *is commutative.*

(b) There exist skew fields F *for which the group* $\mathrm{PGL}(2,F)$ *is* 4*-transitive on* $\mathrm{PG}(1,F)$*.*

Proof The first part follows just as in the proof of the FTPG, since any three points of $\mathrm{PG}(1,F)$ have the property that no two are linearly dependent. Again, as in that theorem, the stabiliser of the three points with coordinates $(1,0)$, $(0,1)$ and $(1,1)$ is the group of inner automorphisms of F, and so is trivial if and only if F is commutative.

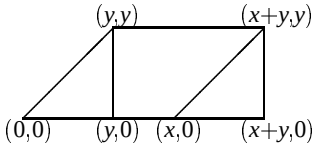

Figure 1.5: Affine addition

There exist skew fields F with the property that any two elements different from 0 and 1 are conjugate in the multiplicative group of F. Clearly these have the required property. (This fact is due to P. M. Cohn [15]; it is established by a construction analogous to that of Higman, Neumann and Neumann [20] for groups. Higman *et al.* used their construction to show that there exist groups in which all non-identity elements are conjugate; Cohn's work shows that there are multiplicative groups of skew fields with this property. Note that such a field has characteristic 2. For, if not, then $1+1 \neq 0$, and any automorphism must fix $1+1$.) ■

Finally, we consider collineations of affine spaces.

Parallelism in an affine space has an intrinsic, geometric definition. For two d-flats are parallel if and only if they are disjoint and some $(d+1)$-flat contains both. It follows that any collineation of $\mathrm{AG}(n,F)$ preserves parallelism. The hyperplane at infinity can be constructed from the parallel classes (as we saw in Section 1.2); so any collineation of $\mathrm{AG}(n,F)$ induces a collineation of this hyperplane, and hence of the embedding $\mathrm{PG}(n,F)$. Hence:

Theorem 1.9 *The collineation group of* $\mathrm{AG}(n,F)$ *is the stabiliser of a hyperplane in the collineation group of* $\mathrm{PG}(n,F)$. ■

Using this, it is possible to determine the structure of this group for $n > 1$ (see Exercise 2).

Proposition 1.10 *For* $n > 1$, *the collineation group of* $\mathrm{AG}(n,F)$ *is the semi-direct product of the additive group of* F^n *and* $\Gamma\mathrm{L}(n,F)$.

This group is denoted by $\mathrm{A}\Gamma\mathrm{L}(n,F)$. The additive group acts by translation, and the semilinear group in the natural way.

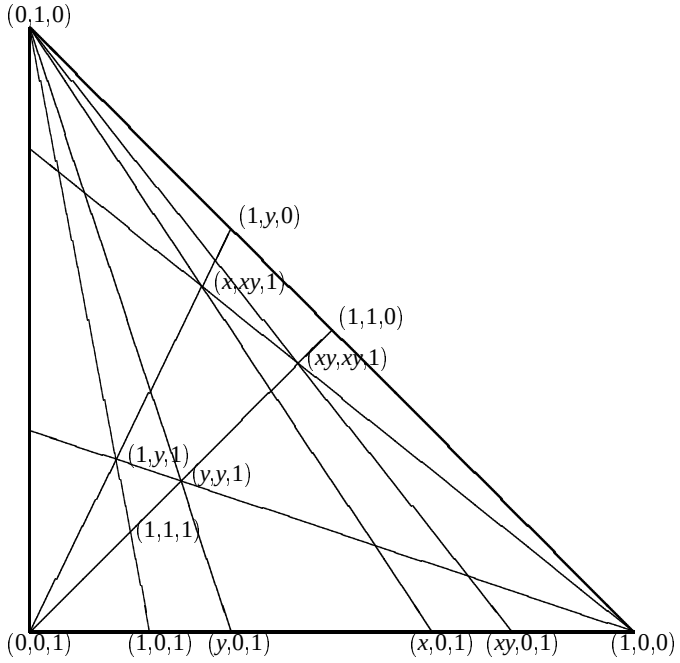

Figure 1.6: Multiplication

Exercises

1. Prove the FTPG for $n > 2$.

2. Use the correspondence between the two definitions of $\mathrm{AG}(n,F)$ given in the last section to deduce Proposition 1.10 from Theorem 1.9.

1.4 Finite projective spaces

Over the finite field $\mathrm{GF}(q)$, the n-dimensional projective and affine spaces and their collineation groups are finite, and can be counted. In this section, we display some of the relevant formulæ. We abbreviate $\mathrm{PG}(n,\mathrm{GF}(q))$ to $\mathrm{PG}(n,q)$, and similarly for affine spaces, collineation groups, etc.

A vector space of rank n over $\mathrm{GF}(q)$ is isomorphic to $\mathrm{GF}(q)^n$, and so the number of vectors is q^n. In consequence, the number of vectors outside a subspace

of rank k is $q^n - q^k$.

Proposition 1.11 *The number of subspaces of rank k in a vector space of rank n over $\mathrm{GF}(q)$ is*

$$\frac{(q^n-1)(q^n-q)\cdots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\cdots(q^k-q^{k-1})}.$$

Remark This number is called a *Gaussian coefficient*, and is denoted by $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Proof First we count the number of choices of k linearly independent vectors. The i^{th} vector may be chosen arbitrarily outside the subspace of rank $i-1$ spanned by its predecessors, hence in $q^n - q^{i-1}$ ways. Thus, the numerator is the required number of choices.

Now any k linearly independent vectors span a unique subspace of rank k; so the number of subspaces is found by dividing the number just calculated by the number of choices of a basis for a space of rank k. But the latter is given by the same formula, with k replacing n. ■

Proposition 1.12 *The order of $\mathrm{GL}(n,q)$ is*

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

The order of $\Gamma\mathrm{L}(n,q)$ is the above number multiplied by d, where $q = p^d$ with p prime; and the orders of $\mathrm{PGL}(n,q)$ and $\mathrm{P\Gamma L}(n,q)$ are obtained by dividing these numbers by $(q-1)$.

Proof An element of $\mathrm{GL}(n,q)$ is uniquely determined by the image of the standard basis, which is an arbitrary basis of $\mathrm{GF}(q)^n$; and the proof of Proposition 1.11 shows that the number of bases is the number quoted. The remainder of the proposition follows from the remarks in Section 1.3, since $\mathrm{GF}(q)$ has $q-1$ non-zero scalars, and its automorphism group has order d. ■

The formula for the Gaussian coefficient makes sense, not just for prime power values of q, but for any value of q different from 1. There is a combinatorial interpretation for any integer $q > 1$ (Exercise 3). Moreover, by l'Hôpital's rule, $\lim_{q\to 1}(q^a-1)/(q^b-1) = a/b$; it follows that

$$\lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}.$$

This illustrates just one of the many ways in which subspaces of finite vector spaces resemble subsets of sets.

It follows immediately from Propopsition 1.11 that the numbers of k-dimensional flats in $\mathrm{PG}(n,q)$ and $\mathrm{AG}(n,q)$ are $\begin{bmatrix} n+1 \\ k+1 \end{bmatrix}_q$ and $q^{n-k}\begin{bmatrix} n \\ k \end{bmatrix}_q$ respectively.

Projective and affine spaces provide important examples of designs, whose parameters can be expressed in terms of the Gaussian coefficients.

A *t-design* with *parameters* (v,k,λ), or *t-(v,k,λ) design*, consists of a set X of *v points*, and a collection $\mathcal{B}$ of k-element subsets of X called *blocks*, with the property that any t distinct points of X are contained in exactly λ blocks. Designs were first used by statisticians, such as R. A. Fisher, for experimental design (e.g. to facilitate analysis of variance). The terms "design" and "block", and the letter v (the initial letter of "variety"), reflect this origin.

Proposition 1.13 *(a) The points and m-dimensional flats in $\mathrm{PG}(n,q)$ form a 2-design with parameters*

$$\left(\begin{bmatrix} n+1 \\ 1 \end{bmatrix}_q, \begin{bmatrix} m+1 \\ 1 \end{bmatrix}_q, \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q \right).$$

(b) The points and m-dimensional flats of $\mathrm{AG}(n,q)$ form a 2-design with parameters

$$\left(q^n,\, q^m,\, \begin{bmatrix} n-1 \\ m-1 \end{bmatrix}_q \right).$$

If $q = 2$, then it is a 3-design, with $\lambda = \begin{bmatrix} n-2 \\ m-2 \end{bmatrix}_2$.

Proof The values of v and k are clear in both cases.

(a) Let V be the underlying vector space of rank $n+1$. We want to count the subspaces of rank $m+1$ containing two given rank 1 subspaces P_1 and P_2. If $L = P_1 + P_2$, then L has rank 2, and a subspace contains P_1 and P_2 if and only if it contains L. Now, by the Third Isomorphism Theorem, the rank $m+1$ subspaces containing L are in 1-1 correspondence with the rank $m-1$ subspaces of the rank $n-1$ space V/L.

(b) In $\mathrm{AG}(n,q)$, to count subspaces containing two points, we may assume (by translation) that one of the points is the origin. An affine flat containing the origin is a vector subspace, and a subspace contains a non-zero vector if and only if it contains the rank 1 subspace it spans. The result follows as before. In the case when $q = 2$, a rank 1 subspace contains only one non-zero vector, so any two distinct non-zero vectors span a rank 2 subspace. ∎

Remark The essence of the proof is that the quotient of either $\mathrm{PG}(n,q)$ or $\mathrm{AG}(n,q)$ by a flat F of dimension d is $\mathrm{PG}(n-d-1,q)$. (The flats of the quotient space are precisely the flats of the original space containing F.) This assertion is true over any field at all, and lies at the basis of an approach to geometry which we will consider in Chapter 5.

An *automorphism* of a design is a permutation of the points which maps any block to a block.

Proposition 1.14 *For $0 < m < n$, the design of points and m-dimensional flats in $\mathrm{PG}(n,q)$ or $\mathrm{AG}(n,q)$ is $\mathrm{P\Gamma L}(n+1,q)$ or $\mathrm{A\Gamma L}(n+1,q)$ respectively, except in the affine case with $q=2$ and $m=1$.*

Proof By the results of Section 1.3, it suffices to show that the entire geometry can be recovered from the points and m-dimensional flats. This follows immediately from two observations:

(a) the unique line containing two points is the intersection of all the m-dimensional flats containing them;

(b) except for affine spaces over $\mathrm{GF}(2)$, a set of points is a flat if and only if it contains the line through any two of its points.

Affine spaces over $\mathrm{GF}(2)$ are exceptional: lines have just two points, and any two points form a line. However, analogous statements hold for planes: three points lie in a unique plane, and we have

(aa) the plane through three points is the intersection of all the flats of dimension m which contain them (for $m > 1$);

(bb) a set of points is a flat if and only if it contains the plane through any three of its points.

The proofs are left as exercises. ■

Exercises

1. Prove the assertions (a), (b), (aa), (bb) in Proposition 1.14.

2. Prove that the probability that a random $n \times n$ matrix over a given finite field $\mathrm{GF}(q)$ is non-singular tends to a limit $c(q)$ as $n \to \infty$, where $0 < c(q) < 1$.

3. Prove that the total number $F(n)$ of subspaces of a vector space of rank n over a given finite field $\mathrm{GF}(q)$ satisfies the recurrence

$$F(n+1) = 2F(n) + (q^n - 1)F(n-1).$$

4. Let S be an "alphabet" of size q, with two distinguished elements 0 and 1 (but not necessarily a finite field). A $k \times n$ matrix with entries from S is (as usual) in *reduced echelon form* if

- it has no zero rows;
- the first non-zero entry in any row is a 1;
- the "leading 1s" in later rows occur further to the right;
- the other entries in the column of a "leading 1" are all 0.

Prove that the number of $k \times n$ matrices in reduced echelon form is $\begin{bmatrix} n \\ k \end{bmatrix}_q$. Verify in detail in the case $n = 4$, $k = 2$.

5. Use the result of Exercise 4 to prove the recurrence relation

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = q^n \begin{bmatrix} n-1 \\ k \end{bmatrix}_q + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q.$$