

# Chapter 1

## Examples

We introduce projective and affine spaces over fields.

### 1.1 Incidence Structures

An *incidence structure* consists of a point set  $\mathcal{P}$  and a block set  $\mathcal{B}$  and a relation on  $\mathcal{P} \times \mathcal{B}$ , called *incidence*. In many cases the blocks are subsets of  $\mathcal{P}$  and then a point  $x$  is incident with a block  $\beta$  if  $x \in \beta$ . The *dual incidence structure* is produced by swapping  $\mathcal{P}$  and  $\mathcal{B}$ . An incidence structure is a *linear space* if each pair of distinct points lies in exactly one block. It is a *partial linear space* if each pair of points lies in at most one block; if this holds then for any pair of distinct blocks there is at most one point incident with both. Thus the dual of a partial linear space is a partial linear space. However the dual of a linear space need not be linear.

An *automorphism* of an incidence structure  $(\mathcal{P}, \mathcal{B})$  consists of a pair of permutations  $(\pi, \sigma)$  such that if  $x \in \mathcal{P}$  and  $\beta \in \mathcal{B}$ , then  $x$  is incident with  $\beta$  if and only if  $x^\pi$  is incident with  $\beta^\sigma$ . For linear spaces we often use the term *collineation* in place of automorphism.

The *incidence graph* of an incidence structure is the bipartite graph with points as one color class, blocks as the second and with two vertices adjacent if one is a point and the other is a blocks incident with it. Strictly speaking an incidence graph is not just bipartite but bicolored—we know which color class corresponds to the points and which to the lines. If we swap the colors we obtain the incidence graph of the dual incidence structure. Two graphical properties that are useful geometrically are the girth and diameter.

## 1. EXAMPLES

---

**1.1.1 Lemma.** *An incidence structure is a partial linear space if and only if its incidence graph has girth at least six.*  $\square$

The *incidence matrix*  $N$  of a finite incidence structure  $(\mathcal{P}, \mathcal{B})$  is the 01-matrix with rows indexed by  $\mathcal{P}$ , columns by  $\mathcal{B}$  and with  $N_{x,\beta} = 1$  if and only if the point  $x$  is incident with the block  $\beta$ . Then  $N^T$  is the incidence matrix of the dual structure and the adjacent matrix of the incidence graph is

$$\begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}.$$

A finite incidence structure is *point regular* if each point lies on the same number of blocks and *block regular* if each block is incident with the same number of points. An incidence structure is *thick* if each point is on at least three blocks and each block is on at least three points. If  $X$  is a graph with vertex set  $V$  and edge set  $E$ , then  $(V, E)$  is an incidence structure which is block regular and is point regular if and only if  $X$  is regular as a graph.

If  $x, y$  are distinct points that are incident with at least one common block, we define the *line*  $x \vee y$  to be the set of points that are incident with each block incident with both  $x$  and  $y$ . The points and lines of an incidence structure form a partial linear space, conversely the lines of a partial linear space are its blocks. In dealing with partial linear spaces, we normally refer to the blocks as lines.

A set  $S$  of points in a partial linear space is a *subspace* if whenever two distinct points of  $S$  are incident with a line  $\ell$ , and then all points incident with  $\ell$  belong to  $S$ . The unique line through the points  $p$  and  $q$  will be denoted by  $p \vee q$ . A set of points is *collinear* if it is contained in some line.

## 1.2 Posets and Lattices

We assume familiarity with the basics of posets. A *chain* is a set of elements such that two are comparable. Any chain has a unique maximal element (and a unique minimal element). A chain is maximal if it is not a proper subset of a larger one. A poset is *ranked* if for each element  $a$  all maximal chains with  $a$  as their greatest element have the same size. The *length* is one less than its size. In a ranked poset, the rank of an element  $a$  is the maximum length of a chain with  $a$  as its greatest element.

Both the subsets of a set and the subspaces of a vector space form ranked posets.

A poset is a lattice if each pair of elements has a least upper bound and a greatest lower bound. The least upper bound of  $a$  and  $b$  is denoted by  $a \vee b$ , the greatest lower bound by  $a \wedge b$ . In a finite lattice, there is always a unique minimal element, usually denoted  $0$ , and unique maximal element, denoted  $1$ . We may refer to  $a \vee b$  as the *join* of  $a$  and  $b$ , and to  $a \wedge b$  as the *meet*. The meet and join operations satisfy the following axioms:

- (a)  $a \wedge a = a, a \vee a = a.$
- (b)  $a \wedge b = b \wedge a, a \vee b = b \vee a.$
- (c)  $a \wedge (b \wedge c) = (a \wedge b) \wedge c, a \vee (b \vee c) = (a \vee b) \vee c.$

If the lattice has  $0$  and  $1$ , we require  $a \vee 0 = a$  and  $a \wedge 1 = a$  as well.

If each pair of elements  $a$  and  $b$  in a finite poset has a greatest lower bound, we can define their join to be the meet of all elements  $x$  such that  $x \geq a, b$ . This gives us a lattice and this is the unique lattice compatible with the meet operation. We leave the proof of this as an exercise.

By way of example, consider the subspaces of a partial linear space. The *join* of two subspaces  $H$  and  $K$  is defined to be the intersection of all subspaces which contain both  $H$  and  $K$ , and is denoted by  $H \vee K$ . Every subset  $S$  of the points of a linear space determines a subspace, namely the intersection of all subspaces which contain it. This subspace is said to be *spanned* by  $S$ . We thus get a lattice of subspaces, which need not be ranked.

In geometric settings a chain in a poset is usually called a *flag*, and a flag that is maximal under inclusion may be called a *chamber*. A poset is *thick* if non-maximal flag lies in at least three chambers. (Remark: these terms are usually applied in more restricted settings. We will apply them to the lattice of flats of a rank function.)

## 1.3 Rank Functions

A *rank function*  $\text{rk}$  on a set  $P$  is a function from the subsets of  $P$  to the non-negative integers such that:

- (a) if  $A \subseteq P$  then  $0 \leq \text{rk}(A) \leq |A|$  and

## 1. EXAMPLES

---

(b) if  $B \subseteq A$  then  $\text{rk}(B) \leq \text{rk}(A)$ .

If, in addition

(c)  $\text{rk}(A \cup B) + \text{rk}(A \cap B) \leq \text{rk}(A) + \text{rk}(B)$

then we say the rank function is submodular.

A set equipped with a submodular rank function is called a *matroid*. A *flat* in a matroid is a subset  $F$  such that, if  $p \notin F$  then  $\text{rk}(p \cup F) > \text{rk}(F)$ . A *combinatorial geometry* is a set  $P$ , together with a submodular rank function  $\text{rk}$  such that if  $A \subseteq P$  and  $|A| \leq 2$  then  $\text{rk}(A) = |A|$ . Any combinatorial geometry can be regarded as a linear space with the flats of rank one as its points and the flats of rank two as its lines. The flats of rank three are its *planes*. The maximal proper flats of a combinatorial geometry are its *hyperplanes*; it is left as an exercise to show that these must all have the same rank. The rank of a combinatorial geometry is the maximum value of its rank function. We will always restrict ourselves to combinatorial geometries where the rank is finite, even if the point set is not.

The flats relative to a rank function form a lattice, such lattices are called *geometric lattices*. Note that in this case the join  $F_1 \vee F_2$  of two flats is not (in general) equal to  $F_1 \cup F_2$ , although  $F_1 \wedge F_2 = F_1 \cap F_2$ . If for any two flats  $A$  and  $B$  we have

$$\text{rk}(A \vee B) + \text{rk}(A \wedge B) = \text{rk}(A) + \text{rk}(B)$$

we say that our rank function is *modular*. The lattices of subspaces of a vector space provides the most important example.

### 1.4 Graphs

We have already met incidence graphs, but these are just one of many families of graphs that arise in geometry. As another example we can define a the *point graph* of a partial linear space to be the graph on the points of the space, where two points are adjacent if they are collinear. (This is not very useful for linear spaces.)

A further class of examples is provided by the *Grassmann graphs*. Here the vertices are the  $k$ -dimensional subspaces of  $V(n, q)$ , two subspaces  $\alpha$  and  $\beta$  are adjacent if  $\alpha \cap \beta$  has dimension  $k - 1$ . We denote this by  $J_q(n, k)$ .

You might check that  $J(v, k)$  is isomorphic to  $J(v, v - k)$ . Clearly  $J_q(n, 1)$  is a complete graph. One important feature of the Grassmann graphs is that they are *distance transitive*. To prove this, first verify that two subspaces are at distance  $r$  in  $J_q(n, k)$  if and only if their intersection has dimension  $k - r$ . Then show that the linear group acts transitively on pairs of  $k$ -dimensional subspace with intersection of dimension  $k - r$ .

The incidence graph of the points and hyperplanes of a projective space is distance regular. and is distance transitive if the space has rank at least four.

In an association scheme with  $d$  classes, each of the graphs has diameter at most  $d$ . If equality holds for one of the graphs we say that the scheme is *metric* relative to that graph, and we say that the graph is *distance regular*. It can be shown shown that an association scheme is metric relative to at most two classes. Most schemes are not metric.

## 1.5 Automorphisms and Isomorphisms

We offer some basic remarks on automorphisms. The first remark is that a geometer will often use the term *collineation* rather than automorphism.

There is a minor technical problem in dealing with the automorphisms of incidence structures: a block need not be determined by the set of points incident with it. If we have incidence structures  $(\mathcal{P}_1, \mathcal{B}_1)$  and  $(\mathcal{P}_2, \mathcal{B}_2)$  then an isomorphism consists of bijection  $\pi$  from  $\mathcal{P}_1$  to  $\mathcal{P}_2$  and a bijection  $\beta$  from  $\mathcal{B}_1$  to  $\mathcal{B}_2$  such that if  $p$  is incident to  $\ell$  then  $p^\pi$  is incident with  $\ell^\beta$ . For graph theorists, it can be more convenient to view an isomorphism as an isomorphism between incidence graphs that maps point-vertices to point-vertices. No matter which viewpoint we take, an automorphism is just an isomorphism from a structure to itself and a duality is an isomorphism from a structure to its dual.

## 1.6 Some Counting

We introduce the *Gaussian binomial coefficients*. Let  $q$  be fixed and not equal to 1. We define

$$[n] := \frac{q^n - 1}{q - 1}.$$

## 1. EXAMPLES

---

If the value of  $q$  needs to be indicated we might write  $[n]_q$ . We next define  $[n]!$  by declaring that  $[0] := 1$  and

$$[n + 1]! = [n + 1][n]!$$

Note that  $[n]$  is a polynomial in  $q$  of degree  $n - 1$  and  $[n]!$  is a polynomial in  $q$  of degree  $\binom{n}{2}$ . Finally we define the Gaussian binomial coefficient by

$$\begin{bmatrix} n \\ k \end{bmatrix} := \frac{[n]!}{[k]![n - k]!}.$$

**1.6.1 Theorem.** *Let  $V$  be a vector space of dimension  $n$  over a field of finite order  $q$ . Then the number of subspaces of  $V$  with dimension  $k$  is  $\begin{bmatrix} n \\ k \end{bmatrix}$ .*

*Proof.* First we count the number  $N_r$  of  $n \times r$  matrices over  $GF(q)$  with rank  $r$ . There are  $q^n - 1$  non-zero vectors in  $V$ , so  $N_1 = q^n - 1$ .

Suppose  $A$  is an  $n \times r$  matrix with rank  $r$ . Then there are  $q^r - 1$  non-zero vectors in  $\text{col}(A)$ , and therefore there are  $q^n - q^r$  non-zero vectors not in  $\text{col}(A)$ . If  $x$  is one of these, then  $(A, x)$  is an  $n \times (r + 1)$  matrix with rank  $r$ , and therefore

$$N_{r+1} = (q^n - q^r)N_r.$$

Hence

$$N_r = (q^n - q^{r-1}) \cdots (q^n - 1) = q^{\binom{r}{2}} (q - 1)^r \frac{[n]!}{[n - r]!}.$$

Note that  $N_n$  is the number of invertible  $n \times n$  matrices over  $GF(q)$ . Count pairs consisting of a subspace  $U$  of dimension  $r$  and an  $n \times r$  matrix  $A$  such that  $U = \text{col}(A)$ . If  $\nu_r$  denotes the number of  $r$ -subspaces then

$$N_r = \nu_r q^{\binom{r}{2}} (q - 1)^r [r]!$$

This yields the theorem. □

Suppose  $U_1$  and  $U_2$  are subspaces of  $V$ . We say that  $U_1$  and  $U_2$  are *skew* if  $U_1 \cap U_2 = \{0\}$ ; geometrically this means they are skew if they have no points in common. We say that  $U_1$  and  $U_2$  are *complements* if they are skew and  $V = U_1 + U_2$ ; in this case

$$\dim V = \dim U_1 + \dim U_2.$$

Now suppose that  $U$  and  $W$  are complements in  $V$  and  $\dim(U) = k$ . If  $H$  is a subspace of  $V$  that contains  $U$ , define  $\rho(H)$  by

$$\rho(H) = H \cap W.$$

We claim that  $\rho$  is a bijection from the set of subspaces of  $V$  that contain  $U$  and have dimension  $k + \ell$  to the subspaces of  $W$  with dimension  $\ell$ .

We have  $H + W = V$  and therefore

$$\begin{aligned} n = \dim(H + W) &= \dim(H) + \dim(W) - \dim(H \cap W) \\ &= k + \ell + n - k - \dim(H \cap W) \\ &= n + \ell - \dim(H \cap W). \end{aligned}$$

This implies that  $\dim(H \cap W) = \ell$ . It remains for us to show that  $\rho$  is a bijection.

If  $W_1$  is a subspace of  $W$  with dimension  $\ell$ , then  $U + W_1$  is a subspace of  $V$  with dimension  $k + \ell$  that contains  $U$ . Then

$$\rho(U + W_1) = W_1,$$

which shows that  $\rho$  is surjective. Suppose  $\rho(H_1) = \rho(H_2)$ . Then

$$H_1 \cap W = H_2 \cap W$$

and so both  $H_1$  and  $H_2$  contain  $U + (H_1 \cap W)$ . Since these three spaces all have dimension  $k + \ell$ , it follows that they are equal. Therefore  $\rho$  is injective.

We also notes that  $H$  and  $K$  are subspaces of  $V$  that contain  $U$  and  $H \leq K$ , then  $\rho(H) \leq \rho(K)$ . Therefore  $\rho$  is an inclusion-preserving bijection from the subspaces of  $V$  that contain  $U$  to the subspaces of  $W$ . The subspaces of  $W$  form a projective space of rank  $n - \dim(U)$  and so it follows that we view the subspaces of  $V$  that contain  $U$  as a projective space.

**1.6.2 Lemma.** *Let  $V$  be a vector space of dimension  $n$  over a field of order  $q$ , and let  $U$  be a subspace of dimension  $k$ . The number of subspaces of  $V$  with dimension  $\ell$  that are skew to  $U$  is  $q^{k\ell} \begin{bmatrix} n-k \\ \ell \end{bmatrix}$ .*

*Proof.* The number of subspaces of  $V$  with dimension  $k + \ell$  that contain  $U$  is  $\begin{bmatrix} n-k \\ \ell \end{bmatrix}$ . If  $W_1$  has dimension  $\ell$  and is skew to  $U$ , then  $U + W_1$  is a subspace of dimension  $k + \ell$  that contains  $U$ . Hence the subspaces of dimension  $k + \ell$  that contain  $U$  partition the set of subspaces of dimension  $\ell$  that are skew

## 1. EXAMPLES

---

to  $U$ . The number of subspaces of dimension  $k + \ell$  in  $V$  that contain  $U$  is  $\binom{n-k}{\ell}$ . We determine the number of complements to  $U$  in a space  $W$  of dimension  $m$  that contains  $U$ .

We identify  $W$  with  $\mathbb{F}^{m \times 1}$ . Since  $\dim W = m$  and  $\dim U = k$ , we may assume that  $U$  is the column space of the  $m \times k$  matrix

$$\begin{pmatrix} I_k \\ 0 \end{pmatrix}$$

Suppose  $W_1$  is a subspace of  $W$  with dimension  $m - k$ . We may assume that  $W$  is the column space of the  $m \times (m - k)$  matrix

$$\begin{pmatrix} A \\ B \end{pmatrix}$$

where  $B$  is  $(m - k) \times (m - k)$ . Then  $W_1$  is a complement to  $U$  if and only if the matrix

$$\begin{pmatrix} I_k & A \\ 0 & B \end{pmatrix}$$

is invertible, and this holds if and only if  $B$  is invertible. If  $B$  is invertible, then  $W_1$  is the column space of

$$\begin{pmatrix} AB^{-1} \\ I_{m-k} \end{pmatrix}.$$

So there is a bijection from the set of complements to  $U$  in  $W$  to the set of  $m \times (m - k)$  matrices over  $\mathbb{F}$  of the form

$$\begin{pmatrix} M \\ I \end{pmatrix},$$

and therefore the number of complements of  $U$  is equal to  $q^{k(m-k)}$ , the number of  $k \times (m - k)$  matrices over  $\mathbb{F}$ .  $\square$

## Exercises

1. Show that the Grassmann graph  $G(v, d)$  is distance transitive with diameter  $\min\{d, v - d\}$ .

2. Let  $U$  be a subspace of  $V(m+n, q)$  with dimension  $m$  and let  $\mathcal{S}$  denote the set of subspaces of dimension  $n$  that are skew to  $U$ . Show that  $|\mathcal{S}| = q^{mn}$  by finding a bijection from  $\mathcal{S}$  to the set of  $m \times n$  matrices over  $GF(q)$ , such that if  $W_1$  and  $W_2$  are elements of  $\mathcal{S}$  with associated matrices  $M_1$  and  $M_2$  then  $\dim(W_1 \cap W_2)$  is determined by  $\text{rk}(M_1 - M_2)$ .
3. Let  $X$  be the graph whose vertices are the  $m \times n$  matrices over  $GF(q)$ , where two matrices  $M_1$  and  $M_2$  are adjacent if  $\text{rk}(M_1 - M_2) = 1$ . Prove that  $X$  is distance-transitive.
4. Determine the diameter of the graph in the previous exercise.
5. In a poset we say that an element  $a$  covers  $b$  if  $a > b$  and if  $a \geq x \geq b$ , then  $x = a$  or  $x = b$ . A lattice is *semimodular* if whenever  $a$  covers  $a \wedge b$  then  $a \vee b$  covers  $b$ . Define the rank of an element  $a$  of a semimodular lattice  $L$  to be the maximum length of a flag in the interval  $[0, a]$ . Prove that the rank function of a semimodular lattice is submodular.
6. Prove that the number of invertible  $d \times d$  matrices over  $GF(q)$  is equal to  $q^{\binom{d}{2}}(q-1)^d[d]!$ .
7. Let  $V$  be a vector space of dimension  $n$  over  $GF(q)$  and let  $U$  be a subspace of dimension  $k$ . Determine the number of subspaces of  $W$  with dimension  $\ell$  such that  $U \cap W = 0$ .
8. Let  $\mathcal{P}$  be the projective space of rank  $d-1$  over  $GF(q)$ . Let  $S$  be a set of points that meets every subspace of rank  $e$ . Show that  $|S|$  contains at least as many points as a subspace of rank  $d-e+1$ ; if equality holds prove that  $S$  is a subspace.
9. Prove that the number of invertible  $d \times d$  matrices over  $GF(q)$  is equal to  $q^{\binom{d}{2}}(q-1)^d[d]!$ .



# Chapter 2

## Projective and Affine Spaces

We start by considering geometries in the abstract, and then projective and affine geometries in particular.

### 2.1 Axiomatics

A *projective geometry* is an incidence structure such that:

- (a) Any two distinct points lie on exactly one line.
- (b) If  $x$ ,  $y$  and  $z$  are non-collinear points and the line  $\ell$  meets  $x \vee y$  and  $x \vee z$  in distinct points then it meets  $y \vee z$ ,
- (c) Every line contains at least three points.

The second condition is known as *Pasch's axiom*. Partial linear spaces satisfying the second condition, along with its dual, are often said to be *thick*.

We show that  $\mathbb{P}(n, \mathbb{F})$  satisfies these axioms, making use of the fact that the rank function on subspaces is modular. Suppose that  $x$ ,  $y$ ,  $z$  are three non-collinear points and that  $\ell$  is a line meeting  $x \vee y$  and  $x \vee z$  in distinct points. Then

$$\text{rk}(\ell \cap (y \vee z)) = \text{rk}(\ell) + \text{rk}(y \vee z) - \text{rk}(\ell \vee (y \vee z)). \quad (2.1.1)$$

Our conditions imply that

$$\ell = (\ell \cap (x \vee y)) \vee (\ell \cap (x \vee z)).$$

## 2. PROJECTIVE AND AFFINE SPACES

---

Since  $\ell$  thus contains two points of the subspace  $x \vee y \vee z$ , it must be contained in it. It follows that  $\ell \vee (y \vee z)$  is also contained in it. Now  $x$ ,  $y$  and  $z$  are not collinear and therefore  $(x \vee y) \cap z = \emptyset$ . Thus

$$\text{rk}(x \vee y \vee z) = \text{rk}(x \vee y) + \text{rk}(z) - \text{rk}((x \vee y) \cap z) = \text{rk}(x \vee y) + \text{rk}(z) = 3.$$

and consequently  $\text{rk}(\ell \vee (y \vee z)) \leq 3$ . From (2.1.1) we now infer that

$$\text{rk}(\ell \cap (y \vee z)) \geq 1,$$

which implies that  $\ell$  meets  $y \vee z$ . Since any field has at least two elements, any line of  $\mathbb{P}(n, \mathbb{F})$  contains at least three points. This proves our claim.

We make some comments about projective planes. The standard description of a projective plane is that it is an incidence structure of points and lines such that

- (a) any two distinct points lie on a unique line,
- (b) any two distinct lines have a unique point in common,
- (c) there are four points, such that no three are collinear.

The third axiom is equivalent to the requiring that every line should have at least three points, and that there be at least two lines. (The proof of this claim is an important exercise.) It is easy to verify that any projective plane is a projective geometry of rank three; the converse is less immediate.

## 2.2 Projective Geometries and Planes

The main result of the first part of this course will be that any finite projective geometry with rank  $n$  at least four is isomorphic to  $\mathbb{P}(n-1, \mathbb{F})$  for some finite field  $\mathbb{F}$ . (This result also holds for infinite projective geometries of finite dimension, if we allow  $\mathbb{F}$  to be non-commutative.) We begin working towards a proof of this.

**2.2.1 Lemma.** *Let  $\mathcal{G}$  be a projective geometry. If  $H$  is a subspace of  $\mathcal{G}$  and  $p$  is a point not on  $H$  then  $p \vee H$  is the union of the lines through  $p$  which contain a point of  $H$ .*

*Proof.* Let  $S$  be the set of all points which lie on a line joining  $p$  to a point of  $H$ . We will show that  $S$  is a subspace of  $\mathcal{G}$ . Suppose that  $\ell$  is a line containing the points  $x$  and  $y$  from  $S$ . We have to show that each point of  $\ell$  lies on a line joining  $p$  to a point of  $H$ .

By the definition of  $S$ , the point  $y$  is on line joining  $p$  to a point in  $H$  and if  $x = p$  then this line must be  $\ell$ .

If both  $x$  and  $y$  lie in  $H$  then  $\ell \in H$ , since  $H$  is a subspace.

Finally assume that  $x$  and  $y$  are both distinct from  $p$  and do not lie in  $H$ . It follows that both  $x$  and  $y$  lie on lines through  $p$  which meet  $H$ . Suppose that they meet  $H$  in  $x'$  and  $y'$  respectively. The line  $\ell$  meets the line  $p \vee x'$  and  $p \vee y'$  in distinct points; therefore it must intersect  $x' \vee y'$  in some point  $q$ . If  $u$  is a point on  $\ell$  then the line  $p \vee u$  meets  $y \vee y'$  in  $p$  and  $y \vee q$  in  $u$ . Hence it must meet the line  $q \vee y'$ , which lies in  $H$ . As  $u$  was chosen arbitrarily on  $\ell$ , it follows that each point of  $\ell$  lies on a line joining  $p$  to a point of  $H$ .

Thus we have shown that all points on  $\ell$  lie in  $S$ , and so  $S$  is a subspace. Any subspace which contains both  $p$  and  $H$  must contain all points on the lines joining  $p$  to points of  $H$ . Thus  $S$  is the intersection of all subspaces containing  $p$  and  $H$ , i.e.,  $S = p \vee H$ .  $\square$

**2.2.2 Corollary.** *Let  $p$  be a point not in the subspace  $H$ . Then each line through  $p$  in  $p \vee H$  intersects  $H$ .*

*Proof.* Let  $\ell$  be a line through  $p$  in  $p \vee H$ . If  $x$  is point other than  $p$  in  $\ell$  then  $x$  lies on a line through  $p$  which meets  $H$ . Since  $x$  and  $p$  lie on exactly one line, it must be  $\ell$ . Thus  $\ell$  meets  $H$ .  $\square$

We can now prove one of classical results in projective geometry, due to Veblen and Young.

**2.2.3 Theorem.** *A linear space is a projective geometry if and only if every subspace of rank three is a projective plane.*

*Proof.* We prove that any two lines in a projective geometry of rank three must intersect. This implies that projective geometries of rank three are projective planes. Suppose that  $\ell_1$  and  $\ell_2$  are two lines in a rank three geometry. Let  $p$  be a point in  $\ell_1$  but not in  $\ell_2$ . From the previous corollary, each line through  $p$  in  $p \vee \ell_2$  must meet  $\ell_2$ . Since  $p \vee \ell_2$  has rank at least three, it must be the entire geometry. Hence  $\ell_1 \in p \vee \ell_2$  and so it meets  $\ell_2$

as required. To prove the converse, note that Pasch's axiom is a condition on subspaces of rank three, that is, it holds in a linear space if and only if it holds in all subspaces of rank three. But as we noted earlier, if every two lines in a linear space of rank three meet then it is trivial to verify that Pasch's axiom holds in it.  $\square$

## 2.3 Projective Geometries from Vector Spaces

We describe the most important construction of projective geometries. Let  $V$  a vector space with dimension at least two over a field  $\mathbb{F}$ . Let  $\mathcal{P}(V)$  denote incidence structure formed by the 1-dimensional and 2-dimensional subspaces of  $V$ , where a 1-dimensional subspace is incident with the 2-dimensional subspaces that contain it.

We define a rank function on subsets of  $V$  by defining the rank of a subset to be the dimension of the subspace it spans. Here the flats are precisely the subspaces of  $V$ , and the join of two subspaces  $H$  and  $K$  is the subspace sum  $H + K$ . Since for two subspaces  $H$  and  $K$  we have

$$\dim(H + K) = \dim(H) + \dim(K) - \dim(H \cap K)$$

it is easy to verify that the rank function is submodular.

A projective space of rank two is a *projective line* while a space of rank three is a *projective plane*.

We can represent each point of  $\mathcal{P}(V)$  by a non-zero element  $x$  of  $V$ , provided we understand that any non-zero scalar multiple of  $x$  represents the same point. We can represent a subspace of  $V$  with dimension  $k$  by an  $n \times k$  matrix  $M$  over  $\mathbb{F}$  with linearly independent columns. The column space of  $M$  is the subspace it represents. Clearly two matrices  $M$  and  $N$  represent the same subspace if and only if there is an invertible  $k \times k$  matrix  $A$  such that  $M = NA$ . (The subspace will be determined uniquely by the reduced column-echelon form of  $M$ .)

Any invertible linear mapping of  $V$  to itself permutes the 1-dimensional and 2-dimensional subspaces of  $V$  and preserves incidence. Hence it gives rise to an automorphism of the projective space. Note though that the scalar matrices  $cI$  give rise to the identity automorphism on the projective

space. We can also verify that any field automorphism gives rise to an automorphism of our projective space. The automorphism group of a projective space acts transitively on the set of subspaces of given rank.

If  $M$  represents a hyperplane, then  $\dim(\ker M^T) = 1$  and so we can specify the hyperplane by a non-zero element  $a$  of  $\mathbb{F}^d$  such that  $a^T M = 0$ . Then  $x$  is a vector representing a point on this hyperplane if and only if  $a^T x = 0$ .

The following lemma records a fundamental property of Desarguesian projective spaces.

**2.3.1 Lemma.** *Suppose  $V$  is a vector space of dimension at least three of the field  $\mathbb{F}$ . If  $\ell$  is a line and  $H$  is a hyperplane in  $\mathcal{P}(V)$ , then  $\ell \cap H \neq \emptyset$ .*

*Proof.* Suppose the line is the subspace spanned by  $x$  and  $y$  and the hyperplane  $H$  is given by a vector  $a$ . If  $a^T x = 0$  then  $x$  is on  $H$ , otherwise the vector

$$(a^T x)y - (a^T y)x$$

is on  $H$  (and on our line). □

You might also prove this using the formula for  $\dim(H + K)$ .

## 2.4 The Rank Function of a Projective Geometry

One of the most important properties of projective geometries is that their rank functions are modular. Proving this is the main goal of this section. Note that if  $p$  is a point and  $H$  a subspace in any linear space then  $\text{rk}(p \vee H) \geq \text{rk}(H) + 1$ . We will use this fact repeatedly.

**2.4.1 Lemma.** *Let  $H$  and  $K$  be two subspaces of a projective geometry such that  $H \subset K$  and let  $p$  be a point not in  $K$ . Then  $p \vee H \subset p \vee K$ .*

*Proof.* Clearly  $p \vee H \subseteq p \vee K$  and if  $p \vee H = p \vee K$  then  $K \subseteq p \vee H$ . If the latter holds and  $k \in K \setminus H$  then the line  $p \vee k$  must contain a point,  $h$  say, of  $H$ . This implies that  $p \in h \vee k$  and, since  $h \vee k \subseteq K$ , that  $p \in K$ . □

**2.4.2 Corollary.** *Let  $H$  be a subspace of a projective geometry and let  $p$  be a point not in  $H$ . Then  $H$  is a maximal subspace of  $p \vee H$ .*

## 2. PROJECTIVE AND AFFINE SPACES

---

*Proof.* Let  $K$  be a subspace of  $p \vee H$  strictly containing  $H$ . If  $p \in K$  then  $K = p \vee H$ . If  $p \notin K$  then, by the previous lemma,  $p \vee H$  is strictly contained in  $p \vee K$ . Since this contradicts our assumption that  $K \subseteq p \vee H$ , our result is proved.  $\square$

**2.4.3 Theorem.** *All maximal subspaces of a projective geometry have the same rank.*

*Proof.* We will actually prove a more powerful result. Let  $H$  and  $K$  be two distinct maximal subspaces. Let  $h$  be point in  $H \setminus K$  and let  $k$  be a point in  $K \setminus H$ . The line  $h \vee k$  cannot contain a second point,  $h'$  say, of  $H$  since then we would have  $k \in h \vee h' \subseteq H$ . Similarly  $h \vee k$  cannot contain a point of  $K$  other than  $k$ . By the third axiom for a projective geometry,  $h \vee k$  must contain a point  $p$  distinct from  $h$  and  $k$  and, by what we have just shown,  $p \notin H \cup K$ . Since  $H$  and  $K$  are maximal  $p \vee H = p \vee K$ . By Corollary 2.2.2, each line through  $p$  must contain a point of  $H$  and a point of  $K$ . Using  $p$  we construct a mapping  $\phi_p$  from  $H$  into  $K$ . If  $h \in H$  then

$$\phi_p(h) := (p \vee h) \cap K.$$

If  $\phi_p(h_1) = \phi_p(h_2)$  then the lines  $p \vee h_1$  and  $p \vee h_2$  have two points in common, and therefore coincide. This implies that they meet  $H$  in the same point and hence  $\phi_p$  is injective.

If  $k \in K$  then  $k \vee p$  must contain a point  $h'$  say, of  $H$ . We have  $\phi_p(h') = k$ , whence  $\phi_p$  is surjective. Thus we have shown that  $\phi_p$  is a bijection.

We prove next that  $\phi_p$  maps subspaces onto subspaces.

Let  $L$  be a subspace of  $H$ . Then  $\phi_p(L)$  lies in  $(p \vee L) \cap K$ . Conversely, if  $x \in (p \vee L) \cap K$  then  $x$  is on a line joining  $p$  to a point of  $L$  and so  $x \in \phi_p(L)$ . Hence  $\phi_p(L) = (p \vee L) \cap K$ . Since  $p \vee L$  is a subspace, so is  $(p \vee L) \cap K$ . As  $\phi_p$  is bijective on points, it must map distinct subspaces of  $H$  onto distinct subspaces of  $K$ . A similar argument to the above shows that  $\phi_p^{-1}$  maps subspaces of  $K$  onto subspaces of  $H$ . Consequently we have shown that  $\phi_p$  induces an isomorphism from the lattice of subspaces of  $H$  onto the subspaces of  $K$ . This implies immediately that  $H$  and  $K$  have the same rank. (It is also worth noting that it implies that  $\phi_p$  is a collineation—it must map subspaces of rank two to subspaces of rank two.)  $\square$

A more general form of the next result is stated in the Exercises.

**2.4.4 Lemma.** *Let  $H$  and  $K$  be subspaces of a projective geometry and let  $p$  be a point in  $H$ . Then  $(p \vee K) \cap H = p \vee (H \cap K)$ .*

*Proof.* As  $H \cap K$  is contained in both  $p \vee K$  and  $H$  and as  $p \in H$ , it follows that  $p \vee (H \cap K) \subseteq (p \vee K) \cap H$ . Let  $x$  be a point in  $(p \vee K) \cap H$ . By Corollary 2.2.2, there is a point  $k$  in  $K$  such that  $x \in p \vee k$ . Now  $p \vee k = p \vee x$  and so  $k \in p \vee x$ . Since  $x \in H$  then this implies that  $p \vee x \subseteq H$  and thus that  $k$  lies in  $H$  as well as  $K$ . Summing up, we have shown that if  $x \in (p \vee K) \cap H$  then  $x \in p \vee k$ , where  $k \in H \cap K$ , i.e., that  $x \in p \vee (H \cap K)$ .  $\square$

**2.4.5 Theorem.** *If  $H$  and  $K$  are subspaces of a projective geometry then*

$$\text{rk}(H \vee K) + \text{rk}(H \cap K) = \text{rk}(H) + \text{rk}(K).$$

*Proof.* We use induction on  $\text{rk}(H) - \text{rk}(H \cap K)$ . Suppose first that this difference is equal to one. This implies  $H \cap K$  is maximal in  $H$  and accordingly

$$\text{rk}(H) - \text{rk}(H \cap K) = 1. \quad (2.4.1)$$

If  $p \in H \setminus K$  then, using the maximality of  $H \cap K$  in  $H$ , we find that  $p \vee (H \cap K) = H$  and  $H \vee K = p \vee K$ . By Corollary 2.4.2 it follows that  $K$  is maximal in  $H \vee K$  and so

$$\text{rk}(H \vee K) - \text{rk}(K) = 1. \quad (2.4.2)$$

Subtracting (2.4.1) from (2.4.2) and rearranging yields the conclusion of the Theorem.

Assume now that  $H \cap K$  is not maximal in  $H$ . Then we can find a point  $p \in H \cap K$  such that  $p \vee (H \cap K) \neq H$ . Suppose  $L = p \vee (H \cap K)$ . Then  $H \cap K$  is maximal in  $L$  (by Corollary 2.4.2) and so, by what we have already proved,

$$\text{rk}(L \vee K) + \text{rk}(L \cap K) = \text{rk}(L) + \text{rk}(K). \quad (2.4.3)$$

Next we note that  $\text{rk}(H) - \text{rk}(L \vee K) < \text{rk}(H) - \text{rk}(H \cap K)$  and so by induction we have

$$\text{rk}(H \vee (L \vee K)) + \text{rk}(H \cap (L \vee K)) = \text{rk}(L \vee K) + \text{rk}(H). \quad (2.4.4)$$

Now  $L \vee K = p \vee (H \cap K) \vee K = p \vee K$ . By the previous lemma then,

$$H \cap (L \vee K) = H \cap (p \vee K) = p \vee (H \cap K) = L.$$

Furthermore  $H \vee (L \vee K) = H \vee K$ , and so (2.4.4) can be rewritten as

$$\text{rk}(H \vee K) + \text{rk}(L) = \text{rk}(L \vee K) + \text{rk}(H). \quad (2.4.5)$$

Since  $L \cap K = H \cap K$ , we can now derive the theorem by adding (2.4.3) to (2.4.5) and rearranging.  $\square$

An important consequence of this theorem is that the rank of a subspace of a projective geometry spanned by a set  $S$  is at most  $|S|$ . In particular, three pairwise non-collinear points must span a plane, rather than some subspace of larger rank.

## 2.5 Duality

Let  $H$  and  $K$  be two maximal subspaces of a projective geometry with rank  $n$ . Then  $\text{rk}(H \vee K) = n$  and from Theorem 2.4.5 we have

$$\text{rk}(H \cap K) = \text{rk}(H) + \text{rk}(K) - \text{rk}(H \vee K) = (n - 1) + (n - 1) - n = n - 2.$$

Thus any pair of maximal subspaces intersect in a subspace of rank  $n - 2$ , and therefore we can view the subspaces of rank  $n - 1$  and the subspaces of rank  $n - 2$  as the points and lines of a linear space. We call this the *dual* of our projective geometry. (In general the dual of a linear space need not be linear.)

**2.5.1 Theorem.** *The dual of a projective geometry is a projective geometry.*

*Proof.* We first show that each line in the dual lies on at least three points. Let  $K$  be space of rank  $n - 2$  and let  $H_1$  be a hyperplane which contains it. Since  $H_1$  is not the whole space, there must be point  $p$  not in it. Then  $K$  is maximal in  $p \vee K$  and so  $p \vee K$  is a subspace of rank  $n - 1$  on  $k$ . It is not equal to  $H$ , because  $p$  is in it. Now choose a point  $q$  in  $H \setminus K$ . The line  $p \vee q$  must contain a third point,  $x$  say. If  $x \in H$  then  $p \in x \vee q \subseteq H$ , a contradiction. Similarly  $x$  cannot lie in  $K$  and so it follows that  $x \vee K$  is a third subspace of rank  $n - 1$  on  $K$ .

Now we should verify the second axiom. However we will show that any two subspaces of rank  $n - 2$  intersecting in a subspace of rank  $n - 3$  lie in a subspace of rank  $n - 1$ . This implies that any two lines in the dual which

line a subspace of rank three must intersect, and so all rank three subspaces are projective planes. An appeal to Theorem 2.2.3 now completes the proof. So, suppose that  $K_1$  and  $K_2$  are subspaces with rank  $n - 2$  which meet in a subspace of rank  $n - 3$ . Then

$$\text{rk}(K_1 \vee K_2) = \text{rk}(K_1) + \text{rk}(K_2) - \text{rk}(K_1 \cap K_2) = (n-2) + (n-2) - (n-3) = n-1$$

and  $K_1 \vee K_2$  has rank  $n - 1$  as required.  $\square$

Our next task is to determine the relation between the subspaces of a projective geometry and those of its dual. It is actually quite simple—it is equality.

**2.5.2 Lemma.** *Let  $\mathcal{G}$  be a projective geometry and let  $L$  be a subspace of it. Then the hyperplanes which contain  $L$  are a subspace in the dual of  $\mathcal{G}$ .*

*Proof.* Suppose that  $\mathcal{G}$  has rank  $n$ . The lines of the dual are the sets of hyperplanes which contain a given subspace of rank  $n - 2$ . Suppose that if  $K$  is a subspace of rank  $n - 2$  and  $H_1$  and  $H_2$  are two maximal subspaces which contain  $K$ . If both  $H_1$  and  $H_2$  contain  $L$  then  $L \subseteq H_1 \cap H_2 = K$ . This proves the lemma.  $\square$

It is clear from the axioms that any subspace  $H$  of a projective geometry is itself a projective geometry. The previous lemma yields that the hyperplanes which contain  $H$  are also the points of a projective geometry. Furthermore, if  $K$  is a subspace of rank  $m$  contained in  $H$  then the maximal subspaces of  $H$  which contain  $K$  are again the points of a projective geometry. Applying duality to this last remark, we see that the subspaces of rank  $m + 1$  in  $H$  which contain  $K$  are the points of projective geometry. We will denote this geometry by  $H/K$ , and refer to it as an *interval* of the original geometry. Duality is a useful, but somewhat slippery concept. It will reappear in later sections, sometimes saving half our work.

## 2.6 Affine Geometries

We have already met the affine spaces  $AG(n, \mathbb{F})$ . An *affine geometry* is defined as follows. Let  $\mathcal{G}$  be a projective geometry and let  $H$  be a hyperplane in it. If  $S$  is a set of points in  $\mathcal{G} \setminus H$ , define  $\text{rk}_H(S)$  to be  $\text{rk}(S)$ . This can be shown to be a submodular rank function on the points not on  $H$ , and the combinatorial geometry which results is an *affine geometry*. (It will

## 2. PROJECTIVE AND AFFINE SPACES

---

sometimes be denoted by  $\mathcal{G}^H$ .) The flats of  $\mathcal{A}$  are the subsets of the form  $K \setminus H$ , where  $K$  is a flat/subspace of  $\mathcal{G}$ . They will be referred to as *affine subspaces*; these are all linear subspaces. However, in some cases there will be linear subspaces which are not flats. (This point will be considered in more detail at the start of the following section.)

If  $K_1$  and  $K_2$  are two subspaces of  $\mathcal{G}$  such that  $K_1 \cap K_2 \subseteq H$  and

$$\text{rk}(K_1 \cap K_2) = \text{rk}(K_1) + \text{rk}(K_2) - \text{rk}(K_1 \vee K_2),$$

we say that they are *parallel*. The most important cases are parallel hyperplanes and parallel lines. The hyperplane  $H$  is often called the “hyperplane at infinity”, since it is where parallel lines meet. From the definition we see that two disjoint subspaces of an affine geometry are parallel if and only if the dimension of their join is ‘as small as possible’. In particular, two lines are parallel if and only if they are disjoint and coplanar. It is not too hard to verify that parallelism is an equivalence relation on the subspaces of an affine geometry. (This is left as an exercise.) The lines of  $\mathcal{G}$  which pass through a given point of  $H$  partition the point set of the affine geometry. We call such a set of lines a *parallel class*. Any set of parallel lines can be extended uniquely to a parallel class. For given two parallel lines, we can identify the point  $p$  on  $H$  where they meet; the remaining lines in the parallel class are those that also meet  $H$  at  $p$ .

Any collineation  $\alpha$  of an affine geometry must map parallel lines to parallel lines, since it must map disjoint coplanar lines to disjoint coplanar lines. Thus  $\alpha$  determines a bijection of the point set of  $H$ . It actually determines a collineation. To prove this we must find a way of recognising when the ‘points at infinity’ of three parallel classes are collinear. Suppose that we have three parallel classes. Choose a line  $\ell$  in the first. Since the parallel classes partition the points of the affine geometry, any point  $p$  on  $\ell$  is also on a line from the second and the third parallel class. The points at infinity on these three lines are collinear, in  $H$ , if and only if the lines are coplanar. It follows that any collineation of an affine geometry determines a collineation of the hyperplane at infinity, and hence of the projective geometry. Because of the previous result, we can equally well view an affine geometry as a projective geometry  $\mathcal{G}$  with a distinguished hyperplane. The points not on the hyperplane are the *affine points* and the lines of  $\mathcal{G}$  not contained in  $H$  are the *affine lines*. It is important to realize that there are two different viewpoints available, and in the literature it is common to find an author shift from one to the other, without explicit warning.

We consider an example to illustrate some issues. Let  $V$  be a vector space of dimension  $d$  over  $GF(2)$ . We can form an incidence structure with the vectors in  $V$  as points and the cosets of the 1-dimensional subspaces as lines. Then each pair of points is a line and so each subset of points is a subspace. We could view this as a combinatorial geometry where each subset is a flat and the rank of a subset  $S$  is  $|S|$ ; this means we that we are ignoring a lot of structure. However there is a second rank function available: define the rank of a set of vectors to be the dimension of the affine space that they span, plus one. Now the flats are the affine subspaces. It is this rank function that we will use.

## 2.7 Axioms for Affine Spaces

There is a difficulty in providing a set of axioms for affine spaces, highlighted by the following. Consider the projective plane  $PG(2, 2)$ . Removing a line from it gives the affine plane  $AG(2, 2)$  which has four points and six lines; each line has exactly two points on it. (Thus we could identify its points and lines with the vertices and edges of the complete graph  $K_4$  on four vertices.) This is a linear space but, unfortunately for us, it has rank four: any set of three points is a subspace of rank three. More generally, any subset of the points of  $AG(n, 2)$  is a subspace of  $AG(n, 2)$ , viewed as a linear space. However not all subspaces are flats.

One set of axioms for affine spaces has been provided by H. Lenz. An *affine space* is an incidence structure equipped with an equivalence relation on its lines, called parallelism and denoted by  $\parallel$ , such that the following hold.

- (a) Any two points lie on a unique line.
- (b) Given any line  $\ell$  and point  $p$  not on  $\ell$ , there is a unique line  $\ell'$  through  $p$  and parallel to  $\ell$ .
- (c) If  $\ell_0, \ell_1$  and  $\ell_2$  are lines such that  $\ell_0 \parallel \ell_1$  and  $\ell_1 \parallel \ell_2$  then  $\ell_0 \parallel \ell_2$ . (Or more clearly: parallelism is an equivalence relation on lines.)
- (d) If  $a \vee b$  and  $c \vee d$  are parallel lines, and  $p$  is a point on  $a \vee c$  distinct from  $a$  then  $p \vee b$  intersects  $c \vee d$ .

## 2. PROJECTIVE AND AFFINE SPACES

---

- (e) If  $a, b$  and  $c$  are three points, not all on one line, then there is a point  $d$  such that  $a \vee b \parallel c \vee d$  and  $a \vee c \parallel b \vee d$ .
- (f) Any line has at least two points.

It is not hard to show that all lines in an affine space must have the same number of points. This number is called the *order* of the space. If the order is at least three then the axiom (e) is implied by the other axioms. On the other hand, if all lines have two points then (d) is vacuously satisfied. Hence we are essentially treating separately the cases where the order is two, and where the order is at least three. Any line trivially satisfies the above set of axioms. If any two disjoint lines are parallel then we have an *affine plane*. These may be defined more simply as linear spaces which are not lines and have the property that, given any point  $p$  and line  $\ell$  not on  $p$ , there is a unique line through  $p$  disjoint from  $\ell$ . We can provide a simpler set of axioms for thick affine spaces. Call two lines in a linear space *strongly parallel* if they are disjoint and coplanar. Then the linear space  $\mathcal{L}$  is an affine space if:

- (a) strong parallelism is an equivalence relation on the lines of  $\mathcal{L}$ ,
- (b) if  $p$  is a point, and  $\ell$  is a line of  $\mathcal{A}$ , then there is a unique line through  $p$  strongly parallel to  $\ell$ .

As with our first set of axioms, no mention is made of affine subspaces. However, in this case they are just the linear spaces. In the sequel, we will distinguish this set of axioms by referring to them as the “axioms for thick affine spaces”. The first, official, set will be referred to as “Lenz’s axioms”.

### 2.8 Affine Spaces in Projective Space

We outline a proof that any thick affine space arises by deleting a hyperplane from a suitable projective plane.

**2.8.1 Lemma.** *Let  $\mathcal{A}$  be a thick affine space with rank at least four. Let  $\pi$  be a plane in  $\mathcal{A}$  and let  $D$  be a line intersecting, but not contained in  $\pi$ . Then the union of the point sets of those planes which contain  $D$ , and meet  $\pi$  in a line, is a subspace.*

*Proof.* Let  $W$  denote the union described. Since the subspace  $D \vee \pi$  is the join of  $D$  and any line in  $\pi$  which does not meet  $D$ , no line in  $\pi$  which does not meet  $D$  can be coplanar with it. Hence no line in  $\pi$  is parallel to  $D$ .

If  $x$  is point in  $W$  which is not on  $D$  then  $x \vee D$  is a plane. Since  $x \in W$ , there is a plane containing  $x$  and  $D$  which meets  $\pi$  in a line. Thus  $x \vee D$  must meet  $\pi$  in line,  $l$  say. As  $x$  is not on  $l$ , there is unique line,  $l'$  say, parallel to it through  $x$ . Since  $D$  is not parallel to  $l$ , it is not parallel to  $l'$ . Therefore  $D$  meets  $l'$ . We will denote the point of intersection of  $D$  with  $l'$  by  $d(x)$ . Now suppose that  $x$  and  $y$  are distinct points of  $W$ . We seek to show that any point on  $x \vee y$  lies in  $W$ . There are unique lines through  $x$  and  $y$  parallel to  $D$ ; since they lie in  $x \vee D$  and  $y \vee D$  respectively they meet  $\pi$  in points  $x'$  and  $y'$ . If  $u$  is a point on  $x \vee y$  then the unique line through  $u$  parallel to  $D$  must intersect  $x' \vee y'$ . Hence  $u$  lies in the plane spanned by this point of intersection and  $D$ , and so  $u \in W$ .  $\square$

This lemma provides a very useful tool for working with affine spaces. We note some consequences.

**2.8.2 Corollary.** *Let  $\pi$  be a plane in the affine space  $\mathcal{A}$  and let  $x$  and  $y$  be two points not on  $\pi$  such that  $x \vee \pi = y \vee \pi$ . If  $x \vee y$  is disjoint from  $\pi$  then it is parallel to some line contained in  $\pi$ .*

*Proof.* Let  $p$  be a point in  $\pi$ . From the previous lemma we see that since  $y \in x \vee \pi$ , the plane spanned  $y$  and the line  $x \vee p$  meets  $\pi$  in a line  $l$ . As  $l$  lies on  $\pi$  it is disjoint from  $x \vee y$  and hence it is parallel to it.  $\square$

**2.8.3 Corollary.** *Let  $\mathcal{A}$  be an affine space. If two planes in  $\mathcal{A}$  have a point in common and are contained in subspace of rank four, they must have a line in common.*

*Proof.* Suppose that  $p$  is contained in the two planes  $\sigma$  and  $\pi$ . Let  $l$  be a line in  $\sigma$  which does not pass through  $p$ . As  $l$  is disjoint from  $\pi$  it is, by the previous corollary, parallel to a line  $l'$  in  $\pi$ . Let  $m$  be the line through  $p$  in  $\sigma$  parallel to  $l$  and let  $m'$  be the line in  $\pi$  parallel to  $p$ . Then

$$m' \parallel l', l' \parallel l, l \parallel m$$

and thus  $m = m'$ . Therefore  $m \subseteq \sigma \cap \pi$ .  $\square$

## 2. PROJECTIVE AND AFFINE SPACES

---

Let  $\mathcal{A}$  be an affine geometry. We show how to embed it in a projective geometry. Assume that the rank of  $\mathcal{A}$  is at least three. (If the rank is less than three, there is almost nothing to prove.) Let  $P$  be a set with cardinality equal to the number of parallel classes. We begin by adjoining  $P$  to the point set of  $\mathcal{A}$ . If a line of  $\mathcal{A}$  lies in the  $i$ -th parallel class, we extend it by adding the  $i$ -th point of  $P$ . It is straightforward to show that each plane in  $\mathcal{A}$  has now been extended to a projective plane. Each plane in  $\mathcal{A}$  determines a set of parallel classes, and thus a subset of  $P$ . These subsets are defined to be lines of the extended geometry; the original lines will be referred to as *affine* lines if necessary. Two points  $a$  and  $b$  of  $\mathcal{A}$  are collinear with a point  $p$  of  $P$  if and only if the line  $a \vee b$  is in the parallel class associated with  $p$ . With the additional points and lines as given, we now have a new incidence structure  $\mathcal{P}$ . We must verify that it is a linear space.

Let  $a$  and  $b$  be two points. If these both lie in  $\mathcal{A}$  then there is a unique line through them. If  $a \in \mathcal{A}$  and  $b \in P$  then there is a unique line in the parallel class determined by  $b$  which passes through  $a$ . Finally, suppose that  $a$  and  $b$  are both in  $P$ . Let  $l$  be a line in the parallel class determined by  $a$ . If  $x$  is an affine point in  $l$  then there is a unique line in the parallel class of  $b$  passing through it. With  $l$ , this line determines a plane which contains all the lines in  $b$  which meet  $l$ . This shows that each line  $l$  in  $a$  determines a unique plane.

We claim that it is a projective space. This can be proved by showing that each plane in  $\mathcal{P}$  is projective. The only difficult case is to verify that the planes contained in  $P$  are projective. Each plane of  $P$  corresponds to a subspace of  $\mathcal{A}$  with rank four, so studying the planes of  $P$  is really studying these subspaces of  $\mathcal{A}$ . The planes contained in  $P$  are projective planes if every pair of lines in them intersect. Thus we must prove that if  $\sigma$  and  $\pi$  are two planes of  $\mathcal{A}$  contained in a subspace of rank four, then there is a line in  $\sigma$  parallel to  $\pi$ . There are two cases to consider. Suppose first that  $\sigma \cap \pi = \emptyset$ . Then, by Corollary 2.8.2, any line in  $\sigma$  is parallel to a line in  $\pi$ , and therefore there is a point in  $P$  lying on both the lines determined by  $\sigma$  and  $\pi$ . Suppose next that  $\sigma$  and  $\pi$  have a point in common. Then, by Corollary 2.8.3, these planes must have a line in common and so the parallel class containing it lies on the lines in  $P$  determined by them. This completes the proof that all thick affine spaces are projective spaces with a hyperplane removed.

We can embed affine geometries of order two in an ad hoc fashion. One approach would be to verify the result for  $AG(d, 2)$ , and to note that Corol-

lary 2.8.2 and Corollary 2.8.3 both hold. Next, show that any affine geometry of rank four and order two is isomorphic to  $AG(4, 2)$ , whence these two corollaries hold for any affine geometry of order two.

In the next chapter we will use our axiomatic characterization of affine spaces to show that all projective spaces of rank at least four have the form  $\mathbb{P}(n, \mathbb{F})$ , that is, are projective spaces over some skew field.

## 2.9 Characterizing Affine Spaces by Planes

We have seen that a linear space with rank at least three is a projective geometry if and only if every plane in it is a projective plane. The corresponding result for affine geometries is more delicate and is due to Buekenhout.

**2.9.1 Theorem.** *Let  $\mathcal{A}$  be a linear space with rank at least three. If each line has at least four points, and if all planes of  $\mathcal{A}$  are affine planes, then  $\mathcal{A}$  is an affine geometry.*

*Proof.* We verify that the axioms for thick affine spaces hold. Since the second of these axioms is a condition on planes, it is automatically satisfied. Thus we need only prove that parallelism is an equivalence relation on the lines of  $\mathcal{A}$ . If  $\pi$  is a plane and  $D$  a line meeting  $\pi$  in the point  $a$ , we define  $W = W(\pi, D)$  to be the union of the point sets of the planes which contain  $D$  and meet  $\pi$  in a line.

Suppose  $w \in W \setminus D$ . The only plane containing  $w$  and  $D$  is  $w \vee D$ , hence the points of this plane must belong to  $W$ . In particular, it must meet  $\pi$  in a line  $l$ . Since  $w$  is not on  $l$ , there is a unique line  $m$  in  $w \vee D$  through  $w$  and parallel to  $l$ . The line  $D$  meets  $l$  in  $a$ , and is therefore not parallel to it. Hence it is not parallel to  $m$ . Denote the point of intersection of  $m$  and  $D$  by  $d(w)$ . Note that if  $b$  is point on  $D$ , other than  $a$  or  $d(w)$  then  $bw$  is a line in  $w \vee D$  not parallel to  $l$ . Thus it must intersect  $l$  in a point.

Our next step is to show that  $W$  is a subspace. This means we must prove that if  $x$  and  $y$  are points in  $W \setminus \pi$  then all points on  $xy$  lie in  $W$ . Suppose first that  $xy \cap \pi = \emptyset$ . Since the lines of  $\mathcal{A}$  have at least four points on them, there is a point  $b$  on  $D$  distinct from  $a$ ,  $d(x)$  and  $d(y)$ . The line  $bx$  and  $by$  must meet  $\pi$ , in points  $x'$  and  $y'$  say. As  $xy$  and  $\pi$  are disjoint,  $xy \cap x'y' = \emptyset$ . Accordingly  $xy$  and  $x'y'$  are parallel (they both lie in the plane  $b \vee xy$ ). If  $u$  is point on  $xy$  then  $bu$  cannot be parallel to  $x'y'$  and so  $u$  is on a line joining  $b$  to a point of  $\pi$ . This implies that the plane  $u \vee D$

## 2. PROJECTIVE AND AFFINE SPACES

---

meets  $\pi$  in two distinct points. Hence it is contained in  $W$ , and so  $u \in W$ , as required.

Assume next that  $xy$  meets  $\pi$  in a point,  $z$  say. Let  $\sigma$  be the plane  $y \vee x \vee d(x)$ . If  $\sigma \cap \pi$  is a line then, since it is disjoint from  $x \vee d(x)$ , it is parallel to it. So, if  $u$  is a point distinct from  $x$  and  $y$  on  $xy$  then  $u \vee d(x)$  cannot be parallel to  $\sigma \cap \pi$ . Accordingly  $u \vee d(x)$  contains a point of  $\pi$ , implying as before that  $u \vee D$  is in  $W$ . Hence  $u \in W$ . The only possibility remaining is that  $\sigma \cap \pi$  is a point, in which case it is  $z$ . Assume  $u$  is a point distinct from  $x$  and  $y$  on  $xy$ . Since the line  $z \vee d(x)$  has at least four points, and since there is only one line in  $\sigma$  parallel to  $x \vee d(x)$  through  $u$ , there is a line through  $u$  meeting  $x \vee d(x)$  and  $z \vee d(x)$  in points  $x'$  and  $y'$  respectively. Now  $x \vee d(x)$  is disjoint from  $\pi$  and therefore all points on it are in  $W$ . Also all points on  $z \vee d(x)$  are in  $W$ . Hence  $x'$  and  $y'$  lie in  $W$ . Since  $z$  does not lie on  $x'y'$ , this line is disjoint from  $\pi$ . This shows that all points on it lie in  $W$ . We have finally shown that  $W$  is a subspace, and can now complete the proof of the theorem.

Suppose that  $l_1, l_2$  and  $l_3$  are lines in  $\mathcal{A}$ , with  $l_1 \parallel l_2$  and  $l_2 \parallel l_3$ . Let  $\pi$  be the plane  $l_1 \vee l_2$ , let  $D$  be a line joining a point  $b$  on  $l_3$  to a point  $a$  in  $l_2$  and let  $W = W(\pi, D)$ . Since  $b \in W$  and  $W$  is a subspace, the plane  $b \vee l_1$  lies in  $W$ . In this plane there is a unique line through  $b$  parallel to  $l_1$ . Denote it by  $l'_3$ . As  $l_3 \vee l_2$  meets  $\pi$  in  $l_2$ , we see that  $l_3$  is disjoint from  $\pi$ . Similarly  $l'_3 \vee l_1$  meets  $\pi$  in  $l_1$ , and so  $l'_3$  is disjoint from  $\pi$ . The plane  $a \vee l'_3$  is contained in  $W$ , and contains  $D$ . By the definition of  $W$ , any point of  $a \vee l'_3$  lies in a plane which contains  $D$  and meets  $\pi$  in a line. This plane must be  $a \vee l'_3$ . Denote its line of intersection with  $\pi$  by  $l'_2$ . Since  $l'_3$  is disjoint from  $\pi$ , the lines  $l'_2$  and  $l'_3$  are parallel. If  $l_2 = l'_2$  then  $l_3$  and  $l'_3$  are two lines in  $b \vee l_2$  intersecting in  $b$  and parallel to  $l_2$ . Hence they must be equal. If  $l_2 \neq l'_2$  then  $l'_2$  must intersect  $l_1$ , in a point  $c$  say. But then  $l_1$  and  $l'_2$  are lines in  $c \vee l_3$  parallel to  $l_3$ . Therefore  $l_1 = l'_2$ , which is impossible since  $a \in l'_2$  and  $a \notin l_1$ . Thus we are forced to conclude that  $l_1 \parallel l_3$ .  $\square$

The above proof is based in part on some notes of U. S. R. Murty. There are examples of linear spaces which are not affine geometries, but where every plane is affine. These were found by M. Hall; all lines in them have exactly three points.

## 2.10 Affine Spaces

We define *affine  $n$ -space* over  $\mathbb{F}$  to be  $\mathbb{F}^n$ , equipped with the relation of affine dependence. A sequence of points  $v_1, \dots, v_k$  from  $\mathbb{F}^n$  is *affinely dependent* if there are scalars  $a_1, \dots, a_k$  not all zero such that

$$\sum_i a_i = 0, \quad \sum_i a_i v_i = 0.$$

We also say that  $v$  is an *affine linear combination* of  $v_1, \dots, v_k$  if

$$v = \sum_i a_i v_i$$

where

$$\sum_i a_i = 1.$$

Thus if  $v$  is an affine linear combination of  $v_1, \dots, v_k$ , then the vectors  $-v, v_1, \dots, v_k$  are affinely dependent.

Note that if  $v \neq 0$  and  $a \neq 1$  then the vectors  $v, av$  are not affinely dependent. In particular if  $v \neq 0$ , then  $0, v$  is not affinely dependent. In affine spaces the zero vector does not play a special role.

If  $u$  and  $v$  are distinct vectors, then the set

$$\{au + (1 - a)v : a \in \mathbb{F}\}$$

consist of all affine linear combinations of  $u$  and  $v$ . If  $\mathbb{F} = \mathbb{R}$  then it is the set of points on the straight line through  $u$  and  $v$ ; in any case we call it the affine line through  $u$  and  $v$ . A subset  $S$  of  $V$  is an *affine subspace* if it is closed under taking affine linear combination of its elements. Equivalently,  $S$  is a subspace if, whenever it contains distinct points  $u$  and  $v$ , it contains the affine line through  $u$  and  $v$ . (Prove it.) A single vector is an affine subspace. The affine subspaces of  $\mathbb{F}^n$  are the cosets of its linear subspaces.

Suppose  $\mathcal{A}$  denotes the elements of  $\mathbb{F}^{n+1}$  with last coordinate equal to 1. Then a subset  $S$  of  $\mathcal{A}$  is linearly dependent in  $\mathbb{F}^{n+1}$  if and only if it is affinely dependent. This allows us to identify affine  $n$ -space over  $\mathbb{F}$  with a subset of projective  $n$ -space over  $\mathbb{F}$ . (In fact projective  $n$ -space is the union of  $n + 1$  copies of affine  $n$ -space.)

## 2.11 Coordinates

We start with the easy case. If  $\mathcal{A}$  is the affine space  $\mathbb{F}^n$ , then each point of  $\mathcal{A}$  is a vector and the coordinates of a point are the coordinates of the associated vector.

Now suppose  $\mathcal{P}$  is the projective space associated to  $\mathbb{F}^n$ . Two non-zero vectors  $x$  and  $y$  represent the same point if and only if there is a non-zero scalar  $a$  such that  $y = ax$ . Thus a point is an equivalence class of non-zero vectors. As usual it is often convenient to represent an equivalence class by one of its elements. Here there is no canonical choice, but we could take the representative to be the vector with first non-zero coordinate equal to 1. Normally we will **not** do this.

The map that takes a vector in  $\mathbb{F}^n$  to its  $i$ -th coordinate is called a *coordinate function*. It is an element of the dual space of  $\mathbb{F}^n$ . The sum of a set of coordinate functions is a function on  $\mathbb{F}^n$ . If  $f_1, \dots, f_k$  is a set of coordinate functions then the product  $f_1 \cdots f_k$  is a function on  $\mathbb{F}^n$ . The set of all linear combinations of products of coordinate functions is the algebra of polynomials on  $\mathbb{F}^n$ . Many interesting structures can be defined as the set of common zeros of a collection of polynomials.

Defining functions on projective space is trickier, because each point is represented by a set of vectors. However if  $p$  is a homogeneous polynomial in  $n$  variables with degree  $k$  and  $x \in \mathbb{F}^n$ , then

$$p(ax) = a^k p(x).$$

Thus it makes sense to consider structures defined as the set of common zeros of a set of homogeneous polynomials.

If we are working over the reals, another approach is possible. If  $x$  is a unit vector in  $\mathbb{R}^n$ , then the  $n \times n$  matrix  $xx^T$  represents orthogonal projection onto the 1-dimensional subspace spanned by  $x$ . Thus we obtain a bijection between the points of the projective space and the set of symmetric  $n \times n$  matrices  $X$  with  $\text{rk}(X) = 1$  and  $\text{tr}(X) = 1$ . However it is a little tricky to decide if three such matrices represent collinear points. (A similar trick works for complex projective space; we use matrices  $xx^*$ , which are Hermitian matrices with rank one.)

## Exercises

1. Determine the projective spaces that are not thick.
2. If  $H$ ,  $K$  and  $L$  are subspaces of a projective geometry and  $L \subseteq H$ , show that

$$H \cap (L \vee K) = L \vee (H \cap K)$$

(This is equivalent to requiring that  $H \cap (L \vee K) = (H \cap L) \vee (H \cap K)$ , and is known in lattice theory as the *modular law*.)

3. Let  $\mathcal{A}$  be an affine space of rank  $d$  and order two. Show that each parallel class of lines determines a permutation of the points of  $\mathcal{A}$  with all orbits of length two. Show that this set of permutations, together with the identity, forms an abelian group of order  $2^d$  where each non-identity element has order two. (Such a group is said to be *elementary abelian* of exponent two.)
4. Prove that each elementary abelian group of exponent two determines an affine geometry.
5. Prove that in a projective space of rank  $r$ , any subspace of rank at most  $r - 2$  is the intersection of the subspaces that cover it.



# Chapter 3

## Collineations and Perspectivities

The main result of this chapter is a proof that all projective spaces of rank at least four, and all ‘Desarguesian’ planes, have the form  $\mathbb{P}(n, \mathbb{F})$  for some field  $\mathbb{F}$ .

### 3.1 Collineations of Projective Spaces

A *collineation* of a linear space is a bijection  $\phi$  of its point set such that  $\phi(A)$  is a line if and only if  $A$  is. It is fairly easy to describe the collineations of the projective spaces over fields. Consider  $\mathbb{P}(n, \mathbb{F})$ , the points of which are the 1-dimensional subspaces of  $V = V(n+1, \mathbb{F})$ . Any invertible linear mapping of  $V$  maps 2-dimensional subspaces onto 2-dimensional subspaces, and hence induces a collineation of  $\mathbb{P}(n, \mathbb{F})$ . The set of all such collineations forms a group, called the projective linear group, and denoted by  $PGL(n, \mathbb{F})$ . There is however another class of collineations. Suppose  $\tau$  is an automorphism of  $\mathbb{F}$ , e.g., if  $\mathbb{F} = \mathbb{C}$  and  $\tau$  maps a complex number to its complex conjugate. If  $\alpha \in \mathbb{F}$ ,  $x \in V$  and  $\alpha^\tau \neq \alpha$  then

$$\alpha x^\tau = \alpha^\tau x^\tau \neq \alpha x^\tau.$$

Thus  $\tau$  does not induce a linear mapping of  $V$  onto itself, but it does map subspaces to subspaces, and therefore does induce a collineation. If we apply any sequence of linear mappings and field automorphisms to  $\mathbb{P}(n, \mathbb{F})$

### 3. COLLINEATIONS AND PERSPECTIVITIES

---

then we can always obtain the same effect by applying a single linear mapping followed by a field automorphism (or a field automorphism then a linear mapping). The composition of a linear mapping and a field automorphism is called a *semi-linear* mapping. The set of all collineations obtained by composing linear mappings and field automorphisms is called the group of projective semi-linear transformations of  $\mathbb{P}(n, \mathbb{F})$ , and is denoted by  $PGL(n+1, \mathbb{F})$ . It contains  $PGL(n, \mathbb{F})$  as a normal subgroup of index equal to  $|\text{Aut}(\mathbb{F})|$ . (If  $\mathbb{F}$  is finite of order  $p^m$ , where  $p$  is prime, then  $\text{Aut}(\mathbb{F})$  is a cyclic group of order  $m$  generated by the mapping which sends an element  $x$  of  $\mathbb{F}$  to  $x^p$ .) We can now state the “fundamental theorem of projective geometry”.

**3.1.1 Theorem.** *Every collineation of  $\mathbb{P}(n, \mathbb{F})$  lies in  $PGL(n+1, \mathbb{F})$ .*

*Proof.* Look it up, for example in Tsuzuku  $\square$ .

This theorem can be readily extended to cover collineations between distinct projective spaces over fields. These are all semi-linear too. It is even possible to describe all ‘homomorphisms’, that is, mappings from one projective space which take points to points and lines to lines, but which are not necessarily injective. (This requires the use of valuations of fields.) The most important property of  $PGL(n+1, \mathbb{F})$  is that it is large. One way of making this more precise is as follows.

**3.1.2 Theorem.** *The group  $PGL(n, \mathbb{F})$  acts transitively on the set of all maximal flags of  $\mathbb{P}(n-1, \mathbb{F})$ .*

*Proof.* Exercise.  $\square$

Every invertible linear transformation of  $V = V(n, \mathbb{F})$  determines a collineation of  $\mathbb{P}(n-1, \mathbb{F})$ . The group of all invertible linear transformations of  $V$  is denoted by  $GL(n, \mathbb{F})$ . This group acts on  $\mathbb{P}(n-1, \mathbb{F})$ , but not faithfully—any linear transformation of the form  $cI$ , where  $c \neq 0$ , induces the identity collineation. (You will show as one of the exercises that all the linear transformations which induce the identity collineation are of this form.)

To compute the order of  $PGL(n, \mathbb{F})$  when  $\mathbb{F}$  is finite with order  $q$ , we first compute the order of  $GL(n, \mathbb{F})$ . This is just the number of non-singular  $n \times n$  matrices over  $\mathbb{F}$ . We can construct such matrices one row at a time. The number of possible first rows is  $q^n - 1$  and, in general, the number of

possible  $(k + 1)$ -th rows is the number of vectors not in the span of the first  $k$  rows, that is, it is  $q^n - q^k$ . Hence

$$|GL(n, q)| = \prod_{i=0}^{n-1} (q^n - q^i) = q^{\binom{n}{2}} (q - 1)^n [n]!$$

The number of maximal flags in  $\mathbb{P}(n - 1, \mathbb{F})$  is  $[n]!$ . Thus we deduce, using Theorem 1.2, that the subgroup  $G$  of  $GL(n, \mathbb{F})$  fixing a flag must have order  $q^{\binom{n}{2}} (q - 1)^n$ . This subgroup is isomorphic to the subgroup of all upper triangular matrices.

A  $k$ -arc in a projective geometry of rank  $n$  is a set of  $k$  points, no  $n$  of which lie in a hyperplane. To construct an  $(n + 1)$ -arc in  $\mathbb{P}(n - 1, \mathbb{F})$ , take a basis  $x_1, \dots, x_n$  of  $V(n, \mathbb{F})$ , together with a vector  $y$  of the form  $\sum_i a_i x_i$ , where none of the  $a_i$  are zero. The linear transformation which sends each vector  $x_i$  to  $a_i x_i$  maps  $\sum x_i$  to  $\sum a_i x_i$ . Hence the subgroup of  $PGL(n, \mathbb{F})$  fixing each of  $x_1, \dots, x_n$  acts transitively on the set of points of the form  $\sum a_i x_i$ , where the  $a_i$  are non-zero. It is also possible to show that a collineation of  $\mathbb{P}(n - 1, \mathbb{F})$  which fixes each point in an  $(n + 1)$ -arc is the identity. (The proof of this is left as an exercise.) Together these statements imply that the subgroup of  $GL(n, \mathbb{F})$  fixing each of  $x_1, \dots, x_n$  acts regularly on the set of points of the form  $\sum a_i x_i$ , where the  $a_i$  are non-zero, and hence that it has order  $(q - 1)^n$ . The subgroup of  $PGL(n + 1, \mathbb{F})$  fixing each point in an  $(n + 1)$ -arc can be shown to be isomorphic to the automorphism group of the field  $\mathbb{F}$ . (See Hughes and Piper [1].)

## 3.2 Perspectivities and Projections

A *perspectivity* of a projective geometry is a collineation which fixes each point in some fixed hyperplane (its *axis*), and each hyperplane through some point (its *centre*). The latter condition is equivalent to requiring that each line through some point be fixed, since every line is the intersection of the hyperplanes which contain it. While it is clear that this is a reasonable definition, it is probably not clear why we would wish to consider collineations suffering these restrictions. However perspectivities arise very naturally. Let  $\mathcal{G}$  be a projective geometry of rank four, and let  $H$  and  $K$  be two hyperplanes in it. Choose points  $p$  and  $q$  not contained in  $H \cup K$ . If  $h \in H$ , define  $\phi_p(h)$  by

$$\phi_p(h) := (p \vee h) \cap K.$$

### 3. COLLINEATIONS AND PERSPECTIVITIES

---

This works because  $H$  is a hyperplane, and so every line in  $\mathcal{G}$  meets  $H$ . Similarly if  $k \in K$  then we define  $\psi_q(k)$  by

$$\psi_q(k) = (q \vee k) \cap H.$$

It is a routine exercise to show that  $\phi_p$  is a collineation from  $H$  to  $K$  and  $\psi_q$  is a collineation from  $K$  to  $H$ . Hence their composition  $\phi_p\psi_q$  is a collineation of  $H$ . (We made use of  $\phi_p$  earlier in proving Theorem 4.3, that is, that all maximal subspaces of a projective geometry have the same rank.)

If  $\mathcal{G}$  has rank  $n$  then the hyperplanes  $H$  and  $K$  meet in a subspace of rank  $n-2$  and each point in this subspace is fixed by  $\phi_p\psi_q$ . All lines through the point  $(p \vee q) \cap H$  are also left fixed by  $\phi_p\psi_q$ . As  $H \cap K$  is a hyperplane in  $H$ , it follows that  $\phi_p\psi_q$  is a perspectivity. We will make considerable use of these perspectivities in proving that all projective geometries of rank at least four arise as the 1- and 2-dimensional subspaces of a vector space.

We provide a class of linear mappings of a vector space which induce perspectivities of the associated projective space  $\mathbb{P}(n, \mathbb{F})$ . Let  $V = V(n, \mathbb{F})$  and let  $H$  be a hyperplane in  $V$ . A linear mapping  $\tau$  of  $V$  is a *transvection* with axis  $H$  if  $x\tau = x$  for all  $x$  in  $H$ , and  $x\tau - x \in H$  for all  $x$  not in  $H$ . They are easy to construct. First, choose a bilinear form  $\langle \cdot, \cdot \rangle$  on  $V$ . Next choose non-zero vectors  $h$  and  $a$  such that  $\langle h, a \rangle = 0$  and define  $\tau_{h,a}$  by setting

$$x\tau_{h,a} = x - \langle x, h \rangle a.$$

Then  $x$  is fixed by  $\tau_{h,a}$  if and only if  $\langle h, x \rangle = 0$ . Thus  $\tau_{h,a}$  fixes all points of the hyperplane with equation  $\langle h, x \rangle = 0$ . If  $x$  is not fixed by  $\tau_{h,a}$  then  $x\tau_{h,a} - x$  is a multiple of  $a$  and, since  $\langle h, a \rangle = 0$ , it follows that  $a$  lies in the hyperplane of points fixed by  $\tau_{h,a}$ . As  $\tau_{h,a}$  fixes  $a$ , it follows that it also fixes all the 2-dimensional subspaces  $a \vee x$ .

## 3.3 Groups of Perspectivities

**3.3.1 Lemma.** *Let  $H$  be hyperplane in the projective geometry  $\mathcal{G}$ . If the collineation  $\tau$  fixes all the points in  $H$  then it fixes all lines through some point of  $\mathcal{G}$ , and is therefore a perspectivity.*

*Proof.* Assume first that  $\tau$  fixes some point  $c$  not in  $H$  and let  $l$  be a line through  $c$ . Then  $l$  must meet  $H$  in some point,  $x$  say. As  $x \in H$ , it is fixed

by  $\tau$  and thus  $\tau$  fixes two distinct points of  $l$ . This implies that  $l$  is fixed by  $\tau$ .

Assume now that there are no points off  $H$  fixed by  $\tau$ . Let  $p$  be a point not in  $H$  and let  $l = p \vee p\tau$ . Once again  $l$  must intersect  $H$  in some point,  $x$  say. As  $\tau$  fixes  $x$  and maps  $p$  in  $l$  to  $p\tau$  in  $l$ , it follows that it fixes  $l$ .

Let  $q$  be a point not on  $H$  or  $l$ . The plane  $\pi = q \vee l$  meets  $H$  in a line  $l'$  (why?). Since  $\tau$  fixes the distinct lines  $l$  and  $l'$  from  $\pi$ , it also fixes  $\pi$ . This implies that  $q\tau \in \pi$ . Now  $q\tau \neq q$ , since  $q \notin H$ , and so the  $q \vee q\tau$  is a line in  $\pi$ . Hence it intersects  $l'$  and, since  $l' \subseteq H$ , the point of intersection is fixed by  $\tau$ . Therefore  $q \vee q\tau$  is fixed by  $\tau$ . The line  $q \vee q\tau$  must intersect  $l$  in some point,  $c$  say. As  $q \vee q\tau$  and  $l$  are both fixed by  $\tau$ , so is  $c$ . Therefore  $c \in H$  and so  $c = H \cap l = x$ . Thus we have shown that the lines  $q \vee q\tau$ , where  $q \notin H$ , all pass through the point  $c$  in  $H$ . From this it follows that all lines through  $c$  are fixed by  $\tau$ .  $\square$

**3.3.2 Corollary.** *The set of perspectivities with axis  $H$  form a group.*

*Proof.* If  $\tau$  is the product of two perspectivities with axis  $H$ , then it must fix all points in  $H$ . By the lemma, it is a perspectivity.  $\square$

Lemma 2.1 shows that perspectivities are the collineations which fix as many points as possible, and thus makes them more natural objects to study. By duality it implies that any collineation which fixes all hyperplanes on some point must fix all the points in some hyperplane. Note however that we cannot derive the lemma itself by appealing to duality, that is, by asserting that if  $\tau$  fixes all points on some hyperplane then, by duality, it fixes all hyperplanes on some point. A perspectivity with its centre on its axis is called an *elation*. If its centre is not on its axis it is a *homology*. (Classical geometry is full of strange terms.) From our remarks above, any transvection induces an elation. It can be shown that the perspectivities of  $\mathbb{P}(n-1, \mathbb{F})$  all belong to  $PGL(n, \mathbb{F})$ , and not just to  $P\Gamma L(n, \mathbb{F})$ . (In fact  $PGL(n, \mathbb{F})$  is generated by perspectivities in it.)

**3.3.3 Corollary.** *Let  $\tau$  be a collineation fixing all points in the hyperplane  $H$ . If  $\tau$  fixes no points off  $H$  it is an elation, if it fixes one point off  $H$  it is a homology and if it fixes two points off  $H$  it is the identity.*

*Proof.* Only the last claim needs proof. Suppose  $a$  and  $b$  are distinct points off  $H$  fixed by  $\tau$ . If  $p$  is a third point, not in  $H$ , then  $\tau$  fixes the point

### 3. COLLINEATIONS AND PERSPECTIVITIES

---

$H \cap pa$  as well as  $a$ . hence  $\tau$  fixes  $pa$  and similarly it fixes  $pb$ . Therefore  $p = pa \cap pb$  is fixed by  $\tau$ . This shows that  $\tau$  fixes all points not in  $H$ .  $\square$

**3.3.4 Lemma.** *Let  $\tau_1$  and  $\tau_2$  be perspectivities of the projective geometry  $\mathcal{G}$  with common axis  $H$ . Then  $\tau_1\tau_2$  is a perspectivity with axis  $H$  and centre on the line joining the centres of  $\tau_1$  and  $\tau_2$ .*

*Proof.* The challenge is to show that the centre of  $\tau_1\tau_2$  is on the line joining the centers of  $\tau_1$  and  $\tau_2$ .

Denote the respective centres of  $\tau_1$  and  $\tau_2$  by  $c_1$  and  $c_2$ . If  $c_1 = c_2$ , then  $c_1$  is the center of  $\tau_1\tau_2$  and we are done. So we may assume throughout that  $c_1 \neq c_2$  and that neither  $\tau_1$  nor  $\tau_2$  is the identity.

We note that any line that is fixed by a perspectivity and which is not contained in its axis must contain the center of the perspectivity.

Suppose first the  $\tau_1$  is a homology, i.e.,  $c_1 \notin H$ . Then  $c_1\tau_2 \neq_1$  and the line  $m = c_1 \vee c_1\tau_2$  is fixed by  $\tau_2$  (because its intersection with  $H$  is fixed by  $\tau_2$ ). It follows that  $m$  contains the centre of  $\tau_2$ . Since  $m$  contains the center of  $\tau_1$ , it is also fixed by  $\tau_1$ . We conclude that  $\tau_1\tau_2$  fixes  $m$  and therefore the center of  $\tau_1\tau_2$  is on  $m$ . As  $m = c_1 \vee c_2$ , we are done.

So we may assume that  $\tau_1$  and  $\tau_2$  are elations. If  $p$  is a point off  $H$  fixed by  $\tau_1\tau_2$ , then

$$p\tau_1 = p\tau_2^{-1}$$

and therefore the line  $p \vee p\tau_1 = p \vee p\tau_2^{-1}$  is fixed by  $\tau_1$  and  $\tau_2$ . Hence this line must contain the centers of both elations and therefore  $c_1 = c_2$ . We conclude that  $\tau_1\tau_2$  does not fix any point of  $H$  and therefore it is an elation.

If our projective space has rank three, then  $H = c_1 \vee c_2$  and so the center of  $\tau_1\tau_2$  is on  $c_1 \vee c_2$  as required. Suppose the rank is greater than three and let  $q$  be a point off  $H$ . Since  $\tau_1$  fixes  $q \vee c_1$ , it fixes the plane  $\pi = q \vee (c_1 \vee c_2)$ . Since  $\tau_2$  fixes  $q \vee c_2$  it also fixes  $\pi$ . Hence  $\tau_1\tau_2$  fixes  $\pi$ ; as it induces a perspectivity of  $\pi$  and the center  $p$  of this must be on  $\pi \cap H$ ., it must fix all lines in  $\pi$  through some point on  $c_1 \vee c_2$ . We conclude that  $p$  is the center of  $\tau_1\tau_2$ .  $\square$

One consequence of the previous lemma is that the product of two elations with axis  $H$  is always a perspectivity with axis  $H$  and centre on  $H$ , that is, it is an elation. It is possible for the product of two homologies with axis  $H$  to be an elation—with its centre the point of intersection of  $H$  with the line through the centres of the homologies.

### 3.4 Transitivity Conditions

We now come to an important definition. Let  $p$  be a point and  $H$  a hyperplane in the projective geometry  $\mathcal{G}$  and let  $\Gamma$  be a group of collineations of  $\mathcal{G}$ . Let  $\Gamma(p, H)$  denote the subgroup of  $\Gamma$  formed by the perspectivities with centre  $p$  and axis  $H$ . We say that  $\Gamma$  is  $(p, H)$ -transitive if, for any line  $\ell$  through  $p$  which is not contained in  $H$ , the subgroup  $\Gamma(p, H)$  acts transitively on the set of points of  $\ell$  which are not on  $H$  and not equal to  $p$ . If  $\text{Aut}(\mathcal{G})$  is itself  $(p, H)$ -transitive then we say that  $\mathcal{G}$  is  $(p, H)$ -transitive.

This is a reasonable point to explain some group theoretic terms as well. If  $\Gamma$  is a permutation group acting on a set  $S$  and  $x \in S$  then  $\Gamma_x$  is the subgroup of  $\Gamma$  formed by the permutations which fix  $x$ . Recall that the length of the orbit of  $x$  under the action of  $\Gamma$  is equal to the index of  $\Gamma_x$  in  $\Gamma$ . The group  $\Gamma$  is transitive if it has just one orbit on  $S$ . It acts *fixed-point freely* on  $S$  if the only element which fixes a point of  $S$  is the identity, that is, if  $\Gamma_x$  is the trivial subgroup for each element  $x$  in  $S$ . In this case each orbit of  $\Gamma$  on  $S$  will have length equal to  $|\Gamma|$  (and so  $|\Gamma|$  divides  $|S|$  when everything is finite).

Suppose that  $\Gamma$  is the group of all perspectivities of  $\mathcal{G}$  with centre  $p$  and axis  $H$ . Let  $q$  be a point not in  $H$  and distinct from  $p$ . If an element  $\gamma$  of  $\Gamma$  fixes  $q$  then it is the identity. For since  $q \notin H$  and since  $\gamma$  fixes each point in  $H$  it fixes all lines joining  $q$  to a point in  $H$ . But as  $H$  is a hyperplane, this means that it fixes all lines through  $q$ . Hence  $q$  must be the centre of  $\gamma$ , and so  $q = p$ . This contradiction shows that  $\Gamma$  must act fixed-point freely on the points of  $\mathcal{G}$  not in  $H \cup p$ . In particular, for any line  $l$ , we see that  $\Gamma$  acts fixed-point freely on the points of  $l \setminus p$  not in  $H$ . (Since  $p \in l$ , the line  $l$  must be fixed as a set by  $\Gamma$ .) Therefore if  $\mathcal{G}$  is finite and  $p \notin H$  then  $|\Gamma|$  must divide  $|l| - 2$ , and if  $p \in H$  then  $|\Gamma|$  divides  $|l| - 1$ .

### 3.5 Desarguesian Projective Planes

Let  $\mathcal{P}$  be a projective plane, with  $p$  a point and  $\ell$  a line in it. The condition that  $\mathcal{P}$  be  $(p, \ell)$ -transitive can be expressed in a geometric form. A *triangle* in a projective plane is a set of three non-collinear points  $\{a_1, a_2, a_3\}$ , together with the lines  $a_1 \vee a_2$ ,  $a_2 \vee a_3$  and  $a_3 \vee a_1$ . These lines are also known as the *sides* of the triangle. For convenience we will now begin to abbreviate expressions such as  $a_1 \vee a_2$  to  $a_1 a_2$ . Two triangles  $\{a_1, a_2, a_3\}$  and  $\{b_1, b_2, b_3\}$

### 3. COLLINEATIONS AND PERSPECTIVITIES

---

are said to be *in perspective from a point*  $p$  if the three lines  $a_1b_1$ ,  $a_2b_2$  and  $a_3b_3$  all pass through  $p$ . They are *in perspective from a line*  $\ell$  if the points  $a_1a_2 \cap b_1b_2$ ,  $a_2a_3 \cap b_2b_3$  and  $a_3a_1 \cap b_3b_1$  all lie on  $\ell$ . We have the following classical result, known as *Desargues' theorem*.

**3.5.1 Theorem.** *Let  $\mathcal{P}$  be the projective plane  $\mathbb{P}(2, \mathbb{F})$ . If two triangles in  $\mathcal{P}$  are in perspective from a point then they are in perspective from a line.*

*Proof.* Wait. □

A projective plane is  $(p, \ell)$ -Desarguesian if:

- whenever two triangles  $\{a_1, a_2, a_3\}$  and  $\{b_1, b_2, b_3\}$  are in perspective from  $p$ , and
- both  $a_1a_2 \cap b_1b_2$  and  $a_2a_3 \cap b_2b_3$  lie on  $\ell$ ,

then  $a_3a_1 \cap b_3b_1$  lies on  $\ell$ . We call a plane *Desarguesian* if it is  $(p, \ell)$ -Desarguesian for all points  $p$  and lines  $\ell$ . Since the projective planes over fields are all Desarguesian, by the previous theorem, this concept is quite natural. However we will see that a plane is Desarguesian if and only if it is of the form  $\mathbb{P}(2, \mathbb{F})$  for some skew-field  $\mathbb{F}$ .

**3.5.2 Theorem.** *A projective plane is  $(p, \ell)$ -transitive if and only if it is  $(p, \ell)$ -Desarguesian.*

*Proof.* Suppose  $\mathcal{P}$  is a  $(p, \ell)$ -transitive plane. Let  $\{a_1, a_2, a_3\}$  and  $\{b_1, b_2, b_3\}$  be two triangles in perspective from  $p$  with both  $a_1a_2 \cap b_1b_2$  and  $a_2a_3 \cap b_2b_3$  lying on  $\ell$ . By hypothesis, there is a perspectivity  $\tau$  with centre  $p$  and axis  $\ell$  which maps  $a_1$  to  $b_1$ . Let  $x$  be the point  $a_1a_2 \cap \ell$ . Since  $x\tau = x$ , the perspectivity  $\tau$  maps  $xa_1$  onto  $xb_1$ . Now  $xa_1 = a_1a_2$  and  $xb_1 = b_1b_2$ ; thus  $\tau$  maps  $a_1a_2$  onto  $b_1b_2$ . Since the line  $pa_2$  is fixed by  $\tau$ , we deduce that  $a_2 = pa_2 \cap a_1a_2$  is mapped onto  $pa_2 \cap b_1b_2 = b_2$ . A similar argument reveals that  $a_3\tau = b_3$ . Thus  $(a_2a_3)\tau = b_2b_3$  and therefore  $(a_2a_3 \cap \ell)\tau = b_2b_3 \cap \ell$ . As  $\tau$  fixes each point of  $\ell$ , this implies that  $a_2a_3 \cap \ell = b_2b_3 \cap \ell$  and hence that  $a_2a_3$  and  $b_2b_3$  meet at a point on  $\ell$ . Thus our two triangles are  $(p, \ell)$ -perspective.

We turn now to the slightly more difficult task of showing that if  $\mathcal{P}$  is  $(p, \ell)$ -Desarguesian then it is  $(p, \ell)$ -transitive. Let  $x$  be a point distinct from  $p$  and not on  $\ell$  and let  $y$  be a point of  $px$  distinct from  $p$  and not on  $\ell$ . We

need to construct a perspectivity with centre  $p$  and axis  $\ell$  which sends  $x$  to  $y$ . If  $a$  is a point not on  $px$  or  $\ell$ , define

$$a\tau := ((ax \cap \ell) \vee y) \cap pa$$

and if  $a \in \ell$ , set  $a\tau$  equal to  $a$ . As thus defined,  $\tau$  is a permutation of the point set of the affine plane obtained by deleting  $px$  from  $\mathcal{P}$ .

We will prove that it is a collineation of this affine plane, and hence determines a collineation of  $\mathcal{P}$  fixing  $px$ . Since  $a\tau \in pa$ , the mapping  $\tau$  fixes the lines through  $p$ . Hence, if  $\tau$  is a collineation then it is a perspectivity with centre and axis in the right place. Suppose that  $a$  and  $b$  are two distinct points of  $\mathcal{P}$  not on  $px$ . If  $b \in xa$  then  $ax = ab$  and  $((ax \cap \ell) \vee y) = ((ab \cap \ell) \vee y)$ , implying that  $b\tau$  is collinear with  $y = x\tau$  and  $a\tau$ . Conversely, if  $b\tau$  is collinear with  $y$  and  $a\tau$  then  $b$  must be collinear with  $x$  and  $a$ .

Thus we may assume that  $x$ ,  $a$  and  $b$  are not collinear. Then  $\{x, a, b\}$  and  $\{y, a\tau, b\tau\}$  are two triangles in perspective from the point  $p$ . By construction  $xa$  meets  $y \vee a\tau$  and  $xb$  meets  $y \vee b\tau$  on  $\ell$ . Therefore  $a \vee b$  must meet  $a\tau \vee b\tau$  on  $\ell$ . Let  $u$  be a point on  $ab$ . Then, applying Desargues' theorem a second time, we deduce that  $au$  and  $a\tau \vee u\tau$  meet on  $\ell$ . Since  $au = ab$ , they must actually meet at  $ab \cap \ell$ . Therefore

$$a\tau \vee u\tau = a\tau \vee (\ell \cap ab) = a\tau \vee (\ell \cap (a\tau \vee b\tau)) = a\tau \vee b\tau$$

and so  $u\tau$  is on  $a\tau \vee b\tau$ , as required.  $\square$

**3.5.3 Lemma.** *Let  $\mathcal{G}$  be a projective geometry of rank at least four. Then all subspaces of rank three are Desarguesian projective planes.*

*Proof.* Let  $\pi$  be a plane in  $\mathcal{G}$  and let  $p$  a point and  $\ell$  a line in  $\pi$ . Let  $a$  and  $b$  be distinct points on a line in  $\pi$  through  $p$ , neither equal to  $p$  or on  $\ell$ . Let  $\sigma$  be a second plane meeting  $\pi$  in  $\ell$  and let  $v$  be a point not in  $\pi \vee \sigma$  but not in  $\pi$  or  $\sigma$ . If  $x \in \pi$  then  $v \vee x$  must meet  $\sigma$  in a point. The mapping sending  $x$  to  $(v \vee x) \cap \sigma$  is collineation  $\phi_v$  from  $\pi$  to  $\sigma$ . The line  $ba'$  is contained in the plane  $p \vee a \vee v$ , as is  $pv$ . Hence  $ba'$  meets  $pv$  in a point,  $w$  say. Note that  $w$  cannot lie in  $\pi$  or  $\sigma$ . Hence it determines a collineation  $\phi_w$  from  $\sigma$  to  $\pi$  which maps  $a'$  to  $b$ . Both  $\phi_v$  and  $\phi_w$  fix each point in  $\ell$ , and so their composition is a collineation of  $\pi$  which fixes each point of  $\ell$  and maps  $a$  to  $b$ . This shows that  $\pi$  is a  $(p, \ell)$ -transitive plane. As our choice of  $p$  and  $\ell$  was arbitrary, it follows from the previous two results that all planes in  $\mathcal{G}$  are Desarguesian.

**3.5.4 Theorem.** *A projective geometry with rank at least four is  $(p, H)$ -transitive for all points  $p$  and hyperplanes  $H$ .*

*Proof.* Let  $x$  and  $y$  be distinct points on a line through  $p$ , neither in  $H$ . If  $a$  is a point in  $\mathcal{G}$  not on  $px$  define

$$a\tau = (((ax \cap H) \vee y) \cap pa).$$

(This is the same mapping we used in proving that a  $(p, \ell)$ -transitive plane is  $(p, \ell)$ -Desarguesian.) Let  $\pi$  be a plane through  $pa$  meeting  $H$  in a line. If  $a \in \pi$  then  $a\tau \in \pi$  and, from the proof of Theorem 4.2, it follows that  $\tau$  induces a perspectivity on  $\pi$  with centre  $p$  and axis  $\pi \cap H$ . Thus if  $a$  and  $b$  are points not both on  $H$  and  $ab$  is coplanar with  $px$ , the image of  $ab$  under  $\tau$  is a line. (The proof of Theorem 4.2 can also be used to show that  $\tau$  can be extended to the points on  $px$ ; we leave the details of this to the reader.) Suppose then that  $a$  and  $b$  are points not both on  $H$  and  $ab$  is not coplanar with  $px$ . The plane  $x \vee ab$  meets  $H$  in a line  $\ell$ , hence if  $c \in ab$  then  $c\tau$  lies in the intersection of the planes  $p \vee ab$  and  $y \vee \ell$ . As  $y \in px$ , we have

$$y \vee \ell \subseteq px \vee \ell = px \vee ab.$$

Therefore  $y \vee \ell$  is a hyperplane in  $px \vee ab$  and so it meets  $p \vee ab$  in a line. By construction, this line contains the image of  $ab$  under  $\tau$ , and so we have shown that  $\tau$  is a collineation.  $\square$

There are projective planes which are not Desarguesian, and so the restriction on the rank in the previous theorem cannot be removed. We will call an affine plane  $\mathcal{P}^l$  Desarguesian if  $\mathcal{P}$  is.

## 3.6 Translation Groups

Let  $H$  be a hyperplane in the projective geometry  $\mathcal{G}$ . (We assume that  $\mathcal{G}$  has rank at least three.) The ordered pair  $(\mathcal{G}, H)$  is an affine geometry and an elation of  $\mathcal{G}$  with axis  $H$  and centre on  $H$  is called a *translation*. From Lemma 3.1, it follows that the set of all translations form a group. We are going to investigate the relation between the structure of  $\mathcal{A}$  and this group. Some group theory must be introduced. A group  $\Gamma$  is *elementary abelian* if it is abelian and its non-identity elements all have the same order. If  $\Gamma$  is elementary abelian then so is any subgroup. As any element generates

a cyclic group, and as the only elementary abelian cyclic groups are the groups of prime order, all non-zero elements of a finite elementary abelian group must have order  $p$ , for some prime  $p$ . The group itself thus has order  $p^n$  for some  $n$ . We will usually use multiplication to represent the group operation, and consequently refer to the ‘identity element’ rather than the ‘zero element’. (There will be one important exception, when we consider endomorphisms.) If  $H$  and  $K$  are subsets of the group  $G$  then we define

$$HK = \{hk : h \in H, k \in K\}.$$

If  $H$  and  $K$  are subgroups and at least one of the two is normal then  $HK$  is a subgroup of  $G$ . If  $S \subseteq G$  then  $\langle S \rangle$  is the subgroup generated by  $S$  and  $\langle 1 \rangle$  is the trivial, or identity subgroup. Let  $\mathcal{G}$  be a projective geometry and let  $H$  be a hyperplane in it. Let  $\mathcal{A}$  be the affine geometry with  $H$  as the hyperplane at infinity. If  $F$  is a subspace of  $H$  then  $T(F)$  is the group of all elations with axis  $H$  and centre in  $F$ . If we need to identify  $H$  explicitly we will write  $T_H(F)$ .

**3.6.1 Lemma.** *Let  $H$  be a hyperplane in the projective geometry  $\mathcal{G}$ . If  $p$  and  $q$  are distinct points on  $H$  such that  $T(p)$  and  $T(q)$  are both non-trivial then  $T(H)$  is elementary abelian.*

*Proof.* Since a non-identity elation has a unique centre,  $T(p) \cap T(q) = \langle 1 \rangle$ . Suppose that  $\alpha$  and  $\beta$  are non-identity elements of  $T(p)$  and  $T(q)$  respectively. If  $l$  is a line through  $p$  then so is  $l\beta^{-1}$ . Hence the latter is fixed by  $\alpha$  and

$$l\beta^{-1}\alpha\beta = l\beta^{-1}\beta = l.$$

This shows that  $\beta^{-1}\alpha\beta \in T(p)$ . In other words,  $T(p)$  is normalized by the elements of  $T(q)$ . If  $\beta^{-1}\alpha\beta \in T(p)$  then the commutator  $\alpha^{-1}\beta^{-1}\alpha\beta$  must also lie in  $T(p)$ . A similar argument shows that  $\alpha^{-1}\beta^{-1}\alpha \in T(q)$ . Accordingly  $\alpha^{-1}\beta^{-1}\alpha\beta$  also lies in  $T(q)$ . As  $T(p) \cap T(q) = \langle 1 \rangle$ , it follows that  $\alpha^{-1}\beta^{-1}\alpha = 1$ . Consequently  $\alpha\beta = \beta\alpha$ . (In other words, two non-identity elations with the same axis and distinct centres commute.)

We now show that  $T(p)$  is abelian. Let  $\alpha'$  be a second non-identity element of  $T(p)$ . Then  $\alpha'\beta$  is an elation. If its centre is  $p$  then  $\beta$  must belong to  $T(p)$ . Thus its centre is not  $p$ . Arguing as before, but with  $\alpha'\beta$  in place of  $\beta$ , we deduce that  $\alpha$  and  $\alpha'\beta$  commute. This implies in turn that  $\alpha$  and  $\alpha'$  commute. Finally, assume that  $\alpha$  is an element of  $T(p)$  with order

### 3. COLLINEATIONS AND PERSPECTIVITIES

---

*m.* If  $\beta^m \neq 1$  then

$$(\alpha\beta)^m = \alpha^m \beta^m = \beta^m \in T(q). \quad (3.6.1)$$

Since  $\alpha\beta$  is an elation with axis  $H$ , so is  $(\alpha\beta)^m$ , and (3.6.1) shows that its centre is  $q$ . Therefore the centre of  $\alpha\beta$  is  $q$  and so  $\alpha\beta \in T(q)$ . Since  $\beta \in T(q)$ , we infer that  $\alpha$  also lies in  $T(q)$ . This is impossible, and forces us to conclude that  $\beta^p = 1$ . Thus we have proved that two non-identity elations with distinct centres must have the same order. It is now trivial to show that  $T(H)$  is elementary abelian.  $\square$

The group  $T(p)$  may contain no elements of finite order, but in this case it is still elementary abelian.

**3.6.2 Lemma.** *Let  $H$  be a hyperplane in the projective geometry  $\mathcal{G}$ . If  $\mathcal{G}$  is  $(p, H)$ -transitive and  $(q, H)$ -transitive for  $p$  and  $q$  on  $H$ , then it is  $(r, H)$ -transitive for all points  $r$  on  $p \vee q$ .*

*Proof.* If  $p = q$  there is nothing to prove, so assume they are not equal. Let  $r$  be a point on  $pq$  and let  $a$  and  $b$  be distinct points not on  $H$  and collinear with  $r$ . We construct an elation mapping  $a$  to  $b$ . The lines  $ab$  and  $pq$  are coplanar; let  $x$  be the point  $pa \cap ab$ . Since  $\mathcal{G}$  is  $(p, H)$ -transitive, there is an element  $\alpha$  of  $T(p)$  which maps  $a$  to  $x$ . Similarly there is an element  $\beta$  of  $T(q)$  mapping  $x$  to  $b$ . Hence the product  $\alpha\beta$  maps  $a$  to  $b$ . It fixes  $r$ , and therefore it fixes the line  $ra = ab$ . Thus it is an elation with centre  $r$ .  $\square$

Any element of  $T(p)T(q)$  is an elation with centre on  $p \vee q$ . Thus the proof of the lemma implies the following.

**3.6.3 Corollary.** *If  $\mathcal{G}$  is  $(p, H)$ - and  $(q, H)$ -transitive then  $T(p \vee q) = T(p)T(q)$ .  $\square$*

## 3.7 A Field and a Vector Space

Let  $H$  be a hyperplane in a projective geometry  $\mathcal{P}$ . Assuming that  $\mathcal{P}$  is  $(p, H)$ -transitive for all points  $p$  in  $H$ , we show that  $T(H)$  can be viewed as a vector space over a skew field whose elements correspond to the  $(o, H)$ -homologies for a point  $o$  off  $H$ .

**3.7.1 Lemma.** *Let  $H$  be a hyperplane in the projective geometry  $\mathcal{P}$ . Then any  $(o, H)$ -homology of  $\mathcal{P}$  determines an automorphism of  $T$  which fixes each subgroup  $T(p)$ .*

*Proof.* Let  $\alpha$  be an  $(o, H)$ -homology of  $\mathcal{G}$ . If  $\tau \in T$ , then we regard it as an elation of  $\mathcal{G}$  and thus we can define  $\tau^\alpha = \alpha^{-1}\tau\alpha$ . Then  $\tau^\alpha$  fixes each point off  $H$  and the line joining  $o$  to the centre of  $\tau$ . Hence, if  $\tau \in T_i$ , so is  $\tau^\alpha$ . As  $\alpha$  is an element and  $T$  a subgroup of the collineation group of  $\mathcal{A}$ , the mapping  $\tau \mapsto \tau^\alpha$  is an automorphism of  $T$ .  $\square$

**3.7.2 Lemma.** *Let  $H$  be a hyperplane in the projective geometry  $\mathcal{P}$  and let  $p$  and  $q$  be distinct points on  $H$ . If  $r \in H$  and  $T(r) \cap T(p)T(q) \neq \emptyset$ , then  $T(r) \subseteq T(p)T(q)$  and if  $r \neq p$  then  $T(p)T(r) = T(p)T(q)$ .*

*Proof.* Note the elements of  $T(p)T(q)$  are elations with axis  $H$  and center on  $pq$ . Hence any element of  $T(r) \cap T(p)T(q)$  must be an elation with center on  $pq$ , and therefore  $r \in pq$ . If  $r = q$  then certainly  $T(p)T(r) = T(p)T(q)$ . If  $r \neq p, q$  and  $r \in pq$  then  $pr = pq$  and  $T(p)T(r) = T(p)T(q)$ .  $\square$

For the remainder of this section, we will represent the group operation in abelian groups by addition, rather than multiplication. This also means that the identity now becomes the zero element. If  $\alpha$  and  $\beta$  are automorphisms of the abelian group  $T$  then we can define their sum  $\alpha + \beta$  by setting  $\tau^{\alpha+\beta}$  equal to  $\tau^\alpha + \tau^\beta$ , for all elements  $\tau$  of  $T$ . This will not be an automorphism in general, but it is always an endomorphism of  $T$ . The endomorphisms of an abelian group form a ring with identity.

**3.7.3 Lemma.** *Let  $H$  be a hyperplane in the projective geometry  $\mathcal{P}$ . Then the set of all endomorphisms of  $T(H)$  which map each subgroup  $T(p)$  into itself forms a skew field.*

*Proof.* Let  $K$  be the set of endomorphisms referred to. We show first that the elements of  $K$  are injective. Suppose that  $\alpha \in K$  and  $x\alpha = 0$  for some element  $x$  of  $T(H)$ . For convenience we assume that the points on  $H$  have been indexed and that  $T_i$  denotes  $T(p_i)$ . Assume that  $x$  is a non-zero element of  $T_1$  and let  $y$  be a non-zero element of  $T_i$  for some  $i$ . Then

$$(x + y)\alpha = x\alpha + y\alpha = y\alpha$$

and therefore  $(x + y)\alpha$  must lie in  $T_i$ , since  $y\alpha$  does. On the other hand,  $x + y$  cannot lie in  $T_i$ , and therefore  $(x + y)\alpha = 0$ . This shows that  $y\alpha = 0$ .

As our choice of  $y$  in  $T_i$  was arbitrary, it follows that each element of  $T_i$  is mapped to zero and, as our choice of  $i$  was arbitrary, that  $(T \setminus T_i)\alpha = 0$ . Since  $y\alpha = 0$ , we may also reverse the role of  $x$  and  $y$  in the first step of our argument and hence deduce that  $T_1\alpha = 0$ . Thus we have proved that if  $\alpha$  is not injective then it is the zero endomorphism.

We now show that the non-zero elements of  $K$  are surjective. Suppose that  $v \in T_i + T_j$  and  $\alpha \in K$ . We prove that  $v$  is in the range of  $\alpha$ . We may assume that  $v \in T_i$ . Choose a non-zero element  $u$  of  $T_j$ . Then  $u\alpha \neq 0$  and we may also assume that  $u\alpha - v \neq 0$ . Then  $u\alpha - v$  must lie in some subgroup  $T_k$  and  $T_k$  must be contained in  $T_i + T_j$ . Since  $T_k + T_j = T_i + T_j$ , we see that  $T_k$  is a complete set of coset representatives for  $T_j$  in  $T_i + T_j$  and so  $T_k + u$  must contain a non-zero element  $w$  of  $T_i$ . Now  $w - u \in T_k$  and therefore  $(w - u)\alpha \in T_k$ . As  $u\alpha - v \in T_k$  we see that  $w\alpha - v \in T_k$ . On the other hand,  $v$  and  $w$  belong to  $T_i$  and so  $w\alpha - v \in T_i$ . Hence  $w\alpha - v \in T_i \cap T_k = 0$ . Consequently  $v$  lies in the range of  $\alpha$ . We have now proved that any non-zero element of  $K$  is bijective. It follows that all non-zero elements of  $K$  are invertible, and hence that it is a skew field.  $\square$

A famous result due to Wedderburn asserts that all finite skew fields are fields. It is useful to keep this in mind. It is a fairly trivial exercise to show that any endomorphism of a geometric partition induces a homology of the corresponding projective geometry.

### 3.8 Geometric Partitions

Assume now that  $\mathcal{G}$  is a projective geometry which is  $(p, H)$ -transitive for all points  $p$  on the hyperplane  $H$ , e.g., any projective geometry with rank at least four, or any Desarguesian plane. Then  $T(H)$  is an elementary abelian group and the subgroups  $T(p)$ , where  $p \in H$ , partition its non-identity elements. In fact  $T(H)$ , together with the subgroups  $T(p)$ , completely determines  $\mathcal{G}$ . The connection is quite simple: the elements of  $T = T(H)$  correspond to the points of  $\mathcal{G} \setminus H$  and the cosets of the subgroups  $T(p)$  are the lines. The correspondence between points and elements of  $T$  arise as follows. Let  $o$  be a point not in  $H$ . We associate with the identity of  $T$ . If  $a$  is a second point not on  $H$  then there is a unique elation  $\tau_a$  with axis  $H$  and centre  $H \cap oa$  which maps  $o$  to  $a$ . Then the map  $a \mapsto \tau_a$  is a bijection from  $T$  to the points of  $\mathcal{G}^H$ . If  $l$  is a line of  $\mathcal{G}^H$  then the affine points of  $l$  are an orbit of  $T(l \cap H)$ , and conversely, each such orbit is a line. This leads us

naturally to conjecture that an elementary abelian group  $T$ , together with a collection of subgroups  $T_i$  ( $i = 1, \dots, m$ ) such that the sets  $T_i \setminus 1$  partition  $T \setminus 1$ , determines an affine geometry. This conjecture is wrong, but easily fixed. Let  $T$  be an elementary abelian group. A collection of subgroups  $T_i$  ( $i = 1, \dots, m$ ) is a *geometric partition* of  $T$  if

- (a) The sets  $T_i \setminus 1$  partition  $T \setminus 1$ ,
- (b)  $T_i \cap T_j T_k \neq \emptyset$  implies that  $T_i \leq T_j T_k$ .

A set of subgroups for which (a) holds is called a *partition* of  $T$ , although it is not quite. The partitions we have been studying are all geometric. For  $T(p)T(q) = T(p \vee q)$  and so if  $\tau \in T(r) \cap T(p)T(q)$  then  $r$  must lie on  $p \vee q$  and so  $T(r) \leq T(p)T(q)$ . A geometric partition of an elementary abelian group determines an affine geometry  $\mathcal{G}^H$ . We take the affine points to be the elements of  $T$  and the lines to be the cosets of the subgroups  $T_i$ . This gives us a linear space. Showing that this is an affine geometry is left as an exercise.

**3.8.1 Lemma.** *Let  $T_i$  ( $i = 1, \dots, m$ ) be a geometric partition of the elementary abelian group  $T$  and let  $\mathcal{A} = \mathcal{G}^H$  be the affine geometry it determines. If  $o$  is the point of  $\mathcal{A}$  corresponding to the identity of  $T$  then any  $(o, H)$ -homology of  $\mathcal{G}$  determines an automorphism of  $T$  which fixes each subgroup  $T_i$ , and conversely.*

*Proof.* Let  $\alpha$  be an  $(o, H)$ -homology of  $\mathcal{G}$ . If  $\tau \in T$ , then we regard it as an elation of  $\mathcal{G}$  and thus we can define  $\tau^\alpha = \alpha^{-1}\tau\alpha$ . Then  $\tau^\alpha$  fixes each point off  $H$  and the line joining  $o$  to the centre of  $\tau$ . Hence, if  $\tau \in T_i$ , so is  $\tau^\alpha$ . As  $\alpha$  is an element and  $T$  a subgroup of the collineation group of  $\mathcal{A}$ , the mapping  $\tau \mapsto \tau^\alpha$  is an automorphism of  $T$ . The proof of the converse is a routine exercise.  $\square$

For the remainder of this section, we will represent the group operation in abelian groups by addition, rather than multiplication. This also means that the identity now becomes the zero element. If  $\alpha$  and  $\beta$  are automorphisms of the abelian group  $T$  then we can define their sum  $\alpha + \beta$  by setting  $\tau^{\alpha+\beta}$  equal to  $\tau^\alpha + \tau^\beta$ , for all elements  $\tau$  of  $T$ . This will not be an automorphism in general, but it is always an endomorphism of  $T$ . The endomorphisms of an abelian group form a ring with identity. We require one preliminary result.

### 3. COLLINEATIONS AND PERSPECTIVITIES

---

**3.8.2 Lemma.** *Let  $T_i$  ( $i = 1, \dots, m$ ) be a geometric partition of the elementary abelian group  $T$ . If  $T_k \leq T_i + T_j$  and  $k \neq i$  then  $T_i + T_j = T_i + T_k$ .*

*Proof.* This can be proved geometrically, but we offer an alternative approach. We claim that

$$T_i + ((T_i + T_k) \cap T_j) = (T_i + T_k) \cap (T_i + T_j). \quad (3.8.1)$$

To prove this, note first that both terms on the left hand side are contained in the right hand side. Conversely, if  $u$  belongs to the right hand side then we can write it both as  $x + y$  where  $x \in T_i$  and  $y \in T_j$ , and as  $x' + z$  where  $x' \in T_i$  and  $z \in T_k$ . Since  $x + y = x' + z$  we have  $y = -x + x' + z \in (T_i + T_k)$  and so  $y \in (T_i + T_k) \cap T_j$ . If  $T_k \leq T_i + T_j$  then the right hand side of (3.8.1) is equal to  $T_i + T_k$  while, since the partition is geometric, the left hand side equals  $T_i$  or  $T_i + T_j$ . As  $T_k \neq T_i$ , this proves the lemma.  $\square$

**3.8.3 Lemma.** *Let  $T_i$  ( $i = 1, \dots, m$ ) be a geometric partition of the elementary abelian group  $T$ . Then the set of all endomorphisms of  $T$  which map each subgroup  $T_i$  into itself forms a skew field.*

*Proof.* Let  $K$  be the set of endomorphisms referred to. We show first that the elements of  $K$  are injective. Suppose that  $\alpha \in K$  and  $x\alpha = 0$  for some element  $x$  of  $T$ . Assume that  $x$  is a non-zero element of  $T_1$  and let  $y$  be a non-zero element of  $T_i$  for some  $i$ . Then

$$(x + y)\alpha = x\alpha + y\alpha = y\alpha$$

and therefore  $(x + y)\alpha$  must lie in  $T_i$ , since  $y\alpha$  does. On the other hand,  $x + y$  cannot lie in  $T_i$ , and therefore  $(x + y)\alpha = 0$ . This shows that  $y\alpha = 0$ . As our choice of  $y$  in  $T_i$  was arbitrary, it follows that each element of  $T_i$  is mapped to zero and, as our choice of  $i$  was arbitrary, that  $(T \setminus T_i)\alpha = 0$ . Since  $y\alpha = 0$ , we may also reverse the role of  $x$  and  $y$  in the first step of our argument and hence deduce that  $T_1\alpha = 0$ . Thus we have proved that if  $\alpha$  is not injective then it is the zero endomorphism.

We now show that the non-zero elements of  $K$  are surjective. Suppose that  $v \in T_i + T_j$  and  $\alpha \in K$ . We prove that  $v$  is in the range of  $\alpha$ . We may assume that  $v \in T_i$ . Choose a non-zero element  $u$  of  $T_j$ . Then  $u\alpha \neq 0$  and we may also assume that  $u\alpha - v \neq 0$ . Then  $u\alpha - v$  must lie in some subgroup  $T_k$  and  $T_k$  must be contained in  $T_i + T_j$ . Since  $T_k + T_j = T_i + T_j$ ,

we see that  $T_k$  is a complete set of coset representatives for  $T_j$  in  $T_i + T_j$  and so  $T_k + u$  must contain a non-zero element  $w$  of  $T_i$ . Now  $w - u \in T_k$  and therefore  $(w - u)\alpha \in T_k$ . As  $u\alpha - v \in T_k$  we see that  $w\alpha - v \in T_k$ . On the other hand,  $v$  and  $w$  belong to  $T_i$  and so  $w\alpha - v \in T_i$ . Hence  $w\alpha - v \in T_i \cap T_k = 0$ . Consequently  $v$  lies in the range of  $\alpha$ . We have now proved that any non-zero element of  $K$  is bijective. It follows that all non-zero elements of  $K$  are invertible, and hence that it is a skew field.  $\square$

A famous result due to Wedderburn asserts that all finite skew fields are fields. It is useful to keep this in mind. It is a fairly trivial exercise to show that any endomorphism of a geometric partition induces a homology of the corresponding projective geometry.

## 3.9 The Climax

The following result will enable us to characterise all projective geometries of rank at least four, and all Desarguesian projective planes.

**3.9.1 Theorem.** *Let  $\mathcal{G}$  be a projective geometry of rank at least two, and let  $H$  be a hyperplane such that  $\mathcal{G}$  is  $(p, H)$ -transitive for all points  $p$  in  $H$ . Then if  $\mathcal{G}$  is  $(o, H)$ -transitive for some point  $o$  not in  $H$ , it is isomorphic to  $\mathbb{P}(n, \mathbb{F})$  for some skew field  $\mathbb{F}$ .*

*Proof.* Let  $T = T(H)$  and let  $K$  be the skew field of endomorphisms of the geometric partition determined by the subgroups  $T(p)$ , where  $p \in H$ . The non-zero elements of  $K$  form a group isomorphic to the group of all homologies of  $\mathcal{G}$  with axis  $H$  and centre some point  $o$  off  $H$ . Since  $K$  is a skew field, we can view  $T$  as a vector space (over  $K$ ) and the subgroups  $T(p)$  as subspaces. As  $T$  acts transitively on the points of  $\mathcal{G}$  not in  $H$ , it follows that  $\mathcal{G}$  is  $(o, H)$ -transitive. This implies that  $K \setminus 0$  acts transitively on the non-identity elements of  $T(p)$ , and hence that  $T(p)$  is 1-dimensional subspace of  $T$ . Consequently the affine geometry  $\mathcal{G}^H$  has as its points the elements of the vector space  $T$ , and as lines the cosets of the 1-dimensional subspaces of  $T$ . Hence it is  $AG(n, K)$ , for some  $n$ . This completes the proof.  $\square$

We showed earlier that every projective geometry  $\mathcal{G}$  with rank at least four was  $(p, H)$ -transitive for any hyperplane  $H$  and any point  $p$ . Hence we obtain:

**3.9.2 Corollary.** *A projective geometry of rank at least four has the form  $\mathbb{P}(n, \mathbb{F})$  for some skew field  $\mathbb{F}$ .*  $\square$

Similarly we have the following.

**3.9.3 Corollary.** *A Desarguesian projective plane has the form  $\mathbb{P}(2, \mathbb{F})$  for some skew field  $\mathbb{F}$ .*  $\square$

If  $\mathcal{P}$  is a projective plane which is  $(p, l)$ -transitive for all points on some line  $l$  then the affine plane  $\mathcal{P}^l$  is called a *translation plane*. Translation planes which are not Desarguesian do exist, and some will be found in the next chapter.

## Exercises

1. Let  $\mathbb{F}$  be a finite field of characteristic  $p$ . Show that any  $p$ -element in  $PGL(n+1, \mathbb{F})$  fixes some point in  $\mathbb{P}(n, \mathbb{F})$ . Hence show that any Sylow  $p$ -subgroup of  $PGL(n+1, \mathbb{F})$  fixes a maximal flag. Finally show that any maximal flag is fixed by a unique Sylow  $p$ -subgroup.
2. Let  $V$  the vector space of dimension  $d$  over  $GF(q)$ . If  $a, h$  are non-zero vectors in  $V$ , define the map  $\tau_{h,a}$  from  $V$  to itself by

$$\tau_{h,a}(x) = x - (h^T x)a.$$

Show that  $\tau_{h,a}$  is a perspectivity of the projective space  $\mathcal{P}(V)$  and determine its center and axis. Prove that  $\mathcal{P}(V)$  is  $(p, H)$ -transitive for all  $p$  and  $H$ .

3. If a projective plane is  $(p, \ell)$ -transitive and  $(q, \ell)$ -transitive for distinct point  $p$  and  $q$  off  $\ell$ , show that it is  $(r, \ell)$ -transitive for all points  $r$  on  $p \vee q$ .
4. Let  $\mathcal{G}$  be a projective geometry with rank at least four. Show that any two triangles in perspective from a point of  $\mathcal{G}$  are in perspective from a line. (Note: if the triangles are coplanar, this will follow from a result in the notes, but they need not be coplanar and so there is still work to do.)

5. Let  $T$  be a group and let  $T_i$ , ( $i = 1, \dots, m$ ) be a collection of at least two subgroups such that the sets  $T_i \setminus 1$  partition  $T$  and, if  $i \neq j$  then  $T_i T_j = T$ . Show that the incidence structure with the elements of  $T$  as its points and the cosets of the subgroups  $T_i$  as its lines is an affine plane. (Note that we are not assuming that  $T$  is abelian, nor that the subgroups  $T_i$  are normal.)
6. Show that all finite translation planes have prime-power order, and that a translation plane of prime order is Desarguesian.



# Chapter 4

## Spreads and Planes

We are going to construct some non-Desarguesian translation planes. This will make extensive use of the theory developed in the previous chapter.

### 4.1 Spreads

Every projective geometry which is  $(p, H)$ -transitive for all points  $p$  on some hyperplane  $H$  gives rise, as we have seen, to a geometric partition of an abelian group  $T$ . The ring of endomorphisms of this partition is a skew field  $K$  and  $T$  is a vector space over  $K$  and the subgroups  $T(p)$  are subspaces. These all have the same dimension over  $K$ . To see this note that  $T(p)T(q)$  contains elements not in  $T(p) \cup T(q)$  and so there is a point  $r$ , not equal to  $p$  or  $q$ , such that  $T(r) \subseteq T(p)T(q)$ . Since  $T(p)T(r) = T(q)T(r)$  and  $T(p)$ ,  $T(q)$  and  $T(r)$  are disjoint, it follows that  $T(p)$  and  $T(q)$  must have the same dimension. Our claim follows easily from this. It is not hard to see that the original geometry is a plane if and only if  $T = T(p)T(q)$  for any pair of distinct points  $p$  and  $q$ . A geometric partition with this property is called a *spread*.

Since projective geometries with rank at least four are all of the form  $\mathbb{P}(n, \mathbb{F})$ , we no longer have much reason to bother working with geometric partitions in general. However spreads remain objects of considerable interest. Spreads can be defined conveniently as follows. Let  $V = V(2n, \mathbb{F})$  be a vector space over the skew field  $\mathbb{F}$ . A spread is set of  $n$ -dimensional subspaces of  $V$  which partitions the non-zero elements of  $V$ . These subspaces are often referred as the *components* of the spread. Every spread

determines a translation plane, on which the vector space  $V$  acts as a group of translations. The ring consisting of the endomorphisms of  $V$  which fix each component is the *kernel* of the spread (or of the plane it determines). As we have seen, it is a skew field, which necessarily contains  $\mathbb{F}$  in its centre. The points of the affine plane can be identified with the elements of  $V$  and the lines are then the cosets (in  $V$ ) of the components of  $\mathcal{S}$ . The point corresponding to the zero of  $V$  will be denoted by  $o$ .

**4.1.1 Lemma.** *Let  $\mathcal{A}$  be the affine plane determined by the spread  $\mathcal{S}$  of  $V(2n, \mathbb{F})$  and let  $K$  be its kernel. Then the collineations of  $\mathcal{A}$  which fix  $o$  are induced by the semilinear mappings of  $V$  which map the components of  $\mathcal{S}$  onto themselves.*

*Proof.* Let  $\alpha$  be a collineation of  $\mathcal{A}$  fixing  $o$ . If  $v \in V$ , define the mapping  $\tau_u$  on the points of  $\mathcal{A}$  by

$$\tau_u(x) = x + u.$$

A routine check shows that this is a translation of  $\mathcal{A}$ . It is also easy to show that if  $\tau$  is a translation then so is  $\alpha^{-1}\tau\alpha$ . Hence the mapping

$$\tau \mapsto \alpha^{-1}\tau\alpha$$

is an automorphism of the group of translations of  $\mathcal{A}$ . Thus it induces an additive mapping of  $V$ . Similarly we see that if  $\beta$  is a homology of  $\mathcal{A}$  with centre  $o$  and axis the line at infinity then so is  $\alpha^{-1}\beta\alpha$ . The group formed by these homologies is isomorphic to the multiplicative group formed by the non-zero elements of  $K$ . As  $V$  is a vector space over  $K$ , it follows that  $\alpha$  induces a semilinear mapping of  $V$ . That is, it can be represented as the composition of a linear mapping and an automorphism of the skew field  $K$ . The converse is straightforward.  $\square$

Lemma 1.1 can be extended without thought to isomorphisms between translation planes. The next result is an important tool for working with spreads.

**4.1.2 Lemma.** *Let  $V = V(2n, \mathbb{F})$  and let  $X_1, X_2, X_3$  and  $Y_1, Y_2$  and  $Y_3$  be subspaces such that*

$$X_1 \oplus X_2 = X_2 \oplus X_3 = X_3 \oplus X_1 = V$$

and

$$Y_1 \oplus Y_2 = Y_2 \oplus Y_3 = Y_3 \oplus Y_1 = V.$$

Then there is linear mapping  $\sigma$  in  $GL(V)$  such  $X_i\sigma = Y_i$ .

*Proof.* Our hypothesis implies all six subspaces have dimension  $n$  and that  $X_1$  and  $X_2$  are disjoint (well, excepting zero). Each subspace can be represented as the row space of an  $n \times 2n$  matrix over  $\mathbb{F}$ . There is an element  $\alpha$  of  $GL(V)$  sending  $X_1$  to the subspace equal to the row space of the  $n \times 2n$  matrix  $[I\ 0]$  and  $X_2$  to the row space of  $[0\ I]$ . Suppose that  $X_3\alpha$  is the row space of  $[A\ B]$ . Since  $X_3$  is disjoint from  $X_1$ , the matrix

$$\begin{pmatrix} I & 0 \\ A & B \end{pmatrix}$$

must be non-singular. This implies that  $B$  must be non-singular. As  $X_3$  is disjoint from  $X_2$ , we deduce similarly that  $A$  is non-singular. Let  $\beta$  be the element

$$\begin{pmatrix} A^{-1} & 0 \\ 0 & B^{-1} \end{pmatrix}$$

of  $GL(V)$ . Then  $[A\ B]\beta = [I\ I]$ , while the row spaces of  $[I\ 0]$  and  $[0\ I]$  are both fixed by  $\beta$ . (Do not forget that  $[I\ 0]$  and  $[A^{-1}\ 0]$  have the same row space.) Thus there is an element of  $GL(V)$  which sends  $X_1$ ,  $X_2$  and  $X_3$  respectively to the row spaces of the matrices  $[I\ 0]$ ,  $[0\ I]$  and  $[I\ I]$ . The lemma follows at once from this.  $\square$

The representation of the components of a spread in  $V(2n, \mathbb{F})$  by the row spaces of  $n \times 2n$  matrices is very useful. By virtue of the previous lemma, we may assume that a given spread contains the rows spaces of the matrices  $[0\ I]$  and  $[I\ 0]$ . Thus any third subspace is the row space of a matrix  $[A\ B]$  where  $A$  and  $B$  are non-singular. As the row space of  $[A\ B]$  and  $[I\ A^{-1}B]$  are equal, this means each of the remaining subspaces can be specified by a  $n \times n$  invertible matrix. (In this case,  $A^{-1}B$ .) The condition that the row spaces of  $[I\ A]$  and  $[I\ B]$  be disjoint is equivalent to the condition that the matrix

$$\begin{pmatrix} I & A \\ I & B \end{pmatrix}$$

be non-singular. This is equivalent to requiring that  $B - A$  be non-singular, since this is the determinant of the above matrix. If  $A$  and  $B$  are elements of  $GL(U)$  then  $B - A$  is invertible if and only if  $(I - B^{-1}A)$  is, and the latter holds if and only if there is no non-zero vector  $u$  such that  $B^{-1}Au = u$ . Thus  $B - A$  is invertible if and only if  $I - B^{-1}A$  acts fixed point freely on the

non-zero elements of  $U$ . We will find that it is sometimes more convenient to verify that  $A^{-1}B$  acts fixed-point freely than to show that  $A - B$  is invertible. If  $\sigma$  is an  $n \times n$  matrix then the row space of the matrix  $[I \ \sigma]$  will be denoted by  $V(\sigma)$ . The row space of  $[0 \ I]$  will be denoted by  $V(\infty)$ .

**4.1.3 Theorem.** *Let  $V = U \oplus U$  be a  $2n$ -dimensional vector space over  $\mathbb{F}$ . Then a spread of  $V$  is equivalent to a set  $\Sigma$  of elements of  $GL(U)$ , indexed by the non-zero elements of  $U$ , such that the difference of any two elements of  $\Sigma$  is invertible.*

*Proof.* Suppose we are given the set  $\Sigma$ . Then the subspaces  $V(\infty)$ ,  $V(0)$  and  $V(\sigma)$  where  $\sigma \in \Sigma$  are pairwise skew. To show that they form a spread we must verify that if  $(u, v)$  is a non-zero vector in  $V$  then it lies in one of these subspaces. If  $u = 0$  or  $v = 0$  then this is immediate. Consider the vectors  $(u, u\sigma)$ , where  $\sigma$  ranges over the elements of  $\Sigma$ . Since these act fixed-point freely on  $U$ , the vectors we obtain are all distinct. We obtain all vectors with first ‘coordinate’  $u$  if and only if  $|\Sigma| = |U \setminus 0|$ .  $\square$

Theorem 1.3 provides us with a compact representation of a spread. Note that different spreads can give rise to the same translation plane. If  $\alpha$  is the matrix

$$\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$$

in  $GL(U \oplus U)$  then  $\alpha$  maps the row space of  $[I \ A]$  to the row space of  $[W + AY \ X + AZ]$ . If  $W + AY$  is invertible this shows that the subspace parameterised by  $A$  is mapped to the subspace parameterised by  $(W + AY)^{-1}(X + AZ)$ . If  $\alpha$  fixes  $[I \ 0]$  and  $[0 \ I]$  then both  $X$  and  $Y$  must zero. If  $\Sigma\alpha = \Sigma$  then  $\alpha$  induces a collineation of the affine plane determined by  $\Sigma$ .

## 4.2 Collineations of Translation Planes

Let  $V = U \oplus U$  and let  $\Sigma$  be a subset of  $GL(U)$  determining a spread  $\mathcal{S}$  of  $V$ . Let  $\mathcal{A}$  be the affine plane belonging to  $\mathcal{S}$ . The subspaces  $V(\sigma)$  are the lines through the point  $o = (0, 0)$  in  $\mathcal{A}$ . The elements of  $V$  can all be written in the form  $(u, v)$ , where  $u$  and  $v$  belong to  $U$ . Then

$$V(\infty) = \{(0, u) : u \in U\}$$

and

$$V(\sigma) = \{(u, u\sigma) : u \in U\}$$

for any element  $\sigma$  in  $\Sigma \cup 0$ . Since  $U$  is a vector space over the kernel  $K$  of  $\mathcal{S}$ , it follows that any non-identity automorphism of  $K$  must act non-trivially on it. (That is, it cannot fix each element of  $U$ .) From this it follows in turn that any perspectivity of  $\mathcal{A}$  fixing  $o$  must be induced by a linear mapping of  $V$ , and not just a semilinear one. We consider the line at infinity  $l_\infty$  in  $\mathcal{A}$  as a distinguished line, rather than as a missing line. Let  $(0)$  and  $(\infty)$  be the points at which  $V(0)$  and  $V(\infty)$  respectively meet  $l_\infty$ .

**4.2.1 Theorem.** *The set  $\{\sigma \in GL(U) : \sigma\Sigma = \Sigma\}$  is a group, and is isomorphic to the group of homologies of  $\mathcal{A}$  with centre  $(0)$  and axis  $V(\infty)$ . The set  $\{\sigma \in GL(U) : \Sigma\sigma = \Sigma\}$  is also a group, and is isomorphic to the group of homologies of  $\mathcal{A}$  with centre  $(\infty)$  and axis  $V(0)$ .*

*Proof.* Suppose that  $\delta'$  is a homology of  $\mathcal{A}$  with centre  $(0)$  and axis  $V(\infty)$ . Since  $\delta'$  fixes each point on the line  $V(\infty)$ , it is induced by a linear mapping. Since  $\delta'$  fixes the lines  $V(0)$  and  $V(\infty)$ , it must map  $(u, v)$  to  $(u\delta, v\gamma)$  for some elements  $\delta$  and  $\gamma$  of  $GL(U)$ . (This follows from one of the remarks at the end of the previous section.) Since  $\delta'$  fixes each point on  $V(\infty)$ , we must have  $\gamma = 1$ . Suppose that  $\delta'$  maps  $V(\sigma)$  to  $V(\tau)$ . Then

$$(u, u\sigma)\delta' = (u\delta, u\sigma)$$

and therefore  $\delta^{-1}\sigma = \tau$ . From this we infer that  $\delta^{-1}\Sigma = \Sigma$ , and so the first part of the lemma is proved. The second part follows similarly. The converse is routine.  $\square$

**4.2.2 Corollary.** *If  $\Sigma$  contains the identity of  $GL(U)$  and the plane it determines is Desarguesian, then  $\Sigma$  is a group.*

*Proof.* If  $\mathcal{A} = \mathcal{P}^l$  is Desarguesian then it is  $(p, H)$ -transitive for all points  $p$  and lines  $H$ . By the previous lemma, it follows that

$$\{\sigma \in GL(U) : \sigma\Sigma = \Sigma\}$$

has the same cardinality as  $\Sigma$ . Since  $I \in \Sigma$ , we see that if  $\sigma\Sigma = \Sigma$  then  $\sigma$  must belong to  $\Sigma$ . Consequently  $\Sigma$  is closed under multiplication. As it consists of invertible matrices and contains the identity matrix, it is therefore a group.  $\square$

The group of homologies with centre  $(0)$  and axis  $V(\infty)$  in the previous lemma has the same cardinality as  $\Sigma$ . This implies our claim immediately.

The converse to this corollary is false. (See the next section.) There is an analog of Lemma 2.1 for elations.

**4.2.3 Lemma.** *Let  $\Sigma_0 = \Sigma \cup 0$ . The set*

$$\{\sigma \in \Sigma_0 : \sigma + \Sigma_0 = \Sigma_0\}$$

*is an abelian group, and is isomorphic to the group of elations with centre  $(\infty)$  and axis  $V(\infty)$ .*

*Proof.* If  $\alpha$  is represented by the matrix

$$\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$$

and  $(u, v) \in V$  then

$$(u, v)\alpha = (uW + vY, uX + vZ).$$

If  $(0, v) \in V(\infty)$  then  $(0, v)\alpha = (Yv, Zv)$ . Hence if each point on  $V(\infty)$  is fixed by  $\alpha$  then  $Y = 0$  and  $Z = I$ . If  $\alpha$  also fixes all lines through  $(\infty)$  then it must fix the cosets of  $V(\infty)$ . The elements of a typical coset of  $V(\infty)$  have the form  $(a, b + v)$ , where  $v$  ranges over the elements of  $U$ . Now

$$(a, b + v)\alpha = (aW, aX + b + v)$$

and so if  $\alpha$  fixes the lines parallel to  $V(\infty)$  then  $W = I$ . Consequently, if  $\alpha$  is an elation with centre  $(\infty)$  and axis  $V(\infty)$  and  $\sigma \in \Sigma$  then

$$(u, u\sigma)\alpha = (u, uX + u\sigma)$$

As  $\alpha$  is a collineation fixing  $o$ , it maps  $V(\sigma)$  to  $V(\tau)$  for some  $\tau$  in  $\Sigma$ , or to  $V(0)$ . Therefore  $X + \Sigma_0 = \Sigma_0$ . Thus we have shown that the elations with centre  $(\infty)$  and axis  $V(\infty)$  correspond to elements  $\sigma \in \Sigma$  such that  $\sigma + \Sigma_0 = \Sigma_0$ . The proof of the converse is routine.  $\square$

**4.2.4 Corollary.** *If the plane  $\mathcal{P}$  determined by  $\Sigma$  is Desarguesian then  $\Sigma_0$  is a skew field.*

*Proof.* Since  $\mathcal{P}$  is  $(p, l)$ -transitive for all points  $p$  and lines  $l$ , we deduce from Lemma 2.1 that  $\Sigma$  is a group and from Lemma 2.3 that  $\Sigma_0$  is a group under addition. If  $\sigma \in \Sigma$  then  $\sigma^{-1}\Sigma = \Sigma$ , implying that  $I = \sigma^{-1}\sigma \in \Sigma$ . As both addition and multiplication are the standard matrix operations, the usual associative and distributive laws hold. Therefore  $\Sigma_0$  is a skew field.  $\square$

**4.2.5 Lemma.** *If, for all elements  $\sigma$  and  $\tau$  of  $\Sigma$  we have  $\sigma\tau = \tau\sigma$  then  $\Sigma_0$  is a field and the plane determined by  $\Sigma$  is Desarguesian.*

*Proof.* Suppose that  $\alpha$  is an element of  $GL(U)$  which commutes with each element of  $\Sigma$ . Then the map sending  $(u, u\sigma)$  to

$$(u\alpha, u\sigma\alpha) = (u\alpha, u\alpha\sigma)$$

fixes each component of the spread  $\mathcal{S}$  and hence it must lie in its kernel. Denote this by  $K$ . The hypothesis of the lemma thus implies that  $\Sigma$  is a commutative subset of  $K \setminus 0$ . The elements of  $\Sigma$  determine distinct homologies of the plane determined by the spread, with centre  $o$  and axis  $l_\infty$ . Hence the plane must be Desarguesian (by Theorem 2.7.1) and  $\Sigma$  must coincide with  $K \setminus 0$ .  $\square$

## 4.3 Some Non-Desarguesian Planes

We propose to construct non-Desarguesian planes of order 9 and 16. Let  $U$  be a vector space over  $\mathbb{F}$  and let  $\Sigma$  be a subset of  $GL(U)$  determining a spread  $\mathcal{S}$  of  $V = U \oplus U$ . As customary, we assume that  $V(0)$  and  $V(\infty)$  are components of  $\mathcal{S}$ . The plane determined by  $\mathcal{S}$  is a *nearfield plane* if  $\Sigma$  is a group. (Thus Desarguesian planes are nearfield planes.)

First we construct a plane of order nine. Consider the group  $SL(2, 3)$  of  $2 \times 2$  matrices over  $GF(3)$  with determinant 1. Let  $U$  be the 2-dimensional vector space over  $GF(3)$ . We take  $\Sigma$  to be a Sylow 2-subgroup of  $SL(2, 3)$ . Since  $SL(2, 3)$  has order 24, this means  $\Sigma$  has the right size. There is also no question that its elements are invertible.

To show that  $\Sigma$  determines a spread, we first show that 2-elements of  $SL(2, 3)$  act fixed-point freely on  $U$ . Suppose that  $\alpha^2 = 1$ . If  $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  then the off-diagonal entries of  $\sigma^2$  are  $b(a + d)$  and  $c(a + d)$ . Hence either

#### 4. SPREADS AND PLANES

---

$b = c = 0$  or  $a + d = 0$ . In the first case, since  $\det \alpha = 1$ , we deduce that  $\alpha = \pm I$ . Otherwise it follows that  $\alpha$  has the form

$$\begin{pmatrix} a & b \\ -(1+a^2)/b & -a \end{pmatrix}$$

whence a simple calculation shows that  $\alpha^2 = -1$ . Thus  $-1$  is the only involution in  $SL(2, 3)$ . As it acts fixed-point freely on  $U$ , all 2-elements of  $SL(2, 3)$  must act fixed-point freely. If  $\sigma$  and  $\tau$  belong to  $\Sigma$  then  $\sigma^{-1}\tau$  is a 2-element, and so acts fixed point freely on  $U$ . Hence  $\sigma - \tau$  is invertible and therefore  $\Sigma$  determines a spread of  $U \oplus U$ . Since  $\Sigma$  is not commutative, the plane we obtain is not Desarguesian.

Our second plane needs more work. Consider the projective plane over  $GF(2)$ . If we number its points 1 through 7, its lines may be taken to be

$$123, 145, 167, 246, 257, 347, 356.$$

Each line gives us two 3-cycles belonging to the alternating group  $A_7$ . (For example the line 257 produces (257) and (275).) Let  $\Sigma$  be the set formed by these fourteen 3-cycles, together with the identity. Let  $X$  be the 4-dimensional vector space over  $GF(2)$ . We claim that  $A_7$  can be viewed as a subgroup of  $GL(4, 2)$  acting transitively on the 15 non-zero elements of  $X$ . The proof of this is given in the next section. We prove that if  $\sigma$  and  $\tau$  are elements of  $\Sigma$  then  $\sigma^{-1}\tau$  acts fixed-point freely on the non-zero vectors of  $X$ . A routine check shows that  $\sigma^{-1}\tau$  is either a 3-cycle or a 5-cycle. If  $x$  is a non-zero vector in  $X$  then the subgroup of  $A_8$  leaving it fixed has order  $8!/30 = 21 \cdot 2^6$ . Thus this subgroup contains no elements of order 5, and so all elements of order 5 in  $A_8$  must act fixed-point freely. Suppose then that  $\theta = \sigma^{-1}\tau$  is 3-cycle in  $A_8$ . Then there is a 5-cycle  $\phi$  which commutes with  $\theta$ . If  $x$  is non-zero vector fixed by  $\theta$  then

$$x\phi\theta = x\theta\phi = x\phi$$

and so  $x\phi$  is also fixed by  $\theta$ . This shows that the number of non-zero vectors fixed by  $\theta$  is divisible by 5. As  $\theta$  has order three, the number of non-zero vectors not fixed by it is divisible by three. This implies that  $\theta$  cannot fix 5 or 10 vectors, and hence that it must have 15 fixed points, that is, it is the identity element. Thus we have now shown that  $\Sigma$  determines a spread of  $X \oplus X$ . The resulting plane is not a nearfield plane, for then  $\Sigma$  would be a

group of order 15. The only group of order 15 is cyclic, and hence abelian. But the Sylow 2-subgroups of  $SL(2, 3)$  are isomorphic to the quaternion group, which is not abelian. The plane we have constructed is called the *Lorimer-Rahilly* plane. Note that the collineation group of the plane over  $GF(2)$  induces a group of collineations of the new plane fixing  $V(0)$ ,  $V(1)$  and  $V(\infty)$ , and acting transitively on the remaining components.

## 4.4 $\text{Alt}(8)$ and $GL(4, 2)$ are Isomorphic

We outline a proof that  $A_8$  is isomorphic to  $GL(4, 2)$ . Let  $S$  be the set  $\{0, 1, \dots, 7\}$ . There are 35 partitions of  $S$  into two sets of size four and since  $S_8$  acts on  $S$ , it also acts on this set of partitions. Any partition can be described by giving the elements of the component containing 1. Let  $\Omega$  be the set of all 35 triples from  $S \setminus 0$ . It is not hard to check that  $A_7$  acts transitively on  $\Omega$ . A set of seven triples from  $\Omega$  will be called a *heptad* if it has the property that every pair of triples from it intersect in precisely one point, and there is no point in all seven. We say that a set of triples are *concurrent* if there is some point common to them all, and the intersection of any two of them is this common point. A *star* is a set of three concurrent triples. The remainder of the argument is broken up into a number of separate claims.

**4.4.1 Claim.** *No two distinct heptads have three non-concurrent triples in common.*

It is only necessary to check that for one set of three non-concurrent triples, there is a unique heptad containing them.

**4.4.2 Claim.** *Each star is contained in exactly two heptads.*

Without loss of generality we may take our star to be 123, 145 and 167. By a routine calculation one finds that there are two heptads containing

#### 4. SPREADS AND PLANES

---

this star:

123	123
145	145
167	167
246	247
257	256
347	346
356	357

Note that the second of these heptads can be obtained from the first by applying the permutation (67) to each of its triples.

**4.4.3 Claim.** *There are exactly 30 heptads.*

There are 15 stars on each point, thus we obtain 210 pairs consisting of a star and a heptad containing it. As each heptad contains exactly 7 stars, it follows that there must be 30 heptads.

**4.4.4 Claim.** *Any two heptads have 0, 1 or 3 triples in common.*

If two heptads have four (or more) triples in common then they have three non-concurrent triples in common. Hence two heptads can have at most three triples in common. If two triples meet in precisely one point, there is a unique third triple concurrent with them. Any heptad containing the first two triples must contain the third. (Why?)

**4.4.5 Claim.** *The automorphism group of a heptad has order 168, and consists of even permutations.*

First we note that  $\text{Sym}(7)$  acts transitively on the set of heptads. As there are 30 heptads, we deduce that the subgroup of  $\text{Sym}(7)$  fixing a heptad must have order 168. Now consider the first of our heptads above. It is mapped onto itself by the permutations (24)(35), (2435)(67), (246)(357) and (1243675). The first two of these generate a group of order 8. Hence the group generated by these four permutations has order divisible by 8, 3 and 7. Since its order must divide 168, we deduce that the given permutations in fact generate the full automorphism group of the heptad.

**4.4.6 Claim.** *The heptads form two orbits of length 15 under the action of  $A_7$ . Any two heptads in the same orbit have exactly one triple in common.*

Since the subgroup of  $A_7$  fixing a heptad has order 168, the number of heptads in an orbit is 15. Let  $\Pi$  denote the first of the heptads above. The permutations (123), (132) and (145) lie in  $A_7$  and map  $\Pi$  onto three distinct heptads, having exactly one triple in common with  $\Pi$ . (Check it!) From each triple in  $\Pi$  we obtain two 3-cycles in  $A_7$ , hence we infer that there are 14 heptads in the same orbit as  $\Pi$  under  $A_7$  and with exactly one triple in common with  $\Pi$ . Since there are only 15 heptads in an  $A_7$  orbit, and since all heptads in an  $A_7$  orbit are equivalent, it follows that any two heptads in such an orbit have exactly one triple in common.

**4.4.7 Claim.** *Each triple from  $\Omega$  lies in exactly six heptads, three from each  $A_7$  orbit.*

Simple counting.

**4.4.8 Claim.** *A heptad in one  $A_7$  orbit meets seven heptads from the other in a star, and is disjoint from the remaining eight.*

More counting.

Now we construct a linear space. Choose one orbit of heptads under the action of  $A_7$ , and call its elements points. Let the triples be the lines, and say that a point is on a line if the corresponding heptad contains the triple. The elements of the second orbit of heptads under  $A_7$  determine subspaces of rank three, each isomorphic to a projective plane. It is now an exercise to show that there are no other non-trivial subspaces, and thus we have a linear space of rank four, with all subspaces of rank three being projective planes. Hence our linear space is a projective geometry, of rank four. Since its lines all have cardinality three, it must be the projective space of rank four over  $GF(2)$ . As  $GF(2)$  has no automorphisms, the collineation group of our linear space consists entirely of linear mappings; hence it is isomorphic to  $GL(4, 2)$ . (Note that we have just used the characterisation of projective geometries as linear spaces with all subspaces of rank three being projective planes, the fact that projective geometries of rank at least four are all of the form  $\mathbb{P}(n, \mathbb{F})$  and the fundamental theorem of projective geometry, i.e., that the collineations of  $\mathbb{P}(n, \mathbb{F})$  are semilinear mappings.) Our argument has thus revealed that  $A_7$  is isomorphic to a subgroup of  $GL(4, 2)$ . A direct computation reveals that it has index eight.

With a little bit of group theory it is now possible to show that  $GL(4, 2)$  is isomorphic to  $A_8$ . We outline an alternative approach. Let  $\Phi$  be the set

of all partitions of  $S$  into two sets of size four. These sets can be described by giving the three elements of  $S \setminus 0$  which lie in the same component of the partition as 0. Since  $S_8$  acts on  $S$ , we thus obtain an action of  $S_8$  on the 35 triples in  $\Omega$ . This action does not preserve the cardinality of the intersection of triples. However if two triples meet in exactly one point then so do their images. (Because two triples meet in one point if and only if the meet of the corresponding partitions is a partition of  $S$  into four pairs.) Hence the action of  $S_8$  on  $\Omega$  does preserve heptads. More work shows that, in this action,  $A_8$  and  $A_7$  have the same orbits on heptads. Thus  $A_8$  is isomorphic to a subgroup of  $GL(4, 2)$ , and hence to  $GL(4, 2)$ .

## 4.5 Moufang Planes

A line  $l$  in a projective plane  $\mathcal{P}$  is a *translation line* if  $\mathcal{P}$  is  $(p, l)$ -transitive for all points  $p$  on  $l$ , that is, if  $\mathcal{P}^l$  is a translation plane. We call  $p$  a *translation point* if  $\mathcal{P}$  is  $(p, l)$ -transitive for all lines  $l$  on it. From Lemma 2.3.1, we know that if  $\mathcal{P}$  is  $(p, l)$ -transitive and  $(q, l)$ -transitive for distinct points  $p$  and  $q$  on  $l$  then  $l$  is translation line. Dually, if  $\mathcal{P}$  is  $(p, l)$ - and  $(p, m)$ -transitive for two lines  $l$  and  $m$  through  $p$  then  $p$  is a translation point. The existence of more than one translation line (or point) in a projective plane is a strong restriction on its structure. The first consequence is the following.

**4.5.1 Lemma.** *If  $l$  and  $m$  are translation lines in the projective plane  $\mathcal{P}$  then all lines through  $l \cap m$  are translation lines.*

*Proof.* Suppose  $p = l \cap m$ . Then  $p$  is a translation point in  $\mathcal{P}$ . Let  $l'$  be a line through  $p$  distinct from  $l$  and  $m$ . Since  $\mathcal{P}$  is  $(p, m)$ -transitive, there is an elation with centre  $p$  and axis  $m$  mapping  $l$  to  $l'$ . (Why?) As  $l$  is a translation line, it follows that  $l'$  must be one too.  $\square$

It follows from this lemma that if there are three non-concurrent translation lines then all lines are translation lines. A plane with this property is called a *Moufang plane*. We have the following deep results, with no geometric proofs known.

**4.5.2 Theorem.** *If a projective plane has two translation lines, it is Moufang.*  $\square$

**4.5.3 Theorem.** *A finite Moufang plane is Desarguesian.*  $\square$

These are both proved in Chapter VI of Hughes and Piper[]. A Moufang plane which is not Desarguesian can be constructed using the Cayley numbers. These form a vector space  $\mathcal{O}$  of dimension eight over  $\mathbb{R}$  with a multiplication such that

- (a) if  $x$  and  $y$  lie in  $\mathcal{O}$  and  $xy = 0$  then either  $x = 0$  or  $y = 0$
- (b) if  $x, y$  and  $z$  belong to  $\mathcal{O}$  then  $x(y+z) = xy+xz$  and  $(y+z)x = yx+zx$ .

It is worth noting that this multiplication is neither commutative, nor associative. To each element  $a$  of  $\mathcal{O}$  we can associate an element  $\rho_a$  of  $GL(\mathcal{O})$ , defined by

$$\rho_a(x) = xa$$

for all  $x$  in  $\mathcal{O}$ . (This mapping is not a homomorphism.) Then  $\rho_a$  is injective and, since  $\mathcal{O}$  is finite dimensional, it must be invertible. Moreover, if  $a$  and  $b$  both belong to  $\mathcal{O}$  then  $(\rho_a - \rho_b)x = xa - xb = x(a - b)$  and so  $\rho_a - \rho_b$  is also invertible. Thus the set

$$\Sigma = \{\rho_x : x \in \mathcal{O} \setminus 0\}$$

gives rise to a spread of  $\mathcal{O} \oplus \mathcal{O}$ . As  $\Sigma$  is not closed under multiplication, the plane  $\mathcal{P}$  determined by  $\Sigma$  cannot be Desarguesian. Since  $\rho_{(x+y)} = \rho_x + \rho_y$  we see that  $\Sigma$  is a vector space over  $\mathbb{R}$ . By Lemma 2.3, this implies that  $\mathcal{P}$  has two translation lines and hence that it is Moufang.

## 4.6 Exercises

1. Let  $\Sigma$  be subset of  $GL(U)$  determining a spread  $\pi$  of  $V = U \oplus U$ . If  $\sigma \in \Sigma$  and  $\sigma\Sigma^{-1}\sigma = \Sigma$ , show that the mapping which sends  $(u, v)$  to  $(v\sigma^{-1}, u\sigma)$  is a perspectivity of the plane  $\mathcal{P}(\pi)$  with axis  $V(\sigma)$  which interchanges  $V(0)$  and  $V(\infty)$ . From this deduce that the collineation group of a nearfield plane has at most three orbits on its points, and no fixed points.
2. Let  $\mathcal{P}^\ell$  be a nearfield plane. Suppose that  $m$  is a translation line in  $\mathcal{P}$  distinct from  $\ell$ . The group of all perspectivities with axis  $m$  and centre  $\ell \cap m$  acts transitively on the points of  $\ell \setminus m$ . Deduce from this that group of collineations of  $\mathcal{P}$  fixing  $\ell$  acts transitively on the points of  $\ell \setminus m$ , and hence that there is a point  $y$  of  $\ell \setminus m$  and a line  $h$  on  $\ell \cap m$  not containing  $y$  such that  $\mathcal{P}$  is  $(y, h)$ -transitive. Finally deduce that  $\mathcal{P}$  is Desarguesian.

#### 4. SPREADS AND PLANES

---

3. Use the results of the previous two exercises to show that a non-Desarguesian nearfield plane is not self-dual.
4. Let  $U$  be a vector space and let  $\Sigma$  be a subset of  $GL(U)$  determining a spread of  $V = U \oplus U$ . If  $\Sigma$  is a group, show that the mappings  $t(\sigma, u)$  with  $\sigma \in \Sigma$  and  $u \in U$  given by

$$t(\sigma, u) : x \mapsto x\sigma + u$$

form a sharply 2-transitive group of permutations of  $U$ . (This shows that every nearfield plane determines a sharply 2-transitive permutation group. It is not too difficult to show that every sharply 2-transitive group determines an affine plane and with more effort it can be shown that resulting planes are translation planes.)

# Chapter 5

## Varieties

This chapter will provide an introduction to some elementary results in Algebraic Geometry.

### 5.1 Definitions

Let  $V = V(n, \mathbb{F})$  be the  $n$ -dimensional vector space over the field  $\mathbb{F}$ . An *affine hypersurface* in  $V$  is the solution set of the equation  $p(\mathbf{x}) = 0$ , where  $p$  is a polynomial in  $n$  variables, together with the polynomial  $p$ . If  $n = 2$  then a hypersurface is usually called a curve, and in three dimensions is known as a surface. An *affine variety* is the solution set of a set of polynomials in  $n$  variables together with the ideal, in the ring of all polynomials over  $\mathbb{F}$ , generated by the polynomials associated to the hypersurfaces. (This ideal is the ideal of polynomials which vanish at all points on the variety.) It is an important result that every affine variety can be realised as the solution set of a finite collection of polynomials. Affine varieties may also be defined as the intersection of a set of hypersurfaces.

A *projective hypersurface* is defined by a homogeneous polynomial in  $n + 1$  variables, usually  $x_0, \dots, x_n$ . If  $p$  is such a polynomial and  $p(\mathbf{x}) = 0$  then  $p(\alpha\mathbf{x}) = 0$  for all scalars  $\alpha$  in  $\mathbb{F}$ . The 1-dimensional subspaces spanned by the vectors  $\mathbf{x}$  such that  $p(\mathbf{x}) = 0$  are a subset of  $\mathbb{P}(n, \mathbb{F})$ , this subset is the projective hypersurface determined by  $p$ . A projective variety is defined in analogy to an affine variety. The ‘ideal’ of all homogeneous polynomials which vanish on the intersection is used in place of the ideal of all polynomials.

## 5. VARIETIES

---

A *quadric* is a hypersurface defined by a polynomial of degree two. It may be affine or projective. A projective curve is a hypersurface in  $\mathbb{P}(2, \mathbb{F})$  and a projective surface is a hypersurface in  $\mathbb{P}(3, \mathbb{F})$ . The hypersurface determined by the equation  $g(\mathbf{x}) = 0$  will be denoted by  $\mathcal{V}_g$ . Only the context will determine if  $g$  is homogeneous or not. A *conic* is a quadric given by a polynomial of degree two.

Every affine variety gives rise to a projective variety in a natural way. This happens as follows. Let  $p$  be a polynomial in  $n$  variables  $x_1, \dots, x_n$  with degree  $k$ . Let  $x_0$  be a new variable and let  $q$  be the polynomial  $x_0^k p(x_1/x_0, \dots, x_n/x_0)$ . This is a homogeneous polynomial of degree  $k$  in  $n+1$  variables. By way of example, if  $p$  is the polynomial  $x^2 - y - 1$  then  $q$  can be taken to be  $x^2 - yz - z^2$ . If we set  $z = 1$  in  $q$  then we recover the polynomial  $p$ . Geometrically, this corresponds to deleting the line  $z = 0$  from  $\mathbb{P}(2, \mathbb{F})$  to produce an affine space. The only point on the curve  $q(\mathbf{x}) = 0$  in  $\mathbb{P}(2, \mathbb{F})$  and on the line  $z = 0$  is spanned by  $(0, 1, 0)^T$ . The remaining points are spanned by the vectors  $(x, x^2 - 1, 1)^T$ , and these correspond to the points on the affine curve  $p(\mathbf{x}) = 0$ . We can also obtain affine planes by deleting lines other than  $z = 0$ . Thus if we delete the line  $y = 0$  then remaining points on our curve are spanned by the vectors  $(x, 1, z)^T$  such that  $x^2 - z - z^2 = 0$ . Although the original affine curve  $x^2 - y - 1$  was a parabola, this curve is a hyperbola. This shows that each projective variety determines a collection of affine varieties. These affine varieties are said to be obtained by *dehomogenisation*. (But we will say this as little as possible.) Two affine varieties obtained in this way are called *projectively equivalent*. The number of different affine varieties that can be obtained from a given projective variety is essentially the number of ways in which it is met by a projective hyperplane.

The affine variety determined by a homogeneous polynomial  $g$  is said to be a *cone*. More generally,  $\mathcal{V}_g$  is a cone at a point  $\mathbf{a}$  if  $g(\mathbf{y})$  is a homogeneous polynomial in  $\mathbf{y} = \mathbf{x} - \mathbf{a}$ . The projective variety associated with  $\mathcal{V}_g$  is also said to be a cone at  $\mathbf{a}$ . Everything we have said so far is true whether or not the underlying field is finite or not. One difficulty in dealing with the finite case is that it may not be clear how many points lie on a given hypersurface. (Of course similar problems arise if we are working over the reals.) The next result is useful; it is known as Warning's theorem.

**5.1.1 Theorem.** *Let  $f$  be a polynomial of degree  $k$  in  $n$  variables over the field  $\mathbb{F}$  with  $q = p^r$  elements. If  $k < n$  then the number of solutions of*

$f(\mathbf{x}) = 0$  is zero modulo  $p$ .

*Proof.* We begin with some observations concerning  $\mathbb{F}$ . If  $a \in \mathbb{F}$  then  $a^{q-1}$  is zero if  $a = 0$  and is otherwise equal to 1. For a non-zero element  $\lambda$  of  $\mathbb{F}$ , consider the sum

$$S(\lambda) = \sum_{a \in \mathbb{F}} (\lambda a)^d.$$

Then  $S(\lambda) = \lambda^d S(1)$ . On the other hand, when  $a$  ranges over the elements of  $\mathbb{F}$ , so does  $\lambda a$ . Hence  $S(\lambda) = S(1)$ , which implies that either  $S(1) = 0$  or  $\lambda^d = 1$ . We may choose  $\lambda$  to be a primitive element of  $\mathbb{F}$ , in which case  $\lambda^d = 1$  if and only if  $q-1$  divides  $d$ . This shows that if  $q-1$  does not divide  $d$  then  $S(1) = 0$ . If  $q-1$  divides  $d$  then  $S(1) \equiv q-1$  modulo  $p$ .

We now prove the theorem. The number of (affine) points  $\mathbf{x}$  such that  $f(\mathbf{x}) \neq 0$  is congruent modulo  $p$  to

$$\sum_{\mathbf{a} \in \mathbb{F}^n} f(\mathbf{a})^{q-1}. \quad (5.1.1)$$

The expansion of  $f(\mathbf{x})^{q-1}$  is a linear combination of monomials of the form

$$x_1^{k(1)} \cdots x_n^{k(n)}$$

where

$$\sum_i k(i) \leq (q-1)k < (q-1)n.$$

This shows that for some  $i$  we must have  $k(i) < q-1$ . Therefore

$$\sum_{a_i \in \mathbb{F}} a_i^{k(i)}$$

is congruent to zero modulo  $p$ . This implies in turn that (5.1.1) is congruent to zero modulo  $p$ .  $\square$

The following result is due to Chevalley.

**5.1.2 Corollary.** *If  $f$  is a homogeneous polynomial of degree  $k$  in  $n+1$  variables over the field  $F$  and  $k \leq n$  then  $\mathcal{V}_f$  contains at least one point of  $\mathbb{P}(n, \mathbb{F})$ .*  $\square$

These results generalise to sets of polynomials in  $n$  variables, subject to the condition that the sum of the degrees of the polynomials in the set is less than  $n$ . (See the exercises.)

## 5.2 The Tangent Space

Let  $f$  be a polynomial over  $\mathbb{F}$  in the variables  $x_0, \dots, x_n$ . By  $f_i$  we denote the partial derivative of  $f$  with respect to  $x_i$ . Even when  $\mathbb{F}$  is finite, differentiation works more or less as usual. In particular both the product and chain rules still hold. The chief surprise is the constant functions are no longer the only functions with derivative zero. Thus, over  $GF(2)$  we find that  $\frac{\partial}{\partial x_i} x_i^2 = 0$ . If  $f$  is homogeneous and  $\mathbf{a} \in \mathcal{V}_f$  then the *tangent space of  $\mathcal{V}_f$  at  $\mathbf{a}$*  is the subspace given by the equation

$$\sum_{i=0}^n f_i(\mathbf{a})x_i = 0.$$

It will be denoted by  $T_{\mathbf{a}}(\mathcal{V}_f)$ , or  $T_{\mathbf{a}}(f)$ . The tangent space at  $\mathbf{a}$  always contains  $\mathbf{a}$ . This follows from Euler's Theorem, which asserts that if  $f$  is a homogeneous polynomial of degree  $k$  then

$$\sum_{i=0}^n x_i f_i = kf.$$

(The proof of this is left as a simple exercise. Note that it is enough to verify it for monomials.) The tangent space at the point  $\mathbf{a}$  in the variety  $\mathcal{V}$  defined by a set  $S$  of polynomials is defined to be the intersection of the tangent spaces of the hypersurfaces determined by the elements of  $S$ . If  $f_i(\mathbf{a}) = 0$  for all  $i$  then  $\mathbf{a}$  is a *singular point* of the hypersurface  $\mathcal{V}_f$ . When  $\mathbf{a}$  is a singular point,  $T_{\mathbf{a}}$  is the entire projective space and has dimension  $n$ . If  $\mathbf{a}$  is not a singular point then  $T_{\mathbf{a}}$  has dimension  $n - 1$  as a vector space. A singular point of a general variety can be defined as a point where the dimension of the tangent space is 'too large', but we will not go into details. A point which is not singular is called *smooth*, and a variety on which all points are non-singular is itself called *smooth* or *non-singular*. Questions about the behaviour of a variety at a particular point can usually be answered by working in affine space, since we can choose some hyperplane not on the point as the hyperplane at infinity.

## 5.3 Tangent Lines

If  $f$  is a homogeneous polynomial then the *degree* of the hypersurface  $\mathcal{V}_f$  is the degree of  $f$ . The degree is important because it is an upper bound on

the number of points in which  $\mathcal{V}$  is met by a line. To see this, we proceed as follows. Assume that  $f$  is homogeneous of degree  $k$ , that  $a$  is a point and that  $b$  is a point not on  $\mathcal{V}_f$ . We consider the number of points in which  $a \vee b$  meets  $\mathcal{V}$ . Suppose that  $\mathbf{a}$  and  $\mathbf{b}$  are vectors representing  $a$  and  $b$ . All points on  $a \vee b$  are represented by vectors of the form  $\lambda\mathbf{a} + \mu\mathbf{b}$ . Thus the points of intersection of  $a \vee b$  with  $\mathcal{V}$  are determined by the values of  $\lambda$  and  $\mu$  such that  $f(\lambda\mathbf{a} + \mu\mathbf{b}) = 0$ . Since  $f(\mathbf{b}) \neq 0$  and  $f$  is homogeneous, all the points of intersection may be written in the form  $\mathbf{a} + t\mathbf{b}$ . Thus the number of points of intersection is the number of distinct solutions of

$$f(\mathbf{a} + t\mathbf{b}) = 0.$$

Now  $f(\mathbf{a} + t\mathbf{b})$  is a polynomial of degree  $k$  in  $t$ , and hence has at most  $k$  distinct zeros. If the field we are working over is infinite then it can be shown that the degree of a hypersurface is actually equal to the maximum number of points in which it is met by a line. With finite fields this is not guaranteed—in fact the hypersurface itself is not guaranteed to have  $k$  distinct points on it. There is more to be said about the way in which a line can meet a hypersurface. Continuing with the notation used above, we can write

$$f(\mathbf{a} + t\mathbf{b}) = F^{(0)}(\mathbf{b}) + tF^{(1)}(\mathbf{b}) + \cdots + t^k F^{(k)}(\mathbf{b}), \quad (5.3.1)$$

where  $F^{(i)}$  is a polynomial in the entries of  $\mathbf{b}$ , with coefficients depending on  $\mathbf{a}$ . If the first nonzero term in (5.3.1) has degree  $m$  in  $t$ , we say that the *intersection multiplicity at  $a$  of  $a \vee b$  and  $\mathcal{V}_f$*  is  $m$ . If  $a \in \mathcal{V}$  then  $F^{(0)}(\mathbf{b}) = 0$ ; thus the intersection multiplicity is greater than zero if and only if  $a$  is on  $\mathcal{V}$ . We have

$$F^{(1)}(\mathbf{b}) = \sum_{i=0}^n f_i(\mathbf{a}) b_i.$$

and so the intersection multiplicity is greater than 1 if and only if  $b$  lies in the tangent space  $T_a(f)$ . Since  $a \in T_a(f)$ , the point  $b$  is in  $T_a(f)$  if and only if the line  $a \vee b$  lies in  $T_a(f)$ . A line having intersection multiplicity greater than one with  $\mathcal{V}_f$  is a *tangent line*. We have just shown that  $T_a(f)$  is the union of all the tangent lines to  $\mathcal{V}_f$  at  $a$ . A subspace is *tangent* to  $\mathcal{V}_f$  at  $a$  if it is contained in  $T_a(f)$ . It is possible for the hypersurface  $\mathcal{V}$  to completely contain a given line  $a \vee b$ . In this case the left side of (5.3.1) must be zero for all  $t$ , whence it follows that  $a \vee b$  is a tangent. More generally, a subspace contained in  $\mathcal{V}_f$  is tangent to  $\mathcal{V}_f$  at each point in it. There is another important consequence of (5.3.1) which must be remarked on.

**5.3.1 Lemma.** *Any line meets a projective hypersurface of degree  $k$  in at most  $k$  points, or is contained in it.*

*Proof.* Let  $l$  be a line and let  $a$  be a point on  $l$  which is not on the hypersurface  $\mathcal{V}_f$ . The points of  $l$  on  $\mathcal{V}$  are given by the solutions of (5.3.1). If this is identically zero then  $l$  is contained in the hypersurface, otherwise it is a polynomial of degree  $k$  and has at most  $k$  zeros.  $\square$

We have only considered tangent spaces to hypersurfaces. Everything extends nicely to the case of varieties; we simply define the tangent space of the variety  $\mathcal{V}$  at  $a$  to be the intersection of the tangent spaces at  $a$  of the hypersurfaces which intersect to form  $\mathcal{V}$ . Since we will not be working with tangent spaces to anything other than hypersurfaces, we say no more on this topic. The tangent space to a quadric is easily described, using the following result, which is a special case of Taylor's theorem.

**5.3.2 Lemma.** *Let  $f$  be a homogeneous polynomial of degree two in  $n + 1$  variables over the field  $\mathbb{F}$  and let  $H = H(f)$  be the  $(n + 1) \times (n + 1)$  matrix with  $ij$ -entry equal to  $\frac{\partial^2}{\partial x_i \partial x_j} f$ . Then*

$$f(\lambda \mathbf{x} + \mu \mathbf{y}) = \lambda^2 f(\mathbf{x}) + \lambda \mu \mathbf{x}^T H \mathbf{y} + \mu^2 f(\mathbf{y}). \quad \square$$

The matrix  $H(f)$  is the *Hessian* of  $f$ . It is a symmetric matrix and, if the characteristic of  $\mathbb{F}$  is even, its diagonal entries are zero. The tangent plane at the point  $\mathbf{a}$  has equation  $\mathbf{a}^T H \mathbf{x} = 0$ , and therefore  $\mathbf{a}$  is singular if and only if  $\mathbf{a}^T H = 0$ . Consequently the quadric determined by  $f$  is smooth if  $H(f)$  is non-singular. (However it is possible for the quadric to be smooth when  $H$  is singular. For example, consider any smooth conic in a projective plane over a field of even order.) If the characteristic of  $\mathbb{F}$  is not even then  $f(\mathbf{x}) = \frac{1}{2} \mathbf{x}^T H(f) \mathbf{x}$ . Since we do not wish to restrict the characteristic of our fields, we will not be making use of this observation. One important consequence of Lemma 3.2 is that if a tangent to a quadric at  $a$  meets it at a second point  $b$  then it is contained in the quadric. (For these conditions imply that  $f(\mathbf{a}) = \mathbf{a}^T H \mathbf{b} = f(\mathbf{b}) = 0$ .) Since all lines through a singular point are tangents, it follows that a line which passes through a singular point and one other point must be contained in the quadric. Of course any line meeting a quadric in three or more points must be contained in it, by Lemma 3.1. A line which meets a quadric in two points is a *secant*.

**5.3.3 Lemma.** *Any line which meets a quadric in exactly one point is a tangent.*

*Proof.* Suppose  $l$  is a line passing through the point  $a$  on a given quadric  $f(\mathbf{x}) = 0$  and that  $b \in l$ . Then the points of  $l$  on the quadric are given by the solutions of the quadratic in  $\lambda$  and  $\mu$ :

$$\lambda^2 f(\mathbf{a}) + \lambda\mu \mathbf{a}^T \mathbf{A} \mathbf{b} + \mu^2 f(\mathbf{b}) = 0.$$

Since  $f(\mathbf{a}) = 0$  this quadratic has only one solution if and only  $\mathbf{a}^T \mathbf{A} \mathbf{b} = 0$ , i.e.,  $\mathbf{b} \in T_a(f)$ . Thus any line which meets the quadric in only the single point  $a$  must lie in the tangent space  $T_a$ .  $\square$

## 5.4 Intersections of Hyperplanes and Hypersurfaces

Suppose that  $f$  is a homogeneous polynomial defined over a field  $\mathbb{F}$ . Then  $f$  is irreducible if it does not factor over  $\mathbb{F}$ , and it is *absolutely irreducible* if it does not factor over the algebraic closure of  $\mathbb{F}$  of  $\mathbb{F}$ . If  $g$  is a factor of  $F$  over  $\overline{\mathbb{F}}$  then  $\mathcal{V}_g$  is a *component* of  $\mathcal{V}_f$ . Thus  $\mathcal{V}_f$  is a union of components, although not necessarily a disjoint union. Over finite fields the situation is a little delicate, in that  $\mathcal{V}_g$  may be empty. However this possibility will not be the source of problems—such components tend to remain completely invisible.

A hyperplane can be viewed as a projective space in its own right. By changing coordinates if needed, we may assume that the hyperplane has equation  $x_0 = 0$ . Suppose that  $f$  is homogeneous in  $n + 1$  variables with degree  $k$  and that  $g$  is the polynomial obtained by setting  $x_0$  equal to zero. Now  $g$  might be identically zero, in which case we must have  $f = x_0 f'$  with  $f'$  a homogeneous polynomial of degree  $k - 1$ . Thus the hyperplane is a component of  $\mathcal{V}_f$ . If  $g$  is not zero then it is a homogeneous polynomial of degree  $k$  in  $n$  variables, and defines a nontrivial hypersurface. One interesting case is when the intersecting hyperplane is the tangent space to  $\mathcal{V}_f$  at the point  $a$ . Every line through  $a$  in  $T_a(f)$  is a tangent line to  $\mathcal{V}_f$  and hence to  $T_a(f) \cap \mathcal{V}_f$ . Thus  $a$  is a singular point in the intersection. We will not have much cause to consider the intersection of two general hypersurfaces. There is one case concerning intersecting ‘hypersurfaces’ in projective planes where we will need some information. This result is called *Bézout’s theorem*.

**5.4.1 Theorem.** *Let  $f$  and  $g$  be homogeneous polynomials over  $\mathbb{F}$  in three variables with degree  $k$  and  $l$  respectively. Then either the curves  $\mathcal{V}_f$  and  $\mathcal{V}_g$  meet in at most  $kl$  points in  $\mathbb{P}(2, \mathbb{F})$ , or they have a common component.  $\square$*

In general two hypersurfaces of degrees  $k$  and  $l$  meet in a variety of degree  $kl$ . The theory describing the intersection of varieties is very complicated, even by the standards of Algebraic Geometry. The proof of the above result is quite simple though. (It can be found in “Algebraic Curves” by Robert J. Walker, Springer (New York) 1978. The proof of Bézout’s theorem given there is over the complex numbers, but is valid for algebraically closed fields of any characteristic.) In making use of Bézout’s lemma, we will need the following result, which is an extension of the fact that if a polynomial in one variable  $t$  over  $\mathbb{F}$  vanishes at  $\lambda$  then it must have  $t - \lambda$  as a factor.

**5.4.2 Lemma.** *Let  $f$  and  $g$  be polynomials in  $n + 1$  variables over an algebraically closed field, with  $f$  absolutely irreducible. If  $g(\mathbf{x}) = 0$  whenever  $f(\mathbf{x}) = 0$  then  $f$  divides  $g$ .  $\square$*

As an immediate application of the previous ideas, we prove the following.

**5.4.3 Lemma.** *There is a unique conic through any set of five points which contains a 4-arc.*

*Proof.* Suppose that  $abcd$  is a 4-arc. Let  $f$  be the homogeneous quadratic polynomial describing the conic formed by the union of the two lines  $a \vee b$  and  $c \vee d$ , and let  $g$  be the quadratic describing the union of the lines  $a \vee d$  and  $b \vee c$ . Consider the set of all quadratic polynomials of the form

$$\lambda f + \mu g. \tag{5.4.1}$$

Each of these is a quadratic, and thus describes a conic. If  $x$  is a point not on the 4-arc then the member of (5.4.1) with  $\lambda = g(\mathbf{x})$  and  $\mu = -f(\mathbf{x})$  vanishes at  $x$  and at each point of the 4-arc. This establishes the existence of a conic through any set five points containing a 4-arc. Suppose now that  $\mathcal{C}$  and  $\mathcal{C}'$  are two conics meeting on the 4-arc  $abcd$  and the fifth point  $p$ . By Bézout’s lemma, these two conics must have a common component. If the conics are distinct, this component must be described by a linear polynomial, i.e., it must be a line  $\ell$ . Hence  $\mathcal{C}$  and  $\mathcal{C}'$  must each be the union

#### 5.4. Intersections of Hyperplanes and Hypersurfaces

---

of two lines, possibly the same line twice. But now each conic contains  $\ell$  and at least two points from the 4-arc not on  $\ell$ . We conclude that the conics must coincide.  $\square$

The hypersurfaces determined by the set of polynomials

$$\lambda f + \mu g, \quad \lambda, \mu \in \mathbb{F}$$

are said to form a *pencil*. We shall see that pencils can be very useful.



# Chapter 6

## Conics

We now begin our study of quadrics in  $\mathbb{P}(2, \mathbb{F})$ , i.e., conics. We will prove the well known theorems of Pappus and Pascal, along with Segre's theorem, which asserts that a  $(q + 1)$ -arc in a projective plane over a field of odd order is a conic.

### 6.1 The Kinds of Conics

By Corollary 4.1.2, every conic over the field  $\mathbb{F}$  contains at least one point. We will see that conics with only one point on them exist, but there is little to be said about them. There are two obvious classes of singular conics. The first consists of the ones with equations  $(\mathbf{a}^T \mathbf{x})^2 = 0$ , with all points singular. We will call this a *double line*. The second have equations  $(\mathbf{a}^T \mathbf{x})(\mathbf{b}^T \mathbf{x}) = 0$ , with  $\mathbf{a}$  and  $\mathbf{b}$  independent. The variety defined by such an equation is the union of two distinct lines; the point of intersection of these two lines is the unique singular point. A single point is also a conic. To see this, take an irreducible quadratic  $f(x_0, x_1)$ , then view it as a polynomial in three variables  $x_0, x_1$  and  $x_2$ . Its solution set in the projective plane is the point  $(0, 0, 1)^T$ . Smooth conics do exist—the points of the form  $(1, t, t^2)^T$  where  $t$  ranges over the elements of  $\mathbb{F}$ , together with the point  $(0, 0, 1)^T$  provide one example. (This is the variety defined by the equation  $x_0x_2 - x_1^2 = 0$ . You should verify that it is smooth.) The four examples just listed exhaust the possibilities.

**6.1.1 Theorem.** *A conic in  $\mathbb{P}(2, \mathbb{F})$  is either*

## 6. CONICS

---

- (a) a single point,
- (b) a double line,
- (c) the union of two distinct lines, or
- (d) smooth, and a  $(q + 1)$ -arc if  $\mathbb{F}$  is finite with order  $q$ .

*Proof.* To begin we establish an important preliminary result, namely that if  $a$  is a non-singular point in a conic  $\mathcal{C} = \mathcal{V}_f$  then

$$|\mathcal{C}| = q + |T_a(\mathcal{C}) \cap \mathcal{C}|$$

(This implies that the cardinality of  $\mathcal{C}$  is either  $q + 1$  or  $2q + 1$ .) Suppose  $f$  is homogeneous of degree two and that  $f(\mathbf{a}) = 0$ . Then

$$f(\lambda\mathbf{a} + \mu\mathbf{x}) = \lambda\mu\mathbf{a}^T A\mathbf{x} + \mu^2 f(\mathbf{x}).$$

If  $\mathbf{a}^T A\mathbf{x} \neq 0$ , this implies that  $f(\mathbf{x})\mathbf{a} - (\mathbf{a}^T A\mathbf{x})\mathbf{x}$  is a second point on the line through  $a$  and  $x$  which is on the conic. This shows that there is a bijection between the lines through  $a$  not in  $T_a(f)$  and the points of  $\mathcal{V}_f \setminus T_a(f)$ . If  $a$  is a non-singular point then  $T_a$  is a line. By the previous lemma it contains either 1 or  $q + 1$  points of the conic. There are  $q + 1$  lines through any point in  $\mathbb{P}(2, \mathbb{F})$ . Thus if  $a$  is non-singular then the conic contains either  $q + 1$  or  $2q + 1$  points according as the tangent at  $a$  is contained in  $\mathcal{C} = \mathcal{V}_f$  or not.

We now prove the theorem. Suppose that  $\mathcal{C}$  is a conic. Assume first that it contains two singular points  $a$  and  $b$ . From our observations at the end of the previous section, all points on  $a \vee b$  must belong to  $\mathcal{C}$ . If  $c$  is point of the conic not on  $a \vee b$  then all points on  $c \vee a$  and  $c \vee b$  must also lie in  $\mathcal{C}$ . If  $x$  is a point in  $\mathbb{P}(2, \mathbb{F})$  then there is a line through  $x$  meeting  $c \vee a$ ,  $c \vee b$  and  $a \vee b$  in distinct points. Hence this line lies in  $\mathcal{C}$  and so  $x \in \mathcal{C}$ . This proves that  $\mathcal{C}$  is the entire plane, which is impossible. Thus we have shown that if  $\mathcal{C}$  contains two singular points then it must consist of all points on the line joining them, i.e., it is a repeated line.

Assume then that  $\mathcal{C}$  contains exactly one singular point,  $a$  say, and a further point  $b$ . Then  $a \vee b$  is contained in  $\mathcal{C}$ . As there is only one singular point, there must a point of  $\mathcal{C}$  which is not on  $a \vee b$ . The line joining this point to  $a$  is also in  $\mathcal{C}$ . This accounts for  $2q + 1$  points of  $\mathcal{C}$ , hence our conic must be the union of two distinct lines. Finally suppose that  $\mathcal{C}$  contains at least two points, and no singular points. If  $|\mathcal{C}| = 2q + 1$  then each point of

$\mathcal{C}$  must lie in a line contained in  $\mathcal{C}$ . Hence  $\mathcal{C}$  must contain two distinct lines, and their point of intersection is singular. Consequently  $\mathcal{C}$  can contain no lines, but must rather be a  $(q + 1)$ -arc.  $\square$

This theorem is still valid over infinite fields, but the proof in this case is left to the reader. One consequence of it is that a conic is smooth if and only if it contains a 5-arc. In combination with Lemma 5.1, this implies that there is a unique smooth conic containing a given 5-arc.

## 6.2 Pascal and Pappus

The theorems of Pascal and Pappus are two of the most important results concerning projective planes over fields. We will prove both of these results using Bézout's lemma, and then give some of their applications. There are a few matters to settle before we can begin. A *hexagon* in a projective plane consists of cyclically ordered set of six points  $A_0, A_1, \dots, A_5$ , together with the six lines  $A_i A_{i+1}$ . Here the addition in the subscripts is computed modulo six. The six lines, which we require to be distinct, are the *sides* of the hexagon. Two sides are *opposite* if they are of the form  $A_i A_{i+1}$  and  $A_{i+3} A_{i+4}$ . Let  $\mathbf{a}_{i,i+1}$ ,  $i = 0, \dots, 5$  be the homogeneous coordinate vectors of the sides of the hexagon. Then the polynomial

$$f(\mathbf{x}) = (\mathbf{x}^T \mathbf{a}_{01})(\mathbf{x}^T \mathbf{a}_{23})(\mathbf{x}^T \mathbf{a}_{45}) \quad (6.2.1)$$

is homogeneous with degree three. Similarly, the three sides opposite to those used in (6.2.1) determine a second cubic,  $g$  say. By Bézout's lemma, two cubics with no common component meet in at most nine points. A common component of our two cubics would have to contain a line, and our hypothesis that the sides are distinct prevents this. Therefore  $\mathcal{V}_f$  and  $\mathcal{V}_g$  meet in the six points of our hexagon, together with the points of intersection of the three pairs of opposite sides.

**6.2.1 Theorem.** (*Pascal*). *The six points of a hexagon lie on a conic if and only if the points of intersection of the three pairs of opposite sides lie on a line.*

*Proof.* Let  $A_0, A_1, \dots, A_5$  be a hexagon. Suppose that the three points

$$A_0 A_1 \cap A_3 A_4, \quad A_1 A_2 \cap A_4 A_5, \quad A_2 A_3 \cap A_0 A_5$$

## 6. CONICS

---

lie on a line  $l$ , with equation  $\mathbf{a}^T \mathbf{x} = 0$ . Let  $f$  and  $g$  be the two cubics defined above. For any scalars  $\lambda$  and  $\mu$ , the polynomial  $F = \lambda f + \mu g$  is cubic and contains the nine points in which  $\mathcal{V}_f$  and  $\mathcal{V}_g$  intersect. We wish to choose the scalars so that the line  $l$  is contained in  $\mathcal{V}_F$ . If  $l$  has only three points, there is no work to be done. Thus we may choose a fourth point  $p$  on  $l$ , and choose  $\lambda$  and  $\mu$  so that  $F(p) = 0$ . Thus the cubic curve  $\mathcal{V}_F$  meets the line  $l$  in four points, and if we extend  $\mathbb{F}$  to its algebraic closure, then the line extending  $l$  still meets the extension of  $\mathcal{V}_F$  in at least four points. Bézout's theorem now implies that  $l$  must be contained in the curve and so we deduce, by Lemma 4.4.2, that  $F = (\mathbf{a}^T \mathbf{x})G$  for some polynomial  $F_1$ . But  $G$  must be homogeneous of degree two and therefore  $\mathcal{V}_G$  is a conic. Thus  $\mathcal{V}_F$  is the union of the line  $l$  and the conic  $\mathcal{V}_G$ . If the hexagon is contained in the union of two lines then it is on a conic, and we are finished. Otherwise a simple check shows that no points on the hexagon lie on  $L$  (do it), hence they line on the conic. This proves the first part of the theorem.

Assume now that the points of the hexagon lie on a conic. There is no loss on assuming that this conic is not a double line or a single point. Thus it is either the union of two distinct lines, or is smooth. It is convenient to treat these two cases separately. Suppose then that our conic is the union of the two lines  $l$  and  $m$ , with respective equations  $\mathbf{a}^T \mathbf{x} = 0$  and  $\mathbf{b}^T \mathbf{x} = 0$ . As the sides of our hexagon are distinct, no four points of it are collinear. (Why?) Hence three points of the hexagon lie on  $l$  and three on  $m$ . In particular,  $p = l \cap m$  is not a point of the hexagon. Now choose  $\lambda$  and  $\mu$  so that  $F = \lambda f + \mu g$  passes through  $p$ . Then the lines  $l$  and  $m$  each meet the cubic  $F$  in four points, and so they must lie in  $\mathcal{V}_F$ . Hence  $F$  is divisible by  $(\mathbf{a}^T \mathbf{x})(\mathbf{b}^T \mathbf{x})$  and the quotient with respect to this product must be linear. Thus  $F$  is the union of three lines. Consequently the points of intersection of the opposite sides of the hexagon must be collinear.

There remains the case that the points of the hexagon lie on a smooth conic  $\mathcal{C}$ , with equation  $h(\mathbf{x}) = 0$ . This conic meets any curve of the form

$$F(\mathbf{x}) := \lambda f(\mathbf{x}) + \mu g(\mathbf{x}) = 0 \tag{6.2.2}$$

in at least the six points of the hexagon. As  $|\mathcal{C}| \geq 6$ , our field must have order at least five. If it is exactly five then  $\mathcal{C}$  is contained in the solution set of (6.2.2) for any choice of scalars; otherwise we may choose a point  $p$  of  $\mathcal{C}$  not in the hexagon and then choose  $\lambda$  and  $\mu$  so that  $\mathcal{V}_F$  meets  $\mathcal{C}$  in at least seven points. By Bézout's theorem, this implies that these two curves have

a common component. The only component of  $\mathcal{C}$  is  $\mathcal{C}$  itself, thus  $F = hG$  for some linear polynomial  $G$ . Hence  $\mathcal{V}_F$  is the union of a line and the conic  $\mathcal{C}$ , and the points of intersection of the opposite sides of our hexagon must be on the line.  $\square$

Pappus' theorem is the assertion that the intersections of the opposite sides of a hexagon are collinear if the points of the hexagon lie on two lines. It is particularly important because it can be proved that a projective plane has the form  $\mathbb{P}(2, \mathbb{F})$ , where  $\mathbb{F}$  is a field, if and only if Pappus' theorem holds. Thus, if we could prove geometrically that Pappus' theorem held in all finite Desarguesian planes then we would have a geometric proof that a finite skew field is a field. No such proof is known. Planes for which Pappus' theorem is valid are called *Pappian*. All Pappian planes are, of course, Desarguesian.

## 6.3 Automorphisms of Conics

If  $\mathcal{C}$  is a conic described by the equation  $f(\mathbf{x}) = 0$  and  $\tau \in PGL(3, \mathbb{F})$  then we let  $f^\tau$  denote the polynomial defining the conic  $\mathcal{C}\tau$ . The *automorphism group* of a conic in the Pappian plane  $\mathbb{P}(2, \mathbb{F})$  is the subgroup of  $PGL(3, \mathbb{F})$  which fixes it as a set. The concept is well defined in all cases, but we will mainly be interested in automorphisms of smooth conics. Our previous theorem implies that smooth conics have many automorphisms.

**6.3.1 Theorem.** *Let  $abcd$  be a 4-arc in a Pappian projective plane and let  $\mathcal{C}$  be a conic containing it. Then there is an involution  $\tau$  in the automorphism group of  $\mathcal{C}$  such that  $a\tau = d$  and  $b\tau = c$ .*

*Proof.* As  $PGL(3, \mathbb{F})$  is transitive on ordered 4-arcs, it contains an element  $\tau$  mapping  $abcd$  to  $badc$ . Hence  $\tau$  fixes both the conics  $ac \cup bd$  and  $ab \cup cd$ . Suppose that these conics are defined by the polynomials  $f$  and  $g$  respectively. For any  $\lambda$  and  $\mu$  in  $\mathbb{F}$ , we find that

$$(\lambda f + \mu g)\tau = \lambda f^\tau + \mu g^\tau = \lambda f + \mu g.$$

Hence  $\tau$  fixes each quadric in the pencil determined by  $f$  and  $g$ . Since every conic containing the given 4-arc belongs to this pencil, this proves the theorem.  $\square$

One immediate consequence of this theorem is the following result.

**6.3.2 Corollary.** *Let  $\mathcal{C}$  be a smooth conic in a Pappian plane. Then its automorphism group acts sharply 3-transitively on the points in it.*

*Proof.* If  $|\mathbb{F}| = 2$  or  $3$ , this result can be verified easily. Assume then that  $|\mathbb{F}| > 3$ . From the theorem,  $\text{Aut}(\mathcal{C})$  is 2-transitive on the points of  $\mathcal{C}$ . To prove that  $\text{Aut}(\mathcal{C})$  is 3-transitive it will suffice to prove that if  $A, B, C$  and  $D$  are four points on  $\mathcal{C}$  then there is an automorphism of it fixing  $A$  and  $B$  and mapping  $C$  to  $D$ .

Let  $X$  be a fifth point on the conic. By the theorem, there is an involution in  $\text{Aut}(\mathcal{C})$  swapping  $A$  and  $B$ , and sending  $C$  to  $X$ . Similarly, there is an involution swapping  $B$  and  $A$  and sending  $X$  to  $D$ . The product of these two involutions is the required automorphism. Suppose that  $A, B$  and  $C$  are three points on the conic. Any automorphism which fixes these three points must fix the tangents at  $A$  and  $B$ . Hence it fixes their point of intersection, which we denote by  $P$ . Thus the automorphism fixes each point in a 4-arc, and the only element of  $PGL(3, \mathbb{F})$  which fixes a 4-arc is the identity.  $\square$

It follows at once from the corollary that if  $|\mathbb{F}| = q$  then  $|\text{Aut}(\mathcal{C})| = q^3 - q$ . We have already seen that the conics in  $\mathbb{P}(2, \mathbb{F})$  correspond to the points in  $\mathbb{P}(5, \mathbb{F})$ , and are thus easily counted, there are

$$[6] = q^5 + q^4 + q^3 + q^2 + q + 1$$

of them. As for the smooth conics, we have:

**6.3.3 Lemma.** *Let  $\mathbb{F}$  be the field with  $q$  elements, where  $q > 3$ . Then the number of smooth conics in  $\mathbb{P}(2, \mathbb{F})$  is equal to  $q^5 - q^2$ .*

*Proof.* Let  $n_k$  denote the number of ordered  $k$ -arcs and let  $N$  be the number of smooth conics. Then, as we noted at the end of Section 6, there is a unique smooth conic containing a given 5-arc. Hence

$$N(q+1)q(q-1)(q-2)(q-3) = n_5. \tag{6.3.1}$$

We find that

$$n_3 = (q^2 + q + 1)(q^2 + q)q^2.$$

Let  $ABC$  be a 3-arc. There  $q-1$  lines through  $A$  which do not pass through  $B$  or  $C$ , and on each of these lines there are  $q-1$  points which do not lie on any line joining  $B$  and  $C$ . Thus we can extend a  $ABC$  to a 4-arc using

any one of  $(q - 1)^2$  points, and so  $n_4 = (q - 1)^2 n_3$ . There are  $q - 2$  lines through a point in a 4-arc  $ABCD$  which do not meet a second point on the arc, and each of these lines contains  $q - 3$  points not on the lines  $BC$ ,  $BD$  or  $CD$ . Thus  $n_5 = (q - 2)(q - 3)n_4$ . Accordingly

$$n_5 = (q - 3)(q - 2)(q - 1)^2 q^3 (q + 1)(q^2 + q + 1)$$

and, on comparing this with (6.3.1), we obtain that  $N = (q^2 + q + 1)q^2(q - 1)$  as claimed.  $\square$

The group  $PGL(3, \mathbb{F})$  permutes the smooth conics in  $\mathbb{P}(2, \mathbb{F})$  amongst themselves. The number of conics in the orbit containing  $\mathcal{C}$  is equal to

$$|PGL(3, \mathbb{F})|/|\text{Aut}(\mathcal{C})|.$$

The order of  $PGL(3, \mathbb{F})$  is

$$(q - 1)^{-1}(q^3 - 1)(q^3 - q)(q^3 - q^2) = (q^2 + q + 1)(q + 1)q^3(q - 1)^2.$$

Since the automorphism group of a smooth conic has order  $q^3 - q$ , the orbit of  $\mathcal{C}$  has cardinality equal to

$$(q^2 + q + 1)(q + 1)^2 q^3 (q - 1)^2 / (q^3 - q) = (q^5 - q^2).$$

As there are altogether  $q^5 - q^2$  smooth conics, this implies the following.

**6.3.4 Theorem.** *All smooth conics in the Pappian plane  $\mathbb{P}(2, \mathbb{F})$  are equivalent under the action of  $PGL(3, \mathbb{F})$ .*  $\square$

## 6.4 Ovals

An oval in a projective plane of order  $q$ , i.e., with  $q + 1$  points on each line, is simply a  $(q + 1)$ -arc. Every smooth conic in a Pappian plane is a  $(q + 1)$ -arc; we show now that ovals have many properties in common with conics. As usual, some definitions are needed. Let  $\mathcal{K}$  be a  $k$ -arc. A *secant* to  $\mathcal{K}$  is a line which meets it in two points, a *tangent* meets it in one point. A line which does not meet the arc is an *external line*. Since no line meets  $\mathcal{K}$  in three points, it has exactly  $\binom{k}{2}$  secants. Each point in  $\mathcal{K}$  lies on  $k - 1$  of these secants, whence there are  $q + 2 - k$  tangents through each point and  $k(q + 2 - k)$  tangents altogether. An immediate consequence of these

deliberations is that a  $k$ -arc has at most  $q + 2$  points on it. (If  $q$  is odd this bound can be reduced to  $q + 1$ . Proving this is left as an exercise.) Our next result is an analog of the fact that a circle in the real plane divides the points into three classes:

- (a) the points outside the circle, which each lie on two tangents
- (b) the points on the circle, which lie on exactly one tangent
- (c) the points inside the circle, which lie on no tangents.

**6.4.1 Lemma.** *Let  $\mathbb{F}$  be the field of order  $q$ , where  $q$  is odd, and let  $\mathcal{Q}$  be a  $(q + 1)$ -arc in  $\mathbb{P}(2, \mathbb{F})$ . Then there are  $\binom{q+1}{2}$  points, each lying on exactly two tangents to  $\mathcal{Q}$ , and  $\binom{q}{2}$  points which lie on none.*

*Proof.* Suppose  $P$  is a point on a tangent to  $\mathcal{Q}$ , but not on  $\mathcal{Q}$ . Then the lines through  $P$  meet  $\mathcal{Q}$  in at most two points, and thus they partition the points of  $\mathcal{Q}$  into pairs and singletons. Each singleton determines a tangent to  $\mathcal{Q}$  through  $P$ . Since  $q + 1$  is even,  $P$  lies on an even number of tangents. As  $P$  is on one tangent, it therefore lies on at least two. On the other hand, each pair of tangents to  $\mathcal{Q}$  meet at a point off  $\mathcal{Q}$ , and this point is on two tangents. Thus there are at most  $\binom{q+1}{2}$  triples formed from a pair of distinct tangents and their point of intersection. This implies that any point off  $\mathcal{Q}$  which is on a tangent is on exactly two.  $\square$

When  $q$  is even, the tangents to a  $(q + 1)$ -arc behave in an unexpected fashion.

**6.4.2 Lemma.** *Let  $\mathbb{F}$  be the field of order  $q$ , where  $q$  is even, and let  $\mathcal{Q}$  be a  $(q + 1)$ -arc in  $\mathbb{P}(2, \mathbb{F})$ . Then the tangents to  $\mathcal{Q}$  are concurrent. Thus there is one point which lies on all tangents to  $\mathcal{Q}$ , and the remaining points off  $\mathcal{Q}$  all lie on exactly one tangent.*

*Proof.* Let  $P$  and  $Q$  be two distinct points on  $\mathcal{Q}$ . Since the number of points in the oval is odd, each point on the line  $PQ$  which is not on  $\mathcal{Q}$  must lie on a tangent to it. As  $P$  and  $Q$  both lie on tangents, it follows that each point on  $PQ$  is on a tangent. The number of tangents to  $\mathcal{Q}$  is  $q + 1$  and the number of points on  $PQ$  is also  $q + 1$ . Thus each point on a secant to  $\mathcal{Q}$  is on a unique tangent. Now let  $K$  be the point of intersection of two tangents which do not meet on  $\mathcal{Q}$ . Then  $K$  cannot lie on any secant, and so all lines through  $K$  are tangents to  $\mathcal{Q}$ .  $\square$

The point  $K$  is called the *nucleus* or *knot* of the oval. The oval, together with its nucleus forms a  $(q + 2)$ -arc. A  $(q + 2)$ -arc is sometimes called a *hyperoval*. Since we can delete any point from a hyperoval to obtain an oval, a given oval can thus be used to form a number of distinct ovals. In particular, if we start with a conic in a Pappian plane of even order, we can construct  $(q + 1)$ -arcs which are not conics.

## 6.5 Segre's Characterisation of Conics

B. Segre proved that, if  $q$  is odd, any  $(q + 1)$ -arc in the projective plane over  $GF(q)$  is a conic. We now present the proof of this important result. We first describe one property of  $(q + 1)$ -arcs in projective planes over fields of odd order.

**6.5.1 Lemma.** *Let  $\mathcal{Q}$  be a  $(q + 1)$ -arc in the projective plane over  $GF(q)$ , where  $q$  is odd. Let  $A_0, A_1$  and  $A_2$  be three distinct points on  $\mathcal{Q}$  and let  $l_0, l_1$  and  $l_2$  be the tangents at these three points. Then the triangle  $A_0A_1A_2$  is in perspective with the triangle formed by the points  $l_1 \cap l_2, l_0 \cap l_2$  and  $l_0 \cap l_1$ .*

*Proof.* Since  $PGL(3, \mathbb{F})$  is transitive on 3-arcs, we may take the points  $A_0, A_1$  and  $A_2$  to be represented by

$$(1, 0, 0)^T, (0, 1, 0)^T, (0, 0, 1)^T$$

respectively. The line  $A_0A_1$  can be represented by  $(0, 0, 1)$  and  $A_0A_2$  by  $(0, 1, 0)$ . Hence the tangent to  $\mathcal{Q}$  at  $A_0$  can be represented by a vector of the form

$$(0, 1, 0) - k_0(0, 0, 1) = (0, 1, -k_0)$$

Similarly the tangents at  $A_1$  and  $A_2$  are represented by  $(-k_1, 0, 1)$  and  $(1, -k_2, 0)$ . We will show that  $k_0k_1k_2 = -1$ , and then deduce the lemma from this. Let  $B$  be a point  $(b_0, b_1, b_2)^T$  on  $\mathcal{Q}$  distinct from  $A_0$ . The line  $A_0B$  can be taken to be represented by the vector

$$(0, 1, -h_0)$$

for some scalar  $h_0 = h_0(B)$ , and this scalar is non-zero if the line does not pass through  $A_1$ . Similarly, if  $B$  is distinct from  $A_1$ , the line  $A_1B$  can be represented by

$$(-h_1, 0, 1)$$

## 6. CONICS

---

and, if  $B$  is distinct from  $A_2$  then  $A_2B$  can be represented by

$$(1, -h_2, 0).$$

Since  $B$  lies on the lines represented by these three vectors, we find that

$$b_1 = h_0b_2, \quad b_2 = h_1b_0, \quad b_0 = h_2b_1.$$

This shows that if one coordinate of  $B$  is zero then all coordinates are zero. Hence none of  $b_0$ ,  $b_1$  and  $b_2$  is equal to zero, and this implies in turn that

$$h_0(B)h_1(B)h_2(B) = 1. \tag{6.5.1}$$

Conversely, if  $h$  is an element of  $\mathbb{F}$  different from 0 and  $k_0$  then the line represented by  $(0, 1, -h)$  passes through  $A_0$  and some point on  $\mathcal{Q}$  distinct from  $A_1$  and  $A_2$ . The product of the  $q - 1$  non-zero elements of  $\mathbb{F}$  is equal to  $-1$  and so the product of the parameters  $h_0(B)$  as  $B$  ranges over the points of  $\mathcal{Q}$  distinct from  $A_0$ ,  $A_1$  and  $A_2$  must be  $-1/k_0$ . It follows now using (6.5.1) that

$$\frac{(-1)^3}{k_0k_1k_2} = 1$$

and hence  $k_0k_1k_2 = -1$ , as claimed. The tangents at  $A_0$  and  $A_1$  meet at  $(1, k_0k_1, k_1)^T$  and the line joining this to  $A_2$  is represented by the vector

$$(k_0k_1, -1, 0).$$

The tangents at  $A_1$  and  $A_2$  meet at  $(k_2, 1, k_1k_2)$  and the line joining this to  $A_0$  is given by

$$(0, k_1k_2, -1).$$

The tangents at  $A_2$  and  $A_0$  meet at  $(k_0k_2, k_0, 1)$  and this joined to  $A_1$  by the line

$$(-1, 0, k_0k_2).$$

These three lines are concurrent, passing through the point  $(1, k_0k_1, -k_1)$ .  $\square$

**6.5.2 Theorem.** (Segre). *If  $q$  is odd then any  $(q + 1)$ -arc in the projective plane over  $GF(q)$  is a conic.*

*Proof.* We continue with the notation of the previous lemma. Since  $PGL(3, \mathbb{F})$  is transitive on ordered 4-arcs, we may assume without loss that the triangles of the lemma are in perspective from the point  $(1, 1, 1)^T$ , i.e., that  $k_0 = k_1 = k_2 = -1$ . Let  $B$  be a fourth point on  $\mathcal{Q}$  with coordinate vector  $(x_1, x_2, x_3)^T$  and tangent vector  $(l_0, l_1, l_2)$ . The line joining  $B$  to the intersection of the tangents at  $A_0$  and  $A_1$  has coordinate vector of the form

$$\alpha_0(0, 1, 1) + \beta_0(1, 0, 1).$$

Since this line passes through  $B$  we may take  $\alpha = x_0 + x_2$  and  $\beta = -(x_1 + x_2)$ . Similarly the line through  $A_0$  and the intersection of the tangents at  $A_1$  and  $B$  can be taken to have coordinate vector

$$l_0(1, 0, 1) - (l_0, l_1, l_2)$$

while the line joining  $A_1$  to the intersection of the tangents at  $B$  and  $A_0$  has coordinate vector

$$(l_0, l_1, l_2) - l_1(0, 1, 1).$$

Since these three coordinate vectors represent concurrent lines, they are linearly dependent. Since the tangents at  $A_0$ ,  $A_1$  and  $B$  are not concurrent, they are linearly independent. Since we have the former written as linear combinations of the latter, it follows that the matrix of coefficients

$$\begin{pmatrix} 0 & x_0 + x_2 & -(x_1 + x_2) \\ -1 & 0 & l_0 \\ 1 & -l_1 & 0 \end{pmatrix}$$

must have determinant zero. This implies that

$$l_1(x_1 + x_2) = l_0(x_0 + x_2).$$

The last identity was derived by working with the three points  $B$ ,  $A_0$  and  $A_1$ . If instead we use  $B$ ,  $A_1$  and  $A_2$  we obtain

$$l_2(x_0 + x_2) = l_1(x_0 + x_1).$$

Thus the respective ratios between  $l_0$ ,  $l_1$  and  $l_2$  are the same as the ratios between  $x_1 + x_2$ ,  $x_0 + x_2$  and  $x_0 + x_1$ . We also have

$$l_0x_0 + l_1x_1 + l_2x_2 = 0,$$

since  $B$  lies on the tangent to  $\mathcal{Q}$  at  $B$ . Hence we get

$$0 = (x_1 + x_2)x_0 + (x_0 + x_2)x_1 + (x_0 + x_1)x_2 = 2(x_0x_1 + x_1x_2 + x_0x_2).$$

Since our field has odd order, we can now divide this by two, and thus deduce that the points of  $\mathcal{Q}$  distinct from  $A_0$ ,  $A_1$  and  $A_2$  lie on the conic

$$x_0x_1 + x_1x_2 + x_0x_2 = 0.$$

It is trivial to check that  $A_0$ ,  $A_1$  and  $A_2$  lie on it too.  $\square$

More general results are known. Every  $q$ -arc in a projective plane over a field of odd order  $q \geq 5$  must be contained in a conic. (We present one proof of this in the next section. A more elementary proof will be found in Lüneburg.) In addition to its beauty, Segre's theorem has a number of important applications. We will meet some of these later. There do exist  $(q+1)$ -arcs in projective planes over fields of even order which are not related to conics. (See the Exercises for an example.)

## 6.6 $q$ -Arcs

Let  $\mathcal{K}$  be a  $k$ -arc in the projective plane over the field of order  $q$ . Then each point in the arc lies on

$$(q + 1) - (k - 1) = q + 2 - k$$

tangents to the arc. These tangents thus form a set of  $k(q + 2 - k)$  points in the dual space. We have the following result. A proof will be found in Hirschfeld [PGOFF].

**6.6.1 Theorem.** (Segre). *Let  $\mathcal{K}$  be a  $k$ -arc in the projective plane over the field of order  $q$ . Then the points in the dual plane corresponding to the tangents to the arc lie on a curve. This curve does not contain a point corresponding to a secant, and has degree  $q + 2 - k$  if  $q$  is even and degree  $2(q + 2 - k)$  if  $q$  is odd.  $\square$*

**6.6.2 Corollary.** (Segre). *Let  $\mathcal{K}$  be a  $q$ -arc in the projective plane over the field with order  $q$ , and let  $q$  be odd. Then  $\mathcal{K}$  is contained in a conic.*

*Proof.* We have already proved that every 3-arc is contained in a 4-arc, so we may assume that  $q > 3$ . By the theorem, there is a curve of degree four  $\mathcal{C}$  in the dual plane which contains the  $2q$  points corresponding to the tangents to  $\mathcal{K}$ , and none of the points corresponding to the secants. Let  $a$  be a point off  $\mathcal{K}$ . Since  $q$  is odd, the number of tangents to  $\mathcal{K}$  through  $a$  is odd. Suppose that  $a$  lies on at least five tangents to  $\mathcal{K}$ . The lines through  $a$  correspond to the points on a line  $\ell$  in the dual plane, and  $\ell$  meets  $\mathcal{C}$  in at least five points. Since  $\mathcal{C}$  has degree four, Bézout's theorem yields that  $\ell$  must be a component of  $\mathcal{C}$ . Thus all the points of  $\ell$  are on  $\mathcal{C}$ , and so none of the lines through  $a$  can be secants to  $\mathcal{K}$ . Therefore all the lines through  $a$  which meet  $\mathcal{K}$  are tangents, and so  $\mathcal{K} \cup a$  is a  $(q + 1)$ -arc. Since  $q$  is odd, all  $(q + 1)$ -arcs are conics by Theorem 5.2.

We can complete the proof by showing that for any  $q$ -arc, there is a point  $a$  on at least five tangents. If  $y \notin \mathcal{K}$ , let  $t_y$  be the number of tangents to  $\mathcal{K}$  through  $y$ . By counting the pairs  $(\ell, y)$ , where  $y$  is a point off  $\mathcal{K}$  and  $\ell$  is a tangent through  $y$ , we find that

$$\sum_{y \notin \mathcal{K}} t_y = 2q^2$$

and by counting the triples  $(\ell, \ell', y)$  where  $\ell$  and  $\ell'$  are distinct tangents and  $y = \ell \cap \ell'$ , we obtain

$$\sum_{y \notin \mathcal{K}} t_y(t_y - 1) = 2q(2q - 2).$$

Together these equations imply that

$$\sum_{y \notin \mathcal{K}} (t_y - 1)(t_y - 3) = (q - 1)(q - 3).$$

Since  $q$  is odd,  $t_y$  is odd for all points  $y$  not on  $\mathcal{K}$ . As  $q > 3$ , the last equation thus implies that  $t_y \geq 5$  for some point  $y$  not on  $\mathcal{K}$ .  $\square$

The above proof is an improvement on the original argument of Segre, due to Thas.