4

Various topics

This chapter collects some topics, any of which could be expanded into an entire chapter (or even a book!): spreads and translation planes; subsets of projective spaces; projective lines; and the simplicity of $\mathrm{PSL}(n,F)$.

4.1 Spreads and translation planes

Let V be a vector space over F, having even rank $2n$. A *spread* $\mathcal{S}$ is a set of subspaces of V of rank n, having the property that any non-zero vector of V lies in a unique member of $\mathcal{S}$. A trivial example occurs when $n = 1$ and $\mathcal{S}$ consists of all the rank 1 subspaces.

The importance of spreads comes from the following result, whose proof is straightforward.

Proposition 4.1 *Let $\mathcal{S}$ be a spread in V, and $\mathcal{L}$ the set of all cosets of members of $\mathcal{S}$. Then $(V,\mathcal{L})$ is an affine plane. The projective plane obtained by adding a line at infinity L_∞ is (p,L_∞)-transitive for all $p \in L_\infty$.* ■

For finite planes, the converse of the last statement is also true. An affine plane with the property that the projective completion is (p,L_∞)-transitive for all $p \in L_\infty$ is called a *translation plane*.

Example. Let K be an extension field of F with degree n. Take V to be a rank 2 vector space over K, and $\mathcal{S}$ the set of rank 1 K-subspaces. Then, of course, the resulting affine plane is $\mathrm{AG}(2,K)$. Now forget the K-structure, and regard V

as an F- vector space. Such a spread is called *Desarguesian*, because it can be recognised by the fact that the affine plane is Desarguesian.

Projectively, a spread is a set of $(n-1)$-dimensional flats in $\mathrm{PG}(2n-1,F)$, which partitions the points of F. We will examine further the case $n=1$, which will be considered again in section 4.5. **Assume that F is commutative.**

Lemma 4.2 *Given three pairwise skew lines in* $\mathrm{PG}(3,F)$*, there is a unique common transversal through any point on one of the lines.*

Proof Let L_1, L_2, L_3 be the lines, and $p \in L_1$. The quotient space by p is a projective plane $\mathrm{PG}(2,F)$, and $\Pi_1 = \langle p, L_2 \rangle$ and $\Pi_2 = \langle p, L_3 \rangle$ are distinct lines in this plane; they meet in a unique point, which corresponds to a line M containing p and lying in Π_1 and Π_2, hence meeting L_2 and L_3. ■

Now let $\mathcal{R}'$ be the set of common transversals to the three pairwise skew lines. The lines in $\mathcal{R}'$ are pairwise skew, by 4.2.

Lemma 4.3 *A common transversal to three lines of $\mathcal{R}'$ is a transversal to all of them.* ■

For the proof, see Exercise 2, or Section 8.4.

Let $\mathcal{R}$ be the set of all common transversals to $\mathcal{R}'$. The set $\mathcal{R}$ is called a *regulus*, and $\mathcal{R}'$ (which is also a regulus) is the *opposite regulus*. Thus, three pairwise skew lines lie in a unique regulus.

A spread is *regular* if it contains the regulus through any three of its lines.

Theorem 4.4 *A spread is Desarguesian if and only if it is regular.* ■

(The proof of the forward implication is given in Exercise 2.)

If we take a regular spread, and replace the lines in a regulus in this spread by those in the opposite regulus, the result is still a spread; for a regulus and its opposite cover the same set of points. This process is referred to as *derivation*. It gives rise to non-Desarguesian translation planes:

Proposition 4.5 *If $|F| > 2$, then a derivation of a regular spread is not regular.*

Proof Choose two reguli $\mathcal{R}_1$, $\mathcal{R}_2$ with a unique line in common. If we replace $\mathcal{R}_1$ by its opposite, then the regulus $\mathcal{R}_2$ contains three lines of the spread but is not contained in the spread. ■

It is possible to push this much further. For example, any set of pairwise disjoint reguli can be replaced by their opposites. I will not discuss this any further.

The concept of a spread of lines in $\mathrm{PG}(3,F)$ can be dualised. (For the rest of the section, F is not assumed commutative.) A set $\mathcal{S}$ of pairwise skew lines is called a *cospread* if every plane contains a (unique) line of $\mathcal{S}$; in other words, if $\mathcal{S}$ corresponds to a spread in the dual space $\mathrm{PG}(2,F^\circ)$. Call $\mathcal{S}$ a *bispread* if it is both a spread and a cospread.

If F is finite, then every spread is a bispread. (For there are equally many, viz. $(q+1)(q^2+1)$, points and planes; and a set of n pairwise skew lines accounts for $(q+1)n$ points and the same number of planes.) Moreover, a Desarguesian spread is a bispread; and any derivation of a bispread is a bispread (since the concept of a regulus is self-dual). The reader may be wondering if there are any spreads which are not bispreads! That they exist in profusion is a consequence of the next result (take $\mathcal{P}=\emptyset$), and gives us lots of strange translation planes.

Theorem 4.6 *Let F be an infinite field. Let $\mathcal{P}$, $\mathcal{Q}$ be sets of points and planes in $\mathrm{PG}(3,F)$, with the property that $|\mathcal{P}|+|\mathcal{Q}|<|F|$. Then there is a set $\mathcal{S}$ of pairwise skew lines, satisfying*

(a) the point p lies on a line of $\mathcal{S}$ if and only if $p\notin\mathcal{P}$;

(b) the plane Π contains a line of $\mathcal{S}$ if and only if $\Pi\notin\mathcal{Q}$.

Proof We use the fact that $\mathrm{PG}(2,F)$ is not the union of fewer than $|F|$ points and lines. For, if S is any set of fewer than $|F|$ points and lines, and L is a line not in S, then L is not covered by its intersections with members of S.

The proof is a simple transfinite induction. (Note that we are using the Axiom of Choice here; but, in any case, the proof is valid over any field which can be well-ordered, in particular, over any countable field.) For readers unfamiliar with set theory, assume that F is countable, delete the word "transfinite", and ignore comments about limit ordinals in the following argument.

Let α be the initial ordinal of cardinality $|F|$. Well-order the points of $\mathrm{PG}(3,F)$ not in $\mathcal{P}$ and the planes not in $\mathcal{Q}$ in a single sequence of order-type α, say $(X_\beta:\beta<\alpha)$. Construct a sequence $(\mathcal{S}_\beta:\beta<\alpha)$ by transfinite recursion, as follows.

Set $\mathcal{S}_0=\emptyset$.

Suppose that β is a successor ordinal, say $\beta=\gamma+1$. Suppose that X_β is a point (the other case is dual). If $\mathcal{S}_\gamma$ contains a line incident with X_β, then set $\mathcal{S}_\beta=\mathcal{S}_\gamma$. Suppose not. Consider the projective plane $\mathrm{PG}(3,F)/X_\beta$. By our initial remark,

this plane is not covered by fewer than α lines of the form $\langle L, X_\beta\rangle/X_\beta$ (for $L \in \mathcal{S}_\gamma$) or Π/X_β (for $\Pi \in \mathcal{Q}$ with $X_\beta \in \Pi$) and points $\langle p, X_\beta\rangle/X_\beta$ (for $p \in \mathcal{P}$). So we can choose a point lying outside the union of these points and lines, that is, a line L_β containing X_β so that $L_\beta \cap L = \emptyset$ (for $L \in \mathcal{S}_\gamma$), $L_\beta \notin \Pi$ (for $\Pi \in \mathcal{Q}$), and $p \notin L_\beta$ (for $p \in \mathcal{P}$). Set $\mathcal{S}_\beta = \mathcal{S}_\gamma \cup \{L_\beta\}$.

If β is a limit ordinal, set

$$\mathcal{S}_\beta = \bigcup_{\gamma<\beta} \mathcal{S}_\gamma.$$

Then $\mathcal{S}_\alpha$ is the required set of lines. ■

Exercises

1. Show that, if three pairwise skew lines in $\mathrm{PG}(3,F)$ are given, then it is possible to choose coordinates so that the lines have equations

$x_1 = x_2 = 0$;

$x_3 = x_4 = 0$;

$x_3 = x_1$, $x_4 = x_2$.

Find the common transversals to these three lines.

2. Now let F be commutative. Show that the common transversals to any three of the lines found in the last question are the original three lines and the lines with equations

$x_1 = x_3\alpha$, $x_2 = x_4\alpha$

for $\alpha \in F$, $\alpha \neq 0, 1$.

Deduce that the Desarguesian spread defined by a quadratic extension of F is regular.

3. Prove that Lemma 4.3 is valid in $\mathrm{PG}(3,F)$ if and only if F is commutative.

4. Use Theorem 4.6 to show that, if F is an infinite field, then there is a spread of lines in $\mathrm{AG}(3,F)$ which contains one line from each parallel class.

4.2 Some subsets of projective spaces

For most of the second half of these lecture notes, we will be considering subsets of projective spaces which consist of the points (and general subspaces) on

which certain forms vanish identically. In this section, I will describe some more basic subsets of projective spaces, and how to recognise them by their intersections with lines. The first example is a fact we have already met.

Proposition 4.7 *(a) A set S of points in a projective space is a subspace if and only if, for any line L, S contains no point, one point, or all points of L.*

(b) A set S of points in a projective space is a hyperplane if and only if, for any line L, S contains one or all points of L. ■

The main theorem of this section is a generalisation of Proposition 4.7(a). What if we make the condition symmetric, that is, ask that S contains none, one, all but one, or all points of any line L? The result is easiest to state in the finite case:

Theorem 4.8 *Let S be a set of points of $X = \mathrm{PG}(n,F)$ such that, for any line L, S contains none, one, all but one, or all points of S. Suppose that $|F| > 2$. Then there is a chain*

$$\emptyset = X_0 \subset X_1 \subset \ldots \subset X_m = X$$

of subspaces of X, such that either $S = \bigcup_{i\geq 0}(X_{2i+1} \setminus X_{2i})$, or $S = \bigcup_{i\geq 0}(X_{2i+2} \setminus X_{2i+1})$.

The hypothesis that $|F| > 2$ is necessary: over the field $\mathrm{GF}(2)$, a line has just three points, so the four possibilities listed in the hypothesis cover all subsets of a line. This means that any subset of the projective space satisfies the hypothesis! (Nevertheless, see Theorem 4.10 below.)

Note that the hypothesis on S is "self-complementary", and the conclusion must reflect this. It is more natural to talk about a colouring of the points with two colours such that each colour class satisfies the hypothesis of the theorem. In this language, the result can be stated as follows.

Theorem 4.9 *Let the points of a (possibly infinite) projective space X over F be coloured with two colours c_1 and c_2, such that every colour class contains none, one, all but one, or all points of any line. Suppose that $|F| > 2$. Then there is a chain $\mathcal{C}$ of subspaces of X, and a function $f : \mathcal{C} \to \{c_1, c_2\}$, so that*

(a) $\bigcup \mathcal{C} = X$;

(b) for $Y \in \mathcal{C}$, there exist points of Y lying in no smaller subspace in $\mathcal{C}$, and all such points have colour $f(Y)$.

The proof proceeds in a number of stages.

Step 1 The result is true for a projective plane (Exercise 1).

Now we define four relations $<_1$, $<_2$, $<$, $\|$ on X, as follows:

- $p <_1 q$ if p is the only point of its colour on the line pq; (this relation or its converse holds between p and q if and only if p and q have different colours);
- $p <_2 q$ if there exists q with $p <_1 r$ and $r <_1 q$ (this holds only if p and q have the same colour);
- $p < q$ if $p <_1 q$ or $p <_2 q$;
- $p \| q$ if neither $p < q$ nor $q < p$ (this holds only if p and q have the same colour).

Step 2 There do not exist points p, q with $p <_2 q$ and $q <_2 p$.

For, if so, then (with $p_1 = p$, $q_1 = q$) there are points p_2, q_2 such that

$$p_1 <_1 p_2 <_1 q_1 <_1 q_2 <_2 p_1.$$

Let c_i be the colour of p_i and q_i, $i = 1, 2$. By Step 1, the colouring of the plane $p_1p_2q_1$ is determined; and every point of this plane off the line p_1p_2. In particular, if $x_1 \in p_1q_1$, $x_1 \neq p_1, q_1$, then every point of x_1p_2 except p_2 has colour c_1. Similarly, every point of x_1q_2 except q_2 has colour c_1; and then every point of x_1x_2 except x_2 has colour c_1, where $x_2 \in p_2q_2$, $x_2 \neq p_2, q_2$.

But, by the same argument, every point of x_1x_2 except x_1 has colour c_2, giving a contradiction.

Step 3 $<$ is a partial order.

The antisymmetry follows by definition for $<_1$ and by Step 2 for $<_2$; we must prove transitivity. So suppose that $p < q < r$, and consider cases. If $p <_1 q <_1 r$, then $p <_2 r$ by definition. If $p <_1 q <_2 r$ or $p <_2 q <_1 r$, then p and r have different colours and so are comparable; and $r <_1 p$ contradicts Step 2. Finally, if $p <_2 q <_2 r$, then $p <_1 s <_1 q$ for some s; then $s <_1 r$, so that $p <_2 r$.

Step 4 If $p < q \| r$ or $p \| q < r$, then $p < r$; and if $p \| q \| r$, then $p \| r$.

Suppose that $p < q \| r$. If $p <_1 q$, then p and r have different colours and so are comparable; and $r <_1 p$ would imply $r < q$ by Step 3, so $p <_1 r$. The next case is similar. The last assertion is a simple consequence of the other two.

Step 5 If $p < q$, then $p < r$ for all points r of pq except p; and the points of pq other than p are pairwise incomparable.

This holds by assumption if $p <_1 q$, and by the proof of Step 2 if $p <_2 q$.

Now let $S(p) = \{q : p \not< q\}$, and $T(p) = \{q : q < p\}$.

Step 6 $S(p)$ and $T(p)$ are subspaces, with $p \in S(p) \setminus T(p)$. Moreover, $T(p)$ is the union of the spaces $S(q)$ for $q < p$, and is spanned by the points of $S(p)$ with colour different from that of p; and we have

$p \| q$ implies $S(p) = S(q)$;

$q < p$ implies $S(q) \subseteq T(p)$.

All of this follows by straightforward argument from the preceding steps.

Now the proof of the Theorem follows: we set $\mathcal{C} = \{S(p) : p \in X\}$, and let $f(S(p))$ be the colour of p. The conclusions of the Theorem follow from the assertions in Step 6. ■

Remark. The only place in the above argument where the hypothesis $|F| > 2$ was used was in Step 1. Now $\mathrm{PG}(2,2)$ has seven points; so, up to complementation, a subset of $\mathrm{PG}(2,2)$ is empty, a point, a line with a point removed, a line, or a triangle. Only the last case fails to satisfy the conclusion of the Theorem. So we have the following result:

Theorem 4.10 *The conclusions of Theorems 4.8 and 4.9 remain true in the case $F = \mathrm{GF}(2)$ provided that we add the extra hypothesis that no colour class intersects a plane in a triangle (or, in 4.8, that no plane meets S in a triangle or the complement of one).* ■

Exercise

1. Prove that Theorem 4.8 holds in any projective plane of order greater than 2 (not necessarily Desarguesian).

4.3 Segre's Theorem

For projective geometries over finite fields, it is very natural to ask for characterisations of interesting sets of points by hypotheses on their intersections with

lines. Very much finer discriminations are possible with finite than with infinite cardinal numbers; for example, all infinite subsets of a countably infinite set whose complements are also infinite are alike.

It is not my intention to survey even a small part of this vast literature. But I will describe one of the earliest and most celebrated results of this kind. I begin with some generalities about algebraic curves. Assume that F is a *commutative* field.

If a polynomial f in $x_1,\ldots,x_{n+1}$ is *homogeneous*, that is, a sum of terms all of the same degree, then $f(\mathbf{v})=0$ implies $f(\alpha\mathbf{v})=0$ for all $\alpha\in F$. So, it f vanishes at a non-zero vector, then it vanishes at the rank 1 subspace (the point of $\mathrm{PG}(n,F)$) it spans. The *algebraic variety* defined by f is the set of points spanned by zeros of f. We are concerned here only with the case $n=2$, in which case (assuming that f does not vanish identically) this set is called an *algebraic curve*.

Now consider the case where f has degree 2, and $F=\mathrm{GF}(q)$, where q is an *odd* prime power. The curve it defines may be a single point, or a line, or two lines; but, if none of these occurs, then it is equivalent (under the group $\mathrm{PGL}(3,q)$) to the curve defined by the equation $x_1^2+x_2^2+x_3^2=0$ (see Exercise 1). Any curve equivalent to this one is called a *conic* (or *irreducible conic*).

It can be shown (see Exercise 2) that a conic has $q+1$ points, no three of which are collinear. The converse assertion is the content of Segre's Theorem:

Theorem 4.11 (Segre's Theorem) *For q odd, a set of $q+1$ points in $\mathrm{PG}(2,q)$, with no three collinear, is a conic.*

Proof Let $\mathcal{O}$ be an oval. We begin with some combinatorial analysis which applies in any plane of odd order; then we introduce coordinates.

Step 1 Any point not on $\mathcal{O}$ lies on 0 or 2 tangents.

Proof Let p be a point not on $\mathcal{O}$. Since $|\mathcal{O}|=q+1$ is even, and an even number of points lie on secants through p, an even number must lie on tangents also. Let x_i be the number of points outside $\mathcal{O}$ which lie on i tangents. Now we have

$$\begin{aligned}\sum x_i &= q^2,\\ \sum ix_i &= (q+1)q,\\ \sum i(i-1)x_i &= (q+1)q.\end{aligned}$$

(These are all obtained by double counting. The first holds because there are q^2 points outside $\mathcal{O}$; the second because there are $q+1$ tangents (one at each point

of O), each containing q points not on O; and the third because any two tangents intersect at a unique point outside O.)

From these equations, we see that $\sum i(i-2)x_i = 0$. But the term $i = 1$ in the sum vanishes (any point lies on an even number of tangents); the terms $i = 0$ and $i = 2$ clearly vanish, and $i(i-2) > 0$ for any other value of i. So $x_i = 0$ for all $i \neq 0$ or 2, proving the assertion.

Remark Points not on O are called *exterior points* or *interior points* according as they lie on 2 or 0 tangents, by analogy with the real case. But the analogy goes no further. In the real case, every line through an interior point is a secant; this is false for finite planes.

Step 2 The product of all the non-zero elements of $\mathrm{GF}(q)$ is equal to -1.

Proof The solutions of the quadratic $x^2 = 1$ are $x = 1$ and $x = -1$; these are the only elements equal to their multiplicative inverses. So, in the product of all the non-zero elements, everything except 1 and -1 pairs off with its inverse, leaving these two elements unpaired.

For the next two steps, note that we can choose the coordinate system so that the sides of a given triangle have equations $x = 0$, $y = 0$ and $z = 0$ (and the opposite vertices are $[1,0,0]$, $[0,1,0]$, and $[0,0,1]$ respectively). We'll call this the *triangle of reference.*

Step 3 Suppose that concurrent lines through the vertices of the triangle of reference meet the opposite sides in the points $[0,1,a]$, $[b,0,1]$, and $[1,c,0]$. Then $abc = 1$.

Proof The equations of the concurrent lines are $z = ay$, $x = bz$ and $y = cx$ respectively; the point of concurrency must satisfy all three equations, whence $abc = 1$.)

Remark This result is equivalent to the classical Theorem of Menelaus.

Step 4 Let the vertices of the triangle of reference be chosen to be three points of O, and let the tangents at these points have equations $z = ay$, $x = bz$ and $y = cx$ respectively. Then $abc = -1$.

Proof There are $q-2$ further points of $\mathcal{O}$, say $p_1,\dots,p_{q-2}$. Consider the point $[1,0,0]$. It lies on the tangent $z=ay$, meeting the opposite side in $[0,1,a]$; two secants which are sides of the triangle; and $q-2$ further secants, through $p_1,\dots,p_{q-2}$. Let the secant through p_i meet the opposite side in $[0,1,a_i]$. Then $a\prod_{i=1}^{q-2}a_i=-1$, by Step 2. If b_i,c_i are similarly defined, we have also $b\prod_{i=1}^{q-2}b_i=c\prod_{i=1}^{q-2}c_i=-1$. Thus

$$abc\prod_{i=1}^{q-2}(a_ib_ic_i)=-1.$$

But, by Step 3, $a_ib_ic_i=1$ for $i=1,\dots,q-2$; so $abc=-1$.

Step 5 Given any three points p,q,r of $\mathcal{O}$, there is a conic $\mathcal{C}$ passing through p,q,r and having the same tangents at these points as does $\mathcal{O}$.

Proof Choosing coordinates as in Step 4, the conic with equation

$$yz-czx+caxy=0$$

can be checked to have the required property. (For example, $[1,0,0]$ lies on this conic; and, putting $z=ay$, we obtain $ay^2=0$, so $[1,0,0]$ is the unique point of the conic on this line.)

Step 6 Now we are finished if we can show that the conic $\mathcal{C}$ of Step 5 passes through an arbitrary further point s of $\mathcal{O}$.

Proof Let $\mathcal{C}'$ and $\mathcal{C}''$ be the conics passing through p,q,s and p,r,s respectively and having the correct tangents there. Let the conics $\mathcal{C}$, $\mathcal{C}'$ and $\mathcal{C}''$ have equations $f=0$, $f'=0$, $f''=0$ respectively. (These equations are determined up to a constant factor.) Let L_p,L_q,L_r,L_s be the tangents to $\mathcal{O}$ at p,q,r,s respectively. Since all three conics are tangent to L_p at p, we can choose the normalisation so that f,f',f'' agree identically on L_p.

Now consider the restrictions of f' and f'' to L_s. Both are quadratic functions having a double zero at s, and the values at the point $L_s\cap L_p$ coincide; so the two functions agree identically on L_s. Similarly, f and f' agree on L_q, and f and f'' agree on L_r. But then f, f' and f'' all agree at the point $L_q\cap L_r$. So the quadratic functions f' and f'' agree on L_p, L_s, and $L_q\cap L_r$, which forces them to be equal. So the three conics coincide, and our claim is proved (and with it Segre's Theorem). ∎

The argument in the last part of the proof can be generalised to give the following result (of which it forms the case $n = q+1$, $m = 2$, with $L_1, \ldots, L_n$ the tangents to the oval, and $\{p_{i1}, p_{i2}\}$ the point of tangency of L_i taken with multiplicity 2).

Proposition 4.12 *Let $L_1, \ldots, L_n$ be lines in $\mathrm{PG}(2,q)$, no three concurrent. Let $p_{i1}, \ldots, p_{im}$ be points of L_i, not necessarily distinct, but lying on none of the other $L_{i'}$. Suppose that, for any three of the lines, there is an algebraic curve of degree m whose intersections with those lines are precisely the specified points (counted with the appropriate multiplicity). Then there is a curve of degree m, meeting each line in just the specified points.* ■

Proposition 4.12 has been generalised [32] to arbitrary sets of lines (without the assumption that no three are concurrent).

Proposition 4.13 *Let $L_1, \ldots, L_n$ be lines in $\mathrm{PG}(2,q)$. Let $p_{i1}, \ldots, p_{im}$ be points of L_i, not necessarily distinct, but lying on none of the other $L_{i'}$. Suppose that, for any three of the lines which form a triangle, and for the set of all lines passing through any point of the plane (whenever there are at least three such lines), there is an algebraic curve of degree m whose intersections with those lines are precisely the specified points (counted with the appropriate multiplicity). Then there is a curve of degree m, meeting each line in just the specified points.* ■

The analogue of Segre's Theorem over $\mathrm{GF}(q)$ with even q is false. In this case, the tangents to an oval S all pass through a single point n, the *nucleus* of the oval (Exercise 4); and, for any $p \in S$, the set $S \cup \{n\} \setminus \{p\}$ is also an oval. But, if $q > 4$, then at most one of these ovals can be a conic (see Exercise 5: these ovals have q common points). For sufficiently large q (viz., $q \geq 64$), and also for $q = 16$, there are other ovals, not arising from this construction. We refer to [3] or [14] for up-to-date information on ovals in planes of even order.

We saw that there are ovals in infinite projective planes which are not conics. However, there is a remarkable characterisation of conics due to Buekenhout. A hexagon is said to be *Pascalian* if the three points of intersection of opposite sides are collinear. In this terminology, Pappus' Theorem asserts that a hexagon whose vertices lie alternately on two lines is Pascalian. Since a pair of lines forms a "degenerate conic", this theorem is generalised by Pascal's Theorem:

Theorem 4.14 (Pascal's Theorem) *In a Pappian projective plane, a hexagon inscribed in a conic is Pascalian.* ■

We know from Theorem 2.3 that a projective plane satisfying Pappus' Theorem is isomorphic to $\mathrm{PG}(2,F)$ for a commutative field F. The theorem of Buekenhout completes this circle of ideas. Its proof is group-theoretic, using a characterisation of $\mathrm{PGL}(2,F)$ as sharply 3-transitive group due to Tits.

Theorem 4.15 (Buekenhout's Theorem) *Let S be an oval in a projective plane Π. Suppose that every hexagon with vertices in S is Pascalian. Then Π is isomorphic to $\mathrm{PG}(2,F)$ for some commutative field F, and S is a conic in Π.* ■

Exercises

1. (a) By completing the square, prove that any homogeneous polynomial of degree 2 in n variables, over a commutative field F with characteristic different from 2, is equivalent (by non-singular linear transformation) to the polynomial

$$\alpha_1 x_1^2 + \ldots + \alpha_n x_n^2.$$

(b) Prove that multiplication of any α_i in the above form by a square in F gives an equivalent form.

(c) Now let $F = \mathrm{GF}(q)$ and $n = 3$; let η be a fixed nonsquare in F. Show that the curves defined by x_1^2, $x_1^2 - x_2^2$ and $x_1^2 - \eta x_2^2$ are respectively a line, two lines, and a point. Show that there exists α such that $\eta = 1 + \alpha^2$. Observing that

$$(x+\alpha y)^2 + (\alpha x - y)^2 = \eta(x^2+y^2),$$

prove that the forms $x_1^2 + x_2^2 + x_3^2$ and $x_1^2 + \eta x_2^2 + \eta x_3^2$ are equivalent. Deduce the classification of curves of degree 2 over $\mathrm{GF}(q)$ given in the text.

2. Count the number of secants through an exterior point and through an interior point of an oval in a projective plane of odd order q. Also, count the number of points of each type.

3. Prove that a curve of degree 2 over any commutative field is empty, a point, a line, a pair of lines, or an oval. Prove also that a curve of degree 2 over a finite field is non-empty.

4. Prove that, if q is even, then the tangents to an oval in a projective plane of order q are concurrent. Deduce that there is a set of $q+2$ points with no three collinear, having no tangents (i.e., meeting every line in 0 or 2 points). (Removing any one of these points then gives an oval.)

Remark. A set of $n+2$ points in a plane of order n, no three collinear, is called a *hyperoval*.

5. Prove that, in any infinite projective plane, for any integer $k > 1$, there is a set of points meeting every line in exactly k points.

6. Prove that five points of $\mathrm{PG}(2,F)$, with no three collinear, are contained in a unique conic. (Take four of the points to be the standard set $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ and $(1,1,1)$; the fifth is $(1,\alpha,\beta)$, where α and β are distinct from one another and from 0 and 1.)

4.4 Ovoids and inversive planes

Ovoids are 3-dimensional analogues of ovals. They have added importance because of their connection with inversive planes, which are one-point extensions of affine planes. (The traditional example is the relation between the Riemann sphere and the "extended complex plane".)

Fields in this section are commutative.

An *ovoid* in $\mathrm{PG}(3,F)$ is a set O of points with the properties

(O1) no three points of O are collinear;

(O2) the tangents to O through a point of O form a plane pencil.

(If a set of points satisfies (O1), a line is called a *secant*, *tangent* or *passant* if it meets the set in 2, 1 or 0 points respectively. The plane containing the tangents to an ovoid at a point x is called the *tangent plane* at x.)

The classical examples of ovoids are the *elliptic quadrics*. Let $\alpha x^2+\beta x+\gamma$ be an irreducible quadratic over the field F. The elliptic quadric consists of the points of $\mathrm{PG}(3,F)$ whose coordinates (x_1,x_2,x_3,x_4) satisfy

$$x_1x_2+\alpha x_3^2+\beta x_3x_4+\gamma x_4^2=0.$$

The proof that these points do form an ovoid is left as an exercise.

Over finite fields, ovoids are rare. Barlotti and Panella showed the following analogue of Segre's theorem on ovals:

Theorem 4.16 *Any ovoid in* $\mathrm{PG}(3,q)$*, for q an odd prime power, is an elliptic quadric.* ■

For even q, just one further family is known, the *Suzuki–Tits ovoids*, which we will construct in Section 8.4.

An *inversive plane* is, as said above, a one-point extension of an affine plane. That is, it is a pair $(X, \mathcal{C})$, where X is a set of points, and $\mathcal{C}$ a collection of subsets of X called *circles*, satisfying

(I1) any three points lie in a unique circle;

(I2) if x, y are points and C a circle with $x \in C$ and $y \notin C$, then there is a unique circle C' satisfying $y \in C'$ and $C \cap C' = \{x\}$;

(I3) there exist four non-concircular points.

It is readily checked that, for $x \in X$, the points different from x and circles containing x form an affine plane. The *order* of the inversive plane is the (common) order of its derived affine planes.

Proposition 4.17 *The points and non-trivial plane sections of an ovoid form an inversive plane.*

Proof A plane section of the ovoid O is non-trivial if it contains more than one point. Any three points of O are non-collinear, and so define a unique plane section. Given x, the points of O different from x and the circles containing x correspond to the lines through x not in the tangent plane T_x and the planes through x different from T_x; these are the points of the quotient space not incident with the line T_x/x and the lines different from T_x/x, which form an affine plane. ■

An inversive plane arising from an ovoid in this way is called *egglike*. Dembowski proved:

Theorem 4.18 *Any inversive plane of even order is egglike (and so its order is a power of 2).* ■

This is not known to hold for odd order, but no counterexamples are known.

There are configuration theorems (the *bundle theorem* and *Miquel's theorem* respectively) which characterise egglike inversive planes and "classical" inversive planes (coming from the elliptic quadric) respectively.

Higher-dimensional objects can also be defined. A set O of points of $\mathrm{PG}(n, F)$ is an *ovoid* if

(O1) no three points of O are collinear;

(O2') the tangents to $\mathcal{O}$ through a point x of $\mathcal{O}$ are all the lines through x in a hyperplane of $\mathrm{PG}(n,F)$.

Proposition 4.19 *If F is finite and $n \geq 4$, then $\mathrm{PG}(n,F)$ contains no ovoid.* ∎

However, there can exist such ovoids over infinite fields (Exercise 3).

Exercises

1. Prove Proposition 4.19. [Hint: it suffices to prove it for $n = 4$.]

2. Prove that, for q odd, a set of points in $\mathrm{PG}(3,q)$ which satisfies (O1) has cardinality at most q^2+1, with equality if and only if it is an ovoid.

(This is true for q even, $q > 2$ also, though the proof is much harder. For $q = 2$, the complement of a hyperplane is a set of 8 points in $\mathrm{PG}(3,2)$ satisfying (O1).)

3. Show that the set of points of $\mathrm{PG}(n,\mathbb{R})$ whose coordinates satisfy

$$x_1x_2 + x_3^2 + \ldots + x_n^2 = 0$$

is an ovoid.

4.5 Projective lines

A projective line over a field F has no non-trivial structure as an incidence geometry. From the Kleinian point of view, though, it does have geometric structure, derived from the fact that the group $\mathrm{PGL}(2,F)$ operates on it. As we saw earlier, the action of this group is 3-transitive (sharply so if F is commutative), and can even be 4-transitive for special skew fields of characteristic 2. However, we assume in this section that the field is commutative.

It is conventional to label the points of the projective line over F with elements of $F \cup \{\infty\}$, as follows: the point $\langle(1,\alpha)\rangle$ is labelled by α, and the point $\langle(0,1)\rangle$ by ∞. (If we regard points of $\mathrm{PG}(2,F)$ as lines in the affine plane $\mathrm{AG}(2,F)$, then the label of a point is the slope of the corresponding line.)

Since $\mathrm{PGL}(2,F)$ is sharply 3-transitive, distinguishing three points must give unique descriptions to all the others. This is conveniently done by means of the *cross ratio*, the function from 4-tuples of distinct points to $F \setminus \{0,1\}$, defined by

$$f(x_1,x_2,x_3,x_4) = \frac{(x_1-x_3)(x_4-x_2)}{(x_1-x_4)(x_3-x_2)}.$$

In calculating cross ratio, we use the same conventions for dealing with ∞ as when elements of $\mathrm{PGL}(2,F)$ are represented by linear fractional transformations; for example, $\infty - \alpha = \infty$, and $\alpha\infty/\beta\infty = \alpha/\beta$. Slightly differing forms of the cross ratio are often used; the one given here has the property that $f(\infty,0,1,\alpha) = \alpha$.

Proposition 4.20 *The group of permutations of* $\mathrm{PG}(1,F)$ *preserving the cross ratio is* $\mathrm{PGL}(2,F)$.

Proof Calculation establishes that linear fractional transformations do preserve cross ratio. Also, the cross ratio as a function of its fourth argument, with the first three fixed, is one-to-one, so a permutation which preserves cross ratio and fixes three points is the identity. The result follows from these two assertions. ∎

The cross ratio of four points is unaltered if the arguments are permuted in two cycles of length 2: for example, $f(x_3,x_4,x_1,x_2) = f(x_1,x_2,x_3,x_4)$. These permutations, together with the identity, form a normal subgroup of index six in the symmetric group S_4. Thus, in general, six different values are obtained by permuting the arguments. If α is one of these values, the others are $1-\alpha$, $1/\alpha$, $(\alpha-1)/\alpha$, $1/(1-\alpha)$, and $\alpha/(\alpha-1)$. There are two special cases where the number of values is smaller, that is, where two of the six coincide. The relevant sets are $\{-1,2,\frac{1}{2}\}$, and $\{-\omega,-\omega^2\}$, where ω is a primitive cube root of unity. A quadruple of points is called *harmonic* if its cross ratios belong to the first set, *equianharmonic* if they belong to the second. The first type occurs over any field of characteristic different from 2, while the second occurs only if F contains primitive cube roots of 1. (But note that, if F has characteristic 3, then the two types effectively coincide: $-1 = 2 = \frac{1}{2}$, and the cross ratio of a harmonic quadruple is invariant under all permutations of its arguments!)

In the arguments below, we regard a "quadruple" as being an equivalence class of ordered quadruples (all having the same cross-ratio). So, for example, a harmonic quadruple (in characteristic different from 3) is a 4-set with a distinguished partition into two 2-sets.

Proposition 4.21 *Suppose that the characteristic of* F *is not equal to* 2. *Then the group of permutations which preserve the set of harmonic quadruples is* $\mathrm{P\Gamma L}(2,F)$.

Proof Again, any element of $\mathrm{P\Gamma L}(2,F)$ preserves the set of harmonic quadruples. To see the converse, note that $\mathrm{PGL}(2,F)$ contains a unique conjugacy class

of involutions having two fixed points, and that, if x_1, x_2 are fixed points and (x_3, x_4) a 2-cycle of such an involution, then $\{x_1, x_2, x_3, x_4\}$ is harmonic (and the disthinguished partition is $\{\{x_1, x_2\}, \{x_3, x_4\}\}$). Thus, these involutions can be reconstructed from the set of harmonic quadruples. So any permutation preserving the harmonic quadruples normalises the group G generated by these involutions. We see below that G is $\mathrm{PSL}(2, F)$ if F contains square roots of -1, or contains this group as a subgroup of index 2 otherwise. The normaliser of G is thus $\mathrm{P\Gamma L}(2, F)$, as required. ■

($\mathrm{PSL}(n, F)$ is the group induced on the projective space by the invertible linear transformations with determinant 1.)

We look further at the claim about G in the above proof. A *transvection* is a linear transformation g with all eigenvalues equal to 1, for which $\ker(g-1)$ has codimension 1. In our present case, any 2×2 upper unitriangular matrix different from the identity is a transvection. The collineation of projective space induced by a transvection is called an *elation*. An elation is characterised by the fact that its fixed points form a hyperplane, known as the *axis* of the elation. Dually, an elation fixes every line through a point, called the *centre* of the elation, which is incident with the axis. In the present case $n = 2$, the centre and axis of an elation coincide.

Proposition 4.22 *The elations in* $\mathrm{PGL}(2, F)$ *generate* $\mathrm{PSL}(2, F)$.

Proof The elations fixing a specified point, together with the identity, form a group which acts sharply transitively on the remaining points. Hence the group generated by the elations is 2-transitive. If $\alpha = -1 - 1/\beta$ and $\gamma = \alpha/\beta$, then

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix} = \begin{pmatrix} -1/\beta & 0 \\ 0 & -\beta \end{pmatrix},$$

so the two-point stabiliser in the group generated by all the elations contains that in $\mathrm{PSL}(2, F)$. But elations have determinant 1, and so the group they generate is a subgroup of $\mathrm{PSL}(2, F)$. So we have equality. ■

Now, if two distinct involutions have a common fixed point, then their product is a elation. Since all elations are conjugate, all can be realised in this way. Thus the group G in the proof of Proposition 4.21 contains all elations, and hence contains $\mathrm{PSL}(2, F)$.

We conclude with a different way of giving structure to the projective line. Suppose that E is a subfield of F. Then $\{\infty\} \cup E$ is a subset of the projective line $\{\infty\} \cup F$ having the structure (in any of the senses previously defined) of projective line over E. We call any image of this set under an element of $\mathrm{PGL}(2,F)$ a *circle*. Then any three points lie in a unique circle. The points and circles form an incidence structure which is an extension of the point-line structure of affine space $\mathrm{AG}(n,E)$, where n is the degree of F over E. (For consider the blocks containing ∞. On removing the point ∞, we can regard F as an E-vector space of rank n; E itself is an affine line, and the elements of $\mathrm{PGL}(2,F)$ fixing ∞ are affine transformations; so, for any circle C containing ∞, $C \setminus \{\infty\}$ is an affine line. Since three points lie in a unique circle, every affine line arises in this way.)

Sometimes, as we will see, this geometry can be represented as the points and plane sections of a quadric over E. the most familiar example is the Riemann sphere, which is the projective line over $\mathbb{C}$, and can be identified with a sphere in real 3-space so that the "circles" are plane sections.

4.6 Generation and simplicity

In this section, we extend to arbitrary rank the statement that $\mathrm{PSL}(n,F)$ is generated by elations, and show that this group is simple, except in two special cases.

As before, F is a commutative field.

Theorem 4.23 *For any $n \geq 2$, the group $\mathrm{PSL}(n,F)$ is generated by all elations.*

Proof We use induction on n, the case $n = 2$ having been settled by Proposition 4.22. The induction is based on the fact that, if W is a subspace of the axis of an elation g, then g induces an elation on the quotient projective space modulo W. Given $g \in \mathrm{PSL}(n,F)$, with $g \neq 1$, we have to express g as a product of elations. We may suppose that g fixes a point x. (For, if $xg = y \neq x$, and h is any elation mapping x to y, then gh^{-1} fixes x, and gh^{-1} is a product of elations if and only if g is.

By induction, we may multiply g by a product of elations (whose axes contain x) to obtain an element fixing every line through x; so we may assume that g itself does so. Considering a matrix representing g, and using the fact that $g \in \mathrm{PSL}(n,F)$, we see that g is an elation. ∎

Theorem 4.24 *Suppose that either $n \geq 3$, or $n = 2$ and $|F| > 3$. Then any non-trivial normal subgroup of $\mathrm{PGL}(n,F)$ contains $\mathrm{PSL}(n,F)$.*

Proof We begin with an observation — if N is a normal subgroup of G, and $g \in N$, $g_1 \in G$, then $[g,g_1] \in N$, where $[g,g_1] = g^{-1}g_1^{-1}gg - 1$ is the *commutator* of g and g_1 — and a lemma:

Lemma 4.25 *Under the hypotheses of Theorem 4.24, if $g \in \mathrm{PGL}(n,F)$ maps the point p_1 of $\mathrm{PG}(n-1,F)$ to the point p_2, then there exists $g_1 \in PGL(n,F)$ which fixes p_1 and p_2 and doesn't commute with g.*

Proof *Case 1*: $p_2 g = p_3 \neq p_2$. We can choose g_1 to fix p_1 and p_2 and move p_3. (If p_1, p_2, p_3 are not collinear, this is clear. If they are collinear, use the fact that $\mathrm{PGL}(2,F)$ is 3-transitive on the projective line, which has more than three points.

Case 2: $p_2 g = p_1$. Then g fixes the line $p_1 p_2$, and we can choose coordinates on this line so that $p_1 = \infty$, $p_2 = 0$. Now g acts as $x \mapsto \alpha/x$ for some $\alpha \in F$. Let g_1 induce $x \mapsto \beta x$ on this line; then $[g,g_1]$ induces $x \mapsto \beta^2 x$. So choose $\beta \neq 0, 1, -1$, as we may since $|F| > 3$. ■

So let N be a non-trivial subgroup of $\mathrm{PGL}(n,F)$. Suppose that $g \in N$ maps the hyperplane H_1 to $H_2 \neq H_1$. By the dual form of the Lemma, there exists g_1 fixing H_1 and H_2 and not commuting with g; then $[g,g_1]$ fixes H_2. So we may assume that $g \in N$ fixes a hyperplane H.

Next, suppose that g doesn't fix H pointwise. The group of elations with axis H is isomorphic to the additive group of a vector space whose associated projective space is H; so there is a transvection g_1 with axis H not commuting with g. Then $[g,g_1]$ fixes H pointwise. So we may assume that g fixes H pointwise.

If g is not an elation, then it is a *homology* (induced by a diagonalisable linear map with two eigenvalues, one having multiplicity $n-1$; equivalently, its fixed points form a hyperplane and one additional point). Now if g_1 is an elation with axis H, then $[g,g_1]$ is a non-identity elation.

We conclude that N contains an elation. But then N contains all elations (since they are conjugate), whence N contains $\mathrm{PSL}(n,F)$. ■

For small n and small finite fields $F = \mathrm{GF}(q)$, the group $\mathrm{PSL}(n,q) = \mathrm{PSL}(n,F)$ is familiar in other guises. For $n = 2$, recall that it is sharply 3-transitive of degree $q+1$. Hence we have $\mathrm{PSL}(2,2) \cong S_3$, $\mathrm{PSL}(2,3) \cong A_4$, and $\mathrm{PSL}(2,4) \cong A_5$ (the alternating groups of degrees 4 and 5 — the former is not simple, the latter is the unique simple group of order 60). Less obviously, $\mathrm{PSL}(2,5) \cong A_5$, since it is also simple of order 60. Furthermore, $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$ (the unique simple group of order 168), $\mathrm{PSL}(2,9) \cong A_6$, and $\mathrm{PSL}(4,2) \cong A_8$ (for reasons we will see later).

There has been a lot of work, much of it with a very geometric flavour, concerning groups generated by subsets of the set of elations. For example, McLaughlin [22, 23] found all irreducible groups generated by "full elation subgroups" (all elations with given centre and axis). This result was put in a wider context by Cameron and Hall [11]. (In particular, they extended the result to spaces of infinite dimension.) Note that an important ingredient in the arguments of Cameron and Hall is Theorem 4.9: under slight additional hypotheses, the set of all elation centres satisfies the conditions on a colour class in that theorem. The result of Theorem 4.9, together with the irreducibility of the group, then implies that every point is an elation centre.

Exercises

1. (a) Prove that the non-negative integer m is the number of fixed points of an element of $\mathrm{PGL}(n,q)$ if and only if, when written in the base q, its digits are non-decreasing and have sum not exceeding n.

(b) (Harder) Prove that the non-negative integer m is the number of fixed points of an element of $\mathrm{P\Gamma L}(n,F)$ if and only if there exists r such that q is a power of r and, when m is written in the base r, its digits are non-decreasing and have sum at most n.

2. Prove that a simple group of order 60 possesses five Sylow 2-subgroups, which it permutes by conjugation; deduce that such a group is isomorphic to A_5.

3. Modify the proof of Theorem 4.6.2 to show that, under the same hypotheses, $\mathrm{PSL}(n,F)$ is simple. [It is only necessary to show that the various g_1s can be chosen to lie in $\mathrm{PSL}(n,F)$. The only case where this fails is Case 2 of the Lemma when $n=2$, $F=\mathrm{GF}(5)$.]

4. (a) Let Π be a projective plane of order 4 containing a hyperoval X (six points, no three collinear). Prove that there are natural bijections between the set of lines meeting X in two points and the set of 2-subsets of X; and between the set of points outside X and the set of partitions of X into three 2-subsets. Find a similar description of a set bijective with the set of lines disjoint from X. Hence show that Π is unique (up to isomorphism).

(b) Let Π be a projective plane of order 4. Prove that any four points, no three collinear, are contained in a hyperoval. Hence show that there is a unique projective plane of order 4 (up to isomorphism).

(See Cameron and Van Lint [F] for more on the underlying combinatorial principle.)