2 Linear and projective groups

In this section, we define and study the general and special linear groups and their projective versions. We look at the actions of the projective groups on the points of the projective space, and discuss transitivity properties, generation, and simplicity of these groups.

2.1 The general linear groups

Let F be a division ring. As we saw, a vector space of rank n over F can be identified with the standard space F^n (with scalars on the left) by choosing a basis. Any invertible linear transformation of V is then represented by an invertible $n\times n$ matrix, acting on F^n by right multiplication.

We let $\mathrm{GL}(n,F)$ denote the group of all invertible $n\times n$ matrices over F, with the operation of matrix multiplication.

The group $\mathrm{GL}(n,F)$ acts on the projective space $\mathrm{PG}(n-1,F)$, since an invertible linear transformation maps a subspace to another subspace of the same dimension.

Proposition 2.1 *The kernel of the action of* $\mathrm{GL}(n,F)$ *on the set of points of* $\mathrm{PG}(n-1,F)$ *is the subgroup*

$$\{cI : c\in Z(F), c\neq 0\}$$

of central scalar matrices in F*, where* $Z(F)$ *denotes the centre of* F*.*

Proof Let $A=(a_{ij})$ be an invertible matrix which fixes every rank 1 subspace of F^n. Thus, A maps each non-zero vector $(x_1,\ldots,x_n)$ to a scalar multiple $(cx_1,\ldots,cx_n)$ of itself.

Let e_i be the ith basis vector, with 1 in position i and 0 elsewhere. Then $e_iA=c_ie_i$, so the ith row of A is c_ie_i. This shows that A is a diagonal matrix.

Now for $i\neq j$, we have

$$c_ie_i+c_je_j=(e_i+e_j)A=d(e_i+e_j)$$

for some d. So $c_i=c_j$. Thus, A is a diagonal matrix cI.

Finally, let $a\in F$, $a\neq 0$. Then

$$c(ae_1)=(ae_1)A=a(e_1A)=ace_1,$$

so $ac=ca$. Thus, $c\in Z(F)$. ■

Let Z be the kernel of this action. We define the *projective general linear group* $\mathrm{PGL}(n,F)$ to be the group induced on the points of the projective space $\mathrm{PG}(n-1,F)$ by $\mathrm{GL}(n,F)$. Thus,

$$\mathrm{PGL}(n,F) \cong \mathrm{GL}(n,F)/Z.$$

In the case where F is the finite field $\mathrm{GF}(q)$, we write $\mathrm{GL}(n,q)$ and $\mathrm{PGL}(n,q)$ in place of $\mathrm{GL}(n,F)$ and $\mathrm{PGL}(n,F)$ (with similar conventions for the groups we meet later). Now we can compute the orders of these groups:

Theorem 2.2 *(a)* $|\mathrm{GL}(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$*;*

(b) $|\mathrm{PGL}(n,q)| = |\mathrm{GL}(n,q)|/(q-1)$.

Proof (a) The rows of an invertible matrix over a field are linearly independent, that is, for $i = 1,\ldots,n$, the ith row lies outside the subspace of rank $i-1$ generated by the preceding rows. Now the number of vectors in a subspace of rank $i-1$ over $\mathrm{GF}(q)$ is q^{i-1}, so the number of choices for the ith row is $q^n - q^{i-1}$. Multiplying these numbers for $i = 1,\ldots,n$ gives the result.

(b) $\mathrm{PGL}(n,q)$ is the image of $\mathrm{GL}(n,q)$ under a homomorphism whose kernel consists of non-zero scalar matrices and so has order $q-1$. ■

If the field F is commutative, then the determinant function is defined on $n \times n$ matrices over F and is a multiplicative map to F:

$$\det(AB) = \det(A)\det(B).$$

Also, $\det(A) \neq 0$ if and only if A is invertible. So det is a homomorphism from $\mathrm{GL}(n,F)$ to F^*, the multiplicative group of F (also known as $\mathrm{GL}(1,F)$). This homomorphism is onto, since the matrix with c in the top left corner, 1 in the other diagonal positions, and 0 elsewhere has determinant c.

The kernel of this homomorphism is the *special linear group* $\mathrm{SL}(n,F)$, a normal subgroup of $\mathrm{GL}(n,F)$ with factor group isomorphic to F^*.

We define the *projective special linear group* $\mathrm{PSL}(n,F)$ to be the image of $\mathrm{SL}(n,F)$ under the homomorphism from $\mathrm{GL}(n,F)$ to $\mathrm{PGL}(n,F)$, that is, the group induced on the projective space by $\mathrm{SL}(n,F)$. Thus,

$$\mathrm{PSL}(n,F) = \mathrm{SL}(n,F)/(SL(n,F) \cap Z).$$

The kernel of this homomorphism consists of the scalar matrices cI which have determinant 1, that is, those cI for which $c^n = 1$. This is a finite cyclic group whose order divides n.

Again, for finite fields, we can calculate the orders:

Theorem 2.3 *(a)* $|\mathrm{SL}(n,q)| = |\mathrm{GL}(n,q)|/(q-1)$*;*

(b) $|\mathrm{PSL}(n,q)| = |\mathrm{SL}(n,q)|/(n,q-1)$*, where* $(n,q-1)$ *is the greatest common divisor of* n *and* $q-1$*.*

Proof (a) $\mathrm{SL}(n,q)$ is the kernel of the determinant homomorphism on $\mathrm{GL}(n,q)$ whose image F^* has order $q-1$.

(b) From the remark before the theorem, we see that $\mathrm{PSL}(n,q)$ is the image of $\mathrm{SL}(n,q)$ under a homomorphism whose kernel is the group of nth roots of unity in $\mathrm{GF}(q)$. Since the multiplicative group of this field is cyclic of order $q-1$, the nth roots form a subgroup of order $(n,q-1)$. ■

A group G acts *sharply transitively* on a set Ω if its action is regular, that is, it is transitive and the stabiliser of a point is the identity.

Theorem 2.4 *Let* F *be a division ring. Then the group* $\mathrm{PGL}(n,F)$ *acts transitively on the set of all* $(n+1)$*-tuples of points of* $\mathrm{PG}(n-1,F)$ *with the property that no* n *points lie in a hyperplane; the stabiliser of such a tuple is isomorphic to the group of inner automorphisms of the multiplicative group of* F*. In particular, if* F *is commutative, then* $\mathrm{PGL}(n,F)$ *is sharply transitive on the set of such* $(n+1)$*-tuples.*

Proof Consider n points not lying in a hyperplane. The n vectors spanning these points form a basis, and we may assume that this is the standard basis $e_1,\dots,e_n$ of F^n, where e_i has ith coordinate 1 and all others zero. The proof of Proposition 2.1 shows that G acts transitively on the set of such n-tuples, and the stabiliser of the n points is the group of diagonal matrices. Now a vector v not lying in the hyperplane spanned by any $n-1$ of the basis vectors must have all its coordinates non-zero, and conversely. Moreover, the group of diagonal matrices acts transitively on the set of such vectors. This proves that $\mathrm{PG}(n,F)$ is transitive on the set of $(n+1)$-tuples of the given form. Without loss of generality, we may assume that $v = e_1 + \cdots + e_n = (1,1,\dots,1)$. Then the stabiliser of the $n+1$ points consists of the group of scalar matrices, which is isomorphic to the multiplicative group F^*. We have seen that the kernel of the action on the projective space is $Z(F^*)$, so the group induced by the scalar matrices is $F^*/Z(F^*)$, which is isomorphic to the group of inner automorphisms of F^*. ■

Corollary 2.5 *The group* $\mathrm{PGL}(2,F)$ *is* 3*-transitive on the points of the projective line* $\mathrm{PG}(1,F)$*; the stabiliser of three points is isomorphic to the group of inner* *automorphisms of the multiplicative group of F. In particular, if F is commutative, then* $\mathrm{PGL}(2,F)$ *is sharply* 3*-transitive on the points of the projective line.*

For $n>2$, the group $\mathrm{PGL}(n,F)$ *is* 2*-transitive on the points of the projective space* $\mathrm{PG}(n-1,F)$.

This follows from the theorem because, in the projective plane, the hyperplanes are the points, and so no two distinct points lie in a hyperplane; while, in general, any two points are independent and can be extended to an $(n+1)$-tuple as in the theorem.

We can represent the set of points of the projective line as $\{\infty\}\cup F$, where $\infty=\langle(1,0)\rangle$ and $a=\langle(a,1)\rangle$ for $a\in F$. Then the stabiliser of the three points $\infty,0,1$ acts in the natural way on $F\setminus\{0,1\}$ by conjugation.

For consider the effect of the diagonal matrix aI on the point $\langle(x,1)\rangle$. This is mapped to $\langle(xa,a)\rangle$, which is the same rank 1 subspace as $\langle(a^{-1}xa,1)\rangle$; so in the new representation, aI induces the map $x\mapsto a^{-1}xa$.

In this convenient representation, the action of $\mathrm{PGL}(2,F)$ can be represented by linear fractional transformations. The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ maps $(x,1)$ to $(xa+c,xb+d)$, which spans the same point as $((xb+d)^{-1}(xa+c),1)$ if $xb+d\neq 0$, or $(1,0)$ otherwise. Thus the transformation induced by this matrix can be written as

$$x\mapsto (xb+d)^{-1}(xa+c),$$

provided we make standard conventions about ∞ (for example, $0^{-1}a=\infty$ for $a\neq 0$ and $(\infty b+d)^{-1}(\infty a+c)=b^{-1}a$. If F is commutative, this transformation is conveniently written as a fraction:

$$x\mapsto \frac{ax+c}{bx+d}.$$

Exercise 2.1 Work out carefully all the conventions required to use the linear fractional representation of $\mathrm{PGL}(2,F)$.

Exercise 2.2 By Theorem 2.4, the order of $\mathrm{PGL}(n,q)$ is equal to the number of $(n+1)$-tuples of points of $\mathrm{PG}(n-1,q)$ for which no n lie in a hyperplane. Use this to give an alternative proof of Theorem 2.2.

Paul Cohn constructed an example of a division ring F such that all elements of $F\setminus\{0,1\}$ are conjugate in the multiplicative group of F. For a division ring F with this property, we see that $\mathrm{PGL}(2,F)$ is 4-transitive on the projective line. This is the highest degree of transitivity that can be realised in this way.

Exercise 2.3 Show that, if F is a division ring with the above property, then F has characteristic 2, and the multiplicative group of F is torsion-free and simple.

Exercise 2.4 Let F be a commutative field. Show that, for all $n \geq 2$, the group $\mathrm{PSL}(n,F)$ is 2-transitive on the points of the projective space $\mathrm{PG}(n-1,F)$; it is 3-transitive if and only if $n = 2$ and every element of F is a square.

2.2 Generation

For the rest of this section, we assume that F is a commutative field. A *transvection* of the F-vector space V is a linear map $: V \to V$ which satisfies $\mathrm{rk}(T-I) = 1$ and $(T-I)^2 = 0$. Thus, if we choose a basis such that e_1 spans the image of $T-I$ and $e_1,\ldots.e_{n-1}$ span the kernel, then T is represented by the matrix $I+U$, where U has entry 1 in the top right position and 0 elsewhere. Note that a transvection has determinant 1. The *axis* of the transvection is the hyperplane $\ker(T-I)$; this subspace is fixed elementwise by T. Dually, the *centre* of T is the image of $T-I$; every subspace containing this point is fixed by T (so that T acts trivially on the quotient space).

Thus, a transvection is a map of the form

$$x \mapsto x + (xf)a,$$

where $a \in V$ and $f \in V^*$ satisfy $af = 0$ (that is, $f \in a^\dagger$). Its centre and axis are $\langle a \rangle$ and $\ker(f)$ respectively.

The transformation of projective space induced by a transvection is called an *elation*. The matrix form given earlier shows that all elations lie in $\mathrm{PSL}(n,F)$.

Theorem 2.6 *For any $n \geq 2$ and commutative field F, the group $\mathrm{PSL}(n,F)$ is generated by the elations.*

Proof We use induction on n.

Consider the case $n = 2$. The elations fixing a specified point, together with the identity, form a group which acts regularly on the remaining points. (In the linear fractional representation, this elation group is

$$\{x \mapsto x + a : a \in F\},$$

fixing ∞.) Hence the group G generated by the elations is 2-transitive. So it is enough to show that the stabiliser of the two points ∞ and 0 in G is the same as in $\mathrm{PSL}(2,F)$, namely

$$\{x \mapsto a^2 x : a \in F, a \neq 0\}.$$

Given $a \in F$, $a \neq 0$, we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a-a^2 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix},$$

and the last matrix induces the linear fractional map $x \mapsto ax/a^{-1} = a^2x$, as required.

(The proof shows that two elation groups, with centres ∞ and 0, suffice to generate $\mathrm{PSL}(2,F)$.)

Now for the general case, we assume that $\mathrm{PSL}(n-1,F)$ is generated by elations. Let G be the subgroup of $\mathrm{PSL}(n,F)$ generated by elations. First, we observe that G is transitive; for, given any two points p_1 and p_2, there is an elation on the line $\langle p_1, p_2 \rangle$ carrying p_1 to p_2, which is induced by an elation on the whole space (acting trivially on a complement to the line). So it is enough to show that the stabiliser of a point p is generated by elations. Take an element $g \in \mathrm{PSL}(n,F)$ fixing p.

By induction, G_p induces at least the group $\mathrm{PSL}(n-1,F)$ on the quotient space V/p. So, multiplying g by a suitable product of elations, we may assume that g induces an element on V/p which is diagonal, with all but one of its diagonal elements equal to 1. In other words, we can assume that g has the form

$$\begin{pmatrix} \lambda & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ x_1 & x_2 & \dots & x_{n-1} & \lambda^{-1} \end{pmatrix}.$$

By further multiplication by elations, we may assume that $x_1 = \ldots = x_{n-1} = 0$. Now the result follows from the matrix calculation given in the case $n = 2$.

Exercise 2.5 A *homology* is an element of $\mathrm{PGL}(n,F)$ which fixes a hyperplane pointwise and also fixes a point not in this hyperplane. Thus, a homology is represented in a suitable basis by a diagonal matrix with all its diagonal entries except one equal to 1.

(a) Find two homologies whose product is an elation.

(b) Prove that $\mathrm{PGL}(n,F)$ is generated by homologies.

2.3 Iwasawa's Lemma

Let G be a permutation group on a set Ω: this means that G is a subgroup of the symmetric group on Ω. Iwasawa's Lemma gives a criterion for G to be simple. We will use this to prove the simplicity of $\mathrm{PSL}(n,F)$ and various other classical groups.

Recall that G is *primitive* on Ω if it is transitive and there is no non-trivial equivalence relation on Ω which is G-invariant: equivalently, if the stabiliser G_α of a point $\alpha \in \Omega$ is a maximal subgroup of G. Any 2-transitive group is primitive.

Iwasawa's Lemma is the following.

Theorem 2.7 *Let G be primitive on Ω. Suppose that there is an abelian normal subgroup A of G_α with the property that the conjugates of A generate G. Then any non-trivial normal subgroup of G contains G'. In particular, if $G = G'$, then G is simple.*

Proof Suppose that N is a non-trivial normal subgroup of G. Then $N \not\leq G_\alpha$ for some α. Since G_α is a maximal subgroup of G, we have $NG_\alpha = G$.

Let g be any element of G. Write $g = nh$, where $n \in N$ and $h \in G_\alpha$. Then

$$gAg^{-1} = nhAh^{-1}n^{-1} = nAn^{-1},$$

since A is normal in G_α. Since N is normal in G we have $gAg^{-1} \leq NA$. Since the conjugates of A generate G we see that $G = NA$.

Hence

$$G/N = NA/N \cong A/(A \cap N)$$

is abelian, whence $N \geq G'$, and we are done. ■

2.4 Simplicity

We now apply Iwasawa's Lemma to prove the simplicity of $\mathrm{PSL}(n,F)$. First, we consider the two exceptional cases where the group is not simple.

Recall that $\mathrm{PSL}(2,q)$ is a subgroup of the symmetric group S_{q+1}, having order $(q+1)q(q-1)/(q-1,2)$.

(a) If $q = 2$, then $\mathrm{PSL}(2,q)$ is a subgroup of S_3 of order 6, so $\mathrm{PSL}(2,2) \cong S_3$. It is not simple, having a normal subgroup of order 3.

(b) If $q = 3$, then $\mathrm{PSL}(2,q)$ is a subgroup of S_4 of order 12, so $\mathrm{PSL}(2,3) \cong A_4$. It is not simple, having a normal subgroup of order 4.

(c) For comparison, we note that, if $q = 4$, then $\mathrm{PSL}(2,q)$ is a subgroup of S_5 of order 60, so $\mathrm{PSL}(2,4) \cong A_5$. This group is simple.

Lemma 2.8 *The group* $\mathrm{PSL}(n,F)$ *is equal to its derived group if* $n > 2$ *or if* $|F| > 3$.

Proof The group $G = \mathrm{PSL}(n,F)$ acts transitively on incident point-hyperplane pairs. Each such pair defines a unique elation group. So all the elation groups are conjugate. These groups generate G. So the proof will be concluded if we can show that some elation group is contained in G'.

Suppose that $|F| > 3$. It is enough to consider $n = 2$, since we can extend all matrices in the argument below to rank n by appending a block consisting of the identity of rank $n-2$. There is an element $a \in F$ with $a^2 \neq 0,1$. We saw in the proof of Theorem 2.6 that $\mathrm{SL}(2,F)$ contains the matrix $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$. Now

$$\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)x \\ 0 & 1 \end{pmatrix};$$

this equation expresses any element of the corresponding transvection group as a commutator.

Finally suppose that $|F| = 2$ or 3. As above, it is enough to consider the case $n = 3$. This is easier, since we have more room to manoeuvre in three dimensions: we have

$$\begin{pmatrix} 1 & -x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \quad \blacksquare$$

Lemma 2.9 *Let* Ω *be the set of points of the projective space* $\mathrm{PG}(n-1,F)$. *Then, for* $\alpha \in \Omega$, *the set of elations with centre* α, *together with the identity, forms an abelian normal subgroup of* G_α.

Proof This is more conveniently shown for the corresponding transvections in $\mathrm{SL}(n,F)$. But the transvections with centre spanned by the vector a consist of all maps $x \mapsto x + (xf)a,$, for $f \in A^\dagger$; these clearly form an abelian group isomorphic to the additive group of $a^\dagger$. $\blacksquare$

Theorem 2.10 *The group* $\mathrm{PSL}(n,F)$ *is simple if* $n > 2$ *or if* $|F| > 3$.

Proof let $G = \mathrm{PSL}(n,F)$. Then G is 2-transitive, and hence primitive, on the set Ω of points of the projective space. The group A of elations with centre α is an abelian normal subgroup of G_α, and the conjugates of A generate G (by Theorem 2.6, since every elation has a centre). Apart from the two excluded cases, $G = G'$. So G is simple, by Iwasawa's Lemma. ■

2.5 Small fields

We now have the family $\mathrm{PSL}(n,q)$, for $(n,q) \neq (2,2),(2,3)$ of finite simple groups. (The first two members are not simple: we observed that $\mathrm{PSL}(2,2) \cong S_3$ and $\mathrm{PSL}(2,3) \cong A_4$, neither of which is simple.) As is well-known, Galois showed that the alternating group A_n of degree $n \geq 5$ is simple.

Exercise 2.6 Prove that the alternating group A_n is simple for $n \geq 5$.

Some of these groups coincide:

Theorem 2.11 *(a)* $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$.

(b) $\mathrm{PSL}(2,7) \cong \mathrm{PSL}(3,2)$.

(c) $\mathrm{PSL}(2,9) \cong A_6$.

(d) $\mathrm{PSL}(4,2) \cong A_8$.

Proofs of these isomorphisms are outlined below. Many of the details are left as exercises. There are many other ways to proceed!

Theorem 2.12 *Let G be a simple group of order $(p+1)p(p-1)/2$, where p is a prime number greater than* 3. *Then $G \cong \mathrm{PSL}(2,p)$.*

Proof By Sylow's Theorem, the number of Sylow p-subgroups is congruent to 1 mod p and divides $(p+1)(p-1)/2$; also this number is greater than 1, since G is simple. So there are $p+1$ Sylow p-subgroups; and if P is a Sylow p-subgroup and $N = N_G(P)$, then $|N| = p(p-1)/2$.

Consider G acting as a permutation group on the set Ω of cosets of N. Let ∞ denote the coset N. Then P fixes ∞ and permutes the other p cosets regularly. So we can identify Ω with the set $\{\infty\} \cup \mathrm{GF}(p)$ such that a generator of P acts on Ω

as the permutation $x \mapsto x+1$ (fixing ∞). We see that N is permutation isomorphic to the group

$$\{x \mapsto a^2x+b : a,b \in \mathrm{GF}(p), a \neq 0\}.$$

More conveniently, elements of N can be represented as linear fractional transformations of Ω with determinant 1, since

$$a^2x+b = \frac{ax+a^{-1}b}{0x+a^{-1}}.$$

Since G is 2-transitive on Ω, N is a maximal subgroup of G, and G is generated by N and an element t interchanging ∞ and 0, which can be chosen to be an involution. If we can show that t is also represented by a linear fractional transformation with determinant 1, then G will be a subgroup of the group $\mathrm{PSL}(2,p)$ of all such transformations, and comparing orders will show that $G = \mathrm{PSL}(2,p)$.

We treat the case $p \equiv -1 \pmod 4$; the other case is a little bit trickier.

The element t must normalise the stabiliser of ∞ and 0, which is the cyclic group $C = \{x \mapsto a^2x\}$ of order $(p-1)/2$ (having two orbits of size $(p-1)/2$, consisting of the non-zero squares and the non-squares in $\mathrm{GF}(p)$). Also, t has no fixed points. For the stabiliser of three points in G is trivial, so t cannot fix more than 2 points; but the two-point stabiliser has odd order $(p-1)/2$. Thus t interchanges the two orbits of C.

There are various ways to show that t inverts C. One of them uses Burnside's Transfer Theorem. Let q be any prime divisor of $(p-1)/2$, and let Q be a Sylow q-subgroup of C (and hence of G). Clearly $N_G(Q) = C\langle t\rangle$, so t must centralise or invert Q. If t centralises Q, then $Q \leq Z(N_G(Q)$, and Burnside's Transfer Theorem implies that G has a normal q-complement, contradicting simplicity. So t inverts every Sylow subgroup of C, and thus inverts C.

Now $C\langle t\rangle$ is a dihedral group, containing $(p-1)/2$ involutions, one interchanging the point 1 with each point in the other C-orbit. We may choose t so that it interchanges 1 with -1. Then the fact that t inverts C shows that it interchanges a^2 with $-a^{-2}$ for each non-zero $a \in \mathrm{GF}(p)$. So t is the linear fractional map $x \mapsto -1/x$, and we are done. ■

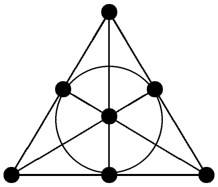
Theorem 2.11(b) follows, since $\mathrm{PSL}(3,2)$ is a simple group of order

$$(2^3-1)(2^3-2)(2^3-2^2) = 168 = (7+1)7(7-1)/2.$$

Exercise 2.7 (a) Complete the proof of the above theorem in the case $p = 5$. Hence prove Theorem 2.11(a).

(b) Show that a simple group of order 60 has five Sylow 2-subgroups, and hence show that any such group is isomorphic to A_5. Give an alternative proof of Theorem 2.11(a).

Proof of Theorem 2.11(d) The simple group $\mathrm{PSL}(3,2)$ of order 168 is the group of collineations of the projective plane over $\mathrm{GF}(2)$, shown below.



Since its index in S_7 is 30, there are 30 different ways of assigning the structure of a projective plane to a given set $N = \{1,2,3,4,5,6,7\}$ of seven points; and since $\mathrm{PSL}(3,2)$, being simple, contains no odd permutations, it is contained in A_7, so these 30 planes fall into two orbits of 15 under the action of A_7.

Let Ω be one of the A_7-orbits. Each plane contains seven lines, so there $15 \times 7 = 105$ pairs (L,Π), where L is a 3-subset of N, $\Pi \in \Omega$, and L is a line of Π. Thus, each of the $\binom{7}{3} = 35$ triples is a line in exactly three of the planes in Ω.

We now define a new geometry $\mathcal{G}$ whose 'points' are the elements of Ω, and whose 'lines' are the triples of elements containing a fixed line L. Clearly, any two 'points' lie in at most one 'line', and a simple counting argument shows that in fact two 'points' lie in a unique line.

Let Π' be a plane from the other A_7-orbit. For each point $n \in N$, the three lines of Π' containing n belong to a unique plane of the set Ω. (Having chosen three lines through a point, there are just two ways to complete the projective plane, differing by an odd permutation.) In this way, each of the seven points of N gives rise to a 'point' of Ω. Moreover, the three points of a line of Π' correspond to three 'points' of a 'line' in our new geometry $\mathcal{G}$. Thus, $\mathcal{G}$ contains 'planes', each isomorphic to the projective plane $\mathrm{PG}(2,2)$.

It follows that $\mathcal{G}$ is isomorphic to $\mathrm{PG}(3,2)$. The most direct way to see this is to consider the set $A = \{0\} \cup \Omega$, and define a binary operation on A by the rules

$$\begin{aligned} 0+\Pi = \Pi+0 = \Pi &\quad \text{for all } \Pi \in \Omega; \\ \Pi+\Pi = 0 &\quad \text{for all } \Pi \in \Omega; \\ \Pi+\Pi' = \Pi'' &\quad \text{if } \{\Pi,\Pi',\Pi''\} \text{ is a 'line'}. \end{aligned}$$

Then A is an elementary abelian 2-group. (The associative law follows from the fact that any three non-collinear 'points' lie in a 'plane'.) In other words, A is the additive group of a rank 4 vector space over $\mathrm{GF}(2)$, and clearly $\mathcal{G}$ is the projective geometry based on this vector space.

Now $A_7 \leq \mathrm{Aut}(\mathcal{G}) = \mathrm{PSL}(4,2)$. (The last inequality comes from the Fundamental Theorem of Projective Geometry and the fact that $\mathrm{PSL}(4,2) = \mathrm{P\Gamma L}(4,2)$ since $\mathrm{GF}(2)$ has no non-trivial scalars or automorphisms.) By calculating orders, we see that A_7 has index 8 in $\mathrm{PSL}(4,2)$. Thus, $\mathrm{PSL}(4,2)$ is a permutation group on the cosets of A_7, that is, a subgroup of S_8, and a similar calculation shows that it has index 2 in S_8. We conclude that $\mathrm{PSL}(4,2) \cong A_8$. ■

The proof of Theorem 2.11(c) is an exercise. Two approaches are outlined below. Fill in the details.

Exercise 2.8 The field $\mathrm{GF}(9)$ can be represented as $\{a+b\mathrm{i} : a,b \in \mathrm{GF}(3)\}$, where $\mathrm{i}^2 = -1$. Let

$$A = \begin{pmatrix} 1 & 1+\mathrm{i} \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then

$$A^3 = I, \quad B^2 = -I, \quad (AB)^5 = -I.$$

So the corresponding elements $a,b \in G = \mathrm{PSL}(2,9)$ satisfy

$$a^3 = b^2 = (ab)^5 = 1,$$

and so generate a subgroup H isomorphic to A_5. Then H has index 6 in G, and the action of G on the cosets of H shows that $G \leq S_6$. Then consideration of order shows that $G \cong A_6$.

Exercise 2.9 Let $G = A_6$, and let H be the normaliser of a Sylow 3-subgroup of G. Let G act on the 10 cosets of H. Show that H fixes one point and acts is isomorphic to the group

$$\{x \mapsto a^2x+b : a,b \in \mathrm{GF}(9), a \neq 0\}$$

on the remaining points. Choose an element outside H and, following the proof of Theorem 2.12, show that its action is linear fractional (if the fixed point is labelled as ∞). Deduce that $A_6 \leq \mathrm{PSL}(2,9)$, and by considering orders, show that equality holds.

Exercise 2.10 A *Hall subgroup* of a finite group G is a subgroup whose order and index are coprime. Philip Hall proved that a finite soluble group G has Hall subgroups of all *admissible* orders m dividing $|G|$ for which $(m, |G|/m) = 1$, and that any two Hall subgroups of the same order in a finite soluble group are conjugate.

(a) Show that $\mathrm{PSL}(2,5)$ fails to have a Hall subgroup of some admissible order.

(b) Show that $\mathrm{PSL}(2,7)$ has non-conjugate Hall subgroups of the same order.

(c) Show that $\mathrm{PSL}(2,11)$ has non-isomorphic Hall subgroups of the same order.

(d) Show that each of these groups is the smallest with the stated property.

Exercise 2.11 Show that $\mathrm{PSL}(4,2)$ and $\mathrm{PSL}(3,4)$ are non-isomorphic simple groups of the same order.