

3 Linear groups

Finite fields. A *field* is a set F with operations of addition, subtraction, multiplication and division satisfying the usual rules. That is, F has an element 0 such that $(F, +, -, 0)$ is an abelian group, and $F \setminus \{0\}$ contains an element 1 such that $(F \setminus \{0\}, \cdot, /, 1)$ is an abelian group, and $x(y+z) = xy + xz$. It is an easy exercise to show that the subfield F_0 generated by the element 1 in a finite field F is isomorphic to the integers modulo p , for some p , and therefore p is prime (called the *characteristic* of the field). Moreover, F is a vector space over F_0 , as the vector space axioms are special cases of the field axioms. As every finite-dimensional vector space has a basis of n vectors, v_1, \dots, v_n , say, and every vector has a unique expression $\sum_{i=1}^n a_i v_i$ with $a_i \in F_0$, it follows that the field F has p^n elements.

Conversely, for every prime p and every positive integer d there is a field of order p^d , which is unique up to isomorphism. [See below.]

The most important fact about finite fields which we need is that the multiplicative group of all non-zero elements is cyclic. For the polynomial ring $F[x]$ over any field F is a Euclidean domain and therefore a unique factorization domain. In particular a polynomial of degree n has at most n roots. If the multiplicative group F^\times of a field of order q has exponent e strictly less than $q-1$, then $x^e - 1$ has $q-1$ roots, which is a contradiction. Therefore the exponent of F^\times is $q-1$, so F^\times contains elements of order $q-1$, since it is abelian, and therefore it is cyclic.

Note also that all elements x of F satisfy $x^q = x$, and so the polynomial $x^q - x$ factorizes in $F[x]$ as $\prod_{\alpha \in F} (x - \alpha)$. Moreover, the number of solutions to $x^n = 1$ in F is the greatest common divisor $(n, q-1)$ of n and $q-1$.

We now show that fields of order p^d exist and are unique up to isomorphism. Observe that if f is an irreducible polynomial of degree d over the field $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ of order p , then $\mathbb{F}_p[x]/(f)$ is a field of order p^d . Conversely, if F is a field of order p^d , let x be a generator for F^\times , so that the minimum polynomial for x over \mathbb{F}_p is an irreducible polynomial f of degree d , and $F \cong \mathbb{F}_p[x]/(f)$. One way to see that such a field exists is to observe that any field of order $q = p^d$ is a splitting field for the polynomial $x^q - x$. Splitting fields always exist, by adjoining roots one at a time until the polynomial factorises into linear factors. But then the set of roots of $x^q - x$ is closed

under addition and multiplication, since if $x^q = x$ and $y^q = y$ then $(xy)^q = x^q y^q = xy$ and $(x+y)^q = x^q + y^q = x+y$. Hence this set of roots is a subfield of order q , as required.

To show that the field of order $q = p^d$ does not depend on the particular irreducible polynomial we choose, suppose that f_1 and f_2 are two such, and $F_i = \mathbb{F}_p[x]/(f_i)$. Since $f_2(t)$ divides $t^q - t$, and $t^q - t$ factorizes into linear factors over F_1 , it follows that F_1 contains an element y with $f_2(y) = 0$. Hence the map $x \mapsto y$ extends to a field homomorphism from F_2 to a subfield of F_1 . Moreover, the kernel is trivial, since fields have no quotient fields, so this map is a field isomorphism, since the fields are finite.

If also $f_1 = f_2$ then any automorphism of $F = F_1 = F_2$ has this form, so is defined by the image of x , which must be one of the d roots of f_1 . Hence the group of automorphisms of F has order d . On the other hand, the map $y \mapsto y^p$ (for all $y \in F$) is an automorphism of F , and has order d . Hence $\text{Aut}(F)$ is cyclic of order d .

General linear groups. Let V be a vector space of dimension n over the finite field \mathbb{F}_q of order q . The *general linear group* $\text{GL}(V)$ is the set of invertible linear maps from V to itself. Without much loss of generality, we may take V as the vector space \mathbb{F}_q^n of n -tuples of elements of \mathbb{F}_q , and identify $\text{GL}(V)$ with the group (denoted $\text{GL}_n(q)$) of invertible $n \times n$ matrices over \mathbb{F}_q .

There are certain obvious normal subgroups of $G = \text{GL}_n(q)$. For example, the centre, Z say, consists of all the scalar matrices λI_n , where $0 \neq \lambda \in \mathbb{F}_q$ and I_n is the $n \times n$ identity matrix. Thus Z is a cyclic normal subgroup of order $q - 1$. The quotient G/Z is called the *projective general linear group*, and denoted $\text{PGL}_n(q)$.

Also, since $\det(AB) = \det(A)\det(B)$, the determinant map is a group homomorphism from $\text{GL}_n(q)$ onto the multiplicative group of the field, so its kernel is a normal subgroup of index $q - 1$. This kernel is called the *special linear group* $\text{SL}_n(q)$, and consists of all the matrices of determinant 1. Similarly, we can quotient $\text{SL}_n(q)$ by the subgroup of scalars it contains, to obtain the *projective special linear group* $\text{PSL}_n(q)$, sometimes abbreviated to $L_n(q)$. [The alert reader will have noticed that as defined here, $\text{PSL}_n(q)$ is not a necessarily a subgroup of $\text{PGL}_n(q)$. However, there is an obvious isomorphism between $\text{PSL}_n(q)$ and a normal subgroup of $\text{PGL}_n(q)$, so we shall ignore the subtle distinction.]

The orders of the linear groups. Now an invertible matrix takes a basis to a basis, and is determined by the image of an ordered basis. The only condition on this image is that the i th vector is linearly independent of the previous ones—but these span a space of dimension $i - 1$, which has q^{i-1} vectors in it, so the order of $\text{GL}_n(q)$ is

$$\begin{aligned} |\text{GL}_n(q)| &= (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) \\ &= q^{n(n-1)/2} (q-1)(q^2-1) \cdots (q^n-1). \end{aligned} \quad (1)$$

The orders of $\text{SL}_n(q)$ and $\text{PGL}_n(q)$ are equal, being $|\text{GL}_n(q)|$ divided by $q - 1$. To obtain the order of $\text{PSL}_n(q)$, we need to know which scalars λI_n have determinant 1.

But $\det(\lambda I_n) = \lambda^n$, and the number of solutions to $x^n = 1$ in the field \mathbb{F}_q is the greatest common divisor $(n, q-1)$ of n and $q-1$. Thus the order of $\text{PSL}_n(q)$ is

$$|\text{PSL}_n(q)| = \frac{1}{(n, q-1)} q^{n(n-1)/2} \prod_{i=2}^n (q^i - 1). \quad (2)$$

The groups $\text{PSL}_n(q)$ are all simple except for the small cases $\text{PSL}_2(2) \cong S_3$ and $\text{PSL}_2(3) \cong A_4$. We shall prove the simplicity of these groups below. First we note that these exceptions are genuine. For $\text{PSL}_2(2) \cong \text{GL}_2(2)$, and $\text{GL}_2(2)$ permutes the three non-zero vectors of \mathbb{F}_2^2 ; moreover, any two of these vectors form a basis for the space, so the action of $\text{GL}_2(2)$ is 2-transitive, and faithful, so $\text{GL}_2(2) \cong S_3$.

Similarly, $\text{GL}_2(3)$ permutes the four 1-dimensional subspaces of \mathbb{F}_3^2 , spanned by the vectors $(1,0)$, $(0,1)$, $(1,1)$ and $(1,-1)$. The action is 2-transitive since the group acts transitively on ordered bases. Moreover, fixing the standard basis, up to scalars, the matrix $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ interchanges the other two 1-spaces, so the action of $\text{GL}_2(3)$ is S_4 . The kernel of the action is just the group of scalar matrices, and the matrices of determinant 1 act as even permutations, so $\text{PSL}_2(3) \cong A_4$.

We use the term *linear group* loosely to refer to any of the groups $\text{GL}_n(q)$, $\text{SL}_n(q)$, $\text{PGL}_n(q)$ or $\text{PSL}_n(q)$.

The projective line and some exceptional isomorphisms. There are many isomorphisms between the small linear groups and other groups. Some of the most interesting are

$$\begin{aligned} \text{L}_2(2) &\cong S_3, \\ \text{L}_2(3) &\cong A_4, \\ \text{L}_2(4) \cong \text{L}_2(5) &\cong A_5, \\ \text{L}_2(9) &\cong A_6 \end{aligned} \quad (3)$$

We have already proved the first two of these. In this section we use the projective line to prove the other three. It is convenient to work in $\text{PSL}_2(q)$ directly as a group of permutations of the 1-dimensional subspaces of \mathbb{F}_q^2 , and to this end we label the 1-spaces by the ratio of the coordinates: that is $\langle(x,1)\rangle$ is labelled x , and $\langle(1,0)\rangle$ is labelled ∞ . The set of 1-spaces is then identified with the set $\mathbb{F}_q \cup \{\infty\}$, called the *projective line* over \mathbb{F}_q , and denoted $\text{PL}(q)$. The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(q)$ now acts on the projective line as $z \mapsto \frac{az+c}{bz+d}$, or, working in the traditional way with column vectors rather than row vectors,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}. \quad (4)$$

If $z \mapsto z$ for all z in the projective line, then putting $z = 0$ gives $c = 0$ and putting $z = \infty$ gives $b = 0$, and putting $z = 1$ then gives $a = d$, so the matrix is a scalar. In

other words, we get a faithful action of $\mathrm{PGL}_2(q)$ on the projective line. Notice that any two points of the projective line determine a basis of the 2-space, up to scalar multiplications of the two basis vectors separately. Given any change of basis matrix we can multiply by a diagonal matrix to make the determinant of the product 1. Thus $\mathrm{PSL}_2(q)$ is also 2-transitive on the points of the projective line.

The isomorphism $\mathrm{PSL}_2(4) \cong A_5$. Now $\mathrm{PSL}_2(4) \cong \mathrm{SL}_2(4)$ permutes the five points of $\mathrm{PL}(4)$ 2-transitively. The field \mathbb{F}_4 of order 4 may be defined as $\{0, 1, \omega, \bar{\omega}\}$ where $\bar{\omega} = \omega^2$ and $\omega^2 + \omega = 1$. Fixing the points 0 and ∞ in $\mathrm{PL}(4) = \{\infty, 0, 1, \omega, \bar{\omega}\}$ we still have the map $z \mapsto \bar{\omega}z/\omega = \omega z$ (defined by the matrix $\begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix}$) which acts as a 3-cycle on the remaining three points 1, ω , $\bar{\omega}$. Thus the action of $\mathrm{PSL}_2(4)$ contains at least a group A_5 . But the orders of $\mathrm{PSL}_2(4)$ and A_5 are the same, and therefore the two groups are isomorphic.

The isomorphism $\mathrm{PSL}_2(5) \cong A_5$. The isomorphism $\mathrm{L}_2(5) \cong A_5$ may be shown by putting a projective line structure onto the set of six Sylow 5-subgroups of A_5 . For example if we label $\langle(1, 2, 3, 4, 5)\rangle$ as ∞ and, reading modulo 5, label $\langle(t + 1, t + 3, t + 2, t, t + 4)\rangle$ as t for $t = 0, 1, 2, 3, 4$, then the generators $(1, 2, 3, 4, 5)$ and $(2, 3)(4, 5)$ of A_5 act on the line as $z \mapsto z + 1$ and $z \mapsto -1/z$. Hence there is a homomorphism $\phi : A_5 \rightarrow \mathrm{L}_2(5)$, which is easily seen to be injective. Moreover $|A_5| = |\mathrm{L}_2(5)|$, so the two groups are isomorphic.

The isomorphism $\mathrm{PSL}_2(9) \cong A_6$. The isomorphism $\mathrm{L}_2(9) \cong A_6$ is best shown by labelling the ten points of the projective line $\mathrm{PL}(9)$ with the ten partitions of six points into two subsets of size 3 (equivalently, the ten Sylow 3-subgroups of A_6). Take $\mathbb{F}_9 = \{0, \pm 1, \pm i, \pm 1 \pm i\}$, where $i^2 = -1$. Let the 3-cycle $(1, 2, 3)$ act on the points by $z \mapsto z + 1$ and let $(4, 5, 6)$ act by $z \mapsto z + i$. Then the point ∞ fixed by these two 3-cycles corresponds to the partition $(123|456)$, and we may choose the point 0 to correspond to the partition $(423|156)$, so that the rest of the correspondence is determined by the action of the 3-cycles above. We can now generate $\mathrm{PSL}_2(9)$ by adjoining the map $z \mapsto -1/z$, which we can check acts on the points in the same way as the permutation $(2, 3)(1, 4)$. Thus we have a homomorphism from $\mathrm{L}_2(9)$ onto A_6 , and since these two groups have the same order, they are isomorphic. Notice incidentally that an odd permutation of S_6 realises a field automorphism of \mathbb{F}_9 : for example, the map $z \mapsto z^3$ corresponds to the transposition $(5, 6)$. Thus $S_6 \cong \mathrm{P}\Sigma\mathrm{L}_2(9)$, which is not isomorphic to $\mathrm{PGL}_2(9)$.

The actions of $\mathrm{PSL}_2(11)$ on 11 points. The action of $\mathrm{PSL}_2(q)$ on the $q + 1$ points of the projective line is usually the smallest permutation action. However, we have seen that $\mathrm{PSL}_2(5) \cong A_5$ so has an action on 5 points. Similarly, $\mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2)$, so has an action on 7 points (indeed, it has two such actions: one on the seven 1-dimensional

subspaces, and one on the seven 2-dimensional subspaces: see below). The only other simple group $\mathrm{PSL}_2(p)$ which has an action on fewer than $p + 1$ points is $\mathrm{PSL}_2(11)$, which has two distinct actions on 11 points.

Consider the partition of the projective line $\mathrm{PL}(11)$ into six pairs

$$(\infty, 0)(1, 2)(3, 6)(4, 8)(5, X)(9, 7),$$

where we write $X = 10$ to avoid confusion. It is easy to see that this partition has just 11 images under the subgroup 11:5 of $\mathrm{PSL}_2(11)$ generated by $z \mapsto z + 1$ and $z \mapsto 3z$. Now consider the action of $z \mapsto -1/z$ on these 11 partitions. Label them p_t , so that p_t is the partition in which ∞ is paired with t . A small calculation shows that $z \mapsto -1/z$ preserves this set of partitions, and acts as the permutation $(1, 9)(2, 6)(4, 5)(7, 8)$ on the p_t . Of course, the map $z \mapsto z + 1$ on $\mathrm{PL}(11)$ acts as $t \mapsto t + 1$, and similarly $z \mapsto 3z$ acts as $t \mapsto 3t$.

The other action on 11 points may be obtained by taking the image under $z \mapsto -z$ of the partitions given above.

Projective planes. Analogous to the construction of a projective line from a 2-dimensional vector space, a 3-dimensional vector space gives rise to a *projective plane*. This consists of *points* (i.e. 1-dimensional subspaces of the vector space) and *lines* (i.e. 2-dimensional subspaces). If the underlying field is \mathbb{F}_q , then there are $q^2 + q + 1$ points and $q^2 + q + 1$ lines, with $q + 1$ points on each line, and $q + 1$ lines through each point.

For example if $q = 2$ there are 7 points and 7 lines. If the points are labelled by integers modulo 7, then the lines may be taken as the seven sets $\{t, t + 1, t + 3\}$. The automorphism group $\mathrm{PGL}_3(2)$ may then be generated by the permutations $t \mapsto t + 1$, $t \mapsto 2t$ and $(1, 2)(3, 6)$ of the points.

Similarly if $q = 3$ the thirteen points may be labelled by the integers modulo 13 (where for convenience we write $X = 10$, $E = 11$ and $T = 12$) in such a way that the lines are $\{t, t + 1, t + 3, t + 9\}$. Then the automorphism group $\mathrm{PGL}_3(3)$ is generated by the permutations $t \mapsto t + 1$, $t \mapsto 3t$ and $(1, 3)(2, 6)(8, E)(X, T)$ of the points.

Simplicity of $\mathrm{PSL}_n(q)$. For $n \geq 2$ we let $\mathrm{SL}_n(q)$ act on the set Ω of 1-dimensional subspaces of \mathbb{F}_q^n , so that the kernel of the action is just the set of scalar matrices, and we obtain an action of $\mathrm{PSL}_n(q)$ on Ω . Moreover, this action is 2-transitive, and therefore primitive.

To study the stabiliser of a point, we might as well take this point to be the 1-space $\langle(1, 0, \dots, 0)\rangle$. The stabiliser then consists of all matrices whose first row is $(\lambda, 0, \dots, 0)$. It is easy to check that the subgroup of matrices of the shape $\begin{pmatrix} 1 & 0_{n-1} \\ v_{n-1} & I_{n-1} \end{pmatrix}$, where v_{n-1} is an arbitrary column vector of length $n - 1$, is a normal abelian subgroup A . Moreover, all non-trivial elements of A are *transvections*, that is, matrices (or linear maps) t such that $t - I_n$ has rank 1 and $(t - I_n)^2 = 0$. By suitable choice of basis (but

remember that the base change matrix must have determinant 1) it is easy to see that every transvection is contained in some conjugate of A .

We have two more things to verify: first, that $\mathrm{SL}_n(q)$ is generated by transvections, and second, that $\mathrm{SL}_n(q)$ is perfect, except for the cases $\mathrm{SL}_2(2)$ and $\mathrm{SL}_2(3)$. The first fact is a restatement of the elementary result that every matrix of determinant 1 can be reduced to the identity matrix by a finite sequence of elementary row operations of the form $r_i \mapsto r_i + \lambda r_j$. To prove the second it suffices to verify that every transvection is a commutator of elements of $\mathrm{SL}_n(q)$. An easy calculation shows that the commutator

$$\left[\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -x & 0 & 1 \end{pmatrix}, \quad (5)$$

so by suitable choice of basis we see that if $n > 2$ then every transvection is a commutator in $\mathrm{SL}_n(q)$. If $n = 2$ and $q > 3$, then \mathbb{F}_q contains a non-zero element x with $x^2 \neq 1$, and then the commutator

$$\left[\begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix}, \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \right] = \begin{pmatrix} 1 & 0 \\ y(x^2 - 1) & 1 \end{pmatrix}, \quad (6)$$

which is an arbitrary element of A .

We can now apply Iwasawa's Lemma, and deduce that $\mathrm{PSL}_n(q)$ is simple provided $n > 2$ or $q > 3$.