Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Notes 6 **Autumn 2011**

6 Linear groups

In this section we study the next important family of linear groups, the "projective special linear groups" $\mathrm{PSL}(n,F)$. The proof of their simplicity is an application of Iwasawa's Lemma.

6.1 Finite fields

Our constructions of simple groups in this chapter work over any field, and give finite groups if and only if the field is finite.

The finite fields were classified by Galois (this was one of the few pieces of work published in his lifetime). His theorem is:

Theorem 6.1 *The order of a finite field is a prime power. Conversely, for any prime power $q > 1$, there is a field with q elements, unique up to isomorphism.*

We will not prove this theorem here, since the techniques come from ring theory rather than group theory. Here is a simple example, a field of four elements. We construct it by adjoining to the field $\mathbb{Z}_2$ a root of an irreducible polynomial of degree 2. Of the four polynomials of degree 2 over $\mathbb{Z}_2$, namely,

$$x^2, \quad x^2+1=(x+1)^2, \quad x^2+x=x(x+1), \quad x^2+x+1,$$

only the last is irreducible, so we add an element α satisfying $\alpha^2=\alpha+1$. (Remember that, since $-1=1$ in $\mathbb{Z}_2$, we have $-u=u$ for any element u in the field we are constructing.) Thus the addition and multiplication tables of our field are the following, where we have put $\beta=\alpha+1=\alpha^2$:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Finite fields are called *Galois fields*. The unique Galois field of given prime power order q is denoted by $\mathbb{F}_q$ or $\mathrm{GF}(q)$. Note that $\mathbb{F}_q \cong \mathbb{Z}_q$ if and only if q is prime.

Note that the additive group of $\mathbb{F}_4$ is the Klein group, while the multiplicative group is cyclic of order 3. This is an instance of a general fact.

Theorem 6.2 *Let $q = p^r$, where p is prime. Then:*

(a) The additive group of $\mathbb{F}_q$ is elementary abelian of order q, that is, the direct product of r copies of C_p.

(b) The multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$.

(c) The automorphism group of $\mathbb{F}_q$ is cyclic of order r, generated by the Frobenius map $a \mapsto a^p$.

Proof (a) For $n \in \mathbb{N}$ and $u \in \mathbb{F}_q$, let $nu = u + \cdots + u$ (n terms). This is the additive analogue of raising u to the nth power.

Since the additive group has order p^r, there is an element $u \neq 0$ with order p, thus $pu = 0$. But then $pv = (pu)(u^{-1}) = 0$ for all $v \in \mathbb{F}_q$. Thus the additive group is elementary abelian.

(b) Let k be the exponent of the multiplicative group of $\mathbb{F}_q$ (the smallest positive integer such that $u^k = 1$ for all $u \neq 0$). Then k divides the order $q-1$ of the multiplicative group. But the equation $x^k - 1 = 0$ has at most k solutions. So we must have $k = q-1$. Now in our proof of the Fundamental Theorem of Finite Abelian Groups, we saw that there is an element whose order is equal to the exponent. So the multiplicative group is cyclic.

(c) We will not prove this, but simply describe an automorphism of the field which generates the automorphism group. This is the *Frobenius map* $u \mapsto u^p$. To show that it is a homomorphism:

$$\begin{aligned} (u+v)^p &= \sum_{i=0}^{p} \binom{p}{i} u^{p-i} v^i = u^p + v^p, \\ (uv)^p &= u^p v^p. \end{aligned}$$

In the first line we use the fact that the binomial coefficient $\binom{p}{i}$ is divisible by p for $i = 1, \ldots, p-1$, so that $\binom{p}{i} x = 0$ in $\mathbb{F}_q$.

Now a field has no non-trivial ideals, so the kernel of the Frobenius map is $\{0\}$, that is, it is one-to-one. Since $\mathbb{F}_q$ is a finite set, this implies that the Frobenius map is a bijection, that is, an automorphism.

6.2 Linear groups

Let F be any field. We denote by $\mathrm{GL}(n,F)$ the group of all invertible $n \times n$ matrices over F; this group is the *general linear group* of dimension n over F. For brevity, we write $\mathrm{GL}(n,q)$ instead of $\mathrm{GL}(n,\mathbb{F}_q)$. We always assume that $n \geq 2$; for $\mathrm{GL}(1,F)$ is simply the multiplicative group $F^\times$ of F, and is abelian (and cyclic if F is finite).

Proposition 6.3

$$|\mathrm{GL}(n,q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

Proof A matrix is invertible if and only if its rows are linearly independent; this holds if and only if the first row is non-zero and, for $k = 2,\ldots,n$, the kth row is not in the subspace spanned by the first $k-1$ rows. The number of possible rows is q^n, and the number lying in any i-dimensional subspace is q^i. So the number of choices of the first row of an invertible matrix is q^n-1, while for $k = 2,\ldots,n$, the number of choices for the kth row is $q^n - q^{k-1}$. Multiplying these together gives the result.

Next we investigate normal subgroups of $\mathrm{GL}(n,q)$.

Proposition 6.4 *The determinant map* $\det : \mathrm{GL}(n,F) \to F^\times$ *is a homomorphism.*

Proof This is the simple fact from linear algebra that $\det(AB) = \det(A)\det(B)$.

The kernel of the determinant map is the set of $n \times n$ matrices with determinant 1. This is denoted $\mathrm{SL}(n,F)$, the *special linear group* of dimension n over F. Thus, $\mathrm{SL}(n,F) \lhd \mathrm{GL}(n,F)$, and

$$\mathrm{GL}(n,F)/\mathrm{SL}(n,F) \cong F^\times$$

(the last fact follows from the First Isomorphism Theorem, since it is easy to see that det is onto: for every element $u \in F$ there exists an $n \times n$ matrix A with $\det(A) = u$.

In particular, we see that

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

Let Ω denote the set of 1-dimensional subspaces of F^n, the n-dimensional vector space over F. (The set Ω is the set of points of the $(n-1)$-dimensional *projective space*, denoted by $\mathrm{PG}(n-1,q)$. Really it is a geometric object and has a lot of structure, but we only need to regard it as a set.) We have

$$|\Omega| = \frac{q^n-1}{q-1}.$$

For there are $q^n - 1$ non-zero vectors in F^n, each of which spans a 1-dimensional subspace; but each 1-dimensional subspace is spanned by any of its $q-1$ non-zero vectors.

There is an action of $\mathrm{GL}(n,F)$ on Ω: the matrix A maps the subspace $\langle v \rangle$ to the subspace $\langle vA \rangle$.

Proposition 6.5 *The following conditions on a matrix $A \in \mathrm{GL}(n,F)$ are equivalent:*

(a) $A \in Z(GL(n,F))$;

(b) A belongs to the kernel of the action of $\mathrm{GL}(n,F)$ on Ω;

(c) A is a scalar matrix, that is, $A = \lambda I$ for some $\lambda \in F^\times$.

Proof (a) $\Leftrightarrow$ (c): Clearly scalar matrices commute with everything and so lie in the centre of the group. Suppose $A \in Z(\mathrm{GL}(n,q))$. If E is the matrix with entries 1 on the diagonal and in position $(1,2)$ and zero elsewhere, then EA is obtained from A by adding the second row to the first, while AE is obtained by adding the first column to the second. If these are equal, then the first and second diagonal elements of A are equal, and the other entries in the first column and second row are zero. Repeating the argument for the ith row and jth column, we conclude that A is a scalar matrix.

(b) $\Leftrightarrow$ (c): Again it is clear that a scalar matrix fixes every 1-dimensional subspace. Let A be a matrix which fixes all 1-dimensional subspaces. Let $e_1, \ldots, e_n$ be the standard basis vectors. Then we have $e_i A = \alpha_i e_i$ for $i = 1, \ldots, n$, (for some $\alpha_1, \ldots, \alpha_n \in F^\times$), so A is a diagonal matrix. Also,

$$\begin{aligned} (e_i + e_j)A &= \beta(e_i + e_j) \text{ for some } \beta \in F^\times, \\ e_i A + e_j A &= \alpha_i e_i + \alpha_j e_j, \end{aligned}$$

so $\alpha_i = \beta = \alpha_j$. Thus A is a scalar matrix.

Thus we see that $Z(\mathrm{GL}(n,F))$ is the group of scalar matrices, and is isomorphic to $F^\times$ (so is cyclic of order $q-1$ if $F = \mathbb{F}_q$).

We define the *projective general and special linear groups* by

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

where $Z = Z(\mathrm{GL}(n,q))$. Thus, the projective groups are the images of the linear groups in the action on the projective space Ω, so we can think of them as groups of permutations of this space.

We have $|\mathrm{PGL}(n,q)| = |\mathrm{GL}(n,q)|/(q-1) = |\mathrm{SL}(n,q)|$. What is the order of $\mathrm{PSL}(n,q)$?

The kernel of the action of $\mathrm{SL}(n,F)$ on the projective space consists of the scalar matrices λI with determinant 1, that is, for which $\lambda^n = 1$. If $F = \mathbb{F}_q$, then the multiplicative group is cyclic of order $q-1$, and the number of solutions of $\lambda^n = 1$ is $\gcd(n, q-1)$. So we have

$$|\mathrm{PSL}(n,q)| = |\mathrm{SL}(n,q)|/\gcd(n,q-1).$$

In particular, if $\gcd(n,q-1) = 1$, then $\mathrm{PSL}(n,q) = \mathrm{PGL}(n,q) = \mathrm{SL}(n,q)$: for in this case, the first group is a subgroup of the second and a quotient of the third, but all three have the same order.

For $n = 2$, we find that

$$|\mathrm{PSL}(2,q)| = \begin{cases} (q+1)q(q-1) & \text{if } q \text{ is a power of 2,} \\ (q+1)q(q-1)/2 & \text{if } q \text{ is odd.} \end{cases}$$

In this case, the number of points of Ω is $(q^2-1)/(q-1) = q+1$, and so $\mathrm{PGL}(2,q)$ and $\mathrm{PSL}(2,q)|$ are subgroups of the symmetric group S_{q+1}. We examine the first few cases.

$q = 2$: $\mathrm{PSL}(2,2) = \mathrm{PGL}(2,2)$ is a subgroup of S_3 of order $3 \cdot 2 \cdot 1 = 6$; so it is isomorphic to S_3.

$q = 3$: $\mathrm{PGL}(2,3)$ is a subgroup of S_4 of order $4 \cdot 3 \cdot 2 = 24$; so $\mathrm{PGL}(2,3) \cong S_4$. Also $\mathrm{PSL}(2,3)$ is a subgroup of index 2, so $\mathrm{PSL}(2,3) \cong A_4$.

$q = 4$: $\mathrm{PGL}(2,4) = \mathrm{PSL}(2,4)$ is a subgroup of S_5 of order $5 \cdot 4 \cdot 3 = 60$; so $\mathrm{PSL}(2,4) \cong A_5$.

$q = 5$: $\mathrm{PGL}(2,5)$ is a subgroup of S_6 of order $6 \cdot 5 \cdot 4 = 120$, and hence index 6; so it is the stabiliser of a synthematic total, and hence is isomorphic to S_5. Moreover, $\mathrm{PSL}(2,5)$ is a subgroup of index 2, so is isomorphic to A_5.

$q = 7$: $\mathrm{PSL}(2,7)$ has order $8 \cdot 7 \cdot 6/2 = 168$. It turns out to be isomorphic to the group we met on Problem Sheet 1.

There is a simpler way to think of the action of $\mathrm{PSL}(2,F)$ on the projective line. The 1-dimensional subspaces of F^2 are of two types: those with a unique spanning vector with first coordinate 1, say $(1,x)$ for $x \in F$; and one spanned by $(0,1)$. We denote points of the first type by the corresponding field element x, and the point of the second type by ∞. Then the elements of $\mathrm{PGL}(2,F)$ are the *linear fractional* maps

$$x \mapsto \frac{ax+b}{cx+d}$$

for $a,b,c,d \in F$, $ad - bc \neq 0$, with the "natural" conventions for dealing with ∞: for $a \neq 0$ we have $a/0 = \infty$, $a\infty = \infty$, and $(b\infty)/(a\infty) = b/a$; also $\infty + c = \infty$ for any c. The group $\mathrm{PSL}(2,F)$ consists of those linear fractional maps with $ad - bc = 1$.

6.3 Simplicity of $\mathrm{PSL}(n,F)$

The main result is:

Theorem 6.6 *For $n \geq 2$ and any field F, the group $\mathrm{PSL}(n,F)$ is simple, except in the two cases $n = 2$, $F = \mathbb{F}_2$ or $n = 2$, $F = \mathbb{F}_3$.*

We saw the two exceptional cases (which are isomorphic to S_3 and A_4) in the preceding section. The remainder of this section is devoted to the proof of simplicity in the other cases.

We have two preliminary jobs, concerning transitivity and generation.

Proposition 6.7 *For $n \geq 2$, the group $\mathrm{PSL}(n,F)$ acts doubly transitively on the points of the projective space Ω.*

Proof Let $\langle v_1 \rangle$ and $\langle v_2 \rangle$ be two distinct 1-dimensional subspaces of F^n. Then v_1 and v_2 are linearly independent, and so for any other pair $\langle w_1 \rangle$ and $\langle w_2 \rangle$, there is a linear map carrying v_1 to w_1 and v_2 to w_2. (Simply extend both (v_1, v_2) and (w_1, w_2) to bases, and take the unique linear map taking the first basis to the second.) If this map has determinant c, we can follow it by the map multiplying the first basis vector by c^{-1} and fixing the rest to find one with determinant 1 which does the job.

A *transvection* is a linear map of a vector space V of the form $v \mapsto v + f(v)a$, where $a \in V$, $f \in V^*$ (that is, f is a linear map from V to F), and $f(a) = 0$. We will call the corresponding map of the projective space a transvection also, though geometers sometimes use the term "elation". A transvection of F^2 is also called a "shear". We denote the above transvection by $T(a,f)$.

For $a \neq 0$, let $A(a)$ be the set of all transvections $T(a,f)$ with given a, as f runs over all elements of V^* satisfying $f(a) = 0$. Since $T(a,f_1)T(a,f_2) = T(a,f_1+f_2)$, we see that $A(a)$ is an abelian group isomorphic to $\mathrm{Ann}(a)$, the *annihilator* of a, a subspace of codimension 1 in V^*.

Any transvection belongs to $\mathrm{SL}(n,F)$. (Transvections have determinant 1 since they are represented by strictly upper triangular matrices with respect to a suitable basis. Indeed, if we let a be the first vector in a basis, then a transvection is represented by the matrix

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ * & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ * & 0 & 0 & \dots & 1 \end{pmatrix}$$

whose first column represents the element $f \in V^*$.

The transvection group $A(a)$ acts faithfully on the projective space, since it is clearly disjoint from the group Z of scalar matrices (the kernel of the action). It is obviously normal in the stabiliser of a, since it is easy to check that $g^{-1}A(a)g = A(ag)$ for any $g \in \mathrm{PSL}(n,F)$.

Proposition 6.8 *For $n \geq 2$, the group $\mathrm{PSL}(n,F)$ is generated by transvections.*

Proof We use induction on n.

For $n = 2$, represent $\mathrm{PSL}(2,F)$ as the group of linear fractional transformations. The transvections with $a = \langle (0,1) \rangle$ are the maps of the form $x \mapsto x + a$ (fixing ∞); they form a group acting transitively on the points different from ∞. So the group H generated by all transvections is 2-transitive. It suffices now to show that the stabiliser of two points in H is the same as that in $\mathrm{PSL}(2,F)$.

Now the stabiliser of ∞ and 0 in $\mathrm{PSL}(2,F)$ is the group of maps of the form $x \mapsto ax/d$ with $ad = 1$, in other words, $x \mapsto a^2 x$. We have to show that we can generate this map by transvections, which we show by the following calculation:

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

Now suppose the result is true for $n-1$. Let H be the subgroup of $\mathrm{PSL}(n,F)$ generated by transvections. First, we observe that G is transitive on the projective line, since given two subspaces $\langle a \rangle$ and $\langle b \rangle$, we have transvections of $\langle a,b \rangle$ fixing a complement pointwise, and in the group they generate we can map one point to the other. So it suffices to show that the stabiliser of a point $\langle a \rangle$ is generated by transvections.

Now the stabiliser of $\langle a \rangle$ in G contains all the transvections of $\mathrm{PSL}(n-1,F)$ acting on the quotient space $V/\langle a \rangle$. By induction, these generate $\mathrm{PSL}(n-1,F)$. So if we take an arbitrary element of $\mathrm{PSL}(n,F)$ fixing $\langle a \rangle$, we can multiply it by a suitable product of transvections so that on the quotient space it is diagonal with all but one diagonal entry equal to 1. That is, we can reduce to a matrix of 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 can reduce to the case where $x_1 = \ldots = x_{n-1} = 0$. Now apart from the identity in the middle, we have just the matrix

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

which is dealt with as in the case $n = 2$.

Proof of the Theorem First, we recall the statement of Iwasawa's Lemma:

Theorem 6.9 *Let G be a group with a faithful primitive action on Ω. Suppose that there is an abelian normal subgroup A of $\mathrm{Stab}(\alpha)$ 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.*

We will take $G = \mathrm{PSL}(n,F)$ acting on Ω. (The action is doubly transitive and hence primitive.) We have seen that the transvection group $A(a)$ is abelian and normal in the stabiliser of $\langle a \rangle$, and that its conjugates generate G. So only one thing remains to be proved:

Proposition 6.10 *For $n \geq 2$, the group $\mathrm{PSL}(n,F)$ is equal to its derived group except in the cases $n = 2$, $F = \mathbb{F}_2$, and $n = 2$, $F = \mathbb{F}_3$.*

Proof Since all transvection groups are conjugate, it suffices to find a transvection group in the derived group; that is, to express the elements of one transvection group as commutators.

Suppose first that $|F| > 3$. It suffices to do the case $n = 2$, since all the calculations below can be done in the upper left-hand corner of a matrix with the identity in the bottom right and zeros elsewhere. Since $|F| > 3$, there is an element $a \in F$ satisfying $a^2 \neq 0, 1$. Then $\mathrm{SL}(2,F)$ contains the matrix $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, as we saw above; and

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

and $(a^2-1)x$ runs through F as x does.

Now suppose that $n \geq 3$, and that $|F| = 2$ or $|F| = 3$ (indeed this argument works for all F). Again we need only consider 3×3 matrices. We have

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

The proof is complete.