Queen Mary
University of London

MTH714U/MTHM024 Group theory

Extended notes **Autumn 2008**

---

1 Review of basic group theory

Almost all of the material in this chapter is in the syllabus for the level 3 course MAS305 Algebraic Structures II, and will therefore be treated mainly as revision. However, in practice not all of it may have been covered thoroughly in Algebraic Structures II, so please let me know how much detail you require me to give in the lectures as we go along. Also let me know if there are significant parts you have not seen before, that you need me to cover in more detail.

Groups, subgroups and cosets A *group* is a (finite) set G with an *identity* element 1, a (binary) *multiplication* $x.y$ (or xy) and a (unary) *inverse* x^{-1} satisfying the *associative law* $(xy)z = x(yz)$, the *identity laws* $x1 = 1x = x$ and the *inverse laws* $xx^{-1} = x^{-1}x = 1$ for all $x, y, z \in G$ (and the *closure laws* $xy \in G$ and $x^{-1} \in G$ which we take for granted). It is *abelian* if $xy = yx$ for all $x, y \in G$, *non-abelian* otherwise. A *subgroup* is a subset H closed under multiplication and inverses. (It is sufficient to check $xy^{-1} \in H$ for all $x, y \in H$. For then $xx^{-1} = 1 \in H$, so $1.y^{-1} = y^{-1} \in H$, and then $x.(y^{-1})^{-1} \in H$.) *Left cosets* of H in G are subsets $gH = \{gh \mid h \in H\}$ and *right cosets* are $Hg = \{hg \mid h \in H\}$. The left (or right) cosets all have the same size, and partition G, so that $|G| = |H||G : H|$ (*Lagrange's Theorem*), where $|G|$ is the *order* of G (i.e. the number of elements in G) and $|G : H|$ is the *index* of H in G, i.e. the number of left (or right) cosets. The *order* of an element $g \in G$ is the order n of the *cyclic group* $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$ it *generates*, and the *exponent* of G is the lowest common multiple of the orders of the elements, that is the smallest positive integer e such that $g^e = 1$ for all $g \in G$.

Cyclic groups: if S is a set of elements of a group G, then the subgroup generated by S, written $\langle S \rangle$, is the smallest subgroup of G which contains all these elements. I.e. $\langle S \rangle$ contains all elements ${x_1}^{\pm 1}.{x_2}^{\pm 1}.\cdots.{x_k}^{\pm 1}$ for $x_i \in S$. Cyclic groups are generated by a single element g. Thus $\langle g \rangle = \{1, g, g^2, \ldots\}$. If n is the smallest positive integer with $g^n = 1$, then $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$. Then n is the order of g.

Homomorphisms and quotient groups A *homomorphism* is a map $\phi : G \to H$ which preserves the multiplication, $\phi(xy) = \phi(x)\phi(y)$ (from which it follows that $\phi(1) =$

1 and $\phi(x^{-1}) = \phi(x)^{-1}$). The *kernel* of ϕ is $\ker\phi = \{g \in G \mid \phi(g) = 1\}$, and is a subgroup which satisfies $g(\ker\phi) = (\ker\phi)g$, i.e. its left and right cosets are equal (such a subgroup N is called *normal*, written $N \trianglelefteq G$, or $N \triangleleft G$ if also $N \neq G$). An *isomorphism* is a bijective homomorphism, i.e. one satisfying $\ker\phi = \{1\}$ and $\phi(G) = H$: in this case we write $G \cong H$.

If N is a normal subgroup of G, the *quotient* group G/N has elements xN (for all $x \in G$) and group operations $(xN)(yN) = (xy)N$, and $(xN)^{-1} = x^{-1}N$. The *first isomorphism theorem* states that if $\phi : G \to H$ is a homomorphism then the image of ϕ, $\phi(G) \cong G/\ker\phi$ (and the isomorphism is given by $\phi(x) \mapsto x\ker\phi$).

The *correspondence theorem*: The subgroups H/N of G/N are in one-to-one correspondence with the subgroups H of G which contain N. The normal subgroups of G/N are in one-to-one correspondence with the normal subgroups K of G which contain N. The *second isomorphism theorem* is $(G/N)/(K/N) \cong G/K$. To prove this, let $\phi : G/N \to G/K$ be defined by $\phi(gN) = (gK)$. This is well-defined because $N \subseteq K$, and is obviously a group homomorphism. Its kernel is $\{gN \mid gK = K, \text{ i.e. } g \in K\} = K/N$, so the result follows by the first isomorphism theorem.

If H is any subgroup of G, and N is any normal subgroup of G, then $HN = \{xy \mid x \in H, y \in N\}$ is a subgroup of G and $N \cap H$ is a normal subgroup of H. The *third isomorphism theorem* is $HN/N \cong H/(N \cap H)$. To prove this, let $\phi : H \to KH/K$ be defined by $\phi(h) = hK = Kh$. This is obviously a group homomorphism, and its kernel is $\{h \in H \mid hK = K, \text{ i.e. } h \in K\} = H \cap K$.

Example of first isomorphism theorem: $S_3 = \{1, (1,2,3), (1,3,2), (1,2), (1,3), (2,3)\}$ and $A_3 = \{1, (1,2,3), (1,3,2)\} \cong C_3$. The multiplication table of S_3 looks like this:

1	$(1,2,3)$	$(1,3,2)$	$(1,2)$	$(2,3)$	$(1,3)$
$(1,2,3)$	$(1,3,2)$	1	$(2,3)$	$(1,3)$	$(1,2)$
$(1,3,2)$	1	$(1,2,3)$	$(1,3)$	$(1,2)$	$(2,3)$
$(1,2)$	$(1,3)$	$(2,3)$	1	$(1,3,2)$	$(1,2,3)$
$(2,3)$	$(1,2)$	$(1,3)$	$(1,2,3)$	1	$(1,3,2)$
$(1,3)$	$(2,3)$	$(1,2)$	$(1,3,2)$	$(1,2,3)$	1

The four boxes enclose the cosets A_3 and $A_3(1,2) = (1,2)A_3$ and show the multiplication table of $S_3/A_3 \cong C_2$.

Another example: S_4 has a subgroup $V = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, which is normal.

$$\begin{aligned} V.(1,2,3) &= \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\} \\ &= V.(1,3,4) = V.(2,4,3) = V.(1,4,2) \\ &= (1,2,3).V \end{aligned}$$

The six cosets of V are V, $V.(1,2,3)$, $V.(1,3,2)$, $V.(1,2)$, $V.(2,3)$, $V.(1,3)$, so we see $S_4/V \cong S_3$. To illustrate the correspondence theorem, A_3 normal in S_3 corresponds to A_4 normal in S_4. A subgroup S_2 of S_3 corresponds to a subgroup D_8 of S_4.

Simple groups and composition series A group S is *simple* if it has exactly two normal subgroups (1 and S). In particular, an abelian group is simple if and only if it has prime order. A series

$$1 = G_0 \lhd G_1 \lhd G_2 \quad \lhd \cdots \lhd \quad G_{n-1} \lhd G_n = G \tag{1}$$

for a group G is called a *composition series* if all the factors G_i/G_{i-1} are simple (and they are then called *composition factors*). For example, S_4 has a composition series

$$1 \lhd C_2 \lhd V \lhd A_4 \lhd S_4$$

and the composition factors are C_2, C_2, C_3 and C_2.

The *fourth isomorphism theorem* (or *Zassenhaus's butterfly lemma*) states that if $X \lhd Y \leq G$ and $A \lhd B \leq G$ then

$$\frac{(Y \cap B)X}{(Y \cap A)X} \cong \frac{(Y \cap B)}{(Y \cap A)(X \cap B)} \cong \frac{(Y \cap B)A}{(X \cap B)A}.$$

(We shall give two proofs of this in a moment.) Hence (see below) any two series for G have isomorphic *refinements*, and by induction on the length of a composition series, any two composition series for a finite group have the same composition factors, counted with multiplicities (the *Jordan–Hölder Theorem*). A *normal series* is one in which all terms G_i are normal in G, and if it has no proper refinements it is called a *chief series*, and its factors G_i/G_{i-1} *chief factors*.

Zassenhaus's butterfly lemma A proof of Zassenhaus's butterfly lemma goes as follows. Define the map $\phi : Y \cap B \to (Y \cap B)X/(Y \cap A)X$ by $\phi(y) = y(Y \cap A)X$. This is easily seen to be a group homomorphism (exercise: where does this use the fact that $X \lhd Y$? Where does it use the fact that $A \lhd B$?). Moreover, since $Y \cap A \subseteq Y \cap B$, it is easy to see that the image of ϕ is $(Y \cap B)X/(Y \cap A)X$. The tricky part of the proof is to identify the kernel of ϕ: we need to prove that $\ker\phi = (Y \cap A)(X \cap B)$. On the one hand, if $y \in Y \cap A$ then $\phi(y)$ is the identity coset $(Y \cap A)X$. Similarly, if $y \in X \cap B$ then $\phi(y) = y(Y \cap A)X \subseteq X(Y \cap A)X \subseteq (Y \cap A)X$ since $X \lhd Y$. Therefore $(Y \cap A)(X \cap B) \subseteq \ker\phi$. Conversely, if $y \in \ker\phi$ then $y \in (Y \cap A)X$, so we can write $y = ax$ with $a \in Y \cap A$ and $x \in X$. But now $y \in B$ and $a \in B$ so $x \in B$ and therefore $y \in (Y \cap A)(X \cap B)$, showing that $\ker\phi \subseteq (Y \cap A)(X \cap B)$. So we have $\ker\phi = (Y \cap A)(X \cap B)$ and the result follows from the first isomorphism theorem.

In Figure 1, single lines represent subgroups, and double lines represent normal subgroups. For example, X is normal in $(Y \cap A)X$, since X is normal in Y, but $X \cap B$ is not necessarily normal in X. More accurately, the double lines represent *quotient groups*, and any two parallel double lines represent isomorphic quotient groups. The isomorphisms of the vertical lines are given by Zassenhaus's butterfly lemma. The bottom two parallelograms consist of two instances of isomorphisms of the form $PQ/Q \cong P/(P \cap Q)$. Indeed, so do the top two parallelograms, although this is not so easy to see.

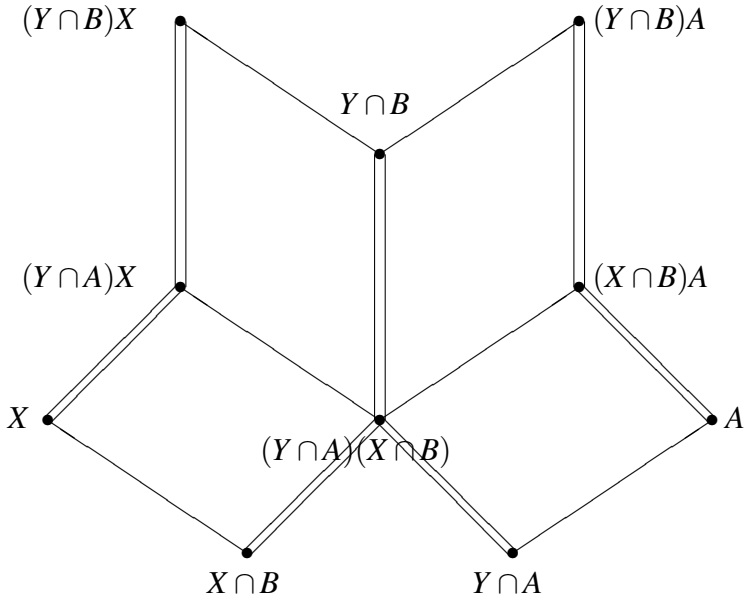

Figure 1: Zassenhaus's butterfly

To prove the last statement (and hence get an alternative proof of Zassenhaus's lemma using the third isomorphism theorem) use the so-called *Dedekind modular law*: if P, Q, and R are subgroups of a group G, and $R \subseteq P$, then $P\cap(QR) = (P\cap Q)R$. Proof: if $x \in (P\cap Q)R$ then $x = yz$ with $y \in P\cap Q \subseteq P$ and $z \in R \subseteq P$, so $x \in P$; clearly $x \in QR$, so $x \in P\cap(QR)$. Conversely, if $x \in P\cap QR$ then $x = qr$ with $q \in Q$ and $r \in R \subseteq P$, and therefore $q = xr^{-1} \in P$, so $x \in (P\cap Q)R$.

Now to deduce Zassenhaus's lemma, observe that by Dedekind's law, $(Y\cap B)\cap A(X\cap B) = (Y\cap B\cap A)(X\cap B) = (Y\cap A)(X\cap B)$. Then the result follows from the third isomorphism theorem.

The Jordan–Hölder Theorem We use Zassenhaus's lemma to prove the Jordan–Hölder theorem. If

$$\begin{array}{l} 1 = G_0 \lhd G_1 \lhd G_2 \quad \lhd \cdots \lhd \quad G_{n-1} \lhd G_n = G \\ 1 = H_0 \lhd H_1 \lhd H_2 \quad \lhd \cdots \lhd \quad H_{m-1} \lhd H_m = G \end{array} \tag{2}$$

are two composition series of G, then we use the second series to refine the first: in the gap between G_i and G_{i+1} we put the series

$$\begin{array}{rcl} G_i & = & (G_{i+1}\cap H_0)G_i \trianglelefteq (G_{i+1}\cap H_1)G_i \trianglelefteq (G_{i+1}\cap H_2)G_i \trianglelefteq \\ & & \cdots \trianglelefteq (G_{i+1}\cap H_{m-1})G_i \trianglelefteq (G_{i+1}\cap H_m)G_i = G_{i+1} \end{array} \tag{3}$$

Similarly, we use the first series to refine the second: in the gap between H_j and H_{j+1} we put the series

$$H_j \quad = \quad (H_{j+1}\cap G_0)H_j \trianglelefteq (H_{j+1}\cap G_1)H_j \trianglelefteq (H_{j+1}\cap G_2)H_j \trianglelefteq$$

$$\cdots \lhd (H_{j+1} \cap G_{n-1})H_j \trianglelefteq (H_{j+1} \cap G_n)H_j = H_{j+1} \tag{4}$$

Then Zassenhaus's lemma says the quotients in the refinement of the first series are equal (in some order) to the quotients in the refinement of the second series. Most of these quotients will be the trivial group: deleting repetitions gives back the two composition series.

Soluble groups A group is *soluble* if it has a composition series with abelian (hence cyclic of prime order) composition factors. A *commutator* is an element $x^{-1}y^{-1}xy$, denoted $[x,y]$, and the subgroup generated by all commutators $[x,y]$ of elements $x,y \in G$ is the *commutator subgroup* (or *derived subgroup*), written $[G,G]$ or G'. Writing $G^{(0)} = G$ and $G^{(n)} = (G^{(n-1)})'$, it follows that G is soluble if and only if $G^{(n)} = 1$ for some n. It is easy to see that $G' \trianglelefteq G$. Also G/N is abelian if and only if N contains G', so G/G' is the *largest abelian quotient* of G.

To prove this, first assume G/N is abelian, so $gN.hN = hN.gN$ for all $g,h \in G$. Therefore $gh.N = hg.N$, so $g^{-1}h^{-1}ghN = N$, so $[g,h] \in N$. Conversely, if $[g,h] \in N$ then reversing the steps of the argument gives $gN.hN = hN.gN$, so G/N is abelian.

Group actions and conjugacy classes The *right regular representation* of a group G is the identification of each element $g \in G$ with the permutation $x \mapsto xg$ of the elements of G. This shows that every finite group is isomorphic to a group of permutations (*Cayley's theorem*). If G is a group of permutations on a set Ω, and $a \in \Omega$, the *stabilizer* of a is the subgroup H of all permutations in G which map a to itself. (Exercise: verify that H is a subgroup.) Then Lagrange's theorem can be re-written as the *orbit–stabilizer theorem*, that $|G|/|H|$ equals the number of images of a under G (i.e. the *length* of the *orbit* of a).

Indeed, there is a natural bijection between the orbit Ω and the set $\{Hg \mid g \in G\}$ of (right) cosets of the stabilizer H of a point $a \in \Omega$, given by $Hg \leftrightarrow a^g$. This is well-defined and injective (one-to-one) because $Hg = Hk$ iff $gk^{-1} \in H$, iff $a^{gk^{-1}} = a$, iff $a^g = a^k$. It is surjective (onto) by definition, so is a bijection. More generally, we say a group G *acts on* a set Ω if there is a homomorphism ϕ from G to a subgroup of $\mathrm{Sym}\Omega$. If $\ker\phi = 1$ we say the action is *faithful*; in this case G is isomorphic to the image of ϕ, and we might as well say $G = \mathrm{im}\phi$.

Now let G act on itself by conjugation, $g : x \mapsto g^{-1}xg$, so that the orbits are the *conjugacy classes* $[x] = \{g^{-1}xg \mid g \in G\}$, and the stabilizer of x is the *centralizer* of x, $C_G(x) = \{g \in G \mid g^{-1}xg = x\}$. In particular, the conjugacy classes partition G, and their sizes divide the order of G. Also, the centralizer of any element is a subgroup of G.

An element x is in a conjugacy class of size 1 if and only if x *commutes* with every element of G, i.e. $x \in Z(G) = \{y \in G \mid g^{-1}yg = y \text{ for all } g \in G\}$, the *centre* of G, which is a normal subgroup of G. Indeed, the centre of G is exactly the kernel of the given action. Notice that $Z(G) = G$ if and only if G is abelian.

p-groups and nilpotent groups Example: $G = D_8 = \langle (1,2,3,4),(1,3) \rangle$ has centre $Z = Z(D_8) = \{1,(1,3)(2,4)\}$. Then the quotient

$$D_8/Z = \{Z, Z(1,3), Z(1,2)(3,4), Z(1,2,3,4)\} \cong V,$$

the Klein four-group. In particular, V is abelian, so $Z(V) = V$. In other words $Z(D_8/Z(D_8)) = D_8/Z(D_8)$.

More generally, for any group G we can define $Z_1(G) = Z(G)$ and $Z_n(G)/Z_{n-1}(G) = Z(G/Z_{n-1}(G))$. We prove by induction on n that $Z_n(G) \trianglelefteq G$. For if $Z_i(G) \trianglelefteq G$ then $Z(G/Z_i(G)) \trianglelefteq G/Z_i(G)$ so by the correspondence theorem, $Z_{i+1}(G) \trianglelefteq G$.

A finite group is called a *p-group* if its order is a power of the prime p (and so by Lagrange's Theorem all its elements have order some power of p). Every conjugacy class in G has p^a elements for some a, and $\{1\}$ is a conjugacy class, so there are at least p conjugacy classes of size 1, and $Z(G)$ has order at least p. Therefore by induction, if G is a p-group then $Z_n(G) = G$ for some n. A group with this property is called *nilpotent* (of *class* at most n), and the series

$$1 = Z_0(G) \lhd Z_1(G) \lhd Z_2(G) \lhd \cdots$$

is called the *upper central series*.

Cauchy's theorem: if q is a prime, and q divides the order of the group G, then G contains an element of order q. Proof: Let $\Omega = \{(g_1,\ldots,g_q) \mid g_i \in G, g_1.g_2.\cdots.g_q = 1\}$. Then $|\Omega| = |G|^{q-1}$ so is divisible by q. Let $C_q = \langle x \rangle$ act on Ω by $x : (g_1,\ldots,g_q) \mapsto (g_q,g_1,\ldots,g_{q-1})$. This is an action because $g_1 g_2 \cdots g_q = 1$ implies

$$1 = {g_1}^{-1} g_1 g_2 \cdots g_q . g_1 = g_2 g_3 \cdots g_q g_1.$$

The orbit lengths divide the order of the group, so are 1 or q. Now $\{(1,1,\ldots,1)\}$ is an orbit of length 1, so there are at least $q-1$ other orbits of length 1. Any such orbit is $\{(g,g,\ldots,g)\}$ with $q^q = 1$ but $g \neq 1$.

A consequence of this is that any group all of whose elements have order a power of p, has order a power of p. For otherwise, there is a prime q dividing the order of G, so by Cauchy's theorem G has elements of order q.

The *direct product* $G_1 \times \cdots \times G_k$ of groups $G_1,\ldots,G_k$ is defined on the set $\{(g_1,\ldots,g_k) \mid g_i \in G_i\}$ by the group operations $(g_1,\ldots,g_k)^{-1} = (g_1^{-1},\ldots,g_k^{-1})$ and $(g_1,\ldots,g_k)(h_1,\ldots,h_k) = (g_1h_1,\ldots,g_kh_k)$. A finite group is nilpotent if and only if it is a direct product of p-groups.

A proof in one direction follows from the fact that if G and H are nilpotent then $G \times H$ is nilpotent. This is because $Z(G \times H) = Z(G) \times Z(H)$. Proof: $(x,y) \in Z(G \times H)$ iff $(x,y)(g,h) = (g,h)(x,y)$ for all $(g,h) \in G \times H$, iff $(xg,yh) = (gx,hy)$, iff $xg = gx$ and $yh = hy$, iff $x \in Z(G)$ and $y \in Z(H)$, iff $(x,y) \in Z(G) \times Z(H)$. (We shall not give the proof in the other direction.)

Sylow's theorems If G is a finite group of order $p^k n$, where p is prime and n is not divisible by p, then the *Sylow theorems* state that

(a) G has subgroups of order p^k, called *Sylow p-subgroups*;

(b) these Sylow p-subgroups are all conjugate; and

(c) the number s_p of Sylow p-subgroups satisfies $s_p \equiv 1 \bmod p$. (Note also that, by the orbit–stabilizer theorem, s_p is a divisor of n).

To prove the first statement, let G act by right multiplication on the set Ω of all subsets S of G of size p^k: thus $g : S \mapsto Sg = \{xg \mid x \in S\}$. Now the number of these subsets is

$$|\Omega| = \binom{p^k n}{p^k} = \frac{p^k n.(p^k n-1).\cdots.(p^k n-p).\cdots.(p^k n-p^n+1)}{p^k.(p^k-1).\cdots.(p^k-p).\cdots.1}$$

and the powers of p in the terms on the top are equal to the powers of p in the corresponding terms on the bottom, so $|\Omega|$ is not divisible by p. Therefore there is an orbit of length not divisible by p, so the corresponding point stabilizer has order divisible by p^k. But if x is any element of S and g is in the stabilizer of S, then $xg \in S$, so there are at most p^k choices for xg, and therefore at most p^k choices for g. Therefore the stabilizer has order equal to p^k, and is a subgroup of G.

To prove the second statement, and also to prove that any p-subgroup is contained in a Sylow p-subgroup, let any p-subgroup Q act on the right cosets Pg of any Sylow p-subgroup P by right multiplication. Since the number of cosets is not divisible by p, but all orbits have length a power of p, by the orbit–stabilizer theorem, there is an orbit $\{Pg\}$ of length 1, so $PgQ = Pg$ and gQg^{-1} lies inside P. In particular, if P and Q have the same order, then $gQg^{-1} = P$, so all Sylow p-subgroups are conjugate in G.

To prove the third statement, let a Sylow p-subgroup P act by conjugation on the set Ω of all the other Sylow p-subgroups: we want to show that $|\Omega|$ is divisible by p. Now the orbit lengths are powers of p, so it is sufficient to show that there is no orbit of length 1. But if $\{Q\}$ is such an orbit, then $Q^x = Q$ for all $x \in P$. Therefore $P \leq N(G(Q)$ and $Q \leq N_G(Q)$ are two distinct Sylow p-subgroups of $N_G(Q)$. But this is a contradiction, since Q is normal in $N_G(Q)$, so it is the unique Sylow p-subgroup of $N_G(Q)$.

[Definition: if $H \leq G$, define $N_G(H) = \{x \in G \mid H^x = H\}$, the *normalizer* in G of H. It is a subgroup because it is the stabilizer of H in the action of G by conjugation on the conjugates H^g of H. It is the largest subgroup of G in which H is normal.]

An important corollary of Sylow's theorems is the *Frattini argument*: if $N \lhd G$ and P is a Sylow p-subgroup of N, then $G = N_G(P)N$. To prove this, pick any $g \in G$ and consider the subgroup P^g. We have $P^g \leq N^g = N$, so both P and P^g are Sylow p-subgroups of N. Therefore they are conjugate inside N, that is, there exists $h \in N$ such that $P^g = P^h$. Hence $P^{gh^{-1}} = P$, so $gh^{-1} \in N_G(P)$, and $g \in N_G(P).N$, as required.

Applications of Sylow's theorems Example: groups of order pq, where p,q are distinct primes, say $p > q$. The number of Sylow p-subgroups divides q and is congruent to 1 mod p, so is 1. Therefore G has a normal Sylow p-subgroup N, and G/N has order q. In particular G is soluble. The number of Sylow q-subgroups divides p, so is either 1 or p. In the first case, both Sylow subgroups are normal, so $G \cong C_p \times C_q \cong C_{pq}$. In the second case we must have $p \equiv 1 \bmod q$ by Sylow's theorem.

Example (continued): consider the case $q = 2$, so $P \cong C_p = \langle g \rangle \lhd G$ of index 2, and $Q \cong C_2 = \langle h \rangle$ acts on P. So $g^h = g^r$ for some integer r. Therefore $g = g^{h^2} = g^{r^2}$, so $r^2 \equiv 1 \bmod p$, which means $r \equiv \pm 1 \bmod p$. The case $r = 1$ gives $C_p \times C_2 \cong C_{2p}$ again, and the case $r = -1$ gives the dihedral group D_{2p}.

Similarly in the general case, the same argument gives $g = g^{h^q} = g^{r^q}$ so $r^q \equiv 1 \bmod p$. There are $q-1$ non-trivial solutions, all giving isomorphic groups (by replacing h by h^2, h^3, ...). For example, if $p = 7$ and $q = 3$ we could have $r = 1, 2, 4$. The first gives $C_7 \times C_3 \cong C_{21}$, and the other two gives groups $\langle g, h \mid g^7 = h^3 = 1, g^h = g^2 \rangle$ and $\langle g, k \mid g^7 = k^3 = 1, g^k = g^4 \rangle$, which are isomorphic via $k \leftrightarrow h^2$.

Automorphism groups An *automorphism* of a group G is just an isomorphism of G with itself. The set of all automorphisms of G is easily seen to form a group under composition, and is denoted $\mathrm{Aut}(G)$. The *inner* automorphisms are the automorphisms ϕ_g for $g \in G$, defined by $\phi_g : x \mapsto g^{-1}xg$. To see that this is an automorphism, observe that $\phi_g(x,y) = \phi_g(x)\phi_g(y)$. These form a subgroup $\mathrm{Inn}(G)$ of $\mathrm{Aut}(G)$. Indeed, if $\alpha \in \mathrm{Aut}(G)$, then it easy to check that $\phi_g^\alpha = \phi_{g^\alpha}$ (where $\phi_g^\alpha = \alpha^{-1}\phi_g\alpha$, read from left to right for conformity with our notation for permutations), so that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$. Proof: If $\phi_g \in \mathrm{Inn}(G)$ and $\alpha \in \mathrm{Aut}(G)$, then $\alpha^{-1}\phi_g\alpha$ maps x via $x^{\alpha-1}$ and $g^{-1}x^{\alpha^{-1}}g$ to

$$(g^{-1}x^{\alpha^{-1}}g)^\alpha = ((g^\alpha)^{-1}(x^{\alpha^{-1}})^\alpha g^\alpha = (g^\alpha)^{-1}xg^\alpha.$$

But ϕ_{g^α} maps x to the same element, for all x. Therefore $\alpha^{-1}\phi_g\alpha = \phi_{g^\alpha} \in \mathrm{Inn}(G)$.

Now it is easy to check that $\phi_{gh} = \phi_g\phi_h$, and that $\phi_g = \phi_h$ if and only if $gh^{-1} \in Z(G)$, so the map ϕ defined by $\phi : g \mapsto \phi_g$ is a homomorphism from G onto $\mathrm{Inn}(G)$ with kernel $\{g \in G \mid \phi_g = id\} = \{g \in G \mid g^{-1}xg = x\} = Z(G)$. Therefore $\mathrm{Inn}(G) \cong G/Z(G)$ and, in particular, if $Z(G) = 1$ then $G \cong \mathrm{Inn}(G)$. In this case, we can therefore identify G with $\mathrm{Inn}(G)$, and thus embed G as a normal subgroup of $\mathrm{Aut}(G)$.

We define $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$, called the *outer automorphism group* of G. Note that, despite its name, its elements are not automorphisms! It is a quotient group, not a subgroup, of $\mathrm{Aut}(G)$.

Example: $G = C_p$, p prime. Say $G = \langle g \rangle$. Then $Z(G) = G$, so $\mathrm{Inn}(G) = \{1\}$. Now any map $\alpha : g \mapsto g^r$ defines an automorphism (for $r = 1, 2, \ldots, p-1$). So $\mathrm{Aut}(G)$ has order $p-1$. In fact $\mathrm{Aut}(G) \cong C_{p-1}$ since primitive roots exist. (We'll not prove this here, but it's in other courses, e.g. cryptography.)

The structure theorem for finite abelian groups If A is a finite abelian group then

$$A \cong C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r},$$

with each n_{i+1} dividing n_i. Moreover, the n_i are uniquely determined by A.

Proof: (by induction on the order of A) Let n_1 be the largest order of any element of A. Then the order of every element divides n_1 (For if not, there is an element x of order n_1 and an element y of order k not dividing n_1, so there is an element $z = y^{\gcd(k,n_1)}$ of order $k' = k/\gcd(k,n_1)$, which is coprime to n_1. Therefore xz has order $k'n_1 > n_1$, which contradicts the choice of n_1.)

Now let $B = \langle x \rangle \cong C_{n_1}$, so that $C = A/B$ is abelian of smaller order, so by induction

$$C \cong C_{n_2} \times \cdots \times C_{n_r}$$

with each $n_{i+1}|n_i$. Also $n_2|n_1$ because n_2 is the order of some element yB in $C = A/B$, which divides the order of y in A.

We have $C = \langle x_2B \rangle \times \langle x_3B \rangle \times \cdots \times \langle x_rB \rangle$ where x_iB has order n_i in A/B, and we need to choose coset representatives $x_i' \in x_iB$ such that

$$C \cong \langle x_2' \rangle \times \cdots \times \langle x_r' \rangle \leq A.$$

We know that $y_i = (x_i)^{n_i} \in B$. Now the order of x_i divides n_1 so the order of y_i divides n_1/n_i. Since B is a cyclic group of order n_1, there is an element $z_i \in B$ with $(z_i)^{n_i} = y_i$, so if we define $x_i' = x_i {z_i}^{-1}$ then we have $(x_i')^{n_i} = y_i y_i^{-1} = 1$. Therefore

$$C \cong \langle x_2' \rangle \times \cdots \times \langle x_r' \rangle \leq A$$

as required.

Let $D = \langle x_2', \ldots, x_r' \rangle$. Then $A = BD$. But also $|A| = |B|.|D|$ so $B \cap D = \{1\}$. Therefore $A \cong B \times D$.

Finally we need to prove that the n_i are determined by the group, i.e. if we choose a different element x then we still get the same answer. So suppose that

$$C_{n_1} \times \cdots C_{n_r} \cong C_{m_1} \times \cdots \times C_{m_s},$$

with $n_{i+1}|n_i$ and $m_{i+1}|m_i$. Then the largest order of any element is n_1 and also m_1, so $m_1 = n_1$. Let i be the smallest integer such that $n_i \neq m_i$, say $n_i < m_i$. Then the number of elements of order dividing n_i is

$$(n_i)^i.n_{i+1}.n_{i+2}.\cdots.n_r = (n_i)^i|A|/(n_1.\cdots.n_i).$$

But calculating this in the second representation of the group gives

$$(n_i)^i.m_{i+1}.\cdots.m_s = (n_i)^i|A|/(n_1.\cdots.n_{i-1}.m_i).$$

Therefore $m_i = n_i$. Contradiction.

End of Chapter 1

2 Permutation groups

We first define the *symmetric group* $\mathrm{Sym}(\Omega)$ on a set Ω as the group of all permutations of that set. Here a *permutation* is simply a bijection from the set to itself. If Ω has cardinality n, then we might as well take $\Omega = \{1,\ldots,n\}$. The resulting symmetric group is denoted S_n, and called *the* symmetric group of degree n.

Since a permutation π of Ω is determined by the images $\pi(1)$ (n choices), $\pi(2)$ ($n-1$ choices, as it must be distinct from $\pi(1)$), $\pi(3)$ ($n-2$ choices), and so on, we have that the number of permutations is $n(n-1)(n-2)\ldots 2.1 = n!$ and therefore $|S_n| = n!$.

A permutation π may be written simply as a list of the images $\pi(1),\ldots,\pi(n)$ of the points in order, or more explicitly, as a list of the points $1,\ldots,n$ with their images $\pi(1),\ldots,\pi(n)$ written underneath them. For example, $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{pmatrix}$ denotes the permutation fixing 1, and mapping 2 to 5, 3 to 2, 4 to 3, and 5 to 4. If we draw lines between equal numbers in the two rows, the lines cross over each other, and the crossings indicate which pairs of numbers have to be interchanged in order to produce this permutation. In this example, the line joining the 5s crosses the 4s, 3s and 2s in that order, indicating that we may obtain this permutation by first swapping 5 and 4, then 5 and 3, and finally 5 and 2.

The alternating groups A single interchange of two elements is called a *transposition*, so we have seen how to write any permutation as a product of transpositions. However, there are many different ways of doing this. But if we write the identity permutation as a product of transpositions, and the line connecting the is crosses over the line connecting the js, then they must cross back again: thus the number of crossings for the identity element is even. If we follow one permutation by another, it is clear that the number of transpositions required for the product is the sum of the number of transpositions for the two original permutations. It follows that if π is written in two different ways as a product of transpositions, then either the number of transpositions is even in both cases, or it is odd in both cases. Therefore the map ϕ from S_n onto the group $\{\pm 1\}$ of order 2 defined by $\phi(\pi) = 1$ whenever π is the product of an even number of transpositions, is a (well-defined) group homomorphism. As ϕ is onto, its kernel is a normal subgroup of index 2, which we call the *alternating* group of degree n. It has order $\frac{1}{2}n!$, and its elements are called the *even* permutations. The other elements of S_n are the *odd* permutations.

A possibly more convincing proof that the sign of a permutation is well-defined may be obtained by letting S_n act on the set $\{\pm 1\}$ by multiplying by

$$\prod_{i>j} \frac{i^\pi - j^\pi}{i-j},$$

and proving that this does define a group action, with kernel A_n. The hard part of this is to prove that it really is a group action, that is, the action of gh is the same as the

action of g followed by the action of h. To see this, gh acts as

$$\begin{aligned}\frac{\prod(j^{gh}-i^{gh})}{\prod(j-i)} &= \frac{\prod(j^{gh}-i^{gh})}{\prod(j^g-i^g)}\frac{\prod(j^g-i^g)}{\prod(j-i)} \\ &= \frac{\prod(a^h-b^h)}{\prod(a-b)}\frac{\prod(j^g-i^g)}{\prod(j-i)}\end{aligned}$$

where $\{a,b\}$ runs over all unordered pairs of $\{i,j\}$, but in a different order.

The notation for permutations as functions (where $\pi\rho$ means ρ followed by π) is unfortunately inconsistent with the normal convention for permutations that $\pi\rho$ means π followed by ρ. Therefore we adopt a different notation, writing a^π instead of $\pi(a)$, to avoid this confusion. We then have $a^{\pi\rho} = \rho(\pi(a))$, and permutations are read from left to right, rather than right to left as for functions.

Transitivity Given a group H of permutations, i.e. a subgroup of a symmetric group S_n, we are interested in which points can be mapped to which other points by elements of the group H. If every point can be mapped to every other point, we say H is *transitive* on the set Ω. In symbols, this is expressed by saying that for all a and b in Ω, there exists $\pi \in H$ with $a^\pi = b$. In any case, the set $\{a^\pi \mid \pi \in H\}$ of points reachable from a is called the *orbit* of H containing a. It is easy to see that the orbits of H form a partition of the set Ω.

More generally, if we can simultaneously map k points wherever we like, the group is called *k-transitive*. This means that for every list of k distinct points $a_1,\ldots,a_k$ and every list of k distinct points $b_1,\ldots,b_k$ there exists an element $\pi \in H$ with $a_i^\pi = b_i$ for all i. In particular, 1-transitive is the same as transitive.

For example, it is easy to see that the symmetric group S_n is k-transitive for all $k \leq n$, and that the alternating group A_n is k-transitive for all $k \leq n-2$.

It is obvious that if H is k-transitive then H is $(k-1)$-transitive, and is therefore m-transitive for all $m \leq k$. There is however a concept intermediate between 1-transitivity and 2-transitivity which is of interest in its own right. This is the concept of primitivity, which is best explained by defining what it is not.

Primitivity A *block system* for a subgroup H of S_n is a partition of Ω preserved by H; we call the elements of the partition *blocks*. In other words, if two points a and b are in the same block of the partition, then for all elements $\pi \in H$, the points a^π and b^π are also in the same block as each other. There are two block systems which are always preserved by every group: one is the partition consisting of the single block Ω; at the other extreme is the partition in which every block consists of a single point. These are called the trivial block systems. A non-trivial block system is often called a *system of imprimitivity* for the group H. If $n \geq 3$ then any group which has a system of imprimitivity is called *imprimitive*, and any non-trivial group which is not imprimitive is called *primitive*. (It is usual also to say that S_2 is primitive, but that S_1 is neither primitive nor imprimitive.)

It is obvious that

$$\text{if } H \text{ is primitive, then } H \text{ is transitive.} \tag{5}$$

For, if H is not transitive, then the orbits of H form a system of imprimitivity for H, so H is not primitive. On the other hand, there exist plenty of transitive groups which are not primitive. For example, in S_4, the subgroup H of order 4 generated by $\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$ and $\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$ is transitive, but preserves the block system $\{\{1,2\},\{3,4\}\}$. It also preserves the block systems $\{\{1,3\},\{2,4\}\}$ and $\{\{1,4\},\{2,3\}\}$.

Example: D_8 acting on 4 vertices $1,2,3,4$ of a square, generated by the rotation $(1,2,3,4)$ and a reflection $(1,3)$, preserves the partition $\{\{1,3\},\{2,4\}\}$, in the sense that every group element maps each part of the partition to itself or another part of the partition. So here $(1,3)$ fixes the two part of the partition, while $(1,2,3,4)$ maps $\{1,3\}$ to $\{2,4\}$ and vice versa. The permutation action on the parts of the partition gives rise to a quotient group. In this example the quotient is S_2, and the generators of D_8 map to -1 and 1 respectively in the quotient. The kernel of this action is the normal subgroup $\{1,(1,3),(2,4),(1,3)(2,4)\} \cong C_2 \times C_2$.

Another important basic result about primitive groups is that

$$\text{every 2-transitive group is primitive.} \tag{6}$$

For, if H is imprimitive, we can choose three distinct points a, b and c such that a and b are in the same block, while c is in a different block. (This is possible since the blocks have at least two points, and there are at least two blocks.) Then there can be no element of H taking the pair (a,b) to the pair (a,c), so it is not 2-transitive.

Example: D_8in its natural action on 4 points is transitive but not primitive. D_{10} in its natural action on 5 points is primitive but not 2-transitive.

Example: S_5 acting on unordered pairs of 5 points is transitive, but not 2-transitive, since it is not possible to map $\{1,2\}$ to itself and simultaneously map $\{1,3\}$ to $\{4,5\}$. To see this another way, look at the stabilizer of $\{1,2\}$. This is a group $S_2 \times S_3$ generated by $(1,2),(3,4),(4,5)$, and its orbits on the pairs have lengths 1, 3 and 6. Therefore any block containing $\{1,2\}$ would be a union of some of these orbits, so would have length 4 or 7. But neither of these numbers divides 10, so the action is primitive.

Group actions Suppose that G is a subgroup of S_n acting transitively on Ω. Let H be the stabilizer of the point $a \in \Omega$, that is, $H = \{g \in G : a^g = a\}$. Recall (the orbit–stabilizer theorem) that the points of Ω are in natural bijection with the (right) cosets Hg of H in G. This bijection is given by $Hx \leftrightarrow a^x$. In particular, $|G:H| = n$.

We can turn this construction around, so that given any subgroup H in G, we can let G act on the right cosets of H according to the rule $(Hx)^g = Hxg$. Numbering the cosets of H from 1 to n, where $n = |G:H|$, we obtain a permutation action of G on these n points, or in other words a group homomorphism from G to S_n.

Maximal subgroups This correspondence between transitive group actions on the one hand, and subgroups on the other, permits many useful translations between combinatorial properties of Ω and properties of the group G. For example, a primitive group action corresponds to a maximal subgroup, where a subgroup H of G is called *maximal* if there is no subgroup K with $H < K < G$. More precisely:

Proposition 1 *Suppose that the group G acts transitively on the set Ω, and let H be the stabilizer of $a \in \Omega$. Then G acts primitively on Ω if and only if H is a maximal subgroup of G.*

Proof. oqed=Fndisplskip=F We prove both directions of this in the contrapositive form. First assume that H is not maximal, and choose a subgroup K with $H < K < G$. Then the points of Ω are in bijection with the (right) cosets of H in G. Now the cosets of K in G are unions of H-cosets, so correspond to sets of points, each set containing $|K : H|$ points. But the action of G preserves the set of K-cosets, so the corresponding sets of points form a system of imprimitivity for G on Ω.

Conversely, suppose that G acts imprimitively, and let Ω_1 be the block containing a in a system of imprimitivity. Since G is transitive, it follows that the stabilizer of Ω_1 acts transitively on Ω_1, but not on Ω. Therefore this stabilizer strictly contains H and is a proper subgroup of G, so H is not maximal.

For example, consider S_n acting on the set $\Omega = \{\{1,2\},\ldots,\{n-1,n\}\}$ of $n(n-1)/2$ unordered pairs from n points. The stabilizer H of $\{1,2\}$ is $S_2 \times S_{n-2}$, and provided $n > 4$ this subgroup is maximal: if $g \notin H$, then there are points $i, j > 2$ such that $i^g \in \{1,2\}$ but j^g is not. Then the transposition (i^g, j^g) is in the subgroup generated by H and g, and therefore so are all the transpositions. It follows that S_n acts primitively on the given $n(n-1)/2$ objects.

Wreath products The concept of imprimitivity leads naturally to the idea of a *wreath product* of two permutation groups. Recall the *direct product*

$$G \times H = \{(g,h) : g \in G, h \in H\} \tag{7}$$

with identity element $1_{G\times H} = (1_G, 1_H)$ and group operations

$$\begin{aligned} (g_1,h_1)(g_2,h_2) &= (g_1,g_2,h_1h_2) \\ (g,h)^{-1} &= (g^{-1},h^{-1}). \end{aligned} \tag{8}$$

Recall also the *semidirect product* $G{:}H$ or $G{:}_\phi H$, where $\phi : H \to \mathrm{Aut}(G)$ describes an action of H on G. We define $G{:}H = \{(g,h) : g \in G, h \in H\}$ with identity element $1_{G:H} = (1_G, 1_H)$ and group operations

$$\begin{aligned} (g_1,h_1)(g_2,h_2) &= (g_1 g_2^{\phi(h_1^{-1})},h_1h_2) \\ (g,h)^{-1} &= ((g^{-1})^{\phi(h)},h^{-1}). \end{aligned} \tag{9}$$

Most of the group axioms are obvious, but associativity takes a little work to check:

$$\begin{aligned}((g_1,h_1)(g_2,h_2))(g_3,h_3) &= (g_1 g_2^{\phi(h_1^{-1})}, h_1h_2)(g_3,h_3)\\ &= (g_1 g_2^{\phi(h_1^{-1})} g_3^{\phi((h_1h_2)^{-1})}, h_1h_2h_3)\\ (g_1,h_1)((g_2,h_2)(g_3,h_3) &= (g_1,h_1)(g_2 g_3^{\phi(h_2^{-1})}, h_2h_3)\\ &= (g_1(g_2g_3)^{\phi(h_2^{-1})})^{\phi(h_1^{-1})}, h_1h_2h_3)\end{aligned}$$

which is the same thing since ϕ is a group homomorphism.

Example: $G = C_2 \times C_2 = \{1,a,b,ab\}$ with $a^2 = b^2 = (ab)^2 = 1$, and $H = C_3 = \langle h\rangle$, with action given by $\phi(h) : a \mapsto b \mapsto ab \mapsto a$. Then for example $(a,h)(b,h) = (ab^{\phi(h^{-1})}, h^2) = (aa, h^2) = (1,h^2)$. You can check that $G{:}_\phi H \cong A_4$ via $(a,1) \mapsto (1,2)(3,4)$, $(b,1) \mapsto (1,3)(2,4)$, $(1,h) \mapsto (1,3,2)$. (Don't get confused by the notation $(a,1)$ meaning an ordered pair and the same notation $(1,2)$ meaning the transposition swapping 1 and 2.)

The subgroup $\{(g,1) \mid g \in G\}$ is obviously isomorphic to G. Moreover it is normal, since

$$\begin{aligned}(g,h)^{-1}(g_1,1)(g,h) &= ((g^{\phi(h)})^{-1}, h^{-1})(g_1g,h)\\ &= (g_2,h)\end{aligned}$$

for some $g_2 \in G$. The subgroup $\{(1,h) \mid h \in H\}$ is obviously isomorphic to H, but is not normal in general. The special case when $\phi(h) = 1$ for all h is the direct product.

Now suppose that H is a permutation group acting on $\Omega = \{1,\ldots,n\}$. Define $G^n = G \times G \times \cdots \times G = \{(g_1,\ldots,g_n) : g_i \in G\}$, the direct product of n copies of G, and let H act on G^n by permuting the n subscripts. That is $\phi : H \to \mathrm{Aut}(G^n)$ is defined by

$$\phi(\pi) \quad : \quad (g_1,\ldots,g_n) \mapsto (g_{1\pi^{-1}},\ldots,g_{n\pi^{-1}}). \tag{10}$$

Then the *wreath product* $G \wr H$ is defined to be $G^n{:}_\phi H$. For example, if $H \cong S_n$ and $G \cong S_m$ then the wreath product $S_m \wr S_n$ can be formed by taking n copies of S_m, each acting on one of the sets Ω_1, ..., Ω_n of size m, and then permuting the subscripts 1, ..., n by elements of H. This gives an imprimitive action of $S_m \wr S_n$ on $\Omega = \bigcup_{i=1}^n \Omega_i$, preserving the partition of Ω into the Ω_i. More generally, any (transitive) imprimitive group can be embedded in a wreath product: if the blocks of imprimitivity for G are $\Omega_1, \ldots, \Omega_k$, then G is a subgroup of $\mathrm{Sym}(\Omega_1) \wr S_k$.

Iwasawa's Lemma and simplicity The key to proving simplicity of many of the finite simple groups is Iwasawa's Lemma:

Theorem 2 *If G is a finite perfect group, acting faithfully and primitively on a set Ω, such that the point stabilizer H has a normal abelian subgroup A whose conjugates generate G, then G is simple.*

Proof. oqed=Fndisplskip=F For otherwise, there is a normal subgroup K with $1 < K < G$, which does not fix all the points of Ω, so we may choose a point stabilizer H with $K \not\leq H$. Therefore HK is a subgroup (since K is normal) which is strictly bigger then H, and so $G = HK$ since H is a maximal subgroup of G. So any $g \in G$ can be written $g = hk$ with $h \in H$ and $k \in K$, and therefore every conjugate of A is of the form $g^{-1}Ag = k^{-1}h^{-1}Ahk = k^{-1}Ak \leq AK$, since A is normal in H and K is normal in G. But G is generated by these A^k so $G = AK$. Therefore $G/K = AK/K \cong A/A \cap K$ is abelian, contradicting the assumption that G is perfect.

To see this in action, let us prove that A_n is simple whenever $n \geq 7$. (The argument also works for $n = 5$, but needs slight modification if $n = 6$.) Let Ω be the set of unordered triples (i.e. subsets of size 3) from the set $\{1, 2, \ldots, n\}$. The stabilizer of one of these triples is $A_n \cap (S_3 \times S_{n-3})$, which has a normal subgroup of order 3, cyclically permuting the three points in the triple. These 3-cycles generate the alternating group. Also, provided $n \geq 5$, they are commutators, since $(a,b,c) = (a,b)(d,e)(a,c)(d,e) = [(ac)(de),(bc)(de)]$.Therefore every one of the generators is in the commutator subgroup, so the commutator subgroup is the whole group. To show that the action of A_n on triples is faithful, observe that if $\{a,b,c\}$ and $\{a,d,e\}$ are fixed, then so is the point a: thus if all triples are fixed, then all points are fixed. Finally, we need to show that the action of A_n on Ω is primitive. We can prove this by showing by brute force that the stabilizer H of a triple is maximal. (Iit isn't maximal if $n = 6$, so we need a different proof in this case.) Then apply Iwasawa's Lemma.

To show maximality of H, let H be the stabilizer of the triple $\{1,2,3\}$ and let g be any element of A_n not in H. Letting $K = \langle H, g \rangle$, we want to show that K contains all the 3-cycles. Without loss of generality we can assume g maps 4 to 1 and 5 to a point not in the triple. Then 6 could map either into or outside the triple. Therefore g conjugates the 3-cycle $(4,5,6)$ either to w.l.o.g. $(1,6,2)$ or $(1,6,7)$. In the former case it contains also $(2,7,3)$ and therefore contains $(1,6,2)^{(2,7,3)} = (1,6,7)$, and in the latter case it contains also $(2,6,7)$ and therefore contains $(1,6,7)^(2,6,7) = (1,7,2)$. Now in both cases, conjugating these 3-cycles by elements of H gives us all the 3-cycles in A_n, as required.

In the case $n = 6$, the action on triples is *not* primitive, because each triple comes with its complement. Thus the 20 triples come in 10 pairs of complementary triples, thus: $(123|456)$, $(124|356)$ etc. It is easy to see that the stabilizer of $(123|456)$ contains the 3-cycles $(1,2,3)$ and $(4,5,6)$ and is transitive on the other 9 objects. Therefore A_6 acts 2-transitively, so primitively.

More on automorphisms More generally, if $G \trianglelefteq H$, then each element of H induces an automorphism of G, by conjugation in H. Thus for example if $n \geq 4$ then S_n is (isomorphic to) a subgroup of $\mathrm{Aut}(A_n)$. It turns out that for $n \geq 7$ it is actually the whole of $\mathrm{Aut}(A_n)$. We shall not prove this here.

Observe that, since $(a,b,c)(a,b,d) = (a,d)(b,c)$, the group A_n is generated by its 3-cycles. Indeed, it is generated by the 3-cycles $(1,2,3)$, $(1,2,4)$, $\ldots$, $(1,2,n)$. Also

note that for $n \geq 5$, A_n has no subgroup of index k less than n—for if it did there would be a homomorphism from A_n onto a transitive subgroup of A_k, contradicting the fact that A_n is simple.

The outer automorphism of S_6 Of all the symmetric groups, S_6 is perhaps the most remarkable. One manifestation of this is its exceptional outer automorphism. This is an isomorphism from S_6 to itself which does not correspond to a permutation of the underlying set of six points. What this means is that there is a completely different way for S_6 to act on six points.

To construct a non-inner automorphism ϕ of S_6 we first note that ϕ must map the point stabilizer S_5 to another subgroup $H \cong S_5$. However, H does not fix one of the six points on which S_6 acts. Therefore H is transitive on these six points.

So our first job is to construct a transitive action of S_5 on six points. This may be obtained in a natural way as the action of S_5 by conjugation on its six Sylow 5-subgroups. (If we wish to avoid using Sylow's theorems at this point we can simply observe that the 24 elements of order 5 belong to six cyclic subgroups $\langle(1,2,x,y,z)\rangle$, and that these are permuted transitively by conjugation by elements of S_5.)

In other words, we have constructed a group homomorphism $\phi : S_5 \to S_6$ such that $\phi(S_5)$ is a transitive subgroup H of S_6. Now H has order 120, so index 6, and therefore we can construct the action of S_6 by right multiplication on the 6 right cosets of H. In this action, H fixes the identity coset H, and permutes the other 5 cosets. Therefore this is a different action of S_6 from the natural action, where H acts transitively. Any permutation in S_6 acts in some way on the cosets of H: if we relabel these cosets with the numbers 1 to 6, then for each permutation in S_6 we get another one, given by this action on the cosets of H. This gives us an automorphism of S_6 which is not inner.

More explicitly, we have a group homomorphism $\phi : S_6 \to \mathrm{Sym}(\{Hg : g \in S_6\}) \cong S_6$. The kernel of ϕ is trivial, since S_6 has no non-trivial normal subgroups of index 6 or more. Hence ϕ is a group isomorphism, i.e. an automorphism of S_6. But ϕ is not an inner automorphism, because it maps the transitive subgroup H to the stabilizer of the trivial coset H, whereas inner automorphisms preserve transitivity.

There is another, more concrete, way to see this outer automorphism. From the six points we get 15 unordered pairs. Each point corresponds to the 5 pairs it is contained in. Now consider the partitions into three pairs: each pair is in 3 such partitions, so the number of these partitions is also 15. Call these partitions 'synthemes', and write them as 12|34|56, 12|35|46, 12|36|45, ..., 16|25|34. Now our automorphism is going to swap the pairs with the synthemes, so what does it do to the points? A point must map to something corresponding to 5 synthemes. The 'obvious' thing is a set of 5 synthemes which between them contain all 15 pairs, once each. Such a set of synthemes is called a 'synthematic total'. There are 6 such totals, as you can readily check:

$$\begin{array}{ll} A: & 12|34|56, 13|25|46, 14|26|35, 15|36|24, 16|23|45 \\ B: & 12|34|56, 13|26|45, 14|25|36, 15|23|46, 16|35|24 \end{array}$$

$$
\begin{array}{ll}
C: & 12|35|46, 13|24|56, 14|36|25, 15|26|34, 16|23|45 \\
D: & 12|35|46, 13|26|45, 14|23|56, 15|24|36, 16|34|25 \\
E: & 12|36|45, 13|24|56, 14|35|26, 15|23|46, 16|25|34 \\
F: & 12|36|45, 13|25|46, 14|23|56, 15|34|26, 16|24|35
\end{array}
$$

The generators $(1,2)$ and $(2,3,4,5,6)$ act on these totals as $(A,B)(C,D)(E,F)$ and $(A,B,D,F,C)(E)$ respectively. Relabelling A,B,C,D,E,F as $1,2,3,4,5,6$ we obtain an automorphism of S_6 as

$$
\begin{array}{rcl}
(1,2) & \mapsto & (1,2)(3,4)(5,6) \\
(2,3,4,5,6) & \mapsto & (1,2,4,6,3)
\end{array}
$$

Incidentally, S_6 is the only symmetric group with a non-trivial outer automorphism group. We shall not prove this here.

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 $(F\setminus\{0\},.,/,1)$ 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, $v_1,\ldots,v_n$, 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.]

Example: if $f(x)$ is an irreducible polynomial of degree d over $\mathbb{F}_p$, where $\mathbb{F}_p$ denotes the field of order p, then the quotient ring $\mathbb{F}_p[x]/(f(x))$ is a field of order p^d. All the field axioms are obvious except for the existence of inverses. But if $g(x)$ is a coset representative which is not divisible by $f(x)$, then by Euclid's algorithm for polynomials there are polynomials $s(x)$ and $t(x)$ such that $1=s(x)g(x)+t(x)f(x)$, so that $s(x)$ is an inverse to $g(x)$ modulo $f(x)$.

Example: $\mathbb{F}_3[x]/(x^2+1)=\{0,\pm1,\pm x,\pm x\pm1\}$ is a field of order 9, where $x^2+1=0$, i.e. $x^2=-1$.

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 $(xy)^q=x^qy^q=xy$ and $(x+y)^q=x^q+y^q=x+y$. Hence this set of roots is a subfield. This polynomial has no repeated roots, as it is coprime to its formal

derivative, so the field has 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 $\mathrm{Aut}(F)$ is cyclic of order d.

General linear groups. Let V be a vector space of dimension n over the finite field $F = \mathbb{F}_q$ of order q. Then V has a basis $\{v_1, \ldots, v_n\}$, say, and $V = \{\sum_{i=1}^n \lambda_i v_i \mid \lambda_i \in F\}$. Moreover, if $\sum_{i=1}^n \lambda_i v_i = 0$ then all $\lambda_i = 0$. Since there are q choices for each λ_i we have $|V| = |F|^n = q^n$. Hence V is isomorphic to the standard space of n-tuples $(\lambda_1, \ldots, \lambda_n)$, with vector space operations

$$\begin{aligned}(\lambda_1, \ldots, \lambda_n) + (\mu_1, \ldots, \mu_n) &= (\lambda_1 + \mu_1, \ldots, \lambda_n + \mu_n)\\ \mu(\lambda_1, \ldots, \lambda_n) &= (\mu\lambda_1, \ldots, \mu\lambda_n)\end{aligned}$$

Linear maps on V are maps $f : V \to V$ such that

$$f(\lambda v + w) = \lambda f(v) + f(w).$$

They can be represented by matrices with respect to a basis, i.e.

$$f(v_i) = \sum_{j=1}^{n} f_{ij} v_j.$$

The *general linear group* $\mathrm{GL}(V)$ 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 $\mathrm{GL}(V)$ with the group (denoted $\mathrm{GL}_n(q)$) of invertible $n \times n$ matrices over $\mathbb{F}_q$.

There are certain obvious normal subgroups of $G = \mathrm{GL}_n(q)$. 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 $\mathrm{PGL}_n(q)$.

Also, since $\det(AB) = \det(A)\det(B)$, the determinant map is a group homomorphism from $\mathrm{GL}_n(q)$ 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* $\mathrm{SL}_n(q)$, and consists of all the matrices of determinant 1. Similarly, we can quotient $\mathrm{SL}_n(q)$ by the subgroup of scalars it contains, to obtain the *projective special linear group* $\mathrm{PSL}_n(q)$, sometimes abbreviated to $\mathrm{L}_n(q)$. [The alert reader will have noticed that as defined

here, $\mathrm{PSL}_n(q)$ is not a necessarily a subgroup of $\mathrm{PGL}_n(q)$. However, there is an obvious isomorphism between $\mathrm{PSL}_n(q)$ and a normal subgroup of $\mathrm{PGL}_n(q)$, 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 ith 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 $\mathrm{GL}_n(q)$ is

$$\begin{aligned} |\mathrm{GL}_n(q)| &= (q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}) \\ &= q^{n(n-1)/2}(q-1)(q^2-1)\cdots(q^n-1). \end{aligned} \tag{11}$$

The orders of $\mathrm{SL}_n(q)$ and $\mathrm{PGL}_n(q)$ are equal, being $|\mathrm{GL}_n(q)|$ divided by $q-1$. To obtain the order of $\mathrm{PSL}_n(q)$, 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 $q-1$. (This is because we know that $x^{q-1} = 1$ for all non-zero elements x, so that $x^n = 1$ is equivalent to $x^{\gcd(n,q-1)} = 1$: but the latter equation has exactly $\gcd(n,q-1)$ solutions in the cyclic group of order $q-1$.) Thus the order of $\mathrm{PSL}_n(q)$ is

$$|\mathrm{PSL}_n(q)| = \frac{1}{(n,q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1). \tag{12}$$

The groups $\mathrm{PSL}_n(q)$ are all simple except for the small cases $\mathrm{PSL}_2(2) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$. We shall prove the simplicity of these groups below.

Example: $\mathrm{PSL}_2(2) \cong \mathrm{GL}_2(2)$, and $\mathrm{GL}_2(2)$ 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 $\mathrm{GL}_2(2)$ is 2-transitive, and faithful, so $\mathrm{GL}_2(2) \cong S_3$. More explicitly,

$$\mathrm{GL}_2(2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}.$$

Writing a, b, c for the row vectors $(1,0)$, $(0,1)$, $(1,1)$ respectively, the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ acts as the permutation $(a,b)(c)$, while the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ acts as $(a,c)(b)$, and these permutations generate S_3.

Example: $\mathrm{GL}_2(3)$ has order $(3^2-1)(3^2-3) = 48$ so $\mathrm{PGL}_2(3)$ has order 24. Similarly, $\mathrm{GL}_2(3)$ 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 $\mathrm{GL}_2(3)$ 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 $\mathrm{PSL}_2(3) \cong A_4$.

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

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

$$\begin{array}{rcl} \mathrm{PSL}_2(2) & \cong & S_3, \\ \mathrm{PSL}_2(3) & \cong & A_4, \\ \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) & \cong & A_5, \\ \mathrm{PSL}_2(9) & \cong & A_6 \end{array} \tag{13}$$

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 $\mathrm{PSL}_2(q)$ 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 $\mathrm{PL}(q)$. The matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(q)$ 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,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ z \mapsto \frac{az+b}{cz+d}. \tag{14}$$

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 $\{0, 1, \omega, \overline{\omega}\}$ where $\overline{\omega} = \omega^2$ and $\omega^2 + \omega = 1$. Fixing the points 0 and ∞ in $PL(4) = \{\infty, 0, 1, \omega, \overline{\omega}\}$ we still have the map $z \mapsto \overline{\omega} z/\omega = \omega z$ (defined by the matrix $\begin{pmatrix} \overline{\omega} & 0 \\ 0 & \omega \end{pmatrix}$) which acts as a 3-cycle on the remaining three points 1, ω, $\overline{\omega}$. 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 general case. The 2-dimensional vector space over $\mathbb{F}_q$ has q^2-1 non-zero vectors, so $(q^2-1)/(q-1) = q+1$ subspaces of dimension 1, namely $\langle(1,0)\rangle$ (call this $\infty = 1/0$) and $\langle(x,1)\rangle$ (call this $x = x/1$). So $\langle(x,y)\rangle = \langle y^{-1}(x,y)\rangle = \langle(y^{-1}x,1)\rangle$ is called $y^{-1}x$ or x/y. If $y=0$, then $\langle(x,y)\rangle = \langle(x,0)\rangle = \langle(1,0)\rangle$ which corresponds to ∞, and again $x/y = \infty$.

The group $\mathrm{GL}_2(q)$ permutes these $q+1$ subspaces. The *projective line* $\mathrm{PL}(q) = \mathbb{F}_q \cup \{\infty\}$. Working with column vectors instead of row vectors we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

so this matrix acts as $x/y \mapsto (ax+by)/(cx+dy)$ i.e. $z \mapsto (az+b)/(cx+d)$. For example, if $q=5$ then $\begin{pmatrix} 2 & 1 \\ 3 & 3 \end{pmatrix} : z \mapsto (2z+1)/(3z+3)$ so acts as the permutation $(0,2)(1,3)(4,\infty)$.

This gives a homomorphism $\mathrm{GL}_2(q) \to \mathrm{Sym}(\mathrm{PL}(q)) \cong S_{q+1}$. To calculate the kernel of the action, note that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ acts as the identity then it maps 0 to 0, so $(a0+b)/(c0+d) = 0$ and therefore $b=0$; also $\infty \mapsto \infty$ so $(a\infty+b)/(c\infty+d) = \infty$ so $a/c = \infty$ i.e. $c=0$; and $1 \mapsto 1$ so $(a+b)/(c+d) = 1$ so $a=d$. Conversely, $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ maps z to $az/a = z$ for all z. Therefore the kernel of the action is exactly the group of scalar matrices, and the quotient by the kernel is $\mathrm{PGL}_2(q)$.

Example: $q=5$. The projective line $\mathrm{PL}(5) = \{\infty,0,1,2,3,4\}$. We saw that $\mathrm{PGL}_2(5)$ has order $(5^2-1)(5^2-5)/(5-1) = 120 = 5!$, and in fact $\mathrm{PGL}_2(5) \cong S_5$. To prove this, recall the action of S_5 by conjugation on its 6 Sylow 5-subgroups. We show that we can label these subgroups by the 6 points of the projective line, in such a way that the action of S_5 by conjugation on the subgroups is the same as the action of $\mathrm{PGL}_2(5)$ on the points of the projecive line. Many such labellings are possible: here is one.

$$\begin{aligned} H_\infty &= \langle(1,2,3,4,5)\rangle \\ H_0 &= \langle(1,2,4,3,5)\rangle \\ H_1 &= \langle(2,3,5,4,1)\rangle \\ H_2 &= \langle(3,4,1,5,2)\rangle \\ H_3 &= \langle(4,5,2,1,3)\rangle \\ H_4 &= \langle(5,1,3,2,4)\rangle \end{aligned}$$

Check the generators $(1,2)$ and $(1,2,3,4,5)$ for S_5. Now $(1,2,3,4,5)$ acts on the H_t as $(H_\infty)(H_0,H_1,H_2,H_3,H_4)$ so corresponds to the map $z \mapsto (z+1)/(2z+4)$, which is the permutation $(\infty,3)(0,4)(1,2)$of the projective line.

So our homomorphism $\phi : S_5 \to \mathrm{PGL}_2(5)$ has image of size bigger than 2, so is onto (since the only normal subgroups of S_5 are $1, A_5, S_5$). But S_5 and $\mathrm{PGL}_2(5)$ both have order 120, so they are isomorphic. It follows that the two maps $z \mapsto z+1$ and $z \mapsto (z+1)/(2z+4)$ generate $\mathrm{PGL}_2(5)$.

The isomorphism $\mathrm{PSL}_2(5) \cong A_5$**.** The isomorphism $\mathrm{PSL}_2(5) \cong A_5$ 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 $\phi : A_5 \to \mathrm{L}_2(5)$, which is easily seen to be injective. Moreover $|A_5| = |\mathrm{L}_2(5)|$, so the two groups are isomorphic.

Generators for $\mathrm{PGL}_2(q)$ **and** $\mathrm{PSL}_2(q)$**.** More generally, $z \mapsto z+\lambda$ is in $\mathrm{PGL}_2(q)$ for any $\lambda \in \mathbb{F}_q$. These elements form a subgroup isomorphic to the additive group of the field. Similarly, if $\lambda \neq 0$ then $z \mapsto \lambda z$ is in $\mathrm{PGL}_2(q)$ (represented by the matrix $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(q)$). These form a subgroup isomorphic to the multiplicative group of the field. Moreover this subgroup normalizes the additive subgroup

$$z \mapsto \lambda z \mapsto \lambda z + \mu \mapsto \lambda^{-1}(\lambda z + \mu) = z + \lambda^{-1}\mu.$$

So these two subgroups together form a group of order $q(q-1)$ consisting of all maps $z \mapsto \lambda z + \mu$ with $a \neq 0$. This group fixes ∞ and conversely it is the full stabilizer of ∞ (by the orbit–stabilizer theorem, since there are $q = 1$ points and the group $\mathrm{PGL}_2(q)$ has order $(q^2-1)q = (q+1)q(q-1)$).

The map $z \mapsto 1/z$ extends this subgroup to the whole of $\mathrm{PGL}_2(q)$. The corresponding matrices $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ generate $\mathrm{GL}_2(q)$.

As a corollary, note that $\mathrm{PGL}_2(q)$ acts 3-transitively on the projective line. For it is obviously transitive, and $z \mapsto z+\lambda$ fixes ∞ and is transitive on the other q points. Finally, $z \mapsto \lambda z$ fixes ∞ and 0, and is transitive on the rest of the points.

Now $\mathrm{PSL}_2(q)$ has index $(2, q-1)$ in $\mathrm{PGL}_2(q)$. So if $q = 2^k$ then $\mathrm{PSL}_2(q) \cong \mathrm{PGL}_2(q)$. if q is odd then $\mathrm{PSL}_2(q)$ has index 2 in $\mathrm{PGL}_2(q)$, generated by

$$\begin{array}{rcl} z & \mapsto & z+\lambda \\ z & \mapsto & \lambda^2 z \\ z & \mapsto & -1/z \end{array}$$

corresponding to the matrices of determinant 1:

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

The stabilizer of ∞ then has order $q(q-1)/2$ and consists of all maps of the form $z \mapsto \lambda^2 z + \mu$.

The isomorphism $\mathrm{PSL}_2(9) \cong A_6$**.** The isomorphism $\mathrm{PSL}_2(9) \cong A_6$ 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 $i^2 = -1$. The additive group is $C_3 \times C_3$, generated by 1 and i. The multiplicative group is C_8, generated by $1+i$, say. So the stabilizer of the point ∞ is generated by $z \mapsto z+1$ and $z \mapsto iz$, and has order 36. We want this to correspond to the stabilizer of a partition of the 6 points into two threes. Now the stabilizer of $(123|456)$ is generated by $(1,2,3)$ and $(1,4)(2,5,3,6)$.

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 have

$$\begin{aligned}
\infty &\mapsto (123|456)\\
0 &\mapsto (423|156)\\
1 &\mapsto (431|256)\\
-1 &\mapsto (412|356)\\
i &\mapsto (523|164)\\
1+i &\mapsto (531|264)\\
-1+i &\mapsto (512|364)\\
-i &\mapsto (623|145)\\
1-i &\mapsto (631|245)\\
-1-i &\mapsto (612|345)
\end{aligned}$$

Now $z \mapsto z+1$ corresponds to the permutation $(1,2,3)$, and $z \mapsto iz$ corresponds to $(1,4)(2,5,3,6)$. 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 $\mathrm{PSL}_2(9)$ 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 $S_6 \cong \mathrm{P\Sigma L}_2(9)$, which is not isomorphic to $\mathrm{PGL}_2(9)$. Indeed, $\mathrm{PGL}_2(9)$ contains the element $z \mapsto (1+i)z$ of order 8, but S_6 has no elements of order 8.

The actions of $\mathrm{PSL}_2(11)$ on 11 points. (This section was not lectured in 2008.)

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.

Simplicity of $\mathrm{PSL}_n(q)$. We shall first prove that $\mathrm{PSL}_2(q)$ is simple if and only if $q \geq 4$. (We shall consider $\mathrm{PSL}_n(q)$ for $n \geq 3$ later on.) First note that if $q \leq 3$ we have $\mathrm{PSL}_2(2) \cong S_3$ and $\mathrm{PSL}_2(3) \cong A_4$, neither of which is simple.

Conversely, we have shown that $\mathrm{PSL}_2(q)$ acts faithfully, and 2-transitively, so primitively, on the projective line $\mathbb{F}_q \cup \{\infty\}$. The stabilizer of the point ∞ consists of all maps $z \mapsto a^2 z + b$. (If $q = 2^k$, then the map $a \mapsto a^2$ is an automorphism of the field, so a^2 is an arbitrary non-zero element. If q is odd, exactly half of the non-zero elements of $\mathbb{F}_q$ are squares.)

The subgroup $A = \{z \mapsto z+b \mid b \in \mathbb{F}_q\}$ is an abelian normal subgroup of the point stabilizer. If $q > 3$, then $\mathbb{F}_q$ contains a non-zero element x with $x^2 \neq 1$, and then the commutator

$$\left[\begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix}\right] = \begin{pmatrix} 1 & y(x^2-1) \\ 0 & 1 \end{pmatrix}, \tag{15}$$

which is an arbitrary element of A. Therefore every conjugate of A lies in the derived subgroup. The only remaining thing to check is that $\mathrm{PSL}_2(q)$ is generated by conjugates of A. We can now apply Iwasawa's Lemma, and deduce that $\mathrm{PSL}_2(q)$ is simple provided $q > 3$.

Now consider the case of $\mathrm{PSL}_n(q)$ where $n \geq 3$. 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 $\langle (1,0,\ldots,0) \rangle$. The stabiliser then consists of all matrices whose first row is $(\lambda,0,\ldots,0)$. 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. 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

$$\left[\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & x & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -x & 0 & 1 \end{pmatrix}, \tag{16}$$

so by suitable choice of basis we see that if $n > 2$ then every transvection is a commutator in $\mathrm{SL}_n(q)$. We can now apply Iwasawa's Lemma, and deduce that $\mathrm{PSL}_n(q)$ is simple provided $n > 2$.

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.