Topics in Discrete Mathematics MA30002 Permutation Groups

Dr. Justin M^{c}Inroy

February 20, 2015

In the part of the course, we will be looking at actions of groups on various combinatorial objects. We will mostly focus on transitive groups and will look at primitive and imprimitive actions, before turning our attention to multiply transitive actions. Our aim is to give a brief overview of this topic and in particular show that primitive groups are small and rare and that multiply transitive groups are also rare. These notes are a *brief* introduction to the topic - there is much material that couldn't be covered here for time reasons. Also, in many examples, assertions (sometimes implicit) are made about things being groups, or something being an action etc. These are often flagged, but even if not these should be checked by the reader!

Any good book on undergraduate group theory will be a good place to look at actions and many will include discussion of transitive, primitive and imprimitive actions. More specialised, but harder, books are the following. The second has a more computational flavour.

- Permutation Groups, Dixon and Mortimer, Graduate Texts in Mathematics, 163. Springer-Verlag, New York, 1996. xii+346 pp. ISBN: 0-387-94599-7

- Permutation Groups, Cameron, London Mathematical Society Student Texts, 45. Cambridge University Press, Cambridge, 1999. x+220 pp. ISBN: 0-521-65302-9; 0-521-65378-9

1 Background

We will begin by briefly recalling some basic definitions which you have seen before.

Definition 1.1 A *group* G is a non-empty set G together with a binary operation, called multiplication, such that the following axioms hold:

(1) For all $g, h \in G$, their product gh is in G.

(2) There exists an identity $1 \in G$, such that $1g = g1 = g$ for all $g \in G$.

(3) For every $g \in G$ there exists an inverse $g^{-1} \in G$ such that $gg^{-1} = g^{-1}g = 1$.

(4) The group multiplication is associative. That is, $g(hk) = (gh)k$, for all $g, h, k \in G$.

In this course we will focus on finite groups, although much of the theory, with some alterations, can be extended to infinite groups.

We denote by S_n the *symmetric group* of all permutations on the set $\{1, \ldots, n\}$. The *alternating group* is denoted A_n and is the group of all even permutations, that is, those which are the product of an even number of transpositions.

Conjugation in a group is denoted by $h^g := g^{-1}hg$. Note that elsewhere the notation h^g may mean ghg^{-1} instead, but our notation is more normal in group theory. This is linked to the fact that our actions will be on the right (as is common in group theory) rather than the left (as might be common elsewhere, when composing maps for instance). This will become clear later…

Recall that if $H \leq G$, then a (*right*) *coset* of H is a set $Hg = \{hg : h \in H\}$. These are all equal or disjoint and partition G. Hence, we have:

Theorem 1.2 (Lagrange's theorem) *Let G be a group and $H \leq G$ a subgroup. Then,*

$$|G| = |G : H||H|$$

where $|G : H|$ is the number of cosets of H in G, called the index *of H in G.*

We say two elements h and k are *conjugate* if there exists $g \in G$ such that $h^g = k$. Likewise, two subgroups $H, K \leq G$ are *conjugate* if there exists $g \in G$ such that $H^g = K$. Being conjugate is an equivalence relation.

Definition 1.3 A *normal subgroup*, written $N \trianglelefteq G$, is a subgroup $N \leq G$ such that for all $h \in N$ and $g \in G$, $h^g \in N$.

When N is a normal subgroup of G, we may form the *quotient group* G/N whose elements are cosets of N and multiplication is given by

$$Ng.Nh = Ngh$$

We also have maps between groups:

Definition 1.4 A (*group*) *homomorphism* is a well-defined map $\varphi : G \to H$ between two groups G and H which preserves the multiplicative structure. In other words,

$$\varphi(gk) = \varphi(g)\varphi(k)$$

for all $g, k \in G$.

A bijective homomorphism is called an *isomorphism.* When there is an isomorphism between two groups G and H, we say G and H are *isomorphic* and we write $G \cong H$.

Theorem 1.5 (1st isomorphism theorem) *Let G and H be groups and $\varphi : G \to H$ be a homomorphism. Then, $N := \ker \varphi$ is a normal subgroup of G and the induced map*

$$\begin{aligned} \bar{\varphi} : G/N &\to \mathrm{Im}(\varphi) \leq H \\ Ng &\mapsto \varphi(g) \end{aligned}$$

is an isomorphism between the quotient group G/N and the image $\mathrm{Im}(\varphi)$*.*

2 Group actions

We now come to what will be the main topic of study:

Definition 2.1 Let Ω be a non-empty finite set and G a group. We say that G acts on Ω if there is a map $\varphi : \Omega \times G \to \Omega$ such that

(1) $\mu(\mu(\alpha, g), h) = \mu(\alpha, gh)$

(2) $\mu(\alpha, 1) = \alpha$

for all $\alpha \in \Omega$ and $g, h \in G$. If Ω is finite, then we say the action, or G, has *degree* $|\Omega|$.

The above notation with μ is a little clumsy, so instead we will write αg for $\mu(\alpha, g)$. Then our axioms become:

(1) $(\alpha g)h = \alpha(gh)$

(2) $\alpha 1 = \alpha$

This is called writing our action *on the right.* We could just have well have chosen to write our actions on the left, as one usually does with maps, but it is more common in group theory to use right actions. Note also, that in many places you will see actions written exponentially, that is, writing α^g for αg – there are notational issues with left and right actions here too.

Remark 2.2 The axioms here just say that the action respects the multiplicative structure in the group. For example, if $\alpha g = \beta$, then $\beta g^{-1} = \alpha$. (Exercise!).

Example 2.3 We already know some examples of group actions:

(1) (*Trivial action*) Let G be a group and Ω a set. Define $\mu(\alpha, g) = \alpha$ for all $\alpha \in \Omega$ and $g \in G$. Clearly, every group has the trivial action on every set, but this is not very enlightening!

(2) Let $G = S_n$ acting on the set $\Omega = \{1, \ldots, n\}$ by natural permutation. e.g. pick $3 \in \Omega = \{1, \ldots, 4\}$ and $(132) \in S_4$, then $3.(132) = 2$.

(3) (*Right regular action*) Let G be a group and take $\Omega = G$. The right regular action is given by multiplying $\alpha \in \Omega = G$ on the right by an element $g \in G$ i.e. $\mu(\alpha, g) = \alpha g$. Since group multiplication is associative, the first axiom is satisfied and the second is also satisfied by the identity axiom in the group.

(4) (*Coset action*) Let G be a group and $H \leq G$ be a subgroup. We take Ω to be the set of (right) cosets of H in G, denote by $(G : H)$. That is, $\Omega := (G : H) = \{Hx : x \in G\}$. Define $\mu(Hx, g) = Hxg$. Again, since group multiplication is associative, the first axiom is satisfied and the second is too by the identity axiom. You should also check that it is well-defined.

(5) (*Conjugation action*) Let G be a group and $\Omega := G$. Define $\mu(x, g) = x^g$ to be conjugation in the group. This is one action that is always written exponentially, for obvious reasons. You can also have conjugation action on a set of subgroups of G.

(6) Let Ω be some object. Then the automorphism group of Ω acts on Ω. For example, the automorphism group of (non-trivial) vectors in a vector space V is $GL(V)$, the automorphism group of a set Ω is $Sym(\Omega)$. The set Ω could also be a graph, design, geometry etc.

Remark 2.4 The last example is one reason why actions are so important. Whenever you have any object in mathematics, it has an automorphism group which acts on it. It might be trivial, but more often than not it is non-trivial and can give important information about the object itself.

Lemma 2.5 *Every group G is isomorphic to a permutation group. That is, there exists an injective group homomorphism $\varphi : G \to S_n$, for some $n \in \mathbb{N}$, and hence $G \cong \operatorname{Im}(\varphi) \leq S_n$.*

Proof. Consider the right regular action of G on itself. Since each $g \in G$ is invertible, g is a bijective map on the set $\Omega = G$. Recalling that S_n is the set of all all bijections from a set of size n to itself, we see that there is a natural bijection φ from G to S_n, where $n = |\Omega| = |G|$. By the first axiom for an action, φ is a homomorphism. Suppose that $g \in G$ was in the kernel of φ, that is, g fixes every point in Ω i.e. $\alpha g = \alpha$ for all $\alpha \in \Omega$. However, $\Omega = G$ and the only such element in G is 1. Hence, φ is injective. Using the 1^{st} isomorphism theorem, $G \cong \mathrm{Im}(\varphi)$. □

Remark 2.6 The title of this part of the course is permutation groups, so we might think that only means subgroups of S_n. In fact, the above Lemma 2.5 shows up the 'only' in the last sentence. Using actions, all groups can be considered as subgroups of some symmetric group S_n.

Definition 2.7 The *kernel* of the action is

$$\{g \in G : \alpha g = \alpha \text{ for all } \alpha \in \Omega\} \trianglelefteq G$$

We say that G acts *faithfully* if it acts with no non-trivial kernel.

Note that we could extend the proof of the above lemma to cover an arbitrary action. We would still have a homomorphism $\varphi : G \to S_n$, where $n = |\Omega|$, but in general the action would have a (non-trivial) kernel. In fact, such an argument would show that our definition of an action on a set of size n is equivalent to saying that there exists a group homomorphism into S_n.

If an action of G on Ω does have a kernel K, we may always study G/K which acts faithfully on Ω. Hence, we will often assume that a permutation group acts faithfully.

3 Orbits and Stabilisers

Definition 3.1 Let G be a group acting on a set Ω. We define the *orbit* containing α to be

$$\begin{aligned} \alpha G :=& \{\beta \in \Omega : \exists g \in G \text{ s.t. } \beta = \alpha g\} \\ =& \{\alpha g : g \in G\} \end{aligned}$$

and the stabiliser of α in G to be

$$G_\alpha := \{g \in G : \alpha g = \alpha\}$$

Note that if one is writing the action exponentially, the notation α^G is used instead of αG for an orbit.

Example 3.2 Let G be a group acting on itself by conjugation. The orbits are called *conjugacy classes* in G and the stabiliser of a point $x \in G$ is the *centraliser*:

$$C_G(x) := \{g \in G : x^g = x\}$$

Similarly, if a group G acts by conjugation on a set of subgroups, the orbits are conjugate subgroups and the stabiliser of a subgroup H is the *normaliser* of H in G:

$$\begin{aligned} N_G(H) :=& \{g \in G : h^g \in H \text{ for all } h \in H\} \\ =& \{g \in G : H^g = H\} \end{aligned}$$

Proposition 3.3 *Let G be a group acting on a set Ω, $g, h \in G$ and $\alpha, \beta \in \Omega$.*

(1) *The set of all orbits of G on Ω form a partition of Ω.*

(2) *The stabiliser G_α is a subgroup of G. Moreover, if $\beta = \alpha g$, then*

$$G_\alpha^g = G_\beta$$

(3) *$\alpha g = \alpha h$ if and only if $G_\alpha g = G_\alpha h$.*

Proof. Clearly $\alpha \in \Omega$ is in the orbit αG. So it remains to show that orbits are distinct, or equal. Let γ be a point in two different orbits αG and βG. Then, there exists $g, h \in G$ such that $\alpha g = \gamma$ and $\beta h = \gamma$. So, $\alpha g h^{-1} = \beta$. Now,

$$\begin{aligned} \beta G &= \{\beta k : k \in G\} \\ &= \{\alpha g h^{-1} k : k \in G\} \\ &= \{\alpha x : x \in G\} \\ &= \alpha G \end{aligned}$$

as when k runs over G, $gh^{-1}k$ also runs over G and vice versa.

To show G_α is a subgroup, we must show it is closed under multiplication and has inverses. If $g, h \in G_\alpha$, then by the first axiom for actions

$$\alpha(gh) = (\alpha g)h = \alpha h = \alpha$$

So, $gh \in G_\alpha$. Clearly, if $\alpha g = \alpha$, then $\alpha g^{-1} = \alpha$, so $g^{-1} \in G_\alpha$. Hence, G_α is a subgroup.

Now, suppose that $\beta = \alpha g$, so $\alpha = \beta g^{-1}$. Then,

$$h \in G_\alpha \iff \beta g^{-1} h = \beta g^{-1} \iff \beta g^{-1} h g = \beta$$

So, $G_\alpha^g = G_\beta$.

Finally,

$$\alpha g = \alpha h \iff \alpha g h^{-1} = \alpha \iff g h^{-1} \in G_\alpha \iff G_\alpha g = G_\alpha h \qquad \square$$

Definition 3.4 A group G acting on a set Ω is *transitive* if for all $\alpha, \beta \in \Omega$ there exists $g \in G$ such that $\alpha g = \beta$. A group which does not act transitively is called *intransitive.*

Note that, if you pick an orbit αG of G, G will act transitively on it. So, we can study the action of an intransitive group G by studying the action on each of its orbits. Hence, for most of the rest of this course we will study transitive groups. But first, we will introduce the following important theorem.

Theorem 3.5 (Orbit-Stabiliser theorem) *Let G be a group acting on a set Ω. Then, for all $\alpha \in \Omega$,*

$$|G_\alpha||\alpha G| = |G|$$

Proof. By Proposition 3.3 (3), the points αg of the orbit αG are in bijection with the cosets $G_\alpha g$. So, $|\alpha G| = |G : G_\alpha|$. Finally, by Lagrange's theorem,

$$|G_\alpha||\alpha G| = |G_\alpha||G : G_\alpha| = |G| \qquad \square$$

Example 3.6 Recall from Example 3.2, the orbits of the conjugation action are called conjugacy classes. By the Orbit-stabiliser theorem, the size of each conjugacy class divides the order of G. From the previous Proposition 3.3, we also see that $C_G(H)$ and $N_G(H)$ are both subgroups of G.

Definition 3.7 A transitive action of G on Ω is called *regular* if $G_\alpha = 1$ for all $\alpha \in \Omega$. Equivalently, $g \in G$ fixes no point in Ω.

Corollary 3.8 *Let G act transitively of degree n on a set Ω. Then,*

(1) *All the stabilisers G_α, for $\alpha \in \Omega$, are conjugate.*

(2) *The index $|G : G_\alpha| = n$ for every $\alpha \in \Omega$.*

(3) *The action is regular if and only if $|G| = n$.*

Proof. Since the action is transitive, by Proposition 3.3 (2), all the G_α are conjugate. The second two parts follow from the Orbit-Stabiliser theorem and Lagrange's theorem. □

Note that, from the first part of the above Corollary, a transitive group G is regular if there exists $\alpha \in \Omega$ such that $G_\alpha = 1$.

Exercise 3.9 You should convince yourselves that:

(1) The right regular action is transitive and regular!

(2) Coset action is transitive.

Example 3.10 Let V be a n-dimensional vector space over the finite field $\mathbb{F}_q$. Define projective space in the normal way

$$\mathbb{P}_{n-1} = \mathbb{P}_{n-1}(q) = V/\sim$$

where $\sim$ is an equivalence relation given by $v \sim w$ if and only if there exists $\alpha \in \mathbb{F}_q$ such that $v = \alpha w$. So, the equivalence classes are 1-dimensional subspaces of V; we call these *points* of $\mathbb{P}_{n-1}$.

Let $G = GL_n(q)$, the set of all invertible $n \times n$ matrices with entries in $\mathbb{F}_q$. Now, $GL_n(q)$ acts transitively on the set of all non-zero vectors V, so it also acts transitively on the points (1-dimensional subspaces) of $\mathbb{P}_{n-1}$. However, there is now a kernel to this action, given by scalar matrices

$$\begin{pmatrix} \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda \end{pmatrix} = \lambda I_n$$

Since this is the kernel of the action (and in fact the centre $Z(GL(V))$), these matrices form a normal subgroup of $GL_n(q)$. We define:

$$PGL_n(q) := GL_n(q)/\langle scalars \rangle$$

the *projective general linear group.* This still acts transitively on the points of $\mathbb{P}_{n-1}$ and it has order $|PGL_n(q)| = q^{n(n-1)/2}(q^2-1)\dots(q^n-1)$ We may also define the *projective special linear group* to be

$$PSL_n(q) := SL_n(q)/\langle scalars \rangle$$

It has order

$$|PSL_n(q)| = \frac{1}{(n, q-1)} q^{n(n-1)/2} \prod_{i=2}^{n} (q^i - 1)$$

where $(n, q-1) = \text{hcf}(n, q-1)$ is the highest common factor of n and $q-1$. This turns out to be an important family of groups as they are all simple, i.e. they have no non-trivial normal subgroups, except for when $n = 2$ and $q = 2, 3$.

Definition 3.11 Let G be a group which has an action on Ω and Ω'. We say these actions are *isomorphic* if there exists a bijection $\varphi : \Omega \to \Omega'$ such that for all $\alpha \in \Omega$, $g \in G$,

$$\varphi(\alpha g) = \varphi(\alpha)g$$

In other words, such that the following diagram commutes for all $g \in G$.

$$\begin{tikzcd}
\Omega \arrow[r, "\varphi"'] \arrow[d, "g"'] & \Omega' \arrow[d, "g"'] \\
\Omega \arrow[r, "\varphi"] & \Omega'
\end{tikzcd}$$

Note that this is the natural definition – it just says that G acts the same way on Ω as it does on Ω'.

Proposition 3.12 *Let G act transitively on a set Ω. Then, there exists a subgroup $H \leq G$ such that the action of G on Ω is isomorphic to the coset action of G on $(G : H)$, the cosets of H in G.*

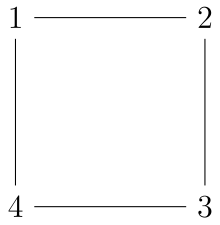
Proof. Pick $\alpha \in \Omega$ and set $H = G_\alpha$. Define $\varphi : \Omega \to (G : G_\alpha)$ by $\alpha g \mapsto G_\alpha g$. By Proposition 3.3 (3), this is a bijection. The isomorphism property is also clear,

$$\varphi(\alpha g) = G_\alpha g = (G_\alpha 1)g = \varphi(\alpha)g. \qquad \square$$

Note that the last proposition limits the possible transitive actions a group G can have. The possible Ω on which G can have a transitive action must correspond to a subgroup H at index $|\Omega|$. It also tells us that when we are doing permutation groups and actions, we are really studying group theory.

4 Primitive and imprimitive actions

Example 4.1 Consider the symmetries of a square:



Recall that the group of symmetries of a square is D_8, which contains four reflections and four rotations. By numbering the vertices, we may consider that D_8 acts on $\Omega = \{1, 2, 3, 4\}$. It is easy to see that D_8 acts transitively on Ω. However, since D_8 must preserve the square, wherever we map 1, 3 must be opposite. Similarly for 2 and 4.

If instead we consider S_4 acting on Ω, this is also transitive, but we may map 1 wherever we like without 3 having to be opposite. So, these two transitive actions are fundamentally different.

Definition 4.2 Let G be a group acting transitively on a set Ω. Let $\mathcal{B}$ be a set of subsets B that partition Ω. If

$$B \cap Bg = \emptyset \text{ or } B$$

for all $g \in G$, $B \in \mathcal{B}$, then we say that $\mathcal{B}$ is a *system of imprimitivity*, or a *system of blocks*. The subsets B are called *blocks*.

Note that, we may always take $\mathcal{B}$ to be $\{\Omega\}$, or $\{\{\alpha\} : \alpha \in \Omega\}$. These are known as *trivial systems*.

A group G is *imprimitive* if there exists a non-trivial system of imprimitivity; G is *primitive* if no such system exists.

Example 4.3 The group D_8 acting naturally on $\Omega = \{1, 2, 3, 4\}$ is imprimitive with blocks $\{1, 3\}$ and $\{2, 4\}$. The group S_4 acting on Ω is primitive. (You should convince yourselves that no non-trivial system of imprimitivity exists for S_4.)

Note that since G is transitive, if $\mathcal{B}$ is a system of imprimitivity, then given any $B \in \mathcal{B}$,

$$\mathcal{B} = \{Bg : g \in G\}.$$

Hence, all the blocks B in $\mathcal{B}$ have the same size.

Definition 4.4 An equivalence relation $\sim$ is called a *G-congruence* if it is preserved under the action of the group. That is,

$$\alpha \sim \beta \iff \alpha g \sim \beta g$$

for all $g \in G$.

Lemma 4.5 *Let $\mathcal{B}$ be a system of imprimitivity for Ω. Then, we may define a G-congruence by $\alpha \sim \beta$ if α and β are in the same block of $\mathcal{B}$.*

Conversely, if $\sim$ is a G-congruence on Ω, then the equivalence classes of $\sim$ form a system of imprimitivity.

Proof. Exercise. □

This gives us an equivalent definition of primitive and imprimitive groups:

Corollary 4.6 *A group G is imprimitive if there exists a non-trivial G-congruence relation. It is primitive if no non-trivial G-congruence exists.*

Lemma 4.7 *Suppose G has a transitive action of prime degree n. Then, G acts primitively.*

Proof. Exercise. □

We must now take a short detour to define the semidirect product of groups. This is a generalisation of direct product of groups.

Let N and H be two groups. Suppose H acts on N in such a way that it respects the multiplicative structure of N. That is, $h \in H$ acts on N as an automorphism of N. For reasons which will become clear, we will write this action exponentially: $n \mapsto n^h$ is an automorphism of N.

We define a group $G = \{(n, h) : n \in N, h \in H\}$ with multiplication

$$(n, h)(m, g) := (nm^{h^{-1}}, hg)$$

We call G the *semidirect product* of N by H.

Exercise 4.8 Check that G is a group. What is the identity element? What is the inverse of (n, h)?

It is easy to see that $N' := \{(n, 1) : n \in N\}$ and $H' := \{(1, h) : h \in H\}$ are subgroups of G which are isomorphic to N and H, respectively. We see that $N' \cap H' = 1$ and $N'H' = G$. (Note that $XY := \{xy : x \in X, y \in Y\}$.)

Moreover, N' is a normal subgroup of G and conjugation by an element of H' is given by:

$$(1,h)^{-1}(n,1)(1,h) = (n^h, 1)$$

So, conjugation of N' by H' matches exactly the action on N of H. (This is why we write the action exponentially here – H' acts on N' by conjugation). Because of this, we normally drop the dashes and simply write N and H for N' and H'. Note that this is exactly the same as for direct products. In the same way, we also simplify the notation for G, writing elements as nh rather than (n,h) $(= (n,1)(1,h))$.

We often write $G = N : H$, or $G = N \rtimes H$ to signify that G is a semidirect product of N by H. Note that this notation relies implicitly on knowing the action of H on N.

You may also see the semidirect product defined in a different way:

Definition 4.9 Let G be a group, $N \trianglelefteq G$ and $H \leq G$. Then, G is a *semidirect product* of N by H if

$$G = NH \quad \text{and} \quad N \cap H = 1.$$

Exercise 4.10 Check that the two definitions are equivalent. Here, the action of H on N is the conjugation action of the subgroup H on N.

Example 4.11 (1) Let G be the direct product of two groups H and K, $G := H \times K$. Then, G is the semidirect product of H by K and the semidirect product of K by H. So, semidirect products are a generalisation of direct products.

(2) Let $G = D_8$. Let V_4 be the subgroup of D_8 given by

$$V_4 = \{1, (13), (24), (13)(24)\} = C_2 \times C_2$$

Now V_4 is a normal subgroup of D_8 (Show this!). Let $H \cong C_2$ be the subgroup $\langle (12)(34) \rangle$. Then, certainly $V_4 \cap H = 1$. By considering the product V_4H, we see that every element of G can be written this way. That is, $G = V_4H$. So, D_8 is a semidirect product of V_4 by C_2.

(3) Let $G = D_8$. Let N be the subgroup of D_8 of all the rotations of the square. Let a denote the rotation by 90°, (1234). Then, $N = \langle a \rangle = C_4$ the cyclic group.

$$N := \{1, (1234), (13)(24), (1432)\}$$

Pick $H := \langle (13) \rangle$. Again, we see that N is a normal subgroup, $G = NH$ and clearly $N \cap H = 1$. So, D_8 is also a semidirect product of C_4 by C_2.

Note that we could also have chosen different subgroups H as long as they were isomorphic to C_2 and not contained in the normal subgroup and the construction would still have worked.

We now have the machinery to describe some important examples of primitive and imprimitive groups.

Definition 4.12 (Wreath product) Let $N = \underbrace{A \times \cdots \times A}_{m}$ be the direct product of m copies of the group A. Let H be a group which acts on N by permuting the m copies of A. We define G to be the semidirect product of N by H. This is called the *wreath product* of A by H, A is called the *base group* and G is written $G = A \wr H$, or $G = A \operatorname{wr} H$.

Example 4.13 The group $C_2 \wr S_3 = (C_2 \times C_2 \times C_2) : S_3$ is a wreath product. We could construct this directly by taking:

$$N := \langle (12) \rangle \times \langle (34) \rangle \times \langle (56) \rangle$$

Then, we need a group H isomorphic to S_3 which acts on the 6 points so as to preserve the multiplicative structure of N (needed for the semidirect product). It turns out that taking

$$H := \langle (135)(246), (13)(24) \rangle$$

this works (check this!).

Note that G acts on $\Omega = \{1, \ldots, 6\}$ with blocks $\{\{1, 2\}, \{3, 4\}, \{5, 6\}\}$. So, $G = C_2 \wr C_3$ acts imprimitively on Ω.

Look back to Example 4.11 (2) to see that D_8 can be written as a wreath product $D_8 = C_2 \wr C_2$ and it preserves precisely the system of imprimitivity that we observed in Example 4.1.

Remark 4.14 In fact, it is not difficult to see that any imprimitive group can be written as a wreath product. In particular, we may study imprimitive groups by studying the action of the base group on a block and the action of the group permuting the blocks. If the system of imprimitivity has blocks of minimal size, then the action of the base group will be primitive. Hence, we see that primitive groups are the building blocks of permutation groups.

Example 4.15 (Affine general linear group) Let Ω be all the vectors of the vector space V over a field F (including the 0-vector). This set is preserved by translations as well as by the action of $GL(V)$. So, elements of the form

$$t_{a,v} : u \mapsto uA + v$$

where $A \in GL(V)$, act on Ω. The group of all such elements is called the *affine general linear group* and is denoted $AGL(V)$, or if V is n-dimensional over a field F, $AGL_n(F)$ (show this is a group).

Let $N := \{t_{1,v} : v \in V\}$. This is a normal subgroup of $AGL(V)$ (check this!). You can also find a subgroup of $AGL(V)$ which is isomorphic to $GL(V)$, disjoint from N and such that $AGL(V) = N\,GL(V)$. Hence, $AGL(V)$ is a semidirect product. Since N has the same size as number of vectors in the vector space V, it is often written:

$$AGL(V) \cong V : GL(V) \quad \text{or} \quad AGL_n(F) \cong F^n : GL_n(F)$$

It is clear that the action here is transitive, as any vector can be reached by a translation. It is also true that this action is primitive. You should convince yourself of this now (!), but in a later section we will have a better way of showing this.

5 Primitive groups

We will now discuss some results which tell us something about the structure of primitive groups.

Proposition 5.1 *Let G act on a set Ω and $N \trianglelefteq G$. Then,*

(1) *The orbits of N form a system of blocks for G.*

(2) *If there exists $\alpha \in \Omega$ which is fixed by N, then N fixes all of Ω i.e. it lies in the kernel of the action.*

Proof. Let Δ be an orbit of N on Ω. Then, Δg is an orbit for the group N^g. Since N is normal, $N^g = N$. However, G is transitive, so the set of all these orbits covers Ω. Since orbits are disjoint, these form a system of imprimitivity.

If α is fixed by N, then it is a block of size one. However, every block in a system of imprimitivity has the same size. □

Note that the system of imprimitivity in part (1) could be trivial (as it is in part (2)). In particular, this will be the case in the following corollary:

Corollary 5.2 *If G acts primitively on Ω and $N \trianglelefteq G$, then N either acts transitively on Ω, or it is in the kernel of the action.* □

For the following theorem we need a short definition:

Definition 5.3 Let G be a group and $H \leq G$ a subgroup. Then H is *maximal* in G if there does not exists a subgroup K of G such that

$$H \lneqq K \lneqq G$$

We will now prove the following very important theorem about primitive actions. First we need some notation. If Δ is a subset of Ω, then let $G_{\{\Delta\}}$ denote the setwise stabiliser of Δ in G. (Clearly, if $\alpha \in \Omega$, $G_\alpha = G_{\{\alpha\}}$.)

Theorem 5.4 *Let G act transitively on Ω, $\alpha \in \Omega$. Then,*

$$G \text{ is primitive} \quad \Longleftrightarrow \quad G_\alpha \text{ is maximal in } G.$$

Proof. Let $\alpha \in \Omega$. Consider all the possible systems of imprimitivity on Ω. We let Σ be the set of all blocks B in such a system of imprimitivity with $\alpha \in B$. Let S be the set of all subgroups H of G such that $G_\alpha \leq H$. We will prove the theorem by showing that there is a bijection between these two sets. Indeed, define $\Psi : \Sigma \to S$ by $\Psi(B) = G_{\{B\}}$ and $\Phi : S \to \Sigma$ by $\Phi(H) = \alpha H$. We will show that these two maps are bijections and mutually inverse.

First, consider Ψ. Let $g \in G_\alpha$. Then, $\alpha \in B \cap Bg$ and so, since B is a block, $B = Bg$. Hence, $g \in G_{\{B\}}$ and we have $G_\alpha \leq G_{\{B\}} = \Psi(B)$. So Ψ does indeed map Σ into S.

Next, consider Φ. Let $B = \alpha H$ and $g \in G$. Clearly, if $g \in H$, then $Bg = B$. We claim that if $g \notin H$, then $B \cap Bg = \emptyset$. Suppose not, then there exists $h, k \in H$ such that $\alpha h = \alpha k g \in B \cap Bg$. So, $kgh^{-1} \in G_\alpha$ and by rearranging we get that $g \in k^{-1} G_\alpha h \subseteq H$, a contradiction. Hence, B is a block in some block system and Φ does map S into Σ. Moreover, the above argument shows that if $B = \alpha H$, then $B = Bg$ if and only if $g \in H$. So, $H = G_{\{B\}}$. Therefore, $\Psi \circ \Phi(H) = \Psi(\alpha H) = G_{\{\alpha H\}} = H$.

It remains to show that Ψ followed by Φ is the identity. Now, $\Psi(B) = G_{\{B\}}$, so we need just show that $G_{\{B\}}$ acts transitively on the block B and then $\Phi \circ \Psi(B) = \alpha G_{\{B\}} = B$. However, if $g \in G$ such that $\alpha g = \beta$ for $\alpha, \beta \in B$, then $\beta \in B \cap Bg$. Hence, $B = Bg$ and $g \in G_{\{B\}}$. □

Remark 5.5 The above theorem tells us that studying primitive actions of G, we are finding all maximal subgroups of G. This is the first step in finding the subgroup lattice of a group G. So again, we see that in studying permutation groups, we are really doing group theory.

Since we may always factor out the kernel of the action, we may turn our attention to primitive groups which act faithfully. Then, they may be considered to be a subgroup of $Sym(\Omega)$ and we may interpret elements in them accordingly.

Theorem 5.6 *Let G be a primitive group acting faithfully on Ω.*

(1) *If G contains a 3-cycle, then $G \geq Alt(\Omega)$.*

(2) *If G contains a 2-cycle, then $G = Sym(\Omega)$.*

Proof. (1) Let $\Delta \subseteq \Omega$. We will write $Alt(\Delta)$ for the subgroup of $Alt(\Omega)$ which fixes $\Omega - \Delta$ pointwise and acts as the alternating group on Δ. Pick Δ to be the maximal subset of Ω such that $G \geq Alt(\Delta)$. Now G contains a 3-cycle, hence a copy of $A_3 \cong C_3$, so such a Δ certainly exists. Suppose for a contradiction that $\Delta \subsetneqq \Omega$.

We claim that there always exists a 3-cycle in G with exactly two points in Δ. Since G is primitive, Δ is not a block. So, there exists $g \in G$ such that $\Delta \cap \Delta g$ is not $\emptyset$, or Δ.

Suppose $\Delta \cap \Delta g = \{\alpha\}$ is a single point. There are certainly 3-cycles of the form $h := (\alpha\beta\gamma) \in Alt(\Delta) \leq G$, where $\beta, \gamma \in \Delta$. However, since $Alt(\Delta g) = Alt(\Delta)^g \leq G$, G also contains 3-cycles of the form $k := (\alpha\delta\epsilon) \in Alt(\Delta g)$, where $\delta, \epsilon \in \Delta g$. Now,

$$\begin{aligned} k^{-1}h^{-1}kh &= (\alpha\epsilon\delta)(\alpha\gamma\beta)(\alpha\delta\epsilon)(\alpha\beta\gamma) \\ &= (\alpha\beta\delta) \end{aligned}$$

which is a 3-cycle in G with exactly two points in Δ.

Now, suppose that $\Delta \cap \Delta g$ contains at least two points, say α and β. Pick $\delta \in \Delta g - \Delta$. Then, the 3-cycle $(\alpha\beta\delta) \in Alt(\Delta g) \leq G$ has exactly two points in Δ. Hence, there exist 3-cycles in G with exactly two points in Δ.

Let $(\alpha\beta\delta)$ be such a 3-cycle in G with exactly two points α, β in Δ. Set $\Gamma = \Delta \cup \{\delta\}$. We claim that $G \geq Alt(\Gamma)$. Since $G \geq Alt(\Delta)$, it is enough to show that G contains all elements $h \in Alt(\Gamma)$ such that $\delta h \neq \delta$. Since $\gamma := \delta h \in \Delta$, there exists $k \in Alt(\Delta) \leq G$ such that $\gamma k = \beta$. Now, $hk(\alpha\beta\delta)$ is certainly in $Alt(\Gamma)$ and moreover it fixes δ. Hence, it is in $Alt(\Delta) \leq G$. However, since k and $(\alpha\beta\delta)$ are both elements of G, h is also in G. Therefore, $G \geq Alt(\Gamma)$ contradicting the maximality of Δ.

(2) If $|\Omega| = 2$ and G contains a 2-cycle, then G is all of $S_2 = C_2$. Hence, we may assume that $|\Omega| \geq 3$. Suppose G contains the 2-cycle $(\alpha\beta)$. Since G is primitive, $\{\alpha, \beta\}$ is not a block, so again we have $g \in G$ such that $\{\alpha, \beta\} \cap \{\alpha, \beta\}g$ is neither $\emptyset$, nor $\{\alpha, \beta\}$. Hence, it must be $\{\alpha\}$ say. So, $\{\alpha, \beta\}g = \{\alpha, \gamma\}$ with $\gamma \neq \beta$. Then, $(\alpha\beta)g^{-1}(\alpha\beta)g = (\alpha\beta)(\alpha\gamma) = (\alpha\beta\gamma)$. So, G contains a 3-cycle. By the first part, $G \geq Alt(\Omega)$. However, G also contains a 2-cycle, which is an odd permutation, so $G \geq \langle(\alpha\beta), Alt(\Omega)\rangle = Sym(\Omega)$. □

So, if a primitive group contains just one 2- or 3-cycle, it already is the whole of S_n, or A_n, respectively. This suggests that, if other faithful primitive groups of degree n do exist, they must be much smaller than $n!$. We will come back to such thoughts later in Section 7…

6 Multiply transitive groups

Definition 6.1 Let G be a group acting on a set Ω. Suppose $\alpha_1, \ldots, \alpha_k$ are k distinct points of Ω and $\beta_1, \ldots, \beta_k$ are a second set of k distinct points of Ω. Then, G is *k-transitive* if there exists $g \in G$ such that

$$\alpha_1 g = \beta_1, \ \ldots, \alpha_k g = \beta_k$$

Clearly, if a group is k-transitive, then it is also $(k-1)$-transitive.

Exercise 6.2 (1) S_n is n-transitive.

(2) A_n is $(n-2)$-transitive, provided $n \geq 3$.

Lemma 6.3 *A group G is k-transitive on Ω if and only if*

(1) *G is transitive and*

(2) *G_α is $(k-1)$-transitive on $\Omega - \{\alpha\}$.*

Proof. Exercise. □

Lemma 6.4 *Let G be a group which acts 2-transitively on Ω. Then G is primitive.*

Proof. Exercise. □

Note that using the above lemma can be a good way to show that a group is primitive. For example, it is straightforward to show that $AGL(V)$ is 2-transitive (Exercise), hence we see that it is also primitive.

We gave two examples of infinite families of multiply transitive groups above, but how many other groups are multiply transitive? It seems like quite a strong constraint…

Searching for such groups began as far back as the 1860s with Mathieu and others. The classification of all such groups was only concluded using the Classification of Finite Simple Groups (CFSG) (this is a huge piece of work completed in 2008, taking 50+ years and estimated at over 10,000 pages of proof). The only known proof of the classification of doubly transitive groups relies on this! However, we can do without this for larger k. We will give you one such result after we make the following definition.

Definition 6.5 A group G is *sharply* k-transitive if it is k-transitive and the pointwise stabiliser of any k distinct points is trivial.

So, a regular group is a sharply 1-transitive group.

Proposition 6.6 (Jordan 1870s) *Let G be a sharply 4-transitive group of degree n. Then, n is 4, 5, 6, or 11.*

Proof. Let $\Omega = \{1, 2, 3, 4, \dots, n\}$. Let $t \in G$ be a element which switches 1 and 2 and fixes 3 and 4. Since t^2 must fix $1, 2, 3, 4$ and G is sharply 4-transitive, $t^2 = 1$. So, t must have the form

$$t = (12)(3)(4)\dots(ij)\dots(kl)\dots$$

Let H be the subgroup of G_1 of elements which commute with t.

$$H := C_{G_1}(t) = \{g \in G : 1g = 1 \text{ and } tg = gt\}$$

Now, t fixes at least two points (3 and 4) and at most 3 points, since otherwise $t = 1$. Let $\mathrm{fix}_\Omega(t)$ denote the set of fixed points and consider the action of H on $\mathrm{fix}_\Omega(t)$. Let α be such a fixed point of t. Then, $\alpha ht = \alpha th = \alpha h$. So, αh is a fixed point of t and H permutes $\mathrm{fix}_\Omega(t)$.

We claim that H also acts faithfully. Indeed, suppose $h \in H$ fixes every point in $\mathrm{fix}_\Omega(t)$. However, it also fixes 1 and so 2 as well, hence it fixes at least 4 points. So, $h = 1$ and H acts faithfully on $\mathrm{fix}_\Omega(t)$. Therefore, $|H| \bigm| |Sym(\mathrm{fix}_\Omega(t))|$. If n is even, then t must have two fixed points and if n is odd it must have three. So, if n is even, $|H| \bigm| 2$ and if n is odd, $|H| \bigm| 6$.

Now let C be the set of transpositions other than (12) in t. We claim that H acts transitively on C. Pick $g \in G$ such that $1g = 1$, $2g = 2$, $ig = k$,

$jg = l$. Observe that g moves the transposition $(ij) \in C$ to (kl). Now, t^g swaps 1 and 2 and swaps k and l. So, t^g agrees with t on 1, 2, k and l. Since G is sharply 4-transitive, $t^g = t$ and so $g \in H$. Hence, H acts transitively on C. Now, the stabiliser of an element of C has order at least 2. Just take $k = j$, $l = i$ in the choice of g. Then, g fixes (ij). Since the stabiliser of an element of C has order at least 2 and $|H| \leq 6$, by the Orbit-Stabiliser theorem, $|C| \leq 3$.

If n is odd, then $|C| \leq 3$ and $n \leq 2 + 3 + 3.2 = 11$. If n is even, $|H| \leq 2$ and $|C| \leq 1$, so $n \leq 2 + 2 + 1.2 = 6$. It remains to eliminate the cases of $n = 7, 9$ – this is left as an exercise. □

The groups in question in the above proposition turn out to all be unique. For $n = 4, 5, 6$, we have S_4, S_5 and A_6 which are familiar. However, the last group is called M_{11} and is new (note that is must be a proper subgroup of S_{11}). It is a *Mathieu* group which is named after Mathieu who found it. He found several other Mathieu groups too. In fact, M_{12} is a sharply 5-transitive group of degree 12 with M_{11} as the stabiliser of a point. The stabiliser of two points is M_{10} which is sharply 3-transitive, M_9 is sharply 2-transitive etc. The group M_{12} is the automorphism group of the Steiner system $S(5, 6, 12)$ (see next part of the course).

He also discovered another group M_{24} which is a 5-transitive group of degree 24. Its point stabiliser M_{23} is 4-transitive, and M_{22} is 3-transitive etc. The automorphism group of the Steiner system $S(5, 8, 24)$ is M_{24}. It also turns out that M_{24}, M_{23}, M_{22}, M_{21}, M_{12} and M_{11} are also all (sporadic) simple groups (groups with no non-trivial normal subgroups) which makes them extremely interesting!

Remark 6.7 The point the above proposition is to demonstrate that multiply transitive groups are rare. In fact,

- The only 5-transitive groups apart from S_n and A_n are M_{24} and M_{12}.
- The only 4-transitive groups apart from S_n and A_n are M_{23} and M_{11}.
- The 2- and 3-transitive groups are all known. There are some infinite families as well as some individual groups.

7 Bases for permutation groups

For vector spaces, bases are very important – a linear transformation is completely determined by its action on a basis. For permutation groups we wish to define an analogous concept. This will lead to information about the possible primitive groups of a given degree.

We begin with a bit of notation: if $\Delta \subseteq \Omega$, then define $G_{(\Delta)}$ to be the pointwise stabiliser in G of Δ. (Compare this to $G_{\{\Delta\}}$ being the setwise stabiliser.)

Definition 7.1 A subset $\Sigma \subseteq \Omega$ is a *base* for G if $G_{(\Sigma)} = 1$. That is, if the only element which fixes Σ pointwise is the identity.

It is clear that every group G which acts faithfully has a base.

Define $\operatorname{supp}(g)$ to be the set of points of Ω which are moved by g; this is called the *support* of g.

Lemma 7.2 *Let G be a group acting on a set Ω and $\Sigma \subseteq \Omega$. The following are all equivalent:*

(1) *Σ is a base for G.*

(2) *Σg is a base for G, for all $g \in G$.*

(3) *For all $g, h \in G$, if $\alpha g = \alpha h$ for all $\alpha \in \Sigma$, then $g = h$.*

(4) *$\Sigma \cap \operatorname{supp}(g) \neq \emptyset$, for all $1 \neq g \in G$.*

Proof. Exercise. □

Note that if Σ is a base for G, then any set containing Σ is also a base for G. Hence, we are interested in finding bases with the smallest possible size.

Example 7.3 Let $G = S_n$. Using the fourth part of the above lemma, we see that a base for S_n must have size at least $n - 1$.

Exercise 7.4 Show that the smallest base for $AGL_n(F)$ has size $n + 1$.

Lemma 7.5 *Let G be a faithful permutation group of degree n whose smallest base has size b. Then,*

$$2^b \leq |G| \leq n(n-1)\dots(n-b+1) \leq n^b$$

Proof. We may assume that $G \leq S_n$ and the base is $\{e_1, \dots, e_b\}$. By Lagrange's theorem, we have

$$\begin{aligned} |G| &= |G : G_{e_1}||G_{e_1} : G_{(e_1,e_2)}| \dots |G_{(e_1,\dots,e_{b-1})} : G_{(e_1,\dots,e_b)}||G_{(e_1,\dots,e_b)}| \\ &= |G : G_{e_1}||G_{e_1} : G_{(e_1,e_2)}| \dots |G_{(e_1,\dots,e_{b-1})} : G_{(e_1,\dots,e_b)}| \end{aligned}$$

We consider $|G_{(e_1,\dots,e_k)} : G_{(e_1,\dots,e_{k+1})}|$ for each $k = 0, \dots b-1$. By the Orbit-Stabiliser theorem, we have that this is less than $n - k$. However, since the base smallest possible size, $G_{(e_1,\dots,e_{k+1})} \lneqq G_{(e_1,\dots,e_k)}$. So, $|G_{(e_1,\dots,e_k)} : G_{(e_1,\dots,e_k,e_{k+1})}|$ is also greater than 2 and the lemma is proved. □

We have already seen that A_n and S_n are both primitive groups in general. We asked earlier about what we can say about other (faithful) primitive groups of degree n. We make a definition:

Definition 7.6 A *proper primitive group* is a faithful primitive group of degree n which is not A_n, or S_n.

Theorem 7.7 (Bochert 1889) *Let $G \leq Sym(\Omega)$ be a proper primitive group of degree n. Then, G has a base of size at most $n/2$.*

Proof. Let $\Sigma \subseteq \Omega$ be a base for G of minimal size and suppose for a contradiction that $|\Sigma| > n/2$. By minimality, $\Delta := \Omega - \Sigma$ is not a base. So, there exists $1 \neq g \in G$ such that its support is disjoint from Δ. That is, $\mathrm{supp}(g) \subseteq \Sigma$. Pick $\alpha \in \mathrm{supp}(g)$. By minimality, $\Sigma - \{\alpha\}$ is also not a base for G, so there exists $1 \neq h \in G$ whose support is disjoint from $\Sigma - \{\alpha\}$. However, since Σ is a base, $\mathrm{supp}(h) \cap \Sigma \neq \emptyset$, so $\alpha \in \mathrm{supp}(h)$. Hence,

$$\mathrm{supp}(g) \cap \mathrm{supp}(h) = \{\alpha\}$$

Let $\beta = \alpha g$ and $\gamma = \alpha h$. Then,

$$[g, h] = g^{-1}h^{-1}gh = (\alpha\gamma\beta)$$

is a 3-cycle contained in G (check this). However, by Theorem 5.6, $G \geq Alt(\Omega)$, a contradiction. □

Corollary 7.8 *A proper primitive group $G \leq Sym(\Omega)$ of degree n has order*

$$|G| \leq n(n-1)\ldots(n - \lfloor n/2 \rfloor + 1)$$

and index

$$|Sym(\Omega) : G| \geq (n - \lfloor n/2 \rfloor)!$$

Proof. We use Lemma 7.5 and Theorem 7.7. □

For example, let $B(n)$ be the bound given by the above Corollary 7.8 and let $M(n)$ be the order of the largest (faithful) proper primitive group of degree n. We compare the two in Table 1. We have also added the size of the symmetric group for comparison.

We do have better bounds than the one given by Bochert, however the one given is still quite useful. Finding a good bound, often for specific families of groups, is still an active area of research.

n	5	6	7	8	9	10	11	12
$M(n)$	20	120	168	1,344	1,512	1,440	7,920	95,040
$B(n)$	20	120	210	1,680	3,024	30,240	55,440	665,280
$\|S_n\|$	120	720	5,040	4,032	362,880	3,268,800	39,916,800	479,001,600

Table 1: Bochert's bound for primitive groups

Remark 7.9 As is suggested by Table 1, primitive groups are small. To give another example, consider S_{16}. It has an intransitive subgroup of index 16. The largest imprimitive subgroup has index 6,435 (order 3,251,404,800) whereas the largest proper primitive subgroup has index 64,864,800 (order 322,560). Can you construct these groups?

We have also given some results which restrict the structure of a primitive group – there are plenty more! These mean that the structure is quite restricted and so proper primitive groups are rare as is demonstrated in Table 2.

n	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$P(n)$	0	0	3	2	5	5	9	7	6	4	7	2	4	20	8	2	6	2

Table 2: Number of proper primitive groups of degree n

In fact, there are infinitely many n for which there are no proper primitive groups; that is, the only primitive groups are A_n and S_n.

Remark 7.10 Since the beginning of group theory and permutation groups, people have been trying to list the primitive permutation groups. Even for quite small n, say $n \leq 20$ this is a hard task to do by hand! Not much progress was made until the advent of computer algebra packages in the 60s. The O'Nan-Scott theorem was proved in 1979, which classified the possible maximal subgroups of S_n. However, it was Cameron in 1981 who realised that, using the CFSG, this could be applied to greatly restrict the structure of primitive permutation groups and split them into half a dozen different classes. These fall roughly into two types, affine and non-affine. This allowed much more efficient computation of the primitive permutation groups.

- 1871, Jordan, $n \leq 17$ with omissions in $n = 9, 12, 15, 16, 17$
- 1874, Jordan, $n = 19$
- 1893, Cole, $n = 9$
- 1895-1900, Miller, corrected $n = 12, \ldots, 17$

- 1912, Martin (1901) and Bennett (1912), $n \leq 20$
- 1960s, Sims, $n \leq 50$, lists passed around the mathematical community and formed one of the earliest databases in computational group theory
- 1988, Dixon & Mortimer, $n < 1000$ non-affine, using the O'Nan-Scott theorem
- 1991, Short, $n < 256$ soluble affine
- 2003, Eick & Höfling, $n < 6561$ soluble affine
- 2003, Roney-Dougal & Unger, $n < 1,000$ affine
- 2005, Roney-Dougal, all $n < 2,500$
- 2009, Coutts, Quick & Roney-Dougal, all $n < 4,096$