Queen Mary
University of London

MTHM024/MTH714U **Group Theory**

Peter Cameron's 2010 Revision Notes, Section 3, slightly updated by LHS, 2014

3 Group actions

A group is an abstract object, and often we need to represent it in a more concrete way, for example, by permutations of a set, or by matrices over a field. We want the multiplication of the permutations or matrices to reflect the operation in the given group; that is to say, we want to have a homomorphism from the group to either a symmetric group or a general linear group. Using a homomorphism allows us a little extra flexibility: it is possible that the homomorphism is not injective, so that different group elements are represented by the same permutation or matrix.

In this chapter we look at representations by permutations, describe their structure, and look briefly at some other counting problems which are developed further in Enumerative Combinatorics.

3.1 Definition

An *action* of a group G on a set Ω is a homomorphism from G to the symmetric group $\mathrm{Sym}(\Omega)$. In other words, to each group element we associate a permutation, and the product of group elements is associated with the composition of the corresponding permutations. We will always have in mind a fixed action θ; so $g\theta$ is a permutation of Ω, and we can talk about $\alpha(g\theta)$ for $\alpha \in \Omega$. To simplify notation, we suppress the name of the action, and simply write αg (or α^g) for the image of α under the permutation corresponding to g.

Alternatively, we can define an action of G on Ω as a map μ from $\Omega \times G$ to Ω satisfying the two laws

(a) $\mu(\mu(\alpha,g),h) = \mu(\alpha,gh)$ for all $g,h \in G$, $\alpha \in \Omega$.

(b) $\mu(\alpha,1) = \alpha$ for all $\alpha \in \Omega$.

Again we simplify notation by suppressing the name μ: we write $\mu(\alpha,g)$ as αg. Then (a) says that $(\alpha g)h = \alpha(gh)$; it follows from (a) and (b) that the map $\alpha \mapsto \alpha g$ is a permutation of Ω (its inverse is $\alpha \mapsto \alpha g^{-1}$), and so we do indeed have a homomorphism from G to $\mathrm{Sym}(\Omega)$.

Example Let $G = S_4$, and let Ω be the set of three partitions of $\{1,2,3,4\}$ into two sets of size 2. Any permutation in G can be used to transform the partitions: for example, $g = (1,3,4)$ maps $12|34 \mapsto 14|23 \mapsto 13|24$. This gives an action of G on a set of size 3, that is, a homomorphism from S_4 to S_3. It is easily checked that this homomorphism is onto, and that its kernel is the Klein group V_4 consisting of the identity, $(1,2)(3,4)$, $(1,3)(2,4)$ and $(1,4)(2,3)$. Thus V_4 is a normal subgroup of S_4, and $S_4/V_4 \cong S_3$ (by the First Isomorphism Theorem).

Example There are several ways of making a group act on itself (that is, we take $\Omega = G$):

Right multiplication: $\mu(x,g) = xg$.

Left multiplication: $\mu(x,g) = g^{-1}x$ (the inverse is needed to ensure that acting with g and then with h is the same as acting with gh).

Conjugation: $\mu(x,g) = g^{-1}xg$.

The first of these actions has an important consequence. The action by right multiplication is *faithful*: if $\mu(x,g) = \mu(x,h)$ for all $x \in G$, then $g = h$. (Indeed, $1g = 1h$ implies $g = h$.) This means that the action homomorphism from G into $\mathrm{Sym}(G)$ is one-to-one (its kernel is the identity). By the First Isomorphism Theorem, the image of this map is a subgroup of $\mathrm{Sym}(G)$ which is isomorphic to G. Hence:

Theorem 3.1 (Cayley's Theorem) *Every group is isomorphic to a subgroup of some symmetric group.*

As well as motivating the study of symmetric groups and their subgroups, this theorem has historical importance. As noted earlier, group theory had existed as a mathematical subject for a century before the group laws were written down by Walther von Dyck in 1882. In those days the word "group" meant what we would now describe as a *permutation group* or *transformation group*, that is, a subgroup of the symmetric group. (In detail, a group was a set of transformations of a set which is closed under composition, contains the identity transformation, and contains the inverse of each of its elements. Since composition of transformations is associative, we see that every transformation group is a group in the modern sense. In the other direction, Cayley's theorem shows that every group is isomorphic to a transformation group; so, despite the change in foundations, the actual subject matter of group theory didn't change at all!

Finally, we note that the permutation group given by Cayley's Theorem can be written down from the Cayley table of G: the permutation of G corresponding to the element $g \in G$ is just the column labelled g of the Cayley table. Referring back to the two Cayley tables in Section 1.1, we see that as permutation groups

$$\begin{aligned} C_4 &= \{1,(e,a,b,c),(e,b)(a,c),(e,c,b,a)\}, \\ V_4 &= \{1,(e,a)(b,c),(e,b)(a,c),(e,c)(a,b)\}. \end{aligned}$$

Both these groups are abelian so we could have used rows rather than columns to get the same result; but in general it makes a difference.

3.2 Orbits and stabilisers

Let G act on Ω. We define a relation $\equiv$ on Ω by the rule that $\alpha \equiv \beta$ if there is an element $g \in G$ such that $\alpha g = \beta$. Then $\equiv$ is an equivalence relation. (You should prove this as an exercise. It is instructive to see how the reflexive, symmetric and transitive laws for $\equiv$ follow from the identity, inverse and closure laws for G.) The equivalence classes of this relation are called *orbits*; we say that the action is *transitive* (or that G acts *transitively* on Ω) if there is just one orbit.

We denote the orbit containing a point α by $\mathrm{Orb}_G(\alpha)$. Note that

$$\mathrm{Orb}_G(\alpha) = \alpha G = \{\alpha g : g \in G\}.$$

For example, the action of G on itself by right multiplication is transitive; in the action by conjugation, the orbits are the conjugacy classes.

Given a point α, the *stabiliser* of α is the set of elements of G which map α to itself:

$$\mathrm{Stab}_G(\alpha) = G_\alpha = \{g \in G : \alpha g = \alpha\}.$$

Theorem 3.2 (Orbit-Stabiliser Theorem) *Let G act on Ω, and choose $\alpha \in \Omega$. Then $\mathrm{Stab}_G(\alpha)$ is a subgroup of G; and there is a bijection between the set of right cosets of $\mathrm{Stab}_G(\alpha)$ in G and the orbit $\mathrm{Orb}_G(\alpha)$ containing α.*

It follows from the Orbit-Stabiliser Theorem that if G is finite then $|\mathrm{Stab}_G(\alpha)| \cdot |\mathrm{Orb}_G(\alpha)| = |G|$.

The correspondence works as follows. Given $\beta \in \mathrm{Orb}_G(\alpha)$, by definition there exists $h \in G$ such that $\alpha h = \beta$. Now it can be checked that the set of all elements mapping α to β is precisely the right coset $(\mathrm{Stab}_G(\alpha))h$.

Every subgroup of G occurs as the stabiliser in a suitable transitive action of G. For let H be a subgroup of G. Let Ω be the set of all right cosets of H in G, and define an action of G on Ω by, formally, $\mu(Hx, g) = Hxg$. (Informally we would write $(Hx)g = Hxg$, but this conceals the fact that $(Hx)g$ means the result of acting on the point Hx with the element g, not just the product in the group, though in fact it comes to the same thing!) It is readily checked that this really is an action of G, that it is transitive, and that the stabiliser of the coset $H1 = H$ is the subgroup H (exercise).

So the Orbit-Stabiliser Theorem can be regarded as a refinement of Lagrange's Theorem.

3.3 The Orbit-Counting Lemma

The Orbit-Counting Lemma is a formula for the number of orbits of a finite group G acting on a finite set Ω, in terms of the numbers of fixed points of all the permutations in G. Given an action of G on Ω, and $g \in G$, let $\mathrm{fix}(g)$ be the number of fixed points of g (strictly, of the permutation of Ω induced by g). The Lemma says that the number of orbits is the average value of $\mathrm{fix}(g)$, for $g \in G$.

Theorem 3.3 (Orbit-Counting Lemma) *Let G be a finite group acting on a finite set Ω. Then the number of orbits of G on Ω is equal to*

$$\frac{1}{|G|}\sum_{g\in G}\mathrm{fix}(g).$$

The proof illustrates the Orbit-Stabiliser Theorem. We form a bipartite graph with vertex set $\Omega \cup G$; we put an edge between $\alpha \in \Omega$ and $g \in G$ if $\alpha g = \alpha$. Now we count the edges of this graph.

On one hand, every element $g \in G$ lies in $\mathrm{fix}(g)$ edges; so the number of edges is $\sum_{g\in G}\mathrm{fix}(g)$.

On the other hand, the point α lies in $|\mathrm{Stab}_G(\alpha)|$ edges; so the number of edges passing through points of $\mathrm{Orb}_G(\alpha)$ is $|\mathrm{Orb}_G(\alpha)| \cdot |\mathrm{Stab}_G(\alpha)| = |G|$, by the Orbit-Stabiliser Theorem. So each orbit accounts for $|G|$ edges, and the total number of edges is equal to $|G|$ times the number of orbits.

Equating the two expressions and dividing by $|G|$ gives the result.

Example The edges of a regular pentagon are coloured red, green and blue. How many different ways can this be done, if two colourings which differ by a rotation or reflection of the pentagon are regarded as identical?

The question asks us to count the orbits of the dihedral group D_{10} (the group of symmetries of the pentagon) on the set Ω of colourings with three colours. There are

3^5 colourings altogether, all fixed by the identity. For a colouring to be fixed by a non-trivial rotation, all the edges have the same colour; there are just three of these. For a colouring to be fixed by a reflection, edges which are images of each other under the reflection must get the same colour; three colours can be chosen independently, so there are 3^3 such colourings.

Since there are four non-trivial rotations and five reflections, the Orbit-Counting Lemma shows that the number of orbits is

$$\frac{1}{10}(1 \cdot 243 + 4 \cdot 3 + 5 \cdot 27) = 39.$$

3.4 Appendix: How many groups?

The number of $n \times n$ arrays with entries chosen from a set of size n is n^{n^2}. So certainly this is an upper bound for the number of groups of order n.

In fact one can do much better, using two results from elementary group theory: the theorems of Lagrange and Cayley.

Theorem 3.4 *The number of groups of order n is at most* $n^{n \log_2 n}$.

Proof By Cayley's Theorem, every group of order n is isomorphic to a subgroup of the symmetric group S_n. So if we can find an upper bound for the number of such subgroups, this will certainly bound the number of groups up to isomorphism.

We use Lagrange's Theorem in the following way. We say that a set $\{g_1, \ldots, g_k\}$ of elements of a group G *generates* G if no proper subgroup of G contains all these elements. Equivalently, every element of G can be written as a product of these elements and their inverses.

Now we have the following:

Proposition 3.5 *A group of order n can be generated by a set of at most* $\log_2 n$ *elements.*

To see this, pick a non-identity element g_1 of G, and let G_1 be the subgroup generated by g_1. If $G_1 = G$, stop; otherwise choose an element $g_2 \notin G_1$, and let G_2 be the subgroup generated by g_1 and g_2. Continue in this way until we find $g_1, \ldots, g_k$ which generate G.

We claim that $|G_i| \geq 2^i$ for $i = 1, \ldots, k$. The proof is by induction on i. The assertion is clear for $i = 1$, since by assumption $|G_1| > 1$, so $|G_1| \geq 2$. Now suppose that $|G_i| \geq 2^i$. Now G_i is a subgroup of G_{i+1}, and so $|G_i|$ divides $|G_{i+1}|$, by Lagrange's Theorem; since $G_i \neq G_{i+1}$, we have that $|G_{i+1}| \geq 2|G_i| \geq 2^{i+1}$. So the assertion is proved by induction.

Finally, $n = |G| = |G_k| \geq 2^k$, so $k \leq \log_2 n$.

Thus, to specify a subgroup G of order n of S_n, we only have to pick $k = \lfloor \log_2 n \rfloor$ elements which generate G. There are at most $n!$ choices for each element, so the number of subgroups is at most

$$(n!)^k \leq (n^n)^{\log_2 n} = n^{n \log_2 n},$$

since clearly $n! \leq n^n$.

We have seen a proof that there is a unique group of prime order. Here are proofs that the numbers of groups of orders 4, 6, 8 are 2, 2 and 5 respectively.

Order 4**:** Let G be a group of order 4. If G contains an element of order 4, then it is cyclic; otherwise all its elements apart from the identity have order 2. Let $G = \{1, x, y, z\}$. What is xy? By the cancellation laws, xy cannot be 1 (since $xx = 1$), or x, or y; so $xy = z$. Similarly the product of any two of x, y, z is the third, and the multiplication table is determined. So there is at most one type of non-cyclic group. But the group $C_2 \times C_2$ realises this case.

Order 6**:** Again suppose that there is no element of order 6, so that elements of G have orders 1, 2 and 3 only. All these orders actually appear [why?]. Let a have order 3 and b order 2. Then it is easy to see that $G = \{1, a, a^2, b, ab, a^2b\}$. We cannot have $ba = ab$, since then we would find that this element has order 6. All other possibilities for ba except $ba = a^2b$ are eliminated by the cancellation laws. So $ba = a^2b$, and then the multiplication table is determined. This case is realised by the symmetric group S_3.

Order 8**:** If there is an element of order 8, then G is cyclic; if no element has order greater than 2, then $G = C_2 \times C_2 \times C_2$ (this is a bit harder). So assume that a is an element of order 4, and let b be an element which is not a power of a. Then $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. This time we need to know which of these eight elements is b^2, and which is ba, in order to determine the group. We find that $b^2 = 1$ or $b^2 = a^2$, and that $ba = ab$ or $ba = a^3b$. There seem to be four different possibilities; but two of these turn out to be isomorphic (namely, the cases $b^2 = 1, ba = ab$ and $b^2 = a^2, ba = ab$). So there are three different groups of this form. All of them actually occur: they are $C_4 \times C_2$ and the dihedral and quaternion groups. These together with the two we already found make five altogether.