CHAPTER 1

General theory

1.1 History

Until about 1850, the term 'group' referred to a set G of transformations of a set Ω, such that G is closed under composition, contains the identity transformation, and contains the inverse of each of its elements. This is what would now be called a 'permutation group'. (Because of the last requirement, every element of G has an inverse, and so is one-to-one and onto, that is, a permutation.)

In the modern, axiomatic approach, a group is a set with a binary operation (a function from G^2 to G) which satisfies the closure, associativity, identity and inverse laws. (In fact, closure is not necessary, since a binary operation satisfies it by definition. It remains as a historical relic.)

Of course, the two approaches are essentially the same; we take the modern viewpoint because we do not want to restrict group elements to being transformations of something. Any permutation group is an abstract group with the operation of function composition (since this operation is necessarily associative). Conversely, Cayley's Theorem asserts that any abstract group is isomorphic to a transformation group. Note that, though the axioms (apart from the associative law) match up, the interpretation is different: the identity in an abstract group is defined by its properties with respect to the group operation, and has to be proved unique; the identity in a permutation group is a specific function.

There are two good practical reasons for preferring the modern approach. First, the same group may act as a permutation group on more than one set. This is familiar in parts of combinatorics, such as design theory, where a group of automorphisms of a design acts on both the points and the blocks

of the design. Second, we can take the powerful theory of abstract groups (including, for example, the classification of the finite simple groups) and apply its conclusions to permutation groups.

On the other hand, when we are studying a particular permutation group, the work we are doing would not be unfamiliar to mathematicians of the 'classical' period such as Lagrange, Galois, or Jordan.

1.2 Actions and G-spaces

Let Ω be a set. (Since Wielandt's pioneering book [186], it has been customary to use Ω for the set on which permutation groups act, and lowercase Greek letters for its elements.) The *symmetric group* on Ω, written $\mathrm{Sym}(\Omega)$, is the set of all permutations of Ω: it forms a group, with the operation of composition. We write permutations on the right, and compose from left to right: that is, the image of α under the permutation g is αg, and the composition of g and h is gh (so that $\alpha(gh) = (\alpha g)h$). If Ω is a finite set with n elements, we write S_n for the symmetric group on Ω.

A *permutation group* on Ω is a subgroup of $\mathrm{Sym}(\Omega)$.

Let G be a group. An *action* of G on Ω is a homomorphism ϕ from G to $\mathrm{Sym}(\Omega)$. We usually abbreviate $\alpha(g\phi)$ (the image of α under the permutation corresponding to ϕ) to αg.

The image of an action of G on Ω is a permutation group, called the permutation group *induced* on Ω by G, and written G^Ω. We say that an action is *faithful* if its kernel is the identity. If this holds, then G is isomorphic to G^Ω.

There is another way to formalise this concept, in axiomatic terms. A *G-space* is a set Ω with a function $\mu : \Omega \times G \to \Omega$ satisfying the conditions

(A1) $\mu(\mu(\alpha, g), h) = \mu(\alpha, gh)$ for all $\alpha \in \Omega$ and $g, h \in G$;

(A2) $\mu(\alpha, 1) = \alpha$ for any $\alpha \in \Omega$, where 1 is the identity of G.

This is essentially the same thing. For, if ϕ is an action of G on Ω, then the function μ defined by $\mu(\alpha, g) = \alpha(g\phi)$ makes Ω into a G-space. Conversely, suppose that (Ω, μ) is a G-space. For each $g \in G$, there is a function $\pi_g : \Omega \to \Omega$ given by $\alpha\pi_g = \mu(\alpha, g)$. Then π_1 is the identity function, and $\pi_{g^{-1}}$ is the inverse function to π_g, so each function π_g is a permutation; and then (A1) shows that the map $\phi : g \mapsto \pi_g$ is a homomorphism, that is, an action of G.

Accordingly, when there is no risk of confusion, we will write $\mu(\alpha, g)$ simply as αg.

Each point of view leads to slightly different language for describing the situation. Thus, when we define the property of transitivity in the next

section, we will say that G is a transitive permutation group, or that G acts transitively on Ω, or that Ω is a transitive G-space, all meaning the same thing.

We say that two G-spaces Γ and Δ are *isomorphic* if there is a bijection $\theta : \Gamma \to \Delta$ such that, for any $\alpha \in \Gamma$ and $g \in G$, we have

$$\mu_\Gamma(\alpha, g)\theta = \mu_\Delta(\alpha\theta, g).$$

In other words, the diagram of Figure 1.1 commutes, where g on the left refers

$$\begin{array}{ccc} \Gamma & \xrightarrow{\theta} & \Delta \\ g_\Gamma \downarrow & & \downarrow g_\Delta \\ \Gamma & \xrightarrow{\theta} & \Delta \end{array}$$

Figure 1.1: G-space isomorphism

to the action on Γ, and on the right to the action on Δ. Informally, the two sets Γ and Δ can be matched up in such a way that the actions of G on them are 'the same'.

As is usual in algebra, we regard isomorphic G-spaces as being the same. In the next two sections, we will give a classification of G-spaces up to isomorphism.

Finally, we define the *degree* of a permutation group, group action, or G-space to be the cardinality of the set Ω (a finite or infinite cardinal number).

1.3 Orbits and transitivity

Let Ω be a G-space. We define a relation $\sim$ on Ω by the rule that $\alpha \sim \beta$ if and only if there is an element $g \in G$ with $\alpha g = \beta$. Now $\sim$ is an equivalence relation. (The reflexive, symmetric and transitive laws come directly from the identity, inverse and closure laws in the 'old' definition of a permutation group.) The equivalence classes of $\sim$ are the *orbits* of G; and we say that G is *transitive* (or Ω is a *transitive* G-space) if there is just one orbit. Note that each orbit is a G-space in its own right. So we have our first structure theorem:

Theorem 1.1 *Every G-space can be uniquely expressed as a disjoint union of transitive G-spaces.*

From the point of view of permutation groups, however, the situation is not so simple. Suppose that G is a permutation group on Ω, with orbits Ω_i

for $i \in I$, where I is some index set for the set of orbits. Then G acts on each set Ω_i, and so induces a transitive permutation group G^{Ω_i}. These groups G^{Ω_i}, for $i \in I$, are called the *transitive constituents* of G. How is G built from its transitive constituents?

Let $(G_i : i \in I)$ be a family of groups. We define the *cartesian product* $G = \prod_{i \in I} G_i$ to be the set of all functions f from I to $\bigcup_{i \in I} G_i$ which have the property that $f(i) \in G_i$ for all $i \in I$; the group operation is defined 'coordinatewise', that is, for $f_1, f_2 \in G$, we define $f_1 f_2$ by the rule that $(f_1 f_2)(i) = f_1(i) f_2(i)$ for each $i \in I$.

There is a projection map $\phi_i : G \to G_i$ for each $i \in I$, which maps each function f to the element $f(i) \in G_i$. (This construction generalises the *direct product* of finitely many groups.) We say that a subgroup H of G is a *subcartesian product* of the groups $(G_i : i \in I)$ if the restriction of ϕ_i maps H onto G_i for each $i \in I$. Then we have:

Theorem 1.2 *Any permutation group is a subcartesian product of its transitive constituents.*

Example. Consider the two permutation groups G_1 and G_2 on the set $\{1,2,3,4\}$ given by

$$G_1 = \{(1), (1\ 2)(3\ 4)\},$$
$$G_2 = \{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

Each has two orbits, namely $\{1,2\}$ and $\{3,4\}$; in each case, both the transitive constituents are cyclic groups of order 2. We see that G_2 is the full cartesian product of these two cyclic groups, whereas G_1 is a proper subcartesian product.

1.4 Transitive groups and coset spaces

Let H be a subgroup of G. The (right) *coset space* $H\backslash G$ is the set of right cosets $\{Hx : x \in G\}$, with action of G given by $\mu(Hx, g) = Hxg$ for all $x, g \in G$. (The action is written formally in the μ form here since, with our less formal convention, it would read $Hxg = Hxg$!) It is a transitive G-space. Note that $H\backslash G$ is not the same thing as the set-theoretic difference $H \setminus G$, though typographically they are almost identical. The notation suggests right cosets, with elements of G placed on the right of H. The set of left cosets would be written G/H. Some authors write $G : H$ or $(G : H)$ indiscriminately for either coset space.

The classification of transitive G-spaces, up to isomorphism, is given by the following theorem. If G acts on Ω and $\alpha \in \Omega$, the *stabiliser* of α is the set

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

of all group elements for which the corresponding permutation fixes α. It is a subgroup of G. If Ω is the coset space $H\backslash G$, then the stabiliser of the *coset* $H1 = H$ is the *subgroup* H.

Theorem 1.3 *(a) Let Ω be a transitive G-space. Then Ω is isomorphic to the coset space $H\backslash G$, where $H = G_\alpha$ for $\alpha \in \Omega$.*

(b) Two coset spaces $H\backslash G$ and $K\backslash G$ are isomorphic if and only if H and K are conjugate subgroups of G.

Sketch proof. (a) The isomorphism is given by

$$\beta \in \Omega \leftrightarrow \{g \in G : \alpha g = \beta\},$$

the set on the right being a right coset of G_α.

(b) The conjugates of G_α are the stabilisers of the points of Ω: this proves the reverse implication. For the forward implication, let θ be an isomorphism between the coset spaces $H\backslash G$ and $K\backslash G$. If θ maps H to Kx, then the stabiliser of H (which is just H) is equal to the stabiliser of Kx (which is $x^{-1}Kx$, a conjugate of K).

So the transitive G-spaces are classified by the conjugacy classes of subgroups of G.

We note two important consequences.

Corollary 1.4 *Let G act transitively on Ω, and $\alpha \in \Omega$.*

(a) A subset S of G is a set of right coset representatives for G_α in G if and only if S contains just one element mapping α to β for all $\beta \in \Omega$.

(b) If G is finite, then

$$|G| = |\Omega| \cdot |G_\alpha|.$$

The second part of the corollary is a form of Lagrange's Theorem, since any subgroup H of G is a point stabiliser in some transitive action of G (namely, on the coset space $G\backslash H$).

From the perspective of permutation groups, once again, the situation is a bit more complicated. The *core* of the subgroup H of G is given by

$$\mathrm{Core}_G(H) = \bigcap_{x \in G} x^{-1}Hx;$$

it is the largest normal subgroup of G which is contained in H. Now the conjugates $x^{-1}Hx$ are the stabilisers of the points Hx of the coset space $H\backslash G$; so $\mathrm{Core}_G(H)$ is the kernel of the action of G on the coset space. In other words, given a group G, the transitive permutation groups isomorphic to G (that is, the faithful transitive actions) are classified by the conjugacy classes of *core-free* subgroups (those whose core is the identity).

Example. Let G be the Klein group $C_2 \times C_2$. How many isomorphism types of n-element G-spaces are there?

The group G has one subgroup of order 4, three of order 2, and one of order 1. Each is conjugate only to itself, since G is abelian. So there are just five transitive G-spaces up to isomorphism, with cardinalities $1, 2, 2, 2, 4$.

Let a_n be the total number of n-element G-spaces, up to isomorphism. Then a_n is the number of ways of paying a bill of n cents with a supply of 1-cent coins, three different kinds of 2-cent coins, and 4-cent coins. By standard combinatorial arguments, we have

$$\sum_{n\geq 0} a_n x^n = \frac{1}{(1-x)(1-x^2)^3(1-x^4)}.$$

Now the right-hand side is analytic in $\mathbb{C}$ apart from poles at 1, -1, i, and $-$i. So the asymptotic form of a_n can be found by standard analytic arguments.

Clearly the same process can be performed (in principle) for any finite group G.

1.5 Sylow's Theorem

We will illustrate the ideas of group actions by proving Sylow's Theorem, the most important result in elementary finite group theory. This was originally proved using arguments with double cosets; the proof given here, based on group actions, is due to Wielandt [182].

Theorem 1.5 (Sylow's Theorem) *Let G be a group of order $n = p^a m$, where p is prime and doesn't divide m. Then*

(a) G has a subgroup of order p^a;

(b) all subgroups of order p^a are conjugate;

(c) any subgroup of p-power order is contained in a subgroup of order p^a.

Proof. To show (a), we let Ω be the set of all subsets of G of cardinality p^a. Then Ω is a set of cardinality $\binom{n}{p^a}$. We define an action of G on Ω by right multiplication: $\mu(S, g) = Sg$ for $S \in \Omega$, $g \in G$. Then Ω is the union of the G-orbits of this action. Note that each G-orbit, as a set of subsets of G, covers all of G: for if $x \in S$, then $y \in Sx^{-1}y$. So there are two types of orbit:

Type 1: orbits containing exactly $n/p^a = m$ sets, covering G without overlapping;

Type 2: orbits containing more than m sets.

Now if S is in a Type 1 orbit, then its stabiliser has order $n/m = p^a$, and so is a subgroup P of the required order. (In this case, if S is chosen to contain the identity, then $S = P$, and the orbit of S is just the set of right cosets of P.) On the other hand, if S is in a Type 2 orbit Δ, then $|\Delta| > m$, so $|\Delta|$ is divisible by p. So, if we can show that $|\Omega|$ is not divisible by p, then it will follow that there must be Type 1 orbits, and (a) will be proved.

It follows from Lucas' Theorem on congruence of binomial coefficients (or can be proved directly) that $\binom{p^a m}{p^a} \equiv m \pmod{p}$. So the number of sets in Type 1 orbits is congruent to m mod p, and the number of subgroups of order p^a is congruent to 1 mod p.

Alternatively, this can be proved with a trick. Consider the cyclic group of order n. This has exactly one subgroup of order p^a, so for this group the number of sets in Type 1 orbits is congruent to m mod p^a. It follows that $\binom{p^a m}{p^a} \equiv m \pmod{p}$, as required.

We prove (b) and (c) together by using a different action of G, by conjugation on the set Ξ of subgroups of order p^a. We need the following observation. Let $|P| = p^a$ and $|Q| = p^b$ $(b \leq a)$. If Q fixes P in this action, then $Q \leq P$. For Q normalises P, and so PQ is a subgroup, of order $|P| \cdot |Q|/|P \cap Q|$. This is a power of p, and hence (by Lagrange's Theorem) cannot be larger than $|P| = p^a$. So $|P \cap Q| \geq |Q|$, whence we have $Q \leq P$. In particular, a subgroup of order p^a can fix only one element of Ξ, namely itself.

We see that P has one orbit of size 1 on Ξ (itself), and all other orbits have size divisible by p. Thus, $|\Xi| \equiv 1 \pmod{p}$, in agreement with our observation in the proof of (a). But we also see that one G-orbit (the one containing P) has size congruent to 1 mod p, and all the others (if any) have size divisible by p. But this argument applies for any subgroup of order p^a, and shows that any such subgroup lies in the unique orbit of size congruent to 1 mod p. So there is only one orbit: in other words, all subgroups of order p^a are conjugate. We have proved (b).

Now Q certainly has a fixed point P in Ξ, since $|\Xi| \equiv 1 \pmod{p}$. By the above remarks, $Q \leq P$. Thus (c) is proved.

1.6 Regular groups

The permutation group G is *semiregular* if only the identity has a fixed point; it is *regular* if it is transitive and semiregular. By the structure theorem for transitive groups (Theorem 1.3), if G is regular on Ω, then Ω is isomorphic to the space of right cosets of the identity; each such coset is a 1-element set, so we can identify the coset space with the set G, on which G acts by right multiplication: $\mu(x, g) = xg$. This is the *right regular representation* of G, which occurs in the proof of Cayley's Theorem.

There is also a *left regular representation* of G on itself, given by the rule that $\mu(x,g) = g^{-1}x$. (The inverse is required here to make a proper action: note that $h^{-1}(g^{-1}x) = (gh)^{-1}x$.) It is, as the name says, also a regular action, and so must be isomorphic to the right regular action: indeed the map $x \mapsto x^{-1}$ is an isomorphism.)

The left and right regular representations commute with each other:

$$g^{-1}(xh) = (g^{-1}x)h.$$

(Note how the associative law for G translates into the commutative law for these actions.) In fact, it can be shown that the centraliser, in the symmetric group, of the (image of the) right regular representation is the left regular representation.

So we have an action of $G^* = G \times G$ on G, the product of the two regular actions:

$$\mu(x,(g,h)) = g^{-1}xh.$$

This transitive action contains both the left and the right regular actions as normal subgroups. The stabiliser of the identity is the *diagonal subgroup*

$$\{(g,g) : g \in G\},$$

acting by conjugation on G. For this reason we call G^* a *diagonal group*.

Example. Higman, Neumann and Neumann [92] constructed an infinite group G with the property that all the non-identity elements of G are conjugate. (Such a group, of course, is simple.) Then the diagonal group G^* has the property that the stabiliser of the identity is transitive on the non-identity elements. As we will see, this means that G is *2-transitive*. Yet it is the direct product of two regular subgroups.

We outline the proof, which depends on the so-called *HNN-construction*. Let G be a group, A and B subgroups of G, and $\phi : A \to B$ an isomorphism. Then the group

$$G' = \langle G, t : t^{-1}at = a\phi \text{ for all } a \in A\rangle$$

has the properties

- G is embedded isomorphically in G';
- any element of G' with finite order lies in a conjugate of G (so that, if G is torsion-free, so is G');
- $t^{-1}Gt \cap G = B$ and $tGt^{-1} \cap G = A$.

In particular, if G is torsion-free and a, b are non-identity elements of G, then G can be embedded in a torsion-free group G' in which a and b are conjugate.

Repeating this process for each pair of non-identity elements of G, we see that, if G is countable and torsion-free, then G can be embedded in a group $G^\dagger$ such that any two non-identity elements of G are conjugate in $G^\dagger$; and $G^\dagger$ is also countable and torsion-free.

Now put $G_0 = G$ and $G_{n+1} = G_n^\dagger$ for all $n \in \mathbb{N}$, and $G^* = \bigcup_{n\in\mathbb{N}} G_n$. Then G^* is countable; and any two non-identity elements of G^* lie in G_n for some n, so are conjugate in G_{n+1} (and *a fortiori* in G^*).

1.7 Groups with regular normal subgroups

Let G be a permutation group on Ω with a regular normal subgroup N. Then there is a bijection from Ω to N, which takes the given action of N on Ω to its action on itself by right multiplication: pick $\alpha \in \Omega$ and set

$$n \in N \leftrightarrow \beta = \alpha n \in \Omega.$$

It turns out that this map is also an isomorphism between the given action of G_α on Ω and its action on the normal subgroup N by conjugation: for, if $g \in G_\alpha$ maps β to γ, and $\alpha n_1 = \beta$, $\alpha n_2 = \gamma$, then

$$\alpha(g^{-1}n_1g) = \alpha n_1 g = \beta g = \gamma,$$

and since $g^{-1}n_1g \in N$, and N is regular, we have $g^{-1}n_1g = n_2$, as required.

Since $G = NG_1$ and $N \cap G_1 = 1$, we have that G is a *semidirect product* of N by G_1.

Conversely, if N is any group, and H a subgroup of its automorphism group $\mathrm{Aut}(N)$, then the semidirect product of N by H acts as a permutation group on N, with N as regular normal subgroup and H as the stabiliser of the identity: the element hn of $N \rtimes H$ acts on N by the rule

$$\mu(x, hn) = x^h n$$

for $x, n \in N$, $h \in H$.

Example 1. If $Z(N) = 1$, then $N \cong \mathrm{Inn}(N)$, the group of inner automorphisms of G, and the semidirect product $N \rtimes \mathrm{Inn}(N)$ is the diagonal group $N^* = N \times N$ described earlier. (Note that $Z(N) = 1$ is a necessary and sufficient condition for the action of N^* to be faithful: see Exercise 1.6.)

Example 2. The group $N \rtimes \mathrm{Aut}(N)$ is the *holomorph* of N.

Example 3. Let V be a vector space, N its additive group, and $H = \mathrm{GL}(V)$, the *general linear group* (the group of all invertible linear transformations of V). Then $N \rtimes H$ is the *affine general linear group* $\mathrm{AGL}(V)$.

1.8 Multiple transitivity

Let k be a positive integer less than $|\Omega|$. We say that G is *k-transitive* on Ω if it acts transitively on the set of all k-tuples of distinct elements of Ω (where the action is *componentwise*: $(\alpha_1, \ldots, \alpha_k)g = (\alpha_1 g, \ldots, \alpha_k g)$).

For $k > 1$, G is k-transitive on Ω if and only if

- G is transitive on Ω, and
- G_α is $(k-1)$-transitive on $\Omega \setminus \{\alpha\}$.

(A special case of this result was used in the example in Section 1.6.)

Note that a k-transitive group is l-transitive for all $l \leq k$. The symmetric group S_n is n-transitive, while the *alternating group* A_n (the set of elements of S_n with even parity) is $(n-2)$-transitive. This is because there are exactly two permutations in S_n which map a given $(n-2)$-tuple of distinct points to another; and they differ by a transposition of the remaining two points, so one is even and one is odd. (See Section 1.17 for a discussion of parity.)

We now investigate when groups with regular normal subgroups can be k-transitive.

Theorem 1.6 *Let G be k-transitive and have a regular normal subgroup N. Assume that $G \neq S_k$.*

(a) If Ω is finite and $k = 2$, then N is an elementary abelian p-group for some prime p.

(b) If $k \geq 3$, then N is an elementary abelian 2-group.

Proof. If G is k-transitive, then G_α acts as a group of automorphisms of N, which is $(k-1)$-transitive on the non-identity elements.

(a) Suppose that G is finite and $k = 2$. Take $x_1, x_2 \in N \setminus \{1\}$. Then some element of G_1 conjugates x_1 to x_2, so these elements have the same order. This order must be prime, since if x has composite order rs then x^r has order s. So N is a p-group. Now $Z(N) \neq 1$, and since no automorphism can map an element of $Z(N)$ to one outside, we must have $Z(N) = N$, and N is elementary abelian.

This fails for infinite groups, as the Higman–Neumann–Neumann diagonal example shows.

(b) Now suppose that $k = 3$, and $|N| > 3$ (possibly infinite). We claim that every element $x \in N$ satisfies $x^2 = 1$. Suppose that $x^2 \neq 1$, and choose $y \neq 1, x, x^2$. Then no automorphism can map x to x and x^2 to y, contrary to assumption. So N is an elementary abelian 2-group.

Note that the affine group $\mathrm{AGL}(V)$ is always 2-transitive, and that it is 3-transitive if V is a vector space over the field with 2 elements.