PART I

The Algebraic Background

1
Groups

It is likely that the reader has already met the concept of a group. It was Galois who first understood the imporance of groups in the study of the roots of a polynomial equation; since then, group theory has blossomed, and developed as a subject in its own right. In this chapter we simply develop those parts of the theory which we shall need later; one of the main purposes is to explain the notation and terminology that we shall use.

1.1 Groups

Suppose that S is a set. A *law of composition* $\circ$ on S is a mapping from the Cartesian product $S \times S$ into S; that is, for each ordered pair (s_1, s_2) of elements of S there is defined an element $s_1 \circ s_2$ of S.

A group G is a non-empty set with a law of composition $\circ : G \times G \to G$ with the following properties:

(i) $g_1 \circ (g_2 \circ g_3) = (g_1 \circ g_2) \circ g_3$ for all g_1, g_2, g_3 in G – that is, composition is associative;
(ii) there is an element e in G (the *unit* or *neutral* element) such that $e \circ g = g \circ e = g$ for each g in G;
(iii) to each g in G there corresponds an element g^{-1} (the *inverse* of g) such that $g \circ g^{-1} = g^{-1} \circ g = e$.

Exercise

1.1 Suppose that G is a group. Show that the identity element e is unique, and that for each $g \in G$ the inverse element g^{-1} is also unique.

Two elements g and h of a group *commute* if $g \circ h = h \circ g$. The *commutator* $[g,h]$ of g and h is the element $g^{-1} \circ h^{-1} \circ g \circ h$; thus g and h commute if and only if $[g,h] = e$. A subset A of a group G is said to be *commutative*, or *abelian*, if and only if any two elements of A commute.

The notation that is used for the law of composition varies from situation to situation. Frequently, there is no symbol, and elements are simply placed side by side: $g \circ h = gh$. When G is abelian, it often happens that the law is denoted by $g \circ h = g + h$, the identity element is denoted by 0 and the inverse of an element g is denoted by $-g$.

Let us give some examples of groups. The integers $\mathbb{Z}$ (positive, zero and negative) form an abelian group under addition, with identity element 0, but the non-zero elements do not form a group under multiplication (2 has no multiplicative inverse in $\mathbb{Z}$). The non-zero complex numbers $\mathbb{C}^*$ form an abelian group under multiplication, with identity element 1.

If S is a non-empty set, a mapping σ from S to S is called a *permutation* of S if it is a bijection: that is, if $\sigma(x) = \sigma(y)$ then $x = y$, and if $z \in S$ there exists w in S for which $\sigma(w) = z$. The set Σ_S of all permutations of S is a group under the natural composition of mappings. It is not abelian if S has more than two elements. If $S = (1, \dots, n)$, we write Σ_n for Σ_S. We shall consider S_n in more detail in Sections 1.3 and 1.4.

A subset H of a group G is a *subgroup* of G if it is a group under the law of composition defined on G; that is, if h_1 and h_2 are elements of H then so are $h_1 \circ h_2$ and h_1^{-1}. If G is a group, $\{e\}$ and G are subgroups; these are the *trivial* subgroups of G. If $n \in \mathbb{Z}$ the set $n\mathbb{Z} = \{nm : m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$. The set $\mathbb{T} = \{z : |z| = 1\}$ is a subgroup of the multiplicative group $\mathbb{C}^*$, and if $n > 0$ the set $R_n = \{e^{2\pi ik/n} : 0 \leq k < n\}$ of nth roots of unity is a subgroup of $\mathbb{T}$.

A group is *cyclic* if there is an element $g \in G$ such that every element of G is the composition of finitely many copies of g or or finitely many copies of g^{-1}.

A group is a *finite group* if it has finitely many elements. The *order* of a finite group is the number of its elements, and its *exponent* $e(G)$ is the smallest positive integer n such that $g^n = e$ for all $g \in G$.

Exercises

1.2 Show that if H is a subgroup of $\mathbb{Z}$, then H is cyclic.

1.3 Show that a subgroup F of a cyclic group is cyclic.

If $\{G_\alpha\}_{\alpha \in A}$ is a family of groups, then the product $\prod_{\alpha \in A} G_\alpha$ is a group, when composition is defined by $(g \circ h)_\alpha = g_\alpha \circ h_\alpha$ for $\alpha \in A$.

The intersection of subgroups of a group G is a subgroup, and so if S is a subset of a group G, there is a smallest group containing S, the subgroup generated by S; this is denoted by $\langle S\rangle$. It consists of all finite products of elements of S and their inverses, and is called the subgroup *generated by* S. For example, if G is a group, the *derived group* $\delta(G)$ is the subgroup generated by the set of all commutators $[g,h]$ in G. In the case where S is a singleton $\{a\}$, we write $\langle a\rangle$ for $\langle S\rangle$; $\langle a\rangle$ is then an abelian group, the *cyclic* subgroup generated by a, and consists of $\{a^n : n > 0\}$, e and $\{a^{-n} : n > 0\}$, where a^n is $a \circ a \circ \cdots \circ a$ (n terms) and a^{-n} is $a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}$ (n terms).

Suppose that A is a subset of a group G. The *centralizer* $Z(A)$ is the set $\{g \in G : [g,h] = e, \text{for all } h \in A\}$ of all elements of G which commute with every element of A.

Exercise

1.4 Suppose that A, A_1 and A_2 are subsets of a group G, and that $A_1 \subseteq A_2$. Show that

(i) $Z(A)$ is a subgroup of G
(ii) $Z(A_2) \subseteq Z(A_1)$
(iii) $A \subseteq Z(Z(A))$
(iv) $Z(A) = Z(Z(Z(A)))$
(v) $A \subset Z(A)$ if and only if A is abelian.

The group $Z(G)$ is called the *centre* of G; it is an abelian subgroup of G.

If G is a *finite group* (a group with finitely many elements) then the *order* of G is the number $|G|$ of elements of G. (If G is infinite, its order is ∞.) If $a \in G$ then the *order* of a is the order of $\langle a\rangle$. If a has finite order, the order of a is the least positive integer n such that $a^n = e$.

A mapping ϕ from a group G to a group H is a *homomorphism* if $\phi(g_1 \circ g_2) = \phi(g_1) \circ \phi(g_2)$ for all g_1 and g_2 in G. A homomorphism which is injective is called a *monomorphism*, one which is surjective is called an *epimorphism* and one which is both is called an *isomorphism*. If there is an isomorphism of a group G onto a group H, we say that G and H are *isomorphic* and write $G \cong H$. An isomorphism from a group onto itself is called an *automorphism*. For example, if $k \in G$, we set $g^k = k^{-1} \circ g \circ k$, for each $g \in G$. Then the mapping $g \to g^k$ is an automorphism of G (*conjugation by* k), an *inner* automorphism of G.

If A is a subset of a group G, and $k \in G$, we set $A^k = \{a^k : a \in A\}$. Two subsets A and B of a group G are *conjugate* if there exists $h \in G$ such that $B = A^h$; conjugacy is an equivalence relation on the subsets of G; we denote

the equivalence class to which A belongs by $conj(A)$. If $\{g\}$ is a singleton, we write $conj(g)$; $conj(g)$ is called a *conjugacy class*. A set A is *self-conjugate* if $conj(A) = \{A\}$. Thus a group is abelian if and only if every singleton is self-conjugate.

A subgroup H of a group G is a *normal* subgroup if it is self-conjugate; if so, we write $H \lhd G$. Thus a subgroup H of G is normal if and only if it is the union of conjugacy classes. Every subgroup of an abelian group is normal. If g, h, k are elements of a group G then $[g,h]^k = [g^k, h^k]$, so that $\delta(G) \lhd G$.

Suppose that A is a non-empty subset of a group G. The *normalizer* $N(A) = N_G(A)$ is the set $N(A) = \{g \in G : a^g \in A \text{ for all } a \in A\}$. $N(A)$ is a subgroup of G; $Z(A) \subseteq N(A)$. We write $N(a)$ for $N(\{a\})$ and $Z(a)$ for $Z(\{a\})$; then $Z(a) = N(a)$ and $Z(A) = \cap_{a \in A} Z(a)$.

If H is a subgroup of G then $H \subseteq N(H)$ and $H \lhd N(H)$; if K is a subgroup of G containing H then $H \lhd K$ if and only if $K \subseteq N(H)$; thus $H \lhd G$ if and only if $N(H) = G$.

If ϕ is a homomorphism from a group G to a group H, its *image* $\phi(G)$ is a subgroup of H, and its *kernel* $\phi^{-1}(e)$ is a subgroup of G.

Exercise

1.5 Show that if ϕ is a homomorphism of a group G into a group H then its kernel is a normal subgroup of G.

If G is a group and $g \in G$, let $r_g(h) = h \circ g$ and $l_g(h) = g^{-1} \circ h$, for each $h \in G$. Then l_g and r_g are permutations of G, and the mappings $g \to r_g$ and $g \to l_g$ are monomorphisms of G into the permutation group Σ_G. If H is a subgroup of G then a set $r_g(H) = H \circ g$ is called a *right coset* and a set $l_g(H) = g^{-1} \circ H$ is called a *left coset*. (Terminology here varies, but this seems preferable.)

Proposition 1.1 *Let H be a subgroup of a group G. If g_1 and g_2 are elements of G then either $g_1^{-1} \circ g_2 \in H$, in which case $r_{g_1}(H) = r_{g_2}(H)$, or $g_1^{-1} \circ g_2 \notin H$, in which case $r_{g_1}(H)$ and $r_{g_2}(H)$ are disjoint. Thus the distinct right cosets form a partition of G. Similarly for left cosets.*

Proof Simple verification. □

The set of right cosets H in G is denoted by G/H. The number $|G/H|$ of right cosets H in G is called the *index* of H in G.

Exercise

1.6 Suppose that A is a non-empty subset of a group G and that $g \in G$. Let $\psi_A(g) = A^g$. Show that ψ_A maps G onto $conj(A)$, and $\psi_A(g') = \psi_A(g)$

if and only if $g' \in N(A)g$. Thus if G is a finite group then $|conj(A)| = |G/N(A)|$, so that $|conj(A)|.|N(A)| = |G|$.

Proposition 1.2 (Lagrange's theorem) *If H is a subgroup of a finite group G then $|G| = |G/H|.|H|$.*

Proof For if $H \circ g \in G/H$, $H \circ g = r_g(H)$, so $|H_g| = |H|$; the cosets of H have the same number of elements as H. □

Corollary 1.3 *(i) If a is an element of a finite group G and a has order k, then k divides $|G|$.*

(ii) If G is a cyclic group of order n, and $a \in G$, then $a^n = e$.

The left and right cosets need not be the same.

Proposition 1.4 *Suppose that H is a subgroup of a group G. Then H is normal in G if and only if the left cosets and right cosets of H are the same.*

Proof Suppose that H is a normal subgroup of G. If $g \in G$ and $h \in H$, let $h' = h^g$ and $h'' = h^{g^{-1}}$. Then $h \circ g = g \circ h'$ and $g \circ h = h'' \circ g$, from which it follows that $g \circ H = H \circ g$.

Conversely, suppose that the left cosets and right cosets of H are the same. If $g \in G$ then $C = H \circ g$ is a right coset, and is therefore a left coset. Since $g \in C$, $C = g \circ H$, so that $g \circ H = H \circ g$, and $h^g \in H$ for each $h \in H$. Since this holds for each $g \in G$, H is normal in G. □

Exercise

1.7 Show that if G is a finite group and H is a subgroup of G with index 2 in G, then H is a normal subgroup of G.

Theorem 1.5 *Suppose that $H \triangleleft G$ and that $C_1 = H \circ g_1$ and $C_2 = H \circ g_2$ are two cosets of H in G. Then $C_1 \circ C_2$ is again a coset of H in G, and under this law of composition, G/H is a group (the quotient group) with H as neutral element, and the quotient mapping $q : G \to G/H$ (which sends g to $H \circ g$) is an epimorphism of G onto G/H, with kernel H.*

Proof

$$\begin{aligned} C_1 \circ C_2 &= \{h \circ g_1 \circ k \circ g_2 : h,k \in H\} \\ &= \{h \circ k^{g_1^{-1}} \circ (g_1 \circ g_2) : h,k \in H\} \\ &= \{h \circ (g_1 \circ g_2) : h \in H\} = H \circ (g_1 \circ g_2), \end{aligned}$$

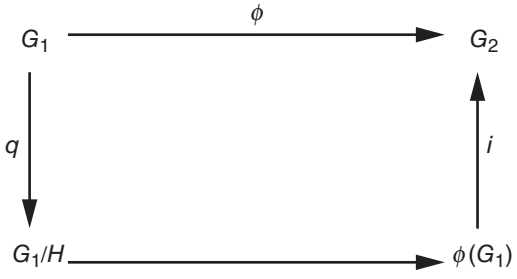
from which the result follows easily. □

Exercise

1.8 Show that if G is a group, then $G/\delta(G)$ is abelian, and if $H \lhd G$ then G/H is abelian if and only if $\delta(G) \subseteq H$.

Theorem 1.6 (The first isomorphism theorem) *Suppose that ϕ is a homomorphism from a group G_1 into a group G_2, with kernel H. Then $H \lhd G_1$, and there is an isomorphism $\tilde{\phi}$ from G/H onto $\phi(G_1)$ such that $\phi = i.\tilde{\phi}.q$, where $q : G \to G/H$ is the quotient mapping and $i : \phi(G_1) \to G_2$ is the inclusion mapping (which is of course a monomorphism).*

Proof If $C = H \circ g \in G_1/H$, let $\tilde{\phi}(C) = \phi(g)$. This does not depend on the choice of g in C, $\tilde{\phi}$ is a homomorphism of G/H onto $\phi(G_1)$, and $\tilde{\phi}(C) = e$ if and only if $C = H$. Then $\phi = q.\tilde{\phi}.i$ is an isomorphism of G_1/H onto $\phi(G_1)$:



□

As an example, if $n > 0$ let $\phi(k) = e^{2\pi ik/n}$. Then ϕ is a homomorphism of $(\mathbb{N}, +)$ into $(\mathbb{T}, \times)$, with kernel $n\mathbb{Z}$ and image $\mathbb{T}_n$, the set of nth roots of unity. We write $(\mathbb{Z}_n, +)$ for the group $(\mathbb{Z}/n\mathbb{Z}, +)$. Thus $(\mathbb{Z}_n, +)$ is isomorphic to $(\mathbb{T}_n, \times)$: $\mathbb{Z}_n$ is the set of equivalence classes of $\mathbb{Z} \pmod n$.

Here is an application of the first isomorphism theorem.

Theorem 1.7 *Suppose that G is a group, that $H \lhd G$ and that A is a subgroup of G.*

(i) $H \cap A \lhd A$, and $A/(H \cap A) \cong \langle H, A\rangle/H$.
(ii) If $H \subseteq A$ and $A \lhd G$, then $H \lhd A$, $A/H \lhd G/H$ and $(G/H)/(A/H) \cong G/A$.

Proof (i) If $h \in H \cap A$ and $a \in A$ then $h^a \in H \cap A$, so that $H \cap A \lhd A$. If $j : A \to G$ is the inclusion mapping and $q : G \to G/H$ is the quotient mapping then $q \circ j$ is a homomorphism from A into G/H with kernel $H \cap A$ and image $\langle H, A\rangle/H$, so that the result follows from the first isomorphism theorem.

(ii) Certainly $H \lhd A$, by (i). If C is a right coset of H in G, let $A \circ C = \{a \circ c : a \in A, c \in C\}$; $A \circ C$ is a right coset of A in G. Let $\theta(C) = A \circ C$.

Then $\theta : G/H \to G/A$ is an epimorphism with kernel A/H, so that the result also follows from the first isomorphism theorem. □

Exercises

1.9 Suppose that G has exactly one subgroup H of order k. Show that H is a normal subgroup of G.

1.10 Suppose that H is a normal subgroup of G and that K is a normal subgroup of H. Is K necessarily a normal subgroup of G?

1.11 Show that a group G is generated by each of its elements (other than the unit element) if and only if G is a finite cyclic group of prime order.

1.12 Describe the elements of $\mathbb{Z}_n$ which generate $\mathbb{Z}_n$ (for any positive integer n).

1.13 Give an example of a non-abelian group of order 8 all of whose subgroups are normal.

From now on, if g and h are elements of a group G, we shall write gh for $g \circ h$ (unless G is an abelian group, written additively).

1.2 Finite Abelian Groups

A finite cyclic group such as $\mathbb{Z}_n$ or $\mathbb{T}_n$ is a very simple example of a finite abelian group. Any finite abelian group is isomorphic to a finite product of cyclic groups.

Theorem 1.8 *Suppose that $(G,+)$ is a finite abelian group. G is isomorphic to a product of cyclic groups:*

$$G \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}.$$

Further, the isomorphism can be chosen so that $d_j | d_k$ for $1 \leqslant j < k \leqslant s$. The number s is characterized by the property that G is generated by s elements, but it is not generated by $s-1$ elements.

Proof We prove this by induction on $|G|$. Suppose that the result is true for all abelian groups of order less than n, and that $|G| = n$.

There exists an integer s such that G is generated by s elements, but is not generated by fewer than s elements. Let m be the least positive number such that there exists a set $\{g_1, \ldots, g_s\}$ of generators and a relation

$$mg_1 + a_2 g_2 + \cdots + a_s g_s = 0$$

(with $a_2, \dots, a_s$ in $\mathbb{Z}$). Note that $m > 1$, since otherwise G would be generated by $\{g_2, \dots, g_s\}$. We can write $a_i = mq_i + r_i$ with $0 \leqslant r_i < m$, for $2 \leqslant i \leqslant s$. Then if $h_1 = g_1 + q_2 g_2 + \cdots + q_s g_s$, G is generated by $\{h_1, g_2, \dots, g_s\}$ and

$$mh_1 + r_2 g_2 + \cdots + r_s g_s = 0.$$

The minimality of m implies that $r_2 = r_3 = \cdots = r_s = 0$, and so $mh_1 = 0$. We now claim that G is isomorphic to $\langle h_1 \rangle \times \langle g_2, \dots, g_s \rangle$. If $(a, b) \in \langle h_1 \rangle \times \langle g_2, \dots, g_s \rangle$, let $\theta(a, b) = a + b$. The map θ is a homomorphism of $\langle h_1 \rangle \times \langle g_2, \dots, g_s \rangle$ into G. It is an epimorphism, since $\{h_1, g_2, \dots, g_s\}$ generates G. If (a, b) is in the kernel of θ, $a+b = 0$. Writing $a = j_1 h_1, b = j_2 g_2 + \cdots + j_r g_s$, with $0 \leqslant j_1 < m$, we have

$$j_1 h_1 + j_2 g_2 + \cdots + j_s g_s = 0.$$

It follows from the minimality of m that $j_1 = 0$, and so $a = b = 0$. Thus θ is an isomorphism.

We now apply the inductive hypothesis to $\langle g_2, \dots, g_s \rangle$, which is clearly generated by $s - 1$ elements, but not by $s - 2$ elements: the subgroup $\langle g_2, \dots, g_s \rangle$ is isomorphic to

$$\mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s},$$

with $d_j | d_k$ for $2 \leqslant j < k \leqslant s$. Consequently $G \cong \mathbb{Z}_m \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s}$. Let $h_1, \dots, h_s$ be the corresponding generators in G. It follows from the minimality of m that $m \leqslant d_2$. Let $d_2 = e_2 m + f_2$, where $0 \leqslant f_2 < m$, and let $h_1' = h_1 + e_2 h_2$. Then G is generated by $\{h_1', h_2, \dots, h_s\}$. As

$$mh_1' + f_2 h_2 = 0$$

it follows that $f_2 = 0$, and so $m | d_2$. This completes the proof. □

Corollary 1.9 *If G is a finite abelian group, there exists $g \in G$ whose order is its exponent $e(G)$.*

We can extend this theorem. We begin with a lemma.

Lemma 1.10 *If G is a cyclic group of order jk, where j and k are coprime (that is, if n divides both j and k, then $n = 1$) then G is isomorphic to a product $J \times K$, where J is a cyclic group of order j and K is a cyclic group of order k.*

Proof Let a be a generator of G, and let J and K be cyclic groups of orders j and k, with generators b and c, respectively. If $h = (rb, sc) \in J \times K$, let $\phi(h) = (kr + js)a$. Then $\phi : J \times K \to G$ is a homomorphism. Since j and k

are coprime, there exist r and s such that $kr + js = 1$. It therefore follows that $a \in \phi(J \times K)$, and so ϕ is surjective. But $J \times K$ has the same order as G, and so ϕ is an isomorphism. □

Theorem 1.11 *If $(G, +)$ is a finite abelian group, then G is isomorphic to a product of cyclic groups of prime power order.*

Proof It follows by induction that a cyclic abelian group is the product of cyclic groups of prime power order, and the result then follows from Theorem 1.8. □

Exercises

1.14 Suppose that G is a finite abelian group for which every element other than the identity has order k. Show that k is a prime number, and that G is isomorphic to the product of cyclic groups, each of order k.

1.15 Suppose that a and b are positive integers with highest common factor d. Show that

$$\mathbb{Z}_a \times \mathbb{Z}_b \cong \mathbb{Z}_d \times \mathbb{Z}_{ab/d}.$$

1.16 Suppose that G is an abelian group. Show that the set T of elements of finite order is a subgroup of G and that every element of G/T, except the identity, is of infinite order.

1.17 Suppose that G is a finitely generated abelian group every element of which, except the identity, has infinite order. Show that $G \cong \mathbb{Z}^s$, where s is defined by the property that G is generated by s elements, but is not generated by $s - 1$ elements.

1.18 Suppose that G is a finitely generated abelian group. Show that $G \cong \mathbb{Z}^s \times T$, where T is a finite group.

1.3 Finite Permutation Groups

We now describe the terminology that we use concerning permutation groups, and establish some basic facts about them.

Suppose that G is a subgroup of Σ_S. Set $x \sim_G y$ if there is $\sigma \in G$ such that $y = \sigma(x)$. This is an equivalence relation on S. The equivalence classes are called the *orbits* O_G of G; we denote the orbit to which x belongs by $O_G(x)$. Let $stab_G(x) = \{g \in G : g(x) = x\}$; $stab_G(x)$ is the *stabilizer* of x in G.