1
Groups and homomorphisms

This book is devoted to the study of an aspect of group theory, so we begin with a résumé of facts about groups, most of which you should know already. In addition, we introduce several examples, such as dihedral groups and symmetric groups, which we shall use extensively to illustrate the later theory. An elementary course on abstract algebra would normally cover all the material in the chapter, and any book on basic group theory will supply you with further details. One or two results which we shall use only infrequently are demoted to the exercises at the end of the chapter – you can refer to the solutions if necessary.

Groups

A *group* consists of a set G, together with a rule for combining any two elements g, h of G to form another element of G, written gh; this rule must satisfy the following axioms:

(1) for all g, h, k in G,

$$(gh)k = g(hk);$$

(2) there exists an element e in G such that for all g in G,

$$eg = ge = g;$$

(3) for all g in G, there exists an element g^{-1} in G such that

$$gg^{-1} = g^{-1}g = e.$$

We refer to the rule for combining elements of G as the *product operation* on G.

Axiom (1) states that the product operation is *associative*; the element e in axiom (2) is an *identity* element of G; and g^{-1} is an *inverse* of g in axiom (3).

It is elementary to see that G has just one identity element, and that every g in G has just one inverse. Usually we write 1, rather than e, for the identity element of G.

The product of an element g with itself, gg, is written g^2; similarly $g^3 = g^2 g$, $g^{-2} = (g^{-1})^2$, and so on. Also, $g^0 = 1$.

If the number of elements in G is finite, then we call G a *finite group*; the number of elements in G is called the *order* of G, and is written $|G|$.

1.1 Examples

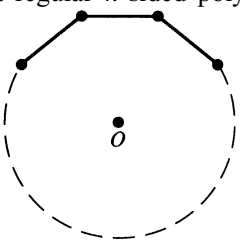
(1) Let n be a positive integer, and denote by $\mathbb{C}$ the set of all complex numbers. The set of nth roots of unity in $\mathbb{C}$, with the usual multiplication of complex numbers, is a group of order n. It is written as C_n and is called the *cyclic* group of order n. If $a = e^{2\pi i/n}$, then

$$C_n = \{1, a, a^2, \ldots, a^{n-1}\},$$

and $a^n = 1$.

(2) The set $\mathbb{Z}$ of all integers, under addition, is a group.

(3) Let n be an integer with $n \geqslant 3$, and consider the rotation and reflection symmetries of a regular n-sided polygon.



There are n rotation symmetries: these are $\rho_0, \rho_1, \ldots, \rho_{n-1}$ where ρ_k is the (clockwise) rotation about the centre O through an angle $2\pi k/n$. There are also n reflection symmetries: these are reflections in the n lines passing through O and a corner or the mid-point of a side of the polygon.

These $2n$ rotations and reflections form a group under the product operation of *composition* (that is, for two symmetries f and g, the product fg means 'first do f, then do g'). This group is called the *dihedral group* of order $2n$, and is written D_{2n}.

Let A be a corner of the polygon. Write b for the reflection in the

line through O and A, and write a for the rotation ρ_1. Then the n rotations are

$$1, a, a^2, \ldots, a^{n-1}$$

(where 1 denotes the identity, which leaves the polygon fixed); and the n reflections are

$$b, ab, a^2b, \ldots, a^{n-1}b.$$

Thus all elements of D_{2n} are products of powers of a and b – that is, D_{2n} is *generated* by a and b.

Check that

$$a^n = 1,\ b^2 = 1 \text{ and } b^{-1}ab = a^{-1}.$$

These relations determine the product of any two elements of the group. For example, we have $ba^j = a^{-j}b$ (using the relation $ba = a^{-1}b$), and hence

$$(a^ib)(a^jb) = a^iba^jb = a^ia^{-j}bb = a^{i-j}.$$

We summarize all this in the presentation

$$D_{2n} = \langle a, b \colon a^n = 1,\ b^2 = 1,\ b^{-1}ab = a^{-1} \rangle.$$

(4) For n a positive integer, the set of all permutations of $\{1, 2, \ldots, n\}$, under the product operation of composition, is a group. It is called the *symmetric group* of degree n, and is written S_n. The order of S_n is $n!$.

(5) Let F be either $\mathbb{R}$ (the set of real numbers) or $\mathbb{C}$ (the set of complex numbers). The set of all invertible $n \times n$ matrices with entries in F, under matrix multiplication, forms a group. This group is called the *general linear group* of degree n over F, and is denoted by $\mathrm{GL}(n, F)$. It is an infinite group. The identity of $\mathrm{GL}(n, F)$ is of course the identity matrix, which we denote by I_n or just I.

A group G is said to be *abelian* if $gh = hg$ for all g and h in G. While C_n and $\mathbb{Z}$ are abelian, most of the other examples given above are non-abelian groups.

Subgroups

Let G be a group. A subset H of G is said to be a *subgroup* if H is itself a group under the product operation inherited from G. We use the notation $H \leqslant G$ to indicate that H is a subgroup of G.

It is easy to see that a subset H of a group G is a subgroup if and only if the following two conditions hold:

(1) $1 \in H$, and
(2) if $h, k \in H$ then $hk^{-1} \in H$.

1.2 Examples

(1) For every group G, both $\{1\}$ and G are subgroups of G.

(2) Let G be a group and $g \in G$. The subset

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

is a subgroup of G, called the *cyclic subgroup generated by* g. If $g^n = 1$ for some $n \geqslant 1$, then $\langle g \rangle$ is finite. In this case, let r be the least positive integer such that $g^r = 1$; then r is equal to the number of elements in $\langle g \rangle$ – indeed,

$$\langle g \rangle = \{1, g, g^2, \ldots, g^{r-1}\}.$$

We call r the *order* of the element g.

If $G = \langle g \rangle$ for some $g \in G$ then we call G a *cyclic* group. The groups C_n and $\mathbb{Z}$ in Examples 1.1 are cyclic.

(3) Let G be a group and let $a, b \in G$. Define H to be the subset of G consisting of all elements which are products of powers of a and b – that is, all elements of the form

$$a^{i_1} b^{j_1} a^{i_2} b^{j_2} \ldots a^{i_n} b^{j_n}$$

for some n, where $i_k, j_k \in \mathbb{Z}$ for $1 \leqslant k \leqslant n$. Then H is a subgroup of G; we call H the subgroup *generated* by a and b, and write

$$H = \langle a, b \rangle.$$

Given any finite set S of elements of G, we can similarly define $\langle S \rangle$, the subgroup of G generated by S.

This construction gives a powerful method of finding new groups as subgroups of given groups, such as general linear or symmetric groups. We illustrate the construction in the next example, and again in Example 1.5 below.

(4) Let $G = \mathrm{GL}(2, \mathbb{C})$, the group of invertible 2×2 matrices with entries in $\mathbb{C}$, and let

$$A = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Put $H = \langle A, B \rangle$, the subgroup of G generated by A and B. Check that

$$A^4 = I,\ A^2 = B^2,\ B^{-1}AB = A^{-1}.$$

Using the third relation, we see that every element of H has the form A^iB^j for some integers i, j; and using the first two relations, we can take $0 \leqslant i \leqslant 3$ and $0 \leqslant j \leqslant 1$. Hence H has at most eight elements. Since the matrices

$$A^iB^j \quad (0 \leqslant i \leqslant 3,\ 0 \leqslant j \leqslant 1)$$

are all distinct, in fact $|H| = 8$.

The group H is called the *quaternion group* of order 8, and is written Q_8. The above three relations determine the product of any two elements of Q_8, so we have the presentation

$$Q_8 = \langle A, B\colon A^4 = I, A^2 = B^2, B^{-1}AB = A^{-1} \rangle.$$

(5) A *transposition* in the symmetric group S_n is a permutation which interchanges two of the numbers $1, 2, \ldots, n$ and fixes the other $n - 2$ numbers. Every permutation g in S_n can be expressed as a product of transpositions. It can be shown that either all such expressions for g have an even number of transpositions, or they all have an odd number of transpositions; we call g an *even* or an *odd* permutation, accordingly. The subset

$$A_n = \{g \in S_n\colon\ g \text{ is an even permutation}\}$$

is a subgroup of S_n, called the *alternating group* of degree n.

Direct products

We describe a construction which produces a new group from given ones.

Let G and H be groups, and consider

$$G \times H = \{(g, h)\colon g \in G \text{ and } h \in H\}.$$

Define a product operation on $G \times H$ by

$$(g, h)(g', h') = (gg', hh')$$

for all $g, g' \in G$ and all $h, h' \in H$. With this product operation, $G \times H$ is a group, called the *direct product* of G and H.

More generally, if $G_1, \ldots, G_r$ are groups, then the direct product $G_1 \times \ldots \times G_r$ is

$$\{(g_1, \ldots, g_r) : g_i \in G_i \text{ for } 1 \leqslant i \leqslant r\},$$

with product operation defined by

$$(g_1, \ldots, g_r)(g_1', \ldots, g_r') = (g_1 g_1', \ldots, g_r g_r').$$

If all the groups G_i are finite, then $G_1 \times \ldots \times G_r$ is also finite, of order $|G_1| \ldots |G_r|$.

1.3 Example
The group $C_2 \times \ldots \times C_2$ (r factors) has order 2^r and all its non-identity elements have order 2.

Functions

A *function* from one set G to another set H is a rule which assigns a unique element of H to each element of G. In this book, we generally apply functions on the *right* – that is, the image of g under a function ϑ is written as $g\vartheta$, not as ϑg. We often indicate that ϑ is a function from G to H by the notation $\vartheta : G \to H$. By an expression $\vartheta : g \to h$, where $g \in G$ and $h \in H$, we mean that $h = g\vartheta$.

A function $\vartheta : G \to H$ is *invertible* if there is a function $\phi : H \to G$ such that for all $g \in G$, $h \in H$,

$$(g\vartheta)\phi = g \text{ and } (h\phi)\vartheta = h.$$

Then ϕ is called the *inverse* of ϑ, and is written as ϑ^{-1}. A function ϑ from G to H is invertible if and only if it is both *injective* (that is, $g_1\vartheta = g_2\vartheta$ for $g_1, g_2 \in G$ implies that $g_1 = g_2$) and *surjective* (that is, for every $h \in H$ there exists $g \in G$ such that $g\vartheta = h$). An invertible function is also called a *bijection*.

Homomorphisms

Given groups G and H, those functions from G to H which 'preserve the group structure' – the so-called homomorphisms – are of particular importance.

If G and H are groups, then a *homomorphism* from G to H is a function $\vartheta : G \to H$ which satisfies

$$(g_1 g_2)\vartheta = (g_1\vartheta)(g_2\vartheta) \quad \text{for all } g_1, g_2 \in G.$$

An invertible homomorphism is called an *isomorphism*. If there is an isomorphism ϑ from G to H, then G and H are said to be *isomorphic*, and we write $G \cong H$; also, ϑ^{-1} is an isomorphism from H to G, so $H \cong G$.

The following example displays a technique which can often be used to prove that certain functions are homomorphisms.

1.4 Example
Let $G = D_{2n} = \langle a, b : a^n = b^2 = 1, \ b^{-1}ab = a^{-1} \rangle$, and write the $2n$ elements of G in the form $a^i b^j$ with $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant 1$. Let H be any group, and suppose that H contains elements x and y which satisfy

$$x^n = y^2 = 1, \ y^{-1}xy = x^{-1}.$$

We shall prove that the function $\vartheta : G \to H$ defined by

$$\vartheta : a^i b^j \to x^i y^j \quad (0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant 1)$$

is a homomorphism.

Suppose that $0 \leqslant r \leqslant n-1$, $0 \leqslant s \leqslant 1$, $0 \leqslant t \leqslant n-1$, $0 \leqslant u \leqslant 1$. Then

$$a^r b^s a^t b^u = a^i b^j$$

for some i, j with $0 \leqslant i \leqslant n-1$, $0 \leqslant j \leqslant 1$. Moreover, i and j are determined by repeatedly using the relations

$$a^n = b^2 = 1, \ b^{-1}ab = a^{-1}.$$

Since we have $x^n = y^2 = 1$, $y^{-1}xy = x^{-1}$, we can also deduce that

$$x^r y^s x^t y^u = x^i y^j.$$

Therefore,

$$\begin{aligned}(a^r b^s a^t b^u)\vartheta &= (a^i b^j)\vartheta = x^i y^j = x^r y^s x^t y^u \\ &= (a^r b^s)\vartheta \cdot (a^t b^u)\vartheta,\end{aligned}$$

and so ϑ is a homomorphism.

We now demonstrate the technique of Example 1.4 in action.

1.5 Example
Let $G = S_5$ and let x, y be the following permutations in G:

$$x = (1\ 2\ 3\ 4\ 5), \ y = (2\ 5)(3\ 4).$$

(Here we adopt the usual cycle notation – thus, (1 2 3 4 5) denotes the permutation $1 \to 2 \to 3 \to 4 \to 5 \to 1$, and so on.) Check that

$$x^5 = y^2 = 1,\ y^{-1}xy = x^{-1}.$$

Let H be the subgroup $\langle x, y\rangle$ of G. Using the above relations, we see that

$$H = \{x^i y^j \colon 0 \leqslant i \leqslant 4,\ 0 \leqslant j \leqslant 1\},$$

a group of order 10.

Now recall that

$$D_{10} = \langle a, b \colon a^5 = b^2 = 1,\ b^{-1}ab = a^{-1}\rangle.$$

By Example 1.4, the function $\vartheta \colon D_{10} \to H$ defined by

$$\vartheta \colon a^i b^j \to x^i y^j \quad (0 \leqslant i \leqslant 4,\ 0 \leqslant j \leqslant 1)$$

is a homomorphism. Since ϑ is invertible, it is an isomorphism. Thus, $H = \langle x, y\rangle \cong D_{10}$.

Cosets

Let G be a group and let H be a subgroup of G. For x in G, the subset

$$Hx = \{hx \colon h \in H\}$$

of G is called a *right coset* of H in G. The distinct right cosets of H in G form a partition of G (that is, every element of G is in precisely one of the cosets).

Suppose now that G is finite, and let $Hx_1, \ldots, Hx_r$ be all the distinct right cosets of H in G. For all i, the function

$$h \to hx_i \quad (h \in H)$$

is a bijection from H to Hx_i, and so $|Hx_i| = |H|$. Since

$$G = Hx_1 \cup \ldots \cup Hx_r, \text{ and}$$
$$Hx_i \cap Hx_j \text{ is empty if } i \neq j,$$

we deduce that

$$|G| = r|H|.$$

In particular, we have

1.6 Lagrange's Theorem
If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$.

The number r of distinct right cosets of H in G is called the *index* of H in G, and is written as $|G: H|$. Thus

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

when G is finite.

Normal subgroups

A subgroup N of a group G is said to be a *normal* subgroup of G if $g^{-1}Ng = N$ for all $g \in G$ (where $g^{-1}Ng = \{g^{-1}ng: n \in N\}$); we write $N \lhd G$ to indicate that N is a normal subgroup of G.

Suppose that $N \lhd G$ and let G/N be the set of right cosets of N in G. The importance of the condition $g^{-1}Ng = N$ (for all $g \in G$) is that it can be used to show that for all $g, h \in G$, we have

$$\{xy: x \in Ng \text{ and } y \in Nh\} = Ngh.$$

Hence we can define a product operation on G/N by

$$(Ng)(Nh) = Ngh \quad \text{for all } g, h \in G.$$

This makes G/N into a group, called the *factor group* of G by N.

1.7 Examples
(1) For every group G, the sub-groups $\{1\}$ and G are normal sub-groups of G.

(2) For $n \geqslant 1$, we have $A_n \lhd S_n$. If $n \geqslant 2$ then there are just two right cosets of A_n in S_n, namely

$$A_n = \{g \in S_n: g \text{ even}\}, \text{ and}$$
$$A_n(1\ 2) = \{g \in S_n: g \text{ odd}\}.$$

Thus $|S_n:A_n| = 2$, and so $S_n/A_n \cong C_2$.

(3) Let $G = D_8 = \langle a, b: a^4 = b^2 = 1, \quad b^{-1}ab = a^{-1}\rangle$ and let $N = \langle a^2\rangle = \{1, a^2\}$. Then $N \lhd G$ and

$$G/N = \{N, Na, Nb, Nab\}.$$

Since $(Na)^2 = (Nb)^2 = (Nab)^2 = N$, we see that $G/N \cong C_2 \times C_2$.

The subgroup $\langle a\rangle$ is also normal in G, but the subgroup $H = \langle b\rangle$ is not normal in G, since $b \in H$ while $a^{-1}ba = a^2b \notin H$.

Simple groups

A group G is said to be *simple* if $G \neq \{1\}$ and the only normal subgroups of G are $\{1\}$ and G. For example, the cyclic group C_p, with p a prime number, is simple. We shall give examples of non-abelian simple groups in later chapters – the smallest one is A_5.

If G is a finite group which is not simple, then G has a normal subgroup N such that both N and G/N have smaller order than G; and in a sense, G is 'built' out of these two smaller groups. Continuing this process with the smaller groups, we eventually see that G is 'built' out of a collection of simple groups. (This is analogous to the fact that every positive integer is built out of its prime factors.) Thus, simple groups are fundamental to the study of finite groups.

Kernels and images

To conclude the chapter, we relate normal subgroups and factor groups to homomorphisms. Let G and H be groups and suppose that $\vartheta\colon G \to H$ is a homomorphism. We define the *kernel* of ϑ by

$$\operatorname{Ker}\vartheta = \{g \in G\colon g\vartheta = 1\}. \tag{1.8}$$

Then $\operatorname{Ker}\vartheta$ is a normal subgroup of G. Also, the *image* of ϑ is

$$\operatorname{Im}\vartheta = \{g\vartheta\colon g \in G\}, \tag{1.9}$$

and $\operatorname{Im}\vartheta$ is a subgroup of H.

The following result describes the way in which the kernel and image of ϑ are related.

1.10 Theorem
Suppose that G and H are groups and let $\vartheta\colon G \to H$ be a homomorphism. Then

$$G/\operatorname{Ker}\vartheta \cong \operatorname{Im}\vartheta.$$

An isomorphism is given by the function

$$Kg \to g\vartheta \quad (g \in G)$$

where $K = \operatorname{Ker}\vartheta$.