Order 3 By similar arguments, there are four (why not eight?) subgroups of order 3, such as {id, (123), (132)}.

Order 4 A subgroup of order 4 is isomorphic to C_4 or $C_2 \times C_2$ (Ex. 20.6.4). Since there are no elements of order 4, C_4 is impossible. The three elements of order 2, namely (12)(34), (13)(24), (14)(23), together with the identity, do form a subgroup isomorphic to $C_2 \times C_2$; and this is the only possibility, since the elements of order 3 cannot belong to a subgroup of order 4 (why?).

Order 6 Suppose K is a subgroup of order 6. Since there are only four elements of A_4 which do not have order 3, K must contain at least one element of order 3, say $x = (123)$, and its inverse $x^{-1} = (132)$. The elements of order 3 in K occur in pairs, such as x and x^{-1}, and so there are an even number of them. But K also contains the identity, and so in order to make the total number of elements even, K must contain at least one of the elements of order 2. Now if one such element y is in K, so are xyx^{-1} and $x^{-1}yx$ (by the subgroup property). These elements are conjugate to y and so they have the same type as y, and they are distinct. Hence the elements y, xyx^{-1}, and $x^{-1}yx$ are the three elements of order 2 (that is, (12)(34), (13)(24), and (14)(23)) is some order.

But we showed that these three elements, together with the identity, form a subgroup of order 4, which must be a subgroup of K. By Lagrange's theorem, the order of K is a multiple of 4, contradicting the assumption that $|K| = 6$. Hence there are no subgroups of order six.

Order 12 Clearly, the only possibility is A_4 itself. □

It is convenient to arrange the subgroups in a *lattice* (Fig. 20.4). In general, the lattice of subgroups can be extremely complicated, but in the next section we shall see that in the case of a cyclic group the lattice can be described in simple arithmetical terms.

Exercises 20.8

1 Let H be a subgroup of G, and define a relation $\sim$ on G by the rule that $x \sim y$ means $x^{-1}y \in H$. Show that $\sim$ is an equivalence relation and its equivalence classes are the left cosets of H.

2 Describe explicitly the partition of the triangle group by the *right* cosets of the subgroup $H = \{i, x\}$. Check that the partition is not the same as that given by the left cosets of H.

3 The symmetry group of a regular pentagon is a group of order 10. Show that it has subgroups of each of the orders allowed by Lagrange's theorem, and sketch the lattice of subgroups.

4 Suppose that a finite group G and a prime number p are given, and G has exactly m subgroups of order p. Show that the number of elements of order p in G is $m(p-1)$.

5 Use Ex. 4 to show that a non-cyclic group of order 55 has at least one subgroup of order 5 and at least one subgroup of order 11.

6 Sketch the lattice of subgroups of the symmetric group S_4. [Hint: you will need a large sheet of paper.]

now know that these are the only subgroups. Furthermore, any two subgroups having the same order are identical. By simple calculations we can verify these facts explicitly, as in Table 20.9.1. Another way of illustrating the result is to say that the lattice of subgroups of C_{12} is the same as the lattice of divisors of 12 (Fig. 20.5).

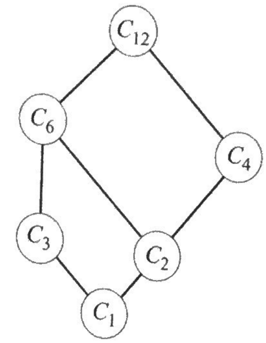

Fig. 20.5
The lattice of subgroups of C_{12}.

Table 20.9.1

Subgroup	Elements	Isomorphism class
$\langle 1 \rangle$	1	C_1
$\langle z^6 \rangle$	$1, z^6$	C_2
$\langle z^4 \rangle$, $\langle z^8 \rangle$	$1, z^4, z^8$	C_3
$\langle z^3 \rangle$, $\langle z^9 \rangle$	$1, z^3, z^6, z^9$	C_4
$\langle z^2 \rangle$, $\langle z^{10} \rangle$	$1, z^2, z^4, z^6, z^8, z^{10}$	C_6
$\langle z \rangle$, $\langle z^5 \rangle$, $\langle z^7 \rangle$, $\langle z^{11} \rangle$	$1, z, z^2, \ldots, z^{11}$	C_{12}

Exercises 20.9

1 Sketch the lattice of subgroups of the cyclic group C_{24}. If z is a generator of C_{24}, identify the subgroups generated by z^3, z^8, and z^9.

2 How many elements of C_{60} generate the whole group?

3 Suppose that r and s are divisors of n, and the cyclic group C_n is generated by x. Write down generators for the cyclic subgroups C_r and C_s of C_n. Find the order of $C_r \cap C_s$, and write down a generator for this subgroup.

4 Explain how Theorem 20.8.4 can be deduced from Theorem 20.9.

20.10 Miscellaneous Exercises

1 Suppose x, y, and z are elements of a group G. Simplify the following expressions in G.

(i) $(x^{-1}z^{-1})(y^{-1}x)^{-1}y$, (ii) $(xzy)^{-1}x(xyz^{-1})^{-1}$.

2 When x and y are elements of a group G the **conjugate** of x with respect to y is yxy^{-1}, which is written x^y, and the **commutator** of x and y is $xyx^{-1}y^{-1}$, which is written $[x, y]$. Show that for any elements a, b, c in G,

(i) $[ab, c] = [b, c]^a[a, c]$, (ii) $[a, bc] = [a, b][a, c]^b$.

3 Let $t_{a,\,b}$ denote the function from the set $\mathbb{R}$ of real numbers to itself defined by

$$t_{a,\,b}(x) = ax + b,$$

where a and b are real numbers and $a \neq 0$. Show that the set of all such functions forms a group under the operation of composition of functions.

4 Show that the group defined in the previous exercise contains infinitely many elements of order 2.

5 Show that if H is a subgroup of index 2 in a group G then the left coset gH is the same as the right coset Hg for all g in G.

6 Define a binary operation $*$ on the set $\mathbb{R}$ of real numbers by $x * y = xy + x + y$, where the symbols on the right-hand side of the equation have their usual meanings. Show that, with respect to $*$, $\mathbb{R}$ satisfies three of the axioms for a group, but that not every element of $\mathbb{R}$ has an inverse.

7 Let α and β denote the functions defined (on a suitable subset of the real numbers) by

$$\alpha(x) = 1/x, \qquad \beta(x) = 1/(1-x).$$

Let K denote the group obtained by the composition of α and β and their powers in all possible ways. Show that K is isomorphic to the triangle group $G_\triangle$ defined in Section 20.2.

8 Let J_m denote the set of complex numbers z which satisfy $z^m = 1$, where m is a positive integer. Show that J_m is a cyclic group of order m, with respect to the usual multiplication of complex numbers.

9 Show that the set of all 2×2 matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (a, b, c, d \in \mathbb{R}),$$

such that $ad \neq bc$, is a group under the usual matrix multiplication.

10 Let K and L be finite subgroups of a group G and let

$$KL = \{g \in G \mid g = kl \text{ for some } k \in K \text{ and } l \in L\}$$

Prove that $|K|\,|L| = |KL|\,|K \cap L|$.

11 Show that the subset KL defined in the previous exercise is a subgroup of G if and only if $KL = LK$.

12 Show that any group of order six is isomorphic to C_6 or S_3.

13 Let H and K be subgroups of a finite group G such that gcd $(|H|, |K|) = 1$. Show that $|H \cap K| = 1$.

14 Let X be the set of ordered pairs (n, f) where n is an integer and f is a rational number (fraction). Define a binary operation $\circ$ on X by the rule

$$(n_1, f_1) \circ (n_2, f_2) = (n_1 + n_2, 2^{n_2} f_1 + f_2).$$

Show that X is a group with respect to the $\circ$ operation. Which of the following are subgroups of X?

(i) The subset of elements of the form $(n, 0)$.
(ii) The subset of elements of the form $(0, f)$.

15 Let M be the group obtained by the construction given in Ex. 3 when the set $\mathbb{R}$ is replaced by the set $\mathbb{Z}_5$ of integers modulo 5. Show that

(i) $|M| = 20$;
(ii) M contains subgroups of each of the orders allowed by Lagrange's theorem.

Sketch the lattice of subgroups of this group. (It may be helpful to consider elements of M as permutations of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.)

16 Write out the partition of A_4 (Section 20.8, *Example*) formed by the left cosets of the cyclic subgroup generated by (123), and verify that the partition formed by the right cosets of the same subgroup is different.

17 Show that S_5 has no subgroup of order 15.

18 Let p be a prime. The group $GL_2(\mathbb{Z}_p)$ is defined to be the group of those 2×2 matrices with entries in $\mathbb{Z}_p$ which have an inverse with respect to matrix multiplication. Show that

(i) $GL_2(\mathbb{Z}_2)$ is isomorphic to the symmetric group S_3.
(ii) The order of $GL_2(\mathbb{Z}_p)$ is $p(p^2 - 1)$.
(iii) The centre of $GL_2(\mathbb{Z}_p)$ consists of the matrices αI, where I is the identity matrix and $\alpha \neq 0$ in $\mathbb{Z}_p$.

19 Let F denote the set of all functions $f\colon \mathbb{Z} \to \mathbb{Z}$, and let V be the set of ordered pairs (n, f) such that n is in $\mathbb{Z}$ and f is in F. Define a binary operation $*$ on V by the rule

$$(n_1, f_1) * (n_2, f_2) = (n_1 + n_2, f_3)$$

where $f_3(m) = f_1(m - n_1) + f_2(m)$. Show that V is a group with respect to the $*$ operation.

20 Let V and F be as in the previous exercise, and let E be the subset of F containing those functions f for which $f(n) = n$ except for a finite set of integers n. Show that the subset of elements of the form $(0, f)$ for which is f is in E is a subgroup of V.

21 Show that there are just five different (that is, mutually non-isomorphic) groups of order eight.

22 Let x be an element of order m in a finite group G. Show that the order of x^t in G is m/d, where $d = \gcd(m, t)$.

23 Let G be a finite group and H a subgroup of index k in G. Prove that there is a set $\{g_1, g_2, \ldots, g_k\}$ of elements of G which is simultaneously a set of representatives for the left cosets, and for the right cosets, of H in G. In other words, we can write

$$G = g_1 H \cup \cdots \cup g_k H = H g_1 \cup \cdots \cup H g_k.$$

[Hint: Ex. 17.7.15.]

21
Groups of permutations

21.1 Definitions and examples

Contents

When we began our study of permutations we remarked that the rule of composition in the symmetric group S_n has four fundamental properties. In the previous chapter we used those properties as the axioms for a group. Now we shall return to the study of permutations, using the group-theoretical terminology to guide our investigations.

Let G be a set of permutations of a finite set X. If G is a group (with respect to the rule for combining permutations) then we say that G is a **group of permutations of X**.

If we take $X = \{1, 2, \ldots, n\}$ then a group of permutations of X is simply a subgroup of S_n. For example, here is a list of all the subgroups of S_3, each of which is also a group of permutations of $\{1, 2, 3\}$.

$$H_1 = \{\mathrm{id}\}, \qquad H_2 = \{\mathrm{id}, (12)\}, \qquad H_3 = \{\mathrm{id}, (13)\},$$
$$H_4 = \{\mathrm{id}, (23)\}, \qquad H_5 = \{\mathrm{id}, (123), (132)\}, \qquad H_6 = S_3.$$

In order to verify whether or not a given subset of S_n is a subgroup it is convenient to use Theorem 20.7, which tells us that (since S_n is finite) we need only verify the closure property.

Exercises 21.1

1 Which of the following are groups of permutations of the set $\{1, 2, 3, 4, 5\}$, that is, which of them are subgroups of S_5?

(i) $\{(12345), (124)(35)\}$.

(ii) $\{\mathrm{id}, (12345), (13524), (14253), (15432)\}$.

(iii) $\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$.

(iv) $\{\mathrm{id}, (12)(345), (135)(24), (15324), (12)(45), (134)(25), (143)(25)\}$.

An important subgroup of S_n is the subgroup consisting of all the even permutations, which is known as the **alternating group** A_n. The results obtained in Section 12.6 imply that the composite of two even permutations is even (so that A_n is indeed a subgroup of S_n) and that the order of A_n is $\frac{1}{2}n!$

For example, if the permutation (135) is part of an automorphism α, then α must transform 2 to 4, since 2 is the only vertex adjacent to both 1 and 3, and 4 is only vertex adjacent to both 3 and 5. Similarly, α must transform 4 to 6 and 6 to 2, and so we must have $\alpha = (135)(246)$. In the same way, each of the six permutations of $\{1, 3, 5\}$ can be extended in a unique manner to give an automorphism of the graph

id	extends to	id,	(13)	extends to	(13)(46),
(135)	extends to	(135)(246),	(15)	extends to	(15)(24),
(153)	extends to	(153)(264),	(35)	extends to	(35)(26).

It follows that there are just six automorphisms of the graph, and they are the six extended permutations listed above. □

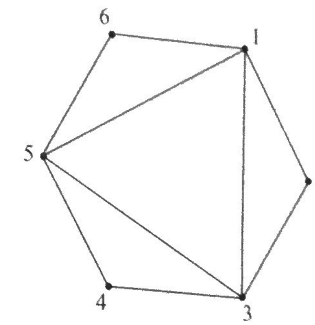

Fig. 21.3
How many automorphisms?

Exercises 21.1 (continued)

2 Find the orders of the following permutations, considered as elements of the symmetric group S_8:

(i) (1235)(48)(67); (ii) (12)(35)(48)(67);

(iii) (13672)(458).

3 According to Theorem 20.8.3 the order of any element of S_8 is a divisor of $|S_8| = 8!$ By considering the cycle structure of the permutations in S_8 write down the orders of elements which actually occur in S_8, and give an example of a divisor of 8! which is not the order of an element of S_8.

4 List all the symmetries of a regular pentagon, regarded as permutations of the corners 1, 2, 3, 4, 5, labelled in cyclic order.

5 Find the group of automorphisms of the graph given by the following adjacency list. (A picture will help.)

1	2	3	4	5	6	7	8
2	1	1	1	2	3	4	4
3	3	2	7	7	7	5	5
4	5	6	8	8	8	6	6

21.2 Orbits and stabilizers

Suppose that G is a group of permutations of a set X. We shall show that the group structure of G leads naturally to a partition of X.

Define a relation $\sim$ on X by the rule

$$x \sim y \quad \Leftrightarrow \quad g(x) = y \text{ for some } g \in G.$$

We can check that $\sim$ is an equivalence relation in the usual way.

(Reflexivity) Since id belongs to any group, and $\mathrm{id}(x) = x$ for all $x \in X$, we have $x \sim x$.

(Symmetry) Suppose $x \sim y$, so that $g(x) = y$ for some $g \in G$. Since G is a group, g^{-1} belongs to G, and since $g^{-1}(y) = x$ we have $y \sim x$, as required.

(Transitivity) If $x \sim y$ and $y \sim z$ we must have $y = g_1(x)$ and $z = g_2(y)$ for some g_1 and g_2 in G. Since G is a group, $g_2 g_1$ is in G and since $g_2 g_1(x) = z$ we have $x \sim z$, as required.

It follows that the distinct equivalence classes of $\sim$ form a partition of X; x and y are in the same part if and only if there is a permutation in G which transforms x