11. Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square (where the vertices of the square are labelled as in Section 2).

12. Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action (label vertices as usual).

13. Find the kernel of the left regular action.

14. Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

15. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = ag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action of G on itself.

16. Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a = gag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action (this action of G on itself is called *conjugation*).

17. Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by

$$x \mapsto gxg^{-1}.$$

For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself (i.e., is an automorphism of G — cf. Exercise 20, Section 6). Deduce that x and gxg^{-1} have the same order for all x in G and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

18. Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \qquad \text{if and only if} \qquad a = hb \quad \text{for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.)

19. Let H be a subgroup (cf. Exercise 26 of Section 1) of the finite group G and let H act on G (here $A = G$) by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map

$$H \to \mathcal{O} \qquad \text{defined by} \qquad h \mapsto hx$$

is a bijection (hence all orbits have cardinality $|H|$). From this and the preceding exercise deduce *Lagrange's Theorem*:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

20. Show that the group of rigid motions of a tetrahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4.

21. Show that the group of rigid motions of a cube is isomorphic to S_4. [This group acts on the set of four pairs of opposite vertices.]

22. Show that the group of rigid motions of an octahedron is isomorphic to a subgroup (cf. Exercise 26 of Section 1) of S_4. [This group acts on the set of four pairs of opposite faces.] Deduce that the groups of rigid motions of a cube and an octahedron are isomorphic. (These groups are isomorphic because these solids are "dual" — see *Introduction to Geometry* by H. Coxeter, Wiley, 1961. We shall see later that the groups of rigid motions of the dodecahedron and icosahedron are isomorphic as well — these solids are also dual.)

23. Explain why the action of the group of rigid motions of a cube on the set of three pairs of opposite faces is not faithful. Find the kernel of this action.

CHAPTER 2

Subgroups

2.1 DEFINITION AND EXAMPLES

One basic method for unravelling the structure of any mathematical object which is defined by a set of axioms is to study *subsets* of that object which also *satisfy the same axioms*. We begin this program by discussing subgroups of a group. A second basic method for unravelling structure is to study quotients of an object; the notion of a quotient group, which is a way (roughly speaking) of collapsing one group onto a smaller group, will be dealt with in the next chapter. Both of these themes will recur throughout the text as we study subgroups and quotient groups of a group, subrings and quotient rings of a ring, subspaces and quotient spaces of a vector space, etc.

Definition. Let G be a group. The subset H of G is a *subgroup* of G if H is nonempty and H is closed under products and inverses (i.e., $x, y \in H$ implies $x^{-1} \in H$ and $xy \in H$). If H is a subgroup of G we shall write $H \leq G$.

Subgroups of G are just subsets of G which are themselves groups with respect to the operation defined in G, i.e., the binary operation on G restricts to give a binary operation on H which is associative, has an identity in H, and has inverses in H for all the elements of H.

When we say that H is a subgroup of G we shall always mean that the operation for the group H is the operation on G restricted to H (in general it is possible that the subset H has the structure of a group with respect to some operation other than the operation on G restricted to H, cf. Example 5(a) following). As we have been doing for functions restricted to a subset, we shall denote the operation for G and the operation for the subgroup H by the same symbol. If $H \leq G$ and $H \neq G$ we shall write $H < G$ to emphasize that the containment is proper.

If H is a subgroup of G then, since the operation for H is the operation for G restricted to H, any equation in the subgroup H may also be viewed as an equation in the group G. Thus the cancellation laws for G imply that the identity for H is the same as the identity of G (in particular, every subgroup must contain 1, the identity of G) and the inverse of an element x in H is the same as the inverse of x when considered as an element of G (so the notation x^{-1} is unambiguous).

Examples

(1) $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ with the operation of addition.

(2) Any group G has two subgroups: $H = G$ and $H = \{1\}$; the latter is called the *trivial subgroup* and will henceforth be denoted by 1.

(3) If $G = D_{2n}$ is the dihedral group of order $2n$, let H be $\{1, r, r^2, \ldots, r^{n-1}\}$, the set of all rotations in G. Since the product of two rotations is again a rotation and the inverse of a rotation is also a rotation it follows that H is a subgroup of D_{2n} of order n.

(4) The set of even integers is a subgroup of the group of all integers under addition.

(5) Some examples of subsets which are *not* subgroups:

(a) $\mathbb{Q} - \{0\}$ under multiplication is not a subgroup of $\mathbb{R}$ under addition even though both are groups and $\mathbb{Q} - \{0\}$ is a subset of $\mathbb{R}$; the operation of multiplication on $\mathbb{Q} - \{0\}$ is not the restriction of the operation of addition on $\mathbb{R}$.

(b) $\mathbb{Z}^+$ (under addition) is not a subgroup of $\mathbb{Z}$ (under addition) because although $\mathbb{Z}^+$ is closed under $+$, it does not contain the identity, 0, of $\mathbb{Z}$ and although each $x \in \mathbb{Z}^+$ has an additive inverse, $-x$, in $\mathbb{Z}$, $-x \notin \mathbb{Z}^+$, i.e., $\mathbb{Z}^+$ is not closed under the operation of taking inverses (in particular, $\mathbb{Z}^+$ is not a group under addition). For analogous reasons, $(\mathbb{Z} - \{0\}, \times)$ is not a subgroup of $(\mathbb{Q} - \{0\}, \times)$.

(c) D_6 is not a subgroup of D_8 since the former is not even a subset of the latter.

(6) The relation "is a subgroup of" is transitive: if H is a subgroup of a group G and K is a subgroup of H, then K is also a subgroup of G.

As we saw in Chapter 1, even for easy examples checking that all the group axioms (especially the associative law) hold for any given binary operation can be tedious at best. Once we know that we have a group, however, checking that a subset of it is (or is not) a subgroup is a much easier task, since all we need to check is closure under multiplication and under taking inverses. The next proposition shows that these can be amalgamated into a single test and also shows that for *finite* groups it suffices to check for closure under multiplication.

Proposition 1. *(The Subgroup Criterion)* A subset H of a group G is a subgroup if and only if

(1) $H \neq \emptyset$, and

(2) for all $x, y \in H$, $xy^{-1} \in H$.

Furthermore, if H is finite, then it suffices to check that H is nonempty and closed under multiplication.

Proof: If H is a subgroup of G, then certainly (1) and (2) hold because H contains the identity of G and the inverse of each of its elements and because H is closed under multiplication.

It remains to show conversely that if H satisfies both (1) and (2), then $H \leq G$. Let x be any element in H (such x exists by property (1)). Let $y = x$ and apply property (2) to deduce that $1 = xx^{-1} \in H$, so H contains the identity of G. Then, again by (2), since H contains 1 and x, H contains the element $1x^{-1}$, i.e., $x^{-1} \in H$ and H is closed under taking inverses. Finally, if x and y are any two elements of H, then H contains x and y^{-1} by what we have just proved, so by (2), H also contains $x(y^{-1})^{-1} = xy$. Hence H is also closed under multiplication, which proves H is a subgroup of G.