Chapter 1

Elementary Group Theory

1.1 Abstract Groups

A group is an abstract mathematical entity which expresses the intuitive concept of symmetry.

Defintion. A **group** G is a set of objects $\{g, h, k, \ldots\}$ (not necessarily countable) together with a binary operation which associates with any ordered pair of elements g, h in G a third element gh. The binary operation (called **group multiplication**) is subject to the following requirements:

(1) There exists an element e in G called the **identity element** such that $ge = eg = g$ for all $g \in G$.

(2) For every $g \in G$ there exists in G an **inverse element** g^{-1} such that $gg^{-1} = g^{-1}g = e$.

(3) **Associative law.** The identity $(gh)k = g(hk)$ is satisfied for all $g, h, k \in G$.

Thus, any set together with a binary operation which satisfies conditions (1)–(3) is called a group. If $gh = hg$ we say that the elements g and h **commute.** If all elements of G commute then G is a **commutative** or **abelian** group. If G has a finite number of elements it has **finite order** $n(G)$, where $n(G)$ is the number of elements. Otherwise, G has **infinite order.**

A **subgroup** H of G is a subset which is itself a group under the group multiplication defined in G. The subgroups G and $\{e\}$ are called **improper** subgroups of G. All other subgroups are **proper.**

Theorem 1.1. A nonempty subset H of a group G is a subgroup if and only if the following two conditions hold:

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

Proof. If H is a subgroup then (1) and (2) clearly hold. Conversely, suppose these conditions hold. We show that H satisfies the requirements for a group. The associative law holds since it holds for G. There exists some $h \in H$ since H is nonempty and by (2) we have $h^{-1} \in H$. By (1), $hh^{-1} = e \in H$, so H has an identity. Q.E.D.

The identity element e of a group is unique: Suppose $e' \in G$ such that $e'g = ge' = g$ for all $g \in G$. Setting $g = e$, we find $ee' = e'e = e$. But $e'e = e'$ since e is an identity element. Therefore, $e' = e$.

A similar proof shows that the inverse element g^{-1} of g is unique. Suppose $g' \in G$ such that $gg' = e$. Multiplying on the left by g^{-1} and using the associative law, we get $g^{-1} = g^{-1}e = g^{-1}(gg') = (g^{-1}g)g' = eg' = g'$.

The following examples indicate the variety of mathematical objects which have the structure of groups. (For most groups in this book the associative law will be trivial to verify. We shall specifically verify the law only in those cases where it is not obvious.)

Example 1. The real numbers R with addition as the group product. The product of two elements r_1, r_2 is their sum $r_1 + r_2$. The identity is 0 and the inverse of an element is its negative. R is an infinite abelian group. Among the subgroups of R are the integers, the even integers, and the group consisting of the element zero alone.

Example 2. The nonzero real numbers in R with multiplication of real numbers as the group product. The identity is 1 and the inverse of $r \in R$ is $1/r$. Group multiplication is again commutative. One of the subgroups is the group of positive numbers.

Example 3. The group containing two elements $\{0, 1\}$ with group multiplication given by $0 \cdot 0 = 0$, $0 \cdot 1 = 1 \cdot 0 = 1$, $1 \cdot 1 = 0$. The identity element is 0. This is an abelian group of order two. It has only two subgroups, $\{0\}$ and $\{0, 1\}$.

Example 4. The **complex general linear group** $GL(n, \mathbb{C})$. Here n is a positive integer. The group elements A are nonsingular $n \times n$ matrices with complex coefficients:

$$(1.1) \quad GL(n, \mathbb{C}) = \{A = (A_{ij}), \quad 1 \leq i, j \leq n : A_{ij} \in \mathbb{C} \quad \text{and} \quad \det A \neq 0\}.$$

Group multiplication is ordinary matrix multiplication. The identity element is the identity matrix $E = (\delta_{ij})$, where δ_{ij} is the **Kronecker delta,** (see the Symbol Index). The inverse of an element A is its matrix inverse, which exists since A is nonsingular. Clearly $GL(n, \mathbb{C})$ is infinite and nonabelian. Among its subgroups are the **real general linear group** $GL(n, R)$ which consists of the **real** $n \times n$ nonsingular matrices, the **complex special linear group**

$$SL(n, \mathbb{C}) = \{A \in GL(n, \mathbb{C}) : \det A = 1\}, \tag{1.2}$$

and the **real special linear group**

$$SL(n, R) = \{A \in GL(n, R) : \det A = 1\}. \tag{1.3}$$

Example 5. The **symmetric group** S_n. Let n be a positive integer. A **permutation of** n **objects** (say the set $X = \{1, 2, \ldots, n\}$) is a 1–1 mapping of X onto itself. Such a permutation s is written

$$s = \begin{pmatrix} 1 & 2 & \cdots & n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix} \tag{1.4}$$

and we say: 1 is mapped into p_1, 2 into $p_2, \ldots, n$ into p_n. The numbers $p_1, \ldots, p_n$ are a reordering of $1, 2, \ldots, n$ and no two of the p_j are the same. The order in which the columns of (1.4) are written is unimportant. The **inverse** permutation s^{-1} is given by

$$s^{-1} = \begin{pmatrix} p_1 & p_2 & \cdots & p_n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

The **product** of two permutations s and t,

$$t = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ 1 & 2 & \cdots & n \end{pmatrix},$$

is given by the permutation

$$st = \begin{pmatrix} q_1 & q_2 & \cdots & q_n \\ p_1 & p_2 & \cdots & p_n \end{pmatrix},$$

where the product is read from right to left. That is, the integer q_i is mapped to i by t and i is mapped to p_i by s, so q_i is mapped to p_i by st. The **identity** permutation is

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

With these definitions it is easy to show that the permutations of n objects form a group S_n called the symmetric group. S_n has order $n!$.

Instead of (1.4) we will often use the convenient **cycle notation,** which is

best explained by an example. Consider the permutation

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 6 & 7 & 4 & 3 & 2 & 8 \end{pmatrix}.$$

Starting with the symbol 1, we see that s maps 1 into 5, 5 into 4, 4 into 7, 7 into 2, and 2 into 1, closing a **cycle**. We write (15472). We now chose a symbol in the top line which is not in the first cycle, say 3. The permutation generates a second cycle (36). The only remaining symbol in the top row is 8, which is mapped into itself and generates the cycle (8). Finally we write

$$s = (15472)(36)(8) = (15472)(36),$$

where in the second expression we have omitted the unpermuted symbol. (This last simplification can only be used if we keep in mind the number of elements permuted.) In writing an individual cycle it makes no difference where we start. Thus, $(36) = (63)$ and $(15472) = (21547) = (72154) = (47215) = (54721)$. Furthermore, it makes no difference in which order we write the cycles in a given permutation as long as the cycles contain no common elements, e.g., $(15472)(36) = (36)(15472)$. We present a final example showing the computation of a product of permutations in S_8 with the cycle notation: $(872)(34)(432) = (2387)$.

1.2 Subgroups and Cosets

Let H be a subgroup of the group G and $g \in G$. The set

$$gH = \{gh: h \in H\}$$

is called a **left coset** of H. There is a similar definition for right cosets. Every element g in G is contained in some left coset of H. In particular, $g = ge \in gH$. Furthermore, two left cosets are either identical or have no element in common. To see this, assume the cosets gH and kH have at least one element a in common. Thus, $a = gh_1 = kh_2$ with $h_1, h_2 \in H$, which implies $g = kh_2h_1^{-1} \in kH$ and $gH \subseteq kH$. Similarly, $k = gh_1h_2^{-1} \in gH$ and $kH \subseteq gH$. We conclude that $gH = kH$, i.e., the sets gH and kH have the same elements.

Suppose G is a finite group of order $n(G)$. Then the subgroup H is also finite and it is easy to show that each left coset gH contains exactly $n(H)$ distinct elements. As we have seen, it is possible to partition the elements of G into a finite number of disjoint left cosets $g_1H, g_2H, \ldots, g_mH$. That is, every element of G lies in exactly one of the cosets g_iH. Since there are m cosets and each coset contains $n(H)$ elements, it follows that $n(G) = m \cdot n(H)$. The integer $m = n(G)/n(H)$ is called the **index** of H in G. We have proved the following theorem due to Lagrange.

Theorem 1.2. The order of a subgroup of a finite group divides the order of the group.

Lagrange's theorem severely restricts the possible orders of subgroups. Thus, a group G of order 15 can have at most subgroups of order 1, 3, 5, or 15. The subgroup of order 15 is G itself, the group of order 1 is $\{e\}$, while the other possibilities lead to proper subgroups of G. A group of order p, where p is prime, has no proper subgroups.

By using left (or right) cosets we have partitioned the elements of G into disjoint sets. Another way to partition G is by means of conjugacy classes. A group element h is said to be **conjugate** to the group element k, $h \sim k$, if there exists a $g \in G$ such that $k = ghg^{-1}$. It is easy to show that conjugacy is an equivalence relation, i.e., (1) $h \sim h$ (reflexive), (2) $h \sim k$ implies $k \sim h$ (symmetric), and (3) $h \sim k$, $k \sim j$ implies $h \sim j$ (transitive). Thus, the elements of G can be divided into **conjugacy classes** of mutually conjugate elements. The class containing e consists of just one element since $geg^{-1} = e$ for all $g \in G$. Different conjugacy classes do not necessarily contain the same number of elements. We will study specific examples of conjugacy classes later where it will become apparent that such classes have simple geometrical interpretations.

If G is finite the number of elements in each conjugacy class is a factor of $n(G)$. To see this, choose some $g \in G$ and consider the set

$$H^g = \{h \in G: hgh^{-1} = g\}.$$

H^g is clearly a subgroup of G. The number of elements conjugate to g is equal to the number of distinct elements kgk^{-1} which can be formed by letting k run over G. We show that this is just the number of left cosets of H^g, a factor of $n(G)$. Indeed, if $k_1 g k_1^{-1} = k_2 g k_2^{-1}$, then $(k_1^{-1}k_2)g(k_1^{-1}k_2)^{-1} = g$, so $k_1^{-1}k_2 \in H^g$ or $k_2 \in k_1 H^g$. Conversely, if $k_2 \in k_1 H^g$ then $k_1 g k_1^{-1} = k_2 g k_2^{-1}$. Q.E.D.

The subgroup H of G is said to be **conjugate** to the subgroup K if there is a $g \in G$ such that $K = gHg^{-1}$ as sets, i.e., $Kg = gH$. Note that gHg^{-1} is a subgroup of G for any $g \in G$. Just as above, we can use this notion to partition the subgroups of G into conjugacy classes. A subgroup N is **normal (invariant, self-conjugate)** if $gNg^{-1} = N$ for all $g \in G$. Equivalently, N is normal if and only if $gN = Ng$ for all $g \in G$.

If N is a normal subgroup we can construct a group from the cosets of N, called the **factor group** G/N. The elements of G/N are the cosets gN, $g \in G$. Of course two cosets gN, $g'N$ containing the same elements of G define the same element of G/N: $gN = g'N$. Since N is normal it follows that $(g_1N)(g_2N) = (g_1N)(Ng_2) = g_1Ng_2 = g_1g_2N$ as sets. (Note that $NN = N$ as sets.) There-

fore, we define group multiplication in G/N by

$$(g_1N)(g_2N) = g_1g_2N.$$

If G is finite, the order of G/N is clearly the index of N in G.

Corresponding to any element g of G we define the group element g^n, n an integer, by

$$g^n = \begin{cases} e & \text{if } n = 0 \\ gg \cdots g \quad (n \text{ times}) & \text{if } n > 0 \\ g^{-1}g^{-1} \cdots g^{-1} \quad (-n \text{ times}) & \text{if } n < 0. \end{cases}$$

The reader can easily verify that $g^{n+m} = g^n g^m$ and $g^n g^{-n} = e$.

Suppose $S = \{g, h, \ldots\}$ is an arbitrary subset of G. Consider the set G_S consisting of all finite products of the form $g_1^{n_1}g_2^{n_2} \cdots g_j^{n_j}$, where $g_1, \ldots, g_j \in S, n_1, \ldots, n_j$ run over the integers, and j runs over the positive integers. Under the group product inherited from G, G_S is a subgroup called the subgroup **generated** by the set S. Here G_S can be characterized as follows: If H is a subgroup of G and $S \subseteq H$ then $G_S \subseteq H$. That is, G_S is the smallest subgroup of G containing S. If a group H is generated by $S = \{g\}$, i.e., if every $h \in H$ can be written in the form $h = g^n$, then H is **cyclic.**

The **order of an element** $g \in G$ is the order of the cyclic subgroup generated by $\{g\}$, i.e., the smallest positive integer m such that $g^m = e$. By Theorem 1.2, m divides the order of G.

Theorem 1.3. If G is a finite group of order $2n$ and N is a subgroup of order n then N is normal and the factor group G/N is cyclic of order two.

Proof. Since $2n(N) = n(G)$ there are only two left cosets in G: $eN = N$ and gN, where $g \notin N$. Similarly, there are only two right cosets N and Ng. Since every element of G is contained in exactly one left coset and exactly one right coset, we must have $gN = Ng$ for all $g \in G, g \notin N$. This last relation is also true if $g \in N$. Therefore, N is normal. The relations $NN = N$, $N(gN) = (gN)N = gN$, and $(gN)(gN) = N$, $g \notin N$, imply G/N is cyclic of order two The last relation follows from the fact that $g^2 \in N$. For, if $g^2 \in gN$ then $g \in N$, a contradiction. Q.E.D.

1.3 Homomorphisms, Isomorphisms, and Automorphisms

A **homomorphism** μ is a mapping from a group G into a group G' which transforms products into products. Thus, to every $g \in G$ there is associated $\mu(g) \in G'$ such that $\mu(g_1g_2) = \mu(g_1)\mu(g_2)$ for all $g_1, g_2 \in G$. Let e, e' be the identity elements of G, G', respectively. Then $\mu(e) = \mu(ee) = \mu(e)\mu(e)$, which implies $\mu(e) = e'$ by multiplication on the right with $\mu(e)^{-1} \in G'$.

Thus, μ maps the identity element of G into the identity element of G'. A similar argument shows $\mu(g^{-1}) = \mu(g)^{-1}$, i.e., μ maps inverses into inverses.

Homomorphisms are important because they are exactly the maps from one group to another that preserve group structure. They are the group analogy of linear transformations on vector spaces. Here we discuss homomorphisms from an abstract viewpoint, but in the following sections we will return to this topic and stress its geometrical aspects.

A homomorphism μ from G to G' is often designated by $\mu: G \longrightarrow G'$. The **domain** of μ is G, the **range** of μ is $\mu(G) = \{\mu(g) \in G' : g \in G\}$. Clearly, $\mu(G)$ is a subgroup of G'. If $\mu(G) = G'$ then μ is said to be **onto**. In case $\mu(g_1) \neq \mu(g_2)$ whenever $g_1 \neq g_2$ we say μ is 1–1. A homomorphism which is 1–1 and onto is an **isomorphism**. If μ is an isomorphism then it can be inverted in an obvious manner to define an isomorphism μ^{-1} of G' onto G. From the point of view of abstract group theory, isomorphic groups can be identified. In particular, isomorphic groups have identical multiplication tables. However, for the purposes of physical and geometrical applications it is frequently useful to distinguish between groups which are abstractly isomorphic. We shall return to this point in Section 1.4.

The above concepts are obvious analogies for groups of concepts related to a linear mapping of one vector space into another. We continue this analogy by defining the **kernel** K of μ as the set

$$K = \{g \in G : \mu(g) = e'\}.$$

The kernel of μ is the analogy of the null space of a linear transformation.

Theorem 1.4. K is a normal subgroup of G.

Proof. If $k_1, k_2 \in K$ then $\mu(k_1 k_2) = \mu(k_1)\mu(k_2) = e'e' = e'$, so $k_1 k_2 \in K$. Furthermore, if $k \in K$ then $\mu(k^{-1}) = \mu(k)^{-1} = (e')^{-1} = e'$, so $k^{-1} \in K$. By Theorem 1.1, K is a subgroup of G. To prove that K is normal it is enough to show $gkg^{-1} \in K$ for all $k \in K, g \in G$. This follows from $\mu(gkg^{-1}) = \mu(g)\mu(k)\mu(g)^{-1} = \mu(g)e'\mu(g)^{-1} = e'$. Q.E.D.

All elements in a left coset gK are mapped into the same element $\mu(g)$ in G' since $\mu(gk) = \mu(g)\mu(k) = \mu(g)$ for all $k \in K$. Furthermore, two elements with the same image under μ lie in the same left coset. Indeed, if $\mu(g_1) = \mu(g_2)$ then $\mu(g_1^{-1}g_2) = e'$, which implies $g_1^{-1}g_2 \in K$ or $g_2 \in g_1 K$. This argument leads to several important results. First of all, μ is 1–1 if and only if the kernel consists of the identity element alone. Second, the fact that μ is constant on left cosets of K means that we can define a transformation $\mu': G/K \longrightarrow \mu(G)$ mapping the factor space G/K (which makes sense since K is normal) onto the subgroup $\mu(G)$ of G'. This map is defined by $\mu'(gK) =$

$\mu(g)$, $g \in G$. The above argument shows μ' is 1–1 and onto. It is a homomorphism since $\mu'[(g_1K)(g_2K)] = \mu'[g_1g_2K] = \mu(g_1g_2) = \mu(g_1)\mu(g_2) = \mu'(g_1K)\mu'(g_2K)$.

Theorem 1.5. Let K be the kernel of the homomorphism $\mu: G \longrightarrow G'$. Then $\mu(G)$ is isomorphic to the factor group G/K.

An isomorphism $v: G \longrightarrow G$ of a group G onto itself is called an **automorphism.** For fixed $h \in G$ the map $v_h(g) = hgh^{-1}$ is an automorphism, since $v_h(g_1g_2) = hg_1g_2h^{-1} = (hg_1h^{-1})(hg_2h^{-1}) = v_h(g_1)v_h(g_2)$ and v_h is clearly 1–1 and onto. The mappings v_h, $h \in G$, are called **inner automorphisms.** It is not necessarily true that all automorphisms of a group are inner. The set of all automorphisms of G itself forms a group $A(G)$, the **automorphism group**. The product v_1v_2 of two automorphisms is defined by $v_1v_2(g) = v_1(v_2(g))$, $g \in G$, and the identity automorphism is the identity map of G onto itself. The set $I(G)$ of inner automorphisms of G forms a subgroup of $A(G)$.

1.4 Transformation Groups

Up to now our presentation of group theory has been entirely abstract and there has been little apparent connection with the study of symmetry. The missing link between abstract group theory and the notion of symmetry is the transformation group.

Definition. A **permutation** of a nonempty set X is a 1–1 mapping of X onto itself.

Thus, if the elements of X are denoted $x, y, z, \ldots$ a permutation $\boldsymbol{\sigma}$ is a map from X to X such that (1) $\boldsymbol{\sigma}(x) = \boldsymbol{\sigma}(y)$ if and only if $x = y$ and (2) for every $z \in X$ there exists an $x \in X$ such that $\boldsymbol{\sigma}(x) = z$. One such permutation is the **identity permutation** $\mathbf{1}(x) = x$ for all $x \in X$. The set S_X of all permutations of X forms a group, the **full symmetric group on** X. The product $\boldsymbol{\sigma\tau}$ of two permutations $\boldsymbol{\sigma}, \boldsymbol{\tau} \in S_X$ is given by $\boldsymbol{\sigma\tau}(x) = \boldsymbol{\sigma}(\boldsymbol{\tau}(x))$ for all $x \in X$. clearly $\boldsymbol{\sigma\tau}$ is again a permutation of X. The identity element of S_X is $\mathbf{1}$ and the inverse $\boldsymbol{\sigma}^{-1}$ of $\boldsymbol{\sigma}$ is defined by the requirement $\boldsymbol{\sigma}^{-1}(x) = y$ if and only if $\boldsymbol{\sigma}(y) = x$. Elements of S_X are said to **act** or **operate** on elements of X.

The set X may have an infinite number of elements, e.g., it may consist of all the points in the plane. If X is infinite then S_X is an infinite group. If X has a finite number of elements, say n, then we can identify S_X with the symmetric group S_n defined in Section 1.1. In other words, the groups S_X and S_n are isomorphic in case X has n elements. Recall that S_n has order $n!$.

Definition. A **transformation (permutation) group** on X is a subgroup of S_X.

If G is a transformation group on X then the elements $\mathbf{g}$ of G define permutations $\mathbf{g}(x)$ of X. (Henceforth we will drop the parentheses and write $\mathbf{g}x$ for these mappings. This should not result in any confusion.) These permutations can be used to decompose X into mutually disjoint subsets. Let $x, y \in X$.

Definition. We say x is ***G*-equivalent** to y ($x \sim y$) if $\mathbf{g}x = y$ for some $g \in G$.

Let us show that $\sim$ is an equivalence relation. Now $\mathbf{1}x = x$ implies $x \sim x$. Furthermore, if $\mathbf{g}x = y$ then $x = \mathbf{g}^{-1}\mathbf{g}x = \mathbf{g}^{-1}y$, so $x \sim y$ implies $y \sim x$. Suppose $x \sim y$ and $y \sim z$. Then there exist elements $\mathbf{g}_1, \mathbf{g}_2$ in G such that $\mathbf{g}_1 x = y$, $\mathbf{g}_2 y = z$. But $(\mathbf{g}_2\mathbf{g}_1)x = \mathbf{g}_2 y = z$, so $x \sim z$ and $\sim$ is an equivalence relation.

Definition. The equivalence classes of X under the equivalence relation $\sim$ are called ***G*-orbits** or just **orbits**.

Thus x and y belong to the same orbit if and only if $y = \mathbf{g}x$ for some $\mathbf{g} \in G$. The orbit containing x is the set $\{\mathbf{g}x : \mathbf{g} \in G\}$. If there is only one G-orbit in X we say G is **transitive**. In this case for every pair of points x, y in X there is a $\mathbf{g} \in G$ such that $y = \mathbf{g}x$.

Example. Introduce a rectangular coordinate system (x_1, x_2) in the Euclidean plane X and let G be the set of all rotations about the origin. The elements $\mathbf{g}_\varphi$ of G are labeled by the continuous parameter φ, which is the angle of rotation in radians measured from the positive x_1-axis. If $x \in X$ has coordinates (x_1, x_2) then $y = \mathbf{g}_\varphi x$ has coordinates

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Note that $\mathbf{g}_\varphi = \mathbf{g}_{\varphi+2\pi}$, since both group elements lead to the same transformation of the plane. The elements $\mathbf{g}_\varphi$ clearly form a group since $\mathbf{g}_\varphi\mathbf{g}_\theta = \mathbf{g}_{\varphi+\theta}$. The orbits are concentric circles about the origin. The rotation group in two-space is clearly isomorphic to the matrix group $SO(2, R)$,

$$\begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \qquad 0 \leq \varphi < 2\pi$$

called the **real special orthogonal group in two-space**.

If Y is a subset of X and $\mathbf{g} \in G$, we denote by $\mathbf{g}(Y)$ the set $\{\mathbf{g}y : y \in Y\}$.

Definition. A subset Y of X is ***G*-invariant** or just **invariant** if $\mathbf{g}(Y) \subseteq Y$ for all $\mathbf{g} \in G$.

In particular, the subset $\{x\}$ of X is invariant if and only if $\mathbf{g}x = x$ for all $\mathbf{g} \in G$, i.e., if and only if the G-orbit containing x consists of x alone. In the above example the only invariant point is the origin. A general invariant set is formed by taking arbitrary unions of concentric circles about the origin.

We are now in a position to state a major theme of this book. Given a transformation group G we can look for all G-invariant subsets Y of X. The group G is an invariance or symmetry group of the objects Y. As in the example given above, such subsets often have geometrical significance. They can always be expressed as unions of orbits. Similarly, given an arbitrary subset Y of X we can find a subgroup

$$K = \{\mathbf{g} \in G: \mathbf{g}(Y) \subseteq Y\}.$$

It is easy to show that K is itself a transformation group and Y is a K-invariant subset of X. Frequently we shall refer to K as the ***G*-symmetry** or **symmetry** group of the object Y. This simple relationship between objects and their symmetry groups provides us with a means of applying group-theoretic concepts to geometrical problems.

Example. The symmetries of the square.

Let X be the Euclidean plane and G the group $O(2)$ of all rotations and reflections in the plane which leave a fixed point p invariant. [We will explicitly define the orthogonal group $O(2)$ later. Its exact definition is not important for our example.]

Consider the square $ABCD$ with center p as pictured in Fig. 1.1. We look for all rotations and reflections in $O(2)$ which map the square onto itself. There are eight such symmetries of the square: the identity permutation **1**, the 90° clockwise rotation **r**, clockwise rotations $\mathbf{r}^2$ and $\mathbf{r}^3$ through 180° and

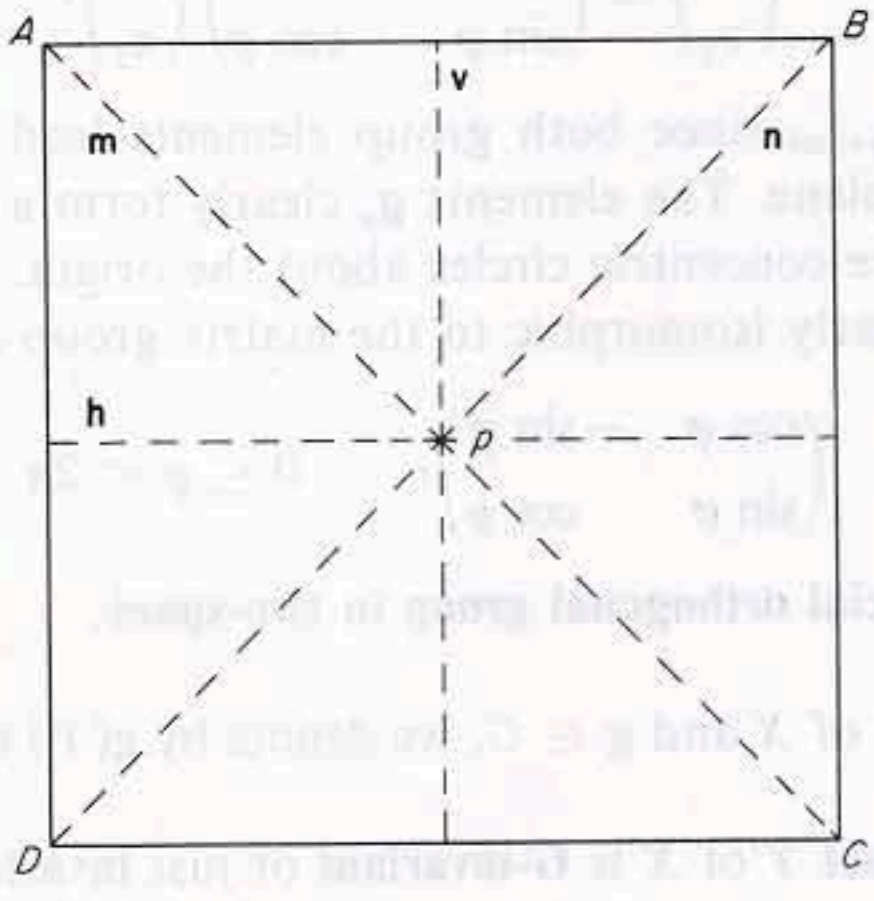

FIGURE 1.1

270°, respectively, and four reflections **h**, **v**, **m**, and **n** about horizontal, vertical, major diagonal, and minor diagonal axes, respectively. A convenient way to list these symmetries is by means of the cycle notation for the permutation of the vertices induced by each symmetry. Thus, we can write $\mathbf{r} = (ABCD)$, $\mathbf{r}^2 = (AC)(BD)$, $\mathbf{r}^3 = (ADCB)$, $\mathbf{h} = (AD)(BC)$, $\mathbf{v} = (AB)(CD)$, $\mathbf{m} = (BD)$, and $\mathbf{n} = (AC)$. These eight symmetries form the group D_4, the dihedral group of order eight. Indeed $\mathbf{1} \in D_4$ and the inverse of each $\mathbf{g} \in D_4$ is in D_4, e.g., $\mathbf{h}^{-1} = \mathbf{h}$, $\mathbf{r}^{-1} = \mathbf{r}^3$. Furthermore, the product of two symmetries is again a symmetry. Thus $\mathbf{nh} = (AC)(AD)(BC) = (ADCB) = \mathbf{r}^3$, or the result of reflecting the square about the horizontal axis followed by a reflection about the minor axis is equivalent to a clockwise rotation of 270°. Recall that the group operations are performed from right to left. (The reader would do well to work out the complete multiplication table for D_4 to be sure he understands this important example.) Note that D_4 is isomorphic to a subgroup of S_4 and our realization of D_4 by permutations constitutes a 1–1 homomorphism of D_4 into S_4.

The conjugacy classes of D_4 can contain possibly one, two, or four elements since those are the factors of eight. (No conjugacy class can contain eight elements since $\{\mathbf{1}\}$ is always a class by itself.) A simple computation shows that there are five classes, $\{\mathbf{1}\}$, $\{\mathbf{r}, \mathbf{r}^3\}$, $\{\mathbf{r}^2\}$, $\{\mathbf{h}, \mathbf{v}\}$, and $\{\mathbf{m}, \mathbf{n}\}$. Note that **1** and $\mathbf{r}^2$ commute with all $\mathbf{g} \in D_4$ and thus lie in classes containing only one element. The conjugacy classes have a simple geometrical interpretation. They correspond to rotations through 0°, 90°, and 180°, respectively, and reflections about an axis through either the midpoints of opposite sides or two opposite vertices. Note that a clockwise rotation of 270° leads to the same result as a counterclockwise rotation through 90°. A conjugacy relation such as $\mathbf{rhr}^{-1} = \mathbf{v}$ can be interpreted as follows: To perform a reflection about the vertical axis, rotate the square counterclockwise 90°, reflect in the horizontal axis, and then rotate back 90° in the clockwise direction.

We now return to a general discussion of the transformation group G on X. For any $x \in X$ the group

$$G^x = \{\mathbf{g} \in G: \mathbf{g}x = x\}$$

is called the **isotropy subgroup** of G at x. It contains those elements of G that leave x invariant.

Theorem 1.6. Each left coset of G^x consists of all elements of G that map x to a specific point y. Thus there is a 1–1 relationship between the points in the G-orbit containing x and the left cosets of G^x. If G is finite, the G-orbit containing x consists of $n(G)/n(G^x)$ points, a factor of $n(G)$.

Proof. The last statement is immediate once we establish the 1–1 relationship between points in the G-orbit through x and left cosets of G^x. Let $y \in X$

such that $x \sim y$, i.e., there is a $\mathbf{g} \in G$ such that $y = \mathbf{g}x$. Then $\mathbf{gh}x = \mathbf{g}x = y$ for all $\mathbf{h} \in G^x$, so all elements in the coset $\mathbf{g}G^x$ map x onto y. Conversely, if $y = \mathbf{k}x$ for some $k \in G$ then $\mathbf{g}x = \mathbf{k}x$ or $x = \mathbf{g}^{-1}\mathbf{k}x$, so $\mathbf{g}^{-1}\mathbf{k} \in G^x$, which implies $\mathbf{k} \in \mathbf{g}G^x$. Q.E.D.

This theorem provides an important connection between the algebraic notion of coset and the geometrical notion of orbit.

It is sometimes helpful to view a transformation group G as an abstract group $\tilde{G}$ together with a 1–1 homomorphism μ of $\tilde{G}$ into the group S_X of permutations of X. Then, $\mu(\tilde{G}) = G$ is isomorphic to $\tilde{G}$. Here we are distinguishing between the abstract multiplicative structure $\tilde{G}$ and the transformation group G on X. Clearly the same abstract group can have many different realizations as a transformation group. We will usually distinguish between two abstractly isomorphic transformation groups if they correspond to physically distinct types of transformations. For example, the cyclic group of order two consists of the elements $\{e, g\}$ with $g^2 = e$. This group can be realized as a transformation group in the plane where g corresponds to a 180° rotation about a point p, e.g., $g = \mathbf{r}^2$ in our last example. Another realization is obtained by letting g correspond to a reflection about a line in the plane, e.g., $g = \mathbf{v}$ in the last example. These groups are isomorphic, but for the purposes of applications to physics and geometry we usually distinguish between them. Nevertheless, we will often use the same symbol G to describe both an abstract group and any transformation group obtained from it.

Any abstract group G can be realized as a transformation group acting on itself. Indeed the mapping $L: G \longrightarrow G$, called the **left regular representation** of G and defined by $\mathbf{L}(a)g = ag$, $a, g \in G$, is easily shown to be a 1–1 homomorphism of G into S_G. That is, $\mathbf{L}(ab) = \mathbf{L}(a)\mathbf{L}(b)$ for $a, b \in G$, each $\mathbf{L}(a)$ is a permutation of G, and $\mathbf{L}(a) = \mathbf{1}$ if and only if $a = e$. This proves Cayley's theorem, which is as follows.

Theorem 1.7. Any group G is isomorphic to a subgroup of the full permutation group S_G. In particular, any finite group of order n is isomorphic to a subgroup of S_n.

Note that the left regular representation is transitive. However, if we restrict L to a proper subgroup H of G, thus defining H as a transformation group on G, the space $G = X$ splits up into orbits which are exactly the right cosets Hg of H.

As a final remark we clarify the meaning of conjugacy in a transformation group. Let G be a transformation group acting on X, $\mathbf{g}, \mathbf{h} \in G$ and $x, y \in X$.

Theorem 1.8. (1) The permutation $\mathbf{g}$ sends x into y if and only if $\mathbf{hgh}^{-1}$ sends $\mathbf{h}x$ into $\mathbf{h}y$.

(2) The point x is invariant under $\mathbf{g}$ if and only if $\mathbf{h}x$ is invariant under $\mathbf{hgh}^{-1}$.

(3) If G^x is the isotropy group of x and $\mathbf{h}$ sends x into y, then $\mathbf{h}G^x\mathbf{h}^{-1} = G^y$, i.e., points in the same G-orbit have conjuate, hence isomorphic, isotropy groups.

Proof. (1) $\mathbf{g}x = y$ if and only if $(\mathbf{hgh}^{-1})\mathbf{h}x = y$. (2) $\mathbf{g}x = x$ if and only if $(\mathbf{hgh}^{-1})\mathbf{h}x = \mathbf{h}x$. (3) Follows from (2). Q.E.D.

1.5 New Groups from Old Ones

Given the groups G and G', we discuss two different ways to construct new groups which contain subgroups isomorphic to G and G'.

Definition. The **direct product** $G \times G'$ is the group consisting of all ordered pairs (g, g') with $g \in G$ and $g' \in G'$. The product of two group elements is given by $(g_1, g_1')(g_2, g_2') = (g_1g_2, g_1'g_2')$.

It is easy to show that $G \times G'$ is a group with identity element (e, e') where e, e' are the identity elements of G, G', respectively. Indeed $(g, g')^{-1} = (g^{-1}, g'^{-1})$ and the associative law is trivial to verify. The subgroup $G \times \{e'\} = \{(g, e') : g \in G\}$ of $G \times G'$ is isomorphic to G with the ismorphism given by $(g, e') \leftrightarrow g$. Similarly the subgroup $\{e\} \times G'$ is isomorphic to G'. Since $(g, e')(e, g') = (e, g')(g, e') = (g, g')$ it follows that (1) the elements of $G \times \{e'\}$ commute with the elements of $\{e\} \times G'$ and (2) every element of $G \times G'$ can be written uniquely as a product of an element in $G \times \{e'\}$ and an element in $\{e\} \times G'$. Frequently one identifies the isomorphic groups $G \times \{e'\}$ and G as well as $\{e\} \times G'$ and G', and writes $(g, e') = g$, $(e, g') = g'$, $(g, g') = gg' = g'g$ for $g \in G$, $g' \in G'$. This point of view leads to the following definition.

Definition. A group G is the **direct product** of its subgroups H and K $(G = H \times K)$ if (1) $hk = kh$ for all $h \in H$, $k \in K$, and (2) every $g \in G$ can be expressed uniquely in the form $g = hk, h \in H, k \in K$. The subgroups H and K are said to be **direct factors** of G.

It follows from (2) that H and K have only the identity element in common. For, if $g \in H \cap K$ then $g = ge = eg$ and by uniqueness we must have $g = e$. Furthermore, the reader can show that H and K are normal subgroups of G.

The above definitions can easily be extended to define direct products $G_1 \times G_2 \times \cdots \times G_n$ of n groups. Furthermore, if the G_i have finite order it

is clear that the order of the direct product is the product of the orders of the direct factors.

As an example we use the first definition to construct the direct product $G \times G'$ of the cyclic group of order two, $G = \{e, a\}$, $a^2 = e$, and the cyclic group of order three, $G' = \{e', b, b^2\}$, $b^3 = e'$. The group $G \times G'$ has order six and contains the element $j = (a, b)$ of order six. Thus, $G \times G'$ is the cyclic group of order six generated by j.

A more general, but more complicated, method of building a new group from two old ones is the semidirect product.

Definition. Let H and K be groups and let the map $k \longrightarrow v_k$ be a homomorphism of K into the automorphism group $A(H)$ of H. Then the set of all ordered pairs $\langle h, k\rangle$, $h \in H$, $k \in K$, forms a group, the **semidirect product** of H and K, with group multiplication

$$\langle h, k\rangle\langle h', k'\rangle = \langle hv_k(h'), kk'\rangle. \tag{5.1}$$

It is necessary to verify that this definition makes sense. First of all, the map v_k is an automorphism of H for each $k \in K$. Furthermore, $v_e = 1$, the identity automorphism, and $v_{kk'}(h) = v_k[v_{k'}(h)]$ for all $k, k' \in K$, $h \in H$. To show that the binary relation (5.1) defines a group, we check the standard group definition in Section 1.1. The associative law follows from

$$\begin{aligned}(\langle h_1, k_1\rangle\langle h_2, k_2\rangle)\langle h_3, k_3\rangle &= \langle h_1 v_{k_1}(h_2), k_1k_2\rangle\langle h_3, k_3\rangle \\ &= \langle h_1 v_{k_1}(h_2) v_{k_1k_2}(h_3), k_1k_2k_3\rangle\end{aligned} \tag{5.2}$$

and

$$\begin{aligned}\langle h_1, k_1\rangle(\langle h_2, k_2\rangle\langle h_3, k_3\rangle) &= \langle h_1, k_1\rangle\langle h_2 v_{k_2}(h_3), k_2k_3\rangle \\ &= \langle h_1 v_{k_1}(h_2 v_{k_2}(h_3)), k_1k_2k_3\rangle \\ &= \langle h_1 v_{k_1}(h_2) v_{k_1k_2}(h_3), k_1k_2k_3\rangle.\end{aligned} \tag{5.3}$$

The identity element is $\langle e, e\rangle$ since

$$\begin{aligned}\langle h, k\rangle\langle e, e\rangle &= \langle hv_k(e), k\rangle = \langle h, k\rangle \\ \langle e, e\rangle\langle h, k\rangle &= \langle v_e(h), k\rangle = \langle h, k\rangle.\end{aligned} \tag{5.4}$$

It is left as an exercise to verify that the element inverse to $\langle h, k\rangle$ is $\langle v_{k^{-1}}(h^{-1}), k^{-1}\rangle$.

If $v_k \equiv 1$ for all $k \in K$ then the semidirect product reduces to the direct product. Just as with the direct product, we can identify the groups $\langle H, e\rangle$ and H using the map $\langle h, e\rangle \longleftrightarrow h$ as well as the groups $\langle e, K\rangle$ and K. Thus we can write any element g of the semidirect product G uniquely in the form $g = \langle h, k\rangle = hk$ and group multiplication becomes

$$(h_1k_1)(h_2k_2) = (h_1 v_{k_1}(h_2))(k_1k_2). \tag{5.5}$$

From this identification it follows that $H \cap K = \{e\}$, K is a subgroup of G, and H is a normal subgroup of G. Indeed, if $k \in K$ and $h \in H$ then

$$khk^{-1} = \langle e, k\rangle\langle h, k^{-1}\rangle = v_k(h), \tag{5.6}$$

so for $g = hk \in G$, $h' \in H$, we have

$$gh'g^{-1} = (hk)h'(k^{-1}h^{-1}) = h(kh'k^{-1})h^{-1} \in H, \tag{5.7}$$

and H is normal.

As an example we note that the dihedral group D_4 is isomorphic to a semidirect product of the cyclic group H of order four and the cyclic group K of order two. If h, k are the generators of H, K respectively, then the automorphism v_k of H is defined by $v_k(h) = h^{-1} = h^3$, i.e., $khk^{-1} = h^{-1}$. We shall see later that the Euclidean and Poincaré groups can also be expressed as semidirect products of simpler groups.

Problems

1.1 Prove: A group G has no proper subgroups if and only if the order of G is finite and prime.

1.2 Let G be a finite group and S a nonempty subset of G such that $gh \in S$ for all g, $h \in S$. Prove that S is a subgroup. What if G is an infinite group?

1.3 Prove: If the group G has exactly one element h of order two then $gh = hg$ for every $g \in G$.

1.4 Show that there are exactly two groups of order four, one of which is cyclic. Find all groups of order six.

1.5 Construct a homomorphism of D_4 onto the cyclic group of order two.

1.6 Determine all subgroups of S_4 and sort them into classes of conjugate subgroups.

1.7 Show that the symmetry group of a regular hexagon consists of 12 elements and determine the conjugacy classes.

1.8 The **commutator subgroup** G_c is the subgroup of G generated by all elements of the form $ghg^{-1}h^{-1}$, $g, h \in G$. Prove that G_c is a normal subgroup of G and G/G_c is commutative.

1.9 Let g, h, k be elements of the group G. Prove that ghk, hkg, and kgh have the same order.