Chapter 2

Elements of Abstract Group Theory

Mathematics is a game played according to certain simple rules with meaningless marks on paper.
—David Hilbert[1]

The importance of symmetry in physics, and for quantum mechanics in particular, was discussed in the preceding chapter. In this chapter, we begin our development of the algebraic structure which enables us to formalize what we mean by "symmetry" by introducing the notion of a group and some related concepts. In the following chapters we will explore the consequences of this algebraic structure for applications to physics.

2.1 Groups: Definitions and Examples

The motivation for introducing an algebraic structure to describe symmetry in physical problems is based on transformations. But the definition of a group is based on a much more abstract notion of what a "transformation" entails. Accordingly, we first set out the conditions

[1]As quoted in, N. Rose, *Mathematical Maxims and Minims* (Rome Press, Raleigh, North Carolina, 1988).

that an *abstract* group must satisfy and then consider both abstract and concrete examples.

Definition. A **group** G is a set of elements $\{a, b, c, \ldots\}$ together with a binary composition law, called *multiplication*, which has the following properties:

1. **Closure.** The composition of any two elements a and b in G, called the *product* and written ab, is itself an element c of G: $ab = c$.
2. **Associativity.** The composition law is associative, i.e., for any elements a, b, and c in G, $(ab)c = a(bc)$.
3. **Identity.** There exists an element, called the **unit** or **identity** and denoted by e, such that $ae = ea = a$ for every element a in G.
4. **Inverses.** Every element a in G has an inverse, denoted by a^{-1}, which is also in G, such that $a^{-1}a = aa^{-1} = e$.

The closure property ensures that the binary composition law does not generate any elements outside of G. Associativity implies that the computation of an n-fold product does not depend on how the elements are grouped together.[2] For example, the product abc is unambiguous because the two interpretations allowed by the existence of a binary composition rule, $(ab)c$ and $a(bc)$, are equal. As will be shown in Sec. 2.3, the left and right identities are equal and unique, as are the left and right inverses of each element. Thus we can replace the existence of an identity and inverses in the definition of a group with the more "minimal" statements:

3′. **Identity.** There exists a unique element, called the **unit** or **identity** and denoted by e, such that $ae = a$ for every element a in G.

4′. **Inverses.** Every element a in G has a unique inverse, denoted by a^{-1}, which is also in G, such that $a^{-1}a = e$.

[2] In abstract algebra (the theory of calculation), binary composition can be associative or non-associative. The most important non-associative algebras in physics are Lie algebras, which will be discussed later in this course.

The terms "multiplication," "product," and "unit" used in this definition are not meant to imply that the composition law corresponds to ordinary multiplication. The multiplication of two elements is only an abstract rule for combining an ordered pair of two group elements to obtain a third group element. The difference from ordinary multiplication becomes even more apparent from the fact that the composition law need not be commutative, i.e., the product ab need not equal ba for distinct group elements a and b. If a group does have a commutative composition law, it is said to be **commutative** or **Abelian**.

Despite the somewhat abstract tone of these comments, a moment's reflection leads to the realization that the structure of groups is ideally suited to the description of symmetry in physical systems. The group elements often correspond to coordinate transformations of either geometrical objects or of equations of motion, with the composition law corresponding to matrix multiplication or the usual composition law of functions,[3] so the associativity property is guaranteed.[4] If two operations each correspond to symmetry operations, then their product clearly must as well. The identity corresponds to performing no transformation at all and the inverse of each transformation corresponds to performing the transformation in reverse, which must exist for the transformation to be well-defined (cf. Example 2.4).

Example 2.1. Consider the set of integers,

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots$$

with the composition rule being ordinary addition. The sum of any two integers is an integer, thus ensuring closure, addition is an associative operation, 0 is the identity, and the inverse of n is $-n$, which is clearly an integer. Thus, the integers form a group under addition. This group is denoted by Z (derived from the German word *Zahlen* for integers).

[3]For two functions $f(x)$ and $g(x)$, the application of f, followed by the application of g is $g[f(x)]$, and the application of g followed by the application of f is $f[g(x)]$.

[4]The associativity of linear operations in general, and matrices in particular, is discussed by Wigner in *Group Theory* (Academic, New York, 1959), along with other group properties.

Since the order in which two integers are added is immaterial, Z is an Abelian group. ∎

Example 2.2. The importance of the composition law for determining whether a set of elements forms a group can be seen by again considering the integers, but now with ordinary multiplication as the composition rule. The product of any two integers is again an integer, multiplication is associative, the unit is 1, but the inverse of n is $1/n$, which is *not* an integer if $n \neq 1$. Hence, the integers with ordinary multiplication do not form a group. ∎

Example 2.3. Consider the elements $\{1, -1\}$ under ordinary multiplication. This set is clearly closed under multiplication and associativity is manifestly satisfied. The unit element is 1 and each element is its own inverse. Hence, the set $\{1, -1\}$ is a two-element group under multiplication. ∎

Example 2.4. Consider the set of 2×2 matrices with real entries

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tag{2.1}$$

such that the determinant, $ad - bc$, is non-zero. The composition law is the usual rule for matrix multiplication:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ c_1a_2 + d_1c_2 & c_1b_2 + d_1d_2 \end{pmatrix}.$$

To determine if this set of matrices forms a group, we must first show that the product of two matrices with non-zero determinant is also a matrix with non-zero determinant. This follows from that fact that for any pair of 2×2 matrices A and B, their determinants, denoted by $\det(A)$ and $\det(B)$, satisfy $\det(AB) = (\det A)(\det B)$. Associativity can be verified with a straightforward, but laborious, calculation. The identity is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and the inverse of (2.1) is

$$\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

which explains the requirement that $ad-bc \neq 0$. This group is denoted by GL(2,$\mathbf{R}$), for *general linear* group of 2×2 matrices with real entries. Note that the elements of this group form a *continuous* set, so GL(2,$\mathbf{R}$) is a continuous group. ∎

2.2 Permutation Groups

A permutation of n objects is a rearrangement of those objects. When combined with the usual rule for function composition for successive permutations (see below), these permutations are endowed with the structure of a group, which is denoted by S_n. At one time, permutation groups were the only groups studied by mathematicians and they maintain a special status in the subject through **Cayley's theorem**, which establishes a relationship between S_n and *every* group with n elements. In this section, we will examine the structure of S_3, both as an abstract group and as the symmetry group of an equilateral triangle.

The group S_3 is the set of all permutations of three distinguishable objects, where each element corresponds to a particular permutation of the three objects from a given reference order. Since the first object can be put into any one of three positions, the second object into either of two positions, and the last object only into the remaining position, there are $3 \times 2 \times 1 = 6$ elements in the set. These are listed below:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \qquad f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

In this notation, the top line represents the initial, or reference, order of the objects and the bottom line represents the effect of the permutation. The composition law corresponds to performing successive

permutations and is carried out by rearranging the objects according to the first permutation and then using this as the reference order to rearrange the objects according to the second permutation. As an example, consider the product ad, where we will use the convention that operations are performed from right to left, i.e., permutation d is performed first, followed by permutation a. Element d permutes the reference order $(1, 2, 3)$ into $(3, 1, 2)$. Element a then permutes this by putting the first object in the second position, the second object into the first position, and leaves the third object in position three, i.e.,

$$a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 & 2 \\ 1 & 3 & 2 \end{pmatrix} .$$

Notice that it is only the permutation of the distinct objects, not their labelling, which is important for specifying the permutation. Hence,

$$ad = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = b \,,$$

An analogous procedure shows that

$$da = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = c \,,$$

which shows that the composition law is not commutative, so S_3 is a non-Abelian group.

A geometric realization of S_3 can be established by considering the symmetry transformations of an equilateral triangle (Fig. 2.1). The elements a, b, and c correspond to reflections through lines which intersect the vertices at 3, 1, and 2, respectively, and d and f correspond to clockwise rotations of this triangle by $\frac{2}{3}\pi$ and $\frac{4}{3}\pi$ radians, respectively. The effects of each of these transformations on the positions of the vertices of the triangle is identical with the corresponding element of S_3. Thus, there is a one-to-one correspondence between these transformations and the elements of S_3. Moreover, this correspondence is preserved by the composition laws in the two groups. Consider for example, the products ad and da calculated above for S_3. For the equilateral triangle, the product ad corresponds to a rotation followed by

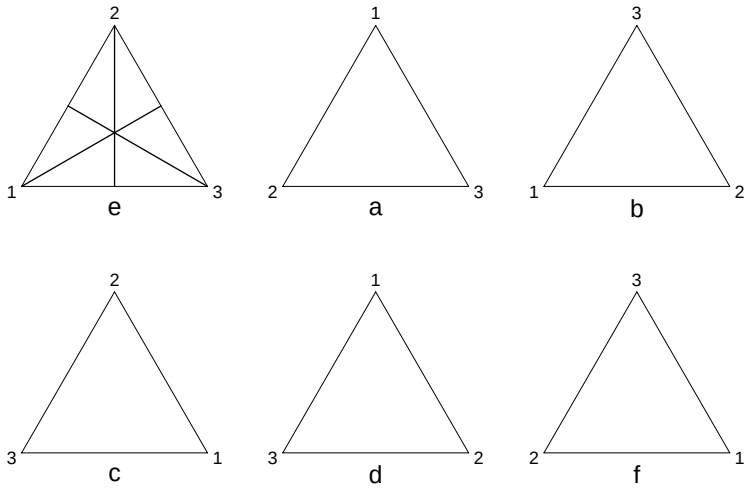
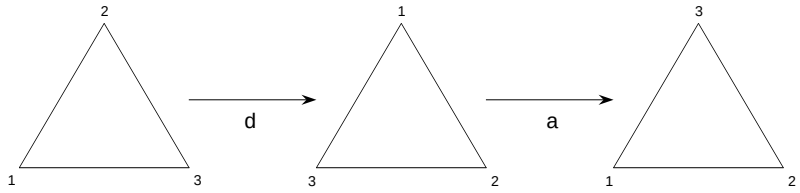


Figure 2.1: The symmetry transformations of an equilateral triangle labelled by the corresponding elements of S_3. The lines in the diagram corresponding to the identity are lines through which reflections of transformations a, b and c are taken. The transformations d and f are rotations.

a reflection. Thus, beginning with the standard order shown for the identity the successive application of these transformations is shown below:



By comparing with Fig. 2.1, we see that the result of these transformations is equivalent to the transformation b. Similarly, one can show that $da = c$ and, in fact, that all the products in S_3 are identical to those of the symmetry transformations of the equilateral triangle. Two such groups that have the same algebraic structure are said to be **isomorphic** to one another and are, to all intents and purposes, identical. This highlights the fact that it is the algebraic structure of the group

which is important, not any particular realization of the group. Further discussion of this point will be taken up in the next chapter.

2.3 Elementary Properties of Groups

The examples in the preceding section showed that all groups are endowed with several general properties. In this section, we deduce some additional properties which, although evident in particular examples, can be shown generally to follow from the properties of abstract groups.

Theorem 2.1. (Uniqueness of the identity) The identity element in a group G is unique.

Proof. Suppose there are two identity elements e and e' in G. Then, according to the definition of a group, we must have that

$$ae = a$$

and

$$e'a = a$$

for all a in G. Setting $a = e'$ in the first of these equations and $a = e$ in the second shows that

$$e' = e'e = e\,,$$

so $e = e'$. ∎

This theorem enables us to speak of *the* identity e of a group. The notation e is derived from the German word *Einheit* for unity.

Another property common to all groups is the cancellation of common factors within equations. This property owes its existence to the associativity of the group composition rule.

Theorem 2.2. (Cancellation) In a group G, the left and right cancellation laws hold, i.e., $ab = ac$ implies $b = c$ and $ba = ca$ implies $b = c$.

Proof. Suppose that $ab = ac$. Let a^{-1} be an inverse of a. Then, by left-multiplying by this inverse,

$$a^{-1}(ab) = a^{-1}(ac)$$

and invoking associativity,

$$(a^{-1}a)b = (a^{-1}a)c\,,$$

we obtain

$$eb = ec\,,$$

so $b = c$. Similarly, beginning with $ba = ca$ and right-multiplying by a^{-1} shows that $b = c$ in this case also. ∎

Notice that the proof of this theorem does not require the inverse of a group element to be unique; only the existence of *an* inverse was required. In fact, the cancellation theorem can be used to prove that inverses are, indeed, unique.

Theorem 2.3. (Uniqueness of inverses) For each element a in a group G, there is a unique element b in G such that $ab = ba = e$.

Proof. Suppose that there are two inverses b and c of a. Then $ab = e$ and $ac = e$. Thus, $ab = ac$, so by the Cancellation Theorem, $b = c$. ∎

As in the case of the identity of a group, we may now speak of *the* inverse of every element in a group, which we denote by a^{-1}. As was discussed in Sec. 2.1, this notation is borrowed from ordinary multiplication, as are most other notations for the group composition rule. For example, the n-fold product of a group element g with itself is denoted

by g^n. Similarly $g^n g^m = g^{n+m}$, which conforms to the usual rule of exponents for real numbers. However, there are some notable exceptions. For two group elements a and b, the equality of $(ab)^n$ and $a^n b^n$ does not generally hold. As the examples in Sec. 2.1 demonstrated, as long as this notation is interpreted in the context of the appropriate group composition rule, no confusion should arise.

2.4 Discrete and Continuous Groups

Groups are divided into two general categories: discrete and continuous. The basis definitions apply to both types of group, but the discussion of a number of properties depends sensitively on the discrete or continuous nature of the group. In this course, we will focus our attention on discrete groups first, to establish a conceptual base, and consider continuous groups later in the course.

2.4.1 Finite Groups

One of the most fundamental properties of a group G is number of elements contained in the group. This is termed the **order** of G and is denoted by $|G|$. The group Z of integers under addition, has infinite order and the order of S_3, the group of permutations of three objects, is 6. We will be concerned initially with *finite* groups which, apart from their applicability to a range of physical problems, have a number interesting arithmetic properties.

Finite groups also have properties which are not shared by either infinite or continuous groups. For example, if an element g of a finite group G is multiplied by itself enough times, the unit e is eventually recovered. Clearly, multiplying any element g by itself a number of times greater than $|G|$ *must* eventually lead to a recurrence of the product, since the number of distinct products is bounded from above by $|G|$. To show this explicitly, we denote a recurring product by a and write

$$a = g^p = g^q \,,$$

where $p = q + n$. Then, by using the associativity of the composition

law, $g^{q+n} = g^q g^n = g^n g^q$, so

$$g^p = g^q g^n = g^n g^q = g^q \,,$$

and, from the definition of the identity and its uniqueness, we conclude that

$$g^n = e \,.$$

Thus, the set of elements $g, g^2, g^3, \ldots$ represents a recurring sequence. The **order of an element** g, denoted by $|g|$, is the *smallest* value of k such that $g^k = e$. The **period** of such an element g is the collection of elements $\{e, g, g^2, \ldots, g^{k-1}\}$.

Example 2.5. Using S_3 as an example, $|a| = |b| = |c| = 2$ and $|d| = |f| = 3$. The corresponding periods are $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, and $\{e, d, f = d^2\}$. ∎

Theorem 2.4. (Rearrangement Theorem) If $\{e, g_1, g_2, \ldots, g_n\}$ are the elements of a group G, and if g_k is an arbitrary group element, then the set of elements

$$Gg_k = \{eg_k, g_1 g_k, g_2 g_k, \ldots, g_n g_k\}$$

contains each group element once and only once.

Proof. The set Gg_k contains $|G|$ elements. Suppose two elements of Gg_k are equal: $g_i g_k = g_j g_k$. By the Cancellation Theorem, we must have that $g_i = g_j$. Hence, each group element appears once and only once in Gg_k, so the sets G and Gg_k are identical apart from a rearrangement of the order of the elements if g_k is not the identity. ∎

2.4.2 Multiplication Tables

One application of this theorem is in the representation of the composition law for a finite group as a **multiplication table**. Such a table is a square array with the rows and columns labelled by the elements of the group and the entries corresponding to the products, i.e., the element g_{ij} in the ith row and jth column is the product of the element g_i labelling that row and the element g_j labelling that column: $g_{ij} = g_i g_j$. To see how the construction of multiplication tables proceeds by utilizing only the abstract group properties, consider the simplest nontrivial group, that with two distinct elements $\{e, a\}$. We clearly must have the products $e^2 = e$ and $ea = ae = a$. The Rearrangement Theorem then requires that $a^2 = e$. The multiplication table for this group is shown below:

	e	a
e	e	a
a	a	e

Note that the entries of this table are symmetric about the main diagonal, which implies that this group is Abelian.

Now consider the group with three distinct elements: $\{e, a, b\}$. The only products which we must determine explicitly are ab, ba, a^2, and b^2 since all other products involve the unit e. The product ab cannot equal a or b, since that would imply that either $b = e$ or $a = e$, respectively. Thus, $ab = e$. The Cancellation Theorem then *requires* that $a^2 = e$, $b^2 = a$, and $ba = e$. The multiplication table for this group is shown below:

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Because the entries of this table are symmetric about the main diagonal, this group is also Abelian. Our procedure shows that *every* group with two or three elements *must* have the multiplication tables just

calculated, i.e., the algebraic structures of group with two and three elements are *unique*! Thus, we can speak of *the* group with two elements and *the* group with three elements. A similar procedure for groups with four elements $\{e, a, b, c\}$ yields *two* distinct multiplication tables (Problem Set 2). As a final example, the multiplication table for S_3 is shown below:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	e	d	f	b	c
b	b	f	e	d	c	a
c	c	d	f	e	a	b
d	d	c	a	b	f	e
f	f	b	c	a	e	d

As is immediately evident from this table, S_3 *not* Abelian.

2.5 Subgroups and Cosets

If, from a group G, we select a subset H of elements which themselves form a group under the same composition law, H is said to be a **subgroup** of G. According to this definition, the unit element $\{e\}$ forms a subgroup of G, and G is a subgroup of itself. These are termed *improper* subgroups. The determination of *proper* subgroups is one of the central concerns of group theory. In physical applications, subgroups arise in the description of symmetry-breaking, where a term is added to a Hamiltonian or a Lagrangian which lowers the symmetry to a subgroup of the original symmetry operations.

Example 2.6. The group S_3 has a number of proper subgroups: $\{e, a\}$, $\{e, b\}$, $\{e, c\}$, and $\{e, d, f\}$. The identification of these subgroups is most easily carried out by referring to the symmetry operations of an equilateral triangle (Fig. 2.1). ∎

If $H = \{e, h_1, h_2, \ldots, h_r\}$ is a subgroup of a group G, and g is an element of G, then the set

$$Hg = \{eg, h_1g, h_2g, \ldots, h_rg\}$$

is a **right coset** of H. Similarly, the set

$$gH = \{ge, gh_1, gh_2, \ldots, gh_r\}$$

is a **left coset** of H. A coset need not be a subgroup; it will be a subgroup only if g is an element of H.

Theorem 2.5. Two cosets of a subgroup either contain exactly the same elements or else have no common elements.

Proof. These cosets either have no common elements or have at least one common element. We will show that if there is a single in common, then all elements are common to both subgroups. Let Hg_1 and Hg_2 be two right cosets. If one common element of these cosets is $h_ig_1 = h_jg_2$, then

$$g_2g_1^{-1} = h_j^{-1}h_i$$

so $g_2g_1^{-1}$ is in H. But also contained in H are the elements

$$Hg_2g_1^{-1} = \{eg_2g_1^{-1}, h_1g_2g_1^{-1}, h_2g_2g_1^{-1}, \ldots, h_rg_2g_1^{-1}\}$$

since, according to the Rearrangement Theorem, each element of H appears once and only once in this sequence. Therefore, the elements of Hg_1 are identical to those of

$$(Hg_2g_1^{-1})g_1 = Hg_2(g_1^{-1}g_1) = Hg_2$$

so these two cosets have only common elements. ∎

Example 2.7. Consider again the group S_3 and its subgroup $H = \{e, a\}$ (Example 2.6). The right cosets of this subgroup are

$$\{e, a\}e = \{e, a\}, \quad \{e, a\}a = \{a, e\}, \quad \{e, a\}b = \{b, d\}$$

$$\{e, a\}c = \{c, f\}, \quad \{e, a\}d = \{d, b\}, \quad \{e, a\}f = \{f, c\}$$

We see that there are three distinct right cosets of $\{e, a\}$,

$$\{e, a\}, \qquad \{b, d\}, \qquad \{c, f\}$$

of which only the first is a subgroup (why?). Similarly, there are three *left* cosets of $\{e, a\}$:

$$\{e, a\}, \qquad \{c, d\}, \qquad \{b, f\}$$

Notice that the left and right cosets are *not* the same. ∎

Theorem 2.6 (Lagrange's theorem). The order of a subgroup H of a finite group G is a divisor of the order of G, i.e., $|H|$ divides $|G|$.

Proof. Cosets either have all elements in common or they are distinct (Theorem 2.5). This fact, combined with the Rearrangement Theorem, means that every element of the group must appear in exactly one distinct coset. Thus, since each coset clearly has the same number of elements, the number of distinct cosets, which is called the **index** of the subgroup, multiplied by the number of elements in the coset, is equal to the order of the group. Hence, since the order of the coset and the subgroup are equal, the order of the group divided by the order of the subgroup is equal to the number of distinct cosets, i.e., an integer. ∎

Example 2.8. The subgroup $\{e, a\}$ of S_3 is of order 2 and the subgroup $\{e, d, f\}$ is of order 3. Both 2 and 3 are divisors of $|S_3| = 6$. ∎

Lagrange's theorem identifies the allowable orders of the subgroups of a given group. But the converse of Lagrange's theorem is *not* generally valid, i.e., the orders of the subgroups of a group G need not span the divisors of G.

2.6 The Quotient Group

2.6.1 Conjugacy Classes

Two elements a and b of a group G are said to be **conjugate** if there is an element g in the group, called the conjugating element, such that $a = gbg^{-1}$. Conjugation is an example of what is called an **equivalence relation**, which is denoted by "$\equiv$," and is defined by three conditions:

1. $a \equiv a$ (reflexive).
2. If $a \equiv b$, then $b \equiv a$ (symmetric).
3. If $a \equiv b$ and $b \equiv c$, then $a \equiv c$ (transitive).

To show that conjugacy corresponds to an equivalence relation we consider each of these conditions in turn. By choosing $g = e$ as the conjugating element, we have that $a = eae^{-1} = a$, so $a \equiv a$. If $a \equiv b$, then $a = gbg^{-1}$, which we can rewrite as

$$g^{-1}ag = g^{-1}a(g^{-1})^{-1} = b$$

so $b \equiv a$, with g^{-1} as the conjugating element. Finally, to show transitivity, the relations $a \equiv b$ and $b \equiv c$ imply that there are elements g_1 and g_2 such that $b = g_1 a g_1^{-1}$ and $c = g_2 b g_2^{-1}$. Hence,

$$c = g_2 b g_2^{-1} = g_2 g_1 a g_1^{-1} g_2^{-1} = (g_2 g_1) a (g_2 g_1)^{-1}$$

so c is conjugate to a with the conjugating element $g_1 g_2$. Thus, conjugation fulfills the three conditions of an equivalency class.

One important consequence of equivalence is that it permits the assembly of **classes**, i.e., sets of equivalent quantities. In particular, a **conjugacy class** is the totality of elements which can be obtained from a given group element by conjugation. Group elements in the same conjugacy class have several common properties. For example, all elements of the same class have the same order. To see this, we begin with the definition of the order n of an element a as the smallest integer such that $a^n = e$. An arbitrary conjugate b of a is $b = gag^{-1}$. Hence,

$$b^n = \underbrace{(gag^{-1})(gag^{-1})\cdots(gag^{-1})}_{n \text{ factors}} = ga^n g^{-1} = geg^{-1} = e$$

so b has the same order as a.

Example 2.9. The group S_3 has three classes: $\{e\}$, $\{a, b, c\}$, and $\{d, f\}$. As we discussed in Example 2.5, the order of a, b, and c is two, and the order of d and f is 3. The order of the unit element is 1 and is always in a class by itself. Notice that each class corresponds to a distinct kind of symmetry operation on an equilateral triangle. The operations a, b, and c correspond to reflections, while d and f correspond to rotations. In terms of operations in S_3, the elements d and f correspond to *cyclic* permutations of the reference order, e.g., $1 \rightarrow 2$, $2 \rightarrow 3$, and $3 \rightarrow 1$, while a, b, and c correspond to permutations which are not cyclic. ∎

2.6.2 Self-Conjugate Subgroups

A subgroup H of G is **self-conjugate** if the elements gHg^{-1} are identical with those of H for all elements g of G. The terms **invariant subgroup** and **normal subgroup** are also used. A group with no self-conjugate proper subgroups is called **simple**. If $gHg^{-1} = H$ for all g in G, then given an element h_1 in H, for any a, we can find an element h_2 in H such that $ah_1a^{-1} = h_2$, which implies that $ah_1 = h_2a$, or that $aH = Ha$. This last equality yields another definition of a self-conjugate subgroup as one whose left and right cosets are equal. From the definition of self-conjugacy and of classes, we can furthermore conclude that a subgroup H of G is self-conjugate if and only if it contains elements of G in complete classes, i.e., H contains either all or none of the elements of classes of G.

The cosets of a self-conjugate subgroup are themselves endowed with a group structure, with multiplication corresponding to an element-by-element composition of two cosets and discounting duplicate products. We show first that the multiplication of the elements of two right cosets of a conjugate subgroup yields another right coset. Let H be a self-conjugate subgroup of G and consider the two right cosets Ha and Hb. Then, the multiplication of Ha and Hb produces products of the form

$$h_iah_jb = h_i(ah_j)b$$

The product ah_j can be written as $h_k a$ for some h_k in H, since H is assumed to be self-conjugate. Thus, we have

$$h_i(ah_j)b = h_i(h_k a)b = (h_i h_k)(ab)$$

which is clearly an element of a right coset of H.

Example 2.10. Consider the subgroup $\{e, d, f\}$ of S_3. Right-multiplying this subgroup by each element of S_3 yields the right cosets of this subgroup:

$$\{e,d,f\}e = \{e,d,f\}, \quad \{e,d,f\}a = \{a,c,b\}, \quad \{e,d,f\}b = \{b,a,c\}$$

$$\{e,d,f\}c = \{c,b,a\}, \quad \{e,d,f\}d = \{d,f,e\}, \quad \{e,d,f\}f = \{f,e,d\}$$

Similarly, left-multiplying by each element of S_3 produces the left cosets of this subgroup:

$$e\{e,d,f\} = \{e,d,f\}, \quad a\{e,d,f\} = \{a,b,c\}, \quad b\{e,d,f\} = \{b,c,a\}$$

$$c\{e,d,f\} = \{c,a,b\}, \quad d\{e,d,f\} = \{d,f,e\}, \quad f\{e,d,f\} = \{f,e,d\}$$

Thus, since the right and left cosets of $\{e, d, f\}$ are the same, these elements form a self-conjugate subgroup of S_3 whose distinct cosets are $\{e, d, f\}$ and $\{a, b, c\}$. Multiplying these subgroups together and neglecting duplicate elements yields

$$\{e,d,f\}\{e,d,f\} = \{e,d,f\}, \quad \{e,d,f\}\{a,b,c\} = \{a,b,c\}$$

$$\{a,b,c\}\{e,d,f\} = \{a,b,c\}, \quad \{a,b,c\}\{a,b,c\} = \{e,d,f\}$$

∎

The **quotient group** (also called the **factor group**) of a self-conjugate subgroup is the collection of cosets, each being considered an element. The order of the factor group is equal to the index of the self-conjugate subgroup. With the notation used above, the quotient group is denoted by G/H.

Example 2.11. The cosets of the self-conjugate subgroup $\{e, d, f\}$ of S_3 are $\{e, d, f\}$ and $\{a, b, c\}$, so the order of the factor group is two. If we use the notation

$$\mathcal{E} = \{e, d, f\}, \qquad \mathcal{A} = \{a, b, c\} \tag{2.2}$$

for the elements of the factor group, we can use the results of Example 2.8 to construct the multiplication table for this group (shown below) from which see that $\mathcal{E}$ is the identity of the factor group, and $\mathcal{E}$ and

	$\mathcal{E}$	$\mathcal{A}$
$\mathcal{E}$	$\mathcal{E}$	$\mathcal{A}$
$\mathcal{A}$	$\mathcal{A}$	$\mathcal{E}$

$\mathcal{A}$ are their own inverses. Note that this multiplication table has the identical structure as the two-element group $\{e, a\}$ discussed in Sec. 2.4. ∎

2.7 Summary

In this chapter, we have covered only the most basic properties of groups. One of the remarkable aspects of this subject, already evident in some of the discussion here, is that the four properties that define a group, have such an enormous implication for the properties of groups, quite apart from their implications for physical applications, which will be explored throughout this course. A comprehensive discussion of the mathematical theory of groups, including many wider issues in both pure and applied mathematics, may be found in the book by Gallian.[5]

[5] J.A. Gallian, *Contemporary Abstract Algebra* 4th edn. (Houghton Mifflin, Boston, 1998).