Chapter 1

Basic Concepts of Group Theory

The theory of groups and vector spaces has many important applications in a number of branches of modern theoretical physics. These include the formal theory of classical mechanics, special and general relativity, solid state physics, general quantum theory, and elementary particle physics. Thus, I will summarize the basic concepts of group theory and vector spaces, especially for the benefit of those among you who have not had an exposure to these before. I hope you will find these useful not only for this course in classical mechanics, but for most others that you will take during you graduate studies as well.

1.1 Groups

1.1.1 Monoids

A group is a mathematical set equipped with a law of combining any two elements to produce a third element in the set. This law of combination is required to satitsfy certain crucial axioms which, over the years, have been found to produce a mathematical structure of exceptional importance and interest. One of the most significant concrete examples of group structure is associated with the family of maps of any set into itself. This specific example is in many ways paradigmatic for the entire theory of groups.

Let X and Y be any pair of sets. A *map* (or *function*) from X to Y is an assignment of a unique element of Y to each element of X. If f is such a function then we often write $f : X \to Y$ to indicate the pair of spaces X and Y involved as well as the map itself. The unique element in Y associated with a specific element x in X is denoted by $f(x)$ (or sometimes by f_x). We shall frequently deal with the family of all possible maps from X to Y and this set will be denoted $\mathrm{Map}(X, Y)$.

Note that a typical map from X to Y will be:

1. Many-to-one: more than one element in X is mapped to the same element in Y, i.e., $f(x_1) = f(x_2)$ for some x_1 and x_2.

2. Strictly "into" Y: there will, in general, be some elements y in Y for which there is *no* element x in X for which $y = f(x)$.

A map from X to Y which is both one-to-one and "onto" is called a *bijection* from X to Y. It establishes a unique correspondence between the elements of X and Y which means that, from a purely set theoretic viewpoint, these can be regarded as the "same" set. Bijections between X and Y will exist if and only if they have the same number of elements.

For our purposes, the set $\mathrm{Map}(X, X)$ of all maps of a set into itself is of special importance. This is because given $f : X \to X$ and $g : X \to X$, we can combine them to form a third element $f \cdot g : X \to X$ which is defined on any element x in X by first mapping it to $g(x)$ and then mapping this image point to $f(g(x))$. Thus $f \cdot g : X \to X$ is defined by

$$f \cdot g : X \to X \equiv f(g(x)) \qquad \text{for all } x \text{ in } X. \tag{1.1}$$

Two particularly significant properties of the set $\mathrm{Map}(X, X)$ and the law of composition "$\cdot$" are:

1. If f, g, h are three maps from X to X then

$$f \cdot (g \cdot h) = (f \cdot g) \cdot h; \tag{1.2}$$

2. The *identity* map from X onto itself is denoted by i_x and is defined in the obvious way as

$$i_x(x) \equiv x \qquad \text{for all } x \text{ in } X. \tag{1.3}$$

Then it follows that, for any function $f : X \to X$, we have

$$f \cdot i_x = i_x \cdot f = f. \tag{1.4}$$

Definitions.

1. A *law of composition* on a set A is a rule that associates with each pair of elements (a_1, a_2) (where a_1 and a_2 belong to A), a third element in A written as $a_1 a_2$.

2. The law is associative if

$$a_1(a_2 a_3) = (a_1 a_2) a_3 \qquad \text{for any } a_1, a_2 \text{ and } a_3 \text{ in } A. \tag{1.5}$$

3. an element e in A is said to be the *unit element* if

$$ae = ea = a \qquad \text{for all } a \text{ in } A. \tag{1.6}$$

4. A set is a *monoid* if it has a law of composititon that is associative and for which there is a unit element. (We shall shortly see that the idea of a monoid is a natural precursor to the concept of a group.)

Note. If such a unit element e exists, then it is unique. For if e' is any other unit, we have $e = ee' = e'$.

Examples.

1. The set of mappings $\mathrm{Map}(X, X)$ is a monoid for any set X.
2. The set of integers $\mathbb{Z}$ is a monoid if the law of composition is ordinary addition with the unit element being the number 0.
3. $\mathbb{Z}$ also is a monoid if the law of composition is defined to be ordinary multiplication. In this case, the unit element is the number 1.

Generally speaking, the "product" $a_1 a_2$ of a pair of elements a_1 and a_2 in a monoid will not be the same element as the product $a_2 a_1$. However, the monoids for which all such producs are equal are of particular importance and warrant a special definition.

Definition.
A monoid is said to be *commutative* (or *abelian*) if

$$a_1 a_2 = a_2 a_1 \text{ for all } a_1 \text{ and } a_2 \text{ in } A.$$

Examples.

1. The set of integers $\mathbb{Z}$ is an abelian monoid with regard to both monoid structures defined in the above examples.
2. In general, a monoid $\mathrm{Map}(X, X)$ is not commutative. For example, let $\mathbb{R}$ denote the real numbers. Consider $\mathrm{Map}(\mathbb{R}, \mathbb{R})$ and the two particular functions

$$f : \mathbb{R} \to \mathbb{R} \qquad f(x) \equiv x^2,$$
$$g : \mathbb{R} \to \mathbb{R} \qquad g(x) \equiv x + 1.$$

   Then $f \cdot g(x) = (x+1)^2$ whereas $g \cdot f(x) = x^2 + 1$, and of course these are not the same.
3. An important example of a monoid is provided by the set $M(n, \mathbb{R})$ of all $n \times n$ real matrices where the composition of two elements M_1 and M_2 is defined to be the conventional matrix multiplication:

$$(M_1 M_2)_{ij} \equiv \sum_{k=1}^{n} M_{1ik} M_{2kj}$$

   and the unit element is the unit matrix $\mathbf{1} \equiv \mathrm{diag}(1, 1, \ldots, 1)$. This monoid structure is clearly non-abelian and the same applies to the analogous monoid structure defined on the set $M(n, \mathbb{C})$ of all $n \times n$ complex matrices.

4. However, as in the case of integers, there is another monoid structure that can be defined on $M(n, \mathbb{R})$, and similarly on $M(n, \mathbb{C})$, which is abelian. This involves defining the composition of two matrices as the *sum* of the matrices, rather than the product. In this case, the unit element is the null matrix, i.e., the matrix whose elements are all zero.

1.1.2 The basic idea of a group

The essential difference between a monoid and a group is that, in the latter, every element has an *inverse*. This property is of fundamental significance for the applicability of group theory to physics, and is formalized in the following definition.

Definitions.

1. An element b in a monoid A is said to be an *inverse* of an element a in A if
$$ba = ab = 1. \tag{1.7}$$

2. A *group* is a monoid in which every element has an inverse.

Note. If b and b' are both inverses of a then they are equal since

$$b' = b'e = b'(ab) = (b'a)b = eb = b.$$

Thus inverses are unique and it is meaningful to speak of *the* inverse of an element a in A. The inverse of an element a is usually wrirtten as a^{-1}.

Examples.

1. The set of integers $\mathbb{Z}$ is an abelian group with respect to the monoid structure in which the composition is defined as addition. The inverse of an integer n is clearly $-n$.

   This set $\mathbb{Z}$, however, is *not* a group under the alternatitve monoid structure in which the composition is defined as multiplication, whence the inverse of an integer n would have to be $1/n$, but this is not itself an integer.

2. The set $\mathbb{Q}$ of all rational numbers is an abelian group under the law of addition.

3. The set $\mathbb{Q}_*$ of all non-zero rational numbers is an abelian group under multiplication if the inverse of the rational number n/m is defined to be the rational number m/n.

4. In the monoid $\mathrm{Map}(X, X)$, the inverse of a function $f : X \to X$ would be a function $g : X \to X$ such that $f \cdot g = g \cdot f = i_X$, i.e., $f(g(x)) = g(f(x))$ for all x in X.

   A function f will not have an inverse if it is many-to-one or if it maps strictly "into" X. Such functions will always exist whenever the set X

contains more than one element. Hence, except in that rather trivial case, $\mathrm{Map}(X, X)$ is never a group.

This property of $\mathrm{Map}(X, X)$ motivates the following, very important, definition.

Definitions.

1. A map $f : X \to X$ is said to be a *bijection* (or *permutation*) of X if
   (a) f is a one-to-one map (i.e., it is *injective*), and
   (b) f maps X onto iself (i.e., it is *surjective*).
2. Every such map has an inverse and it follows that the set $\mathrm{Perm}(X)$ of all bijections of X onto itself is a group. If N, the number of elements in X, is finite, then $\mathrm{Perm}(X)$ is often called the *symmetric group* S_N.

Note. The number of elements in a group G is called the *order* of the group and is written as $|G|$. It is easy to see that the order of S_N is $N!$.

When manipulatitng groups, it is convenient to define the "powers" of a group element g in G by $g^2 \equiv gg$, $g^3 \equiv g(g^2)$ and so on. We then say that an element g has *order* n if $g^n = e$ and n is the smallest integer with this property.

Definition.
Two groups G_1 and G_2 are said to be *isomorphic* (written as $G_1 \cong G_2$) if their elements can be put in a one-to-one correspondence in a way that preserves the group combination law.

More precisely, there must exist a bijection $j : G_1 \to G_2$ such that

$$j(ab) = j(a)j(b) \qquad \text{for all } a \text{ and } b \text{ in } G_1. \tag{1.8}$$

The map j is said to be an *isomorphism* of G_1 with G_2.

Definition.
A subset H of a group G is said to be a *subgroup* of G if

1. The identity element e of G belongs to H.
2. If h_1 and h_2 are in H, then so is the product h_1h_2. (We say that H is "closed" under the composition law of G.)
3. If h belongs to H, then so does h^{-1}. (We say that H is "closed" under inversion with the composition law of G.)

The theoretic inclusion sign $H \subset G$ is often used to denote that H is a subgroup of G.

Theorem (Cayley).
Any group G is isomorphic to a subgroup of $\mathrm{Perm}(X)$ for some choice of the set X.

1.1.3 Continuous Groups

An important class of groups is those that have an infinite number of elements (i.e., groups of infinite order) in which the infinity concerned is "continuous" rather than "countable". Groups of this type play a fundamental rorle in modern theoretical physics.

Examples.

1. The set $\mathbb{R}$ of all real numbers is an abelian group in which the group composition law is the usual addition of numbers. Note that the countably infinite groups $\mathbb{Z}$ and $\mathbb{Q}$ can be regarded as subgroups of $\mathbb{R}$.

2. The set $\mathbb{R}_+$ of positive real numbers is a continuously infinite abelian group under the law of multiplication.

3. Let $\mathbb{R}^n$ denote the product n times the abelian group $\mathbb{R}$. Thus the group elements are sets of real numbers $(r_1, r_2, \ldots, r_n)$ with the law of composition

$$(r_1, r_2, \ldots, r_n) + (r'_1, r'_2, \ldots, r'_n) = (r_1 + r'_1, r_2 + r'_2, \ldots, r_n + r'_n)$$

   and with the unit element $(0, 0, \ldots, 0)$. Note that $\mathbb{R}^n$ is an abelian group, which is why the composition law has been written as "+". It clearly has a continuously infinite number of group elements. An analogous set of remarks apply to $\mathbb{C}^n$.

4. The set U(1) of all complex numbers of modulus one is a continuously infinite abelian group under the usual multiplication law of complex numbers.

An important refinement of the notion of "continuously infinite" is the concept of *real dimension* of such a group. Roughly speaking, this is defined to be the number of real numbers that are needed to specify a group element. Thus the group $\mathbb{R}$ and $\mathbb{R}^n$ have dimension 1 and n, respectively.

Definition.
A *Lie group* of real dimension n is a set G that is

1. A group in the general sense discussed in Sec. 1.1.2.

2. A n-dimensional "differential manifold" in the sense that the points of G can be parametrized in sufficiently small regions by a set of n real numbers and that, if a second set of n coordinates is used to parametrize points in a region that overlaps the first then, on the overlap region, the either set of the parameters/coordinates must be differentiable functions of the other set.

It is also required that the group composition law, and the taking of inverses, should be "smooth" operations in the sense that

1. The coordinates of the product gg' should be differentiable functions of the coordinates of g and $g\prime$ so long as all three group elements g, g' and gg' lie in a region where a common set of coordinates can be used.

2. The coordinates of g^{-1} should be differentiable functions of the coordinates of g as long as they lie in the same coordinate region.

We will now give some important examples of Lie groups.

Examples.

1. The necessary and sufficient condition for a matrix in $M(n,\mathbb{R})$ to be invertible is that its determinant should be non-zero. This motivates the definition of the *general linear* group in n dimensions

$$\mathrm{GL}(n,\mathbb{R}) \equiv \{A \text{ in } M(n,\mathbb{R}) \text{ such that } \det(A) \neq 0.\}$$

   This is a n^2 dimensional group under matrix multiplication in which the inverse of a group element is simply its inverse as a matrix in the usual sense, and the unit element is the unit matrix $\mathbf{1}$.

   Many groups of major significance in theoretical physics appear as explicit subgroups of the general linear group.

2. The *special linear group* is a defined as

$$\mathrm{SL}(n,\mathbb{R}) \equiv \{A \text{ in } \mathrm{GL}(n,\mathbb{R}) \text{ such that } \det(A) = 1.\}$$

   It can be shown that $\mathrm{SL}(n,\mathbb{R})$ is a subgroup of $\mathrm{GL}(n,\mathbb{R})$. Indeed, $\mathrm{SL}(n,\mathbb{R})$ is itself a Lie group of dimension n^2-1.

3. Another important example is the real *orthogonal* group, which is the subgroup of $\mathrm{GL}(n,\mathbb{R})$ of all real $n\times n$ orthogonal matrices;

$$\mathrm{O}(n,\mathbb{R}) \equiv \{A \text{ in } \mathrm{GL}(n,\mathbb{R}) \text{ such that } AA^{\mathrm{T}} = \mathbf{1}\},$$

   where A^{T} denotes the transpose of the matrix A. The dimension of $\mathrm{O}(n,\mathbb{R})$ is $n(n-1)/2$.

4. The equation $AA^{\mathrm{T}} = \mathbf{1}$ implies that $\det(A) = \pm 1$. The continuous group $O(n,\mathbb{R})$ decomposes into two disjoint pieces according to the sign of $\det(A)$, which motivates the definition of the *special orthogonal group*

$$\mathrm{SO}(n,\mathbb{R}) \equiv \{A \text{ in } \mathrm{O}(n,\mathbb{R}) \text{ such that } \det(A) = 1.\}$$

   The dimension of $\mathrm{SO}(n,\mathbb{R})$ is the same as that of $\mathrm{O}(n,\mathbb{R})$, namely $n(n-1)/2$.

   The simplest non-trivial example of a special orthogonal group is $\mathrm{SO}(2,\mathbb{R})$ which is he set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfying the conditions

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{1.9}$$

and

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1. \tag{1.10}$$

Equation 1.9 is equivalent to the three equations

$$a^2 + b^2 = 1, \tag{1.11}$$

$$c^2 + d^2 = 1, \tag{1.12}$$

$$ac + bd = 0, \tag{1.13}$$

while Eq. 1.10 implies

$$ad - bc = 1. \tag{1.14}$$

It follows that

$$c = -b, \qquad d = a. \tag{1.15}$$

Without any loss of generality, we can write $a = \cos\theta$ and $b = \sin\theta$, for some (real) angle θ. So the most general form for a matrix in $\mathrm{SO}(2,\mathbb{R})$ can be written as

$$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \qquad \text{with } 0 \le \theta \le 2\pi. \tag{1.16}$$

This shows rather clearly that $\mathrm{SO}(2,\mathbb{R})$ has the topological structure of a circle, just as does the group $\mathrm{U}(1)$. In fact, these two abelian, 1-dimensional Lie groups are isomorphic with an isomorphism that maps the group element $e^{i\theta}$ in $\mathrm{U}(1)$ onto the matrix in $\mathrm{SO}(2,\mathbb{R})$ in Eq. 1.16.

5. In analogy with the real orthogonal group, the *unitary group* $\mathrm{U}(n)$ is defined for each n as

$$\mathrm{U}(n) \equiv \{A \text{ in } \mathrm{GL}(n,\mathbb{C}) \text{ such that } AA^\dagger = \mathbf{1}\},$$

where $A^\dagger$ denotes the adjoint of the matrix A and is defined as $(A^\dagger)_{ij} \equiv A^*_{ji}$, where A^*_{ij} is the complex conjugate of the matrix element A_{ij}. $\mathrm{U}(n)$ is a n^2-dimensional subgroup of $\mathrm{GL}(n,\mathbb{C})$. It is non-abelian for $n > 1$.

6. A group that plays a central role in the classification of elementary particles and in the construction of grand unified theories is the *special unitary group* defined for each n as

$$\mathrm{SU}(n) \equiv \{A \text{ in } \mathrm{U}(n) \text{ such that } \det(A) = 1.\}$$

$\mathrm{SU}(n)$ is a subgroup of $\mathrm{U}(n)$, and has a dimension of $n^2 - 1$.

A concrete realization of $\mathrm{SU}(2)$ in the general matrix form (with the usual matrix muliplication being the law of composition) is given by

$$A = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix} \qquad \text{with } |a|^2 + |b|^2 = 1. \tag{1.17}$$

Topologically speaking, the group $\mathrm{SU}(2)$ is a 3-sphere embedded in the real 4-dimensional Cartesian space $\mathbb{R}^4$ with coordinates $\mathrm{Re}(a)$, $\mathrm{Im}(a)$, $\mathrm{Re}(b)$, $\mathrm{Im}(b)$.