

Chapter 1

The Basics

Def: A *group* is a pair (G, \circ) , where G is a set, and \circ is a binary operation (“multiplication”) defined on G such that:

1. G is closed under \circ :

$$a \circ b \in G \quad \forall a, b \in G.$$

2. \circ is associative:

$$(a \circ b) \circ c = a \circ (b \circ c) \quad \forall a, b, c \in G.$$

3. \exists a right identity element, $e \in G$, such that:

$$a \circ e = a \quad \forall a \in G.$$

4. For some right identity e , \exists for each $a \in G$ at least one right inverse, $a^{-1} \in G$, such that

$$a \circ a^{-1} = e.$$

We say “ (G, \circ) is a group”, or simply, “ G is a group.” The operation, \circ , is referred to as the group multiplication, or, simply, multiplication.

Some examples to illustrate this definition:

- The set of integers under addition is a group (denoted Z).
- The set of people is not a group (need an operation).
- The set of non-singular 2×2 matrices under matrix multiplication is a group (denoted $GL(2)$, for “general linear group in 2 dimensions”).

There are several immediate consequences of the group axioms:

Theorem: If $x \in G$ and $x \circ x = x$, and if e is a right identity such that property (4) holds, then $x = e$.

Proof:

$$\begin{aligned}
 x &= x \circ e && e = \text{right identity} \\
 &= x \circ (x \circ x^{-1}) && \text{property (4)} \\
 &= (x \circ x) \circ x^{-1} && \text{associativity} \\
 &= x \circ x^{-1} && \text{by assumption} \\
 &= e && \text{property (4)}
 \end{aligned}$$

QED

Theorem: The right inverse is also a left inverse: If (G, \circ) is a group with identity e , and $a \circ a^{-1} = e$, then $a^{-1} \circ a = e$.

Proof: Let $f = a^{-1} \circ a$. Then:

$$\begin{aligned}
 f \circ f &= (a^{-1} \circ a) \circ (a^{-1} \circ a) \\
 &= a^{-1} \circ (a \circ (a^{-1} \circ a)) && \text{associativity} \\
 &= a^{-1} \circ ((a \circ a^{-1}) \circ a) && \text{associativity} \\
 &= a^{-1} \circ (e \circ a) && \text{right inverse} \\
 &= (a^{-1} \circ e) \circ a && \text{associativity} \\
 &= a^{-1} \circ a && \text{right identity} \\
 &= f && \text{assumption} \\
 &= e && \text{previous theorem}
 \end{aligned}$$

QED

Hence, we may drop the “right” and simply say “inverse”.

Several other properties can also be quickly proven:

Theorem: The right identity is unique.

Theorem: The right identity is also a left identity.

Theorem: The inverse is unique.

Theorem: The solutions to $a \circ x = b$ and to $x \circ a = b$, where $a, b \in G$ exist ($x \in G$), and are unique.

Theorem: The inverse of a product $a \circ b$ is:

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

This may be readily extended to higher order products.

We usually drop the explicit notation for the group multiplication, and use concatenation to denote multiplication, unless doing so would be unclear.

Some important groups have an additional property:

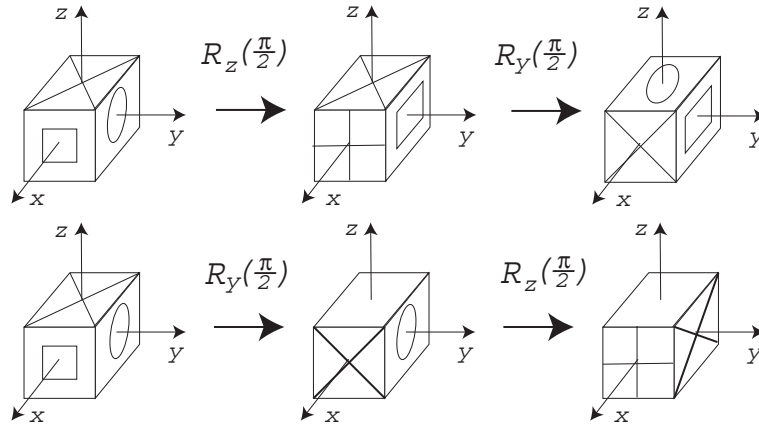


Figure 1.1: Illustration that the result of successive rotations in three dimensions depends on the order of the rotations.

Def: If G is a group such that

$$ab = ba \quad \forall a, b \in G,$$

then G is called an *abelian*, or *commutative*, group.

For example, Z is an abelian group. $GL(2)$ is a non-abelian group:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

For a more “physically relevant” example, the group of rotations in two dimensions is abelian, but the group of rotations in three dimensions is non-abelian:

$$R_z(\pi/2)R_y(\pi/2) \neq R_y(\pi/2)R_z(\pi/2).$$

See Fig. 1.

Some groups are almost trivial:

Def: If G is a group such that the powers of one element generate the group, then the group is called *cyclic*:

$$a, a^2, a^3, \dots, a^n = e.$$

For example, the group $Z_n = \{0, \dots, n-1\}$ under modulo n addition is a cyclic group. The powers of 1 generate the group, with $1^n = 0 = e$. Obviously, a cyclic group is also abelian.

The number of elements in a group is an important basic parameter:

Def: If there are a finite number, n , of elements in a group, then it is said to be a *finite group*, of order n . Otherwise, it is an *infinite group*.

For an infinite group, the infinity may be denumerable (for example, Z), or non-denumerable (for example, $GL(2)$) For a finite group, we may explicitly give a multiplication table, or *Cayley table*, as a table with n columns and n rows. For example consider a group of order five, with elements a, b, c, d , and e , where e is the identity. A possible multiplication table for such a group is:

Table 1.1: An example of a multiplication table for a group of order five. The row labels indicate the left multiplicand and the column labels the right multiplicand. Thus, for example, the product $db = a$ may be found in the last row of the table.

L \ R	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

We can remark several things concerning this table:

- By the uniqueness of the solution to $ax = b$, the multiplication table must be a Latin square – every element occurs exactly once in each row or column. This is a statement of the so-called “rearrangement lemma”: If $pb = pc$, then $b = c$.
- Since our example is symmetric about the diagonal, it specifies an abelian group.
- Noting that $b = a^2$, $c = ab = a^3$, $d = ac = a^4$, and $e = ad = a^5$, we see that this is a cyclic group.
- Finally, we may remark that there exists no group of order five which is not cyclic. In fact, we have given the only group multiplication table for order five, up to renaming of the elements.

1.1 Permutation Group

We introduce here a very important class of groups, known as the *permutation* or *symmetry* groups. We denote by S_n the group of all possible permutations or rearrangements of n objects. As there are $n!$ ways of rearranging n objects (taken to be distinct), S_n is a group of order $n!$.

Let us develop some of the notational tools used in discussing S_n . We imagine that we have a set of n “slots”, arranged in a line, into which we are going to place our n objects, one per slot. For example, we use the array:

$$(1, 2, 3, \dots, n) \quad (1.1)$$

to denote that object “1” is in the first slot (the first position in the array), object “2” is in the second slot, etc. A permutation of these objects may be written as

$$p = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ p_1 & p_2 & p_3 & \dots & p_n \end{pmatrix}. \quad (1.2)$$

In this case, object “1” in slot one has been replaced by object “ p_1 ”, object “2” in slot two has been replaced by object “ p_2 ”, etc.

The identity element is just to “do nothing”:

$$e = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}. \quad (1.3)$$

The inverse of element p above is:

$$p^{-1} = \begin{pmatrix} p_1 & p_2 & p_3 & \dots & p_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix}. \quad (1.4)$$

That is, we have the product $e = p^{-1}p$:

$$p^{-1}p = \begin{pmatrix} p_1 & p_2 & p_3 & \dots & p_n \\ 1 & 2 & 3 & \dots & n \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ p_1 & p_2 & p_3 & \dots & p_n \end{pmatrix}. \quad (1.5)$$

This notation is a bit more cumbersome than we need, since we don’t really need to keep track of the slots, only what objects are replacing which other objects. For example, consider the permutation in S_5 :

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}. \quad (1.6)$$

In this case, object one is being replaced by object 4, which is being replaced by object two, and object two is being replaced by object one. Also, objects 3 and 5 are being switched. We could write this as $(1 \rightarrow 4 \rightarrow 2 \rightarrow 1)$ and $(3 \rightarrow 5 \rightarrow 3)$. We call these sub-rearrangements “cycles”, and shorten the notation to $p = (142)(35)$. Permutation p consists of a “3-cycle” and a “2-cycle”. Note that $(142) = (214)$, but (142) is not the same as (124) . The inverse permutation is:

$$p^{-1} = \begin{pmatrix} 4 & 1 & 5 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = (412)(35) = (124)(35). \quad (1.7)$$

We may check in cycle notation:

$$pp^{-1} = [(142)(35)][(124)(35)] = e \quad (1.8)$$

For example, in the first operation, object 1 is replaced by object 2. In the second operation, object 2 is replaced by object 1, putting object 1 back into its original position. On final simplification in notation – we may drop the “one-cycles” as understood, for example:

$$(123)(4)(5)(6) = (123). \quad (1.9)$$

As an example, the reader is encouraged to construct the following multiplication table for S_3 . Notice that this is a non-abelian group.

Table 1.2: The multiplication table for permutation group S_3 .

L \ R	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

The reader is cautioned that different conventions exist for the notation for the elements of the symmetry groups. Here, I adopt the convention of Wu-Ki Tung and of Hamermesh; and not that of Mathews & Walker.

This concludes our introduction to the most basic elements of group theory. We now proceed to slightly more sophisticated notions.

1.2 Classes

We first introduce the idea of equivalence of two elements of a group:

Def: Given a group G , two elements $a, b \in G$ are said to be *equivalent* if there exists an element $u \in G$ such that

$$u^{-1}au = b. \quad (1.10)$$

The equivalence of two elements is denoted $a \sim b$.

We remark that this defines a true equivalence relation, since the following properties of an equivalence are satisfied:

1. Reflexivity: $a \sim a$, $\forall a \in G$. To see this, simply take $u = e$.
2. Symmetry: If $a \sim b$, then $b \sim a$. Since, if $u^{-1}au = b$, then $a = v^{-1}bv$, where $v = u^{-1}$.

3. Transitivity: If $a \sim b$, and $b \sim c$, then $a \sim c$. The reader should verify this.

If we consider groups of operators, the equivalence of two group elements may be described as: If you first “do u ”, then “do a ” and finally “undo u ”, and the result of all this is the operation b , then a and b are equivalent. More concretely, consider the group of all rotations in three dimensions. A rotation by 45° about the x -axis is equivalent to a rotation by 45° about the y axis. To see this, take u to be a rotation about the z -axis by 90° :

$$R_x(45^\circ) = R_z(-90^\circ)R_y(45^\circ)R_z(90^\circ). \quad (1.11)$$

More generally, any two rotations by the same angle are equivalent. This gives a nice intuitive feel for what equivalence means: Since we can find a rotation relating any two given axes of rotations, rotations by the same angle about these two axes are equivalent. We remark that in the future we will consider smaller groups of rotations which may not contain the necessary rotation from one axis to another. In this case the rotations by the same angle will no longer be equivalent.

The notion of equivalence will permit a great simplification in the study of group structure, through the use of equivalence classes:

Def: The subsets of G consisting of elements of G which are equivalent to each other are called the *classes* of G .

Some remarks are in order:

1. The simplification we will achieve will be attained through the treatment of a class as a single object, where the distinctions among its members is (often) unimportant.
2. Different classes of a group are, by transitivity, disjoint sets. Every element of the group belongs to some class, that is, the union of all classes is the entire group.
3. The identity element is always in a class by itself, since

$$u^{-1}eu = e, \quad \forall u \in G. \quad (1.12)$$

4. In an abelian group, every element is in a class by itself, since in this case

$$u^{-1}au = a, \quad \forall u \in G. \quad (1.13)$$

1.3 Subgroups

Another important concept in the study of group structure is the possibility that a group may contain other groups as subsets:

Def: If (G, \circ) is a group, and $S \subset G$ is a non-empty subset of G , such that (S, \circ) is a group, then S is called a *subgroup* of G .

For example, $\{e\}$ is a subgroup of G , and G itself is a subgroup of G . A subgroup which is neither of these “trivial” cases is referred to as a *proper subgroup* of G . For a more interesting example, consider once again the group of all rotations in three dimensions. Pick any axis. The set of all rotations about the chosen axis is a proper subgroup of the entire rotation group.

For finite groups there is an important theorem concerning the order of subgroups:

Theorem: (Lagrange) The order of a subgroup of a finite group is a divisor of the order of the group.

Thus, any group of prime order has only two subgroups, $\{e\}$ and G , and no proper subgroups. For example, consider the group of rotations about a given axis by angles $2\pi(m/n)$, where $n > 1$ is a prime number, and $m = 0, 1, \dots, n-1$. This group is of prime order, hence has no proper subgroups according to the theorem. The reader should quickly verify that this is indeed the case.

The proof of Lagrange’s theorem is instructive, and introduces some additional concepts:

Proof: Consider group G of order $g < \infty$, and subgroup H of order h . If $H = G$, then the theorem is trivially satisfied, with $h = g$.

Suppose $H \neq G$. Let a be an element in G that is not in H . Denote the elements of H by

$$e = H_1, H_2, H_3, \dots, H_h. \quad (1.14)$$

Form the products

$$\{ae = a, aH_2, aH_3, \dots, aH_h\} = “aH” = \{aH_i | i = 1, 2, \dots, h\}. \quad (1.15)$$

Each product must be distinct, since if $aH_i = aH_j$ then $a^{-1}(aH_i = aH_j)$ yields $H_i = H_j$. Furthermore, no product aH_i is contained in H , since if $aH_i \in H$ for some i , then $(aH_i)H_i^{-1} = a \in H$ (since $H_i^{-1} \in H$). But $a \notin H$ by assumption.

Thus, we have two disjoint sets of h distinct elements, H and aH , which are contained in G . If $\{z | z \in H \text{ or } z \in aH\} = G$, then $g = 2h$, and the theorem holds. Otherwise, there must be an element $b \in G$ such that $b \notin H$ and $b \notin aH$. In this case, we proceed as before, forming the set

$$bH = \{bH_i | i = 1, 2, \dots, h\}, \quad (1.16)$$

again finding that bH and H are disjoint sets.

Furthermore, aH and bH are disjoint sets, since if $aH_i = bH_j$ for some i and j , then $aH_iH_j^{-1} = bH_jH_j^{-1} = b \in aH$. But $b \notin aH$ by assumption. If the sets H , aH , and bH comprise all of the elements of G then $g = 3h$ and the theorem holds. Otherwise, we repeat the process of finding disjoint

subsets with h elements each, until we have exhausted the elements of G . Thus, G is the sum of a finite number of distinct sets containing h elements each:

$$G = H + aH + bH + \dots + kH, \quad (1.17)$$

and hence $g = mh$ where m is an integer (called the **index** of the subgroup H under the group G). This completes the proof.

The sets of elements of the form aH , where $a \in G$ and H is a subgroup of G are called the **left cosets** of H in G . We could just as easily have proven the theorem using **right cosets**, that is sets of the form Ha .

We may note that for a finite group G , any element a will have some lowest power p , called its **order**, such that $a^p = e$. This is true because the sequence a, a^2, a^3, \dots cannot continue to generate new elements for a finite group; it must eventually repeat. The sequence $a, a^2, a^3, \dots, a^p = e$ is called the **period** of a . Notice now that the period of a is the smallest subgroup of G which contains a . Since it is a subgroup, the order of a must be a divisor of the order of G , for any finite group G . Thus, we find in particular that any finite group of prime order *must* be a cyclic group (and hence also abelian).

It is useful to keep in mind these facts as we examine the structure of groups.

Def: If a subgroup $S \subset G$ is such that

$$g^{-1}Sg = S, \quad \forall g \in G, \quad (1.18)$$

then S is called an **invariant subgroup** of G .

The notation Sg , where S is a set of elements and g is an element, means the set of elements obtained by multiplying every element of S by g . An invariant subgroup consists of classes – if it contains part of a class, it must contain the entire class. For example, any subgroup of an abelian group is an invariant subgroup. For an invariant subgroup we also have that:

$$gS = Sg, \quad \forall g \in G. \quad (1.19)$$

That is, the left and right cosets of S in G are identical.

To get a better intuition into the notion of an invariant subgroup, the reader should ponder the following examples of subgroups of the rotation group:

1. Consider the group of all proper and improper rotations (that, is, we include the spatial inversion, or parity operator, \mathcal{P}). The group of all proper rotations is an invariant subgroup of this group.
2. Consider the group of all (proper) rotations. The subgroup of all rotations about a specified axis is not an invariant subgroup.

Finally, the concepts of “simple” and “semi-simple” groups will be useful in the classification of groups in terms of basic subgroup structure:

Def: A group is called *simple* if it does not contain any proper invariant subgroups. A group is called *semi-simple* if it does not contain any abelian invariant subgroups.

1.4 Some Groups

We'll conclude this chapter with a table of some groups that we encounter frequently:

Symbol	Elements	Operation
Z	integers	addition
Z_n	$0, 1, \dots, n - 1$	addition, modulo n
Q	rationals	addition
Q^*	rationals, except 0	multiplication
R	reals	addition
R^*	reals, except 0	multiplication
C	complex	addition
C^*	complex, except 0	multiplication
S	complex on unit circle	multiplication
S_n	n th roots of unity	multiplication
S_n	permutations of n objects	successive permutations
$GL(n)$	non-singular complex $n \times n$ matrices	matrix multiplication
$GL(nR)$	non-singular real $n \times n$ matrices	matrix multiplication
$SL(n)$	$GL(n)$ with determinant one	matrix multiplication
$U(n)$	$n \times n$ unitary matrices	matrix multiplication
$SU(n)$	$U(n)$ with determinant one	matrix multiplication
$O(n)$	$n \times n$ real unitary matrices	matrix multiplication
$SO(n) \equiv O^+(n)$	$O(n)$ with determinant one	matrix multiplication

The “ G ” in the symbols stands for “general”, the “ L ” is for “linear”, the “ U ” is for “unitary”, and the “ O ” is for “orthogonal”. For the matrix groups, the “ S ” is for “special”, and means determinant one.

1.5 Exercises

- Which of the following define groups? If not a group, give at least one axiom which is violated.
 - The set of all real numbers, excluding zero, under division. That is, if a and b are non-zero real numbers, the proposed binary group operation is $c = a \circ b \equiv a/b$.
 - The set of all Hermitian $n \times n$ matrices, under matrix multiplication.
 - The set of all Hermitian $n \times n$ matrices, under matrix addition.
 - The set of all operations (rotations and reflections) which leave a tetrahedron invariant. For convenience, you may wish to imagine a coordinate system in which the origin is at the “center” of the tetrahedron (this is a “fixed” point under the symmetry operations).
- Prove the five theorems stated at the bottom of page 2.

3. Write down the multiplication table, using cycle notation, for symmetry group S_4 . You don't need to do the whole table if you find it too tedious, but at least do all columns, and enough rows to show an example of each cycle structure.
4. Decompose symmetry group S_4 into classes.
5. List all of the proper subgroups of symmetry group S_4 .
6. Find all of the invariant subgroups of symmetry group S_4 .