

## Chapter 2

### Basic Group Theory

**Problem 2.1** Prove that the identities (i)  $e^{-1} = e$ , (ii)  $a^{-1}a = e$ , and (iii)  $ea = a$  for all  $a \in G$  follow from the basic axioms of Definition 2.1.

**SOLUTION:** (i) Since  $e \in G$ , it follows from Definition 2.1-(iii) that  $e$  has an inverse, say  $e^{-1} \in G$ , such that

$$ee^{-1} = e.$$

Multiply both sides of this equation by  $e^{-1}$  from the left:

$$e^{-1}(ee^{-1}) = e^{-1}e.$$

Using associativity, rewrite this as:

$$(e^{-1}e)e^{-1} = e^{-1}e.$$

But  $ae = a$ , for all  $a \in G$ . In particular, this is true for  $e^{-1}$ :

$$e^{-1}e^{-1} = e^{-1}.$$

Furthermore,  $e^{-1}$  has an inverse, call it  $(e^{-1})^{-1}$ , such that  $(e^{-1})(e^{-1})^{-1} = e$ . Multiplying both sides of the above equation on the right by this inverse yields:

$$(e^{-1}e^{-1})(e^{-1})^{-1} = e.$$

Using associativity once more:

$$e^{-1}(e^{-1}(e^{-1})^{-1}) = e,$$

or

$$e^{-1} = e.$$

(ii) Definition 2.1-(iii) states that for all  $a \in G$  there is an  $a^{-1} \in G$ , such that

$$aa^{-1} = e.$$

Multiply both sides on the left by  $a^{-1}$  to get

$$a^{-1}(aa^{-1}) = a^{-1}.$$

Using associativity

$$(a^{-1}a)a^{-1} = a^{-1}.$$

Multiply both sides on the right by  $(a^{-1})^{-1}$  to get

$$a^{-1}a = e$$

for all  $a \in G$ .

(iii) Starting with the equation we just proved, multiply both sides on the left by  $a$ :

$$a(a^{-1}a) = a.$$

Using associativity, rewrite this as

$$(aa^{-1})a = a,$$

and now Definition 2.1-(iii) yields

$$ea = a.$$

■

**Problem 2.2** Show that there is only one group of order three, using a step-by-step procedure to construct the group multiplication table.

**SOLUTION:** Let  $G = \{e, a, b\}$  — with the implicit assumption  $e \neq a \neq b$  — and define an operation denoted by juxtaposition such that  $G$  equipped with this operation is a group.

The trivial part of the multiplication table is:

$$\begin{array}{ccc} e & a & b \\ a & & \\ b & & \end{array}$$

The Rearrangement Lemma implies that the entries in a row or column of a multiplication table are distinct, i.e. any element of the group appears only once in any given row or column. It follows that there is only one possibility for the completion of the second row:  $a^2 = b$  which implies  $ab = e$ . (The other choice  $a^2 = e$  implies  $ab = b$  and then  $b$  would appear twice in column three).

The table so far looks like this:

$$\begin{array}{ccc} e & a & b \\ a & b & e \\ b & & \end{array}$$

Requiring that the elements in the second and third columns be distinct leads uniquely to the completed table:

$e$	$a$	$b$
$a$	$b$	$e$
$b$	$e$	$a$

Therefore, there is a unique way to construct the multiplication table of a group of order three; this implies that, up to isomorphism, the group  $G$  of order three is unique. ■

**Problem 2.3** Construct the multiplication table of the permutation group  $S_3$  using the cycle structure notation. (The geometrical interpretation represented by Fig. 2.2 should be of great help).

**SOLUTION:** Let me introduce a graphical way of representing permutations of  $n$  objects:

Draw  $n$  evenly spaced dots, much like this:

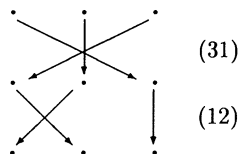


They represent  $n$  positions each holding one of  $n$  distinguishable objects, which, for obvious reasons, are not shown.

A permutation consists of moving the  $n$  objects to new positions. This is denoted by drawing a new series of dots under the first one and drawing an arrow pointing from the old location to the new one. For example, the permutation (12) among three objects would look something like this:



To compute the product of two permutations, remember that permutations are operations. The product (12)(123) is a composition: it instructs you to apply (123) first and then apply (12) to the result. Let's compute (31)(12):



To obtain the result, go to the top row, and, starting at position 1, trace the arrows to the bottom row:

$$1 \longrightarrow 3 \longrightarrow 3.$$

In —incomplete— cycle structure notation:  $(13\cdots)$ . Go back to the top row; trace the arrows starting at position 3, in order to figure out where the object that used to be in position 3 ends up.

$$3 \rightarrow 1 \rightarrow 2.$$

Since these are permutations among three objects, we are done:

$$(12)(31) = (132)$$

The above notation has numerous advantages:

- It works equally well for arbitrary  $n$ , as opposed to the geometrical interpretation such as that of Fig. 2.2 which gets rather tedious as  $n$  gets large.
- The nature of permutations as operations is made explicit.
- Computing long strings of compositions is much easier this way — compare with the cycle structure notation.

As practice, establish the following three results that will prove useful in the following:

$$\begin{aligned} (31)(12) &= (123) \\ (23)(12) &= (321) \\ (123)(12) &= (31) \end{aligned}$$

The trivial part of the multiplication table with the above three results is:

$e$	$(12)$	$(23)$	$(31)$	$(123)$	$(321)$
$(12)$	$e$				
$(23)$	$(321)$	$e$			
$(31)$	$(123)$		$e$		
$(123)$	$(31)$			$(312)$	$e$
$(321)$				$e$	$(123)$

It immediately follows that  $(321)(12) = (23)$  — no other choices.

At this point, it would be fairly easy to explicitly calculate all the remaining elements. However, it is more instructive to proceed in a deductive manner — we will have an opportunity to see how tight the group structure is.

Using these results, we can find all operations whose result is  $(12)$ . For example:

$$(321) = (23)(12)$$

which implies that

$$\begin{aligned} (23)(321) &= (23)(23)(12) \\ &= e(12) \\ &= (12). \end{aligned}$$

Similarly,

$$\begin{array}{lll} (123) = (31)(12) & \text{implies} & (31)(123) = (12) \\ (31) = (123)(12) & \text{implies} & (321)(31) = (12) \\ (23) = (321)(12) & \text{implies} & (123)(23) = (12) \end{array}$$

The partially completed table is:

$e$	$(12)$	$(23)$	$(31)$	$(123)$	$(321)$
$(12)$	$e$				
$(23)$	$(321)$	$e$			$(12)$
$(31)$	$(123)$		$e$		
$(123)$	$(31)$	$(12)$		$(312)$	$e$
$(321)$	$(23)$		$(12)$	$e$	$(123)$

Furthermore, observe:

- $(123)(31)$  can only be equal to  $(23)$  — the only element of the group that does not already appear in row five.
- Similarly, we have:  $(321)(23) = (31)$ .
- $(23)(123)$  cannot be equal to  $(123)$ ; so  $(23)(123) = (31)$ . This, in turn, implies that  $(23)(31) = (123)$  and  $(12)(31) = (321)$ .
- Similarly,  $(12)(123) = (23)$ , which implies  $(31)(123) = (12)$ .
- Again,  $(31)(321)$  cannot be  $(31)$ , so it is  $(23)$ , which implies the following:  $(31)(23) = (321)$ ,  $(12)(321) = (13)$  and, finally,  $(12)(23) = (123)$

The complete  $S_3$  multiplication table is:

$e$	$(12)$	$(23)$	$(31)$	$(123)$	$(321)$
$(12)$	$e$	$(123)$	$(321)$	$(23)$	$(13)$
$(23)$	$(321)$	$e$	$(123)$	$(31)$	$(12)$
$(31)$	$(123)$	$(321)$	$e$	$(12)$	$(23)$
$(123)$	$(31)$	$(12)$	$(23)$	$(312)$	$e$
$(321)$	$(23)$	$(31)$	$(12)$	$e$	$(123)$

■

**Problem 2.4** Show that every element of a group belongs to one and only one class, and the identity element forms a class by itself.

SOLUTION: Let  $[a]$  stand for the equivalence class of  $a$ , i.e.

$$[a] = \{g \in G : g \sim a\}$$

- (i) A statement equivalent to the one we are supposed to prove states:

Two equivalence classes are either disjoint or identical.

If  $[a]$  and  $[b]$  are disjoint there is nothing to prove. Otherwise, there exists a  $p \in G$  such that  $p \in [a]$  and  $p \in [b]$ ; our goal is to show  $[a] = [b]$ . Indeed:

For all  $q \in [a]$  we have  $p \sim q$ ; but  $p \sim b$  and transitivity implies that  $q \sim b$ , that is,  $q \in [b]$ , for all  $q \in [a]$ . This proves

$$[a] \subseteq [b].$$

Similarly,  $p \sim q'$  for all  $q' \in [b]$ ; but  $p \sim a$ . Transitivity implies that  $q' \in [a]$ , and this yields

$$[b] \subseteq [a].$$

These two imply that  $[a] = [b]$ , which completes the proof of the first statement.

(ii) Consider the equivalence class of  $e$ . Let  $p \in [e]$ ; then there exists a  $g \in G$  such that  $p = geg^{-1}$ , by the very definition of the equivalence relation. But this implies  $p = gg^{-1} = e$ . Therefore, all the  $p \in [e]$  are identity elements, and uniqueness of the identity implies that  $[e] = \{e\}$ . ■

**Problem 2.5** Enumerate the subgroups and classes of the group  $S_4$ . Which of the subgroups are invariant ones? Find the factor groups of the invariant subgroups.

SOLUTION: The group  $S_4$  is:

$$S_4 = \{e, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (124), (132), (134), (142), (143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432)\}.$$

It has five conjugacy classes:

$$\begin{aligned} &\{e\}, \\ &\{(12), (13), (14), (23), (24), (34)\}, \\ &\{(12)(34), (13)(24), (14)(23)\}, \\ &\{(123), (124), (132), (134), (142), (143), (234), (243)\}, \\ &\{(1234), (1243), (1324), (1342), (1423), (1432)\}. \end{aligned}$$

It is of order 24, so it can only have proper subgroups of orders 2,3,4,6,8 and 12. In addition to the two trivial ones— $S_4$  itself and  $\{e\}$ —some of the subgroups are:

- One invariant subgroup of order twelve, isomorphic to the tetrahedral group.

$$T = \{e, (12)(34), (13)(24), (14)(23), (123), (124), (132), (134), (142), (143), (234), (243)\}.$$

- The following subgroup of order eight is isomorphic to the dihedral group of Problem 2.8.

$$D_4 = \{e, (1234), (13)(24), (1432), (13), (12)(34), (24), (14)(23)\}.$$

- Four subgroups of order six, all isomorphic to  $S_3$ . Indeed they are the groups of permutations of any three of the four objects, leaving the fourth invariant.
- Three subgroups of order four are isomorphic to  $C_4$ , the cyclic group of order four. They are groups of the form  $\{e, g, g^2, g^3\}$  with  $g$  any 4-cycle.
- However, there is only one invariant subgroup of order four:

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$$

known as Klein's 4-group.

- Four subgroups of order three, of the form  $\{e, g, g^2\}$  with  $g$  any 3-cycle.
- Six of the subgroups of order two are of the form  $\{e, (ij)\}$ . Three more are obtained by considering  $\{e, (ij)(kl)\}$ .

This list of subgroups is not necessarily complete. However, we have found all the invariant ones:  $T$  and  $V_4$ .

The factor groups are:

- $S_4/T = \{T, (ij)T\}$  with  $(ij)$  any 2-cycle. This factor group is isomorphic to  $C_2$ .
- $S_4/V_4 = \{V_4, (12)V_4, (23)V_4, (13)V_4, (123)V_4, (321)V_4\}$ , isomorphic to  $S_3$ .

■

**Problem 2.6** *Let  $H$  be any subgroup of  $G$ , which is not necessarily invariant. Is it possible to define products of left cosets directly by the equation  $pH \odot qH = (pq)H$ , hence obtain a "factor group" consisting of left cosets? Apply this definition to the special case of  $H = \{e, (12)\}$  for  $S_3$ , and point out logical difficulties if there are any.*

**SOLUTION:** The definition of a group requires the existence of a *well defined* operation that associates an ordered pair of elements of the underlying set  $G$  with another one in the same set. This "association" is a mapping between two sets:

- The set of all ordered pairs of elements of  $G$ , denoted by  $G \times G$  and called the Cartesian product set,

and

- $G$ .

The shorthand notation for all this is

$$\odot : G \times G \longrightarrow G$$

There is also a notation to explicitly display the action of a mapping by showing its result on a pair of elements:

$$\odot : (a, b) \longrightarrow c$$

for  $a, b, c \in G$ .

For a mapping to be well-defined, each element of the domain must have a *unique* image. To be more specific, suppose  $a = b \in G$ . Then, given an element  $c \in G$ , it must be true that  $a \odot c = b \odot c$ , where we have used the more familiar infix notation for the group operation. This is exactly the requirement that our “definition” fails to meet, as we shall presently show.

First some more notation: Let  $L_H$  denote the set of all left cosets of  $H$ , i.e.

$$L_H = \{X \subseteq G : X = gH, \forall g \in G\}$$

Define a binary operation that combines two elements of  $L_H$  and produces another one, or, in symbols:

$$\odot : L_H \times L_H \longrightarrow L_H$$

by

$$pH \odot qH \longmapsto (pq)H$$

We must investigate whether this operation is *well defined*.

Let's suppose that  $H$  is not an invariant subgroup. Then, there exists a  $p \in G$  such that  $pHp^{-1} \neq H$ , which implies that there exists an  $h \in H$  such that  $php^{-1}$  does not belong to  $H$ . For these special  $p, h$  we have:

$$\begin{aligned} (pH) \odot [(hH) \odot (p^{-1}H)] &= (pH) \odot (hp^{-1})H \\ &= (php^{-1})H. \end{aligned}$$

Since  $php^{-1}$  does not belong to  $H$ , it follows that:

$$(php^{-1})H \neq H.$$

Furthermore,  $h \in H$ , which implies that  $hH = eH$ , by the rearrangement lemma. So,  $(pH) \odot [(hH) \odot (p^{-1}H)]$  must be equal to  $(pH) \odot [(eH) \odot (p^{-1}H)]$ . However,

$$\begin{aligned} (pH) \odot [(eH) \odot (p^{-1}H)] &= pH \odot (ep^{-1})H \\ &= pH \odot p^{-1}H \\ &= eH \\ &= H. \end{aligned}$$

We have shown that:

$$(pH) \odot [(hH) \odot (p^{-1}H)] \neq (pH) \odot [(eH) \odot (p^{-1}H)]$$

despite the fact that  $eH = hH$ . Therefore, “ $\odot$ ” is indeed poorly defined.

If  $H$  were invariant,  $(php^{-1})H$  would be equal to  $H$  and this problem would not arise. ■

**Problem 2.7** Prove that  $G = H_1 \otimes H_2$  implies  $G/H_1 \simeq H_2$  and  $G/H_2 \simeq H_1$ , where  $\simeq$  means “isomorphic to”.

SOLUTION: Since  $H_1, H_2$  are invariant subgroups, the sets  $G/H_1$  and  $G/H_2$  equipped with the usual multiplication of cosets are groups. If it is also true that  $G = H_1 \otimes H_2$ , we have:

$$\begin{aligned} G/H_1 &= \{gH_1 : g \in G\} \\ &= \{h_1h_2H_1 : h_1 \in H_1, h_2 \in H_2\} \\ &= \{(h_1H_1)(h_2H_1) : h_1 \in H_1, h_2 \in H_2\} \\ &= \{(eH_1)(h_2H_1) : h_2 \in H_2\} \\ &= \{h_2H_1\} \end{aligned}$$

This states that the cosets of  $H_1$  generated by the elements of  $H_2$  are the only elements of the factor group  $G/H_1$ .

The above equation suggests a natural correspondence

$$h_2 \in H_2 \xrightarrow{\mathbf{T}} h_2H_1 \in G/H_1$$

which is trivially one-to-one and onto. This identification is a homomorphism since

$$\begin{aligned} \mathbf{T}(hh') &= (hh')H \\ &= (hH)(h'H) \\ &= \mathbf{T}(h)\mathbf{T}(h') \end{aligned}$$

for all  $h, h' \in G$ . Therefore  $\mathbf{T}$  is an isomorphism and

$$G/H_1 \simeq H_2.$$

Similarly for  $G/H_2 \simeq H_1$ . ■

**Problem 2.8** Consider the dihedral group  $D_4$  which is the symmetry group of the square consisting of rotations around the center and reflections about the vertical, horizontal, and diagonal axes. Enumerate the group elements, the classes, the subgroups, and the invariant subgroups. Identify the factor groups. Is the full group the direct product of some of its subgroups?

SOLUTION: Let a rotation by  $\pi/2$  about the centre be denoted by  $g$  and let a reflection about the (24)-diagonal be denoted by  $h$ . Then

$$D_4 = \{e, g, g^2, g^3, h, gh, g^2h, g^3h\}$$

subject to  $e = g^4 = h^2 = (gh)^2$ . One says that  $D_4$  is generated by  $g$  and  $h$ .<sup>1</sup>

The group  $D_4$  has five conjugacy classes:

$$\{e\}, \{g^2\}, \{g, g^3\}, \{h, g^2h\}, \{gh, g^3h\}.$$

It is of order 8 and therefore has non-trivial subgroups of orders 2 and 4 only:

<sup>1</sup>In cycle notation:  $g = (1234)$ ,  $g^2 = (13)(24)$ ,  $g^3 = (1432)$ ,  $h = (13)$ ,  $gh = (12)(34)$ ,  $g^2h = (24)$ ,  $g^3h = (14)(23)$ .

Order 2:

$$N_2 = \begin{aligned} &\{e, h\}, \\ &\{e, gh\}, \\ &\{e, g^2\}, \\ &\{e, g^2h\}, \\ &\{e, g^3h\}. \end{aligned}$$

Order 4:

$$\begin{aligned} N^1_4 &= \{e, g, g^2, g^3\}, \\ N^2_4 &= \{e, g^2, gh, g^3h\}, \\ N^3_4 &= \{e, g^2, h, g^2h\}. \end{aligned}$$

The indicated ones are the invariant subgroups.

The factor groups are:

$$\begin{aligned} D_4/N_2 &= \{N_2, gN_2, hN_2, ghN_2\}, \\ D_4/N^1_4 &= \{N^1_4, hN^1_4\}, \\ D_4/N^2_4 &= \{N^2_4, gN^2_4\}, \\ D_4/N^3_4 &= \{N^3_4, hN^3_4\}. \end{aligned}$$

It is now easy to see that  $D_4$  is not the direct product of any of its subgroups, since the factor group  $D_4/N_2$  is not isomorphic to any of the invariant subgroups of order 4. (Another way to prove this is to observe that if a group is the direct product of any of its invariant subgroups, then the intersection of these invariant subgroups must contain exactly one element: the identity [Prove!].)

For reference, here is the multiplication table for  $D_4$ :

$e$	$g$	$g^2$	$g^3$	$h$	$gh$	$g^2h$	$g^3h$
$g$	$g^2$	$g^3$	$e$	$gh$	$g^2h$	$g^3h$	$h$
$g^2$	$g^3$	$e$	$g$	$g^2h$	$g^3h$	$h$	$gh$
$g^3$	$e$	$g$	$g^2$	$g^3h$	$h$	$gh$	$g^2h$
$h$	$g^3h$	$g^2h$	$gh$	$e$	$g^3$	$g^2$	$g$
$gh$	$h$	$g^3h$	$g^2h$	$g$	$e$	$g^3$	$g^2$
$g^2h$	$gh$	$h$	$g^3h$	$g^2$	$g$	$e$	$g^3$
$g^3h$	$g^2h$	$gh$	$h$	$g^3$	$g^2$	$g$	$e$

■