

### 3.1 Definition of a Group

This section contains these definitions: *binary operation*, *group*, *abelian group*, and *finite group*. These definitions provide the language you will be working with, and you simply *must* know this language. Try to learn it so well that you don't have even a trace of an accent!

Loosely, a group is a set on which it is possible to define a binary operation that is associative, has an identity element, and has inverses for each of its elements. The precise statement is given in Definition 3.1.3; you must pay careful attention to each part, especially the quantifiers (“for all”, “for each”, “there exists”), which must be stated in exactly the right order.

From one point of view, the axioms for a group give us just what we need to work with equations involving the operation in the group. For example, one of the rules you are used to says that you can multiply both sides of an equation by the same value, and the equation will still hold. This still works for the operation in a group, since if  $x$  and  $y$  are elements of a group  $G$ , and  $x = y$ , then  $a \cdot x = a \cdot y$ , for any element  $a$  in  $G$ . This is a part of the guarantee that comes with the definition of a binary operation. It is important to note that on both sides of the equation,  $a$  is multiplied on the left. We could also guarantee that  $x \cdot a = y \cdot a$ , but we can't guarantee that  $a \cdot x = y \cdot a$ , since the operation in the group may not satisfy the commutative law.

The existence of inverses allows cancellation (see Proposition 3.1.6 for the precise statement). Remember that in a group there is no mention of division, so whenever you are tempted to write  $a \div b$  or  $a/b$ , you must write  $a \cdot b^{-1}$  or  $b^{-1} \cdot a$ . If you are careful about the side on which you multiply, and don't fall victim to the temptation to divide, you can be pretty safe in doing the familiar things to an equation that involves elements of a group.

Understanding and remembering the definitions will give you one level of understanding. The next level comes from knowing some good examples. The third level of understanding comes from using the definitions to prove various facts about groups.

Here are a few of the important examples. First, the sets of numbers  $\mathbf{Z}$ ,  $\mathbf{Q}$ ,  $\mathbf{R}$ , and  $\mathbf{C}$  form groups under addition. Next, the sets  $\mathbf{Q}^\times$ ,  $\mathbf{R}^\times$ , and  $\mathbf{C}^\times$  of nonzero numbers form groups under multiplication. The sets  $\mathbf{Z}$  and  $\mathbf{Z}_n$  are groups under addition, while  $\mathbf{Z}_n^\times$  is a group under multiplication. It is common to just list these sets as groups, without mentioning their operations, since in each case only one of the two familiar operations can be used to make the set into a group. Similarly, the set  $M_n(\mathbf{R})$  of all  $n \times n$  matrices with entries in  $\mathbf{R}$  is a group under addition, but not multiplication, while the set  $GL_n(\mathbf{R})$  of all invertible  $n \times n$  matrices with entries in  $\mathbf{R}$  is a group under multiplication, but not under addition. There shouldn't be any confusion in just listing these as groups, without specifically mentioning which operation is used.

In the study of finite groups, the most important examples come from groups of matrices. I should still mention that the original motivation for studying groups

came from studying sets of permutations, and so the symmetric group  $\mathcal{S}_n$  still has an important role to play.

### SOLVED PROBLEMS: §3.1

22. Use the dot product to define a multiplication on  $\mathbf{R}^3$ . Does this make  $\mathbf{R}^3$  into a group?
23. For vectors  $(x_1, y_1, z_1)$  and  $(x_2, y_2, z_2)$  in  $\mathbf{R}^3$ , the cross product is defined by  $(x_1, y_1, z_1) \times (x_2, y_2, z_2) = (y_1z_2 - z_1y_2, z_1x_2 - x_1z_2, x_1y_2 - y_1x_2)$ . Is  $\mathbf{R}^3$  a group under this multiplication?
24. On the set  $G = \mathbf{Q}^\times$  of nonzero rational numbers, define a new multiplication by  $a * b = \frac{ab}{2}$ , for all  $a, b \in G$ . Show that  $G$  is a group under this multiplication.
25. Write out the multiplication table for  $\mathbf{Z}_9^\times$ .
26. Write out the multiplication table for  $\mathbf{Z}_{15}^\times$ .
27. Let  $G$  be a group, and suppose that  $a$  and  $b$  are any elements of  $G$ . Show that if  $(ab)^2 = a^2b^2$ , then  $ba = ab$ .
28. Let  $G$  be a group, and suppose that  $a$  and  $b$  are any elements of  $G$ . Show that  $(aba^{-1})^n = ab^n a^{-1}$ , for any positive integer  $n$ .
29. In Definition 3.1.3 of the text, replace condition (iii) with the condition that there exists  $e \in G$  such that  $e \cdot a = a$  for all  $a \in G$ , and replace condition (iv) with the condition that for each  $a \in G$  there exists  $a' \in G$  with  $a' \cdot a = e$ . Prove that these weaker conditions (given only on the left) still imply that  $G$  is a group.
30. The previous exercise shows that in the definition of a group it is sufficient to require the existence of a left identity element and the existence of left inverses. Give an example to show that it is *not* sufficient to require the existence of a left identity element together with the existence of *right* inverses.
31. Let  $F$  be the set of all *fractional linear transformations* of the complex plane. That is,  $F$  is the set of all functions  $f(z) : \mathbf{C} \rightarrow \mathbf{C}$  of the form  $f(z) = \frac{az + b}{cz + d}$ , where the coefficients  $a, b, c, d$  are integers with  $ad - bc = 1$ . Show that  $F$  forms a group under composition of functions.
32. Let  $G = \{x \in \mathbf{R} \mid x > 1\}$  be the set of all real numbers greater than 1. For  $x, y \in G$ , define  $x * y = xy - x - y + 2$ .
  - (a) Show that the operation  $*$  is closed on  $G$ .
  - (b) Show that the associative law holds for  $*$ .

- (c) Show that 2 is the identity element for the operation  $*$ .
- (d) Show that for element  $a \in G$  there exists an inverse  $a^{-1} \in G$ .