

---

# Groups

---

## 3.1 SOLUTIONS

22. Use the dot product to define a multiplication on  $\mathbf{R}^3$ . Does this make  $\mathbf{R}^3$  into a group?

*Solution:* The dot product of two vectors is a scalar, not a vector. This means that the dot product does not even define a binary operation on the set of vectors in  $\mathbf{R}^3$ .

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?

*Solution:* The cross product of the zero vector and any other vector is the zero vector, so the cross product cannot be used to make the set of all vectors in  $\mathbf{R}^3$  into a group.

Even if we were to exclude the zero vector we would still have problems. The cross product of two nonzero vectors defines a vector that is perpendicular to each of the given vectors. This means that the operation could not have an identity element, again making it impossible to define a group structure.

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.

*Solution:* If  $a$  and  $b$  are nonzero rational numbers, then  $ab$  is a nonzero rational number, and so is  $\frac{ab}{2}$ , showing that the operation is closed on the set  $G$ . The operation is associative since

$$a * (b * c) = a * \left( \frac{bc}{2} \right) = \frac{a \left( \frac{bc}{2} \right)}{2} = \frac{a(bc)}{4}$$

and

$$(a * b) * c = \left( \frac{ab}{2} \right) * c = \frac{\left( \frac{ab}{2} \right) c}{2} = \frac{(ab)c}{4}.$$

The number 2 acts as the multiplicative identity, and if  $a$  is nonzero, then  $\frac{4}{a}$  is a nonzero rational number that serves as the multiplicative inverse of  $a$ .

25. Write out the multiplication table for  $\mathbf{Z}_9^\times$ .

*Solution:*  $\mathbf{Z}_9^\times = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$ . We will write  $m$  for  $[m]_9$ .

·	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

*Comment:* Rewriting the table, with the elements in a slightly different order, gives a different picture of the group.

·	1	2	4	8	7	5
1	1	2	4	8	7	5
2	2	4	8	7	5	1
4	4	8	7	5	1	2
8	8	7	5	1	2	4
7	7	5	1	2	4	8
5	5	1	2	4	8	7

Each element in the group is a power of 2, and the second table shows what happens when we arrange the elements in order, as successive powers of 2.

26. Write out the multiplication table for  $\mathbf{Z}_{15}^\times$ .

*Solution:*  $\mathbf{Z}_{15}^\times = \{[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [8]_{15}, [11]_{15}, [13]_{15}, [14]_{15}\}$ . We will write the elements as  $\{1, 2, 4, 7, -7, -4, -2, -1\}$ .

·	1	-1	2	-2	4	-4	7	-7
1	1	-1	2	-2	4	-4	7	-7
-1	-1	1	-2	2	-4	4	-7	7
2	2	-2	4	-4	-7	7	-1	1
-2	-2	2	-4	4	7	-7	1	-1
4	4	-4	-7	7	1	-1	-2	2
-4	-4	4	7	-7	-1	1	2	-2
7	7	-7	-1	1	-2	2	4	-4
-7	-7	7	1	-1	2	-2	-4	4

*Comment:* Notice how much easier it makes it to use the representatives  $\{\pm 1, \pm 2, \pm 4, \pm 7\}$  when listing the congruence classes in the group.

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  $ba = ab$ .

*Solution:* Assume that  $a$  and  $b$  are elements of  $G$  for which  $(ab)^2 = a^2b^2$ . Expanding this equation gives us

$$(ab)(ab) = a^2b^2.$$

Since  $G$  is a group, both  $a$  and  $b$  have inverses, denoted by  $a^{-1}$  and  $b^{-1}$ , respectively. Multiplication in  $G$  is well-defined, so we can multiply both sides of the equation on the left by  $a^{-1}$  without destroying the equality.

If we are to be precise about using the associative law, we have to include the following steps.

$$\begin{aligned} a^{-1}((ab)(ab)) &= a^{-1}(a^2b^2) \\ (a^{-1}(ab))(ab) &= (a^{-1}a^2)b^2 \\ ((a^{-1}a)b)(ab) &= ((a^{-1}a)a)b^2 \\ (eb)(ab) &= (ea)b^2 \\ b(ab) &= ab^2 \end{aligned}$$

The next step is to multiply on the right by  $b^{-1}$ . The associative law for multiplication essentially says that parentheses don't matter, so we don't really need to include all of the steps we showed before.

$$\begin{aligned} b(ab)b^{-1} &= (ab^2)b^{-1} \\ (ba)(bb^{-1}) &= (ab)(bb^{-1}) \\ ba &= ab \end{aligned}$$

This completes the proof, since we have shown 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  $n$ .

*Solution:* To give a careful proof we need to use induction. The statement for  $n = 1$  is simply that  $aba^{-1} = aba^{-1}$ , which is certainly true. Now assume that the result holds for  $n = k$ . Using this induction hypothesis, we have the following calculation.

$$\begin{aligned} (aba^{-1})^{k+1} &= (aba^{-1})^k(aba^{-1}) \\ &= (ab^k a^{-1})(aba^{-1}) \\ &= (ab^k)(a^{-1}a)(ba^{-1}) \\ &= (ab^k)(ba^{-1}) \\ &= ab^{k+1}a^{-1} \end{aligned}$$

Thus the statement holds for  $n = k + 1$ , so by induction it holds for all values of  $n$ .

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.

*Solution:* Assume that the two replacement conditions hold. Note the  $e \cdot e = e$ , and that the associative law holds.

We will first show that  $a \cdot e = a$ , for all  $a \in G$ . Let  $a'$  be an element in  $G$  with  $a' \cdot a = e$ . Then

$$a' \cdot (a \cdot e) = (a' \cdot a) \cdot e = e \cdot e = e = a' \cdot a,$$

and since there exists an element  $a'' \in G$  with  $a'' \cdot a' = e$ , we can cancel  $a'$  from the left of the above equation, to get  $a \cdot e = a$ . This shows that  $e$  is a multiplicative identity for  $G$ , and so the original condition (iii) is satisfied.

We also have the equation

$$a' \cdot (a \cdot a') = (a' \cdot a) \cdot a' = e \cdot a' = a' = a' \cdot e,$$

and then (as above) we can cancel  $a'$  to get  $a \cdot a' = e$ , which shows that  $a'$  is indeed the multiplicative inverse of  $a$ . Thus the original condition (iv) holds, and so  $G$  is a group under the given operation.

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.

*Solution:* On the set  $G$  of nonzero real numbers, define the operation  $a * b = |a|b$ , for all  $a, b \in G$ . Then  $a * b \neq 0$  if  $a \neq 0$  and  $b \neq 0$ , so we have defined a binary operation on  $G$ . The operation is associative since  $a*(b*c) = a*(|b|c) = |a||b|c = |ab|c$  and  $(a*b)*c = (|a|b)*c = ||a|b|c = |ab|c$ . The number 1 is a left identity element, since  $1*a = |1|a = a$  for all  $a \in G$ . There is no right identity element, since the two equations  $1*x = 1$  and  $(-1)*x = -1$  have no simultaneous solution in  $G$ . Finally,  $1/|a|$  is a right inverse for any  $a \in G$ , but the equation  $x*a = 1$  has no solution for  $a = -1$ , so  $-1$  has no left inverse.

In summary, we have shown that  $G$  is not a group, even though it has a left identity element and 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.

*Solution:* We first need to check that composition of functions defines a binary operation on  $F$ , so we need to check the closure axiom in Definition 3.1.3.

Let  $f_1(z) = \frac{a_1z + b_1}{c_1z + d_1}$ , and  $f_2(z) = \frac{a_2z + b_2}{c_2z + d_2}$ , with  $a_1d_1 - b_1c_1 = 1$  and  $a_2d_2 - b_2c_2 = 1$ . Then for any complex number  $z$  we have

$$\begin{aligned} f_2 \circ f_1(z) &= f_2(f_1(z)) = \frac{a_2f_1(z) + b_2}{c_2f_1(z) + d_2} \\ &= \frac{a_2\left(\frac{a_1z + b_1}{c_1z + d_1}\right) + b_2}{c_2\left(\frac{a_1z + b_1}{c_1z + d_1}\right) + d_2} \\ &= \frac{a_2(a_1z + b_1) + b_2(c_1z + d_1)}{c_2(a_1z + b_1) + d_2(c_1z + d_1)} \\ &= \frac{(a_2a_1 + b_2c_1)z + (a_2b_1 + b_2d_1)}{(c_2a_1 + d_2c_1)z + (c_2b_1 + d_2d_1)}. \end{aligned}$$

You can see that verifying all of the axioms is going to be painful. We need a better way to look at the entire situation, so let's look at the following matrix product.

$$\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} = \begin{bmatrix} a_2a_1 + b_2c_1 & a_2b_1 + b_2d_1 \\ c_2a_1 + d_2c_1 & c_2b_1 + d_2d_1 \end{bmatrix}$$

If we associate with the fractional linear transformations  $f_2(z) = \frac{a_2z + b_2}{c_2z + d_2}$  and  $f_1(z) = \frac{a_1z + b_1}{c_1z + d_1}$  the matrices  $\begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$  and  $\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ , respectively, then we can see that composition of two fractional linear transformations

corresponds to the product of the two associated matrices. Furthermore, the condition that  $ad - bc = 1$  for a fractional linear transformation corresponds to the condition that the determinant of the associated matrix is equal to 1. All of this means that it is fair to use what we already know about matrix multiplication. The proof that the determinant of a product is the product of the determinants can be used to show that in the composition  $f_2 \circ f_1$  we will still have the required condition on the coefficients that we calculated.

Composition of functions is always associative (compare Exercise 3.1.2 in the text, for matrices), and the identity function will serve as an identity element for  $F$ . We only need to check that it can be written in the correct form, as a fractional linear transformation, and this can be shown by choosing coefficients  $a = 1$ ,  $b = 0$ ,  $c = 0$ , and  $d = 1$ . Finally, we can use the formula for the inverse of a  $2 \times 2$  matrix with determinant 1 to find an inverse function for  $f(z) = \frac{az + b}{cz + d}$ . This gives  $f^{-1}(z) = \frac{dz - b}{-cz + a}$ , and completes the proof 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  $G$ .

*Solution:* If  $a, b \in G$ , then  $a > 1$  and  $b > 1$ , so  $b - 1 > 0$ , and therefore  $a(b - 1) > (b - 1)$ . It follows immediately that  $ab - a - b + 2 > 1$ .

(b) Show that the associative law holds for  $*$ .

*Solution:* For  $a, b, c \in G$ , we have

$$\begin{aligned} a * (b * c) &= a * (bc - b - c + 2) \\ &= a(bc - b - c + 2) - a - (bc - b - c + 2) + 2 \\ &= abc - ab - ac - bc + a + b + c. \end{aligned}$$

On the other hand, we have

$$\begin{aligned} (a * b) * c &= (ab - a - b + 2) * c \\ &= (ab - a - b + 2)c - (ab - a - b + 2) - c + 2 \\ &= abc - ab - ac - bc + a + b + c. \end{aligned}$$

Thus  $a * (b * c) = (a * b) * c$ .

(c) Show that 2 is the identity element for the operation  $*$ .

*Solution:* Since the operation is commutative, the one computation  $2 * y = 2y - 2 - y + 2 = y$  suffices to show that 2 is the identity element.

(d) Show that for element  $a \in G$  there exists an inverse  $a^{-1} \in G$ .

*Solution:* Given any  $a \in G$ , we need to solve  $a * y = 2$ . This gives us the equation  $ay - a - y + 2 = 2$ , which has the solution  $y = a/(a - 1)$ .

This solution belongs to  $G$  since  $a > a - 1$  implies  $a/(a - 1) > 1$ . Finally,  
 $a*(a/a-1) = a^2/(a-1) - a - a/(a-1) + 2 = (a^2 - a^2 + a - a)/(a-1) + 2 = 2$ .