

## 3.4 SOLUTIONS

21. Show that  $\mathbf{Z}_{17}^\times$  is isomorphic to  $\mathbf{Z}_{16}$ .

*Solution:* The element  $[3]$  is a generator for  $\mathbf{Z}_{17}^\times$ , since  $3^2 = 9$ ,  $3^3 = 27 \equiv 10$ ,  $3^4 \equiv 3 \cdot 10 \equiv 30 \equiv 13$ ,  $3^5 \equiv 3 \cdot 13 \equiv 39 \equiv 5$ ,  $3^6 \equiv 3 \cdot 5 \equiv 15$ ,  $3^7 \equiv 3 \cdot 15 \equiv 45 \equiv 11$ , and  $3^8 \equiv 3 \cdot 11 \equiv 33 \equiv -1 \not\equiv 1$ . Therefore  $\mathbf{Z}_{17}^\times$  is a cyclic group with 16 elements. This provides the clue as to how to define the isomorphism we need, since  $\mathbf{Z}_{16}$  is also a cyclic group, with generator  $[1]_{16}$ , and Proposition 3.4.3 (a) implies that any isomorphism between cyclic groups must map a generator to a generator.

Define  $\phi : \mathbf{Z}_{16} \rightarrow \mathbf{Z}_{17}^\times$  by setting  $\phi([1]_{16}) = [3]_{17}$ ,  $\phi([2]_{16}) = [3]_{17}^2$ , etc. The general formula is  $\phi([n]_{16}) = [3]_{17}^n$ , for all  $[n]_{16} \in \mathbf{Z}_{16}$ . Since  $\phi$  is defined by using a representative  $n$  of the equivalence class  $[n]_{16}$ , we have to show that the formula for  $\phi$  does not depend on the particular representative that is chosen. If  $k \equiv m \pmod{16}$ , then it follows from Proposition 3.2.8 (c) that  $[3]_{17}^k = [3]_{17}^m$  since  $[3]_{17}$  has order 16 in  $\mathbf{Z}_{17}^\times$ . Therefore  $\phi([k]_{16}) = \phi([m]_{16})$ , and so  $\phi$  is a well-defined function.

Proposition 3.2.8 (c) shows that  $\phi([k]_{16}) = \phi([m]_{16})$  only if  $k \equiv m \pmod{16}$ , and so  $\phi$  is a one-to-one function. Then because both  $\mathbf{Z}_{16}$  and  $\mathbf{Z}_{17}^\times$  have 16 elements, it follows from Proposition 2.1.5 that  $\phi$  is also an onto function. The proof that  $\phi$  respects the two group operations follows the proof in Example 3.4.1. For any elements  $[n]_{16}$  and  $[m]_{16}$  in  $\mathbf{Z}_{16}$ , we first compute what happens if we combine  $[n]_{16}$  and  $[m]_{16}$  using the operation in  $\mathbf{Z}_{16}$ , and then substitute the result into the function  $\phi$ :

$$\phi([n]_{16} + [m]_{16}) = \phi([n + m]_{16}) = [3]_{17}^{n+m}.$$

Next, we first apply the function  $\phi$  to the two elements,  $[n]_{16}$  and  $[m]_{16}$ , and then combine the results using the operation in  $\mathbf{Z}_{17}^\times$ :

$$\phi([n]_{16}) \cdot \phi([m]_{16}) = [3]_{17}^n [3]_{17}^m = [3]_{17}^{n+m}.$$

Thus  $\phi([n]_{16} + [m]_{16}) = \phi([n]_{16}) \cdot \phi([m]_{16})$ , and this completes the proof that  $\phi$  is a group isomorphism.

22. Let  $\phi : \mathbf{R}^\times \rightarrow \mathbf{R}^\times$  be defined by  $\phi(x) = x^3$ , for all  $x \in \mathbf{R}$ . Show that  $\phi$  is a group isomorphism.

*Solution:* The function  $\phi$  preserves multiplication in  $\mathbf{R}^\times$  since for all  $a, b \in \mathbf{R}^\times$  we have  $\phi(ab) = (ab)^3 = a^3 b^3 = \phi(a)\phi(b)$ . The function is one-to-one and onto since for each  $y \in \mathbf{R}^\times$  the equation  $\phi(x) = y$  has the unique solution  $x = \sqrt[3]{y}$ .

23. Let  $G_1, G_2, H_1, H_2$  be groups, and suppose that  $\theta_1 : G_1 \rightarrow H_1$  and  $\theta_2 : G_2 \rightarrow H_2$  are group isomorphisms. Define  $\phi : G_1 \times G_2 \rightarrow H_1 \times H_2$  by

$\phi(x_1, x_2) = (\theta_1(x_1), \theta_2(x_2))$ , for all  $(x_1, x_2) \in G_1 \times G_2$ . Prove that  $\phi$  is a group isomorphism.

*Solution:* If  $(y_1, y_2) \in H_1 \times H_2$ , then since  $\theta_1$  is an isomorphism there is a unique element  $x_1 \in G_1$  with  $y_1 = \theta_1(x_1)$ . Similarly, since  $\theta_2$  is an isomorphism there is a unique element  $x_2 \in G_2$  with  $y_2 = \theta_2(x_2)$ . Thus there is a unique element  $(x_1, x_2) \in G_1 \times G_2$  such that  $(y_1, y_2) = \phi(x_1, x_2)$ , and so  $\phi$  is one-to-one and onto.

Given  $(a_1, a_2)$  and  $(b_1, b_2)$  in  $G_1 \times G_2$ , we have

$$\begin{aligned}\phi((a_1, a_2) \cdot (b_1, b_2)) &= \phi((a_1 b_1, a_2 b_2)) = (\theta_1(a_1 b_1), \theta_2(a_2 b_2)) \\ &= (\theta_1(a_1)\theta_1(b_1), \theta_2(a_2)\theta_2(b_2)) \\ \phi((a_1, a_2)) \cdot \phi((b_1, b_2)) &= (\theta_1(a_1), \theta_2(a_2)) \cdot (\theta_1(b_1), \theta_2(b_2)) \\ &= (\theta_1(a_1)\theta_1(b_1), \theta_2(a_2)\theta_2(b_2))\end{aligned}$$

and so  $\phi : G_1 \times G_2 \rightarrow H_1 \times H_2$  is a group isomorphism.

24. Prove that the group  $\mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$  is isomorphic to the group  $\mathbf{Z}_6 \times \mathbf{Z}_{10}$ .

*Solution:* You can check that  $\mathbf{Z}_7^\times$  is cyclic of order 6, generated by  $[3]_7$ , and that  $\mathbf{Z}_{11}^\times$  is cyclic of order 10, generated by  $[2]_{11}$ . Just as in Problem 21, you can show that  $\theta_1 : \mathbf{Z}_6 \rightarrow \mathbf{Z}_7^\times$  defined by  $\theta_1([n]_6) = [3]_7^n$  and  $\theta_2 : \mathbf{Z}_{10} \rightarrow \mathbf{Z}_{11}^\times$  defined by  $\theta_2([m]_{10}) = [2]_{11}^m$  are group isomorphisms. It then follows from Problem 23 that  $\phi : \mathbf{Z}_6 \times \mathbf{Z}_{10} \rightarrow \mathbf{Z}_7^\times \times \mathbf{Z}_{11}^\times$  defined by  $\phi([n]_6, [m]_{10}) = ([3]_7^n, [2]_{11}^m)$ , for all  $[n]_6 \in \mathbf{Z}_6$  and all  $[m]_{10} \in \mathbf{Z}_{10}$ , is a group isomorphism.

25. Define  $\phi : \mathbf{Z}_{30} \times \mathbf{Z}_2 \rightarrow \mathbf{Z}_{10} \times \mathbf{Z}_6$  by  $\phi([n]_{30}, [m]_2) = ([n]_{10}, [4n + 3m]_6)$ , for all  $([n]_{30}, [m]_2) \in \mathbf{Z}_{30} \times \mathbf{Z}_2$ . First prove that  $\phi$  is a well-defined function, and then prove that  $\phi$  is a group isomorphism.

*Solution:* If  $([n]_{30}, [m]_2)$  and  $([k]_{30}, [j]_2)$  are equal elements of  $\mathbf{Z}_{30} \times \mathbf{Z}_2$ , then  $30 \mid n - k$  and  $2 \mid m - j$ . It follows that  $10 \mid n - k$ , and so  $[n]_{10} = [k]_{10}$ . Furthermore,  $30 \mid 4(n - k)$ , so  $6 \mid 4(n - k)$ , and then  $6 \mid 3(m - j)$ , which together imply that  $6 \mid (4n + 3m) - (4k + 3j)$ , showing that  $[4n + 3m]_6 = [4k + 3j]_6$ . Thus  $([n]_{10}, [4n + 3m]_6) = ([k]_{10}, [4k + 3j]_6)$ , which shows that the formula for  $\phi$  does yield a well-defined function.

For any elements  $([a]_{30}, [c]_2)$  and  $([b]_{30}, [d]_2)$  we have

$$\begin{aligned}\phi(([a]_{30}, [c]_2) + ([b]_{30}, [d]_2)) &= \phi([a + b]_{30}, [c + d]_2) \\ &= ([a + b]_{10}, [4(a + b) + 3(c + d)]_2) \\ &= ([a + b]_{10}, [4a + 4b + 3c + 3d]_2) \\ \phi([a]_{30}, [c]_2) + \phi([b]_{30}, [d]_2) &= ([a]_{10}, [4a + 3c]_2) + ([b]_{10}, [4b + 3d]_2) \\ &= ([a + b]_{10}, [4a + 3c + 4b + 3d]_2) \\ &= ([a + b]_{10}, [4a + 4b + 3c + 3d]_2)\end{aligned}$$

and so  $\phi$  respects the operations in the two groups. This means that we can use Proposition 3.4.4 to show that  $\phi$  is one-to-one. If  $\phi([n]_{30}, [m]_2) = ([0]_{10}, [0]_6)$ , then  $([n]_{10}, [4n + 3m]_6) = ([0]_{10}, [0]_6)$ , so  $10 \mid n$ , say  $n = 10q$ , for some  $q \in \mathbf{Z}$ , and  $6 \mid (4n + 3m)$ , or  $6 \mid (40q + 3m)$ . It follows that  $2 \mid (40q + 3m)$  and  $3 \mid (40q + 3m)$ , and therefore  $2 \mid 3m$  since  $2 \mid 40q$ , and  $3 \mid 40q$  since  $3 \mid 3m$ . Then since 2 and 3 are prime numbers, it follows that  $2 \mid m$ , so  $[m]_2 = [0]_2$ , and  $3 \mid q$ , so  $[n]_{30} = [10q]_{30} = [0]_{30}$ . We have now shown that if  $\phi([n]_{30}, [m]_2) = ([0]_{10}, [0]_6)$ , then  $([n]_{30}, [m]_2) = ([0]_{30}, [0]_2)$ , and so the condition in Proposition 3.4.4 is satisfied. We conclude that  $\phi$  is a one-to-one function. Since the two groups both have 60 elements, it follows that  $\phi$  must also be an onto function. We have therefore checked all of the necessary conditions, so we may conclude that  $\phi$  is a group isomorphism.

26. Let  $G$  be a group, and let  $H$  be a subgroup of  $G$ . Prove that if  $a$  is any element of  $G$ , then the subset

$$aHa^{-1} = \{g \in G \mid g = aha^{-1} \text{ for some } h \in H\}$$

is a subgroup of  $G$  that is isomorphic to  $H$ .

*Solution:* By Exercise 3.4.13 in the text, the function  $\phi : G \rightarrow G$  defined by  $\phi(x) = axa^{-1}$ , for all  $x \in G$ , is a group isomorphism. By Exercise 3.4.15 the image under  $\phi$  of any subgroup of  $G$  is again a subgroup of  $G$ , so  $aHa^{-1} = \phi(H)$  is a subgroup of  $G$ . It is then clear that function  $\theta : H \rightarrow aHa^{-1}$  defined by  $\theta(x) = axa^{-1}$  is an isomorphism.

27. Let  $G, G_1, G_2$  be groups. Prove that if  $G$  is isomorphic to  $G_1 \times G_2$ , then there are subgroups  $H$  and  $K$  in  $G$  such that  $H \cap K = \{e\}$ ,  $HK = G$ , and  $hk = kh$  for all  $h \in H$  and  $k \in K$ .

*Solution:* Let  $\phi : G_1 \times G_2 \rightarrow G$  be an isomorphism. Exercise 3.3.9 in the text shows that in  $G_1 \times G_2$  the subgroups  $H^* = \{(x_1, x_2) \mid x_2 = e\}$  and  $K^* = \{(x_1, x_2) \mid x_1 = e\}$  have the properties we are looking for. Let  $H = \phi(H^*)$  and  $K = \phi(K^*)$  be the images in  $G$  of  $H^*$  and  $K^*$ , respectively. We know (by Exercise 3.4.15) that  $H$  and  $K$  are subgroups of  $G$ , so we only need to show that  $H \cap K = \{e\}$ ,  $HK = G$ , and  $hk = kh$  for all  $h \in H$  and  $k \in K$ .

Let  $y \in G$ , with  $y = \phi(x)$ , for  $x \in G_1 \times G_2$ . If  $y \in H \cap K$ , then  $y \in H$ , and so  $x \in H^*$ . Since  $y \in K$  as well, we must also have  $x \in K^*$ , so  $x \in H^* \cap K^*$ , and therefore  $x = (e_1, e_2)$ , where  $e_1$  and  $e_2$  are the respective identity elements in  $G_1$  and  $G_2$ . Thus  $y = \phi((e_1, e_2)) = e$ , showing that  $H \cap K = \{e\}$ . Since  $y$  is any element of  $G$ , and we can write  $x = h^*k^*$  for some  $h^* \in H^*$  and some  $k^* \in K^*$ , it follows that  $y = \phi(h^*k^*) = \phi(h^*)\phi(k^*)$ , and thus  $G = HK$ . It is clear that  $\phi$  preserves the fact that elements of  $H^*$  and  $K^*$  commute. We conclude that  $H$  and  $K$  satisfy the desired conditions.

28. Show that for any prime number  $p$ , the subgroup of diagonal matrices in  $\text{GL}_2(\mathbf{Z}_p)$  is isomorphic to  $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ .

*Solution:* Since each matrix in  $GL_2(\mathbf{Z}_p)$  has nonzero determinant, it is clear that the mapping  $\phi : \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times \rightarrow GL_2(\mathbf{Z}_p)$  defined by  $\phi(x_1, x_2) = \begin{bmatrix} x_1 & 0 \\ 0 & x_2 \end{bmatrix}$ , for each  $(x_1, x_2) \in \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$ , is one-to-one and maps  $\mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$  onto the subgroup of diagonal matrices. This mapping respects the operations in the two groups, since for  $(a_1, a_2), (b_1, b_2) \in \mathbf{Z}_p^\times \times \mathbf{Z}_p^\times$  we have

$$\begin{aligned} \phi((a_1, a_2)(b_1, b_2)) &= \phi((a_1 b_1, a_2 b_2)) \\ &= \begin{bmatrix} a_1 b_1 & 0 \\ 0 & a_2 b_2 \end{bmatrix} = \begin{bmatrix} a_1 & 0 \\ 0 & b_1 \end{bmatrix} \begin{bmatrix} a_2 & 0 \\ 0 & b_2 \end{bmatrix} \\ &= \phi((a_1, a_2))\phi((b_1, b_2)). \end{aligned}$$

Thus  $\phi$  is the desired isomorphism.

29. (a) In the group  $G = GL_2(\mathbf{R})$  of invertible  $2 \times 2$  matrices with real entries, show that

$$H = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in GL_2(\mathbf{R}) \mid a_{11} = 1, a_{21} = 0, a_{22} = 1 \right\}$$

is a subgroup of  $G$ .

*Solution:* Closure:  $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix}$ .

Identity: The identity matrix has the correct form.

Existence of inverses:  $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \in H$ .

- (b) Show that  $H$  is isomorphic to the group  $\mathbf{R}$  of all real numbers, under addition.

*Solution:* Define  $\phi : \mathbf{R} \rightarrow H$  by  $\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}$ , for all  $x \in \mathbf{R}$ . You can easily check that  $\phi$  is an isomorphism. (The computation necessary to show that  $\phi$  preserves the respective operations is the same computation we used to show that  $H$  is closed.)

30. Let  $G$  be the subgroup of  $GL_2(\mathbf{R})$  defined by

$$G = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \mid m \neq 0 \right\}.$$

Show that  $G$  is not isomorphic to the direct product  $\mathbf{R}^\times \times \mathbf{R}$ .

*Solution:* Our approach is to try to find an algebraic property that would be preserved by any isomorphism but which is satisfied by only one of the two groups in question. By Proposition 3.4.3 (b), if one of the groups is abelian but the other is not, then the groups cannot be isomorphic.

The direct product  $\mathbf{R}^\times \times \mathbf{R}$  is an abelian group, since each factor is abelian. On the other hand,  $G$  is not abelian, since  $\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix}$  but  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}$ . Thus the two groups cannot be isomorphic.

31. Let  $H$  be the following subgroup of group  $G = GL_2(\mathbf{Z}_3)$ .

$$H = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in GL_2(\mathbf{Z}_3) \mid m, b \in \mathbf{Z}_3, m \neq 0 \right\}$$

Show that  $H$  is isomorphic to the symmetric group  $\mathcal{S}_3$ .

*Solution:* This group is small enough that we can just compare its multiplication table to that of  $\mathcal{S}_3$ , as given in Table 3.3.3 (on page 104 of the text). Remember that constructing an isomorphism is the same as constructing a one-to-one correspondence between the elements of the group, such that all entries in the respective group tables also have the same one-to-one correspondence.

In this case we can explain how this can be done, without actually writing out the multiplication table. Let  $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  and  $B = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$ . Then just as in Problem 3.3.25, we can show that  $BA = A^{-1}B$ , and that each element of  $H$  has the form can be written uniquely in the form  $A^i B^j$ , where  $0 \leq i < 3$  and  $0 \leq j < 2$ . This information should make it plausible that the function  $\phi: \mathcal{S}_3 \rightarrow H$  defined by  $\phi(a^i b^j) = A^i B^j$ , for all  $0 \leq i < 3$  and  $0 \leq j < 2$ , gives a one-to-one correspondence between the elements of the groups which also produces multiplication tables that look exactly the same.

32. Let  $G$  be a group, and let  $S$  be any set for which there exists a one-to-one and onto function  $\phi: G \rightarrow S$ . Define an operation on  $S$  by setting  $x_1 \cdot x_2 = \phi(\phi^{-1}(x_1)\phi^{-1}(x_2))$ , for all  $x_1, x_2 \in S$ . Prove that  $S$  is a group under this operation, and that  $\phi$  is actually a group isomorphism.

*Solution: (Outline only)* The operation is well-defined on  $S$ , since  $\phi$  and  $\phi^{-1}$  are functions and the operation on  $G$  is well-defined. The associative law holds in  $S$  because it holds in  $G$ ; the identity element in  $S$  is  $\phi(e)$ , where  $e$  is the identity of  $G$ , and it is easy to check that if  $x \in S$ , then  $x^{-1} = \phi((\phi^{-1}(x))^{-1})$ .

*Comment:* This reveals the secret behind problems like Exercises 3.1.11 and 3.4.12 in the text. Given a known group  $G$  such as  $\mathbf{R}^\times$ , we can use one-to-one functions defined on  $G$  to produce new groups with operations that look rather different from the usual examples.