

7.3.22 (a) Let  $p$  be prime and let  $b$  be a nonzero element of  $\mathbb{Z}_p$ . Show that  $b^{p-1} = 1$ .  
 [Hint: Corollary 7.3 and Theorem 7.15.]

By the Example on page 47,  $\mathbb{Z}_p$  is a field (see Theorem 2.8). By Corollary 7.3, the nonzero elements form a group  $U_p$  under multiplication. Since  $U_p$  is finite, it is a finite subgroup of the multiplicative group of a field and, hence, is cyclic by Theorem 7.15. Therefore, there is an element  $a \in U_p$ , such that  $U_p = \langle a \rangle$ . Since  $U_p$  has  $p - 1$  elements, the order of  $a$  is  $p - 1$ . Since  $b$  is a nonzero element of  $\mathbb{Z}_p$ ,  $b \in U_p$  and so  $b = a^k$  for some  $k \in \mathbb{Z}$ . Thus,

$$b^{p-1} = (a^k)^{p-1} = a^{k(p-1)} = (a^{p-1})^k = 1^k = 1,$$

as required. ◆

(b) Prove **Fermat's Little Theorem**: If  $p$  is a prime and  $a$  is any integer, then  $a^p \equiv a \pmod{p}$ .  
 [Hint: Let  $b$  be the congruence class of  $a$  in  $\mathbb{Z}_p$  and use part (a).]

Let  $a \in \mathbb{Z}$  and let  $b \in \mathbb{Z}_p$  be its congruence class (so  $b = [a]$ ). If  $b = 0$ , then  $b^p = 0^p = 0 = b$ . If  $b \neq 0$ , then by part (a)

$$b^p = b^{p-1}b = 1 \cdot b = b.$$

Hence,  $b^p = b$  for all  $b \in \mathbb{Z}_p$  and thus  $a^p \equiv a \pmod{p}$ . ◆

7.3.25 Let  $G$  be a group and  $a \in G$ . The **centralizer of  $a$**  is the set  $C(a) = \{g \in G \mid ga = ag\}$ . Prove that  $C(a)$  is a subgroup of  $G$ .

We apply Theorem 7.10 to show that  $C(a)$  is a subgroup. Since  $ea = a = ae$ , we have  $e \in C(a)$  so  $C(a)$  is nonempty. Let  $g, h \in C(a)$ . Then since  $ha = ah$  and  $ga = ag$  we have

$$gha = gah = agh;$$

hence,  $gh \in C(a)$  and condition (i) holds. Now let  $g \in C(a)$ . then  $ag = ga$  and so

$$g^{-1}a = g^{-1}agg^{-1} = g^{-1}gag^{-1} = ag^{-1}.$$

Hence  $g^{-1} \in C(a)$  and condition (ii) holds. Therefore,  $C(a)$  is a subgroup of  $G$ . ◆

7.3.46 Prove that  $\{(\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix}) \mid n \in \mathbb{Z}\}$  is a cyclic subgroup of  $GL(2, \mathbb{R})$ .

Denote the given set  $H$ . Clearly,  $H \subseteq GL(2, \mathbb{R})$ . By Theorem 7.13 and the following definition it suffices to prove that  $H = \langle a \rangle$  where  $a = (\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$ . This will follow from the claim that  $a^n = (\begin{smallmatrix} 1 & n \\ 0 & 1 \end{smallmatrix})$  for all  $n \in \mathbb{Z}$ . We first use induction to prove the claim for  $n \geq 0$ . For  $n = 0$ , we have  $a^0 = I = (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})$  and so the base case holds. Now suppose that the claim holds for  $n = k$  for some  $k \geq 0$ . Then

$$a^{k+1} = a^k a = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

Thus the claim holds for  $n = k + 1$  and so by induction the claim is proved for all  $n \geq 0$ . A simple calculation shows that for  $n \in \mathbb{Z}$ ,

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

So these two matrices are inverses of each other. So for  $n > 0$ , we have

$$a^{-n} = (a^n)^{-1} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

Thus the claim holds for all  $n \in \mathbb{Z}$  and the desired result follows. ◆

7.4.2 Show that the function  $g : \mathbb{R}^{**} \rightarrow \mathbb{R}^{**}$  given by  $g(x) = \sqrt{x}$  is an isomorphism.

Let  $x, y \in \mathbb{R}^{**}$ . Then we have

$$g(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = g(x)g(y).$$

Hence,  $g$  is a homomorphism. Let  $h : \mathbb{R}^{**} \rightarrow \mathbb{R}^{**}$  be given by  $g(x) = x^2$ . Then since  $g \circ h = 1_{\mathbb{R}^{**}}$  and  $h \circ g = 1_{\mathbb{R}^{**}}$ ,  $g$  has an inverse and is therefore bijective. Therefore  $g$  is an isomorphism as required. ◆

7.4.18 If  $G = \langle a \rangle$  is a cyclic group and  $f : G \rightarrow H$  is a surjective homomorphism of groups, show that  $f(a)$  is a generator of  $H$ , that is,  $H$  is the cyclic group  $\langle f(a) \rangle$ .

[Hint: Exercise 11.]

Let  $G = \langle a \rangle$  be a cyclic group and let  $f : G \rightarrow H$  be a surjective homomorphism of groups. Let  $h \in H$ ; then since  $f$  is surjective, there is a  $g \in G$  such that  $h = f(g)$ . But since  $G = \langle a \rangle$  (for some  $a \in G$ ), there is  $k \in \mathbb{Z}$  such that  $g = a^k$ . Hence, by Exercise 11,  $h = f(g) = f(a^k) = f(a)^k$ . Since, every element of  $H$  is of the form  $f(a)^k$  for some  $k \in \mathbb{Z}$ , we have  $H = \langle f(a) \rangle$ , that is,  $H$  is a cyclic group with generator  $f(a)$ . ◆

7.4.28 Explain why the two groups are *not* isomorphic.

(a)  $\mathbb{Z}_6$  and  $S_3$

If two groups are isomorphic. Then one is abelian if and only if the other is. Since  $\mathbb{Z}_6$  is abelian but  $S_3$  is not, the two groups are not isomorphic.  $\blacklozenge$

(c)  $\mathbb{Z}_4 \times \mathbb{Z}_2$  and  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

The element  $(1, 0)$  in  $\mathbb{Z}_4 \times \mathbb{Z}_2$  has order 4 since  $4(1, 0) = (0, 0)$  but  $k(1, 0) = (k, 0) \neq (0, 0)$  for  $k = 1, 2, 3$ . But there is no element in  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  of order 4, since every element of  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$  has order at most 2. Indeed, for  $(a, b, c) \in \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ , we have  $2(a, b, c) = (2a, 2b, 2c) = (0, 0, 0)$ . Thus the two groups are not isomorphic, since one has an element of order 4 but not the other.  $\blacklozenge$