

3.7 SOLUTIONS

17. Find all group homomorphisms from
- \mathbf{Z}_4
- into
- \mathbf{Z}_{10}
- .

Solution: Example 3.7.5 shows that any group homomorphism from \mathbf{Z}_n into \mathbf{Z}_k must have the form $\phi([x]_n) = [mx]_k$, for all $[x]_n \in \mathbf{Z}_n$. Under any group homomorphism $\phi : \mathbf{Z}_4 \rightarrow \mathbf{Z}_{10}$, the order of $\phi([1]_4)$ must be a divisor of 4 and of 10, so the only possibilities are 1 and 2. Thus $\phi([1]_4) = [0]_{10}$, which defines the zero function, or else $\phi([1]_4) = [5]_{10}$, which leads to the formula $\phi([x]_4) = [5x]_{10}$, for all $[x]_4 \in \mathbf{Z}_4$.

18. (a) Find the formulas for all group homomorphisms from
- \mathbf{Z}_{18}
- into
- \mathbf{Z}_{30}
- .

Solution: Example 3.7.5 shows that any group homomorphism from \mathbf{Z}_{18} into \mathbf{Z}_{30} must have the form $\phi([x]_{18}) = [mx]_{30}$, for all $[x]_{18} \in \mathbf{Z}_{18}$. Since $\gcd(18, 30) = 6$, the possible orders of $[m]_{30} = \phi([1]_{18})$ are 1, 2, 3, 6. The corresponding choices for $[m]_{30}$ are $[0]_{30}$, of order 1, $[15]_{30}$, of order 2, $[10]_{30}$ and $[20]_{30}$, of order 3, and $[5]_{30}$ and $[25]_{30}$, of order 6.

(b) Choose one of the nonzero formulas in part (a), and for this formula find the kernel and image, and show how elements of the image correspond to cosets of the kernel.

Solution: For example, consider $\phi([x]_{18}) = [5x]_{30}$. The image of ϕ consists of the multiples of 5 in \mathbf{Z}_{30} , which are 0, 5, 10, 15, 20, 25. We have $\ker(\phi) = \{0, 6, 12\}$, and then cosets of the kernel are defined by adding 1, 2, 3, 4, and 5, respectively. We have the following correspondence

$$\begin{aligned} \{0, 6, 12\} &\longleftrightarrow \phi(0) = 0, & \{3, 9, 15\} &\longleftrightarrow \phi(3) = 15, \\ \{1, 7, 13\} &\longleftrightarrow \phi(1) = 5, & \{4, 10, 16\} &\longleftrightarrow \phi(4) = 20, \\ \{2, 8, 14\} &\longleftrightarrow \phi(2) = 10, & \{5, 11, 17\} &\longleftrightarrow \phi(5) = 25. \end{aligned}$$

19. (a) Show that
- \mathbf{Z}_7^\times
- is cyclic, with generator
- $[3]_7$
- .

Solution: Since $3^2 \equiv 2$ and $3^3 \equiv 6$, it follows that $[3]_7$ must have order 6.

- (b) Show that
- \mathbf{Z}_{17}^\times
- is cyclic, with generator
- $[3]_{17}$
- .

Solution: The element $[3]_7$ is a generator for \mathbf{Z}_{17}^\times , since $3^2 = 9$, $3^3 = 27 \equiv 10$, $3^4 \equiv 3 \cdot 10 \equiv 13$, $3^5 \equiv 3 \cdot 13 \equiv 5$, $3^6 \equiv 3 \cdot 5 \equiv 15$, $3^7 \equiv 3 \cdot 15 \equiv 11$, $3^8 \equiv 3 \cdot 11 \equiv 16 \neq 1$.

- (c) Completely determine all group homomorphisms from
- \mathbf{Z}_{17}^\times
- into
- \mathbf{Z}_7^\times
- .

Solution: Any group homomorphism $\phi : \mathbf{Z}_{17}^\times \rightarrow \mathbf{Z}_7^\times$ is determined by its value on the generator $[3]_{17}$, and the order of $\phi([3]_{17})$ must be a common divisor of 16 and 6. The only possible orders are 1 and 2, so either $\phi([3]_{17}) = [1]_7$ or $\phi([3]_{17}) = [-1]_7$. In the first case, $\phi([x]_{17}) = [1]_7$ for all $[x]_{17} \in \mathbf{Z}_{17}^\times$, and in the second case $\phi([3]_{17}^n) = [-1]_7^n$, for all $[x]_{17} = ([3]_{17})^n \in \mathbf{Z}_{17}^\times$.

20. Define $\phi : \mathbf{Z}_4 \times \mathbf{Z}_6 \rightarrow \mathbf{Z}_4 \times \mathbf{Z}_3$ by $\phi(x, y) = (x + 2y, y)$.

(a) Show that ϕ is a well-defined group homomorphism.

Solution: If $y_1 \equiv y_2 \pmod{6}$, then $2y_1 - 2y_2$ is divisible by 12, so $2y_1 \equiv 2y_2 \pmod{4}$, and then it follows quickly that ϕ is a well-defined function. It is also easy to check that ϕ preserves addition.

(b) Find the kernel and image of ϕ , and apply the fundamental homomorphism theorem.

Solution: If (x, y) belongs to $\ker(\phi)$, then $y \equiv 0 \pmod{3}$, so $y = 0$ or $y = 3$. If $y = 0$, then $x = 0$, and if $y = 3$, then $x = 2$. Thus the elements of the kernel K are $(0, 0)$ and $(2, 3)$.

It follows that there are $24/2 = 12$ cosets of the kernel. These cosets are in one-to-one correspondence with the elements of the image, so ϕ must map $\mathbf{Z}_4 \times \mathbf{Z}_6$ onto $\mathbf{Z}_4 \times \mathbf{Z}_3$. Thus $(\mathbf{Z}_4 \times \mathbf{Z}_6)/\{(0, 0), (2, 3)\} \cong \mathbf{Z}_4 \times \mathbf{Z}_3$.

21. Let n and m be positive integers, such that m is a divisor of n . Show that $\phi : \mathbf{Z}_n^\times \rightarrow \mathbf{Z}_m^\times$ defined by $\phi([x]_n) = [x]_m$, for all $[x]_n \in \mathbf{Z}_n^\times$, is a well-defined group homomorphism.

Solution: First, ϕ is a well-defined function, since if $[x_1]_n = [x_2]_n$ in \mathbf{Z}_n^\times , then $n \mid (x_1 - x_2)$, and this implies that $m \mid (x_1 - x_2)$, since $m \mid n$. Thus $[x_1]_m = [x_2]_m$, and so $\phi([x_1]_n) = \phi([x_2]_n)$.

Next, ϕ is a homomorphism since for $[a]_n, [b]_n \in \mathbf{Z}_n^\times$, $\phi([a]_n[b]_n) = \phi([ab]_n) = [ab]_m = [a]_m[b]_m = \phi([a]_n)\phi([b]_n)$.

22. For the group homomorphism $\phi : \mathbf{Z}_{36}^\times \rightarrow \mathbf{Z}_{12}^\times$ defined by $\phi([x]_{36}) = [x]_{12}$, for all $[x]_{36} \in \mathbf{Z}_{36}^\times$, find the kernel and image of ϕ , and apply the fundamental homomorphism theorem.

Solution: The previous problem shows that ϕ is a group homomorphism. It is evident that ϕ maps \mathbf{Z}_{36}^\times onto \mathbf{Z}_{12}^\times , since if $\gcd(x, 12) = 1$, then $\gcd(x, 36) = 1$. The kernel of ϕ consists of the elements in \mathbf{Z}_{36}^\times that are congruent to 1 mod 12, namely $[1]_{36}, [13]_{36}, [25]_{36}$. It follows that $\mathbf{Z}_{12}^\times \cong \mathbf{Z}_{36}^\times / \langle [13]_{36} \rangle$.

23. Let G , G_1 , and G_2 be groups. Let $\phi_1 : G \rightarrow G_1$ and $\phi_2 : G \rightarrow G_2$ be group homomorphisms. Prove that $\phi : G \rightarrow G_1 \times G_2$ defined by $\phi(x) = (\phi_1(x), \phi_2(x))$, for all $x \in G$, is a well-defined group homomorphism.

Solution: Given a, b in G , we have

$$\begin{aligned} \phi(ab) &= (\phi_1(ab), \phi_2(ab)) \\ &= (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b)) \end{aligned}$$

$$\begin{aligned} \phi(a)\phi(b) &= (\phi_1(a), \phi_2(a)) \cdot (\phi_1(b), \phi_2(b)) \\ &= (\phi_1(a)\phi_1(b), \phi_2(a)\phi_2(b)) \end{aligned}$$

and so $\phi : G \rightarrow G_1 \times G_2$ is a group homomorphism.

24. Let p and q be different odd primes. Prove that \mathbf{Z}_{pq}^\times is isomorphic to the direct product $\mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$.

Solution: Using Problem 21, we can define group homomorphisms $\phi_1 : \mathbf{Z}_{pq}^\times \rightarrow \mathbf{Z}_p^\times$ and $\phi_2 : \mathbf{Z}_{pq}^\times \rightarrow \mathbf{Z}_q^\times$ by setting $\phi_1([x]_{pq}) = [x]_p$, for all $[x]_{pq} \in \mathbf{Z}_{pq}^\times$, and $\phi_2([x]_{pq}) = [x]_q$, for all $[x]_{pq} \in \mathbf{Z}_{pq}^\times$.

Using Problem 23, we can define a group homomorphism $\phi : \mathbf{Z}_{pq}^\times \rightarrow \mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$ by setting $\phi([x]_{pq}) = (\phi_1([x]_{pq}), \phi_2([x]_{pq}))$, for all $[x]_{pq} \in \mathbf{Z}_{pq}^\times$. If $[x]_{pq} \in \ker(\phi)$, then $[x]_p = [1]_p$ and $[x]_q = [1]_q$, so $p \mid (x-1)$ and $q \mid (x-1)$, and this implies that $pq \mid (x-1)$, since p and q are relatively prime. It follows that $[x]_{pq} = [1]_{pq}$, and this shows that ϕ is a one-to-one function. Exercise 1.4.27 in the text states that if $m > 0$ and $n > 0$ are relatively prime integers, then $\varphi(mn) = \varphi(m)\varphi(n)$. It follows that \mathbf{Z}_{pq}^\times and $\mathbf{Z}_p^\times \times \mathbf{Z}_q^\times$ have the same order, so ϕ is also an onto function. This completes the proof that ϕ is a group isomorphism.