Homework 6: Sections 13 & 14

Algebra

Author

Paul Beggs
BeggsPA@Hendrix.edu

Instructor

Dr. Christopher Camfield, Ph.D.

Due

November 18, 2025

Section 13

In Exercises 4 and 5, determine whether the given map φ is a homomorphism. [*Hint:* The straightforward way to proceed is to check whether $\varphi(ab) = \varphi(a)\varphi(b)$ for all a and b in the domain of φ. However, if we should happen to notice that $\varphi^{-1}[\{e'\}]$ is not a subgroup whose left and right cosets coincide, or that φ does not satisfy the properties given in Exercise 44 or 45 for finite groups, then we can say at once that φ is not a homomorphism.]

4. Let $\varphi : \mathbb{Z}_6 \to \mathbb{Z}_2$ be given by $\varphi(x) =$ the remainder of x when divided by 2, as in the division algorithm.

Solution. We know $\varphi(x) = x \bmod 2$, and we have binary operators $(a+b) \bmod 6$ for $\mathbb{Z}_6$ and $(a+b) \bmod 2$ for $\mathbb{Z}_2$. This leaves us with the following equation to check:

$$\varphi((a+b) \bmod 6) \stackrel{?}{=} (\varphi(a) + \varphi(b)) \bmod 2$$

For the left-hand side:

$$\varphi((a+b) \bmod 6) = ((a+b) \bmod 6) \bmod 2.$$

This simplifies down to $(a+b) \bmod 2$ since $6 \equiv 0 \pmod 2$. For the right-hand side:

$$(\varphi(a) + \varphi(b)) \bmod 2 = (a \bmod 2 + b \bmod 2) \bmod 2.$$

Since addition is commutative and associative in both groups, we can rewrite this as:

$$(a+b) \bmod 2.$$

Therefore, the equation holds, and the map is a homomorphism.

5. Let $\varphi : \mathbb{Z}_9 \to \mathbb{Z}_2$ be given by $\varphi(x) =$ the remainder of x when divided by 2, as in the division algorithm.

Solution. This is not a homomorphism because the two sides of the equation are not equal:

$$\varphi((3+7) \bmod 9) = \varphi(1) = 1,$$

but

$$(\varphi(3) + \varphi(7)) \bmod 2 = (1+1) \bmod 2 = 0.$$

In Exercises 19 and 23, compute the indicated quantities for the given homomorphism φ. (See Exercise 46.)

19. $\ker(\varphi)$ and $\varphi(20)$ for $\varphi : \mathbb{Z} \to S_8$ such that $\varphi(1) = (1, 4, 2, 6)(2, 5, 7)$.

Solution. We know $\varphi(1) = (1, 4, 2, 6)(2, 5, 7) = (1, 4, 2, 5, 7, 6)$ has order 6, so $\ker(\varphi) = 6\mathbb{Z}$. Then, we know from the homomorphism property:

$$\varphi(20) = (\varphi(1))^{20} = (\varphi(1))^{18}(\varphi(1))^2 = (\varphi(1))^2 = (1, 2, 7)(4, 5, 6).$$

23. $\ker(\varphi)$ and $\varphi(4, 6)$ for $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\varphi(1, 0) = (2, -3)$ and $\varphi(0, 1) = (-1, 5)$.

Solution. We have:

$$\varphi(x, y) = \varphi(x, 0) + \varphi(0, y) = x\varphi(1, 0) + y\varphi(0, 1) = (2x - y, -3x + 5y).$$

To find the kernel, we set $\varphi(x, y) = (0, 0)$:

$$2x - y = 0 \quad \text{and} \quad -3x + 5y = 0$$

From the first equation, we have $y = 2x$. Substituting into the second equation gives:

$$-3x + 5(2x) = -3x + 10x = 7x = 0 \implies x = 0.$$

Thus, $y = 0$ as well. Therefore, $\ker(\varphi) = \{(0, 0)\}$. Now, we find $\varphi(4, 6)$:

$$\varphi(4, 6) = (2(4) - 6, -3(4) + 5(6)) = (8 - 6, -12 + 30) = (2, 18).$$

44. Let $\varphi : G \to G'$ be a group homomorphism. Show that if $|G|$ is finite, then $|\varphi[G]|$ is finite and is a divisor of $|G|$.

Proof. Let $\varphi : G \to G'$ be a group homomorphism, and let $H = \ker(\varphi)$. Our goal is to show that the order of the preimage of G, $|\varphi[G]|$, is finite, and a divisor of $|G|$, given G is finite. The theorem $aH = \varphi^{-1}[\{\varphi(a)\}]$ maps a single coset to the same single element $\varphi(a)$ in the image. This establishes a one-to-one correspondence between the set of all cosets (G/H) and the set of all images, $\varphi[G]$. Because there is a one-to-one correspondence, the two sets must have equal size: $|G/H| = |\varphi[G]|$. Then, by Lagrange's Theorem, since G is finite, the number of cosets (G/H) must be a finite number that divides the order of the group, $|G|$. Since $|G/H| = |\varphi[G]|$, it follows that $|\varphi[G]|$ must also be a finite number that divides $|G|$. □

45. Let $\varphi : G \to G'$ be a group homomorphism. Show that if $|G'|$ is finite, then $|\varphi[G]|$ is finite and is a divisor of $|G'|$.

Proof. From Theorem 13.12 (3) (the fundamental properties of homomorphisms), if H is a subgroup of G, then $\varphi[H]$ is a subgroup of G'. Now, let $H = G$. It is certainly true that G is a subgroup of G, so $\varphi[G]$ is a subgroup of G'. Then, by Lagrange's Theorem, since $|G'|$ is finite, the order of its subgroup, $|\varphi[G]|$ is also a finite number that divides $|G'|$. □

49. Show that if G, G', and G'' are groups and if $\varphi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms, then the composite map $\gamma\varphi : G \to G''$ is a homomorphism.

Proof. Let $a, b \in G$. Then,

$$\begin{aligned}(\gamma\varphi)(ab) &= \gamma(\varphi(ab)) && (1)\\ &= \gamma(\varphi(a)\varphi(b)) && (2)\\ &= \gamma(\varphi(a))\gamma(\varphi(b)) && (3)\\ &= (\gamma\varphi)(a)(\gamma\varphi)(b). && (4)\end{aligned}$$

Equations (1) and (4) are from the definition of a composite map, and (2) and (3) are from the homomorphic properties of φ and γ, respectively. Therefore, we have shown that the composite map is a homomorphism. □

Section 14

In Exercises 2 and 6, find the order of the given factor group.

2. $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle 2\rangle \times \langle 2\rangle)$

Solution. In $\mathbb{Z}_4$, the subgroup generated by $\langle 2\rangle$ is $\{0, 2\}$. Then, in $\mathbb{Z}_{12}$, the subgroup generated by $\langle 2\rangle$ is $\{0, 2, 4, 6, 8, 10\}$. Thus, the subgroup $\langle 2\rangle \times \langle 2\rangle$ has order $2 \times 6 = 12$, and $\mathbb{Z}_4 \times \mathbb{Z}_{12}$ has order $4 \times 12 = 48$. By Lagrange's Theorem, the order of the factor group is $48/12 = 4$.

6. $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle(4, 3)\rangle$

Solution. The order of $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$ is $12 \times 18 = 216$. In $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$, the subgroup generated by $\langle(4, 3)\rangle$ has order 6. So, by Lagrange's Theorem, the order of the factor group is $216/6 = 36$.

In Exercises 11 and 15, give the order of the element in the factor group.

11. $(2,1) + \langle(1,1)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,1)\rangle$

Solution. In $\mathbb{Z}_3 \times \mathbb{Z}_6$, $\langle(1,1)\rangle = \{(1,1),(2,2),(0,3),(1,4),(2,5),(0,0)\}$. Then, we test the powers of $(2,1)$ until we find one that is in $\langle(1,1)\rangle$:

$$(2,1)(2,1) = (1,2), \quad (1,2)(2,1) = (0,3).$$

So, the order of $(2,1) + \langle(1,1)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle(1,1)\rangle$ is 3.

15. $(2,0) + \langle(4,4)\rangle$ in $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle(4,4)\rangle$

Solution. Since $(2,0)$ is in $\langle(4,4)\rangle$, $(2,0) + \langle(4,4)\rangle$ has order 1.

27. A subgroup H is **conjugate to a subgroup** K of a group G if there exists an inner automorphism i_g of G such that $i_g[H] = K$. Show that conjugacy is an equivalence relation on the collection of subgroups of G.

Proof. Let H, K, and L be subgroups of G. To show that conjugacy is an equivalence relation on the collection of subgroups of G, we must show the following:

- **Reflexive:** We must show that H is conjugate to itself. That is, we must find an element $g \in G$ such that $H = i_g[H] = gHg^{-1}$. The obvious choice is the identity element $e \in G$:

$$H = i_e[H] = eHe^{-1} = \{ehe^{-1} \mid h \in H\} = \{h \mid h \in H\} = H.$$

  Thus, we have found an element $g = e$ such that $i_g[H] = H$, so the subgroup is conjugate to itself. Therefore, the relation is reflexive.

- **Symmetric:** Assume H to be congruent to K (i.e., $K = i_g[H] = gHg^{-1}$ for some $g \in G$). We must show K is congruent to H. That is, for some $g' \in G$, $H = i_{g'}[K] = g'Kg'^{-1}$. If we multiply $K = gHg^{-1}$ by g^{-1} and g on the left and right, respectively, we get $g^{-1}Kg = H$. Thus, we have found our elements $g' = g^{-1}$, and $g'^{-1} = g$. Therefore, the relation is symmetric.

- **Transitive:** Assume H to be congruent to K and K to be congruent to L. Then, $K = gHg^{-1}$ and $L = pKp^{-1}$ for some $p \in G$. We want to show $L = g''Hg''^{-1}$. We can do that by using substitution:

$$L = pKp^{-1} = pgHg^{-1}p^{-1}.$$

  Notice $pg = g''$ and $g^{-1}p^{-1} = (pg)^{-1} = g''$. The product pg and $(pg)^{-1}$ are both in G because G is a group. Thus, we have shown that H is conjugate to L. Therefore, the relation is transitive. □

30. Let H be a normal subgroup of a group G, and let $m = (G : H)$. Show that $a^m \in H$ for every $a \in G$.

Proof. Let H be a normal subgroup of G and let $m = (G : H)$. Because H is normal, we can form the factor group G/H. The order of this group, $|G/H|$, is equal to the index of H in G, so $|G/H| = m$. Now, let a be any element in G. The corresponding element in the factor group G/H is the coset aH. Let k be the order of this element aH in the factor group. By the definition of order, $(aH)^k = H$ (where H is the identity element of the factor group). By Lagrange's Theorem, the order of an element must divide the order of the group. Therefore, k divides m. This implies that $m = kq$ for some integer q. Now, we can compute $(aH)^m$:

$$(aH)^m = (aH)^{kq} = ((aH)^k)^q.$$

Since $(aH)^k = H$, we can substitute this back in:

$$((aH)^k)^q = H^q = H.$$

Thus, we have shown that $(aH)^m = a^m H = H$. By the properties of cosets, $gH = H$ implies $g \in H$. Consequently, $a^m \in H$. $\square$