Homework 11 Solution

Chapter 10.

7. If ϕ is a homomorphism from G to H and σ is a homomorphism from H to K, show that $\sigma\phi$ is a homomorphism from G to K. How are $\ker\phi$ and $\ker\sigma\phi$ related? If ϕ and σ are onto and G is finite, describe $[\ker\sigma\phi : \ker\phi]$ in terms of $|H|$ and $|K|$.

   For $a, b \in G$,

   $$\sigma\phi(ab) = \sigma(\phi(ab)) = \sigma(\phi(a)\phi(b)) = \sigma(\phi(a))\sigma(\phi(b)) = \sigma\phi(a)\sigma\phi(b).$$

   So $\sigma\phi$ is a homomorphism.

   If $a \in \ker\phi$, then $\sigma\phi(a) = \sigma(e_H) = e_K$ where e_H (resp. e_K) is the identity of H (resp. K). Therefore $a \in \ker\sigma\phi$. This implies that $\ker\phi \le \ker\sigma\phi$. Furthermore, $\ker\phi \triangleleft \ker\sigma\phi$. Indeed, $\ker\phi \triangleleft G$ so for every element $g \in \ker\sigma\phi \le G$, $g\ker\phi g^{-1} \subset \ker\phi$.

   Moreover, if ϕ and σ are onto and G is finite, then from the first isomorphism theorem, $|G| = |\ker\phi||\phi(G)| = |\ker\phi||H|$ and $|G| = |\ker\sigma\phi||\sigma\phi(G)| = |\ker\sigma\phi||K|$. So

   $$[\ker\sigma\phi : \ker\phi] = |\ker\sigma\phi|/|\ker\phi| = \frac{|G|/|K|}{|G|/|H|} = |H|/|K|.$$

9. Prove that the mapping from $G \oplus H$ to G given by $(g, h) \to g$ is a homomorphism. What is the kernel? This mapping is called the *projection* of $G \oplus H$ onto G.

   Let $\phi : G \oplus H \to G$ be a map defined as $\phi(g, h) = g$. For $(g_1, h_1), (g_2, h_2) \in G \oplus H$,

   $$\phi((g_1, h_1)(g_2, h_2)) = \phi(g_1g_2, h_1h_2) = g_1g_2 = \phi(g_1, h_1)\phi(g_2, h_2).$$

   Therefore ϕ is a homomorphism.

   Note that

   $$(g, h) \in \ker\phi \Leftrightarrow \phi(g, h) = g = e.$$

   Therefore $\ker\phi = \{(e, h) \mid h \in H\} = \{e\} \oplus H$ (This group is isomorphic to H.).

12. Suppose that k is a divisor of n. Prove that $\mathbb{Z}_n/\langle k\rangle \cong \mathbb{Z}_k$.

   For these kind of problems, the best approach is using the first isomorphism theorem.

   Define a map $\phi : \mathbb{Z}_n \to \mathbb{Z}_k$ as $\phi(m) = m \bmod k$. If $m_1 \bmod n = m_2 \bmod n$, then $n|m_1 - m_2$. Because $k|n$, $k|m_1 - m_2$ and $m_1 \bmod k = m_2 \bmod k$. Therefore ϕ is well-defined. Moreover, $\phi(m_1 + m_2) = m_1 + m_2 \bmod k = m_1 \bmod k + m_2 \bmod k$. So ϕ is a homomorphism. Furthermore, for $0 \le m \le k - 1$, $\phi(m) = m$. Therefore ϕ is onto.

Because

$$m \in \ker \phi \Leftrightarrow m \bmod k = 0 \Leftrightarrow k|m,$$

$\ker \phi = \langle k \rangle$. By the first isomorphism theorem, $\mathbb{Z}_n/\langle k \rangle = \mathbb{Z}_n/\ker \phi \approx \phi(\mathbb{Z}_n) = \mathbb{Z}_k$.

16. Prove that there is no homomorphism from $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ onto $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.

    Suppose that $\phi : \mathbb{Z}_8 \oplus \mathbb{Z}_2 \to \mathbb{Z}_4 \oplus \mathbb{Z}_4$ is a homomorphism.

    Sol 1. Because $|\mathbb{Z}_8 \oplus \mathbb{Z}_2| = 16 = |\mathbb{Z}_4 \oplus \mathbb{Z}_4|$, if ϕ is onto, then it is an isomorphism. But $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ has an element of order 8 ($(1, 0)$), and all elements of $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ have order at most 4. Therefore they are not isomorphic.

    Sol 2. Because all elements of $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ have order at most 4, $\phi(4 \cdot a) = 4\phi(a) = 0$ for every $a \in \mathbb{Z}_8 \oplus \mathbb{Z}_2$. In particular, $\phi(4, 0) = \phi(4 \cdot (1, 0)) = 0$ and $(4, 0) \in \ker \phi$ and $|\ker \phi| > 1$. Therefore

    $$|\phi(\mathbb{Z}_8 \oplus \mathbb{Z}_2)| = |\mathbb{Z}_8 \oplus \mathbb{Z}_2|/|\ker \phi| < |\mathbb{Z}_8 \oplus \mathbb{Z}_2| = 16 = |\mathbb{Z}_4 \oplus \mathbb{Z}_4|$$

    and ϕ is not onto.

18. Can there be a homomorphism from $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ onto $\mathbb{Z}_8$? Can there be a homomorphism from $\mathbb{Z}_{16}$ onto $\mathbb{Z}_2 \oplus \mathbb{Z}_2$? Explain your answers.

    For any homomorphism $\phi : \mathbb{Z}_4 \oplus \mathbb{Z}_4 \to \mathbb{Z}_8$, $|\phi(a)| \le |a| \le 4$ because any element in $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ has order at most 4. But in $\mathbb{Z}_8$, there is an element of order 8. So ϕ is not onto.

    For a homomorphism $\psi : \mathbb{Z}_{16} \to \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\psi(\mathbb{Z}_{16})$ is a cyclic group generated by $\psi(1)$. But $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not cyclic, so $\psi(\mathbb{Z}_{16}) \ne \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Therefore ψ is not onto.

22. Suppose that ϕ is a homomorphism from a finite group G onto $\overline{G}$ and that $\overline{G}$ has an element of order 8. Prove that G has an element of order 8. Generalize.

    Let's prove a general statement: For a surjective homomorphism $\phi : G \to \overline{G}$ between finite groups, if $\overline{G}$ has an element of order n, then so does G.

    Let $a \in \overline{G}$ be an element of order n. Because ϕ is onto, there is $b \in G$ such that $\phi(b) = a$. We have $|a| = |\phi(b)|||b|$, so $|b|$ is a multiple of n. Let $|b| = nk$. Then $|b^k| = n$.

29. Suppose that there is a homomorphism from a finite group G onto $\mathbb{Z}_{10}$. Prove that G has normal subgroups of indexes 2 and 5.

    Let $\phi : G \to \mathbb{Z}_{10}$ be such a homomorphism. Because $\mathbb{Z}_{10}$ is Abelian, $\langle 5 \rangle$ (resp. $\langle 2 \rangle$) is a normal subgroup of $\mathbb{Z}_{10}$ of order 2 (resp. 5). Then $H := \phi^{-1}(\langle 5 \rangle)$ and $K := \phi^{-1}(\langle 2 \rangle)$ are normal subgroups of G.

    If $n = |\ker \phi|$, then $\phi : G \to \mathbb{Z}_{10}$ is $n : 1$ map. So $|G| = 10n$. Also, $|H| = n|\langle 5 \rangle = 2n$ and $|K| = n|\langle 2 \rangle| = 5n$. Therefore

    $$[G : H] = |G|/|H| = 10n/2n = 5$$

    and

    $$[G : K] = |G|/|K| = 10n/5n = 2.$$

40. For each pair of positive integers m and n, we can define a homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_m \oplus \mathbb{Z}_n$ by $x \to (x \bmod m, x \bmod n)$. What is the kernel when $(m, n) = (3, 4)$? What is the kernel when $(m, n) = (6, 4)$? Generalize.

    Let's prove a general statement. Let $\phi : \mathbb{Z} \to \mathbb{Z}_m \oplus \mathbb{Z}_n$ be the homomorphism defined as $\phi(x) = (x \bmod m, x \bmod n)$. If $x \in \ker \phi$, then $x \bmod n = 0$ and $x \bmod n = 0$. Therefore x is a common multiple of m and n, so x is a multiple of $\mathrm{lcm}(m, n)$. On the other hand, if $\mathrm{lcm}(m, n)|x$, then $m|x$ and $n|x$. Thus $\phi(x) = (0, 0)$ and $x \in \ker \phi$. In summary, $\ker \phi = \langle \mathrm{lcm}(m, n)\rangle$.

46. Let N be a normal subgroup of a finite group G. Use the theorems of this chapter to prove that the order of the group element gN in G/N divides the order of g.

    If $|g| = n$, then $(gN)^n = g^n N = eN = N$. So $|gN||n = |g|$.

51. Let N be a normal subgroup of a group G. Use property 7 of Theorem 10.2 to prove that every subgroup of G/N has the form H/N, where H is a subgroup of G.

    Define $\phi : G \to G/N$ as $\phi(a) = aN$. Then $\phi(ab) = abN = aNbN = \phi(a)\phi(b)$, so ϕ is a homomorphism. Also from the definition, it is obvious that ϕ is onto.

    Let $\overline{H}$ be a subgroup of G/N. Then $H := \phi^{-1}(\overline{H}) \le G$. Because ϕ is onto, $\phi(H) = \phi(\phi^{-1}(\overline{H})) = \overline{H}$. On the other hand, $\phi(H) = H/N$. Therefore $\overline{H} = H/N$.

61. Prove that every group of order 77 is cyclic.

    Let G be a group of order 77.

    Step 1. There is a unique subgroup H of order 11.

    Because 11 is a prime divisor of 77, there is $a \in G$ with $|a| = 11$. In particular, there is a subgroup $|\langle a\rangle|$ of order 11. If there are two distinct subgroups H and K of order 11, then $|H \cap K|||H| = 11$, so $|H \cap K| = 1$. So

$$77 = |G| \ge |HK| = \frac{|H||K|}{|H \cap K|} = 121,$$

    which is impossible. Therefore there is a unique subgroup of order 11. Let H be the unique subgroup of order 11.

    Step 2. H is a normal subgroup.

    For any $g \in G$, gHg^{-1} is a subgroup of order 11. Because there is a unique subgroup of order 11, $gHg^{-1} = H$ for every $g \in G$. Therefore $H \lhd G$.

    Step 3. Define a homomorphism $f : G \to \mathrm{Aut}(H)$.

    Now define a map $f : G \to \mathrm{Aut}(H)$ by $f(a) = \phi_a$, where $\phi_a(h) = aha^{-1}$. Note that $H \lhd G$, so $aha^{-1} \in H$ for every $a \in G$. On the other hand,

$$\phi_{ab}(h) = abh(ab)^{-1} = abhb^{-1}a^{-1} = a\phi_b(h)a^{-1} = \phi_a\phi_b(h),$$

    so $\phi_{ab} = \phi_a\phi_b$. So $f(ab) = \phi_{ab} = \phi_a\phi_b = f(a)f(b)$ and f is a homomorphism.

Step 4. $gh = hg$ for all $g \in G$ and $h \in H$.

Because $\mathrm{Aut}(H) \approx \mathrm{Aut}(\mathbb{Z}_{11}) \approx U(11) \approx \mathbb{Z}_{10}$ and $|G| = 77$ is relatively prime to $|\mathrm{Aut}(H)| = 10$, f is a trivial homomorphism, i.e., $\phi_g = f(g) = \mathrm{id} \in \mathrm{Aut}(H)$ for all $g \in G$. Therefore for any $g \in G$, $\phi_g(h) = ghg^{-1} = h$. Therefore $gh = hg$ for every $g \in G$ and $h \in H$.

Step 5. Find a generator of G.

Finally, let b be an element of order 7. Then $(ba)^i = b^i a^i$ because $a \in H$. Then $|ba|$ is 1, 7, 11, or 77. If $|ba| = 1$, then $b = a^{-1} \in H$ so it is impossible. If $|ba| = 7$, then $e = (ba)^7 = b^7 a^7 = a^7$. But $|a| = 11$ so it is also impossible. By a similar reason, $|ba| = 11$ is also impossible. Therefore $|ba| = 77$ and $G = \langle ba \rangle$.

62. Determine all homomorphisms from $\mathbb{Z}$ onto S_3. Determine all homomorphisms from $\mathbb{Z}$ to S_3.

Let $\phi : \mathbb{Z} \to S_3$ be a homomorphism. $\phi(\mathbb{Z})$ is an Abelian group, so $\phi(\mathbb{Z}) \neq S_3$. So there is no surjective homomorphism.

Note that ϕ is completely determined by $\phi(1)$ because $\mathbb{Z} = \langle 1 \rangle$. There are 6 elements in S_3. So there are six homomorphisms from $\mathbb{Z}$ to S_3.

66. Let p be a prime. Determine the number of homomorphisms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$ into $\mathbb{Z}_p$.

Note that $\mathbb{Z}_p \oplus \mathbb{Z}_p$ has two generators $(1, 0)$ and $(0, 1)$. So the homomorphism $\phi : \mathbb{Z}_p \oplus \mathbb{Z}_p \to \mathbb{Z}_p$ is completely determined by $\phi(1, 0)$ and $\phi(0, 1)$ because $\phi(m, n) = m\phi(1, 0) + n\phi(0, 1)$.

Conversely, for any $a, b \in \mathbb{Z}_p$, if we define a map $\phi : \mathbb{Z}_p \oplus \mathbb{Z}_p \to \mathbb{Z}_p$ as $\phi(m, n) = ma + nb \bmod p$, then this map is well-defined. Indeed, if $(m_1, n_1) = (m_2, n_2)$, then $m_1 \bmod p = m_2 \bmod p$ and $n_1 \bmod p = n_2 \bmod p$ so $m_1 a + n_1 b \bmod p = m_2 a + n_2 b \bmod p$. Furthermore, ϕ is a homomorphism because $\phi((m_1, n_1) + (m_2, n_2)) = \phi(m_1 + m_2, n_1 + n_2) = (m_1 + m_2)a + (n_1 + n_2)b \bmod p = m_1 a + n_1 b \bmod p + m_2 a + n_2 b \bmod p = \phi(m_1, n_1) + \phi(m_2, n_2)$.

Because $|(1, 0)| = |(0, 1)| = p$ and any element in $\mathbb{Z}_p$ has order p or 1, so $\phi(1, 0)$ and $\phi(0, 1)$ can be any element of $\mathbb{Z}_p$. Therefore the number of homomorphisms is p^2.