Solutions: Homework 5

March 6, 2020

Problem 1. List the elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$. Find the order of each element. Is this group cyclic?

Proof. The elements of $\mathbb{Z}_3 \times \mathbb{Z}_4$ and its orders are

\[
\begin{align*}
(0,0) & \text{ order:1} \\
(0,1) & \text{ order:4} \\
(0,2) & \text{ order:2} \\
(0,3) & \text{ order:4} \\
(1,0) & \text{ order:3} \\
(1,1) & \text{ order:12} \\
(1,2) & \text{ order:6} \\
(1,3) & \text{ order:12} \\
(2,0) & \text{ order:3} \\
(2,1) & \text{ order:12} \\
(2,2) & \text{ order:6} \\
(2,3) & \text{ order:12}
\end{align*}
\]

Since $\mathbb{Z}_3 \times \mathbb{Z}_4$ has an element of order 12 = $|\mathbb{Z}_3 \times \mathbb{Z}_4|$, it is cyclic. \(\square\)

Problem 2. Find the maximum possible order for some element of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

Proof. We note that for any element $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$, the order of $(a, b)$ is the lcm of the order of $a$ in $\mathbb{Z}_4$ and the order of $b$ in $\mathbb{Z}_6$. Since the order of $a$ divides 4 and the order of $b$ divides 6, we must have that their lcm should divide lcm(4, 6) = 12. So, any element of $\mathbb{Z}_4 \times \mathbb{Z}_6$ should have order \(\leq 12\). Note that $(1,1)$ has order 12. So, we have an element of order 12. So, 12 is the maximum possible order for an element of $\mathbb{Z}_4 \times \mathbb{Z}_6$. \(\square\)

Problem 3. (a) Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic?
(b) Are the groups $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_{36} \times \mathbb{Z}_{10}$ isomorphic?
Proof. (a) Note that \( \mathbb{Z}_2 \times \mathbb{Z}_{12} \) is isomorphic to \( \mathbb{Z}_2 \times (\mathbb{Z}_3 \times \mathbb{Z}_4) = (\mathbb{Z}_2 \times \mathbb{Z}_3) \times \mathbb{Z}_4 \). But \( \mathbb{Z}_2 \times \mathbb{Z}_3 \) is isomorphic to \( \mathbb{Z}_6 \). So, we have that \( \mathbb{Z}_2 \times \mathbb{Z}_{12} \) is isomorphic to \( \mathbb{Z}_4 \times \mathbb{Z}_6 \).

(b) Similarly, we have that \( \mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15} \) is isomorphic to \( \mathbb{Z}_4 \times (\mathbb{Z}_2 \times \mathbb{Z}_9) \times (\mathbb{Z}_5 \times \mathbb{Z}_3) \). Grouping the \( \mathbb{Z}_5 \) and the \( \mathbb{Z}_2 \) together and the \( \mathbb{Z}_4 \) and the \( \mathbb{Z}_9 \) together, we get \( \mathbb{Z}_3 \times \mathbb{Z}_{36} \times \mathbb{Z}_{10} \). So, \( \mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15} \) and \( \mathbb{Z}_3 \times \mathbb{Z}_{36} \times \mathbb{Z}_{10} \) are isomorphic.

Problem 4. Determine if the given map is a homomorphism.

(a) Let \( \phi : \mathbb{R} \to \mathbb{Z} \) be given by \( \phi(x) = \) the greatest integer \( \leq x \).

(b) Let \( \phi : \mathbb{R}^\times \to \mathbb{R}^\times \) be given by \( \phi(x) = |x| \).

(c) Let \( G \) be an abelian group and let \( \phi : G \to G' \) be given by \( \phi(g) = g^{-1} \). What if \( G \) is not abelian?

Proof. (a) No, because \( \phi(0.5) = 0 \), but \( \phi(1) = 1 \neq \phi(0.5) + \phi(0.5) = 0 \).

(b) Let \( x, y \in \mathbb{R}^\times \). Then \( \phi(xy) = |xy| = |x||y| = \phi(x)\phi(y) \). So, \( \phi \) is a homomorphism.

(c) Let \( g, h \in G \). Then \( \phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} \) because \( G \) is abelian. Now, \( g^{-1}h^{-1} = \phi(g)\phi(h) \). So, \( \phi(gh) = \phi(g)\phi(h) \) for all \( g, h \in G \). Suppose \( G \) is not abelian. Then there exists \( g, h \in G \) such that \( gh \neq hg \). Then \( \phi(gh) = (gh)^{-1} \) and \( \phi(g)\phi(h) = g^{-1}h^{-1} = (hg)^{-1} \). Since \( gh \neq hg \), \( \phi(gh) \neq \phi(g)\phi(h) \). Hence \( \phi \) cannot be a homomorphism.

Problem 5. (a) Suppose \( G = \langle a \rangle \) is a cyclic group. Prove that any homomorphism \( \phi : G \to G' \) is uniquely determined by the value \( \phi(a) \).

(b) How many homomorphisms are there from \( \mathbb{Z} \to \mathbb{Z} \)?

(c) How many onto homomorphisms are there from \( \mathbb{Z} \to \mathbb{Z} \)?

Proof. (a) Suppose \( \phi : G \to G' \) is a homomorphism. We know that \( G = \langle a \rangle \). Suppose that we know \( \phi(a) \). Let \( g \in G \). Then \( g = a^n \) for some \( n \in \mathbb{Z} \). Then \( \phi(g) = \phi(a^n) = \phi(a)a...a = \phi(a)^n \) because \( \phi \) is a homomorphism. (Here, be \( a.a...a \), we mean \( a \) multiplied \( n \) times.) So, for any \( g \in G \), we know what \( \phi(g) \) is by just knowing what \( \phi(a) \) is. So, any homomorphism \( \phi : G \to G' \) is determined by \( \phi(a) \). Now, suppose that we have two homomorphisms \( \phi, \psi : G \to G' \) with \( \phi(a) = \psi(a) \). Then \( \phi(a^n) = \phi(a)^n = \psi(a)^n = \phi(a)^n \). So, for all \( g \in G \), \( \phi(g) = \psi(g) \) and hence \( \phi = \psi \). So, \( \phi(a) \) uniquely determines \( \phi \).

(b) Since \( Z \) is a cyclic group with generator 1, any homomorphism from \( \mathbb{Z} \to \mathbb{Z} \) is determined by \( \phi(1) \). Suppose that \( \phi(1) = n \). Then we see that for any \( x \in \mathbb{Z} \), \( \phi(x) = x\phi(1) = nx \). So, the homomorphism is given by \( \phi(x) = nx \) for all \( x \in \mathbb{Z} \). Now, for any \( n \in \mathbb{Z} \), we see that this has to be a homomorphism. So, all the homomorphisms from \( \mathbb{Z} \to \mathbb{Z} \) are given by \( \phi(x) = nx \) for some \( n \in \mathbb{Z} \). So, there are infinitely many homomorphisms, one each corresponding to each \( n \in \mathbb{Z} \).

(c) From part (b) above, we know that all the homomorphisms from \( \mathbb{Z} \to \mathbb{Z} \) are of the form \( \phi_n \) for \( n \in \mathbb{Z} \), where \( \phi_n(x) = nx \) for all \( x \in \mathbb{Z} \). If \( \phi_n \) is onto, there exists \( x \) such that \( nx = \phi_n(x) = 1 \). This implies that \( n \) divides 1. Hence \( n \) has to be 1 or -1. But note that \( \phi_1 \) and \( \phi_{-1} \) are clearly onto homomorphisms. So, there are two onto homomorphisms from \( \mathbb{Z} \to \mathbb{Z} \).

Problem 6. Let \( \phi : G \to G' \) be a homomorphism and suppose that \(|G| = p\), a prime number. Prove that \( \phi \) is either the trivial function \( \phi(g) = e' \) or \( \phi \) is one-to-one.
Proof. We know that \( \ker \phi \) is a subgroup of \( G \). So, by Lagrange’s theorem, \(|\ker \phi|\) divides \(|G|\) = \( p \). So, \(|\ker \phi| = 1 \) or \( p \). If \(|\ker \phi| = 1 \), then \( \ker \phi = \{e\} \). Suppose that \( \phi(g) = \phi(h) \) for some \( g, h \in G \). Then, \( \phi(g h^{-1}) = \phi(g) \phi(h^{-1}) = \phi(g) (\phi(h))^{-1} = e' \). Hence, \( g h^{-1} \in \ker \phi \), which implies that \( g h^{-1} = e \), and so \( g = h \). So, \( \phi \) is one-to-one. Now suppose that \(|\ker \phi| = p \). This implies that \( \ker \phi = G \). So, for all \( g \in G \), \( \phi(g) = e' \). So, this proves that \( \phi \) is either the trivial function or is one-to-one.

Problem 7. Show that if \( G, G' \) and \( G'' \) are groups and \( \phi : G \to G' \) and \( \psi : G' \to G'' \) are homomorphisms, then the composition \( \psi \circ \phi : G \to G'' \) is a homomorphism.

Proof. Let \( g, h \in G \). Then \((\psi \circ \phi)(gh) = \psi(\phi(gh)) = \psi(\phi(g)\phi(h)) = \psi(\phi(g))\psi(\phi(h)) = (\psi \circ \phi)(g)\psi(\phi)(h) \). So, \( \psi \circ \phi \) is a homomorphism.

Problem 8. Find the order of the given quotient group.
(a) \( \mathbb{Z}_6/\langle 3 \rangle \).
(b) \( (\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle (4, 3) \rangle \).

Proof. (a) \( \langle 3 \rangle = \{0, 3\} \). So, \(|\langle 3 \rangle| = 2 \). Therefore, \( |\mathbb{Z}_6/\langle 3 \rangle| = |\mathbb{Z}_6|/2 = 3 \).
(b) The order of \( 4 \) in \( \mathbb{Z}_{12} \) is 3 and that of \( 3 \) in \( \mathbb{Z}_{18} \) is 6. So, the order of \( (4, 3) \) in \( \mathbb{Z}_{12} \times \mathbb{Z}_{18} \) is \( \text{lcm}(3, 6) = 6 \). So, \(|\langle (4, 3) \rangle| = 6 \). Therefore, \(|(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle (4, 3) \rangle| = |\mathbb{Z}_{12} \times \mathbb{Z}_{18}|/6 = 216/6 = 36 \).

Problem 9. Show that \( A_n \) is a normal subgroup of \( S_n \) and compute \( S_n/A_n \). That is, find a known group to which \( S_n/A_n \) is isomorphic.

Proof. For any \( \sigma \in S_n \) and any \( \tau \in A_n \), note that \( \sigma \tau \sigma^{-1} \in A_n \). This is because since \( \tau \in A_n \), \( \tau \) is an even permutation, and both even.even and odd.even.odd are even permutations. So, \( \sigma \tau \sigma^{-1} \in A_n \) for any \( \sigma \in S_n \). This implies that \( A_n \) is a normal subgroup of \( S_n \). Now, \( |S_n/A_n| = |S_n|/|A_n| = n!/n!/2 = 2 \). We know that, up to isomorphism, the only group of order 2 is \( \mathbb{Z}_2 \). So, \( S_n/A_n \) is isomorphic to \( \mathbb{Z}_2 \).

Problem 10. (a) Show that all automorphisms of a group \( G \) form a group under function composition.
(b) Show that the inner automorphisms of a group \( G \) form a normal subgroup of the group in part (a).

Proof. (a) Let us denote by \( \text{Aut}(G) \) the set of all automorphisms of \( G \). We prove that this forms a group under function composition. Let \( \sigma, \tau \in \text{Aut}(G) \). Then, by Problem \( \sigma \circ \tau : G \to G \) is still a homomorphism. Also, we know that the composition of two bijective functions is bijective. So, \( \sigma \circ \tau \) is a bijective homomorphism, hence an automorphism. This proves that \( \text{Aut}(G) \) is closed under function composition. We already know that function composition is associative, so we just need to look for an identity element and then find inverses for each element. Let \( i : G \to G \) denote the function \( i(g) = g \) for all \( g \in G \). Then \( i \) is clearly an automorphism. So, \( i \in \text{Aut}(G) \). For any \( f \in \text{Aut}(G) \), we have \( f \circ i = f = i \circ f \). So, \( i \) acts as the identity. Now, let \( f \in \text{Aut}(G) \). Since \( f \) is a bijection, we can look at \( f^{-1} \). Obviously, \( f^{-1} \) is bijective. If we show that \( f^{-1} \) is a homomorphism, it shows that \( f^{-1} \in \text{Aut}(G) \), and hence
completes the proof of the fact that $\text{Aut}(G)$ is a group. So, let $g, h \in G$. Then, we have $gh = f(f^{-1}(gh))$ and $gh = f(f^{-1}(g))f(f^{-1}(h)) = f(f^{-1}(g)f^{-1}(h))$ where the last equality holds because $f$ is a homomorphism. So, we have $f(f^{-1}(gh)) = f(f^{-1}(g)f^{-1}(h))$. Since $f$ is bijective, this implies that $f^{-1}(gh) = f^{-1}(g)f^{-1}(h)$. So $f^{-1}$ is a homomorphism and hence, $\text{Aut}(G)$ is a group.

(b) Let us denote by $I$ the set of inner automorphisms of $G$, i.e. $I = \{\sigma_g | g \in G\}$ where $\sigma_g : G \to G$ is given by $\sigma_g(x) = gxg^{-1}$ for all $x \in G$. We first show that $I$ is a subgroup of $\text{Aut}(G)$. Note that $\sigma_e(x) = exe^{-1} = x$ for all $x \in G$. So $\sigma_e = i$, which implies that $i \in I$. So, $I$ contains the identity element of $\text{Aut}(G)$. Now, suppose that $\sigma_g, \sigma_h \in I$. We want to show that $\sigma_g \circ \sigma_h \in I$. Note that $(\sigma_g \circ \sigma_h)(x) = \sigma_g(\sigma_h(x)) = \sigma_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = ghx(gh)^{-1} = \sigma_{gh}(x)$. So, $\sigma_g \circ \sigma_h = \sigma_{gh} \in I$. So, $I$ is closed under function composition. Now, this computation above implies that for any $g \in G, \sigma_g \circ \sigma_g^{-1} = \sigma_{gg^{-1}} = \sigma_e = i$. So, $\sigma_g^{-1} = \sigma_{g^{-1}} \in I$. So, $I$ is also closed under inverses. This shows that $I$ is a subgroup of $\text{Aut}(G)$. Now let $\tau \in \text{Aut}(G)$ and $\sigma_g \in I$. Then $\tau \circ \sigma_g \circ \tau^{-1}(x) = \tau(\sigma_g(\tau^{-1}(x))) = \tau(g\tau^{-1}(x)g^{-1}) = \tau(g)\tau(\tau^{-1}(x))\tau(g^{-1}) = \tau(g)x\tau(g)^{-1} = \sigma_{\tau(g)}(x)$ for all $x \in G$. So, $\tau \circ \sigma_g \circ \tau^{-1} = \sigma_{\tau(g)} \in I$. So, for any $\tau \in \text{Aut}(G)$ and any $\sigma_g \in I, \tau \circ \sigma_g \circ \tau^{-1} \in I$. So, $I$ is a normal subgroup of $\text{Aut}(G)$. \qed