THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 5 Solutions
29th February 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. G is a group of order 6, to show that $G \cong \mathbb{Z}_6$, it suffices to find a generator of order 6. Note that under the group operation, $2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5$ and $2^6 = 1$. Thus $G = \langle 2 \rangle$, therefore there exists a group isomorphism $\mathbb{Z}_6 \to G$ by $1 \mapsto 2$.

2. Let $\phi : G \to G'$ be a bijective group homomorphism, suppose $x, y \in G'$, then there exists unique $g, h \in G$ such that $\phi(g) = x$ and $\phi(h) = y$. Then $\phi^{-1}(xy) = \phi^{-1}(\phi(g)\phi(h)) = \phi^{-1}(\phi(gh)) = gh = \phi^{-1}(x)\phi^{-1}(y)$. And we have $\phi^{-1}(x^{-1})\phi^{-1}(x) = \phi^{-1}(x^{-1}x) = \phi^{-1}(e) = e$, therefore $\phi^{-1}(x^{-1})$ is the inverse of $\phi^{-1}(x)$, i.e. $\phi^{-1}(x^{-1}) = \phi^{-1}(x)^{-1}$.

3. (a) Since the group operation is given by matrix multiplication, it is associative. It suffices to compute the products and inverse of the elements and show that they are in G. Denote $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, then $G = \{I, -I, A, -A\}$. It is clear that I is the identity element since it is the identity matrix. And $-I \cdot A = A \cdot (-I) = -A, (-I) \cdot (-A) = (-A) \cdot (-I) = A$; $(-I)^2 = A^2 = (-A)^2 = I$; and $A \cdot (-A) = (-A) \cdot A = I$. In particular, every non-identity element has order 2, so they are their own inverses. So G forms a group.

   (b) Define $\varphi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$ by $\varphi(1, 0) = A, \varphi(0, 1) = -I$ and $\varphi(1, 1) = -A$. Then we claim that φ is an isomorphism. Indeed, φ is a group homomorphism by the calculations in part (a), for example $\varphi((1, 0) + (0, 1))) = -A = A \cdot (-I) = \varphi(1, 0)\varphi(0, 1)$. Clearly φ is bijective from construction, therefore it is an isomorphism.

   Alternatively, one can define $\psi : \mathbb{Z} \times \mathbb{Z} \to G$ by $\psi(1, 0) = A$ and $\psi(0, 1) = -I$ and apply first isomorphism theorem. The kernel in this case would be $\ker \psi = (2\mathbb{Z}) \times (2\mathbb{Z}) = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : \ a, b \in 2\mathbb{Z}\}$.

4. (a) Yes, define $\varphi : (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ by $\varphi(x) = e^x$, we wish to show that φ is an isomoprhism. For $x, y \in (\mathbb{R}, +)$, we have $e^{x-y} = e^x(e^y)^{-1}$ so φ is a homomorphism. Suppose that $e^x = 1 \in \mathbb{R}_{>0}$, then by injectivity of the exponential function (c.f. calculus) we have that x necessarily equals to 1. As for surjectivity, given any $t \in \mathbb{R}_{>0}$, $\log(t)$ is well-defined and we have $e^{\log(t)} = t$. So φ is indeed an isomorphism.

   (b) No, suppose on the contrary that there is an isomorphism $\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}_{>0}, \cdot)$, then there exists some $a \in \mathbb{Q}$ so that $\varphi(a) = 2$. This implies that $2 = \varphi(a) = \varphi(\frac{a}{2} + \frac{a}{2}) = \varphi(\frac{a}{2})^2$. So we have $(\frac{a}{2}) \in \mathbb{Q}_{>0}$ is a rational number whose square is 2, which is absurd.

5. Recall that by proposition 6.4.2 from the lecture note, $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$. In our case, this implies that $\mathbb{Z}_2 \times \mathbb{Z}_{12} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_6 \times \mathbb{Z}_4$ since $\gcd(3, 4) = \gcd(3, 2) = 1$.

6. (a) Note that $\phi : G \to G$ defined by $\phi(g) = g^{-1}$ is a group homomorphism iff $\phi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \phi(g)\phi(h)$ for any $g, h \in G$ iff $g'h' = h'g'$ for any $g', h' \in G$ iff G is abelian.

   (b) Note that $\phi : G \to G$ defined by $\phi(g) = g^2$ is a group homomorphism iff $\phi(gh) = (gh)^2 = ghgh = g^2h^2 = \varphi(g)\varphi(h)$ for any $g, h \in G$ iff $hg = gh$ for any $g, h \in G$ (by cancelling g on the left and h on the right) iff G is abelian.

7. (a) Let ϕ, ψ be automorphisms, then by Q2, ϕ^{-1} is also a bijective group homomorphism from G to itself, hence it is an automorphism again, and $\phi \circ \psi$ is also a bijective homomorphism. This shows that $\mathrm{Aut}(G)$ is closed under the group operation and taking inverse. Composition is always associative. And it is clear that the identity function is an automorphism, therefore $\mathrm{Aut}(G)$ is a group.

   (b) Note that for any $a, b \in G$ we have $i_g(ab^{-1}) = g(ab)g^{-1} = gag^{-1}gb^{-1}g^{-1} = (gag^{-1})(gbg^{-1})^{-1} = i_g(a)i_g(b)^{-1}$. Therefore, i_g is a group homomorphism, its inverse is given by $i_{g^{-1}}$, since $i_g \circ i_{g^{-1}}(a) = gg^{-1}ag^{-1}g = \mathrm{id}(a)$. So i_g is an automorphism.

   (c) It is clear that $\mathrm{Inn}(G)$ is a subgroup, since $i_g \circ i_h = i_{gh}$ and $i_g^{-1} = i_{g^{-1}}$, so it is closed under compositions and inverses. To show that it is normal, let ϕ be an automorphism, and consider $\phi \circ i_g \circ \phi^{-1}(a) = \phi(g\phi^{-1}(a)g^{-1}) = \phi(g)\phi(\phi^{-1}(a))\phi(g^{-1}) = \phi(g)a\phi(g)^{-1} = i_{\phi(g)}(a)$. This means that any conjugation of inner automorphism is again an inner automorphism, i.e. $\phi\mathrm{Inn}(G)\phi^{-1} \leq \mathrm{Inn}(G)$ for any $\phi \in \mathrm{Aut}(G)$, thus $\mathrm{Inn}(G)$ is normal.

Optional Part

1. (a) Consider $1^2 = 5^2 = 7^2 = 11^2 = 13^2 = 17^2 = 19^2 = 23^2 = 1$ in G, so every element has order 2. This implies G is not isomorphic to $\mathbb{Z}_8$ since there is an element of order 8 in $\mathbb{Z}_8$, which does not exist in G.

   (b) The answer is (iii). As we observed above, every element has order 2 in G, in the three choices, only (iii) satisfies the above condition.

2. Suppose that $G = \langle g \rangle$, then for any isomorphism $\phi : G \to G'$, for any $g' \in G'$, there exists some $h \in G$ so that $\phi(h) = g'$, but then $h = g^k$ for some $k \in \mathbb{Z}$, therefore $g' = \phi(h) = \phi(g^k) = \phi(g)^k$. Thus every element in G' is a power of $\phi(g)$, so $G' = \langle \phi(g) \rangle$.

3. Let G be a non-abelian group of order 6, if G has an element of order 6, then it is cyclic, and hence abelian, this gives rise to a contradiction. Thus G has no element of order 6, but every element has order dividing 6, so there must be elements of order 2 or 3. Note that the order 3 elements come in pairs, i.e. for every order 3 subgroup, there are two generators. Therefore, it is impossible for all non-identity elements in G to have order 3. So there exists some order 2 element $x \in G$. Now consider the order 2 subgroup $H = \{e, x\} \leq G$. If it is a normal subgroup, let aH be a generator of $G/H \cong \mathbb{Z}_3$, then $a^3H = H$, i.e. $a^3\{e, x\} = \{e, x\}$. There are two possibilities, either $a^3 = e$ or $a^3 = x$.

If $a^3 = e$, then we have a is of order 3 in G, with $axa^{-1} = x$. Thus ax has order 6, which is a contradiction. Otherwise, $a^3 = x$ and $a^6 = e$, it is impossible for $a^2 = e$ since that would imply $(aH)^2 = H \in G/H$. In this case, a has order 6, which is again a contradiction.

Thus, H must be an order 2 subgroup of G that is not normal. Therefore G permutes the left cosets of H in G, i.e. we consider X the set of left cosets of H in G, and define $\varphi : G \to \mathrm{Sym}(X) \cong S_3$ by $\varphi(g) : X \to X$ sending a coset aH to $(ga)H$. We claim that φ is a group isomorphism. It is a homomorphism since $\varphi(g) \circ \varphi(g')(aH) = \varphi(g)(g'aH) = gg'aH = \varphi(gg')(aH)$, and $\varphi(g) \circ \varphi(g^{-1})(aH) = gg^{-1}aH = \mathrm{id}(aH)$. To prove that φ defines an isomorphism, it suffices to show that it is injective, then by $|G| = |S_3| = 6$, we can conclude that φ is bijective. Suppose that $\varphi(g) = \mathrm{id}$ the identity permutation, then in particular $\varphi(g)(H) = gH = H$, therefore $g \in H = \{e, x\}$. Furthermore, $\varphi(g)(aH) = gaH = aH$, so that $ga \in aH$, i.e. $a^{-1}ga \in H$. Since H is not normal, there exists some $a \in G$ so that $a^{-1}xa \notin H$. Therefore the only element satisfying this condition is the identity, so $\ker \varphi = \{e\}$. This completes the proof.

4. (a) Let $k, l \in \mathbb{Z}$, then $\phi(k + (-l)) = \overline{k + (-l)} = \overline{\overline{k} + \overline{(-l)}} = \phi(k) + (-\phi(l))$, therefore ϕ defines a group homomorphism.

   (b) $\ker \phi = \{k \in \mathbb{Z} : \overline{k} = 0 \in \mathbb{Z}_n\} = \{k \in \mathbb{Z}_n : k = n \cdot a, a \in \mathbb{Z}\} = n\mathbb{Z}$. Since ϕ is surjective, by the first isomorphism theorem $\mathbb{Z}/\ker \phi \cong \mathbb{Z}_n$, therefore $|\mathbb{Z}/\ker \phi| = [\mathbb{Z} : \ker \phi] = |\mathbb{Z}_n| = n$.

   (c) Any group homomorphism $\psi : \mathbb{Z}_n \to \mathbb{Z}$ is trivial, i.e. there exists unique homomorphism $\psi : \mathbb{Z}_n \to \mathbb{Z}$, which is given by $\psi(1) = 0$. The reason is that $\mathbb{Z}_n$ is cyclic, so to give a homomorphism $\psi : \mathbb{Z}_n \to \mathbb{Z}$, it suffices to provide $\psi(1) = k \in \mathbb{Z}$, then by property of homomorphism, $\psi(i) = ki$ is required to hold. If $\psi(1) = k$, since $n = 0$ in $\mathbb{Z}_n$, we have $\psi(n) = kn = 0$, this implies that $k = 0$, as claimed.

5. We will treat the question generally and prove that U_m is in fact isomorphic to $\mathbb{Z}_m$, so both (a) and (b) are essentially asking for the number of automorphisms of $\mathbb{Z}_m$. Consider the homomorphism $\varphi_m : \mathbb{Z} \to U_m$ defined by $n \mapsto e^{2\pi i n/m}$. This is well-defined because $(e^{2\pi i n/m})^m = e^{2\pi i n} = 1$. This is a homomorphism because $\varphi_m(n + k) = e^{2\pi i(n+k)/m} = e^{2\pi i n/m} \cdot e^{2\pi i k/m} = \varphi_m(n)\varphi_m(k)$; and $\varphi_m(-n) = e^{-2\pi i n/m} = \varphi_m(n)^{-1}$.

   We know that φ_m is surjective since every m-th root of unity can be written as $e^{2\pi i n/m}$ for some $n \in \mathbb{Z}$. The kernel is given by $\{n \in \mathbb{Z} : e^{2\pi i n/m} = 1\} = \{n \in \mathbb{Z} : n = km \text{ for some } k \in \mathbb{Z}\} = m\mathbb{Z}$. Thus we have $\mathbb{Z}/m\mathbb{Z} \cong U_m$ by the first isomorphism theorem, the former is isomorphic to $\mathbb{Z}_m$ by Q4.

   Now to determine the number of automorphisms of $\mathbb{Z}_m$. Note that since $\mathbb{Z}_m$ is cyclic, by Q2 it must send the generator 1 to another generator $k \in \mathbb{Z}_m$. Note that this determines the automorphism uniquely, since $\varphi(1) = k$ would force $\varphi(j) = jk$ for all $j \in \mathbb{Z}_m$. Conversely, if k is a generator, then defining φ by $\varphi(1) = k$ always gives an automorphism since this map is always bijective. Therefore the number of automorphisms is equal to the number of generators in $\mathbb{Z}_m$, this is given by Euler's totient function ϕ. For prime $m = p$, there are $\phi(p) = p - 1$ many generators, namely every element except $0 \in \mathbb{Z}_p$. As for composite m, $\phi(m) = m \cdot \Pi_{p|m}(1 - 1/p)$ where the product runs over all distinct prime factors of m. So we have $\phi(5) = 4$ and $\phi(12) = 4$.

6. Reflexivity: $G \cong G$ because the identity map is an isomorphism from G to itself.

   Symmetry: If $G \cong G'$, then there exists isomorphism $\phi : G \to G'$, by Q2, $\phi^{-1} : G' \to G$ is also an isomorphism, so $G' \cong G$.

   Transitivity: If $G \cong G'$ and $G' \cong G''$, then there exists isomorphisms $\phi : G \to G'$ and $\psi : G' \to G''$, then $\psi \circ \phi : G \to G''$ is again an isomorphism, so that $G \cong G''$.

7. (a) By assumption that $G = \langle S \rangle$, we can express every element $g \in G$ by $a_1^{m_1} \cdots a_k^{m_k}$ where $k \in \mathbb{Z}_{>0}$, $a_i \in S$ and $m_i \in \mathbb{Z}$. Then $\mu(g) = \mu(a_1)^{m_1} \cdots \mu(a_k)^{m_k} = \lambda(a_1)^{m_1} \cdots \lambda(a_k)^{m_k} = \lambda(g)$. Since g is arbitrary, so we have $\mu = \lambda$.

   (b) We have explained this in Q5 already. The order of $\mathrm{Aut}(\mathbb{Z}_{15})$ is the number of generators in $\mathbb{Z}_{15}$, which is given by $\phi(15) = 8$.