THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Tutorial 6 Solutions
26th February 2024

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

1. By the first isomorphism theorem, it suffices to find a group homomorphism $\varphi : \mathbb{R} \to U$ such that $\ker \varphi = 2\pi\mathbb{Z}$. Consider $\varphi(t) = e^{it}$, then φ is a group homomorphism from $\mathbb{R}$ to U, since $|e^{it}| = 1$ and $\varphi(t + (-s)) = e^{i(t-s)} = e^{it} \cdot (e^{is})^{-1}$. The kernel $\ker \varphi$ is given by $2\pi\mathbb{Z}$ since $e^{it} = \cos t + i \sin t = 1$ if and only if $t = 2\pi k$ for some $k \in \mathbb{Z}$.

2. If $\varphi : G \to G'$ is a surjective homomorphism, and if G is cyclic, then $G = \langle g \rangle$ for some $g \in G$. By surjectivity, for any $x \in G'$ there exists some $h \in G$ so that $\varphi(h) = x$. For this h, there exists some $k \in \mathbb{Z}$ so that $g^k = h$, therefore $x = \varphi(h) = \varphi(g^k) = \varphi(g)^k$. Hence every element $x \in G'$ is some power of $\varphi(g)$, in other words, $G' = \langle \varphi(g) \rangle$.

   Now assume that G is abelian. For any $g', h' \in G'$, there exists some $g, h \in G$ such that $\varphi(g) = g'$ and $\varphi(h) = h'$. Therefore $g'h' = \varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g) = h'g'$, and so G' is abelian.

3. (a) For any $g \in G$, we define $\varphi : \mathbb{Z} \to G$ by $\varphi(n) = g^n$. This is a group homomorphism because $\varphi(n + (-m)) = g^{n-m} = g^n \cdot g^{-m} = \varphi(n)\varphi(m)^{-1}$ for any $n, m \in \mathbb{Z}$ (see HW1 compulsory Q3c). This is a group homomorphism that satisfies $\varphi(1) = g$.

   (b) Let $\varphi : D_n \to G$ be a homomorphism, since we have $r^n = s^2 = rsrs = e$ in D_n, applying the homomorphism to these relations yields $\varphi(r)^n = \varphi(s)^2 = (\varphi(r)\varphi(s))^2 = e_G$.

   Remark: More generally, one can ask the question of how do we determine the set of homomorphism from G to G'. The above exercise hinted on a condition of when can one construct a homomorphism. If $\varphi : G \to G'$ is a homomorphism, and G is a group that is generated by some elements $G = \langle g_1, ..., g_n \rangle$, then whatever relations that the g_i's satisfy in G, their images $\varphi(g_1), ..., \varphi(g_n)$ have to satisfy as well. If one has a "complete" set of relations for the generators for the g_i's, then the data of a homomorphism is nothing but choosing what the targets $\varphi(g_i)$ are, providing they satisfy the same relations! This is particularly helpful, because it can reduce the computations of many different group operations to that of the ones involving the generators.

4. If two groups are isomorphic, then all the group properties are preserved. For example, $\mathbb{Z}$ is cyclic, so if we can show that $\mathbb{Q}$ is not cyclic, then $\mathbb{Q} \ncong \mathbb{Z}$. The group $\mathbb{Q}$ is not cyclic, because if $\mathbb{Q} = \langle g \rangle$, then $1 = kg = g + g + ... + g$, so $g = \frac{1}{k}$. Then this would imply $\frac{1}{2k} \notin \mathbb{Q}$, clearly a contradiction.

   On the other hand, $\mathbb{Q}$ is not isomorphic to $\mathbb{R}$ for completely different reason. The two group has different cardinality, since an isomorphism is in particular a bijection between the underlying sets, it is impossible for them to be isomorphic.

5. Firstly, φ is well-defined because $\varphi_g : G \to G$ is a bijective function (i.e. a permutation on the set G). The reason is simply due to φ_g has an inverse function, given by $\varphi_{g^{-1}}$. Indeed, $\varphi_g \circ \varphi_{g^{-1}}(x) = g(g^{-1}x) = x$ and $\varphi_{g^{-1}} \circ \varphi_g = g^{-1}(gx) = x$. In particular, this means that $\varphi(g)^{-1} = \varphi_g^{-1} = \varphi_{g^{-1}} = \varphi(g^{-1})$. Next, we also have to show φ preserves products, this is due to $\varphi(gh)(x) = \varphi_{gh}(x) = (gh)x = g(hx) = \varphi_g(\varphi_h(x)) = \varphi_g \circ \varphi_h(x)$. So we have $\varphi(gh) = \varphi(g) \circ \varphi(h)$.

   Finally, to show that φ is an injective homomorphism, it suffices to show that $\ker \varphi = \{e\}$. This is because $\varphi_g = \mathrm{id}$ implies that $\varphi_g(e) = g \cdot e = g = e = \mathrm{id}(e)$, so $g = e$. Conversely, if $g = e$, we have $\varphi_e(x) = e \cdot x = \mathrm{id}(x)$.

6. (a) Let $\varphi : G \to \mathrm{Sym}(X)$ be defined in the question, then an element $g \in \ker \varphi$ fixes all left H cosets. In particular, this means that $\varphi_g(H) = gH = \mathrm{id}(H)$, which is equivalent to $g \in H$. Therefore, $\ker \varphi \leq H$, in general the two groups may not be the same.

   (b) Since there are $[G : H] = n$ left H cosets, so $|X| = n$ and the group $\mathrm{Sym}(X)$ has order $n!$. By the first isomorphism theorem, $G/\ker \varphi \cong \mathrm{Im}(\varphi) \leq \mathrm{Sym}(G)$. Therefore $[G : \ker \varphi] = |G/\ker \varphi| = |\mathrm{Im}(\varphi)| \leq n!$, so $\ker \varphi$ is a normal subgroup of G with index at most $n!$.

   (c) Suppose now that G is an infinite group with an index n subgroup, then by part (b) there exists a normal subgroup of index at most $n!$, therefore it must be a nontrivial normal subgroup of G.

7. Define $\psi : G \to \mathrm{Inn}(G)$ by $\psi(g) = \psi_g : G \to G$ defined by $\psi_g(x) = gxg^{-1}$. This defines a homomorphism because $\psi_g \circ \psi_h(x) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = \psi_{gh}(x)$ for any $g, h, x \in G$, and $\psi_g \circ \psi_{g^{-1}}(x) = \psi_e(x) = \mathrm{id}(x)$. By definition of $\mathrm{Inn}(G)$, ψ is surjective. Therefore, it suffices to show that $\ker \psi = Z(G)$ to conclude by first isomorphism theorem that $G/Z(G) \cong \mathrm{Inn}(G)$.

   Indeed, $\psi_g = \mathrm{id}$ exactly when $gxg^{-1} = x$ for all x. This by definition is equivalent to $g \in Z(G)$.

8. Recall that by Q3a, a homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ is uniquely determined by $\varphi(1) = n \in \mathbb{Z}$. Note that the image in this case $\mathrm{Im}(\varphi) = \langle n \rangle = n\mathbb{Z}$. If φ is an isomorphism, the image is the whole $\mathbb{Z}$, so n has to be a generator of $\mathbb{Z}$. So the only choices are $n = \pm 1$. It is clear that $\varphi(1) = -1$ defines an automorphism, since it is its own inverse. So $\mathrm{Aut}(\mathbb{Z}) = \mathbb{Z}_2$.

   Remark: $\varphi(1) = -1$ defines an automorphism that is not inner. In an abelian group, any inner automorphism is trivial, since every element commutes with each other.

9. The question should instead read: there does not exist non-trivial homomorphism $\mathbb{Z}_m \to \mathbb{Z}_n$.

   Assume on the contrary that there is some homomorphism $\varphi : \mathbb{Z}_m \to \mathbb{Z}_n$, then $\varphi(1) \in \mathbb{Z}_n$ satisfies $\varphi(n) = \varphi(1)^n = 0 \in \mathbb{Z}_n$. Since $\gcd(m, n) = 1$, there exists integers a, b so that $am + bn = 1$. Then $\varphi(1) = \varphi(am + bn) = \varphi(bn) = \varphi(n + n + ... + n) = \varphi(n) + ... + \varphi(n) = 0$. Therefore the only homomorphism from $\mathbb{Z}_m \to \mathbb{Z}_n$ is the zero homomorphism, sending every element to 0.