MAT301 Groups and Symmetry
Assignment 6 Solutions

1. The two parts of this question are not related to one another.

(a) Let G be a group and H a normal subgroup of G. Suppose the index $[G : H]$ is finite. Let $g \in G$ be an element of finite order such that $\gcd(|g|, [G : H]) = 1$. Show that $g \in H$.

(b) Let G be a group and $H \leq G$ a subgroup of index 2. Show that if $g, g' \in G - H$, then $gg' \in H$.

Solution: (a) Since H is a normal subgroup, we have the quotient group G/H. Let $\pi : G \to G/H$ be the quotient map. Since g has finite order and π is a homomorphism, $\pi(g)$ has finite order and we have $|\pi(g)| \mid |g|$. On the other hand, by Lagrange's theorem, $|\pi(g)| \mid |G/H| = [G : H]$. Since $\gcd(|g|, [G : H]) = 1$, it follows that $|\pi(g)| = 1$, i.e. $gH = H$ (remember $\pi(g) = gH$ and the identity of G/H is H). Thus $g \in H$.

(b) Being a subgroup of index 2, H is normal in G. Let $g, g' \in G - H$. Then gH and $g'H$ are not equal to H. Since H has only two cosets, it follows that $gH = g'H$. In the quotient group G/H (which is a group of order $[G : H] = 2$), we have $(gg')H = gH \cdot g'H = (gH)^2 = H$ (because square of an element in a group of order 2 is identity). Thus $gg' \in H$.

2. In each part, show that the given two groups are isomorphic.

(a) $GL_n(\mathbb{Q})/SL_n(\mathbb{Q})$ and $\mathbb{Q}^\times$
(b) $\mathbb{C}/\mathbb{Z}$ and $\mathbb{C}^\times$
(c) $\mathbb{R}/\mathbb{Z}$ and the unit circle $S = \{z \in \mathbb{C}^\times : |z| = 1\}$ (the latter under multiplication)
(d) $\mathbb{C}^\times/\mathbb{R}_{>0}$ and the unit circle (defined above)
(e) $\mathbb{C}^\times/\mathbb{R}^\times$ and the unit circle S

Solution: (a) Consider the determinant map $\det : GL_n(\mathbb{Q}) \to \mathbb{Q}^\times$. Its kernel is $SL_n(\mathbb{Q})$ and its image is $\mathbb{Q}^\times$. Applying the first isomorphism theorem to det we get an isomorphism $GL_n(\mathbb{Q})/SL_n(\mathbb{Q}) \to \mathbb{Q}^\times$ (given by $A \cdot SL_n(\mathbb{Q}) \mapsto \det(A)$).

(b) Define $\phi : \mathbb{C} \to \mathbb{C}^\times$ by $\phi(z) = e^{2\pi i z}$. Then ϕ is surjective and $\ker(\phi) = \mathbb{Z}$. Applying the first isomorphism theorem to ϕ we get an isomorphism $\mathbb{C}/\mathbb{Z} \to \mathbb{C}^\times$ (what is the isomorphism induced by ϕ?).

(c) Consider $\phi : \mathbb{R} \to \mathbb{C}^\times$ defined by $\phi(x) = e^{2\pi i x}$. We have $\ker(\phi) = \mathbb{Z}$ and $\mathrm{Im}(\phi) = S$ (why?). By the first isomorphism theorem we have $\mathbb{R}/\mathbb{Z} \simeq S$.

(d) Define $\phi : \mathbb{C}^\times \to \mathbb{C}^\times$ by $\phi(z) = \dfrac{z}{|z|}$. Note that ϕ is a homomorphism (why?), $\ker(\phi) = \mathbb{R}_{>0}$ and $\mathrm{Im}(\phi) = S$. By the first isomorphism theorem $\mathbb{C}^\times/\mathbb{R}_{>0} \simeq S$.

(e) Define $\phi : \mathbb{C}^\times \to \mathbb{C}^\times$ by $\phi(z) = \dfrac{z}{\bar{z}}$, where $\bar{z}$ is the complex conjugate of z. Note that ϕ is a homomorphism (why?), $\ker(\phi) = \mathbb{R}^\times$ and $\mathrm{Im}(\phi) = S$. By the first isomorphism theorem $\mathbb{C}^\times/\mathbb{R}^\times \simeq S$.

3. (a) Give a complete list of abelian groups of order 32, up to isomorphism. (Your list must contain exactly one group from each isomorphism class. In other words, your list must be such that every abelian group of order 32 is isomorphic to exactly one group from the list.)

(b) Find the order of $[3]$ in $U(64)$. (The computations for this should not be difficult at all.)

(c) Show that $U(64)$ is isomorphic to $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution: (a)

(i) $\mathbb{Z}/32$ (This is cyclic.)
(ii) $\mathbb{Z}/16 \times \mathbb{Z}/2$ (This has an element of order 16.)
(iii) $\mathbb{Z}/8 \times \mathbb{Z}/4$ (No element of order 16 and the equation $2x = 0$ has 4 solutions.)
(iv) $\mathbb{Z}/8 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ (It has an element of order 8 and the equation $2x = 0$ has 8 solution.)
(v) $\mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}/2$ (no element of order 8 and 8 solutions to $2x = 0$)
(vi) $\mathbb{Z}/4 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ (16 solutions to $2x = 0$)
(vii) $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$ (32 solutions to $2x = 0$)

Since every finite abelian group is isomorphic to a direct product of cyclic groups, every abelian group of order 32 is isomorphic to one of the seven groups above. Moreover, the seven groups listed above are mutually non-isomorphic (each is distinguished from the other groups by the property mentioned in front of it).

(b) Since $|U(64)| = 32$, by Lagrange, $|[3]| \mid 32$. Since $U(64)$ is not cyclic (see Assignment 3, Question 2b), $|[3]| \neq 32$. Thus $|[3]|$ is one of $2, 4, 8$, or 16. We have $[3]^2 = [9]$, $[3]^4 = [9]^2 = [81] = [17]$, and $[3]^8 = [17]^2 = [289] \neq [1]$. Thus $[3]$ must have order 16.

(c) The group $U(64)$ is an abelian group of order 32, and as such, it is isomorphic to exactly one of the groups we listed in Part (a). It is not cyclic and contains an element of order 16. The only group on the list with those properties is $\mathbb{Z}/16 \times \mathbb{Z}/2$.

4. Throughout this question, we use the following notation: given integers a and n, we denote the residue class of a mod n by $[a]_n$.

(a) Let m and n be positive integers. Show that we have a well-defined homomorphism

$$\psi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

given by $\psi([a]_{mn}) = [a]_m$.

(b) Prove the *Chinese remainder theorem*: If $\gcd(m, n) = 1$, then the map

$$\Phi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

given by $\Phi([a]_{mn}) = ([a]_m, [a]_n)$ is an isomorphism. (You may use the fact that when m and n are relatively prime, a number is divisible by both m and n if and only if it is divisible by mn.)

(c) true or false (no explanation necessary): If m and n are positive integers with $\gcd(m, n) = 1$, then for every integers a and b, there exists an integer x which satisfies the system of equations

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}.$$

Moreover, x is unique mod mn.

Solution: (a) For the map to be well-defined, we need to have that if $[a]_{mn} = [b]_{mn}$ for integers a and b, then $[a]_m = [b]_m$. For this note that if $[a]_{mn} = [b]_{mn}$, then $mn \mid a - b$. Since $m \mid mn$, we then have $m \mid a - b$, and hence $[a]_m = [b]_m$.

The following calculation shows that ψ is a homomorphism. Here a and b are arbitrary integers.

$$\psi([a]_{mn} + [b]_{mn}) = \psi([a + b]_{mn}) = [a + b]_m = [a]_m + [b]_m = \psi([a]_{mn}) + \psi([b]_{mn}).$$

(b) The fact that Φ is a homomorphism is because each of its coordinate functions is a homomorphism. More precisely, let $\psi_1 : \mathbb{Z}/mn \to \mathbb{Z}/m$ be given by $[a]_{mn} \mapsto [a]_m$ and $\psi_2 :$

$\mathbb{Z}/mn \to \mathbb{Z}/n$ given by $[a]_{mn} \mapsto [a]_n$. Then ψ_1 and ψ_2 are homomorphisms by part (a), and we have

$$\begin{aligned}\Phi([a+b]) = (\psi_1([a+b]), \psi_2([a+b])) &= (\psi_1([a]) + \psi_1([b]), \psi_2([a]) + \psi_2([b])) \\ &= (\psi_1([a]), \psi_2([a])) + (\psi_1([b]), \psi_2([b])) \\ &= \Phi([a]) + \Phi([b]).\end{aligned}$$

(All the residue classes in the above calculation are mod mn.)

Since the domain and codomain of Φ both have mn elements, to show that Φ is bijective it is enough to show that it is injective. Let $[a]_{mn} \in \ker(\Phi)$. This means $[a]_m = [0]_m$ and $[a]_n = [0]_n$, i.e. $m \mid a$ and $n \mid a$. Since m and n are relatively prime, it follows that $mn \mid a$, i.e. $[a]_{mn} = [0]_{mn}$. This $\ker(\Phi)$ is trivial.

(c) true (The statement is just paraphrasing bijectivity of the map Φ of part (b).)

5. Let G_1, G_2 and H be abelian groups. Construct a bijective function

$$\mathrm{Hom}(G_1 \times G_2\,, H) \longrightarrow \mathrm{Hom}(G_1, H) \;\times\; \mathrm{Hom}(G_2, H)$$

(and prove that your function is bijective).

Solution: Let $\iota_1 : G_1 \to G_1 \times G_2$ and $\iota_2 : G_2 \to G_1 \times G_2$ be the natural embeddings (given by $\iota_1(g_1) = (g_1, e)$ and $\iota_2(g_2) = (e, g_2)$). Then we define

$$F : \mathrm{Hom}(G_1 \times G_2\,, H) \longrightarrow \mathrm{Hom}(G_1, H) \;\times\; \mathrm{Hom}(G_2, H)$$

by

$$\phi \mapsto (\phi \circ \iota_1, \phi \circ \iota_2).$$

(Note that given any homomorphism $\phi : G_1 \times G_2 \to H$, the composition $\phi \circ \iota_1$ is a function $G_1 \to H$, and being a composition of homomorphisms it is a homomorphism. Similarly $\phi \circ \iota_2$ is a homomorphism $G_2 \to H$.)

We claim that F is a bijection. First, let us check injectivity. Suppose $\phi, \psi \in \mathrm{Hom}(G_1 \times G_2\,, H)$ and $F(\phi) = F(\psi)$. This means that $\phi \circ \iota_1 = \psi \circ \iota_1$and $\phi \circ \iota_2 = \psi \circ \iota_2$. Given an arbitrary element $(g_1, g_2) \in G_1 \times G_2$, we have $(g_1, g_2) = (g_1, e)(e, g_2) = \iota_1(g_1)\iota_2(g_2)$. Thus

$$\phi(g_1, g_2) = \phi(\iota_1(g_1))\phi(\iota_2(g_2)) = \psi(\iota_1(g_1))\psi(\iota_2(g_2)) = \psi(g_1, g_2),$$

where in the first and last equality we used the fact that ϕ and ψ are homomorphisms, and in the middle equality we used the assumption that $\phi \circ \iota_1 = \psi \circ \iota_1$ and $\phi \circ \iota_2 = \psi \circ \iota_2$. Thus $\phi = \psi$.

We now show that F is surjective. Let

$$(\phi_1, \phi_2) \in \mathrm{Hom}(G_1, H) \;\times\; \mathrm{Hom}(G_2, H).$$

We shall define a homomorphism $\phi : G_1 \times G_2 \to H$ such that $\phi \circ \iota_1 = \phi_1$ and $\phi \circ \iota_2 = \phi_2$ (so that $F(\phi) = (\phi_1, \phi_2)$). For any $(g_1, g_2) \in G_1 \times G_2$, set

$$\phi(g_1, g_2) = \phi_1(g_1)\phi_2(g_2).$$

This defines a function $G_1 \times G_2 \to H$: both $\phi_1(g_1)$ and $\phi_2(g_2)$ belong to H, so we can multiply them in H. We claim that ϕ is a homomorphism. Indeed,

$$(1) \qquad \phi((g_1, g_2)(g_1', g_2')) = \phi(g_1 g_1', g_2 g_2') = \phi_1(g_1 g_1')\phi_2(g_2 g_2') = \phi_1(g_1)\phi_1(g_1')\phi_2(g_2)\phi_2(g_2'),$$

since ϕ_1, ϕ_2 are homomorphisms. On the other hand,

$$(2) \qquad \phi(g_1, g_2)\phi(g_1', g_2') = \phi_1(g_1)\phi_2(g_2)\phi_1(g_1')\phi_2(g_2').$$

Comparing (1) and (2), in view of the fact that H is abelian, we conclude that ϕ is a homomorphism. Finally, note that

$$\phi \circ \iota_1(g_1) = \phi(g_1, e) = \phi_1(g_1)\phi_2(e) = \phi_1(g_1),$$

so that $\phi \circ \iota_1 = \phi_1$. Similarly, one check that $\phi \circ \iota_2 = \phi_2$, completing the proof.

6. Give an example of an abelian group G and a subgroup $H \leq G$ such that G is not isomorphic to $H \times (G/H)$. Give two examples, one with G finite and one with G infinite.

Solution: finite: Take $G = \mathbb{Z}/4$ and $H = \langle [2] \rangle$. Then H and G/H are both cyclic of order 2, so that $H \times (G/H)$ is not cyclic (and hence not isomorphic to $\mathbb{Z}/4$).

infinite: Take $G = \mathbb{Z}$ and $H = 2\mathbb{Z}$. Then $H \times (G/H)$ is $2\mathbb{Z} \times (\mathbb{Z}/2)$, which is not cyclic (as it is infinite but has a nontrivial element of finite order, namely, $(0, [1])$).