# Abstract Algebra I

## Homework 4

B13902024 張沂魁

Due: 8th October 2025

1. For two groups $G, H$ with identities $e_G, e_H$ respectively, define the direct product of $G$ and $H$ to be the group whose underlying set is $G \times H$ and whose binary operation is given by

$$(g,h)(g',h') = (gg', hh'), \quad g, g' \in G, \ h, h' \in H.$$

   (a) Let $p \neq q$ be two prime numbers. Prove that $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \cong \mathbb{Z}/pq\mathbb{Z}$ by constructing an isomorphism explicitly.

   (b) Let $G, H$ be cyclic groups. Prove that $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

   (c) Deduce that $S_3$ is not a direct product of any of its proper subgroups.

**Solution:**

(a) Consider a map $\phi : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ defined by $\phi\left([a]_{pq}\right) = \left([a]_p, [a]_q\right)$ where $[a]_k$ means the equivalence class of $a$ modulo $k$. Note that this map is well-defined since for $a \equiv b \mod pq$, we know $a = b + pqk$ for some integer $k$, so $a \equiv b \mod p$ and $a \equiv b \mod q$, which means $\phi\left([a]_{pq}\right) = \phi\left([b]_{pq}\right)$. We claim $\phi$ is an isomorphism. We first show that $\phi$ is a homomorphism.

$$\begin{aligned}\phi\left([a]_{pq}[b]_{pq}\right) &= \phi\left([ab]_{pq}\right) = \left([ab]_p, [ab]_q\right) \\ &= \left([a]_p[b]_p, [a]_q[b]_q\right) = \left([a]_p, [a]_q\right)\left([b]_p, [b]_q\right) = \phi\left([a]_{pq}\right)\phi\left([b]_{pq}\right).\end{aligned}$$

Now we show that $\phi$ is bijective. If $\phi\left([k_1]_{pq}\right) = \phi\left([k_2]_{pq}\right)$, and suppose $0 \leq k_2 < k_1 \leq pq - 1$ , then

$$\left([k_1]_p, [k_1]_q\right) = \left([k_2]_p, [k_2]_q\right),$$

so we know $k_1 \equiv k_2 \mod p$ and $k_1 \equiv k_2 \mod q$. Now since $p \neq q$ are two prime numbers, so $pq \mid k_1 - k_2$, but $0 < k_1 - k_2 < pq$, so it is impossible. Hence, $\phi$ is injective. Now we show that $\phi$ is surjective. If not, then since $|\mathbb{Z}/pq\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z}|\,|\mathbb{Z}/q\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}|$, so by Pigeonhole principle, there exists $n_1 \not\equiv n_2 \mod pq$ s.t. $\phi\left([n_1]_{pq}\right) = \phi\left([n_2]_{pq}\right)$, but this is impossible since we have shown that $\phi$ is injective. Thus, $\phi$ is surjective and thus bijective. Now we know $\phi$ is bijective and homomorphic, so $\phi$ is an isomorphism between $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ and $\mathbb{Z}/pq\mathbb{Z}$.

(b) Suppose $G = \langle g \rangle$ and $H = \langle h \rangle$, and note that $|G \times H| = |G|\,|H|$.

($\implies$) Suppose $G \times H = \langle (g_1, h_1) \rangle$, then we know

$$(g_1, h_1)^{|G||H|} = \left(g_1^{|G||H|}, h_1^{|G||H|}\right) = (e_G, e_H).$$

Note that $o\left((g_1, h_1)\right) = |G|\,|H|$. Now if $\gcd\left(|G|, |H|\right) = d > 1$, then

$$\operatorname{lcm}\left(|G|, |H|\right) = \frac{|G|\,|H|}{d} < |G|\,|H|.$$

Note that $o(g_1) = |G|$ and $o(g_2) = |H|$ since $g_1, h_1$ must run through $G$ and $H$ respectively in $\{(g_1, h_1), (g_1, h_1)^2, \dots\}$. Hence, we have

$$(g_1, h_1)^{\operatorname{lcm}(|G|,|H|)} = (e_G, e_H),$$

but if $\gcd\left(|G|, |H|\right) > 1$, then $(g_1, h_1)^{\operatorname{lcm}(|G|,|H|)} = (e_G, e_H)$, and

$$\operatorname{lcm}\left(|G|, |H|\right) < |G|\,|H| = o\left((g_1, h_1)\right),$$

so this is a contradiction.

( $\Longleftarrow$ ) Suppose $\gcd\left(|G|, |H|\right) = 1$, then since $(g, h)^{|G||H|} = (e_G, e_H)$, so

$$o\left((g, h)\right) \leq |G|\,|H|.$$

Also, if there exists $k > 0$ s.t. $(g, h)^k = (e_G, e_H)$, then $g^k = e_G$ and $h^k = e_H$, so $|H| \mid k$ and $|G| \mid k$, which means $|H|\,|G| \mid k$ since $\gcd\left(|H|, |G|\right) = 1$, so we hvae $k \geq |G|\,|H|$. Hence, we must have $o\left((g, h)\right) = |G|\,|H|$. Now if $\exists\, |G|\,|H| > i > j \geq 0$ s.t. $(g, h)^i = (g, h)^j$, then $(g, h)^{i-j} = (e_G, e_H)$, but $|G|\,|H| > i - j > 0$, so it is impossible, and thus $|\langle (g, h) \rangle| = |G|\,|H|$, and since $\langle (g, h) \rangle \subseteq G \times H$, so we must have $G \times H = \langle (g, h) \rangle$, and thus $G \times H$ is cyclic.

(c) Suppose $S_3$ is a direct product of its proper subgroups, say $S_3 = A \times B$, then WLOG suppose $|A| \geq |B|$, and we have $|A| = 3$ and $|B| = 2$ since $|S_3| = 6$. Note that this means

$$\begin{aligned} A &= \{(1), (12)\}, \{(1), (13)\}, \{(1), (23)\} \\ B &= \{(1), (123), (132)\}, \end{aligned}$$

and thus we know $A, B$ must be cyclic. Also, since $\gcd(2, 3) = 1$, so $A \times B = S_3$ must be cyclic by (b), but $S_3$ is not cyclic, so $S_3$ is not a direct product of any of its proper subgroups.

2. Find the order of the following group:

$$G = \langle a, b \mid a^6 = 1,\ b^2 = a^3,\ ba = a^{-1}b \rangle.$$

And then show that it is not isomorphic to the group

$$H = \langle r, s \mid r^6 = s^2 = 1,\ srs^{-1} = r^{-1} \rangle.$$

**Solution:** We can check that

$$G = \left\{e, a, a^2, a^3, a^4, a^5, b, ab, a^2b, a^3b, a^4b, a^5b\right\}$$

since $ba = a^{-1}b$ gives $ba^k = a^{-k}b$ and thus all representation of $a, b$ like $a^i b^j a^k b^l \dots$ can be reduced to the above 12 elements. Hence, the order of $G$ is 12. Also, note that

$$H = \left\{e, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\right\},$$

and since $o(s) = o(r^3) = 2$ and $s \neq r^3$ (Otherwise $r^{-1} = srs^{-1} = r^7$, which is impossible.) , and the only element of $G$ has order 2 is $a^3$, so $G$ and $H$ are not isomorphic.

3. The symmetric group $S_4$ has a natural action on the set $T = \{1, 2, 3, 4\}$. For a subgroup $H \leq S_4$ and $n \in T$, we define the orbit $O(n)$ of $n$ to be the set $\{\sigma(n) : \sigma \in H\}$. In this exercise, the *orbit of* $H$ refers to the set $\{O(n) : n \in T\}$.

   (a) Find the orbits of the following subgroups of $S_4$ defined by their action on $T$:

   $$\langle (12) \rangle, \quad \langle (123) \rangle, \quad V.$$

   (Recall that $V$ is the unique Klein 4-group in $S_4$, and we saw in class that $V \trianglelefteq S_4$.)

   (b) Find another proper subgroup of $S_4$ with the same set of orbits as that of $V$.

   (c) Prove that the following subgroup of $S_4$ is trivial:

   $$Z(S_4) = \{\sigma \in S_4 : \tau^{-1}\sigma\tau = \sigma, \text{ for all } \tau \in S_4\}.$$

   (Recall that we encountered such a subgroup in class. It is called the *center* of $S_4$, and $Z(S_4) \trianglelefteq S_4$. The notation $Z(G)$ for the center of a group $G$ is standard.)

**Solution:**

(a)
- Case 1: $H = \langle (12) \rangle = \{(1), (12)\}$, then

  $$O(1) = \{1, 2\} \quad O(2) = \{2, 1\} \quad O(3) = \{3\} \quad O(4) = \{4\}.$$

  Thus, the orbit of $H$ is $\{\{1, 2\}, \{3\}, \{4\}\}$.
- Case 2: $H = \langle (123) \rangle = \{(1), (123), (132)\}$, then since

  $$(123) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad (132) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$

  so we have

  $$O(1) = \{1, 2, 3\} \quad O(2) = \{2, 3, 1\} \quad O(3) = \{3, 1, 2\} \quad O(4) = \{4\}.$$

  Thus, the orbit of $H$ is $\{\{1, 2, 3\}, \{4\}\}$.
- Case 3: $H = V = \{(1), (12)(34), (13)(24), (14)(23)\}$, then since

  $$(12)(34) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \quad (13)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad (14)(23) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

  so we have

  $$O(1) = O(2) = O(3) - O(4) = \{1, 2, 3, 4\},$$

  and thus the orbit of $H$ is $\{\{1, 2, 3, 4\}\}$.

(b) We want to find some proper subgroup of $S_4$ other than $V$ nad has orbit $\{1, 2, 3, 4\}$, so we can pick

$$H = \{(1), (1234), (13)(24), (1432)\},$$

note that this is a group sibce $((13)(24))^2 = (1)$ and $(1234)(1432) = (1)$. Since

$$(1234) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad (13)(24) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad (1432) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

so $O(1) = O(2) = O(3) = O(4) = \{\{1, 2, 3, 4\}\}$.

(c) We want to show that $Z(S_4) = \{e\}$. If not, then $\exists \sigma' \in Z(S_4)$ s.t. $\sigma'(a) = b$ for some $a \neq b$. However, if we pick $\tau = (ac)$, then

$$\tau\sigma'(a) = \tau(b) = b \quad \sigma'\tau(a) = \sigma'(c) \neq b$$

since $\sigma'$ is bijective, so $\tau\sigma' \neq \sigma'\tau$ here, and thus $\sigma' \notin Z(S_4)$. Hence, $Z(S_4)$ is trivial.

4. Let $G$ be a group and $H \leq G$ a subgroup. For a set $S$, denote by $\mathrm{Perm}(S)$ the group of all permutations of $S$.

(a) If $G$ acts on $S$, show that one has an induced homomorphism $G \to \mathrm{Perm}(S)$.

(b) Now let $S = \{gH : g \in G\}$. Show that the kernel of the induced homomorphism

$$G \to \mathrm{Perm}(S)$$

is contained in $H$.

(c) Suppose $|G|/|H| = n$ and that no nontrivial normal subgroup of $G$ is contained in $H$. Prove that $G$ is isomorphic to a subgroup of $S_n$.

**Solution:**

(a) $G$ acts on $S$ means there exists $\rho : G \times S \to S$ s.t. $\rho(g, s) = g \cdot s$ with

$$e \cdot s = s \ \forall s \in S \quad \text{and} \quad (g_1g_2)(s) = g_1(g_2s) \ \forall g_1, g_2 \in G, s \in S.$$

Now we show that $\Phi : G \to \mathrm{Perm}(S)$ defined by $\Phi(g) = \pi_g$, where $\pi_g : S \to S$ is defined by $\pi_g(s) = g \cdot s$, is a homomorphism between $G$ and $\mathrm{Perm}(S)$. We first show that $\pi_g$ is a permutation on $S$ for all $g \in G$, which is equivalent to show $\pi_g$ is bijective. We first show that $\pi_g$ is injective. If $\pi_g(s_1) = \pi_g(s_2)$, then $gs_1 = gs_2$, so $g^{-1}gs_1 = g^{-1}gs_2$, which means $s_1 = s_2$, and thus $\pi_g$ is injective. Now we show that $\pi_g$ is surjective. For any $s \in S$, $\pi_g(g^{-1}s) = g \cdot g^{-1}s = s$, so $\pi_g$ is surjective. Now we show that $\Phi$ is a homomorphism. Note that for all $g_1, g_2 \in G$, we have

$$\Phi(g_1g_2) = \pi_{g_1g_2} \quad \Phi(g_1)\Phi(g_2) = \pi_{g_1}\pi_{g_2},$$

so for all $s \in S$, we have

$$\Phi(g_1g_2)(s) = (g_1g_2)s = g_1(g_2s) = g_1(\Phi(g_2)(s)) = \Phi(g_1)(\Phi(g_2)(s)).$$

Hence, $\Phi$ is a homomorphism.

(b) Note that $G$ acts on $S$. Hence, we can use the result of (a). Now if $k \in \ker \Phi$, then $\pi_k = e$, which means $\pi_k(s_i) = s_i$ for all $s_i \in S$, so $k \cdot s_i = s_i$ for all $s_i \in S$. Equivalently, $k \cdot (gH) = gH$ for all $g \in G$. Hence, $(kg)H = gH$ for all $g \in G$. Hence, for all $g \in G$, $kgh_1 = g$ for some $h_1 \in H$, which means $k = gh_1^{-1}g^{-1}$. Now if we pick $g = e$, then $k = h_1^{-1} \in H$. Thus, $\ker \Phi \subseteq H$.

(c) Consider the induced homomorphism in (a), where $S$ is the $S$ in (b), we know $G/\ker \Phi \simeq \mathrm{Im}\Phi$ by first isomorphism theorem. Now since $\ker \Phi \lhd G$ and $\ker \Phi \subseteq H$ by (b), and by the condition given in the problem, we know no nontrivial normal subgroup of $G$ is contained in $H$, so $\ker \Phi = \{e\}$, so $G/\ker \Phi = G/\{e\} = G$, so we know $G \simeq \mathrm{Im}\Phi$, where $\mathrm{Im}\Phi$ is a subgroup of $S_n$ since $n = |S|$.