# Abstract algebra I Homework 4

**B13902022 賴昱錡**

## 1)

### (a)

Define the homomorphism $\varphi$ as below, where the congruent class modulo $p$ is denoted as $[x]_p$:

$$\varphi : \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z} \ \varphi(([x]_p, [x]_q)) = [x]_{pq}$$

Suppose $[x]_p = [y]_p, [x]_q = [y]_q$, then $\varphi(([x]_p, [x]_q)) = [x]_{pq}$. Since $p|(x-y)$ and $q|(x-y)$, we have $pq|(x-y), [x]_{pq} = [y]_{pq}$. Hence, $[x]_{pq} = [y]_{pq} = \varphi(([y]_p, [y]_q)) = \varphi(([x]_p, [x]_q))$. Thus $\varphi$ is well-defined.

$\varphi(([x]_p, [x]_q) + ([y]_p, [y]_q)) = \varphi(([x+y]_p, [x+y]_q)) = [x+y]_{pq} = [x]_{pq} + [y]_{pq} = \varphi(([x]_p, [x]_q)) + \varphi(([y]_p, [y]_q))$, so $\varphi$ is a homomorphism.

Suppose $\varphi([x]_p, [x]_q) = 0$, $x$ must be multiple of $pq$, hence, $([x]_p, [x]_q) = ([0]_p, [0]_q)$. Since $\ker\varphi = \{([0]_p, [0]_q)\}$, $\varphi$ is injective, and obviously $|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}| = |\mathbb{Z}/pq\mathbb{Z}| = pq$, $\varphi$ is also surjective. By proposition above, $\varphi$ is an isomorphism.

### (b)

Let $G = \langle g \rangle, H = \langle h \rangle, |G| = n, |H| = m$. If $G \times H$ is cyclic, there exists an integer $d$ such that $(g,h)^d = (e_G, e_H)$. Since $G, H$ are cyclic, we have $n|d, m|d \to \operatorname{lcm}(n,m)|d$. The minimum integer we can choose for $d$ is $\operatorname{lcm}(n,m)$, it's also the order of $G \times H$. Since $|G \times H| = nm = \operatorname{lcm}(n,m)$, we conclude that $\gcd(n,m) = 1$.

Suppose $\gcd(n,m) = 1$, $\langle (g,h) \rangle$ can generate $G \times H$, since the least integer $d$ such that $(g,h)^d = (e_G, e_H)$ is $\operatorname{lcm}(n,m) = nm$, which equals to the order of $G \times H$. Thus, $G \times H$ is cyclic if and only if $\gcd(|G|, |H|) = 1$.

### (c)

$S_3 = (e, (12), (13), (23), (123), (132))$, the only proper subgroups are

$$\{e\}, \{e, (12)\}, \{e, (13)\}, \{e, (23)\}, \{e, (123), (132)\}$$

Since every two distinct subgroups follow the property: their orders are coprime and both are cyclic, their direct product should also be cyclic group by the result of last subproblem. But $S_3$ is not cyclic, thus it's not direct product of any of its proper subgroups.

# 2)

$G$ is the dicyclic group $\text{Dic}_3$, it contains $\{e_G, a, a^2, a^3, a^4, a^5, ab, a^2b, a^3b, a^4b, a^5b\}$, where $e_G$ is its identity. The order is 12.

$H$ is the dihedral group $D_3$, it contains $\{e_H, r, r^2, r^3, r^4, r^5, rs, r^2s, r^3s, r^4s, r^5s\}$, where $e_H$ is its identity. The order is 12.

Consider the order of each element in $H$, $|e_H| = 1, |r| = 6, |r^2| = 3, |r^3| = 2, |r^4| = 3, |r^5| = 6$. Since $sr = r^{-1}s, sr^2 = r^{-1}sr = r^{-2}s, \cdots \Rightarrow sr^i = r^{-i}s$ and $s^2 = 1$, all elements in the form of $r^is$ have order of 2. Since $(r^is)^2 = r^isr^is = r^ir^{-i}ss = e_H$.

Consider the order of each element in $G$, $|e_G| = 1, |a| = 6, |a^2| = 3, |a^3| = 2, |a^4| = 3, |a^5| = 6$. Since $ba = a^{-1}b, ba^2 = a^{-1}ba = a^{-2}b \cdots \Rightarrow ba^i = a^{-i}b$ and $b^2 = a^3, b^4 = 1$, all the elements in the form of $a^ib$ have order of 4 ($(a^ib)^2 = a^iba^ib = b^2 = a^3$, the order of $a^3$ is 2).

Suppose there exists an isomorphism $\varphi$ from $H$ to $G$, for any element $h \in H$, we have $|\varphi(h)|$ divides $|h|$, since if $|h| = m$, then $\varphi(h^m) = \varphi(e_H) = \varphi(h)^m = e_G$, so the order of $\varphi(h) \in G$ have the order divides $m$. But the elements with order 4 in $G$ can't divides the orders of any of $H$, hence, $G$ and $H$ can't be isomorphic.

# 3)

## (a)

## (b)

## (c)

# 4)

## (a)

## (b)

## (c)