Abstract algebra I Homework 4

B13902022 賴昱錡

1)

(a)

Define the homomorphism φ 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 φ 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 φ 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 $\ker\varphi = \{([0]_p, [0]_q)\}$, φ is injective, and obviously $|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}| = |\mathbb{Z}/pq\mathbb{Z}| = pq$, φ is also surjective. By proposition above, φ 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 $n \mid d, m \mid d \to \operatorname{lcm}(n, m) \mid d$. 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 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. (All the elements are distinct, since if $i \neq j$ such that $a^i = a^j, a^{i-j}$, creates a contradiction, hence $i \neq j$ implies $a^i \neq a^j$,similarily, $a^ib \neq a^jb$. Suppose $a^u = a^vb, u \neq v$, we have $b = a^{u-v}, b^2 = a^{2(u-v)}$, it's impossible that $2(u-v) \equiv 3 \pmod 6$, thus, $a^u \neq a^vb$ when $u \neq v$. So every element in G is distinct.)

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. (To check all elements are distinct, we can use the method in last paragraph.)

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 φ 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)

By definition, the orbit of $\langle(12)\rangle = \{e, (12)\}$ is $\{\{1, 2\}, \{3\}, \{4\}\}$, and the orbit of $\langle(123)\rangle = \{e, (123), (132)\}$ is $\{\{1, 2, 3\}, \{4\}\}$. $V = \{e, (12)(34), (13)(24), (14)(23)\}$, its orbit is $\{\{1, 2, 3, 4\}\}$.

(b)

$C_4 = \langle(1234)\rangle$. It's a subgroup of S_4, since every elements $\sigma^i \in C_4$ for some integer i in $\{0, 1, \ldots, 4\}$, it has a inverse σ^{4-i} (σ^0 is considered as identity) in C_4. Also C_4 is clearly closed under multiplication. Its orbit is also $\{\{(1234)\}\}$.

(c)

Suppose $\sigma \in S_n$, where $n \geq 3$. If $(12)\sigma = \sigma(12)$, then $1, 2$ are either fixed or swapped. If $(23)\sigma = \sigma(23)$, then $3, 4$ are also either fixed or swapped. If σ commutes with (12) and (23), then $1, 2, 3$ must be the fixed points of σ. By simple induction, if σ commutes with $(12), (23), (34), \ldots, (n-1, n)$, then $1, 2, \ldots, n$ are all fixed points of σ. Hence σ must be the identity of S_n, i.e., $Z(S_n) = \{e\}$. Since $4 \geq 3$, $Z(S_4) = \{e\}$ is trivial.

4)

(a)

Define for each $g \in G$, the map:

$$\varphi_g : S \to S, \varphi_g(s) = g \cdot s$$

. Then φ_g is a permutation of S (i.e. a bijection).

The inverse of φ_g is $\varphi_{g^{-1}}$, for every $s \in S$, $\varphi_g(\varphi_{g^{-1}}(s)) = s$ (Bijectivity). Also for any $g \in G, s_1, s_2 \in S$, if $\varphi_g(s_1) = \varphi_g(s_2)$, then $\varphi_{g^{-1}}(\varphi_g(s_1)) = \varphi_{g^{-1}}(\varphi_g(s_2)) \Rightarrow s_1 = s_2$ (injectivity). Thus, φ_g is bijective, $\varphi_g \in \mathrm{Perm}(S)$.

Now define $f : G \to \mathrm{Perm}(S)$, $f(g) = \varphi_g$, since $f(gh)(s) = \varphi_{gh}(s) = (gh) \cdot s$ and $(f(g) \circ f(h))(s) = g \cdot (h \cdot s) = (gh) \cdot s$. Hence, $G \to \mathrm{Perm}(S)$ is a homomorphism.

(b)

By last subproblem, $G \to \mathrm{Perm}(S)$ induced a homomorphism ϕ.

$$\phi : G \to \mathrm{Perm}(S), \phi(x)(gH) = x \cdot (gH) = (xg)H$$

$x \in \ker \phi$ if and only if $\phi(x)(gH) = gH \forall g \in G$, i.e., $x \cdot (gH) = (xg)H = gH$. $(xg)H = gH$ must holds for all $g \in G$. Choose $g = e$, we have $xH = H$, by the property of coset, $x \in H$. Thus, $\ker \phi \subseteq H$.

(c)

$|G|/|H| = [G : H] = n$. Let G acts on the set of left cosets of H in G, which we will denote as $X = \{gH | g \in G\}$, by 4(a) and 4(b), here induces a homomorphism.

$$\phi : G \to \mathrm{Perm}(X), \phi(x)(gH) = x \cdot (gH) = (xg)H, gH \in X$$

By the first isomorphism theorem, $\ker \phi \triangleleft G$, also by 4(b) $\ker \phi \subseteq H$. Since no nontrivial normal subgroup of G is contained in H, we concludes that $\ker \phi = \{e\}$.

The first isomorphism theorem states that $G/\ker\phi \cong \mathrm{Im}\phi$, also $G/\{e\} \cong G$, hence we have $G \cong \mathrm{Im}\phi$. Since the image of ϕ are some of the permutations on X where $|X| = n$, clearly G is isomorphic to a subgroup of S_n.