Question 1

Problem a

$$
\begin{aligned}
&\text{Cayley's Theorem :}\\
&\forall \text{ finite group } G, \exists H \subseteq S_n : |G| = n : G \cong H\\
&H \subseteq S_n \implies H \subseteq S_{n+1}\\
&\text{By induction :}\\
&H \in S_{\mathbb{Z}}\\
\Rightarrow &\forall \text{ finite group } G, \exists H \subseteq S_{\mathbb{Z}} : |G| = n : G \cong H
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&G \coloneqq \{\sigma^n | n \in \mathbb{Z}\}\\
&\sigma : \mathbb{Z} \to \mathbb{Z}, \sigma(x) \coloneqq x + 1\\
&G \text{ is a subgroup :}\\
&Id = \sigma^0 \in G\\
&\forall \sigma^n(x) = x + n \in G, \exists \sigma^{-n}(x) = x - n : \sigma^n \circ \sigma^{-n}(x) = Id(x) = n \in G\\
&\forall \sigma^m(x), \sigma^n(x) \in G, \exists \sigma^{m+n}(x) = x + m + n = \sigma^m \circ \sigma^n(x) \in G\\
&\phi : \mathbb{Z} \to G\\
&\phi(i) \coloneqq \sigma^i
\end{aligned}
$$

Injective :

$$\exists i, j \in \mathbb{Z} : \phi(i) = \phi(j)$$
$$\sigma^i(x) = \sigma^j(x)$$
$$x + i = x + j$$
$$\Rightarrow i = j$$

Surjective :

$$\forall \sigma^m \in G, \exists n = m \in \mathbb{Z} : \sigma^n = \sigma^m \in G$$

Homomorphism :

$$\phi(m+n) = \sigma^{m+n}$$
$$\sigma^{m+n} = \sigma^m \cdot \sigma^n = \phi(m)\phi(n)$$
$$\phi(m+n) = \phi(m)\phi(n)$$

Problem c

Identity :

$Id \coloneqq \sigma(x) = x \forall x \in \mathbb{Z}$

$\Rightarrow Id \in H$

Inverse :

$\exists \sigma \in H$

$\sigma^{-1} \circ \sigma(x) = x$

σ moves only finitely many elements

$\Rightarrow \sigma^{-1}$ moves finitely many elements

$\Rightarrow \sigma^{-1} \in H, \forall \sigma \in H$

Closure :

$\exists \sigma, \tau \in H$

Suppose σ moves m entries and τ moves n entries

$\sigma \circ \tau$ moves at most $m + n$ entries

m, n are finite $\implies m + n$ is finite

$\Rightarrow \forall \sigma, \tau \in H, \sigma \circ \tau \in H$

$\Rightarrow H$ is a subgroup

Problem d

$\sigma(x) = 2 - x$

$\sigma^2(x) = 2 - (2 - x) = x$

$\Rightarrow$orbit is $\{\{1\}, \{0, 2\}, ...\{n, 2 - n\}, ...\}$

$\tau(x) = x + 3$

$\tau^2(x) = x + 2 \times 3$

$\Rightarrow \tau^n(x) = x + 3n$

$\Rightarrow$orbit is $\{\{..., -3, 0, 3, ...\}, \{..., -2, 1, 4, ...\}, \{..., -1, 2, 5, ...\}\}$

Question 2

$\sigma = \mu_1\mu_2...\mu_k$
$m \coloneqq ord(\sigma)$
$\Rightarrow \sigma^m = e$
$\mu_1{}^m\mu_2{}^m...\mu_k{}^m = e$
$\Rightarrow \mu_1{}^m = \mu_2{}^m = ... = \mu_k{}^m = e$
$\mu_1{}^{l_1} = \mu_2{}^{l_2} = ... = \mu_k{}^{l_k} = e$
$\Rightarrow l_1|m \wedge l_2|m \wedge ... \wedge l_k|m$
$\Rightarrow m = n \times \text{lcm}(l_1, l_2, ..., l_k)$
Since bigger common multiple is a multiple of least common multiple which cannot be the order m needs to be the smallest common multiple
$\Rightarrow ord(\sigma) = \text{lcm}(l_1, l_2, ..., l_k)$

Question 3

Problem a

$$
\begin{aligned}
&\text{Injective :} \\
&\exists m, n \in G : c_x(m) = c_x(n) \\
&xmx^{-1} = xnx^{-1} \\
&x^{-1}xmx^{-1} = x^{-1}xnx^{-1} \\
&mx^{-1} = nx^{-1} \\
&mx^{-1}x = nx^{-1}x \\
\Rightarrow &m = n \\
\Rightarrow &\forall m, n \in G : c_x(m) = c_x(n) \implies m = n \\
\\
&\text{Surjective :} \\
&\forall g \in G, c_x(h) = xhx^{-1} = g \\
&h = x^{-1}gx \in G \\
\Rightarrow &\forall g \in G, \exists h \in G : c_x(h) = g \\
\Rightarrow &c_x \text{ is bijective} \\
\Rightarrow &c_x \text{ is a permutation} \\
\Rightarrow &c_x \in S_G
\end{aligned}
$$

Problem b

$\exists x, y \in G$

$c_{xy}(g) = xyg(xy)^{-1} = xygy^{-1}x^{-1}$

$c_x \circ c_y(g) = c_x(c_y(g)) = xc_y(g)x^{-1} = xygy^{-1}x^{-1}$

$\Rightarrow c_{xy} = c_x \circ c_y$

ϕ is homomorphic

$G \coloneqq \mathbb{Z}_3$

$1 \neq 2$

$\phi(1) = \phi(2) = Id$

ϕ is not injective

Question 4

Problem a

$$
\begin{aligned}
&\text{Identity :} \\
&\exists a \in G, e_G = a * a^{-1} \\
&\phi \text{ is an homomorphism} \\
\Rightarrow &\phi(a *_G a^{-1}) = \phi(a) *_H \phi(a^{-1}) \\
&\phi(a) *_H \phi(a^{-1}) = \phi(a) *_H \phi(a)^{-1} = e_H \\
\Rightarrow &\phi(e_G) = e_H \\
\Rightarrow &e_G \in \ker\phi \\
&\text{Inverse :} \\
&\exists a \in \ker\phi \\
\Rightarrow &\phi(a) = e_H \\
&\phi(a *_G a^{-1}) = \phi(a) *_H \phi(a^{-1}) = \phi(e_G) = e_H \\
\Rightarrow &e_H *_H \phi(a^{-1}) = e_H \\
\Rightarrow &\phi(a^{-1}) = e_H \\
\Rightarrow &\forall a \in \ker\phi, a^{-1} \in \ker\phi \\
&\text{Closure :} \\
&\exists a, b \in \ker\phi \\
&\phi(a) = \phi(b) = e_H \\
&\phi(ab) = \phi(a) *_H \phi(b) = e_H *_H e_H = e_H \\
\Rightarrow &ab \in \ker\phi \\
\Rightarrow &\forall a, b \in \ker\phi, ab \in \ker\phi \\
\Rightarrow &\ker\phi \text{ is a subgroup of } G
\end{aligned}
$$

Problem b

$$
\begin{aligned}
& g \in \ker \phi \\
\Rightarrow & \phi(g) = e_H \\
& \phi(c_x(g)) = \phi(xgx^{-1}) \\
& \phi(xgx^{-1}) = \phi(x) *_H \phi(g) *_H \phi(x^{-1}) \leftarrow \text{homomorphism} \\
\Rightarrow & \phi(c_x(g)) = \phi(x) *_H e *_H *_H \phi(x^{-1}) = \phi(x) *_H \phi(x^{-1}) \\
& phi(x^{-1}) = \phi(x)^{-1} \leftarrow \text{homomorphism} \\
\Rightarrow & \phi(c_x(g)) = \phi(x) *_H \phi(x)^{-1} = e_H \\
\Rightarrow & c_x(g) = \in \ker \phi, \forall x \in G
\end{aligned}
$$

Problem c

$$
\begin{aligned}
& \phi \text{ is injective } \implies \ker \phi = \{e_G\} : \\
& \phi(e_G) = \phi(a *_G a^{-1}) = \phi(a) *_H \phi(a^{-1}) = \phi(a) *_H \phi(a)^{-1} = e_H \\
& \phi \text{ is injective} \\
\Rightarrow & \forall a, b \in G, \phi(a) = \phi(b) \Rightarrow a = b \\
& \text{Suppose} : \exists a \neq e_G \in G, \phi(a) = e_H \\
& \phi(a) = \phi(e_G) \\
& \forall a, b \in G, \phi(a) = \phi(b) \Leftrightarrow a = b \\
\Rightarrow & a = e_G \not\Leftrightarrow a \neq e_G \\
\Rightarrow & \forall a \neq e_G \in G, \phi(a) \neq e_H \\
\Rightarrow & \ker \phi = \{e_G\}
\end{aligned}
$$

$$
\begin{aligned}
& \ker \phi = \{e_G\} \implies \phi \text{ is injective} : \\
& \text{Suppose} : \phi \text{ is not injective} \\
\Rightarrow & \exists a \neq b \in G : \phi(a) = \phi(b) \\
\Rightarrow & \phi(a) *_H \phi(a)^{-1} = \phi(b) *_H \phi(a)^{-1} \\
\Rightarrow & e_H = \phi(b) *_H \phi(a)^{-1} \\
& \phi(b) *_H \phi(a)^{-1} = \phi(b * a^{-1}) \\
& \phi(b * a^{-1}) = e_H \\
& \ker \phi = \{e_G\} \\
\Rightarrow & b * a^{-1} = e_G \\
\Rightarrow & b = a \not\Leftrightarrow a \neq b \\
\Rightarrow & \phi \text{ is injective} \\
\Rightarrow & \phi \text{ is injective} \Leftrightarrow \ker \phi = \{e_G\}
\end{aligned}
$$

Question 5

Problem a

$$
\begin{aligned}
&\text{Identity :}\\
&Id : G \to G\\
&Id(x) \coloneqq x\\
&\text{Injection :}\\
&\exists a, b \in G : f(a) = f(b) = m\\
&f(a) = m \implies a = m\\
&f(b) = m \implies b = m\\
\Rightarrow &a = b\\
\Rightarrow &\forall a, b \in G, f(a) = f(b) \implies a = b\\
&\text{Surjection :}\\
&\forall g \in G : Id(g) = g, g \in G\\
\Rightarrow &Id \text{ is surjective}\\
&\text{Homomorphism :}\\
&\exists a, b \in G\\
&Id(ab) = ab\\
&Id(a) = a, Id(b) = b\\
\Rightarrow &Id(ab) = Id(a)Id(b)\\
\Rightarrow &Id \in \text{Aut}(G)\\
\\
&\text{Inverse :}\\
&\exists f \in \text{Aut}(G)\\
&f \text{ is a bijection}\\
\Rightarrow &f^{-1} \text{ is a bijection}\\
&f(f^{-1}(mn)) = mn\\
&f(f^{-1}(m)f^{-1}(n)) = f(f^{-1}(m))f(f^{-1}(n)) = mn\\
\Rightarrow &f(f^{-1}(mn)) = f(f^{-1}(m)f^{-1}(n))\\
\Rightarrow &f^{-1}(mn) = f^{-1}(m)f^{-1}(n) \leftarrow f \text{ is isomorphic}\\
\Rightarrow &f^{-1} \text{ is isomorphic}\\
\Rightarrow &f^{-1} \in \text{Aut}(G)\\
&\forall f \in \text{Aut}(G), f^{-1} \in \text{Aut}(G)
\end{aligned}
$$

$$
\begin{aligned}
&\text{Closure :}\\
&\exists f, G \in \mathrm{Aut}(G)\\
&f : G \to G, g : G \to G\\
\Rightarrow &f \circ g : G \to G\\
&f, g \text{ are bijections}\\
\Rightarrow &f \circ g \text{ is bijective}\\
&\exists a, b \in G\\
&f \circ g(ab) = f(g(ab))\\
&g(ab) = g(a)g(b)\\
\Rightarrow &f(g(ab)) = f(g(a))f(g(b)) = f \circ g(a) f \circ g(b)\\
\Rightarrow &f \circ g(ab) = f \circ g(a) f \circ g(b)\\
\Rightarrow &\forall f, g \in \mathrm{Aut}(G) : f \circ g \in \mathrm{Aut}(G)\\
\Rightarrow &\mathrm{Aut}(G) \subset S_G
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&x \in G \\
\Rightarrow &x^{-1} \in G \\
\Rightarrow &xgx^{-1} \in G, \forall g \in G \\
\Rightarrow &c_x : G \to G \\
&\text{Injection :} \\
&\text{Suppose : } c_x(a) = c_x(b), a, b \in G \\
\Rightarrow &xax^{-1} = xbx^{-1} \\
\Rightarrow &x^{-1}xax^{-1} = x^{-1}xbx^{-1} \\
&ax^{-1} = bx^{-1} \\
&ax^{-1}x = bx^{-1}x \\
\Rightarrow &a = b \\
\Rightarrow &c_x(a) = c_x(b) \implies a = b \\
&\text{Surjective :} \\
&\forall g \in G, c_x(g) = xgx^{-1} \\
&xgx^{-1} \in G \\
\Rightarrow &\forall g \in G, \exists xgx^{-1} \in G : c_x(g) = xgx^{-1} \\
&\text{Homomorphism :} \\
&\exists a, b \in G \\
&c_x(ab) = xabx^{-1} \\
&c_x(a) = xax^{-1} \\
&c_x(b) = xbx^{-1} \\
&c_x(a)c_x(b) = xax^{-1}xbx^{-1} = xabx^{-1} \\
\Rightarrow &c_x(ab) = c_x(a)c_x(b) \\
\Rightarrow &c_x \in \text{Aut}(G)
\end{aligned}
$$

Problem c

$$
\begin{aligned}
&G = \langle a \rangle \\
\Rightarrow &\forall g \in G, \exists n \in \mathbb{Z} : g = a^n \\
&\forall i \neq j \in [0, |\langle a \rangle|] \cap \mathbb{Z} : a^i \neq a^j \\
&\phi \text{ is bijective} \\
\Rightarrow &\phi(a^i) \neq \phi(a^j) \\
\Rightarrow &\phi(a)^i \neq \phi(a)^j \\
&\forall i \neq j \in [0, |\langle a \rangle|] \cap \mathbb{Z} : \phi(a)^i \neq \phi(a)^j \\
\Rightarrow &\forall g \in G, \exists p \in \mathbb{Z} : g = \phi(a)^p \\
\Rightarrow &G = \langle \phi(a) \rangle
\end{aligned}
$$

Problem d

$$
\begin{aligned}
&\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle \\
\Rightarrow &a = 1 \vee a = 3 \\
&\mathbb{Z}_4 = \langle \phi(a) \rangle \\
\Rightarrow &\phi(a) = 1 \vee \phi(a) = 3 \\
&\phi \text{ is homomorphic} \implies \phi(0) = 0 \\
\Rightarrow &\text{Aut}(\mathbb{Z}_4) = \{\phi | \phi(0) = 0 \wedge \phi(1) = m \wedge \phi(3) = n, m \neq n \in \{1, 3\}\} \\
&\mathbb{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle \\
\Rightarrow &\phi(a) = 1 \vee \phi(a) = 2 \vee \phi(a) = 3 \vee \phi(a) = 4 \\
&\phi \text{ is homomorphic} \implies \phi(0) = 0 \\
\Rightarrow &\text{Aut}(\mathbb{Z}_5) = \{\phi | \phi(0) = 0 \wedge \phi(1) = m \wedge \phi(2) = n \wedge \phi(3) = p \wedge \phi(4) = q, m \neq n \neq p \neq q \in \{1, 2, 3, 4\}\}
\end{aligned}
$$

Reference

Jeffery Shu