Question 1

Problem a

$$\begin{aligned}
ord(a^{25}) &= \frac{105}{\gcd(105, 25)} = \frac{105}{5} = 21 \\
ord(a^{44}) &= \frac{105}{\gcd(105, 44)} = \frac{105}{1} = 105 \\
ord(a^{70}) &= \frac{105}{\gcd(105, 70)} = \frac{105}{35} = 3
\end{aligned}$$

Problem b

$$\begin{aligned}
&\exists a^n \in \langle a \rangle : ord(a^n) = 6 \\
\Rightarrow &\frac{6000}{\gcd(6000, n)} = 6 \\
&\gcd(6000, n) = 1000 \\
\Rightarrow &n = 1000 \lor n = 5000 \\
\Rightarrow &a^{1000}, a^{5000}
\end{aligned}$$

Problem c

$$\begin{aligned}
&G = \langle a \rangle \text{ has a nontrivial subgroup of order } 11 \\
&n \coloneqq ord(G) \\
&G \text{ has a subgroup of order } 11 \\
\Rightarrow &11 \text{ is a factor of } n \text{ other than the trivial } 1 \text{ and } n \\
&G \text{ has exactly one subgroup} \\
\Rightarrow &11 \text{ is the only factor other than the trivial ones} \\
\Rightarrow &n = 11^2 = 121 \\
\Rightarrow &ord(G) = 121
\end{aligned}$$

Problem d

$$\begin{aligned}
&\text{Define } G \text{ as the group of order} pq \\
&p, q \text{ are distinct primes} \\
\Rightarrow &pq = p \times q \text{ is the only way of factorization} \\
\Rightarrow &G \text{ only has two proper subgroups of order } p \text{ and } q \\
\Rightarrow &G \text{ has four subgroups} \\
&p, q \text{ are primes} \\
\Rightarrow &\gcd(p, p-1) = \gcd(p, p-2) = ... = \gcd(p, 1) = 1 \\
&\gcd(q, q-1) = \gcd(q, q-2) = ... = \gcd(q, 1) = 1 \\
\Rightarrow &G \text{ has } (p-1)(q-1) = pq - p - q + 1 \text{ generators}
\end{aligned}$$

Problem e

$$\begin{aligned}
&\text{Define } G \text{ as the group of order} p^n \\
&\text{factors of } p^n : \{p^k | k \in [0, n] \cap \mathbb{Z}\} \\
&\text{There are } n+1 \text{ factors} \\
\Rightarrow &\text{There are } n+1 \text{ subgroups} \\
&p \text{ is prime} \\
&\text{Only } \gcd(p^n, p \times n) \neq 1 \forall n \in [1, p^{n-1}] \cap \mathbb{Z} \\
\Rightarrow &\text{There are } p^n - p^{n-1} \text{ elements not coprime to } p^n \\
\Rightarrow &\text{There are } p^n - p^{n-1} \text{ generators}
\end{aligned}$$

Question 2

Case 1 : $G = \bigcup G_i, G_i$ is the subgroup of $G \to G \neq \langle g \rangle, \forall g \in G$

Suppose : $\exists g \in G : G = \langle g \rangle$

$n \coloneqq ord(\langle G \rangle)$

$\Rightarrow G_i$should have orders $m : \gcd(m, n) > 1$

Considerg^{n-1}

$\gcd(n, n-1) = 1$

$\Rightarrow g^{n-1} \notin \bigcup G_i$

$g^{n-1} \in \langle g \rangle$

$\Rightarrow G \neq \bigcup G_i \not\Leftrightarrow G = \bigcup G_i$

$\Rightarrow \nexists g \in G : G = \langle g \rangle$

Case 2 : $G \neq \langle g \rangle, \forall g \in G \to G = \bigcup G_i, G_i$ is the subgroup of G

$\forall g \in G, \langle g \rangle$ is a proper subgroup of G $\leftarrow G \neq \langle g \rangle$

$G_i \coloneqq \langle g_i \rangle$

$\Rightarrow \forall g_i \in G, g_i \in \langle g_i \rangle \subset \bigcup \langle g_i \rangle = \bigcup G_i$

$\Rightarrow G \subseteq \bigcup G_i$

$\forall g_i \in \langle g_i \rangle, \exists {g_i}^{-1} : g_i {g_i}^{-1} = e_G$

G is a group $\to {g_i}^{-1} \in G$

$\Rightarrow \langle g_i \rangle \subset G \leftarrow$ all elements of $\langle g_i \rangle$ are in G

This stands for all G_i

$\Rightarrow \forall g_i \in G, G_i = \langle g_i \rangle \subset G$

$\Rightarrow \bigcup G_i = \bigcup \langle g_i \rangle \subseteq G$

$\Rightarrow G = \bigcup G_i$

$G = \bigcup G_i, G_i$ is the subgroup of $G \Leftrightarrow G \neq \langle g \rangle, \forall g \in G$

Q.E.D.

Question 3

$G \coloneqq S_3$

Subgroups of S_3 :

$e = Id$

$\sigma_1 = (1 \;\; 2)$

$\sigma_2 = (1 \;\; 3)$

$\sigma_3 = (2 \;\; 3)$

$\tau_1 = (1 \;\; 2 \;\; 3)$

$\tau_2 = (1 \;\; 3 \;\; 2)$

$\sigma_1 \circ \tau_1 = (1 \;\; 2)(1 \;\; 2 \;\; 3) = (2 \;\; 3)$

$\tau_1 \circ \sigma_1 = (1 \;\; 2 \;\; 3)(1 \;\; 2) = (1 \;\; 3)$

$\Rightarrow \sigma_1 \circ \tau_1 \neq \tau_1 \circ \sigma_1$

proper subgroups : $\{e, \sigma_1\}, \{e, \sigma_2\}, \{e, \sigma_3\}, \{e, \tau_1, \tau_2\} \rightarrow$ abelian

$\Rightarrow S_3$ is not abelian though all the subgroups are abelian

Question 4

$$
\begin{aligned}
&\sigma \coloneqq (1\ \ 2)\\
&\tau \coloneqq (1\ \ 2\ \ 3)\\
&e = Id = \sigma^2 = \tau^3\\
&(1\ \ 2) = \sigma\\
&(1\ \ 2\ \ 3) = \tau\\
&(1\ \ 3\ \ 2) = \tau^2\\
&(1\ \ 3) = (1\ \ 2)(1\ \ 3\ \ 2) = \sigma\tau^2\\
&(2\ \ 3) = (1\ \ 2)(1\ \ 2\ \ 3) = \sigma\tau\\
\Rightarrow &S_3 = \langle \sigma, \tau \rangle
\end{aligned}
$$

Question 5

$$\begin{aligned}
&\text{Identity :}\\
&\forall x \in A : Id(x) = x\\
\Rightarrow &Id \in G_x\\
&\text{Inverse :}\\
&\sigma(x) = x\\
\Rightarrow &\exists \sigma^{-1} : \sigma^{-1}(\sigma(x)) = \sigma^{-1}(x)\\
&\sigma^{-1}(\sigma(x)) = x\\
\Rightarrow &\sigma^{-1}(x) = x\\
\Rightarrow &\forall \sigma \in G_x, \exists \sigma^{-1}(x) \in G_x\\
&\text{Closure :}\\
&\exists \sigma, \tau \in G_x\\
\Rightarrow &\sigma(x) = \tau(x) =\\
&\sigma\tau(x) = \sigma(\tau(x)) = \sigma(x) = x\\
\Rightarrow &\forall \sigma, \tau \in G_x : \sigma\tau \in G_x\\
\Rightarrow &G_x \text{ is a subgroup}
\end{aligned}$$

Question 6

$$G \coloneqq \{Id, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$$
$$A \coloneqq (1\ \ 2)(3\ \ 4)$$
$$B \coloneqq (1\ \ 3)(2\ \ 4)$$
$$C \coloneqq (1\ \ 4)(2\ \ 3)$$

Identity :

$$Id \in G$$

Inverse :

$$A^2 = (1\ \ 2)(3\ \ 4)(1\ \ 2)(3\ \ 4) = Id$$
$$\Rightarrow A^{-1} = A \in G$$
$$B^2 = (1\ \ 3)(2\ \ 4)(1\ \ 3)(2\ \ 4) = Id$$
$$\Rightarrow B^{-1} = B \in G$$
$$C^2 = (1\ \ 4)(2\ \ 3)(1\ \ 4)(2\ \ 3) = Id$$
$$\Rightarrow C^{-1} = C \in G$$

Closure :

$$AB = (1\ \ 2)(3\ \ 4)(1\ \ 3)(2\ \ 4) = (1\ \ 4)(2\ \ 3) = C \in G$$
$$AC = (1\ \ 2)(3\ \ 4)(1\ \ 4)(2\ \ 3) = (1\ \ 3)(2\ \ 4) = B \in G$$
$$BC = (1\ \ 3)(2\ \ 4)(1\ \ 4)(2\ \ 3) = (1\ \ 2)(3\ \ 4) = A \in G$$
$$A^2 = Id \in G$$
$$B^2 = Id \in G$$
$$C^2 = Id \in G$$
$$Id \times A = A \in G$$
$$Id \times B = B \in G$$
$$Id \times C = C \in G$$

$\Rightarrow G$ is a subgroup of S_4

$$\mathbb{V}_4: \begin{array}{c|cccc} * & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array}$$

$$G: \begin{array}{c|cccc} \times & Id & A & B & C \\ \hline Id & Id & A & B & C \\ A & A & Id & C & B \\ B & B & C & Id & A \\ C & C & B & A & Id \end{array}$$

$\leftarrow$ from the calculation above

V_4 and G have the same group table structure

$\Rightarrow G \cong V_4$

Question 7

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\2\\3\end{bmatrix}$$
$$\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}2\\3\\1\end{bmatrix}$$
$$\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\1\\2\end{bmatrix}$$
$$\begin{bmatrix}1&0&0\\0&0&1\\0&1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}1\\3\\2\end{bmatrix}$$
$$\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\2\\1\end{bmatrix}$$
$$\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}2\\1\\3\end{bmatrix}$$

The group has order 6

The group represents the permutation of the values in the vector

$\Rightarrow S_3$ can form an isomorphism with the group

Question 8

$$\begin{aligned}
&\sigma = (1 \;\; 2) \\
&\tau = (3 \;\; 4 \;\; 5) \\
&H = \langle \sigma, \tau \rangle \\
&\sigma^2 = e \\
&\tau^3 = e \\
&\exists m, n \in \mathbb{Z}_{>0} : \sigma^m \tau^n = e \\
\Rightarrow &H \text{ is cyclic} \\
&ord(H) = \text{lcm}(ord(\sigma), ord(\tau)) = 2 \times 3 = 6 \\
&\sigma \text{ and } \tau \text{ are disjoint} \\
\Rightarrow &(1 \;\; 2), (3 \;\; 4 \;\; 5) \text{ can generate } H
\end{aligned}$$

Question 9

Problem a

$$
\begin{aligned}
&\sigma, \tau : H \to H, H = \{1, 2, 3\} \\
&\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1 \;\; 3 \;\; 2) \\
&\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2 \;\; 3) \\
&\sigma \circ \tau = (1 \;\; 3) \\
&\tau \circ \sigma = (1 \;\; 2) \\
\Rightarrow &\sigma \circ \tau \neq \tau \circ \sigma \\
\Rightarrow &S_3 \text{ is not abelian} \\
&S_3 \subset S_4 \subset ... \subset S_n \\
&\text{Suppose } S_n \text{ is abelian} \\
\Rightarrow &S_3 \text{ is abelian} \not\Leftrightarrow S_3 \text{ is not abelian} \\
\Rightarrow &S_n \text{ is not abelian } \forall n \geqslant 3
\end{aligned}
$$

Problem b

Suppose there are no odd permutations in H

All elements of H are even

Suppose there is a subgroup $H_n \in H$ having all the even permutations

$H = H_n \cup \{\sigma \in H | \sigma \text{ is odd}\}$

$\Phi : H_n \to H \setminus H_n$

$\Phi(\tau) = (1, 2)\tau, \tau \in H_n$

$\forall \tau \in H_n, (1, 2)\tau$ is odd

$\Rightarrow H_n \cap \Phi(H_n) = \emptyset$

$\exists \sigma_1, \sigma_2 \in H_n : \Phi(\sigma_1) = \Phi(\sigma_2)$

$(1 \ \ 2)\sigma_1 = (1 \ \ 2)\sigma_2$

$\Rightarrow \sigma_1 = \sigma_2$

$\forall \tau \in \Phi(H_n), \exists \sigma \in H_n : (1 \ \ 2)\sigma = \tau$

$\Rightarrow \Phi$ is bijective

$\Rightarrow |H_n| = |\Phi(H_n)|$

$H_n \cup \Phi(H_n)$

$\Rightarrow$exactly half of the elements are even

Question 10

Problem a

$$
\begin{aligned}
&\sigma(1) = 2 \\
&\sigma(2) = 1 \\
\Rightarrow &(1 \quad 2) \\
&\sigma(3) = 4 \\
&\sigma(4) = 5 \\
&\sigma(5) = 3 \\
\Rightarrow &(3 \quad 4 \quad 5) \\
&\sigma(6) = 7 \\
&\sigma(7) = 8 \\
&\sigma(8) = 9 \\
&\sigma(9) = 10 \\
&\sigma(10) = 6 \\
\Rightarrow &(6 \quad 7 \quad 8 \quad 9 \quad 10) \\
\Rightarrow &\sigma = (1 \quad 2)(3 \quad 4 \quad 5)(6 \quad 7 \quad 8 \quad 9 \quad 10)
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&\sigma = (1 \quad 2)(3 \quad 4 \quad 5)(6 \quad 7 \quad 8 \quad 9 \quad 10) \\
\Rightarrow &\sigma = (1 \quad 2)(3 \quad 5)(3 \quad 4)(6 \quad 10)(6 \quad 9)(6 \quad 8)(6 \quad 7) \\
&\text{There are seven transpositions} \\
\Rightarrow &\sigma \text{ is odd}
\end{aligned}
$$

Problem c

$$
\begin{aligned}
&\sigma = (1\ \ 2)(3\ \ 4\ \ 5)(6\ \ 7\ \ 8\ \ 9\ \ 10) \\
&|(1\ \ 2)| = 2 \\
&|(3\ \ 4\ \ 5)| = 3 \\
&|(6\ \ 7\ \ 8\ \ 9\ \ 10)| = 5 \\
\Rightarrow &\text{Order of } \sigma = \operatorname{lcm}(2,3,5) = 30
\end{aligned}
$$

Reference

Jeffery Shu