Question 1

Problem a

$$
\begin{aligned}
A^0 &= e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\
A^1 &= A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \\
A^2 &= \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \\
A^3 &= \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \\
A^4 &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e \\
\Rightarrow \langle A \rangle &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \right\}
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&z^0 = e = 1 \\
&e^1 = z = \frac{1}{2} + \frac{\sqrt{3}}{2} i = e^{\frac{1}{3}\pi i} \\
&e^2 = e^{\frac{2}{3}\pi i} \\
&e^3 = e^{\pi i} \\
&e^4 = e^{\frac{4}{3}\pi i} \\
&e^5 = e^{\frac{5}{3}\pi i} \\
&e^6 = e^{2\pi i} = 1 = e \\
&\langle z \rangle = \{1, e^{\frac{1}{3}\pi i}, e^{\frac{2}{3}\pi i}, e^{\pi i}, e^{\frac{4}{3}\pi i}, e^{\frac{5}{3}\pi i}\}
\end{aligned}
$$

Question 2

Problem a

$U_k = \langle z \rangle$

$z^m = z^n \Leftrightarrow m \equiv n \mod k$

$\Rightarrow m := ak + b, n := ck + b, a, c \in \mathbb{Z}_{\geqslant 0}, b \in [0, k) \cap \mathbb{Z}$

$$f(z^m) = \begin{bmatrix} \cos(m\theta) & \sin(m\theta) \\ -\sin(m\theta) & \cos(m\theta) \end{bmatrix} = \begin{bmatrix} \cos(\frac{(ak+b)2\pi}{k}) & \sin(\frac{(ak+b)2\pi}{k}) \\ -\sin(\frac{(ak+b)2\pi}{k}) & \cos(\frac{(ak+b)2\pi}{k}) \end{bmatrix} = \begin{bmatrix} \cos(\frac{2b\pi}{k}) & \sin(\frac{2b\pi}{k}) \\ -\sin(\frac{2b\pi}{k}) & \cos(\frac{2b\pi}{k}) \end{bmatrix}$$

$$f(z^n) = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix} = \begin{bmatrix} \cos(\frac{(ck+b)2\pi}{k}) & \sin(\frac{(ck+b)2\pi}{k}) \\ -\sin(\frac{(ck+b)2\pi}{k}) & \cos(\frac{(ck+b)2\pi}{k}) \end{bmatrix} = \begin{bmatrix} \cos(\frac{2b\pi}{k}) & \sin(\frac{2b\pi}{k}) \\ -\sin(\frac{2b\pi}{k}) & \cos(\frac{2b\pi}{k}) \end{bmatrix}$$

$\Rightarrow z^m = z^n \implies f(z^m) = f(z^n)$

Problem b

$\cos(n\theta), \pm\sin(n\theta) \in \mathbb{R} \forall n, \theta \in \mathbb{R}$

$\Rightarrow \forall h \in H, h \in GL_2(\mathbb{R})$

$\Rightarrow H \subseteq GL_2(\mathbb{R})$

Identity :

$e \in GL_2(\mathbb{R}) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$n = 0$

$\Rightarrow f(z^0) = \begin{bmatrix} \cos(0) & \sin(0) \\ -\sin(0) & \cos(0) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = e$

$\Rightarrow e \in H$

Inverse :

$f(z^n) = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}$

$(f(z^n))^{-1} \times f(n^z) = e$

$\Rightarrow (f(z^n))^{-1} \times \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\Rightarrow (f(z^n))^{-1} = \begin{bmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{bmatrix} = \begin{bmatrix} \cos(-n\theta) & \sin(-n\theta) \\ -\sin(-n\theta) & \cos(-n\theta) \end{bmatrix} = f(z^{-n})$

$\Rightarrow (f(z^n))^{-1} = f(z^{-n}) \in H$

Closure :

$A \coloneqq f(z^m), B \coloneqq f(z^n)$

$$A = \begin{bmatrix} \cos(m\theta) & \sin(m\theta) \\ -\sin(m\theta) & \cos(m\theta) \end{bmatrix}, B = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}$$

$$AB = \begin{bmatrix} \cos(m\theta) & \sin(m\theta) \\ -\sin(m\theta) & \cos(m\theta) \end{bmatrix} \times \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}$$

$$\Rightarrow AB = \begin{bmatrix} \cos(m\theta)\cos(n\theta) - \sin(n\theta)\sin(n\theta) & \cos(m\theta)\sin(n\theta) + \sin(m\theta)\cos(n\theta) \\ -\sin(m\theta)\cos(n\theta) - \cos(m\theta)\sin(n\theta) & -\sin(m\theta)\sin(n\theta) + \cos(m\theta)\cos(n\theta) \end{bmatrix}$$

$$AB = \begin{bmatrix} \cos((m+n)\theta) & \sin((m+n)\theta) \\ -\sin((m+n)\theta) & \cos((m+n)\theta) \end{bmatrix} = f(z^{m+n}) \in H$$

$\Rightarrow H$ is a subgroup

Problem c

Injective :

$f(z^m) = f(z^n)$

$$\begin{bmatrix} \cos(m\theta) & \sin(m\theta) \\ -\sin(m\theta) & \cos(m\theta) \end{bmatrix} = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix}$$

$\Rightarrow m\theta \equiv n\theta \mod 2\pi$

$\Rightarrow m \equiv n \mod k \leftarrow \theta = \dfrac{2\pi}{k}$

$\Rightarrow z^m = z^n \in U_k \leftarrow$ Problem a

$\Rightarrow f$ is injective

Surjective :

$$\forall z^m \in U_k, f(z^m) = \begin{bmatrix} \cos(m\theta) & \sin(m\theta) \\ -\sin(m\theta) & \cos(m\theta) \end{bmatrix}$$

$\forall m \in \mathbb{Z}, \exists n \in [0, k) \in \mathbb{Z} : m \equiv n \mod k$

$$\Rightarrow \forall z^m \in U_k, \begin{bmatrix} \cos(m\theta) & \sin(m\theta) \\ -\sin(m\theta) & \cos(m\theta) \end{bmatrix} = \begin{bmatrix} \cos(n\theta) & \sin(n\theta) \\ -\sin(n\theta) & \cos(n\theta) \end{bmatrix} \in H$$

$\Rightarrow f$ is surjective

Homomorphism :

$AB = f(z^{m+n}) \leftarrow$ Problem b

$A = f(z^m), B = f(z^n)$

$\Rightarrow f(z^{m+n}) = f(z^m)f(z^n)$

$\Rightarrow f(z^m z^n) = f(z^m)f(z^n)$

$\Rightarrow f$ is isomorphic

Question 3

$$
\begin{aligned}
&\det(A) \neq 1 \\
\Rightarrow &\det(A^n) \neq 1 \forall n \neq 0 \in \mathbb{Z} \\
\Rightarrow &\nexists n \neq 0 \in \mathbb{Z} : A^n = e \\
&\langle A \rangle \text{ is infinite} \\
&\langle A \rangle \text{ is generated by } A \\
\Rightarrow &\langle A \rangle \text{ is a cyclic group by definition} \\
\Rightarrow &\langle A \rangle \cong \begin{cases} \langle \mathbb{Z}, + \rangle, |\langle A \rangle| = \infty \\ \langle \mathbb{Z}, +_k \rangle, |\langle A \rangle| = k, k \in \mathbb{Z}_{>0} \end{cases} \\
\Rightarrow &\langle A \rangle \cong \langle \mathbb{Z}, + \rangle
\end{aligned}
$$

Question 4

Identity :

$\exists a \in G, a \sim a = a^{-1}a = e$

$\Rightarrow e \in H$

Inverse :

$\exists a \in H : a \in G, a \sim e \implies a^{-1}e = a^{-1} \in H$

Closure :

$\exists a, b \in H$

$\Rightarrow a^{-1} \in H$

$\Rightarrow a^{-1} \sim b \implies (a^{-1})^{-1}b = ab \in H$

$\Rightarrow a, b \in H \implies ab \in H$

$\Rightarrow a \sim b \implies H$ is a subgroup

Question 5

Problem a

$$
\begin{aligned}
&\forall x \in \mathbb{Z}, \exists! q \in \mathbb{Z} \wedge r \in [0,n) \cap \mathbb{Z} : x = nq + r, n \in \mathbb{Z}_{>0} \\
&r \in \{0,1,2,...,n-1\} \\
&|\{0,1,2,...,n-1\}| = n \\
\Rightarrow &n \text{ different equivalence classes} \\
&\forall x \in \mathbb{Z}, \exists! r \in [0,n) \cap \mathbb{Z} : n - r = nq \\
\Rightarrow &\forall x \in \mathbb{Z}, x \in \overline{r} \in \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\} \\
\Rightarrow &\text{There are exactly } n \text{ equivalent classes} : \overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}
\end{aligned}
$$

Problem b

$$
\begin{aligned}
&\overline{c_1} \coloneqq C_1, c_1 \in [0,n) \cap \mathbb{Z} \\
&\overline{c_2} \coloneqq C_2, c_2 \in [0,n) \cap \mathbb{Z} \\
&x_1 \in C_1 \implies x_1 = k_1 n + c_1, k_1 \in \mathbb{Z} \\
&x_2 \in C_2 \implies x_2 = k_2 n + c_2, k_2 \in \mathbb{Z} \\
&x_1 + x_2 = k_1 n + c_1 + k_2 n + c_2 = (c_1 + c_2) + (k_1 + k_2)n \sim c_1 + c_2 \\
&\text{The result is inpendent of } k_1, k_2 \\
\Rightarrow &\forall x_1 \in C_1, x_2 \in C_2 : x_1 + x_2 \sim c_1 + c_2 \\
&C_1 + C_2 = \overline{x_1 + x_2} \text{ is well defined}
\end{aligned}
$$

Problem c

Closure :

$\exists a, b \in [0, n) \cap \mathbb{Z}, A \coloneqq \overline{a}, B \coloneqq \overline{b} \in S$

$\Rightarrow A + B = \overline{a+b} \leftarrow$ Problem b

$a, b \in [0, n) \cap \mathbb{Z} \implies a + b \in [0, 2n) \cap \mathbb{Z}$

$$a + b = \begin{cases} a + b, a + b \in [0, n) \cap \mathbb{Z} \\ a + b - n, a + b \in [n, 2n) \cap \mathbb{Z} \end{cases}$$

$\Rightarrow a + b \in [0, n) \cap \mathbb{Z}$

$\Rightarrow \overline{a+b} \in S$

Identity :

$\exists \overline{a} \in S$

$\overline{a} + \overline{0} = \overline{a+0} = \overline{a} \in S$

$\Rightarrow e = \overline{0} \in S$

Inverse :

$\exists \overline{a} \in S$

$\overline{a} + \overline{n-a} = \overline{a+n-a} = \overline{n} = \overline{0} \in S$

$\Rightarrow \forall \overline{a} \in S, \exists \overline{n-a} \in S : \overline{a} + \overline{n-a} = e$

Associativity :

$\exists \overline{a}, \overline{b}, \overline{c} \in S$

$(\overline{a} + \overline{b}) + \overline{c} = \overline{a+b} + \overline{c} = \overline{a+b+c}$

$\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a+b+c}$

$\Rightarrow (\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$

$\Rightarrow S$ is a group

$\overline{1} \in S$

$\forall k \in \mathbb{Z}_{>0} : \overline{k} = \underbrace{\overline{1} + \overline{1} + \overline{1} + ... + \overline{1}}_{k \text{ times}}$

$\overline{0} = \overline{n} = \underbrace{\overline{1} + \overline{1} + \overline{1} + ... + \overline{1}}_{n \text{ times}}$

$\Rightarrow \overline{1}$ can generate all the elements in S

$\Rightarrow \overline{1}$ is a generator of $\langle S, + \rangle$

S is cyclic

Question 6

Problem a

False

$\mathbb{Z}_5$

$\langle 1\rangle = \langle 2\rangle = \langle 3\rangle = \langle 4\rangle = \mathbb{Z}_5$

The generator is not unique for $\mathbb{Z}_5$

Problem b

False

$\mathbb{Z}_4$

$\langle 2\rangle = \{0, 2\} \neq \mathbb{Z}_4$

Not all elements in a cyclic group is a generator

Problem c

False

Consider $\mathbb{V}_4$:

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\Rightarrow e^2 = a^2 = b^2 = c^2 = e$

Problem d

True

All cyclic groups are isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$

$\mathbb{Z}:$

$\mathbb{Z} = \langle a \rangle = \{..., a^{-2}, a^{-1}, e, a^1, a^2, ...\}$

$\langle a \rangle$ is infinite $\implies \forall n \in Z, \nexists m \neq e \in \langle a \rangle : a^n = e$

$\Rightarrow a^2 = e \implies a = e \leftarrow$ unique solution

$\mathbb{Z}_n :$

$a^2 = e \Leftrightarrow 2a \equiv 0 \mod n$

$\forall a \in [0, n), 2a \in [0, 2n)$

$\Rightarrow 2a \equiv 0 \mod n \implies 2a = 0 \vee 2a = n$

$2|n :$

$a = 0 \vee a = n$

two solutions

$2|n + 1 :$

$a = 0$

unique solution

$\Rightarrow$at most two solutions

Problem e

True

$n = 1 :$ group is trivial

$n > 1 : \exists \mathbb{V}_n$ as a group of order n

$\mathbb{V}_n$ is abelian

Problem f

$$
\begin{aligned}
&g \in G \\
\Rightarrow &g^{-1} \in G \\
&G \text{ has only one gneerator :} \\
\Rightarrow &g = g^{-1} \\
\Rightarrow &g^2 = e \\
\Rightarrow &G = \{e, g\} = \langle g \rangle
\end{aligned}
$$

Question 7

Problem a

$$
\begin{aligned}
\langle 0\rangle &= \{0\}\\
\langle 1\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
\langle 2\rangle &= \{0,2,4,6\}\\
\langle 3\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
\langle 4\rangle &= \{0,4\}\\
\langle 5\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
\langle 6\rangle &= \{0,2,4,6\}\\
\langle 7\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8
\end{aligned}
$$

Problem b

$$
\begin{aligned}
\langle 1\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
\langle 3\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
\langle 5\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
\langle 7\rangle &= \{0,1,2,3,4,5,6,7\} = \mathbb{Z}_8\\
&\Rightarrow 1,3,5,7 \text{ are the generators of the group}
\end{aligned}
$$

Question 8

$\mathbb{Z}_5$:
$\langle 1\rangle = \langle 2\rangle = \langle 3\rangle = \langle 4\rangle = \mathbb{Z}_5$
$\langle 0\rangle = \{0\}$

$$\begin{tikzcd}[arrows=dash]
\langle 1\rangle = \mathbb{Z}_5 \arrow[d] \\
\langle 0\rangle
\end{tikzcd}$$

$\mathbb{Z}_6$:
$\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$
$\langle 2\rangle = \langle 4\rangle = \{0, 2, 4\}$
$\langle 3\rangle = \{0, 3\}$
$\langle 0\rangle = \{0\}$

$$\begin{tikzcd}[arrows=dash]
 & \langle 1\rangle = \mathbb{Z}_6 \arrow[dl] \arrow[dr] & \\
\langle 2\rangle \arrow[dr] & & \langle 3\rangle \arrow[dl] \\
 & \langle 0\rangle &
\end{tikzcd}$$

$\mathbb{Z}_8$:
$\langle 1\rangle = \langle 3\rangle = \langle 5\rangle = \langle 7\rangle = \mathbb{Z}_8$
$\langle 2\rangle = \langle 6\rangle = \{0, 2, 4, 6\}$
$\langle 4\rangle = \{0, 4\}$
$\langle 0\rangle = \{0\}$

$$\begin{tikzcd}[arrows=dash]
\langle 1\rangle = \mathbb{Z}_8 \arrow[d] \\
\langle 2\rangle \arrow[d] \\
\langle 4\rangle \arrow[d] \\
\langle 0\rangle
\end{tikzcd}$$

$\mathbb{Z}_{12}:$
$\langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle 11\rangle = \mathbb{Z}_{12}$
$\langle 2\rangle = \langle 10\rangle = \{0, 2, 4, 6, 8, 10\}$
$\langle 3\rangle = \langle 9\rangle = \{0, 3, 6, 9\}$
$\langle 4\rangle = \langle 8\rangle = \{0, 4, 8\}$
$\langle 6\rangle = \{0, 6\}$
$\langle 0\rangle = \{0\}$

$$\begin{tikzcd}[arrows=dash]
 & & \langle 1\rangle = \mathbb{Z}_{12} \arrow[dl] \arrow[dr] & \\
 & \langle 2\rangle \arrow[dl] \arrow[dr] & & \langle 3\rangle \arrow[dl] \\
\langle 4\rangle \arrow[dr] & & \langle 6\rangle \arrow[dl] & \\
 & \langle 0\rangle & &
\end{tikzcd}$$

Question 9

$$
\begin{aligned}
& G \neq \{e\} \\
\Rightarrow & g \neq e \in G \\
\Rightarrow & \langle g \rangle \subseteq G \\
& \langle g \rangle \neq \{e\} \\
\Rightarrow & \langle g \rangle = G \\
\Rightarrow & G \text{ is cyclic} \\
& \langle g^2 \rangle = \{e\} \vee \langle g^2 \rangle = G = \langle g \rangle \\
& \langle g^2 \rangle = \{e\} \implies |G| = 2 \\
& \langle g^2 \rangle = G = \langle g \rangle : \\
& \exists k \in \mathbb{Z} : g^{2k} = g \\
\Rightarrow & e = g^{2k-1} \\
& |G| \coloneqq m \\
& \exists h \in (1, n) \in \mathbb{Z} : \langle g^h \rangle = \langle g \rangle \\
\Rightarrow & \exists n \in \mathbb{Z} g^{nh} = g \\
& g^{nh-1} = e \\
\Rightarrow & m | nh - 1 \\
\Rightarrow & \gcd(m, h) = 1 \forall h \in (1, n) \\
\Rightarrow & m \text{ is prime}
\end{aligned}
$$

Question 10

$$\langle \mathbb{Z}, +_5 \rangle$$
$$|\langle \mathbb{Z}, +_5 \rangle| = 5$$
$$\langle \mathbb{Z}, +_5 \rangle = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle$$
$$\langle \mathbb{Z}, +_8 \rangle$$
$$|\langle \mathbb{Z}, +_8 \rangle| = 8$$
$$\langle \mathbb{Z}, +_8 \rangle = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$$
$$\langle \mathbb{Z}, +_{10} \rangle$$
$$|\langle \mathbb{Z}, +_{10} \rangle| = 10$$
$$\langle \mathbb{Z}, +_{10} \rangle = \langle 1 \rangle = \langle 3 \rangle = \langle 7 \rangle = \langle 9 \rangle$$