1. (a) Let e be the identity of G. Then $e \in H$ and $e \in K$. Hence $e \in H \cap K$, so $H \cap K$ is a non-empty subset of G. Let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$. But each of H and K is a subgroup of G. Thus $x * y^{-1} \in H$ and $x * y^{-1} \in K$ It follows that $x * y^{-1} \in H \cap K$, and by the one-step subgroup test, $H \cap K$ is a subgroup of G.

(b) $H \cup K = \{0, 2, 3, 4\}$.

(i) $H \cup K$ is not a subgroup of G, since $2 + 3 = 5 \notin H \cup K$.

(ii) As $|H \cup K| = 4$ and $|G| = 6$, and $4 \nmid 6$, we have $|H \cup K| \nmid |G|$ so by Lagrange's theorem $H \cup K$ is not a subgroup of G.

2. Let $(a, b), (c, d)$ be two arbitrary elements of $\mathbb{Z} \times \mathbb{Z}$. Then φ is a function from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$ since it associates with each (a, b) just ONE image $3a - 6b$. Also

$$\begin{aligned} \varphi((a, b) * (c, d)) &= \varphi(a + c, b + d) \\ &= 3(a + c) - 6(b + d) \\ &= (3a - 6b) + (3c - 6d) \\ &= \varphi((a, b)) + \varphi((c, d)). \end{aligned}$$

Hence φ is a homomorphism from $\mathbb{Z} \times \mathbb{Z}$ to $\mathbb{Z}$. $\ker(\varphi) = \{\, x \in \mathbb{Z} \times \mathbb{Z} : \varphi(z) = 0 \,\}$, since 0 is the identity of $(\mathbb{Z}, +)$. If $x \in \mathbb{Z} \times \mathbb{Z}$ then $x = (a, b)$ for some $a, b \in \mathbb{Z}$. But $\varphi((a, b)) = 3a - 6b$ so if $\varphi(x) = \varphi((a, b)) = 0$ then $3a - 6b = 0$, so $a = 2b$. Thus

$$\ker(\varphi) = \{\, (2b, b) : b \in \mathbb{Z} \,\}.$$

3. As $e^3 = e$, $e \in H$ and so H is a non-empty subset of G. Let $x, y \in H$. Then $x^3 = e$ and $y^3 = e$. Is $x * y \in H$? Since G is abelian, $(x * y)^3 = x^3 * y^3$ (by a theorem given in class), and hence $(x * y)^3 = x^3 * y^3 = e * e = e$. So $x * y \in H$. Is $y^{-1} \in H$? Since $y^3 = e$, we have $y^{-1} = y^2$, and $(y^2)^3 = (y^3)^2 = e^2 = e$, and so $y^{-1} \in H$. Hence by the two-step subgroup test, H is a subgroup of G.

4. (a) Let $A, B \in G$. Then $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$ for some $a, b, c, d \in \mathbb{R}$ and $\det(A) \neq 0$, $\det(B) \neq 0$. It follows that $AB = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}$, and clearly $\det(AB) = \det(A)\det(B) \neq 0$. Hence $AB \in G$, and the closure law is satisfied. To show the other conditions of the group are satisfied, we have:

(i) As the matrix multiplication is associative for all 2×2 real matrices, the associative law holds for G;

(ii) $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of G; and

(iii) for all $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$ there exists

$$A^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & \frac{-b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in G$$

and $AA^{-1} = A^{-1}A = I$.

Hence $(G, \cdot)$ forms a group.

(b) Define $f : (\mathbb{C} \setminus \{0\}) \to (G, \cdot)$ by $f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, where $a, b \in \mathbb{R}$, $a^2 + b^2 \neq 0$.

(i) f is well-defined because for all $a, b, c, d \in \mathbb{R}$, if $a + ib = c + id$ then $a = c$ and $b = d$, and hence $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, i.e. $f(a+ib) = f(c+id)$.

(ii) f is one-to-one because if $a+ib, c+id \in \mathbb{C} \setminus \{0\}$ such that $f(a+ib) = f(c+id)$ then $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$, and hence $a = c$ and $b = d$. Therefore $a + ib = c + id$.

(iii) f is onto, because for all $y = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in G$, $a, b \in \mathbb{R}$ and $a^2 + b^2 \neq 0$ we can find $x = a + ib \in \mathbb{C} \setminus \{0\}$ such that $f(x) = f(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = y$.

(iv) Finally, f is a homomorphism because for all $x = a + ib$ and $y = c + id$ in $\mathbb{C} \setminus \{0\}$ we have

$$\begin{aligned} f(x \cdot y) &= f((a+ib)(c+id)) \\ &= f((ac - bd) + i(ad + bc)) \\ &= \begin{pmatrix} ac - bd & ad + bc \\ -(ad+bc) & ac - bd \end{pmatrix} \\ &= \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= f(a+ib) \cdot f(c+id) \\ &= f(x) \cdot f(y) \end{aligned}$$

It follows that $(C \setminus \{0\}, \cdot) \simeq (G, \cdot)$.

5. (a) H is a non-empty subset of G, since $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ (notice that $\det(I) = 1 = 7^0$). If $A, B \in H$ then $\det(A) = 7^i$ and $\det(B) = 7^j$ for some $i, j \in \mathbb{Z}$. Then $\det(AB) = \det(A)(\det(B))^{-1} = 7^{i-j}$. Since $i - j \in \mathbb{Z}$, it follows that $AB^{-1} \in H$, and by the one-step subgroup test, H is a subgroup of G.

(b) $\det(A) = -2 = 5$, and $5^{-1} = 3$, so

$$A^{-1} = 3 \begin{pmatrix} 3 & -4 \\ -2 & 2 \end{pmatrix} = \begin{pmatrix} 9 & -12 \\ -6 & 6 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 1 & 6 \end{pmatrix}$$

in $\mathbb{Z}_7$.