1. (20 pts.) Suppose that $H$ is a subgroup of $G$ and $|H| = 2$. Comment: By assumption $H$ has two elements. Therefore $H = \{e, a\}$ where $a \neq e$.

a) Suppose that $H$ is normal subgroup of $G$. Show that $H$ is in the center of $G$.

Solution: Suppose that $H = \{e, a\}$ is a normal subgroup of $G$ which has two elements. Let $x \in G$. Then $xH = \{xe, xa\} = \{x, xa\}$ and $Hx = \{ex, ax\} = \{x, ax\}$ are equal since $H$ is normal. Thus $\{x, xa\} = \{x, ax\}$ which means $xa = x$ or $xa = ax$. If $xa = x$ then $xa = x = xe$ which implies $a = e$ by cancelation. This is a contradiction since $a \neq e$. Therefore $xa = ax$.

We have shown that $a \in Z(G)$. Since $Z(G)$ is a subgroup of $G$, $e \in Z(G)$ as well. Therefore $H \subseteq Z(G)$. (12 points)

b) Suppose that $H$ is in the center of $G$. Show that $H$ is a normal subgroup of $G$.

Solution: Suppose that $H \subseteq Z(G)$ and let $x \in G$. Then $xa = ax$ since $a \in Z(G)$. Thus $xH = \{xe, xa\} = \{x, xa\} = \{x, ax\} = Hx$.

We have shown that $xH = Hx$ for all $x \in G$. Therefore $H$ is a normal subgroup of $G$. (8 points)

2. (20 pts.) Let $G = \langle a \rangle$ be cyclic of order $n$ and suppose that $f : G \rightarrow G'$ is a group homomorphism.

a) Show that $f(a)$ has finite order and $|f(a)|$ divides $n = |a|$.

Solution: There are various reasons. Since $b^n = f(a)^n = f(a^n) = f(e) = e$ it follows that $b$ has finite order and $|b|$ divides $n$. (4 points)

b) Suppose that $b \in G'$ has finite order and $|b|$ divides $n$. Show that the rule $\phi : G \rightarrow G'$ given by $\phi(a^m) = b^m$ is a well-defined group homomorphism. (Well-defined here means that $a^m = a^{m'}$ implies that $b^m = b^{m'}$.)

Solution: First of all $\phi$ is well-defined. Suppose that $a^m = a^{m'}$. Then $n = |a|$ divides the difference $m - m'$. Since $|b|$ divides $n$ it follows that $|b|$ divides $m - m'$. Therefore $b^m = b^{m'}$. (6 points)

Next, $\phi$ is a homomorphism since

$$\phi(a^ka^m) = \phi(a^{k+m}) = b^{k+m} = b^kB^M = \phi(a^k)\phi(a^m)$$

for all integers $k, m$. (6 points)
c) Show that the rule \( \phi : \mathbb{Z}/7\mathbb{Z} \rightarrow \mathbb{Z}/8\mathbb{Z} \) given by \( \phi(m + 7\mathbb{Z}) = m + 8\mathbb{Z} \) is not a well-defined function by finding specific integers \( m, m' \) such that \( m + 7\mathbb{Z} = m' + 7\mathbb{Z} \) but \( m + 8\mathbb{Z} \neq m' + 8\mathbb{Z} \).

\[ \text{Solution:} \quad 0, 7 \in 7\mathbb{Z}; \text{ however } 0 + 8\mathbb{Z} = 8\mathbb{Z} \neq 7 + 8\mathbb{Z} \text{ since } 7 \text{ is not a multiple of } 8. \] (4 points)

3. (20 pts.) Let \( R, S \) be rings with unity.

a) Show that \( U(R \oplus S) = U(R) \oplus U(S) \) as groups.

\[ \text{Solution:} \quad \text{Suppose that } (r, s) \in U(R \oplus S). \text{ Then there is an } (r', s') \in U(R \oplus S) \text{ such that} \]
\[ (r, s)(r', s') = (1, 1) = (r', s')(r, s), \] (1)

or equivalently
\[ (rr', ss') = (1, 1) = (r'r, s's). \] (2)

Since ordered pairs are equal if and only if corresponding components are equal we have
\[ rr' = 1 = r'r \quad \text{and} \quad ss' = 1 = s's. \] (3)

Thus \( r \in U(R) \) and \( s \in U(S) \) by definition. We have shown \( U(R \oplus S) \subseteq U(R) \oplus U(S) \). (4 points)

Conversely, suppose that \( r \in U(R) \) and \( s \in U(S) \). Then there are \( r' \in R \) and \( s' \in S \) such that (3) holds. Therefore (2) holds, and its equivalent (1) does as well. We have shown that \( U(R) \oplus U(S) \subseteq U(R \oplus S) \). Therefore \( U(R \oplus S) = U(R) \oplus U(S) \).

These are the same as groups since in both cases multiplication is component multiplication. (4 points)

b) List the elements of \( U(\mathbb{Z}_5 \oplus \mathbb{Z}_6) \).

\[ \text{Solution:} \quad \text{The units of } \mathbb{Z}_n \text{ are the generators of the additive group } \mathbb{Z}_n. \text{ Thus the units of } \mathbb{Z}_5 \oplus \mathbb{Z}_6 \text{ are listed by} \]
\[ (1, 1), \ (1, 5), \ (2, 1), \ (2, 5), \ (3, 1), \ (3, 5), \ (4, 1), \ (4, 5). \] (12 points)

4. (20 pts.) Let \( R = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, d \in 2\mathbb{Z}, b, c \in 3\mathbb{Z} \}. \) (Recall that \( n\mathbb{Z} = \{nq \mid q \in \mathbb{Z}\} \) for all \( n \in \mathbb{Z} \).)

\[ \text{Comment:} \quad \text{Observe that } R = \left\{ \begin{pmatrix} 2x & 3y \\ 3z & 2w \end{pmatrix} \mid x, y, z, w \in \mathbb{Z} \right\}. \]
a) Show that $R$ is an additive subgroup of $M(2, R)$.

Solution: With $x = y = z = w = 0$ we have $0 \in R$. Therefore $R \neq \emptyset$. Since

$$
\begin{pmatrix}
2x & 3y \\
3z & 2w
\end{pmatrix}
- \begin{pmatrix}
2x' & 3y' \\
3z' & 2w'
\end{pmatrix}
= \begin{pmatrix}
2(x - x') & 3(y - y') \\
3(z - z') & 2(w - w')
\end{pmatrix}
$$

for $x, y, z, w, x', y', z', w' \in \mathbb{Z}$, and since $\mathbb{Z}$ is a group under addition, it follows that $R$ is an additive subgroup of $M(2, R)$. (14 points)

b) Determine whether or not $R$ is a subring of $M(2, R)$.

Solution: $R$ is not a subring. For example $\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \in R$ but

$$
\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix} = \begin{pmatrix} 13 & * \\ * & * \end{pmatrix} \not\in R. (6 points)
$$

5. (20 pts.) Let $R$ be a ring.

a) Define ideal of $R$.

Solution: An ideal of the ring $R$ is an additive subgroup $I$ of $R$ such that $ra, ar \in I$ for all $a \in I$ and $r \in R$. (6 points)

b) Suppose that $R$ is commutative and $a, b \in R$. Show that $I = \{ra + sb | r, s \in R\}$ is an ideal of $R$.

Solution: Let $a, b \in R$ and $I = \{ra + sb | r, s \in R\}$, where $R$ is commutative. Since $0 = 0a + 0b$ it follows that $0 \in I$. Thus $I$ is not empty. (2 points). Suppose that $ra + sb, r'a + s'b \in I$. Then

$$(ra + sb) - (r'a + s'b) = (r - r')a + (s - s')b \in I. (6 points)$$

Therefore $I$ is an additive subgroup of $R$. Now suppose that $x \in R$ and $ra + sb \in I$. Then

$$x(ra + sb) = (xr)a + (xs)b \in I. (6 points)$$

Since $R$ is commutative it follows that $I$ is an ideal of $R$. (6 points)