Instructions. Answer each of the questions on your own paper and be sure to show your work so that partial credit can be adequately assessed. There is a total of 75 points possible. Put your name on each page of your paper.

1. [**12 Points**] Complete the following definitions.

   (a) A subset I of a ring R is an *ideal* of R if ... *I is an additive subgroup of R and for each $a \in I$ and $r \in R$, $ar \in I$ and $ra \in I$.*

   (b) If R is a commutative ring with identity, and P is an ideal of R with $P \neq R$, then P is a *prime ideal* of R if ... *whenever a, $b \in R$ satisfy $ab = 0$, then $a = 0$ or $b = 0$.*

   (c) If R is a commutative ring with identity, then the *characteristic* of R is ... *the order of the multiplicative unit element 1 of R.*

2. [**12 Points**] Let $G = \left\{ \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix} : a,\, b \in \mathbb{R},\ b \neq 0 \right\}$, and $H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{R} \right\}$. You may assume that G is a subgroup of the invertible 2×2 matrices with real coefficients under matrix multiplication. Let $\mathbb{R}^*$ denote the group of nonzero real numbers under multiplication.

   (a) Show that the function $f : G \to \mathbb{R}^*$ given by $f\left(\begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix} \right) = b$ is a group homomorphism.

   ▶ **Solution.** Let $A = \begin{bmatrix} 1 & a \\ 0 & b \end{bmatrix}$ and $B = \begin{bmatrix} 1 & c \\ 0 & d \end{bmatrix}$ be elements of G. Then

   $$f(AB) = f\left(\begin{bmatrix} 1 & 1 \\ 0 & b \end{bmatrix} \begin{bmatrix} 1 & c \\ 0 & d \end{bmatrix} \right) = f\left(\begin{bmatrix} 1 & c + ad \\ 0 & bd \end{bmatrix} \right) = bd = f(A)f(B).$$

   Thus f is a group homomorphism. ◀

   (b) Find $\mathrm{Ker}(f)$.

   ▶ **Solution.** The identity of $\mathbb{R}^*$ is 1, so the kernel of f is the set of all $A \in G$ with $f(A) = 1$, which is exactly the subgroup H of G ◀

   (c) Show that H is a normal subgroup of G and that $G/H \cong \mathbb{R}^*$. (*Hint*: Parts (a), (b) and First Isomorphism Theorem.)

   ▶ **Solution.** Since $H = \mathrm{Ker}(f)$, H is a normal subgroup of G. The first isomorphism theorem then shows that $G/\mathrm{Ker}(f) \cong f(G)$. But $H = \mathrm{Ker}(f)$ by part (b) and f is onto since, for any $b \in \mathbb{R}^*$, $b = f(A)$ for $A = \begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix}$, so $f(G) = \mathbb{R}^*$. Thus, $G/H \cong \mathbb{R}^*$ ◀

3. [**12 Points**]

(a) Find all distinct isomorphism classes of abelian groups of order 75.

► **Solution.** Since $75 = 5^2 \cdot 3$ There are 2 abelian groups of order 75: $\mathbb{Z}_{25} \times \mathbb{Z}_3$ and $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3$. ◄

(b) If G is a finite abelian group of order 75, explain why G has one subgroup of order 5 or six subgroups of order 5.

► **Solution.** If G is an abelian group of order 75, then G is isomorphic to one of the two groups in part (a).

Case 1: Suppose that G is isomorphic to $\mathbb{Z}_{25} \times \mathbb{Z}_3$. It is sufficient to compute the number of subgroups of $\mathbb{Z}_{25} \times \mathbb{Z}_3$ of order 5, since this will be the same as for G. A subgroup H of $\mathbb{Z}_{25} \times \mathbb{Z}_3$ of order 5 is a cyclic subgroup of order 5 generated by (a, b) where the order of (a, b) is 5. Since this order is the least common multiple of the order of a and the order of b, it follows that $|a| = 5$ and $|b| = 1$ since $|a| \mid 25$ and $|b| \mid 3$. Thus, $b = 1$ and the generator of H is $(a, 1)$ where a is an element of order 5 in $\mathbb{Z}_{25}$. But $\mathbb{Z}_{25}$ is cyclic of order 25, and hence has a unique subgroup K of order 5, namely the subgroup of $\mathbb{Z}_{25}$ generated by 5, and each nonzero element of $\langle 5 \rangle$ is also an element of $\mathbb{Z}_{25}$ that generates K. Thus, the only subgroup of $\mathbb{Z}_{25} \times \mathbb{Z}_3$ of order 5 is $K \times \langle 1 \rangle$ where K is the unique subgroup of $\mathbb{Z}_{25}$ of order 5.

Case 2: Suppose that G is isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3$. Then it is sufficient to compute the number of subgroups of $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3$ of order 5. As in Case 1, a subgroup of $\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_3$ will be $K \times \langle 1 \rangle$ where K is a subgroup of $\mathbb{Z}_5 \times \mathbb{Z}_5$ of order 5. Any nonzero element (a, b) of $\mathbb{Z}_5 \times \mathbb{Z}_5$ has order $\operatorname{lcm}(|a|, |b|) = 5$ since both a and b have order 1 or 5 and at least one of them has order 5. Thus, the subgroups of $\mathbb{Z}_5 \times \mathbb{Z}_5$ are the cyclic subgroups $\langle (a, b) \rangle$ generated by a nonzero element (a, b) of $\mathbb{Z}_5 \times \mathbb{Z}_5$. Each subgroup of order 5 has 4 nonzero elements, each of order 5. Moreover, if K_1 and K_2 are two subgroups of order 5, then $K_1 \cap K_2$ is a subgroup of both K_1 and K_2. Thus, $|K_1 \cap K_2| = 1$ or 5. If $|K_1 \cap K_2| = 1$ then K_1 and K_2 have only the identity $(0, 0)$ in common. Otherwise, $K_1 = K_2$ since $|K_1 \cap K_2| = 5$ and $|K_1 \cap K_2|$ is a subgroup of both K_1 and K_2. Thus, each subgroup of $\mathbb{Z}_5 \times \mathbb{Z}_5$ consists of 4 elements of order 5 plus the identity $(0, 0)$. Since there are 24 nonzero elements of $\mathbb{Z}_5 \times \mathbb{Z}_5$ and each subgroup of order 5 accounts for 4 of them, it follows that there are 6 subgroups of $\mathbb{Z}_5 \times \mathbb{Z}_5$. Hence, there are exactly 6 subgroups of G in Case 2.

Since Cases 1 and 2 cover all abelian groups of order 75, it follows that each such group has either 1 subgroup of order 5 (Case 1) or 6 subgroups of order 5 (Case 2). ◄

4. [**12 Points**] Determine which of the following are ideals of the rings given. For those that are, no proof is required. For those which are not, an explanation is required.

(a) Is $3\mathbb{Z}$ an ideal of $\mathbb{Z}$? **Answer:** This is an ideal. (All ideals of $\mathbb{Z}$ are of the form $n\mathbb{Z}$ for $n \in \mathbb{Z}$.

(b) Is $\mathbb{R}$ an ideal of $\mathbb{R}[x]$? **Answer:** This is not an ideal since $1 \in \mathbb{R}$ and $x \in \mathbb{R}[x]$, but $1 \cdot x = x \notin \mathbb{R}$.

(c) Is $I = \left\{ \begin{bmatrix} a & 0 \\ c & 0 \end{bmatrix} \middle| a,\, c \in \mathbb{Z} \right\}$ an ideal of $M_2(\mathbb{Z})$? **Answer:** This is not an ideal since $A = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in I$ and $B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{Z})$, but $AB = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \notin I$.

5. **[15 Points]** Let $I = \langle 2 \rangle = 2\mathbb{Z}[i] = \{2a + 2bi : a,\, b \in \mathbb{Z}\}$ be the principal ideal generated by 2 in the Gaussian integers $\mathbb{Z}[i]$.

(a) Describe all the elements in $\mathbb{Z}[i]/I$, with justification. Give an explicit list of distinct elements.

▶ **Solution.** Let $a + bi \in \mathbb{Z}[i]$. Divide each of a and b by 2 to get $a = 2q_1 + r$ and $b = 2q_2 + s$ where $0 \le r,\, s < 2$. Then

$$a + bi = (2q_1 + r) + (2q_2 + s)i = (r + si) + 2(q_1 + q_2 i).$$

Hence, any element $a + bi$ can be written as a sum of an element of I (namely $2(q_1 + q_2 i)$ and an element $r + si$ where $0 \le r,\, s < 1$. Thus, every element of $\mathbb{Z}[i]/I$ is one of the 4 cosets

$$0 + I,\ 1 + I,\ i + I,\ (1 + i) + I.$$

These elements are all distinct since the difference between any two different elements $0,\, 1,\, i,\, 1 + i$ is not of the form $2(m + ni)$ and hence not in I. Thus, the 4 listed elements are all of the distinct cosets in $\mathbb{Z}[i]/I$. ◀

(b) Calculate:

i. $((1 + i) + I) + ((3 - 2i) + I)$ **Answer:** $(4 - i) + I = i + I$

ii. $((1 + i) + I)((1 + i) + I)$ **Answer:** $(1 + i)^2 + I = 2i + i = 0 + I$

(c) Show that I is not a prime ideal in $\mathbb{Z}[i]$.

▶ **Solution.** $(1 + i)^2 = 2i \in I$ but $1 + i \notin I$ since 1 is odd. ◀

6. **[12 Points]** Let R be an integral domain.

(a) Prove that cancellation holds over R. That is, if $a,\, b,\, c \in R$, with $ab = ac$ and $a \neq 0$, then prove that $b = c$.

▶ **Solution.** Assume that R is an integral domain and $ab = ac$ but $a \neq 0$. Then subtracting ac from both sides of the equation gives $ab - ac = 0$ so that $a(b - c) = 0$. Since R is an integral domain, this means that $a = 0$ or $b - c = 0$. Since $a \neq 0$ this means that $b - c = 0$ which implies that $b = c$ by adding c to both sides of the equation. ◀

(b) An element $c \in R$ is *idempotent* if $c^2 = c$. Prove that in an integral domain R, if c is a nonzero idempotent, then $c = 1$.

▶ **Solution.** Use the cancellation property proved above. If c is an idempotent, then $c^2 = c$ which implies that $c \cdot c = c \cdot 1$, which, by part (a), implies that $c = 1$. ◀