Problem 1. Prove that if $0 = 1$ in a ring R, then R is the zero ring (that is, its only element is 0).

Proof. $\forall r \in R, r = 1 \cdot r = 0 \cdot r = 0 \implies R = \{0\}$.

$\square$

Problem 2. A category C' is a subcategory of a category C if

  (1) $\mathrm{Obj}(C') \subseteq \mathrm{Obj}(C)$, and

  (2) for all $A, B \in \mathrm{Obj}(C')$, $\mathrm{Hom}_{C'}(A, B) \subseteq \mathrm{Hom}_C(A, B)$.

It is a full subcategory if in addition $\mathrm{Hom}_{C'}(A, B) = \mathrm{Hom}_C(A, B)$ for all $A, B \in \mathrm{Obj}(C')$.

Ring with unity is a subcategory of Ring (you do not need to prove this). Show that it is not a full subcategory.

Proof. $\varphi : \mathbb{Z}_6 \mapsto \mathbb{Z}_6$ defined via $\varphi(a) = [0]a$ belongs to $\mathrm{Hom}_{\mathrm{Ring}}(\mathbb{Z}_6, \mathbb{Z}_6)$ but not $\mathrm{Hom}_{\mathrm{Ring\ with\ unity}}(\mathbb{Z}_6, \mathbb{Z}_6)$ since $\varphi([1]) = [0] \neq [1]$, and a ring homomorphism in $\mathrm{Hom}_{\mathrm{Ring\ with\ unity}}(\mathbb{Z}_6, \mathbb{Z}_6)$ must preserve unity. So $\mathrm{Hom}_{\mathrm{Ring\ with\ unity}}(A, B) \neq \mathrm{Hom}_{\mathrm{Ring}}(A, B)$ for $A = B = \mathbb{Z}_6 \in \mathrm{Obj}(\mathrm{Ring\ with\ unity})$.

Thus,

$$\text{Ring with unity is not a full subcategory of Ring.}$$

$\square$

Problem 3. Let a and b be zero-divisors in a ring R. Either prove $a + b$ is always a zero-divisor or provide a specific counterexample.

Proof. Consider $[2], [3] \in \mathbb{Z}_6$. $[2] \cdot [3] = [0]$ and both are non-zero, so they are both zero-divisors. Yet $[2] + [3] = [5]$, which isn't a zero divisor since $([5][m])_{m=0}^5 = ([0], [5], [4], [3], [2], [1])$.

Thus,

$$\text{the sum of two zero-divisors is not always a zero-divisor.}$$

$\square$

Problem 4. The center of a ring R is $Z(R) = \{z \in R \mid rz = zr$ for all $r \in R\}$. Prove that the center of a ring R is a subring of R.

Proof. $\forall a, b \in Z(R)$, and $\forall r \in R$,

$$[\mathbf{1}] : 1r = r1 = r \implies 1 \in Z(R)$$
$$[\leq_+] : (a - b)r = ar - br = (ra) - (rb) = r(a - b) \implies a - b \in Z(R)$$
$$[\cdot] : (ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab) \implies ab \in Z(R).$$

Thus,

$$Z(R) \text{ is a subring of } R.$$

$\square$

Problem 5. An element x in a ring R is called nilpotent if $x^m = 0$ for some $m \in \mathbb{Z}^+$ (here x^m denotes $x \cdot x \cdots x$ (m times)).

Prove that the nilpotent elements of a commutative ring R form an ideal (this is called the nilradical of R).

Proof. Let R be a commutative ring with unity, and let $\mathrm{nil}(R)$ be the set of all nilpotent elements of R; $\mathrm{nil}(R) = \{x \in R \mid x^m = 0 \text{ for some } m \in \mathbb{Z}^+\}$. Notice that in general for $r \in \mathrm{nil}(R)$: if $r^N = 0$, then $r^{N+k} = r^N r^k = (0) r^k = 0 \implies r^j = 0, \forall j \geq N$.

Now let $x, y \in \mathrm{nil}(R)$. Then $x^m = 0, y^n = 0$ for some $m, n \in \mathbb{Z}^+$. By the Binomial Theorem,

$$(x-y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i (-y)^{m+n-i} = \sum_{i=0}^{m+n} (-1)^{m+n-i} \binom{m+n}{i} x^i (y)^{m+n-i} = 0$$

$$\text{Since } i \geq m \implies x^i = 0 \text{ or } 0 \leq i < m \implies m+n-i \geq n \implies y^{m+n-i} = 0$$

So $x - y \in \mathrm{nil}(R)$, and therefore it is an additive subgroup of R.

Since R is commutative, $(rx)^k = r^k x^k$ For all $k \geq 1$. So then obviously $(rx)^m = r^m x^m = r^m(0) = 0 \implies rx = xr \in \mathrm{nil}(R)$.

Thus,
$$\text{The nilradical } \mathrm{nil}(R) \text{ of R is a two-sided ideal of } R.$$

$\square$

Problem 6. Let $n \in \mathbb{N}$.

 (a) Show that if $n = ab$ for some integers a, b, then ab is a nilpotent element of $\mathbb{Z}/n\mathbb{Z}$.

 (b) If $a \in \mathbb{Z}$, show that the element $a \in \mathbb{Z}/n\mathbb{Z}$ is nilpotent if and only if every prime divisor of n divides a. In particular, determine the nilpotent elements of $\mathbb{Z}/72\mathbb{Z}$.

We quickly prove a lemma, which follows from **Euclid's Lemma**.

Lemma 1. *If p is prime, $a \in \mathbb{Z}$, and $n \in \mathbb{Z}^+$ such that $p \mid a^n$, then $p \mid a$.*

Proof. Trivially, $p \mid a \implies p \mid a$. Next, $p \mid a^2 = a(a) \implies p \mid a$ or $p \mid a \implies p \mid a$ by **Euclid's Lemma**. Now suppose that $p \mid a^k \implies p \mid a$ for some $k \geq 2$. Then, by **Euclid's Lemma**, $p \mid a^{k+1} = a(a^k) \implies (i)p \mid a$ or $(ii)p \mid a^k$ and so (i) $p \mid a$ or by our inductive step $(ii)p \mid a^k \implies p \mid a$. So $p \mid a^{k+1} \implies p \mid a$. Therefore, by induction, $p \mid a^n \implies p \mid a$ for all $n \geq 1$, and the statement is proven. $\square$

Proof. **(a):** Since $ab = n \implies (ab)^1 = ab = n = 0 \in \mathbb{Z}_n \implies ab \in \mathrm{nil}(\mathbb{Z}_n)$.

(b): ($\implies$) If $a \in \mathbb{Z}$ is nilpotent in $\mathbb{Z}_n$, then $a^m = 0$ for some $m \in \mathbb{Z}^+$. So then $a^m = 0 \in \mathbb{Z}_n \implies a^m = qn \in \mathbb{Z}$ for some $q \in \mathbb{Z}$ and $n \mid a^m$. Well, for any prime divisor p of n, we must then have that $p \mid n$ and $n \mid a^m \implies p \mid a^m$. Therefore by **Lemma 1** $p \mid a$.

($\impliedby$) Let $n = \prod_{i=1}^k p_i^{b_i}$ be the prime decomposition of n where $p_1, \ldots, p_k$ are all distinct prime divisors of n, and $b_1, \ldots, b_k \in \mathbb{Z}^+$. If each prime divisor p_i divides a, then $\exists q_i \in \mathbb{Z}$ such that $a = p_i q_i$ and $a^{b_i} = p_i^{b_i} q_i^{b_i}$ for all $1 \leq i \leq k$. Therefore, since $\mathbb{Z}$ is commutative,

$$a^{\sum_{i=1}^k b_i} = \prod_{i=1}^k a^{b_i} = \prod_{i=1}^k p_i^{b_i} q_i^{b_i} = \prod_{i=1}^k q_i (\prod_{i=1}^k p_i^{b_i}) = (\prod_{i=1}^k q_i)n \implies a^{\sum_{i=1}^k b_i} = 0 \in \mathbb{Z}_n \implies a \in \mathrm{nil}(\mathbb{Z}_n).$$

Thus,

$$a \in \mathbb{Z} \text{ is nilpotent in } \mathbb{Z}_n \text{ for } n \in \mathbb{N} \iff \text{ every prime divisor of } n \text{ divides } a.$$

$\square$

$72 = 9(8) = 2^3 3^2$ and so the nilpotent elements of $\mathbb{Z}_{72}$ are all $a \in \mathbb{Z}_{72}$ which are divisible by both 2 and 3. That is, all multiples of 6 in $\mathbb{Z}_{72}$. So $\mathrm{nil}(\mathbb{Z}_{72}) = \langle 6 \rangle = \{0, 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66\}$.

Problem 7. Let R and S be rings.

 (a) Prove that the direct product $R \times S = \{(r,s) \mid r \in R,\ s \in S\}$ forms a ring under componentwise addition and multiplication.

 (b) Prove that $R \times S$ is commutative if and only if both R and S are commutative.

Proof. **(a):** For all $a = (r_1, s_1), b = (r_2, s_2), c = (r_3, s_3) \in R \times S$, we verify the ring axioms.

$[+_1]$ (associativity)$:$
$$(a+b)+c = (r_1 + r_2,\ s_1 + s_2) + (r_3, s_3)$$
$$= ((r_1 + r_2) + r_3,\ (s_1 + s_2) + s_3) = (r_1 + (r_2 + r_3),\ s_1 + (s_2 + s_3))$$
$$= (r_1, s_1) + (r_2 + r_3,\ s_2 + s_3) = a + (b+c).$$

$[+_2]$ (commutativity)$:$ $\quad a + b = (r_1 + r_2,\ s_1 + s_2) = (r_2 + r_1,\ s_2 + s_1) = b + a.$

$[0]$ (zero)$:$ $\quad a + (0_R, 0_S) = (r_1 + 0_R, s_1 + 0_S) = (0_R + r_1, 0_S + s_1) = (0_R, 0_S) + a = a \implies 0_{R \times S} = (0_R, 0_S).$

$[+_3]$ (additive inverse)$:$ $\quad$ Let $-a = (-r_1, -s_1)$. Then $a + (-a) = (r_1 - r_1,\ s_1 - s_1) = (0_R, 0_S) = 0_{R \times S}.$

$[\cdot_1]$ (associativity)$:$ $\quad (ab)c = (r_1 r_2,\ s_1 s_2)(r_3, s_3) = ((r_1 r_2) r_3,\ (s_1 s_2) s_3)$
$$= (r_1 (r_2 r_3),\ s_1 (s_2 s_3)) = (r_1, s_1)(r_2 r_3,\ s_2 s_3) = a(bc).$$

$[D_1]$ (left distributivity)$:$ $\quad a(b+c) = (r_1, s_1)(r_2 + r_3,\ s_2 + s_3) = (r_1(r_2 + r_3),\ s_1(s_2 + s_3))$
$$= (r_1 r_2 + r_1 r_3,\ s_1 s_2 + s_1 s_3) = (r_1 r_2,\ s_1 s_2) + (r_1 r_3,\ s_1 s_3) = ab + ac.$$

$[D_2]$ (right distributivity)$:$ $\quad (a+b)c = (r_1 + r_2,\ s_1 + s_2)(r_3, s_3) = ((r_1 + r_2) r_3,\ (s_1 + s_2) s_3)$
$$= (r_1 r_3 + r_2 r_3,\ s_1 s_3 + s_2 s_3) = (r_1 r_3,\ s_1 s_3) + (r_2 r_3,\ s_2 s_3) = ac + bc.$$

$[1]$ (unity)$:$ $\quad (1_R, 1_S)a = (1_R \cdot r_1, 1_S \cdot s_1) = (r_1 \cdot 1_R, s_1 \cdot 1_S) = (r_1, s_1) = a \implies 1_{R \times S} = (1_R, 1_S).$

Thus,

$$R \times S \text{ is a ring with unity.}$$

$\hfill\square$

Proof. **(b):** ($\implies$) If $R \times S$ is commutative, then for all $r_1, r_2 \in R$ and all $s_1, s_2 \in S$, $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) = (r_2, s_2)(r_1, s_1) = (r_2 r_1, s_2 s_1)$. So then for all $r_1, r_2 \in R$, $s_1, s_2 \in S$, we have that $r_1 r_2 = r_2 r_1$ and $s_1 s_2 = s_2 s_1$, since such pairs are only equal if their components are equal. Therefore, R and S are both commutative.

($\impliedby$) If R and S are both commutative, then for all $r_1, r_2 \in R$ and all $s_1, s_2 \in S$, $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2) = (r_2 r_1, s_2 s_1) = (r_2, s_2)(r_1, s_1)$. So $R \times S$ is commutative.

$\hfill\square$

Problem 8. Let R be a commutative ring. Define the ring $R[[x]]$ of formal power series by

$$R[[x]] = \left\{ \sum_{n=0}^{\infty} a_n x^n \;\middle|\; a_i \in R \right\}.$$

(a) Prove that $R[[x]]$ is a commutative ring, and be sure to explain how to add and multiply elements.

(b) Show that $1-x$ is a unit with inverse $1+x+x^2+\cdots = \sum_{n=0}^{\infty} x^n$.

(c) (Optional Challenge) Prove that $\sum_{n=0}^{\infty} a_n x^n$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R.

Proof. **(a):** For all $A(x) = \sum_{i=0}^{\infty} a_i x^i, B(x) = \sum_{j=0}^{\infty} b_j x^j \in R[[x]]$, addition is just adding coefficients of the same index (like in $R[x]$) and multiplication is termwise multiplication (Like in $R[x]$) which is called the *Cauchy Product* for series. These are defined as follows:

$$A(x)B(x) = (\sum_{i=0}^{\infty} a_i x^i)(\sum_{j=0}^{\infty} b_j x^j) = \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j)x^n$$

$$A(x) + B(x) = (\sum_{i=0}^{\infty} a_i x^i) + (\sum_{j=0}^{\infty} b_j x^j) = \sum_{n=0}^{\infty} (a_n + b_n)x^n$$

It is given that $R[[x]]$ is a ring, so we just show multiplication is commutative. Recall that R and $\mathbb{Z}$ are commutative. So:

$$A(x)B(x) = \sum_{n=0}^{\infty} (\sum_{i+j=n} a_i b_j)x^n = \sum_{n=0}^{\infty} (\sum_{j+i=n} b_j a_i)x^n = B(x)A(x)$$

<div align="right">□</div>

Proof. **(b):**

$$(1-x) \sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} x^n - x\sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} x^n(1-x) = \sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} x^{n+1} = \sum_{n=0}^{\infty} x^n - \sum_{n=1}^{\infty} x^n = 1$$

<div align="right">□</div>

Problem 9. Decide which of the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$:

(a) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$

(b) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$

(c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$

Proof. Let us refer to the mappings in $(a), (b), (c)$ via $\varphi_a, \varphi_b, \varphi_c$, respectively.

(a): $\varphi_a(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}) = 1 = \varphi_a(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix})\varphi_a(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}) \neq 2 = \varphi_a(\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}) = \varphi_a(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix})$. So φ_a is not a ring homomorphism.

(b): $\varphi_b(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}) = 1 = \varphi_b(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix})\varphi_b(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}) \neq 2 = \varphi_b(\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}) = \varphi_b(\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix})$. So φ_b is not a ring homomorphism.

(c): $\varphi_c(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}) + \varphi_c(\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}) = 0 + 0 = 0 \neq 1 = \varphi_c(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) = \varphi_c(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix})$ So φ_c is not a ring homomorphism.

So none of them are ring homomorphisms.

$\square$

Problem 10. Let
$$R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \;\middle|\; a,b,d \in \mathbb{Z} \right\}.$$

Prove that the map
$$\varphi : R \to \mathbb{Z} \times \mathbb{Z}, \qquad \varphi\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \right) = (a,d)$$

is a surjective ring homomorphism and describe its kernel.

Proof. For all $\alpha = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} \\ a_{21}=0 & a_{22} \end{pmatrix}, \beta = (b_{ij}) = \begin{pmatrix} b_{11} & b_{12} \\ b_{21}=0 & b_{22} \end{pmatrix} \in R,$

$[1] : \varphi(I_2) = (1,1) = 1_{\mathbb{Z} \times \mathbb{Z}}$

$[+] : \varphi(\alpha) + \varphi(\beta) = (a_{11}, a_{22}) + (b_{11}, b_{22}) = (a_{11} + b_{11}, a_{22} + b_{22}) = \varphi((a_{ij} + b_{ij})) = \varphi(\alpha + \beta)$

$[\cdot] : \varphi(\alpha)\varphi(\beta) = (a_{11}, a_{22})(b_{11}, b_{22}) = (a_{11}b_{11}, a_{22}b_{22}) = \varphi(\begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} + a_{12}b_{22} \\ 0 & a_{22}b_{22} \end{pmatrix})) = \varphi(\alpha\beta)$

$[\text{Onto}] : \forall (m,n) \in \mathbb{Z} \times \mathbb{Z}, \; \varphi(\begin{pmatrix} m & 0 \\ 0 & n \end{pmatrix})) = (m,n)$

$\varphi(\alpha) = (0,0) \implies a_{11} = a_{22} = 0 \implies \alpha \in \{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \}$ and so $\ker \varphi \subseteq \{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \}$ and

obviously $\varphi(\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix})) = (0,0)$ for all $b \in \mathbb{Z}$ so $\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \} \subseteq \ker \varphi$

Thus,

$$\varphi \text{ is a surjective ring homomorphism with} \ker \varphi = \{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \mathbb{Z} \}$$

$\square$

Problem 11. Decide which of the following are ideals of $\mathbb{Z} \times \mathbb{Z}$:

(a) $\{(a,a) \mid a \in \mathbb{Z}\}$

(b) $\{(2a,2b) \mid a,b \in \mathbb{Z}\}$

(c) $\{(2a,0) \mid a \in \mathbb{Z}\}$

(d) $\{(a,-a) \mid a \in \mathbb{Z}\}$

Proof. Call the subsets of $\mathbb{Z} \times \mathbb{Z}$ specified in $(a),(b),(c),(d)$: A,B,C,D, respectively.

(a): $(1,2) \in \mathbb{Z} \times \mathbb{Z}$ and $(1,1) \in A$ but $(1,2)(1,1) = (1,1)(1,2) = (1,2) \notin A$, so this is not an ideal.

(b): For all $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ and all $(2a,2b),(2\alpha,2\beta) \in B$, $((2a,2b)-(2\alpha,2\beta)) = (2(a-\alpha),2(b-\beta)) \in B$ and $(m,n)(2a,2b) = (m2a,n2b) = (2(ma),2(nb)) = (2(am),2(bn)) = (2a,2b)(m,n) \in B = 2\mathbb{Z} \times 2\mathbb{Z}$. This is a two-sided ideal.

(c): For all $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ and all $(2a,0),(2\alpha,0) \in C$, $((2a,0)-(2\alpha,0)) = (2(a-\alpha),0) \in C$ and then $(m,n)(2a,0) = (m2a,0) = (2(ma),0) = (2(am),0) = (2a,0)(m,n) \in C = 2\mathbb{Z} \times \{0\}$. This is a two-sided ideal.

(d): $(1,-1) \in D$ but $(1,-1)(1,-1) = (1,1) \notin D$ so it's not closed under multiplication and therefore not an ideal.

$\square$

Problem 12. The characteristic of a ring R (denoted char$R$) is the smallest $n \in \mathbb{N}$ such that

$$\underbrace{1_R + \cdots + 1_R}_{n \text{ times}} = 0,$$

and if there is no such n we say the characteristic of R is 0.

Prove that an integral domain has characteristic 0 or a prime.

Proof. Let R be an integral domain and suppose Char $R = p > 0$ where p is not prime. If a ring has characteristic 1, then $1 = 0$ and the ring is $\{0\}$, which isn't an integral domain by definition. So, $1 < p = ab$ for some non-trivial divisors $1 < a,b < p$. But then $(\sum_{i=1}^{a} 1)(\sum_{j=1}^{b} 1) = \sum_{n=1}^{ab} 1 = \sum_{n=1}^{p} 1 = 0 \in R$ and $a = \sum_{i=1}^{a} 1, b = \sum_{j=1}^{b} 1$ are both non-zero zero-divisors in R since $a,b < $ Char $R = p \implies (\sum_{i=1}^{a} 1),(\sum_{j=1}^{b} 1) \neq 0 \in R$, a contradiction since R is an integral domain. Therefore, if Char R is non-zero, it is prime. Otherwise Char $R = 0$.

Thus,

An integral domain R has characteristic 0 or a prime $p > 0$.

$\square$