Math 111B HW2

Zih-Yu Hsieh

January 19, 2025

1

Question 1 *Let $\{R_i\}_{i\geq 0}$ be a collection of rings and let $R' = \bigoplus_{i\geq 0} R_i$ and $R = \prod_{i\geq 0} R_i$. Show that R' can not be a subring of R under coordinatewise addition and multiplication in R.*

Pf:

We'll prove by contradiction. Suppose R' is a subring of R, then there exists a unity element $e = (e_1, ..., e_n, ...) \in R'$, such that for all $a = (a_1, ..., a_n, ...) \in R'$, $ea = ae = a$.

Since $e \in R'$ (direct sum), then it has finitely many nonzero elements, thus there exists a maximum index k, such that $e_k \neq 0 \in R_k$. In other words, for all $n > k$, $e_n = 0 \in R_n$.

However, consider the following $a \in R'$, such that $a_i = 0$ for all index $i \leq k$ and $i > (k+1)$, and $a_{k+1} = 1 \in R_{k+1}$. (i.e. $a = (0, ..., 0, 1, 0, ...)$, where 1 is in the $(k+1)^{th}$ entry). Then, ae is defined as follow:

$$ae = (0, ..., 0, 1, 0, ...) \cdot (e_1, ..., e_k, 0, 0, ...) = (0e_1, ..., 0e_k, 1 \cdot 0, 0 \cdot 0, ...) = (0, ..., 0, 0, 0, ...) = 0 \in R'$$

Since $a_{k+1} = 1 \in R'$, then $a \neq 0$; but here $ae = 0 \neq a$, showing that e is not an identity.

Therefore, it is a contradiction, which R' cannot be a subring of R.

2

Question 2 *Let R be an integral domain. Prove or disprove that $R[[X]]$ is an integral domain.*

Pf:

Suppose $a = \sum_{n=0}^{\infty} a_n X^n \in R[[X]]$ is a nonzero element, then there exists a smallest index $k \in \mathbb{N}$, such that $a_k \neq 0$. Thus, $a = \sum_{n=k}^{\infty} a_n X^n$ (since $a_0, ..., a_{k-1} = 0$).

Now, suppose $b = \sum_{n=0}^{\infty} b_n X^n \in R[[X]]$ satisfies $c = ab = ba = 0$. Then, we can use induction to prove that every $n \in \mathbb{N}$ satisfies $b_n = 0$.

Base Case: For $n = 0$, consider the coefficient of degree k of ab:

$$0 = c_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i=0}^{k-1} a_i b_{k-i} + a_k b_0$$

Notice that for index $i \in \{0, ..., k-1\}$, $a_i = 0$, thus:

$$0 = \sum_{i=0}^{k-1} a_i b_{k-i} + a_k b_0 = \sum_{i=0}^{k-1} 0 \cdot b_{k-i} + a_k b_0 = a_k b_0$$

Since $a_k \neq 0$ by assumption, and R is an integral domain, thus for $a_k b_0 = 0$, $b_0 = 0$.

Inductive Process:
Now, suppose for given $n \in \mathbb{N}$, every integer $0 \leq i \leq n$ satisfies $b_i = 0$. Then, consider b_{n+1}:

$$0 = c_{k+(n+1)} = \sum_{i=0}^{k+(n+1)} a_i b_{k+(n+1)-i} = \sum_{i=0}^{k-1} a_i b_{k+(n+1)-i} + a_k b_{(n+1)} + \sum_{j=(k+1)}^{k+(n+1)} a_j b_{k+(n+1)-j}$$

Again, for index $i \in \{0, ..., k-1\}$, $a_i = 0$; then, for index $j \in \{k+1, ..., k+(n+1)\}$, since $(k+1) \leq j \leq k+(n+1)$, then $-k-(n+1) \leq -j \leq -(k+1)$, so $0 \leq k+(n+1)-j \leq n$, thus $b_{k+(n+1)-j} = 0$ by induction hypothesis. Thus, the above equation becomes:

$$\begin{aligned} 0 &= \sum_{i=0}^{k-1} a_i b_{k+(n+1)-i} + a_k b_{(n+1)} + \sum_{j=(k+1)}^{k+(n+1)} a_j b_{k+(n+1)-j} \\ &= \sum_{i=0}^{k-1} 0 \cdot b_{k+(n+1)-i} + a_k b_{(n+1)} + \sum_{j=(k+1)}^{k+(n+1)} a_j \cdot 0 \\ &= a_k b_{(n+1)} \end{aligned}$$

However,since $a_k \neq 0$ by assumption, then since R is an integral domain, for $a_k b_{(n+1)} = 0$, $b_{(n+1)} = 0$.

Thus, by Principle of Mahematical Induction, for all $n \in \mathbb{N}$, $b_n = 0$. Thus, $b = 0$.

So, for any nonzero $a \in R[[X]]$, there there doesn't exist any nonzero $b \in R[[X]]$ with $ab = ba = 0$. This shows $R[[X]]$ is also an integral domain.

3

Question 3 *Show that for any integer $m \geq 2$, the set $\mathbb{Z}_m[i]$ of Gaussian integers modulo m is a ring under the addition and multiplication of $\mathbb{Z}[i]$ modulo m.*

Pf:
Given $\mathbb{Z}_m[i] = \{a + bi \mid a, b \in \mathbb{Z}_m\}$, to show it's a ring, there are several criteria to check:

(1) It's closed under addition and multiplication: Given any $(a+bi), (c+di) \in \mathbb{Z}_m[i]$:

$$(a+bi) + (c+di) = (a+c \mod m) + (b+d \mod m)i$$

$$(a+bi)(c+di) = (ac-bd \mod m) + (ad+bc \mod m)i$$

Which, since $a, b, c, d \in \mathbb{Z}_m$, addition and multiplication $\mod m$ is closed, thus the coordinates after addition and multiplication of gaussian integers are still integers within $\mathbb{Z}_m$, which the operations are closed.

Furthermore, since addition and multiplication $\mod m$ is associative, the operations on $\mathbb{Z}_m[i]$ is also associative.

Also, the two operations are based on $\mathbb{Z}[i]$, which are both commutative.

(2) Existence of Zero and Unity Element: Since $m \geq 2$, then $0 = (0 + 0i)$ and $1 = (1 + 0i)$ are both elements of $\mathbb{Z}_m[i]$. Which, for all $(a + bi) \in \mathbb{Z}_m[i]$:

$$0 + (a + bi) = (a + 0) + (b + 0)i = (a + bi)$$

$$1 \cdot (a + bi) = (1 \cdot a - 0 \cdot b) + (1 \cdot b + 0 \cdot a)i = (a + bi)$$

Which, since the operations are commutative, then $0+(a+bi) = (a+bi)+0$, and $1\cdot(a+bi) = (a+bi)\cdot 1$, which 0 is the zero element, and 1 is the unity element.

(3) Existence of Additive Inverse: For all $(a + bi) \in \mathbb{Z}_m[i]$, take $(m - a \mod m) + (m - b \mod m)i$:

$$(a+bi)+((m-a \mod m)+(m-b \mod m)i) = (a+(m-a) \mod m)+(b+(m-b) \mod m)i$$

$$= (m \mod m) + (m \mod m)i = 0$$

Which, there exists additive inverse for all element in $\mathbb{Z}_m[i]$.

(4) Distributive Property: Given any $(a + bi), (c + di), (e + fi) \in \mathbb{Z}_m[i]$:

$$((a + bi) + (c + di))(e + fi) = ((a + c) + (b + d)i)(e + fi)$$

$$= ((a + c)e - (b + d)f \mod m) + ((a + c)f + (b + d)e \mod m)i$$

$$= ((ae - bf) + (ce - df) \mod m) + ((af + be) + (cf + de) \mod m)i$$

$$= ((ae - bf \mod m) + (af + be \mod m)i) + ((ce - df \mod m) + (cf + de \mod m)i)$$

$$= (a + bi)(e + fi) + (c + di)(e + fi)$$

Since both multiplication and addition can commute with the modulo operation, thus distributive property still holds under $\mathbb{Z}_m[i]$.

Since $\mathbb{Z}_m[i]$ is closed under associative and commutative addition, has additive identity, and each element has an inverse, thus it is an abelian group under addition.

Furthermore, it is closed under associative multiplication, and has a multiplcative identity, which it is a monoid under multiplication.

Along with the condition that addition and multiplication under modulo is distributive, $\mathbb{Z}_m[i]$ is a ring.

4

Question 4 *Show that $\mathbb{Z}_3[i]$ is a field but $\mathbb{Z}_2[i]$ is not a field.*

Pf:

$\mathbb{Z}_2[i]$ **is not a field:**

Consider the element $(1+i) \in \mathbb{Z}_2[i]$, which the following is true:

$$(1+i)(1+i) = (1-1) + (1+1)i = 0 + (2 \mod 2)i = 0 + 0i = 0$$

Thus, $(1+i)$ is a nonzero element of $\mathbb{Z}_2[i]$, yet $(1+i)^2 = 0$, which it is a zero divisor, showing that $\mathbb{Z}_2[i]$ is not a field.

$\mathbb{Z}_3[i]$ **is a field:**

Before proving every nonzero element has an inverse, we'll prove that given $a, b \in \mathbb{Z}_3$ (where at least one is nonzero), then (a^2+b^2) has an inverse in $\mathbb{Z}_3$.

Since $\mathbb{Z}_3$ is a field, it suffices to show that given $a, b \in \mathbb{Z}_3$ (where at least one is nonzero), $(a^2+b^2) \neq 0 \mod 3$.

Suppose there exists $a, b \in \mathbb{Z}_3$ where $a \neq 0$, such that $a^2 + b^2 = 0 \mod 3$. Since $a \neq 0$, then $a = 1$ or $a = 2$; thus, $a^2 = 1$ (if $a = 1$), or $a^2 = (4 \mod 3) = 1$ (if $a = 2$). Which, in case for $a^2 + b^2 = 0 \mod 3$, $b^2 = -a^2 \mod 3 = -1 \mod 3 = 2$.

Yet, if $b = 1$ or $b = 2$, $b^2 = 1 \mod 3$; else if $b = 0$, $b^2 = 0 \mod 3$, which none of the element in $\mathbb{Z}_3$ satisfies $b^2 = 2 \mod 3$. So, this is a contradiction. Thus, given $a, b \in \mathbb{Z}_3$ with at least one being nonzero, $a^2 + b^2 \neq 0 \mod 3$, which there exists an inverse.

Now, For any nonzero $(a+bi) \in \mathbb{Z}_3[i]$ (which there exists a nonzero element in a, b), consider the element $x = (a^2+b^2)^{-1}(a-bi)$:

(Note: Here (a^2+b^2) represents the inverse of (a^2+b^2) in $\mathbb{Z}_3$)

Since $(a^2+b^2)^{-2} \in \mathbb{Z}_3$, then $x = ((a^2+b^2)^{-1}a \mod 3) + ((a^2+b^2)^{-1}(-b) \mod 3)i \in \mathbb{Z}_3[i]$ (since $a, -b$ are both integers, thus after multiplying $(a^2+b^2)^{-1}$ which is an integer given in $\mathbb{Z}_3$, the coefficients are still integers, hence modulo arithmetic is well-defined).

Then, consider $(a+bi)x$:

$$(a+bi)x = (a+bi)((a^2+b^2)^{-1}(a-bi)) = (a^2+b^2)^{-1}((a+bi)(a-bi))$$

$$= (a^2+b^2)^{-1}(a^2+b^2) = 1$$

Thus, x is an inverse of $(a+bi)$, showing that every nonzero element in $\mathbb{Z}_3[i]$ has an inverse in the same ring. Which, $\mathbb{Z}_3[i]$ is a division ring; furthermore, since it is commutative, it is a field.

5

Question 5 *Let R be the ring of differentiable functions $f : (0,1) \to \mathbb{R}$ under pointwise addition and multiplication. Prove or disprove that R is an integral domain.*

Pf:
R is not a ring in this case. Consider the following functions $f, g : (0,1) \to \mathbb{R}$:

$$f(x) = \begin{cases} (x-\frac{1}{2})^2 & 0 < x < \frac{1}{2} \\ 0 & \frac{1}{2} \le x < 1 \end{cases}, \qquad g(x) = \begin{cases} 0 & 0 < x < \frac{1}{2} \\ (x-\frac{1}{2})^2 & \frac{1}{2} \le x < 1 \end{cases}$$

Notice that the functions are zero divisors:

$$f(x)g(x) = g(x)f(x) = \begin{cases} (x-\frac{1}{2})^2 \cdot 0 & 0 < x < \frac{1}{2} \\ 0 \cdot (x-\frac{1}{2})^2 & \frac{1}{2} \le x < 1 \end{cases} = 0$$

Also, for all $x_0 \in (0,1)$ with $x_0 \neq \frac{1}{2}$, the functions $f(x), g(x)$ are differentiable, since they're well-defined polynomial or constant function at x_0. So, to show that $f, g \in R$, it suffices to show that f, g are differentiable at $\frac{1}{2}$.

Differentiability of f:
It is true that $f(\frac{1}{2}) = 0$. For all $x < \frac{1}{2}$, $f(x) = (x-\frac{1}{2})^2$, and for all $x > \frac{1}{2}$, $f(x) = 0$. Which, the derivative at $\frac{1}{2}$ is as follow:

$$\lim_{x \to \frac{1}{2}^-} \frac{f(x) - f(\frac{1}{2})}{x - \frac{1}{2}} = \lim_{x \to \frac{1}{2}^-} \frac{(x-\frac{1}{2})^2 - 0}{x - \frac{1}{2}} = \lim_{x \to \frac{1}{2}^-} (x - \frac{1}{2}) = 0, \qquad \lim_{x \to \frac{1}{2}^+} \frac{f(x) - f(\frac{1}{2})}{x - \frac{1}{2}} = \lim_{x \to \frac{1}{2}^+} \frac{0 - 0}{x - \frac{1}{2}} = 0$$

Since the left limit and right limit exist while agree, $\lim_{x \to \frac{1}{2}} \frac{f(x) - f(\frac{1}{2})}{x - \frac{1}{2}} = 0$, thus $f'(\frac{1}{2}) = 0$. So, f is differentiable on $(0,1)$, hence $f \in R$.

Differentiability of g:
It is true that $g(\frac{1}{2}) = (\frac{1}{2} - \frac{1}{2})^2$. For all $x < \frac{1}{2}$, $g(x) = 0$, and for all $x > \frac{1}{2}$, $g(x) = (x-\frac{1}{2})^2$. Which, the derivative at $\frac{1}{2}$ is as follow:

$$\lim_{x \to \frac{1}{2}^-} \frac{g(x) - g(\frac{1}{2})}{x - \frac{1}{2}} = \lim_{x \to \frac{1}{2}^-} \frac{0 - 0}{x - \frac{1}{2}} = 0, \qquad \lim_{x \to \frac{1}{2}^+} \frac{g(x) - g(\frac{1}{2})}{x - \frac{1}{2}} = \lim_{x \to \frac{1}{2}^+} \frac{(x-\frac{1}{2})^2 - 0}{x - \frac{1}{2}} = \lim_{x \to \frac{1}{2}^+} (x - \frac{1}{2}) = 0$$

Since the left limit and right limit exist while agree, $\lim_{x \to \frac{1}{2}} \frac{g(x) - g(\frac{1}{2})}{x - \frac{1}{2}} = 0$, thus $g'(\frac{1}{2}) = 0$. So, g is also differentiable on $(0,1)$, hence $g \in R$.

Since both $f, g \in R$ are nonzero elements, while $fg = gf = 0$, then R (ring of differentiable functions from $(0,1)$ to $\mathbb{R}$) is not an integral domain.

6

Question 6 *Let R_1 and R_2 be two integral domains. Prove or disprove that $R_1 \times R_2$ is an integral domain under coordinatewise addition and multiplication.*

Pf:

$R_1 \times R_2$ is not an integral domain. Consider $(1,0),(0,1) \in R_1 \times R_2$:

Both elements are nonzero, since the zero element is $(0,0) \in R_1 \times R_2$, and we can assume that R_1, R_2 are not zero-rings (which zero and unity element are different).

However, under coordinate wise multiplication, $(1,0)\cdot(0,1) = (1\cdot 0, 0\cdot 1) = (0,0) = (0\cdot 1, 1\cdot 0) = (0,1)\cdot(1,0)$. Which, both $(1,0)$ and $(0,1)$ are zero divisors, while being nonzero elements.

Thus, $R_1 \times R_2$ is not an integral domain.

7

Question 7 *Does there exist a division ring which is countable as a set? Justify your answer.*

Pf:

(1) Case for Commutative Division Ring (Field):

Consider the field $\mathbb{Q}$, since it is a field, it is also a division ring. Which, $\mathbb{Q}$ is a countable set.

(2) Case for Non-Commutative Division Ring:

Consider $\mathbb{H}_{\mathbb{Q}} = \{(a+bi+cj+dk) \in \mathbb{H} \mid a,b,c,d \in \mathbb{Q}\}$. Notice that since $\mathbb{H}$ is isomorphic to $\mathbb{R}^4$ as a set, here $\mathbb{H}_{\mathbb{Q}}$ is also isomorphic to $\mathbb{Q}^4$ as a set, which is countable.

Since rational is closed under both addition and multiplication, $\mathbb{H}_{\mathbb{Q}}$ is a ring (since the zero element 0 and unity element 1 are both in there, while the coefficients of two elements' sum or products, are the operations on multiple rationals, which are still in rational). So, to say it's a division ring, it suffices to show that every nonzero element has an inverse in $\mathbb{H}_{\mathbb{Q}}$.

Now, for all nonzero element $(a+bi+cj+dk) \in \mathbb{H}_{\mathbb{Q}} \subset \mathbb{H}$, the inverse is given as follow:

$$(a+bi+cj+dk)^{-1} = \frac{1}{a^2+b^2+c^2+d^2}(a-bi-cj-dk)$$

Since $a,b,c,d \in \mathbb{Q}$, then $\frac{1}{a^2+b^2+c^2+d^2} \in \mathbb{Q}$; so, since $(a-bi-cj-dk) \in \mathbb{H}_{\mathbb{Q}}$, the rational scalar multiplication of $(a-bi-cj-dk)$ is still in $\mathbb{H}_{\mathbb{Q}}$. Thus, $(a+bi+cj+dk)^{-1} \in \mathbb{H}_{\mathbb{Q}}$.

8

Question 8 *Let R be a commutative ring. Show that R is an integral domain if and only if for any $a, b, c \in R$ with $a \neq 0$, one has that $ab = ac \implies b = c$.*

Pf:

$\implies$: Suppose R is an integral domain, then for all $a, b, c \in R$ with $a \neq 0$, if $ab = ac$, then $ab - ac = 0$, thus $a(b - c) = 0$. However, since R is an integral domain, and $a \neq 0$, in case for $a(b - c) = 0$, $(b - c) = 0$. Thus, $b = c$.

So, $ab = ac \implies b = c$ if R is an integral domain.

$\impliedby$: Suppose for all $a, b, c \in R$ with $a \neq 0$, $ab = ac \implies b = c$.

Then, given any $a \in R$ with $a \neq 0$, for all $b \in R$ with $ab = 0$, since $0 = a \cdot 0$, $ab = a \cdot 0$, which according to the assumption, this implies $b = 0$. Thus, there doesn't exist nonzero element such that $ab = ba = 0$, which a is not a zero divisor.

Since every nonzero element $a \in R$ is not a zero divisor, R is an integral domain.

With the above two implications, it is true that R is an integral domain if and only if for any $a, b, c \in R$ with $a \neq 0$, $ab = bc \implies b = c$.