Math 111B HW1

Zih-Yu Hsieh

January 13, 2025

1

Question 1 *Prove or disprove that the ring $\mathbb{Z}$ has no proper subring.*

Pf:
We'll prove that $\mathbb{Z}$ has no proper subring: Suppose $R \subseteq \mathbb{Z}$ is a subring.

Since R is a ring, there exists unity element $b \in R \subseteq \mathbb{Z}$, such that for all $a \in R$, $ab = ba = a$. In particular, $b^2 = bb = b$ also. So, it satisfies the following:

$$b^2 = b, \quad b^2 - b = 0, \quad b(b-1) = 0$$

However, since unity element is different from zero element, so $b \neq 0$. Thus, for $b(b-1) = 0$ to be true under $\mathbb{Z}$ (where two nonzero elements have product being nonzero), $(b-1) = 0$, or $b = 1$.

But, since $1 \in R$, then by the property of group, $\langle 1 \rangle = \{k \cdot 1 \mid k \in \mathbb{Z}\} = \mathbb{Z}$ is a subgroup of R under addition. Thus, $\mathbb{Z} \subseteq R$, which $R = \mathbb{Z}$.
So, any subring of $\mathbb{Z}$ is itself, showing that it has no proper subring.

2

Question 2 *Let D be a rational number that is not a square of any rational number and consider $\mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\}$ as a subset of $\mathbb{C}$. Show that $\mathbb{Q}(\sqrt{D})$ is a ring under the addition and multiplication in $\mathbb{C}$. Prove or disprove that every non-zero element of $\mathbb{Q}(\sqrt{D})$ has an inverse in $\mathbb{Q}(\sqrt{D})$. Prove or disprove that every element of $\mathbb{Q}(\sqrt{D})$ has a unique expression of the form $a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$. Is $\mathbb{Q}(\sqrt{D})$ a subring of $\mathbb{R}$?*

Pf:
$\mathbb{Q}(\sqrt{D})$ is a ring in $\mathbb{C}$:
There are several criteria to test before saying it's a ring in $\mathbb{C}$:

(1) For all $w, z \in \mathbb{Q}(\sqrt{D})$, there exists $a, b, c, d \in \mathbb{Q}$, such that $w = a + b\sqrt{D}$ and $z = c + d\sqrt{D}$.

Which, the following equations are true:

$$w + z = (a + b\sqrt{D}) + (c + d\sqrt{D}) = (a + c) + (b\sqrt{D} + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$$

$$wz = (a + b\sqrt{D})(c + d\sqrt{D}) = a(c + d\sqrt{D}) + b\sqrt{D}(c + d\sqrt{D}) = ac + ad\sqrt{D} + bc\sqrt{D} + bd(\sqrt{D})^2$$

$$wz = ac + ad\sqrt{D} + bc\sqrt{D} + bd(\sqrt{D})^2 = (ac + bdD) + (ad + bc)\sqrt{D}$$

Notice that since $a, b, c, d, D \in \mathbb{Q}$, which is closed under addition and multiplication, then $(a + c), (b + d), (ac + bdD), (ad + bc) \in \mathbb{Q}$. Which:

$$w + z = \ (a + c) + (b + d)\sqrt{D} \ \in \mathbb{Q}(\sqrt{D})$$

$$wz = \ (ac + bdD) + (ad + bc)\sqrt{D} \ \in \mathbb{Q}(\sqrt{D})$$

So, $\mathbb{Q}(\sqrt{D})$ is closed under both addition and multiplication (and the two operations are associative since they were inherited from $\mathbb{C}$).

(2) Consider $0, 1 \in \mathbb{C}$: Since $0 = 0 + 0\sqrt{D}$ and $1 = 1 + 0\sqrt{D}$, while $0, 1 \in \mathbb{Q}$, thus $0, 1 \in \mathbb{Q}(\sqrt{D})$.

Since both the zero and unity elements (0 and 1 respectively) of $\mathbb{C}$ is contained in $\mathbb{Q}(\sqrt{D})$, then they also satisfy the condition as the zero and unity element of $\mathbb{Q}(\sqrt{D})$ (since $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{C}$). Thus, 0 is the additive identity, and 1 is the multiplicative identity (since identities are unique).

(3) For all $(a + b\sqrt{D}) \in \mathbb{Q}(\sqrt{D})$, consider $(-a - b\sqrt{D})$: Since $a, b \in \mathbb{Q}$, then $(-a), (-b) \in \mathbb{Q}$. Thus, $(-a) + (-b)\sqrt{D} = (-a - b\sqrt{D}) \in \mathbb{Q}(\sqrt{D})$.

Also, the following is true:

$$(a + b\sqrt{D}) + (-a - b\sqrt{D}) = (a + (-a)) + (b\sqrt{D} + (-b)\sqrt{D}) = 0 + (b + (-b))\sqrt{D} = 0 + 0\sqrt{D} = 0$$

$$(-a - b\sqrt{D}) + (a + b\sqrt{D}) = (a + b\sqrt{D}) + (-a - b\sqrt{D}) = 0$$

Thus, $(-a - b\sqrt{D})$ is the additive inverse of $(a + b\sqrt{D})$. Every element in $\mathbb{Q}(\sqrt{D})$ has an additive inverse.

Given the above conditions, consider $(\mathbb{Q}(\sqrt{D}), +)$: (1) proves that it is closed under addition that's associative, (2) proves the existence of additive identity in the set, and (3) proves the existence of additive inverse for all element in the set. Thus, $(\mathbb{Q}(\sqrt{D}), +)$ is a group; furthermore, since $+$ is a commutative operation on $\mathbb{C}$, then the group is in fact abelian.

Then, consider $(\mathbb{Q}(\sqrt{D}), \cdot)$: (1) proves that it is closed under multiplication which is associative, and (2) proves the existence of multiplicative identity in the set, which $(\mathbb{Q}(\sqrt{D}), \cdot)$ is a monoid.

Also, the distributive property follows from the distributive property of $\mathbb{C}$, thus $(\mathbb{Q}(\sqrt{D}), +, \cdot)$ is a ring.

Existence of Inverse:

For all nonzero $(a + b\sqrt{D}) \in \mathbb{Q}(\sqrt{D})$, since D is a rational number that is not a square of any rational number, then $\sqrt{D} \notin \mathbb{Q}$.

These conditions imply that $a \neq b\sqrt{D}$: Suppose $a = b\sqrt{D}$, then $b\sqrt{D}$ is rational. However, if $b \neq 0$, $b\sqrt{D} \neq 0$ is not rational (since $b\sqrt{D} = a$, $\sqrt{D} = \frac{a}{b} \in \mathbb{Q}$, which contradicts), so b=0. Yet, this implies that $a = b\sqrt{D} = 0\sqrt{D} = 0$, which $(a + b\sqrt{D}) = (0 + 0\sqrt{D}) = 0$, and this contradicts the assumption that $(a + b\sqrt{D}) \neq 0$. So, $a \neq b\sqrt{D}$, which $(a - b\sqrt{D}) \neq 0$.

Now, consider the element $\frac{a-b\sqrt{D}}{(a+b\sqrt{D})(a-b\sqrt{D})}$, which is defined since $(a + b\sqrt{D})$ and $(a - b\sqrt{D})$ are both nonzero:

$$\frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a - b\sqrt{D}}{a^2 - (b\sqrt{D})^2} = \frac{a - b\sqrt{D}}{a^2 - b^2D} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D}\sqrt{D}$$

(Note: since $a \neq b\sqrt{D}$, $a^2 \neq b^2D$, so $a^2 - b^2D \neq 0$.)

Given that a, b, D are all rationals, which $\frac{a}{a^2-b^2D}$, $\frac{-b}{a^2-b^2D}$ are both rationals. Thus:

$$\frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a}{a^2 - b^2D} - \frac{b}{a^2 - b^2D}\sqrt{D} \in \mathbb{Q}(\sqrt{D})$$

Also, the following is true:

$$(a + b\sqrt{D}) \cdot \frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = 1 = \frac{(a - b\sqrt{D})}{(a + b\sqrt{D})(a - b\sqrt{D})} \cdot (a + b\sqrt{D})$$

Which, $\frac{a-b\sqrt{D}}{(a+b\sqrt{D})(a-b\sqrt{D})}$ is the Multiplicative Inverse of $(a + b\sqrt{D})$, and it exists in $\mathbb{Q}(\sqrt{D})$. Hence, every nonzero element of $\mathbb{Q}(\sqrt{D})$ has a multiplicative inverse in $\mathbb{Q}(\sqrt{D})$.

Unique Expression:

For all $w \in \mathbb{Q}(\sqrt{D})$, suppose $a, a_1, b, b_1 \in \mathbb{Q}$ satisfy $(a + b\sqrt{D}) = (a_1 + b_1\sqrt{D}) = w$. Then:

$$a + b\sqrt{D} = a_1 + b_1\sqrt{D}, \quad (a - a_1) = (b_1\sqrt{D} - b\sqrt{D}) = (b_1 - b)\sqrt{D}$$

This implies that $(b_1 - b) = 0$: Suppose $(b_1 - b) \neq 0$, then since $(a - a_1)$ is rational, the above equation implies $(a - a_1) = (b_1 - b)\sqrt{D} \in \mathbb{Q}$. Which, $\sqrt{D} = \frac{(a-a_1)}{(b_1-b)} \in \mathbb{Q}$. Yet, since D is not a square of any rational number, $\sqrt{D}$ must be not rational, and this is a contradiction. Thus, $(b_1 - b) = 0$, or $b_1 = b$.

Then, $(a - a_1) = (b_1 - b)\sqrt{D} = 0\sqrt{D} = 0$, which $a = a_1$.

So, there exists unique $a, b \in \mathbb{Q}$ with $w = a + b\sqrt{D}$, there exists a unique expression of all element of $\mathbb{Q}(\sqrt{D})$.

$\mathbb{Q}(\sqrt{D})$ is Not Necessarily a Subring of $\mathbb{R}$:

Consider $D = -1$: For all $q \in \mathbb{Q}$, since $q^2 \geq 0$, so $q^2 \neq -1 = D$. Thus, $\sqrt{D} = \sqrt{-1} = i$, which $\mathbb{Q}(\sqrt{D}) \not\subseteq \mathbb{R}$, since $i = \sqrt{D} = 0 + 1\sqrt{D} \in \mathbb{Q}(\sqrt{D})$, while $i \notin \mathbb{R}$.

In fact, if $D < 0$, then $\mathbb{Q}(\sqrt{D}) \not\subseteq \mathbb{R}$ (since $\sqrt{D} \notin \mathbb{R}$); but if $D \geq 0$, $\mathbb{Q}(\sqrt{D}) \subseteq \mathbb{R}$ (since $\sqrt{D} \in \mathbb{R}$).

3

Question 3 *Let R be a ring and R_1, R_2 two subrings of R. Is $R_1 \cap R_2$ also subring of R? Justify your answer.*

Pf:

If the zero-ring is not considered as a ring, then $R_1 \cap R_2$ need not to be a ring, even if both are subrings of R.

Consider $R = M_2(\mathbb{R})$, and let R_1, R_2 be defined as follow:

$$R_1 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \ : \ a \in \mathbb{R} \right\}, \quad R_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} \ : \ b \in \mathbb{R} \right\}$$

We'll prove that both are subrings of R:

(1) For all $a, b \in \mathbb{R}$, the following is true:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} (a+b) & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & (a+b) \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & ab \end{pmatrix}$$

Which, both R_1 and R_2 are closed under both addition and multiplication that are both associative. Also, addition is commutative since real matrices' addition is commutative.

(2) Consider $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in R_1$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \in R_2$: for all $a \in \mathbb{R}$, the following is true:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, the given matrices are the multiplicative identities of their sets.

Also, the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ are in both sets, which is the additive identity.

(3) For all $a \in \mathbb{R}$, the following is true:

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} -a & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & -a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & -a \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$$

Thus, every element in R_1 and R_2 all have additive inverse.

Thus, since both R_1, R_2 are closed under commutative and associative addition, has additive identity, and every element has additive inverse, so both are groups under addition; also, since they're closed under associative matrix multiplication and both have multiplicative identities, they're both monoids under multiplication.

Also, the distributive property of R_1, R_2 follows from the distributive property of $M_2(\mathbb{R})$. So, R_1, R_2 are both rings, which they're subrings of R.

Yet, consider $R_1 \cap R_2$: For all $a, b, c, d \in \mathbb{R}$, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R_1 \cap R_2$, then since R_1 are all matrices with only the $(1,1)$ entry could be nonzero, $b = c = d = 0$; furthermore, since R_2 are all matrices with only the $(2,2)$ entry could be nonzero, then $a = 0$. Thus:

$$R_1 \cap R_2 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \right\}$$

But, it is not considered as a ring, since it's the zero-ring.

4

Question 4 *Let R be ring such that $a^2 = a$ for every $a \in R$. Prove or disprove that R is a commutative ring.*

Pf:

For all $a \in R$, since $(-a)^2 = a^2$, then $-a = (-a)^2 = a^2 = a$. Thus, for all $a, b \in R$, $(a-b) = (a+(-b)) = (a+b)$. Now, consider $(a+b) = (a+b)^2 = (a+b)(a-b)$:

$$(a+b) = (a+b)(a-b) = a(a-b) + b(a-b) = a^2 - ab + ba - b^2$$

Which, $a^2 = a$ and $-b^2 = -b = b$. So:

$$(a+b) = a - ab + ba + b, \quad 0 = -ab + ba, \quad ab = ba$$

Since $ab = ba$ for all $a, b \in R$, R is commutative under multiplication.