Math 395

Homework 1
Due: 2/1/2024

Name: Avinash Iyer

Collaborators: ____________________

Problem 1

Let S be the subset of $\text{Mat}_2(\mathbf{R})$ be the set consisting of matrices of the form $\begin{bmatrix} a & a \\ b & b \end{bmatrix}$.

(a) To show that S is a ring, we will show that S is a subring of the ring $\text{Mat}_2(\mathbf{R})$, by showing that S is not empty, S is closed under subtraction, and S is closed under multiplication.

To show non-emptiness, we can see that the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is an element of S by its definition.

To show S is closed under subtraction, let $a, b, c, d \in \mathbf{R}$, and let $e = a - c$ and $f = b - d$. Then,

$$\begin{aligned} \begin{bmatrix} a & a \\ b & b \end{bmatrix} - \begin{bmatrix} c & c \\ d & d \end{bmatrix} &= \begin{bmatrix} a & a \\ b & b \end{bmatrix} + \begin{bmatrix} -c & -c \\ -d & -d \end{bmatrix} \\ &= \begin{bmatrix} a + (-c) & a + (-c) \\ b + (-d) & b + (-d) \end{bmatrix} \\ &= \begin{bmatrix} a - c & a - c \\ b - d & b - d \end{bmatrix} \\ &= \begin{bmatrix} e & e \\ f & f \end{bmatrix}, \end{aligned}$$

which is an element of S. Thus, S is closed under subtraction.

Next, we need to show that S is closed under multiplication. Letting $a, b, c, d \in \mathbf{R}$ as before, let $g = ac + ad$ and $h = bc + bd$. Then,

$$\begin{aligned} \begin{bmatrix} a & a \\ b & b \end{bmatrix} \cdot \begin{bmatrix} c & c \\ d & d \end{bmatrix} &= \begin{bmatrix} ac + ad & ac + ad \\ bc + bd & bc + bd \end{bmatrix} \\ &= \begin{bmatrix} g & g \\ h & h \end{bmatrix}, \end{aligned}$$

which is an element of S. Thus, S is closed under multiplication.

Since S is non-empty, closed under subtraction, and closed under multiplication, S is a subring of $\text{Mat}_2(\mathbf{R})$, and so is a ring.

(b) To show that $J = \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}$ is a right identity, we multiply an arbitrary matrix in S on the right by J.

$$\begin{aligned} AJ &= \begin{bmatrix} a & a \\ b & b \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a & a \\ b & b \end{bmatrix} \\ &= A. \end{aligned}$$

(c) Let $B = \begin{bmatrix} a & a \\ b & b \end{bmatrix}$. Then, since

$$\begin{aligned} JB &= \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & a \\ b & b \end{bmatrix} \\ &= \begin{bmatrix} a+b & a+b \\ 0 & 0 \end{bmatrix} \\ &\neq B, \end{aligned}$$

J is not a left identity for S.

Problem 3

Let $a \oplus b = a + b - 1$ and $a \odot b = ab - (a + b) + 2$ be defined as such on $\mathbf{Z}$. We will show that these operations under $\mathbf{Z}$ form an integral domain.

First, we will show that $\mathbf{Z}$ under $\oplus$ is an Abelian group. Since $\mathbf{Z}$ is closed under ordinary addition and subtraction, $\mathbf{Z}$ is closed under $\oplus$. We can exhibit the associative property as follows:

$$\begin{aligned} a \oplus (b \oplus c) &= a + (b \oplus c) - 1 \\ &= a + (b + c - 1) - 1 \\ &= (a + b - 1) + c - 1 \\ &= (a \oplus b) + c - 1 \\ &= (a \oplus b) \oplus c. \end{aligned}$$

Additionally, 1 is an additive identity for $\mathbf{Z}$ under $\oplus$, as $(a \oplus 1) = a + 1 - 1 = a$. Therefore, $2 - a$ is the additive inverse for $\mathbf{Z}$ under $\oplus$, exhibited as follows:

$$\begin{aligned} a \oplus (2 - a) &= a + (2 - a) - 1 \\ &= 1. \end{aligned}$$

Finally, since $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$, the $\oplus$ operator is commutative.

Next, we will show that $\mathbf{Z}$ under $\odot$ satisfies the necessary properties for a commutative ring with identity.

Since $\odot$ consists of regular addition, subtraction, and multiplication under $\mathbf{Z}$, $\odot$ is closed under $\mathbf{Z}$. We will show associativity as follows. Let $a, b, c \in \mathbf{Z}$; then,

$$\begin{aligned} a \odot (b \odot c) &= a(b \odot c) - (a + (b \odot c)) + 2 \\ &= a(bc - (b + c) + 2) - (a + (bc - (b + c) + 2)) + 2 \\ &= abc - ab - ac + 2a - a - bc + b + c - 2 + 2 \\ &= abc - ab - ac - bc + a + b + c, \end{aligned}$$

and

$$\begin{aligned} (a \odot b) \odot c &= (ab - (a + b) + 2) \odot c \\ &= (ab - (a + b) + 2)c - (ab - (a + b) + 2 + c) + 2 \\ &= abc - ac - bc + 2c - ab + a + b - 2 - c + 2 \\ &= abc - ab - ac - bc + a + b + c, \end{aligned}$$

so

$$(a \odot b) \odot c = a \odot (b \odot c).$$

We will show that $\odot$ is distributive over $\oplus$ as follows:

$$\begin{aligned}
a \odot (b \oplus c) &= a \odot (b + c - 1) \\
&= a(b + c - 1) - (a + (b + c - 1)) + 2 \\
&= ab + ac - a - a - b - c + 1 + 2 \\
&= (ab - (a + b) + 2) + (ac - (a + c) + 2) - 1 \\
&= (a \odot b) \oplus (a \odot c) \\
(a \oplus b) \odot c &= (a + b - 1) \odot c \\
&= (a + b - 1)c - (a + b - 1 + c) + 2 \\
&= ac + bc - c - a - b - c + 1 + 2 \\
&= (ac - (a + c) + 2) + (bc - (b + c) + 2) - 1 \\
&= (a \odot c) \oplus (b \odot c)
\end{aligned}$$

To show commutativity, we can see that $a \odot b = ab - (a + b) + 2 = ba - (b + a) + 2 = b \odot a$. Additionally, we can show that 2 is a multiplicative identity under $\odot$ as follows:

$$\begin{aligned}
a \odot 2 &= (a)(2) - (a + 2) + 2 \\
&= 2a - a - 2 + 2 \\
&= a,
\end{aligned}$$

meaning $\odot$ is closed, associative, distributive, commutative, and has identity.

In order to show that $(\mathbf{Z}, \oplus, \odot)$ is an integral domain, we must show that this commutative ring with identity has no zero divisors (i.e., there is no number not equal to 1 that yields 1 when multiplied under $\odot$). Suppose toward contradiction that $a, b \neq 1$ and $a \odot b = 1$. Then,

$$\begin{aligned}
1 &= a \odot b \\
1 &= ab - (a + b) + 2 \\
1 &= ab - a - b + 2 \\
0 &= ab - a - b + 1 \\
0 &= a(b - 1) - (b - 1) \\
0 &= (b - 1)(a - 1),
\end{aligned}$$

meaning $a = 1$ or $b = 1$, and we have a contradiction.

Therefore, $(\mathbf{Z}, \oplus, \odot)$ is a commutative ring with identity without zero divisors, meaning it is an integral domain.

Problem 4

Let R be a ring, and $Z(R) = \{a \mid ar = ra, \text{ for all } r \in R\}$. We will prove that $Z(R)$ is a subring of R.

To show $Z(R)$ is a subring of R, we will show that $Z(R)$ is non-empty, closed under subtraction, and closed under multiplication. To start, we can see that $0_R \in Z(R)$, as $(0_R)(r) = (r)(0_R) = 0_R$. Therefore, $Z(R)$ is nonempty.

Let $a, b \in Z(R)$. We will show that $a - b \in Z(R)$. Since $a \in Z(R)$, for any $r \in R$, it is the case that $ar = ra$. Subtracting br from both sides, we have $ar - br = ra - br$. However, since $br \in Z(R)$, it is the case that $br = rb$, meaning we have $ar - br = ra - rb$. Using the distributive property of multiplication, we have $(a - b)r = r(a - b)$, meaning $a - b \in Z(R)$, and $Z(R)$ is closed under subtraction.

Let $a, b \in Z(R)$. We will show that $ab \in Z(R)$. Since $b \in Z(R)$, for any $r \in R$, it is the case that $br = rb$. Multiplying a, where $a \in Z(R)$, on the left, we have $a(br) = a(rb)$. Using the associative property of multiplication, we have $(ab)r = (ar)b$. Finally, since $a \in Z(R)$, we have $ar = ra$, meaning $(ab)r = (ra)b$, and using the associative property once again, we have $(ab)r = r(ab)$. Thus, $ab \in Z(R)$, and $Z(R)$ is closed under multiplication.

Since $Z(R)$ is non-empty, closed under subtraction, and closed under multiplication, $Z(R)$ is a subring of R.

Problem 6

Let S and T be subrings of R.

(a) We will show that $S \cap T$ is a subring of R. We will show that $S \cap T$ is non-empty, closed under subtraction, and closed under multiplication. First, since the additive identity is an element of both S and T, the additive identity is in $S \cap T$, meaning $S \cap T$ is non-empty.

Let $a, b \in S \cap T$. Since S is a subring, S is closed under subtraction, meaning $a - b \in S$. Additionally, since T is a subring, $a - b \in T$. Therefore, since $a - b \in S$ and $a - b \in T$, it is the case that $a - b \in S \cap T$, meaning $S \cap T$ is closed under subtraction.

Let $a, b \in S \cap T$. Since S is a subring, S is closed under multiplication, meaning $ab \in S$. Additionally, since T is a subring, T is closed under multiplication, meaning $ab \in T$. Since $ab \in S$ and $ab \in T$, it is the case that $ab \in S \cap T$, meaning $S \cap T$ is closed under multiplication.

(b) Consider the subrings $S = 2\mathbf{Z}$ and $T = 5\mathbf{Z}$ of the ring $R = \mathbf{Z}$. The union, $S \cup T$, is not closed under addition, as for $a = 2 \in S \cup T$ and $b = 5 \in S \cup T$, $a + b = 2 + 5 = 7 \notin S \cup T$, meaning $S \cup T$ cannot be a subring of $\mathbf{Z}$.