Math 110A Homework 3

Jiaping Zeng

1/26/2021

1. A field of order 4: Let $F = \{0, e, a, b\}$ with operations given by the following tables:

$+$	0	e	a	b
0	0	e	a	b
e	e	0	b	a
a	a	b	0	e
b	b	a	e	0

$\cdot$	0	e	a	b
0	0	0	0	0
e	0	e	a	b
a	0	a	b	e
b	0	b	e	a

Assume that associativity and distributivity hold for these operations. Show that F is a field by checking the other axioms.

Answer:

(a) (Closure for addition) as seen in the addition table, every entry is an element of F, therefore F is closed under addition.

(b) (Associative addition) we assume associativity holds.

(c) (Commutative addition) the addition table is symmetric across the diagonal, therefore we have $a+b = b+a$ for any $a, b \in F$.

(d) (Additive identity of zero element) the first row and the first column of the addition table is the same as their respective headers; in addition, the values are symmetric. Therefore the zero element satisfies $a + 0 = a = 0 + a$ for any $a \in F$.

(e) Note that under every row header of the addition table, there is an entry with value 0. The same applies for every column header. Therefore $a + x = 0$ always has a solution in F.

(f) (Closure for multiplication) as seen in the multiplication table, every entry is an element of F, therefore F is closed under multiplication.

(g) (Associative multiplication) we assume associativity holds.

(h) (Distributive laws) we assume distributivity holds.

2. Which of the following sets of matrices are subrings of $M_2(\mathbb{R})$ (the ring of 2×2 matrices with real coefficients)? Which ones have an identity?

(b) All matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ with $a, b, c \in \mathbb{Z}$.

Answer: We have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ 0 & c - c' \end{pmatrix}$$

, so it is closed under substraction. We also have

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} ad & ab'+bc' \\ 0 & cc' \end{pmatrix}$$

, so it is also closed under multiplication. Therefore it is a subring by Theorem 3.6 with identity matrix I_2.

(c) All matrices of the form $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$ with $a \in \mathbb{R}$.

Answer: We have

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

, so it is closed under substraction. We also have

$$\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}\begin{pmatrix} a' & 0 \\ a' & 0 \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ aa' & 0 \end{pmatrix}$$

, so it is also closed under multiplication. Therefore it is a subring by Theorem 3.6 without an identity matrix since I_2 is not an element.

(d) All matrices of the form $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ with $a \in \mathbb{R}$.

Answer: We have

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

, so it is closed under substraction. We also have

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a' & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ 0 & 0 \end{pmatrix}$$

, so it is also closed under multiplication. Therefore it is a subring by Theorem 3.6 without an identity matrix since I_2 is not an element.

3. (a) Define a new multiplication in $\mathbb{Z}$ by $ab = 0$. Show that with ordinary addition and this new multiplication, $\mathbb{Z}$ is a commutative ring.

Answer: Since $\mathbb{Z}$ under ordinary addition and multiplication is a ring, we only need to check axioms 6-9 to see if it is a commutative ring under the new multiplication. Note that we have $ab = 0 \in \mathbb{Z}$ (axiom 6), $a(bc) = 0 = (ab)c$ (axiom 7), $a(b+c) = 0 = ab + ac$ and $(a+b)c = ac + bc$ (axiom 8) and $ab = 0 = ba$ (axiom 9) for any $a, b, c \in \mathbb{Z}$, so $\mathbb{Z}$ is a commutative ring under the new multiplication.

(b) Define a new multiplication in $\mathbb{Z}$ by $ab = 1$. With ordinary addition and this new multiplication, is $\mathbb{Z}$ a ring?

Answer: No because it fails axiom 8, e.g. $1(2+3) = 1 \neq 2 = 1 \cdot 2 + 1 \cdot 3$.

4. Let L be the set of positive real numbers. Define a new addition and multiplication on L by $a \oplus b = ab$ and $a \otimes b = a^{\log b}$.

(a) Is L a ring under these operations?

Answer:

i. (Closure for addition) since L is closed under the standard multiplication, L is closed under $\oplus$.

ii. (Associative addition) since L is associative under the standard multiplication, L is associative under $\oplus$.

iii. (Commutative addition) $a \oplus b = ab = ba = b \oplus a$, so L is commutative under $\oplus$.

iv. (Additive identity of zero element) since $1 \oplus a = 1 \cdot a = a$ for any $a \in L$, $0_L = 1$ is the additive identity.

v. We have $a \oplus \frac{1}{a} = 1 = 0_L$ for any $a \in L$, so we can always take $x = \frac{1}{a}$ to be a solution of $a + x = 0_L$.

vi. (Closure for multiplication) since $a > 0$, any power of a is also positive. Therefore $a \otimes b \in L$ and L is closed under $\otimes$.

vii. (Associative multiplication) by log properties, we have $a \otimes (b \otimes c) = a^{(\log b^{\log c})} = (a^{\log b})^{\log c} = (a \otimes b) \otimes c$, so L is associative under $\otimes$.

viii. (Distributive laws) we have $a \otimes (b \oplus c) = a^{\log bc} = a^{\log b} \cdot a^{\log c} = a \otimes b \oplus a \otimes c$; similarly, we also have $(a \oplus b) \otimes c = (ab)^{\log c} = a^{\log b} \cdot b^{\log c}$, so distributivity holds.

(b) Is L a commutative ring?

Answer: Take $a, b \in L$, we have $a \otimes b = a^{\log b} = e^{\log a^{\log b}} = e^{\log b \cdot \log a} = e^{\log b^{\log a}} = b^{\log a}$. Therefore L is a commutative ring.

(c) Is L a field?

Answer: Note that we have $1_L = e$ since $a \otimes e = a^{\log e} = a = e^{\log a} = e \otimes a$, therefore $1_L = e \neq 1 = 0_L$. Now we want to show that $a \otimes x = 1_L \implies a^{\log x} = e$ has a solution for $a \neq 0_L = 1$. We can take $x = e^{(\log a)^{-1}}$ for $a \in L$, then $a \otimes x = e = 1_L$. Therefore L is a field by definition.

5. Let R be a ring, and let $Z(R) = \{a \in R | ar = ra \text{ for every } r \in R\}$. In other words, $Z(R)$ consists of all elements of R that commute with every other element of R. Prove that $Z(R)$ is a subring of R. $Z(R)$ is called the **center** of R.

Answer: Suppose we have $a, b \in Z(R)$ such that $ar = ra$ and $br = rb$ for any $r \in R$, then we also have $ar + br = ra + rb \implies (a+b)r = r(a+b)$. Therefore $(a+b) \in Z(R)$ and $Z(R)$ is closed under addition. Similarly, $ar \cdot br = abr^2 = br \cdot ar$, so $ab \in Z(R)$ and $Z(R)$ is closed under multiplication. We have $0 \in Z(R)$ since $0 \cdot r = r \cdot 0$ for any r, and $a + x = 0$ always has a solution in $Z(R)$ as $ar = ra \implies (-a)r = r(-a) \implies (-a) \in R(Z)$. Therefore $Z(R)$ is a subring of R by Theorem 3.2.

6. **The quaternions:** In the ring $M_2(\mathbb{C})$, let

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The product of a real number r and a matrix is given by $r \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ra & rb \\ rc & rd \end{pmatrix}$.

The set H of **real quaternions** consists of all matrices of the form:

$$a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + c \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

where a, b, c, d are real numbers.

(b) Prove that H is a ring.

Answer: Take arbitrary $a, b, c, d, a', b', c', d' \in \mathbb{R}$, then $a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ is an element of H. Similarly, so is $a'\mathbf{1} + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. Then the difference between the two is $(a-a')\mathbf{1} + (b-b')\mathbf{i} + (c-c')\mathbf{j} + (d-d')\mathbf{k}$ which satisfies the form so it is also in H, therefore H is closed under subtraction.
For multiplication, we have

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}\begin{pmatrix} a'+b'i & c'+d'i \\ -c'+d'i & a'-b'i \end{pmatrix}$$

$$= \begin{pmatrix} (aa'-bb'-cc'-dd')+(ab'+ba'+cd'-dc')i & (ac'-bd'+ca'+db')+(ad'+bc'-cb'+da')i \\ -(ac'-bd'+ca'+db')+(ad'+bc'-cb'+da')i & (aa'-bb'-cc'-dd')-(ab'+ba'+cd'-dc')i \end{pmatrix}$$

Note that the product also follows the form, so H is also closed under multiplication.
Therefore H is a ring by Theorem 3.6.

(c) Show that H is a division ring.

Answer: Note that the identity $I_2 \in H$, so H has an identity where $1_H \neq 0_H$. In addition, take the an arbitrary matrix in H, its determinant is $(a+bi)(a-bi) - (c+di)(-c+di) = a^2+b^2+c^2+d^2$, which is always positive unless $a = b = c = d = 0$. Therefore every matrix in H is invertible and is therefore a unit. Suppose we have an arbitrary matrix $M = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in H$, take $x = ta - tb\mathbf{i} - tc\mathbf{j} - td\mathbf{k} \in H$ where $t = 1/(a^2+b^2+c^2+d^2)$. Then $Mx = ta^2\mathbf{1} - tab\mathbf{i} - tac\mathbf{j} - tad\mathbf{k} + tab\mathbf{i} - tb^2\mathbf{i}^2 - tbc\mathbf{ij} - tbd\mathbf{ik} + tac\mathbf{j} - tbc\mathbf{ij} - tc^2\mathbf{j}^2 - tcd\mathbf{jk} + tad\mathbf{k} - tbd\mathbf{ik} - tcd\mathbf{jk} - td^2\mathbf{k}^2$. By part (a), we have $Mx = ta^2\mathbf{1} - tab\mathbf{i} - tac\mathbf{j} - tad\mathbf{k} + tab\mathbf{i} + tb^2\mathbf{1} - tbc\mathbf{k} + tbd\mathbf{j} + tac\mathbf{j} + tbc\mathbf{k} + tc^2\mathbf{1} - tcd\mathbf{i} + tad\mathbf{k} - tbd\mathbf{j} + tcd\mathbf{i} + td^2\mathbf{1} = ta^2\mathbf{1} + tb^2\mathbf{1} + tc^2\mathbf{1} + td^2\mathbf{1} = t(a^2+b^2+c^2+d^2)\mathbf{1} = \mathbf{1} = 1_H$. Therefore $ax = 1_H$ always has a solution and H is a division ring.

(d) Show that the polynomial equation $x^2 + 1 = 0$ has *infinitely many* solutions in H.

Answer: Take $M = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ with $b^2+c^2+d^2 = 1$, then by part (a), $M^2 = b^2\mathbf{i}^2 + bc\mathbf{ij} + bd\mathbf{ik} + bc\mathbf{ji} + c^2\mathbf{j}^2 + cd\mathbf{jk} + bd\mathbf{ki} + cd\mathbf{kj} + d^2\mathbf{k}^2 = -b^2\mathbf{1} + bc\mathbf{k} - bd\mathbf{j} - bc\mathbf{k} - c^2\mathbf{1} + cd\mathbf{i} + bd\mathbf{j} - cd\mathbf{i} - d^2\mathbf{1} = -b^2\mathbf{1} - c^2\mathbf{1} - d^2\mathbf{1} = -(b^2+c^2+d^2)\mathbf{1} = -\mathbf{1}$. Therefore $M^2 = -\mathbf{1} \implies M^2 + \mathbf{1} = 0$ for any $M = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ satisfying $b^2+c^2+d^2 = 1$.

7. Let S and T be subrings of a ring R. In (a) and (b), if the answer is "yes", prove it. If the answer is "no", give a counter-example.

(a) Is $S \cap T$ a subring of R?

Answer: Yes; take $a, b \in S \cap T$, since $a, b \in S$, $a - b \in S$ and $ab \in S$; since $a, b \in T$, $a - b \in T$ and $ab \in T$. Therefore $a - b \in S \cap T$ and $ab \in S \cap T$, so $S \cap T$ is a subring of R by Theorem 3.6.

(b) Is $S \cup T$ a subring of R?

Answer: No; take S to be the ring of even integers and $T = \mathbb{Z}/5\mathbb{Z}$, note that $3 \in S \cup T$ but does not have an inverse, so $S \cup T$ is not a ring.

8. If R is a *finite* ring (i.e. a ring with only finitely many elements), prove that R has characteristic n for some $n > 0$.

Answer: Since $\mathbb{Z}$ is infinite and R is finite, we must have some $a, b \in \mathbb{Z}$ such that $a \cdot 1_R = b \cdot 1_R$ where $a \neq b$, or else there would exist a unique element in R for every element in $\mathbb{Z}$. Upon renaming we have $a > b$, then

$a \cdot 1_R = b \cdot 1_R \implies a \cdot 1_R - b \cdot 1_R = 0 \implies (a-b)1_R = 0$ where $(a-b) > 0$. Now let $n = a - b$ and by definition of characteristic R has characteristic n for some $n > 0$.

9. Let R be a ring with identity of characteristic $n > 0$.

   (a) Prove that $na = 0_R$ for every $a \in R$.

   Answer: Since R has an identity, we have $a = 1_R \cdot a$. Then $na = n \cdot 1_R \cdot a = 0_R \cdot a = 0_R$ by definition of characteristic.

   (b) If R is an integral domain, prove that n is prime.

   Answer: By contradiction. Suppose R is an integral domain and $n > 0$ is not prime. Then we must have $n = 1$ or $n = pq$ for some positive $pq \in \mathbb{Z}$ where p, q are not 1 or n. If $n = 1$, we have $1 \cdot 1_R = 0_R$ which cannot be true by definition of integral domain. If $n = pq$, then we must have either $p \cdot 1_R = 0_R$ or $q \cdot 1_R = 0_R$. But since both p and q are positve integers smaller than n, n is not the smallest positive integer that satisfies $n \cdot 1_R = 0_R$ and therefore cannot be the characteristic. Therefore n must be prime by contradiction.