Chapter 3

Ethan Mahintorabi

March 9, 2018

(3.A)

(i)

The reason $\mathbb{N}$ fails to meet the definition of a ring is because $\mathbb{N}$ has no additive identity element 0 and thus there can be no additive inverse. However, $\mathbb{N}$ does satisfy the associative property of addition and multiplication. Addition is commutative under the set $\mathbb{N}$. We also know that multiplication distributes over addition over the set.

(ii)

If we take the definition of a polynomial of degree n as $p(x) = a_0 + a_1X^1 + a_2X^2 + \cdots + a_nX^n = \sum_{i=0}^{n} a_iX^i$ we can define multiplication and addition in terms of summation notation. To define the addition operation on the elements of the set $\mathbb{N}[X]$ we will first define two elements $a, b \in \mathbb{N}[X]$. The expression $a + b$ could be defined as

$$a + b = \sum_{i=0}^{n}(a_i + b_i)X^i. \tag{1}$$

The definition of polynomial multiplication is a bit more complicated as each term needs to be multiplied by every other term in the other. We also must consider that by multiplying two polynomials the degree of the highest term will be $n + m$ where n is the highest degree of a and m is the highest degree of b. We can define the polynomial multiplication as the following summation notation

$$ab = \sum_{i=0}^{n+m}\sum_{j=0}^{i}(a_{i-j}b_j)X^i. \tag{2}$$

This notation works in all cases including where the polynomials a and b are different degrees because we can add zero terms to one of the polynomials to match the degree of the other.

(2.B)

(i)

As shown in 2.B(i) we know that the the multiplication operator as defined is not associative which is required in the definition of a ring and thus cannot be a ring.

(iii)

We can show that the set of 2×2 matrices with entries in $\mathbb{R}$ and non zero-determinant is not a ring because the operation of addition over this set is not closed. We will show by counter example with the following degenerate case where

$$A = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, B = \begin{bmatrix} -1 & -2 \\ -2 & -1 \end{bmatrix}.$$

In this case we can see that both A and B are both matrices with non-zero determinants. However, under the operation of addition we find a degenerate case of the operation. When we perform $A + B$ we find that the result

$$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix},$$

is a matrix with zero determinant. Since the result has a zero determinant we must conclude that addition over this set is not an operation, and must also conclude that it cannot be a ring because of the lack of an addition operation.

(iv)

We can show that the set of 2×2 matrices with entries in $\mathbb{R}$ determinant equal to 1 is not a ring because the operation of addition over this set is not closed. We will show by counter example with the following degenerate case where

$$A = \begin{bmatrix} 2 & 1 \\ 3 & 2 \end{bmatrix}, B = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}.$$

In this case we can see that both A and B are both matrices with determinant equal to 1. However, under the operation of addition we find a degenerate case of the operation. When we perform $A + B$ we find that the result

$$\begin{bmatrix} 4 & 2 \\ 6 & 4 \end{bmatrix},$$

is a matrix with determinant equal to 2. Since the result has a determinant not equal to 1 we must conclude that addition over this set is not an operation, and must also conclude that it cannot be a ring because of the lack of an addition operation.

(v)

The set of upper triangular 2×2 matrices with entries in $\mathbb{R}$ is a ring. To prove that the set is a ring we will begin by showing that both addition and multiplication are associative. In the case of addition we will define three matrices A, B and C as

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, B = \begin{bmatrix} d & e \\ 0 & f \end{bmatrix}, \text{and } C = \begin{bmatrix} g & h \\ 0 & i \end{bmatrix}.$$

We will begin by showing

$$\begin{aligned} (A+B)+C &= \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \right) + \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} a+d & b+e \\ 0 & c+f \end{bmatrix} + \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} a+d+g & b+e+h \\ 0 & c+f+i \end{bmatrix} \end{aligned}$$

and then showing that

$$\begin{aligned} A+(B+C) &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \left(\begin{bmatrix} d & e \\ 0 & f \end{bmatrix} + \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \right) \\ &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d+g & e+h \\ 0 & f+i \end{bmatrix} \\ &= \begin{bmatrix} a+d+g & b+e+h \\ 0 & c+f+i \end{bmatrix} \end{aligned}$$

as we can now see both additions result in 2×2 upper triangular matrix with real entries such that $(A+B)+C = A+(B+C)$. Thus, we have shown that addition over this set is associative by the definition of associativity.

The next thing we must show is that multiplication is associative over the defined set. We will use the definitions of A, B and C above with

$$\begin{aligned} (A \cdot B) \cdot C &= \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \right) \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} ad & ae+bf \\ 0 & cf \end{bmatrix} \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} adg & adh+iae+ibf \\ 0 & cfi \end{bmatrix} \end{aligned}$$

and we will also show

$$\begin{aligned}
A \cdot (B \cdot C) &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot \left(\begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \right) \\
&= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} dg & dh + ei \\ 0 & fi \end{bmatrix} \\
&= \begin{bmatrix} adg & adh + iae + ibf \\ 0 & cfi \end{bmatrix}
\end{aligned}$$

as we can now see both additions result in 2×2 upper triangular matrix with real entries such that $(A \cdot B) \cdot C = A \cdot (B \cdot C)$. Thus, we have shown that multiplication over this set is associative by the definition of associativity.

We will now show that addition is commutative on the set as defined above. We will use the definitions of A and B to show that

$$\begin{aligned}
A + B &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \\
&= \begin{bmatrix} a + d & b + e \\ 0 & c + f \end{bmatrix}
\end{aligned}$$

and that

$$\begin{aligned}
B + A &= \begin{bmatrix} e & e \\ 0 & f \end{bmatrix} + \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \\
&= \begin{bmatrix} e + a & e + b \\ 0 & f + c \end{bmatrix}
\end{aligned}$$

Since we know that addition is commutative over the real numbers we know that $A + B = B + A$ and thus, general addition over upper triangular 2×2 matrices is commutative.

We must now show that multiplication distributes over addition with the same definitions of A, B and C. We will show that $(A + B) \cdot C = AC + BC$ and that $C \cdot (A + B) = CA + CB$ we will begin with

$$\begin{aligned}
C \cdot (A + B) &= \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \cdot \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \right) \\
&= \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \cdot \begin{bmatrix} a + d & b + e \\ 0 & c + f \end{bmatrix} \\
&= \begin{bmatrix} ga + gd & gb + ge + hc + hf \\ 0 & ic + if \end{bmatrix}
\end{aligned}$$

and now

$$\begin{aligned} CA+CB &= \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \cdot \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \cdot \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \\ &= \begin{bmatrix} ga & gb+hc \\ 0 & ic \end{bmatrix} + \begin{bmatrix} gd & ge+hf \\ 0 & if \end{bmatrix} \\ &= \begin{bmatrix} ga+gd & gb+ge+hc+hf \\ 0 & ic+if \end{bmatrix} \end{aligned}$$

Since the expressions $C \cdot (A+B) = CA+CB$ we have shown that this set has left distributivity. We will now prove that it has right distributivity by showing

$$\begin{aligned} (A+B)\cdot C &= \left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \right) \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} a+d & b+e \\ 0 & c+f \end{bmatrix} \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} ag+dg & ah+dh+bi+ei \\ 0 & ci+fi \end{bmatrix} \end{aligned}$$

and now

$$\begin{aligned} AC+BC &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} + \begin{bmatrix} d & e \\ 0 & f \end{bmatrix} \cdot \begin{bmatrix} g & h \\ 0 & i \end{bmatrix} \\ &= \begin{bmatrix} ag & ah+bi \\ 0 & ic \end{bmatrix} + \begin{bmatrix} gd & dh+ei \\ 0 & fi \end{bmatrix} \\ &= \begin{bmatrix} ag+dg & ah+dh+bi+ei \\ 0 & ci+fi \end{bmatrix}. \end{aligned}$$

As we can see $(A+B)\cdot C = AC+BC$ and thus the set of upper triangular 2×2 matrices have left distributivity. We have shown both sides of the distributive property thus, the set has distributivity.

There exists an additive identity called 0 for the set upper triangular 2×2 matrices with real entries defined as

$$\mathbf{0} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

we will now prove that $A+0=A$ for any A in the set there is not need however to prove the other side of the addition because we know addition is commutative over this set. We find that

$$\begin{aligned} A+0 &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \end{aligned}$$

and thus we have shown that there exists an additive identity for the set. We will finally show that there exists A' in the set such that $A + A' = 0$. If A is defined as

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

then we will define A' as

$$A' = \begin{bmatrix} -a & -b \\ 0 & -c \end{bmatrix}.$$

we will now show that this A' is the inverse for all element in the set by showing that

$$\begin{aligned} A + 0 &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} -a & -b \\ 0 & -c \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \end{aligned}$$

for all elements in the set. Since we also know addition is commutative we do not need to show the converse case. We have now shown that the set of 2 × 2 upper triangular matrices with real entries is a ring as it satisfies all the necessary properties. It is not a division ring because not all matrices have an inverse. It is not a commutative ring because the matrices in this set do not commute over multiplication. It is however a ring with identity defined as

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

We can prove this is true by showing that $A \cdot 1 = A$ and $1 \cdot A = A$. We will now show that

$$\begin{aligned} A \cdot \mathbf{1} &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \end{aligned}$$

and

$$\begin{aligned} \mathbf{1} \cdot A &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \end{aligned}$$

thus we have shown that there exists an identity element for multiplication.

(3.C)

(i)

There should be n equivalence classes as the definition suggests that one of the other ways that modular arithmetic could be defined is as the remainder of an integer divided by n. Thus, there would only be n possible remainders specifically $0 \cdots (n-1)$.

(iii)

(a)

To show that addition is well defined we will assume that addition is well defined for $\mathbb{Z}/n\mathbb{Z}$ we must show that if $[x] = [x']$ and $[y] = [y']$ then $[x+y] = [x'+y']$. To show this we must first take the definition of equivalence as $x = x' + nk_1$ where $k_1 \in \mathbb{Z}$ and $y = y' + nk_2$ where $k_2 \in \mathbb{Z}$.

$$\begin{aligned} x + y &= x' + nk_1 + y' + nk_2 \\ &= x' + y' + n(k_1 + k_2) \\ (x + x') - (y + y') &= n(k_1 + k_2) \end{aligned}$$

Thus by the definition of the equivalence class we have shown that $[x+y] = [x'+y']$ and addition is well defined.

To show that multiplication is well defined we will once again take the definitions $x = x' + nk_1$ where $k_1 \in \mathbb{Z}$ and $y = y' + nk_2$ where $k_2 \in \mathbb{Z}$. And then show that

$$\begin{aligned} xy &= (x' + nk_1)(y' + nk_2) \\ &= x'y' + x'nm_2 + y\prime nm_1 + n^2 m_1 m_2 \\ &= x'y' + n(x'm_2 + y\prime m_1 + nm_1 m_2) \\ xy - x'y' &= n(x'm_2 + y\prime m_1 + nm_1 m_2) \end{aligned}$$

Thus by definition of the equivalence relation we know that $[xy] \equiv [x'y']$.

We will now show that both operations are associative. First we will show that addition is associative via

$$\begin{aligned} ([x] + [y]) + [z] &= [x] + ([y] + [z]) \\ ([x + y]) + [z] &= [x] + ([y + z]) \\ [x + y + z] &= [x + y + z] \end{aligned}$$

Thus we have shown that addition is associative. We will now show multiplication is associative.

$$\begin{aligned} ([x] \cdot [y]) \cdot [z] &= [x] \cdot ([y] \cdot [z]) \\ ([x \cdot y]) \cdot [z] &= [x] \cdot ([y \cdot z]) \\ [x \cdot y \cdot z] &= [x \cdot y \cdot z] \end{aligned}$$

Thus we have shown that multiplication is associative. We will now show that addition is commutative by showing

$$\begin{aligned}[x] + [y] &= [y] + [x] \\ [x + y] &= [y + x].\end{aligned}$$

Since addition is commutative over the integers we know that $[x+y] = [y+x]$ and that addition is commutative.

We will also show that multiplication distributes over addition by showing that

$$\begin{aligned}[z]([x] + [y]) &= [zx] + [zy] \\ [z][x] + [z][y] &= [zx] + [zy] \\ [zx] + [zy] &= [zx] + [zy].\end{aligned}$$

and

$$\begin{aligned}([x] + [y])[z] &= [xz] + [yz] \\ [x][z] + [y][z] &= [xz] + [yz] \\ [xz] + [yz] &= [xz] + [yz].\end{aligned}$$

Thus multiplication distributes over addition.

There exists an additive identity called [0] for all element in $\mathbb{Z}/n\mathbb{Z}$ because

$$\begin{aligned}[x] + [0] &= [x + 0] \\ [x] + [0] &= [x].\end{aligned}$$

Since addition is commutative we have shown there is an additive identity for $\mathbb{Z}/n\mathbb{Z}$. Lastly we must show that there is an additive inverse for all element in $\mathbb{Z}/n\mathbb{Z}$. We will show that for any element $\mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned}[x] + [-x] &= [x + -x] \\ [x] + [-x] &= [0].\end{aligned}$$

Since by definition $[-x]$ and $[x]$ is an element in $\mathbb{Z}/n\mathbb{Z}$ we have shown all elements have an additive inverse. Thus, $\mathbb{Z}/n\mathbb{Z}$ is a ring by definition.

(iv)

Because the way we defined add and multiplication may have not held with different choices of x. Thus we need to show under all choices of x in the equivalence class the operations hold.

(v)

Every element if n is not prime will not have a multiplicative inverse thus it cannot be a field.