CS201 Assignment 1: The Concept of Numbers

Pragati Agrawal (220779)

Maximum Marks: $20 \times 5 = 100$

Before we start discussion on numbers, let us examine the axioms of set theory and why they are required. Define U to be the collection of all sets.

- Show that U is not a set as per the Zermalo Fraenkel Axioms.

  Proof: Given that U is the non-empty collection of all sets.
  Let $U = \{U_1, U_2, \dots, U, \dots \infty\}$.
  Then, as per Zermelo-Fraenkel's Axiom of Separation, let $\mathcal{P}$ be a predicate defined on the set U as $\mathcal{P} = \{x \in U \mid x = U\}$. Then the axiom says that set formed on applying $\mathcal{P}$ on set $\{U\}$ will also a set, let it be called B.
  Hence $B = \{U\}$.
  Now, $B \cap U = \{U\} \cap U = \emptyset$.
  But, $B \cap U = \{U\} \cap \{U_1, U_2, U_3, \dots, U, \dots \infty\} = U$
  Since $U \neq \emptyset$, therefore, we arrive at a contradiction, and such a set U is not possible.

The motivation to define these axioms was a paradox discovered by Bertrand Russell: Suppose we allow U to be a set. Then $U \in U$ by definition. Define:

$$V = \{A \mid A \notin A\}.$$

- Derive a contradiction using the question "is $V \in V$?".
  Proof: Let $V \in V$. Then by definition of $V = \{A \mid A \notin A\}$, substituting $A = V$, it is implied that if $V \in V$ then $V \notin V$, which is a contradiction.
  Otherwise, let $V \notin V$. Then, by definition of V, V must belong to V. But we assumed that $V \notin V$. Hence our assumption is incorrect.
  Therefore, such a set $V = \{A \mid A \notin A\}$. cannot be defined.

  This is the reason that circularity in definition of sets was explicitly not permitted by the axioms.

Let us now move to numbers. In the class, we discussed the definition of natural numbers through Peano's Axioms. How does one define numbers in general? One possible way is to define numbers as any set that admits four arithmetic operations: addition, subtraction, multiplication, and division. But to define arithmetic operations, we need numbers! This is resolved by defining both together. Let us develop axioms for this. Consider addition and subtraction first.

Define set of *numbers with addition* $(N, +)$ as:0

1. $+ : N \times N \mapsto N$. We will write $+(a, b)$ as $a + b$.
2. $(a + b) + c = a + (b + c)$ for all $a, b, c \in N$.
3. There is an element $0 \in N$ such that $a + 0 = 0 + a = a$ for all $a \in N$.
4. For all $a \in N$, there is an element $b \in N$ such that $a + b = 0$.
5. $a + b = b + a$ for all $a, b \in N$.

With above definition, subtraction can be defined as: $a - b = a + c$ where c is such that $b + c = 0$. Does this capture the addition and subtraction properly? Show that:

- There is a unique number 0 satisfying third axiom.

  Proof: Let there be two distinct elements in the set $b, c \in (N, +)$ such that
  $a + b = b + a = a$ for all $a \in N$, and
  $a + c = c + a = a$ for all $a \in N$.
  Since the first equation is true for all $a \in N$, substituting $a = c$, we get
  $c + b = b + c = c$.
  Similarly substituting $a = b$ in the second equation, we get
  $b + c = c + b = b$.
  Since, $b + c = c + b$ by axiom 5, therefore, $b = c$ for all $a \in N$.
  Hence, there is a unique element 0 in the set $(N, +)$ satisfying the third axiom.

- For every $a \in N$, there is a unique b satisfying fourth axiom.
  Proof: To prove that b is unique, on the contrary, assume that b is not unique. So $\exists\, b, c \in (N, +)$ such that : $a+b = 0$ and $a+c = 0$, where $b \neq c$. We need to show that $b = c$ for all $a \in N$. Now, consider the expression $E = (a + b) + c$**.**
  Since $a + b = 0$, so $E = (a + b) + c = 0 + c = c$ (by axiom 3).
  Also, $E = (a + b) + c = c + (a + b)$ (by axiom 5). Now, by axiom 2, $c + (a + b) = (c + a) + b$. Again by axiom 5, $(c + a) + b = (a + c) + b$. So, eventually, $E = (a + c) + b = 0 + b = b$.
  Since $E = b$ and $E = c$ therefore, $b = c$ if $a + b = 0$ and $a + c = 0$.
  Hence for all $a \in N$, there is a unique element $b \in N$ such that $a + b = 0$.

- Define $-a$ to be the number such that $a + (-a) = 0$. For every $a, b \in N$, $a - b = -(b - a)$.
  Proof:
  Claim 1: a-a=0
  Using the definition of subtraction on N as $a - b = a + c$ such that b+c=0, for all $a, b \in N$. Substituting $b = a$, we get $a - a = a + c$, such that $a + c = 0$. Therefore, $a - a = 0$.

  Claim 2: 0-b=-b

We know that $a-b=a+c$ such that $b+c=0$. Substituting $a=0$ in this equation, we get $0-b=0+c$ such that $b+c=0$. Now, $0+c=c=0-b$. Also, $b+(-b)=0$. Hence, $b+c=0=b+(-b)$. Adding $(-b)$ on both sides, we get $b+c+(-b)=b+(-b)+(-b)$ which implies $b+(-b)+c=b+(-b)+(-b)$ i.e. $0+c=0+(-b)$. Hence, by addition axiom 3, $c=-b$.

But $c=0-b$ and $c=-b$, hence $0-b=-b$.

Claim 3: +(-a)=-a

We know that $a+(-a)=0$, and also that $a-a=0$. Adding $(-a)$ to both sides of equation 2, we get, $a-a+(-a)=0+(-a)=+(-a)$. Let $a-a=t$ in the LHS.

So LHS simplifies to $t+(-a)=(-a)+t=(-a)+a-a=0-a$. Using the above claim, since $0-a=-a$, therefore, LHS$=-a$. Hence, $+(-a)=-a$.

Claim 4: -a+a=0

we know that $a+(-a)=0$. Using axiom 5 of addition, we get, $-a+a=0$.

Now consider $(a-b)+(-(a-b))=0$ and $(b-a)+(-(b-a))=0$. Adding $(-(b-a))$ to both sides of the equation 1, we get,

$(a-b)+(-(a-b))+(-(b-a))=0+(-(b-a))$.

$\implies (a-b)+(-(b-a))+(-(a-b))=-(b-a)$

$\implies (a-b)-(b-a)-(a-b)=-(b-a)$.......... (i)

Simplifying the LHS using the subtraction axiom, we get,

$(a-b)-(b-a)=(a-b)+c$.........(ii),

such that $(b-a)+c=0=c+(b-a)$.This implies $c+b-a=0$.

Adding a to both sides of the equation, we get, $c+b-a+a=0+a$.

This implies $c+b+0=a$. Now, adding $(-b)$ to both sides, we get, $c+b+(-b)=a+(-b)$, $\implies c+0=c=a-b$.

Substituting $c=a-b$ in (ii), $(a-b)-(b-a)=(a-b)+c$, we get, $(a-b)-(b-a)=(a-b)+(a-b)$.

Substituting this back in expression (i), we get,

$(a-b)+(a-b)-(a-b)=-(b-a)$.

$\implies (a-b)+0=(a-b)=-(b-a)$.

Hence proved, $(a-b)=-(b-a)$.

Now let us add multiplication and division. Define set of *numbers with multiplication* $(N,*)$ as:

1. $*: N\times N \mapsto N$. We will write $*(a,b)$ as $a*b$.
2. $(a*b)*c=a*(b*c)$ for all $a,b,c\in N$.
3. There is an element $1\in N$ such that $a*1=1*a=a$ for all $a\in N$.
4. For all $a\in N$, there is an element $b\in N$ such that $a*b=1$.
5. $a*b=b*a$ for all $a,b\in N$.

These axioms are identical to first ones except for the name of operation and replacement of 0 by 1. Division operation is defined analogously to subtraction.

It is easy to see that the definition of '$-$' and '$/$' is entirely determined by the definition of $+$ and $*$ respectively.

Finally define set of *numbers with addition and multiplication* $(N, +, *)$ as:

1. $(N, +)$ is a set of numbers with addition.
2. $(N\backslash\{0\}, *)$ is a set of numbers with multiplication.
3. For all $a, b, c \in N$, $a * (b + c) = a * b + a * c$.

Why is the number '0' excluded from N in second axiom above? It is to avoid division by zero. Show that:

- If 0 is included in N for the second axiom, then $1 = 0$.
  Proof: *Claim:* $0 * a = 0$ *for* $a \in N$
  Using the third axiom, For all $a, b, c \in N$, $a * (b + c) = a * b + a * c$. Substituting $b = 0$, we get $a*(0+c) = a*0+a*c$. Since axioms of $(N, +)$ state that $0 + c = c$, therefore, we can write, $a * c = a * 0 + a * c$. Now, adding an equal quantity $(-(a * c))$ to both sides of the equality, we get, $a*c+(-(a*c)) = a*0+a*c+(-(a*c))$. Also, we know that $a+(-a) = 0$. Therefore, the expression simplifies to $0 = a * 0 + 0 = a * 0$ (by axiom 3 of $(N, +)$). Hence, $0 = a * 0$.

  The definition of division says $a/b = a * c$ where $b * c = 1$ $\forall(a, b) \in N$. If 0 is included in the above axioms, we can substitute $b = 0$ giving us $a/0 = a * c$ where $0 * c = 1$. Now, according to our above claim, $0 * c = 0$. Hence, if 0 is included in N for the second axiom, then $1 = 0$.

The addition and multiplication operations can be different for different sets of numbers:

- Give two examples of sets of numbers with different addition and multiplication operations.
  Proof: Consider the set of numbers $P = \{-1, 0, 1\}$ such that $(+)$ is defined as
  $\{-1 + 0 = -1,$
  $0 + 0 = 0,$
  $0 + 1 = 1,$
  $-1 + -1 = 1,$
  $1 + 1 = -1,$
  $-1 + 1 = 0,$
  $1 + (-1) = 0\}.$
  Similarly, $(*)$ is defined on $P\backslash\{0\}$as:
  $\{-1 * -1 = 1,$
  $1 * 1 = 1,$
  $-1 * 1 = -1,$
  $1 * -1 = -1\}$

To show that the set $(P, +, *)$ follows all the axioms stated above:
Axioms of Addition +:

1. $+ : P \times P \mapsto P$, we will write it as $+(a, b)$ as $a + b$
2. $(a + b) + c = a + (b + c)$ for all $a, b, c \in P$.
   Proof: Consider $a = -1, b = 0, c = 1$:
   Then, LHS $= (a + b) + c = (-1 + 0) + 1 = -1 + 1 = 0$.
   Then RHS $= a + (b + c) = -1 + (0 + 1) = -1 + 1 = 0$.
   Similarly, let $a = 1, b = 1, c = 0$:
   Then, LHS $= (a + b) + c = (1 + 1) + 0 = -1 + 0 = -1$.
   Then RHS $= a + (b + c) = 1 + (1 + 0) = 1 + 1 = -1$.
   Similarly, let $a = 0, b = 1, c = -1$:
   Then, LHS $= (a + b) + c = (0 + 1) + -1 = 1 + -1 = 0$.
   Then RHS $= a + (b + c) = 0 + (1 + -1) = 0 + 0 = 0$.
   We can verify all other possible cases similarly.
3. There is an element $0 \in P$ such that $a + 0 = 0 + a = a$ for all $a \in P$.
   Proof: The set $P = \{-1, 0, 1\}$. Consider:
   $a = -1$, then $-1 + 0 = 0 + -1 = -1$.
   $a = 0$, then $0 + 0 = 0$
   $a = 1$, then $1 + 0 = 0 + 1 = 1$.
4. For all $a \in P$, there is an element $b \in P$ such that $a + b = 0$. **Proof:**
   The set $P = \{-1, 0, 1\}$. Consider:
   $a = -1$, then $-1 + 1 = 0$.
   $a = 0$, then $0 + 0 = 0$
   $a = 1$, then $1 + (-1) = 0$.
5. $a + b = b + a$ for all $a, b \in P$.
   Proof: The set $P = \{-1, 0, 1\}$. Consider:
   $a = -1, b = -1$, then $-1 + -1 = -1 + -1 = 1$.
   $a = 1, b = 1$, then $1 + 1 = 1 + 1 = -1$.
   $a = 0, b = 0$, then $0 + 0 = 0 + 0 = 0$.
   $a = -1, b = 0$, then $-1 + 0 = 0 + -1 = -1$.
   $a = -1, b = 1$, then $-1 + 1 = 1 + -1 = 0$
   $a = 1, b = 0$, then $1 + 0 = 0 + 1 = 1$.

*Axioms of Multiplication *:*

1. $* : P \times P \mapsto P$, we will write it as (a, b) as $a * b$
2. $(a * b) + c = a * (b * c)$ for all $a, b, c \in P \backslash \{0\}$.
   Proof: Consider $a = -1, b = 1, c = 1$:
   Then, LHS $= (a * b) * c = (-1 * 1) * 1 = -1 * 1 = -1$.
   Then RHS $= a * (b * c) = -1 * (1 * 1) = -1 * 1 = -1$.
   Similarly, let $a = 1, b = 1, c = -1$:
   Then, LHS $= (a * b) * c = (1 * 1) * -1 = 1 * -1 = -1$.
   Then RHS $= a * (b * c) = 1 * (1 * -1) = 1 * -1 = -1$.
   Similarly, let $a = -1, b = 1, c = -1$:

Then, LHS $= (a * b) * c = (-1 * 1) * -1 = -1 * -1 = 1$.
Then RHS $= a * (b * c) = -1 * (1 * -1) = -1 * -1 = 1$.
We can verify all other possible cases similarly.

3. There is an element $1 \in P$ such that $a*1 = 1*a = a$ for all $a \in P\backslash\{0\}$.
   Proof: The set $P\backslash\{0\} = \{-1, 1\}$. Consider:
   $a = -1$, then $-1 * 1 = 1 * -1 = -1$.
   $a = 1$, then $1 * 1 = 1 * 1 = 1$.
4. For all $a \in P\backslash\{0\}$, there is an element $b \in P\backslash\{0\}$ such that $a * b = 1$.
   Proof: The set $P = \{-1, 1\}$. Consider:
   $a = -1$, then $-1 * -1 = 1$.
   $a = 1$, then $1 * 1 = 1$.
5. $a * b = b * a$ for all $a, b \in P\backslash\{0\}$.
   Proof: The set $P = \{-1, 1\}$. Consider:
   $a = -1, b = -1$, then $-1 * -1 = -1 * -1 = 1$.
   $a = 1, b = 1$, then $1 * 1 = 1 * 1 = 1$.
   $a = -1, b = 1$, then $-1 * 1 = 1 * -1 = -1$

Consider another set of numbers $(M, \#, \$)$ defined by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $(a, b, c, d) \in N$ and their addition operation, denoted by $(\#)$ is as :
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\#) \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$, where $(+)$ is the addition operation defined on $(N, +)$.
Similarly, their multiplication operation, denoted by $(\$)$ is as:
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (\$) \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a*e & b*f \\ c*g & d*h \end{pmatrix}$, where $(*)$ is the multiplication operation defined on $(N, *)$.
To show that $(M, \#, \$)$ follow the axioms stated above,
Axioms of Addition $\#$:

1. $\# : M \times M \mapsto M$. We will write $\#(a, b)$ as $a\#b$.
2. $(a\#b)\#c = a\#(b\#c)$ for all $a, b, c \in M$.
   Proof: Consider three elements $a, b, c \in M$ as:
   $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, c = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$
   Then , $(a\#b)\#c = \begin{pmatrix} x+e & y+f \\ z+g & w+h \end{pmatrix} \# \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} x+e+i & y+f+j \\ z+g+k & w+h+l \end{pmatrix}$
   Also, $a\#(b\#c) = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \# \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix} = \begin{pmatrix} x+e+i & y+f+j \\ z+g+k & w+h+l \end{pmatrix}$
3. There is an element $0 \in M$ such that $a\#0 = 0\#a = a$ for all $a \in M$
   Proof: Consider $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$
   $a\#0 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \# \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} x+0 & y+0 \\ z+0 & w+0 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = a$
   $0\#a = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \# \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 0+x & 0+y \\ 0+z & 0+w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = a$

4. For all $a \in M$, there is an element $b \in M$ such that $a\#b = 0$.
   Proof: Consider $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} -x & -y \\ -z & -w \end{pmatrix}$
   $a\#b = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \# \begin{pmatrix} -x & -y \\ -z & -w \end{pmatrix} = \begin{pmatrix} x+(-x) & y+(-y) \\ z+(-z) & w+(-w) \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0$

5. $a\#b = b\#a$ for all $a, b \in M$.
   Proof: Consider $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$
   $a\#b = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \# \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} x+e & y+f \\ z+g & w+h \end{pmatrix}$
   $b\#a = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \# \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} e+x & f+y \\ g+z & h+w \end{pmatrix}$

Axioms of Multiplication \$:

1. $\$: M \times M \mapsto M$. We will write $\$(a, b)$ as $a\$b$.
2. $(a\$b)\$c = a\$(b\$c)$ for all $a, b, c \in M$
   Proof: Consider three elements $a, b, c \in M$ as:
   $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, c = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$
   Then , $(a\$b)\$c = \begin{pmatrix} x*e & y*f \\ z*g & w*h \end{pmatrix} \$ \begin{pmatrix} i & j \\ k & l \end{pmatrix} = \begin{pmatrix} x*e*i & y*f*j \\ z*g*k & w*h*l \end{pmatrix}$
   Also, $a\$(b\$c) = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} e*i & f*j \\ g*k & h*l \end{pmatrix} = \begin{pmatrix} x*e*i & y*f*j \\ z*g*k & w*h*l \end{pmatrix}$
3. There is an element $1 \in M$ such that $a\$1 = 1\$a = a$ for all $a \in M$
   Proof: Consider $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, 1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$
   $a\$1 = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} x*1 & y*1 \\ z*1 & w*1 \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = a$
   $1\$a = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \$ \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 1*x & 1*y \\ 1*z & 1*w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix} = a$
4. For all $a \in M$, there is an element $b \in M$ such that $a\$b = 1$.
   Proof: *Claim:* $x*(1/x) = 1$
   We know that $a/b = a*c$, such that $b*c = 1$. Substituting $a = 1$ in this, we get $1/b = 1*c = c$, such that $b*c = 1$. Since $c = 1/b$, therefore $b*(1/b) = 1$. Now consider $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} 1/x & 1/y \\ 1/z & 1/w \end{pmatrix}$
   $a\$b = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} 1/x & 1/y \\ 1/z & 1/w \end{pmatrix} = \begin{pmatrix} x*(1/x) & y*(1/y) \\ z*(1/z) & w*(1/w) \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = 1$
5. $a\$b = b\$a$ for all $a, b \in M$.
   Proof: Consider $a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$

$$a\$b = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} x*e & y*f \\ z*g & w*h \end{pmatrix}$$
$$b\$a = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \$ \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} e*x & f*y \\ g*z & h*w \end{pmatrix}$$

To prove: **For all** $a, b, c \in M$**,** $a\$(b\#c) = a\$b\#a\$c$**.**
Proof: Consider three elements $a, b, c \in M$ as:

$$a = \begin{pmatrix} x & y \\ z & w \end{pmatrix}, b = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, c = \begin{pmatrix} i & j \\ k & l \end{pmatrix}$$
$$a\$(b\#c) = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} e+i & f+j \\ g+k & h+l \end{pmatrix} = \begin{pmatrix} x*(e+i) & y*(f+j) \\ z*(g+k) & w*(h+l) \end{pmatrix} =$$
$$\begin{pmatrix} x*e+x*i & y*f+y*j \\ z*g+z*k & w*h+w*l \end{pmatrix}$$
$$a\$b\#a\$c = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} e & f \\ g & h \end{pmatrix} \# \begin{pmatrix} x & y \\ z & w \end{pmatrix} \$ \begin{pmatrix} i & j \\ k & l \end{pmatrix} =$$
$$\begin{pmatrix} x*e & y*f \\ z*g & w*h \end{pmatrix} \# \begin{pmatrix} x*i & y*j \\ z*k & w*l \end{pmatrix} =$$
$$\begin{pmatrix} x*e+x*i & y*f+y*j \\ z*g+z*k & w*h+w*l \end{pmatrix}$$

Hence proved.

Does a set of numbers defined as above contains natural numbers? Show that:

- There is a set of numbers $(N, +, *)$ such that N is finite.
  Proof: Consider the set of numbers $N = \{-1, 0, 1\}$ such that $(+)$ is defined as
  $\{-1 + 0 = -1,$
  $0 + 0 = 0,$
  $0 + 1 = 1,$
  $-1 + -1 = 1,$
  $1 + 1 = -1,$
  $-1 + 1 = 0\}.$
  The operation $*$ is defined on $N\backslash\{0\}$ as:
  $\{-1 * -1 = 1,$
  $1 * 1 = 1,$
  $-1 * 1 = -1,$
  $1 * -1 = -1\}.$

As proved in the previous question, this set $(N, +, *)$ follows all the axioms and is finite.

Does this mean that we have not been able to capture the notion of numbers properly? Later in the course, we will show that it is not so. A set of numbers *can* be finite, and such numbers are extremely useful!

In order to identify set of numbers that contain $\mathbb{N}$, define *multiplicity* of set $(N, +, *)$ to be the smallest k for which $\underbrace{1 + 1 + \cdots + 1}_{k \text{ times}} = 0$. When there is no such k, then we set multiplicity of $(N, +, *)$ to 0. Show that:

- Multiplicity of $(N, +, *)$ is either 0 or a prime number.
  Proof: Consider the expression $\mathcal{E} = 1 + 1 + 1 + ... + 1 = 0$ (k times). If we are unable to find any such k, we would say the multiplicity to be 0. So, if multiplicity is non-zero, we need to show that it must be prime.
  As we have shown in **question 6**, that if we allow division by 0, we arrive at the absurd result, that $1 = 0$. Since we are defining multiplicity on $(N, +, *)$, we cannot have $1 = 0$. Hence $k \neq 1$.
  Now, assume that $k > 1$ is not a prime number, so it has factors other than 1 and itself. Let $\exists a, b \in N$ such that $1 < a, b < k$ and $a * b = k$. Also, let the expression $\mathcal{F} = 1 + 1 + 1 + ... + 1$ (a times) be equal to some $c \in N$. The expression $\mathcal{E}$ can be simplified as:
  $\mathcal{E} = (1 + 1 + ... + 1)(atimes) + (1 + 1 + ... + 1)(atimes) + ... + (1 + 1 + ... + 1)(atimes)$, i.e. each bracket has 1 added *a times*, and there are b such brackets.
  So, $\mathcal{E} = c + c + c + ... + c(btimes)$.
  Also, using the distributive axiom, we can say that:
  $c * (1 + 1 + 1 + ... + 1)(btimes) = c * 1 + c * 1 + ... + c * 1(btimes)$
  So, $c * (1 + 1 + ... + 1) = c + c + c + ... + c(btimes)$
  Let $(1 + 1 + 1 + ... + 1)(btimes) = d \in N$
  So, $c * d = c + c + c.... + c(btimes)$
  So, $\mathcal{E} = c * d = 0$. Since we have defined $(*)$ on the set $N \backslash \{0\}$ hence, we cannot have a product equal to 0. Hence, multiplicity of N cannot be a composite number.
  Therefore, multiplicity is either 0 or prime number.

- Any set of numbers $(N, +, *)$ of multiplicity 0 contains $\mathbb{N}$.
  Proof: To show that $(N, +, *)$ contains $\mathbb{N}$, consider a subset P of N, defined as $P = \{0, 1, 1 + 1, 1 + 1 + 1, 1 + 1 + 1 + 1, ...\}$.
  Claim 1: P has all elements distinct.
  The multliplicity of the set P is also 0, since it is a subset of $(N, +, *)$. We need to prove that all the elements of P are distinct.
  Clearly, $0 \neq 1$.
  Consider any element of P, $(1 + 1 + 1 + ... + 1)$ (a times) . Let its value be equal to $x_a \in N$. Similarly, for (b times), let the value be $x_b \in N$, and so on.
  To show that the elements of P are distinct, we assume two elements of P that are not distinct:
  Let $(1 + 1 + 1 + ... + 1)$(a times)=$(1 + 1 + 1 + ... + 1)$(b times).
  $\implies x_a = x_b$.
  Without loss of generality, assume, $b > a$. So the expression simplifies to:

(1+1+1+....+1) (a times) =(1+1+1+...+1) (a times) + (1+1+1+....+1) (b-a times)
$\implies x_a = x_a + x_{b-a}$.
Now, adding $-x_a$ on both sides, we get,
$\implies x_a + (-x_a) = x_a + x_{b-a} + (-x_a) = x_a + (-x_a) + x_{b-a}$
$\implies 0 = x_{b-a}$.
$\implies 0 = (1 + 1 + 1 + ... + 1)$ (b-a times) But this is not possible, since the multiplicity of the set P is 0, hence any $k = b - a > 0$ cannot sum to 0. Hence proved, all the elements of the set P are distinct.

Claim: P follows **Peano's axioms:**

1. $0 \in P$

2. Let there be a map $S : P \times P \mapsto P$, the successor function $S(x) = x+1$.
Claim: $0 \notin$ range (S)
Proof: Clearly, $S(0) = 0 + 1 = 1 \in$ range (S).
Consider some arbitrary $x_a \neq 0 \in P$. Since multiplicity =0, therefore, $x_{a+1} \neq 0$.
$S(x_a) = x_a + 1 = (1 + 1 + 1 + ... + 1)(atimes) + 1 = (1 + 1 + 1 + ... + 1)(a + 1times) = x_{a+1}$.
Since $x_{a+1} \neq 0$, hence $S(x_a) \neq 0$.
Hence, $0 \notin$ range (S).

3. The map S is an injective map.
Proof: Let two numbers, $x_a, x_b \in P$, such that $a \neq b$ and $S(x_a) = S(x_b)$.
Then, $x_a + 1 = x_b + 1$
$\implies (1 + 1 + 1 + ... + 1)$(a times)+1=$(1 + 1 + 1 + ... + 1)$(b times)+1.
$(1 + 1 + 1 + ... + 1)$ (a+1 times) = $(1 + 1 + 1 + ... + 1)$ (b+1 times)
$\implies x_{a+1} = x_{b+1}$. Since, we had proved earlier, that all elements of P are distinct, therefore $x_{a+1} \neq x_{b+1}$. Hence, our assumption was incorrect, and S is an injective map.

4. For any set A, if $0 \in A$, and for all $x_a \in P \cap A$, $S(x_a) \in A$, then $P \subseteq A$.
Proof by induction:
Claim: For $x_a \in P \cap A \implies x_{a+1} \in A$.
Base case: Consider $0 \in P$. Also $0 \in A$. So $S(0) \in A$
Consider $1 \in P$. Then $S(0) = 0 + 1 = 1 \in A$.
Now consider some $x_a \in P$. Since, $x_a \in A$, hence $x_a \in P \cap A$. Then $S(x_a) \in A$.
So $S(x_a) = x_a + 1 = x_{a+1} \in A$.
Hence proved by induction that if $x_a \in P$ and $x_a \in A$, then $x_{a+1} \in A$. Hence, all $x_a \in A$. Therefore, $P \subseteq A$.

Thus shown that the subset $P \subseteq N$ follows the Peano's axioms. Hence, P

is a set of natural numbers $\mathbb{N}$ contained in $(N, +, *)$.

- For any set of numbers $(N, +, *)$ of multiplicity 0, for any $k \in \mathbb{N} \subseteq N$, for any $a \in N$, $k * a = \underbrace{a + a + \cdots + a}_{k \text{ times}}$.
  Proof: Consider $E = 1 + 1 + 1 + ... + 1$ (k times).
  Now, we can consider the set P proven above, to be the usual set of natural numbers $\mathbb{N} = \{0, 1, 2, 3, ...\}$, where $(1 + 1 + 1 + ... + 1(ktimes)) = k$.
  So the expression simplifies to $E = k$.
  Then applying the distributive axiom, we get:
  $(1 + 1 + 1 + ... + 1) * a = 1 * a + 1 * a + 1 * a + ... + 1 * a$ (k times)
  $\implies k * a = a + a + a + ... + a$ (k times).

As was done in the class with $\mathbb{N}$, is there way to identify a unique set of numbers using equivalence classes? The answer is no, as there can be finite as well as infinite set of numbers. Moreover, there are binary operations defined on numbers and any equivalence between two sets of numbers must equate the operations as well. Define an *isomorphism* h between two sets of numbers $(N_1, +_1, *_1)$ and $(N_2, +_2, *_2)$ as:

1. $h : N_1 \mapsto N_2$ is a bijection,
2. For all $a, b \in N_1$, $h(a +_1 b) = h(a) +_2 h(b)$,
3. For all $a, b \in N_1$, $h(a *_1 b) = h(a) *_2 h(b)$.

Show that:

- The relation defined by isomorphism between two sets of numbers is an equivalence relation on the set of all sets of numbers.
  Proof: To show that the relation is an equivalence relation, we need to show that h is reflexive, symmetric and transitive relation.:

  (i) *Claim:* h **is reflexive.**
  Consider the mapping $h : N_1 \to N_1$, defined as $h(x) = x$, for $x \in N_1$.
  1. *Claim:* h **is a bijection.**
  (i)h **is one-one.**
  Let there be $x_1, x_2 \in N_1$, $x_1 \neq x_2$, such that $h(x_1) = h(x_2) = a$. Since $h(x_1) = x_1$ and $h(x_2) = x_2$, and they are both equal to a, therefore, $x_1 = a$ and $x_2 = a$, which implies $x_1 = x_2$. Hence h is one-one map.
  (ii) h **is onto.**
  "A function $f : AßB$ is onto if, for every element bB, there exists an element aA such that $f(a) = b$".
  Hence, take any element $x \in N_1$. Now, since $h(x) = x$ by definition, therefore, there exists an $x \in N_1$, such that $h(x) = x$. Hence h is an onto map.

2. *Claim:* **For all** $a, b \in N_1$**,** $h(a +_1 b) = h(a) +_1 h(b)$
Proof: By definition, $h(a) = a, h(b) = b$, and , $h(a +_1 b) = a +_1 b$.
Therefore, LHS= $a +_1 b$. RHS= $a +_1 b$. Hence proved.
3. *Claim:* **For all** $a, b \in N_1$**,** $h(a *_1 b) = h(a) *_1 h(b)$**.**
Proof: By definition, $h(a *_1 b) = a *_1 b$, and, $h(a) = a, h(b) = b$.
Therefore, LHS= $a *_1 b$. RHS= $a *_1 b$. Hence proved.

(ii) *Claim:* h **is symmetric**.
We have the map $h : N_1 \to N_2$, such that
1. $h : N_1 \mapsto N_2$ is a bijection,
2. For all $a, b \in N_1$, $h(a +_1 b) = h(a) +_2 h(b)$,
3. For all $a, b \in N_1$, $h(a *_1 b) = h(a) *_2 h(b)$.
Now, consider the map $h^{-1} : N_2 \mapsto N_1$, defined as for $x \in N_2$,
1. Since inverse of a bijection is also a bijection, therefore, h^{-1} is a bijection.
2. For all $a', b' \in N_2$, $h^{-1}(a' +_2 b') = h^{-1}(a') +_1 h^{-1}(b)$,
Let $a = h^{-1}(a'), b = h^{-1}(b')$. Then, $a' = h(a)$, $b' = h(b)$.
This implies $h^{-1}(a' +_2 b') = h^{-1}(h(a) +_2 h(b)) = h^{-1}(h(a +_1 b)) = a +_1 b = h^{-1}(a') +_1 h^{-1}(b')$. 3. For all $a', b' \in N_2$, $h^{-1}(a' *_2 b') = h^{-1}(a') *_1 h^{-1}(b)$,
Let $a = h^{-1}(a'), b = h^{-1}(b')$. Then, $a' = h(a)$, $b' = h(b)$.
This implies $h^{-1}(a' *_2 b') = h^{-1}(h(a) *_2 h(b)) = h^{-1}(h(a *_1 b)) = a *_1 b = h^{-1}(a') *_1 h^{-1}(b')$.
Hence, h^{-1} is also an isomorphism. So, h is symmetric.

(iii) *Claim:* h **is transitive.**
We have the map $h : N_1 \to N_2$, such that
1. $h : N_1 \mapsto N_2$ is a bijection,
2. For all $a, b \in N_1$, $h(a +_1 b) = h(a) +_2 h(b)$,
3. For all $a, b \in N_1$, $h(a *_1 b) = h(a) *_2 h(b)$.
We have the map $g : N_2 \to N_3$, such that
1. $g : N_2 \mapsto N_3$ is a bijection,
2. For all $a, b \in N_2$, $h(a +_2 b) = h(a) +_3 h(b)$,
3. For all $a, b \in N_2$, $h(a *_2 b) = h(a) *_3 h(b)$.
Claim: The map $g \circ h : N_1 \to N_3$, such that
1. $g \circ h : N_1 \mapsto N_3$ is a bijection,
Since h and g are bijections, therefore, $g \circ h$ is also a bijection.
2. For all $a, b \in N_1$, $g \circ h(a +_1 b) = g \circ h(a) +_3 g \circ h(b)$,
Proof: $h(a +_1 b) = h(a) +_2 h(b)$. Now, $g \circ h(a +_1 b) = g(h(a) +_2 h(b)) = g \circ h(a) +_3 g \circ h(b)$.
3. For all $a, b \in N_1$, $g \circ h(a *_1 b) = g \circ h(a) *_3 g \circ h(b)$.
Proof: $h(a *_1 b) = h(a) *_2 h(b)$. Now, $g \circ h(a *_1 b) = g(h(a) *_2 h(b)) = g \circ h(a) *_3 g \circ h(b)$.
Hence, the relation is transitive.
Hence proved that the isomorphism h is an equivalence relation on the set of numbers.

- If h is an isomorphism from $(N_1, +_1, *_1)$ to $(N_2, +_2, *_2)$ then $h(0_1) = 0_2$ and $h(1_1) = 1_2$.
  Proof: Using axiom 2, we have: $h(a +_1 b) = h(a) +_2 h(b)$. Substituting $b = 0_1$, we get: $h(a +_1 0_1) = h(a) +_2 h(0_1)$. Since $h : N_1 \rightarrow N_2$, so $h(a +_1 0_1) = h(a)$. So, the expression simplifies to $h(a) = h(a) +_2 h(0_1)$. Adding $(-h(a))$ to both sides, we get,
  $h(a) +_2 (-h(a)) = h(a) +_2 h(0_1) +_2 (-h(a))$
  Applying commutative axiom $(a + b = b + a)$, and using $a + (-a) = 0$, the expression simplifies to
  LHS= $h(a) +_2 (-h(a)) = 0_2$
  RHS=$h(a) +_2 h(0_1) +_2 (-h(a)) = h(a) +_2 (-h(a)) +_2 h(0_1)$
  $= 0_2 +_2 h(0_1) = h(0_1)$.
  Hence proved, $h(0_1) = 0_2$.

  Using axiom 3, we have: $h(a *_1 b) = h(a) *_2 h(b)$. Substituting $b = 1_1$, we get: $h(a *_1 1_1) = h(a) *_2 h(1_1)$. Since $h : N_1 \rightarrow N_2$, so $h(a *_1 1_1) = h(a)$. So, the expression simplifies to $h(a) = h(a) *_2 h(1_1)$..... (i) Using the division axiom, we get,
  $h(a)/h(a) = h(a) * c$, such that $h(a) * c = 1_2$. Therefore, $h(a)/h(a) = 1_2$.
  Multiplying both sides by c in equation (i), we get:
  $h(a) *_2 c = h(a) *_2 h(1_1) *_2 c$, using multiplication axiom 5:
  $1_2 = h(a) *_2 c *_2 h(1_1) = 1_2 *_2 h(1_1) = h(1_1)$.
  Hence proved, $h(1_1) = 1_2$.

- If h is an isomorphism from $(N_1, +_1, *_1)$ to $(N_2, +_2, *_2)$ then $h(a -_1 b) = h(a) -_2 h(b)$ and $h(a/_1 b) = h(a)/_2 h(b)$.
  Proof: (i) To prove:$h(a -_1 b) = h(a) -_2 h(b)$
  Using the subtraction axiom, let $a -_1 b = a +_1 c$, such that $b +_1 c = 0_1$.
  Substituting this in the LHS expression:

  $h(a -_1 b) = h(a +_1 c) = h(a) +_2 h(c)$, such that $b +_1 c = 0_1$.
  So, $h(b +_1 c) = h(0_1) \implies h(b) +_2 h(c) = h(0_1)$
  $\implies h(b) +_2 h(c) +_2 (-_2 h(b)) = h(b) +_2 (-_2 h(b)) +_2 h(c) = 0_2 +_2 (-_2 h(b))$
  $\implies 0_2 +_2 h(c) = h(c) = -_2 h(b)$.
  So, the LHS of expression simplifies to :
  $h(a -_1 b) = h(a) +_2 h(c) = h(a) +_2 (-_2 h(b))$.
  Similarly, the RHS can be simplified as:
  Let $h(a) -_2 h(b) = h(a) +_2 y$, $y \in N_2$ such that $h(b) +_2 y = 0_2$
  $\implies h(b) +_2 y +_2 (-_2 h(b)) = 0_2 +_2 (-_2 h(b))$
  $\implies h(b) +_2 (-_2 h(b)) +_2 y = +_2(-_2 h(b))$
  $\implies 0_2 +_2 y = y = +_2(-_2 h(b))$
  So, $h(a) -_2 h(b) = h(a) +_2 y = h(a) +_2 (-_2 h(b))$. Hence proved, LHS =RHS.

  (ii) To prove:$h(a/_1 b) = h(a)/_2 h(b)$
  Using the division axiom, let $a/_1 b = a *_1 c$, such that $b *_1 c = 1_1$. Substi-

tuting this in the LHS expression:
$h(a/_1b) = h(a *_1 c) = h(a) *_2 h(c)$, such that $b *_1 c = 1_1$.
So, $h(b *_1 c) = h(1_1) \implies h(b) *_2 h(c) = h(1_1) = 1_2$
$\implies h(b) *_2 h(c) *_2 (1_2/_2h(b)) = h(b) *_2 (1_2/_2h(b)) *_2 h(c) = 1_2 *_2 (1_2/_2h(b))$
$\implies 1_2 *_2 h(c) = h(c) = 1_2/_2h(b)$.
So, the LHS of expression simplifies to :
$h(a/_1b) = h(a) *_2 h(c) = h(a) *_2 (1_2/_2h(b))$.

Similarly, the RHS can be simplified as:
Let $h(a)/_2h(b) = h(a)*_2h(c)$, such that $h(b)*_2h(c) = 1_2 \implies h(b)*_2h(c)*_2 (1_2/_2h(b)) = 1_2 *_2 (1_2/_2h(b)) \implies h(b) *_2 (1_2/_2h(b)) *_2 h(c) = 1_2/_2h(b)$
So, $h(a)/_2h(b) = h(a) *_2 h(c) = h(a) *_2 (1_2/_2h(b))$. Hence proved, LHS =RHS.

Do two sets of numbers of same cardinality always have isomorphism between them? The answer is no. Define a 0-1 polynomial to be $\sum_{i=0}^{k} c_i x^i$ with $c_i = 0, 1$. Define addition of these polynomials as $x^i + x^i = 0$ for every i. **Correction:** $F_2(x)$ **contains rational functions of the kind p(x)/q(x) where both p and q are 0-1 polynomials as defined, and q(x) is not zero.**

- Prove that the set of 0-1 polynomials with addition defined as above and usual multiplication of polynomials is a set of numbers. It is represented as $F_2(x)$.
  Proof: To show that $F_2(x)$ is a set of numbers.
  Consider an element $\alpha = p(x)/q(x) \in F_2(x)$, such that $q(x) \neq 0$.
  Similarly, let $\beta = e(x)/f(x) \in F_2(x)$, such that $f(x) \neq 0$.
  And, let $\gamma = m(x)/n(x) \in F_2(x)$, such that $n(x) \neq 0$.
  To prove that $F_2(x)$ is a set of numbers, we show the following axioms on this set:
  1. *Claim:* Addition of two 0-1 polynomials gives a 0-1 polynomial.
  Consider 0-1 polynomials, $a(x) = \sum_{i=0}^{k} a_i x^i$ and $b(x) = \sum_{i=0}^{k} b_i x^i$,and $c(x) = \sum_{i=0}^{k} c_i x^i$.
  Now, similarly, $a(x) + b(x) = \sum_{i=0}^{k} a_i x^i + \sum_{i=0}^{k} b_i x^i = \sum_{i=0}^{k} (a_i + b_i) x^i$, which is a 0-1 polynomial.
  2. *Claim:* Multiplication of two 0-1 polynomials is a 0-1 polynomial.
  Consider two 0-1 polynomials, $a(x) = \sum_{i=0}^{k} a_i x^i$ and $b(x) = \sum_{i=0}^{k} b_i x^i$and $c(x) = \sum_{i=0}^{k} c_i x^i$.
  Now, similarly, $a(x) * b(x) = \sum_{i=0}^{k} a_i x^i * \sum_{i=0}^{k} b_i x^i = \sum_{i=0,p+q=i}^{k} (a_p + b_q) x^i$, which is a 0-1 polynomial.
  3.Define $(\alpha + \beta) = (p(x) * f(x) + e(x) * q(x))/(f(x) * q(x))$. Then $\alpha + \beta \in F_2(x)$. Since product and sum of two 0-1 polynomials is a 0-1 polynomial, therefore, we can say both the numerator and denominator are 0-1 polynomials. Also, since $(f(x) \neq 0, g(x) \neq 0)$, therefore, $(f(x) * g(x)) \neq 0$. Hence, $(\alpha + \beta) \in F_2(x)$.
  4. Define $(\alpha * \beta) = (p(x) * e(x))/(f(x) * q(x))$. Then, $(\alpha * \beta) \in F_2(x)$.
  Since multiplication of two 0-1 polynomials is a 0-1 polynomial, the numer-

ators and denominators are 0-1 polynomials, and again $(f(x) * q(x) \neq 0)$. Therefore, $\alpha * \beta \in F_2(x)$.

5. $\alpha + \beta = \beta + \alpha$.

$(\alpha + \beta) = \frac{(p(x)*f(x)+e(x)*q(x))}{(f(x)*q(x))}$.

$(\beta + \alpha) = \frac{(e(x)*q(x)+p(x)*f(x))}{(q(x)*f(x))}$.

Hence, $\alpha + \beta = \beta + \alpha$.

6. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$

$(\alpha + \beta) = \frac{(p(x)*f(x)+e(x)*q(x))}{(f(x)*q(x))}$.

Then, $(\alpha + \beta) + \gamma = \frac{(p(x)*f(x)*n(x)+e(x)*q(x)*n(x))+f(x)*q(x)*m(x)}{(f(x)*q(x)*n(x))}$.

Similarly, $(\beta + \gamma) = \frac{(e(x)*n(x)+f(x)*m(x))}{(f(x)*n(x))}$.

Then, $\alpha + (\beta + \gamma) = \frac{(p(x)*f(x)*n(x)+e(x)*q(x)*n(x))+f(x)*q(x)*m(x)}{(f(x)*q(x)*n(x))}$.

7. $0 \in F_2$.

Consider the case when, for α, $q(x) = 1$, and all the coefficients c_i of $p(x)$ are 0. Then $\alpha \in F_2(x) = 0$.

8. For all $\alpha \in F_2$, there exists $\beta \in F_2$, such that $\alpha + \beta = 0$.

Consider $\beta = \alpha$. Then $\alpha + \beta = \alpha + \alpha = (p(x) + p(x))/q(x) = 0$, since for all $i = 0$ to k, we know that $x^i + x^i = 0$, so all coefficients of $(p(x) + p(x))$ will become 0.

9. $\alpha * \beta = \beta * \alpha$.

$(\alpha * \beta) = \frac{(p(x)*e(x))}{(q(x)*f(x))}$.

$(\beta * \alpha) = \frac{(e(x)*p(x)))}{(f(x)*q(x))}$.

Hence, $\alpha * \beta = \beta * \alpha$.

10. $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$

$(\alpha * \beta) = \frac{(p(x)*e(x)}{(f(x)*q(x))}$.

Then, $(\alpha * \beta) * \gamma = \frac{(p(x)*e(x)*m(x)}{(q(x)*f(x)*n(x))}$.

Similarly, $(\beta * \gamma) = \frac{(e(x)*m(x))}{(f(x)*n(x))}$.

Then, $\alpha * (\beta * \gamma) = \frac{(p(x)*e(x)*m(x)}{(f(x)*q(x)*n(x))}$.

11. $1 \in F_2$.

Consider the case when, for α, $q(x) = 1$, the first coefficient $c_0 = 1$ and all the other coefficients c_i of $p(x)$ are 0. Then $\alpha \in F_2(x) = 1$.

12. For all $\alpha \in F_2$, there exists $\beta \in F_2$, such that $\alpha * \beta = 1$. Consider $\beta = \alpha$. Then $\alpha + \beta = \alpha + \alpha = (p(x) + p(x))/q(x) = 0$, since for all $i = 0$ to k, we know that $x^i + x^i = 0$, so all coefficients of $(p(x) + p(x))$ will become 0.

13. The distributive property is held true:

$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$

LHS$= (\beta + \gamma) = \frac{(e(x)*n(x)+f(x)*m(x))}{(f(x)*n(x))}$.

$\alpha * (\beta + \gamma) = \frac{p(x)}{q(x)} * \frac{(e(x)*n(x)+f(x)*m(x))}{(f(x)*n(x))}$

$\implies \alpha * (\beta + \gamma) = \frac{(p(x)*e(x)*n(x)+p(x)*f(x)*m(x))}{(q(x)*f(x)*n(x))}$

RHS$= \alpha * \beta + \alpha * \gamma = \frac{(p(x)*e(x))}{(q(x)*f(x))} + \frac{(p(x)*m(x))}{(q(x)*n(x))}$

$\implies \alpha * \beta + \alpha * \gamma = \frac{(p(x)*e(x)*n(x)+p(x)*f(x)*m(x))}{(q(x)*f(x)*n(x))}$
Hence proved, $\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$.
Hence proved, that the set $F_2(x)$ is a set of numbers.

- Show that there is a bijection between rational numbers $\mathbb{Q}$ and $F_2(x)$.
  Proof: If there is a one-one map $f : \mathbb{Q} \mapsto F_2(x)$, and another one-one map $g : F_2(x) \mapsto \mathbb{Q}$, then by *Canto-Schroeder-Bernstein Theorem,* there is a bijection between $\mathbb{Q}$ and $F_2(x)$.
  Consider any element of $\mathbb{Q}$ as $(-1)^{sign}p/q$, such that $q \neq 0$, sign$\in \{0,1\}$.
  Now, if $p = 0$, we map it to $F_2(x)$, such that $q(x) = 1$ and $p(x)$ is such that $c_i = 0 \forall i$.
  If sign=0, the rational number is positive, and we map it to:
  $F_2(x)$, such that $q(x) = 1$ and $p(x)$ is such that $c_i = 0$ for all $i \leq p$, and $c_i = 1$ for all $p+1 \leq i \leq p+k$.
  If sign=1, the rational number is negative, and we map it to:
  $F_2(x)$, such that $q(x) = 1$ and $p(x)$ is such that $c_0 = 1, c_i = 0$ for all $1 \leq i \leq p+1$, and $c_i = 1$ for all $p+2 \leq i \leq p+k+1$.
  This mapping from $\mathbb{Q} \mapsto F_2(x)$ is clearly one-one.

  Consider any element $p(x)/q(x) \in F_2(x)$.
  We take all the coefficients of $p(x)$ in a linear form and form a binary number of them. Now, we convert this binary number to decimal number. Let this number be a. Similarly, we get a decimal number for $q(x)$, let it be b. Now, we make a rational number p/q from these as $p = 3^a$, and $q = 5^b$.
  This mapping from $F_2(x) \mapsto \mathbb{Q}$ is also one-one.
  Hence proved that there exists a bijection between $\mathbb{Q}$ and $F_2(x)$.

- Show that there is no isomorphism between $\mathbb{Q}$ and $F_2(x)$.
  Proof: Consider a map $h : (\mathbb{Q}, +_{\mathbb{Q}}, *_{\mathbb{Q}}) \mapsto (F_2(x), +_{F_2}, *_{F_2})$, such that:
  (i) h is a bijection.
  (ii) For all $a, b \in \mathbb{Q}$, $h(a +_{\mathbb{Q}} b) = h(a) +_{F_2} h(b)$.
  (iii) For all $a, b \in N_1$, $h(a *_1 b) = h(a) *_2 h(b)$.
  Now, consider some element $x \neq 0 \in \mathbb{Q}$, such that $h(x) = k \neq 0 \in F_2(x)$.
  Then, $h(x +_{\mathbb{Q}} x) = h(x) +_{F_2} h(x) = 0_{F_2} = h(0_{\mathbb{Q}})$.
  But since h is a bijection, this is possible only for $(x +_{\mathbb{Q}} x = 0_{\mathbb{Q}})$, which means only $x = 0_{\mathbb{Q}}$. But we had assumed $x \neq 0$.
  Hence proved that there's no bijection between $\mathbb{Q}$ and $F_2(x)$.

As per the definition above, the set of integers $\mathbb{Z}$ is not a set of numbers. This is unsatisfactory. The problem is that division is generally not possible in $\mathbb{Z}$. To address this, define a set of *numbers without division* $(N, +, *)$ to be a set of numbers in which the fourth axiom for $(N, *)$ is removed. Show that:

- $(\mathbb{Z}, +, *)$ is a set of numbers without division.
  Proof: Removing the fourth axiom on $(N, *)$, let the set be $(M, +, *)$. Now consider $a, b, c \in \mathbb{Z}$, such that the division axiom is as $a/b = a*c$ such that $b * c = 1$. Let $a = 1$, then $1/b = 1 * c$, such that $b * c = 1$. Consider three cases:
  (i) $b > 1 \implies c = 1/b \in (0, 1)$. Since $c \in \mathbb{Z}$, but there's no integer between $(0, 1)$. Hence, $c \notin \mathbb{Z} \implies b \leq 1$.
  (ii) $b < -1 \implies c = 1/b \in (-1, 0)$. Since $c \in \mathbb{Z}$, but there's no integer between $(-1, 0)$. Hence, $c \notin \mathbb{Z} \implies b \geq -1$.
  (iii) If $b = 0$, we'll get the contradiction stated in **question 6**. Hence $b \neq 0$.
  Hence, the only possibility is that $b = 1$.
  If $b = 1$, then since $c = 1/b$, therefore $c = 1$, and hence, division axiom has no meaning.
  $a/1 = a = a * 1$.
  $a/-1 = -a = a * (-1)$.
  Therefore, the set $(\mathbb{Z}, +, *)$ is a set of numbers without division.

Such a set of numbers can also have unexpected properties. Show that:

- There is a set of numbers without division $(N, +, *)$ such that there are $a, b \in N$, $a \neq 0$, $b \neq 0$, but $a * b = 0$.
  Proof: Consider the set $N = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, such that the operations $(+), (*)$ are defined as:
  for $a, b \in N$, $+(a, b) = (a +_{\mathbb{N}} b) \pmod 9$.
  for $a, b \in N$, $*(a, b) = (a *_{\mathbb{N}} b) \pmod 9$,
  where $(+_{\mathbb{N}})$ and $(*_{\mathbb{N}})$ are the usual addition and multiplication operations on the set of $\mathbb{N}$. Consider $a = 3, b = 6$. Clearly, both are non zero. Now, $*(3, 6) = (3 *_{\mathbb{N}} 6)$(mod 9)= (18)(mod9)= 0.
  Hence proved.

- There is a set of numbers without division $(N, +, *)$ such that there is $a \in N$, $a \neq 0$, but $a^3 = a * a * a = 0$.
  Proof: Consider the set $N = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, such that the operations $(+), (*)$ are defined as:
  for $a, b \in N$, $+(a, b) = (a +_{\mathbb{N}} b) \pmod 9$.
  for $a, b \in N$, $*(a, b) = (a *_{\mathbb{N}} b) \pmod 9$.
  where $(+_{\mathbb{N}})$ and $(*_{\mathbb{N}})$ are the usual addition and multiplication operations on the set of $\mathbb{N}$. Consider $a = 3$. Now,
  $a * a * a = ((a *_{\mathbb{N}} a)(\text{mod } 9)) * a = ((3 *_{\mathbb{N}} 3)(\text{mod } 9))*a$
  $= (0 *_{\mathbb{N}} a)$(mod 9)= 0.
  Hence proved.

Later in the course, we will see utility of these types of numbers as well.