CS201 Assignment 1: The Concept of Numbers

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.

  Ans.
  Let U be a collection of all sets. Suppose U itself is a set.
  Then, by the definition of U, U$\in$U.
  According to the Axiom of Regularity of the Zermalo-Fraenkel Axioms of Set Theory, for every non-empty set A, $\exists$ an x$\in$A such that x$\cap$A=ϕ.

  Consider a set A={U}. Since A is a non-empty set, it should satisfy the Axiom of Regularity.
  Since U is the only element of A, Axiom of Regularity implies U$\cap$A=ϕ.
  However, by assumption, U$\in$U. Hence, U$\cap$A=U, where U$\neq \phi$.
  We arrive at a contradiction which arose due to a wrong assumption.
  Thus, U is not a set as per Zermalo-Fraenkel Axioms of Set Theory.

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 $V \in V$?".

  Ans.
  Suppose V is a set such that V contains all sets that don't contain themselves.

  Case 1: V$\in$V
  For any X$\in$V, X$\notin$X i.e. X doesn't contain itself.
  Since V$\in$V, V doesn't contain itself.
  $\rightarrow$V$\notin$V.
  Thus, we arrive at a contradiction.

  Case 2: V$\notin$V
  V is a set of all sets that don't contain themselves.
  Since V$\notin$V, V contains itself.
  $\rightarrow$V$\in$V
  Thus, we arrive at a contradiction.

Thus, we arrive at a contradiction in both possible cases.

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:

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.

  Ans.
  Suppose there is a number 0' in addition to 0 satisfying the third axiom. Since 0'∈N, it satisfies the third axiom.

$$\rightarrow 0' = 0' + 0 \tag{1}$$

  Since 0∈N, it satisfies the third axiom.

$$\rightarrow 0 = 0 + 0' \tag{2}$$

  Since 0,0'∈N, they satisfy the fifth axiom.

$$\rightarrow 0' + 0 = 0 + 0' \tag{3}$$

  Using (1),(2) and (3):

$$0'=0'+0=0+0'=0$$
$$\rightarrow 0'=0$$

Hence,there is a unique number 0 satisfying the third axiom.

- For every $a \in N$, there is a unique b satisfying fourth axiom.

Ans.
Suppose $\exists$ a$\in$N such that for b,c $\in$ N , b$\neq$c, the fourth axiom is satisfied.
Since b$\in$N, it satisfies the third axiom for the unique no. 0

$$\rightarrow b = b + 0 \tag{4}$$

From the assumption,

$$\rightarrow 0 = a + c \tag{5}$$

Using (4) and (5):

$$\rightarrow b = b + (a + c) \tag{6}$$

Since c$\in$N, it satisfies the third axiom for the unique no. 0

$$\rightarrow c = c + 0 \tag{7}$$

From the assumption,

$$\rightarrow 0 = a + b \tag{8}$$

Using (6) and (7):

$$\rightarrow c = c + (a + b) \tag{9}$$

Since a,b,c $\in$N, they satisfy the second and the fifth axioms.

$$\rightarrow b + (a + c) = (b + a) + c = c + (a + b) \tag{10}$$

Using (6),(9) and (10):

$$b=b+(a+c)=c+(a+b)=c$$

Thus, we arrive at a contradiction that arises due to wrong assumption.
Hence, for every a$\in$N, there is a unique b satisfying fourth axiom.

- Define $-a$ to be the number such that $a + (-a) = 0$. For every $a, b \in N$, $a - b = -(b - a)$.

  Ans.
  Since a∈N, a satisfies the fourth axiom.
  Hence, there is a unique d∈N such that a+d=0.
  Consider −a such that a+(−a)=0
  In Q4., we proved that d is unique→ −a=d
  Hence, $-a$∈N.
  Consider a b∈N. Since −a,b∈N, they satisfy the first axiom.

  $$-a+b \in N.$$

  Similarly,

  $$a-b \in N.$$

  Since a,(−a),b,(−b),(a−b) and (−a+b) belong to N, they satisfy the second third and fifth axioms
  Now, consider (a−b) + (−a+b)
  (a−b)+(−a+b) = ((a−b)+(−a))+b = ((−b)+(a+−a))+b = ((−b)+0)+b
  =(−b)+b = 0
  We have already proven that for any a,d ∈ N such that a+d=0→(−a)=d.
  Hence,for every a,b∈N,

  $$a\text{-}b = -(b-a)$$

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 $1 = 0$.

  Ans.
  Suppose 0∈N for the second axiom→there exists a d∈N such that d*0=1
  Since d,0∈N, they satisfy the third axiom. Put a=d; b,c=0.

$$a * (0 + 0) = a * 0 + a * 0 = 1 + 1 \tag{11}$$

$$a * (0 + 0) = a * 0 = 1 \tag{12}$$

  Using (11) and (12):

$$1+1=1$$

  Since 1∈N, it satisfies the third axiom of addition.

$$1=0$$

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.

Ans.
Example 1
Consider the set of numbers (N, +', *') defined as above. We thus have the definitions of 0 and 1.
Define 3 to be 1 + 1 + 1.
For any a,b∈(N, +, *), define +(a,b) to be (a -' 1) +' (b +' 1) where +' is the usual addition and -' is the usual subtraction
For any a,b∈(N, +, *), define *(a,b) to be (2*'a)*'(2*'b) where *' is the usual multiplication operations.

- Axioms of Addition:
  - for any a,b∈(N, +', *'), +(a,b)= (a-1) +' (b+1)∈(N, +, *) since (N, +, *) will satisfy the first axiom of addition on +' and -'
  - for any (a,b,c)∈(N, +', *'), a+(b+c) = (a -' 1) +' ((b-'1+'c+'1)+1) = a+'b+'c
    (a+b)+c) =((a-'1+'b+'1)-'1)+'(c+'1) = a+'b+'c
    Thus, the second axiom of addition is satisfied

- For any a∈(N, +, *) , consider +(a,0).
  Clearly, +(a,0)=(a-'1)+'(0+'1)=a
  Thus, the third axiom is satisfied.
- Clearly, (-a) as defined for (N, +', *') satisfies the fourth axiom for (N, +, *) as well since +(a,-a)=0
- For any a,b∈(N, +, *), +(a,b) = (a-'1)+'(b+'1) = a+'b
  Similarly +(b,a) = b+'a
  Since (N, +, *) satisfies the fifth axiom on usual addition, it satisfies the fifth axiom on our addition operation as well.

• Axioms of Multiplication:

- for any a,b∈(N, +, *), *(a,b)= 2*'a*'2*'b∈(N, +, *) since (N, +, *) will satisfy the first axiom of multiplication on *'
- for any (a,b,c)∈(N, +', *'), a*(b*c) = (2*'a)*'(2*'b*'2*'c) = 8*'a*'b*'c'
  since (N, +, *) satisfies the second axiom of multiplication on *'
  Similarly, (a*b)*c=(2*'a*'2*'b)*'(2*'c) = 8*'a*'b*'c'
  Thus, the second axiom of multiplication is satisfied
- For any a∈(N, +, *) , consider *(a,1/4).
  Consider 1+1+1+1 represented by 4 in (N, +', *'). Since this is unequal to 0, there exists a number n in (N, +', *') such that 4*b=1.
  Let b be represented by 1/4.
  Clearly, *(a,1/4)=2*'a*'2*'(1/4)=a
  Thus, the third axiom is satisfied.
- For any a≠0, consider b to be the multiplicative inverse of a defined on (N, +', *'). Thus, a*'b=1.
  Let c = b*(1/4)*(1/4) where (1/4) is as defined above.
  (a,c)=2*'a*'2*'c= (1/4)
  Thus, the fourth axiom is satisfied.
- For any a,b∈(N, +, *), *(a,b) = (2*'a*'2*'b) = 4*'a*'b
  Similarly *(b,a) = (2*'b*'2*'a) = 4*'b*'a
  Since (N, +, *) satisfies the fifth axiom on usual multiplication, it satisfies the fifth axiom on our multiplication operation as well.

• Axioms of Addition and Multiplication:

- We have already proven that the axioms of addition are satisfied
- WE have already proven that the axioms of multiplication are satisfied ∀a∈(N, +, *) such that a≠0.
- For any a,b,c ∈(N, +, *), consider a*(b+c) and a*b + a*c
  a*(b+c) = (2*'a)*'(2*'(b-'1+'c+'1)) = (2*'a)*'(2*'(b+'c))
  Since (N, +, *) satisfies the third axiom for +' and *':
  (2*'a)*'(2*'(b+'c)) = 4*'a*'b + 4*'a*'c
  Thus, a*(b+c) = 4*'a*'b + 4*'a*'c
  Now, a*b + a*c = (2*'a*'2*'b) -'1 +' (2*'a*'2*'c) +' 1 = 4*'a*'b +

4*'a*'c
Thus, the third axiom is satisfied.

Example 2. Consider a subset of (N, +', *') as {0, 0+'1, 0+'1+'1, 0+'1+'1+'1, 0+'1+'1+'1} represented by {0, 1, 2, 3, 4} where +' and *' are the usual addition and multiplication operations
Define addition on this set(suppose it's called A) to be +(a,b) = (a+'b) mod 5.
Define multiplication to be *(a,b) = (a*'b) mod 5.

- Axioms of Addition
  - Since modulus with respect to 5 can only be 0, 1, 2, 3, 4, the first axiom is satisfied.
  - Since A satisfies the second axiom on +', a+'(b+'c)= (a+'b) +'c
    Thus, since the numerators in the cases +(a,+(b,c)) and +(+(a,b),c) are equal, second axiom is satisfied.
  - Since all the numbers is the set A are less than 5, the modulus upon division by 5 will be the number itself.
    Now, +(a,0) = (a+'0) mod 5 = a mod 5 = a
    Thus, the third axiom is satisfied.
  - For every element a∈A such that a≠0, consider (5-'a).
    We can verify that (5-'a)∈A ∀ a ∈ A such that a≠0.
    Consider +(a,5-'a) = (a+'(5-'a)) mod 5 = 0.
    For a=0, consider 0 itself.
    Consider +(0,0) = (0+'0) mod 5 = 0.
    Thus, for every a∈A, we can get a b such that +(a,b)=0
  - A satisfies the fifth axiom on addition:
    +(a,b) = (a+'b) mod 5 = (b+'a) mod 5 = +(b,a)
    Thus, the fifth axiom is satisfied.
- Axioms of Multiplication
  - Since modulus with respect to 5 can only be 0, 1, 2, 3, 4, the first axiom is satisfied.
  - Since A satisfies the second axiom on *', a*'(b*'c)= (a*'b) *'c
    Thus, since the numerators in the cases *(a,*(b,c)) and *(*(a,b),c) are equal, second axiom is satisfied.
  - Since all the numbers is the set A are less than 5, the modulus upon division by 5 will be the number itself.
    Now, *(a,1) = (a*'1) mod 5 = a mod 5 = a
    Thus, the third axiom is satisfied.
  - We can verify that ∀a∈A such that a≠ 0, there exists a b∈A such that *(a,b) = 5.
    For 1, it's 1. For 2, it's 3. For 3, it's 2. For 4, it's 4.
    Thus, for every a∈A≠0, we can get a b such that *(a,b)=1

- A satisfies the fifth axiom on multiplication:
  (a,b) = (a*'b) mod 5 = (b*'a) mod 5 = *(b,a)
  Thus, the fifth axiom is satisfied.

- Axioms of Addition and Multiplication
  - We have already proven that the axioms of addition are satisfied
  - WE have already proven that the axioms of multiplication are satisfied ∀a∈A such that a≠0.
  - For any a,b,c ∈(N, +, *), consider a*(b+c) and a*b + a*c
    Since A satisfies the third axiom on usual addition and multiplication, a*'(b+'c) = a*'b + a*'c
    Thus, a*(b+c) = (a*'(b+'c)) mod 5 = (a*'b +' a*'c) mod 5 = a*b + a*c
    Thus, the third axiom is satisfied.

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.

Ans.
Example 2 in the question above is the example of a finite set.

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.

  Ans.
  Suppose there exists a composite k such that k=m*n where m,n∈ ℕ and m,n are non-trivial divisors of k(i.e. m,n≠1,k)
  Suppose k is the multiplicity of (N,+,*)
  Then, 1+1+1..(k times)=0
  Since k=m*n, we can divide the 1s into groups of size m. Suppose 1+1+1...(n times)=p
  Case 1: p=0
  p=0→ 1+1+1...(m times)=0
  Since m is a non-trivial divisor of composite k, m¡k
  Multiplicity has to be the smallest number such that 1+1+1...(k times)=0.
  Hence, multiplicity≤m*l*k
  Contradiction.

Case 2: p≠0
Since p∈N and p≠0, there ∃ an l∈N such that p*l=1.
Consider and a∈N. Since a,0,0 ∈N, they satisfy the third axiom of (N,+,*)
Then,

$$a*(0+0)= a*0 + a*0 \text{ and } a*(0+0) = a*0$$
$$\rightarrow a*0 + a*0 = a*0$$
$$\rightarrow a*0 = 0$$

Since 1+1+1...(k times) was grouped into group of size m and value p, p+p+p...(n times)=0

$$l*(p+p+p...(n \text{ times}))=l*0$$
$$\rightarrow l*p + l*p + l*p...(n \text{ times})=0$$
$$\rightarrow 1 + 1 + 1...(n \text{ times})=0$$

Since n is a non-trivial divisor of k, n≤k
Multiplicity has to be the smallest number such that 1+1+1...(k times)=0.
Hence, multiplicity≤n≤k
Contradiction.

Thus, contradiction arises in both the possible cases due to wrong assumption.
Multiplicity of N can be 0 or prime only.

- Any set of numbers $(N, +, *)$ of multiplicity 0 contains $\mathbb{N}$.

  Ans.

  Consider the set (N, +, *) of multiplicity 0.
  According to Peano's Axioms, a set containing 0 is the set of natural numbers if we can create a map S such that ∀x∈ $\mathbb{N}$, S(x) is one-one and S(x)≠0.
  Suppose the set defined on (N,+,*) be A={0, 0+1, 0+1+1, 0+1+1+1,.....}
  We claim that this map is the set of natural numbers of (N, +, *).
  This set contains 0→ Peano's first axiom is satisfied.
  Suppose we define our map S(x) ∀ x ∈ $\mathbb{N}$ as S(x) = x+1.
  We claim that this is a one - one map that doesn't contain 0.

  - S is one-one
    Suppose for some x, x' ∈ A, S(x) = S(x')
    Then, 0+1+1+....+1(k times) = 0+1+1+...+1(k' times)
    0+1+1+...+1(k' times) + 1+1+...+1(k-k' times) = 0+1+1+...+1(k' times)
    Since according to Q3., (N, +, *) has a unique 0:

1+1+...+1(k-k' times) = 0
If k≠k', we get a number greater than 0(k - k') such that 1+1+1+...+1(k-k' times) = 0.
Hence, multiplicity≠0. Contradiction.
Thus k=k' which implies x=x' → S is one-one.

– S(x)≠0
Suppose ∃x ∈ A such that S(x) = 0
Then, 0+1+1+1+...+1(k times) = 0 where k≥1.
Since according to Q3., (N, +, *) has a unique 0:
1+1+1+...+1(k times) = 0 where k≥1.
We get a number greater than 0(k) such that 1+1+1+...+1(k times) = 0.
Hence, multiplicity≠0. Contradiction.
Thus, S(x)≠0

Thus, Peano's second and third axioms are satisfied.
Peano's fourth axiom states that a set B contains ℕ iff 0∈B and ∀x∈ℕ∩B, S(x)∈N.
Clearly, 0∈(N, +, *).
We can prove the second requirement inductively.
P(1):
0∈N∩B and (N, +, *) satisfies the first axiom of addition. Thus, 0+1 ∈N.
P(m):
Suppose 0+1+1+1+...+1(m times) ∈N.
P(m+1):
0+1+1+1+...+1(m times) ∈N∩B.
(N, +, *) satisfies the first axiom of addition.
Thus, 0+1+1+1+...+1(m+1 times) ∈N.
Thus, P(m+1) is true→ claim proven inductively.

The set {0, 0+1, 0+1+1, ...} can be represented as {0, 1, 2,...} by defining these symbols as such.
N contains ℕ.

- For any set of numbers $(N, +, *)$ of multiplicity 0, for any $k \in \mathbb{N} \subseteq N$, for any $a \in N$, $k * a = \underbrace{a + a + \cdots + a}_{k \text{ times}}$.

Ans.
In the previous question, we proved that any k∈ℕ can be represented as 1 + 1 + 1 +...+ 1(k times) by creating a map on the set (N, +, *) of multiplicity 0.
(N, +, *) satisfies the axiom which states ∀a, b, c∈(N, +, *), a*(b+c) = a*b + a*c
It also satisfies the second axiom of addition.
a+a+a+...+a(k times) = a*(1+1+1+...+1(k times)) (Therefore, a*1 = a)
→a+a+a+...+a(k times) = a*k

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.

  Ans.

  For any relation R to be an equivalence relation on a set A, it has to be reflexive, symmetric and transitive.
  For reflexivity, ∀a∈(A,+,*), aRa.
  For symmetry, ∀a,∈(A,+,*), if aRb, then bRa.
  For transitivity, ∀a,b,c∈(A,+,*), if aRb and bRc, then aRc.

  - Reflexivity
    For any set belonging to the set of all sets of numbers, define h to be the identity function.
    Thus, ∀a∈(A,+,*), define h(a) = a
    - h is a bijection:
      Consider a,b∈A such that h(a) = h(b)
      However, h(a) = a and h(b) = b
      Thus, if h(a) = h(b), a = b
      h is one-one. Consider any a∈A, clearly h(a) = a
      ∀a∈A, a has a pre-image in A.
      h is onto
      Since h is one-one and onto, h is a bijection.
    - h(a + b) = h(a) + h(b) ∀a,b∈(A,+,*):
      Consider a,b∈A. Let a + b = c for some c∈(A,+,*).
      Then, h(a + b) = a + b = c
      Now, h(a) + h(b) = a + b = c
      Thus, h(a + b) = h(a) + h(b) ∀a,b∈(A,+,*)
    - h(a * b) = h(a) * h(b) ∀a,b∈(A,+,*):
      Consider a,b∈A. Let a * b = c for some c∈(A,+,*).
      Then, h(a * b) = a * b = c
      Now, h(a) * h(b) = a * b = c
      Thus, h(a * b) = h(a) * h(b) ∀a,b∈(A,+,*)

Thus, for every A belonging to the set of sets of all numbers, h is an isomorphism.
Reflexivity is satisfied.

- Symmetry:
  Suppose $(A,+_1,*_1),(B,+_2,*_2)$ belong to the set of all sets of numbers.
  Suppose h is an isomorphism between A and B.
  Define h' to be a relation between B and A such that $\forall b \in B$, h'(b) = a, where h(a) = b.
  - h' is a bijection:
    suppose for $b,b' \in B$, h'(b) = h'(b')
    Then, a = a'
    $\rightarrow$ h(a) = h(a')
    $\rightarrow$ b = b'
    h' is one-one.
    Consider a $b \in B$
    Since h' is one-one and onto, h' is a bijection.
  - $h'(a +_2 b) = h'(a) +_1 h'(b) \; \forall \; a,b \in (B,+_2,*_2)$:
    Consider any $a,b \in (B,+_2,*_2)$.
    Suppose h(c) = a and h(d) = d where $c, d \in (A,+_1,*_1)$
    $h(c +_1 d) = h(c) +_2 h(d) = a +_2 b$
    $\rightarrow h'(a +_2 b) = c +_1 d$
    $h'(a) +_1 h'(b) = c +_1 d$
    Thus, $h'(a +_2 b) = h'(a) +_1 h'(b) \; \forall \; a,b \in (B,+_2,*_2)$
  - $h'(a *_2 b) = h'(a) *_1 h'(b) \; \forall \; a,b \in (B,+_2,*_2)$:
    Consider any $a,b \in (B,+_2,*_2)$.
    Suppose h(c) = a and h(d) = d where $c, d \in (A,+_1,*_1)$
    $h(c *_1 d) = h(c) *_2 h(d) = a *_2 b$
    $\rightarrow h'(a *_2 b) = c *_1 d$
    $h'(a) *_1 h'(b) = c *_1 d$
    Thus, $h'(a *_2 b) = h'(a) *_1 h'(b) \; \forall \; a,b \in (B,+_2,*_2)$

  Thus, h' is an isomorphism.
  Symmetry is satisfied.

- Transitivity:
  Suppose there are sets $(A,+_1,*_1),(B,+_2,*_2)$ and $(C,+_3,*_3)$ in the set of all sets of numbers.
  Suppose h is an isomorphism from A to B and h' is an isomorphism from B to C.
  Define h" to a relation from A to C such that $\forall a \in (A,+_1,*_1)$, h"(a) = h'(h(a)).
  - h" is a bijection:
    Suppose for some a,a'*in* $(A,+_1,*_1)$, h"(a) = h"(a')
    h'(h(a)) = h'((a'))
    $\rightarrow$h(a) = h(a') (Since h' is one-one)
    $\rightarrow$a = a' (Since h is one-one)

h" is one-one
Suppose there is some c∈(C,$+_3$,$*_3$)
Then, ∃b ∈(B,$+_2$,$*_2$) such that h'(b) = c (Since h' is onto)
Similarly,∃a ∈(A,$+_1$,$*_1$) such that h(a) = b (Since h is onto)
Thus, h'(h(a)) = c
→ h"(a) = c
h" is onto
h" is a bijection

* ∀a,a'∈(A,$+_1$,$*_1$), h"(a $+_1$ a") = h"(a) $+_3$ h"(a'):
h"(a $+_1$ a") = h'(h(a $+_1$ a')) = h'(h(a) $+_2$ h(a')) = h'(h(a)) $+_3$ h'(h(a')) = h"(a) $+_3$ h"(a') (h,h' are isomorphisms, they satisfy the second property of isomorphisms)
Thus, ∀a,a'∈(A,$+_1$,$*_1$), h"(a $+_1$ a") = h"(a) $+_3$ h"(a')
* ∀a,a'∈(A,$+_1$,$*_1$), h"(a $*_1$ a") = h"(a) $*_3$ h"(a'):
h"(a $*_1$ a") = h'(h(a $*_1$ a')) = h'(h(a) $*_2$ h(a')) = h'(h(a)) $*_3$ h'(h(a')) = h"(a) $*_3$ h"(a') (h,h' are isomorphisms, they satisfy the third property of isomorphisms)
Thus, ∀a,a'∈(A,$+_1$,$*_1$), h"(a $*_1$ a") = h"(a) $*_3$ h"(a')

Thus, h" is an isomorphism. Thus, transitivity is satisfied.

Since isomorphisms are reflexive, symmetric and transitive, they form an equivalence relation.

- If h is an isomorphism from $(N_1, +_1, *_1)$ to $(N_2, +_2, *_2)$ then $h(0_1) = 0_2$ and $h(1_1) = h(1_2)$.

Ans.
For any number a∈N_1, a $+_1$ 0_1 = a.
Since a,0_1∈N_1 and h is an isomorphism-

$$h(a +_1 0_1) = h(a) +_2 h(0_1)$$
$$h(a) = h(a) +_2 h(0_1)$$

Since h:N_1↦N_2 , h(a)∈N_2.
Additionally, since h is a bijection, ∀b ∈ N_2, ∃ an a∈N_1 such that h(a) = b.
Hence, ∀b ∈ N_2,

$$b = b +_2 h(0_1)$$

Using Q3., we can say that 0_2 is unique for the set N_2.

$$h(0_1) = 0_2$$

For any number a∈N_1, a $*_1$ 1_1 = a.
Since a,1_1∈N_1 and h is an isomorphism-

$$\mathrm{h}(\mathrm{a} *_1 1_1) = \mathrm{h}(\mathrm{a}) *_2 \mathrm{h}(1_1)$$
$$\mathrm{h}(\mathrm{a}) = \mathrm{h}(\mathrm{a}) *_2 \mathrm{h}(1_1)$$

Since h:$N_1 \mapsto N_2$, h(a)$\in N_2$.
Additionally, since h is a bijection, $\forall$b $\in N_2$, $\exists$ an a$\in N_1$ such that h(a) = b.
Hence, $\forall$b $\in N_2$,

$$\mathrm{b} = \mathrm{b} *_2 \mathrm{h}(1_1)$$

Suppose the set (N_2, +, *) has 1_2, $1'_2 \in N_2$ such that $\forall$c$\in N_2$, c$*1_2 = 1_2$ and c$*1'_2 = 1'_2$.
Then, since 1_2, $1'_2 \in N_2$,

$$1_2 = 1_2 * 1'_2 = 1'_2$$

Hence, 1_2 is unique.
Since $\forall$b $\in N_2$, b = b $*_2$ h(1_1),

$$1_2 = \mathrm{h}(1_1)$$

- 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 $h(a/_1 b) = h(a)/_2 h(b)$.

  Ans.
  Consider any b$\in N_1$.
  Then,

$$\mathrm{h}(\mathrm{b} -_1 \mathrm{b}) = \mathrm{h}(\mathrm{b}) +_2 \mathrm{h}(-_1 \mathrm{b}) \rightarrow \mathrm{h}(0_1) = \mathrm{h}(\mathrm{b}) +_2 \mathrm{h}(-_1 \mathrm{b})$$

  According to the previous question, h(0_1) = 0_2.
  Hence,

$$0_2 = \mathrm{h}(\mathrm{b}) +_2 \mathrm{h}(-_1 \mathrm{b})$$
$$\rightarrow \mathrm{h}(-_1 \mathrm{b}) = -_2 \mathrm{h}(\mathrm{b})$$
$$\rightarrow \mathrm{h}(\mathrm{a} -_1 \mathrm{b}) = \mathrm{h}(\mathrm{a}) +_2 \mathrm{h}(-_1 \mathrm{b}) = \mathrm{h}(\mathrm{a}) -_2 \mathrm{h}(\mathrm{b})$$

  Consider any b$\in N_1$. There exists a c$\in N_1$ such that b$*_1$c = 1_1.
  Then,

$$\mathrm{h}(\mathrm{b} /_1 \mathrm{b}) = \mathrm{h}(\mathrm{b}) *_2 \mathrm{h}(\mathrm{c}) \rightarrow \mathrm{h}(1_1) = \mathrm{h}(\mathrm{b}) *_2 \mathrm{h}(\mathrm{c})$$

  According to the previous question, h(1_1) = 1_2.
  Hence,

$$1_2 = \mathrm{h}(\mathrm{b}) *_2 \mathrm{h}(\mathrm{c})$$

Let h(c) = d. Clearly, d $*_2$ h(b) = 1_2.

$$\rightarrow \text{h(a } /_1 \text{ b)} = \text{h(a)} *_2 \text{ h(c)} = \text{h(a)} *_2 \text{ d} = \text{h(a)} /_2 \text{ h(b)}$$

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.

- 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 $F_2(x)$.
  Ans.
  F_2(x) is the rational polynomial that can be represented as $\frac{p(x)}{q(x)}$, where p(x) and q(x) are 0-1 polynomials. Suppose we have two F_2(x) numbers $\frac{a(x)}{b(x)}$ and $\frac{c(x)}{d(x)}$, their sum can be defined as $\frac{a(x)*d(x)+b(x)*c(x)}{b(x)*d(x)}$, where * denotes the usual polynomial multiplication and + denotes the addition of two 0-1 polynomials as defined in the question. To show that the set of F_2(x) polynomials is a set of numbers, we need to prove the set satisfies the axioms of addition, multiplication and addition and multiplication occurring together.
  - Axioms of Addition:
    * Consider the addition of any two 0-1 polynomials,a(x) and b(x). Suppose the sum is the polynomial c(x). For any term of power i in c(x), three cases arise-
      · Case 1: term is not present in both a(x) and b(x).
      In this case, c(x) doesn't have the term either. Thus, the coefficient is 0.
      · Case 2: term is present in a(x) or b(x)
      In this case, c(x) does have the term and its coefficient is 1.
      · Case 3: term is present in both a(x) and b(x)
      In this case, keeping in lines with the definition of addition, c(x) doesn't contain the term. Thus, its coefficient is 0.

      Thus, the sum of any two 0-1 polynomials will be a 0-1 polynomial. Since multiplication is repeated addition, the product of two 0-1 polynomials will be a 0-1 polynomial as well. Now consider the addition of two F_2(x) polynomials, $\frac{a(x)}{b(x)}$ and $\frac{c(x)}{d(x)}$. The numerator is ((a(x)*d(x)) + (c(x)*b(x))). Since we have already proven that addition and multiplication of two 0-1 polynomials lead to 0-1 polynomials, the numerator is a 0-1 polynomial.
      Similarly, the denominator b(x)*d(x) is a 0-1 polynomial.
      Thus, the addition of two F_2(x) numbers results in another member of F_2(x).
    * Consider $\frac{a(x)}{b(x)}$, $\frac{c(x)}{d(x)}$ and $\frac{e(x)}{f(x)}$.
      $\frac{a(x)}{b(x)} + (\frac{c(x)}{d(x)} + \frac{e(x)}{f(x)}) = \frac{a(x)*d(x)*f(x)+c(x)*b(x)*f(x)+e(x)*d(x)*b(x)}{f(x)*d(x)*b(x)}$.

$(\frac{a(x)}{b(x)} + \frac{c(x)}{d(x)}) + \frac{e(x)}{f(x)}$ upon expansion gives the same.
Hence, axiom 2 is satisfied.

* Third axiom is satisfied with the additive identity 0 where 0 denotes the 0-1 polynomial with all coefficients= 0 divided by q(x) with the constant term 1.
* For every number in F_2(x), adding the number to itself produces 0.
* Consider two numbers $\frac{a(x)}{b(x)}$ and $\frac{c(x)}{d(x)}$
$(\frac{a(x)}{b(x)}) + (\frac{c(x)}{d(x)}) = \frac{a(x)*d(x)+b(x)*c(x)}{d(x)*b(x)}$
$(\frac{c(x)}{d(x)}) + (\frac{a(x)}{b(x)}) = \frac{b(x)*c(x)+a(x)*d(x)}{d(x)*b(x)}$
Using the cases in the first axiom, we can prove that the addition of two 0-1 polynomials is commutative. Similarly, multiplication is commutative as well.
Thus, fifth axiom is satisfied for F_2(x) polynomials.

– Axioms of Multiplication

* Consider $\frac{a(x)}{b(x)}$ and $\frac{c(x)}{d(x)}$. $*(\frac{a(x)}{b(x)}, \frac{c(x)}{d(x)}) = \frac{a(x)*c(x)}{b(x)*d(x)}$
We have already proven that both the denominator and the numerator will be 0-1 polynomials.
Thus, first axiom is satisfied.
* Consider $\frac{a(x)}{b(x)}$, $\frac{c(x)}{d(x)}$ and $\frac{e(x)}{f(x)}$.
$\frac{a(x)}{b(x)} * (\frac{c(x)}{d(x)} * \frac{e(x)}{f(x)}) = \frac{a(x)}{b(x)} * (\frac{c(x)*e(x)}{d(x)*f(x)}) = \frac{a(x)*c(x)*e(x)}{b(x)*d(x)*f(x)}$
$(\frac{a(x)}{b(x)} * \frac{c(x)}{d(x)}) * \frac{e(x)}{f(x)}$ upon expansion produces the same.
Thus, second axiom is satisfied.
* Third axiom is satisfied for the multiplicative identity being 1, where 1 is obtained when the numerator is the 0-1 polynomial which has the same 0-1 non-zero polynomials as both the numerator and the denominator.
* for every element in F_2(x) of the form $\frac{a(x)}{b(x)}$ where a(x) and b(x) are 0-1 polynomials, consider $\frac{b(x)}{a(x)}$.
Hence, $*(\frac{a(x)}{b(x)}, \frac{b(x)}{a(x)})$=1, where 1 is as defined above.
* $\forall \frac{a(x)}{b(x)}, \frac{c(x)}{d(x)} \in F_2$(x), $*(\frac{a(x)}{b(x)}, \frac{c(x)}{d(x)}) = \frac{a(x)*c(x)}{b(x)*d(x)} = \frac{c(x)*a(x)}{d(x)*b(x)} = *(\frac{c(x)}{d(x)}, \frac{a(x)}{b(x)})$
Hence, the fifth axiom is satisfied.

– Axioms of Addition and Multiplication

* We have already proven that the axioms of addition are satisfied.
* We have already proven that the axioms of multiplication are satisfied.
* $\forall \frac{a(x)}{b(x)}, \frac{c(x)}{d(x)}, \frac{e(x)}{f(x)} \in F_2$(x),:
$\frac{a(x)}{b(x)} * (\frac{c(x)}{d(x)} + \frac{e(x)}{f(x)}) = \frac{a(x)}{b(x)} * (\frac{c(x)*f(x)+e(x)*d(x)}{d(x)*f(x)}) = \frac{c(x)*f(x)*a(x)+e(x)*d(x)*a(x)}{d(x)*f(x)*b(x)}$
$= \frac{a(x)*c(x)}{b(x)*d(x)} + \frac{a(x)*e(x)}{b(x)*f(x)} = \frac{a(x)}{b(x)} * \frac{c(x)}{d(x)} + \frac{a(x)}{b(x)} * \frac{e(x)}{f(x)}$
Thus, the axiom is satisfied.

F_2(x) represents a set of numbers.

- Show that there is a bijection between rational numbers $\mathbb{Q}$ and $F_2(x)$.
  Ans.
  Case 1: $\mathbb{Q} \mapsto F_2(x)$
  We have already proven that $\mathbb{Q}$ and $\mathbb{N}$ have the same cardinality, i.e. there is a one-one function from $\mathbb{Q}$ to N.
  The example of one such function is :
  For any rational number of the form $\frac{m}{n}$, let the corresponding map to $\mathbb{N}$ be $2^m 3^n 5^p$, where p is 0 or 1 depending on whether the rational is $\leq$ or > 0.
  Then the image in F_2(x) can be any number of the form $\frac{p(x)}{q(x)}$ where q(x) just is the constant 1, while p(x) has the coefficient of the map on $\mathbb{N}$ as 1, while the other coefficients are 0.
  Clearly, since each rational number produces a unique natural number, it will produce a corresponding unique p(x).
  We thus get a one-one function.

  Case 2: $F_2(x) \mapsto \mathbb{Q}$
  Consider and $\frac{p(x)}{q(x)} \in F_2$(x).
  Construct a map as follows-
  For any the $(i+1)^{th}$ position in $\mathbb{Q}$:

  - Consider it 1 if both p(x) and q(x) have coefficient of x^i as 0.
  - Consider it 2 if p(x) has coefficient of x^i 1 and coefficient of x^i in q(x) is 0.
  - Consider it 3 if q(x) has coefficient of x^i 1 and coefficient of x^i in p(x) is 0.
  - Consider it 4 if both p(x) and q(x) have coefficient of x^i as 1.

  This process is made to continue till we reach the largest i in p(x) and q(x).

  Since we can define a one-one map from $\mathbb{Q}$ to F_2(x) and vice-versa, by Cantor-Bernstein-Schroeder theorem, there is a bijection between the two.

- Show that there is no isomorphism between $\mathbb{Q}$ and $F_2(x)$.
  Ans.
  Let there be an isomorphism between $\mathbb{Q}$ and $F_2(x)$. We have already proven the symmtery of isomorphisms. Thus, there is an isomorphism from $F_2(x)$ to $\mathbb{Q}$. For any number in F_2(x), the number is its own inverse.
  Let the number be a.
  Then, h(a $+_1$ a) = h(0_1) = h(a) $+_2$ h(a) = 0_2.
  Now, h(a) is a rational number. Adding h(a) to itself is producing 0.
  Thus, $\forall a \in F_2$(x), h(a) = 0.
  But this implies h is not one-one. Thus, we arrive at a contradiction.
  There is no isomorphism 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.

  Ans.
  To prove that $(\mathbb{Z}, +, *)$ is a set of numbers without division, we need to show that it satisfies the axioms of addition, multiplication and addition and multiplication taking place together.

  - Axioms of Addition: Since 0 was originally a part of (N, +) and no changes are made to the axioms as well, all the axioms of addition are satisfied in the same way as before.
    - $\forall$a,b $\in (\mathbb{Z}, +, *)$, a+b $\in (\mathbb{Z}, +, *)$
    - $\forall$a,b,c $\in (\mathbb{Z}, +, *)$, a+(b+c) = (a+b)+c
    - 0$\in(\mathbb{Z}, +, *)$. For all integers a, a+0=a
    - $\forall$a$\in\mathbb{Z}$, $\exists$ (-a) such that +(a, -a)=0
    - $\forall$a,b$\in\mathbb{Z}$, a+b = b+a
  - Axioms of Multiplication: For all members of $\mathbb{Z}$ apart from 0, the remaining 4 axioms of multiplication are satisfied as they were before. Only multiplication of 0 can now be explicitly defined. $\forall$a$\in\mathbb{Z}$, Consider a*(0+0). Since 0 was already included in the set of numbers while defining addition and multiplication taking place together, the third axiom is satisfied. Thus,a*0 = a*(0+0) = a*0 + a*0 $\forall$a$\in\mathbb{Z}$, a*0 = 0.
    - $\forall$a,b$\in\mathbb{Z}$, *(a,b)$\in\mathbb{Z}$. This was already true for all a,b$\neq$0. If a or b=0 , the final product will be 0, which belongs to $\mathbb{Z}$.
    - $\forall$a,b,c$\in\mathbb{Z}$, a*(b*c)=(a*b)*c This was already true $\forall$a,b,c$\in\mathbb{Z}$ when a,b,c$\neq$0. If suppose any one of a,b,c is 0, the final product in both the cases will be 0. Thus, the second axiom is satisfied.
    - As before, $\forall$a$\in\mathbb{Z}$, *(a,1)=a
    - As before, $\forall$a,b$\in\mathbb{Z}$, *(a,b) = *(b,a) This was already proven when a,b$\neq$0. If either of a,b is 0, then the final product is 0 which proves this axiom.
  - Axioms of Addition and Multiplication: These are satisfied as they were before.
    - Axioms of addition are satisfied as proven above.
    - Axioms of multiplication are satisfied as proven above.
    - $\forall$a,b,c$\in\mathbb{Z}$, a*(b+c)= a*b + a*c.

  Thus, $\mathbb{Z}$ is a set of numbers without division.

Such 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 $a * b = 0$.

  Ans.
  Consider the map of natural numbers created in Q8.
  Consider A⊆ℕ such that A = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}.
  Define (A,+) as ∀a,b∈A, +(a,b) = (a +' b) mod 10, where +' is the usual addition of N.
  Define (A,*) as ∀a,b∈B, *(a,b) = (a *' b) mod 10, where *' is the usual multiplication of N.
  Since 0∈A, division is not defined on A.
  However, consider a=2 and b=5.
  a * b = (2 *' 5) mod 10 = 10 mod 10 = 0.
  Hence, in this set of numbers without division, we get a, b such that a, b≠0, yet a∗b= 0.

- There is a set of numbers without division $(N, +, *)$ such that there is $a \in N$, $a \neq 0$, but $a^3 = a * a * a = 0$.

  Ans.
  Consider the map of natural numbers created in Q8.
  Consider B⊆ℕ such that B = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26}.
  Define (B,+) as ∀a,b∈B, +(a,b) = (a +' b) mod 27, where +' is the usual addition of N.
  Define (B,*) as ∀a,b∈B, *(a,b) = (a *' b) mod 27, where *' is the usual multiplication of N.
  Since 0∈B, division is not defined on B.
  However, consider a=3.
  We have already proven that operation of the type (a *' b) mod p is associative.
  Thus, a * a * a = ((a *' a) mod 27) * a = ((3 *' 3) mod 27) * 3 = 9 * 3 = (9 *' 3) mod 27 = 0.
  Hence, in this set of numbers without division, we get a such that a≠0, yet a∗a∗a= 0.

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