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.

Consider the set $\{U\}$ where U is the universal set. Now, by Axiom of regularity $(\forall x \neq \phi, \exists y \in x : y \cap x = \phi)$
$\implies \exists a \in \{U\} : a \cap \{U\} = \phi$, but the only element in $\{U\}$ is U and $U \cap U = \phi$ is a contradiction.
Hence such a universal set U cannot exist as per the Zermalo Fraenkel Axioms. □

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 $V \in V$?".

We have two cases:

1. $V \in V$: According to the definition of V, V contains sets which do not contain themselves and hence $V \notin V$
2. $V \notin V$: Again, since V is a set which does not contain itself, $V \in V$ according to the definition of V

We have contradiction in both the 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.

Suppose on the contrary there are two numbers 0_m and 0_n satisfying the third axiom. We have

$0_m = 0_m + 0_n = 0_n$ by the second axiom.
$\therefore$ There is a unique 0 satisfying fourth axiom.

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

Assuming there are two numbers b_1, b_2 satisfying fourth axiom for every $a \in \mathbb{N}$
$\implies$

$$\begin{aligned} b_1 &= 0 + b_1 \\ &= (a + b_2) + b_1 \\ &= a + (b_2 + b_1) \\ &= (a + b_1) + b_2 \\ &= 0 + b_2 \\ &= b_2 \end{aligned}$$

□

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

$k \overset{\text{def}}{:=} -(b - a) \implies b - a + k = 0$

$$\begin{aligned} \implies a - b &= a - b + 0 \\ &= a - b + b - a + k \\ &= k \\ &= -(b - a) \end{aligned}$$

□

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 $1 = 0$.

By fourth axiom for $(N,*)$, for $0 \in N, \exists b \in N$ such that $0 * b = 1$
LEMMA : For $a \in N, 0*a = 0*a+0 = 0*a+0*a+(-0*a) = (0+0)*a+(-0*a) = 0*a+(-0*a) = 0$
By third axiom, $0 = 0*b = 1 \implies 0 = 1$ □

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.

  - $(N_1, \oplus, \wedge) = \{0,1\}$: Addition defined as $\oplus$ (XOR operation), while multiplication defined as $\wedge$ (AND operation)
  - $(N_2, +, *) = \{0,1,2\}$: Addition defined as usual addition mod 3, Multiplication mod 3

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.

Consider the set of numbers $N_k = \{0,1,2,...,k-1\} \subseteq \mathbb{N}$ with $|N| = k$, where k is a prime, and addition defined as $\forall a,b \in N, a +_n b = (a+b) \mod k$ and multiplication as $a *_n b = (a*b) \mod k$
(Modular inverse exists for $ab \equiv 1 \mod k$ when k is prime)

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.

We first prove that $a*b = 0$ iff atleast either of them is 0. Consider (assuming $a \neq 0, b \neq 0$ $a*(b+1) = a*b+a*1 = a*1 = a \implies b+1 = 1$ (contradiction Let us assume the multiplicity to be a composite number. We can factor the composite number into smaller prime factors (i.e. taking sum of $1'$s that many times) and we claim that the sum is 0.

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

We consider the set $M = 0, 1, S(1), S(S(1)), ...$ where $S(x)$ can be defined as a Successor function, with $S(0) = 1$ and $S(\underbrace{1+1+\cdots+1}_{k \text{ times}}) = \underbrace{S(S(...(S(1))))}_{k \text{ times}}$ Now, since multiplicity is 0, the series $1+1+1+...$ does not sum to 0 i.e. M is indeed $\mathbb{N}$. Evidently, $\mathbb{N} \in N$

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

Let us assume $\underbrace{a+a+\cdots+a}_{k \text{ times}} = \underbrace{(a*1)+(a*1)+\cdots+(a*1)}_{k \text{ times}} = a*(\underbrace{1+1+\cdots+1}_{k \text{ times}}) = a*k$

(Using the definition of Successor function)

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.

  - *Reflexive* :
    For some set of numbers $(N, +_s, *_s)$,
    Consider the identity function $S(x) = x$ from $N \mapsto N$
    $\forall a, b \in N, S(a +_s b) = a +_s b = S(a) +_s S(b)$
    $S(a *_s b) = a *_s b = S(a) *_s S(b)$
    (S is an isomorphism)

  - *Symmetric* :
    Consider an isomorphism T on the sets of numbers $N_1 \mapsto N_2$
    $\implies \forall a, b \in N_1$
    $T(a +_1 b) = T(a) +_2 T(b)$
    $T(a *_1 b) = T(a) *_2 T(b)$
    Now, Since T is a bijection, T^{-1} is also a bijection and satisfies the following:
    $T^{-1}(a +_2 b) = a +_1 b = T^{-1}(T(a)) +_1 T^{-1}(T(b))$
    $T^{-1}(a *_2 b) = a *_1 b = T^{-1}(T(a)) *_1 T^{-1}(T(a))$
    Hence, T^{-1} is also an isomorphism.

  - *Transitive* :
    Consider an Isomorphism $P : N_1 \mapsto N_2$, and $Q : N_2 \mapsto N_3$. Now, the composite function $Q \circ P$ is a bijection from $N_1 \mapsto N_3$
    $\forall a, b \in N_1, P(a +_1 b) = P(a) +_2 P(b)$
    $\forall c, d \in N_2, \in \mathbb{N}_2, Q(c +_2 d) = Q(c) +_3 Q(d)$
    Now, $\forall a, b \in N_1, Q(P(a +_1 b)) = Q(P(a) +_2 P(b)) = Q(P(a)) +_3 Q(P(b))$
    $\implies Q \circ P$ is an isomorphism.

  Hence, Isomorphism is an equivalence relation on the set of all sets of numbers. □

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

$$\begin{aligned}
0_2 &= h(a) +_2 (-h(a)) \\
&= h(a +_1 0_1) + (-h(a)) \\
&= h(a) +_2 h(0_1) +_2 (-h(a)) \\
&= h(0_1) +_2 h(a) +_2 (-h(a)) \\
&= h(0_1)
\end{aligned}$$

$$\begin{aligned}
1_2 &= h(a) *_2 (h(a)^{-1}) \\
&= h(a *_1 1_1) * (h(a)^{-1}) \\
&= h(a) *_2 h(1_1) *_2 (h(a)^{-1}) \\
&= h(1_1) *_2 h(a) *_2 (h(a)^{-1}) \\
&= h(1_1)
\end{aligned}$$

□

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

$-_2 h(b) =$
$-_2\ h(b) + 0_2 = h(b) +_2 (-_2 h(b)) +_2 (-_2 h(b)) = 0_2 +_2 (-_2 h(b)) = h(0_1) +_2 (-_2 h(b)) = h(b +_1 (-_1 b)) +_2 (-_2(h(b))) = h(b) +_2 (-_2(h(b))) +_2 h(-_1 b) = 0_2 + h(-_1 b)$
$= h(-_1 b)$
Similarly, $h(b^{-1}) = (h(b))^{-1}$

$$\begin{aligned}
h(a -_1 b) &= h(a +_1 (-_1 b)) \\
&= h(a) +_2 h(-_1 b) \\
&= h(a) +_2 (-_2 h(b) \\
&= h(a) -_2 h(b)
\end{aligned}$$

$$\begin{aligned}
h(a/_1 b) &= h(a *_1 (b^{-1})) \\
&= h(a) *_2 h(b^{-1}) \\
&= h(a) *_2 (h(b))^{-1} \\
&= h(a)/_2 h(b)
\end{aligned}$$

□

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.

- We define a set $F_2(x)$ which 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. Show that $F_2(x)$ is a set of numbers.

We can define addition as $p(x)/q(x) + r(x)/s(x) = (p(x) * s(x) + r(x) * q(x))/(q(x) * s(x))$ and multiplication as $p(x)/q(x) * r(x)/s(x) = (p(x) * r(x))/(q(x) * s(x))$. Evidently, these numbers are in the form $m(x)/n(x)$ and hence they lie in $F_2(x)$. Other axioms can be verified accordingly.

- Show that there is a bijection between rational numbers $\mathbb{Q}$ and $F_2(x)$.

For the 0-1 polynomials $p(x)$ and $q(x)$ we can define $r = 0.a_0b_0a_1b_1a_2b_2...$ where a_i, b_i are the coefficients of x_i in $p(x), q(x)$ respectively.
Thus, we have a one-one mapping from $F_2(x) \mapsto \mathbb{Q}$
Now, consider a rational number $\frac{m}{n}$ in the reduced form, with $n \neq 0$. We can write the binary representations of m and n and construct a polynomial $p(x)$ such that coefficients $c_i, i = 2k, (k = 0, 1, ...)$ are the coefficients in binary representation of m. Similarly, $c_i, i = 2k + 1, (k = 0, 1, ...)$ correspond to those of n, We can set $q(x) = 1$ in this case
For accomodating negative rationals $-\frac{m}{n} : m, n > 0$, we can set $p(x) = 1$ and define $q(x)$ as we defined $p(x)$ above.
Thus, we have a one-one mapping from $\mathbb{Q} \to F_2(x)$
By CANTOR-BERNSTEIN-SCHROEDER theorem, we can have a bijection $R : F_2(x) \mapsto \mathbb{Q}$

- Show that there is no isomorphism between $\mathbb{Q}$ and $F_2(x)$.

Assuming there is an isomorphism h between Q and $F_2(x)$. If we have two polynomials $p(x)$ and $q(x)$, Consider $h(p(x) + p(x)) = 0 = h(q(x) + q(x))$ since $x^i + x^i = 0$. Hence h does not remain one-one. So, there does not exist an isomorphism between 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.

It can be easily verified that $\mathbb{Z}$ follows other axioms. $2 \in \mathbb{Z}$ but there does not exist a $k \in \mathbb{Z}$ such that $2 * k = 1$ (Contradiction to axiom 4)

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 $a * b = 0$.

Consider the set of numbers N_k as defined earlier.
For some $k = 2m$, we can have $2 * m = 2 *_n m = (2 * m) \mod k = k \mod k = 0$

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

Similarly, for some $k = a^3$, We can have $a^3 = a *_n a *_n a = (a^2 * a_n) \mod k = a^3 \mod k = 0$

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