CS201 Assignment 1: The Concept of Numbers

Dhruv Gupta (220361)

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.
  solution 1
  Proof: Assume U is a set. By definition, U is a collection of all sets so U is an element of itself, i.e., $U \in U$. By Axiom of Separation, we can define a set

  $$W = \{x \mid x \in U, x = U\}.$$

  Clearly, $W = \{U\}$. Now by Axiom of Regularity on W, $U \cap W = \phi$ (Because U is the only element in W, this must be true). But since $U \in U$, $W \subseteq U$. Therefore $U \cap W \neq \phi$, which is a contradiction. Hence, U cannot be a set as per 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 $V \in V$?".
  solution 2
  Proof: Clearly, V is defined as a set of all sets which do not belong to themselves. If $V \in V$, then by definition of V, $V \notin V$ which is a contradiction. And if $V \notin V$, again by definition of V, $V \in V$, again we get a contradiction.

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.
  solution 3
  Proof: Suppose there exist $y_1, y_2 \in N$ *with* $y_1 \neq y_2$ *such that for all* $a \in N$, $y_1 + a = a + y_1 = a$ *and* $y_2 + a = a + y_2 = a$.
  Now since $a + y_1 = a$ *for all* $a \in N$, *put* $a = y_2$.

$$y_2 + y_1 = y_2 \tag{1}$$

  Similarly, from $y_2 + a = a$, *on putting* $a = y_1$, *we get*

$$y_2 + y_1 = y_1 \tag{2}$$

  From (1) *and* (2) *clearly,* $y_1 = y_2$, *which is a contradiction. Hence, there is a unique number satisfying third axiom, and we are representing that number by 0.*

- For every $a \in N$, there is a unique b satisfying fourth axiom.
  solution 4
  Proof: Suppose there exist $b, c \in N$*, such that* $b \neq c, a+b = 0$ *and* $a+c = 0$*.*
  Now

$$c = 0 + c = (a + b) + c = (b + a) + c = b + (a + c) = b + 0 = b \qquad (3)$$

  (Using Axioms 2, 3 and 5)
  This is clearly a contradiction. Hence such a b is unique.

- Define $-a$ to be the number such that $a + (-a) = 0$. For every $a, b \in N$, $a - b = -(b - a)$.
  solution 5
  Proof:
  Claim: $a + (-b) = a - b$, *where* $a, b \in N$.
  Proof for claim: By definition of subtraction, $a - b = a + c$, *such that* $b + c = 0$, *for some* $c \in N$. *Also* $b + (-b) = 0$. *But since such* $-b$ *must be unique,* $c = (-b)$. *Substitute this in first equation to get* $a - b = a + (-b)$.
  Note: From Axioms 2 and 5, it clearly follows that order of addition of numbers does not matter.
  $(a + b) + c = a + (b + c) = a + (c + b) = (a + c) + b$. *Similarly we can extend it to more than three numbers.*
  Now, let $p = a - b, q = b - a, r = -(b - a)$. *Note that* $q + r = 0$.
  $p = p + 0$
  $= p + (q + r)$
  $= (p + q) + r$
  $= ((a - b) + (b - a)) + r$
  $= (a + (-b) + b + (-a)) + r$
  $= ((a + (-a)) + (b + (-b))) + r$
  $= (0 + 0) + r$
  $= 0 + r$
  $= r.$
  or $a - b = -(b - a)$. *Hence proved.*

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 $1 = 0$.
  solution 6
  Proof: Consider the definition of division analogous to subtraction: For all $a, b \in N$, there exists $c \in N$, such that $a/b = a * c$, and $b * c = 1$. If $0 \in N$, put $a = 1$ and $b = 0$. $1/0 = 1 * c$, for some c, such that $0 * c = 1$. Now,
  $0 = c + (-c)$
  $= c * 1 + (-c)$
  $= c * (0 + 1) + (-c)$
  $= c * 0 + c * 1 + (-c)$
  $= 0 * c + c + (-c)$
  $= 1 + 0$
  $= 1$, *or* $1 = 0$.

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.
  solution 7

1. *Consider a set* $P = \{(a, b) \mid a, b \in \mathbb{R}\}$.
   Define addition on P *as*

$$(a, b)\#(c, d) = (a + c, b + d) \tag{4}$$

   where $'+'$ *denotes the usual addition defined on* $\mathbb{R}$.

   (a) $((a, b)\#(c, d))\#(e, f) = (a + c, b + d)\#(e, f) = ((a + c) + e, (b + d) + f) = (a + (c + e), b + (d + f)) = (a, b)\#(c + e, d + f) = (a, b)\#((c, d)\#(e, f))$ *for all* $(a, b), (c, d), (e, f) \in P$.
   (b) We have $(0, 0) \in P$, *such that* $(a, b)\#(0, 0) = (a + 0, b + 0) = (a, b) = (0 + a, 0 + b) = (0, 0)\#(a, b)$ *for all* $(a, b) \in P$.
   (c) For all $(a, b) \in P$ *we have* $(-a, -b) \in P$ *such that* $(a, b)\#(-a, -b) = (a+(-a), b+(-b)) = (0, 0) = ((-a)+a, (-b)+b) = (-a, -b)\#(a, b)$.
   (d) $(a, b)\#(c, d) = (a + c, b + d) = (c + a, d + b) = (c, d)\#(a, b)$ *for all* $(a, b), (c, d) \in P$.

   Define multiplication on $P\backslash\{(0, 0)\}$ *as*

$$(a, b)\$(c, d) = (a * b, c * d) \tag{5}$$

   where $'*'$ *denotes the usual multiplication defined on* $\mathbb{R}$

   (a) $((a, b)\$(c, d))\$(e, f) = (a*c, b*d)\$(e, f) = ((a*c)*e, (b*d*f) = (a*(c*e), b*(d*f)) = (a, b)\$(c*e, d*f) = (a, b)\$((c, d)\$(e, f))$ *for all* $(a, b), (c, d), (e, f) \in P$.
   (b) We have $(1, 1) \in P$, *such that* $(a, b)\$(1, 1) = (a * 1, b * 1) = (a, b) = (1 * a, 1 * b) = (1, 1)\#(a, b)$ *for all* $(a, b) \in P$.
   (c) For all $a, b \in \mathbb{R}\backslash\{0\}$ *there exist* $c, d \in \mathbb{R}\backslash\{0\}$, *such that* $a * c = 1$ *and* $b * d = 1$. *So, for all* $(a, b) \in P\backslash\{0\}$ *we have* $(c, d) \in P\backslash\{0\}$ *such that* $(a, b)\$(c, d) = (a * c, b * d) = (1, 1) = (c * a, d * b) = (c, d)\$(a, b)$.
   (d) $(a, b)\$(c, d) = (a * c, b * d) = (c * a, d * b) = (c, d)\$(a, b)$ *for all* $(a, b), (c, d) \in P$.

   Therefore,
   $(P, \#)$ *is a set of numbers with addition.*
   $(P\backslash\{0\}, \$)$ *is a set of numbers with multiplication.*
   For all $(a, b), (c, d), (e, f) \in P$, $(a + b)\$((c, d)\#(e, f)) = (a + b)\$(c +$

$e, d+f) = (a*(c+e), b*(d+f)) = (a*c+a*e, b*d+b*f) = (a*c, b*d)\#(a*e, b*f) = ((a,b)\$(c,d))\#((a,b)\$(e,f))$.
Hence, $(P, \#, \$)$ *is a set of numbers with addition and multiplication.*

2. *Consider a set* $Q = \{0,1,2\} \subseteq \mathbb{N}$
Define addition as $a\&b = (a+b) \ (mod\ 3)$*, for all* $a, b \in Q$*, where* $'+'$ *is the usual addition defined on* $\mathbb{N}$.

   (a) $(a\&b)\&c = (((a+b) \ (mod\ 3)) + c) \ (mod\ 3) = (a+b) \ (mod\ 3) + c \ (mod\ 3) = ((a+b)+c) \ (mod\ 3) = (a+(b+c)) \ (mod\ 3) = a \ (mod\ 3) + (b+c) \ (mod\ 3) = (a+(b+c) \ (mod\ 3)) \ (mod\ 3) = a\&(b\&c)$ *for all* $a, b, c \in Q$.
   (b) *We have* $0 \in Q$ *such that* $0\&a = (0+a) \ (mod\ 3) = a \ (mod\ 3) = a = (a+0) \ (mod\ 3) = a\&0$ *for all* $a \in Q = \{0,1,2\}$.
   (c) *Note that*
   $0\&0 = (0+0) \ (mod\ 3) = 0 \ (mod\ 3) = 0$
   $1\&2 = (1+2) \ (mod\ 3) = 3 \ (mod\ 3) = 0$
   $2\&1 = (2+1) \ (mod\ 3) = 3 \ (mod\ 3) = 0$
   Hence for every element $a \in Q$ *we have* $a\ b \in Q$ *such that* $a\&b = 0$.
   (d) $a\&b = (a+b) \ (mod\ 3) = (b+a) \ (mod\ 3) = b\&a$

   Define multiplication as $a : b = a * b \ (mod\ 3)$*, for all* $a, b \in Q\backslash\{0\}$*, where* $'*'$ *is the usual multiplication defined on* $\mathbb{N}$.

   (a) $(a:b):c = (((a*b) \ (mod\ 3))*c) \ (mod\ 3) = ((a*b)*c) \ (mod\ 3) = (a*(b*c)) \ (mod\ 3) = (a*((b+c) \ (mod\ 3))) \ (mod\ 3) = a : (b:c)$ *for all* $a, b, c \in Q$.
   (b) *Note that we have* $1 \in Q\backslash\{0\}$ *such that* $1 : a = (1*a) \ (mod\ 3) = a \ (mod\ 3) = (a*1) \ (mod\ 3) = a : 1$ *for all* $a \in Q\backslash\{0\}$.
   (c) *Note that*
   $1 : 1 = (1*1) \ (mod\ 3) = 1 \ (mod\ 3) = 1$
   $2 : 2 = (2*2) \ (mod\ 3) = 4 \ (mod\ 3) = 1$
   Hence for every element $a \in Q\backslash\{0\}$ *we have* $a\ b \in Q\backslash\{0\}$ *such that* $a : b = 1$.
   (d) $a : b = (a*b) \ (mod\ 3) = (b*a) \ (mod\ 3) = b : a$ *for all* $a, b \in Q\backslash\{0\}$.

   Therefore,
   $(Q, \&)$ *is a set of numbers with addition.*
   $(P\backslash\{0\}, :)$ *is a set of numbers with multiplication.*
   For all $a, b, c \in Q$, $a : (b\&c) = (a*(b\&c)) \ (mod\ 3) = (a*((b+c) \ (mod\ 3)) = (a*(b+c)) \ (mod\ 3) = (a*b+a*c) \ (mod\ 3) = ((a*b) \ (mod\ 3) + (a*c) \ (mod\ 3)) \ (mod\ 3) = (a:b)\&(a:c)$.
   Hence, $(Q, \&, :)$ *is a set of numbers with addition and multiplication.*

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.
  solution 8
  Proof: In solution of previous question we have defined a set of numbers $(Q, \&, :)$ *where* Q *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.
  solution 9
  Proof: If no such k exists, then multiplicity is 0*. So now we need to prove that if such a k exists it must be prime. Assume contrary that k is not prime. Now, if* $k = 1$*, we get* $1 = 0$*, which is clearly nor possible. So,* $k \neq 1$*. Let* $k = a * b$*, where* $a \neq 1, b \neq 1$*. Then,*
  $0 = \underbrace{1+1+\cdots+1}_{k \text{ times}} = \underbrace{1+1+\cdots+1}_{a*b \text{ times}}$
  $= (\underbrace{1+1+\cdots+1}_{a \text{ times}}) * (\underbrace{1+1+\cdots+1}_{b \text{ times}}) \in N$
  Because $(\underbrace{1+1+\cdots+1}_{j \text{ times}}) \in N$*, for any value of* j *and also* $p * q \in N$*, for all* $p, q \in N$*. This would mean that* $0 \in N$*, which is a contradiction. Hence* k *must be prime. Therefore, multiplicity is either* 0 *or a prime number.*

- Any set of numbers $(N, +, *)$ of multiplicity 0 contains $\mathbb{N}$.
  solution 10
  Proof: To prove this we will construct a subset of N which follows Peano's Axioms. Such a set will be a set of natural numbers contained by N.
  Consider set $D = \{0\} \cup \{n_k = (1+1+1+...(k\ times)) \mid k \neq 0\}$. Clearly, D is a subset of N.

  1. *Claim 1: All elements of D are distinct. Since multiplicity of $(N, +, *)$ is 0, $(1+1+1+...(k\ times)) \neq 0$ for any k. Hence 0 is a distinct number. Now, suppose there exist $u \neq v$ such that $n_u = n_v$. Without loss of generality, let $u > v$. Then we can write $n_u = n_v + n_{u-v} \implies n_v = n_v + n_{u-v}$. Now it follows from solution 3 that $n_{u-v} = 0$ which implies multiplicity is $u - v \neq 0$. This is a contradiction. Hence no such u, v exist. Hence all elements of D are distinct.*
  2. *Clearly, $0 \in D$.*
  3. *Define successor map as $S : D \mapsto D$ as $S(x) = x + 1$.*
  4. *Claim 2: $0 \notin range(S)$. Clearly, $S(0) = 0+1 = 1 \neq 0$. Also, for any $x = n_k \in D$, $S(x) = S(n_k) = n_k + 1 = (1+1+1+...(k\ times))+1 = (1+1+1+....(k+1\ times) = n_{k+1} \neq 0$. Hence, $S(x) \neq 0$ for any $x \in D$. Hence $0 \notin range(S)$.*
  5. *Claim 3: S is a one-one mapping. For any $n_a, n_b \in D$, $S(n_a) = S(n_b) \implies n_a + 1 = n_b + 1 \implies n_a = n_b$ (By Claim 1) $\implies a = b \implies n_a = n_b$. Hence S is one-one.*
  6. *Consider any set A such that $0 \in A$ and for all $x \in A \cap D$, $S(x) \in A$. Proof by Induction*
     Let us define $n_0 = 0 \in D$ and clearly $n_0 \in A \cap D \subseteq A$. $n_0 \in A \cap D \implies S(n_0) = 1 = n_1 \in A$ (Base Case, $k = 1$)
     Assume $n_k \in A$. Obviously, $n_k \in D$, therefore $n_k \in A \cap D \implies S(n_k) \in A \implies n_k + 1 \in A \implies n_{k+1} \in A$.
     Hence by induction, $n_k \in A$ for all k. Hence $D \subseteq A$. Therefore, for any set A if $0 \in A$ and for all $x \in A \cap D$, $S(x) \in A$ then $D \subseteq A$. So we have proved that D follows all Peano's Axioms, hence D is a set of natural numbers. Therefore, any set of numbers $(N, +, *)$ contains a set of natural numbers.

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

  solution 11
  Proof: Since D is also a set of natural numbers, we can consider D and $\mathbb{N}$ as equivalent. Hence, n_k is equivalent to k for any k. So we can take $k = 1 + 1 + 1 + ...(k\ times)$
  $k*a = (\underbrace{1 + 1 + \cdots + 1}_{k\ times}) * a = (\underbrace{1 * a + 1 * a + \cdots + 1 * a}_{k\ times}) = \underbrace{a + a + \cdots + a}_{k\ times}$
  $n_k * a = (1+1+1+...(k\ times)) * a = (1*a+1*a+1*a+...(k\ times)) = \underbrace{a + a + \cdots + a}_{k\ times}$.

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.
  solution 12
  Proof: Let $S = \{(N, +, *) \mid N$ *is a set of numbers with addition* $'+'$ *and multiplication* $'*'$ *defined* $\}$
  Relation R is given by $(N_1, +_1, *_1)\, R\, (N_2, +_2, *_2) \implies a$ and b have an isomorphism h, where $N_1, N_2 \in S$. We need to prove that the relation R on S is equivalence relation. So we need to prove it to be reflexive, symmetric and transitive.

  1. For reflexive we need to prove$(N, +, *)\, R\, (N, +, *)$ for all $(N, +, *) \in S$.
     Consider any $(N, +, *) \in S$. Consider a map $h : N \mapsto N$, defined as $h(x) = x$, for all $x \in N$. Now, for any $a, b \in N$, $h(a) = h(b) \implies a = b$, hence h is one-one. Also, for every $a \in N$, we have $\alpha \in N$ such that $h(\alpha) = a$, and that α is same as a . So, h is also onto. Hence h is a bijection. Now, for all $a, b \in N$, $h(a + b) = a + b = h(a) + h(b)$ and $h(a * b) = a * b = h(a) * h(b)$ [Since $h(a) = a$ and $h(b) = b$].
     Therefore, h is an isomorphism. Hence we have proved that there is an isomorphism h between $(N, +, *)$ and $(N, +, *)$, i.e., $(N, +, *)R(N, +, *)$ and this is true for all $(N, +, *) \in S$. Therefore, R is reflexive.
  2. For symmetric we need to prove if $(N_1, +_1, *_1)\, R\, (N_2, +_2, *_2)$ then $(N_2, +_2, *_2)\, R\, (N_1, +_1, *_1)$.
     Take any $(N_1, +_1, *_1), (N_2, +_2, *_2) \in S$, such that $(N_1, +_1, *_1)R(N_2, +_2, *_2)$, i.e., an isomorphism h exists between $(N_1, +_1, *_1)$ and $(N_2, +_2, *_2)$.
     h is an isomorphism, so it is a bijection, so its inverse exists. Let that inverse be g. We know that inverse of a bijection is also a bijection, so $g : N_2 \mapsto N_1$ is a bijection.
     Now, h is a bijection so for all $a, b \in N_2$, there exist $\alpha, \beta \in N_1$ such that $h(\alpha) = a$ and $h(\beta) = b$. Also since g is inverse of h, $g(a) = \alpha$ and $g(b) = \beta$.
     $g(a +_2 b) = g(h(\alpha) +_2 h(\beta))$
     $= g(h(\alpha +_1 \beta))$

$= \alpha +_1 \beta$
$= g(a) +_1 g(b)$
Similarly, $g(a *_2 b) = g(h(\alpha) *_2 h(\beta))$
$= g(h(\alpha *_1 \beta))$
$= \alpha *_1 \beta$
$= g(a) *_1 g(b)$
Hence g is an isomorphism between $(N_2, +_2, *_2)$ and $(N_1, +_1, *_1)$. Hence $(N_2, +_2, *_2)\ R\ (N_1, +_1, *_1)$. Therefore R is symmetric.

3. For transitive we need to prove if $(N_1, +_1, *_1)\ R\ (N_2, +_2, *_2)$ and $(N_2, +_2, *_2)\ R\ (N_3, +_3, *_3)$ then $(N_1, +_1, *_1)\ R\ (N_3, +_3, *_3)$, where $(N_1, +_1, *_1), (N_2, +_2, *_2), (N_3, +_3, *_3) \in S$.
Take any $(N_1, +_1, *_1), (N_2, +_2, *_2), (N_3, +_3, *_3) \in S$ such that $(N_1, +_1, *_1) R (N_2, +_2, *_2)$ and $(N_2, +_2, *_2)\ R\ (N_3, +_3, *_3)$, i.e., an isomorphism h_1 (say) exists between $(N_1, +_1, *_1)$ and $(N_2, +_2, *_2)$, and isomorphism h_2 (say) exists between $(N_2, +_2, *_2)$ and $(N_3, +_3, *_3)$.
Consider the map $h_2 \circ h_1 : N_1 \mapsto N_3$. Now, for any $a, b \in N_1$, $h_2 \circ h_1(a) = h_2 \circ h_1(b) \implies h_2(h_1(a)) = h_2(h_1(b)) \implies h_1(a) = h_1(b) \implies a = b$. (Here we have used the fact that h_1 and h_2 are isomorphisms). Hence, $h_2 \circ h_1$ is one-one.
Now, take any $c \in N_3$. Since h_2 is a bijection (i.e., it is onto too), there exist $p \in N_2$ such that $h_2(p) = c$. Similarly, h_1 is a bijection, so for this p we can find $r \in N_1$ such that $h_1(r) = p$.
Now, $h_2 \circ h_1(r) = h_2(h_1(r)) = h_2(p) = c$. Since c was arbitrary, for every $c \in N_3$ there exists $r \in N_1$, such that $h_2 \circ h_1(r) = c$. Hence $h_2 \circ h_1$ is also onto. Therefore, $h_2 \circ h_1$ is a bijection.
Now, take any $a_1, b_1 \in N_1$.
$h_2 \circ h_1(a_1 +_1 b_1) = h_2(h_1(a_1 +_1 b_1))$
$= h_2(h_1(a_1) +_2 h_1(b_1)$
$= h_2(h_1(a_1)) +_3 h_2(h_1(b_1))$
$= h_2 \circ h_1(a_1) +_3 h_2 \circ h_1(b_1)$.
Similarly, $h_2 \circ h_1(a_1 *_1 b_1) = h_2(h_1(a_1 *_1 b_1))$
$= h_2(h_1(a_1) *_2 h_1(b_1)$
$= h_2(h_1(a_1)) *_3 h_2(h_1(b_1))$
$= h_2 \circ h_1(a_1) *_3 h_2 \circ h_1(b_1)$.
Hence, $h_2 \circ h_1 : N_1 \mapsto N_3$ is an isomorphism between $(N_1, +_1, *_1)$ and $(N_3, +_3, *_3)$. Hence $(N_1, +_1, *_1)\ R\ (N_3, +_3, *_3)$. Therefore, R is transitive.

R is reflexive, symmetric and transitive on S. Therefore, R is an equivalence relation on S, 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 $h(1_1) = 1_2$.
  solution 13
  Proof: $0_2 = h(a) +_2 (-h(a))$
  $= h(0_1 +_1 a) +_2 (-h(a))$
  $= (h(0_1) +_2 h(a)) +_2 (-h(a))$
  $= h(0_1) +_2 (h(a) +_2 (-h(a)))$
  $= h(0_1) +_2 0_2 = h(0_1)$
  or $h(0_1) = 0_2$.
  Similarly, $1_2 = h(a) *_2 \alpha$, *(for some* $\alpha \in N_2$*)*
  $= h(1_1 *_1 a) *_2 \alpha$
  $= (h(1_1) *_2 h(a)) *_2 \alpha$
  $= h(1_1) *_2 (h(a) *_2 \alpha)$
  $= h(1_1) *_2 1_2 = h(1_1)$
  or $h(1_1) = 1_2$.

- 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 $h(a/_1 b) = h(a)/_2 h(b)$.
  solution 14
  Proof: By definition of subtraction, for all $a, b \in N_1$,$a -_1 b = a +_1 c$, *for some* $c \in N_1$ *such that* $b +_1 c = 0_1$. *Now,*
  $h(c) = 0_2 +_2 h(c)$
  $= (h(b) +_2 (-_2 h(b))) +_2 h(c)$
  $= ((-_2 h(b)) +_2 h(b)) +_2 h(c)$
  $= (-_2 h(b)) +_2 (h(b) +_2 h(c))$
  $= (-_2 h(b)) + h(b +_1 c)$
  $= (-_2 h(b)) + h(0_1)$
  $= (-_2 h(b)) + 0_2$
  $= (-_2 h(b))$
  Now, $h(a -_1 b) = h(a +_1 c) = h(a) +_2 h(c) = h(a) +_2 (-h(b)) = h(a) -_2 h(b)$
  Similarly, By definition of division, for all $a, b \in N_1 \backslash \{0\}$, $a/_1 b = a *_1 c$, *for some* $c \in N_1$ *such that* $b *_1 c = 1_1$. *Replacing* a *by* b *we get* $b/_1 b = b *_1 c = 1_1$. *Hence dividing a number by itself will give* 1. *Also, Let* $\beta/_2 h(b) = \beta * \gamma$, *for all* $\beta \in N_2 \backslash \{0_2\}$, *for some* $\gamma \in N_2 \backslash \{0_2\}$, *such that* $h(b) *_2 \gamma = 1_2$. *Now*
  $h(c) = 1_2 *_2 h(c) = (h(b) *_2 \gamma) *_2 h(c) = (\gamma *_2 h(b)) *_2 h(c) = \gamma *_2 (h(b) *_2 h(c)) = \gamma *_2 (h(b *_1 c)) = \gamma *_2 1_2 = \gamma$.
  Now, $h(a/_1 b) = h(a *_1 c) = h(a) *_2 h(c) = h(a) *_2 \gamma = h(a)/_2 h(b)$.

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 $F_2(x)$. **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.**
  solution 15
  Proof:

  1. Claim 1: If $p(x)$ and $q(x)$ are 0-1 polynomials, then $p(x) + q(x)$ and $p(x) * q(x)$ are also 0-1 polynomials. Let $p(x) = \sum_{i=0}^{k} c_i x^i$ and $q(x) = \sum_{i=0}^{m} d_i x^i$, with $c_i, d_i = 0, 1$. Without loss of Generality, we can assume $m \geq k$.
     $p(x)+q(x) = \sum_{i=0}^{k} c_i x^i + \sum_{i=0}^{m} d_i x^i = \sum_{i=0}^{k} (c_i x^i + d_i x^i) + \sum_{i=k+1}^{m} d_i x^i$.
     Now, for each i, if exactly one of c_i and d_i is 0 and one of them is 1, then clearly, $c_i x^i + d_i x^i = x^i$, and if both are 0 or both are 1 then $c_i x^i + d_i x^i = 0$. Hence, all coefficients of $p(x) + q(x)$ are either 0 or 1.
     Hence $p(x) + q(x)$ is a 0-1 polynomial.
     $p(x) * q(x) = (\sum_{i=0}^{k} c_i x^i) * (\sum_{j=0}^{m} d_j x^j)$
     $= (c_0 + c_1 x + c_2 x^2 + ...) * ((d_0 + d_1 x + d_2 x^2 + ...)$
     $= (c_0 * d_0 + (c_1 * d_0 x + c_0 * d_1 x) + (c_2 * d_0 x^2 + c_1 * d_1 x^2 + c_0 * d_2 x^2) + ...)$
     $= \sum_{p=0}^{k+m} (\sum_{i=0}^{p} c_i * d_{p-i} x^p)$
     Clearly, for all i, p , $c_i * d_{p-i} = 0$ *or* 1. And since $x^p + x^p = 0$, $\sum_{i=0}^{p} c_i * d_{p-i} x^p = 0$ *or* x^p. From this it follows that all coefficients of $p(x) * q(x)$ are either 0 or 1.
     Hence $p(x) * q(x)$ is a 0-1 polynomial.

  2. Now, take any $p(x)/q(x)$, $r(x)/s(x) \in F_2(x)$. Consider
     $p(x)/q(x) + r(x)/s(x) = (p(x) * s(x) + q(x) * r(x))/(q(x) * s(x)) =$
     $(p_1(x) + q_1(x))/(r_1(x)$(for some $p_1(x), q_1(x), r_1(x)) = s_1(x)/r_1(x) \in$
     $F_2(x)$.

  3. For sake of simplicity, let us represent $p(x)$ by p from now on, and similarly all other polynomials. Also we will represent p/q as $\frac{p}{q}$. for all $p/q, r/s, u/v \in F_2(x)$
     $(\frac{p}{q} + \frac{r}{s}) + \frac{u}{v} = \frac{p*s+q*r}{q*s} + \frac{u}{v} = \frac{(p*s+q*r)*v+(q*s)*u}{(q*s)*v} = \frac{(p*s)*v+q*(r*v+s*u)}{q*(s*v)}$
     $= \frac{p}{q} + \frac{r*v+s*u}{s*v} = \frac{p}{q} + (\frac{r}{s} + \frac{u}{v})$

  4. If for a 0-1 polynomial we set all coefficients as 0 we get a zero polynomial $0_f(say)$.
     Similarly, if we put $c_0 = 1$ and rest all $c_i = 0$. We get a constant

polynomial $1_f(say)$.
$0_f/1_f = 0_F(say) \in F_2(x)$. It can easily be seen that $0_F + p/q = p/q + 0_F = p/q$ for all $p/q \in F_2(x)$.

5. For any $p/q \in F_2(x)$, let $p(x) = \sum_{i=0}^{k} c_i x^i$).
   Note that $(p/q) + (p/q) = (p+p)/q = (\sum_{i=0}^{k} c_i x^i) + \sum_{i=0}^{k} c_i x^i))/q = (\sum_{i=0}^{k} c_i x^i + c_i x^i)/q = 0_F$.
6. For all $p/q, r/s \in F_2(x)$
   $\frac{p}{q} + \frac{r}{s} = \frac{p*s+q*r}{q*s} = \frac{r*q+s*p}{s*q} = \frac{r}{s} + \frac{p}{q}$

   From 2,3,4,5,6 we can say that $F_2(x)$ is a set of numbers with addition. (A)
7. Now, take any $p(x)/q(x)$, $r(x)/s(x) \in F_2(x)\backslash\{0_F\}$. Consider $(p(x)/q(x))*(r(x)/s(x)) = (p(x)*r(x))/(q(x)*s(x)) = p_2(x)/r_2(x) \in F_2(x)\backslash\{0_F\}$ (for some $p_2(x), r_2(x)$).

8. for all $p/q, r/s, u/v \in F_2(x)\backslash\{0_F\}$
   $(\frac{p}{q} * \frac{r}{s}) * \frac{u}{v} = \frac{p*r}{q*s} * \frac{u}{v} = \frac{(p*r)*u}{(q*s)*v} = \frac{p*(r*u)}{q*(s*v)} = \frac{p}{q} * \frac{r*u}{s*v} = \frac{p}{q} * (\frac{r}{s} * \frac{u}{v})$
9. $1_f/1_f = 1_F(say) \in F_2(x)\backslash\{0_F\}$. It can easily be seen that $1_F * p/q = p/q * 1_F = p/q$ for all $p/q \in F_2(x)\backslash\{0_F\}$.
10. For all $p/q \in F_2(x)\backslash\{0_F\}$, we have q/p, such that $p/q * q/p = (p * q)/(q * p) = 1_F$.
11. For all $p/q, r/s \in F_2(x)\backslash\{0_F\}$
    $\frac{p}{q} * \frac{r}{s} = \frac{p*r}{q*s} = \frac{r*p}{s*q} = \frac{r}{s} * \frac{p}{q}$

    From 7,8,9,10,11 we can say that $F_2(x)\backslash\{0_F\}$ is a set of numbers with multiplication. (B)
12. For all $p/q, r/s, u/v \in F_2(x)$
    $\frac{p}{q} * (\frac{r}{s} + \frac{u}{v}) = \frac{p}{q} * \frac{r*v+s*u}{s*v} = \frac{p*(r*v+s*u)}{q*(s*v)} = \frac{p*(r*v)+p*(s*u)}{q*(s*v)} = \frac{p*r*v}{q*s*v} + \frac{p*s*u}{q*s*v} = \frac{p*r}{q*s} + \frac{p*u}{q*v} = (\frac{p}{q} * \frac{r}{s}) + (\frac{p}{q} * \frac{u}{v})$

From (A),(B),12 we can say that $F_2(x)$ is a set of numbers with addition and multiplication.

- *Show that there is a bijection between rational numbers $\mathbb{Q}$ and $F_2(x)$.*
  solution 16
  Proof: We can define a one-one map $f : \mathbb{Q} \mapsto F_2(x)$ as follows
  $f(0) = 0$, i.e., $p(x) = 1, q(x) = 1$. Take any $r \in \mathbb{Q}$, $r \neq 0$. Write r as $(sign)a/b$, where a, b are both co-prime positive integers and $sign$ can either be $+$ or $-$. Define$f(r) = p(x)/q(x)$, where $p(x)$ and $q(x)$ are given as: When r is positive, i.e., $sign$ is $+$, $p(x) = \sum_{i=0}^{k} c_i x^i$, where
  $c_i = 1$ for $i = a + 1, a + 2, ..., a + b$
  0 otherwise and
  $q(x) = 1$.
  When r is negative, i.e., $sign$ is $-$, $p(x) = \sum_{i=0}^{k} c_i x^i$, where
  $c_i = 1$ for $i = 0, a + 1, a + 2, ..., a + b$
  0 otherwise and
  $q(x) = 1$.
  It can be easily seen that f is one-one.
  Now let us define a one-one map $g : F_2(x) \mapsto \mathbb{Q}$. For any number $p(x)/q(x) \in F_2(x)$. Let $p(x) = \sum_{i=0}^{k} c_i x^i$, and $q(x) = \sum_{i=0}^{k} d_i x^i$. Make two binary numbers $a = c_0 c_1 ... c_k$ and $b = d_0 d_1 ... d_k$. Now g maps $p(x)/q(x)$ to $2^a/3^b$. Again, it is easy to see that g is one-one. Hence we have proved that a one-one map exists from $\mathbb{Q}$ to $F_2(x)$ and a one-one map exists from $F_2(x)$ to $\mathbb{Q}$. Therefore by **Canto-Schroeder-Bernstein Theorem** there exists a bijection from $\mathbb{Q}$ to $F_2(x)$.

- *Show that there is no isomorphism between $\mathbb{Q}$ and $F_2(x)$.*
  solution 17
  Suppose there exists an isomorphism $h : \mathbb{Q} \mapsto F_2(x)$. since h is a bijection, there exists $a \in \mathbb{Q}$ such that $h(a) = x$.
  Now $h(a +_{\mathbb{Q}} a) = h(a) +_F h(a) = x +_F x = 0_F = h(0_{\mathbb{Q}})$ (proved in solution 13). But since h is a bijection, $a + a = 0_{\mathbb{Q}}$, which is possible only when $a = 0_{\mathbb{Q}}$. But then $h(a) = h(0_{\mathbb{Q}}) = 0_F \neq x$. This is a contradiction, hence no isomorphism exist 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.
  solution 18
  For defining division on $\mathbb{Z}$ we need the fourth axiom for $(N, *)$. We will prove that $\mathbb{Z}$ does not follow this axiom.
  Consider $2 \in \mathbb{Z}$. Suppose there exists $b \in \mathbb{Z}$ such that $2 * b = 1$. For $b \leq 0$, $2 * b \leq 0 < 1$. For $b \geq 1$, we get $2 * b \geq 2 > 1$, so it is also not possible. And there are no integers between 0 and 1. Hence no such $b \in \mathbb{Z}$ exist. Therefore, fourth axiom for $(N, *)$ can not be applied to $\mathbb{Z}$. So, $\mathbb{Z}$ 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 $a * b = 0$.
  solution 19
  Consider the set $B = \{0, 1, 2, 3\} \subseteq \mathbb{N}$.
  Define addition $'+'$ *as* $a\&b = (a +_N b) \ (mod\ 4)$ *for all* $a, b \in B$
  Define multiplication $'*'$ *as* $a * b = (a *_N b) \ (mod\ 4)$ *for all* $a, b \in B$.
  Here $+_N$ *and* $*_N$ *represent usual addition on and multiplication defined on* $\mathbb{N}$. *Now, it can be shown that* $(B, +, *)$ *is a set of numbers with addition and multiplication in a similar way we proved* $(Q, \&, :)$ *to be a set of numbers in solution* 7. *But since here we have also included* 0 *in* B *in definition of multiplication, division is not defined on* B.
  Hence $(B, +, *)$ *is a set of numbers without division. Now, we have* $2 \in B$ *such that* $2 \neq 0$ *but* $2 * 2 = (2 *_N 2) \ (mod\ 4) = 4 \ (mod\ 4) = 0$.

- There is a set of numbers without division $(N, +, *)$ such that there is $a \in N$, $a \neq 0$, but $a^3 = a * a * a = 0$.
  solution 20
  Proof: In the set of numbers without division $(B, +, *)$ *defined above,* $2 \in B$, $2 \neq 0$, *but* $2^3 = 2 * 2 * 2 = 0 * 2 = (0 *_N 2)\ (mod\ 4) = 0\ (mod\ 4) = 0$.

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