Module 2: Number Systems

Priyanshu Mahato

March 9, 2022

Email: pm21ms002@iiserkol.ac.in.These are my personal notes on Number Systems. We will consider $\mathbb{N}$ (Natural Numbers), $\mathbb{Z}$ (Integers), and $\mathbb{Q}$ (rational Numbers), but not $\mathbb{R}$ (Real Numbers).

§1 Natural Numbers

The natural numbers are $1, 2, 3, 4, \ldots$. The set of all natural numbers is denoted by $\mathbb{N}$.

Definition 1.1. We assume familiarity with the algebraic operations of addition and multiplication on the set $\mathbb{N}$ and also with the linear order relation $<$ on $\mathbb{N}$ defined by "$a < b$ if $a, b \in \mathbb{N}$ and a is less than b".

We discuss the following fundamental properties of the set $\mathbb{N}$.

1. Well Ordering Property
2. Principle of Induction

§1.1 Well Ordering Property

Definition 1.2. Every non-empty subset of $\mathbb{N}$ has a least element.

This means that if S is a non-empty subset of $\mathbb{N}$, then there is an element m in S such that $m \leq s$ for all $s \in S$.
In particular, $\mathbb{N}$ itself has the least element 1.

Proof. Let S be a non-empty subset of $\mathbb{N}$. Let k be an element of S. Then k is a natural number.
We define a subset T by $T = \{x \in S : x \leq k\}$. The T is a non-empty subset of $\{1, 2, 3, \ldots, k\}$.
Clearly, T is a finite subset of $\mathbb{N}$ and therefore it has a least element, say m. Then $1 \leq m \leq k$.
We now show that m is the least element of S. Let s be any element of S.
If $s > k$, then the inequality $m \leq k$ implies $m < s$.
If $s \leq k$, the $s \in T$; and m being the least element of T, we have $m \leq s$.
Thus m is the least element of S. □

§1.2 Principle of Induction

Definition 1.3. Let S be a subset of $\mathbb{N}$ such that,

i) $1 \in S$ and,

ii) if $k \in S$, then $k+1 \in S$.

Then $S = \mathbb{N}$

Proof. Let $T = \mathbb{N} - S$. We prove that $T = \phi$.
Let T be non-empty. then by the *Well Ordering Property* of $\mathbb{N}$, the non-empty subset T has a least element, say m.
Since $1 \in S$ and 1 is the least element of $\mathbb{N}$, $m > 1$.
Hence, $m-1$ is a natural number and $m-1 \notin T$. So, $m-1 \in S$.
But by ii) $m-1 \in S \Rightarrow (m-1)+1 \in S$, i.e., $m \in S$.
This contradicts that m is the least element in T. Therefore, our assumption is wrong and $T = \phi$.
Therefore, $S = \mathbb{N}$. □

Theorem 1.4

Let $P(n)$ be a statement involving a natural number n. If,

i) $P(1)$ is true, and

ii) $P(k+1)$ is true whenever $P(k)$ is true,

then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let S be the set of those natural numbers for which the statement $P(n)$ is true.
Then S has the properties,

(a) $1 \in S$, by (i)

(b) $k \in S \Rightarrow k+1 \in S$ by (ii).

By the *Principle of Induction*, $S = \mathbb{N}$.
Therefore, $P(n)$ is true for all $n \in \mathbb{N}$. □

Remark 1.5. Let a statement $P(n)$ satisfies the conditions,

(i) for some $m \in \mathbb{N}$, $P(m)$ is true (m being the least possible); and

(ii) $P(k)$ is true $\Rightarrow P(k+1)$ is true for all $k \geq m$.

Then $P(n)$ is true for all natural numbers $\geq m$.

Worked Examples

Example 1.6
Prove that for each $n \in \mathbb{N}$, $1+2+3+4+\cdots+n = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

The statement is true for $n = 1$, because $1 = \dfrac{1(1+1)}{2}$.
Let the statement be true for some natural number k.
Then $1+2+3+4+\cdots+k = \dfrac{(k+1)}{2}$ and therefore,

$$(1+2+\cdots+k)+(k+1) = \frac{k(k+1)}{2}+(k+1)$$

$$\text{or, } 1+2+3+\cdots+(k+1) = \frac{(k+1)(k+2)}{2}.$$

This shows that the statement is true for the natural number $k+1$ if it is true for k. By the principle of induction, the statement is true for all natural numbers.

Example 1.7
Prove that for each $n \geq 2$, $(n+1)! > 2^n$.

The equality holds for $n = 2$ since $(2+1)! > 2^2$.
Let the inequality hold for some natural number $k \geq 2$.
Then, $(k+1)! > 2^k$

$$\begin{aligned} \textit{and } (k+2)! &= (k+2)(k+1)! \\ &> 2 \cdot 2^k, \textit{since } k+2 > 2 \\ \textit{or, } (k+2)! &> 2^{k+1} \end{aligned}$$

This shows that if the inequality holds for $k(\geq 2)$ then it also holds for $k+1$.
By the principle of induction, the inequality holds for all natural numbers ≥ 2.
[Note that the inequality does not hold for $n = 1$.]

§1.3 Second Principle of Induction (or, Principle of Strong Induction)

Definition 1.8. Let S be a subset of $\mathbb{N}$ such that

(i) $1 \in S$, and

(ii) if $\{1, 2, 3, 4, \dots\} \subset S$, then $k+1 \in S$.

Then $S = \mathbb{N}$

Proof. Let $T = \mathbb{N} - S$. We prove that $T = \phi$.
Let T be non-empty. Then T will have a least element, say m, by the WOP of $\mathbb{N}$. Since, $1 \in S$, $1 \notin T$.
As m is the least element in T and $1 \notin T$, $m > 1$.
By choice of m, all natural numbers less than m belong to S. That is $1, 2, \dots, m-1$ all belong to S.
Then by (ii) $m \in S$ and consequently, $m \notin T$, a contradiction. It follows that $T = \phi$ and therefore, $S = \mathbb{N}$. □

Worked Examples(continued)

Example 1.9

Prove that for all $n \in \mathbb{N}$, $(3+\sqrt{5})^n + (3-\sqrt{5})^n$ is an even integer.

Let $P(n)$ be the statement "$(3+\sqrt{5})^n + (3-\sqrt{5})^n$ is an even integer".
$P(1)$ is true since $(3+\sqrt{5})^1 + (3-\sqrt{5})^1 = 6$, an even integer.
Let us assume that $P(n)$ is true for $n = 1, 2, \ldots, k$.

$$\begin{aligned}
&(3+\sqrt{5})^{(k+1)} + (3-\sqrt{5})^{(k+1)} \\
&= a^{(k+1)} + b^{(k+1)} \ \textit{where}\ a = 3+\sqrt{5},\ b = 3-\sqrt{5} \\
&= (a^k + b^k)(a+b) - (a^{k-1} + b^{k-1})ab \\
&= 6(a^k + b^k) - 4(a^{k-1} + b^{k-1}).
\end{aligned}$$

It is an even integer, since $a^k + b^k$ and $a^{k-1} + b^{k-1}$ are even integers.
Hence, $P(k+1)$ is true whenever $P(n)$ is true for all $n = 1, 2, \ldots, k$.
By the second principle of induction, $P(n)$ is true for all natural numbers.

§2 Integers

We shall now construct the set of integers using the set of Natural Numbers. Our construction will be through an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Definition 2.1. Define $\sim_{\mathbb{Z}}$ on $\mathbb{N} \times \mathbb{N}$ by, for all $(m,n), (p,q) \in \mathbb{N} \times \mathbb{N}$,

$$(m,n) \sim_{\mathbb{Z}} (p,q) \Leftrightarrow m + q = n + p$$

Lemma 2.2 i) $\sim_{\mathbb{Z}}$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

ii) for all $(m,n) \in \mathbb{N} \times \mathbb{N}$,

$$(m,n) \sim_{\mathbb{Z}} \begin{cases} (\text{m+1-n},\ 1) & \text{for } m \geq n \\ (1,\ \text{n+1-m}) & \text{for } n \geq m \end{cases}$$

iii) $\mathbb{N} \times \mathbb{N} / \sim_{\mathbb{Z}} = \{[(j,1)] : j \in \mathbb{N}\ \&\ j \geq 2\} \cup \{[(1,k)] : k \in \mathbb{N}\ \&\ k \geq 2\} \cup \{[(1,1)]\}$

Proof. Look at MA1101 ps2 (**Problem 2**) □

Definition 2.3. Let us write $\mathbb{Z} \stackrel{\text{def}}{=} \mathbb{N} \times \mathbb{N} / \sim_{\mathbb{Z}} = \{[(m,n)] : (m,n) \in \mathbb{N} \times \mathbb{N}\}$
We also write,

$$\boxed{\overline{0} \stackrel{\text{def}}{=} [(1,1)]\ \&\ \overline{1} \stackrel{\text{def}}{=} [(2,1)]}$$

Let $\overline{a} \stackrel{\text{def}}{=} [(m,n)]$, $\overline{b} \stackrel{\text{def}}{=} [(p,q)] \in \mathbb{Z}$.

i) **Addition**

$$\boxed{a + b \stackrel{\text{def}}{=} [(m+p, n+q)]}$$

ii) **Multiplication**

$$\boxed{a \cdot b \stackrel{\text{def}}{=} [(mp + nq, mq + np)]}$$

We have the following important theorem,

Theorem 2.4 i) $+$ is well-defined, commutative and associative

ii) $a + \overline{0} = a = \overline{0} + a, \forall a \in \mathbb{Z}$

iii) $\forall a \in \mathbb{Z}, \exists$ a unique $x \in \mathbb{Z}$, such that $a + x = \overline{0}$. We write $-a$ for x and say that $-a$ is the negative of a

iv) $\forall a, b \in \mathbb{Z}, \exists$ a unique $x \in \mathbb{Z}$ such that $a + x = b$

v) $\cdot$ is well defined, associative, and commutative

vi) $a \cdot \overline{1} = a = \overline{1} \cdot a, \forall a \in \mathbb{Z}$

vii) $\forall a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$

Remark 2.5. In other words, we can call $(\mathbb{Z}, +, \cdot)$ as a commutative **ring** with identity.

To prove 2.4, we start off with a lemma,

Lemma 2.6
$\forall\ n, p, q \in \mathbb{N}$, if $n + p = n + q \Rightarrow p = q$

Proof. We prove using Induction on n. When $n = 1$, $S(p) = 1 + p = 1 + q = S(q)$. As S is one-one (injective), it follows that $p = q$. Let us suppose that for some $k \in \mathbb{N}$, $k + p = k + q$. Hence, $(k + 1) + p = 1 + (k + p) = 1 + (k + q) = (k + 1) + q$, i.e., the result holds when $n = k + 1$. Therefore, the result is proved using Induction. □

We are now ready to prove Theorem 2.4,

Proof. i) We first check that $+$ is well-defined. Let $a = [(m, n)] = [(m', n')]$, $b = [(p, q)] = [(p', q')]$. We have to show that, $[(m + p, n + q)] = [(m' + p', n' + q')]$ (*)
Indeed, as $[(m, n)] = [(m', n')]$, we have $m + n' = n + m'$.
Similarly, $p + q' = q + p'$.

$$\begin{aligned}
&m + n' + p + q' = n + m' + q + p' \\
\Rightarrow &(m + p) + (n' + q') = (n + q) + (m' + p') \\
\Rightarrow &(m + p, n + q) \sim_{\mathbb{Z}} (m' + p', n' + q') \\
\Rightarrow &[(m + p, n + q)] = [(m' + p', n' + q')],
\end{aligned}$$

which proves (*). Hence, $+$ is well-defined. □

We now check the associativity of +.Let $a, b, c \in \mathbb{Z}$ be written as, $a = [(m, n)], b = [(p, q)], c = [(r, s)]$.
Then,

$$\begin{aligned}(a + b) + c &= ([(m, n)] + [p, q]) + [(r, s)] \\ &= [(m + p, n + q)] + [(r, s)] \\ &= [((m + p) + r, (n + q) + s)] \\ &= [(m + (p + r), n + (q + s))] \\ &= a + (b + c)\end{aligned}$$

which shows that + is associative.

Now, we show that + is commutative. Let $a, b \in \mathbb{Z}$ be written as, $a = [(m, n)], b = [(p, q)]$.
Then,

$$\begin{aligned}a + b &= [(m, n)] + [(p, q)] \\ &= [(m + p, n + q)] \\ &= [(p + m, q + n)] \\ &= b + a\end{aligned}$$

which shows that + is commutative.

ii) Let $a \in \mathbb{Z}$ be written as, $a = [(m, n)]$. Then,

$$\begin{aligned}a + \overline{0} &= [(m, n)] + [(1, 1)] \\ &= \underbrace{[(m + 1, n + 1)] = [(m, n)]} \\ &= \overline{a}\end{aligned}$$

as, $(m + 1, n + 1) \sim_{\mathbb{Z}} (m, n)$. Also, we have earlier proved the commutativity of + over $\mathbb{Z}$. Therefore, we have proved that,

$$a + \overline{0} = \overline{a} = \overline{0} + a, \forall\ a \in \mathbb{Z}$$

iii) Let $a \in \mathbb{Z}$ be written as, $a = [(m, n)]$. We define $x \in \mathbb{Z}$ as, $x \stackrel{\text{def}}{=} [(n, m)]$.
Then,

$$\begin{aligned}a + x &= [(m, n)] + [(n, m)] \\ &= [(m + n, n + m)] \\ &= [(m + n, m + n)] \\ &= [(1, 1)] \\ &= \overline{0}\end{aligned}$$

We now prove the uniqueness of x. Let us suppose that $\exists\ x, y \in \mathbb{Z}$, such that,

$$a + x = x + a = \overline{0}, \text{ and } a + y = y + a = \overline{0}$$

We now show that $x = y$. Indeed, using ii),
$x = \overline{0} + x = (y + a) + x = y + (a + x) = y + \overline{0} = y$, which proves the uniqueness.

iv) Let $a, b \in \mathbb{Z}$ be given.We must define $x = (-a) + b$.
Then,

$$a + x = a + ((-a) + b) = (a + (-a)) + b = \overline{0} + b = b$$

We now prove the uniqueness of x. Let there be $a, b \in \mathbb{Z}$. We must define $x, y \in \mathbb{Z}$ as $x = (-a) + b$ and $y = (-a) + b$. Then,

$$a + x = a + ((-a) + b) = (a + (-a)) + b = 0 + b = (a + (-a)) + b = a + ((-a) + b) = a + y$$

This shows that $x = y$, which in turn proves the uniqueness of x.

We now establish the properties of multiplication on $\mathbb{Z}$.

v) We prove that multiplication on $\mathbb{Z}$ is well-defined. Let $a, b \in \mathbb{Z}$ be defined as, $a = [(m, n)] = [(m', n')]$ and $b = [(p, q)] = [(p', q')]$.
We shall show that,

$$\begin{aligned} &[(m, n)][(p, q)] = [(m', n')][(p', q')] \\ \Rightarrow\ &[(mp + nq, mq + np)] = [(m'p' + n'q', m'q' + n'p')] \end{aligned}$$

$$\Rightarrow \boxed{mp + nq + m'q' + n'p' = m'p' + n'q' + mq + np}$$

To prove this, we proceed as follows. We have,

$$m + n' = m' + n \tag{1}$$
$$p + q' = q + p' \tag{2}$$

$(1) \times p \Rightarrow mp + n'p = m'p + np$
$(1) \times q \Rightarrow mq + n'q = m'q + nq$
$(2) \times m' \Rightarrow pm' + q'm' = qm' + p'm'$
$(2) \times n' \Rightarrow pn' + q'n' = qn' + p'n'$

This implies that,

$$mp + n'p + m'q + nq + pm' + q'm' + qn' + p'n' = m'p + np + mq + n'q + qm' + p'm' + pn' + q'n'$$
$$(mp + nq + m'q' + n'p') + [n'p + m'q + m'p + n'q] = (mq + np + m'p' + n'q') + [n'p + m'q + m'p + n'q]$$

Now, invoking `Lemma 2.6`, we conclude that,

$$mp + nq + m'q' + n'p' = mq + np + m'p' + n'q'$$

which proves our assumption. Hence, the multiplication is well-defined on $\mathbb{Z}$. This proves `(v)` and `(vi)`.

(vii) We prove that $\forall a, b, c \in \mathbb{Z},\ a \cdot (b + c) = a \cdot b + a \cdot c$. Let $a, b, c \in \mathbb{Z}$ be defined as, $a = [(m, n)]$, $b = [(p, q)]$, and $c = [(r, s)]$.

Now, we can say,

$$\begin{aligned} a \cdot (b + c) &= [(m, n)] \cdot ([(p, q)] + [(r, s)]) \\ &= [(m, n)] \cdot [(p + r, s + q)] \\ &= [(mp + mr + ns + nq, ms + mq + np + nr)] \\ ab + ac &= [(m, n)][(p, q)] + [(m, n)][(r, s)] \\ &= [(mp + nq, mq + np)] + [(mr + ns, ms + nr)] \\ &= [(mp + nq + mr + ns, mq + np + ms + nr)] \end{aligned}$$

Since, $a \cdot (b + c) = [(mp + mr + ns + nq, ms + mq + np + nr)] = [(mp + nq + mr + ns, mq + np + ms + nr)] = ab + ac$, we have proved the claim that,

$$\forall\ a, b, c \in \mathbb{Z},\ \ a \cdot (b + c) = a \cdot b + a \cdot c$$

`This completes the proof for Theorem 2.4.`

Before we proceed further, let's introduce the following notation.

Notation:
We write,

$$\boxed{\mathbb{Z}^+ \stackrel{\text{def}}{=} \{[(j, 1)] : j \in \mathbb{N}, j \geq 2\}}$$

Theorem 2.7

`Embedding of` $\mathbb{N}$`:`
Define $f : \mathbb{N} \mapsto \mathbb{Z}$ by,

$$\boxed{f(n) \stackrel{\text{def}}{=} [(n + 1, 1)] \forall\ n \in \mathbb{N}}$$

Then f satisfies the following properties:

i) f is one-one(injective),

ii) $f(\mathbb{N}) = \mathbb{Z}^+$,

iii) $f(1) = \overline{1}$,

iv) $\forall\ m, n \in \mathbb{N}$,

$$f(m + n) = f(m) + f(n),\ \ f(mn) = f(m) \cdot f(n)$$

Proof. i) Let there be $x, y \in \mathbb{N}$ such that $f(x) = f(y)$.

$$\begin{aligned} &[(x + 1, 1)] = [(y + 1, 1)] \\ \Rightarrow\ &(x + 1) + 1 = 1 + (y + 1) \\ \Rightarrow\ &x + 1 + 1 = y + 1 + 1 \\ \Rightarrow\ &x = y \end{aligned}$$

This proves that $f(n)$ is indeed one-one or, injective.

ii) We now show that, $f(\mathbb{N}) = \mathbb{Z}^+$. By definition, $f(\mathbb{N}) = \{f(n) : n \in \mathbb{N}\} = [(n+1,1)] \forall\ n \in \mathbb{N}$. Now, $\mathbb{Z}^+$ is defined as, $\mathbb{Z}^+ = \{[(j,1)] : j \in \mathbb{N}, j \geq 2\}$.

We know from the `Well-Ordering Property` of $\mathbb{N}$, that the minimum element of $\mathbb{N}$ is 1. Thus, we can say that $n+1,\ \forall\ n \in \mathbb{N}$ is greater than 2. This makes the fact evident that,

$$f(\mathbb{N}) = \{f(n) : n \in \mathbb{N}\} = \{[(n+1,1)] : n \in \mathbb{N},\ n+1 \geq 2\} = \{[(j,1)] : j \in \mathbb{N}, j \geq 2\} = \mathbb{Z}^+$$
$$\Rightarrow f(\mathbb{N}) = \mathbb{Z}^+$$

This proves the claim.

iii) We now show that $f(1) = \overline{1}$.

$$\begin{aligned} f(n) &= [(n+1,1)] \forall\ n \in \mathbb{N} \\ \Rightarrow f(1) &= [(2,1)] \\ \overline{1} &= [(2,1)],\ \textit{from } \texttt{Definition } 2.3 \\ \Rightarrow f(1) &= \overline{1} \end{aligned}$$

This proves our claim.

iv) We need to show that, $\forall\ m, n \in \mathbb{N}$, $f(m+n) = f(m) + f(n)$, $f(mn) = f(m) \cdot f(n)$. Let's first try proving, $f(m+n) = f(m) + f(n)$.

$$\begin{aligned} f(m+n) &= [(m+n+1,1)] \\ f(m) &= [(m+1,1)] \\ f(n) &= [(n+1,1)] \\ \Rightarrow f(m) + f(n) &= [(m+1,1)] + [(n+1,1)] \\ &= [(m+n+1+1, 1+1)] \\ &= [(m+n+1,1)] \\ \Rightarrow f(m+n) &= f(m) + f(n) \end{aligned}$$

This proves our claim.

□

Corollary 2.8

Let $f : \mathbb{N} \mapsto \mathbb{Z}$ be the map defined in Theorem 2.7. Then,

$$\mathbb{Z} = \{f(n) : n \in \mathbb{N}\} \cup \{-f(n) : n \in \mathbb{N}\} \cup \overline{0}$$

Convention:

Let $f : \mathbb{N} \mapsto \mathbb{Z}$ be the embedding map defined in Theorem 2.7. We shall identify $f(n)$ with n, $\forall\ n \in \mathbb{N}$. Then, $\mathbb{Z} = \{n \in \mathbb{N}\} \cup \{-n | n \in \mathbb{N}\} \cup \{\overline{0}\}$

Theorem 2.9

`Order in` $\mathbb{Z}$

For all $a, b \in \mathbb{Z}$, we can say that,

1. $a > b$ iff $\exists\ x \in \mathbb{Z}^+$ such that $b + x = a$
2. $a \geq b$ iff either $a = b$ or $a > b$

§3 Rationals

We conclude the chapter by constructing the set of Rational Numbers out of the set of Integers. The construction, in this case as well, proceeds with an appropriate equivalence relation.

Definition 3.1. $\mathbb{Q}$ - Equivalence Relation
Define $\sim_{\mathbb{Q}}$ on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ by, $\forall (a,b),(p,q) \in (\mathbb{Z} \setminus \{0\})$

$$(a,b) \sim_{\mathbb{Q}} (p,q) \Leftrightarrow aq = bp$$

.

Lemma 3.2

$\sim_{\mathbb{Q}}$ is an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

Proof. We now check for the three conditions, viz. Reflexivity, Symmetry and Transitivity for the relation $\sim_{\mathbb{Q}} \forall (a,b),(p,q) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

(i) Reflexivity:
We know that $(a,b) \sim_{\mathbb{Q}} (p,q)$ iff $aq = bp$.
This implies that $(a,b) \sim_{\mathbb{Q}} (a,b) \Leftrightarrow ab = ba$, which is true from Theorem 2.4.
Therefore, it is proven that $\sim_{\mathbb{Q}}$ is Reflexive.

(ii) Symmetry:
We know now that,

$$(a,b) \sim_{\mathbb{Q}} (p,q) \Leftrightarrow aq = bp$$
$$(p,q) \sim_{\mathbb{Q}} (a,b) \Leftrightarrow pb = qa$$

Since both the above relations lead to the same result, we can conclude that $\sim_{\mathbb{Q}}$ is Symmetric.

(iii) Transitivity:
We know now that,

$$(a,b) \sim_{\mathbb{Q}} (p,q) \Leftrightarrow aq = bp$$
$$(p,q) \sim_{\mathbb{Q}} (r,s) \Leftrightarrow ps = qr$$
$$\Rightarrow (a,b) \sim_{\mathbb{Q}} (r,s) \Leftrightarrow as = br$$

□