Module 2: Number Systems

Priyanshu Mahato

March 4, 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. $\square$

§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,
$(1+2+\cdots+k)+(k+1) = \dfrac{k(k+1)}{2} + (k+1)$
or, $1+2+3+\cdots+(k+1) = \dfrac{(k+1)(k+2)}{2}$.
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 $\mathbb{Z} \overset{\text{def}}{=} \mathbb{N} \times \mathbb{N} / \sim_{\mathbb{Z}} = \{[(m,n)] : (m,n) \in \mathbb{N} \times \mathbb{N}\}$

We also write,

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

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

i) **Addition**

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

ii) **Multiplication**

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

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

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 $n + p = n + q \Rightarrow p = q$