CHAPTER 2: NUMBER SYSTEMS

In this chapter, we study number systems. Because of practical uses of numbers in our daily lives, they have profound significance throughout the world. In fact, the usage of numbers is so tied to ~~to~~ human lives that mathematical writing predates literature by more than a thousand years. In even predates the oldest ~~surving~~ surviving written story the Epic of Gilgamesh, a Sumerian poem written ~~about~~ during about 1800 BC. The oldest written record, which is about an exercise in calculating the areas of two fields, dates back to 3350 BC – 3200 BC, predates any known evidence of writing. This was found in the reused building rubble of the city of Uruk.

SECTION 2.1 NATURAL NUMBERS.

We use natural numbers, mainly for counting and ordering. It comes up so 'naturally' in everyday computation that ~~a school~~ it is believed to be a direct consequence of ~~hum~~ human psyche by a school of philosophers. In fact, Kronecker mentioned that 'God made the natural numbers, all else is the work of man."
In opposition to the aforementioned group of philosophers, the constructivists saw a need to define the set of natural numbers rigorously within the framework of set theory. This philosophy was carried out by Grassman, Frege, Peano, just to mention a few.

In this chapter, we assume our familiarity with natural numbers, and construct other number systems from there on. In the appendix, ~~we~~ the Peano's construction is discussed briefly.

NOTATION 2.1.1 (Natural Numbers)

We write $\mathbb{N}$ to denote the set of all ~~non~~ natural numbers. Note that, $\mathbb{N} = \{1, 2, 3, \ldots\}$. $\mathbb{N}$ comes with the distinguished element 1 which is the least element of $\mathbb{N}$. $\mathbb{N}$ has ~~a~~ also the algebraic operations addition (+) and multiplication defined on it. ⊛ We also assume that $\mathbb{N}$ satisfies the following important property (axiom):

⊛ **ASSUMPTION 2.1.1½ (SUCCESSOR MAP)**

The map $S : \mathbb{N} \to \mathbb{N}$ defined as $S(n) := n+1$, for all $n \in \mathbb{N}$ has the following properties i) S is 1-1, and ii) $S(n) \neq 1$, for all $n \in \mathbb{N}$.

AXIOM 2.1.2 (WELL-ORDERING PRINCIPLE)

Every non-empty subset of $\mathbb{N}$ has a least/minimum element. In other words, if $S \subseteq \mathbb{N}$ and if $S \neq \phi$, then, there exists $m \in S$ such that $m \leq x$, for all $x \in S$.

Example 2.1:3

Let $S \subseteq \mathbb{N}$. Then

i) if $S = \mathbb{N}$, the minimum element of S is 1.

ii) if $S \subset \mathbb{N}$ is the set of even numbers, the minimum element of S is 2.

iii) if $S = \{2, 4, 10\}$, the minimum element of S is 2.

The following theorem plays an important role.

Theorem 2.1.4

Following statements are equivalent.

i) Well Ordering Principle (WOP): Every non-empty subset of $\mathbb{N}$ has a least element.

ii) Principle of Induction (POI): Let $S \subseteq \mathbb{N}$ be such that

  a) $1 \in S$, and

  b) $k+1 \in S$ whenever $k \in S$.

Then, $S = \mathbb{N}$.

iii) Principle of Strong Induction (POSI): Let $T \subseteq \mathbb{N}$ be such that

  a) $1 \in T$

  b) $k+1 \in T$ whenever $\{1, \ldots, k\} \subseteq T$.

Then, $T = \mathbb{N}$.

$\mathbb{N}$

PROOF: We prove the theorem in three steps.

STEP 1. (i) $\Rightarrow$ (ii)

In this case, we assume i) i.e. the well-ordering principle. Let $S \subseteq \mathbb{N}$ be such that $1 \in S$, and $k+1 \in S$ whenever $k \in S$. We shall prove that $S = \mathbb{N}$.

Let us suppose, to the contrary, that $S \subsetneq \mathbb{N}$. Let, $X := \mathbb{N} \setminus S$. Then, $X \neq \phi$. Hence, by Well-Ordering principle, X has a least element, say m. Since $1 \in S$, we have $1 \notin X$, and therefore, $m > 1$. As m is the least element of X, we have $m-1 \notin X$. Therefore, $m-1 \in S$, which implies, using a property of S, that $m = (m-1)+1 \in S$. This leads to a contradiction as $m \in X$ and $X \cap S = \phi$, which proves (ii).

In the next step, we prove that

STEP 2. (ii) $\Rightarrow$ (iii)

In this case, we assume ~~that~~ (ii). Let $T \subseteq \mathbb{N}$ be such that $1 \in T$, and $k+1 \in T$ whenever $\{1, \ldots, k\} \subseteq T$. We shall prove that $T = \mathbb{N}$.

To this end, let us define

$$A := \{ k \in \mathbb{N} \mid \{1, \ldots, k\} \subseteq T \}.$$

We claim that $A = \mathbb{N}$. This follows from (ii). Indeed, we note that $1 \in A$ as $1 \in T$. Let us suppose that $k \in A$. This implies that $\{1, \ldots, k\} \subseteq T$. Using the hypothesis on T, it follows that $k+1 \in T$. Therefore,

$$\{1, \ldots, k+1\} = \{1, \ldots, k\} \cup \{k+1\} \subseteq T,$$

which shows that $k+1 \in A$. Hence, A has the following properties $1 \in A$, and $k+1 \in A$ whenever $k \in A$. Invoking ii), we deduce that $A = \mathbb{N}$. Hence, for all $n \in \mathbb{N}$, $\{1, \ldots, n\} \subseteq T$, which implies that $T = \mathbb{N}$. This proves (iii) assuming (ii).

It remains to prove

STEP 3. (iii) $\Rightarrow$ (i)

In this case, we assume (iii). ~~Let $S \subseteq \mathbb{N}$ be non-empty.~~ We shall prove the Well-ordering principle. Let $S \subseteq \mathbb{N}$ be such that S has no least element. We shall show that $S = \phi$. Let us write $B := \mathbb{N} \setminus S$. It is enough to prove that $B = \mathbb{N}$. This is proved using (iii).

a) That $1 \in B$ follows from the observation that $1 \notin S$.

Indeed, if $1 \in S$, S will have the least element 1 which contradicts the hypothesis that S has no least element.

b) Let $\{1, \ldots, k\} \subseteq \cancel{X}$. Then, $a > k$ for all $a \in S$. This implies that $k+1 \notin S$. For if $k+1 \in S$, $k+1$ will be the least element of S. Which again contradicts the hypothesis that S has no least element. Therefore, $k+1 \notin S$ i.e. $k+1 \in X$. Hence, X has the property that $k+1 \in X$ whenever $\{1, \ldots, k\} \subseteq X$.

Hence invoking (iii), we have $X = \mathbb{N}$. i.e. $S = \phi$. This proves (i), which completes the proof of the theorem. (Proved).

Principles of induction have important applications in proving mathematical results.

Theorem 2.1.5 (PROOF USING MATHEMATICAL INDUCTION)

i) Let us suppose that, a statement $P(n)$ is given, for all $n \in \mathbb{N}$. If

a) **BASE STEP:** $P(1)$ is true, and

b) **INDUCTION STEP:** $P(k+1)$ is true whenever $P(k)$ is true.

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

ii) Let us suppose that, a statement $Q(n)$ is given, for all ~~$n \in$~~ $n \in \mathbb{N}$. If

a) **BASE STEP:** $Q(1)$ is true, and

b) **INDUCTION STEP:** $Q(k+1)$ is true whenever $Q(1), \ldots, Q(k)$ are true.

Then, $Q(n)$ is true, for all $n \in \mathbb{N}$.

PROOF: i) Let $A := \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$. It is enough to prove that $A = \mathbb{N}$. Indeed, we note that $1 \in A$ because of a). Furthermore, using b), whenever $k \in A$, we have $k+1 \in A$. Hence, it follows from POI of Theorem 2.1.4 that $A = \mathbb{N}$.

ii) Similar. Use POSI of Theorem 2.1.4. This proves the theorem. (Proved).

Example 2.1.6 (Proofs Using Mathematical Induction)

i) For all $n \in \mathbb{N}$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6} \qquad (*)$$

Let $P(n)$ be the statement $(*)$.

STEP 1. Base Case:

When $n = 1$, LHS = RHS = 1. Therefore $P(1)$ is true.

STEP 2. Induction Step:

Let us suppose that $P(k)$ is true. i.e.

$$\left(1^2 + \cdots + k^2\right) = \frac{k(k+1)(2k+1)}{6}.$$

Then,

$$1^2 + \cdots + (k+1)^2 = \left(1^2 + \cdots + k^2\right) + (k+1)^2$$

$$= \frac{1}{6} k(k+1)(2k+1) + (k+1)^2 = \frac{1}{6}(k+1)\left[k(2k+1) + 6k + 6\right]$$

$$= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right) = \frac{1}{6}(k+1)(k+2)(2k+3),$$

i.e. $P(k+1)$ is true.

Therefore, by Theorem 2.1.5, $P(n)$ is true for all $n \in \mathbb{N}$. This proves the result.

ii) **FIBONACCI SEQUENCE:** Let us define the sequence $(f_n)_{n \in \mathbb{N} \cup \{0\}}$ by,

$$\begin{cases} f_0 := 0 \;;\; f_1 := 1 \;; \\ f_n := f_{n-1} + f_{n-2}, \quad \text{for all } n \in \mathbb{N}, n \geq 2. \end{cases}$$

Then, for all $n \in \mathbb{N} \cup \{0\}$,

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right] \qquad (*)$$

Let $Q(n)$ be the statement $(*)$.

STEP 1. Base Case:

~~Let~~ When $n = 0$, LHS = RHS = 0. Therefore, $Q(0)$ is true

STEP 2. INDUCTION STEP.

Let us suppose that $Q(0), \ldots, Q(k)$ is true. We shall show that $Q(k+1)$ is true. Indeed,

$$f_{k+1} = f_{k} + f_{k-1} = \underbrace{\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k} - \left(\frac{1-\sqrt{5}}{2}\right)^{k}\right]}_{Q(k)} + \underbrace{\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right]}_{Q(k-1)}$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left[\frac{1+\sqrt{5}}{2}+1\right] - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left[\frac{1-\sqrt{5}}{2}+1\right]$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{6+2\sqrt{5}}{4}\right) - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left[\frac{6-2\sqrt{5}}{4}\right]$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k-1}\left(\frac{1+\sqrt{5}}{2}\right)^{2} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\left(\frac{1-\sqrt{5}}{2}\right)^{2}$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{k+1}.$$

i.e. $Q(k+1)$ is true. Hence, it follows from Theorem 2.1.5 that, $Q(n)$ is true, for all $n \in \mathbb{N}$. This proves the result.

iii) FUNDAMENTAL THEOREM OF ARITHMETIC:

Every integer $n \geq 2$ is a product of (not necessarily distinct) primes.

Let $Q(n)$ be the statement that n is a product of (not necessarily distinct) primes.

STEP 1. Base Case

Since 2 is a prime, $Q(2)$ holds true.

STEP 2. INDUCTION STEP

Let us suppose that $Q(2), \ldots, Q(k)$ is true. We shall show that $Q(k+1)$ is true. If $k+1$ is prime, we are done. Otherwise, there exists $a, b \in \mathbb{N}$ with $2 \leq a, b \leq k$ such that $k+1 = ab$.

Since $Q(a)$, $Q(b)$ are assumed to be true, we can write a, b as products of (not necessarily distinct) primes. This, in turn, implies that, $k+1$ can be written as products of (not necessarily distinct) primes. i.e. $Q(k+1)$ is true.

Hence, it follows from Theorem 2.1.5 that $Q(n)$ is true, for all $n \in \mathbb{N}$, $n \geq 2$. This proves the result.

SECTION 2.2 INTEGERS

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

DEFINITION 2.2.1 ($\mathbb{Z}$-equivalence Relation)
Define $\sim_{\mathbb{Z}}$ on $\mathbb{N} \times \mathbb{N}$ by, for all $(m,n), (p,q) \in \mathbb{N} \times \mathbb{N}$,

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

LEMMA 2.2.2

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

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

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

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: Exercise.

DEFINITION 2.2.3 (INTEGERS)

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

$$\boxed{\bar{0} := [(1,1)] \text{ and } \bar{1} := [(2,1)]}$$

Let $a := [(m,n)]$, $b := [(p,q)] \in \mathbb{Z}$. We define

i) ADDITION:

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

ii) MULTIPLICATION:

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

We have the following important theorem.

THEOREM 2.2.4

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

ii) $a+\bar{0} = a = \bar{0}+a$, for all $a \in \mathbb{Z}$.

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

iv) For all $a, b \in \mathbb{Z}$, there exists a unique $x \in \mathbb{Z}$ such that $a+x=b$.

i') $\cdot$ is well-defined, associative and commutative.

ii') $a \cdot \bar{1} = a = \bar{1} \cdot a$, for all $a \in \mathbb{Z}$.

iii') For all $a, b, \in \mathbb{Z}$, $a \cdot (b+c) = a \cdot b + a \cdot c$.

In other words, $(\mathbb{Z}, +, \cdot)$ is a commutative ring with identity.

To prove Theorem 2.2.4, we start with a Lemma.

LEMMA 2.2.5

For all $n, p, q \in \mathbb{N}$, $n+p = n+q \Rightarrow p=q$.

PROOF: We prove using induction on n. When $n=1$, $S(p) = 1+p = 1+q = S(q)$. As S is 1-1, (assumption 2.1.1½) 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. (Proved).

We are now ready to prove Theorem 2.2.4.

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

$$[\cancel{(m,n)}(m+p,\ n+q)] = [(m'+p',\ n'+q')] \quad (*)$$

Indeed, as $[(m,n)] = [(m',n')]$, we have $m+n' = n+m'$.
Similarly, we have $p+q' = q+p'$.

Therefore,
$$\begin{aligned} & m+n'+p+q' = n+m'+q+p'. \\ \Rightarrow\ & (m+p)+(n'+q') = (n+q)+(m'+p'). \\ \Rightarrow\ & (m+p,\ n+q) \sim_{\mathbb{Z}} (m'+p',\ n'+q') \text{ i.e.} \end{aligned}$$

$$[(m+p,\ n+q)] = [(m'+p',\ n'+q')],$$

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

We now check the associativity of $+$. Let $a,b,c \in \mathbb{Z}$ be ~~do~~ written as
$$a = [(m,n)],\quad b = [(p,q)],\quad c = [(r,s)].$$
Then,
$$\begin{aligned} (a+b)+c &= ([(m,n)] + [(p,q)]) + [(r,s)] \\ &= ([(m+p,\ n+q)]) + [(r,s)] \\ &= [((m+p)+r,\ (n+q)+s)] \\ &= [(m+(p+r),\ n+(q+s))] \\ &= a+(b+c), \text{ which shows that } + \text{ is associative.} \end{aligned}$$

Commutativity of $+$ is left as an exercise.

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

$$a + \overline{0} = [(m,n)] + [(1,1)] = [(m+1, n+1)] = [(m,n)] = \overline{a}.$$

as $(m+1, n+1) \sim_{\mathbb{Z}} (m,n)$. Therefore, we have proved that

$$a + \overline{0} = \overline{a} = \overline{0} + a \quad , \text{for all } a \in \mathbb{Z}.$$

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

$$x := [(n, m)].$$

Then, $a + x = [(m,n)] + [(n,m)] = [(m+n, m+n)] = [(1,1)] = \overline{0}$

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

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

We 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 ~~write~~ define $x := (-a) + b$. Then,

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

The uniqueness of x is left as an exercise.

We now establish the properties of multiplication on $\mathbb{Z}$. In this note, we only prove that the multiplication is well-defined. Proofs of other properties of the multiplication is similar to that of the addition operation and are left as exercises.

i') ~~Let us suppos~~ We prove that the multiplication on $\mathbb{Z}$ is well-defined.

Let $a, b \in \mathbb{Z}$ be written as
$a = [(m,n)] = [(m',n')]$, and $b = [(p,q)] = [(p',q')]$.

We shall show that
$$[(m,n)][(p,q)] = [(m',n')][(p',q')]$$
i.e.
$$[(mp+nq, mq+np)] = [(m'p'+n'q', m'q'+n'p')]$$
i.e.
$$\boxed{mp + nq + m'q' + n'p' = mq + np + m'p' + n'q' \cdot \quad (*)}$$

To prove $(*)$, we proceed as follows. We have

$$\begin{cases} m + n' = n + m' & (*_1) \\ p + q' = q + p' & (*_2). \end{cases}$$

Therefore,
$$\begin{aligned}
(*_1) \times p &\Rightarrow & mp + n'p &= np + m'p. \\
(*_1) \times q &\Rightarrow & mq + n'q &= nq + m'q \\
(*_2) \times m' &\Rightarrow & m'p + m'q' &= m'q + m'p' \\
(*_2) \times n' &\Rightarrow & n'p + n'q' &= n'q + n'p'
\end{aligned}$$

This implies that
$$mp + n'p + nq + m'q + m'p + m'q' + n'q + n'p'$$
$$= np + m'p + mq + n'q + m'q + m'p' + n'p + n'q'$$
$$\Rightarrow (mp + nq + m'q' + n'p') + [n'p + m'q + m'p + n'q]$$
$$= (mq + np + m'p' + n'q') + [n'p + m'q + m'p + n'q]$$

Invoking Lemma 2.2.5, we conclude that

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

which proves $(*)$. Hence, the multiplication is well-defined on $\mathbb{Z}$. This proves i') and ii'). Proof of iii') is left as an exercise. This proves the theorem. (Proved)

Before, we proceed further, let us introduce the following notation.

NOTATION 2.2.6

We write
$$\boxed{\mathbb{Z}^+ := \{ [(j,1)] : j \in \mathbb{N}, j \geq 2 \}}.$$

THEOREM 2.2.7 (Embedding of $\mathbb{N}$)

Define $f : \mathbb{N} \to \mathbb{Z}$ by
$$\boxed{f(n) := [(n+1, 1)], \text{ for all } n \in \mathbb{N}.}$$

Then, f satisfies the following properties.

i) f is one-one.

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

iii) $f(1) = \bar{1}$

iv) for all $m, n \in \mathbb{N}$,
$$f(m+n) = f(m) + f(n), \quad f(mn) = f(m) f(n).$$

PROOF: Exercise. (Proved).

COROLLARY 2.2.8

Let $f : \mathbb{N} \to \mathbb{Z}$ be the map defined in Theorem 2.2.7. Then,
$$\mathbb{Z} = \{ f(n) \mid n \in \mathbb{N} \} \cup \{ -f(n) \mid n \in \mathbb{N} \} \cup \{ \bar{0} \}.$$

CONVENTION. 2.2.9

Let $f : \mathbb{N} \to \mathbb{Z}$ be the embedding map defined in Theorem 2.2.7. We shall identify $f(n)$ with n, for all $n \in \mathbb{N}$. Then, $\mathbb{Z} = \{ n \in \mathbb{N} \} \cup \{ -n \mid n \in \mathbb{N} \} \cup \{ \bar{0} \}$. In particular, $\mathbb{N} \subset \mathbb{Z}$.

We conclude the section by introducing order in $\mathbb{Z}$.

DEFINITION 2.2.10 (Order in $\mathbb{Z}$).

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

i) $a > b$ if and only if there exists $x \in \mathbb{Z}^+$ such that $b + x = a$.

ii) $a \geq b$ if and only if either $a > b$ or $a = b$.

SECTION 2.3. RATIONAL NUMBERS

We conclude this chapter by constructing the set of rational numbers out of the set of integers. The construction, in this case as well, proceeds through an appropriate equivalence relation.

DEFINITION 2.3.1 ($\mathbb{Q}$-equivalence Relation)

Define $\sim_{\mathbb{Q}}$ on $\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$ by, for all $(a,b),(p,q)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})$,

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

LEMMA 2.3.2

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

PROOF: Exercise. (Proved).

DEFINITION 2.3.3 (RATIONAL NUMBERS)

Let us write

$$\mathbb{Q} := \mathbb{Z}\times(\mathbb{Z}\setminus\{0\})/\sim_{\mathbb{Q}} = \{[(a,b)] : (a,b)\in\mathbb{Z}\times(\mathbb{Z}\setminus\{0\})\}$$

We also write

$$\bar{0} := [(0,1)]; \quad \bar{1} := [(1,1)].$$

Let $a := [(a_1, a_2)]$, $b := [(b_1, b_2)] \in \mathbb{Q}$. Then, we define

i) ADDITION:

$$a+b :\stackrel{\text{def}^n}{=} [(a_1 b_2 + a_2 b_1 ; a_2 b_2)]$$

ii) MULTIPLICATION:

$$a\cdot b :\stackrel{\text{def}^n}{=} [(a_1 b_1 , a_2 b_2)]$$

In the next theorem, we establish the algebraic properties of $\mathbb{Q}$.

THEOREM 2.3.4

A) ADDITION: ($(\mathbb{Q},+)$ is an Abelian group)

i) $+$ is well defined, associative and commutative.

ii) $a+\bar{0} = a = \bar{0}+a$.

iii) For all $a\in\mathbb{Q}$, there exists a unique x, denoted by $-a$, satisfying $a+x=\bar{0}$. We say that $-a$ is the negative of a.

B) MULTIPLICATION ($(\mathbb{Q}\setminus\{0\}, \cdot)$ is an Abelian group):

i) $\cdot$ is well-defined, associative and commutative.

ii) $a \cdot \bar{1} = a = \bar{1} \cdot a$, for all $a \in \mathbb{Q}\setminus\{0\}$.

iii) For all $a \in \mathbb{Q}\setminus\{0\}$, there exists a unique $y \in \mathbb{Q}$, denoted by a^{-1}, such that $a.y = \bar{1} = y.a$

We say that a^{-1} is the inverse of a.

C) $a.(b+c) = a.b + a.c$ for all $a, b, c \in \mathbb{Q}$.

In other words, $(\mathbb{Q}, +, \cdot)$ is a field.

PROOF: Exercise. (Proved)

DEFINITION 2.3.5 (ORDER IN $\mathbb{Q}$)

Let $a, b \in \mathbb{Q}$. Then, there exists $m, p \in \mathbb{Z}$ and $n, q \in \mathbb{N}$ such that

$$a = [(m, n)], \quad b = [(p, q)].$$

Then, we say that

i) $a > b$ if and only if $mq > np$.

ii) $a \geq b$ if and only if either $a = b$ or $a > b$.

THEOREM 2.3.6 (EMBEDDING OF $\mathbb{Z}$)

Define $I_{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Q}$ by

$$I_{\mathbb{Z}}(n) := [(n, 1)], \text{ for all } n \in \mathbb{Z}.$$

Then,

i) $I_{\mathbb{Z}}$ is one-one

ii) $I_{\mathbb{Z}}(m+n) = f(m) + f(n)$, $I_{\mathbb{Z}}(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}$.

iii) $I_{\mathbb{Z}}(0_{\mathbb{Z}}) = \bar{0}$

iv) $I_{\mathbb{Z}}(1_{\mathbb{Z}}) = \bar{1}$

v) for all $m, n \in \mathbb{Z}$ with $m < n$, we have $I_{\mathbb{Z}}(m) < I_{\mathbb{Z}}(n)$.

PROOF: Exercise. (Proved)

CONVENTION 2.3.7

Identifying $I_{\mathbb{Z}}(n)$ with n for all $n \in \mathbb{Z}$, we say that $\mathbb{Z} \subset \mathbb{Q}$.