2. Number Systems

> "God made the integers;
> all else is the work of man."
> ~ Leopold Kronecker

We shall study number systems in this chapter. There are practical uses of numbers in our daily lives. Naturally, number systems have a profound significance in our world. In fact, mathematical writing predates literature by more than a thousand years. It even predates the oldest surviving written story "The Epic of Gilgamesh," a Sumerian poem written during 1800 BC. The oldest written record, which is about an exercise in calculating the areas of two fields, dates back to 3350 - 3200 BC. This was found in the reused building rubble in the city of Uruk.

§2.1. Natural Numbers

We use natural numbers mainly for counting and ordering. It arises so "naturally" in everyday computations that it is believed to be a direct consequence of human psyche by a school of philosophers; refer to Kronecker's quote. In opposition to the aforementioned group of philosophers, the constructivists saw a need to define natural numbers rigorously within the framework of set theory. This was carried out by Grassmann, Dedekind, Peano and others.

CONVENTION 2.1.1

We write $\mathbb{N}$ to denote the set of all natural numbers. Note that $\mathbb{N} = \{1, 2, 3, \dots\}$ and it comes with a distinguished element 1 which is the least element of $\mathbb{N}$. It also has two algebraic operations: addition $(+)$ and multiplication $(\times)$, defined on it. Moreover, there is also the successor map

$$S : \mathbb{N} \to \mathbb{N}, \quad S(n) := n+1 \text{ for any } n \in \mathbb{N}.$$

Note that S is one-one and $1 \notin \text{range}(S)$. We will also assume that $\mathbb{N}$ satisfies the following important property.

WELL-ORDERING PRINCIPLE (WOP)

Every non-empty subset of $\mathbb{N}$ has a least element, i.e., if $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then there exists $m \in S$ such that $m \leq x$ for any $x \in S$.

EXAMPLES 2.1.2

i) If $S = \mathbb{N}$, then the least element is 1.

ii) If $S = \{2, 4, 6, 8, \dots\}$ is the set of even numbers, then the least element is 2.

iii) If $S = \{7, 13, 19\}$, then the least element is 7.

The following theorem plays an important role.

THEOREM 2.1.3

The 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 $S \subseteq \mathbb{N}$ such that
 a) $1 \in S$ & 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) $k+1 \in S$ whenever $\{1, 2, \dots, k\} \subseteq S$.
 Then $T = \mathbb{N}$.

Proof. We shall prove the theorem in three steps.

STEP 1 i) $\Rightarrow$ ii)

We assume the well-ordering principle. Now let $S \subseteq \mathbb{N}$ be such that $1 \in S$ and $k+1 \in S$ whenever $k \in S$. Assume, on the contrary, that $S \subsetneq \mathbb{N}$. Let $X := \mathbb{N} \setminus S$. As it is non-empty, by well-ordering principle, X has a least element, say m. As $1 \in S$, we have $1 \notin X$. Thus, $m > 1$ & $m-1 \notin X$, m being the least element of X. Therefore, $m-1 \in S$ & by the property of S, $m \in S$. This is a contradiction as $m \in X \cap S$ but $X \cap S = \emptyset$. Thus, $S = \mathbb{N}$.

STEP 2 ii) $\Rightarrow$ iii)

We assume that $T \subseteq \mathbb{N}$ satisfies $1 \in T$ and $k+1 \in T$ whenever $\{1, 2, \dots, k\} \subseteq T$. Let us define

$$A := \{ k \in \mathbb{N} \mid \{1, 2, \dots, k\} \subseteq T \}.$$

Note that $1 \in A$ as $\{1\} \subseteq T$. If $k \in A$, then $\{1, 2, \dots, k\} \subseteq T$ & by the property of T, $k+1 \in T$. Thus,

$$\{1, 2, \dots, k, k+1\} = \{1, 2, \dots, k\} \cup \{k+1\} \subseteq T.$$

This implies that $k+1 \in A$. Invoking ii) for A, we conclude that $A = \mathbb{N}$. Hence, for any $k \in \mathbb{N}$, $\{1, 2, \dots, k\} \subseteq T$, which implies $T = \mathbb{N}$.

STEP 3 iii) $\Rightarrow$ i)

We assume iii) & let $S \subseteq \mathbb{N}$ be a non-empty subset without a least element. We shall show that $S = \emptyset$, arriving at a contradiction. Let $B := \mathbb{N} \setminus S$; we will show that $B = \mathbb{N}$. As S has no least element, $1 \notin S$. Thus, $1 \in B$. Let $\{1, 2, \dots, k\} \subseteq B$; this implies that $a > k$ for any $a \in S$. Note that $k+1 \notin S$ for if it did, then $k+1$ will be the least element of S which contradicts the hypothesis on S. Hence, $k+1 \notin S$ & $k+1 \in B$. Now, invoking iii) for B, we conclude that $B = \mathbb{N}$. This proves i) and completes the proof of the theorem. $\blacksquare$

Principles of induction have important applications in proving mathematical results.

THEOREM 2.1.4 (MATHEMATICAL INDUCTION)

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

a) $P(1)$ is true (base step)

b) $P(k+1)$ is true whenever $P(k)$ is true (inductive step)

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

Proof. Let $A := \{n \in \mathbb{N} \mid P(n) \text{ is true}\}$. It suffices to prove that $A = \mathbb{N}$. Note that $1 \in A$ by a). By b), whenever $k \in A$, we have $k+1 \in A$. By Theorem 2.1.3 ii), it follows that $A = \mathbb{N}$. ■

THEOREM 2.1.5 (STRONG MATHEMATICAL INDUCTION)

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

a) $Q(1)$ is true (base step)

b) $Q(k+1)$ is true whenever $Q(1), \ldots, Q(k)$ are true (inductive step)

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

The proof is left as an exercise; use the principle of strong induction (Theorem 2.1.3).

IN JEST

- THEOREM: All people have the same sex.

  Proof. Base case: In a group of 1 person, obviously everyone has the same sex.

  Inductive step: Suppose all groups of size k have the same sex. For a group of $k+1$ persons, the first k people have the same sex and the last k people have the same sex. Thus, everyone has the same sex & by induction, we are done. ■?

- A math student invented a new method of making liquor, using electromagnetics to distill alcohol. This is an instance of proof by induction.

EXAMPLES 2.1.6

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

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

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

Base case: When $n = 1$, left hand side & right hand side equals 1. Thus, $P(1)$ is true.

Induction step: Suppose that $P(k)$ is true, i.e.,

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

Then, adding $(k+1)^2$ to both sides above, we get

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

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

$$= \frac{(k+1)}{6}(2k^2 + 7k + 6)$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}.$$

Thus, $P(k+1)$ is true. By Theorem 2.1.4, $P(n)$ is true for all $n \in \mathbb{N}$.

ii) Let us define the FIBONACCI SEQUENCE by

$$f_0 := 0, \; f_1 := 1, \; f_n = f_{n-1} + f_{n-2} \text{ for } n \geq 2.$$

We claim that for $n \in \mathbb{N} \cup \{0\}$.

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

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

Base case: As $f_1 = 1$ (by definition) and the right hand side of the expression also equals 1, $Q(1)$ is true. Similarly, $f_0 = 0$ & the right hand side is also zero. as well as f_2 equals the right hand side.

Induction step: Suppose that $Q(1), \ldots, Q(k)$ is true.

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

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

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

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

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

Thus, $Q(k+1)$ is true & by Theorem 2·1·5, $Q(n)$ is true for all $n \in \mathbb{N}$.

iii) We shall prove the fundamental theorem of arithmetic, i.e., 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 primes.

Base case: As 2 is a prime, $Q(2)$ is true.

Induction step: Suppose that $Q(2), \ldots, Q(k)$ is true. If $k+1$ is a prime, then $Q(k+1)$ is true. Otherwise, there exists $a, b \in \mathbb{N}$ with $2 \leq a, b \leq k$ such that $k+1 = ab$. As $Q(a)$ and $Q(b)$ hold, we may write a & b as product of primes. Thus, $k+1 = ab$ can be written as a product of primes and $Q(k+1)$ is true. By Theorem 2·1·5, $Q(n)$ is true for all $n \in \mathbb{N}$.

§2·2 INTEGERS

We shall construct the set of integers from the set of natural numbers. We shall use an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

DEFINITION 2·2·1 ($\mathbb{Z}$-EQUIVALENCE RELATION)

Define $\sim_{\mathbb{Z}}$ on $\mathbb{N} \times \mathbb{N}$ as follows: for $(m,n), (p,q) \in \mathbb{N} \times \mathbb{N}$,

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

The relation is reflexive, symmetric & transitive. Note that

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

Thus, the equivalence classes of $\sim_{\mathbb{Z}}$ may be represented as

$$\{[(j,1)] \mid j \in \mathbb{N}, j \geq 2\} \cup \{[(1,k)] \mid k \in \mathbb{N}, k \geq 2\} \cup \{[(1,1)]\}.$$

We also denote $[(1,1)]$ by $\bar{0}$ & $[(2,1)]$ by $\bar{1}$.

Definition 2.2.2 (Integers)

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

We shall define two binary operations on $\mathbb{Z}$.

i) Addition: If $a=[(m,n)]$ and $b=[(p,q)]$, then
$$a+b := [(m+p,n+q)]$$

ii) Multiplication: $a\cdot b := [(mp+nq, mq+np)]$.

The motivation for multiplication arises from the fact that we are seeing $a-b$ as (a,b). Thus, $(a-b)(c-d)$ corresponds to $[(a,b)][(c,d)]$. As $(a-b)(c-d) = (ac+bd)-(ad+bc)$, this motivates the definition in ii).

Theorem 2.2.3

a) Consider $(\mathbb{Z},+)$.

i) $+$ is well-defined, associative & 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 $a+x=b$.

b) Consider $(\mathbb{Z},\times)$ (or $(\mathbb{Z},\cdot)$).

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

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

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

The above important result can be summarized by saying that $(\mathbb{Z},+,\cdot)$ is a commutative ring with identity. To prove Theorem 2.2.3, we require a lemma.

Lemma 2.2.4

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

Proof. We shall prove this by induction on n. When $n=1$, note that $p+1=S(p)=S(q)=q+1$, where S is the successor map from convention 2.1.1. As S is one-one, it follows that $p=q$. Now suppose that for some k, $k+p'=k+q'$ implies $p'=q'$ for $p', q' \in \mathbb{N}$. Consider $(k+1)+p=(k+1)+q$, rewritten as

$$k+(p+1) = k+(q+1).$$

This implies $p+1=q+1$ and by the base case $p=q$. Now, we are done by induction. $\blacksquare$

Proof of Theorem 2.2.3.

a) i) We first show that $+$ is well-defined. Let

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

This means $m+n'=n+m'$ and $p+q'=q+p'$. Thus,

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

and this proves that $+$ is well-defined.

We now check for associativity of $+$. Let

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

Then,

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

Commutativity of $+$ is left as an exercise.

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

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

as $(m+1,n+1) \sim_{\mathbb{Z}} (m,n)$. Thus, $a+\bar{0}=a$ & similarly we can show $\bar{0}+a=a$.

iii) Let $a=[(m,n)] \in \mathbb{Z}$ and define $x := [(n,m)]$. Then

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

Let us suppose there exists $y \in \mathbb{Z}$ such that $a+y=y+a=\bar{0}$.
Using ii),

$$x = \bar{0}+x = (y+a)+x = y+(a+x) = y+\bar{0} = y.$$

Thus, the uniqueness of x is proven.

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

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

If $a+y=b$ for some $y \in \mathbb{Z}$, then

$$(-a)+b = (-a)+(a+y) = ((-a)+a)+y = \bar{0}+y = y$$

and similarly $(-a)+b = x$, implying $x=y$.

b) i) We show that $\cdot$ is well-defined. Let

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

We shall show that

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

or, $$[(mp+nq, np+mq)] = [(m'p'+n'q', n'p'+m'q')]$$

or, $$mp+nq+m'q'+n'p' = mq+np+m'p'+n'q'. \qquad \text{— (2.1)}$$

We proceed as follows. Note that

$$m+n' = n+m' \qquad \text{— (2.2)}$$
$$p+q' = q+p' \qquad \text{— (2.3)}$$

Thus,

$$(\text{Eq}^{\text{n}}\ 2.2)\times p \Rightarrow \quad mp+n'p = np+m'p$$
$$(\text{Eq}^{\text{n}}\ 2.2)\times q \Rightarrow \quad mq+n'q = nq+m'q$$
$$(\text{Eq}^{\text{n}}\ 2.3)\times m' \Rightarrow \quad m'p+m'q' = m'q+m'p'$$
$$(\text{Eq}^{\text{n}}\ 2.3)\times n' \Rightarrow \quad n'p+n'q' = n'q+n'p'$$

This implies that

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

By Lemma 2.2.4, we conclude that

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

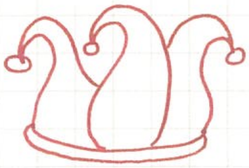
This proves (2.1).

ii) Let $a = [(m,n)]$ & we compute

$$a \cdot \bar{1} = [(m,n)] \cdot [(2,1)] = [(2m+n,\ m+2n)] = [(m,n)]$$

as $(2m+n, m+2n) \sim_{\mathbb{Z}} (m,n)$.

iii) This is left as an exercise. ▨



IN JEST

- We all know 7 ate 9 but why?
  Because it needed to eat three squared meals a day.
- Detective 1: We found a list of negative numbers at the crime scene.
  Detective 2: It doesn't add up!

Let us introduce the following notation.

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

THEOREM 2.2.5 (EMBEDDING OF $\mathbb{N}$)

Define $f : \mathbb{N} \to \mathbb{Z}$ by

$$f(n) := [(n+1, 1)] \text{ for any } n \in \mathbb{N}.$$

Then f satisfies the following properties:

i) f is one-one
ii) $f(\mathbb{N}) = \mathbb{Z}^+$
iii) $f(1) = \bar{1}$
iv) $f(m+n) = f(m) + f(n)$, $f(mn) = f(m) \cdot f(n)$ for $m, n \in \mathbb{N}$.

The proof is left as an exercise. As a corollary, we see that

$$\mathbb{Z} = \{ f(n) \mid n \in \mathbb{N} \} \cup \{ -f(n) \mid n \in \mathbb{N} \} \cup \{ \bar{0} \}.$$

This also allows us to identify $f(n)$ with n for any $n \in \mathbb{N}$. Thus, $\mathbb{N}$, identified with $\mathbb{Z}^+$, is a subset of $\mathbb{Z}$. We end this section by introducing order in $\mathbb{Z}$.

DEFINITION 2.2.6 (ORDER IN $\mathbb{Z}$)

For any $a, b \in \mathbb{Z}$, 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 $a > b$.

Examples 2.2.7

i) Let $n \in \mathbb{N}$ be identified with $[(n+1,1)]$. We note that $n > 0$ (or, equivalently $[(n+1,1)] > [(1,1)] =: \bar{0}$) as

$$[(n+1,1)] = [(n+2,2)] = [(n+1,1)] + [(1,1)]$$

and $n+1 \geqslant 2$.

ii) Let $n \in \mathbb{N}$ & m be a negative integer, i.e.,

$$n = [(n+1,1)] \quad \& \quad m = [(1,1-m)]$$

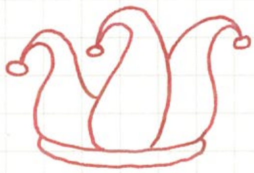
Then

$$[(n+1,1)] = [(n+1+1-m, 1+1-m)] = [(n+1-m,1)] + [(1,1-m)].$$

As $n+1-m \geqslant 3$, $n > m$ follows.

§2.3 Rational Numbers

We conclude this chapter by constructing rational numbers out of the set of integers. The construction, as expected, proceeds via an appropriate equivalence relation.



IN JEST

Holding a gun to the hostage, the terrorist demanded, "Tell me the square root of 2!"
The hostage begged, "Please, let's be rational here."

Definition 2.3.1 ($\mathbb{Q}$-equivalence relation)

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

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

It is clear that $\sim_{\mathbb{Q}}$ is reflexive & symmetric. If $(a,b) \sim_{\mathbb{Q}} (p,q)$ and $(p,q) \sim_{\mathbb{Q}} (r,s)$, then

$$aq = bp \quad \text{and} \quad ps = qr.$$

Multiply the first equality by s and the second by b to get

$$aqs = bps = bqr$$

By cancellation law (refer to Homework set), $as = br$. This shows that $\sim_{\mathbb{Q}}$ is an equivalence relation. We shall use this to define the set of rational numbers.

DEFINITION 2.3.2 (RATIONAL NUMBERS)

Let us write

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

We write $\bar{0} = [(0,1)]$ and $\bar{1} = [(1,1)]$. We define two algebraic operations on $\mathbb{Q}$.

i) Addition: $[(a_1,a_2)] + [(b_1,b_2)] := [(a_1 b_2 + a_2 b_1, a_2 b_2)]$

ii) Multiplication: $[(a_1,a_2)] \cdot [(b_1,b_2)] := [(a_1 b_1, a_2 b_2)]$.

We now establish the algebraic properties of $\mathbb{Q}$.

THEOREM 2.3.3

a) Consider $(\mathbb{Q}, +)$.

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

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

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

b) Consider $(\mathbb{Q}, \cdot)$.

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

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

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

iv) For all $a \in \mathbb{Q} \setminus \{0\}$, there exists a unique $y \in \mathbb{Q}$ such that $a \cdot y = \bar{1} = y \cdot a$. (We write a^{-1} for y and say that a^{-1} is the inverse of a.)

The proof is left as an exercise. Note that

$$[(a,b)] \cdot [(b,a)] = [(ab, ab)] = [(1,1)]$$

if $a \neq 0$ & $b \neq 0$. The notation of $\bar{1} = [(1,1)] \in \mathbb{Q}$ & $\bar{1} = [(2,1)] \in \mathbb{Z}$ are visually at odds with each other but the 1 in $(2,1)$ is the natural number 1 while the 1 in $(1,1)$ is the integer $\bar{1} \in \mathbb{Z}$. Moreover, the result above can be summarized by saying that $(\mathbb{Q}, +, \cdot)$ is a field. In fact, as we shall see, it is an ordered field.

Definition 2.3.4 (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 $a = [(m,n)]$ and $b = [(p,q)]$. We say that

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

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

Note that any $a \in \mathbb{Q}$ can be written as $[(m', n')]$ for $m' \in \mathbb{Z}$, $n' \in \mathbb{Z} \setminus \{0\}$. If $n' \in \mathbb{Z}^+ (= \mathbb{N})$, we let $a = [(m', n')]$. If $n' \notin \mathbb{Z}^+$, then $-n' \in \mathbb{Z}^+$ & $(m', n') \sim_{\mathbb{Q}} (-m', -n')$. Thus, $a = [(-m', -n')]$.

Theorem 2.3.5 (Embedding of $\mathbb{Z}$)

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

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

Then, $I_{\mathbb{Z}}$ has the following properties

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

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

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

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

v) If $m, n \in \mathbb{Z}$ such that $m < n$, then $I_{\mathbb{Z}}(m) < I_{\mathbb{Z}}(n)$.

The proof of Theorem 2.3.5 is very similar to that of Theorem 2.2.5 (embedding of $\mathbb{N}$). We shall identify n with $I_{\mathbb{Z}}(n)$ for all $n \in \mathbb{Z}$ & say that $\mathbb{Z} \subseteq \mathbb{Q}$. In fact, these embeddings provide a formal setup to identify $\mathbb{N}$ in $\mathbb{Z}$ and $\mathbb{Z}$ in $\mathbb{Q}$. The multiplicative identity 1, in each of the three sets are identified under these embeddings.