



# Foundation of Mathematics 2

## *Chapter 2 System of Numbers*

*Dr. Bassam AL-Asadi and Dr. Emad Al-Zangana*

*Mustansiriyah University-College of Science-Department of Mathematics*

*2018-2019*

# Chapter Two

## System of Numbers

### 1. Natural Numbers

Let  $0 = \text{Set with no point, that is; } 0 = \emptyset$ ,  $1 = \text{Set with one point, that is; } 1 = \{0\}$ ,  
 $2 = \text{Set with two points, that is; } 2 = \{0,1\}$ , and so on. Therefore,

$$1 = \{0\} = \{\emptyset\},$$

$$2 = \{0,1\} = \{\emptyset, \{\emptyset\}\},$$

$$3 = \{0,1,2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$$

$$4 = \{0,1,2,3\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\},$$

$\vdots$

$$n = \{0,1,2,3, \dots, n-1\}.$$

**Definition 2.1.1.** Let  $A$  be a set. A **successor** to  $A$  is  $A^+ = A \cup \{A\}$  and denoted by  $A^+$ .

According to above definition we can get the numbers  $0,1,2,3, \dots$  as follows:

$$0 = \emptyset,$$

$$1 = \{0\} = \emptyset \cup \{\emptyset\} = \emptyset^+ = 0^+,$$

$$2 = \{0,1\} = \{0\} \cup \{1\} = 1 \cup \{1\} = 1^+,$$

$$3 = \{0,1,2\} = \{0,1\} \cup \{2\} = 2 \cup \{2\} = 2^+,$$

**Definition 2.1.2.** A set  $A$  is said to be **successor set** if it satisfies the following conditions:

(i)  $\emptyset \in A$ ,

(ii) if  $a \in A$ , then  $a^+ \in A$ .

**Remark 2.1.3.**

- (i) Any successor set should contains the numbers  $0,1,2, \dots n$ .
- (ii) Collection of all successor sets is not empty.
- (iii) Intersection of any non empty collection of successor sets is also successor set.

**Definition 2.1.4.** Intersection of all successor sets is called **the set of natural numbers** and denoted by  $\mathbb{N}$ , and each element of  $\mathbb{N}$  is called **natural element**.

**Peano's Postulate 2.1.5.**

- (P<sub>1</sub>)  $0 \in \mathbb{N}$ .
- (P<sub>2</sub>) If  $a \in \mathbb{N}$ , then  $a^+ \in \mathbb{N}$ .
- (P<sub>3</sub>)  $0 \neq a^+ \in \mathbb{N}$  for every natural number  $a$ .
- (P<sub>4</sub>) If  $a^+ = b^+$ , then  $a = b$  for any natural numbers  $a, b$ .
- (P<sub>5</sub>) If  $X$  is a successor subset of  $\mathbb{N}$ , then  $X = \mathbb{N}$ .

**Remark 2.1.6.**

- (i) P<sub>1</sub> says that 0 should be a natural number.
- (ii) P<sub>2</sub> states that the relation  $+: \mathbb{N} \rightarrow \mathbb{N}$ , defined by  $+(n) = n^+$  is mapping.
- (iii) P<sub>3</sub> as saying that 0 is the first natural number, or that ' - 1 ' is not an element of  $\mathbb{N}$ .
- (iv) P<sub>4</sub> states that the map  $+: \mathbb{N} \rightarrow \mathbb{N}$  is injective.
- (v) P<sub>5</sub> is called the **Principle of Induction**.

**2.1.7. Addition + on  $\mathbb{N}$**

We will now define the operation of addition + using only the information provided in the Peano's Postulates.

Let  $a, b \in \mathbb{N}$ . We define  $+: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  as follows:

$$+(a, b) = a + b = \begin{cases} a + 0 = a & \text{if } b = 0 \\ a + c^+ = (a + c)^+ & \text{if } b \neq 0 \end{cases}$$

where  $b = c^+$ .

Therefore, if we want to compute  $1 + 1$ , we note that  $1 = 0^+$  and get

$$1 + 1 = 1 + 0^+ = (1 + 0)^+ = 1^+ = 2.$$

We can proceed further to compute  $1 + 2$ .

To do so, we note that  $2 = 1^+$  and therefore that

$$1 + 2 = 1 + 1^+ = (1 + 1)^+ = 2^+ = 3.$$

### 2.1.8. Multiplication $\cdot$ on $\mathbb{N}$

We will now define the operation of multiplication  $\cdot$  using only the information provided in the Peano's Postulates.

Let  $a, b \in \mathbb{N}$ . We define  $\cdot: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  as follows:

$$\cdot(a, b) = a \cdot b = \begin{cases} a \cdot 0 = 0 & \text{if } b = 0 \\ a \cdot c^+ = a + a \cdot c & \text{if } b \neq 0 \end{cases}$$

where  $b = c^+$ .

Thus, we can easily show that  $a \cdot 1 = a$  by noting that  $1 = 0^+$  and therefore

$$a \cdot 1 = a \cdot 0^+ = a + (a \cdot 0) = a + 0 = a.$$

We can use this to multiply  $3 \cdot 2$ . Of course, we know that  $2 = 1^+$  and therefore

$$3 \cdot 2 = 3 \cdot 1^+ = 3 + (3 \cdot 1) = 3 + 3 = 3 + 2^+ = (3 + 2)^+ = 5^+ = 6.$$

**Remark 2.1.9.** From 2.1.7 and 2.1.8 we can deduce that for all  $n \in \mathbb{N}$ , if  $n \neq 0$ , then there exist an element  $m \in \mathbb{N}$  such that  $n = m^+$ .

### Theorem 2.1.10.

(i)  $\boxed{n^+ = n + 1}$ ,  $\boxed{n^+ = 1 + n}$ ,  $\boxed{n = n \cdot 1}$ ,  $\boxed{n = 1 \cdot n}$ ,  $\boxed{0 \cdot n = n}$ ,  $\boxed{0 + n = n}$   
 $\forall n \in \mathbb{N}$ .

(ii) (Associative property of  $+$ )  $\boxed{(n + m) + c = n + (m + c)}$ ,  $\forall n, m, c \in \mathbb{N}$ .

(iii) (Commutative property of  $+$ )  $\boxed{n + m = m + n}$ ,  $\forall n, m \in \mathbb{N}$ .

(iv) (Distributive property of  $\cdot$  on  $+$ )  $\forall n, m, c \in \mathbb{N}$ ,

From right  $\boxed{(n + m) \cdot c = n \cdot c + m \cdot c}$ ,

From left  $\boxed{c \cdot (n + m) = c \cdot n + c \cdot m}$  (The prove depend on (vi)).

(v) (Commutative property of  $\cdot$ )  $\boxed{n \cdot m = m \cdot n}$ ,  $\forall n, m \in \mathbb{N}$ .

(vi) (Associative property of  $\cdot$ )  $\boxed{(n \cdot m) \cdot c = n \cdot (m \cdot c)}$ ,  $\forall n, m, c \in \mathbb{N}$ .

(vii) The addition operation  $+$  defined on  $\mathbb{N}$  is unique.

(viii) The multiplication operation  $\cdot$  defined on  $\mathbb{N}$  is unique.

(ix) (Cancellation Law for  $+$ ).  $\boxed{m + c = n + c}$ , for some  $c \in \mathbb{N} \Leftrightarrow \boxed{m = n}$ .

(x)  $0$  is the unique element such that  $0 + m = m + 0 = m$ ,  $\forall m \in \mathbb{N}$ .

(xi)  $1$  is the unique element such that  $1 \cdot m = m \cdot 1 = m$ ,  $\forall m \in \mathbb{N}$ .

**Proof:**

(i)  $n^+ = (n + 0)^+$  (Since  $n = n + 0$ )  
 $= n + 0^+$  (Def. of  $+$ )  
 $= n + 1$  (Since  $0^+ = 1$ )

(ii) Let  $L_{mn} = \{c \in \mathbb{N} | (m + n) + c = m + (n + c)\}$ ,  $m, n \in \mathbb{N}$ .

(1)  $(m + n) + 0 = m + n = m + (n + 0)$ ; that is,  $0 \in L_{mn}$ . Therefore,  $L_{mn} \neq \emptyset$ .

(2) Let  $c \in L_{mn}$ ; that is,  $(m + n) + c = m + (n + c)$ . To prove  $c^+ \in L_{mn}$ .

$$\begin{aligned} (m + n) + c^+ &= ((m + n) + c)^+ \\ &= (m + (n + c))^+ \quad (\text{since } c \in L_{mn}) \\ &= m + (n + c)^+ \quad (\text{Def. of } +) \\ &= m + (n + c^+) \quad (\text{Def. of } +) \end{aligned}$$

Thus,  $c^+ \in L_{mn}$ . Therefore,  $L_{mn}$  is a successor subset of  $\mathbb{N}$ . So, we get by  $\mathbf{P}_5$   $L_{mn} = \mathbb{N}$ .

(iii) Suppose that  $L_m = \{n \in \mathbb{N} | m + n = n + m\}$ ,  $m \in \mathbb{N}$ . Then prove that  $L_m$  is successor subset of  $\mathbb{N}$ .

(iv) Suppose that  $L_{mn} = \{c \in \mathbb{N} | c \cdot (m + n) = c \cdot m + c \cdot n\}$ ,  $m, n \in \mathbb{N}$ . Then prove that  $L_{mn}$  is successor subset of  $\mathbb{N}$ .

(v) Suppose that  $L_m = \{n \in \mathbb{N} | m \cdot n = n \cdot m\}$ ,  $m \in \mathbb{N}$ . Then prove that  $L_m$  is successor subset of  $\mathbb{N}$ .

(vi) Suppose that  $L_{mn} = \{c \in \mathbb{N} | (m \cdot n) \cdot c = m \cdot (n \cdot c)\}$ ,  $m, n \in \mathbb{N}$ . Then prove that  $L_{mn}$  is successor subset of  $\mathbb{N}$ .

(vii) Let  $\oplus$  be another operation on such that

$$\oplus(a, b) = \begin{cases} a \oplus 0 = a & \text{if } b = 0 \\ a \oplus c^+ = (a \oplus c)^+ & \text{if } b \neq 0 \end{cases}$$

where  $b = c^+$ .

Let  $L = \{m \in \mathbb{N} | n + m = n \oplus m, \forall n \in \mathbb{N}\}$ .

(1) To prove  $0 \in L$ .

$n + 0 = n = n \oplus 0$ . Thus,  $0 \in L$ .

(2) To prove that  $k^+ \in L$  for every  $k \in L$ . Suppose  $k \in L$ .

$$\begin{aligned} n + k^+ &= (n + k)^+ && \text{Def. of } + \\ &= (n \oplus k)^+ && (\text{Since } k \in L) \\ &= n \oplus k^+ && \text{Def. of } \oplus \end{aligned}$$

Thus,  $k^+ \in L$ .

From (1), (2) we get that  $L$  is a successor set and  $L \subseteq \mathbb{N}$ . From  $\mathbf{P}_5$  we get that  $L = \mathbb{N}$ .

(viii) Exercise.

(ix) Suppose that

$L = \{c \in \mathbb{N} | m + c = n + c, \text{ for some } c \in \mathbb{N} \Leftrightarrow m = n\}$ ,  $m, n \in \mathbb{N}$ . Then prove that  $L$  is successor subset of  $\mathbb{N}$ .

(x),(xi) Exercise.

**Definition 2.1.11.** Let  $x, y \in \mathbb{N}$ . We say that  $x$  less than  $y$  and denoted by  $x < y$  iff there exist  $k \neq 0 \in \mathbb{N}$  such that  $x + k = y$ .

**Theorem 2.1.12.**

- (i) The relation  $<$  is transitive relation on  $\mathbb{N}$ .
- (ii)  $0 < n^+$  and  $n < n^+$  for all  $n \in \mathbb{N}$ .
- (iii)  $0 < m$  or  $m = 0$ , for all  $m \in \mathbb{N}$ .

**Proof.**

(i),(ii),(iii) Exercise.

**Theorem 2.1.13.(Trichotomy)**

For each  $m, n \in \mathbb{N}$  one and only one of the following is true:

- (1)  $m < n$  or (2)  $n < m$  or (3)  $m = n$ .

**Proof.**

Let  $m \in \mathbb{N}$  and

$$L_1 = \{n \in \mathbb{N} | n < m\},$$

$$L_2 = \{n \in \mathbb{N} | m < n\},$$

$$L_3 = \{n \in \mathbb{N} | n = m\},$$

$$M = L_1 \cup L_2 \cup L_3.$$

(1)  $L_i \neq \emptyset$  and  $L_i \subseteq \mathbb{N}$ ,  $i = 1, 2, 3$ . Therefore,  $M \subseteq \mathbb{N}$  and  $M \neq \emptyset$ .

(2) To prove that  $M$  is a successor set.

(i) To prove that  $0 \in M$ .

(a) If  $m = 0$ , then  $0 \in L_3 \rightarrow 0 \in M$  (Def. of U)

(b) If  $m \neq 0$ , then  $\exists k \in \mathbb{N} \ni$

$$m = k^+$$

$$\rightarrow 0 < k^+ = m \quad (\text{Theorem 2.1.12(ii)}).$$

$$\rightarrow 0 \in L_1 \rightarrow 0 \in M$$

**Or** If  $m \neq 0$ , then  $0 < m$  (Theorem 2.1.12(iii)).

$$\rightarrow 0 \in L_1 \rightarrow 0 \in M$$

(ii) Suppose that  $k \in M$ . To prove that  $k^+ \in M$ .

Since  $k \in M$ , then  $k \in L_1$  or  $k \in L_2$  or  $k \in L_3$  (Def. of U)

(a) If  $k \in L_1$

$$\rightarrow k < m \quad (\text{Def. of } L_1)$$

$$\rightarrow \exists c \neq 0 \in \mathbb{N} \ni m = k + c \quad (\text{Def of } <)$$

$$\rightarrow \exists l \in \mathbb{N} \ni c = l^+ \quad (\text{Remark 2.1.9})$$

$$\rightarrow m = k + c = k + l^+ \quad (\text{Def. of } +)$$

$$= (k + l)^+$$

$$\rightarrow m = (k + l)^+ = (l + k)^+ \quad (\text{Commutative law for } +)$$

$$\rightarrow m = l + k^+ \quad (\text{Def. of } +)$$

$$\begin{cases} \text{if } l = 0, \text{ then } m = k^+ \rightarrow k^+ \in L_3 \\ \text{if } l \neq 0, \text{ then } k^+ < m \text{ (Def. of } < \text{)} \rightarrow k^+ \in L_1 \end{cases}$$

**b) If  $k \in L_2$**

$$\begin{aligned} \rightarrow m < k & \quad (\text{Def. of } L_2) \\ \rightarrow m < k < k^+ & \quad (\text{Theorem 2.1.12(ii)}) \\ \rightarrow m < k^+ & \quad (\text{Theorem 2.1.12(i)}) \\ \rightarrow k^+ \in L_2 & \quad (\text{Def. of } L_2) \\ \rightarrow k^+ \in M & \quad (\text{Def. of } U) \end{aligned}$$

**(c) If  $k \in L_3$**

$$\begin{aligned} \rightarrow m = k & \quad (\text{Def. of } L_2) \\ \rightarrow m = k < k^+ & \quad (\text{Theorem 2.1.12(ii)}) \\ \rightarrow m < k^+ & \quad (\text{Theorem 2.1.12(i)}) \\ \rightarrow k^+ \in L_2 & \quad (\text{Def. of } L_2) \\ \rightarrow k^+ \in M & \quad (\text{Def. of } U) \end{aligned}$$

### **Theorem 2.1.14.**

- (i) For all  $n \in \mathbb{N}$ ,  $0 < n \Leftrightarrow n \neq 0$ .
- (ii) For all  $m, n \in \mathbb{N}$ , if  $n \neq 0$ , then  $m + n \neq 0$ .
- (iii)  $m + k < n + k \Leftrightarrow m < n$ , for all  $m, n, k \in \mathbb{N}$ .
- (iv) If  $m \cdot n = 0$ , then either  $m = 0$  or  $n = 0$ ,  $\forall m, n \in \mathbb{N}$ . ( $\mathbb{N}$  has no zero divisor)
- (v) (**Cancellation Law for  $\cdot$** )  $m \cdot c = n \cdot c$ , for some  $c (\neq 0) \in \mathbb{N} \Leftrightarrow m = n$ .
- (vi) For all  $k (\neq 0) \in \mathbb{N}$ , if  $m < n$ , then  $m \cdot k < n \cdot k$ , for all  $m, n \in \mathbb{N}$ .
- (vii) For all  $k (\neq 0) \in \mathbb{N}$ , if  $m \cdot k < n \cdot k$ , then  $m < n$ , for all  $m, n \in \mathbb{N}$ .

**Proof.**

**(ii) Case 1:**

$$\begin{aligned} \text{If } m = 0. \\ \rightarrow m + n = 0 + n = n \neq 0 \\ \rightarrow m + n \neq 0 \end{aligned}$$

**Case 2:**

$$\text{If } m \neq 0 \rightarrow 0 < m \quad \text{By (i)}$$

Suppose that  $m + n = 0$

$$\begin{aligned} \rightarrow m < 0 \\ \rightarrow m < 0 \text{ and } 0 < m \end{aligned}$$

Contradiction with Trichotomy Theorem; that is,  $m + n \neq 0$ .

(vii) Let  $m \cdot k < n \cdot k$ . Assume that  $m \not< n$

$\rightarrow n < m$  or  $n = m$  (Trichotomy Theorem)

Suppose  $n = m$

$\rightarrow m \cdot k = n \cdot k$  (Cancellation law of  $\cdot$ )

$\rightarrow m \cdot k = n \cdot k$  and  $m \cdot k < n \cdot k$

$\rightarrow$  Contradiction with (Trichotomy Theorem)

Suppose  $n < m$

$\rightarrow n \cdot k < m \cdot k$  (From (vi))

$\rightarrow n \cdot k < m \cdot k$  and  $m \cdot k < n \cdot k$

$\rightarrow$  Contradiction with Trichotomy Theorem

$\rightarrow \therefore m < n$

**(i),(iii),(iv),(v),(vi) Exercise.**



## 2. Construction of Integer Numbers

Let write  $\mathbb{N} \times \mathbb{N}$  as follows:

$$\mathbb{N} \times \mathbb{N} = \left\{ \begin{array}{cccccc} (0,0) & (0,1) & (0,2) & (0,3) & (0,4) & \cdots & \cdots & \cdots & \cdots \\ (1,0) & (1,1) & (1,2) & (1,3) & (1,4) & \cdots & \cdots & \cdots & \cdots \\ (2,0) & (2,1) & (2,2) & (2,3) & (2,4) & \cdots & \cdots & \cdots & \cdots \\ (3,0) & (3,1) & (3,2) & (3,3) & (3,4) & \cdots & \cdots & \cdots & \cdots \\ (4,0) & (4,1) & (4,2) & (4,3) & (4,4) & \cdots & \cdots & \cdots & \cdots \\ (5,0) & (5,1) & (5,2) & (5,3) & (5,4) & \cdots & \cdots & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \right\}$$

Let define a relation on  $\mathbb{N} \times \mathbb{N}$  as follows:

$$(a, b)R^*(c, d) \Leftrightarrow a + d = b + c$$

**Example 2.2.1.**  $(1,0)R^*(4,3)$  since  $1 + 3 = 0 + 4$ .  
 $(1,0)R^*(6,4)$  since  $1 + 4 \neq 0 + 6$ .

**Theorem 2.2.2.** The relation  $R^*$  on  $\mathbb{N} \times \mathbb{N}$  is an equivalence relation.

**Proof.**

- (1) Reflexive. For all  $(a, b) \in \mathbb{N} \times \mathbb{N}$ ,  $a + b = a + b$ ; that is  $(a, b)R^*(a, b)$ .  
 (2) Symmetric. Let  $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$  such that  $(a, b)R^*(c, d)$ . To prove that  $(c, d)R^*(a, b)$ .

$$\begin{aligned} \rightarrow a + d &= b + c && \text{(Def. of } R^*) \\ \rightarrow d + a &= c + b && \text{(Comm. law for } +) \\ \rightarrow c + b &= d + a && \text{(Equal properties)} \\ \rightarrow (c, d)R^*(a, b) &&& \text{(Def. of } R^*) \end{aligned}$$

- (3) Transitive. Let  $(a, b), (c, d), (r, s) \in \mathbb{N} \times \mathbb{N}$  such that  $(a, b)R^*(c, d)$  and  $(c, d)R^*(r, s)$ . To prove  $(a, b)R^*(r, s)$ .

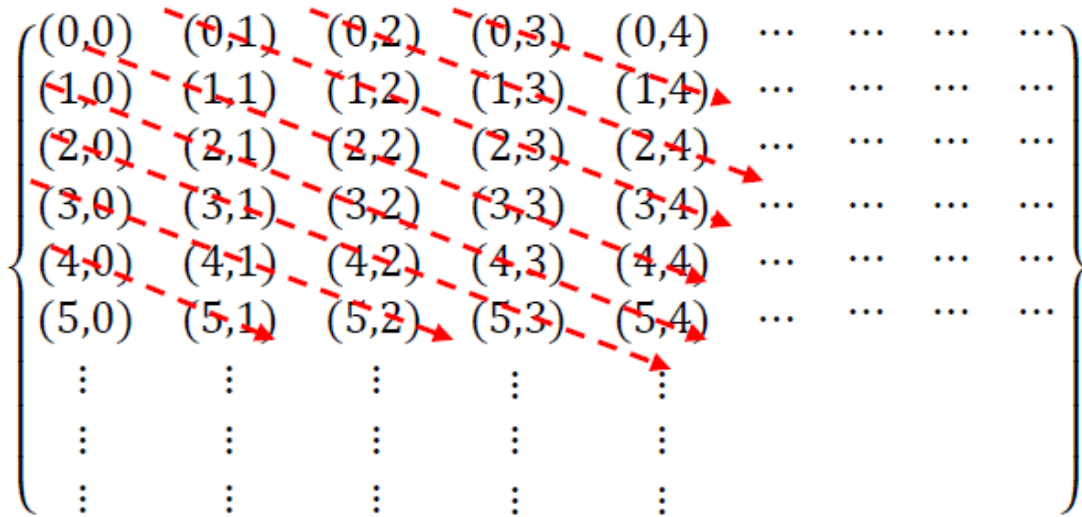
$$\begin{aligned} a + d &= b + c && \text{(Since } (a, b)R^*(c, d)) && \dots(1) \\ c + s &= d + r && \text{(Since } (c, d)R^*(r, s)) && \dots(2) \\ \rightarrow (a + d) + s &= (b + c) + s && \text{(Add } s \text{ to both side of (1))} \\ &= b + (c + s) && \text{(Cancellations low and asso. law for } +) && \dots(3) \\ \rightarrow (a + d) + s &= b + (c + s) && \text{(Sub.(2) in (3))} \\ &= b + (d + r) \end{aligned}$$

- $\rightarrow a + (d + s) = b + (r + d)$  (Asso. law and comm. law for +)  
 $\rightarrow a + (s + d) = b + (r + d)$  (Comm. law for +)  
 $\rightarrow (a + s) + d = (b + r) + d$  (Asso. law for +)  
 $\rightarrow (a + s) = (b + r)$  (Cancellation low for + )  
 $\rightarrow (a, b)R^*(r, s)$  (Def. of  $R^*$ )

**Remark 2.2.3.**

(i) The equivalence class of each  $(a, b) \in \mathbb{N} \times \mathbb{N}$  is as follows:

$$[(a, b)] = [a, b] = \{(r, s) \in \mathbb{N} \times \mathbb{N} | a + s = b + r\}.$$



$$\begin{aligned}
 [1,0] &= \{(x, y) \in \mathbb{N} \times \mathbb{N} | 1 + y = 0 + x\} \\
 &= \{(x, y) \in \mathbb{N} \times \mathbb{N} | x = 1 + y\} \\
 &= \{(y + 1, y) | y \in \mathbb{N}\} \\
 &= \{(1,0), (2,1), (3,2), \dots\}.
 \end{aligned}$$

$$\begin{aligned}
 [0,0] &= \{(x, y) \in \mathbb{N} \times \mathbb{N} | 0 + y = 0 + x\} \\
 &= \{(x, y) \in \mathbb{N} \times \mathbb{N} | x = y\} \\
 &= \{(x, x) | x \in \mathbb{N}\} \\
 &= \{(0,0), (1,1), (2,2), \dots\}.
 \end{aligned}$$

(ii)  $[a, b] = \{(a, b), (a + 1, b + 1), (a + 2, b + 2), \dots\}.$

(iii) These classes  $[(a, b)]$  formed a partition on  $\mathbb{N} \times \mathbb{N}$ .

**Theorem 2.2.4.** For all  $(x, y) \in \mathbb{N} \times \mathbb{N}$ , one of the following hold:

- (i)  $[x, y] = [0,0]$ , if  $x = y$ .  
 (ii)  $[x, y] = [z, 0]$ , for some  $z \in \mathbb{N}$ , if  $x < y$ .  
 (iii)  $[x, y] = [0, z]$ , for some  $z \in \mathbb{N}$ , if  $y < x$ .

**Proof.**

Let  $(x, y) \in \mathbb{N} \times \mathbb{N}$ . Then by Trichotomy Theorem, there are three possibilities.

(1)  $x = y$ ,

$$\rightarrow 0 + y = 0 + x$$

Def. of +

$$\rightarrow (0,0)R^*(x, y)$$

Def. of  $R^*$

$$\rightarrow [0,0] = [x, y]$$

Def. of  $[a, b]$

(2)  $x < y$ ,

$$\rightarrow y = x + z \text{ for some } z \in \mathbb{N}$$

Def. of  $<$

$$\rightarrow x + z = y + 0$$

Def. of +

$$\rightarrow (x, y)R^*(0, z) \rightarrow (0, z)R^*(x, y)$$

Def. of  $R^*$

$$\rightarrow [0, z] = [x, y]$$

Def. of  $[a, b]$

(3)  $y < x$ ,

$$\rightarrow x = y + z \text{ for some } z \in \mathbb{N}$$

Def. of  $<$

$$\rightarrow x + 0 = y + z$$

Def. of +

$$\rightarrow (x, y)R^*(z, 0) \rightarrow (z, 0)R^*(x, y)$$

Def. of  $R^*$

$$\rightarrow [z, 0] = [x, y]$$

Def. of  $[a, b]$

**2.2.5. Constriction of Integer Numbers  $\mathbb{Z}$ .**

Let

$$\mathbb{Z} = \bigcup_{(a,b) \in \mathbb{N} \times \mathbb{N}} [(a, b)] = \bigcup_{a(\neq 0) \in \mathbb{N}} [(a, 0)] \bigcup_{b(\neq 0) \in \mathbb{N}} [(0, b)] \bigcup [(0,0)].$$

**2.2.6. Addition, Subtraction and Multiplication on  $\mathbb{Z}$**

**Addition:**  $\oplus: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ;

$$\boxed{[r, s] \oplus [t, u] = [r + t, s + u]}$$

**Subtraction:**  $\ominus: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ;

$$\boxed{[r, s] \ominus [t, u] = [r, s] \oplus [u, t] = [r + u, s + t]}$$

**Multiplication:**  $\odot: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ ;

$$\boxed{[r, s] \odot [t, u] = [r \cdot t + s \cdot u, r \cdot u + s \cdot t]}$$

**Theorem 2.2.7.** The relations  $\oplus$ ,  $\ominus$  and  $\odot$  are well defined; that is,  $\oplus$  and  $\ominus$  is function.

**Proof.**

To prove  $\oplus$  is function. Assume that  $[r, s] = [r_0, s_0]$  and  $[t, u] = [t_0, u_0]$ .

$$[r, s] \oplus [t, u] = [r + t, s + u]$$

$$[r_0, s_0] \oplus [t_0, u_0] = [r_0 + t_0, s_0 + u_0]$$

To prove  $[r + t, s + u] = [r_0 + t_0, s_0 + u_0]$ .

$$\rightarrow (r, s)R^*(r_0, s_0)$$

$$\rightarrow r + s_0 = s + r_0$$

$$\rightarrow (t, u)R^*(t_0, u_0)$$

$$\rightarrow t + u_0 = u + t_0$$

$$\rightarrow (r + s_0) + (t + u_0) = (s + r_0) + (u + t_0)$$

$$\rightarrow (r + t) + (s_0 + u_0) = (s + u) + (r_0 + t_0)$$

$$\rightarrow (r + t, s + u)R^*(r_0 + t_0, s_0 + u_0)$$

$$\rightarrow [r + t, s + u] = [r_0 + t_0, s_0 + u_0]$$

$$[r, s] = [r_0, s_0] \text{ and Def. of } R^*$$

$$\dots\dots(1)$$

$$[r, s] = [r_0, s_0] \text{ and Def. of } R^*$$

$$\dots\dots(2)$$

Adding (1),(2)

Asso. and comm. for +

Def. of  $R^*$

Def. of  $[a, b]$

$\ominus$  and  $\odot$ (Exercise)

**Example 2.2.8.**

$$[2, 4] \oplus [0, 1] = [2 + 0, 4 + 1] = [2, 4] = [0, 2].$$

$$[5, 2] \oplus [8, 1] = [5 + 8, 2 + 1] = [13, 3] = [10, 0].$$

**Notation 2.2.9.**

(i) Let identify the equivalence classes  $[r, s]$  according to its form as in Theorem 2.2.3.

$$[a, 0] = +a, a \in \mathbb{N}, \text{ called } \mathbf{positive\ integer.}$$

$$[0, b] = -b, b \in \mathbb{N}, \text{ called } \mathbf{negative\ integer.}$$

$$[0, 0] = 0, \text{ called the } \mathbf{zero\ element.}$$

$$[4, 6] = [0, 2] = -2$$

$$[9, 6] = [3, 0] = 3$$

$$[6, 6] = [0, 0] = 0$$

(ii) The relation  $i: \mathbb{N} \rightarrow \mathbb{Z}$ , defined by  $i(n) = [n, 0]$  is 1-1 function, and

$i(n + m) = i(n) \oplus i(m)$ ,  $i(n \cdot m) = i(n) \odot i(m)$ . So, we can identify  $n$  with  $+n$ ;

that is,  $\boxed{+n = n}$ ,  $\boxed{+ = \oplus}$  and  $\boxed{\cdot = \odot}$ .

**Theorem 2.2.10.**

(i)  $a \in \mathbb{Z}$  is positive if there exist  $[x, y] \in \mathbb{Z}$  such that  $a = [x, y]$  and  $y < x$ .

(ii)  $b \in \mathbb{Z}$  is negative if there exist  $[x, y] \in \mathbb{Z}$  such that  $b = [x, y]$  and  $x < y$ .

(iii) For each element  $[x, y] \in \mathbb{Z}$ ,  $[y, x] \in \mathbb{Z}$  is the unique element such that  $[x, y] + [y, x] = 0$ . Denote  $[y, x]$  by  $-[x, y]$ .

(iv)  $\boxed{(-m) \odot n = -(m \cdot n)}$ ,  $\forall n, m \in \mathbb{Z}$ .

(v)  $\boxed{m \odot (-n) = -(m \cdot n)}$ ,  $\forall n, m \in \mathbb{Z}$ .

(vi)  $\boxed{(-m) \odot (-n) = m \cdot n}$ ,  $\forall n, m \in \mathbb{Z}$ .

(vii) (Commutative property of  $+$ )  $\boxed{n + m = m + n}$ ,  $\forall n, m \in \mathbb{Z}$ .

(viii) (Associative property of  $+$ )  $\boxed{(n + m) + c = n + (m + c)}$ ,  $\forall n, m, c \in \mathbb{Z}$ .

(ix) (Commutative property of  $\cdot$ )  $\boxed{n \cdot m = m \cdot n}$ ,  $\forall n, m \in \mathbb{Z}$ .

(x) (Associative property of  $\cdot$ )  $\boxed{(n \cdot m) \cdot c = n \cdot (m \cdot c)}$ ,  $\forall n, m, c \in \mathbb{Z}$ .

(xi) (Cancellation Law for  $+$ ).  $m + c = n + c$ , for some  $c \in \mathbb{Z} \Leftrightarrow m = n$ .

(xii) (Cancellation Law for  $\cdot$ ).  $m \cdot c = n \cdot c$ , for some  $c (\neq 0) \in \mathbb{Z} \Leftrightarrow m = n$ .

(xiii) 0 is the unique element such that  $0 + m = m + 0 = m$ ,  $\forall m \in \mathbb{Z}$ .

(xiv) 1 is the unique element such that  $1 \cdot m = m \cdot 1 = m$ ,  $\forall m \in \mathbb{Z}$ .

(xv) Let  $a, b, c \in \mathbb{Z}$ . Then  $\boxed{c = a - b} \Leftrightarrow \boxed{a = c + b}$ .

(xvi)  $\boxed{-(-b) = b}$ ,  $\forall b \in \mathbb{Z}$ .

**Proof. Exercise.**

**Remark 2.2.11.**

For each element  $a = [x, y] \in \mathbb{Z}$ , the unique element in Theorem 2.2.8(xiv) is  $-a = [y, x]$ .

**Definition 2.2.12. ( $\mathbb{Z}$  as an Ordered)**

Let  $[r, s], [t, u] \in \mathbb{Z}$ . We say that  $[r, s]$  less than  $[t, u]$  and denoted by

$$[r, s] < [t, u] \Leftrightarrow r + u < s + t.$$

This is well defined and agrees with the ordering on  $\mathbb{N}$ .

**Theorem 2.2.13.(Trichotomy For  $\mathbb{Z}$ ) (Well Ordering)**

For each  $[r, s], [t, u] \in \mathbb{Z}$  one and only one of the following is true:

(1)  $[r, s] < [t, u]$  or (2)  $[t, u] < [r, s]$  or (3)  $[r, s] = [t, u]$ .

**Proof.**

Since  $r + u, t + s \in \mathbb{N}$ , so by Trichotomy Theorem for  $\mathbb{N}$  one and only one of the following is true:

- (1)  $r + u < s + t \rightarrow [r, s] < [t, u]$
- (2)  $s + t < r + u \rightarrow [t, u] < [r, s]$
- (3)  $r + u = s + t \rightarrow (r, s)R^*(t, u) \rightarrow [r, s] = [t, u]$ .

**Theorem 2.2.14.**

For each  $[r, s] \in \mathbb{Z}$ ,  $[r, s] < [0, 0] \Leftrightarrow r < s$ .

**Proof.**

$$[r, s] < [0, 0] \Leftrightarrow r + 0 < s + 0 \Leftrightarrow r < s.$$

**Remark 2.2.15.**

According to Theorem 2.2.11 and Notation 2.2.7(i), for all  $[r, s] \in \mathbb{Z}$   
 $[r, s] < [0, 0] \Leftrightarrow r < s \Leftrightarrow [r, r + l] \in \mathbb{Z}$ , where  $s = r + l$  for some  $l$   
 $\Leftrightarrow [0, l] < [0, 0]$   
 $\Leftrightarrow -l < 0$ .