Elements of Set Theory

Chapter 4: Natural Numbers

February 11 & 13, 2014

Lecturer: Fan Yang

Arithmetic

Addition $+ : \omega \times \omega \to \omega$ and multiplication $\cdot : \omega \times \omega \to \omega$ are binary operations on ω. We write $a + b$ and $a \cdot b$ instead of $+(a, b)$ and $\cdot(a, b)$.

For each $m \in \omega$, by Recursion Theorem, there exists a unique unary operation $\mathrm{Add}_m : \omega \to \omega$, "adding m", for which

$$\mathrm{Add}_m(0) = m,$$
$$\mathrm{Add}_m(n^+) = \mathrm{Add}_m(n)^+ \quad \text{for } n \in \omega.$$

Definition 4.11

Addition is the binary operation $+ : \omega \times \omega \to \omega$ defined as

$$m + n = \mathrm{Add}_m(n)$$

for all $m, n \in \omega$.

Theorem 4I

For any $m, n \in \omega$,

$$(A1)\ m + 0 = m, \qquad (A2)\ m + n^+ = (m + n)^+.$$

Example 4.1: Prove: $127 + 2 = 129$.

Proof.

- $127 + 0 = 127$.
- $127 + 1 = 127 + 0^+ = (127 + 0)^+ = 127^+ = 128$.
- $127 + 2 = 127 + 1^+ = (127 + 1)^+ = 128^+ = 129$.

□

Theorem 4K

Let $m, n, k \in \omega$. (1) *Associative law: $m + (n + k) = (m + n) + k$*
(2) *Commutative law: $m + n = n + m$.*

Proof. We only prove (2). It suffices to show that the set

$$A = \{n \in \omega \mid m + n = n + m \text{ for all } m \in \omega\}$$

is inductive, for then $A = \omega$.

Base case: To show $0 \in A$, since $m + 0 = m$ by (A1), it suffices to show that $0 + m = m$ for all $m \in \omega$. To this end, we prove $B = \{m \in \omega \mid 0 + m = m\}$ is inductive.

By (A1), $0 + 0 = 0$, thereby $0 \in B$. Assuming $k \in B$, we have that $0 + k = k$, thus $0 + k^+ = (0 + k)^+ = k^+$, thereby $k^+ \in B$.

Inductive step: Assume $n \in A$. To show $n^+ \in A$, it suffices to show that

$$C = \{m \in \omega \mid m + n^+ = n^+ + m\}$$

is inductive. By Base case, $0 \in A$, thus $n^+ + 0 = 0 + n^+$, thereby $0 \in C$. Assuming $m \in C$, we show that $m^+ \in C$. Indeed,

$$\begin{aligned} m^+ + n^+ &= (m^+ + n)^+ && \text{(by (A2))} \\ &= (n + m^+)^+ && \text{(since } n \in A) \\ &= (n + m)^{++} && \text{(by (A2))} \\ &= (m + n)^{++} && \text{(since } n \in A) \\ &= (m + n^+)^+ && \text{(by (A2))} \\ &= (n^+ + m)^+ && \text{(since } m \in C) \\ &= n^+ + m^+ && \text{(by (A2)).} \end{aligned}$$

□

Similarly, to define multiplication, let us first apply Recursion Theorem to obtain functions $\mathrm{M}_m : \omega \to \omega$ such that $\mathrm{M}_m(n)$ is the result of multiplying m by n. Formally, for each $m \in \omega$, by Recursion Theorem, there exists a unique unary operation $\mathrm{M}_m : \omega \to \omega$ for which

$$\begin{aligned} \mathrm{M}_m(0) &= 0, \\ \mathrm{M}_m(n^+) &= \mathrm{M}_m(n) + m \quad \text{for } n \in \omega. \end{aligned}$$

Definition 4.12

Multiplication is the binary operation $\cdot : \omega \times \omega \to \omega$ defined as

$$m \cdot n = \mathrm{M}_m(n), \text{ for all } m, n \in \omega$$

Theorem 4J

For any $m, n \in \omega$,

$$(M1)\ m \cdot 0 = 0, \qquad (M2)\ m \cdot n^+ = m \cdot n + m.$$

Theorem 4K

Let $m, n, k \in \omega$. (3) *Distributive law: $m \cdot (n + k) = m \cdot n + m \cdot k$.*
(4) *Associative law: $m \cdot (n \cdot k) = (m \cdot n) \cdot k$.*
(5) *Commutative law: $m \cdot n = n \cdot m$.*

Proof. We only prove (3). It suffices to show that

$$A = \{k \in \omega \mid m \cdot (n + k) = m \cdot n + m \cdot k \text{ for all } m, n \in \omega\}$$

is inductive.

Base case: $0 \in A$ since $m \cdot (n + 0) = m \cdot n = m \cdot n + 0 = m \cdot n + m \cdot 0$.

Inductive step: Assume $k \in A$. We show that $k^+ \in A$.

$$\begin{aligned} m \cdot (n + k^+) &= m \cdot (n + k)^+ && \text{(by (A2))} \\ &= m \cdot (n + k) + m && \text{(by (M2))} \\ &= (m \cdot n + m \cdot k) + m && \text{(since } k \in A) \\ &= m \cdot n + (m \cdot k + m) && \text{(by associative law)} \\ &= m \cdot n + m \cdot k^+ && \text{(by (M2)).} \end{aligned}$$

□

In the same manner, we can define exponentiation operation on ω such that

(E1) $m^0 = 1$,

(E2) $m^{n^+} = m^n \cdot m$.

For any $m, n, k \in \omega$, we have that

$$m^{n+k} = m^n \cdot m^k.$$

(Exercise)

Theorem 4N

For any $m, n, k \in \omega$

(i) $m \in n \iff m + k \in n + k$.

(ii) *If $k \neq 0$, then $m \in n \iff m \cdot k \in n \cdot k$.*

Proof. We only prove (ii). For "$\Longrightarrow$", consider fixed $m \in n \in \omega$. We need to show that $m \cdot k \in n \cdot k$ holds for all natural numbers $k \neq 0$. Recall that for any natural number $k \neq 0$, $k = p^+$ for some $p \in \omega$. In view of this, it suffices to show that the set

$$A = \{p \in \omega \mid m \cdot p^+ \in n \cdot p^+\}$$

is inductive.

Clearly, $0 \in A$, since $m \cdot 0^+ = m \cdot 0 + m = m \in n = n \cdot 0 + n = n \cdot 0^+$.

Suppose $p \in A$. We need to show that $m \cdot p^{++} \in n \cdot p^{++}$. Indeed,

$$m \cdot p^{++} = m \cdot p^+ + m.$$

Since $p \in A$, we have $m \cdot p^+ \in n \cdot p^+$. It follows that

$$\begin{aligned} m \cdot p^{++} = m \cdot p^+ + m &\in n \cdot p^+ + m \quad \text{(by (i))} \\ &\in n \cdot p^+ + n \quad \text{(by (i), since } m \in n\text{)} \\ &= n \cdot p^{++}. \end{aligned}$$

For "$\Longleftarrow$", suppose $m \cdot k \in n \cdot k$. Recall that $\in$ satisfies trichotomy, thus exactly one of the following three alternatives holds:

$$m \in n \quad \text{or} \quad m = n \quad \text{or} \quad n \in m.$$

If $m = n$, then the assumption becomes $m \cdot k \in m \cdot k$, which contradicts $m \cdot k = m \cdot k$ by trichotomy.

If $n \in m$, then by "$\Longrightarrow$", we have that $n \cdot k \in m \cdot k$, contradicting the assumption $m \cdot k \in n \cdot k$ by trichotomy.

Hence, we conclude by trichotomy that $m \in n$ must be the case. □

Corollary 4P (Cancellation Law)

For any $m, n, k \in \omega$

(i) $m + k = n + k \Longrightarrow m = n$.

(ii) $m \cdot k = n \cdot k$ *and* $k \neq 0 \Longrightarrow m = n$.

Proof. Follows from Theorem 4N. □

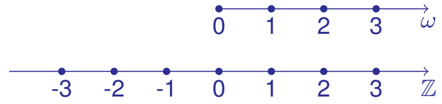
Elements of Set Theory

Chapter 5: Construction of the Real Numbers

February 11 & 13, 2014

Integers

We will extend the set ω of natural numbers to a set $\mathbb{Z}$ of integers, in such a way that $\mathbb{Z}$ will contain an isomorphic copy of ω.

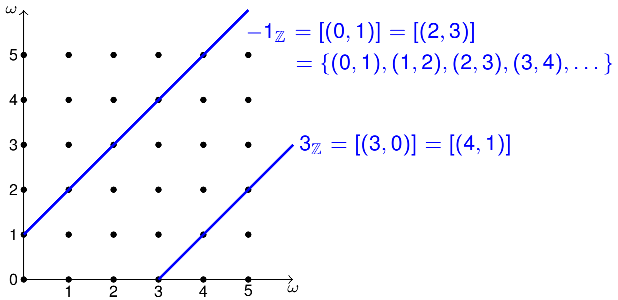


First idea: $-1 = 0 - 1$, $-3 = 0 - 3$, etc.

Define $-1 := (0,1)$, $-3 := (0,3)$, etc.

But, e.g., $0 - 1 = -1 = 2 - 3$ and $(0,1) \neq (2,3)$.

A revised idea: Define an equivalence relation $\sim$ such that $(0,1) \sim (2,3)$. Then $[(0,1)] = [(2,3)]$, and take the integer $-1_{\mathbb{Z}}$[1] to be this equivalence class. Define $\mathbb{Z} := (\omega \times \omega)/\sim$.



Informally, we say that $(m,n) \sim (p,q)$ iff $m - n = p - q$. However, we did not define subtraction $-$ on ω, so the preceding equation does not have a precise meaning yet. But the equation is equivalent to $m + q = p + n$, which does have a meaning.

[1] In order to distinguish non-negative integers from natural numbers, from now on, we denote the integers $-2, -1, 0, 1, 2$, etc. by $-2_{\mathbb{Z}}, -1_{\mathbb{Z}}, 0_{\mathbb{Z}}, 1_{\mathbb{Z}}, 2_{\mathbb{Z}}$, etc. with subscripts "$\mathbb{Z}$".

Definition 5.1

Define a relation $\sim$ on $\omega \times \omega$ as

$$(m,n) \sim (p,q) \quad \text{iff} \quad m + q = p + n.$$

Theorem 5ZA

The relation $\sim$ is an equivalence relation on $\omega \times \omega$.

Proof. Reflexivity: Since $m + n = m + n$, we have $(m,n) \sim (m,n)$.

Symmetricity:

$$(m,n) \sim (p,q) \implies m+q = p+n \implies p+n = m+q \implies (p,q) \sim (m,n).$$

Transitivity:

$$\begin{aligned} & (m,n) \sim (p,q) \text{ and } (p,q) \sim (r,s) \\ \implies & m + q = p + n \text{ and } p + s = r + q \\ \implies & m + q + p + s = p + n + r + q \\ \implies & m + s = n + r \\ \implies & (m,n) \sim (r,s). \end{aligned}$$

□

Definition 5.2

Define the set of integers as $\mathbb{Z} := (\omega \times \omega)/_{\sim}$.

For example, $-1_{\mathbb{Z}} := [(0,1)] = [(1,2)] = \{(1,2),(2,3),(3,4),\dots\}$
$3_{\mathbb{Z}} := [(3,0)] = \{(3,0),(4,1),(5,2),\dots\}$

Informally, for any two integers $[(m,n)]$, $[(p,q)]$, addition acts as

$$(m-n)+(p-q) = (m+p)-(n+q).$$

Definition 5.3 (Addition)

Define the addition operation $+ : \mathbb{Z}\times\mathbb{Z}\to\mathbb{Z}$ *as: for any two integers* $[(m,n)]$, $[(p,q)]$,

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

We have to check that such defined $+$ is well-defined.

Lemma 5ZB

If $(m,n)\sim(m',n')$ *and* $(p,q)\sim(p',q')$, *then*

$$(m+p, n+q)\sim(m'+p', n'+q').$$

Proof. Since $(m,n)\sim(m',n')$ and $(p,q)\sim(p',q')$, we have that

$$m+n' = m'+n \quad \text{and} \quad p+q' = p'+q.$$

Adding both sides of the above two equalities yields

$$m+n'+p+q' = m'+n+p'+q,$$

i.e.,

$$(m+p)+(n'+q') = (m'+p')+(n+q),$$

which means $(m+p,n+q)\sim(m'+p',n'+q')$. □

Example 5.2: Calculate $4_{\mathbb{Z}} + (-5_{\mathbb{Z}})$.

Solution. Since $4_{\mathbb{Z}} = [(4,0)]$ and $-5_{\mathbb{Z}} = [(0,5)]$, we have that

$$4_{\mathbb{Z}} + (-5_{\mathbb{Z}}) = [(4,0)] + [(0,5)] = [(4+0, 0+5)] = [(4,5)] = -1_{\mathbb{Z}}.$$

□

Theorem 5ZC

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

(commutative law) $a+b=b+a$

(associative law) $a+(b+c)=(a+b)+c$

Proof. We only prove commutative law. Let $a=[(m,n)]$ and $b=[(p,q)]$ for some $m,n,p,q\in\omega$. We have that

$$\begin{aligned} a+b &= [(m,n)]+[(p,q)] \\ &= [(m+p,n+q)] \\ &= [(p+m,q+n)] \quad \text{(since + on } \omega \text{ is commutative)} \\ &= [(p,q)]+[(m,n)] \\ &= b+a. \end{aligned}$$

□

Theorem 5ZD

(a) $0_{\mathbb{Z}} = [(0,0)]$ *is an additive identity:* $a + 0_{\mathbb{Z}} = a$ *for all* $a \in \mathbb{Z}$.

(b) For any $a \in \mathbb{Z}$, *there is a unique* $b \in \mathbb{Z}$ *such that*

$$a + b = 0_{\mathbb{Z}}. \qquad (*)$$

The unique integer b is called the additive inverse of a, denoted by $-a$.

Proof. (a) Let $a = [(m,n)]$. We have that

$$a + 0_{\mathbb{Z}} = [(m,n)] + [(0,0)] = [(m+0, n+0)] = [(m,n)] = a.$$

(b) Let $a = [(m,n)]$. Take $b = [(n,m)]$. We have that

$$a + b = [(m,n)] + [(n,m)] = [(m+n, n+m)] = [(0,0)] = 0_{\mathbb{Z}}.$$

For uniqueness, assume $b' \in \mathbb{Z}$ also satisfies equality $(*)$. Then

$$b = b + 0_{\mathbb{Z}} = b + (a + b') = (b + a) + b' = 0_{\mathbb{Z}} + b' = b'.$$

□

From the proof of the above theorem, we see that

- $-[(m,n)] = [(n,m)]$, in particular, $-0_{\mathbb{Z}} = [(0,0)] = 0_{\mathbb{Z}}$.
- $-(-[(m,n)]) = -[(n,m)] = [(m,n)]$

Definition 5.4 (Subtraction)

Define the subtraction operation $- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *as: for any two integers a, b,*

$$a - b = a + (-b).$$

Informally, for any two integers $[(m,n)]$, $[(p,q)]$, multiplication acts as

$$(m-n)\cdot(p-q) = mp - mq - np + nq = (mp+nq) - (mq+np).$$

Definition 5.5 (Multiplication)

Define the multiplication operation $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ *as: for any two integers* $[(m,n)]$, $[(p,q)]$,

$$[(m,n)] \cdot [(p,q)] = [(mp+nq, mq+np)].$$

Example 5.3: For any $a, b \in \mathbb{Z}$,

$$(-a)\cdot b = -(a \cdot b).$$

Proof. Let $a = [(m,n)]$ and $b = [(p,q)]$. It follows that

$$\begin{aligned}(-a)\cdot b &= [(n,m)] \cdot [(p,q)] \\ &= [(np+mq, nq+mp)] \\ &= -[(nq+mp, np+mq)] \\ &= -([(m,n)] \cdot [(p,q)]) \\ &= -(a \cdot b).\end{aligned}$$

□

Lemma 5ZE

If $(m,n) \sim (m',n')$ *and* $(p,q) \sim (p',q')$, *then*

$$(mp+nq, mq+np) \sim (m'p'+n'q', m'q'+n'p').$$

Proof. Since $(m,n) \sim (m',n')$ and $(p,q) \sim (p',q')$, we have that

$$m + n' = m' + n \quad \text{and} \quad p + q' = p' + q.$$

It follows that

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

Adding the four equations yields that

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

namely, $(mp+nq, mq+np) \sim (m'p'+n'q', m'q'+n'p')$.

□

Lemma 5ZF

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

(commutative law) $a \cdot b = b \cdot a$,

(associative law) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,

(distributive law) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Proof. We only prove commutative law.

Let $a = [(m, n)]$ and $b = [(p, q)]$, then

$$a \cdot b = [(m, n)] \cdot [(p, q)] = [(mp + nq, mq + np)],$$

$$b \cdot a = [(p, q)] \cdot [(m, n)] = [(pm + qn, qm + pn)].$$

Hence $a \cdot b = b \cdot a$. □

Theorem 5ZG

(a) $1_{\mathbb{Z}} = [(1, 0)]$ *is a multiplicative identity:* $a \cdot 1_{\mathbb{Z}} = a$ *for all* $a \in \mathbb{Z}$.

(b) $1_{\mathbb{Z}} \neq 0_{\mathbb{Z}}$

(c) *If* $a \cdot b = 0_{\mathbb{Z}}$, *then either* $a = 0_{\mathbb{Z}}$ *or* $b = 0_{\mathbb{Z}}$.

Proof. We only prove (a) and (b).

(a) Let $a = [(m, n)]$. We have that

$$a \cdot 1_{\mathbb{Z}} = [(m, n)] \cdot [(1, 0)] = [(m \cdot 1 + n \cdot 0, m \cdot 0 + n \cdot 1)] = [(m, n)] = a.$$

(b) To check $1_{\mathbb{Z}} = [(1, 0)] \neq [(0, 0)] = 0_{\mathbb{Z}}$, it suffices to check that $(1, 0) \not\sim (0, 0)$, which reduces to checking $1 = 1 + 0 \neq 0 + 0 = 0$. But this is true, as $1 = \{\emptyset\} \neq \emptyset = 0$. □

Informally, we want to define an ordering $<$ on $\mathbb{Z}$ such that for any $[(m, n)], [(p, q)] \in \mathbb{Z}$,

$$m - n < p - q \quad \text{iff} \quad m + q \in p + n.$$

Definition 5.6 (Ordering)

Define an ordering $<$ on $\mathbb{Z}$ as: for any two integers $[(m, n)], [(p, q)]$,

$$[(m, n)] < [(p, q)] \quad \textit{iff} \quad m + q \in p + n.$$

Example 5.4: Show that $-2_{\mathbb{Z}} < 0_{\mathbb{Z}}$.

Proof. Recall that $-2_{\mathbb{Z}} = [(0, 2)]$ and $0_{\mathbb{Z}} = [(0, 0)]$. Since

$$0 + 0 = 0 \in 2 = 0 + 2,$$

we conclude that $-2_{\mathbb{Z}} < 0_{\mathbb{Z}}$. □

We need to show that $<$ is well-defined.

Lemma 5ZH

If $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$, then

$$m + q \in p + n \quad \textit{iff} \quad m' + q' \in p' + n'.$$

Proof. Since $(m, n) \sim (m', n')$ and $(p, q) \sim (p', q')$, we have that

$$m + n' = m' + n \quad \text{and} \quad p + q' = p' + q.$$

It follows that

$$\begin{aligned} m + q \in p + n &\iff m + q + n' + q' \in p + n + n' + q' \\ &\iff m' + n + q + q' \in p' + q + n + n' \\ &\iff m' + q' \in p' + n'. \end{aligned}$$

□

Lemma 5ZI

The relation $<$ is a linear ordering on $\mathbb{Z}$.

Proof. We must show that $<$ is transitive and satisfies trichotomy on $\mathbb{Z}$. Let $a = [(m,n)]$, $b = [(p,q)]$ and $c = [(r,s)]$ be integers.

For trichotomy, we need to show that exactly one of the following three alternatives holds:

$$a < b, \quad a = b, \quad b < a.$$

That is, exactly one of the following holds:

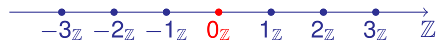
$$m + q \in p + n, \quad m + q = p + n, \quad p + n \in m + q.$$

But this follows from the trichotomy of $\in$ in ω.

For transitivity, we have that

$$\begin{aligned} a < b \text{ and } b < c &\implies m + q \in p + n \text{ and } p + s \in r + q \\ &\implies m + q + s \in p + n + s \text{ and } p + s + n \in r + q + n \\ &\implies m + q + s \in r + q + n \quad \text{(by transitivity of } \in \text{ on } \omega) \\ &\implies m + s \in r + n \\ &\implies a < c. \end{aligned}$$

□



Note: For any integer $[(m,n)]$, we have $[(m, n+1)] < [(m,n)]$. Thus the set $\mathbb{Z}$ does not have a least element with respect to the ordering $<$, implying that $<$ on $\mathbb{Z}$ is not a well ordering.

Definition 5.7

An integer a is called positive iff $0_{\mathbb{Z}} < a$; negative iff $a < 0_{\mathbb{Z}}$.

The trichotomy of $<$ implies that exactly one of the following holds:

$$a \text{ is positive}, \quad a = 0_{\mathbb{Z}}, \quad a \text{ is negative}.$$

Theorem 5ZJ

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

(i) $a < b \iff a + c < b + c$.

(ii) *If $0_{\mathbb{Z}} < c$, then $a < b \iff a \cdot c < b \cdot c$.*

Proof. We only prove (i). Let $a = [(m,n)]$, $b = [(p,q)]$ and $c = [(r,s)]$ be integers. Then

$$a + c = [(m + r, n + s)] \quad \text{and} \quad b + c = [(p + r, q + s)].$$

It follows that

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

□

Example 5.5: For any $a, b \in \mathbb{Z}$,

$$a < b \iff -b < -a.$$

In particular, $c < 0_{\mathbb{Z}} \iff 0_{\mathbb{Z}} < -c$.

Proof. By Theorem 5ZJ (i),

$$a < b \iff a + ((-a) + (-b)) < b + ((-b) + (-a)) \iff -b < -a.$$

□

Corollary 5ZK

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

(i) $a + c = b + c \Longrightarrow a = b$

(ii) $a \cdot c = b \cdot c$ *and* $c \neq 0_{\mathbb{Z}} \Longrightarrow a = b$.

Proof. For (i), we have the derivation:

$$\begin{aligned} a \neq b &\Longrightarrow \text{w.l.o.g. we may assume } a < b \quad \text{(by trichotomy)} \\ &\Longrightarrow a + c < b + c \quad \text{(by Theorem 5ZJ(i))} \\ &\Longrightarrow a + c \neq b + c \quad \text{(by trichotomy).} \end{aligned}$$

For (ii), it suffices to derive

$$a \neq b \text{ and } c \neq 0_{\mathbb{Z}} \Longrightarrow a \cdot c \neq b \cdot c.$$

W.l.o.g. we assume $a < b$. By Theorem 5ZJ(ii)), $c \neq 0_{\mathbb{Z}} \Longrightarrow$

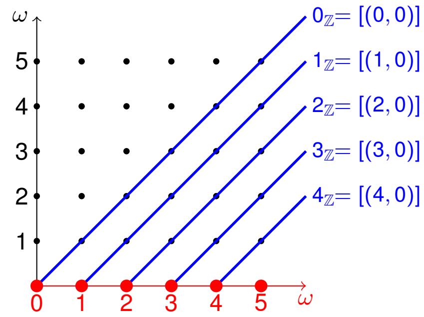
$$\begin{cases} 0_{\mathbb{Z}} < c & \Longrightarrow a \cdot c < b \cdot c \Longrightarrow a \cdot c \neq b \cdot c; \\ \text{or} & \\ c < 0_{\mathbb{Z}} & \Longrightarrow 0_{\mathbb{Z}} < -c \Longrightarrow a \cdot (-c) < b \cdot (-c) \Longrightarrow -(a \cdot c) < -(b \cdot c) \end{cases}$$

$$\Longrightarrow -(a \cdot c) \neq -(b \cdot c) \Longrightarrow a \cdot c \neq b \cdot c.$$

□

By our construction, the set ω is not actually a subset of the set $\mathbb{Z}$. However, $\mathbb{Z}$ has a subset that is "just like" ω.

We call the set ω with addition $+$, multiplication $\cdot$, and the ordering $\in$ a ***structure***, written as $\langle \omega, +, \cdot, \in \rangle$. Similarly, $\langle \mathbb{Z}, +, \cdot, < \rangle$ is also a structure.



The function f defined in the next theorem is an "isomorphic embedding" of the structure $\langle \omega, +, \cdot, \in \rangle$ into the structure $\langle \mathbb{Z}, +, \cdot, < \rangle$.

Theorem 5ZL

Define a function $f : \omega \to \mathbb{Z}$ by taking

$$f(n) = [(n, 0)].$$

The function f is one-to-one and preserves operations and orders, that is, for any $m, n \in \omega$,

(a) $f(m + n) = f(m) + f(n)$;

(b) $f(m \cdot n) = f(m) \cdot f(n)$;

(c) $m \in n$ *iff* $f(m) < f(n)$.

Proof. We first show that f is one-to-one. We have that

$$\begin{aligned} f(m) = f(n) &\Longrightarrow [(m, 0)] = [(n, 0)] \Longrightarrow (m, 0) \sim (n, 0) \\ &\Longrightarrow m + 0 = 0 + n \Longrightarrow m = n. \end{aligned}$$

For (a), $f(m + n) = [(m + n, 0)] = [(m, 0)] + [(n, 0)] = f(m) + f(n)$.

(b) and (c) are left as an exercise. □