Ch. 2 Section 1.

Theorem 2.1.10.

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

Proof:

Suppose that $L = \{n \in \mathbb{N} | n^+ = 1 + n\}$. Then we will prove that L is successor subset of $\mathbb{N}$.
(i) To prove $0 \in L$.

$0^+ = 1 = 1 + 0$ (Def. of $+$)

$\longrightarrow 0 \in L$.

(ii) Let $k \in L$. To prove that $k^+ \in L$.

$1 + k^+ = (1 + k)^+$ (Def. of $+$)

$= (k^+)^+$ (Since $k \in L$)

$\longrightarrow k^+ \in L$.

Thus, L is a successor subset of $\mathbb{N}$. Therefore, by $\mathbf{P}_5$ we get that $L = \mathbb{N}$.

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

Proof:

Suppose that $L = \{n \in \mathbb{N} | n = 1 \cdot n\}$, Then we will prove that L is successor subset of $\mathbb{N}$.
(i) To prove $0 \in L$.

$0 = 1 \cdot 0$ (Def. of $\cdot$)

$\longrightarrow 0 \in L$.

(ii) Let $k \in L$. To prove that $k^+ \in L$.

$1 \cdot k^+ = 1 + 1 \cdot k$ (Def. of $\cdot$)

$= 1 + k$ (Since $k \in L$)

$= k^+$ (Properties of successor)

$\longrightarrow k^+ \in L.$

Thus, L is a successor subset of $\mathbb{N}$. Therefore, by $\mathbf{P_5}$ we get that $L = \mathbb{N}$.

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

Proof:

Suppose that $L_m = \{n \in \mathbb{N} | m + n = n + m\}, m \in \mathbb{N}$. Then we will prove that L_m is successor subset of $\mathbb{N}$.
(i) To prove $0 \in L_m$.

$m + 0 = 0 = 0 + m$

$\longrightarrow 0 \in L_m.$

(ii) Let $k \in L_m$. To prove that $k^+ \in L_m$.

$m + k^+ = (m + k)^+$ (Def. of $+$)

$= (k + m)^+$ (Since $k \in L_m$)

$= 1 + (k + m)$ (Properties of successor)

$= (1 + k) + m$ (Asso. law of $+$)

$= k^+ + m$ (Properties of successor)

Thus, $k^+ \in L_m$; that is, L_m is a successor subset of $\mathbb{N}$. Therefore, by $\mathbf{P_5}$ we get that $L_m = \mathbb{N}$.

(iv) (Distributive property of $\cdot$ on $+$ from right)

$$(n + m) \cdot c = n \cdot c + m \cdot c, \forall\, n, m, c \in \mathbb{N}.$$

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

(i) To prove $0 \in L_{mn}$.
$(n+m) \cdot 0 = 0 = 0 + 0 = n \cdot 0 + m \cdot 0$
$\longrightarrow 0 \in L_{mn}$ (Def. of L_{mn})

(ii) Let $c \in L_{mn}$. To prove that $c^+ \in L_{mn}$.

$(n+m) \cdot c^+ = (n+m) + (n+m) \cdot c$ (Def. of $+$)

$= (n+m) + (n \cdot c + m \cdot c)$ (Since $c \in L_{mn}$)

$= (n + n \cdot c) + (m + m \cdot c)$ (Asso. law and comm. law of $+$)

$= n \cdot c^+ + m \cdot c^+$ (Def. of $\cdot$)

$\longrightarrow c^+ \in L_{mn}$ (Def. of L_{mn})

(ix) (Cancellation Law for $+$). $m + c = n + c$, for some $c \in \mathbb{N} \Leftrightarrow m = n$.
Proof:
(i) If $m + c = n + c$, for some $c \in \mathbb{N} \Longrightarrow m = n$.

Suppose that $L_{mn} = \{n \in \mathbb{N} | m + c = n + c \Longrightarrow m = n\}$, $m, n \in \mathbb{N}$. Then we will prove that L_{mn} is successor subset of $\mathbb{N}$.
(a) To prove $0 \in L_{mn}$.

If $m + 0 = n + 0 \longrightarrow n = m$
$\longrightarrow 0 \in L_{mn}$ (Def. of L_m)
(b) Let $c \in L_{mn}$. To prove that $c^+ \in L_{mn}$.

Let $m + c^+ = n + c^+$

$(m+c)^+ = (n+c)^+$ (Def. of $+$)

$\longrightarrow m + c = n + c$ (By $\mathbf{P}_4$)

$\longrightarrow m = n$ (Since $k \in L_{mn}$)

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

(ii) If $m = n$ then $m + c = n + c$, for some $c \in \mathbb{N}$.

Theorem 2.1.14:

(vi) (Cancellation Law for ·).

$$m \cdot c = n \cdot c, \text{ for some } c(\neq 0) \in \mathbb{N} \Longrightarrow m = n.$$

Proof:

$\boxed{\text{Suppose } m \cdot c = n \cdot c, \quad \text{for some } c(\neq 0) \in \mathbb{N}.}$

If $m \neq n$, then by Trichotomy Theorem either $m < n$ or $n < m$.

If $m < n$, then $\exists k \neq 0 \in \mathbb{N}$ such that $n = m + k$. (Def. of $<$)

$n \cdot c = (m + k) \cdot c$

$n \cdot c = m \cdot c + (k \cdot c)$ (Dist. Law of · on + from right)

But $k \cdot c \neq 0$ (Since $k \neq 0$ and $c \neq 0$)

$m \cdot c < n \cdot c$ (Def. of $<$)

Therefore, $m \cdot c = n \cdot c$ and $m \cdot c < n \cdot c$.

This is contradicted with Trichotomy Theorem. Therefore, $m = n$.

(vii) If $m \cdot n = 0$, then either $m = 0$ or $n = 0$, $\forall\, m, n \in \mathbb{N}$. ($\mathbb{N}$ has no zero divisor)

Proof:

We will prove this statement by contra positive law. So the equivalent statement is

$$\textbf{If } \boldsymbol{n \neq 0} \textbf{ and } \boldsymbol{m \neq 0}\textbf{, then } \boldsymbol{m \cdot n \neq 0}.$$

Suppose that $m \cdot n = 0$. If $n \neq 0$, then we will prove that $m = 0$.

$\exists k \in \mathbb{N}$ such that $n = k^+$ (Since $n \neq 0$)

$0 = m \cdot n = m \cdot k^+ = m + m \cdot k$ (Def. of ·)

$= m \cdot k + m$ (Comm. law of +)

If $m \neq 0$, then $m \cdot k < 0$ (Def. of $<$)

This is contradiction (C!) since $m \cdot k \in \mathbb{N}$ and no natural number less than 0.

Therefore, $m \cdot n \neq 0$.

Another proof.

We will prove the equivalent statement that: if $n \neq 0$ and $m \neq 0$, then $m \cdot n \neq 0$.
Assume that $m \cdot n = 0$
$\longrightarrow m \cdot n = m \cdot 0$ (Def. of $\cdot$)
$\longrightarrow n = 0$ (Cancellation law of $\cdot$)
$\longrightarrow$ Contradiction since $m \neq 0$.
$\longrightarrow \therefore m \cdot n \neq 0$.

Theorem: $m + k < n + k \Longrightarrow m < n$, for all $m, n, k \in \mathbb{N}$.

Proof:
$m + k < n + k \rightarrow \exists l \neq 0 \in \mathbb{N}$ such that $n + k = (m + k) + l$. (Def. of $<$)
$n + k = m + (k + l)$ (Asso. law of $+$)
$n + k = m + (l + k)$ (Comm. law of $+$)
$n + k = (m + l) + k$ (Asso. law of $+$)
$n = m + l$ (Cancellation law of $+$)
$m < n$ (Since $l \neq 0$ and Def. of $<$)