THEOREM 0.3.4 (Distributive Property). *If $l, m$ and $n$ are any natural numbers, then*

$$l \cdot (m+n) = l \cdot m + l \cdot n$$
$$(l+m) \cdot n = l \cdot n + m \cdot n$$

PROOF. We will prove that multiplication is *left* distributive which is the first of the two equations. The proof that it is right distributive will be left as an exercise. We use induction on $n$. The base case can be shown as

$$\begin{aligned} l \cdot (m+0) &= l \cdot m, && \text{Additive identity} \\ &= l \cdot m + 0, && \text{Additive identity} \\ &= l \cdot m + l \cdot 0. && \text{Definition 0.2.2} \end{aligned}$$

Now assume the theorem is true for $n$. Then

$$\begin{aligned} l \cdot (m + (n{+}{+})) &= l \cdot ((m+n){+}{+}), && \text{Definition 0.2.2} \\ &= l \cdot (m+n) + l, && \text{Definition 0.2.2} \\ &= (l \cdot m + l \cdot n) + l, && \text{Induction hypothesis} \\ &= l \cdot m + (l \cdot n + l), && \text{Associativity of addition} \\ &= l \cdot m + l \cdot (n{+}{+}). && \text{Definition 0.2.2} \end{aligned}$$

This concludes the proof of the induction step and the theorem. □

Now let us establish the algebraic properties of multiplication in $\mathbb{N}$.

THEOREM 0.3.5 (Algebraic properties of $(\mathbb{N}, \cdot)$). *following properties hold.*

**Multiplicative identity:** *For any $n \in \mathbb{N}$, $1 \cdot n = n = n \cdot 1$.*
**Associativity of multiplication:** *For any three natural numbers $l, m, n$,*

$$(l \cdot m) \cdot n = l \cdot (m \cdot n) \tag{0.7}$$

**Commutativity of multiplication:** *For any two natural numbers $m, n$,*

$$m \cdot n = n \cdot m \tag{0.8}$$

**Cancellation rule for multiplication:** *For any natural number $n$, if*

$$n \cdot m_1 = n \cdot m_2 \neq 0$$

*then $m_1 = m_2$.*

PROOF. We examine these in order.

**Multiplicative identity:** Let us prove this by induction on $n$. The base case states $1 \cdot 0 = 0 = 0 \cdot 1$. The left equation follows from Definition 0.2.2. The right follows from this definition as well and the definition that $1 = 0{+}{+}$ via the equation $0 \cdot 1 = 0 \cdot (0{+}{+}) = 0 \cdot 0 + 0 = 0 + 0 = 0$. In the last equation we used the additive identity. Now assume $1 \cdot n = n = n \cdot 1$. Then $1 \cdot (n{+}{+}) = 1 \cdot n + 1 = n + 1 = n{+}{+}$ by the induction hypothesis and Proposition 0.2.5. For the other side we have $(n{+}{+}) \cdot 1 = (n{+}{+}) \cdot (0{+}{+}) = [(n{+}{+}) \cdot 0] + n{+}{+} = 0 + n{+}{+} = n{+}{+}$.

**Associativity of multiplication:** Again we proceed by induction on $n$. The base case is easily established

$$\begin{aligned} l \cdot (m \cdot 0) &= l \cdot 0, && \text{Definition 0.2.2} \\ &= 0, && \text{Definition 0.2.2} \\ &= (l \cdot m) \cdot 0. && \text{Definition 0.2.2} \end{aligned}$$

Now assume the induction hypothesis. Then

$$\begin{aligned} l \cdot (m \cdot (n{+}{+})) &= l \cdot (m \cdot n + m), && \text{Definition 0.2.2} \\ &= l \cdot (m \cdot n) + l \cdot m, && \text{Distributive property} \\ &= (l \cdot m) \cdot n + (l \cdot m), && \text{Induction hypothesis} \\ &= (l \cdot m) \cdot (n + 1), && \text{Distributive property} \\ &= (l \cdot m) \cdot (n{+}{+}). && \text{Proposition 0.2.5} \end{aligned}$$

**Commutativity of multiplication:** Again we use induction on $n$. For the base case we have $0 = m \cdot 0$. On the other hand, for any $m$, we also need to show that $0 \cdot m = 0$. For this, observe $0 \cdot m + 0 = 0 \cdot m = (0 + 0) \cdot m = 0 \cdot m + 0 \cdot m$. By the cancellation property for addition, this implies $0 = 0 \cdot m$. Thus, $0 \cdot m = 0 = m \cdot 0$ for all $m$.

Now let us prove the induction step. Observe

$$\begin{aligned} m \cdot (n{+}{+}) &= m \cdot n + m, && \text{Definition 0.2.2} \\ &= n \cdot m + m, && \text{Induction hypothesis} \\ &= n \cdot m + 1 \cdot m, && \text{Multiplicative identity} \\ &= (n + 1) \cdot m, && \text{Distributive property} \\ &= (n{+}{+}) \cdot m. && \text{Proposition 0.2.5} \end{aligned}$$

**Cancellation for multiplication:** Let us prove this by induction on $m_1$. If $m_1 = 0$ then $n \cdot m_1 \neq 0$ is false which implies the statement is true vacuously (this means that an implication $A \Rightarrow B$ is true if $A$ is false). So the base case is established. Now assume cancellation is true for $m_1$. Assume $n \cdot (m_1{+}{+}) = n \cdot m_2$. If $m_2 = 0$, then $n \cdot (m_1{+}{+}) = n \cdot m_2 = 0$ which violates the assumption. Thus $m_2 \neq 0$ and there is a natural number $m_2'$ such that $m_2 = m_2'{+}{+}$. Thus,

$$\begin{aligned} n + n \cdot m_1 &= n \cdot m_1 + n, && \text{Commutativity of addition} \\ &= n \cdot (m_1{+}{+}), && \text{Definition 0.2.2} \\ &= n \cdot m_2, && \text{Assumption} \\ &= n \cdot (m_2'{+}{+}), && \text{Definition of } m_2' \\ &= n \cdot m_2' + n, && \text{Definition 0.2.2} \\ &= n + n \cdot m_2'. && \text{Commutativity of addition} \end{aligned}$$

By the cancellation property of addition, this implies that $n \cdot m_1 = n \cdot m_2'$. By the induction hypothesis, this implies $m_1 = m_2'$ and thus $m_1{+}{+} = m_2'{+}{+} = m_2$. This proves the induction step.

□