1 Multiplication

[readtex `arithmetic/sections/01_arithmetic/02_addition.ftl.tex`]

Let k, l, m, n denote natural numbers.

1.1 Axioms

Having introduced addition in the last section, we now define a multiplication operation on the natural numbers.

Signature 1.1. $n \cdot m$ is a natural number.

Let the product of n and m stand for $n \cdot m$.

Axiom 1.2 (1$^{\text{st}}$ multiplication axiom). $n \cdot 0 = 0$.

Axiom 1.3 (2$^{\text{nd}}$ multiplication axiom). $n \cdot (m + 1) = (n \cdot m) + n$.

1.2 Computation laws

Let us show some basic computation laws for it.

Associativity:

Proposition 1.4. For all n, m, k we have

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

Proof. Define

$$P = \{\, k \in \mathbb{N} \mid n \cdot (m + k) = (n \cdot m) + (n \cdot k) \text{ for all natural numbers } n, m \,\}.$$

(BASE CASE) 0 is an element of P. Indeed for all natural numbers n, m we have $n \cdot (m + 0) = n \cdot m = (n \cdot m) + 0 = (n \cdot m) + (n \cdot 0)$.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

For all natural numbers n, m we have $n \cdot (m + (k + 1)) = (n \cdot m) + (n \cdot (k + 1))$.
Proof. Let n, m be natural numbers.

$$\begin{aligned} & n \cdot (m + (k + 1)) \\ &= n \cdot ((m + k) + 1) \\ &= (n \cdot (m + k)) + n \end{aligned}$$

$$= ((n \cdot m) + (n \cdot k)) + n$$
$$= (n \cdot m) + ((n \cdot k) + n)$$
$$= (n \cdot m) + (n \cdot (k + 1)).$$

Hence the thesis. Qed. Qed.

Therefore every natural number is contained in P. ☐

Distributivity:

Proposition 1.5. For all n, m, k we have

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

Proof. Define

$P = \{ \, k \in \mathbb{N} \mid (n+m) \cdot k = (n \cdot k) + (m \cdot k) \text{ for all natural numbers } n, m \, \}$.

(BASE CASE) 0 belongs to P. Indeed $(n+m) \cdot 0 = 0 = 0+0 = (n \cdot 0)+(m \cdot 0)$ for all natural numbers n, m.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

$(n+m) \cdot (k+1) = (n \cdot (k+1)) + (m \cdot (k+1))$ for all natural numbers n, m.
Proof. Let n, m be natural numbers. We have $((n \cdot k)+((m \cdot k)+n))+m = (((n \cdot k) + n) + (m \cdot k)) + m$. Hence

$$(n + m) \cdot (k + 1)$$
$$= ((n + m) \cdot k) + (n + m)$$
$$= ((n \cdot k) + (m \cdot k)) + (n + m)$$
$$= (((n \cdot k) + (m \cdot k)) + n) + m$$
$$= ((n \cdot k) + ((m \cdot k) + n)) + m$$
$$= (((n \cdot k) + n) + (m \cdot k)) + m$$
$$= ((n \cdot k) + n) + ((m \cdot k) + m)$$
$$= (n \cdot (k + 1)) + (m \cdot (k + 1)).$$

Qed. Qed.

Thus every natural number is an element of P. ☐

Proposition 1.6. $n \cdot 1 = n$.

Proof. $n \cdot 1 = n \cdot (0 + 1) = (n \cdot 0) + n = 0 + n = n$. ☐

Corollary 1.7. $n \cdot 2 = n + n$.

Proof. $n \cdot 2 = n \cdot (1 + 1) = (n \cdot 1) + n = n + n$. ☐

Proposition 1.8. For all n, m, k we have

$$n \cdot (m \cdot k) = (n \cdot m) \cdot k.$$

Proof. Define

$$P = \{ k \in \mathbb{N} \mid n \cdot (m \cdot k) = (n \cdot m) \cdot k \text{ for all natural numbers } n, m \} .$$

(BASE CASE) 0 is contained in P. Indeed for all natural numbers n, m we have $n \cdot (m \cdot 0) = n \cdot 0 = 0 = (n \cdot m) \cdot 0$.

(INDUCTION STEP) For all natural numbers k we have $k \in P \implies k + 1 \in P$.
Proof. Let k be a natural number. Assume $k \in P$.

For all natural numbers n, m we have $n \cdot (m \cdot (k + 1)) = (n \cdot m) \cdot (k + 1)$.
Proof. Let n, m be natural numbers.

$$n \cdot (m \cdot (k + 1))$$

$$= n \cdot ((m \cdot k) + m)$$
$$= (n \cdot (m \cdot k)) + (n \cdot m)$$
$$= ((n \cdot m) \cdot k) + (n \cdot m)$$
$$= ((n \cdot m) \cdot k) + ((n \cdot m) \cdot 1)$$
$$= (n \cdot m) \cdot (k + 1).$$

Qed. Qed.

Hence every natural number is contained in P. ☐

Commutativity:

Proposition 1.9. For all n, m we have

$$n \cdot m = m \cdot n.$$

Proof. Define

$$P = \{ m \in \mathbb{N} \mid n \cdot m = m \cdot n \text{ for all natural numbers } n \} .$$

(BASE CASE 1) 0 is contained in P.
Proof.

For all natural numbers n we have $n \cdot 0 = 0 \cdot n$.
Proof. Define

$$Q = \{ n \in \mathbb{N} \mid n \cdot 0 = 0 \cdot n \}.$$

0 is contained in Q.

For all natural numbers n we have $n \in Q \implies n+1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$. Then

$$(n+1) \cdot 0 = 0 = n \cdot 0 = 0 \cdot n = (0 \cdot n) + 0 = 0 \cdot (n+1).$$

Qed. Qed. Qed.

(BASE CASE 2) 1 belongs to P.
Proof. Let us show that for all natural numbers n we have $n \cdot 1 = 1 \cdot n$. Define

$$Q = \{ n \in \mathbb{N} \mid n \cdot 1 = 1 \cdot n \}.$$

0 is contained in Q.

For all natural numbers n we have $n \in Q \implies n+1 \in Q$.
Proof. Let n be a natural number. Assume $n \in Q$. Then

$$\begin{gathered}(n+1) \cdot 1 \\ = (n \cdot 1) + 1 \\ = (1 \cdot n) + 1 \\ = 1 \cdot (n+1).\end{gathered}$$

Qed.

Thus every natural number is contained in Q. Hence the thesis. End. Qed.

(INDUCTION STEP) For all natural numbers m we have $m \in P \implies m+1 \in P$.
Proof. Let m be a natural number. Assume $m \in P$.

For all natural numbers n we have $n \cdot (m+1) = (m+1) \cdot n$.
Proof. Let n be a natural number. Then

$$\begin{gathered}n \cdot (m+1) \\ = (n \cdot m) + (n \cdot 1) \\ = (m \cdot n) + (1 \cdot n) \\ = (1 \cdot n) + (m \cdot n) \\ = (1 + m) \cdot n \\ = (m+1) \cdot n.\end{gathered}$$

Qed. Qed.

Hence every natural number is contained in P. $\square$

Non-existence of zero-divisors:

Proposition 1.10. For all n, m we have

$$n \cdot m = 0 \implies (n = 0 \text{ or } m = 0).$$

Proof. Let n, m be natural numbers. Assume $n \cdot m = 0$.

If n and m are not equal to 0 then we have a contradiction.
Proof. Assume $n, m \neq 0$. Take natural numbers n', m' such that $n = (n' + 1)$ and $m = (m' + 1)$. Then

$$0$$

$$\begin{aligned} &= n \cdot m \\ &= (n' + 1) \cdot (m' + 1) \\ &= ((n' + 1) \cdot m') + (n' + 1) \\ &= (((n' + 1) \cdot m') + n') + 1. \end{aligned}$$

Hence $0 = k + 1$ for some natural number k. Contradiction. Qed.

Thus $n = 0$ or $m = 0$. $\square$

Cancellation:

Proposition 1.11. Assume $k \neq 0$. Then for all n, m we have

$$n \cdot k = m \cdot k \implies n = m.$$

Proof. Define

$$P = \left\{ n \in \mathbb{N} \,\middle|\, \begin{array}{l} \text{for all natural numbers } m \text{ if } n \cdot k = m \cdot k \text{ and } k \neq 0 \text{ then} \\ n = m \end{array} \right\}.$$

(BASE CASE) 0 is contained in P.
Proof. Let us show that for all natural numbers m if $0 \cdot k = m \cdot k$ and $k \neq 0$ then $0 = m$. Let m, k be natural numbers. Assume that $0 \cdot k = m \cdot k$ and $k \neq 0$. Then $m \cdot k = 0$. Hence $m = 0$ or $k = 0$. Thus $m = 0$. End. Qed.

(INDUCTION STEP) For all natural numbers n we have $n \in P \implies n + 1 \in P$.
Proof. Let n be a natural number. Assume $n \in P$.

For all natural numbers m if $(n + 1) \cdot k = m \cdot k$ and $k \neq 0$ then $n + 1 = m$.
Proof. Let m be natural numbers. Assume $(n + 1) \cdot k = m \cdot k$ and $k \neq 0$.

Case $m = 0$. Then $(n + 1) \cdot k = 0$. Hence $n + 1 = 0$. Contradiction. End.

Case $m \neq 0$. Take a natural number m' such that $m = m' + 1$. Then $(n + 1) \cdot k = (m' + 1) \cdot k$. Hence $(n \cdot k) + k = (m' \cdot k) + k$. Thus $n \cdot k = m' \cdot k$

(by **??**). Then we have $n = m'$. Therefore $n+1 = m'+1 = m$. End. Qed. Qed.

Thus every natural number is contained in P. □

Corollary 1.12. Assume $k \neq 0$. Then for all n, m we have

$$k \cdot n = k \cdot m \implies n = m.$$

Proof. Let n, m be natural numbers. Assume $k \cdot n = k \cdot m$. We have $k \cdot n = n \cdot k$ and $k \cdot m = m \cdot k$. Hence $n \cdot k = m \cdot k$. Thus $n = m$. □