Chapter 1

Multiplication

File: `arithmetic/sections/05_multiplication.ftl.tex`

[readtex `arithmetic/sections/05_subtraction.ftl.tex`]

1.1 Definition of multiplication

ARITHMETIC_06_7897906468093952

Lemma 1.1. There exists a $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\varphi(n, 0) = 0$ and $\varphi(n, m + 1) = \varphi(n, m) + n$ for any $m \in \mathbb{N}$.

Proof. Take $A = [\mathbb{N} \to \mathbb{N}]$. Define $a(n) = 0$ for $n \in \mathbb{N}$. Then A is a set and $a \in A$.

[skipfail on] Define $f(g) = \lambda n \in \mathbb{N}.g(n) + n$ for $g \in A$. [skipfail off]

Then $f : A \to A$. Indeed $f(g)$ is a map from $\mathbb{N}$ to $\mathbb{N}$ for any $g \in A$. Consider a $\psi : \mathbb{N} \to A$ such that ψ is recursively defined by a and f (by **??**). For any objects n, m we have $(n, m) \in \mathbb{N} \times \mathbb{N}$ iff $n, m \in \mathbb{N}$. Define $\varphi(n, m) = \psi(m)(n)$ for $(n, m) \in \mathbb{N} \times \mathbb{N}$. Then φ is a map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$. Indeed $\varphi(n, m) \in \mathbb{N}$ for all $n, m \in \mathbb{N}$.

(1) For all $n \in \mathbb{N}$ we have $\varphi(n, 0) = 0$.
Proof. Let $n \in \mathbb{N}$. Then $\varphi(n, 0) = \psi(0)(n) = a(0) = 0$. Qed.

(2) For all $n, m \in \mathbb{N}$ we have $\varphi(n, m + 1) = \varphi(n, m) + n$.
Proof. Let $n, m \in \mathbb{N}$. Then $\varphi(n, m+1) = \psi(m+1)(n) = f(\psi(m))(n) = \psi(m)(n)+n = \varphi(n, m) + n$. Qed. □

ARITHMETIC_06_2076592937369600

Lemma 1.2. Let $\varphi, \varphi' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi(n, 0) = 0$ and $\varphi(n, m+1) = \varphi(n, m) + n$ for any $m \in \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi'(n, 0) = 0$ and $\varphi'(n, m+1) = \varphi'(n, m) + n$ for any $m \in \mathbb{N}$. Then $\varphi = \varphi'$.

Proof. Define $\Phi = \{m \in \mathbb{N} \mid \varphi(n, m) = \varphi'(n, m) \text{ for all } n \in \mathbb{N}\}$.

(1) $0 \in \Phi$. Indeed $\varphi(n, 0) = 0 = \varphi'(n, 0)$ for all $n \in \mathbb{N}$.

(2) For all $m \in \Phi$ we have $m + 1 \in \Phi$.
Proof. Let $m \in \Phi$. Then $\varphi(n, m) = \varphi'(n, m)$ for all $n \in \mathbb{N}$. Hence $\varphi(n, m+1) = \varphi(n, m) + n = \varphi'(n, m) + n = \varphi'(n, m+1)$ for all $n \in \mathbb{N}$. Qed.

Thus Φ contains every natural number. Therefore $\varphi(n, m) = \varphi'(n, m)$ for all $n, m \in \mathbb{N}$. □

ARITHMETIC_06_6626346484629504

Definition 1.3. mul is the map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\mathrm{mul}(n, 0) = 0$ and $\mathrm{mul}(n, m+1) = \mathrm{mul}(n, m) + n$ for any $m \in \mathbb{N}$.

Let $n \cdot m$ stand for $\mathrm{mul}(n, m)$. Let the product of n and m stand for $n \cdot m$.

ARITHMETIC_06_1682857820946432

Lemma 1.4. Let n, m be natural numbers. Then $(n, m) \in \mathrm{dom}(\mathrm{mul})$.

ARITHMETIC_06_8420678923452416

Lemma 1.5. Let n, m be natural numbers. Then $n \cdot m$ is a natural number.

ARITHMETIC_06_8941041092657152

Lemma 1.6. Let n be a natural number. Then $n \cdot 0 = 0$.

ARITHMETIC_06_2211275408932864

Lemma 1.7. Let n, m be natural numbers. Then $n \cdot (m + 1) = (n \cdot m) + n$.

1.2 Computation laws

Distributivity

ARITHMETIC_06_9001524774567936

Proposition 1.8. Let n, m, k be natural numbers. Then

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

Proof. Define $\Phi = \{k' \in \mathbb{N} \mid n \cdot (m + k') = (n \cdot m) + (n \cdot k')\}$.

(1) 0 is an element of Φ. Indeed $n \cdot (m + 0) = n \cdot m = (n \cdot m) + 0 = (n \cdot m) + (n \cdot 0)$.

(2) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$. Then

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

Hence $n \cdot (m + (k' + 1)) = (n \cdot m) + (n \cdot (k' + 1))$. Thus $k' + 1 \in \Phi$. Qed.

Thus every natural number is contained in Φ. Therefore $n \cdot (m + k) = (n \cdot m) + (n \cdot k)$. □

ARITHMETIC_06_5742967566368768

Proposition 1.9. Let n, m, k be natural numbers. Then

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

Proof. Define $\Phi = \{k' \in \mathbb{N} \mid (n + m) \cdot k' = (n \cdot k') + (m \cdot k')\}$.

(1) 0 belongs to Φ. Indeed $(n + m) \cdot 0 = 0 = 0 + 0 = (n \cdot 0) + (m \cdot 0)$.

(2) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$. Then

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

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

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

Thus every natural number is an element of Φ. Therefore $(n+m) \cdot k = (n \cdot k) + (m \cdot k)$. □

Multiplication with 1 and 2

ARITHMETIC_06_2910559821365248

Proposition 1.10. Let n be a natural number. Then

$$n \cdot 1 = n.$$

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

ARITHMETIC_06_5679541582299136

Corollary 1.11. Let n be a natural number. Then

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

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

Associativity

ARITHMETIC_06_347295585402880

Proposition 1.12. Let n, m, k be natural numbers. Then

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

Proof. Define $\Phi = \{k' \in \mathbb{N} \mid n \cdot (m \cdot k') = (n \cdot m) \cdot k'\}$.

(1) 0 is contained in Φ. Indeed $n \cdot (m \cdot 0) = n \cdot 0 = 0 = (n \cdot m) \cdot 0$.

(2) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$. Then

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

Qed.

Hence every natural number is contained in Φ. Thus $n \cdot (m \cdot k) = (n \cdot m) \cdot k$. □

Commutativity

ARITHMETIC_06_1764759896588288

Proposition 1.13. Let n, m be natural numbers. Then

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

Proof. Define $\Phi = \{m' \in \mathbb{N} \mid n \cdot m' = m' \cdot n\}$.

(1) 0 is contained in Φ.
Proof. Define $\Psi = \{n' \in \mathbb{N} \mid n' \cdot 0 = 0 \cdot n'\}$.

(1a) 0 is contained in Ψ.

(1b) For all $n' \in \Psi$ we have $n' + 1 \in \Psi$.
Proof. Let $n' \in \Psi$. Then

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

Qed.

Hence every natural number is contained in Ψ. Thus $n \cdot 0 = 0 \cdot n$. Qed.

(2) 1 belongs to Φ.
Proof. Define $\Theta = \{n' \in \mathbb{N} \mid n' \cdot 1 = 1 \cdot n'\}$.

(2a) 0 is contained in Θ.

(2b) For all $n' \in \Theta$ we have $n' + 1 \in \Theta$.
Proof. Let $n' \in \Theta$. Then

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

Qed.

Thus every natural number is contained in Θ. Therefore $n \cdot 1 = 1 \cdot n$. Qed.

(3) For all $m' \in \Phi$ we have $m' + 1 \in \Phi$.
Proof. Let $m' \in \Phi$. Then

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

Indeed $((1 \cdot n) + (m' \cdot n)) = (1 + m') \cdot n$. Qed.

Hence every natural number is contained in Φ. Thus $n \cdot m = m \cdot n$. □

Non-existence of zero-divisors

ARITHMETIC_06_3843962875936768

Proposition 1.14. Let n, m be natural numbers such that $n \cdot m = 0$. Then $n = 0$ or $m = 0$.

Proof. Suppose $n, m \neq 0$. Take natural numbers n', m' such that $n = (n' + 1)$ and $m = (m' + 1)$. Then

$$\begin{aligned} &0 \\ &= n \cdot m \end{aligned}$$

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

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

Cancellation

ARITHMETIC_06_31055184658432

Proposition 1.15. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n \cdot k = m \cdot k \quad \text{implies} \quad n = m.$$

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid \text{for all } m' \in \mathbb{N} \text{ if } n' \cdot k = m' \cdot k \text{ and } k \neq 0 \text{ then } n' = m'\}$.

(1) 0 is contained in Φ.
Proof. Let $m' \in \mathbb{N}$. Assume $0 \cdot k = m' \cdot k$ and $k \neq 0$. Then $m' \cdot k = 0$. Hence $m' = 0$ or $k = 0$. Thus $m' = 0$. Qed.

(2) For all $n' \in \Phi$ we have $n' + 1 \in \Phi$.
Proof. Let $n' \in \Phi$.

Let us show that for all $m' \in \mathbb{N}$ if $(n' + 1) \cdot k = m' \cdot k$ and $k \neq 0$ then $n' + 1 = m'$.
Let $m' \in \mathbb{N}$. 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 l such that $m' = l+1$. Then $(n'+1) \cdot k = (l+1) \cdot k$.
Hence $(n' \cdot k) + k = (n' \cdot k) + (1 \cdot k) = (n' \cdot k) + k = (l+1) \cdot k = (l \cdot k) + (1 \cdot k) = (l \cdot k) + k$.
Thus $n' \cdot k = l \cdot k$. Then we have $n' = l$. Indeed if $n' \cdot k = l \cdot k$ and $k \neq 0$ then $n' = l$.
Therefore $n' + 1 = l + 1 = m'$. End. End.

[prover vampire] Hence $n' + 1 \in \Phi$. Qed.

Thus every natural number is contained in Φ. Therefore if $n \cdot k = m \cdot k$ then $n = m$. □

ARITHMETIC_06_8575191374364672

Corollary 1.16. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$k \cdot n = k \cdot m \quad \text{implies} \quad n = m.$$

Proof. 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 $n = m$ (by proposition 1.15). □

1.3 Ordering and multiplication

ARITHMETIC_06_8817333933965312

Proposition 1.17. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n < m \quad \text{iff} \quad n \cdot k < m \cdot k.$$

Proof. Case $n \cdot k < m \cdot k$. Define $\Phi = \{n' \in \mathbb{N} \mid \text{if } n' \cdot k < m \cdot k \text{ then } n' < m\}$.

(1) Φ contains 0.

(2) For all $n' \in \Phi$ we have $n' + 1 \in \Phi$.
Proof. Let $n' \in \Phi$.

Let us show that if $(n' + 1) \cdot k < m \cdot k$ then $n' + 1 < m$. Assume $(n' + 1) \cdot k < m \cdot k$. Then $(n' \cdot k) + k < m \cdot k$. Hence $n' \cdot k < m \cdot k$. Thus $n' < m$. Then $n' + 1 \leq m$. If $n' + 1 = m$ then $(n' + 1) \cdot k = m \cdot k$. Hence $n' + 1 < m$. End. Qed.

Therefore every natural number is contained in Φ. Consequently $n < m$. End.

Case $n < m$. Take a positive natural number l such that $m = n + l$. Then $m \cdot k = (n + l) \cdot k = (n \cdot k) + (l \cdot k)$. $l \cdot k$ is positive. Hence $n \cdot k < m \cdot k$. End. □

ARITHMETIC_06_5048640368279552

Corollary 1.18. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n < m \quad \text{iff} \quad k \cdot n < k \cdot m.$$

Proof. We have $k \cdot n = n \cdot k$ and $k \cdot m = m \cdot k$. Hence $k \cdot n < k \cdot m$ iff $n \cdot k < m \cdot k$. □

ARITHMETIC_06_1826268599287808

Proposition 1.19. Let n, m, k be natural numbers. Then

$$n, m > k \quad \text{implies} \quad n \cdot m > k.$$

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid \text{if } n', m > k \text{ then } n' \cdot m > k\}$.

(1) Φ contains 0.

(2) For all $n' \in \Phi$ we have $n' + 1 \in \Phi$.
Proof. Let $n' \in \Phi$.

Let us show that if $n' + 1, m > k$ then $(n' + 1) \cdot m > k$. Assume $n' + 1, m > k$. Then

$(n'+1)\cdot m = (n'\cdot m)+m$. If $n'=0$ then $(n'\cdot m)+m = 0+m = m > k$. If $n' \neq 0$ then $(n'\cdot m)+m > m > k$. Indeed if $n' \neq 0$ then $n'\cdot m > 0$. Indeed $m > 0$. Hence $(n'+1)\cdot m > k$. Qed. Qed.

Thus every natural number is contained in Φ. Therefore if $n, m > k$ then $n \cdot m > k$. ☐

ARITHMETIC_06_1751605544222720

Corollary 1.20. Let n, m, k be natural numbers. Then

$$n \leq m \quad \text{implies} \quad k\cdot n \leq k \cdot m.$$

ARITHMETIC_06_3965209318260736

Corollary 1.21. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$k\cdot n \leq k\cdot m \quad \text{implies} \quad n \leq m.$$

ARITHMETIC_06_8946886668976128

Corollary 1.22. Let n, m, k be natural numbers. Then

$$n \leq m \quad \text{implies} \quad n\cdot k \leq m \cdot k.$$

ARITHMETIC_06_4374428949413888

Corollary 1.23. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n\cdot k \leq m\cdot k \quad \text{implies} \quad n \leq m.$$

ARITHMETIC_06_8813409145454592

Proposition 1.24. Let n, m, k be natural numbers. Assume $m > 0$ and $k > 1$. Then $k \cdot m > m$.

Proof. Take a natural number l such that $k = l + 2$. Then

$$k \cdot m$$

$$= (l+2)\cdot m$$

$$= (l\cdot m) + (2\cdot m)$$

$$
\begin{aligned}
&= (l \cdot m) + (m + m) \\
&= ((l \cdot m) + m) + m \\
&= ((l + 1) \cdot m) + m \\
&\geq 1 + m \\
&> m.
\end{aligned}
$$

Indeed $((l + 1) \cdot m) + m \geq 1 + m$. □

1.4 Multiplication and subtraction

ARITHMETIC_06_5458841930039296

Proposition 1.25. Let n, m, k be natural numbers such that $n \geq m$. Then

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

Proof. We have

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

Hence $(n - m) \cdot k = (n \cdot k) - (m \cdot k)$. □

ARITHMETIC_06_8461123277815808

Corollary 1.26. Let n, m, k be natural numbers such that $n \geq m$. Then

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