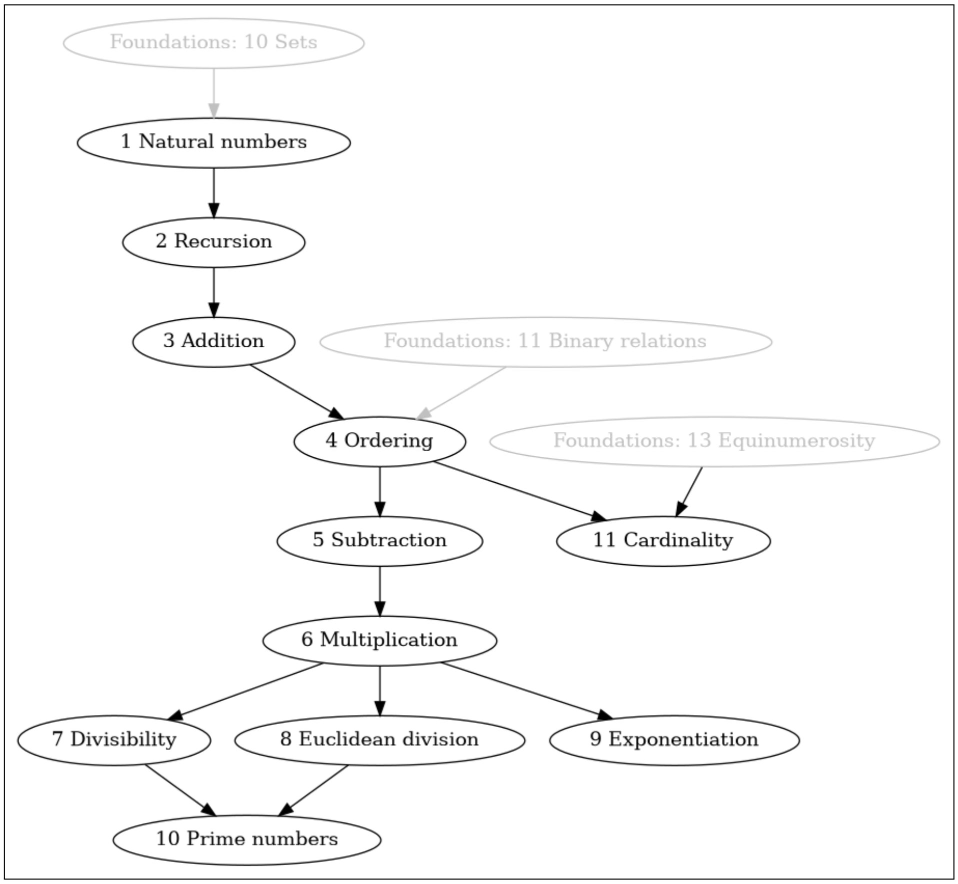
Arithmetic

Marcel Schütz

2022

Contents



Interdependencies of the chapters

Introduction

This is a library providing basic notions of natural numbers arithmetic. It introduces the natural numbers on the basis of the Peano Axioms (chapter 1) and uses Dedekind's Recursion Theorem (chapter 2) to define common arithmetical operations on them. A first example of such operations is given by addition (chapter 3), on the basis of which the standard ordering on the natural numbers is defined (chapter 4) and also a (partial) subtraction operation (chapter 5). Another example of arithmetical operations is provided by multiplication (chapter 6) which is further used to define the notions of divisibility (chapter 7) and Euclidean division (chapter 8). Moreover, an exponentiation operation is defined (chapter 9) and the notion of prime numbers is introduced (chapter 10). Furthermore, a chapter on cardinality (chapter 11) provides notions concerning finite, countable and uncountable sets.

Usage. At the very beginning of each chapter you can find the name of its source file, e.g. `arithmetic/sections/01_natural-numbers.ftl.tex` for chapter 1. This filename can be used to import the chapter via ℕaproche's `readtex` instruction to another ForTheL text, e.g.:

```
[readtex \path{arithmetic/sections/01_natural-numbers.ftl.tex}]
```

Checking times. The checking times for each of the chapters may vary from computer to computer, but on mid-range hardware they are likely to be similar to those given in table below:

	Checking time	
Chapter	**without dependencies**	**with dependencies**
1	00:15 min	06:55 min
2	02:25 min	09:20 min
3	01:55 min	11:15 min
4	03:05 min	14:35 min
5	00:50 min	15:25 min
6	05:35 min	21:00 min
7	00:45 min	21:45 min
8	04:00 min	25:00 min
9	07:55 min	28:55 min
10	03:30 min	29:15 min
11	07:50 min	24:50 min

Chapter 1

Natural numbers

File: `arithmetic/sections/01_natural-numbers.ftl.tex`

[readtex `foundations/sections/10_sets.ftl.tex`]

1.1 The language of Peano Arithmetic

ARITHMETIC_01_3074681254969344

Signature 1.1. A natural number is an object.

ARITHMETIC_01_7367148418629632

Definition 1.2. $\mathbb{N}$ is the class of natural numbers.

ARITHMETIC_01_7633304715001856

Signature 1.3. 0 is a natural number.

Let zero stand for 0. Let n is nonzero stand for $n \neq 0$.

ARITHMETIC_01_1567933815848960

Signature 1.4. Let n be a natural number. $\mathrm{succ}(n)$ is a natural number.

Let the direct successor of n stand for $\mathrm{succ}(n)$.

1.2 The Peano Axioms

ARITHMETIC_01_3604163883696128

Axiom 1.5. Let n, m be natural numbers. If $\mathrm{succ}(n) = \mathrm{succ}(m)$ then $n = m$.

ARITHMETIC_01_4454289938317312

Axiom 1.6. There exists no natural number n such that $\mathrm{succ}(n) = 0$.

ARITHMETIC_01_4764664342773760

Axiom 1.7. Let Φ be a class. Assume $0 \in \Phi$ and for all natural numbers n if $n \in \Phi$ then $\mathrm{succ}(n) \in \Phi$. Then Φ contains every natural number.

1.3 Immediate consequences

ARITHMETIC_01_4966080109871104

Proposition 1.8. Let n be a natural number. Then $n = 0$ or $n = \mathrm{succ}(m)$ for some natural number m.

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid n' = 0 \text{ or } n' = \mathrm{succ}(m') \text{ for some natural number } m'\}$. $0 \in \Phi$ and for all $n' \in \Phi$ we have $\mathrm{succ}(n') \in \Phi$. Hence every natural number is contained in Φ. Thus $n = 0$ or $n = \mathrm{succ}(m)$ for some natural number m. □

ARITHMETIC_01_5996049267163136

Proposition 1.9. Let n be a natural number. Then $n \neq \mathrm{succ}(n)$.

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid n' \neq \mathrm{succ}(n')\}$.

(1) 0 belongs to Φ.

(2) For all $n' \in \Phi$ we have $\mathrm{succ}(n') \in \Phi$.
Proof. Let $n' \in \Phi$. Then $n' \neq \mathrm{succ}(n')$. If $\mathrm{succ}(n') = \mathrm{succ}(\mathrm{succ}(n'))$ then $n' = \mathrm{succ}(n')$. Thus it is wrong that $\mathrm{succ}(n') = \mathrm{succ}(\mathrm{succ}(n'))$. Hence $\mathrm{succ}(n') \in \Phi$. Qed.

Therefore every natural number is an element of Φ. Consequently $n \neq \mathrm{succ}(n)$. ☐

ARITHMETIC_01_6115694068367360

Proposition 1.10. $\mathbb{N}$ is a set.

Proof. Define $f(n) = \mathrm{succ}(n)$ for $n \in \mathbb{N}$. Then f is a map from $\mathbb{N}$ to $\mathbb{N}$. Hence we can take a subset X of $\mathbb{N}$ that is inductive regarding 0 and f. Then $0 \in X$ and for all $n \in X$ we have $\mathrm{succ}(n) \in X$. Hence X contains every natural number. Thus we have $\mathbb{N} \subseteq X$ and $X \subseteq \mathbb{N}$. Therefore $\mathbb{N} = X$. Consequently $\mathbb{N}$ is a set. ☐

1.4 Additional constants

ARITHMETIC_01_7540560137027584

Definition 1.11. $1 = \mathrm{succ}(0)$.

Let one stand for 1.

ARITHMETIC_01_4584236572999680

Definition 1.12. $2 = \mathrm{succ}(1)$.

Let two stand for 2.

ARITHMETIC_01_3836725109456896

Definition 1.13. $3 = \mathrm{succ}(2)$.

Let three stand for 3.

ARITHMETIC_01_1709884968009728

Definition 1.14. $4 = \mathrm{succ}(3)$.

Let four stand for 4.

ARITHMETIC_01_6734726333202432

Definition 1.15. $5 = \mathrm{succ}(4)$.

Let five stand for 5.

ARITHMETIC_01_949139189792768

Definition 1.16. $6 = \mathrm{succ}(5)$.

Let six stand for 6.

ARITHMETIC_01_7245471749767168

Definition 1.17. $7 = \mathrm{succ}(6)$.

Let seven stand for 7.

ARITHMETIC_01_5658172888973312

Definition 1.18. $8 = \mathrm{succ}(7)$.

Let eight stand for 8.

ARITHMETIC_01_7371844250238976

Definition 1.19. $9 = \mathrm{succ}(8)$.

Let nine stand for 9.

Chapter 2

Recursion

File: `arithmetic/sections/02_recursion.ftl.tex`

[readtex `arithmetic/sections/01_natural-numbers.ftl.tex`]

ARITHMETIC_02_4608408013504512

Definition 2.1. Let a be an object and f be a map. Let φ be a map from $\mathbb{N}$ to $\mathrm{dom}(f)$. φ is recursively defined by a and f iff $\varphi(0) = a$ and $\varphi(\mathrm{succ}(n)) = f(\varphi(n))$ for every $n \in \mathbb{N}$.

ARITHMETIC_02_2489427471368192

Theorem 2.2 (Dedekind). Let A be a set and $a \in A$ and $f : A \to A$. Then there exists a $\varphi : \mathbb{N} \to A$ that is recursively defined by a and f.

Proof. Define

$$\Phi = \left\{ H \in \mathcal{P}(\mathbb{N} \times A) \;\middle|\; \begin{array}{l} (0, a) \in H \text{ and for all } n \in \mathbb{N} \text{ and all } x \in A \text{ if } (n, x) \in H \\ \text{then } (\mathrm{succ}(n), f(x)) \in H \end{array} \right\}.$$

Let us show that $\bigcap \Phi \in \Phi$.
Proof.

(1) $\bigcap \Phi \in \mathcal{P}(\mathbb{N} \times A)$.
Proof. We have $\mathbb{N} \times A \in \Phi$. Hence Φ is nonempty. Any element of $\bigcap \Phi$ is contained

in every element of Φ. Hence any element of $\bigcap \Phi$ is contained in $\mathbb{N} \times A$. Thus $\bigcap \Phi \subseteq \mathbb{N} \times A$. $\bigcap \Phi$ is a set. Hence $\bigcap \Phi$ is a subset of $\mathbb{N} \times A$. Qed.

(2) $(0, a) \in \bigcap \Phi$.
Indeed $(0, a) \in \mathbb{N} \times A \in \Phi$.

(3) For all $n \in \mathbb{N}$ and all $x \in A$ if $(n, x) \in \bigcap \Phi$ then $(\mathrm{succ}(n), f(x)) \in \bigcap \Phi$.
Proof. Let $n \in \mathbb{N}$ and $x \in A$. Assume $(n, x) \in \bigcap \Phi$. Then (n, x) is contained in every element of Φ. Hence $(\mathrm{succ}(n), f(x))$ is contained in every element of Φ. Thus $(\mathrm{succ}(n), f(x)) \in \bigcap \Phi$. Qed. Qed.

Let us show that for any $n \in \mathbb{N}$ there exists an $x \in A$ such that $(n, x) \in \bigcap \Phi$.
Proof. Define $\Psi = \{n \in \mathbb{N} \mid \text{there exists an } x \in A \text{ such that } (n, x) \in \bigcap \Phi\}$.

(1) 0 is contained in Ψ. Indeed $(0, a) \in \bigcap \Phi$.

(2) For all $n \in \Psi$ we have $\mathrm{succ}(n) \in \Psi$.
Proof. Let $n \in \Psi$. Take an $x \in A$ such that $(n, x) \in \bigcap \Phi$. Then $(\mathrm{succ}(n), f(x)) \in \bigcap \Phi$. Hence $\mathrm{succ}(n) \in \Psi$. Indeed $f(x) \in A$. Qed. Qed.

Let us show that for all $n \in \mathbb{N}$ and all $x, y \in A$ if $(n, x), (n, y) \in \bigcap \Phi$ then $x = y$.
Proof. (a) Define $\Theta = \{n \in \mathbb{N} \mid \text{for all } x, y \in A \text{ if } (n, x), (n, y) \in \bigcap \Phi \text{ then } x = y\}$.

(1) Θ contains 0.
Proof. Let us show that for all $x, y \in A$ if $(0, x), (0, y) \in \bigcap \Phi$ then $x = y$. Let $x, y \in A$. Assume $(0, x), (0, y) \in \bigcap \Phi$.

Let us show that $x, y = a$. Assume $x \neq a$ or $y \neq a$.

Case $x \neq a$. $(0, x), (0, a)$ are contained in every element of Φ. Then $(0, x), (0, a) \in \bigcap \Phi$. Take $H = (\bigcap \Phi) \setminus \{(0, x)\}$.

Let us show that $H \in \Phi$. (1) $H \in \mathcal{P}(\mathbb{N} \times A)$.

(2) $(0, a) \in H$.

(3) For all $n \in \mathbb{N}$ and all $b \in A$ if $(n, b) \in H$ then $(\mathrm{succ}(n), f(b)) \in H$.
Proof. Let $n \in \mathbb{N}$ and $b \in A$. Assume $(n, b) \in H$. Then $(\mathrm{succ}(n), f(b)) \in \bigcap \Phi$. We have $(\mathrm{succ}(n), f(b)) \neq (0, x)$. Hence $(\mathrm{succ}(n), f(b)) \in H$. Qed. End.

Then $(0, x)$ is not contained in every member of Φ. Contradiction. End.

Case $y \neq a$. $(0, y), (0, a)$ are contained in every element of Φ. Then $(0, y), (0, a) \in \bigcap \Phi$. Take $H = (\bigcap \Phi) \setminus \{(0, y)\}$.

Let us show that $H \in \Phi$. (1) $H \in \mathcal{P}(\mathbb{N} \times A)$.

(2) $(0, a) \in H$.

(3) For all $n \in \mathbb{N}$ and all $b \in A$ if $(n, b) \in H$ then $(\mathrm{succ}(n), f(b)) \in H$.
Proof. Let $n \in \mathbb{N}$ and $b \in A$. Assume $(n, b) \in H$. Then $(\mathrm{succ}(n), f(b)) \in \bigcap \Phi$. We have $(\mathrm{succ}(n), f(b)) \neq (0, y)$. Hence $(\mathrm{succ}(n), f(b)) \in H$. Qed. End.

Then $(0, y)$ is not contained in every member of Φ. Contradiction. End. End. End.

Qed.

(2) For all $n \in \Theta$ we have $\mathrm{succ}(n) \in \Theta$.
Proof. Let $n \in \Theta$. Then for all $x, y \in A$ if $(n, x), (n, y) \in \bigcap \Phi$ then $x = y$. Consider a $b \in A$ such that $(n, b) \in \bigcap \Phi$. Then $(\mathrm{succ}(n), f(b)) \in \bigcap \Phi$.

Let us show that for all $x, y \in A$ if $(\mathrm{succ}(n), x), (\mathrm{succ}(n), y) \in \bigcap \Phi$ then $x = f(b) = y$. Let $x, y \in A$. Assume $(\mathrm{succ}(n), x), (\mathrm{succ}(n), y) \in \bigcap \Phi$. Suppose $x \neq f(b)$ or $y \neq f(b)$.

Case $x \neq f(b)$. Take $H = (\bigcap \Phi) \setminus \{(\mathrm{succ}(n),\, x)\}$.

(a) $H \in \mathcal{P}(\mathbb{N} \times A)$.

(b) $(0, a) \in H$. Indeed $(0, a) \in \bigcap \Phi$ and $(0, a) \notin \{(\mathrm{succ}(n),\, x)\}$.

(c) For all $m \in \mathbb{N}$ and all $z \in A$ if $(m, z) \in H$ then $(\mathrm{succ}(m), f(z)) \in H$.
Proof. Let $m \in \mathbb{N}$ and $z \in A$. Assume $(m, z) \in H$. Then $(m, z) \in \bigcap \Phi$. Hence $(\mathrm{succ}(m), f(z)) \in \bigcap \Phi$. $(\mathrm{succ}(m), f(z)) \neq (\mathrm{succ}(n), x)$. Therefore $(\mathrm{succ}(m), f(z)) \in H$. Qed.

Thus $H \in \Phi$. Therefore every element of $\bigcap \Phi$ is contained in H. Consequently $(\mathrm{succ}(n), x) \in H$. Contradiction. End.

Case $y \neq f(b)$. Take a class H such that $H = (\bigcap \Phi) \setminus \{(\mathrm{succ}(n),\, y)\}$.

(a) $H \in \mathcal{P}(\mathbb{N} \times A)$.

(b) $(0, a) \in H$. Indeed $(0, a) \in \bigcap \Phi$ and $(0, a) \notin \{(\mathrm{succ}(n),\, y)\}$.

(c) For all $m \in \mathbb{N}$ and all $z \in A$ if $(m, z) \in H$ then $(\mathrm{succ}(m), f(z)) \in H$.
Proof. Let $m \in \mathbb{N}$ and $z \in A$. Assume $(m, z) \in H$. Then $(m, z) \in \bigcap \Phi$. Hence $(\mathrm{succ}(m), f(z)) \in \bigcap \Phi$. $(\mathrm{succ}(m), f(z)) \neq (\mathrm{succ}(n), y)$. Therefore $(\mathrm{succ}(m), f(z)) \in H$. Qed.

Thus $H \in \Phi$. Therefore every element of $\bigcap \Phi$ is contained in H. Consequently $(\mathrm{succ}(n), y) \in H$. Contradiction. End.

Hence it is wrong that $x \neq f(b)$ or $y \neq f(b)$. Consequently $x = f(b) = y$. End.

Therefore $\mathrm{succ}(n) \in \Theta$ (by a). Qed. Qed.

Define $\varphi(n) =$ “choose $x \in A$ such that $(n, x) \in \bigcap \Phi$ in x” for $n \in \mathbb{N}$.

(1) Then φ is a map from $\mathbb{N}$ to A and we have $\varphi(0) = a$.

(2) For all $n \in \mathbb{N}$ we have $\varphi(\mathrm{succ}(n)) = f(\varphi(n))$.
Proof. Let $n \in \mathbb{N}$. Take $x \in A$ such that $\varphi(n) = x$. Then $(n, x) \in \bigcap \Phi$. Hence $(\mathrm{succ}(n), f(\varphi(n))) = (\mathrm{succ}(n), f(x)) \in \bigcap \Phi$. Thus $\varphi(\mathrm{succ}(n)) = f(\varphi(n))$. Qed. □

ARITHMETIC_02_7510132520910848

Proposition 2.3. Let A be a set and $a \in A$ and $f : A \to A$. Let $\varphi, \varphi' : \mathbb{N} \to A$. Assume that φ and φ' are recursively defined by a and f. Then $\varphi = \varphi'$.

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

(1) Φ contains 0. Indeed $\varphi(0) = a = \varphi'(0)$.

(2) For all $n \in \Phi$ we have $\mathrm{succ}(n) \in \Phi$.
Proof. Let $n \in \Phi$. Then $\varphi(n) = \varphi'(n)$. Hence $\varphi(\mathrm{succ}(n)) = f(\varphi(n)) = f(\varphi'(n)) = \varphi'(\mathrm{succ}(n))$. Qed.

Thus Φ contains every natural number. Consequently $\varphi(n) = \varphi'(n)$ for each $n \in \mathbb{N}$. □

Chapter 3

Addition

File: `arithmetic/sections/03_addition.ftl.tex`

[readtex `arithmetic/sections/02_recursion.ftl.tex`]

3.1 Definition of addition

ARITHMETIC_03_722195546374144

Lemma 3.1. There exists a $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\varphi(n, 0) = n$ and $\varphi(n, \mathrm{succ}(m)) = \mathrm{succ}(\varphi(n, m))$ for all $m \in \mathbb{N}$.

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

[skipfail on] Define $f(g) = \lambda n \in \mathbb{N}.\, \mathrm{succ}(g(n))$ 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 theorem 2.2). 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 $\mathbb{N}$.

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

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

ARITHMETIC_04_2637025605844992

Lemma 3.2. Let $\varphi, \varphi' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi(n, 0) = n$ and $\varphi(n, \mathrm{succ}(m)) = \mathrm{succ}(\varphi(n, m))$ for all $m \in \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi'(n, 0) = n$ and $\varphi'(n, \mathrm{succ}(m)) = \mathrm{succ}(\varphi'(n, m))$ for all $m \in \mathbb{N}$. 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 $\varphi(n, 0) = n = \varphi'(n, 0)$ for all $n \in \mathbb{N}$.

(2) For all $m \in \Phi$ we have $\mathrm{succ}(m) \in \Phi$.
Proof. Let $m \in \Phi$. Then $\varphi(n, m) = \varphi'(n, m)$ for all $n \in \mathbb{N}$. Hence $\varphi(n, \mathrm{succ}(m)) = \mathrm{succ}(\varphi(n, m)) = \mathrm{succ}(\varphi'(n, m)) = \varphi(n, \mathrm{succ}(m))$ 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_03_4372222701469696

Definition 3.3. add is the map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\mathrm{add}(n, 0) = n$ and $\mathrm{add}(n, \mathrm{succ}(m)) = \mathrm{succ}(\mathrm{add}(n, m))$ for all $m \in \mathbb{N}$.

Let $n + m$ stand for $\mathrm{add}(n, m)$. Let the sum of n and m stand for $n + m$.

ARITHMETIC_03_3886414804549632

Lemma 3.4. Let n, m be natural numbers. Then $(n, m) \in \mathrm{dom}(\mathrm{add})$.

ARITHMETIC_03_5964925614686208

Lemma 3.5. Let n, m be natural numbers. Then $n + m$ is a natural number.

ARITHMETIC_03_777009668030464

Lemma 3.6. Let n be a natural number. Then $\mathrm{succ}(n) = n + 1$.

ARITHMETIC_03_4827955356237824

Lemma 3.7. Let n be a natural number. Then $n + 0 = n$.

ARITHMETIC_03_1031280145727488

Lemma 3.8. Let n, m be natural numbers. Then $n + (m + 1) = (n + m) + 1$.

3.2 The Peano axioms and recursion, revisited

ARITHMETIC_03_3170769680990208

Proposition 3.9. Let n, m be natural numbers. If $n + 1 = m + 1$ then $n = m$.

ARITHMETIC_03_1101538491629568

Proposition 3.10. Let n be a natural number. Then $n + 1 \neq 0$.

ARITHMETIC_03_647949900054528

Proposition 3.11 (Induction). Let A be a class. Assume $0 \in A$. Assume that for all $n \in \mathbb{N}$ if $n \in A$ then $n + 1 \in A$. Then A contains every natural number.

Proposition 3.12. Let a be an object and f be a map. Let φ be a map from $\mathbb{N}$ to $\mathrm{dom}(f)$. φ is recursively defined by a and f iff $\varphi(0) = a$ and $\varphi(n+1) = f(\varphi(n))$ for every $n \in \mathbb{N}$.

3.3 Computation laws

Associativity

ARITHMETIC_03_3235893452210176

Proposition 3.13. Let n, m, k be natural numbers. Then

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

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

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

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

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

Thus $k' + 1 \in \Phi$. Qed.

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

Commutativity

ARITHMETIC_03_4029553232052224

Proposition 3.14. Let n, m be natural numbers. Then

$$n + m = m + n.$$

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

(1) 0 is an element of Φ.
Proof. Define $\Psi = \{n' \in \mathbb{N} \mid n' + 0 = 0 + n'\}$.

(1a) 0 belongs to Ψ.

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

Proof. Let $n' \in \Psi$. Then $n' + 0 = 0 + n'$. Hence

$$(n' + 1) + 0$$

$$= n' + 1$$

$$= (n' + 0) + 1$$

$$= (0 + n') + 1$$

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

Qed.

Hence every natural number belongs to Ψ. Thus $n + 0 = 0 + n$. Therefore 0 is an element of Φ. Qed.

Let us show that (2) $n + 1 = 1 + n$.
Proof. Define $\Theta = \{n' \in \mathbb{N} \mid n' + 1 = 1 + n'\}$.

(2a) 0 is an element of Θ.

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

$$(n' + 1) + 1$$

$$= (1 + n') + 1$$

$$= 1 + (n' + 1).$$

Thus $n' + 1 \in \Theta$. Qed.

Thus every natural number belongs to Θ. Therefore $n + 1 = 1 + n$. Qed.

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

$$n + (m' + 1)$$

$$= (n + m') + 1$$

$$= (m' + n) + 1$$

$$= m' + (n + 1)$$

$$= m' + (1 + n)$$

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

Thus $m' + 1 \in \Phi$. Qed.

Thus every natural number is an element of Φ. Therefore $n + m = m + n$. □

Cancellation

ARITHMETIC_03_3137702874578944

Proposition 3.15. Let n, m, k be natural numbers. Then

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

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

(1) 0 is an element of Φ.

(2) For all $k' \in \Phi$ we have $k' + 1 \in \Phi$.
Proof. Let $k' \in \Phi$. Suppose $n+(k'+1) = m+(k'+1)$. Then $(n+k')+1 = (m+k')+1$. Hence $n + k' = m + k'$. Thus $n = m$. Qed.

Therefore every natural number is an element of Φ. Consequently if $n + k = m + k$ then $n = m$. □

ARITHMETIC_03_8445946379632640

Corollary 3.16. Let n, m, k be natural numbers. Then

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

Proof. Assume $k + n = k + m$. We have $k + n = n + k$ and $k + m = m + k$. Hence $n + k = m + k$. Thus $n = m$. □

Zero sums

ARITHMETIC_03_3520602170195968

Proposition 3.17. Let n, m be natural numbers. If $n + m = 0$ then $n = 0$ and $m = 0$.

Proof. Assume $n + m = 0$. Suppose $n \neq 0$ or $m \neq 0$. Then we can take a $k \in \mathbb{N}$ such that $n = k + 1$ or $m = k + 1$. Hence there exists a natural number l such that $n + m = l + (k + 1) = (l + k) + 1 \neq 0$. Contradiction. □

Chapter 4

Ordering

File: `arithmetic/sections/04_ordering.ftl.tex`

[readtex `foundations/sections/11_binary-relations.ftl.tex`]

[readtex `arithmetic/sections/03_addition.ftl.tex`]

4.1 Definitions and immediate consequences

ARITHMETIC_04_1926295512416256

Definition 4.1. Let n, m be natural numbers. $n < m$ iff there exists a nonzero natural number k such that $m = n + k$.

Let n is less than m stand for $n < m$. Let $n > m$ stand for $m < n$. Let n is greater than m stand for $n > m$. Let $n \not< m$ stand for n is not less than m. Let $n \not> m$ stand for n is not greater than m.

ARITHMETIC_04_3668680374222848

Definition 4.2. Let n be a natural number. $\mathbb{N}_{<n} = \{k \in \mathbb{N} \mid k < n\}$.

ARITHMETIC_04_3670333934534656

Definition 4.3. Let n be a natural number. $\mathbb{N}_{>n} = \{k \in \mathbb{N} \mid k > n\}$.

ARITHMETIC_04_7916616566177792

Definition 4.4. Let n be a natural number. n is positive iff $n > 0$.

ARITHMETIC_04_4593841531256832

Definition 4.5. Let n, m be natural numbers. $n \leq m$ iff there exists a natural number k such that $m = n + k$.

Let n is less than or equal to m stand for $n \leq m$. Let $n \geq m$ stand for $m \leq n$. Let n is greater than or equal to m stand for $n \geq m$. Let $n \nleq m$ stand for n is not less than or equal to m. Let $n \ngeq m$ stand for n is not greater than or equal to m.

ARITHMETIC_04_72501526790144

Definition 4.6. Let n be a natural number. $\mathbb{N}_{\leq n} = \{k \in \mathbb{N} \mid k \leq n\}$.

ARITHMETIC_04_1706933421604864

Definition 4.7. Let n be a natural number. $\mathbb{N}_{\geq n} = \{k \in \mathbb{N} \mid k \geq n\}$.

ARITHMETIC_04_5385415374667776

Proposition 4.8. Let n, m be natural numbers. $n \leq m$ iff $n < m$ or $n = m$.

Proof. Case $n \leq m$. Take a natural number k such that $m = n + k$. If $k = 0$ then $n = m$. If $k \neq 0$ then $n < m$. End.

Case $n < m$ or $n = m$. If $n < m$ then there is a positive natural number k such that $m = n + k$. If $n = m$ then $m = n + 0$. Thus if $n < m$ then there is a natural number k such that $m = n + k$. End. ☐

ARITHMETIC_04_6232154608500736

Definition 4.9. Let n be a natural number. A predecessor of n is a natural number that is less than n.

ARITHMETIC_04_8147686326796288

Definition 4.10. Let n be a natural number. A successor of n is a natural number that is greater than n.

ARITHMETIC_04_4826285599621120

Proposition 4.11. Let n be a natural number. Then n is positive iff n is nonzero.

Proof. Case n is positive. Take a positive natural number k such that $n = 0 + k = k$. Then we have $n \neq 0$. End.

Case n is nonzero. Take a natural number k such that $n = k+1$. Then $n = 0+(k+1)$. $k + 1$ is positive. Hence $0 < n$. End. □

4.2 Basic properties

ARITHMETIC_04_1037693395927040

Proposition 4.12. Let n be a natural number. Then

$$n \nless n.$$

Proof. Assume the contrary. Then we can take a positive natural number k such that $n = n + k$. Then we have $0 = k$. Contradiction. □

ARITHMETIC_04_8266284905005056

Proposition 4.13. Let n, m be natural numbers. Then

$$n < m \quad \text{implies} \quad n \neq m.$$

Proof. Assume $n < m$. Take a positive natural number k such that $m = n + k$. If $n = m$ then $k = 0$. Hence $n \neq m$. □

ARITHMETIC_04_4190604718243840

Proposition 4.14. Let n, m be natural numbers. Then

$$(n \leq m \text{ and } m \leq n) \quad \text{implies} \quad n = m.$$

Proof. Assume $n \leq m$ and $m \leq n$. Take natural numbers k, l such that $m = n + k$ and $n = m + l$. Then $m = (m + l) + k = m + (l + k)$. Hence $l + k = 0$. Thus $l = 0 = k$. Indeed if $l \neq 0$ or $k \neq 0$ then $l + k$ is the direct successor of some natural number. Therefore $m = n$. □

ARITHMETIC_04_6413905244979200

Proposition 4.15. Let n, m, k be natural numbers. Then

$$n < m < k \quad \text{implies} \quad n < k.$$

Proof. Assume $n < m < k$. Take a positive natural number a such that $m = n + a$. Take a positive natural number b such that $k = m + b$. Then $k = (n + a) + b = n + (a + b)$. $a + b$ is positive. Hence $n < k$. □

ARITHMETIC_04_5480385953660928

Proposition 4.16. Let n, m, k be natural numbers. Then

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

Proof. Assume $n \leq m \leq k$. Case $n = m = k$. Obvious. Case $n = m < k$. Obvious. Case $n < m = k$. Obvious. Case $n < m < k$. Obvious. □

ARITHMETIC_04_5098403656630272

Proposition 4.17. Let n, m, k be natural numbers. Then

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

Proof. Assume $n \leq m < k$. If $n = m$ then $n < k$. If $n < m$ then $n < k$. □

ARITHMETIC_04_4809599527944192

Proposition 4.18. Let n, m, k be natural numbers. Then

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

Proof. Assume $n < m \leq k$. If $m = k$ then $n < k$. If $m < k$ then $n < k$. □

ARITHMETIC_04_8584998051381248

Proposition 4.19. Let n, m be natural numbers. Then

$$n < m \quad \text{implies} \quad n + 1 \leq m.$$

Proof. Assume $n < m$. Take a positive natural number k such that $m = n + k$.

Case $k = 1$. Then $m = n + 1$. Hence $n + 1 \leq m$. End.

Case $k \neq 1$. Then we can take a natural number l such that $k = l + 1$. Then $m = n + (l + 1) = (n + l) + 1 = (n + 1) + l$. l is positive. Thus $n + 1 < m$. End. □

ARITHMETIC_04_8201937860165632

Proposition 4.20. Let n, m be natural numbers. Then $n < m$ or $n = m$ or $n > m$.

Proof. Define $\Phi = \{m' \in \mathbb{N} \mid n < m' \text{ or } n = m' \text{ or } n > m'\}$.

(1) Φ contains 0.

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

Case $n < m'$. Obvious.

Case $n = m'$. Obvious.

Case $n > m'$. Take a positive natural number k such that $n = m' + k$.

Case $k = 1$. Obvious.

Case$k \neq 1$. Take a natural number l such that $n = (m' + 1) + l$. Hence $n > m' + 1$. Indeed l is positive. End. Qed. Qed.

Thus every natural number is contained in Φ. Therefore $n < m$ or $n = m$ or $n > m$. □

ARITHMETIC_04_6991525988794368

Proposition 4.21. Let n, m be natural numbers. Then

$$n \not< m \quad \text{iff} \quad n \geq m.$$

Proof. Case $n \not< m$. Then $n = m$ or $n > m$. Hence $n \geq m$. End.

Case $n \geq m$. Assume $n < m$. Then $n \leq m$. Hence $n = m$. Contradiction. End. □

4.3 Ordering and successors

ARITHMETIC_04_7006203091615744

Proposition 4.22. Let n, m be natural numbers. Then

$$n < m \leq n + 1 \quad \text{implies} \quad m = n + 1.$$

Proof. Assume $n < m \leq n+1$. Take a positive natural number k such that $m = n+k$. Take a natural number l such that $n+1 = m+l$. Then $n+1 = m+l = (n+k)+l = n+(k+l)$. Hence $k+l = 1$.

We have $l = 0$.
Proof. Assume the contrary. Then $k, l > 0$.

Case $k, l = 1$. Then $k + l = 2 \neq 1$. Contradiction. End.

Case $k = 1 and l \neq 1$. Then $l > 1$. Hence $k + l > 1 + l > 1$. Contradiction. End.

Case $k \neq 1 and l = 1$. Then $k > 1$. Hence $k + l > k + 1 > 1$. Contradiction. End.

Case $k, l \neq 1$. Take natural numbers a, b such that $k = a + 1$ and $l = b + 1$. Indeed $k, l \neq 0$. Hence $k = a + 1$ and $l = b + 1$. Thus $k, l > 1$. Indeed a, b are positive. End. Qed.

Then we have $n + 1 = m + l = m + 0 = m$. □

ARITHMETIC_04_8792330561650688

Proposition 4.23. Let n, m be natural numbers. Then

$$n \leq m < n + 1 \quad \text{implies} \quad n = m.$$

Proof. Assume $n \leq m < n + 1$.

Case $n = m$. Obvious.

Case $n < m$. Then $n < m \leq n + 1$. Hence $n = m$. End. □

ARITHMETIC_04_1802826644717568

Corollary 4.24. Let n be a natural number. There is no natural number m such that $n < m < n + 1$.

Proof. Assume the contrary. Take a natural number m such that $n < m < n + 1$. Then $n < m \leq n + 1$ and $n \leq m < n + 1$. Hence $m = n + 1$ and $m = n$. Hence $n = n + 1$. Contradiction. □

ARITHMETIC_04_990407185924096

Proposition 4.25. Let n be a natural number. Then

$$n + 1 \geq 1.$$

Proof. Case $n = 0$. Obvious.

Case $n \neq 0$. Then $n > 0$. Hence $n + 1 > 0 + 1 = 1$. End. □

4.4 Ordering and addition

ARITHMETIC_04_7354062662008832

Proposition 4.26. Let n, m, k be natural numbers. Then

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

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

Case $n + k < m + k$. Take a positive natural number l such that $m + k = (n + k) + l$. $(n + k) + l = n + (k + l) = n + (l + k) = (n + l) + k$. Hence $m + k = (n + l) + k$. Thus $m = n + l$. Therefore $n < m$. End. □

ARITHMETIC_04_1901366129721344

Corollary 4.27. Let n, m, k be natural numbers. Then

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

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

ARITHMETIC_04_4203390999461888

Corollary 4.28. Let n, m, k be natural numbers. Then

$$n \leq m \quad \text{iff} \quad k + n \leq k + m.$$

ARITHMETIC_04_5512590832697344

Corollary 4.29. Let n, m, k be natural numbers. Then

$$n \leq m \quad \text{iff} \quad n + k \leq m + k.$$

4.5 The natural numbers are well-ordered

ARITHMETIC_04_4059354166722560

Definition 4.30.

$$< = \{(n, m) \mid n \text{ and } m \text{ are natural numbers such that } n < m\}.$$

ARITHMETIC_04_5933477660721152

Proposition 4.31. Let A be a nonempty subclass of $\mathbb{N}$. Let n, m be least elements of A regarding $<$. Then $n = m$.

Proof. Assume $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n \notin A$. If $m < n$ then $m \notin A$. Hence $n, m \notin A$. Contradiction. Therefore $n = m$. □

ARITHMETIC_04_272317502455808

Proposition 4.32. Let A be a nonempty subclass of $\mathbb{N}$. Then A has a least element regarding $<$.

Proof. Assume the contrary.

Let us show that for each $n \in A$ there exists a $m \in A$ such that $m < n$. Let $n \in A$. A has no least element regarding $<$. Assume that there exists no $m \in A$ such that $m < n$. Then $n \leq m$ for all $m \in A$. Hence n is a least element of A regarding $<$. Contradiction. End.

Define $\Phi = \{n \in \mathbb{N} \mid n \text{ is less than any element of } A\}$.

(1) Φ contains 0.
Proof. $0 \notin A$. Hence 0 is less than every element of A. Thus $0 \in \Phi$. Qed.

(2) For all $n \in \Phi$ we have $n + 1 \in \Phi$.
Proof. Let $n \in \Phi$. Then n is less than any element of A. Assume that Φ does not contain $n+1$. Then we can take an $m \in A$ such that $n+1 \not< m$. Then $n < m \leq n+1$. Hence $m = n + 1$. Thus $n + 1$ is a least element of A regarding $<$. Contradiction. Qed.

Then Φ contains every natural number. Therefore every natural number is less than any element of A. Consequently A is empty. Contradiction. □

ARITHMETIC_04_4280275783647232

Corollary 4.33. $<$ is a wellorder on every nonempty subclass of $\mathbb{N}$.

Proof. Let A be a nonempty subclass of $\mathbb{N}$. For any $n, m \in A$ we have $(n, m) \in <$ iff $n < m$.

(1) $<$ is irreflexive on A. Indeed for any $n \in A$ we have $n \not< n$.

(2) $<$ is transitive on A. Indeed for any $n, m, k \in A$ if $n < m$ and $m < k$ then $n < k$.

(3) $<$ is connected on A. Indeed for any distinct $n, m \in A$ we have $n < m$ or $m < n$.

Hence $<$ is a strict linear order on A. $<$ is wellfounded on A. Indeed every nonempty subclass of A has a least element regarding $<$. Thus $<$ is a wellorder on A. □

4.6 Induction revisited

ARITHMETIC_04_3609801697263616

Theorem 4.34. Let A be a class. Assume for all $n \in \mathbb{N}$ if A contains all predecessors of n then A contains n. Then A contains every natural number.

Proof. Assume the contrary. Take a natural number n that is not contained in A. Then n is contained in $\mathbb{N} \setminus A$. Hence we can take a least element m of $\mathbb{N} \setminus A$ regarding $<$. Then $\mathbb{N} \setminus A$ does not contain any predecessor of m. Therefore A contains all predecessors of m. Consequently A contains m. Contradiction. □

ARITHMETIC_04_4976599269113856

Theorem 4.35. Let A be a class. Let k be a natural number such that $k \in A$. Assume that for all $n \in \mathbb{N}_{\geq k}$ if $n \in A$ then $n + 1 \in A$. Then for all $n \in \mathbb{N}_{\geq k}$ we have $n \in A$.

Proof. Define $\Phi = \{n \in \mathbb{N} \mid \text{if } n \geq k \text{ then } n \in A\}$.

(1) Φ contains 0. Indeed if $0 \geq k$ then $0 = k \in A$.

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

Let us show that if $n + 1 \geq k$ then $n + 1 \in A$. Assume $n + 1 \geq k$.

Case $n < k$. Then $n + 1 = k$. Hence $n + 1 \in A$. End.

Case $n \geq k$. Then $n \in A$. Hence $n + 1 \in A$. End. End.

Therefore $n + 1 \in \Phi$. Qed.

Thus Φ contains every natural number. Consequently for all $n \in \mathbb{N}_{\geq k}$ we have $n \in A$. ∎

Chapter 5

Subtraction

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

[readtex `arithmetic/sections/04_ordering.ftl.tex`]

ARITHMETIC_05_8878757276286976

Definition 5.1. Let n, m be natural numbers such that $n \geq m$. $n - m$ is the natural number k such that $n = m + k$.

Let the difference of n and m stand for $n - m$.

ARITHMETIC_05_874271710642176

Proposition 5.2. Let n, m be natural numbers such that $n \geq m$. Then

$$n - m = 0 \quad \text{iff} \quad n = m.$$

Proof. Case $n - m = 0$. Then $n = (n - m) + m = 0 + m = m$. End.

Case $n = m$. We have $(n - m) + m = n = m = 0 + m$. Hence $n - m = 0$. End. ☐

ARITHMETIC_05_8457713057005568

Corollary 5.3. Let n be a natural number. Then

$$n - n = 0.$$

ARITHMETIC_05_8518521570983936

Proposition 5.4. Let n be a natural number. Then

$$n - 0 = n.$$

Proof. We have $n = (n - 0) + 0 = n - 0$. □

ARITHMETIC_05_4222566117933056

Proposition 5.5. Let n, m be natural numbers such that $n \geq m$. Then

$$n - m \leq n.$$

Proof. We have $(n - m) + m = n$. Hence $n - m \leq n$. □

ARITHMETIC_05_1269537257291776

Proposition 5.6. Let n, m be natural numbers such that $n \geq m$. Then

$$0 \neq m < n \quad \text{implies} \quad n - m < n.$$

Proof. Assume $0 \neq m < n$. Suppose $n - m \geq n$. We have $(n - m) + m = n$. Then $n + m = (n - m) + m = n = n + 0$. Hence $m = 0$. Contradiction. □

ARITHMETIC_05_4767595811045376

Proposition 5.7. Let n, m, k be natural numbers such that $n \geq m$. Then

$$(n - m) + k = (n + k) - m.$$

Proof. We have

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

$$= ((n + k) - m) + m.$$

Hence $(n - m) + k = (n + k) - m$. □

ARITHMETIC_05_7578468875239424

Corollary 5.8. Let n, m, k be natural numbers such that $n \geq m$. Then

$$k + (n - m) = (k + n) - m.$$

ARITHMETIC_05_7595909347016704

Proposition 5.9. Let n, m, k be natural numbers such that $n \geq m + k$. Then

$$(n - m) - k = n - (m + k).$$

Proof. We have

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

Hence $(n - m) - k = n - (m + k)$. □

Chapter 6

Multiplication

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

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

6.1 Definition of multiplication

ARITHMETIC_06_7897906468093952

Lemma 6.1. 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 theorem 2.2). 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 6.2. 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 6.3. 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 6.4. Let n, m be natural numbers. Then $(n, m) \in \mathrm{dom}(\mathrm{mul})$.

ARITHMETIC_06_8420678923452416

Lemma 6.5. Let n, m be natural numbers. Then $n \cdot m$ is a natural number.

ARITHMETIC_06_8941041092657152

Lemma 6.6. Let n be a natural number. Then $n \cdot 0 = 0$.

ARITHMETIC_06_2211275408932864

Lemma 6.7. Let n, m be natural numbers. Then $n \cdot (m+1) = (n \cdot m) + n$.

6.2 Computation laws

Distributivity

ARITHMETIC_06_9001524774567936

Proposition 6.8. 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 6.9. 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

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

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

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 6.10. 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 6.11. 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 6.12. 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 6.13. 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

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

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

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

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 6.14. 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

$$0$$
$$= n \cdot m$$

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

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

Cancellation

ARITHMETIC_06_31055184658432

Proposition 6.15. 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 6.16. 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 6.15). □

6.3 Ordering and multiplication

ARITHMETIC_06_8817333933965312

Proposition 6.17. 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 6.18. 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 6.19. 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 6.20. 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 6.21. 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 6.22. 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 6.23. 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 6.24. 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 $((l + 1) \cdot m) + m \geq 1 + m$. □

6.4 Multiplication and subtraction

ARITHMETIC_06_5458841930039296

Proposition 6.25. 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 6.26. Let n, m, k be natural numbers such that $n \geq m$. Then

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

Chapter 7

Divisibility

File: `arithmetic/sections/07_divisibility.ftl.tex`

[readtex `arithmetic/sections/06_multiplication.ftl.tex`]

ARITHMETIC_07_4239998993825792

Definition 7.1. Let n, m be natural numbers. n divides m iff there exists a natural number k such that $n \cdot k = m$.

Let m is divisible by n stand for n divides m. Let $n \mid m$ stand for n divides m. Let $n \nmid m$ stand for n does not divide m.

ARITHMETIC_07_1478855118290944

Lemma 7.2. Let n, m be natural numbers. n divides m iff there exists a natural number k such that $k \cdot n = m$.

ARITHMETIC_07_1311437490225152

Definition 7.3. Let n be a natural number. A factor of n is a natural number that divides n.

Let a divisor of n stand for a factor of n.

ARITHMETIC_07_2242720387039232

Proposition 7.4. Let n be a natural number. Then

$$n \mid 0.$$

Proof. We have $n \cdot 0 = 0$. Hence $n \mid 0$. ☐

ARITHMETIC_07_8611150130315264

Proposition 7.5. Let n be a natural number. Then

$$0 \mid n \quad \text{implies} \quad n = 0.$$

Proof. Assume $0 \mid n$. Consider a natural number k such that $0 \cdot k = n$. Then $n = 0$. ☐

ARITHMETIC_07_1259086070939648

Proposition 7.6. Let n be a natural number. Then

$$1 \mid n.$$

Proof. We have $1 \cdot n = n$. Hence $1 \mid n$. ☐

ARITHMETIC_07_3944887330275328

Proposition 7.7. Let n be a natural number. Then

$$n \mid n.$$

Proof. We have $n \cdot 1 = n$. Hence $n \mid n$. ☐

ARITHMETIC_07_6917446193643520

Proposition 7.8. Let n be a natural number. Then

$$n \mid 1 \quad \text{implies} \quad n = 1.$$

Proof. Assume $n \mid 1$. Take a natural number k such that $n \cdot k = 1$. Suppose $n \neq 1$. Then $n < 1$ or $n > 1$.

Case $n < 1$. Then $n = 0$. Hence $0 = 0 \cdot k = n \cdot k = 1$. Contradiction. End.

Case $n > 1$. We have $k \neq 0$. Indeed if $k = 0$ then $1 = n \cdot k = n \cdot 0 = 0$. Hence $k \geq 1$. Take a positive natural number l such that $n = 1+l$. Then $1 < 1+l = n = n \cdot 1 \leq n \cdot k$. Hence $1 < n$. Contradiction. End. □

ARITHMETIC_07_7463519983239168

Proposition 7.9. Let n, m, k be natural numbers. Then

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

Proof. Assume $n \mid m$. Take $l \in \mathbb{N}$ such that $n \cdot l = m$. Then $n \cdot (l \cdot k) = (n \cdot l) \cdot k = m \cdot k$. Hence $n \mid m \cdot k$. □

ARITHMETIC_07_1588185794609152

Corollary 7.10. Let n, m, k be natural numbers. Then

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

ARITHMETIC_07_7863858316181504

Proposition 7.11. Let n, m, k be natural numbers. Then

$$n \mid m \mid k \quad \text{implies} \quad n \mid k.$$

Proof. Assume $n \mid m$ and $m \mid k$. Take natural numbers l, l' such that $n \cdot l = m$ and $m \cdot l' = k$. Then $n \cdot (l \cdot l') = (n \cdot l) \cdot l' = m \cdot l' = k$. Hence $n \mid k$. □

ARITHMETIC_07_4933275640397824

Proposition 7.12. Let n, m be natural numbers such that $n \neq 0$. Then

$$(n \mid m \text{ and } m \mid n) \quad \text{implies} \quad n = m.$$

Proof. Assume $n \mid m$ and $m \mid n$. Take natural numbers k, k' such that $n \cdot k = m$ and $m \cdot k' = n$. Then $n = m \cdot k' = (n \cdot k) \cdot k' = n \cdot (k \cdot k')$. Hence $k \cdot k' = 1$. Thus $k = 1 = k'$. Therefore $n = m$. □

ARITHMETIC_07_1283495225720832

Proposition 7.13. Let n, m, k be natural numbers. Then

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

Proof. Assume $n \mid m$. Take a natural number l such that $n \cdot l = m$. Then $(k \cdot n) \cdot l = k \cdot (n \cdot l) = k \cdot m$. Hence $k \cdot n \mid k \cdot m$. □

ARITHMETIC_07_6469492028735488

Proposition 7.14. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

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

Proof. Assume $k \cdot n \mid k \cdot m$. Take a natural number l such that $(k \cdot n) \cdot l = k \cdot m$. Then $k \cdot (n \cdot l) = k \cdot m$. Hence $n \cdot l = m$. Thus $n \mid m$. □

ARITHMETIC_07_4700711333920768

Proposition 7.15. Let n, m, k be natural numbers. Then

$$(k \mid n \text{ and } k \mid m) \quad \text{implies} \quad (k \mid (n' \cdot n) + (m' \cdot m) \text{ for all natural numbers } n', m').$$

Proof. Assume $k \mid n$ and $k \mid m$. Let n', m' be natural numbers. Take natural numbers l, l' such that $k \cdot l = n$ and $k \cdot l' = m$. Then

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

□

ARITHMETIC_07_1556786209357824

Corollary 7.16. Let n, m, k be natural numbers. Then

$$(k \mid n \text{ and } k \mid m) \quad \text{implies} \quad k \mid n + m.$$

Proof. Assume $k \mid n$ and $k \mid m$. Take $n' = 1$ and $m' = 1$. Then $k \mid (n' \cdot n) + (m' \cdot m)$.

$(n' \cdot n) + (m' \cdot m) = n + m$. Hence $k \mid n + m$. □

ARITHMETIC_07_1076947887063040

Proposition 7.17. Let n, m, k be natural numbers. Then

$$(k \mid n \text{ and } k \mid n + m) \quad \text{implies} \quad k \mid m.$$

Proof. Assume $k \mid n$ and $k \mid n + m$.

Case $k = 0$. Obvious.

Case $k \neq 0$. Take a natural number l such that $n = k \cdot l$. Take a natural number l' such that $n + m = k \cdot l'$. Then $(k \cdot l) + m = k \cdot l'$. We have $l' \geq l$. Indeed if $l' < l$ then $n + m = k \cdot l' < k \cdot l = n$. Hence we can take a natural number l'' such that $l' = l + l''$. Then $(k \cdot l) + m = k \cdot l' = k \cdot (l + l'') = (k \cdot l) + (k \cdot l'')$. Indeed $k \cdot (l + l'') = (k \cdot l) + (k \cdot l'')$ (by proposition 6.8). Thus $m = (k \cdot l'')$. Therefore $k \mid m$. End. □

ARITHMETIC_07_2187144577679360

Proposition 7.18. Let n, m be natural numbers such that $n, m \neq 0$. Then

$$m \mid n \quad \text{implies} \quad m \leq n.$$

Proof. Assume $m \mid n$. Take a natural number k such that $m \cdot k = n$. If $k = 0$ then $n = m \cdot k = m \cdot 0 = 0$. Thus $k \geq 1$. Assume $m > n$. Then $n = m \cdot k \geq m \cdot 1 = m > n$. Hence $n > n$. Contradiction. □

Chapter 8

Euclidean division

File: `arithmetic/sections/08_euclidean-division.ftl.tex`

[readtex `arithmetic/sections/06_multiplication.ftl.tex`]

8.1 Quotients and remainders

ARITHMETIC_08_7743986617810944

Theorem 8.1. Let n, m be natural numbers such that $m \neq 0$. Then there exist natural numbers q, r such that

$$n = (m \cdot q) + r$$

and $r < m$.

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid \text{there exist natural numbers } q, r \text{ such that } r < m \text{ and } n' = (m \cdot q) + r\}$.

(1) Φ contains 0. Proof. Take $q = 0$ and $r = 0$. Then $r < m$ and $0 = (m \cdot q) + r$. Hence $0 \in \Phi$. Qed.

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

Let us show that there exist natural numbers q, r such that $r < m$ and $n' + 1 = (m \cdot q) + r$. Take natural numbers q', r' such that $r' < m$ and $n' = (m \cdot q') + r'$. We have $r' + 1 < m$ or $r' + 1 = m$.

Case $r' + 1 < m$. Take $q = q' + 0$ and $r = r' + 1$. Then $r < m$ and $n' + 1 = ((q' \cdot m) + r') + 1 = (q' \cdot m) + (r' + 1) = (q \cdot m) + r$. End.

Case $r'+1 = m$. Take $q = q'+1$ and $r = 0$. Then $r < m$ and $n'+1 = ((q' \cdot m)+r')+1 = (q' \cdot m) + (r' + 1) = (q' \cdot m) + m = (q' \cdot m) + (1 \cdot m) = (q' + 1) \cdot m = (q \cdot m) + r$. End. End.

Hence $n' + 1 \in \Phi$. Qed.

Then Φ contains every natural number. Thus there exist natural numbers q, r such that $n = (m \cdot q) + r$ and $r < m$. □

ARITHMETIC_08_7801804481888256

Proposition 8.2. Let n, m be natural numbers such that $m \neq 0$. Let q, r be natural numbers such that $(m \cdot q) + r = n$ and $r < m$. Let q', r' be natural numbers such that $(m \cdot q') + r' = n$ and $r' < m$. Then $q = q'$ and $r = r'$.

Proof. We have $(m \cdot q) + r = (m \cdot q') + r'$.

Case $q \geq q'$ and $r \geq r'$. (1) $((m \cdot q) + r) - r' = (m \cdot q) + (r - r')$ (by corollary 5.8). (2) $((m \cdot q') + r') - r' = (m \cdot q') + (r' - r') = m \cdot q'$. Hence $(m \cdot q) + (r - r') = m \cdot q'$. Thus $((m \cdot q) - (m \cdot q')) + (r - r') = 0$. Consequently $(m \cdot q) - (m \cdot q') = 0$ and $r - r' = 0$. If $(m \cdot q) - (m \cdot q') = 0$ then $q - q' = 0$. Therefore $q - q' = 0$ and $r - r' = 0$. Thus we have $q = q'$ and $r = r'$. End.

Case $q \geq q'$ and $r < r'$. Take $q'' = q - q'$ and $r'' = r' - r$. Then $(m \cdot (q' + q'')) + r = (m \cdot q') + (r + r'')$. We have $(m \cdot q') + (r + r'') = (m \cdot q') + (r'' + r) = ((m \cdot q') + r'') + r$. Hence $(m \cdot (q' + q'')) + r = ((m \cdot q') + r'') + r$. Thus $m \cdot (q' + q'') = (m \cdot q') + r''$ (by proposition 3.15). We have $m \cdot (q' + q'') = (m \cdot q') + (m \cdot q'')$. Hence $(m \cdot q') + (m \cdot q'') = (m \cdot q') + r''$. [prover vampire] Thus $m \cdot q'' = r''$ (by corollary 3.16). Then we have $m \cdot q'' < m \cdot 1$. Indeed $m \cdot q'' = r'' \leq r' < m = m \cdot 1$. Therefore $q'' < 1$ (by corollary 6.18). Consequently $q - q' = q'' = 0$. Hence $q = q'$. Thus $(m \cdot q) + r = (m \cdot q) + r'$. Therefore $r = r'$. End.

Case $q < q'$ and $r \geq r'$. Take $q'' = q' - q$ and $r'' = r - r'$. Then $(m \cdot q) + (r' + r'') = (m \cdot (q + q'')) + r'$. We have $(m \cdot q) + (r' + r'') = (m \cdot q) + (r'' + r') = ((m \cdot q) + r'') + r'$. Hence $((m \cdot q) + r'') + r' = (m \cdot (q + q'')) + r'$. Thus $(m \cdot q) + r'' = m \cdot (q + q'')$ (by proposition 3.15). We have $m \cdot (q + q'') = (m \cdot q) + (m \cdot q'')$. Hence $(m \cdot q) + r'' = (m \cdot q) + (m \cdot q'')$. [prover vampire] Thus $r'' = m \cdot q''$. Then we have $m \cdot q'' < m \cdot 1$. Indeed $m \cdot q'' = r'' \leq r < m = m \cdot 1$. Therefore $q'' < 1$ (by corollary 6.18). Consequently $q' - q = q'' = 0$. Hence $q' = q$. Thus $(m \cdot q) + r = (m \cdot q) + r'$. Therefore $r = r'$. End.

Case $q < q'$ and $r < r'$. (1) $((m \cdot q') + r') - r = (m \cdot q') + (r' - r)$ (by corollary 5.8). (2) $((m \cdot q) + r) - r = (m \cdot q) + (r - r) = m \cdot q$. Hence $(m \cdot q') + (r' - r) = m \cdot q$. Thus $((m \cdot q') - (m \cdot q)) + (r' - r) = 0$. Consequently $(m \cdot q') - (m \cdot q) = 0$ and $r' - r = 0$. If $(m \cdot q') - (m \cdot q) = 0$ then $q' - q = 0$. Therefore $q' - q = 0$ and $r' - r = 0$. Thus we have $q' = q$ and $r' = r$. End. □

ARITHMETIC_08_8621463798022144

Definition 8.3. Let n, m be natural numbers such that $m \neq 0$. $n \operatorname{div} m$ is the natural number q such that $n = (m \cdot q) + r$ for some natural number r that is less than m.

Let the quotient of n over m stand for $n \operatorname{div} m$.

ARITHMETIC_08_3560980160184320

Definition 8.4. Let n, m be natural numbers such that $m \neq 0$. $n \bmod m$ is the natural number r such that $r < m$ and there exists a natural number q such that $n = (m \cdot q) + r$.

Let the remainder of n over m stand for $n \bmod m$.

8.2 Modular arithmetic

ARITHMETIC_08_5448561831444480

Definition 8.5. Let n, m, k be natural numbers such that $k \neq 0$. $n \equiv m \pmod{k}$ iff $n \bmod k = m \bmod k$.

Let n and m are congruent modulo k stand for $n \equiv m \pmod{k}$.

ARITHMETIC_08_3818318544764928

Proposition 8.6. Let n, k be natural numbers such that $k \neq 0$. Then

$$n \equiv n \pmod{k}.$$

Proof. We have $n \bmod k = n \bmod k$. Hence $n \equiv n \pmod{k}$. □

ARITHMETIC_08_2337210737098752

Proposition 8.7. Let n, m, k be natural numbers such that $k \neq 0$. Then

$$n \equiv m \pmod{k} \quad \text{implies} \quad m \equiv n \pmod{k}.$$

Proof. Assume $n \equiv m \pmod{k}$. Then $n \bmod k = m \bmod k$. Hence $m \bmod k = n \bmod k$. Thus $m \equiv n \pmod{k}$. □

ARITHMETIC_08_7464329746055168

Proposition 8.8. Let n, m, l, k be natural numbers such that $k \neq 0$. Then

$$(n \equiv m \pmod{k} \text{ and } m \equiv l \pmod{k}) \quad \text{implies} \quad n \equiv l \pmod{k}.$$

Proof. Assume $n \equiv m \pmod{k}$ and $m \equiv l \pmod{k}$. Then $n \bmod k = m \bmod k$ and $m \bmod k = l \bmod k$. Hence $n \bmod k = l \bmod k$. Thus $n \equiv l \pmod{k}$. □

ARITHMETIC_08_2034122983735296

Proposition 8.9. Let n, m, k be natural numbers such that $k \neq 0$. Assume $n \geq m$. Then $n \equiv m \pmod{k}$ iff $n = (k \cdot x) + m$ for some natural number x.

Proof. Case $n \equiv m \pmod{k}$. Then $n \bmod k = m \bmod k$. Take a natural number r such that $r < k$ and $n \bmod k = r = m \bmod k$. Take a nonzero natural number l such that $k = r + l$. Consider natural numbers q, q' such that $n = (q \cdot k) + r$ and $m = (q' \cdot k) + r$.

Then $q \geq q'$.
Proof. Assume the contrary. Then $q < q'$. Hence $q \cdot k < q' \cdot k$. Thus $(q \cdot k) + r < (q' \cdot k) + r$ (by proposition 4.26). Indeed $q \cdot k$ and $q' \cdot k$ are natural numbers. Therefore $n < m$. Contradiction. Qed.

Take a natural number x such that $q = q' + x$.

Let us show that $n = (k \cdot x) + m$. We have

$$(k \cdot x) + m$$

$$\begin{aligned}
&= (k \cdot x) + ((q' \cdot k) + r) \\
&= ((k \cdot x) + (q' \cdot k)) + r \\
&= ((k \cdot x) + (k \cdot q')) + r \\
&= (k \cdot (q' + x)) + r
\end{aligned}$$

$$= (k \cdot q) + r$$

$$= n.$$

End. End.

Case $n = (k \cdot x) + m$ for some natural number x. Consider a natural number x such that $n = (k \cdot x) + m$. Take natural numbers r, r' such that $n \bmod k = r$ and $m \bmod k = r'$. Then $r, r' < k$. Take natural numbers q, q' such that $n = (k \cdot q) + r$ and $m = (k \cdot q') + r'$. Then

$$(k \cdot q) + r$$

$$= n$$

$$= (k \cdot x) + m$$

$$= (k \cdot x) + ((k \cdot q') + r')$$

$$= ((k \cdot x) + (k \cdot q')) + r'$$

$$= (k \cdot (x + q')) + r'.$$

Hence $r = r'$. Thus $n \bmod k = m \bmod k$. Therefore $n \equiv m \pmod{k}$. End. □

ARITHMETIC_08_2988318228742144

Proposition 8.10. Let n, m, k, k' be natural numbers such that $k, k' \neq 0$. Then

$$n \equiv m \pmod{k \cdot k'} \quad \text{implies} \quad n \equiv m \pmod{k}.$$

Proof. Assume $n \equiv m \pmod{k \cdot k'}$.

Case $n \geq m$. We can take a natural number x such that $n = ((k \cdot k') \cdot x) + m$. Then $n = (k \cdot (k' \cdot x)) + m$. Hence $n \equiv m \pmod{k}$. End.

Case $m \geq n$. We have $m \equiv n \pmod{k \cdot k'}$. Hence we can take a natural number x such that $m = ((k \cdot k') \cdot x) + n$. Then $m = (k \cdot (k' \cdot x)) + n$. Thus $m \equiv n \pmod{k}$. Therefore $n \equiv m \pmod{k}$. End. □

ARITHMETIC_08_5895145169879040

Corollary 8.11. Let n, m, k, k' be natural numbers such that $k, k' \neq 0$. Then

$$n \equiv m \pmod{k \cdot k'} \quad \text{implies} \quad n \equiv m \pmod{k'}.$$

Proof. Assume $n \equiv m \pmod{k \cdot k'}$. Then $n \equiv m \pmod{k' \cdot k}$. Hence $n \equiv m \pmod{k'}$. □

ARITHMETIC_08_5984712287846400

Proposition 8.12. Let n, k be natural numbers such that $k \neq 0$. Then

$$n + k \equiv n \pmod{k}.$$

Proof. Take $r = n \bmod k$ and $r' = (n + k) \bmod k$. Consider a $q \in \mathbb{N}$ such that $n = (k \cdot q) + r$ and $r < k$. Consider a $q' \in \mathbb{N}$ such that $n + k = (k \cdot q') + r'$ and $r' < k$. Then $(k \cdot q') + r' = n + k = ((k \cdot q) + r) + k = (k + (k \cdot q)) + r = (k \cdot (q + 1)) + r$. Hence $r = r'$. Consequently $n \bmod k = (n + k) \bmod k$. Thus $n + k \equiv n \pmod{k}$. ☐

Chapter 9

Exponentiation

File: `arithmetic/sections/13_exponentiation.ftl.tex`

[readtex `arithmetic/sections/06_multiplication.ftl.tex`]

9.1 Definition of exponentiation

ARITHMETIC_13_2103235571613696

Lemma 9.1. There exists a $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\varphi(n, 0) = 1$ and $\varphi(n, m + 1) = \varphi(n, m) \cdot n$ for any $m \in \mathbb{N}$.

Proof. Take $A = [\mathbb{N} \to \mathbb{N}]$. Define $a(n) = 1$ for $n \in \mathbb{N}$. Then A is a set and $a \in A$.

[skipfail on] Define $f(g) = \lambda n \in \mathbb{N}.g(n) \cdot n$ 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 theorem 2.2). 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 $\varphi(n, 0) = 1$.
Proof. Let $n \in \mathbb{N}$. Then $\varphi(n, 0) = \psi(0)(n) = a(0) = 1$. Qed.

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

Hence for all $n \in \mathbb{N}$ we have $\varphi(n,0) = 1$ and $\varphi(n,m+1) = \varphi(n,m) \cdot n$ for any $m \in \mathbb{N}$. □

ARITHMETIC_13_2359278746730496

Lemma 9.2. Let $\varphi, \varphi' : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi(n,0) = 1$ and $\varphi(n,m+1) = \varphi(n,m) \cdot n$ for any $m \in \mathbb{N}$. Assume that for all $n \in \mathbb{N}$ we have $\varphi'(n,0) = 1$ and $\varphi'(n,m+1) = \varphi'(n,m) \cdot n$ 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 $\varphi(n,0) = 1 = \varphi'(n,0)$ 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 $n \in \mathbb{N}$. $\varphi(n,m), \varphi'(n,m)$ are natural numbers for all $n \in \mathbb{N}$. Hence $\varphi(n,m+1) = \varphi(n,m) \cdot n = \varphi'(n,m) \cdot n = \varphi'(n,m+1)$ for all $n \in \mathbb{N}$. Thus $\varphi(n,m+1) = \varphi'(n,m+1)$ 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_13_3663815629602816

Definition 9.3. exp is the map from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ such that for all $n \in \mathbb{N}$ we have $\exp(n,0) = 1$ and $\exp(n,m+1) = \exp(n,m) \cdot n$ for any $m \in \mathbb{N}$.

Let n^m stand for $\exp(n,m)$.

ARITHMETIC_13_5845266294898688

Lemma 9.4. Let n, m be natural numbers. Then $(n,m) \in \operatorname{dom}(\exp)$.

ARITHMETIC_13_4747809204994048

Lemma 9.5. Let n, m be natural numbers. Then n^m is a natural number.

ARITHMETIC_13_5368818025103360

Lemma 9.6. Let n be a natural number. Then $n^0 = 1$.

ARITHMETIC_13_4140498660884480

Lemma 9.7. Let n, m be natural numbers. Then $n^{m+1} = n^m \cdot n$.

9.2 Computation laws

Exponentiation with 0, 1 and 2

ARITHMETIC_13_4673644676513792

Proposition 9.8. Let n be a natural number. Assume $n \neq 0$. Then

$$0^n = 0.$$

Proof. Take a natural number m such that $n = m+1$. Then $0^n = 0^{m+1} = 0^m \cdot 0 = 0$. □

ARITHMETIC_13_7376849881530368

Proposition 9.9. Let n be a natural number. Then

$$1^n = 1.$$

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid 1^{n'} = 1\}$.

(1) Φ contains 0.

(2) For all $n' \in \Phi$ we have $n' + 1 \in \Phi$.
Proof. Let $n' \in \Phi$. Then $1^{n'+1} = 1^{n'} \cdot 1 = 1 \cdot 1 = 1$. Qed.

Hence every natural number is contained in Φ. Thus $1^n = 1$. □

ARITHMETIC_13_4975279749464064

Proposition 9.10. Let n be a natural number. Then

$$n^1 = n.$$

Proof. We have $n^1 = n^{0+1} = n^0 \cdot n = 1 \cdot n = n$. □

ARITHMETIC_13_8513812055457792

Proposition 9.11. Let n be a natural number. Then

$$n^2 = n \cdot n.$$

Proof. We have $n^2 = n^{1+1} = n^1 \cdot n = n \cdot n$. □

Sums as exponents

ARITHMETIC_13_8152207530655744

Proposition 9.12. Let n, m, k be natural numbers. Then

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

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

(1) Φ contains 0.
Indeed $k^{n+0} = k^n = k^n \cdot 1 = k^n \cdot k^0$.

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

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

Qed.

Hence every natural number is contained in Φ. Thus $k^{n+m} = k^n \cdot k^m$. □

Products as exponents

ARITHMETIC_13_7827956571308032

Proposition 9.13. Let n, m, k be natural numbers. Then

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

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

(1) Φ contains 0. Indeed $(n^m)^0 = 1 = n^0 = n^{m \cdot 0}$.

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

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

Qed.

Therefore every natural number is contained in Φ. Consequently $n^{m \cdot k} = (n^m)^k$. □

Products as base

ARITHMETIC_13_2563032276271104

Proposition 9.14. Let n, m, k be natural numbers. Then

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

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

(1) Φ contains 0. Indeed $((n \cdot m)^0) = 1 = 1 \cdot 1 = n^0 \cdot m^0$.

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

Let us show that $(n^{k'} \cdot m^{k'}) \cdot (n \cdot m) = (n^{k'} \cdot n) \cdot (m^{k'} \cdot m)$.

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

$$= (n^{k'} \cdot (m^{k'} \cdot n)) \cdot m$$
$$= (n^{k'} \cdot (n \cdot m^{k'})) \cdot m$$
$$= ((n^{k'} \cdot n) \cdot m^{k'}) \cdot m$$
$$= (n^{k'} \cdot n) \cdot (m^{k'} \cdot m).$$

Qed.

Hence

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

Qed.

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

Zeroes of exponentiation

ARITHMETIC_13_3860221447372800

Proposition 9.15. Let n, m be natural numbers. Then

$$n^m = 0 \quad \text{iff} \quad (n = 0 \text{ and } m \neq 0).$$

Proof. Case $n^m = 0$. Define $\Phi = \{m' \in \mathbb{N} \mid \text{if } n^{m'} = 0 \text{ then } n = 0 \text{ and } m' \neq 0\}$.

(1) Φ contains 0. Indeed if $n^0 = 0$ then we have a contradiction.

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

Let us show that if $n^{m'+1} = 0$ then $n = 0$ and $m' + 1 \neq 0$. Assume $n^{m'+1} = 0$. Then $0 = n^{m'+1} = n^{m'} \cdot n$. Hence $n^{m'} = 0$ or $n = 0$. We have $m' + 1 \neq 0$ and if $n^{m'} = 0$ then $n = 0$. Hence $n = 0$ and $m' + 1 \neq 0$. End. Qed.

Thus every natural number is contained in Φ. Consequently $m \in \Phi$. Therefore $n = 0$ and $m \neq 0$. End.

Case $n = 0$ and $m \neq 0$. Take a natural number k such that $m = k + 1$. Then $n^m = n^{k+1} = n^k \cdot n = 0^k \cdot 0 = 0$. End. □

9.3 Ordering and exponentiation

ARITHMETIC_13_3373702288769024

Proposition 9.16. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

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

Proof. Case $n < m$. Define $\Phi = \{k' \in \mathbb{N} \mid \text{if } k' > 1 \text{ then } n^{k'} < m^{k'}\}$.

(1) Φ contains 0.

(2) Φ contains 1.

(3) Φ contains 2.
Proof. Case $n = 0$ or $m = 0$. Obvious.

Case $n, m \neq 0$. Then $n \cdot n < n \cdot m < m \cdot m$. Hence $n^2 = n \cdot n < n \cdot m < m \cdot m = m^2$. End. Qed.

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

Let us show that if $k' + 1 > 1$ then $n^{k'+1} < m^{k'+1}$. Assume $k' + 1 > 1$. Then $n^{k'} < m^{k'}$. Indeed $k' \neq 0$ and $if k' = 1$ then $n^{k'} < m^{k'}$.

Case $k' \leq 1$. Then $k' = 0$ or $k' = 1$. Hence $k' + 1 = 1$ or $k' + 1 = 2$. Thus $k' + 1 \in \Phi$. Therefore $n^{k'+1} < m^{k'+1}$. End.

Case $k' > 1$. Case $n = 0$. Then $m \neq 0$. Hence $n^{k'+1} = 0 < m^{k'} \cdot m = m^{k'+1}$. Thus $n^{k'+1} < m^{k'+1}$. End.

Case $n \neq 0$. Then $n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m$. Indeed $n^{k'} < m^{k'} \neq 0$. Take $A = n^{k'+1}$ and $B = m^{k'+1}$. Then $A = n^{k'+1} = n^{k'} \cdot n < m^{k'} \cdot n < m^{k'} \cdot m = m^{k'+1} = B$. Thus $n^{k'+1} = A < B = m^{k'+1}$. End. End.

Hence $n^{k'+1} < m^{k'+1}$. Indeed $k' \leq 1$ or $k' > 1$. End.

Thus $k' + 1 \in \Phi$. Qed.

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

Case $n^k < m^k$. Define $\Psi = \{k' \in \mathbb{N} \mid \text{if } n \geq m \text{ then } n^{k'} \geq m^{k'}\}$.

(1) Ψ contains 0.

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

Let us show that if $n \geq m$ then $n^{k'+1} \geq m^{k'+1}$. Assume $n \geq m$. Then $n^{k'} \geq m^{k'}$. Hence $n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m$. Take $A = n^{k'+1}$ and $B = m^{k'+1}$. Thus $A = n^{k'+1} = n^{k'} \cdot n \geq m^{k'} \cdot n \geq m^{k'} \cdot m = m^{k'+1} = B$. Therefore $n^{k'+1} = A \geq B = m^{k'+1}$. End.

Hence $k' + 1 \in \Psi$. Qed.

Thus every natural number is contained in Ψ. Therefore if $n \geq m$ then $n^k \geq m^k$. [prover vampire] Consequently $n < m$. End. ☐

ARITHMETIC_13_2797602550579200

Corollary 9.17. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

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

Proof. Assume $n^k = m^k$. Suppose $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $n^k < m^k$. If $m < n$ then $m^k < n^k$. Thus $n^k \neq m^k$. Contradiction. ☐

ARITHMETIC_13_6875081963732992

Corollary 9.18. Let n, m, k be natural numbers. Assume $k \neq 0$. Then

$$n^k \leq m^k \quad \text{iff} \quad n \leq m.$$

Proof. If $n^k < m^k$ then $n < m$. If $n^k = m^k$ then $n = m$.

If $n < m$ then $n^k < m^k$. If $n = m$ then $n^k = m^k$. ☐

ARITHMETIC_13_3349764703780864

Proposition 9.19. Let n, m, k be natural numbers. Assume $k > 1$. Then

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

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

(1) Φ contains 0.

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

Let us show that if $n < m' + 1$ then $k^n < k^{m'+1}$. Assume $n < m' + 1$. Then $n \leq m'$. We have $k^{m'} \cdot 1 < k^{m'} \cdot k$. Indeed $k^{m'} \neq 0$.

Case $n = m'$. Take $A = k^n$ and $B = k^{m'+1}$. Then $A = k^n = k^{m'} < k^{m'} \cdot k = k^{m'+1} = B$. Hence $k^n = A < B = k^{m'+1}$. End.

Case $n < m'$. Take $A = k^n$ and $B = k^{m'+1}$. Then $A = k^n < k^{m'} < k^{m'} \cdot k = k^{m'+1} = B$. Hence $k^n = A < B = k^{m'+1}$. End. Qed. Qed.

Hence every natural number is contained in Φ. Thus $k^n < k^m$. End.

Case $k^n < k^m$. Define $\Psi = \{n' \in \mathbb{N} \mid \text{if } n' \geq m \text{ then } k^{n'} \geq k^m\}$.

(1) 0 is contained in Ψ.

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

Let us show that if $n' + 1 \geq m$ then $k^{n'+1} \geq k^m$. Assume $n' + 1 \geq m$.

Case $n' + 1 = m$. Obvious.

Case $n' + 1 > m$. Then $n' \geq m$. Hence $k^{n'} \geq k^m$. We have $k^{n'} \cdot 1 \leq k^{n'} \cdot k$. Indeed $1 \leq k$ and $k^{n'} \neq 0$. Take $A = k^m$ and $B = k^{n'+1}$. Then $A = k^m \leq k^{n'} = k^{n'} \cdot 1 \leq k^{n'} \cdot k = k^{n'+1} = B$. Hence $k^m = A \leq B = k^{n'+1}$. End. Qed. Qed.

Thus every natural number is contained in Ψ. Therefore if $n \geq m$ then $k^n \geq k^m$. [prover vampire] Consequently $n < m$. End. □

ARITHMETIC_13_6780506905509888

Corollary 9.20. Let n, m, k be natural numbers. Assume $k > 1$. Then

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

Proof. Assume $k^n = k^m$. Suppose $n \neq m$. Then $n < m$ or $m < n$. If $n < m$ then $k^n < k^m$. If $m < n$ then $k^m < k^n$. Thus $k^n \neq k^m$. Contradiction. □

ARITHMETIC_13_2876620253691904

Corollary 9.21. Let n, m, k be natural numbers. Assume $k > 1$. Then

$$n \leq m \quad \text{iff} \quad k^n \leq k^m.$$

ARITHMETIC_13_6984104377581568

Proposition 9.22. Let n be a natural number. Then

$$(n + 1)^2 = (n^2 + (2 \cdot n)) + 1.$$

Proof. We have

$$\begin{aligned}
&(n + 1)^2 \\
&= (n + 1) \cdot (n + 1) \\
&= ((n + 1) \cdot n) + (n + 1) \\
&= ((n \cdot n) + n) + (n + 1)
\end{aligned}$$

$$= (n^2 + n) + (n + 1)$$
$$= ((n^2 + n) + n) + 1$$
$$= (n^2 + (n + n)) + 1$$
$$= (n^2 + (2 \cdot n)) + 1.$$

□

ARITHMETIC_13_134060414337024

Proposition 9.23. Let n be a natural number. Assume $n \geq 3$. Then

$$n^2 > (2 \cdot n) + 1.$$

Proof. Define $\Phi = \{n' \in \mathbb{N}_{\geq 3} \mid n'^2 > (2 \cdot n') + 1\}$.

(1) Φ contains 3.

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

(a) $(n'^2+(2\cdot n'))+1 > (((2\cdot n')+1)+(2\cdot n'))+1$. Indeed $n'^2+(2\cdot n') > ((2\cdot n')+1)+(2\cdot n')$.

(b) $(((2 \cdot n') + 1) + (2 \cdot n')) + 1 > ((2 \cdot n') + (2 \cdot n')) + 1$.
Proof. We have $((2 \cdot n') + 1) + (2 \cdot n') > (2 \cdot n') + (2 \cdot n')$. Indeed $(2 \cdot n') + 1 > 2 \cdot n'$.
Qed.

(c) $(2 \cdot (n' + n')) + 1 > (2 \cdot (n' + 1)) + 1$.
Proof. We have $n' + n' > n' + 1$ and $2 \neq 0$. Thus $2 \cdot (n' + n') > 2 \cdot (n' + 1)$ (by corollary 6.18). Indeed $n' + n'$ and $n' + 1$ are natural numbers. Qed.

Take $A = (n' + 1)^2$ and $B = (2 \cdot (n' + 1)) + 1$. Then

$$A$$
$$= (n' + 1)^2$$
$$= (n'^2 + (2 \cdot n')) + 1$$
$$> (((2 \cdot n') + 1) + (2 \cdot n')) + 1$$
$$> ((2 \cdot n') + (2 \cdot n')) + 1$$
$$= (2 \cdot (n' + n')) + 1$$
$$> (2 \cdot (n' + 1)) + 1$$
$$= B.$$

Thus $(n' + 1)^2 = A > B = (2 \cdot (n' + 1)) + 1$. Qed.

Therefore Φ contains every element of $\mathbb{N}_{\geq 3}$ (by theorem 4.35). Consequently $n^2 > (2 \cdot n) + 1$. □

Chapter 10

Prime numbers

File: `arithmetic/sections/09_primes.ftl.tex`

[readtex `arithmetic/sections/07_divisibility.ftl.tex`]

[readtex `arithmetic/sections/08_euclidean-division.ftl.tex`]

ARITHMETIC_10_5438991513944064

Definition 10.1. Let n be a natural number. A trivial divisor of n is a divisor m of n such that $m = 1$ or $m = n$.

ARITHMETIC_10_8768240253665280

Definition 10.2. Let n be a natural number. A nontrivial divisor of n is a divisor m of n such that $m \neq 1$ and $m \neq n$.

ARITHMETIC_10_5450464558579712

Definition 10.3. Let n be a natural number. n is prime iff $n > 1$ and n has no nontrivial divisors.

Let n is compound stand for n is not prime. Let a prime number stand for a natural number that is prime.

ARITHMETIC_10_3834705971511296

Definition 10.4. $\mathbb{P}$ is the class of all prime numbers.

ARITHMETIC_10_8507257891323904

Proposition 10.5. $\mathbb{P}$ is a set.

ARITHMETIC_10_8020087063707648

Definition 10.6. Let n be a natural number. n is composite iff $n > 1$ and n has a nontrivial divisor.

ARITHMETIC_10_7801379464675328

Proposition 10.7. Let n be a natural number such that $n > 1$. Then n is prime iff every divisor of n is a trivial divisor of n.

ARITHMETIC_10_3685624758403072

Proposition 10.8. 2, 3, 5 and 7 are prime.

Proof. Let us show that 2 is prime. Let k be a divisor of 2. Then $0 < k \leq 2$. Hence $k = 1$ or $k = 2$. Thus k is a trivial divisor of 2. End.

Let us show that 3 is prime. Let k be a divisor of 3. Then $0 < k \leq 3$. Hence $k = 1$ or $k = 2$ or $k = 3$. 2 does not divide 3. Therefore $k = 1$ or $k = 3$. Thus k is a trivial divisor of 3. End.

Let us show that 5 is prime. Let k be a divisor of 5. Then $0 < k \leq 5$. Hence $k = 1$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 5$. 2 does not divide 5. 3 does not divide 5. Indeed $3 \cdot m \neq 5$ for all $m \in \mathbb{N}$ such that $m \leq 5$. Indeed $3 \cdot 0, 3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5 \neq 5$. 4 does not divide 5. Therefore $k = 1$ or $k = 5$. Thus k is a trivial divisor of 5. End.

Let us show that 7 is prime. Let k be a divisor of 7. Then $0 < k \leq 7$. Hence $k = 1$ or $k = 2$ or $k = 3$ or $k = 4$ or $k = 5$ or $k = 6$ or $k = 7$. 2 does not divide 7. 3 does not divide 7. Indeed $3 \cdot m \neq 7$ for all $m \in \mathbb{N}$ such that $m \leq 7$. Indeed $3 \cdot 0, 3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5, 3 \cdot 6, 3 \cdot 7 \neq 7$. 4 does not divide 7. 5 does not divide 7. Indeed $5 \cdot m \neq 7$ for all $m \in \mathbb{N}$ such that $m \leq 7$. Indeed $5 \cdot 0, 5 \cdot 1, 5 \cdot 2, 5 \cdot 3, 5 \cdot 4, 5 \cdot 5, 5 \cdot 6, 5 \cdot 7 \neq 7$. 6 does not divide 7. Therefore $k = 1$ or $k = 7$. Thus k is a trivial divisor of 7. End.

□

ARITHMETIC_10_2539250413207552

Proposition 10.9. 4, 6, 8 and 9 are compound.

Proof. $4 = 2 \cdot 2$. Thus 4 is compound.

$6 = 2 \cdot 3$. Thus 6 is compound.

$8 = 2 \cdot 4$. Thus 8 is compound.

$9 = 3 \cdot 3$. Thus 9 is compound. □

ARITHMETIC_10_3606185106210816

Proposition 10.10. Let n be a natural number such that $n > 1$. Then n has a prime divisor.

Proof. Define $\Phi = \{n' \in \mathbb{N} \mid$ if $n' > 1$ then n' has a prime divisor $\}$.

Let us show that for every $n' \in \mathbb{N}$ if Φ contains all predecessors of n' then Φ contains n'. Let $n' \in \mathbb{N}$. Assume that Φ contains all predecessors of n'. We have $n' = 0$ or $n' = 1$ or n' is prime or n' is composite.

Case $n' = 0$ or $n' = 1$. Trivial.

Case n' is prime. Obvious.

Case n' is composite. Take a nontrivial divisor m of n'. Then $1 < m < n'$. m is contained in Φ. Hence we can take a prime divisor p of m. Then we have $p \mid m \mid n'$. Thus $p \mid n'$. Therefore p is a prime divisor of n'. End. End.

[prover vampire] Thus every natural number belongs to Φ (by theorem 4.34). □

ARITHMETIC_10_463197419077632

Definition 10.11. Let n, m be natural numbers. n and m are coprime iff for all nonzero natural numbers k such that $k \mid n$ and $k \mid m$ we have $k = 1$.

Let n and m are relatively prime stand for n and m are coprime. Let n and m are mutually prime stand for n and m are coprime. Let n is prime to m stand for n and m are coprime.

ARITHMETIC_10_5776394594287616

Proposition 10.12. Let n, m be natural numbers. n and m are coprime iff n and m have no common prime divisor.

Proof. Case n and m are coprime. Let p be a prime number such that $p \mid n$ and $p \mid m$. Then p is nonzero and $p \neq 1$. Contradiction. End.

Case n and m have no common prime divisor. Assume that n and m are not coprime. Let k be a nonzero natural number such that $k \mid n$ and $k \mid m$. Assume that $k \neq 1$. Consider a prime divisor p of k. Then $p \mid k \mid n, m$. Hence $p \mid n$ and $p \mid m$. Contradiction. End. □

ARITHMETIC_10_7212152851005440

Proposition 10.13. Let n, m be natural numbers and p be a prime number. If p does not divide n then p and n are coprime.

Proof. Assume $p \nmid n$. Suppose that p and n are not coprime. Take a nonzero natural number k such that $k \mid p$ and $k \mid n$. Then $k = p$. Hence $p \mid n$. Contradiction. □

ARITHMETIC_10_8313676557713408

Proposition 10.14. Let n, m be natural numbers and p be a prime number. Then

$$p \mid n \cdot m \quad \text{implies} \quad (p \mid n \text{ or } p \mid m).$$

Proof. Assume $p \mid n \cdot m$.

Case $p \mid n$. Trivial.

Case $p \nmid n$. Define $\Phi = \{k \in \mathbb{N} \mid k \neq 0 \text{ and } p \mid k \cdot m\}$. Then $p \in \Phi$ and $n \in \Phi$. Hence Φ contains some natural number. Thus we can take a least element a of Φ regarding $<$.

Let us show that a divides all elements of Φ. Let $k \in \Phi$. Take natural numbers q, r such that $k = (a \cdot q) + r$ and $r < a$ (by theorem 8.1). Indeed a is nonzero. Then $k \cdot m = ((q \cdot a) + r) \cdot m = ((q \cdot a) \cdot m) + (r \cdot m)$. We have $p \mid k \cdot m$. Hence $p \mid ((q \cdot a) \cdot m) + (r \cdot m)$.

We can show that $p \mid r \cdot m$. We have $p \mid a \cdot m$. Hence $p \mid (q \cdot a) \cdot m$. Indeed $((q \cdot a) \cdot m) = q \cdot (a \cdot m)$. Take $A = (q \cdot a) \cdot m$ and $B = r \cdot m$. Then $p \mid A + B$ and $p \mid A$. Thus $p \mid B$ (by proposition 7.17). Indeed p, A and B are natural numbers. Consequently $p \mid r \cdot m$. End.

Therefore $r = 0$. Indeed if $r \neq 0$ then r is an element of Φ that is less than a. Hence

$k = q \cdot a$. Thus a divides k. End.

Then we have $a \mid p$ and $a \mid n$. Hence $a = p$ or $a = 1$. Thus $a = 1$. Indeed if $a = p$ then $p \mid n$. Then $1 \in \Phi$. Therefore $p \mid 1 \cdot m = m$. End. □

Chapter 11

Cardinality

File: `arithmetic/sections/11_cardinality.ftl.tex`

[readtex `foundations/sections/13_equinumerosity.ftl.tex`]

[readtex `arithmetic/sections/04_ordering.ftl.tex`]

11.1 Subsections of the natural numbers

ARITHMETIC_11_3625613501923328

Definition 11.1. Let n, m be natural numbers. $\{n, \dots, m\} = \{k \in \mathbb{N} \mid n \leq k \leq m\}$.

ARITHMETIC_11_145331933151232

Proposition 11.2. Let n, m be natural numbers. If $\{1, \dots, n\} = \{1, \dots, m\}$ then $n = m$.

Proof. Assume $\{1, \dots, n\} = \{1, \dots, m\}$.

Case $n = 0$. Then $\{1, \dots, n\} = \emptyset$. Thus $\{1, \dots, m\} = \emptyset$. Hence there exists no $k \in \mathbb{N}$ such that $1 \leq k \leq m$. Therefore $m = 0$. Consequently $n = m$. End.

Case $m = 0$. Then $\{1, \dots, m\} = \emptyset$. Thus $\{1, \dots, n\} = \emptyset$. Hence there exists no $k \in \mathbb{N}$ such that $1 \leq k \leq n$. Therefore $n = 0$. Consequently $n = m$. End.

Case $n, m \geq 1$. For all $k \in \mathbb{N}$ we have $1 \leq k \leq n$ iff $1 \leq k \leq m$. Hence for all $k \in \mathbb{N}$ we have $k \leq n$ iff $k \leq m$.

Let us show by contradiction that $n = m$. Suppose $n \neq m$. Then $n > m$ or $m > n$.

Case $n > m$. Take $k = m + 1$. Then $k \leq n$ and $k \nleq m$. Hence it is wrong that $k \leq n$ iff $k \leq m$. Contradiction. End.

Case $m > n$. Take $k = n + 1$. Then $k \leq m$ and $k \nleq m$. Hence it is wrong that $k \leq n$ iff $k \leq m$. Contradiction. End. End. End. □

ARITHMETIC_11_658708738605056

Proposition 11.3. Let n be a natural number. Then $\{1, \ldots, n+1\} = \{1, \ldots, n\} \cup \{n+1\}$.

Proof. We have $\{1, \ldots, n+1\} \subseteq \{1, \ldots, n\} \cup \{n+1\}$ and $\{1, \ldots, n\} \cup \{n+1\} \subseteq \{1, \ldots, n+1\}$. □

11.2 Finite and infinite sets

Finite sets

ARITHMETIC_11_3694156977274880

Definition 11.4. Let X be a set. X is finite iff there exists a natural number n such that X is equinumerous to $\{1, \ldots, n\}$.

ARITHMETIC_11_3929085203972096

Proposition 11.5. Let X, Y be sets. If X is finite and Y is equinumerous to X then Y is finite.

Proof. Assume that X is finite and Y is equinumerous to X. Take a natural number n and a bijection f between $\{1, \ldots, n\}$ and X and a bijection g between X and Y. Then $g \circ f$ is a bijection between $\{1, \ldots, n\}$ and Y (by **??**). Indeed X, Y are classes. Hence Y is finite. □

Infinite sets

ARITHMETIC_11_6612510618681344

Definition 11.6. Let X be a set. X is infinite iff X is not finite.

ARITHMETIC_11_5814530911240192

Proposition 11.7. Let X, Y be sets. If X is infinite and Y is equinumerous to X then Y is infinite.

Proof. Assume that Y is equinumerous to X. If Y is finite then X is finite. Hence if X is infinite then Y is infinite. □

The cardinality of a set

ARITHMETIC_11_4604295827685376

Signature 11.8. ∞ is an object that is not a natural number.

ARITHMETIC_11_4220669648699392

Definition 11.9. Let X be a set. The cardinality of X is the object κ such that

(if X is finite then κ is the natural number n such that X is equinumerous to $\{1, \ldots, n\}$) and

if X is infinite then $\kappa = \infty$.

Let $|X|$ stand for the cardinality of X.

Let X has finitely many elements stand for $|X| \in \mathbb{N}$. Let X has infinitely many elements stand for $|X| = \infty$.

Let X has exactly n elements stand for $|X| = n$. Let X has at most n elements stand for $|X| \leq n$. Let X has at least n elements stand for $|X| \geq n$.

ARITHMETIC_11_7260344969854976

Proposition 11.10. Let X be a set. X is empty iff $|X| = 0$.

Proof. Case X is empty. Then $X = \emptyset = \{1, \ldots, 0\}$. Hence X is equinumerous to $\{1, \ldots, 0\}$. Thus $|X| = 0$. End.

Case $|X| = 0$. Then X is equinumerous to $\{1, \ldots, 0\}$. $\{1, \ldots, 0\} = \emptyset$. Thus $X = \emptyset$.

End. ☐

ARITHMETIC_11_963914846175232

Proposition 11.11. Let X be a set. X is a singleton set iff $|X| = 1$.

Proof. Case X is a singleton set. Consider an object a such that $X = \{a\}$. Define $f(x) = 1$ for $x \in X$. Then f is a bijection between X and $\{1\}$. We have $\{1\} = \{1, \ldots, 1\}$. Hence $|X| = 1$. End.

Case $|X| = 1$. Take a bijection f between $\{1, \ldots, 1\}$ and X. We have $\{1, \ldots, 1\} = \{1\}$. Hence $X = \{f(1)\}$. End. ☐

ARITHMETIC_11_3151583407767552

Proposition 11.12. Let X be a set. X is an unordered pair iff $|X| = 2$.

Proof. Case X is an unordered pair. Consider distinct objects a, b such that $X = \{a, b\}$. Define

$$f(x) = \begin{cases} 1 & : x = a \\ 2 & : x = b \end{cases}$$

for $x \in X$. Then f is a bijection between X and $\{1, 2\}$. We have $\{1, \ldots, 2\} = \{1, 2\}$. Hence $|X| = 2$. End.

Case $|X| = 2$. Take a bijection f between $\{1, \ldots, 2\}$ and X. We have $\{1, \ldots, 2\} = \{1, 2\}$. Hence $X = \{f(1), f(2)\}$. End. ☐

11.3 Countable and uncountable sets

Countably infinite sets

ARITHMETIC_11_6249029537103872

Definition 11.13. Let X be a set. X is countably infinite iff X is equinumerous to $\mathbb{N}$.

ARITHMETIC_11_803449379749888

Proposition 11.14. Let X, Y be sets. If X is countably infinite and Y is equinumerous to X then Y is countably infinite.

Proof. Assume that X is countably infinite and Y is equinumerous to X. Take a bijection f between $\mathbb{N}$ and X and a bijection g between X and Y. Then $g \circ f$ is a bijection between $\mathbb{N}$ and Y (by **??**). Indeed X, Y are classes. Hence Y is countably infinite. □

Countable sets

ARITHMETIC_11_5412969443753984

Definition 11.15. Let X be a set. X is countable iff X is finite or X is countably infinite.

ARITHMETIC_11_4182588499427328

Proposition 11.16. Let X, Y be sets. If X is countable and Y is equinumerous to X then Y is countable.

Proof. Assume that X is countable and Y is equinumerous to X. If X is finite then Y is finite. If X is countably infinite then Y is countably infinite. Hence Y is countable. □

Uncountable sets

ARITHMETIC_11_2411928395710464

Definition 11.17. Let X be a set. X is uncountable iff X is not countable.

ARITHMETIC_11_1073385358491648

Proposition 11.18. Let X, Y be sets. If X is uncountable and Y is equinumerous to X then Y is uncountable.

Proof. Assume that Y is equinumerous to X. If Y is countable then X is countable. Hence if X is uncountable then Y is uncountable. □

11.4 Systems of sets

Definitions

ARITHMETIC_11_1387314525765632

Definition 11.19. A system of finite sets is a system of sets X such that every element of X is finite.

ARITHMETIC_11_3786392159125504

Definition 11.20. A system of countably infinite sets is a system of sets X such that every element of X is countably infinite.

ARITHMETIC_11_7341152585908224

Definition 11.21. A system of countable sets is a system of sets X such that every element of X is countable.

ARITHMETIC_11_6106935677943808

Definition 11.22. A system of uncountable sets is a system of sets X such that every element of X is uncountable.

Closure under unions

ARITHMETIC_11_3959378992431104

Definition 11.23. Let X be a system of sets. X is closed under arbitrary unions iff $\bigcup U \in X$ for every nonempty subset U of X.

Let X is closed under unions stand for X is closed under arbitrary unions.

ARITHMETIC_11_2377279311183872

Definition 11.24. Let X be a system of sets. X is closed under countable unions iff $\bigcup U \in X$ for every nonempty countable subset U of X.

ARITHMETIC_11_7040118193913856

Definition 11.25. Let X be a system of sets. X is closed under finite unions iff $\bigcup U \in X$ for every nonempty finite subset U of X.

ARITHMETIC_11_4164024962908160

Proposition 11.26. Let X be a system of sets. X is closed under finite unions iff $U \cup V \in X$ for every $U, V \in X$.

Proof. Case X is closed under finite unions. Let $U, V \in X$. Then $\{U, V\}$ is a nonempty finite subset of X. Hence $U \cup V = \bigcup\{U, V\} \in X$. End.

Case $U \cup V \in X$ for every $U, V \in X$. Define $\Phi = \{n \in \mathbb{N} \mid \bigcup U \in X$ for every nonempty subset U of X such that $|U| = n\}$.

(1) Φ contains 0.

(2) For every $n \in \Phi$ we have $n + 1 \in \Phi$.
Proof. Let $n \in \Phi$. Then $\bigcup U \in X$ for every nonempty subset U of X such that $|U| = n$.

Let us show that $\bigcup U \in X$ for every nonempty subset U of X such that $|U| = n + 1$.

Case $n = 0$. Obvious.

Case $n \neq 0$. Let U be a nonempty subset of X such that $|U| = n+1$. Take a bijection f between $\{1, \ldots, n+1\}$ and U. We have $\{1, \ldots, n+1\} = \{1, \ldots, n\} \cup \{n+1\}$. Take $V = f[\{1, \ldots, n\}]$. We have $\{1, \ldots, n\} \subseteq \{1, \ldots, n + 1\}$.

Let us show that $V \subseteq U$. Let $x \in V$. Take $k \in \{1, \ldots, n\}$ such that $x = f(k)$. Hence $x \in U$. End.

V is a nonempty set. Hence V is a nonempty subset of X. U is a class and $f : \{1, \ldots, n + 1\} \hookrightarrow U$. [prover vampire] Hence $f \restriction \{1, \ldots, n\}$ is a bijection between $\{1, \ldots, n\}$ and V (by **??**). [prover eprover] Thus $|V| = n$. Consequently $\bigcup V \in X$. We have $U = V \cup \{f(n+1)\}$. Indeed $U = f[\{1, \ldots, n+1\}] = f[\{1, \ldots, n\} \cup \{n+1\}] = f[\{1, \ldots, n\}] \cup f[\{n + 1\}] = f[\{1, \ldots, n\}] \cup \{f(n + 1)\}$.

Let us show that $\bigcup(A \cup B) = (\bigcup A) \cup (\bigcup B)$ for any nonempty systems of sets A, B. Let A, B be nonempty systems of sets. $\bigcup(A \cup B) \subseteq (\bigcup A) \cup (\bigcup B)$. $((\bigcup A) \cup (\bigcup B)) \subseteq \bigcup(A \cup B)$. End.

Hence $\bigcup U = \bigcup(V \cup \{f(n + 1)\}) = (\bigcup V) \cup (\bigcup\{f(n + 1)\}) = (\bigcup V) \cup f(n + 1) \in X$. Indeed V and $\{f(n + 1)\}$ are nonempty systems of sets. End. End. Qed.

Therefore Φ contains every natural number. Thus $\bigcup U \in X$ for every nonempty finite subset U of X. Consequently X is closed under finite unions. End. $\square$

Closure under intersections

ARITHMETIC_11_2369621166391296

Definition 11.27. Let X be a system of sets. X is closed under arbitrary intersections iff $\bigcap U \in X$ for every nonempty subset U of X.

Let X is closed under intersections stand for X is closed under arbitrary intersections.

ARITHMETIC_11_451771879129088

Definition 11.28. Let X be a system of sets. X is closed under countable intersections iff $\bigcap U \in X$ for every nonempty countable subset U of X.

ARITHMETIC_11_4297814324543488

Definition 11.29. Let X be a system of sets. X is closed under finite intersections iff $\bigcap U \in X$ for every nonempty finite subset U of X.

ARITHMETIC_11_1405012582334464

Proposition 11.30. Let X be a system of sets. X is closed under finite intersections iff $U \cap V \in X$ for every $U, V \in X$.

Proof. Case X is closed under finite intersections. Let $U, V \in X$. Then $\{U, V\}$ is a nonempty finite subset of X. Hence $U \cap V = \bigcap\{U, V\} \in X$. End.

Case $U \cap V \in X$ for every $U, V \in X$. Define $\Phi = \{n \in \mathbb{N} \mid \bigcap U \in X$ for every nonempty subset U of X such that $|U| = n\}$.

(1) Φ contains 0.

(2) For every $n \in \Phi$ we have $n + 1 \in \Phi$.
Proof. Let $n \in \Phi$. Then $\bigcap U \in X$ for every nonempty subset U of X such that $|U| = n$.

Let us show that $\bigcap U \in X$ for every nonempty subset U of X such that $|U| = n + 1$.

Case $n = 0$. Obvious.

Case $n \neq 0$. Let U be a nonempty subset of X such that $|U| = n+1$. Take a bijection f between $\{1, \dots, n+1\}$ and U. We have $\{1, \dots, n+1\} = \{1, \dots, n\} \cup \{n+1\}$. Take $V = f[\{1, \dots, n\}]$. We have $\{1, \dots, n\} \subseteq \{1, \dots, n + 1\}$.

Let us show that $V \subseteq U$. Let $x \in V$. Take $k \in \{1, \dots, n\}$ such that $x = f(k)$. Hence $x \in U$. End.

V is a nonempty set. Hence V is a nonempty subset of X. U is a class and $f : \{1, \ldots, n+1\} \hookrightarrow U$. [prover vampire] Hence $f \restriction \{1, \ldots, n\}$ is a bijection between $\{1, \ldots, n\}$ and V (by **??**). [prover eprover] Thus $|V| = n$. Consequently $\bigcap V \in X$. We have $U = V \cup \{f(n+1)\}$. Indeed $U = f[\{1, \ldots, n+1\}] = f[\{1, \ldots, n\} \cup \{n+1\}] = f[\{1, \ldots, n\}] \cup f[\{n+1\}] = f[\{1, \ldots, n\}] \cup \{f(n+1)\}$.

Let us show that $\bigcap(A \cup B) = (\bigcap A) \cap (\bigcap B)$ for any nonempty systems of sets A, B. Let A, B be nonempty systems of sets. $\bigcap(A \cup B) \subseteq (\bigcap A) \cap (\bigcap B)$. $((\bigcap A) \cap (\bigcap B)) \subseteq \bigcap(A \cup B)$. End.

Hence $\bigcap U = \bigcap(V \cup \{f(n+1)\}) = (\bigcap V) \cap (\bigcap\{f(n+1)\}) = (\bigcap V) \cap f(n+1) \in X$. Indeed V and $\{f(n+1)\}$ are nonempty systems of sets. End. End. Qed.

Therefore Φ contains every natural number. Thus $\bigcap U \in X$ for every nonempty finite subset U of X. Consequently X is closed under finite intersections. End. $\square$