

Peano Arithmetic

We study the axioms that define the usual arithmetic of the natural numbers.

1. The natural numbers

1.1. Axiomatization

The set $\mathbb{N} = \{0, 1, 2, \dots\}$ of natural numbers is familiar to us, and we know many of its properties:

$$x + 0 = x, \quad 0 + x = x, \quad x + y = y + x, \quad \dots$$

But can we identify the “very essence” of $\mathbb{N}$? Which properties play the role of axioms, and which can be proved from these axioms? We already use this approach to define a group $(G, \circ)$ or a vector space $(E, +, \cdot)$ axiomatically.

We will follow this approach to obtain the axioms that define the arithmetic of $\mathbb{N}$. There will be seven basic axioms (for addition and multiplication) and a family of induction axioms; together, they form Peano arithmetic.

What is an axiom? From our point of view, an *axiom* is a closed formula. A set of axioms is therefore a theory. For a set of axioms $\mathcal{A}$ and a formula $\mathcal{Q}$, we are often interested in whether $\mathcal{A} \vdash \mathcal{Q}$. We are also interested in the following equivalent assertion (by the Completeness Theorem): does $\mathcal{A} \models \mathcal{Q}$ hold? But we will mainly work in a specific structure $\mathcal{S}$ and discuss whether $\models_{\mathcal{S}} \mathcal{A}$ implies $\models_{\mathcal{S}} \mathcal{Q}$; that is, if the axioms are true in $\mathcal{S}$, is $\mathcal{Q}$ also true in $\mathcal{S}$? Thus, we will use the term *axioms* rather than *theory*, because we are not seeking to study general properties of theories. We will state and fix a set of formulas: the axioms of Peano arithmetic, denoted by $\mathcal{PA}$. The natural numbers $\mathbb{N}$ form a model of $\mathcal{PA}$; that is, $\models_{\mathbb{N}} \mathcal{PA}$.

1.2. Connection with the Incompleteness Theorems

Gödel’s Incompleteness Theorems apply to sufficiently “rich” theories $\mathcal{T}$. Concretely, the theory must contain the Peano axioms (that is, $\mathcal{PA} \subset \mathcal{T}$; or be able to prove them). Requiring a theory to contain these axioms is not a major demand, since it is difficult to do mathematics without being allowed to work with the natural numbers.

The natural numbers will also appear in the following chapters because the proof of the Incompleteness Theorems relies on an *arithmetization*: every symbol, formula, and proof will be encoded by a natural number in $\mathbb{N}$.

1.3. What is $\mathbb{N}$?

To axiomatize $\mathbb{N}$, it would be useful to be able to define it. Unfortunately, this is not so straightforward.

- A first approach is to define a language $\mathcal{L}$ containing the constant symbol 0 and a “successor” function S that plays the role of $S(n) = n + 1$. We then write $1 = S(0)$, $2 = S(1) = S(S(0))$, $3 = S(2)$. . . $\mathbb{N}$ is the smallest set for which this is possible.
- We can also define $\mathbb{N}$ using set theory: the natural numbers are constructed from the empty set $\emptyset$. We start with a language in which every object is a set (see the chapter “Variables and Structures”).

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{\emptyset\} = \{0\} \\ 2 &= \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\ 3 &= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} \\ &\dots \end{aligned}$$

We thus define $S(n) = n \cup \{n\} = \{0, 1, \dots, n\}$, denoted by $n + 1$.

We require 0 and the $S(n)$ to belong to the set; $\mathbb{N}$ is then the smallest set for which this is possible. We will return to this set-theoretic viewpoint when we discuss the axiomatic theory $\mathcal{ZF}$.

- $\mathbb{N}$ can also be defined uniquely in *second-order* logic if we write the induction axiom in the form:

$$\forall \mathcal{P} \quad \text{Rec}_{\mathcal{P}(x)}$$

(The induction principle $\text{Rec}_{\mathcal{P}(x)}$ will be defined later.) Be careful: this takes us outside the framework of first-order logic because “for every” does not range over an individual variable but over a collection of formulas, which is not allowed in first-order logic.

In every case, although defining $\mathbb{N}$ is not simple, the result does correspond to the set we know. However, there are also nonstandard models, that is, sets that satisfy the Peano axioms but are not $\mathbb{N}$. We could construct some by hand, but their existence will also be a consequence of the Incompleteness Theorem.

2. Peano axioms

The Peano axioms first consist of seven axioms defining elementary arithmetic, followed by an axiom schema for induction.

We consider the first-order language $\mathcal{L}_0 = (0, S, +, \times)$, where:

- 0 is a constant symbol (think of $0 \in \mathbb{N}$).
- S is a unary function, called the *successor* (think of $S(x) = x + 1$).
- $+$ is a binary function (think of addition).
- $\times$ is a binary function (think of multiplication).
- $=$ is the equality predicate.

We write $x \neq y$ for $\neg(x = y)$. The symbols $\leq$ and $<$ will be introduced later.

2.1. Elementary arithmetic

Here are the seven basic axioms:

- $\mathcal{A}_1 : \quad \forall x \quad S(x) \neq 0$
- $\mathcal{A}_2 : \quad \forall x \quad (x = 0) \vee (\exists y \quad x = S(y))$
- $\mathcal{A}_3 : \quad \forall x \quad \forall y \quad (S(x) = S(y)) \rightarrow (x = y)$
- $\mathcal{A}_4 : \quad \forall x \quad x + 0 = x$
- $\mathcal{A}_5 : \quad \forall x \quad \forall y \quad x + S(y) = S(x + y)$
- $\mathcal{A}_6 : \quad \forall x \quad x \times 0 = 0$
- $\mathcal{A}_7 : \quad \forall x \quad \forall y \quad x \times S(y) = (x \times y) + x$

Together, these axioms form *elementary arithmetic*. We will add the induction axioms immediately afterward.

Here are comments on each axiom and its interpretation in $\mathbb{N}$:

- $\mathcal{A}_1$: A successor is never zero. In $\mathbb{N}$, we always have $n + 1 \neq 0$. It is important that we cannot return to the starting point, as would happen if we cycled modulo N : $0, 1, 2, \dots, N - 1$, then 0 .
- $\mathcal{A}_2$: Every nonzero element is a successor. In $\mathbb{N}$, if $n \neq 0$, then there exists $m \in \mathbb{N}$ such that $n = m + 1$. (In fact, “ $m = n - 1$ ”, but subtraction is not available.) This is the only redundant axiom, since it follows from the other axioms and induction (see the exercises). It will nevertheless be important for Robinson arithmetic $\mathcal{Q}$ (see the end of the chapter).
- $\mathcal{A}_3$: The successors of x and y are equal if and only if x and y are equal; in other words, S is injective. With $\mathcal{A}_1$, this implies that starting from 0 , then $1 = S(0)$, $2 = S(1)$, $\dots$, we produce only new elements. In $\mathbb{N}$, this means $(n + 1 = m + 1) \rightarrow (n = m)$. By the definition of a function, if $x = y$, then $S(x) = S(y)$.
- $\mathcal{A}_4$: Adding 0 on the right changes nothing. In $\mathbb{N}$, $n + 0 = n$. In Peano arithmetic we will prove that this is also true on the left, “ $0 + x = x$ ”, but this requires induction. We will see that this becomes problematic for Robinson arithmetic $\mathcal{Q}$.
- $\mathcal{A}_5$: The successor behaves well with respect to addition. In $\mathbb{N}$, we would write $n + (m + 1) = (n + m) + 1$, a consequence of associativity.
- $\mathcal{A}_6$: Multiplication by 0 gives 0 . In $\mathbb{N}$, $n \times 0 = 0$. This will also be true on the left.
- $\mathcal{A}_7$: Addition behaves well with respect to multiplication. In $\mathbb{N}$, $n \times (m + 1) = (n \times m) + n$, a consequence of distributivity.

2.2. Induction axioms

We add not one axiom but infinitely many axioms, called an *axiom schema*. There is one axiom for each formula $\mathcal{P}$ having x as a free variable.

Let $\mathcal{P}$ be a formula of $\mathcal{L}_0$ with a free variable x . We write $\mathcal{P}(x)$ to indicate its dependence on x . This also allows us to write $\mathcal{P}(y)$ instead of $\mathcal{P}[y/x]$.

The induction principle for the formula $\mathcal{P}(x)$ is written:

$$\text{Rec}_{\mathcal{P}(x)} : \quad \mathcal{P}(0) \wedge [\forall x \quad \mathcal{P}(x) \rightarrow \mathcal{P}(S(x))] \quad \rightarrow \quad \forall x \quad \mathcal{P}(x)$$

In $\mathbb{N}$, this is the usual induction principle:

- if $\mathcal{P}(0)$ is true (base case),
- and if $\mathcal{P}(n) \rightarrow \mathcal{P}(n+1)$ for every $n \in \mathbb{N}$ (inductive step),
- then $\mathcal{P}(n)$ is true for every $n \in \mathbb{N}$ (conclusion).

We write:

$$\mathcal{R}ec = \left\{ \mathcal{R}ec_{\mathcal{P}(x)} \mid \mathcal{P} \text{ is a formula of } \mathcal{L}_0 \text{ with a free variable } x \right\}$$

$\mathcal{R}ec$ contains infinitely many (countably many) formulas.

Definition.

On note $\mathcal{P}\mathcal{A} = \{\mathcal{A}_1, \dots, \mathcal{A}_7\} \cup \mathcal{R}ec$. These are the axioms of *Peano arithmetic*.

Remark.

To be slightly more precise in our notation, we can write:

$$\mathcal{R}ec_{\mathcal{P}(x)} : \mathcal{P}[0/x] \wedge (\forall y \mathcal{P}[y/x] \rightarrow \mathcal{P}[S(y)/x]) \rightarrow \forall x \mathcal{P}(x)$$

Furthermore, if there are other free variables $x_1, \dots, x_n$, we write $\mathcal{P}(x, x_1, \dots, x_n)$ and add universal quantifiers at the beginning:

$$\mathcal{R}ec_{\mathcal{P}} : \forall x_1 \dots \forall x_n \left[\mathcal{P}(0, x_1, \dots, x_n) \wedge [\forall x \mathcal{P}(x, x_1, \dots, x_n) \rightarrow \mathcal{P}(S(x), x_1, \dots, x_n)] \right. \\ \left. \rightarrow \forall x \mathcal{P}(x, x_1, \dots, x_n) \right]$$

This version is essential for proving $x + y = y + x$ for every x, y by induction on x .

2.3. Models of $\mathcal{P}\mathcal{A}$

Proposition 1.

$\mathbb{N}$ is a model of $\mathcal{P}\mathcal{A}$.

Consider the structure $\mathcal{S}$, which by an abuse of notation we denote by $\mathbb{N}$, with domain $\mathbb{N}$ and naturally associated with $\mathcal{L}_0$ (0 is zero, $+$ is addition, $\times$ is multiplication, and $S(n) = n + 1$). As noted above, $\mathbb{N}$ satisfies the axioms of $\mathcal{P}\mathcal{A}$; that is, $\models_{\mathbb{N}} \mathcal{A}_1, \dots, \models_{\mathbb{N}} \mathcal{A}_7$, and, for every $\mathcal{P}$, $\models_{\mathbb{N}} \mathcal{R}ec_{\mathcal{P}(x)}$. This proves the proposition.

Corollary 1.

$\mathcal{P}\mathcal{A}$ is consistent.

Recall that this means $\mathcal{P}\mathcal{A} \not\vdash \perp$; in other words, there is no formula $\mathcal{Q}$ for which both $\mathcal{P}\mathcal{A} \vdash \mathcal{Q}$ and $\mathcal{P}\mathcal{A} \vdash \neg \mathcal{Q}$ hold. A theory $\mathcal{T}$ is consistent if and only if it has a model (see the chapter “Completeness Theorem”). Since $\mathbb{N}$ is a model of $\mathcal{P}\mathcal{A}$, $\mathcal{P}\mathcal{A}$ is consistent.

However, there are other models of $\mathcal{P}\mathcal{A}$, called *nonstandard* models. They are all infinite and contain $\mathbb{N}$. This is a very interesting point: we have succeeded in formalizing the essential properties of $\mathbb{N}$, yet this is not enough to characterize $\mathbb{N}$ uniquely. These seemingly paradoxical ideas lie at the heart of this book. In fact, no first-order axiomatization can characterize $\mathbb{N}$ uniquely.

Warning. Gödel’s First Incompleteness Theorem begins with the hypothesis “If $\mathcal{P}\mathcal{A}$ is consistent, ...”. Why is this hypothesis needed, since we have just said that it is true? Working only in the language $\mathcal{L}_0$ of Peano arithmetic, we cannot prove within that language that $\mathcal{P}\mathcal{A}$ is consistent. This is precisely Gödel’s Second Incompleteness Theorem, which says that no sufficiently rich theory can prove its own consistency.

Here, we assume that $\mathbb{N}$ exists. Thus $\mathcal{PA}$ has a model and is necessarily consistent. This certainty rests on a metamathematical acceptance of the existence of $\mathbb{N}$; that is, we must work in a more general theory (for example, $\mathcal{ZFC}$) to confirm this construction.

3. Properties of Peano arithmetic

We deliberately chose a limited number of axioms. We must now recover the usual arithmetic properties from them. We will prove very few, since that would belong more to a mathematics course than to a logic course. Above all, this is an ideal opportunity to use formal proof software.

3.1. Using the basic axioms

Lemma 1.

$$2 + 2 = 4$$

Yes, nothing can be taken for granted! We hardly dare call this a “theorem”, yet we must justify that $\mathcal{PA} \vdash “2 + 2 = 4”$.

Remark. We write $1 = S(0)$, $2 = S(1)$, $3 = S(2)$, $4 = S(3)$. These are only notational conventions: $1, 2, 3, 4$ are not symbols of the language but syntactic abbreviations. Without them, we would have to write $S(S(0)) + S(S(0)) = S(S(S(S(0))))$.

Proof.

$$\begin{aligned} 2 + 2 &= 2 + S(1) && \text{by the definition of } 2 = S(1) \\ &= S(2 + 1) && \text{by } \mathcal{A}_5 \\ &= S(2 + S(0)) && \text{by the definition of } 1 = S(0) \\ &= S(S(2 + 0)) && \text{by } \mathcal{A}_5 \\ &= S(S(2)) && \text{by } \mathcal{A}_4 \\ &= S(3) && \text{by the definition of } S(2) = 3 \\ &= 4 && \text{by the definition of } S(3) = 4 \end{aligned}$$

□

Without induction, no general algebraic property can be proved.

3.2. Using induction

Lemma 2.

$$\forall x \quad 0 + x = x$$

This resembles axiom $\mathcal{A}_4$, “ $\forall x \quad x + 0 = x$ ”, but we do not yet know that addition is commutative.

Proof. Let $\mathcal{P}(x) : 0 + x = x$.

We write the induction proof in the usual mathematical style:

- Base case. $\mathcal{P}(0)$: $0 + 0 = 0$. This is true by $\mathcal{A}_4$ (it is the 0 on the right that applies, not the one on the left!).

- Inductive step. Fix n . Assume $\mathcal{P}(n)$ is true and prove $\mathcal{P}(S(n))$ (the equivalent of $\mathcal{P}(n+1)$).

$\mathcal{P}(n)$ is true
 therefore $0 + n = n$
 therefore $S(0 + n) = S(n)$ because S is a function
 therefore $0 + S(n) = S(n)$ by axiom $\mathcal{A}_5$
 therefore $\mathcal{P}(S(n))$ is true.

Thus $\mathcal{P}(n) \rightarrow \mathcal{P}(S(n))$, and in the logical notation of $\mathcal{PA}$, we have proved $\mathcal{P}(x) \rightarrow \mathcal{P}(S(x))$ for every x .

- Conclusion. By induction, here $\text{Rec}_{\mathcal{P}(x)}$, we deduce “ $\forall x \mathcal{P}(x)$ ”, that is, “ $\forall x 0 + x = x$ ”.

□

Lemma 3.

$$\forall x \forall y \quad S(x) + y = S(x + y)$$

This is like axiom $\mathcal{A}_5$, but with the roles reversed.

Proof. Fix x . We proceed by induction on y . Let $\mathcal{P}(y) : S(x) + y = S(x + y)$.

- Base case. $\mathcal{P}(0)$: $S(x) + 0 = S(x) = S(x + 0)$. This holds.
- Inductive step. Assume $\mathcal{P}(y)$.

$S(x) + y = S(x + y)$ by the induction hypothesis
 therefore $S(S(x) + y) = S(S(x + y))$ because S is a function
 therefore $S(x) + S(y) = S(x + S(y))$ by applying $\mathcal{A}_5$ on the left and right
 therefore $\mathcal{P}(S(y))$ is true.

Thus, for every y , $\mathcal{P}(y) \rightarrow \mathcal{P}(S(y))$.

- Conclusion. By induction, $\forall y \mathcal{P}(y)$. Since this holds for every x , we have $\forall x \forall y \quad S(x) + y = S(x + y)$.

Remark. To be rigorous, we should write $\mathcal{P}(x, y) : S(x) + y = S(x + y)$, then prove $\forall x \mathcal{P}(x, 0)$ and $\forall x \forall y \mathcal{P}(x, y) \rightarrow \mathcal{P}(x, S(y))$, which leads to $\forall x \forall y \mathcal{P}(x, y)$. □

Lemma 4.

$$\forall x \forall y \quad x + y = y + x$$

This is the expected commutativity of addition.

Proof. Fix x . We proceed by induction on y . Let $\mathcal{P}(y) : x + y = y + x$.

- Base case. $\mathcal{P}(0)$: $x + 0 = x$ (by axiom $\mathcal{A}_4$) and $0 + x = x$ (by Lemma 2). Therefore $x + 0 = 0 + x$.
- Inductive step. Assume $\mathcal{P}(y)$ is true.

$x + y = y + x$
 therefore $S(x + y) = S(y + x)$
 therefore $x + S(y) = S(y) + x$ by $\mathcal{A}_5$ on the left and Lemma 3 on the right
 therefore $\mathcal{P}(S(y))$ is true.

- Conclusion. For every x : $\forall y \quad x + y = y + x$.

□

3.3. Other operations

- **Inequality.** $x \neq y$ means $\neg(x = y)$.
- **Nonstrict inequality.** $x \leq y$ means $\exists z \ x + z = y$ (recall that we are modeling the natural numbers; think of z as an element of $\mathbb{N}$).
- **Strict inequality.** $x < y$ means $(x \leq y) \wedge (x \neq y)$.
- **Subtraction.** Be careful: $x - y$ is not a function because it is not always well-defined; for example, $2 - 3$ has no meaning here. For $x \leq y$, however, there exists z such that $x + z = y$, and we could define $y - x = z$.
- Nor is there a well-defined division x/y .

There is now plenty of work to do, for example, proving:

$$\begin{aligned} (x \leq y) \wedge (y \leq z) &\rightarrow x \leq z \\ x \leq y &\rightarrow x \times z \leq y \times z \\ &\dots \end{aligned}$$

3.4. Definable sets

Fix a first-order language $\mathcal{L}$ and an associated structure $\mathcal{S}$ with domain E .

Definition.

A set $A \subset E$ is **definable** if there is a formula $\mathcal{P}(x)$ of $\mathcal{L}$ such that:

$$A = \{a \in E \mid \models_{\mathcal{S}} \mathcal{P}(a)\}$$

In other words, A is exactly the set of all a for which $\mathcal{P}(a)$ is true.

Example.

- The set of even numbers in $\mathbb{N}$ is definable by the formula:

$$\mathcal{P}(x): \exists y \ x = y + y$$

- In $\mathbb{N}$, the set of prime numbers is definable by the formula:

$$\mathcal{P}(x): (x \neq 1) \wedge \left[\forall y \ \forall z \ (x = y \times z) \rightarrow (y = 1) \vee (z = 1) \right]$$

When working formally in Peano arithmetic (independently of the model $\mathbb{N}$), this formula serves as the definition of a prime number (with the abbreviation $1 = S(0)$).

3.5. Strong induction

In an ordinary induction proof, we assume $\mathcal{P}(n)$ to deduce $\mathcal{P}(n+1)$. In strong induction, we assume that $\mathcal{P}(0), \mathcal{P}(1), \dots, \mathcal{P}(n)$ are true to deduce that $\mathcal{P}(n+1)$ is true. This is sometimes very useful.

Here is the strong induction formula for $\mathcal{P}$:

$$\text{RecF}_{\mathcal{P}(x)}: \left[\forall x \ (\forall y \ y < x \rightarrow \mathcal{P}(y)) \rightarrow \mathcal{P}(x) \right] \rightarrow \forall x \ \mathcal{P}(x)$$

Over $\mathbb{N}$, this expresses that the strong inductive step $[\mathcal{P}(0) \wedge \dots \wedge \mathcal{P}(n-1)] \rightarrow \mathcal{P}(n)$ entails $\forall n \ \mathcal{P}(n)$.

The base case is implicit. Taking $x = 0$ in the brackets, the left-hand side of the implication, “ $\forall y \quad y < 0 \rightarrow \mathcal{P}(y)$ ”, is always true (no y is strictly less than 0 in $\mathbb{N}$); therefore $\mathcal{P}(0)$ must be true for the implication to be true.

As an exercise, one could show that strong induction is equivalent to ordinary induction.

4. Other arithmetics

4.1. Presburger arithmetic

This arithmetic is simpler than Peano arithmetic because it has no multiplication. The language is $\mathcal{L} = (0, S, +)$, and we consider only axioms $\mathcal{A}_1, \dots, \mathcal{A}_5$ and $\mathcal{R}_{ec}$. We denote this theory by $\mathcal{PR}$. Although multiplication is absent, we can define $3x$ as $x + x + x$; in contrast, a formula “ $x \times y$ ” is not allowed.

Theorem 1.

$\mathcal{PR}$ is consistent and complete.

Recall what this means. For any (closed) formula $\mathcal{Q}$:

- $\mathcal{PR}$ is consistent, so it cannot prove both $\mathcal{Q}$ and $\neg\mathcal{Q}$.
- $\mathcal{PR}$ is complete; consequently, it proves $\mathcal{Q}$ or $\neg\mathcal{Q}$.

The proof is rather technical and uses “quantifier elimination”: a formula of $\mathcal{L}$ is transformed into an equivalent quantifier-free formula by introducing congruence modulo integers n . We first transform $\forall$ into $\exists$, since “ $\forall x \quad \mathcal{P}(x)$ ” is equivalent to “ $\neg(\exists x \quad \neg\mathcal{P}(x))$ ”. For example, “ y is even” is:

$$\exists x \quad y = x + x$$

that is, $\exists x \quad y = 2x$, which is equivalent to:

$$y \equiv 0 \pmod{2}$$

Thus, using congruence, the formula has no quantifiers. In general, a closed formula yields an algebraic expression modulo an integer n . The formula is provable if and only if this expression is satisfied. Thus, either a formula or its negation is provable.

4.2. Robinson arithmetic $\mathcal{Q}$

We define a new axiomatic theory, with addition and multiplication but without induction. We denote by $\mathcal{Q}$ the theory consisting of axioms $\mathcal{A}_1, \dots, \mathcal{A}_7$, without induction axioms. This time, axiom $\mathcal{A}_2$, which states that every nonzero element is a successor, is essential.

Theorem 2.

$\mathcal{Q}$ is consistent but incomplete.

The theory $\mathcal{Q}$ is consistent because $\mathbb{N}$ is a model of it.

To prove that it is incomplete, we show that the formula

$$\mathcal{G} : \quad \forall x \quad 0 + x = x$$

is not provable, and neither is $\neg\mathcal{G}$. (The letter G stands for “Gödel”.)

Do not confuse $\mathcal{G}$ with axiom $\mathcal{A}_4$, “ $\forall x \quad x + 0 = x$ ”. Recall that proving $\mathcal{G}$ in Peano arithmetic required induction, which is not allowed here.

Proof.

- $\neg\mathcal{G}$ is not provable.

Suppose for a contradiction that $\neg\mathcal{G}$ is provable. Then $\mathcal{Q} \vdash \neg\mathcal{G}$ and, by the Soundness Theorem, $\mathcal{Q} \models \neg\mathcal{G}$. But $\models_{\mathbb{N}} \mathcal{Q}$, so $\models_{\mathbb{N}} \neg\mathcal{G}$. Yet $\mathcal{G}$ is true in $\mathbb{N}$, a contradiction.

- $\mathcal{G}$ is not provable.

We follow the same idea: find a model of $\mathcal{Q}$ in which $\mathcal{G}$ is false. It cannot be $\mathbb{N}$, where $\mathcal{G}$ is true.

Let $\mathcal{S}$ have domain $\mathbb{N} \cup \{a, b\}$. The objects a and b are new and distinct; think of them as two infinities ∞_a and ∞_b .

For two natural numbers, addition is the usual addition, and we set:

- $a + 0 = a$
- $0 + a = b$

We also have $S(a) = a$ and $S(b) = b$ (in the spirit of “ $\infty + 1 = \infty$ ”); we do not need the details of the other operations below.

One can check that all axioms $\mathcal{A}_1, \dots, \mathcal{A}_7$ are satisfied (see the exercises). On the other hand, $\mathcal{G}$ is false because $0 + a = b$ and $a \neq b$.

As before, if $\mathcal{Q} \vdash \mathcal{G}$, then $\mathcal{Q} \models \mathcal{G}$, hence $\models_{\mathcal{S}} \mathcal{G}$, contradicting our construction.

□

But is this the end of our story? The goal of Gödel and of this book is an Incompleteness Theorem, and we have just found an incomplete theory. Why continue? If we are dissatisfied because $\mathcal{Q}$ proves neither $\mathcal{G}$ nor $\neg\mathcal{G}$, we could extend it to $\mathcal{Q}_1 = \mathcal{Q} \cup \{\mathcal{G}\}$, which proves $\mathcal{G}$. But $\mathcal{Q}_1$ is not complete either. There exists $\mathcal{G}_1$ such that neither $\mathcal{Q}_1 \vdash \mathcal{G}_1$ nor $\mathcal{Q}_1 \vdash \neg\mathcal{G}_1$ (see the exercises). We could then consider $\mathcal{Q}_2 = \mathcal{Q}_1 \cup \{\mathcal{G}_1\} \dots$, merely postponing the problem.

We need a general statement showing that we will never obtain a complete theory. This is the power of Gödel’s Incompleteness Theorem: whatever the theory, it will be incomplete, so adding an unprovable formula will not produce a complete theory.

4.3. The axiomatic theories $\mathcal{ZF}$ and $\mathcal{ZFC}$

Zermelo–Fraenkel set theory, denoted by $\mathcal{ZF}$, is an axiomatic set theory that provides, among other things, foundations for arithmetic. The language is $\mathcal{L} = \{\in\}$ (with equality), and every object is a set. See “Variables and Structures” for an introduction. Thus, “ $x \in y$ ” means “the set x belongs to the set y ”. For example, $\{0, 1\} \in \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

It is a more modern and much more powerful theory than Peano arithmetic. However, we will not need it for the Incompleteness Theorems, so this brief introduction to $\mathcal{ZF}$ will not be used later.

We have already seen how to construct the natural numbers from the empty set:

$$0 = \emptyset, \quad 1 = \{\emptyset\}, \quad 2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}, \quad 3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}, \quad \dots$$

and, more generally, $S(n) = n \cup \{n\}$.

$\mathcal{ZF}$ is governed by axioms for manipulating sets. We list them without all the details:

- **Empty set axiom:** there exists a set containing no elements.
- **Axiom of infinity:** it guarantees the existence of an infinite set (containing all the natural numbers).
- **Axiom of extensionality:** two sets having the same elements are equal.

$$\forall x \forall y \quad (\forall z (z \in x \leftrightarrow z \in y) \rightarrow x = y)$$

- **Axiom of foundation:** every nonempty set x has an element y disjoint from x . This rules out membership cycles (such as $x \in x$).

$$\forall x \neq \emptyset \quad \exists y \in x \quad (y \cap x = \emptyset)$$

- **Axiom of union:** for a set x , there exists a set $\bigcup_x$ that is the union of all sets belonging to x .

$$\forall x \exists y \forall z (z \in y \leftrightarrow \exists t (t \in x) \wedge (z \in t))$$

For example, if $x = \{\{1, 2\}, \{2, 3\}, \{4, 5\}\}$, then $\bigcup_x = \{1, 2, 3, 4, 5\}$ (1, 2, ... are regarded as sets).

- **Axiom of pairing:** given two sets x and y , there exists a set $\{x, y\}$ consisting exactly of x and y .
Example: if $x = \{\{1, 2\}, \{3\}\}$ and $y = \{3, 4\}$, then $\{x, y\} = \{\{\{1, 2\}, \{3\}\}, \{3, 4\}\}$. (This is not the union of x and y .)
- **Power set axiom:** for a set x , there exists a set $\mathcal{P}(x)$ containing all subsets of x . For example, if $x = \{0, 1\}$, then $\mathcal{P}(x) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.
- **Axiom schema of separation:** it allows subsets to be defined using a formula $\mathcal{P}$; thus, $\{x \in y \mid \mathcal{P}(x)\}$ is a set.
- **Axiom schema of replacement:** it allows the elements of a set to be replaced by other objects; the result remains a set.

These axioms form $\mathcal{ZF}$.

The following axiom is often added:

- **Axiom of choice $\mathcal{AC}$:** for every set A , there exists a function assigning to every nonempty subset of A an element of that subset.

This axiom is independent of $\mathcal{ZF}$ (neither it nor its negation can be proved from $\mathcal{ZF}$), so it may be added or omitted as needed for infinite sets. It occurs in different forms (Zorn's lemma, Krull's theorem), is essential for certain classical proofs (existence of bases in infinite-dimensional vector spaces, existence of non-Lebesgue-measurable subsets of $\mathbb{R}$), and can simplify others (the Hahn–Banach theorem in the countable case). If we adopt the axiom of choice, the resulting theory is denoted by $\mathcal{ZFC}$. This is the standard framework for modern mathematics.