

Peano Arithmetic

While the algebraic theories of groups, rings, fields, ... have many models, (elementary) number theory studies properties of *one* model, which is called the **standard model** of number theory:

$$\mathcal{N} = (\mathbb{N}, +, \cdot, +1, 0).$$

Let \mathcal{L}_{PA} be the associated language, for which we also choose $+$, \cdot , 0 as (non-logical) symbols, but S for the unary successor operation $+1$. The theory of the standard model, $\text{Th}(\mathcal{N})$, is the set of L_{PA} -sentences that hold in this model. We have already seen as a consequence of the compactness theorem that there exist **non-standard models**, i.e., models that are not isomorphic to the standard model, because they have “infinitely large” numbers.

Moreover, $\text{Th}(\mathcal{N})$ as a theory, while complete, is rather mysterious, since we do not know a priori which sentences exactly it comprises. The most important properties of the standard model are captured by the **Peano Axioms**.

Definition 1: Peano Axioms

- P1.** $Sx \neq 0$
- P2.** $Sx = Sy \rightarrow x = y$
- P3.** $x + 0 = x$
- P4.** $x + Sy = S(x + y)$
- P5.** $x \cdot 0 = 0$
- P6.** $x \cdot Sy = x \cdot y + x$

To these we add the infinitely many **induction axioms**:

- Ind.** $\varphi(0) \wedge \forall x(\varphi(x) \rightarrow \varphi(Sx)) \rightarrow \forall x \varphi(x)$

The theory comprising these axioms is called PA, **Peano Arithmetic**. As every model of $\text{Th}(\mathcal{N})$ is also a model of PA, it follows from the compactness theorem that there are non-standard models of PA.

Theorem 2

There exists a (countable) model \mathcal{N}^* of PA which is not isomorphic to \mathcal{N} .

(In fact, we know by Loewenheim-Skolem that there exists a non-standard model in every infinite cardinality.)

These results can be interpreted as an expressive weakness of the language of first-order logic, because if one moves to a **language of second order**, in which one additionally has the possibility of using **second-order quantifiers** $\exists X, \forall Y$ to quantify over subsets of the respective domain, then one can uniquely characterize (up to isomorphism) the standard model in this stronger theory:

Definition 3: Second-Order Peano Axioms

The theory $\text{PA}^{(2)}$ (Peano Axioms of second order) has the following axioms:

- P1.** $\forall x 0 \neq Sx$
- P2.** $\forall x \forall y (Sx = Sy \rightarrow x = y)$
- IND.** $\forall X (0 \in X \wedge \forall x (x \in X \rightarrow Sx \in X) \rightarrow \forall x x \in X)$

Theorem 4

Every model of $\text{PA}^{(2)}$ is isomorphic to the standard model $(\mathbb{N}, S, 0)$.

The second-order induction axiom (actually a *set-theoretic* axiom) is thus significantly more expressive than the corresponding induction schema, in which only first-order properties are allowed, which can only quantify over elements (instead of also over subsets) of natural numbers.

On the other hand, second-order logic has other disadvantages – most prominently, no completeness theorem holds.

PA^- : Peano Arithmetic without Induction

PA still has infinitely many (induction) axioms. We will introduce a finite subtheory that turns out is strong enough to capture many essential properties of arithmetic.

This theory is formalized in a language \mathcal{L} with the symbols $0, 1, <, +, \cdot$. The first axioms state that addition and multiplication are associative and commutative and satisfy the distributive law, and furthermore that 0 and 1 are neutral elements for the respective operations and 0 is a zero divisor:

Axioms A1-A7:

- **A1:** $(x + y) + z = x + (y + z)$
- **A2:** $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
- **A3:** $x + y = y + x$
- **A4:** $x \cdot y = y \cdot x$
- **A5:** $x \cdot (y + z) = x \cdot y + x \cdot z$
- **A6:** $x + 0 = x \wedge x \cdot 0 = 0$
- **A7:** $x \cdot 1 = x$

Here we use the usual algebraic bracket conventions (\cdot binds more strongly than $+$). For the $<$ -relation, the axioms state that it is a linear order compatible with addition and multiplication:

Axioms A8-A12:

- **A8:** $\neg x < x$
- **A9:** $x < y \wedge y < z \rightarrow x < z$
- **A10:** $x < y \vee x = y \vee y < x$
- **A11:** $x < y \rightarrow x + z < y + z$
- **A12:** $0 < z \wedge x < y \rightarrow x \cdot z < y \cdot z$

A number can be subtracted from a larger one:

Axiom A13:

- **A13:** $x < y \rightarrow \exists z (x + z = y)$

And finally, 1 is the successor of 0 and 0 is the smallest element (where as usual $x \leq y : \Leftrightarrow x < y \vee x = y$):

Axioms A14-A15:

- **A14:** $0 < 1 \wedge \forall x (0 < x \rightarrow 1 \leq x)$
- **A15:** $\forall x (0 \leq x)$

From A14 it follows with A11 that more generally $x + 1$ is the successor of x , and thus the order is *discrete*:

$$x < x + 1 \wedge \forall y (x < y \rightarrow x + 1 \leq y).$$

Examples

1. In Peano Arithmetic PA, one can define the $<$ -relation by $x < y \leftrightarrow \exists z (x + z + 1 = y)$ and thus obtain all axioms of PA^- . In particular, the standard model \mathbb{N} with the usual $<$ -relation, the usual operations, and the natural numbers $0, 1$ is a model of PA^- .

2. The set $\mathbb{Z}[X]$ of polynomials in one variable X with integer coefficients is a commutative ring with the usual operations. One can order this ring by setting for a polynomial $p = a_n X^n + \dots a_1 X + a_0$ with leading coefficient $a_n \neq 0$:

$$a_n X^n + \dots a_1 X + a_0 > 0 : \Leftrightarrow a_n > 0$$

and thus ordering polynomials $p, q \in \mathbb{Z}[X]$ by $p < q : \Leftrightarrow q - p > 0$. The subset $\mathbb{Z}[X]^+$ of polynomials $p \in \mathbb{Z}[X]$ with $p \geq 0$ then becomes a model of PA^- , in which the polynomial X is larger than all constant polynomials and thus “infinitely large”.

Relation to Discretely Ordered Rings

In a ring, there is a group with respect to addition, while A13 only allows a restricted inverse formation. If one replaces axioms A13 and A15 in PA^- with the axiom

Axiom A16:

- **A16:** $\forall x \exists z (x + z = 0)$

one obtains the algebraic theory **DOR** of **discretely ordered rings**, whose models include, for example, the rings \mathbb{Z} and $\mathbb{Z}[X]$. Every model \mathcal{M} of PA^- can be extended to a model \mathcal{R} of the theory **DOR** (following the same pattern by which one extends the natural numbers to the ring of integers), such that the non-negative elements of \mathcal{R} coincide with the original model. Conversely, for every model \mathcal{R} of the theory **DOR**, the restriction to the non-negative elements is a model of PA^- , so that one can *describe* PA^- as the theory of (the non-negative part of) *discretely ordered rings*.