Mathematical Logic (Preliminary Draft - may contain many mistakes)

by Peter Koepke

Table of contents

1 Introduction

Mathematics models real world phenomena like space, time, number, probability, games, etc. It proceeds from initial assumptions to conclusions by rigorous arguments. Its results are "universal" and "logically valid", in that they do not depend on external or implicit conditions which may change with time, nature or society.

It is remarkable that mathematics is also able to *model itself*: mathematical logic defines rigorously what mathematical statements and rigorous arguments are. The mathematical enquiry into the mathematical method leads to deep insights into mathematics, applications to classical field of mathematics, and to new mathematical theories. The study of mathematical language has also influenced the theory of formal and natural languages in computer science, linguistics and philosophy.

1.1 A simple proof

We want to indicate that rigorous mathematical proofs can be generated by applying simple text manipulations to mathematical statements. Let us consider a fragment of the elementary theory of functions which expresses that the composition of two surjective maps is surjective as well:

> Let f and g be *surjective*, i.e., for all y there is x such that $y=f(x)$, and for all y there is x such that $y=g(x)$.
> *Theorem*. $g\circ f$ is surjective, i.e., for all y there is x such that $y=g(f(x))$.
> *Proof*. Consider any y. Choose z such that $y=g(z)$. Choose x such that $z=f(x)$. Then $y=g(f(x))$. Thus there is x such that $y=g(f(x))$. Thus for all y there is x such that $y=g(f(x))$.
> *Qed*.

These statements and arguments are expressed in an austere and systematic language, which can be normalized further. Logical symbols like $\forall$ and $\exists$ abbreviate figures of language like "for all" or "there exists":

> Let $\forall y \exists x\, y=f(x)$.
> Let $\forall y \exists x\, y=g(x)$.
> Theorem. $\forall y \exists x\, y=g(f(x))$.
> Proof. Consider y.

$\exists x\, y = g(x)$.
Let $y = g(z)$.
$\exists x\, z = f(x)$.
Let $z = f(x)$.
$y = g(f(x))$.
Thus $\exists x\, y = g(f(x))$.
Thus $\exists x\, y = g(f(x))$.
Thus $\forall y \exists x\, y = g(f(x))$.
Qed.

These lines can be considered as formal sequences of symbols. Certain sequences of symbols are acceptable as mathematical formulas. There are rules for the formation of formulas which are acceptable in a proof. These rules have a purely formal character and they can be applied irrespectively of the "meaning" of the symbols and formulas.

1.2 Formal proofs

In the example, $\exists x\, y = g(f(x))$ is inferred from $y = g(f(x))$. The rule of *existential quantification*: "put $\exists x$ in front of a formula" can usually be applied. It has the character of a left-multiplication by $\exists x$.

$$\exists x\,, \varphi \mapsto \exists x\, \varphi.$$

Logical rules satisfy certain algebraic laws like associativity. Another interesting operation is *substitution*: From $y = g(z)$ and $z = f(x)$ infer $y = g(f(x))$ by a "find-and-replace"-substitution of z by $f(x)$.

Given a sufficient collection of rules, the above sequence of formulas, involving "keywords" like "let" and "thus" is a *deduction* or *derivation* in which every line is generated from earlier ones by syntactical rules. Mathematical results may be provable simply by the application of formal rules. In analogy with the formal rules of the infinitesimal calculus one calls a system of rules a *calculus*.

1.3 Syntax and semantics

Obviously we do not just want to describe a formal derivation as a kind of domino but we want to *interpret* the occuring symbols as mathematical objects. Thus we let variables x, y, ... range over some domain like the real numbers $\mathbb{R}$ and let f and g stand for functions $F, G: \mathbb{R} \to \mathbb{R}$. Observe that the symbol or "name" f is not identical to the function F, and indeed f might also be interpretated as another function F'. To emphasize the distinction between names and objects, we classify symbols, formulas and derivations as *syntax* whereas the interpretations of symbols belong to the realm of *semantics*.

By interpreting x, y, ... and f, g, ... in a structure like $(\mathbb{R}, F, G)$ we can define straightforwardly whether a formula like $\exists x\, g(f(x))$ is *satisfied* in the structure. A formula is *logically valid* if it is satisfied under *all* interpretations. The fundamental theorem of mathematical logic and the central result of this course is GÖDEL's completeness theorem:

Theorem. *There is a calculus with finitely many rules such that a formula is derivable in the calculus iff it is logically valid.*

1.4 Set theory

In modern mathematics notions can usually be reduced to set theory: non-negative integers correspond to cardinalities of finite sets, integers can be obtained via pairs of non-negative integers, rational numbers via pairs of integers, and real numbers via subsets of the rationals, etc. Geometric notions can be defined from real numbers using analytic geometry: a point is a pair of real numbers, a line is a set of points, etc. It is remarkable that the basic set theoretical axioms can be formulated in the logical language indicated above. So mathematics may be understood abstractly as

Mathematics = (first-order) logic + set theory.

Note that we only propose this as a reasonable abstract viewpoint corresponding to the logical analysis of mathematics. This perspective leaves out many important aspects like the applicability, intuitiveness and beauty of mathematics.

Like most mathematicians we shall usually work in a naive set theory, taking some care that arguments can be carried out in formal axiomatic systems if needed. We shall also restrict the use of the axiom of infinity to semantic considerations and introduce syntax without that axiom. Thus we shall develop syntax in a finitary theory and obtain Gödel's incompleteness theorems for Peano arithmetic.

1.5 Circularity

We shall use *sets* as symbols which can then be used to formulate the axioms of *set* theory. We shall *prove* theorems about *proofs*. This kind of circularity seems to be unavoidable in comprehensive foundational science: linguistics has to *talk* about *language*, *brain research* has to be carried out by brains. Circularity can lead to paradoxes like the liar's paradox: "I am a liar", or "this sentence is false". Circularity poses many problems and seems to undermine the value of foundational theories. We suggest that the reader takes a *naive* standpoint in these matters: there are sets and proofs which are just as obvious as natural numbers. Then theories are formed which abstractly describe the naive objects.

A closer analysis of circularity in logic leads to the famous *incompleteness theorems* of GÖDEL's:

Theorem. *Formal theories which are strong enough to "formalize themselves" are not complete, i.e., there are statements such that neither it nor its negation can be proved in that theory. Moreover such theories cannot prove their own consistency.*

It is no surprise that these results, besides their initial mathematical meaning had a tremendous impact on the theory of knowledge outside mathematics, e.g., in philosophy, psychology, linguistics.

2 Set theoretic preliminaries

To model the mathematical method, we have to formalize mathematical language and general structures by mathematical objects. Usually *sets* are taken to be the most basic mathematical objects. We present some facts from set theory which will be used in the sequel.

In line with our introductory remarks on circularity we initially treat set theory *naively*, i.e., we view sets and set theoretic operations as concrete mental constructs. We shall later introduce a powerful axiom system for sets. From an axiomatic standpoint most of our arguments can be carried out under weak set theoretical hypotheses. In particular it will not be necessary to use sets of high cardinality.

The theory of *finite* sets is based on the *empty set* $\emptyset = \{\}$ and operations like

$$x \mapsto \{x\};\ x, y \mapsto \{x, y\};\ x, y \mapsto x \cup y;\ x, y \mapsto x \cap y;\ x, y \mapsto x \setminus y.$$

These operations form new sets out of given sets. The operations satisfy obvious basic properties like

$$x \cap (y \cup z) = (x \cap y) \cup (x \cap z).$$

It is natural to represent the integer n by a particular set which has n elements. We shall later see that the following formalization can be carried out uniformly in set theory:

$$\begin{aligned} 0 &= \emptyset \\ 1 &= \{0\} \\ 2 &= \{0,1\} \\ &\vdots \\ n+1 &= \{0,1,\ldots,n\} = \{0,1,\ldots,n-1\} \cup \{n\} = n \cup \{n\} \\ &\vdots \\ \mathbb{N} = \omega &= \{0,1,\ldots\} \end{aligned}$$

These integers satisfy the usual laws of complete induction and recursion.

We must discuss the settheoretical status of the collection $\mathbb{N}$ of all natural numbers. A particular problem in set theory is the question whether a collection of sets is again a set. Such collections are often denoted by *class terms* like

ZFC is ZF together with Zorn's Lemma which is equivalent to the Axiom of Choice (AC).

$$\{x \mid x \text{ has the property } P\}.$$

In these lectures we shall work with three set theories ZF, ZFC and ST:

- ZF stands for the common axiom system by Ernst Zermelo and Abraham Fraenkel. ZF implies the existence of infinite sets and in particular that $\mathbb{N}$ is a set.
- ZFC is ZF together with the Axiom of **C**hoice which is equivalent to Zorn's Lemma.
- ST (for **S**et **T**heory) consists of all the ZF-axioms except the axiom of infinity.

The theory ST is not committed about the existence of infinite sets. In the theory ST $\mathbb{N}$ could possibly be a *proper class* but not a set. To accomodate the three set theories in one exposition we shall call collections X which need not be sets *classes*. Furthermore we write that X is a *class** to express that under the stronger theory ZF X is a set. In that sense $\mathbb{N}$ is a class*. In definitions we say that etc

The operation $x, y \mapsto (x, y) = \{\{x\}, \{x, y\}\}$ defines the *ordered pair* of x and y. Its crucial property is that

$$\{\{x\}, \{x, y\}\} = \{\{x'\}, \{x', y'\}\} \text{ if and only if } x = x' \text{ and } y = y'.$$

Ordered pairs allow to formalize (binary) relations and functions:

- a *relation* is a class R of ordered pairs;
- a *function* is a relation f such that for all x, y, y' holds: if $(x, y) \in f$ and $(x, y') \in f$ then $y = y'$. Then $f(x)$ denotes the unique y such that $(x, y) \in f$.

We assume standard notions and notations from relation theory, see also Definition 2 below. For binary relations R we can use the *infix* notation aRb instead of $(a, b) \in R$.

If a function maps the elements of a class a into a class b we write

$$f: a \to b.$$

In case we do not want to specify the target b, we can also write $f: a \to V$ where V is understood to be the *universe* of all sets. We assume the usual notions of function theory like *injective*, *surjective*, *bijective*, etc. If a is a set then its image

$$\{f(x) \mid x \in a\}$$

is a set as well.

A *finite sequence* is a function $w: n \to V$ for some integer $n \in \mathbb{N}$ which is the *length* of w. A finite sequence is a set. We write w_i instead of $w(i)$, and the sequence w may also be denoted by $w_0 \dots w_{n-1}$. Note that the empty set $\emptyset$ is the unique finite sequence of length 0.

For finite sequences $w = w_0 \dots w_{m-1}$ and $w' = w'_0 \dots w'_{n-1}$ let $w\hat{\ }w' = w_0 \dots w_{m-1} w'_0 \dots w'_{n-1}$ be the *concatenation* of w and w'. $w\hat{\ }w': m + n \to V$ can be defined by

$$w\hat{\ }w'(i) = \begin{cases} w(i), \text{ if } i < m; \\ w'(i - m), \text{ if } i \geqslant m. \end{cases}$$

We also write ww' for $w\hat{\ }w'$. This operation is a *monoid* satisfying some cancellation rules:

Proposition 1. *Let w, w', w'' be finite sequences. Then*

a) $(w\hat{\ }w')\hat{\ }w'' = w\hat{\ }(w'\hat{\ }w'')$.

b) $\emptyset\hat{\ }w = w\hat{\ }\emptyset = w$.

c) $w\hat{\ }w' = w\hat{\ }w'' \to w' = w''$.

d) $w'\hat{\ }w = w''\hat{\ }w \to w' = w''$.

Proof. We only check the associative law a). Let $n,n',n''\in\mathbb{N}$ such that $w=w_0...w_{n-1}$, $w'=w'_0...w'_{n'-1}$, $w''=w''_0...w''_{n''-1}$. Then

$$\begin{aligned}(w\hat{\ }w')\hat{\ }w'' &= (w_0...w_{n-1}w'_0...w'_{n'-1})\hat{\ }w''_0...w''_{n''-1}\\ &= w_0...w_{n-1}w'_0...w'_{n'-1}w''_0...w''_{n''-1}\\ &= w_0...w_{n-1}\hat{\ }(w'_0...w'_{n'-1}w''_0...w''_{n''-1})\\ &= w_0...w_{n-1}\hat{\ }(w'_0...w'_{n'-1}\hat{\ }w''_0...w''_{n''-1})\\ &= w\hat{\ }(w'\hat{\ }w'').\end{aligned}$$

The trouble with this argument is the intuitive but vague use of the *ellipses* "...". In mathematical logic we have to ultimately eliminate such vaguenesses. So we show that for all $i<n+n'+n''$

$$((w\hat{\ }w')\hat{\ }w'')(i)=(w\hat{\ }(w'\hat{\ }w''))(i).$$

Case 1: $i<n$. Then

$$\begin{aligned}((w\hat{\ }w')\hat{\ }w'')(i) &= (w\hat{\ }w')(i)\\ &= w(i)\\ &= (w\hat{\ }(w'\hat{\ }w''))(i).\end{aligned}$$

Case 2: $n\leqslant i<n+n'$. Then

$$\begin{aligned}((w\hat{\ }w')\hat{\ }w'')(i) &= (w\hat{\ }w')(i)\\ &= w'(i-n)\\ &= (w'\hat{\ }w'')(i-n)\\ &= (w\hat{\ }(w'\hat{\ }w''))(i).\end{aligned}$$

Case 3: $n+n'\leqslant i<n+n'+n''$. Then

$$\begin{aligned}((w\hat{\ }w')\hat{\ }w'')(i) &= w''(i-(n+n'))\\ &= w'\hat{\ }w''(i-(n+n')+n')=w'\hat{\ }w''(i-n)\\ &= (w\hat{\ }(w'\hat{\ }w''))(i-n+n)\\ &= (w\hat{\ }(w'\hat{\ }w''))(i).\end{aligned}$$

□

A set x is *finite*, if there is an integer $n\in\mathbb{N}$ and a surjective function $f\colon n\to x$. The smallest such n is called the *cardinality* of the finite set x and denoted by $n=\mathrm{card}(x)$. The usual cardinality properties for finite sets follow from properties of finite sequences.

A class* x is *denumerable* or *countable* if there is a surjective function $f\colon\mathbb{N}\to x$. If x is not finite, it is *countably infinite*. Then its cardinality is $\aleph_0$, written as $\aleph_0=\mathrm{card}(x)$. Within our strongest theory ZFC, the union

$$\bigcup_{n\in\omega}x_n$$

where each x_n is a countable set is again a countable countable.

If a class is not countable, it is *uncountable*. Within set theory one can develop an efficient notion of cardinality for uncountable sets.

The theory of infinite sets usually requires the *axiom of choice* which is equivalent to ZORN's lemma.

Definition 2. *Let A be a set and $\leqslant$ be a binary relation. Define*

a) $(A,\leqslant)$ is transitive *if for all $a,b,c\in A$*

$$a\leqslant b \text{ and } b\leqslant c \text{ implies } a\leqslant c.$$

b) $(A,\leqslant)$ is reflexive *if for all $a\in A$ holds $a\leqslant a$.*

c) $(A,\leqslant)$ *is a* partial order *if* $(A,\leqslant)$ *is transitive and reflexive and* $A\neq\emptyset$.

So let $(A,\leqslant)$ *is be a partial order.*

a) $z\in A$ *is a* maximal element *of* A *if there is no* $a\in A$ *with* $z\leqslant a$ *and* $z\neq a$.

b) *If* $X\subseteq A$ *then* u *is an* upper bound *for* X *if for all* $x\in X$ *holds* $x\leqslant u$.

c) $I\subseteq A$ *is* linear *if for all* $a,b\in I$

$$a\leqslant b \text{ or } b\leqslant a.$$

d) $(A,\leqslant)$ *is* inductive *if every linear subset of* A *has an upper bound.*

Zorn's *lemma* states

Theorem 3. *Every inductive partial order has a maximal element.*

3 Symbols and words

Intuitively and also in our theory a word is a finite sequence of symbols. A symbol has some basic information about its role within words. E.g., the symbol $\leqslant$ is usually used to stand for a binary relation. So we let symbols include such type information. We provide us with a sufficient collection of symbols.

Definition 4. *The* basic symbols *of first-order logic are*

a) $\equiv$ *for* equality*,*

b) $\neg,\rightarrow,\bot$ *for the logical operations of* negation*,* implication *and the truth value* false*,*

c) $\forall$ *for* universal quantification*,*

d) (*and*) *for auxiliary* bracketing*,*

e) *variables* v_n *for* $n\in\mathbb{N}$.

Let S_0 *be the class* of basic symbols and let* $\mathrm{Var}=\{v_n|n\in\mathbb{N}\}$ *be the class* of variables. We assume that the basic symbols are pairwise distinct and are distinct from any relation or function symbol. For concreteness one could for example set* $\equiv=0$, $\neg=1$, $\rightarrow=2$, $\bot=3$, $(=4$, $)=5$, *and* $v_n=(1,n)$ *for* $n\in\mathbb{N}$.

An n*-ary* relation symbol*, for* $n\in\mathbb{N}$*, is (a set) of the form* $R=(x,0,n)$*; here* 0 *indicates that the values of a relation will be* truth values*.* 0*-ary relation symbols are also called* propositional constant symbols*. An* n*-ary* function symbol*, for* $n\in\mathbb{N}$*, is (a set) of the form* $f=(x,1,n)$ *where* 1 *indicates that the values of a function will be elements of a structure.* 0*-ary function symbols are also called* constant symbols*.*

A symbol set *or a* language *is a set of relation symbols and function symbols.*

An n-ary relation symbol is intended to denote an n-ary relation; an n-ary function symbol is intended to denote an n-ary function. A symbol set is sometimes called a *type* because it describes the type of structures which will later interpret the symbols. We shall denote variables by letters like x, y, z, ..., relation symbols by P, Q, R, ..., functions symbols by f, g, h, ... and constant symbols by $c, c_0, c_1, \ldots$ We shall also use other typographical symbols in line with standard mathematical practice. A symbol like $<$, e.g., usually denotes a binary relation, and we could assume for definiteness that there is some fixed set theoretic formalization of $<$ like $<=(999,0,2)$. Instead of the arbitrary 999 one could also take the number of $<$ in some typographical font.

Example 5. The *language of group theory* is the language

$$S_{\mathrm{Gr}}=\{\circ,e\},$$

where $\circ$ is a binary (= 2-ary) function symbol and e is a constant symbol. Again one could be definite about the coding of symbols and set $S_{\mathrm{Gr}} = \{(80, 1, 2), (87, 1, 0)\}$, e.g., but we shall not care much about such details. As usual in algebra, one also uses an *extended language of group theory*

$$S_{\mathrm{Gr}} = \{\circ, {}^{-1}, e\}$$

to describe groups, where ${}^{-1}$ is a unary (= 1-ary) function symbol.

Definition 6. *Let S be a language. A* word *over S is a finite sequence*

$$w: n \to S_0 \cup S.$$

Let S^* be the set of all words over S. The empty set $\emptyset$ is also called the empty word.

Let S be a symbol set. We want to formalize how a word like $\exists x\, y = g(f(x))$ can be produced from a word like $y = g(f(x))$.

Definition 7. *A relation $R \subseteq (S^*)^n \times S^*$ is called a* rule *(over S). A* calculus *(over S) is a set $\mathcal{C}$ of rules (over S).*

We work with rules which *produce* words out of given words. A rule

$$\{(\text{arguments, production})|...\}$$

is usually written as a *production rule* of the form

$$\frac{\text{arguments}}{\text{production}} \quad \text{or} \quad \frac{\text{preconditions}}{\text{conclusion}}.$$

For the existential quantification mentioned in the introduction we may for example write

$$\frac{\varphi}{\exists x \varphi}$$

where the production is the concatenation of $\exists x$ and φ.

Definition 8. *Let $\mathcal{C}$ be a calculus over S. Let $R \subseteq (S^*)^n \times S^*$ be a rule of $\mathcal{C}$. For $X \subseteq S^*$ set*

$$R[X] = \{w \in S^* \mid \textit{there are words } u_0, ..., u_{n-1} \in X \textit{ such that } R(u_0, ..., u_{n-1}, w) \textit{ holds}\}.$$

Then the product *of $\mathcal{C}$ is the smallest subset of S^* closed under the rules of $\mathcal{C}$:*

$$\mathrm{Prod}(\mathcal{C}) = \bigcap \{X \subseteq S^* \mid \textit{for all rules } R \in \mathcal{C} \textit{ holds } R[X] \subseteq X\}.$$

The product of a calculus can also be described "from below" by:

Definition 9. *Let $\mathcal{C}$ be a calculus over S. A sequence $w^{(0)}, ..., w^{(k-1)} \in S^*$ is called a* derivation *in $\mathcal{C}$ if for every $l < k$ there exists a rule $R \in \mathcal{C}$, $R \subseteq (S^*)^n \times S^*$ and $l_0, ..., l_{n-1} < l$ such that*

$$R(w^{(l_0)}, ..., w^{(l_{n-1})}, w^{(l)}).$$

This means that every word of the derivation can be derived from earlier words of the derivation by application of one of the rules of the calculus. We shall later define a calculus such that the sequence of sentences

Let $\forall y \exists x\, y = f(x)$.
Let $\forall y \exists x\, y = g(x)$.
Consider y.
$\exists x\, y = g(x)$.
Let $y = g(z)$.
$\exists x\, z = f(x)$.
Let $z = f(x)$.
$y = g(f(x))$.

Thus $\exists x\, y = g(f(x))$.
Thus $\exists x\, y = g(f(x))$.
Thus $\forall y \exists x\, y = g(f(x))$.
Qed.

is basically a derivation in that calculus.

Everything in the product of a calculus can be obtained by a derivation.

Proposition 10. *Let $\mathcal{C}$ be a calculus over S. Then*

$$\mathrm{Prod}(\mathcal{C}) = \{w \,|\, \text{there is a derivation } w^{(0)}, \ldots, w^{(k-1)} = w \text{ in } \mathcal{C}\}.$$

Proof. The equality of sets can be proved by two inclusions.
($\subseteq$) The set

$$X = \{w \,|\, \text{there is a derivation } w^{(0)}, \ldots, w^{(k-1)} = w \text{ in } \mathcal{C}\}$$

satisfies the closure property $R[X] \subseteq X$ for all rules $R \in \mathcal{C}$. Since $\mathrm{Prod}(\mathcal{C})$ is the intersection of all such sets, $\mathrm{Prod}(\mathcal{C}) \subseteq X$.
($\supseteq$) Consider $w \in X$. Consider a derivation $w^{(0)}, \ldots, w^{(k-1)} = w$ in $\mathcal{C}$. We show by induction on $l < k$ that $w^{(l)} \in \mathrm{Prod}(\mathcal{C})$. Let $l < k$ and assume that for all $i < l$ holds $w^{(i)} \in \mathrm{Prod}(\mathcal{C})$. Take a rule $R \in \mathcal{C}$, $R \subseteq (\mathbb{A}^*)^n \times \mathbb{A}^*$ and $l_0, \ldots, l_{n-1} < l$ such that $R(w^{(l_0)}, \ldots, w^{(l_{n-1})}, w^{(l)})$. Since $\mathrm{Prod}(\mathcal{C})$ is closed under application of R we get $w^{(l)} \in \mathrm{Prod}(\mathcal{C})$. Thus $w = w^{(k-1)} \in \mathrm{Prod}(\mathcal{C})$. □

Exercise 1. (Natural numbers 1) Consider the symbol set $S = \{\,|\,\}$. The set $S^* = \{\emptyset, |, ||, |||, \ldots\}$ of words may be identified with the set $\mathbb{N}$ of natural numbers. Formulate a calculus $\mathcal{C}$ such that $\mathrm{Prod}(\mathcal{C}) = S^*$.

4 Induction and recursion on calculi

Derivations in a calculus have finite length so that one can carry out inductions and recursions along the lengths of derivations. We formulate appropriate induction and recursion theorems which generalize *complete induction* and *recursion* for natural numbers. Note the recursion is linked to induction but requires stronger hypothesis.

Theorem 11. (Induction Theorem) *Let $\mathcal{C}$ be a calculus over S and let $\varphi(-)$ be a property which is inherited along the rules of $\mathcal{C}$:*

$$\forall R \in \mathcal{C}, R \subseteq (S^*)^k \times S^*\, \forall w^{(1)}, \ldots, w^{(k)}, w \in S^*, R(w^{(1)}, \ldots, w^{(k)}, w)\ (\varphi(w^{(1)}) \wedge \ldots \wedge \varphi(w^{(k)}) \rightarrow \varphi(w)).$$

Then

$$\forall w \in \mathrm{Prod}(\mathcal{C})\ \varphi(w).$$

Proof. By assumption, $\{w \in S^* | \varphi(w)\}$ is closed under the rules of $\mathcal{C}$. Since $\mathrm{Prod}(\mathcal{C})$ is the intersection of all sets which are closed under $\mathcal{C}$,

$$\mathrm{Prod}(\mathcal{C}) \subseteq \{w \in S^* | \varphi(w)\}.$$ □

Definition 12. *A calculus $\mathcal{C}$ over S is* uniquely readable *if for every $w \in \mathrm{Prod}(\mathcal{C})$ there are a unique rule $R \in \mathcal{C}, R \subseteq (S^*)^k \times S^*$ and unique $w^{(1)}, \ldots, w^{(k)} \in S^*$ such that*

$$R(w^{(1)}, \ldots, w^{(k)}, w).$$

Theorem 13. (Recursion Theorem) *Let $\mathcal{C}$ be a calculus over S which is uniquely readable and let $(G_R | R \in \mathcal{C})$ be a sequence of* recursion rules, *i.e., for $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ let $G_R\colon V^k \rightarrow V$ where V is the universe of all sets. Then there is a uniquely determined function $F\colon \mathrm{Prod}(\mathcal{C}) \rightarrow V$ such that the following* recursion equation *is satisfied for all $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ and $w^{(1)}, \ldots, w^{(k)}, w \in \mathrm{Prod}(\mathcal{C})$, $R(w^{(1)}, \ldots, w^{(k)}, w)$:*

$$F(w) = G_R(F(w^{(1)}), \ldots, F(w^{(k)})).$$

We say that F is defined by recursion along $\mathcal{C}$ *by the recursion rules* $(G_R|R\in\mathcal{C})$.

Proof. We define $F(w)$ by complete recursion on the length of the shortest derivation of w in $\mathcal{C}$. Assume that $F(u)$ is already uniquely defined for all $u\in\mathrm{Prod}(\mathcal{C})$ with shorter derivation length. Let w have shortest derivation $w^{(0)},\ldots,w^{(l-1)}$. By the unique readability of $\mathcal{C}$ there are $R\in\mathcal{C}$, $R\subseteq(S^*)^k\times S^*$ and $w^{(i_0)},\ldots,w^{(i_{k-1})}$ with $i_0,\ldots,i_{k-1}<l-1$ such that

$$R(w^{(i_0)},\ldots,w^{(i_{k-1})},w).$$

Then we can uniquely define

$$F(w)=G_R(F(w^{(i_0)}),\ldots,F(w^{(i_{k-1})})).$$ □

Remark 14. The previous Theorem states the existence of a function F as a set of ordered pairs, but the proof argues that F can be defined (by some intuitive “procedure”). To complete the argument one would have to use the recursion theorem from set theory which says that definitions of a certain kind correspond to certain functions in the set theoretic universe.

5 Terms and formulas

Fix a symbol set S for the remainder of this section. We generate the *terms* and *formulas* of the corresponding language L^S by calculi.

Definition 15. *The* term calculus *(for S) consists of the following rules:*

a) $\frac{}{x}$ *for all variables x;*

b) $\frac{}{c}$ *for all constant symbols $c\in S$;*

c) $\frac{t_0\,t_1\ldots t_{n-1}}{f t_0\ldots t_{n-1}}$ *for all n-ary function symbols $f\in S$.*

*Let T^S be the product of the term calculus. T^S is the set of all S-*terms.

Definition 16. *The* formula calculus *(for S) consists of the following rules:*

a) $\frac{}{\bot}$ *produces* falsity*;*

b) $\frac{}{t_0\equiv t_1}$ *for all S-terms $t_0,t_1\in T^S$ produces* equations*;*

c) $\frac{}{R t_0\ldots t_{n-1}}$ *for all n-ary relation symbols $R\in S$ and all S-terms $t_0,\ldots,t_{n-1}\in T^S$ produces* relational formulas*;*

d) $\frac{\varphi}{\neg\varphi}$ *produces* negations *of formulas;*

e) $\frac{\varphi\quad\psi}{(\varphi\to\psi)}$ *produces* implications*;*

f) $\frac{\varphi}{\forall x\varphi}$ *for all variables x produces* universalizations.

Let L^S be the product of the formula calculus. L^S is the set of all S-formulas, and it is also called the first-order language *for the symbol set S. Formulas produced by rules a-c) are called* atomic formulas *since they constitute the initial steps of the formula calculus.*

Example 17. S-terms and S-formulas formalize the naive concept of a “mathematical formula”. The standard axioms of *group theory* can be written as in the extended language of group theory as $S_{\mathrm{Gr}'}$-formulas:

a) $\forall v_0\,\forall v_1\,\forall v_2\,\circ v_0\circ v_1 v_2\equiv\circ\circ v_0 v_1 v_2$;

b) $\forall v_0\,\circ v_0\, e\equiv v_0$;

c) $\forall v_0\,\circ v_0\,{}^{-1}v_0\equiv e$.

Note that in c) the $^{-1}$-operator is "applied" to the variable v_0 . The term calculus uses the bracket-free *polish notation* which writes operators before the arguments (*prefix* operators). In line with standard notations one also writes operators in *infix* and *postfix* notation, using bracket, to formulate, e.g., associativity:

$$\forall v_0 \forall v_1 \forall v_2\, v_0 \circ (v_1 \circ v_2) \equiv (v_0 \circ v_1) \circ v_2 .$$

Since the particular choice of variables should in general be irrelevant they may be denoted by letters $x, y, z, \ldots$ instead. Thus the group axioms read:

a) $\forall x \forall y \forall z\; x \circ (y \circ z) \equiv (x \circ y) \circ z$;

b) $\forall x\, x \circ e \equiv x$;

c) $\forall x\, x \circ x^{-1} \equiv e$.

Let $\Phi_{\mathrm{Gr}'} = \{\forall x \forall y \forall z\; x \circ (y \circ z) \equiv (x \circ y) \circ z, \forall x\, x \circ e \equiv x, \forall x\, x \circ x^{-1} \equiv e\}$ be the *axioms of group theory* in the extended language.

To work with terms and formulas, it is crucial that the term and formula calculi are uniquely readable. We leave the proof of these facts as exercises.

Although the language introduced will be theoretically sufficient for all mathematical purposes it is often convenient to further extend its expressiveness. We view some additional language constructs as *abbreviations* for formulas in L^S.

Definition 18. *For S-formulas φ and ψ and a variable x write*

- $\top$ *("true") instead of* $\neg\bot$ *;*
- $(\varphi \vee \psi)$ *("φ or ψ") instead of* $(\neg\varphi \rightarrow \psi)$ *is the* disjunction *of* φ, ψ *;*
- $(\varphi \wedge \psi)$ *("φ and ψ") instead of* $\neg(\varphi \rightarrow \neg\psi)$ *is the* conjunction *of* φ, ψ *;*
- $(\varphi \leftrightarrow \psi)$ *("φ iff ψ") instead of* $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$ *is the* equivalence *of* φ, ψ *;*
- $\exists x \varphi$ *("for all x holds φ") instead of* $\neg\forall x \neg\varphi$ *.*

For the sake of simplicity one often omits redundant brackets, in particular outer brackets. So we usually write $\varphi \vee \psi$ instead of $(\varphi \vee \psi)$.

6 Structures and models

We shall *interpret* formulas like $\forall y \exists x\; y = g(f(x))$ in adequate *structures*. This interaction between language and structures is usually called *semantics*. Fix a symbol set S.

Definition 19. *An S-*structure *is a function* $\mathfrak{A}\colon \{\forall\} \cup S \rightarrow V$ *such that*

a) $\mathfrak{A}(\forall) \neq \emptyset$*;* $\mathfrak{A}(\forall)$ *is the* underlying set *of* $\mathfrak{A}$ *and is usually denoted by A or* $|\mathfrak{A}|$*;*

b) for every n-ary relation symbol $R \in S$, $\mathfrak{A}(R)$ *is an n-ary* relation *on A, i.e.,* $a(r) \subseteq A^n$*;*

c) for every n-ary function symbol $f \in S$, $\mathfrak{A}(f)$ *is an n-ary* function *on A, i.e.,* $a(r)\colon A^n \rightarrow A$*.*

Again we use customary or convenient notations for the *components* of the structure $\mathfrak{A}$, i.e., the values of $\mathfrak{A}$. One often writes $R^{\mathfrak{A}}$, $f^{\mathfrak{A}}$, or $c^{\mathfrak{A}}$ instead of $\mathfrak{A}(r)$, $\mathfrak{A}(f)$, or $\mathfrak{A}(c)$ resp. In simple cases, one may simply list the components of the structure and write, e.g.,

$$\mathfrak{A} = (A, R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}, f^{\mathfrak{A}})$$

or "$\mathfrak{A}$ has domain A with relations $R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}$ and an operation $f^{\mathfrak{A}}$".

One also uses the same notation for a structure and its underlying set like in

$$A = (A, R_0^{\mathfrak{A}}, R_1^{\mathfrak{A}}, f^{\mathfrak{A}}).$$

This "overloading" of one notation is quite common in mathematics (and in natural language). There are methods of "disambiguating" the ambiguities introduced by multiple usage. Another common overloading is given by a naive identification of syntax and semantics, i.e., by writing

$$A = (A, R_0, R_1, f).$$

Since we are particularly interested in the interplay of syntax and semantics we shall try to avoid this kind of overloading.

Example 20. Formalize the *ordered field of reals* $\mathbb{R}$ as follows. Define the language of ordered fields

$$S_{\mathrm{oF}} = \{<, +, \cdot, 0, 1\}.$$

Then define the structure $\mathbb{R}: \{\forall\} \cup S_{\mathrm{oF}} \to V$ by

$$\begin{array}{rcl} \mathbb{R}(\forall) & = & \mathbb{R} \\ \mathbb{R}(<) = <^{\mathbb{R}} & = & \{(u, v) \in \mathbb{R}^2 \,|\, u < v\} \\ \mathbb{R}(+) = +^{\mathbb{R}} & = & \{(u, v, w) \in \mathbb{R}^3 \,|\, u + v = w\} \\ \mathbb{R}(\cdot) = \cdot^{\mathbb{R}} & = & \{(u, v, w) \in \mathbb{R}^3 \,|\, u \cdot v = w\} \\ \mathbb{R}(0) = 0^{\mathbb{R}} & = & 0 \in \mathbb{R} \\ \mathbb{R}(1) = 1^{\mathbb{R}} & = & a \in \mathbb{R} \end{array}$$

This defines the standard structure $\mathbb{R} = (\mathbb{R}, <^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, 0^{\mathbb{R}}, 1^{\mathbb{R}})$.

Observe that the symbols could in principle be interpreted in completely different, counterintuitive ways like

$$\begin{array}{rcl} \mathbb{R}'(\forall) & = & \mathbb{N} \\ \mathbb{R}'(<) & = & \{(u, v) \in \mathbb{N}^2 \,|\, u > v\} \\ \mathbb{R}'(+) & = & \{(u, v, w) \in \mathbb{N}^3 \,|\, u \cdot v = w\} \\ \mathbb{R}'(\cdot) & = & \{(u, v, w) \in \mathbb{N}^3 \,|\, u + v = w\} \\ \mathbb{R}'(0) & = & 1 \\ \mathbb{R}'(1) & = & 0 \end{array}$$

Example 21. Define the language of *Boolean algebras* by

$$S_{\mathrm{BA}} = \{\wedge, \vee, -, 0, 1\}$$

where $\wedge$ and $\vee$ are binary function symbols for "and" and "or", $-$ is a unary function symbol for "not", and 0 and 1 are constant symbols. A Boolean algebra of particular importance in logic is the algebra $\mathbb{B}$ of *truth values*. Let $B = |\mathbb{B}| = \{0, 1\}$ with $0 = \mathbb{B}(0)$ and $1 = \mathbb{B}(1)$. Define the operations and $= \mathbb{B}(\wedge)$, or $= \mathbb{B}(\vee)$, and not $= \mathbb{B}(-)$ by *operation tables* in analogy to standard multiplication tables:

and	0	1
0	0	0
1	0	1

,

or	0	1
0	0	1
1	1	1

, and

not	
0	1
1	0

.

Note that we use the non-exclusive "or" instead of the exclusive "either - or".

The notion of structure leads to some related definitions.

Definition 22. *Let $\mathfrak{A}$ be an S-structure and $\mathfrak{A}'$ be an S'-structure. Then $\mathfrak{A}$ is a* reduct *of $\mathfrak{A}'$, or $\mathfrak{A}'$ is an* expansion *of $\mathfrak{A}$, if $S \subseteq S'$ and $\mathfrak{A}' \upharpoonright (\{\forall\} \cup S) = \mathfrak{A}$.*

According to this definition, the additive group $(\mathbb{R}, +, 0)$ of reals is a reduct of the field $(\mathbb{R}, +, \cdot, 0, 1)$.

Definition 23. *Let $\mathfrak{A}$, $\mathfrak{B}$ be S-structures. Then $\mathfrak{A}$ is a* substructure *of $\mathfrak{B}$, $\mathfrak{A} \subseteq \mathfrak{B}$, if $\mathfrak{B}$ is a pointwise extension of $\mathfrak{A}$, i.e.,*

a) $A = |\mathfrak{A}| \subseteq |\mathfrak{B}|$*;*

b) for every n-ary relation symbol $R \in S$ holds $R^{\mathfrak{A}} = R^{\mathfrak{B}} \cap A^n$;

c) for every n-ary function symbol $f \in S$ holds $f^{\mathfrak{A}} = f^{\mathfrak{B}} \upharpoonright A^n$.

Definition 24. *Let $\mathfrak{A}, \mathfrak{B}$ be S-structures and $h: |\mathfrak{A}| \rightarrow |\mathfrak{B}|$. Then h is a* homomorphism *from $\mathfrak{A}$ into $\mathfrak{B}$, $h: \mathfrak{A} \rightarrow \mathfrak{B}$, if*

a) for every n-ary relation symbol $R \in S$ and for every $a_0, \ldots, a_{n-1} \in A$

$$R^{\mathfrak{A}}(a_0, \ldots, a_{n-1}) \textit{ implies } R^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1}));$$

b) for every n-ary function symbol $f \in S$ and for every $a_0, \ldots, a_{n-1} \in A$

$$f^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1})) = h(f^{\mathfrak{A}}(a_0, \ldots, a_{n-1})).$$

h is an embedding *of $\mathfrak{A}$ into $\mathfrak{B}$, $h: \mathfrak{A} \hookrightarrow \mathfrak{B}$, if moreover*

a) h is injective;

b) for every n-ary relation symbol $R \in S$ and for every $a_0, \ldots, a_{n-1} \in A$

$$R^{\mathfrak{A}}(a_0, \ldots, a_{n-1}) \textit{ iff } R^{\mathfrak{B}}(h(a_0), \ldots, h(a_{n-1})).$$

If h is also bijective, it is called an isomorphism*.*

An S-structure interprets the symbols in S. To interpret a formula in a structure one also has to interpret the (occuring) variables.

Definition 25. *Let S be a symbol set. An S-*model *is a function*

$$\mathfrak{M}: \{\forall\} \cup S \cup \mathrm{Var} \rightarrow V$$

such that $\mathfrak{M} \upharpoonright \{\forall\} \cup S$ is an S-structure and for all $n \in \mathbb{N}$ holds $\mathfrak{M}(v_n) \in |\mathfrak{M}|$. $\mathfrak{M}(v_n)$ is the interpretation of the variable v_n in $\mathfrak{M}$.

It will sometimes be important to modify a model $\mathfrak{M}$ at specific variables. For pairwise distinct variables $x_0, \ldots, x_{r-1}$ and $a_0, \ldots, a_{r-1} \in |\mathfrak{M}|$ define

$$\mathfrak{M}\frac{a_0 \ldots a_{r-1}}{x_0 \ldots x_{r-1}} = (\mathfrak{M} \setminus \{(x_0, \mathfrak{A}(x_0)), \ldots, (x_{r-1}, \mathfrak{A}(x_{r-1}))\}) \cup \{(x_0, a_0), \ldots, (x_{r-1}, a_{r-1})\}.$$

7 The satisfaction relation

We now define the semantics of the first-order language by interpreting terms and formulas in models.

Definition 26. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation *$\mathfrak{M}(t) \in |\mathfrak{M}|$ of a term $t \in T^S$ by recursion on the term calculus:*

a) for t a variable, $\mathfrak{M}(t)$ is already defined;

b) for an n-ary function symbol and terms $t_0, \ldots, t_{n-1} \in T^S$, let

$$\mathfrak{M}(f t_0 \ldots t_{n-1}) = f^{\mathfrak{A}}(\mathfrak{M}(t_0), \ldots, \mathfrak{M}(t_{n-1})).$$

This explains the interpretation of a term like $v_3^2 + v_{200}^3$ in the reals.

Definition 27. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation *$\mathfrak{M}(\varphi) \in \mathbb{B}$ of a formula $\varphi \in L^S$, where $\mathbb{B} = \{0, 1\}$ is the Boolean algebra of truth values, by recursion on the formula calculus:*

a) $\mathfrak{M}(\bot) = 0$ *;*

b) *for terms* $t_0, t_1 \in T^S$*:* $\mathfrak{M}(t_0 \equiv t_1) = 1$ *iff* $\mathfrak{M}(t_0) = \mathfrak{M}(t_1)$*;*

c) *for every* n*-ary relation symbol* $R \in S$ *and terms* $t_0, \ldots, t_1 \in T^S$

$$\mathfrak{M}(Rt_0 \ldots t_{n-1}) = 1 \textit{ iff } R^{\mathfrak{M}}(\mathfrak{M}(t_0), \ldots, \mathfrak{M}(t_{n-1}));$$

d) $\mathfrak{M}(\neg\varphi) = 1$ *iff* $\mathfrak{M}(\varphi) = 0$ *;*

e) $\mathfrak{M}(\varphi \rightarrow \psi) = 1$ *iff* $\mathfrak{M}(\varphi) = 1$ *implies* $\mathfrak{M}(\psi) = 1$*;*

f) $\mathfrak{M}(\forall v_n \varphi) = 1$ *iff for all* $a \in |\mathfrak{M}|$ *holds* $\mathfrak{M}\frac{a}{v_n}(\varphi) = 1$.

We write $\mathfrak{M} \vDash \varphi$ *instead of* $\mathfrak{M}(\varphi) = 1$. *We also say that* $\mathfrak{M}$ satisfies φ *or that* φ holds *in* $\mathfrak{M}$. *For* $\Phi \subseteq L^S$ *write* $\mathfrak{M} \vDash \Phi$ *iff* $\mathfrak{M} \vDash \varphi$ *for every* $\varphi \in \Phi$.

Definition 28. *Let* S *be a language and* $\Phi \subseteq L^S$. Φ *is* universally valid *if* Φ *holds in every* S*-model.* Φ *is* satisfiable *if there is an* S*-model* $\mathfrak{M}$ *such that* $\mathfrak{M} \vDash \Phi$.

The language extensions by the symbols $\vee$, $\wedge$, $\leftrightarrow$, $\exists$ is consistent with the expected meanings of the additional symbols:

Exercise 2. Prove:

a) $\mathfrak{M} \vDash (\varphi \vee \psi)$ iff $\mathfrak{M} \vDash \varphi$ *or* $\mathfrak{M} \vDash \psi$;

b) $\mathfrak{M} \vDash (\varphi \vee \psi)$ iff $\mathfrak{M} \vDash \varphi$ *and* $\mathfrak{M} \vDash \psi$;

c) $\mathfrak{M} \vDash (\varphi \leftrightarrow \psi)$ iff $\mathfrak{M} \vDash \varphi$ *is equivalent to* $\mathfrak{M} \vDash \psi$;

d) $\mathfrak{M} \vDash \exists v_n \varphi$ iff *there exists* $a \in |\mathfrak{M}|$ such that $\mathfrak{M}\frac{a}{v_n} \vDash \varphi$.

With the notion of $\vDash$ we can now formally define what it means for a structure to be a group or for a function to be differentiable. Before considering examples we make some auxiliary definitions and simplifications.

It is intuitively obvious that the interpretation of a term only depends on the occuring variables, and that satisfaction for a formula only depends on its free, non-bound variables.

Definition 29. *For* $t \in T^S$ *define* $\mathrm{var}(t) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on the term calculus:*

- $\mathrm{var}(x) = \{x\}$*;*
- $\mathrm{var}(c) = \emptyset$*;*
- $\mathrm{var}(ft_0 \ldots t_{n-1}) = \bigcup_{i<n} \mathrm{var}(t_i)$.

Definition 30. *Für* $\varphi \in L^S$ *define the set of* free variables $\mathrm{free}(\varphi) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on the formula calculus:*

- $\mathrm{free}(t_0 \equiv t_1) = \mathrm{var}(t_0) \cup \mathrm{var}(t_1)$*;*
- $\mathrm{free}(Rt_0 \ldots t_{n-1}) = \mathrm{var}(t_0) \cup \ldots \cup \mathrm{var}(t_{n-1})$*;*
- $\mathrm{free}(\neg\varphi) = \mathrm{free}(\varphi)$*;*
- $\mathrm{free}(\varphi \rightarrow \psi) = \mathrm{free}(\varphi) \cup \mathrm{free}(\psi)$.
- $\mathrm{free}(\forall x \varphi) = \mathrm{free}(\varphi) \setminus \{x\}$.

For $\Phi \subseteq L^S$ *define the set* $\mathrm{free}(\Phi)$ *of* free variables *as*

$$\mathrm{free}(\Phi) = \bigcup_{\varphi \in \Phi} \mathrm{free}(\varphi).$$

Example 31.

$$\begin{aligned}
\mathrm{free}(Ryx \rightarrow \forall y \neg y = z) &= \mathrm{free}(Ryx) \cup \mathrm{free}(\forall y \neg y = z) \\
&= \mathrm{free}(Ryx) \cup (\mathrm{free}(\neg y = z) \setminus \{y\}) \\
&= \mathrm{free}(Ryx) \cup (\mathrm{free}(y = z) \setminus \{y\}) \\
&= \{y, x\} \cup (\{y, z\} \setminus \{y\}) \\
&= \{y, x\} \cup \{z\} \\
&= \{x, y, z\}.
\end{aligned}$$

Definition 32.

a) *For* $n \in \mathbb{N}$ *let* $L_n^S = \{\varphi \in L^S \mid \text{free}(\varphi) \subseteq \{v_0, \ldots, v_{n-1}\}\}$.

b) $\varphi \in L^S$ *is an* S-sentence *if* $\text{free}(\varphi) = \emptyset$; L_0^S *is the set of* S*-sentences.*

Theorem 33. *Let* t *be an* S*-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be* S*-models with the same structure* $\mathfrak{M} \upharpoonright \{\forall\} \cup S = \mathfrak{M}' \upharpoonright \{\forall\} \cup S$ *and* $\mathfrak{M} \upharpoonright \text{var}(t) = \mathfrak{M}' \upharpoonright \text{var}(t)$. *Then* $\mathfrak{M}(t) = \mathfrak{M}'(t)$.

Theorem 34. *Let* t *be an* S*-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be* S*-models with the same structure* $\mathfrak{M} \upharpoonright \{\forall\} \cup S = \mathfrak{M}' \upharpoonright \{\forall\} \cup S$ *and* $\mathfrak{M} \upharpoonright \text{free}(t) = \mathfrak{M}' \upharpoonright \text{free}(t)$. *Then*

$$\mathfrak{M} \vDash \varphi \quad \textit{iff} \quad \mathfrak{M}' \vDash \varphi.$$

Proof. By induction on the formula calculus.
$\varphi = t_0 \equiv t_1$: Then $\text{var}(t_0) \cup \text{var}(t_1) = \text{free}(\varphi)$ and

$$\begin{aligned} \mathfrak{M} \vDash \varphi \ &\text{iff } \ \mathfrak{M}(t_0) = \mathfrak{M}(t_1) \\ &\text{iff } \ \mathfrak{M}'(t_0) = \mathfrak{M}'(t_1) \ \text{ by the previous Theorem,} \\ &\text{iff } \ \mathfrak{M}' \vDash \varphi. \end{aligned}$$

$\varphi = \psi \rightarrow \chi$ and assume the claim to be true for ψ and χ. Then

$$\begin{aligned} \mathfrak{M} \vDash \varphi \ &\text{iff } \ \mathfrak{M} \vDash \psi \text{ implies } \mathfrak{M} \vDash \chi \\ &\text{iff } \ \mathfrak{M}' \vDash \psi \text{ implies } \mathfrak{M}' \vDash \chi \text{ by the inductive assumption,} \\ &\text{iff } \ \mathfrak{M}' \vDash \varphi. \end{aligned}$$

$\varphi = \forall v_n \psi$ and assume the claim to be true for ψ. Then $\text{free}(\psi) \subseteq \text{free}(\varphi) \cup \{v_n\}$. For all $a \in A = |\mathfrak{M}|$: $\mathfrak{M}\frac{a}{v_n} \upharpoonright \text{free}(\psi) = \mathfrak{M}'\frac{a}{v_n} \upharpoonright \text{free}(\psi)$ and so

$$\begin{aligned} \mathfrak{M} \vDash \varphi \ &\text{iff } \ \text{for all } a \in A \text{ holds } \mathfrak{M}\frac{a}{v_n} \vDash \psi \\ &\text{iff } \ \text{for all } a \in A \text{ holds } \mathfrak{M}'\frac{a}{v_n} \vDash \psi \text{ by the inductive assumption,} \\ &\text{iff } \ \mathfrak{M}' \vDash \varphi. \end{aligned}$$

□

This allows further simplifications in notations for $\vDash$:

Definition 35. *Let* $\mathfrak{A}$ *be an* S*-structure and let* $(a_0, \ldots, a_{n-1})$ *be a sequence of elements of* A. *Let* t *be an* S*-term with* $\text{var}(t) \subseteq \{v_0, \ldots, v_{n-1}\}$. *Then define*

$$t^{\mathfrak{A}}[a_0, \ldots, a_{n-1}] = \mathfrak{M}(t),$$

where $\mathfrak{M} \supseteq \mathfrak{A}$ *is an* S*-model with* $\mathfrak{M}(v_0) = a_0, \ldots, \mathfrak{M}(v_{n-1}) = a_{n-1}$.
Let φ *be an* S*-formula with* $\text{free}(t) \subseteq \{v_0, \ldots, v_{n-1}\}$. *Then define*

$$\mathfrak{A} \vDash \varphi[a_0, \ldots, a_{n-1}] \quad \textit{iff} \quad \mathfrak{M} \vDash \varphi,$$

where $\mathfrak{M} \supseteq \mathfrak{A}$ *is an* S*-model with* $\mathfrak{M}(v_0) = a_0, \ldots, \mathfrak{M}(v_{n-1}) = a_{n-1}$.

In case $n = 0$ *also write* $t^{\mathfrak{A}}$ *instead of* $t^{\mathfrak{A}}[a_0, \ldots, a_{n-1}]$ *and* $\mathfrak{A} \vDash \varphi$ *instead of* $\mathfrak{A} \vDash \varphi[a_0, \ldots, a_{n-1}]$. *In this case we also say:* $\mathfrak{A}$ *is a* model *of* φ, $\mathfrak{A}$ satisfies φ *or* φ is true *in* $\mathfrak{A}$.

For $\Phi \subseteq L_0^S$ *a set of sentences also write*

$$\mathfrak{A} \vDash \Phi \quad \textit{iff for all} \quad \varphi \in \Phi \ \textit{holds}: \mathfrak{A} \vDash \varphi.$$

Example 36. *Groups.* $S_{Gr} := \{\circ, e\}$ with a binary function symbol$\circ$ and a constant symbol e is the *language of groups theory*. The group axioms are

a) $\forall v_0 \forall v_1 \forall v_2 \circ v_0 \circ v_1 v_2 \equiv \circ\circ v_0 v_1 v_2$;

b) $\forall v_0 \circ v_0 e \equiv v_0$;

c) $\forall v_0 \exists v_1 \circ v_0 v_1 \equiv e$.

This define the axiom set

$$\Phi_{\mathrm{Gr}} = \{\forall v_0 \forall v_1 \forall v_2 \circ v_0 \circ v_1 v_2 \equiv \circ\circ v_0 v_1 v_2,\ \forall v_0 \circ v_0\, e \equiv v_0,\ \forall v_0 \exists v_1 \circ v_0 v_1 \equiv e\}.$$

An S-structure $\mathfrak{G} = (G, *, k)$ satisfies Φ_{Gr} iff it is a group in the ordinary sense.

Definition 37. *Let S be a language and let $\Phi \subseteq L_0^S$ be a set of S-sentences. Then*

$$\mathrm{Mod}^S \Phi = \{\mathfrak{A} \,|\, \mathfrak{A} \textit{ is an } S\textit{-structure and } \mathfrak{A} \vDash \Phi\}$$

is the model class *of* Φ. *In case* $\Phi = \{\Phi\}$ *we also write* $\mathrm{Mod}^S \varphi$ *instead of* $\mathrm{Mod}^S \Phi$. *We also say that* Φ *is an* axiom system *for* $\mathrm{Mod}^S \Phi$, *or that* Φ axiomatizes *the class* $\mathrm{Mod}^S \Phi$.

Thus $\mathrm{Mod}^{S_{\mathrm{Gr}}} \Phi_{\mathrm{Gr}}$ is the model class of all groups. Model classes are studied in generality within *model theory* which is a branch of mathematical logic. For specific Φ the model class $\mathrm{Mod}^S \Phi$ is examined in subfields of mathematics: group theory, ring theory, graph theory, etc. Some typical questions questions are: Is $\mathrm{Mod}^S \Phi \neq \emptyset$, i.e., is Φ satisfiable? Can we extend $\mathrm{Mod}^S \Phi$ by adequate morphisms between models?

8 Logical implication and propositional connectives

Definition 38. *For a symbol set S and $\Phi \subseteq L^S$ and $\varphi \in L^S$ define that Φ* (logically) implies *φ ($\Phi \vDash \varphi$) iff every S-model $\mathfrak{I} \vDash \Phi$ is also a model of φ.*

Note that logical implication $\vDash$ is a relation between syntactical entities which is defined using the semantic notion of interpretation. We show that $\vDash$ satisfies certain syntactical laws. These laws correspond to the rules of a logical proof calculus.

Theorem 39. *Let S be a symbol set, $t \in T^S$, $\varphi, \psi \in L^S$, and $\Gamma, \Phi \subseteq L^S$. Then*

a) (Monotonicity) If $\Gamma \subseteq \Phi$ and $\Gamma \vDash \varphi$ then $\Phi \vDash \varphi$.

b) (Assumption property) If $\varphi \in \Gamma$ then $\Gamma \vDash \varphi$.

c) ($\rightarrow$-Introduction) If $\Gamma \cup \varphi \vDash \psi$ then $\Gamma \vDash \varphi \rightarrow \psi$.

d) ($\rightarrow$-Elimination) If $\Gamma \vDash \varphi$ and $\Gamma \vDash \varphi \rightarrow \psi$ then $\Gamma \vDash \psi$.

e) ($\bot$-Introduction) If $\Gamma \vDash \varphi$ and $\Gamma \vDash \neg\varphi$ then $\Gamma \vDash \bot$.

f) ($\bot$-Elimination) If $\Gamma \cup \{\neg\varphi\} \vDash \bot$ then $\Gamma \vDash \varphi$.

g) ($\equiv$-Introduction) $\Gamma \vDash t \equiv t$.

Proof. f) Assume $\Gamma \cup \{\neg\varphi\} \vDash \bot$. Consider an S-model with $\mathfrak{M} \vDash \Gamma$. Assume that $\mathfrak{M} \nvDash \varphi$. Then $\mathfrak{M} \vDash \neg\varphi$. $\mathfrak{M} \vDash \Gamma \cup \{\neg\varphi\}$, and by assumption, $\mathfrak{M} \vDash \bot$. But by the definition of the satisfaction relation, this is false. Thus $\mathfrak{M} \vDash \varphi$. Thus $\Gamma \vDash \varphi$. □

9 Substitution and quantification rules

To prove further rules for equalities and quantification, we first have to formalize *substitution*.

Definition 40. *For a term $s \in T^S$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$ define the* (simultaneous) substitution

$$s \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$$

of $t_0,\ldots,t_{r-1}$ *for* $x_0,\ldots,x_{r-1}$ *by recursion:*

a) $x\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=\begin{cases}x, \text{ if } x\neq x_0,\ldots,x\neq x_{r-1}\\ t_i, \text{ if } x=x_i\end{cases}$ *for all variables* x*;*

b) $c\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=c$ *for all constant symbols* c*;*

c) $(fs_0\ldots s_{n-1})\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=fs_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}\ldots s_{n-1}\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *for all* n*-ary function symbols* f*.*

Note that the simultaneous substitution

$$s\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$$

is in general different from a succesive substitution

$$s\frac{t_0}{x_0}\frac{t_1}{x_1}\ldots\frac{t_{r-1}}{x_{r-1}}$$

which depends on the order of substitution. E.g., $x\frac{yx}{xy}=y$, $x\frac{y}{x}\frac{x}{y}=y\frac{x}{y}=x$ and $x\frac{x}{y}\frac{y}{x}=x\frac{y}{x}=y$.

Definition 41. *For a formula* $\varphi\in L^S$*, pairwise distinct variables* $x_0,\ldots,x_{r-1}$ *and terms* $t_0,\ldots,t_{r-1}\in T^S$ *define the* (simultaneous) substitution

$$\varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$$

of $t_0,\ldots,t_{r-1}$ *for* $x_0,\ldots,x_{r-1}$ *by recursion:*

a) $(s_0\equiv s_1)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=s_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}\equiv s_1\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *for all terms* $s_0,s_1\in T^S$*;*

b) $(Rs_0\ldots s_{n-1})\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=Rs_0\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}\ldots s_{n-1}\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *for all* n*-ary relation symbols* R *and terms* $s_0,\ldots,s_{n-1}\in T^S$*;*

c) $(\neg\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=\neg(\varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}})$*;*

d) $(\varphi\to\psi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=(\varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}\to\psi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}})$*;*

e) *for* $(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *distinguish two cases:*

- *if* $x\in\{x_0,\ldots,x_{r-1}\}$*, assume that* $x=x_0$ *. Choose* $i\in\mathbb{N}$ *minimal such that* $u=v_i$ *does not occur in* $\forall x\varphi$*,* $t_0,\ldots,t_{r-1}$ *and* $x_0,\ldots,x_{r-1}$*. Then set*

$$(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=\forall u(\varphi\frac{t_1\ldots t_{r-1}\,u}{x_1\ldots x_{r-1}\,x}).$$

- *if* $x\notin\{x_0,\ldots,x_{r-1}\}$*, choose* $i\in\mathbb{N}$ *minimal such that* $u=v_i$ *does not occur in* $\forall x\varphi$*,* $t_0,\ldots,t_{r-1}$ *and* $x_0,\ldots,x_{r-1}$ *and set*

$$(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=\forall u(\varphi\frac{t_0\ldots t_{r-1}\,u}{x_0\ldots x_{r-1}\,x}).$$

The following substitution theorem shows that syntactic substitution corresponds semantically to a (simultaneous) modification of assignments by interpreted terms.

Theorem 42. *Consider an* S*-model* $\mathfrak{M}$*, pairwise distinct variables* $x_0,\ldots,x_{r-1}$ *and terms* $t_0,\ldots,t_{r-1}\in T^S$*.*

a) *If* $s\in T^S$ *is a term,*

$$\mathfrak{M}(s\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}})=\mathfrak{M}\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})}{x_0\ldots x_{r-1}}(s).$$

b) *If* $\varphi\in L^S$ *is a formula,*

$$\mathfrak{M}\vDash\varphi\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} \text{ iff } \mathfrak{M}\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})}{x_0\ldots x_{r-1}}\vDash\varphi.$$

Proof. By induction on the complexities of s and φ.
a) *Case 1*: $s = x$.
Case 1.1: $x \notin \{x_0, ..., x_{r-1}\}$. Then

$$\mathfrak{M}(x \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}}) = \mathfrak{M}(x) = \mathfrak{M} \frac{\mathfrak{M}(t_0) ... \mathfrak{M}(t_{r-1})}{x_0 ... x_{r-1}}(x).$$

Case 1.2: $x = x_i$. Then

$$\mathfrak{M}(x \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}}) = \mathfrak{M}(t_i) = \mathfrak{M} \frac{\mathfrak{M}(t_0) ... \mathfrak{M}(t_{r-1})}{x_0 ... x_{r-1}}(x).$$

Case 2: $s = c$ is a constant symbol. Then

$$\mathfrak{M}(c \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}}) = \mathfrak{M}(c) = \mathfrak{M} \frac{\mathfrak{M}(t_0) ... \mathfrak{M}(t_{r-1})}{x_0 ... x_{r-1}}(c).$$

Case 3: $s = fs_0 ... s_{n-1}$ where $f \in S$ is an n-ary function symbol and the terms $s_0, ..., s_{n-1} \in T^S$ satisfy the theorem. Then

$$\begin{aligned}
\mathfrak{M}((fs_0 ... s_{n-1}) \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}}) &= \mathfrak{M}(fs_0 \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}} ... s_{n-1} \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}}) \\
&= \mathfrak{M}(f)(\mathfrak{M}(s_0 \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}}), ..., \mathfrak{M}(s_{n-1} \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}})) \\
&= \mathfrak{M}(f)(\mathfrak{M} \frac{\mathfrak{M}(t_0) ... \mathfrak{M}(t_{r-1})}{x_0 ... x_{r-1}}(s_0), ..., \mathfrak{M} \frac{\mathfrak{M}(t_0) ... \mathfrak{M}(t_{r-1})}{x_0 ... x_{r-1}}(s_{n-1})) \\
&= \mathfrak{M} \frac{\mathfrak{M}(t_0) .... \mathfrak{M}(t_{r-1})}{x_0 ... x_{r-1}}(fs_0 ... s_{n-1}).
\end{aligned}$$

Assuming that the substitution theorem is proved for terms, we prove
b) *Case 4*: $\varphi = s_0 \equiv s_1$. Then

$$\begin{aligned}
\mathfrak{I} \vDash (s_0 \equiv s_1) \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}} \quad &\text{iff} \quad \mathfrak{I} \vDash (s_0 \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}} \equiv s_1 \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}}) \\
&\text{iff} \quad \mathfrak{I}(s_0 \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}}) = \mathfrak{I}(s_1 \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}}) \\
&\text{iff} \quad \mathfrak{I} \frac{\mathfrak{I}(t_0) .... \mathfrak{I}(t_{r-1})}{x_0 ... x_{r-1}}(s_0) = \mathfrak{I} \frac{\mathfrak{I}(t_0) .... \mathfrak{I}(t_{r-1})}{x_0 ... x_{r-1}}(s_1) \\
&\text{iff} \quad \mathfrak{I} \frac{\mathfrak{I}(t_0) .... \mathfrak{I}(t_{r-1})}{x_0 ... x_{r-1}} \vDash s_0 \equiv s_1 .
\end{aligned}$$

Propositional connectives of formulas like $\neg$ and $\rightarrow$ behave similar to terms, so we only consider universal quantification:
Case 5: $\varphi = (\forall x \psi) \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}}$, assuming that the theorem holds for ψ.
Case 5.1: $x = x_0$. Choose $i \in \mathbb{N}$ minimal such that $u = v_i$ does not occur in $\forall x \varphi$, $t_0, ..., t_{r-1}$ and $x_0, ..., x_{r-1}$. Then

$$(\forall x \varphi) \frac{t_0 .... t_{r-1}}{x_0 ... x_{r-1}} = \forall u \, (\varphi \frac{t_1 ... t_{r-1} \, u}{x_1 ... x_{r-1} \, x}).$$

$$\begin{aligned}
\mathfrak{M} \vDash (\forall x \varphi) \frac{t_0 ... t_{r-1}}{x_0 ... x_{r-1}} \quad &\text{iff} \quad \mathfrak{M} \vDash \forall u \, (\varphi \frac{t_1 ... t_{r-1} \, u}{x_1 ... x_{r-1} \, x}) \\
&\text{iff} \quad \text{for all } a \in M \text{ holds } \mathfrak{M}\frac{a}{u} \vDash \varphi \frac{t_1 ... t_{r-1} \, u}{x_1 ... x_{r-1} \, x} \\
&\qquad \text{(definition of } \vDash) \\
&\text{iff} \quad \text{for all } a \in M \text{ holds} \\
&\qquad (\mathfrak{M}\frac{a}{u}) \frac{\mathfrak{M}\frac{a}{u}(t_1) ... \mathfrak{M}\frac{a}{u}(t_{r-1}) \, \mathfrak{M}\frac{a}{u}(u)}{x_1 ... x_{r-1} \, x} \vDash \varphi \\
&\qquad \text{(inductive hypothesis for } \varphi) \\
&\text{iff} \quad \text{for all } a \in M \text{ holds}
\end{aligned}$$

$$\begin{array}{ll}
& (\mathfrak{M}\frac{a}{u})\frac{\mathfrak{M}(t_1)\ldots\mathfrak{M}(t_{r-1})\,a}{x_1\ldots x_{r-1}\,x}\vDash\varphi \\
& \text{(since } u \text{ does not occur in } t_i\text{)} \\
\text{iff} & \text{for all } a\in M \text{ holds} \\
& \mathfrak{M}\frac{\mathfrak{M}(t_1)\ldots\mathfrak{M}(t_{r-1})\,a}{x_1\ldots x_{r-1}\,x}\vDash\varphi \\
& \text{(since } u \text{ does not occur in } \varphi\text{)} \\
\text{iff} & \text{for all } a\in M \text{ holds} \\
& (\mathfrak{M}\frac{\mathfrak{M}(t_1)\ldots\mathfrak{M}(t_{r-1})}{x_1\ldots x_{r-1}})\frac{a}{x}\vDash\varphi \\
& \text{(by simple properties of assignments)} \\
\text{iff} & (\mathfrak{M}\frac{\mathfrak{M}(t_1)\ldots\mathfrak{M}(t_{r-1})}{x_1\ldots x_{r-1}})\vDash\forall x\varphi \\
& \text{(definition of } \vDash\text{)} \\
\text{iff} & (\mathfrak{M}\frac{\mathfrak{M}(t_0)\,\mathfrak{M}(t_1)\ldots\mathfrak{M}(t_{r-1})}{x_0\,x_1\ldots x_{r-1}})\vDash\forall x\varphi \\
& \text{(since } x=x_0 \text{ is not free in } \forall x\varphi\text{).}
\end{array}$$

Case 5.2: $x\notin\{x_0,\ldots,x_{r-1}\}$. Then proceed similarly. Choose $i\in\mathbb{N}$ minimal such that $u=v_i$ does not occur in $\forall x\varphi$, $t_0,\ldots.,t_{r-1}$ and $x_0,\ldots,x_{r-1}$. Then

$$(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}=\forall u\,(\varphi\frac{t_0\ldots t_{r-1}\,u}{x_0\ldots x_{r-1}\,x}).$$

$$\begin{array}{rll}
\mathfrak{M}\vDash(\forall x\varphi)\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} & \text{iff} & \mathfrak{M}\vDash\forall u\,(\varphi\frac{t_0\ldots t_{r-1}\,u}{x_0\ldots x_{r-1}\,x}) \\
& \text{iff} & \text{for all } a\in M \text{ holds } \mathfrak{M}\frac{a}{u}\vDash\varphi\frac{t_0\ldots t_{r-1}\,u}{x_0\ldots x_{r-1}\,x} \\
& & \text{(definition of } \vDash\text{)} \\
& \text{iff} & \text{for all } a\in M \text{ holds} \\
& & (\mathfrak{M}\frac{a}{u})\frac{\mathfrak{M}\frac{a}{u}(t_0)\ldots\mathfrak{M}\frac{a}{u}(t_{r-1})\,\mathfrak{M}\frac{a}{u}(u)}{x_0\ldots x_{r-1}\,x}\vDash\varphi \\
& & \text{(inductive hypothesis for } \varphi\text{)} \\
& \text{iff} & \text{for all } a\in M \text{ holds} \\
& & (\mathfrak{M}\frac{a}{u})\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})\,a}{x_0\ldots x_{r-1}\,x}\vDash\varphi \\
& & \text{(since } u \text{ does not occur in } t_i\text{)} \\
& \text{iff} & \text{for all } a\in M \text{ holds} \\
& & \mathfrak{M}\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})\,a}{x_0\ldots x_{r-1}\,x}\vDash\varphi \\
& & \text{(since } u \text{ does not occur in } \varphi\text{)} \\
& \text{iff} & \text{for all } a\in M \text{ holds} \\
& & (\mathfrak{M}\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})}{x_0\ldots x_{r-1}})\frac{a}{x}\vDash\varphi \\
& & \text{(by simple properties of assignments)} \\
& \text{iff} & (\mathfrak{M}\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})}{x_0\ldots x_{r-1}})\vDash\forall x\varphi \\
& & \text{(definition of } \vDash\text{)}
\end{array}$$

□

We can now formulate further properties of the $\vDash$ relation.

Theorem 43. *Let S be a language. Let x,y be variables, $t,t'\in T^S$, $\varphi\in L^S$, and $\Gamma\subseteq L^S$. Then:*

a) *($\forall$-Introduction) If $\Gamma\vDash\varphi\frac{y}{x}$ and $y\notin\mathrm{free}(\Gamma\cup\{\forall x\varphi\})$ then $\Gamma\vDash\forall x\varphi$.*

b) *($\forall$-elimination) If* $\Gamma \vDash \forall x \varphi$ *then* $\Gamma \vDash \varphi \frac{t}{x}$.

c) *($\equiv$-Elimination or substitution) If* $\Gamma \vDash \varphi \frac{t}{x}$ *and* $\Gamma \vDash t \equiv t'$ *then* $\Gamma \vDash \varphi \frac{t'}{x}$.

Proof. a) Let $\Gamma \vDash \varphi \frac{y}{x}$ and $y \notin \text{free}(\Gamma \cup \{\forall x \varphi\})$. Consider an S-model $\mathfrak{I}$ with $\mathfrak{I} \vDash \Gamma$. Let $a \in A = |\mathfrak{I}|$. Since $y \notin \text{free}(\Gamma)$, $\mathfrak{I}\frac{a}{y} \vDash \Gamma$. By assumption, $\mathfrak{I}\frac{a}{y} \vDash \varphi \frac{y}{x}$. By the substitution theorem,

$$(\mathfrak{I}\frac{a}{y})\frac{\mathfrak{I}\frac{a}{y}(y)}{x} \vDash \varphi \text{ and so } (\mathfrak{I}\frac{a}{y})\frac{a}{x} \vDash \varphi$$

Case 1: $x = y$. Then $\mathfrak{I}\frac{a}{x} \vDash \varphi$.
Case 2: $x \neq y$. Then $\mathfrak{I}\frac{a\,a}{y\,x} \vDash \varphi$, and since $y \notin \text{free}(\varphi)$ we have $\mathfrak{I}\frac{a}{x} \vDash \varphi$.

Thus $\mathfrak{I} \vDash \forall x \varphi$. Thus $\Gamma \vDash \forall x \varphi$.

b) Let $\Gamma \vDash \forall x \varphi$. Consider an Smodel $\mathfrak{I}$ with $\mathfrak{I} \vDash \Gamma$. For all $a \in A = |\mathfrak{I}|$ holds $\mathfrak{I}\frac{a}{x} \vDash \varphi$. In particular $\mathfrak{I}\frac{\mathfrak{I}(t)}{x} \vDash \varphi$. By the substitution theorem, $\mathfrak{I} \vDash \varphi \frac{t}{x}$. Thus $\Gamma \vDash \varphi \frac{t}{x}$.

c) Let $\Gamma \vDash \varphi \frac{t}{x}$ and $\Gamma \vDash t \equiv t'$. Consider an S-model $\mathfrak{I}$ mit $\mathfrak{I} \vDash \Gamma$. By assumption $\mathfrak{I} \vDash \varphi \frac{t}{x}$ and $\mathfrak{I} \vDash t \equiv t'$. By the substitution theorem

$$\mathfrak{I}\frac{\mathfrak{I}(t)}{x} \vDash \varphi.$$

Since $\mathfrak{I}(t) = \mathfrak{I}(t')$,

$$\mathfrak{I}\frac{\mathfrak{I}(t')}{x} \vDash \varphi$$

and again by the substitution theorem

$$\mathfrak{I} \vDash \varphi \frac{t'}{x}.$$

Thus $\Gamma \vDash \varphi \frac{t'}{x}$. □

Note that in proving these proof rules we have used corresponding forms of arguments in the language of our discourse. This "circularity" is a general feature in formalizations of logic.

10 A sequent calculus

We can put the rules of implication established in the previous two sections in the form of a calculus which leads from correct implications $\Phi \vDash \varphi$ to further correct implications $\Phi' \vDash \varphi'$. Our *sequent calculus* will work on finite *sequents* $(\varphi_0, \dots, \varphi_{n-1}, \varphi_n)$ of formulas, whose intuition is that $\{\varphi_0, \dots, \varphi_{n-1}\}$ implies φ_n. The Gödel completeness theorem shows that these rules actually generate the implication relation $\vDash$. Fix a language S for this section.

Definition 44. *A finite sequence* $(\varphi_0, \dots, \varphi_{n-1}, \varphi_n)$ *is called a* sequent. *The initial segment* $\Gamma = (\varphi_0, \dots, \varphi_{n-1})$ *is the* antecedent *and* φ_n *is the* succedent *of the sequent. We usually write* $\varphi_0 \dots \varphi_{n-1}\ \varphi_n$ *or* $\Gamma\, \varphi_n$ *instead of* $(\varphi_0, \dots, \varphi_{n-1}, \varphi_n)$. *To emphasize the last element of the antecedent we may also denote the sequent by* $\Gamma'\, \varphi_{n-1}\, \varphi_n$ *with* $\Gamma' = (\varphi_0, \dots, \varphi_{n-2})$.

A sequent $\varphi_0 \dots \varphi_{n-1}\, \varphi$ *is* correct *if* $\{\varphi_0 \dots \varphi_{n-1}\} \vDash \varphi$.

Definition 45. *The* sequent calculus *consists of the following (sequent-)rules:*

- *monotonicity* (MR) $\dfrac{\Gamma \quad\quad \varphi}{\Gamma \quad \psi \quad \varphi}$
- *assumption* (AR) $\dfrac{}{\Gamma \quad \varphi \quad \varphi}$
- *$\to$-introduction* $(\to I)$ $\dfrac{\Gamma \quad \varphi \quad \psi}{\Gamma \quad\quad \varphi \to \psi}$
- *$\to$-elimination* $(\to E)$ $\dfrac{\begin{matrix}\Gamma & \varphi \\ \Gamma & \varphi \to \psi\end{matrix}}{\Gamma \quad \psi}$

– $\bot$-*introduction* ($\bot I$) $\dfrac{\begin{matrix}\Gamma & \varphi\\ \Gamma & \neg\varphi\end{matrix}}{\Gamma\ \ \bot}$

– $\bot$-*elimination* ($\bot E$) $\dfrac{\Gamma\ \ \neg\varphi\ \ \bot}{\Gamma\ \ \ \ \ \ \varphi}$

– $\forall$-*introduction* ($\forall I$) $\dfrac{\Gamma\ \ \varphi\frac{y}{x}}{\Gamma\ \ \forall x\varphi}$, *if* $y \notin \mathrm{free}(\Gamma \cup \{\forall x\varphi\})$

– $\forall$-*elimination* ($\forall E$) $\dfrac{\Gamma\ \ \forall x\varphi}{\Gamma\ \ \varphi\frac{t}{x}}$, *if* $t \in T^S$

– $\equiv$-*introduction* ($\equiv I$) $\dfrac{}{\Gamma\ \ t \equiv t}$, *if* $t \in T^S$

– $\equiv$-*elimination* ($\equiv E$) $\dfrac{\begin{matrix}\Gamma & \varphi\frac{t}{x}\\ \Gamma & t\equiv t'\end{matrix}}{\Gamma\ \ \varphi\frac{t'}{x}}$

The deduction relation *is the smallest subset* $\vdash \subseteq \mathrm{Seq}(S)$ *of the set of sequents which is closed under these rules. We write* $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ *instead of* $\varphi_0 \ldots \varphi_{n-1}\, \varphi \in \vdash$. *For* Φ *an arbitrary set of formulas define* $\Phi \vdash \varphi$ *iff there are* $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ *such that* $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$. *We say that* φ *can be* deduced *or* derived *from* $\varphi_0 \ldots \varphi_{n-1}$ *or* Φ, *resp. We also write* $\vdash\varphi$ *instead of* $\emptyset \vdash \varphi$ *and say that* φ *is a* tautology.

Theorem 46. *A formula* $\varphi \in L^S$ *is derivable from* $\Gamma = \varphi_0 \ldots \varphi_{n-1}$ ($\Gamma \vdash \varphi$) *iff there is a* derivation *or a* formal proof

$$(\Gamma_0\varphi_0, \Gamma_1\varphi_1, \ldots, \Gamma_{k-1}\varphi_{k-1})$$

of $\Gamma\,\varphi = \Gamma_{k-1}\varphi_{k-1}$, *in which every sequent* $\Gamma_i\varphi_i$ *is generated by a sequent rule from sequents* $\Gamma_{i_0}\varphi_{i_0}, \ldots, \Gamma_{i_{n-1}}\varphi_{i_{n-1}}$ *with* $i_0, \ldots, i_{n-1} < i$.

We usually write the derivation $(\Gamma_0\varphi_0, \Gamma_1\varphi_1, \ldots, \Gamma_{k-1}\varphi_{k-1})$ *as a vertical scheme*

$$\begin{array}{ll}\Gamma_0 & \varphi_0\\ \Gamma_1 & \varphi_1\\ \vdots & \\ \Gamma_{k-1} & \varphi_{k-1}\end{array}$$

where we may also mark rules and other remarks along the course of the derivation.

In our theorems on the laws of implication we have already shown:

Theorem 47. *The sequent calculus is* correct, *i.e., every rule of the sequent calculus leads from correct sequents to correct sequents. Thus every derivable sequent is correct. This means that*

$$\vdash \subseteq \models.$$

The converse inclusion corresponds to

Definition 48. *The sequent calculus is* complete *if* $\models \subseteq \vdash$.

The Gödel completeness theorem proves the completeness of the sequent calculus. The definition of $\vdash$ immediately implies the following *finiteness* or *compactness theorem*.

Theorem 49. *Let* $\Phi \subseteq L^S$ *and* $\varphi \in \Phi$. *Then* $\Phi \vdash \varphi$ *iff there is a finite subset* $\Phi_0 \subseteq \Phi$ *such that* $\Phi_0 \vdash \varphi$.

After proving the completeness theorem, such structural properties carry over to the implication relation $\models$.

11 Derivable sequent rules

The composition of rules of the sequent calculus yields *derived sequent rules* which are again correct. First note:

Lemma 50. *Assume that*

$$\begin{array}{ll} \Gamma & \varphi_0 \\ \vdots & \\ \Gamma & \varphi_{k-1} \\ \hline \Gamma & \varphi_k \end{array}$$

is a derived rule of the sequent calculus. Then

$$\begin{array}{ll} \Gamma_0 & \varphi_0 \\ \vdots & \\ \Gamma_{k-1} & \varphi_{k-1} \\ \hline \Gamma & \varphi_k \end{array} \text{, where } \Gamma_0, \ldots, \Gamma_{k-1} \text{ are initial sequences of } \Gamma$$

is also a derived rule of the sequent calculus.

Proof. This follows immediately from iterated applications of the monotonicity rule. □

We now list several derived rules.

11.1 Auxiliary rules

We write the derivation of rules as proofs in the sequent calculus where the premisses of the derivation are written above the upper horizontal line and the conclusion as last row.

ex falso quodlibet $\dfrac{\Gamma \;\; \bot}{\Gamma \;\; \varphi}$:

$$\begin{array}{llll} 1. & \Gamma & & \bot \\ \hline 2. & \Gamma & \neg\varphi & \bot \\ \hline 3. & \Gamma & & \varphi \end{array}$$

$\neg$-*Introduction* $\dfrac{\Gamma \;\; \varphi \;\; \bot}{\Gamma \;\;\;\; \neg\varphi}$:

$$\begin{array}{lllll} 1. & \Gamma & \varphi & & \bot \\ \hline 2. & \Gamma & & & \varphi \to \bot \\ 3. & \Gamma & \neg\neg\varphi & & \neg\neg\varphi \\ 4. & \Gamma & \neg\neg\varphi & \neg\varphi & \neg\varphi \\ 5. & \Gamma & \neg\neg\varphi & \neg\varphi & \bot \\ 6. & \Gamma & \neg\neg\varphi & & \varphi \\ 7. & \Gamma & \neg\neg\varphi & & \bot \\ \hline 8. & \Gamma & & & \neg\varphi \end{array}$$

$$\begin{array}{llll} 1. & \Gamma & & \neg\varphi \\ \hline 2. & \Gamma & \varphi & \varphi \\ 3. & \Gamma & \varphi & \bot \\ 4. & \Gamma & \varphi & \psi \\ \hline 5. & \Gamma & & \varphi \to \psi \end{array}$$

$$\begin{array}{llll} 1. & \Gamma & & \psi \\ \hline 2. & \Gamma & \varphi & \psi \\ \hline 3. & \Gamma & & \varphi \to \psi \end{array}$$

Cut rule

1.	Γ		φ
2.	Γ	φ	ψ
3.	Γ		$\varphi \rightarrow \psi$
4.	Γ		ψ

Contraposition

1.	Γ	φ		ψ
2.	Γ			$(\varphi \rightarrow \psi)$
3.	Γ	$\neg\psi$	φ	$(\varphi \rightarrow \psi)$
4.	Γ	$\neg\psi$	φ	φ
5.	Γ	$\neg\psi$	φ	ψ
6.	Γ	$\neg\psi$	φ	$\neg\psi$
7.	Γ	$\neg\psi$	φ	$\perp$
8.	Γ	$\neg\psi$		$\neg\varphi$

11.2 Introduction and elimination of $\vee, \wedge, \ldots$

$\vee$-*Introduction*

1.	Γ		φ
2.	Γ	$\neg\varphi$	$\neg\varphi$
3.	Γ	$\neg\varphi$	$\perp$
4.	Γ	$\neg\varphi$	ψ
5.	Γ		$\neg\varphi \rightarrow \psi$
6.	Γ		$\varphi \vee \psi$

$\vee$-*Introduction*

1.	Γ		ψ
2.	Γ	$\neg\varphi$	ψ
3.	Γ		$\neg\varphi \rightarrow \psi$
4.	Γ		$\varphi \vee \psi$

$\vee$-*Elimination*

1.	Γ			$\varphi \vee \psi$
2.	Γ			$\varphi \rightarrow \chi$
3.	Γ			$\psi \rightarrow \chi$
4.	Γ			$\neg\varphi \rightarrow \psi$
5.	Γ	$\neg\chi$		$\neg\chi$
6.	Γ	$\neg\chi$	φ	φ
7.	Γ	$\neg\chi$	φ	χ
8.	Γ	$\neg\chi$	φ	$\perp$
9.	Γ	$\neg\chi$		$\neg\varphi$
10.	Γ	$\neg\chi$		ψ
11.	Γ	$\neg\chi$		χ
12.	Γ	$\neg\chi$		$\perp$
13.	Γ			χ

$\wedge$-*Introduction*

1.	Γ		φ
2.	Γ		ψ
3.	Γ	$\varphi \rightarrow \neg\psi$	$\varphi \rightarrow \neg\psi$
4.	Γ	$\varphi \rightarrow \neg\psi$	$\neg\psi$
4.	Γ	$\varphi \rightarrow \neg\psi$	$\perp$
5.	Γ		$\neg(\varphi \rightarrow \neg\psi)$
6.	Γ		$\varphi \wedge \psi$

$\wedge$-*Elimination*

1.	Γ		$\varphi \wedge \psi$
2.	Γ		$\neg(\varphi \rightarrow \neg\psi)$
3.	Γ	$\neg\varphi$	$\neg\varphi$
4.	Γ	$\neg\varphi$	$\varphi \rightarrow \neg\psi$
5.	Γ	$\neg\varphi$	$\perp$
6.	Γ		φ

$\wedge$-*Elimination*

1.	Γ		$\varphi \wedge \psi$
2.	Γ		$\neg(\varphi \rightarrow \neg\psi)$
3.	Γ	$\neg\psi$	$\neg\psi$
4.	Γ	$\neg\psi$	$\varphi \rightarrow \neg\psi$
5.	Γ	$\neg\varphi$	$\perp$
6.	Γ		φ

$\exists$-*Introduction*

1.	Γ		$\varphi\frac{t}{x}$
2.	Γ	$\forall x \neg\varphi$	$\forall x \neg\varphi$
3.	Γ	$\forall x \neg\varphi$	$\neg\varphi\frac{t}{x}$
4.	Γ	$\forall x \neg\varphi$	$\perp$
5.	Γ		$\neg\forall x \neg\varphi$
6.	Γ		$\exists x\varphi$

$\exists$-*Elimination*

1.	Γ		$\exists x\varphi$	
2.	Γ	$\varphi\frac{y}{x}$	ψ	where $y \notin \text{free}(\Gamma \cup \{\exists x\varphi, \psi\})$
3.	Γ		$\neg\forall x \neg\varphi$	
4.	Γ	$\neg\psi$	$\neg\varphi\frac{y}{x}$	
5.	Γ	$\neg\psi$	$\forall x \neg\varphi$	
6.	Γ	$\neg\psi$	$\perp$	
7.	Γ		ψ	

11.3 Manipulations of antecedents

We derive rules which show that the formulas in the antecedent may be permuted arbitrarily, showing that only the *set* of antecedent formulas is relevant.

Transpositions of premisses

1.	Γ	φ	ψ	χ
2.	Γ	φ		$\psi \rightarrow \chi$
3.	Γ			$\varphi \rightarrow (\psi \rightarrow \chi)$
4.	Γ	ψ		ψ
5.	Γ	ψ	φ	φ
6.	Γ	ψ	φ	$\psi \rightarrow \chi$
7.	Γ	ψ	φ	χ

Doublication of premisses

1.	Γ	φ		ψ
2.	Γ	φ	φ	ψ

Elimination of double premisses

1.	Γ	φ	φ	ψ
2.	Γ	φ		$\varphi \rightarrow \psi$
3.	Γ			$\varphi \rightarrow (\varphi \rightarrow \psi)$
4.	Γ	φ		φ
5.	Γ	φ		ψ

Iterated applications of these rules yield:

Lemma 51. *Let $\varphi_0 \ldots \varphi_{m-1}$ and $\psi_0 \ldots \psi_{n-1}$ be antecedents such that*

$$\{\varphi_0, \ldots, \varphi_{m-1}\} = \{\psi_0, \ldots, \psi_{n-1}\}$$

and $\chi \in L^S$. Then

$$\frac{\varphi_0 \;\ldots\; \varphi_{m-1} \;\; \chi}{\psi_0 \;\ldots\; \psi_{n-1} \;\; \chi}$$

is a derived rule.

11.4 Examples of formal proofs

We give some examples of formal proofs which show that within the proof calculus $\equiv$ is an equivalence relation.

Lemma 52. *We prove the following tautologies:*

a) *Reflexivity:* $\vdash \forall x\, x \equiv x$

b) *Symmetry:* $\vdash \forall x \forall y (x \equiv y \rightarrow y \equiv x)$

c) *Transitivity:* $\vdash \forall x \forall y \forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z)$

Proof. a)

$$\frac{x \equiv x}{\forall x\, x \equiv x}$$

b)

$x \equiv y$	$x \equiv y$
$x \equiv y$	$x \equiv x$
$x \equiv y$	$(z \equiv x)\frac{x}{z}$
$x \equiv y$	$(z \equiv x)\frac{y}{x}$
$x \equiv y$	$y \equiv x$
	$x \equiv y \rightarrow y \equiv x$
	$\forall y (x \equiv y \rightarrow y \equiv x)$
	$\forall x \forall y (x \equiv y \rightarrow y \equiv x)$

c)

$x \equiv y \wedge y \equiv z$	$x \equiv y \wedge y \equiv z$
$x \equiv y \wedge y \equiv z$	$x \equiv y$
$x \equiv y \wedge y \equiv z$	$(x \equiv w)\frac{y}{w}$
$x \equiv y \wedge y \equiv z$	$y \equiv z$
$x \equiv y \wedge y \equiv z$	$(x \equiv w)\frac{z}{w}$
$x \equiv y \wedge y \equiv z$	$x \equiv z$
	$x \equiv y \wedge y \equiv z \rightarrow x \equiv z$
	$\forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z)$
	$\forall y \forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z)$
	$\forall x \forall y \forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z)$

□

We show moreover that $\equiv$ is a *congruence relation* from the perspective of $\vdash$.

Theorem 53. *Let* $\varphi \in L^S$ *and* $t_0, \ldots, t_{n-1}, t'_0, \ldots, t'_{n-1} \in T^S$. *Then*

$$\vdash t_0 \equiv t'_0 \wedge \ldots \wedge t_{n-1} \equiv t'_{n-1} \rightarrow (\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \leftrightarrow \varphi \frac{t'_0 \ldots t'_{n-1}}{v_0 \ldots v_{n-1}}).$$

Proof. Choose pairwise distinct "new" variables $u_0, \ldots, u_{n-1}$. Then

$$\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} = \varphi \frac{u_0}{v_0} \frac{u_1}{v_1} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \frac{t_1}{u_1} \ldots \frac{t_{n-1}}{u_{n-1}}$$

and

$$\varphi \frac{t'_0 \ldots t'_{n-1}}{v_0 \ldots v_{n-1}} = \varphi \frac{u_0}{v_0} \frac{u_1}{v_1} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t'_0}{u_0} \frac{t'_1}{u_1} \ldots \frac{t'_{n-1}}{u_{n-1}}.$$

Thus the simultaneous substitutions can be seen as successive substitutions, and the order of the substitutions $\frac{t_i}{u_i}$ may be permuted without affecting the final outcome. We may use the substitution rule repeatedly:

$$\begin{array}{l}
\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \; t_{n-1} \equiv t'_{n-1} \\
\vdots \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \; t_{n-1} \equiv t'_{n-1} \ldots t_0 \equiv t'_0 \\
\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \; t_0 \equiv t'_0 \; \ldots \; t_{n-1} \equiv t'_{n-1}
\end{array}
\qquad
\begin{array}{l}
\varphi \frac{t_0 \ldots t_{n-1}}{v_0 \ldots v_{n-1}} \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t_{n-1}}{u_{n-1}} \\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t_0}{u_0} \ldots \frac{t'_{n-1}}{u_{n-1}} \\
\\
\varphi \frac{u_0}{v_0} \ldots \frac{u_{n-1}}{v_{n-1}} \frac{t'_0}{u_0} \ldots \frac{t'_{n-1}}{u_{n-1}} \\
\varphi \frac{t'_0 \ldots t'_{n-1}}{v_0 \ldots v_{n-1}}.
\end{array}$$

□

12 Consistency

Fix a language S.

Definition 54. *A set* $\Phi \subseteq L^S$ *is* consistent *if* $\Phi \nvdash \bot$. Φ *is* inconsistent *if* $\Phi \vdash \bot$.

We prove some laws of consistency.

Lemma 55. *Let* $\Phi \subseteq L^S$ *and* $\varphi \in L^S$. *Then*

a) Φ *is inconsistent iff there is* $\psi \in L^S$ *such that* $\Phi \vdash \psi$ *and* $\Phi \vdash \neg\psi$.

b) $\Phi \vdash \varphi$ *iff* $\Phi \cup \{\neg\varphi\}$ *is inconsistent.*

c) *If* Φ *is consistent, then* $\Phi \cup \{\varphi\}$ *is consistent or* $\Phi \cup \{\neg\varphi\}$ *is consistent (or both).*

d) *Let* $\mathcal{F}$ *be a family of consistent sets which is linearly ordered by inclusion, i.e., for all* Φ, $\Psi \in \mathcal{F}$ *holds* $\Phi \subseteq \Psi$ *or* $\Psi \subseteq \Phi$. *Then*

$$\Phi^* = \bigcup_{\Phi \in \mathcal{F}} \Phi$$

is consistent.

Proof. a) Assume $\Phi \vdash \bot$. Then by the *ex falso* rule, $\Phi \vdash \psi$ and $\Phi \vdash \neg\psi$.

Conversely assume that $\Phi \vdash \psi$ and $\Phi \vdash \neg\psi$ for some $\psi \in L^S$. Then $\Phi \vdash \bot$ by $\bot$-introduction.
b) Assume $\Phi \vdash \varphi$. Take $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ such that $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$. Then we can extend a derivation of $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ as follows

$$\begin{array}{lllll}
\varphi_0 & \ldots & \varphi_{n-1} & & \varphi \\
\varphi_0 & \ldots & \varphi_{n-1} & \neg\varphi & \neg\varphi \\
\varphi_0 & \ldots & \varphi_{n-1} & \neg\varphi & \bot
\end{array}$$

and $\Phi \cup \{\neg\varphi\}$ is inconsistent.

Conversely assume that $\Phi \cup \{\neg\varphi\} \vdash \bot$ and take $\varphi_0, ..., \varphi_{n-1} \in \Phi$ such that $\varphi_0 ... \varphi_{n-1} \neg\varphi \vdash \bot$. Then $\varphi_0 ... \varphi_{n-1} \vdash \varphi$ and $\Phi \vdash \varphi$.

c) Assume that $\Phi \cup \{\varphi\}$ and $\Phi \cup \{\neg\varphi\}$ are inconsistent. Then there are $\varphi_0, ..., \varphi_{n-1} \in \Phi$ such that $\varphi_0 ... \varphi_{n-1} \vdash \varphi$ and $\varphi_0 ... \varphi_{n-1} \vdash \neg\varphi$. By the introduction rule for $\bot$, $\varphi_0 ... \varphi_{n-1} \vdash \bot$. Thus Φ is inconsistent.

d) Assume that Φ^* is inconsistent. Take $\varphi_0, ..., \varphi_{n-1} \in \Phi^*$ such that $\varphi_0 ... \varphi_{n-1} \vdash \bot$. Take $\Phi_0, ... \Phi_{n-1} \in \mathcal{F}$ such that $\varphi_0 \in \Phi_0$, ..., $\varphi_{n-1} \in \Phi_{n-1}$. Since $\mathcal{F}$ is linearly ordered by inclusion there is $\Phi \in \{\Phi_0, ... \Phi_{n-1}\}$ such that $\varphi_0, ..., \varphi_{n-1} \in \Phi$. Then Φ is inconsistent, contradiction. □

Note that d) implies the inductivity required for the lemma of ZORN. The proof of the completeness theorem will be based on the relation between consistency and satisfiability.

Lemma 56. *Assume that $\Phi \subseteq L^S$ is satisfiable. Then Φ is consistent.*

Proof. Assume that $\Phi \vdash \bot$. By the correctness of the sequent calculus, $\Phi \vDash \bot$. Assume that Φ is satisfiable and let $\mathfrak{I} \vDash \Phi$. Then $\mathfrak{I} \vDash \bot$. This contradicts the definition of the satisfaction relation. Thus Φ is not satisfiable. □

Theorem 57. *The sequent calculus is complete iff every consistent $\Phi \subseteq L^S$ is satisfiable.*

Proof. Assume that the sequent calculus is complete. Let $\Phi \subseteq L^S$ be consistent, i.e., $\Phi \nvdash \bot$. By completeness, $\Phi \nvDash \bot$, and we can take an S-interpretation $\mathfrak{I} \vDash \Phi$ such that $\mathfrak{I} \nvDash \bot$. Thus Φ is satisfiable.

Conversely, assume that every consistent $\Phi \subseteq L^S$ is satisfiable. Assume $\Psi \vDash \psi$. Assume for a contradiction that $\Psi \nvdash \psi$. Then $\Psi \cup \{\neg\psi\}$ is consistent. By assumption there is an S-interpretation $\mathfrak{I} \vDash \Psi \cup \{\neg\psi\}$. $\mathfrak{I} \vDash \Psi$ and $\mathfrak{I} \nvDash \psi$, which contradicts $\Psi \vDash \psi$. Thus $\Psi \vdash \psi$. □

13 Term models and HENKIN sets

In view of the previous lemma, we strive to construct interpretations for given sets $\Phi \subseteq L^S$ of S-formulas. Since we are working in great generality and abstractness, the only material available for the construction of structures is the language L^S itself. We shall build a model out of S-terms.

Definition 58. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. The* term model *$\mathfrak{T}^\Phi$ of Φ is the following S-model:*

a) Define a relation $\sim$ on T^S,

$$t_0 \sim t_1 \text{ iff } \Phi \vdash t_0 \equiv t_1 .$$

$\sim$ is an equivalence relation on T^S.

b) For $t \in T^S$ let $\bar{t} = \{s \in T^S \mid s \sim t\}$ be the equivalence class of t.

c) The underlying set $T^\Phi = \mathfrak{T}^\Phi(\forall)$ of the term model is the set of $\sim$-equivalence classes

$$T^\Phi = \{\bar{t} \mid t \in T^S\}.$$

d) For an n-ary relation symbol $R \in S$ let $R^{\mathfrak{T}^\Phi}$ on T^Φ be defined by

$$(\bar{t}_0, ..., \bar{t}_{n-1}) \in R^{\mathfrak{T}^\Phi} \text{ iff } \Phi \vdash R t_0 ... t_{n-1} .$$

e) For an n-ary function symbol $f \in S$ let $f^{\mathfrak{T}^\Phi}$ on T^Φ be defined by

$$f^{\mathfrak{T}^\Phi}(\bar{t}_0, ..., \bar{t}_{n-1}) = \overline{f t_0 ... t_{n-1}} .$$

f) For $n \in \mathbb{N}$ define the variable interpretation $\mathfrak{T}^\Phi(v_n) = \bar{v_n}$.

The term model is well-defined:

Lemma 59. *In the previous construction the following holds:*

a) $\sim$ *is an equivalence relation on* T^S.

b) *The definition of* $R^{\mathfrak{T}^\Phi}$ *is independent of representatives.*

c) *The definition of* $f^{\mathfrak{T}^\Phi}$*is independent of representatives.*

Proof. a) We derived the axioms of equivalence relations for $\equiv$:

- $\vdash \forall x\, x \equiv x$
- $\vdash \forall x \forall y\, (x \equiv y \rightarrow y \equiv x)$
- $\vdash \forall x \forall y \forall z\, (x \equiv y \wedge y \equiv z \rightarrow x \equiv z)$

Consider $t \in T^S$. Then $\vdash t \equiv t$. Thus for all $t \in T^S$ holds $t \sim t$.

Consider $t_0, t_1 \in T^S$ with $t_0 \sim t_1$. Then $\vdash t_0 \equiv t_1$. Also $\vdash t_0 \equiv t_1 \rightarrow t_1 \equiv t_0$, $\vdash t_1 \equiv t_0$, and $t_1 \sim t_0$. Thus for all $t_0, t_1 \in T^S$ with $t_0 \sim t_1$ holds $t_1 \sim t_0$.

The transitivity of $\sim$ follows similarly.

b) Let $\bar{t_0}, \ldots, \bar{t}_{n-1} \in T^\Phi$, $\bar{t_0} = \bar{s_0}, \ldots, \bar{t}_{n-1} = \bar{s}_{n-1}$ and $\Phi \vdash Rt_0 \ldots t_{n-1}$. Then $\vdash t_0 \equiv s_0$, ... , $\vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule yield $\Phi \vdash Rs_0 \ldots s_{n-1}$. Hence $\Phi \vdash Rt_0 \ldots t_{n-1}$ implies $\Phi \vdash Rs_0 \ldots s_{n-1}$. By the symmetry of the argument, $\Phi \vdash Rt_0 \ldots t_{n-1}$ iff $\Phi \vdash Rs_0 \ldots s_{n-1}$.

c) Let $\bar{t_0}, \ldots, \bar{t}_{n-1} \in T^\Phi$ and $\bar{t_0} = \bar{s_0}, \ldots, \bar{t}_{n-1} = \bar{s}_{n-1}$. Then $\vdash t_0 \equiv s_0$, ... , $\vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule to $\vdash ft_0 \ldots t_{n-1} \equiv ft_0 \ldots t_{n-1}$ yield

$$\vdash ft_0 \ldots t_{n-1} \equiv fs_0 \ldots s_{n-1}$$

and $\overline{ft_0 \ldots t_{n-1}} = \overline{fs_0 \ldots s_{n-1}}$. □

We aim to obtain $\mathfrak{T}^\Phi \vDash \Phi$. The initial cases of an induction over the complexity of formulas is given by

Theorem 60.

a) *For terms* $t \in T^S$ *holds* $\mathfrak{T}^\Phi(t) = \bar{t}$.

b) *For atomic formulas* $\varphi \in L^S$ *holds*

$$\mathfrak{T}^\Phi \vDash \varphi \text{ iff } \Phi \vdash \varphi.$$

Proof. a) By induction on the term calculus. The initial case $t = v_n$ is obvious by the definition of the term model. Now consider a term $t = ft_0 \ldots t_{n-1}$ with an n-ary function symbol $f \in S$, and assume that the claim is true for $t_0, \ldots, t_{n-1}$. Then

$$\begin{aligned} \mathfrak{T}^\Phi(ft_0 \ldots t_{n-1}) &= f^{\mathfrak{T}^\Phi}(\mathfrak{T}^\Phi(t_0), \ldots, \mathfrak{T}^\Phi(t_{n-1})) \\ &= f^{\mathfrak{T}^\Phi}(\bar{t_0}, \ldots, \overline{t_{n-1}}) \\ &= \overline{ft_0 \ldots t_{n-1}}. \end{aligned}$$

b) Let $\varphi = Rt_0 \ldots t_{n-1}$ with an n-ary relation symbol $R \in S$ and $t_0, \ldots, t_{n-1} \in T^S$. Then

$$\begin{aligned} \mathfrak{T}^\Phi \vDash Rt_0 \ldots t_{n-1} &\text{ iff } R^{\mathfrak{T}^\Phi}(\mathfrak{T}^\Phi(t_0), \ldots, \mathfrak{T}^\Phi(t_{n-1})) \\ &\text{ iff } R^{\mathfrak{T}^\Phi}(\bar{t_0}, \ldots, \overline{t_{n-1}}) \\ &\text{ iff } \Phi \vdash Rt_0 \ldots t_{n-1}. \end{aligned}$$

Let $\varphi = t_0 \equiv t_1$ with $t_0, t_1 \in T^S$. Then

$$\begin{aligned} \mathfrak{T}^\Phi \vDash t_0 \equiv t_1 &\text{ iff } \mathfrak{T}^\Phi(t_0) = \mathfrak{T}^\Phi(t_1) \\ &\text{ iff } \bar{t_0} = \bar{t_1} \\ &\text{ iff } t_0 \sim t_1 \\ &\text{ iff } \Phi \vdash t_0 \equiv t_1. \end{aligned}$$

□

To extend the lemma to complex S-formulas, Φ has to satisfy some recursive properties.

Definition 61. *A set* $\Phi \subseteq L^S$ *of S-formulas is a* Henkin set *if it satisfies the following properties:*

a) Φ *is consistent;*

b) Φ *is* (derivation) complete*, i.e., for all* $\varphi \in L^S$

$$\Phi \vdash \varphi \text{ or } \Phi \vdash \neg\varphi;$$

c) Φ contains witnesses*, i.e., for all* $\forall x\varphi \in L^S$ *there is a term* $t \in T^S$ *such that*

$$\Phi \vdash \neg\forall x\varphi \rightarrow \neg\varphi\frac{t}{x}.$$

Lemma 62. *Let* $\Phi \subseteq L^S$ *be a* Henkin *set. Then for all* $\chi, \psi \in L^S$ *and variables* x*:*

a) $\Phi \nvdash \chi$ *iff* $\Phi \vdash \neg\chi$.

b) $\Phi \vdash \chi$ *implies* $\Phi \vdash \psi$*, iff* $\Phi \vdash \chi \rightarrow \psi$.

c) *For all* $t \in T^S$ *holds* $\Phi \vdash \chi\frac{t}{u}$ *iff* $\Phi \vdash \forall x\chi$.

Proof. a) Assume $\Phi \nvdash \chi$. By derivation completeness, $\Phi \vdash \neg\chi$. Conversely assume $\Phi \vdash \neg\chi$. Assume for a contradiction that $\Phi \vdash \chi$. Then Φ is inconsistent. Contradiction. Thus $\Phi \nvdash \chi$.
b) Assume $\Phi \vdash \chi$ implies $\Phi \vdash \psi$.
Case 1. $\Phi \vdash \chi$. Then $\Phi \vdash \psi$ and by a previous derivation $\Phi \vdash \chi \rightarrow \psi$.
Case 2. $\Phi \nvdash \chi$. By the derivation completeness of Φ holds $\Phi \vdash \neg\chi$. And by a previous derivation $\Phi \vdash \chi \rightarrow \psi$.

Conversely assume that $\Phi \vdash \chi \rightarrow \psi$. Assume that $\Phi \vdash \chi$. By $\rightarrow$-elimination, $\Phi \vdash \psi$. Thus $\Phi \vdash \chi$ implies $\Phi \vdash \psi$.
c) Assume that for all $t \in T^S$ holds $\Phi \vdash \chi\frac{t}{u}$. Assume that $\Phi \nvdash \forall x\chi$. By a), $\Phi \vdash \neg\forall x\chi$. Since Φ contains witnesses there is a term $t \in T^S$ such that $\Phi \vdash \neg\forall x\chi \rightarrow \neg\chi\frac{t}{u}$. By $\rightarrow$-elimination, $\Phi \vdash \neg \chi\frac{t}{u}$. Contradiction. Thus $\Phi \vdash \forall x\chi$. The converse follows from the rule of $\forall$-elimination. ☐

Theorem 63. *Let* $\Phi \subseteq L^S$ *be a* Henkin *set. Then*

a) *For all formulas* $\chi \in L^S$*, pairwise distinct variables* $\vec{x}$ *and terms* $\vec{t} \in T^S$

$$\mathfrak{T}^\Phi \vDash \chi\frac{\vec{t}}{\vec{x}} \text{ iff } \Phi \vdash \chi\frac{\vec{t}}{\vec{x}}.$$

b) $\mathfrak{T}^\Phi \vDash \Phi$.

Proof. b) follows immediately from a). a) is proved by induction on the formula calculus. The atomic case has already been proven. Consider the non-atomic cases:
i) $\chi = \bot$. Then $\bot\frac{\vec{t}}{\vec{x}} = \bot$. $\mathfrak{T}^\Phi \vDash \bot\frac{\vec{t}}{\vec{x}}$ is false by definition of the satisfaction relation $\vDash$, and $\Phi \vdash \chi\frac{\vec{t}}{\vec{x}}$ is false since Φ is consistent. Thus $\mathfrak{T}^\Phi \vDash \bot\frac{\vec{t}}{\vec{x}}$ iff $\Phi \vdash \bot\frac{\vec{t}}{\vec{x}}$.
ii.) $\chi = \neg\varphi\frac{\vec{t}}{\vec{x}}$ and assume that the claim holds for φ. Then

$$\begin{aligned}
\mathfrak{T}^\Phi \vDash \neg\varphi\frac{\vec{t}}{\vec{x}} & \text{ iff not } \mathfrak{T}^\Phi \vDash \varphi\frac{\vec{t}}{\vec{x}} \\
& \text{ iff not } \Phi \vdash \varphi\frac{\vec{t}}{\vec{x}} \text{ by the inductive assumption} \\
& \text{ iff } \Phi \vdash \neg\varphi\frac{\vec{t}}{\vec{x}} \text{ by a) of the previous lemma.}
\end{aligned}$$

iii.) $\chi = (\varphi \rightarrow \psi)\frac{\vec{t}}{\vec{x}}$ and assume that the claim holds for φ and ψ. Then

$$\begin{aligned}
\mathfrak{T}^\Phi \vDash (\varphi \rightarrow \psi)\frac{\vec{t}}{\vec{x}} & \text{ iff } \mathfrak{T}^\Phi \vDash \varphi\frac{\vec{t}}{\vec{x}} \text{ implies } \mathfrak{T}^\Phi \vDash \psi\frac{\vec{t}}{\vec{x}} \\
& \text{ iff } \Phi \vdash \varphi\frac{\vec{t}}{\vec{x}} \text{ implies } \Phi \vdash \psi\frac{\vec{t}}{\vec{x}} \text{ by the inductive assumption} \\
& \text{ iff } \Phi \vdash \varphi\frac{\vec{t}}{\vec{x}} \rightarrow \psi\frac{\vec{t}}{\vec{x}} \text{ by a) of the previous lemma} \\
& \text{ iff } \Phi \vdash (\varphi \rightarrow \psi)\frac{\vec{t}}{\vec{x}} \text{ by the definition of substitution.}
\end{aligned}$$

iv.) $\chi = (\forall x\,\varphi)\,\frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}}$ and assume that the claim holds for φ. By definition of the substitution χ is of the form

$$\forall u\,(\varphi\,\frac{t_0 \dots t_{r-1}\,u}{x_0 \dots x_{r-1}\,x}) \text{ oder } \forall u\,(\varphi\,\frac{t_1 \dots t_{r-1}\,u}{x_1 \dots x_{r-1}\,x})$$

with a suitable variable u. Without loss of generality assume that χ is of the first form. Then

$$\begin{aligned}
\mathfrak{T}^\Phi \vDash (\forall x\,\varphi)\,\frac{\vec{t}}{\vec{x}} \quad & \text{iff} \quad \mathfrak{T}^\Phi \vDash \exists u\,(\varphi\,\frac{t_0 \dots t_{r-1}\,u}{x_0 \dots x_{r-1}\,x}) \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^\Phi\frac{\bar{t}}{u} \vDash \varphi\,\frac{t_0 \dots t_{r-1}\,u}{x_0 \dots x_{r-1}\,x} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^\Phi\frac{\mathfrak{I}^\Phi(t)}{u} \vDash \varphi\,\frac{t_0 \dots t_{r-1}\,u}{x_0 \dots x_{r-1}\,x} \quad \text{by a previous lemma} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^\Phi \vDash (\varphi\,\frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}})\,\frac{t}{u} \quad \text{by the substitution lemma} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \mathfrak{T}^\Phi \vDash \varphi\,\frac{t_0 \dots t_{r-1}\,t}{x_0 \dots x_{r-1}\,x} \quad \text{by successive substitutions} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \Phi \vdash \varphi\,\frac{t_0 \dots t_{r-1}\,t}{x_0 \dots x_{r-1}\,x} \quad \text{by the inductive assumption} \\
& \text{iff} \quad \text{for all } t \in T^S \text{ holds } \Phi \vdash (\varphi\,\frac{t_0 \dots t_{r-1}\,u}{x_0 \dots x_{r-1}\,x})\,\frac{t}{u} \quad \text{by successive substitutions} \\
& \text{iff} \quad \Phi \vdash \forall u\,(\varphi\,\frac{t_0 \dots t_{r-1}\,u}{x_0 \dots x_{r-1}\,x}) \quad \text{by c) of the previous lemma} \\
& \text{iff} \quad \Phi \vdash (\forall x\,\varphi)\,\frac{\vec{t}}{\vec{x}}\,.
\end{aligned}$$

□

14 Constructing HENKIN sets

We shall show that every consistent set of formulas can be extended to a HENKIN set by "adding witnesses" and then ensuring negation completeness. We first consider witnesses.

Theorem 64. *Let $\Phi \subseteq L^S$ be consistent. Let $\varphi \in L^S$ and let z be a variable which does not occur in $\Phi \cup \{\varphi\}$. Then the set*

$$\Phi \cup \{\neg\forall x\,\varphi \to \neg\varphi\frac{z}{x}\}$$

is consistent.

Proof. Assume for a contradiction that $\Phi \cup \{(\neg\exists x\,\varphi \vee \varphi\frac{z}{x})\}$ is inconsistent. Take $\varphi_0, \dots, \varphi_{n-1} \in \Phi$ such that

$$\varphi_0 \dots \varphi_{n-1}\ \neg\forall x\,\varphi \to \neg\varphi\frac{z}{x} \vdash \bot\,.$$

Set $\Gamma = (\varphi_0, \dots, \varphi_{n-1})$. Then continue the derivation as follows:

1.	Γ	$\neg\forall x\,\varphi \to \neg\varphi\frac{z}{x}$	$\bot$
2.	Γ	$\neg\neg\forall x\,\varphi$	$\neg\neg\forall x\,\varphi$
3.	Γ	$\neg\neg\forall x\,\varphi$	$\neg\forall x\,\varphi \to \neg\varphi\frac{z}{x}$
4.	Γ	$\neg\neg\forall x\,\varphi$	$\bot$
5.	Γ		$\neg\forall x\,\varphi$
6.	Γ	$\neg\varphi\frac{z}{x}$	$\neg\varphi\frac{z}{x}$
7.	Γ	$\neg\varphi\frac{z}{x}$	$\neg\forall x\,\varphi \to \neg\varphi\frac{z}{x}$
8.	Γ	$\neg\varphi\frac{z}{x}$	$\bot$
9.	Γ		$\varphi\frac{z}{x}$
10.	Γ		$\forall x\,\varphi$
11.	Γ		$\bot$

Hence Φ is inconsistent, contradiction. □

This means that "unused" variables may be used as HENKIN witnesses. Since "unused" constant symbols behave much like unused variables, we get:

Theorem 65. *Let $\Phi \subseteq L^S$ be consistent. Let $\varphi \in L^S$ and let $c \in S$ be a constant symbol which does not occur in $\Phi \cup \{\varphi\}$. Then the set*

$$\Phi \cup \{\neg \forall x \varphi \rightarrow \neg \varphi \frac{c}{x}\}$$

is consistent.

Proof. Assume that $\Phi \cup \{(\neg \exists x \varphi \vee \varphi \frac{c}{x})\}$ is inconsistent. Take a derivation

$$\begin{array}{c} \Gamma_0 \varphi_0 \\ \Gamma_1 \varphi_1 \\ \vdots \\ \Gamma_{n-1} \, \varphi_{n-1} \\ \Gamma_n \; (\neg \forall x \varphi \rightarrow \neg \varphi \frac{c}{x}) \; \bot \end{array} \tag{1}$$

with $\Gamma_n \subseteq \Phi$. Choose a variable z, which does not occur in the derivation. For a formula ψ define ψ' by replacing each occurence of c by z, and for a sequence $\Gamma = (\psi_0, \ldots, \psi_{k-1})$ of formulas let $\Gamma' = (\psi_0', \ldots, \psi_{k-1}')$. Replacing each occurence of c by z in the deriavation we get

$$\begin{array}{c} \Gamma_0' \varphi_0' \\ \Gamma_1' \varphi_1' \\ \vdots \\ \Gamma_{n-1}' \, \varphi_{n-1}' \\ \Gamma_n \; (\neg \forall x \varphi \rightarrow \neg \varphi \frac{z}{x}) \; \bot \end{array} \tag{2}$$

The particular form of the final sequence is due to the fact that c does not occur in $\Phi \cup \{\varphi\}$. To show that (2) is again a derivation in the sequent calculus we show that the replacement $c \mapsto z$ transforms every instance of a sequent rule in (1) into an instance of a (derivable) rule in (2). This is obvious for all rules except possibly the quantifyer rules.

So let

$$\frac{\Gamma \quad \psi \frac{y}{x}}{\Gamma \quad \forall x \psi}, \text{ with } y \notin \text{free}(\Gamma \cup \{\forall x \psi\})$$

be an $\forall$-introduction in (1). Then $(\psi \frac{y}{x})' = \psi' \frac{y}{x}$, $(\forall x \psi)' = \forall x \psi'$, and $y \notin \text{free}(\Gamma' \cup \{(\forall x \psi)'\})$. Hence

$$\frac{\Gamma' \quad (\psi \frac{y}{x})'}{\Gamma' \quad (\forall x \psi)'}$$

is a justified $\forall$-introduction.

Now consider an $\forall$-elimination in (1):

$$\frac{\Gamma \quad \forall x \psi}{\Gamma \quad \psi \frac{t}{x}}$$

Then $(\forall x \psi)' = \forall x \psi'$ and $(\psi \frac{t}{x})' = \psi' \frac{t'}{x}$ where t' is obtained from t by replacing all occurences of c by z. Hence

$$\frac{\Gamma' \quad (\forall x \psi)'}{\Gamma' \quad (\psi \frac{t}{x})'}$$

is a justified $\forall$-elimination.

The derivation (2) proves that

$$\Phi \cup \{(\neg \forall x \varphi \rightarrow \neg \varphi \frac{z}{x}) \vdash \bot,$$

which contradicts the preceding lemma. □

We shall now show that any consistent set of formulas can be consistently expanded to a set of formulas which contains witnesses.

Theorem 66. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^ω and $\Phi^\omega \subseteq L^{S^*}$ such that*

a) S^ω extends S by constant symbols, i.e., $S \subseteq S^\omega$ and if $s \in S^\omega \setminus S$ then s is a constant symbol;

b) $\Phi^\omega \supseteq \Phi$;

c) Φ^ω is consistent;

d) Φ^ω contains witnesses;

e) if L^S is countable then so are L^{S^ω} and Φ^ω.

Proof. For every a define a "new" distinct constant symbol c_a, which does not occur in S, e.g., $c_a = ((a, S), 1, 0)$. Extend S by constant symbols c_ψ for $\psi \in L^S$:

$$S^+ = S \cup \{c_\psi | \psi \in L^S\}.$$

Then set

$$\Phi^+ = \Phi \cup \{\neg\forall x\varphi \rightarrow \neg\varphi\frac{c_{\forall x\varphi}}{x} | \forall x\varphi \in L^S\}.$$

Φ^+ contains witnesses for all universal formulas of S.
(1) $\Phi^+ \subseteq L^{S^+}$ is consistent.
Proof: Assume instead that Φ^+ is inconsistent. Choose a finite sequence $\forall x_0\varphi_0, \ldots, \forall x_{n-1}\varphi_{n-1} \in L^S$ of pairwise distinct universal formulas such that

$$\Phi \cup \{\neg\forall x_0\varphi_0 \rightarrow \neg\varphi_0\frac{c_{\forall x_0\varphi_0}}{x_0}, \ldots, \neg\forall x_{n-1}\varphi_{n-1} \rightarrow \neg\varphi_{n-1}\frac{c_{\forall x_{n-1}\varphi_{n-1}}}{x_{n-1}}\}$$

is inconsistent. By the previous theorem one can inductively show that for all $i < n$ the set

$$\Phi \cup \{\neg\forall x_0\varphi_0 \rightarrow \neg\varphi_0\frac{c_{\forall x_0\varphi_0}}{x_0}, \ldots, \neg\forall x_{n-1}\varphi_{n-1} \rightarrow \neg\varphi_{n-1}\frac{c_{\forall x_{i-1}\varphi_{\mathrm{ni}-1}}}{x_{i-1}}\}$$

is consistent. Contradiction. *qed*(1)

We iterate the +-operation through the integers. Define recursively

$$\begin{aligned}
\Phi^0 &= \Phi \\
S^0 &= S \\
S^{n+1} &= (S^n)^+ \\
\Phi^{n+1} &= (\Phi^n)^+ \\
S^\omega &= \bigcup_{n\in\mathbb{N}} S^n \\
\Phi^\omega &= \bigcup_{n\in\mathbb{N}} \Phi^n.
\end{aligned}$$

S^ω is an extension of S by constant symbols. For $n \in \mathbb{N}$, Φ^n is consistent by induction. Φ^ω is consistent by the lemma on unions of consistent sets.
(2) Φ^ω contains witnesses.
Proof. Let $\forall x\varphi \in L^{S^\omega}$. Let $n \in \mathbb{N}$ such that $\forall x\varphi \in L^{S^n}$. Then $\neg\forall x\varphi \rightarrow \neg\varphi\frac{c_{\forall x\varphi}}{x} \in \Phi^{n+1} \subseteq \Phi^\omega$. *qed*(2)
(3) Let L^S be countable. Then L^{S^ω} and Φ^ω are countable.
Proof. Since L^S is countable, there can only be countably many symbols in the alphabet of $S^0 = S$. The alphabet of S^1 is obtained by adding the countable set $\{c_\psi | \psi \in L^S\}$; the alphabet of S^1 is countable as the union of two countable sets. The set of words over a countable alphabet is countable, hence L^{S^1} and $\Phi^1 \subseteq L^{S^1}$ are countable.

Inductive application of this argument show that for any $n \in \mathbb{N}$, the sets L^{S^n} and Φ^n are countable. Since countable unions of countable sets are countable, $L^{S^\omega} = \bigcup_{n\in\mathbb{N}} L^{S^n}$ and also $\Phi^\omega \subseteq L^{S^\omega}$ are countable. □

To get HENKIN sets we have to ensure derivation completeness.

Theorem 67. *Let S be a language and let $\Phi\subseteq L^S$ be consistent. Then there is a consistent $\Phi^*\subseteq L^S$, $\Phi^*\supseteq\Phi$ which is derivation complete.*

Proof. Define the partial order $(P,\subseteq)$ by

$$P=\{\Psi\subseteq L^S\,|\,\Psi\supseteq\Phi \text{ and } \Psi \text{ is consistent}\}.$$

$P\neq\emptyset$ since $\Phi\in P$. P is *inductively ordered* by a previous lemma: if $\mathcal{F}\subseteq P$ is linearly ordered by inclusion, i.e., for all $\Psi,\Psi'\in\mathcal{F}$ holds $\Psi\subseteq\Psi'$ or $\Psi'\subseteq\Psi$ then

$$\bigcup_{\Psi\in\mathcal{F}}\Psi\in P.$$

Hence $(P,\subseteq)$ satisfies the conditions of ZORN's lemma. Let Φ^* be a maximal element of $(P,\subseteq)$. By the definition of P, $\Phi^*\subseteq L^S$, $\Phi^*\supseteq\Phi$, and Φ^* is consistent. Derivation completeness follows from the following claim.
(1) For all $\varphi\in L^S$ holds $\varphi\in\Phi^*$ or $\neg\varphi\in\Phi^*$.
Proof. Φ^* is consistent. By a previous lemma, $\Phi^*\cup\{\varphi\}$ or $\Phi^*\cup\{\neg\varphi\}$ are consistent.
Case 1. $\Phi^*\cup\{\varphi\}$ is consistent. By the $\subseteq$-maximality of Φ^*, $\Phi^*\cup\{\varphi\}=\Phi^*$ and $\varphi\in\Phi^*$.
Case 2. $\Phi^*\cup\{\neg\varphi\}$ is consistent. By the $\subseteq$-maximality of Φ^*, $\Phi^*\cup\{\neg\varphi\}=\Phi^*$ and $\neg\varphi\in\Phi^*$. □

The proof uses ZORN's lemma. In case L^S is countable one can work without ZORN's lemma.

Proof. (For countable L^S) Let $L^S=\{\varphi_n|n\in\mathbb{N}\}$ be an enumeration of L^S. Define a sequence $(\Phi_n|n\in\mathbb{N})$ by recursion on n such that

i. $\Phi\subseteq\Phi_n\subseteq\Phi_{n+1}\subseteq L^S$;

ii. Φ_n is consistent.

For $n=0$ set $\Phi_0=\Phi$. Assume that Φ_n is defined according to i. and ii.
Case 1. $\Phi_n\cup\{\varphi_n\}$ is consistent. Then set $\Phi_{n+1}=\Phi_n\cup\{\varphi_n\}$.
Case 2. $\Phi_n\cup\{\varphi_n\}$ is inconsistent. Then $\Phi_n\cup\{\neg\varphi_n\}$ is consistent by a previous lemma, and we define $\Phi_{n+1}=\Phi_n\cup\{\neg\varphi_n\}$.

Let

$$\Phi^*=\bigcup_{n\in\mathbb{N}}\Phi_n\,.$$

Then Φ^* is a consistent superset of Φ. By construction, $\varphi\in\Phi^*$ or $\neg\varphi\in\Phi^*$, for all $\varphi\in L^S$. Hence Φ^* is derivation complete. □

According to Theorem 66 a given consistent set Φ can be extended to $\Phi^\omega\subseteq L^{S^\omega}$ containing witnesses. By Theorem 67 Φ^ω can be extended to a derivation complete $\Phi^*\subseteq L^{S^\omega}$. Since the latter step does not extend the language, Φ^* contains witnesses and is thus a HENKIN set:

Theorem 68. *Let S be a language and let $\Phi\subseteq L^S$ be consistent. Then there is a language S^* and $\Phi^*\subseteq L^{S^*}$ such that*

a) $S^*\supseteq S$ is an extension of S by constant symbols;

b) $\Phi^*\supseteq\Phi$ is a HENKIN set;

c) if L^S is countable then so are L^{S^*} and Φ^*.

15 The completeness theorem

We can now combine our technical preparations to show the fundamental theorems of first-order logic.

Combining Theorems 68 and 63, we obtain a general and a countable model existence theorem:

Theorem 69. (HENKIN model existence theorem) *Let* $\Phi \subseteq L^S$. *Then* Φ *is consistent iff* Φ *is satisfiable.*

Theorem 70. (Downward LÖWENHEIM-SKOLEM theorem) *Let* $\Phi \subseteq L^S$ *be a* countable *consistent set of formulas. Then* Φ *possesses a model* $\mathfrak{M} = (\mathfrak{A}, \beta) \vDash \Phi$, $\mathfrak{A} = (A, \ldots)$ *with a* countable *underlying set* A.

The word "downward" emphasises the existence of models of "small" cardinality. We shall soon also consider an upward LÖWENHEIM-SKOLEM theorem. By Lemma 57, Theorem 69 the model existence theorems imply the main theorem.

Theorem 71. (GÖDEL completeness theorem) *The sequent calculus is complete, i.e.,* $\vDash = \vdash$.

Finally the equality of $\vDash$ and $\vdash$ and the compactness theorem 49 for $\vdash$ imply

Theorem 72. (Compactness theorem) *Let* $\Phi \subseteq L^S$ *and* $\varphi \in \Phi$. *Then*

a) $\Phi \vDash \varphi$ *iff there is a finite subset* $\Phi_0 \subseteq \Phi$ *such that* $\Phi_0 \vDash \varphi$.

b) Φ *is satisfiable iff every finite subset* $\Phi_0 \subseteq \Phi$ *is satisfiable.*

The GÖDEL completeness theorem is the fundamental theorem of mathematical logic. It connects syntax and semantics of formal languages in an optimal way. Before we continue the mathematical study of its consequences we make some general remarks about the wider impact of the theorem:

- The completeness theorem gives an *ultimate correctness criterion* for mathematical proofs. A proof is correct if it can (in principle) be reformulated as a formal derivation. Although mathematicians prefer semi-formal or informal arguments, this criterion could be applied in case of doubt.
- Checking the correctness of a formal proof in the above sequent calculus is a syntactic task that can be carried out by computer. We shall later consider a prototypical *proof checker* `Naproche` which uses a formal language which is a subset of natural english.
- By systematically running through all possible formal proofs, *automatic theorem proving* is in principle possible. In this generality, however, algorithms immediately run into very high algorithmic complexities and become practically infeasable.
- Practical automatic theorem proving has become possible in restricted situations, either by looking at particular kinds of axioms and associated intended domains, or by restricting the syntactical complexity of axioms and theorems.
- Automatic theorem proving is an important component of *artificial intelligence* (AI) where a system has to obtain logical consequences from conditions formulated in first-order logic. Although there are many difficulties with artificial intelligence this approach is still being followed with some success.
- Another special case of automatic theorem proving is given by *logic programming* where programs consist of logical statements of some restricted complexity and a run of a program is a systematic search for a solution of the given statements. The original and still most prominent logic programming language is `Prolog` which is still widely used in linguistics and AI.
- There are other areas which can be described formally and where syntax/semantics constellations similar to first-order logic may occur. In the theory of algorithms there is the syntax of programming languages versus the (mathematical) meaning of a program. Since programs crucially involve time alternative logics with time have to be introduced. Now in all such generalizations, the GÖDEL completeness theorem serves as a pattern onto which to model the syntax/semantics relation.
- The success of the formal method in mathematics makes mathematics a leading *formal science*. Several other sciences also strive to present and justify results formally, like computer science and parts of philosophy.

– The completeness theorem must not be confused with the famous Gödel *incompleteness theorems*: they say that certain axiom systems like Peano arithmetic are incomplete in the sense that they do not imply some formulas which hold in the standard model of the axiom system.

16 Cardinalities of models

Definition 73. *An S-structure $\mathfrak{A}$ is* finite, infinite, countable, *or* uncountable, *resp., iff the underlying set $|\mathfrak{A}|$ is finite, infinite, countable, or uncountable, resp..*

Theorem 74. *Assume that $\Phi \subseteq L^S$ has arbitrarily large finite models. Then Φ has an infinite model.*

Proof. For $n \in \mathbb{N}$ define the sentence

$$\varphi_{\geqslant n} = \exists v_0, \ldots, v_{n-1} \bigwedge_{i<j<n} \neg v_i \equiv v_j ,$$

where the big conjunction is defined by

$$\bigwedge_{i<j<n} \psi_{ij} = \psi_{0,1} \wedge \ldots \wedge \psi_{0,n-1} \wedge \psi_{1,2} \wedge \ldots \wedge \psi_{1,n-1} \wedge \ldots \wedge \psi_{n-1,n-1} .$$

For any model $\mathfrak{M}$

$$\mathfrak{M} \vDash \varphi_{\geqslant n} \text{ iff } A \text{ has at least } n \text{ elements.}$$

Now set

$$\Phi' = \Phi \cup \{\varphi_{\geqslant n} \mid n \in \mathbb{N}\}.$$

(1) Φ' has a model.
Proof. By the compactness theorem 72b it suffices to show that every finite $\Phi_0 \subseteq \Phi$ has a model. Let $\Phi_0 \subseteq \Phi$ be finite. Take $n_0 \in \mathbb{N}$ such that

$$\Phi_0 \subseteq \Phi \cup \{\varphi_{\geqslant n} \mid n \leqslant n_0\}.$$

By assumption Φ has a model with at least n_0 elements. Thus $\Phi \cup \{\varphi_{\geqslant n} \mid n \leqslant n_0\}$ and Φ_0 have a model. *qed*(1)

Let $\mathfrak{M} \vDash \Phi'$. Then $\mathfrak{M}$ is an infinite model of Φ. □

Theorem 75. (Upward Löwenheim-Skolem theorem) *Let $\Phi \subseteq L^S$ have an infinite S-model and let X be an arbitrary set. Then Φ has a model into which X can be embedded injectively.*

Proof. Let $\mathfrak{M}$ be an infinite model of Φ. Choose a sequence $(c_x \mid x \in X)$ of pairwise distinct constant symbols which do not occur in S, e.g., setting $c_x = ((x, S), 1, 0)$. Let $S' = S \cup \{c_x \mid x \in X\}$ be the extension of S by the new constant symbols. Set

$$\Phi' = \Phi \cup \{\neg c_x \equiv c_y \mid x, y \in X, x \neq y\}.$$

(1) Φ' has a model.
Proof. It suffices to show that every finite $\Phi_0 \subseteq \Phi'$ has a model. Let $\Phi_0 \subseteq \Phi'$ be finite. Take a finite set $X_0 \subseteq X$ such that

$$\Phi_0 \subseteq \Phi \cup \{\neg c_x \equiv c_y \mid x, y \in X_0, x \neq y\}.$$

Since $|\mathfrak{M}|$ is infinite we can choose an injective sequence $(a_x | x \in X_0)$ of elements of $|\mathfrak{M}|$ such that $x \neq y$ implies $a_x \neq a_y$. For $x \in X \setminus X_0$ choose $a_x \in |\mathfrak{M}|$ arbitrarily. Then in the extended model

$$\mathfrak{M}' = \mathfrak{M} \cup \{(c_x, a_x) | x \in X\} \vDash \Phi \cup \{\neg c_x \equiv c_y \mid x, y \in X_0, x \neq y\} \supseteq \Phi_0 .$$

qed(1)

By (1), choose a model $\mathfrak{M}' \vDash \Phi'$. Then the map

$$i: X \to |\mathfrak{M}'|, x \mapsto \mathfrak{M}'(c_x)$$

is injective. The reduction $\mathfrak{M}'' = \mathfrak{M}' \upharpoonright \{\forall\} \cup S$ is as required. □

We define notions which allow to examine the axiomatizability of classes of structures.

Definition 76. *Let S be a language and $\mathcal{K}$ be a class of S-structures.*

a) $\mathcal{K}$ *ist* elementary *or* finitely axiomatizable *if there is an S-sentence φ with* $\mathcal{K} = \mathrm{Mod}^S\varphi$.

b) $\mathfrak{K}$ *is* Δ-elementary *or* axiomatizable, *if there is a set Φ of S-sentences with* $\mathcal{K} = \mathrm{Mod}^S\Phi$.

We state simple properties of the Mod-operator:

Theorem 77. *Let S be a language. Then*

a) *For* $\Phi \subseteq \Psi \subseteq L_0^S$ *holds* $\mathrm{Mod}^S\Phi \supseteq \mathrm{Mod}^S\Psi$.

b) *For* $\Phi, \Psi \subseteq L_0^S$ *holds* $\mathrm{Mod}^S(\Phi \cup \Psi) = \mathrm{Mod}^S\Phi \cap \mathrm{Mod}^S\Psi$.

c) *For* $\Phi \subseteq L_0^S$ *holds* $\mathrm{Mod}^S\Phi = \bigcap_{\varphi \in \Phi} \mathrm{Mod}^S\varphi$.

d) *For* $\varphi_0, \ldots, \varphi_{n-1} \in L_0^S$ *holds* $\mathrm{Mod}^S\{\varphi_0, \ldots, \varphi_{n-1}\} = \mathrm{Mod}^S(\varphi_0 \wedge \ldots \wedge \varphi_{n-1})$.

e) *For* $\varphi \in L_0^S$ *holds* $\mathrm{Mod}^S(\neg\varphi) = \mathrm{Mod}^S\emptyset \setminus \mathrm{Mod}^S(\varphi)$.

c) explains the denotation Δ-elementary, since $\mathrm{Mod}^S\Phi$ is the intersection ("**D**urchschnitt") of all single $\mathrm{Mod}^S\varphi$.

Theorem 78. *Let S be a language and $\mathcal{K}, \mathcal{L}$ be classes of S-structures with*

$$\mathcal{L} = \mathrm{Mod}^S\emptyset \setminus \mathcal{K}.$$

Then if $\mathcal{K}$ and $\mathcal{L}$ are axiomatizable, they are finitely axiomatizable.

Proof. Take axiom systems Φ_K and Φ_L such that $\mathfrak{K} = \mathrm{Mod}^S\Phi_K$ and $\mathfrak{L} = \mathrm{Mod}^S\Phi_L$. Assume that $\mathfrak{K}$ is not finitely axiomatizable.
(1) Let $\Phi_0 \subseteq \Phi_K$ be finite. Then $\Phi_0 \cup \Phi_L$ is satisfiable.
Proof: $\mathrm{Mod}^S\Phi_0 \supseteq \mathrm{Mod}^S\Phi_K$. Since $\mathfrak{K}$ is not finitely axiomatizable, $\mathrm{Mod}^S\Phi_0 \neq \mathrm{Mod}^S\Phi_K$. Then $\mathrm{Mod}^S\Phi_0 \cap \mathfrak{L} \neq \emptyset$. Take a model $\mathfrak{A} \in \mathfrak{L}$, $\mathfrak{A} \in \mathrm{Mod}^S\Phi_0$. Then $\mathfrak{A} \vDash \Phi_0 \cup \Phi_L$. *qed*(1)
(2) $\Phi_K \cup \Phi_L$ is satisfiable.
Proof: By the compactness theorem 72 it suffices to show that every finite $\Psi \subseteq \Phi_K \cup \Phi_L$ is satsifiable. By (1), $(\Psi \cap \Phi_K) \cup \Phi_L$ is satisfiable. Thus $\Psi \subseteq (\Psi \cap \Phi_K) \cup \Phi_L$ is satisfiable. *qed*(2)

By (2), $\mathrm{Mod}^S\Phi_K \cap \mathrm{Mod}^S\Phi_L \neq \emptyset$. But the classes $\mathfrak{K}$ and $\mathfrak{L}$ are complements, contradiction. Thus $\mathfrak{K}$ is finitely axiomatizable. □

Theorem 79. *Let S be a language.*

a) *The class of all finite S-structures is not axiomatizable.*

b) *The class of all infinite S-structures is axiomatizable but not finitely axiomatizable.*

c) *Let* $\Phi \subseteq L_0^S$ *such that* $\mathrm{Mod}^S\Phi$ *contains infinite structures. Then* $\mathrm{Mod}^S\Phi$ *contains structures of arbitrarily high cardinalities, i.e., for any set X there is a model $\mathfrak{M} \vDash \Phi$ and an injective map from X into M.*

Proof. a) is immediate by Theorem 74.
b) The class of infinite S-structures is axiomatized by

$$\Phi = \{\varphi_{\geqslant n} \mid n \in \mathbb{N}\}.$$

If that class were *finitely* axiomatizable then the complementary class of finite S-structures would also be (finitely) axiomatizable, contradicting a).
c) Let $\{c_x | x \in X\}$ be a set of "new" constant symbols. Let

$$\Phi_X = \Phi \cup \{\neg c_x \equiv c_y \mid x, y \in X, x \neq y\}.$$

Every finite subset of Φ_X is satisfiable in any infinite model of Φ. By the compactness theorem, Φ_X is consistent and satisfiable. Let $\mathfrak{M}_X \vDash \Phi_X$ and let $\mathfrak{M} = \mathfrak{M}_X \upharpoonright S \vDash \Phi$. Define $f: X \to M$ by

$$f(x) = \mathfrak{M}_X(c_x).$$

Then f is injective as required. □

17 Groups

Definition 80. *The* language of group theory *is the language*

$$S_{\mathrm{Gr}} = \{\circ, e\},$$

where $\circ$ *is a binary function symbol and* e *is a constant symbol. The* group axioms *are the following set of sentences:*

$$\Phi_{\mathrm{Gr}} = \{\forall v_0 \forall v_1 \forall v_2 \circ \circ v_0\, v_1\, v_2 \equiv \circ v_0 \circ v_1\, v_2\,, \forall v_0 \circ v_0\, e \equiv v_0\,, \forall v_0 \exists v_1 \circ v_0\, v_1 \equiv e\}.$$

A group *is an* S_{Gr}*-structure* $\mathfrak{G}$ *with* $\mathfrak{G} \vDash \Phi_{\mathrm{Gr}}$.

The group axioms may be written in a more familiar way with variables x, y, z, ..., infix notation and further abbreviations as

- $\forall x, y, z\ (x \circ y) \circ z \equiv x \circ (y \circ z)$ (associativity)
- $\forall x\, x \circ e \equiv x$ (neutral element)
- $\forall x \exists y\, x \circ y \equiv e$ (inverses)

Some elementary facts of group theory have short formal proofs. We show that the neutral element of a group is its own left inverse.

Theorem 81. $\Phi_{\mathrm{Gr}} \vdash \forall v_0\ (v_0 \circ e \equiv e \rightarrow v_0 \equiv e)$.

Proof.

Let $\forall x \forall y \forall z\, ((x*y)*z) = (x*(y*z))$.
Let $\forall x\, (x*e) = x$.
Let $\forall x \exists y\, (x*y) = e$.
Theorem. $\forall u\, ((u*e) = e \rightarrow u = e)$.
Proof. Let $(u*e) = e$. $(u*e) = u$. $u = (u*e)$. $u = e$.
Thus $\forall u\, ((u*e) = e \rightarrow u = e)$. Qed. □

Let us now consider some algebraic details.

Definition 82. *A group* $\mathfrak{G} = (G, \cdot, 1)$ *is a* torsion group *if for all* $g \in G$ *there is* $n \in \mathbb{N} \setminus \{0\}$ *with* $g^n = 1$. *Here,* g^n *is defined recursively by:* $g^0 = 1$, $g^{n+1} = g \cdot g^n$.

Theorem 83. *The class* $\mathcal{T}$ *of all torsion groups is not axiomatizable.*

Proof. Assume $\mathcal{T} = \mathrm{Mod}^{S_{\mathrm{Gr}}} \Phi$, where $\Phi \subseteq L_0^{S_{\mathrm{Gr}}}$. Define

$$\Psi = \Phi \cup \{\neg \underbrace{v_0 \circ \ldots v_0}_{n-\text{times}} \equiv e \,|\, n \in \mathbb{N} \setminus \{0\}\}.$$

Every finite subset of Ψ is satisfiable: Consider a finite $\Psi_0 \subseteq \Psi$. Take $n_0 \in \mathbb{N}$ such that

$$\Psi_0 \subseteq \Phi \cup \{\neg \underbrace{v_0 \circ \ldots v_0}_{n-\text{times}} \equiv e \,|\, 1 \leqslant n \leqslant n_0\}.$$

The right-hand side can be satisfied in every torsion group which has an element of *order* $\geqslant n_0$, e.g., in the additive group of integers *modulo* n_0. Bei the compactness theorem 72, Ψ is satisfiable. Take a model $\mathcal{G} \vDash \Psi$. Then $\mathcal{G}$ is a group in which the element $\mathcal{G}(v_0)$ satisfies all formulas

$$\neg \underbrace{v_0 \circ \ldots v_0}_{n-\text{times}} \equiv e.$$

Hence $\mathcal{G}(v_0)$ has infinite order in $\mathcal{G}$ and $\mathcal{G}$ is not a torsion group, although $\mathcal{G} \vDash \Phi$. Contradiction. □

This theorem demonstrates that mathematical logic also examines the limits of its methods: torsion groups *cannot* be axiomatized in the language of group theory. It is however possible to characterize torsion groups in stronger theories, where the formation of powers v_0^n is uniformly available.

There are several ways to logically treat group theory. One could for example include inversion as a function symbol.

Definition 84. *The* extended language of group theory *is the language*

$$S_{\mathrm{Gr}'} = \{\circ, i, e\},$$

where i is a unary function symbol. The extended group axioms *consist of the axioms*

$$\Phi_{\mathrm{Gr}'} = \{\forall v_0 \forall v_1 \forall v_2 \circ \circ v_0\, v_1\, v_2 \equiv \circ v_0 \circ v_1\, v_2\, , \forall v_0 \circ v_0\, e \equiv v_0\, , \forall v_0 \circ v_0\, i\, v_0 \equiv e\}.$$

An extended group *is an $S_{\mathrm{Gr}'}$-structure $\mathfrak{G}$ with $\mathfrak{G} \vDash \Phi_{\mathrm{Gr}'}$.*

Obviously every extended group can be reduced to a group in the former sense and vice versa. There are, however, model theoretic differences, e.g., concerning substructures.

Theorem 85. *A substructure of a group need not be a group. A substructure of an extended group is an extended group.*

This fact is due to the syntactic structure of the axioms considered.

18 Fields

Fields are *arithmetical structures*, i.e., a field allows addition and multiplication. We describe filed in the *language of arithmetic*

$$S_{\mathrm{Ar}} = \{+, \cdot, 0, 1\}$$

with the usual conventions for infix notation and bracket notation. The axiom system Φ_{Fd} of *field theory* consists of the following axioms:

- $\forall x \forall y \forall z\, (x + y) + z \equiv x + (y + z)$
- $\forall x \forall y \forall z\, (x \cdot y) \cdot z \equiv x \cdot (y \cdot z)$
- $\forall x \forall y x + y \equiv y + x$
- $\forall x \forall y x \cdot y \equiv y \cdot x$
- $\forall x x + 0 \equiv x$
- $\forall x x \cdot 1 \equiv x$
- $\forall x \exists y x + y \equiv 0$
- $\forall x (\neg x \equiv 0 \rightarrow \exists y x \cdot y \equiv 1)$
- $\neg 0 \equiv 1$
- $\forall x \forall y \forall z\, x \cdot (y + z) \equiv (x \cdot y) + (x \cdot z)$

A *field* is an S_{Ar}-model satisfying Φ_{Fd}. The axiom system Φ_{Fd} is not *complete*. There are, e.g., finite and infinite fields and thus there is a natural number n such that the axioms do not decide the sentence $\varphi_{=n}$ which expresses that there are exactly n elements.

Substantial parts of mathematics can be carried out within field theory. Vectors of a finite-dimensional vector space over a field $\mathbb{K}$ can be represented as finite tuples from $\mathbb{K}$. The laws of vector and matrix calculus are sentences about appropriately indexed field elements. Thus the theory of finite-dimensional vector spaces can be carried out within field theory. Technically we say that the theory of n-dimensional vector spaces can be *interpreted* within the theory of fields. That $(z_0, \ldots, z_{n-1})$ is the *vector sum* of $(x_0, \ldots, x_{n-1})$ and $(y_0, \ldots, y_{n-1})$ can be expressed by the S_{Ar}-formula

$$z_0 \equiv x_0 + x_1 \wedge \ldots \wedge z_{n-1} \equiv x_{n-1} + y_{n-1}\, .$$

The *linear independence* of $(x_0, \ldots, x_{n-1})$ and $(y_0, \ldots, y_{n-1})$ is formalizable by

$$\forall\lambda\forall\mu\,((\bigwedge_{i=0}^{n-1} \lambda\cdot x_i + \mu\cdot y_i \equiv 0) \rightarrow (\lambda\equiv 0 \wedge \mu\equiv 0)).$$

Analytic geometry provides means to translate geometric statements into field theory.

18.1 The characteristic of a field

We study some logical aspects of an important field invariant, namely its *characteristic.*

Definition 86. *A field* $\mathbb{K} = (\mathbb{K}, +, \cdot, 0, 1)$ *has* characteristic p, *if* p *is the minimal integer* >0 *such that*

$$\underbrace{1+\ldots+1}_{p-times} = 0.$$

If such a p *exists then* p *is a prime number. Otherwise the* characteristic *of* $\mathbb{K}$ *is defined to be* 0.

Fields of characteristic p can be axiomatized by

$$\Phi_{\mathrm{Fd},p} = \Phi_{\mathrm{Fd}} \cup \{\underbrace{1+\ldots+1}_{p-\mathrm{times}} \equiv 0\},$$

and fields of characteristic 0 by

$$\Phi_{\mathrm{Fd},0} = \Phi_{\mathrm{Fd}} \cup \{\underbrace{1+\ldots+1}_{n-\mathrm{times}} \not\equiv 0 \,|\, n\in\mathbb{N}\setminus\{0\}\}.$$

The axiom system $\Phi_{\mathrm{Fd},0}$ is infinite.

Theorem 87. *The class of fields of characteristic* 0 *cannot be finitely axiomatized.*

Proof. Assume for a contradiction that the sentence φ_0 axiomatizes the class under consideration. Then

$$\Phi_{\mathrm{Fd},0} \vDash \varphi_0 \text{ and } \{\varphi_0\} \vDash \Phi_{\mathrm{Fd},0}\,.$$

By the compactness theorem there is a finite $\Phi_0 \subseteq \Phi_{\mathrm{Fd},0}$ such that

$$\Phi_0 \vDash \varphi_0 \text{ and } \{\varphi_0\} \vDash \Phi_0\,.$$

Without loss of generality, Φ_0 is of the form

$$\Phi_0 = \Phi_{\mathrm{Fd}} \cup \{\underbrace{1+\ldots+1}_{n-\mathrm{times}} \not\equiv 0 \,|\, n = 1, \ldots, n_0\}.$$

This set is equivalent to $\Phi_{\mathrm{Kp},0}$ and also axiomatizes the class of fields of characteristic 0. Take a prime number $p > n_0$. Then the field $\mathbb{K}_p$ of integers *modulo* p has characteristic p and $\mathbb{K}_p \vDash \Phi_0$. But then Φ_0 does *not* axiomatize the class of fields of characteristic 0. Contradiction. □

18.2 Algebraically closed fields

Definition 88. *A field* $\mathbb{K}$ *is* algebraically closed *if every polynomial of degree* $\geqslant 1$ *has a zero in* $\mathbb{K}$.

A polynomial

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

is determined by the sequence $a_{n-1}, \ldots, a_0$ of coefficients. The following axiomatizes algebraically closed fields:

$$\Phi_{\mathrm{acf}} = \Phi_{\mathrm{Fd}} \cup \{\forall a_{n-1} \ldots \forall a_0 \exists x\, x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \equiv 0 \,|\, n\in\mathbb{N}\setminus\{0\}\}.$$

Here x^i denotes the term $\underbrace{x\cdot x\cdots x}_{i-\mathrm{times}}$.

19 Dense linear orders

The structure $\mathbb{Q} = (\mathbb{Q}, <)$ is an example of a *dense linear order*.

Definition 89. *Let* $S_{\text{so}} = \{<\}$ *be the language of* strict orders*. The system* Φ_{slo} *axiomatizing* strict linear orders *consists of the sentences*

- $\forall x \neg x < x$
- $\forall x \forall y \forall z\, (x < y \wedge y < z \rightarrow x < z)$
- $\forall x \forall y\, (x < y \vee x = y \vee y < x)$

The system Φ_{dlo} *axiomatizing* dense linear orders (without endpoints) *consists of* Φ_{slo} *and*

- $\forall x \exists y\, x < y$
- $\forall x \exists y\, y < x$
- $\forall x \forall y\, (x < y \rightarrow \exists z\, (x < z \wedge z < y))$

The following theorem was shown by GEORG CANTOR.

Theorem 90. *Let* $X = (X, <^X)$ *and* $Y = (Y, <^Y)$ *be countable dense linear orders. Then* X *and* Y *are isomorphic.*

Proof. Let $X = \{x_i | i \in \omega\}$ and $Y = \{y_j | j \in \omega\}$. Define a sequence $(f_n | n \in \omega)$ of maps $f_n: X_n \rightarrow Y_n$ such that
(1) $X_n \subseteq X$ and $Y_n \subseteq Y$ have cardinality n;
(2) $f_n: (X_n, <^X \cap X_{n)}^2) \rightarrow (Y_n, <^Y \cap Y_n^2)$ is an isomorphism.

Set $f_0 = X_0 = Y_0 = \emptyset$.

Assume that f_{2n} is constructed according to (1) and (2). Let

$$X_{2n} = \{u_0, \ldots, u_{2n-1}\} \text{ with } u_0 <^X u_1 <^X \ldots <^X u_{2n-1}$$

and

$$Y_{2n} = \{v_0, \ldots, v_{2n-1}\} \text{ with } v_0 <^Y v_1 <^Y \ldots <^Y v_{2n-1}\,.$$

Take $i \in \omega$ minimal such that $x_i \notin X_{2n}$.
Case 1: $x_i <^X u_0$. Then take $j \in \omega$ minimal such that $y_j <^Y v_0$.
Case 2: $u_0 <^X x_i <^X u_{2n-1}$. Take $k < 2n - 1$ such that $u_k <^X x_i <^X u_{k+1}$. Take $j \in \omega$ minimal such that $v_k <^Y y_j <^Y v_{k+1}$.
Case 3: $u_{2n-1} <^X x_i$. Take $j \in \omega$ minimal such that $v_{2n-1} <^Y y_j$.

In all three cases set

$$X_{2n+1} = X_{2n} \cup \{x_i\},\, Y_{2n+1} = Y_{2n} \cup \{y_j\},\, f_{2n+1} = f_{2n} \cup \{(x_i, y_j)\}.$$

Then f_{2n+1} is constructed according to (1) and (2).

Now let

$$X_{2n+1} = \{u_0, \ldots, u_{2n}\} \text{ with } u_0 <^X u_1 <^X \ldots <^X u_{2n}$$

and

$$Y_{2n+1} = \{v_0, \ldots, v_{2n}\} \text{ with } v_0 <^Y v_1 <^Y \ldots <^Y v_{2n}\,.$$

Take $j \in \omega$ minimal such that $y_j \notin Y_{2n+1}$.
Case 1': $y_j <^Y v_0$. Then take $i \in \omega$ minimal such that $x_i <^X u_0$.
Case 2': $v_0 <^Y y_j <^Y v_{2n}$. Take $k < 2n$ such that $v_k <^Y y_j <^Y v_{k+1}$. Take $i \in \omega$ minimal such that $u_k <^X x_i <^X u_{k+1}$.
Case 3': $v_{2n} <^Y y_j$. Take $i \in \omega$ minimal such that $u_{2n} <^X x_i$.

In all three cases set

$$X_{2n+2} = X_{2n+1} \cup \{x_i\},\, Y_{2n+2} = Y_{2n+1} \cup \{y_j\},\, f_{2n+2} = f_{2n+1} \cup \{(x_i, y_j)\}.$$

Then f_{2n+2} is constructed according to (1) and (2).

Obviously, $f_0 \subseteq f_1 \subseteq f_2 \subseteq \ldots$. Let $f = \bigcup_{n \in \omega} f_n$. Then

$$f: (X, <^X) \cong (Y, <^Y). \qquad \square$$

We draw some logical consequences from this isomorphism result.

Definition 91. *Let S be a language. An S-*theory *is a consistent set $\Phi \subseteq L_0^S$ of sentences. A set $\Phi \subseteq L_0^S$ is* complete *if for every $\varphi \in L_0^S$*

$$\Phi \vdash \varphi \textit{ gdw. } \Phi \nvdash \neg\varphi.$$

A complete theory $\Phi \subseteq L_0^S$ "decides" all "questions" which can be posed in the language S. The theories Φ_{Gr} and Φ_{Fd} are not complete. Obviously:

Proposition 92. *Let $\mathfrak{A}$ be an S-structure. Let*

$$\mathrm{Th}(\mathfrak{A}) = \{\varphi \in L_0^S \mid \mathfrak{A} \vDash \varphi\}$$

be the theory *of $\mathfrak{A}$. Then $\mathrm{Th}(\mathfrak{A})$ is complete.*

Definition 93. *Let S be a language and $\Phi \subseteq L_0^S$. Then Φ is ω-*categorical*, if all countably infinite structures $\mathfrak{A} \vDash \Phi$ and $\mathfrak{B} \vDash \Phi$ are isomorphic.*

Theorem 94. *Let S be a countable language and let $\Phi \subseteq L_0^S$ be a consistent ω-categorical set of sentences which has no finite models. Then Φ is complete.*

Proof. Let $\varphi \in L_0^S$. Assume $\Phi \vdash \varphi$. Then $\Phi \nvdash \neg\varphi$ since Φ is consistent.

Conversely assume $\Phi \nvdash \neg\varphi$. Assume for a contradiction that $\Phi \nvdash \varphi$. Then $\Phi \cup \{\varphi\}$ und $\Phi \cup \{\neg\varphi\}$ are consistent. By the LÖWENHEIM-SKOLEM theorem 69 there are countable models $\mathfrak{A}_0 \vDash \Phi \cup \{\varphi\}$ and $\mathfrak{A}_1 \vDash \Phi \cup \{\neg\varphi\}$. Since Φ has not finite models, $\mathfrak{A}_0$ and $\mathfrak{A}_1$ are both countably infinite. By ω-categoricity, $\mathfrak{A}_0$ and $\mathfrak{A}_1$ are isomorphic. But $\mathfrak{A}_0 \vDash \varphi$ and $\mathfrak{A}_1 \vDash \neg\varphi$. Contradiction. $\square$

As an immediate corollary of the previous theorems we obtain:

Theorem 95. *The theory Φ_{dlo} is complete.*

By a main theorem of algebra an algebraically closed field is determined by its characteristic and its *transcendence degree* up to isomorphism. Given an appropriate theory of uncountable cardinalities this implies that two algebraically closed fields of characteristic 0 and of the same *uncountable* cardinality are isomorphic. By arguments similar to the countable case one can show:

Theorem 96. *The theory of algebraically closed fields of characteristic* 0 *is complete.*

20 Peano arithmetic

The language of arithmetic can also be interpreted in the structure $\mathbb{N} = (\mathbb{N}, +, \cdot, 0, 1)$ of integers. We formulate a theory which attempts to describe this structure.

Definition 97. *The axiom system* PA $\subseteq L^{S_{\mathrm{AR}}}$ *of* PEANO arithmetic *consists of the following sentences*

- $\forall x\, x + 1 \neq 0$
- $\forall x \forall y\; x + 1 = y + 1 \rightarrow x = y$
- $\forall x\, x + 0 = x$
- $\forall x \forall y\; x + (y + 1) = (x + y) + 1$
- $\forall x\, x \cdot 0 = 0$

- $\forall x \forall y\, x \cdot (y+1) = x \cdot y + x$
- *Schema of induction: for every formula* $\varphi(x_0, \ldots, x_{n-1}, x_n) \in L^{S_{\mathrm{AR}}}$*:*

$$\forall x_0 \ldots \forall x_{n-1}(\varphi(x_0, \ldots, x_{n-1}, 0) \wedge \forall x_n(\varphi \rightarrow \varphi(x_0, \ldots, x_{n-1}, x_n + 1)) \rightarrow \forall x_n\, \varphi)$$

Then $\mathbb{N} \vDash \mathrm{PA}$. The first incompleteness theorem of Gödel shows that PA is *not* complete, i.e., there are arithmetic sentences which are not decided by PA although in the standard model they have to be either true or false, and they really are true if one is working in a meta-theory which is able to construct the model $\mathbb{N}$.

21 Nonstandard analysis

Analysis was developed using *infinitesimal* numbers. Although infinitesimals in most cases lead to correct results, they are nevertheless paradoxical object (arbitrarily small but not equal to 0) which gave rise to severe foundational controversies.

The following is a caricature of the use of infinitesimals: To determine the derivation of $f = x^2$ in a take an infinitesimal ε and form the difference quotient

$$\frac{(a+\varepsilon)^2 - a^2}{\varepsilon} = \frac{a^2 + 2a\varepsilon + \varepsilon^2 - a^2}{\varepsilon} = 2a + \varepsilon\,.$$

Setting $\varepsilon = 0$, after all, we obtain

$$f'(a) = 2a\,.$$

It is difficult to account for this recipe in terms of a single structure. It seems that there is a structure of *standard* numbers like 0, 2, a, ... in which we want to know the result of the argument. For the argument, however, one seems to enrich the domain by *nonstandard* numbers like $\varepsilon, a + \varepsilon, \ldots$. The nonstandard numbers are then projected back into the standard numbers.

This idea was put on firm foundations by Abraham Robinson, the inventor of *nonstandard analysis*. We give a small impression of this field, emphasizing logical aspects. We extend the structure $\mathbb{R}$ of standard reals to a structure $\mathbb{R}^*$ which also contains "infinitesimals". There is a partial map $\mathrm{st}\colon \mathbb{R} \rightharpoonup \mathbb{R}^*$ which maps an infinitesimal ε to 0.

So let

$$\mathbb{R} = (\mathbb{R}, <, +, \cdot, (r | r \in \mathbb{R}), f, g)$$

be the standard strictly ordered field of reals enriched by constants r for every $r \in \mathbb{R}$ and by unary functions f and g. Let S be an appropriate symbol set for this structure. For simplicity we identify the symbols with their interpretation in $\mathbb{R}$. Let

$$T = \mathrm{Th}(\mathbb{R}) = \{\varphi \in L_0^S | \mathbb{R} \vDash \varphi\}$$

be the theory of $\mathbb{R}$. Let ε be a new constant symbol (for an infinitesimal) and $S^* = S \cup \{\varepsilon\}$. The set

$$T^* = T \cup \{0 < \varepsilon \wedge \varepsilon < r | r \in \mathbb{R} \wedge 0 < r\}$$

of S^*-sentences expresses that ε lies between 0 and all positive standard reals, i.e., that ε is an infinitesimal. Every finite subset $T' \subseteq T^*$ can be satisfied by the structure

$$\mathbb{R}' = (\mathbb{R}, <, +, \cdot, (r | r \in \mathbb{R}), f, g, e)$$

where ε is interpreted by a positive real number e which is smaller than the finitely many positive reals r such that r occurs in the finite set T'. Hence T^* is consistent and satisfiable, and we let

$$(\mathbb{R}^*, <^*, +^*, \cdot^*, (r^* | r \in \mathbb{R}), f^*, g^*, \varepsilon^*) \vDash T^*$$

where ε^* interprets ε. Restrict that structure to the language S to obtain

$$\mathbb{R}^* = (\mathbb{R}^*, <^*, +^*, \cdot^*, (r^* | r \in \mathbb{R}), f^*, g^*) \vDash T\,.$$

Embed $\mathbb{R}$ into $\mathbb{R}^*$ by

$$r \mapsto r^*.$$

Since the theory T contains all first-order information about all elements of $\mathbb{R}$ we get that the embedding is elementary. Via the embedding, we can identify r and r^* for $r \in \mathbb{R}$. Moreover, the relations and functions of $\mathbb{R}^*$ are extension of the corresponding functions in $\mathbb{R}$. We may thus denote the components of $\mathbb{R}^*$ just like the components of $\mathbb{R}$:

$$\mathbb{R}^* = (\mathbb{R}^*, <, +, \cdot, (r | r \in \mathbb{R}), f, g).$$

After the identification we get

Proposition 98. $\mathbb{R}$ *is a proper elementary substructure of* $\mathbb{R}^*$*:* $\mathbb{R} \prec \mathbb{R}^*$.

Proof. Since $0 < \varepsilon < r$ for every positive $r \in \mathbb{R}$ we have $\varepsilon \notin \mathbb{R}$ and $\mathbb{R} \neq \mathbb{R}^*$. □

We now connect the structure $\mathbb{R}^*$ back to $\mathbb{R}$:

Definition 99.

a) $u \in \mathbb{R}^*$ *is* finite *if there are* $a, b \in \mathbb{R}$ *such that* $a < u < b$.

b) $u \in \mathbb{R}^*$ *is* infinite *if* u *is not finite.*

c) *For finite* $u \in \mathbb{R}^*$ *define the* standard part

$$\mathrm{st}(u) = \sup{}_{\mathbb{R}}\{r \in \mathbb{R} | r < u\}$$

as a supremum in the standard numbers. Note that st: $\mathbb{R}^* \rightharpoonup \mathbb{R}$ *is a partial function defined on the finite elements of* $\mathbb{R}^*$.

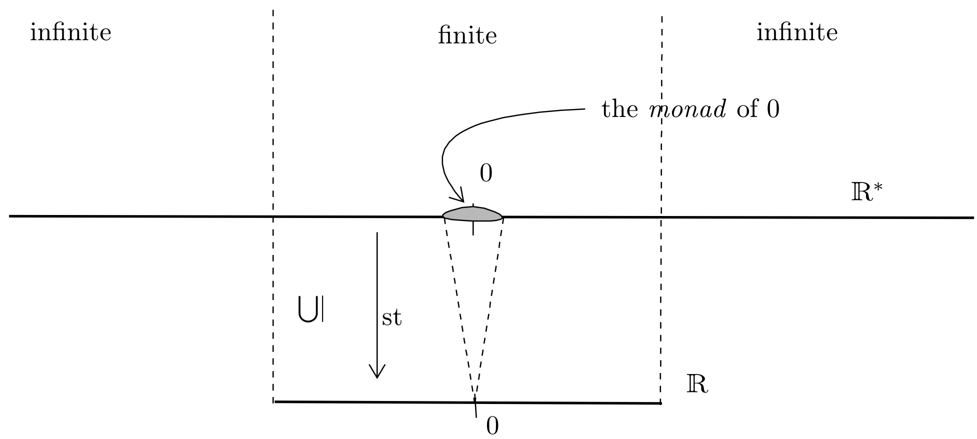
d) $u \in \mathbb{R}^*$ *is* infinitesimal *if* $\mathrm{st}(u) = 0$.

e) $u, v \in \mathbb{R}^*$ *are* infinitesimally near, $u \sim v$, *if* $u - v$ *is infinitesimal.*

Note that by the inequalities $0 < \varepsilon \wedge \varepsilon < r \in T^*$

$$\mathrm{st}(\varepsilon^*) = \sup{}_{\mathbb{R}}\{r \in \mathbb{R} | r < \varepsilon^*\} = \sup{}_{\mathbb{R}}\{r \in \mathbb{R} | r \leqslant 0\} = 0.$$

So $\mathbb{R}^*$ possesses an infinitesimal element $\neq 0$. The two models may be represented graphically by



Proposition 100.

a) *If* $s \in \mathbb{R}$ *then* $\mathrm{st}(s) = s$.

b) $u \in \mathbb{R}^*$ *is infinitesimal iff* $\forall s \in \mathbb{R}\, (s > 0 \rightarrow |u| < s)$.

c) *If* $u \sim 0$ *and* $|v| < |u|$ *then* $v \sim 0$.

d) *Let* $u \sim u'$ *and* $v \sim v'$. *Then* $u + v \sim u' + v'$.

e) *Let* $u \sim u'$, $v \sim v'$, *and* u, v *be finite. Then* $u \cdot v \sim u' \cdot v'$.

Proof. a) $\mathrm{st}(s) = \sup_{\mathbb{R}} \{r \in \mathbb{R} | r < s\} = s$.
b) Let $\mathrm{st}(u) = 0$. Let $s \in \mathbb{R}$, $s > 0$. Assume for a contradiction that $-s \geqslant u$. Then

$$\mathrm{st}(u) \leqslant \mathrm{st}(-s) = -s < 0,$$

contradiction. Assume for a contradiction that $u \geqslant s$. Then

$$\mathrm{st}(u) \geqslant \mathrm{st}(s) = s > 0,$$

contradiction. Thus $-s < u < s$, i.e., $|u| < s$.
c) follows immediately from b).
d) Let $s \in \mathbb{R}$, $s > 0$. By assumption, $|u - u'| < \frac{s}{2}$ and $|v - v'| < \frac{s}{2}$. Then

$$|(u + v) - (u' + v')| = |(u - u') + (v - v')| \leqslant |u - u'| + |v - v'| < \frac{s}{2} + \frac{s}{2} = s.$$

By b), $u + v \sim u' + v'$.
e) Choose $a \in \mathbb{R}$ such that $|u|, |v|, |u'|, |v'| < a$. Let $s \in \mathbb{R}$, $s > 0$. By assumption, $|u - u'| < \frac{s}{2a}$ and $|v - v'| < \frac{s}{2a}$. Then

$$\begin{aligned} |u \cdot v - u' \cdot v'| &= |u \cdot v - u \cdot v' + u \cdot v' - u' \cdot v'| \\ &\leqslant |u \cdot v - u \cdot v'| + |u \cdot v' - u' \cdot v'| \\ &= |u| \cdot |v - v'| + |u - u'| \cdot |v'| \\ &\leqslant a \cdot \frac{s}{2a} + a \cdot \frac{s}{2a} = s. \end{aligned}$$

By b), $u \cdot v \sim u' \cdot v'$. ☐

To demonstrate the potential of the standard-nonstandard setup we give a nonstandard characterization of when the function $g: \mathbb{R} \to \mathbb{R}$ is the derivative f' of the function f.

Theorem 101. $g = f'$ *iff the following criterion holds:*

$$\forall x \in \mathbb{R} \forall \xi \in \mathbb{R}^* \setminus \{0\} \, (\xi \sim 0 \to g(x) \sim \frac{f(x + \xi) - f(\xi)}{\xi}).$$

Proof. To deal with difference quotients we use the common absolute value notation

$$\left| a - \frac{b - c}{d} \right| < e.$$

This abbreviates the formula

$$(d > 0 \to -de < da - b + c \wedge da - b + c < de) \wedge (d < 0 \to de < da - b + c \wedge da - b + c < -de)$$

where we assume $d \neq 0$.

Assume $g = f'$. Let $x \in \mathbb{R}$, $\delta \in \mathbb{R}^* \setminus \{0\}$, and $\delta \sim 0$. To check whether $g(x) \sim \frac{f(x + \xi) - f(\xi)}{\xi}$ let $\eta \in \mathbb{R}$, $\eta > 0$. Since $g(x) = f'(x)$ there exists $\delta \in \mathbb{R}$, $\delta > 0$ such that

$$\mathbb{R} \vDash \forall \delta' \neq 0 \, (|\delta'| < \delta \to \left| g(x) - \frac{f(x + \delta') - f(\delta')}{\delta'} \right| < \eta).$$

This S-sentence is an element of the theory T, and therefore it also holds in $\mathbb{R}^*$:

$$\mathbb{R}^* \vDash \forall \delta' \neq 0 \, (|\delta'| < \delta \to \left| g(x) - \frac{f(x + \delta') - f(\delta')}{\delta'} \right| < \eta).$$

The process of going from $\mathbb{R}$ to $\mathbb{R}^*$ like this or vice versa is called *transfer*; it is one of the most important techniques of nonstandard analysis. We can set $\delta' = \xi$ and get

$$\left| g(x) - \frac{f(x + \xi) - f(\xi)}{\xi} \right| < \eta.$$

Since this holds for every positive $\eta \in \mathbb{R}$ we have

$$g(x) \sim \frac{f(x+\xi) - f(\xi)}{\xi}$$

as required.

Conversely assume that $g \neq f'$. Take $x \in \mathbb{R}$ such that $g(x) \neq f'(x)$. Then there is $\eta \in \mathbb{R}$, $\eta > 0$ such that

$$\mathbb{R} \vDash \forall \delta > 0 \exists \delta', \delta' \neq 0 |\delta'| < \delta \left| g(x) - \frac{f(x+\delta') - f(\delta')}{\delta'} \right| \geqslant \eta.$$

We transfer this property to $\mathbb{R}^*$:

$$\mathbb{R}^* \vDash \forall \delta > 0 \exists \delta', \delta' \neq 0 |\delta'| < \delta \left| g(x) - \frac{f(x+\delta') - f(\delta')}{\delta'} \right| \geqslant \eta.$$

Take some positive *infinitesimal* $\delta \in \mathbb{R}^*$, $\delta > 0$ and apply the last property: there exists $\xi \in \mathbb{R}^* \setminus \{0\}$, $|\xi| < \delta$ such that

$$\left| g(x) - \frac{f(x+\xi) - f(\xi)}{\xi} \right| \geqslant \eta.$$

Since $|\xi| < \delta$ we have that $\xi \sim 0$. Hence

$$g(x) \nsim \frac{f(x+\xi) - f(\xi)}{\xi}.$$

This shows that the criterion is false in case $g \neq f'$. □

The nonstandard criterion for the derivation can be applied in proving the usual laws of the differential calculus. As an example we show the product rule.

Theorem 102. *Let f, g: $\mathbb{R} \to \mathbb{R}$ be differentiable functions. Then the product $f \cdot g$ is differentiable and*

$$(f \cdot g)' = f' \cdot g + f \cdot g'.$$

Proof. The criterion of the previous theorem is satisfied by f', f and g', g respectively. We now show the criterion for $f' \cdot g + f \cdot g'$ and $f \cdot g$. Let $x \in \mathbb{R}$ and $\xi \in \mathbb{R}^* \setminus \{0\}$, $\xi \sim 0$. Calculate in $\mathbb{R}^*$:

$$\begin{aligned}
\frac{(f \cdot g)(x+\xi) - (f \cdot g)(x)}{\xi} &= \frac{f(x+\xi) \cdot g(x+\xi) - f(x) \cdot g(x)}{\xi} \\
&= \frac{f(x+\xi) \cdot g(x+\xi) - f(x) \cdot g(x+\xi) + f(x) \cdot g(x+\xi) - f(x) \cdot g(x)}{\xi} \\
&= \frac{f(x+\xi) - f(x)}{\xi} \cdot g(x+\xi) + f(x) \cdot \frac{g(x+\xi) - g(x)}{\xi}.
\end{aligned}$$

By assumption, $\frac{f(x+\xi) - f(x)}{\xi} \sim f'(x)$ and $\frac{g(x+\xi) - g(x)}{\xi} \sim g'(x)$. The latter near-equality also implies $g(x+\xi) \sim g(x)$. Since $\sim$ commutes with arithmetic operations,

$$\begin{aligned}
\frac{(f \cdot g)(x+\xi) - (f \cdot g)(x)}{\xi} &= \frac{f(x+\xi) - f(x)}{\xi} \cdot g(x+\xi) + f(x) \cdot \frac{g(x+\xi) - g(x)}{\xi} \\
&\sim f'(x) \cdot g(x) + f(x) \cdot g'(x)
\end{aligned}$$

as required. □

The treatment of differentiation has demonstrated that the nonstandard theory allows different argumentations from the standard theory. The relation $\sim$ of nearness allows to to dispense with some explicit calculations of inequalities. Of course the basic laws of the $\sim$-relation were proved using explicit estimates. The use of infinitesimals also seems to eliminate some quantifiers: some familiar properties of the form $\forall \varepsilon \exists \delta \ldots$ can be replaced by properties of the form $\forall \xi \sim 0 \ldots$.

On the other side, one has to be caefully distinguish whether one is working in the standard model or the nonstandard extension. Particular combinations of standard and nonstandard variables are often crucial. A function $f:\mathbb{R}\rightarrow\mathbb{R}$ is continuous iff

$$\forall x\in\mathbb{R}\forall x'\in\mathbb{R}^*(x\sim x'\rightarrow f(x)\sim f(x')).$$

The similar looking property

$$\forall x\in\mathbb{R}^*\forall x'\in\mathbb{R}^*(x\sim x'\rightarrow f(x)\sim f(x'))$$

where both variables range over $\mathbb{R}^*$ is much more restrictive and describes some class of "strongly continuous" functions.

22 ZERMELO-FRAENKEL set theory

All mathematical notions can be defined set-theoretically. The notion of set is adequately formalized in a first-order axiom system introduced by ZERMELO, FRAENKEL and others. Together with the GÖDEL completeness theorem for first-order logic this constitutes a "formalistic" answer to the question "what is mathematics": mathematics consists of formal proofs from the axioms of ZERMELO-FRAENKEL set theory.

We shall first give the axioms ZF of ZERMELO-FRAENKEL set theory, but we shall then develop set theory ZF − Inf without the axiom of infinity.We shall see that ZF − Inf has the same "strength" as first-order Peano arithmetic PA.

Full ZERMELO-FRAENKEL set theory as a foundation for all of mathematics. It will be developed as an independent mathematical theory in the set theory course.

Definition 103. *Let* $\in$ *be a binary infix relation symbol; read* $x\in y$ *as "x is an* element *of y". The* language of set theory *is the language* $\{\in\}$*. The formulas in* $L^{\{\in\}}$ *are called* set theoretical formulas *or* $\in$*-formulas. We write* $L^{\in}$ *instead of* $L^{\{\in\}}$*.*

The "naive" notion of *set* is intuitively understood and was used extensively in previous chapters. The following axioms describe properties of naive sets. Note that the axiom system is an infinite collection - or set - of axioms. It seems unavoidable that we have to go back to some previously given set notions to be able to define the collection of set theoretical axioms - another example of circularity in foundational theories.

Definition 104. *The system* ZF *of the* ZERMELO-FRAENKEL axioms of set theory *consists of the following axioms:*

a) *The* axiom of extensionality (Ext)*:*

$$\forall x\forall y(\forall z(z\in x\leftrightarrow z\in y)\rightarrow x\equiv y)$$

- a set is determined by its elements, sets having the same elements are identical.

b) *The* axiom of set existence (Ex)*:*

$$\exists x\forall y\neg y\in x$$

- there is a set without elements, the empty set*.*

c) *The* separation schema (Sep) *postulates for every* $\in$*-formula* $\varphi(z,x_1,\ldots,x_n)$*:*

$$\forall x_1\ldots\forall x_n\forall x\exists y\forall z\,(z\in y\leftrightarrow z\in x\wedge\varphi(z,x_1,\ldots,x_n))$$

- this is an infinite scheme of axioms, the set z consists of all elements of x which satisfy φ*.*

d) *The* pairing axiom (Pair)*:*

$$\forall x\forall y\exists z\forall w\,(w\in z\leftrightarrow w\equiv x\vee w\equiv y).$$

- z is the unordered pair of x and y.

e) *The* union axiom (Union)*:*

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

- y is the union of all elements of x.

f) *The* powerset axiom (Pow)*:*

$$\forall x\exists y\forall z(z\in y\leftrightarrow\forall w(w\in z\rightarrow w\in x))$$

- y consists of all subsets of x.

g) *The* axiom of infinity (Inf)*:*

$$\exists x(\exists y\,(y\in x\wedge\forall z\neg z\in y)\wedge\forall y(y\in x\rightarrow\exists z(z\in x\wedge\forall w(w\in z\leftrightarrow w\in y\vee w\equiv y))))$$

- by the closure properties of x, x has to be infinite.

h) *The* replacement schema (Rep) *postulates for every $\in$-formula $\varphi(x,y,x_1,\ldots,x_n)$:*

$$\forall x_1\ldots\forall x_n(\forall x\forall y\forall y'((\varphi(x,y,x_1,\ldots,x_n)\wedge\varphi(x,y',x_1,\ldots,x_n))\rightarrow y\equiv y')\rightarrow \forall u\exists v\forall y\,(y\in v\leftrightarrow\exists x(x\in u\wedge\varphi(x,y,x_1,\ldots,x_n))))$$

- v is the image of u under the map defined by φ.

i) *The* foundation schema (Found) *postulates for every $\in$-formula $\varphi(x,x_1,\ldots,x_n)$:*

$$\forall x_1\ldots\forall x_n(\exists x\varphi(x,x_1,\ldots,x_n)\rightarrow\exists x(\varphi(x,x_1,\ldots,x_n)\wedge\forall x'(x'\in x\rightarrow\neg\varphi(x',x_1,\ldots,x_n))))$$

- if φ is satisfiable then there are $\in$-minimal elements x satisfying φ; such x can be called $\in$-minimal examples *or* counterexamples*, depending on the situation.*

By $\mathrm{ZF}-\mathrm{Inf}$ *or by* ST *we denote the above list of axiom, omitting the axiom of infinity. By* FST FS *we denote the system* $\mathrm{ZF}-\mathrm{Inf}$ *together with the negation* $\neg\mathrm{Inf}$ *of the axiom of infinity.* FS *stands for* finite sets.

Until further notice we shall carry out proofs in the theory $\mathrm{ZF}-\mathrm{Inf}$.
Most of the axioms have a form like

$$\forall\vec{x}\,\exists y\forall z\,(z\in y\leftrightarrow\varphi).$$

Intuitively, y is the set of sets z which satisfy φ. The common notation for that set is

$$\{z|\varphi\}.$$

This is to be seen as a term, which assigns to the other parameters in φ the value $\{z|\varphi\}$. Since the result of such a term is not necessarily a set we call such terms *class terms*. It is very convenient to employ class terms *within* $\in$-formulas. We view this notation as an abbreviation for "pure" $\in$-formulas.

Definition 105. *A* class term *is of the form* $\{x|\varphi\}$ *where x is a variable and $\varphi\in L^{\in}$. If* $\{x|\varphi\}$ *and* $\{y|\psi\}$ *are class terms then*

- $u\in\{x|\varphi\}$ *stands for* $\varphi\frac{u}{x}$ *;*
- $u=\{x|\varphi\}$ *stands for* $\forall v\,(v\in u\leftrightarrow\varphi\frac{v}{x})$*;*
- $\{x|\varphi\}=u$ *stands for* $\forall v\,(\varphi\frac{v}{x}\leftrightarrow v\in u)$*;*
- $\{x|\varphi\}=\{y|\psi\}$ *stands for* $\forall v\,(\varphi\frac{v}{x}\leftrightarrow\psi\frac{v}{y})$*;*
- $\{x|\varphi\}\in u$ *stands for* $\exists v(v\in u\wedge v=\{x|\varphi\}$*;*
- $\{x|\varphi\}\in\{y|\psi\}$ *stands for* $\exists v(\psi\frac{v}{y}\wedge v=\{x|\varphi\}$.

In this notation, the separation schema becomes:

$$\forall x_1\ldots\forall x_n\forall x\exists y\,y=\{z\,|\,z\in x\wedge\varphi(z,x_1,\ldots,x_n)\}.$$

We shall further extend this notation, first by giving specific names to important formulas and class terms.

Definition 106.

a) $\emptyset := \{x|x\neq x\}$ *is the* empty set*;*

b) $V := \{x|x = x\}$ *is the* universe*.*

We work in the theory ZF − Inf for the following propositions.

Proposition 107.

a) $\emptyset \in V$*.*

b) $V \notin V$ *(*RUSSELL*'s antinomy).*

Proof. a) $\emptyset \in V$ abbreviates the formula

$$\exists v(v = v \wedge v = \emptyset).$$

This is equivalent to $\exists v\, v = \emptyset$ which again is an abbreviation for

$$\exists v\, \forall w\, (w \in v \leftrightarrow w \neq w).$$

This is equivalent to $\exists v \forall w\, w \notin v$ which is equivalent to the axiom of set existence. So $\emptyset \in V$ is another way to write the axiom of set existence.
b) Assume that $V \in V$. By the schema of separation

$$\exists y\, y = \{z|z \in V \wedge z \notin z\}.$$

Let $y = \{z|z \in V \wedge z \notin z\}$. Then

$$\forall z\ (z \in y \leftrightarrow z \in V \wedge z \notin z).$$

This is equivalent to

$$\forall z\ (z \in y \leftrightarrow z \notin z).$$

Instantiating the universal quantifier with y yields

$$y \in y \leftrightarrow y \notin y$$

which is a contradiction. □

We introduce further abbreviations. By a *term* we understand a class term or a variable, i.e., those terms which may occur in an extended ∈-formula. We also introduce *bounded quantifiers* to simplify notation.

Definition 108. *Let A be a term. Then $\forall x \in A\, \varphi$ stands for $\forall x(x \in A \rightarrow \varphi)$ and $\exists x \in A\, \varphi$ stands for $\exists x\, (x \in A \wedge \varphi)$.*

Definition 109. *Let $x, y, z, \ldots$ be variables and $X, Y, Z, \ldots$ be class terms. Define*

a) $X \subseteq Y := \forall x \in X\, x \in Y$*, X is a* subclass *of Y;*

b) $X \cup Y := \{x|x \in X \vee x \in Y\}$ *is the* union *of X and Y;*

c) $X \cap Y := \{x|x \in X \wedge x \in Y\}$ *is the* intersection *of X and Y;*

d) $X \setminus Y := \{x|x \in X \wedge x \notin Y\}$ *is the* difference *of X and Y;*

e) $\bigcup X := \{x|\exists y \in X\, x \in y\}$ *is the* union *of X;*

f) $\bigcap X := \{x|\forall y \in X\, x \in y\}$ *is the* intersection *of X;*

g) $\mathcal{P}(X) = \{x|x \subseteq X\}$ *is the* power class *of X;*

h) $\{X\} = \{x|x = X\}$ *is the* singleton set *of X;*

i) $\{X, Y\} = \{x|x = X \vee x = Y\}$ *is the* (unordered) pair *of X and Y;*

j) $\{X_0, ..., X_{n-1}\} = \{x | x = X_0 \vee ... \vee x = X_{n-1}\}$.

One can prove well-known boolean properties for these operations. We only give a few examples.

Proposition 110. $X \subseteq Y \wedge Y \subseteq X \rightarrow X = Y$.

Proposition 111. $\bigcup \{x, y\} = x \cup y$.

Proof. We show the equality by two inclusions:
($\subseteq$). Let $u \in \bigcup \{x, y\}$. $\exists v(v \in \{x, y\} \wedge u \in v)$. Let $v \in \{x, y\} \wedge u \in v$. $(v = x \vee v = y) \wedge u \in v$.
Case 1. $v = x$. Then $u \in x$. $u \in x \vee u \in y$. Hence $u \in x \cup y$.
Case 2. $v = y$. Then $u \in y$. $u \in x \vee u \in y$. Hence $u \in x \cup y$.
Conversely let $u \in x \cup y$. $u \in x \vee u \in y$.
Case 1. $u \in x$. Then $x \in \{x, y\} \wedge u \in x$. $\exists v(v \in \{x, y\} \wedge u \in v)$ and $u \in \bigcup \{x, y\}$.
Case 2. $u \in y$. Then $x \in \{x, y\} \wedge u \in x$. $\exists v(v \in \{x, y\} \wedge u \in v)$ and $u \in \bigcup \{x, y\}$. □

Since we also have to formalize numbers in set theory, we define:

Definition 112. *Let x be a variable. Define*

a) $0 = \emptyset$ *for the number* zero*;*

b) $x + 1 = x \cup \{x\}$ *for the* successor *of* x.

c) $1 = 0 + 1$ *for the number* one*;*

d) $2 = 1 + 1$ *for the number* two*.*

e) $3 = 2 + 1$ *for the number* three*.*

Note that

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

Informally, we intend to formalize the natural number n as

$$n = \{0, 1, ..., n-1\}.$$

Although we have not yet introduced sufficient arithmetical operations, we can state some "number-theoretic" properties:

Proposition 113.

a) $\forall x\, x + 1 \neq 0$*;*

b) $0 \neq 1$ *;*

c) $\forall x \forall y\; x + 1 = y + 1 \rightarrow x = y$.

Proof. *a*) Consider a set x. Then $x \in x + 1$ and $x \notin 0$. Hence $x + 1 \neq 0$.
c) Assume that $x + 1 = y + 1$ but that $x \neq y$. Then

$$x \in x \cup \{x\} = y \cup \{y\}$$

and since $x \neq y$ we have $x \in y$. Similarly we obtain $y \in x$. We show that the existence of an $\in$-cycle like

$$x \in y \in x$$

contracts the foundation schema.
By the foundation schema

$$\exists z z \in \{x, y\} \rightarrow \exists z\, (z \in \{x, y\} \wedge \forall z'\, (z' \in z \rightarrow z' \notin \{x, y\})).$$

Take $z\in\{x,y\}$ such that

$$\forall z'\,(z'\in z\to z'\notin\{x,y\}).$$

Case 1. $z=x$. Then $y\in x$ and $y\in\{x,y\}$, contradicting the choice of z.
Case 1. $z=y$. Then $x\in y$ and $x\in\{x,y\}$, contradicting the choice of z. □

We can now reformulate the ZF axioms using class term notation. It is customary with axioms to leave out outer universal quantifiers.

a) Extensionality: $x\subseteq y\wedge y\subseteq x\to x=y$.

b) Set existence: $\emptyset\in V$.

c) Separation schema: for all terms A

$$x\cap A\in V.$$

d) Pairing: $\{x,y\}\in V$.

e) Union: $\bigcup x\in V$.

f) Powerset: $\mathcal{P}(x)\in V$.

g) Infinity: $\exists x\ (0\in x\wedge\forall u\in x\ u+1\in x)$.

h) Replacement: see later.

i) Foundation: for all terms A with free variables $x_0,\ldots,x_{n-1}$

$$A\neq\emptyset\to\exists x\in A\ x\cap A=\emptyset.$$

23 Relations and functions

Ordered pairs are the basis for the theory of relations.

Definition 114. $(x,y)=\{\{x\},\{x,y\}\}$ *is the* ordered pair *of* x *and* y.

Proposition 115. $(x,y)\in V$.
$(x,y)=(x',y')\to x=y\wedge x'=y'$.

Definition 116. *Let* A,B,R *be terms. Define*

a) $A\times B=\{z|\exists a\in A\exists b\in B\ z=(a,b)\}$ *is the* cartesian product *of* A *and* B.

b) R *is a* (binary) relation *if* $R\subseteq V\times V$.

c) If R *is a binary relation write* aRb *instead of* $(a,b)\in R$.

We can now introduce the usual notions for relations:

Definition 117.

a) $\mathrm{dom}(R)=\{x|\exists y\,(x,y)\in R\}$ *is the* domain *of* R.

b) $\mathrm{ran}(R)=\{y|\exists x\,(x,y)\in R\}$ *is the* range *of* R.

c) $R\restriction A=\{z|z\in R\wedge\exists x\exists y((x,y)=z\wedge x\in A)\}$ *is the* restriction *of* R *to* A.

d) $R[A]=\{y|\exists x\in A\ xRy\}$ *is the* image *of* A *under* R.

e) $R^{-1}=\{z|\exists x\exists y\,(xRy\wedge z=(y,x))\}$ *is the* inverse *of* R.

f) $R^{-1}[B]=\{x|\exists y\in B\ xRy\}$ *is the* preimage *of* B *under* R.

One can prove the usual properties for these notions in ZF − Inf. One can now formalize the types of relations, like equivalence relations, partial and linear orders, etc. We shall only consider notions which are relevant for our short introduction to set theory.

Definition 118. *Let F, A, B be terms. Then*

a) *F is a* function *if* $\forall x \forall y, y' (x F y \wedge x F y' \rightarrow y = y')$.

b) $F: A \rightarrow B$ *if F is a function*$\wedge \mathrm{dom}(F) = A \wedge \mathrm{ran}(F) \subseteq B$. *The sequence notions* $(F(x)|x \in A)$ *or* $(F(x))_{x \in A}$ *are common alternative ways to write* $F: A \rightarrow V$.

c) $F(x) = \{v | \exists y (x F y \wedge \forall y' (x F y' \rightarrow y = y') \rightarrow \exists y (x F y \wedge v \in y)\}$ *is the* value *of F at x.*

Note that if $F: A \rightarrow B$ and $x \in A$ then $x F F(x)$. If there is no unique y such that $x F y$ then $F(x) = V$ which we may read as $F(x)$ is "undefined".

Using functional notations we may now write the replacement schema as

for all terms F: F is a function $\rightarrow F[x] \in V$.

24 Ordinal numbers

We have suggested to formalize the natural number n as

$$n = \{0, 1, \ldots, n-1\}.$$

We note some properties of this informal presentation which will be the basis for the "official" formalization of numbers in set theory:

1. "Numbers" are ordered by the $\in$-relation:
$$m < n \text{ iff } m \in n.$$
E.g., $3 \in 5$ but not $5 \in 3$.

2. "Numbers" are "complete" with respect to smaller "numbers"
$$i < j < m \rightarrow i \in m.$$
This can be written
$$i \in j \in m \rightarrow i \in m,$$
a property termed *transitivity*.

Definition 119.

a) *A is* transitive, $\mathrm{Trans}(A)$, *iff* $\forall y \in A \forall x \in y\, x \in A$.

b) *x is an* ordinal (number), $\mathrm{Ord}(x)$, *if* $\mathrm{Trans}(x) \wedge \forall y \in x\, \mathrm{Trans}(y)$.

c) *Let* $\mathrm{Ord} = \{x | \mathrm{Ord}(x)\}$ *be the class of all ordinal numbers.*

We shall see that this defines a notion of "number" which extends the integers and which is in particular adequate for enumerating infinite sets. We work in the theory $\mathrm{ZF} - \mathrm{Inf}$.

Theorem 120.

a) $0 \in \mathrm{Ord}$.

b) $\forall x \in \mathrm{Ord}\ x + 1 \in \mathrm{Ord}$.

Proof. a) $\mathrm{Trans}(\emptyset)$ since formulas of the form $\forall y \in \emptyset \ldots$ are tautologously true. Similarly $\forall y \in \emptyset\, \mathrm{Trans}(y)$.
b) Assume $x \in \mathrm{Ord}$.
(1) $\mathrm{Trans}(x+1)$.
Proof. Let $u \in v \in x + 1 = x \cup \{x\}$.
Case 1. $v \in x$. Then $u \in x \subseteq x + 1$, since x is transitive.
Case 2. $v = x$. Then $u \in x \subseteq x + 1$. *qed*(1)
(2) $\forall y \in x + 1\, \mathrm{Trans}(y)$.
Proof. Let $y \in x + 1 = x \cup \{x\}$.
Case 1. $y \in x$. Then $\mathrm{Trans}(y)$ since x is an ordinal.
Case 2. $y = x$. Then $\mathrm{Trans}(y)$ since x is an ordinal. □

By the previous result, 0, 1, 2, ... $\in$ Ord. The class Ord shares many properties with its elements:

Theorem 121. Ord *is transitive and every element of* Ord *is transitive. Hence* Ord(Ord).

Proof. This follows immediately from the definition of Ord. □

Theorem 122. (Burali-Forti, 1897) Ord$\notin V$.

Proof. Assume that Ord $\in V$. By the previous theorem, Ord $\in$ Ord. But there are no $\in$-cycles in ZF $-$ Inf. □

Theorem 123. *The class* Ord *is strictly linearly ordered by* $\in$, *i.e.,*

a) $\forall x, y, z \in \mathrm{Ord}\,(x \in y \wedge y \in z \rightarrow x \in z)$.

b) $\forall x \in \mathrm{Ord}\, x \notin x$.

c) $\forall x, y \in \mathrm{Ord}\,(x \in y \vee x = y \vee y \in x)$.

Proof. a) Let $x, y, z \in \mathrm{Ord}$ and $x \in y \wedge y \in z$. Then z is transitive, and so $x \in z$.
b) since there are no $\in$-cycles.
c) Assume that there are "incomparable" ordinals. By the foundation schema choose $x_0 \in \mathrm{Ord}$ $\in$-minimal such that $\exists y \in \mathrm{Ord}\, \neg(x_0 \in y \vee x_0 = y \vee y \in x_0)$. Again, choose $y_0 \in \mathrm{Ord}$ $\in$-minimal such that $\neg(x_0 \in y_0 \vee x_0 = y_0 \vee y_0 \in x_0)$. We obtain a contradiction by showing that $x_0 = y_0$:

Let $x \in x_0$. By the $\in$-minimality of x_0, x is comparable with y_0: $x \in y_0 \vee x = y_0 \vee y_0 \in x$. If $x = y_0$ then $y_0 \in x_0$ and x_0, y_0 would be comparable, contradiction. If $y_0 \in x$ then $y_0 \in x_0$ by the transitivity of x_0 and again x_0, y_0 would be comparable, contradiction. Hence $x \in y_0$.

For the converse let $y \in y_0$. By the $\in$-minimality of y_0, y is comparable with x_0: $y \in x_0 \vee y = x_0 \vee x_0 \in y$. If $y = x_0$ then $x_0 \in y_0$ and x_0, y_0 would be comparable, contradiction. If $x_0 \in y$ then $x_0 \in y_0$ by the transitivity of y_0 and again x_0, y_0 would be comparable, contradiction. Hence $y \in x_0$.

But then $x_0 = y_0$ contrary to the choice of y_0. □

Definition 124. *Let* $< = \in \cap \mathrm{Ord} \times \mathrm{Ord} = \{(x, y) | x \in \mathrm{Ord} \wedge y \in \mathrm{Ord} \wedge x \in y\}$ *be the natural strict linear ordering of* Ord *by the* $\in$*-relation.*

Theorem 125. *Let* $x \in \mathrm{Ord}$. *Then* $x + 1$ *is the immediate successor of* x *in the* $\in$*-relation:*

a) $x < x + 1$;

b) if $y = x + 1$, *then* $y = x$ *or* $y < x$.

Definition 126. *An ordinal* α *is a* successor ordinal *if it is of the form* $\alpha = \beta + 1$ *for some* β. α *is a* limit ordinal *if* $\alpha \neq 0$ *and* α *is not a successor ordinal.*

Lemma 127. *The axiom of infinity holds iff there is a limit ordinal.*

Proof. Let λ be a limit ordinal. Then $0 < \lambda$ and $0 \in \lambda$. Moreover, λ is closed under the successor operation: let $x \in \lambda$; then $x + 1 \leqslant \lambda$; since λ is not a successor ordinal, $x + 1 < \lambda$ and $x + 1 \in \lambda$. Thus λ is a set witnessing the axiom of infinity.

Conversely assume the axiom of infinity and take a set z such that $0 \in z$ and $\forall x \in z\, z + 1 \in z$. By the Burali-Forti paradox Ord $\nsubseteq z$. Take λ $\in$-minimal such that $\lambda \in \mathrm{Ord} \setminus z$. We show that λ is a limit ordinal. $\lambda \neq 0$ since $0 \in z$. Assume that λ is a successor ordinal of the form $\lambda = x + 1$. Then $x \in z$ and by the closure properties of z $\lambda = x + 1 \in z$. Contradiction. □

We are now able to define:

Definition 128. $\mathbb{N} = \{n \mid \mathrm{Ord}(n) \wedge \forall m \leqslant n$ (m *is not a limit ordinal*)$\}$ *is the class of* natural numbers.

Lemma 129. *$\mathbb{N}$ is an initial segment of $(\mathrm{Ord},<)$, i.e., $\forall n\in\mathbb{N}\forall m<n\, m\in\mathbb{N}$.*

Proof. Let $m\in n\in\mathbb{N}$. Then $\mathrm{Ord}(m)\wedge\forall i\leqslant m$ (i is not a limit ordinal). Hence $m\in\mathbb{N}$. ☐

Theorem 130. *The following are equivalent:*

a) the axiom of infinity;

b) $\mathbb{N}\neq\mathrm{Ord}$;

c) $\mathbb{N}\in V$.

Proof. The axiom of infinity implies that there is a limit ordinal. Then $\mathbb{N}\neq\mathrm{Ord}$.
Assume $\mathbb{N}\neq\mathrm{Ord}$. Take a limit ordinal λ. By the definition of $\mathbb{N}$ we have $\mathbb{N}\subseteq\lambda$. By separation, $\mathbb{N}\in V$.
Finally, if $\mathbb{N}\in V$ then $\mathbb{N}$ is a set witnessing the axiom of infinity. ☐

25 Induction

Induction on $\in$? The ordinals satisfy an *induction theorem* which generalizes *complete induction* on the integers:

Theorem 131. *Let $\varphi(x,v_0,\ldots,v_{n-1})\in L^{\in}$ and $x_0,\ldots,x_{n-1}\in V$. Assume that the property $\varphi(x, x_0,\ldots,x_{n-1})$ is* inductive, *i.e.,*

$$\forall x\in\mathrm{Ord}\,(\forall y\in x\;\varphi(y,x_0,\ldots,x_{n-1})\rightarrow\varphi(x,x_0,\ldots,x_{n-1})).$$

Then φ holds for all ordinals:

$$\forall x\in\mathrm{Ord}\;\varphi(x,x_0,\ldots,x_{n-1})).$$

Proof. Assume not. This means that there are x satisfying the property:

$$x\in\mathrm{Ord}\wedge\neg\varphi(x,x_0,\ldots,x_{n-1}).$$

According to the schema of foundation one can take an $\in$-minimal x with that property:

$$x\in\mathrm{Ord}\wedge\neg\varphi(x,x_0,\ldots,x_{n-1})\wedge\forall y(y\in x\rightarrow\neg y\in\mathrm{Ord}\wedge\neg\varphi(y,x_0,\ldots,x_{n-1})).$$

The clause $y\in\mathrm{Ord}$ is redundant since $x\subseteq\mathrm{Ord}$:

$$x\in\mathrm{Ord}\wedge\neg\varphi(x,x_0,\ldots,x_{n-1})\wedge\forall y(y\in x\rightarrow\varphi(y,x_0,\ldots,x_{n-1})).$$

By the inductivity of φ the right-hand clause implies $\varphi(x,x_0,\ldots,x_{n-1})$ and so

$$x\in\mathrm{Ord}\wedge\neg\varphi(x,x_0,\ldots,x_{n-1})\wedge\varphi(x,x_0,\ldots,x_{n-1}).$$

Contradiction. ☐

This implies the schema of *complete induction* for $\mathbb{N}$. We shall later see that S_{AR}-formulas can be expressed as $\in$-formulas, so that the schema contains the first-order induction schema of PA.

Theorem 132. *For every $\in$-formula $\varphi(x,x_0,\ldots,x_{n-1})$:*

$$\varphi(0,x_0,\ldots,x_{n-1})\wedge\forall x\in\mathbb{N}(\varphi\rightarrow\varphi(x+1,x_0,\ldots,x_{n-1}))\rightarrow\forall x\in\mathbb{N}\,\varphi$$

Proof. Assume that $\varphi(0,x_0,\ldots,x_{n-1})\wedge\forall x\in\mathbb{N}(\varphi\rightarrow\varphi(x+1,x_0,\ldots,x_{n-1}))$. We apply the general induction schema to the formula

$$\psi(x,x_0,\ldots,x_{n-1})=x\in\mathbb{N}\rightarrow\varphi(x,x_0,\ldots,x_{n-1}).$$

It suffices to see that ψ is inductive. So assume that

$$x\in\mathrm{Ord}\wedge\forall y\in x\ \psi(y,x_0,\ldots,x_{n-1}).$$

Case 1: $x=0$. Then $\varphi(0,x_0,\ldots,x_{n-1})$ and so $\psi(0,x_0,\ldots,x_{n-1})$.
Case 2: $x\in\mathbb{N}$ and $x\neq0$. Then x is a successor ordinal of the form $y+1$. Then $y\in\mathbb{N}$ and $y<x$. By assumption, $\psi(y,x_0,\ldots,x_{n-1})$. Hence $\varphi(y,x_0,\ldots,x_{n-1})$. Since this property is inherited by $+1$ on $\mathbb{N}$ we have $\varphi(x,x_0,\ldots,x_{n-1})$ and hence $\psi(x,x_0,\ldots,x_{n-1})$.
Case 3: $x\notin\mathbb{N}$. Then the implication $x\in\mathbb{N}\rightarrow\varphi(x,x_0,\ldots,x_{n-1})$ holds trivially. □

Applying this theorem to the formula $\varphi(x)=x\in a$ implies the second order induction principle for $\mathbb{N}$:

Theorem 133. *Let $a\subseteq\mathbb{N}$ such that $0\in a$ and $\forall x\in a: x+1\in a$. Then $a=\mathbb{N}$.*

Note that this statement only has mathematical strength when $\mathbb{N}$ is a set, i.e., when the axiom of infinity holds. Otherwise there are no infinite sets a such that $0\in a$ and $\forall x\in a: x+1\in a$.

26 Recursion

Recursion, often called induction, is a ubiquitous method for defining mathematical object. One can show a very general recursion theorem over the class of all ordinals. Here we restrict ourselves to recursion on the class $\mathbb{N}$. also recursion on $\in$?

Theorem 134. *Let $G: V\rightarrow V$. Then there is a canonical class term F such that*

$$F:\mathbb{N}\rightarrow V \text{ and } \forall n\in\mathbb{N}\ F(n)=G(F\restriction n).$$

Also if $F':\mathbb{N}\rightarrow V$ is another class term such that $\forall n\in\mathbb{N}\ F'(n)=G(F'\restriction n)$ then

$$F=F'.$$

We then say that F is defined by recursion *over $\mathbb{N}$ with the* recursion rule *G or by the* recursion equation

$$F(n)=G(F\restriction n).$$

Note that the initial value of F is given by

$$F(0)=G(F\restriction 0)=G(\emptyset).$$

The next values can be calculated as

$$\begin{aligned}F(1) &= G(F\restriction 1)=G((F(0)))=G((G(\emptyset)))\\ F(2) &= G(F\restriction 2)=G((F(0),F(1)))=G((G(\emptyset),G((G(\emptyset)))))\\ F(3) &= G(F\restriction 3)=G((F(0),F(1),F(2)))=G((G(\emptyset),G((G(\emptyset)))\,G((G(\emptyset),G((G(\emptyset)))))))\end{aligned}$$

The basic idea for the definition of F is to use the values of finite initial segments of F.

Proof. Let

$$F=\{(n,f(n))\,|\,n\in\mathbb{N}\wedge f: n+1\rightarrow V\wedge\forall m\leqslant n\, f(m)=G(f\restriction m)\}$$

(1) For all $n\in\mathbb{N}$ there is exactly one $f_n: n+1\rightarrow V$ such that $\forall m\leqslant n\, f_n(m)=G(f_n\restriction m)$.
Proof by complete induction on n. Let

$$f_0=\{(0,G(\emptyset))\}.$$

If the function $g: 1\rightarrow V$ also satisfies $g(0)=G(g\restriction 0)=G(\emptyset)$ then $g=f_0$.

Assume that (1) holds for n. Let

$$f_{n+1}=f_n\cup\{(n+1,G(f_n))\}.$$

Since $f_{n+1}(n+1)=G(f_n)=G(f_{n+1}\upharpoonright n+1)$, f_{n+1} satisfies the recursive equation

$$\forall m\leqslant n+1\, f_{n+1}(m)=G(f_{n+1}\upharpoonright m).$$

Consider a function $g{:}\, n+2\rightarrow V$ such that also $\forall m\leqslant n+1\, g(m)=G(g\upharpoonright m)$. Then $g\upharpoonright n+1$ satisfies the recursive equation for $m\leqslant n$. By the inductive assumption, $g\upharpoonright n+1=f_n$. Also

$$g(n+1)=G(g\upharpoonright n+1)=G(f_n)=f_{n+1}(n+1).$$

Thus $g=f_{n+1}$. *qed*(1)

By this property, $F{:}\,\mathbb{N}\rightarrow V$ is welldefined.

(2) $\forall n\in\mathbb{N}\; F(n)=G(F\upharpoonright n)$.

Proof by induction on n. Assume that (2) holds for all $m<n$. If $n=0$ then $F\upharpoonright n=\emptyset=f_n\upharpoonright n$; if $n>0$ then (1) implies that $F\upharpoonright n=f_n=f_n\upharpoonright n$. Then

$$F(n)=f_n(n)=G(f_n\upharpoonright n)=G(F\upharpoonright n).$$

qed(2)

Finally assume that $F'{:}\,\mathbb{N}\rightarrow V$ satisfies $\forall m\in\mathbb{N}\; F'(m)=G(F'\upharpoonright m)$. Let $n\in\mathbb{N}$. By (1), $F'\upharpoonright n+1=f_n$. Thus

$$F(n)=f_n(n)=F'(n)$$

and $F=F'$. □

The recursion theorem justifies recursion on the previous *course of values*. This includes the following more familiar recursion theorem:

Theorem 135. *Let $a_0\in V$ and $H{:}\,V\rightarrow V$. Then there is a unique canonical class term $F{:}\,\mathbb{N}\rightarrow V$ such that*

$$F(0)=a_0 \text{ and } \forall n\in\mathbb{N}\; F(n+1)=H(F(n)).$$

Proof. Define $G{:}\,V\rightarrow V$ by

$$G(x)=\begin{cases} a_0, \text{ if } x=\emptyset \\ H(x(n)), \text{ if } x \text{ is a function with } \mathrm{dom}(x)=n+1\in\mathbb{N} \\ 0, \text{ else}\end{cases}$$

Let $F{:}\,\mathbb{N}\rightarrow V$ be defined by the recursion equation

$$F(n)=G(F\upharpoonright n).$$

Then

$$F(0)=G(F\upharpoonright 0)=G(\emptyset)=a_0$$

and for $n\in\mathbb{N}$

$$F(n+1)=G(F\upharpoonright n+1)=H((F\upharpoonright n+1)(n))=H(F(n)).$$

□

By recursion we can now define the usual arithmetic operations in ZF − Inf:

Definition 136. *Define recursively the following arithmetical operations $+,\times,\exp$ on $\mathbb{N}$:*

$$\begin{aligned} m+0 &= m \\ m+(n+1) &= (m+n)+1 \\ m\times 0 &= 0 \\ m\times(n+1) &= (m\times n)+m \\ m^0 &= 1 \\ m^{n+1} &= (m^n)\times m \end{aligned}$$

One can show the usual arithmetical laws by complete induction. So we can interpret every arithmetic formula $\varphi\in L^{S_{\mathrm{AR}}}$ by a corresponding $\in$-formula φ': ...

If we view every S_{AR}-formula as an $\in$-formula, ZF − Inf implies the *Schema of induction* from first-order Peano arithmetic: for every formula $\varphi(x_0, \ldots, x_{n-1}, x_n) \in L^{S_{\mathrm{AR}}}$

$$\forall x_0 \ldots \forall x_{n-1}(\varphi(x_0, \ldots, x_{n-1}, 0) \wedge \forall x_n(\varphi \rightarrow \varphi(x_0, \ldots, x_{n-1}, x_n + 1)) \rightarrow \forall x_n\, \varphi).$$

This can be expressed by saying that ZF − Inf *interprets* PA.

We shall later see, that PA interprets ZF − Inf.

27 Formal logic in ZF − Inf

We shall now redo the basic syntactic part of our introduction to logic within the system ZF − Inf.

A *finite sequence* is a function $w: n \rightarrow V$ for some integer $n \in \mathbb{N}$ which is the *length* of w. We write w_i instead of $w(i)$, and the sequence w may also be denoted by $w_0 \ldots w_{n-1}$. Note that the empty set $\emptyset$ is the unique finite sequence of length 0.

For finite sequences $w = w_0 \ldots w_{m-1}$ and $w' = w'_0 \ldots w'_{n-1}$ let $w\hat{\ }w' = w_0 \ldots w_{m-1} w'_0 \ldots w'_{n-1}$ be the *concatenation* of w and w'. $w\hat{\ }w': m + n \rightarrow V$ can be defined by

$$w\hat{\ }w'(i) = \begin{cases} w(i), \text{ if } i < m; \\ w'(i - m), \text{ if } i \geqslant m. \end{cases}$$

We also write ww' for $w\hat{\ }w'$. This operation is a *monoid* satisfying some cancellation rules:

Proposition 137. *Let w, w', w'' be finite sequences. Then*

a) $(w\hat{\ }w')\hat{\ }w'' = w\hat{\ }(w'\hat{\ }w'')$.

b) $\emptyset\hat{\ }w = w\hat{\ }\emptyset = w$.

c) $w\hat{\ }w' = w\hat{\ }w'' \rightarrow w' = w''$.

d) $w'\hat{\ }w = w''\hat{\ }w \rightarrow w' = w''$.

Proof. We only check the associative law a). Let $n, n', n'' \in \mathbb{N}$ such that $w = w_0 \ldots w_{n-1}$, $w' = w'_0 \ldots w'_{n'-1}$, $w'' = w''_0 \ldots w''_{n''-1}$. Then

$$\begin{aligned} (w\hat{\ }w')\hat{\ }w'' &= (w_0 \ldots w_{n-1} w'_0 \ldots w'_{n'-1})\hat{\ }w''_0 \ldots w''_{n''-1} \\ &= w_0 \ldots w_{n-1} w'_0 \ldots w'_{n'-1} w''_0 \ldots w''_{n''-1} \\ &= w_0 \ldots w_{n-1}\hat{\ }(w'_0 \ldots w'_{n'-1} w''_0 \ldots w''_{n''-1}) \\ &= w_0 \ldots w_{n-1}\hat{\ }(w'_0 \ldots w'_{n'-1}\hat{\ }w''_0 \ldots w''_{n''-1}) \\ &= w\hat{\ }(w'\hat{\ }w''). \end{aligned}$$

The trouble with this argument is the intuitive but vague use of the *ellipses* "...". In mathematical logic we have to ultimately eliminate such vaguenesses. So we show that for all $i < n + n' + n''$

$$((w\hat{\ }w')\hat{\ }w'')(i) = (w\hat{\ }(w'\hat{\ }w''))(i).$$

Case 1: $i < n$. Then

$$\begin{aligned} ((w\hat{\ }w')\hat{\ }w'')(i) &= (w\hat{\ }w')(i) \\ &= w(i) \\ &= (w\hat{\ }(w'\hat{\ }w''))(i). \end{aligned}$$

Case 2: $n \leqslant i < n + n'$. Then

$$\begin{aligned} ((w\hat{\ }w')\hat{\ }w'')(i) &= (w\hat{\ }w')(i) \\ &= w'(i - n) \\ &= (w'\hat{\ }w'')(i - n) \\ &= (w\hat{\ }(w'\hat{\ }w''))(i). \end{aligned}$$

Case 3: $n+n'\leqslant i<n+n'+n''$. Then

$$\begin{aligned}((w\hat{}w')\hat{}w'')(i) &= w''(i-(n+n'))\\ &= w'\hat{}w''(i-(n+n')+n') = w'\hat{}w''(i-n)\\ &= (w\hat{}(w'\hat{}w''))(i-n+n)\\ &= (w\hat{}(w'\hat{}w''))(i).\end{aligned}$$

□

A set x is *finite*, if there is an integer $n\in\mathbb{N}$ and a surjective function $f: n\to x$. The smallest such n is called the *cardinality* of the finite set x and denoted by $n=\mathrm{card}(x)$. The usual cardinality properties for finite sets follow from properties of finite sequences.

Definition 138. *The* basic symbols *of first-order logic are*

a) 0 ($\equiv$) *for* equality*,*

b) 1, 2, 3 $\neg$, $\rightarrow$, $\perp$ *for the logical operations of* negation*,* implication *and the truth value* false*,*

c) ??? $\forall$ *for* universal quantification*,*

d) (*and*) *for auxiliary* bracketing*.*

e) variables v_n *for* $n\in\mathbb{N}$*.*

Let $\mathrm{Var}=\{v_n|n\in\mathbb{N}\}$ *be the set of variables and let* S_0 *be the set of basic symbols.*

An n-ary relation symbol*, for* $n\in\mathbb{N}$*, is (a set) of the form* $R=(x,0,n)$*; here* 0 *indicates that the values of a relation will be* truth values*.* 0*-ary relation symbols are also called* propositional constant symbols*. An n-ary* function symbol*, for* $n\in\mathbb{N}$*, is (a set) of the form* $f=(x,1,n)$ *where* 1 *indicates that the values of a function will be elements of a structure.* 0*-ary function symbols are also called* constant symbols*.*

A symbol set *or a* language *is a set of relation symbols and function symbols.*

We assume that the basic symbols are pairwise distinct and are distinct from any relation or function symbol. For concreteness one could for example set $\equiv=0$, $\neg=1$, $\rightarrow=2$, $\perp=3$, $(=4$, $)=5$*, and* $v_n=(1,n)$ *for* $n\in\mathbb{N}$*.*

Definition 139. *Let S be a language. A* word *over S is a finite sequence*

$$w: n\to S_0\cup S.$$

Let S^* *be the class of all words over S. The empty set* $\emptyset$ *is also called the* empty word*.*

Definition 140. *A relation* $R\subseteq(S^*)^n\times S^*$ *is called a* rule *(over S). A* calculus *(over S) is a concretely given schema* $\mathcal{C}$ *of rules (over S).*

Previously we had defined the product of a calculus as

$$\mathrm{Prod}(\mathcal{C})=\bigcap\ \{X\subseteq S^*\,|\,\text{for all rules } R\in\mathcal{C} \text{ holds } R[X]\subseteq X\}.$$

Since we cannot assume that S^* is a set, we define the product of a calculus "from below":

Definition 141. *Let* $\mathcal{C}$ *be a calculus over S. A sequence* $w^{(0)},\dots,w^{(k-1)}\in S^*$ *is called a* derivation *in* $\mathcal{C}$ *if for every* $l<k$ *there exists a rule* $R\in\mathcal{C}$, $R\subseteq(S^*)^n\times S^*$ *and* $l_0,\dots,l_{n-1}<l$ *such that*

$$R(w^{(l_0)},\dots,w^{(l_{n-1})},w^{(l)}).$$

Derivations in a calculus have finite length so that one can carry out inductions and recursions along the lengths of derivations. We formulate appropriate induction and recursion theorems which generalize *complete induction* and *recursion* for natural numbers.

Theorem 142. (Induction Theorem) *Let* $\mathcal{C}$ *be a calculus over S and let* $\varphi(-)$ *be a property which is inherited along the rules of* $\mathcal{C}$*:*

$$\forall R\in\mathcal{C}, R\subseteq(S^*)^k\times S^*\,\forall w^{(1)},\dots,w^{(k)},w\in S^*, R(w^{(1)},\dots,w^{(k)},w)\ (\varphi(w^{(1)})\wedge\dots\wedge\varphi(w^{(k)})\rightarrow\varphi(w)).$$

Then

$$\forall w \in \mathrm{Prod}(\mathcal{C})\ \varphi(w).$$

Definition 143. *A calculus $\mathcal{C}$ over S is* uniquely readable *if for every $w \in \mathrm{Prod}(\mathcal{C})$ there are a unique rule $R \in \mathcal{C}, R \subseteq (S^*)^k \times S^*$ and unique $w^{(1)}, \ldots, w^{(k)} \in S^*$ such that*

$$R(w^{(1)}, \ldots, w^{(k)}, w).$$

Theorem 144. (Recursion Theorem) *Let $\mathcal{C}$ be a calculus over S which is uniquely readable and let $(G_R | R \in \mathcal{C})$ be a sequence of* recursion rules*, i.e., for $R \in \mathcal{C}, R \subseteq (S^*)^k \times S^*$ let $G_R\colon V^k \to V$ where V is the universe of all sets. Then there is a uniquely determined function $F\colon \mathrm{Prod}(\mathcal{C}) \to V$ such that the following* recursion equation *is satisfied for all $R \in \mathcal{C}, R \subseteq (S^*)^k \times S^*$ and $w^{(1)}, \ldots, w^{(k)}, w \in \mathrm{Prod}(\mathcal{C})$, $R(w^{(1)}, \ldots, w^{(k)}, w)$:*

$$F(w) = G_R(F(w^{(1)}), \ldots, F(w^{(k)})).$$

We say that F is defined by recursion along $\mathcal{C}$ *by the recursion rules $(G_R | R \in \mathcal{C})$.*

Proof. We define $F(w)$ by complete recursion on the length of the shortest derivation of w in $\mathcal{C}$. Assume that $F(u)$ is already uniquely defined for all $u \in \mathrm{Prod}(\mathcal{C})$ with shorter derivation length. Let w have shortest derivation $w^{(0)}, \ldots, w^{(l-1)}$. By the unique readability of $\mathcal{C}$ there are $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ and $w^{(i_0)}, \ldots, w^{(i_{k-1})}$ with $i_0, \ldots, i_{k-1} < l - 1$ such that

$$R(w^{(i_0)}, \ldots, w^{(i_{k-1})}, w).$$

Then we can uniquely define

$$F(w) = G_R(F(w^{(i_0)}), \ldots, F(w^{(i_{k-1})})).$$ □

Definition 145. *The* term calculus *(for S) consists of the following rules:*

a) $\frac{}{x}$ *for all variables x;*

b) $\frac{}{c}$ *for all constant symbols $c \in S$;*

c) $\frac{t_0\, t_1 \ldots t_{n-1}}{f t_0 \ldots t_{n-1}}$ *for all n-ary function symbols $f \in S$.*

*Let T^S be the product of the term calculus. T^S is the class of all S-*terms*.*

Definition 146. *The* formula calculus *(for S) consists of the following rules:*

a) $\frac{}{\bot}$ *produces* falsity*;*

b) $\frac{}{t_0 \equiv t_1}$ *for all S-terms $t_0, t_1 \in T^S$ produces* equations*;*

c) $\frac{}{R t_0 \ldots t_{n-1}}$ *for all n-ary relation symbols $R \in S$ and all S-terms $t_0, \ldots, t_{n-1} \in T^S$ produces* relational formulas*;*

d) $\frac{\varphi}{\neg\varphi}$ *produces* negations *of formulas;*

e) $\frac{\varphi \quad \psi}{(\varphi \to \psi)}$ *produces* implications*;*

f) $\frac{\varphi}{\forall x \varphi}$ *for all variables x produces* universalizations*.*

Let L^S be the product of the formula calculus. L^S is the class of all S-formulas, and it is also called the first-order language *for the symbol set S. Formulas produced by rules a-c) are called* atomic formulas *since they constitute the initial steps of the formula calculus.*

Definition 147. *For $t \in T^S$ define $\mathrm{var}(t) \subseteq \{v_n | n \in \mathbb{N}\}$ by recursion on the term calculus:*

– $\mathrm{var}(x) = \{x\}$*;*

- $\mathrm{var}(c) = \emptyset$;
- $\mathrm{var}(ft_0 \ldots t_{n-1}) = \bigcup_{i<n} \mathrm{var}(t_i)$.

Definition 148. *Für $\varphi \in L^S$ define the set of* free variables $\mathrm{free}(\varphi) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on the formula calculus:*

- $\mathrm{free}(t_0 \equiv t_1) = \mathrm{var}(t_0) \cup \mathrm{var}(t_1)$;
- $\mathrm{free}(Rt_0 \ldots t_{n-1}) = \mathrm{var}(t_0) \cup \ldots \cup \mathrm{var}(t_{n-1})$;
- $\mathrm{free}(\neg\varphi) = \mathrm{free}(\varphi)$;
- $\mathrm{free}(\varphi \to \psi) = \mathrm{free}(\varphi) \cup \mathrm{free}(\psi)$.
- $\mathrm{free}(\forall x \varphi) = \mathrm{free}(\varphi) \setminus \{x\}$.

For $\Phi \subseteq L^S$ define the class $\mathrm{free}(\Phi)$ of free variables *as*

$$\mathrm{free}(\Phi) = \bigcup_{\varphi \in \Phi} \mathrm{free}(\varphi).$$

Definition 149. *For a term $s \in T^S$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$ define the* (simultaneous) substitution

$$s \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$$

of $t_0, \ldots, t_{r-1}$ for $x_0, \ldots, x_{r-1}$ by recursion:

a) $x \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = \begin{cases} x, \text{ if } x \neq x_0, \ldots, x \neq x_{r-1} \\ t_i, \text{ if } x = x_i \end{cases}$ *for all variables x;*

b) $c \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = c$ *for all constant symbols c;*

c) $(fs_0 \ldots s_{n-1}) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = fs_0 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \ldots s_{n-1} \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *for all n-ary function symbols f.*

Definition 150. *For a formula $\varphi \in L^S$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$ define the* (simultaneous) substitution

$$\varphi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$$

of $t_0, \ldots, t_{r-1}$ for $x_0, \ldots, x_{r-1}$ by recursion:

a) $(s_0 \equiv s_1) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = s_0 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \equiv s_1 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *for all terms $s_0, s_1 \in T^S$;*

b) $(Rs_0 \ldots s_{n-1}) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = Rs_0 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \ldots s_{n-1} \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *for all n-ary relation symbols R and terms $s_0, \ldots, s_{n-1} \in T^S$;*

c) $(\neg\varphi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = \neg(\varphi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}})$;

d) $(\varphi \to \psi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = (\varphi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \to \psi \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}})$;

e) *for* $(\forall x \varphi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$ *distinguish two cases:*

  - *if $x \in \{x_0, \ldots, x_{r-1}\}$, assume that $x = x_0$. Choose $i \in \mathbb{N}$ minimal such that $u = v_i$ does not occur in $\forall x \varphi$, $t_0, \ldots, t_{r-1}$ and $x_0, \ldots, x_{r-1}$. Then set*

$$(\forall x \varphi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = \forall u \, (\varphi \frac{t_1 \ldots t_{r-1} \, u}{x_1 \ldots x_{r-1} \, x}).$$

  - *if $x \notin \{x_0, \ldots, x_{r-1}\}$, choose $i \in \mathbb{N}$ minimal such that $u = v_i$ does not occur in $\forall x \varphi$, $t_0, \ldots, t_{r-1}$ and $x_0, \ldots, x_{r-1}$ and set*

$$(\forall x \varphi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} = \forall u \, (\varphi \frac{t_0 \ldots t_{r-1} \, u}{x_0 \ldots x_{r-1} \, x}).$$

Definition 151. *A finite sequence* $(\varphi_0, \ldots, \varphi_{n-1}, \varphi_n)$ *is called a* sequent*. The initial segment* $\Gamma = (\varphi_0, \ldots, \varphi_{n-1})$ *is the* antecedent *and* φ_n *is the* succedent *of the sequent. We usually write* $\varphi_0 \ldots \varphi_{n-1}\ \varphi_n$ *or* $\Gamma\,\varphi_n$ *instead of* $(\varphi_0, \ldots, \varphi_{n-1}, \varphi_n)$*. To emphasize the last element of the antecedent we may also denote the sequent by* $\Gamma'\,\varphi_{n-1}\,\varphi_n$ *with* $\Gamma' = (\varphi_0, \ldots, \varphi_{n-2})$*.*

A sequent $\varphi_0 \ldots \varphi_{n-1}\,\varphi$ *is* correct *if* $\{\varphi_0 \ldots \varphi_{n-1}\} \vDash \varphi$*.*

Definition 152. *The* sequent calculus *consists of the following (sequent-)rules:*

- *monotonicity* (MR) $\dfrac{\Gamma \quad\quad \varphi}{\Gamma \ \ \psi \ \ \varphi}$

- *assumption* (AR) $\dfrac{}{\Gamma \ \ \varphi \ \ \varphi}$

- $\rightarrow$*-introduction* $(\rightarrow I)$ $\dfrac{\Gamma \ \ \varphi \ \ \psi}{\Gamma \quad\quad \varphi \rightarrow \psi}$

- $\rightarrow$*-elimination* $(\rightarrow E)$ $\dfrac{\begin{array}{l}\Gamma \ \ \varphi \\ \Gamma \ \ \varphi \rightarrow \psi\end{array}}{\Gamma \ \ \psi}$

- $\perp$*-introduction* $(\perp I)$ $\dfrac{\begin{array}{l}\Gamma \ \ \varphi \\ \Gamma \ \ \neg\varphi\end{array}}{\Gamma \ \ \perp}$

- $\perp$*-elimination* $(\perp E)$ $\dfrac{\Gamma \ \ \neg\varphi \ \ \perp}{\Gamma \quad\quad \varphi}$

- $\forall$*-introduction* $(\forall I)$ $\dfrac{\Gamma \ \ \varphi\frac{y}{x}}{\Gamma \ \ \forall x\varphi}$ *, if* $y \notin \mathrm{free}(\Gamma \cup \{\forall x\varphi\})$

- $\forall$*-elimination* $(\forall E)$ $\dfrac{\Gamma \ \ \forall x\varphi}{\Gamma \ \ \varphi\frac{t}{x}}$*, if* $t \in T^S$

- $\equiv$*-introduction* $(\equiv I)$ $\dfrac{}{\Gamma \ \ t \equiv t}$ *, if* $t \in T^S$

- $\equiv$*-elimination* $(\equiv E)$ $\dfrac{\begin{array}{l}\Gamma \ \ \varphi\frac{t}{x} \\ \Gamma \ \ t \equiv t'\end{array}}{\Gamma \ \ \varphi\frac{t'}{x}}$

The deduction relation *is the smallest subset* $\vdash \subseteq \mathrm{Seq}(S)$ *of the set of sequents which is closed under these rules. We write* $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ *instead of* $\varphi_0 \ldots \varphi_{n-1}\,\varphi \in \vdash$*. For* Φ *an arbitrary set of formulas define* $\Phi \vdash \varphi$ *iff there are* $\varphi_0, \ldots, \varphi_{n-1} \in \Phi$ *such that* $\varphi_0 \ldots \varphi_{n-1} \vdash \varphi$ *. We say that* φ *can be* deduced *or* derived *from* $\varphi_0 \ldots \varphi_{n-1}$ *or* Φ*, resp. We also write* $\vdash \varphi$ *instead of* $\emptyset \vdash \varphi$ *and say that* φ *is a* tautology*.*

Theorem 153. *A formula* $\varphi \in L^S$ *is derivable from* $\Gamma = \varphi_0 \ldots \varphi_{n-1}$ $(\Gamma \vdash \varphi)$ *iff there is a* derivation *or a* formal proof

$$(\Gamma_0\varphi_0, \Gamma_1\varphi_1, \ldots, \Gamma_{k-1}\varphi_{k-1})$$

of $\Gamma\,\varphi = \Gamma_{k-1}\varphi_{k-1}$ *, in which every sequent* $\Gamma_i\varphi_i$ *is generated by a sequent rule from sequents* $\Gamma_{i_0}\varphi_{i_0}, \ldots, \Gamma_{i_{n-1}}\varphi_{i_{n-1}}$ *with* $i_0, \ldots, i_{n-1} < i$ *.*

We usually write the derivation $(\Gamma_0\varphi_0, \Gamma_1\varphi_1, \ldots, \Gamma_{k-1}\varphi_{k-1})$ *as a vertical scheme*

$$\begin{array}{ll}\Gamma_0 & \varphi_0 \\ \Gamma_1 & \varphi_1 \\ \vdots & \\ \Gamma_{k-1} & \varphi_{k-1}\end{array}$$

where we may also mark rules and other remarks along the course of the derivation.

Let us finally also Gödelize ZF − Inf inside ZF − Inf:

Definition 154. $\ulcorner \mathrm{ZF}-\mathrm{Inf} \urcorner$ *is the following class of axioms:*

$$\{ \ulcorner \mathrm{Ext} \urcorner, \ldots\}$$

This allows to Gödelize provability: for $\varphi \in \ulcorner \mathrm{Fml} \urcorner$ *let* $\mathrm{pr}(\varphi) := \exists \Gamma \subseteq \ulcorner \mathrm{ZF}-\mathrm{Inf} \urcorner$ *such that* φ *is derivable from* Γ*.*

These Gödelizations inherit many properties from the informal notions of language and proofs. For most informal objects X there are corresponding "Gödel-objects" $\ulcorner X \urcorner$ such that simple informal properties φ of X become provable in ZF − Inf: $\mathrm{ZF}-\mathrm{Inf} \vdash \ulcorner \varphi \urcorner (\ulcorner X \urcorner)$. This is true for the Gödelizations of the intuitive natural numbers $0, 1, 2, \ldots$:

$$\mathrm{ZF}-\mathrm{Inf} \vdash \ulcorner + \urcorner (\ulcorner 1 \urcorner, \ulcorner 1 \urcorner) = \ulcorner 2 \urcorner$$

Moreover, the intuitive numbers form an initial segment of the ordinals in the following sense: if n is an intuitive natural number then

$$\mathrm{ZF}-\mathrm{Inf} \vdash \forall x \in \ulcorner n \urcorner (x = \ulcorner 0 \urcorner \vee x = \ulcorner 1 \urcorner \vee \ldots \vee x = \ulcorner n-1 \urcorner).$$

This is a schema consisting of provable instances for each n. The proofs of the instances vary with n.

With respect to simple properties, other finitary objects like finite sequences, words, terms, formulas, sequents, or finite sequences of sequents behave much like natural numbers: simple properties can be Gödelized and proved in ZF − Inf. E.g., if a formula φ is provable in ZF − Inf then

$$\mathrm{ZF}-\mathrm{Inf} \vdash \mathrm{pr}(\ulcorner \varphi \urcorner).$$

If a simple property is of the form

there exists a finite object such that a simple quantifier-free property holds

then the corresponding Gödelized property can be proved in ZF − Inf. E.g., if

Conversely, if ZF − Inf proves the existence of some "finite" object this does in general not provide us with a concrete intuitively finite object with those properties.

28 The undefinability of truth

We prove a fix point theorem:

Theorem 155. *Let* $\varphi(v_0)$ *be an* $\in$*-formula. Then there is an* $\in$*-sentence* θ *without free variables such that*

$$\mathrm{ZF}-\mathrm{Inf} \vdash \theta \leftrightarrow \varphi(\ulcorner \theta \urcorner).$$

Proof. For an $\in$-formula $\chi(v_0)$ and another $\in$-formula χ' write $\chi(\ulcorner \chi' \urcorner)$ for

$$\exists v_0 (v_0 = \ulcorner \chi' \urcorner \wedge \chi).$$

By the abbreviation rules for class terms this is an $\in$-formula. The syntactic operation $\chi, \chi' \mapsto \chi(\ulcorner \chi' \urcorner)$ can be seen as a manipulation of symbol sequences. It can thus be formalized within ZF: let $\mathrm{sub}(v_0, v_1, v_2)$ be a canonical $\in$-formula such that for all $\in$-formulas χ, χ'

$$\mathrm{ZF} \vDash (\mathrm{sub}(\ulcorner \chi \urcorner, \ulcorner \chi' \urcorner, z) \text{ iff } z = \ulcorner \chi(\ulcorner \chi' \urcorner) \urcorner = \ulcorner \exists v_0 (v_0 = \ulcorner \chi' \urcorner \wedge \chi) \urcorner).$$

Then let

$$\psi(v_0) = \exists v_1 (\mathrm{sub}(v_0, v_0, v_1) \wedge \exists v_0 (v_0 = v_1 \wedge \varphi)).$$

In ZF

$$\begin{aligned}\psi(\ulcorner\psi\urcorner) &= \exists v_0(v_0=\ulcorner\psi\urcorner\wedge\psi)\\ &= \exists v_0(v_0=\ulcorner\psi\urcorner\wedge\exists v_1(\mathrm{sub}(v_0,v_0,v_1)\wedge\exists v_0(v_0=v_1\wedge\varphi)))\\ &\leftrightarrow \mathrm{sub}(\ulcorner\psi\urcorner,\ulcorner\psi\urcorner,\ulcorner\exists v_0(v_0=\ulcorner\psi\urcorner\wedge\psi)\urcorner)\wedge\exists v_0(v_0=\ulcorner\exists v_0(v_0=\ulcorner\psi\urcorner\wedge\psi)\urcorner\wedge\varphi)\\ &\leftrightarrow \exists v_0(v_0=\ulcorner\exists v_0(v_0=\ulcorner\psi\urcorner\wedge\psi)\urcorner\wedge\varphi)\\ &\leftrightarrow \varphi(\ulcorner\exists v_0(v_0=\ulcorner\psi\urcorner\wedge\psi)\urcorner)\end{aligned}$$

Setting $\theta=\exists v_0(v_0=\ulcorner\psi\urcorner\wedge\psi)$ yields

$$\begin{aligned}\theta &\leftrightarrow \exists v_0(v_0=\ulcorner\theta\urcorner\wedge\varphi)\\ &\leftrightarrow \varphi(\ulcorner\theta\urcorner).\end{aligned}$$

□

The basic idea of constructing a fixed point for φ can be indicated if we omit the distinction between formulas and their GÖDELization:

Let $\theta=\varphi(v_0(v_0))(\varphi(v_0(v_0)))$. Then

$$\theta=\varphi(v_0(v_0))(\varphi(v_0(v_0)))=\varphi(\varphi(v_0(v_0))(\varphi(v_0(v_0))))=\varphi(\theta).$$

The operation $v_0(v_0)$ of "selfapplication" is more common in computing, where a program may also be considered as data. Another theory where this construction can be carried out is the λ-calculus.

Definition 156. *An $\in$-formula $\psi(v_0)$ is a* definition of truth *if for all $\in$-sentences θ:*

$$\mathrm{ZF}\vdash(\theta\leftrightarrow\psi(\ulcorner\theta\urcorner)).$$

Using the fix point theorem we can easily show TARSKI's theorem on the *undefinability of truth*:

Theorem 157. *If* ZF *is consistent then there is no definition of truth.*

Proof. Assume that $\psi(v_0)$ were a definition of truth. By the fix point theorem there is an $\in$-sentence θ such that

$$\mathrm{ZF}\vdash(\theta\leftrightarrow\neg\psi(\ulcorner\theta\urcorner)).$$

Since $\psi(v_0)$ is a definition of truth we also have

$$\mathrm{ZF}\vdash(\theta\leftrightarrow\psi(\ulcorner\theta\urcorner)).$$

Together

$$\mathrm{ZF}\vdash(\neg\psi(\ulcorner\theta\urcorner)\leftrightarrow\psi(\ulcorner\theta\urcorner)),$$

contradiction. □

29 Hereditarily finite sets

Before we embark on the details of the Gödel incompleteness theorems we need to look closer at the finitary objects involved in syntax and proofs.

Definition 158. *Recursively define a function* $\mathrm{TC}\colon V\to V$ *by*

$$\mathrm{TC}(x)=x\cup\bigcup_{y\in x}\mathrm{TC}(y).$$

$\mathrm{TC}(x)$ *is called the* transitive closure *of x.*

This uses $\in$-recursion which was proved in an exercise. $\mathrm{TC}(x)$ is the $\subseteq$-smallest superset of x which is transitive.

Lemma 159.

a) $x\subseteq \mathrm{TC}(x)$;

b) $\mathrm{TC}(x)$ *is transitive;*

c) *if* z *is transitive and* $x\subseteq z$ *then* $\mathrm{TC}(x)\subseteq z$.

Proof. *a)* is trivial.

b) By $\in$-induction. Assume that $\mathrm{TC}(y)$ is transitive for $y\in x$. Let

$$u\in v\in \mathrm{TC}(x)=x\cup \bigcup_{y\in x} \mathrm{TC}(y).$$

Case 1: $v\in x$. Then $u\in v\subseteq \mathrm{TC}(v)\subseteq \mathrm{TC}(x)$.
Case 2: $v\in \mathrm{TC}(y)$ for some $y\in x$. Then by the transitivity of $\mathrm{TC}(y)$ $u\in \mathrm{TC}(y)\subseteq \mathrm{TC}(x)$.

c) Fix a transitive set z. We prove by $\in$-induction: if $x\subseteq z$ then $\mathrm{TC}(x)\subseteq z$. So let $x\subseteq z$ and assume that $\forall y\in x\,(y\subseteq z\rightarrow \mathrm{TC}(y)\subseteq z)$. If $y\in x$ then $y\in z$, and $y\subseteq z$ by the transitivity of z. So $\forall y\in x\,\mathrm{TC}(y)\subseteq z$ and

$$\mathrm{TC}(x)=x\cup \bigcup_{y\in x} \mathrm{TC}(y)\subseteq z.$$

□

Definition 160. *A set* x *is* hereditarily finite *if* $\mathrm{TC}(x)$ *is finite, i.e.,*

$$\exists n\in \mathbb{N}\,\exists f\, f\colon n\leftrightarrow \mathrm{TC}(x).$$

Let HF *denote the class of all hereditarily finite sets.*

A set x is hereditarily finite iff x and all of its "iterated elements" are finite. Obviously we have:

Lemma 161.

a) $\mathbb{N}\subseteq \mathrm{HF}$;

b) *if* $S\subseteq \mathrm{HF}$ *then* $S^*, T^S, \mathrm{Fml}^S\subseteq \mathrm{HF}$;

c)

Remark 162. We can show that inside V HF is a model of $\mathrm{ZF}+\neg\mathrm{Inf}$. All the axioms of ZF − Inf hold in HF and moreover HF is a model of the negation of the axiom of infinity. This can be seen as a prototype of the relative consistency results common in axiomatic set theory. From a model V of $\mathrm{ZF}-\mathrm{Inf}$ another model M (e.g., HF) of a theory T is defined. This proves the *relative consistency* of the theory T with respect to $\mathrm{ZF}-\mathrm{Inf}$:

$$\mathrm{Con}(\mathrm{ZF}-\mathrm{Inf})\rightarrow \mathrm{Con}(\mathrm{ZF}+\neg\mathrm{Inf}).$$

We need an enumeration of the HF sets. This will also lead to an interpretation of $\mathrm{ZF}-\mathrm{Inf}$ in PA.

A natural number n has a unique binary presentation $n=2^{m_0}+2^{m_1}+\ldots+2^{m_{k-1}}$ with natural numbers k and $m_0<m_1<\ldots<m_{k-1}$. One can thus view n as a "code" for the set $\{m_0,\ldots, m_{k-1}\}$. m is a pseudo-element of the "set" n if it is an exponent in the binary presentation. The exponent or binary coefficient m_i is uniquely determined by the existence of n natural numbers a and b such that

$$n=a+2^{m_i}+b$$

where $a<2^{m_i}$ and $2^{m_i+1}|b$. So one can define a pseudo-element relation ε on $\mathbb{N}$ by

$$m\varepsilon n\leftrightarrow \exists a,b\,(a<2^m\wedge 2^{m+1}|b\wedge n=a+2^m+b).$$

So the iterated decoding of a natural number n by a hereditarily finite set $d(n)$ is recursively defined by

$$d(n)=\{d(m)\,|\,m\varepsilon n\}.$$

Using d every hereditarily finite set is uniquely coded by a natural number.

Lemma 163. $d: \mathbb{N} \leftrightarrow \mathrm{HF}$.

Proof. (1) d is injective.
Proof. We show by induction on n : $\forall m\ (d(m) = d(n) \rightarrow m = n)$. Fix n and assume that the claim holds for all $n' < n$. Assume that $d(m) = d(n)$. Then

$$\{d(i) \mid i \varepsilon m\} = \{d(j) \mid j \varepsilon n\}.$$

etc.

□

One can now list the first few values of d for the concrete natural numbers $0, 1, \ldots$

$$\begin{aligned} 0 &\mapsto \emptyset \\ 1 &\mapsto \{\emptyset\} \\ 2 &\mapsto \{\{\emptyset\}\} \\ 3 &\mapsto \{\{\emptyset\}, \emptyset\} \\ 4 &\mapsto \{\{\{\emptyset\}\}\} \\ 5 &\mapsto \{\{\{\emptyset\}\}, \emptyset\} \end{aligned}$$

Let us call this concrete listing function D. Then $d(n)$ is the Gödelization of the concrete set $D(n)$.

We shall use that the intuitive natural numbers form an initial segment of the natural numbers of $\mathrm{ZF} - \mathrm{Inf}$ in the following sense:

Lemma 164. *Let $0, 1, 2, \ldots, n-1, n$ be standard natural numbers. Then*

a) $\mathrm{ZF} - \mathrm{Inf} \vdash n = \{0, 1, 2, \ldots, n-1\}$, *where the symbols $0, 1, \ldots$ after the $\vdash$ denote the corresponding abstraction terms in* $\mathrm{ZF} - \mathrm{Inf}$.

Interpreting ST in PA and vice versa.

Definition 165. *Let S and S' be languages. Let Φ be an S-theory. We say that Φ* interprets *S' if the following properties hold:*

a) *there is an S-formula $\varphi_{S'}(v_0)$ such that $\Phi \vdash \exists v_0 \varphi_{S'}(v_0)$; $\varphi_{S'}$ is supposed to define the domain of an S'-structure within a model of Φ;*

b) *for every n-ary relation symbol $R \in S'$ there is an S-formula $\varphi_R(v_1, \ldots, v_n)$; φ_R is supposed to define the interpretation of R;*

c) *for every n-ary function symbol $f \in S'$ there is an S-formula $\varphi_f(v_0, v_1, \ldots, v_n)$ such that*

$$\Phi \vdash \forall v_1, \ldots, v_n (\varphi_{S'}(v_1) \wedge \ldots \wedge \varphi_{S'}(v_n) \rightarrow \exists! v_0\, (\varphi_{S'}(v_0) \wedge \varphi_f(v_0, v_1, \ldots, v_n)));$$

φ_f is supposed to define the interpretation of f.

Given an interpretation of S' by Φ we define recursively for every term $t \in T^{S'}$ an S-formula φ_t. If $t = v_i$ then set

$$\varphi_t = v_0 \equiv v_i;$$

for $t = f t_1 \ldots t_n$ set

$$\varphi_t = \exists w_1, \ldots, w_n \left(\varphi_{t_1} \frac{w_1}{v_0} \wedge \ldots \wedge \varphi_{t_n} \frac{w_n}{v_0} \wedge \varphi_f(v_0, w_1, \ldots, w_n) \right),$$

where here and in subsequent clauses $w_1, \ldots, w_n$ are appropriately chosen "new" variables. φ_t is supposed to define an interpretation of t.

Furthermore we define for every S'-formula $\chi(v_0, \ldots, v_{n-1})$ its interpretation $\chi^*(v_0, \ldots, v_{n-1}) \in \mathrm{Fml}^S$.

a) *let $\bot^* = \bot$;*

b) *for* $\chi = t_0 \equiv t_1$ *set*

$$\chi^* = \exists w_0 \left(\varphi_{t_0} \frac{w_0}{v_0} \wedge \varphi_{t_1} \frac{w_0}{v_0} \right);$$

c) *for* $\chi = R t_0 \ldots t_{n-1}$ *set*

$$\chi^* = \exists w_0, \ldots, w_{n-1} \left(\varphi_{t_0} \frac{w_0}{v_0} \wedge \ldots \wedge \varphi_{t_{n-1}} \frac{w_{n-1}}{v_0} \wedge \varphi_R(w_0, \ldots, w_{n-1}) \right);$$

d) *for* $\chi = \neg \chi_0$ *set*

$$\chi^* = \neg(\chi_0^*);$$

e) *for* $\chi = (\chi_0 \rightarrow \chi_1)$ *set*

$$\chi^* = (\chi_0^* \rightarrow \chi_1^*);$$

f) *for* $\chi = \forall x \chi_0$ *set*

$$\chi^* = \forall x \, (\varphi_{S'}(x) \rightarrow \chi_0^*(x)).$$

In this situation let Φ' *be an* S'*-theory. Then* Φ interprets Φ' *if for all* $\chi \in \Phi'$

$$\Phi \vdash \chi^* .$$

If Φ *interprets* Φ' then any proof from Φ' can be "pulled back" to Φ.

Lemma 166. *Let* Φ *interpret* Φ'*. Let* $\Phi' \vdash \chi$*. Then* $\Phi \vdash \chi^*$*.*

Proof. This is true for the elements of Φ' by definition. In general one has to work by induction on the sequent calculus. ☐

Lemma 167. *Let* Φ *interpret* Φ' *and let*

Theorem 168. $\mathrm{ZF} - \mathrm{Inf}$ *interprets* PA .

Proof. We have defined natural numbers and their structure within $\mathrm{ZF} - \mathrm{Inf}$. The language of arithmetic is $S_{\mathrm{Ar}} = \{+, \cdot, 0, 1\}$. Let us define

- $\varphi_{S_{\mathrm{Ar}}}(v_0) = \mathrm{Ord}(v_0) \wedge \forall v_1 \leqslant v_0 \, (v_1$ is not a limit ordinal);
- $\varphi_0(v_0) = v_0 \equiv \emptyset$;
- $\varphi_1(v_0) = v_0 \equiv \{\emptyset\}$;
- let $\varphi_+(v_0, v_1, v_2)$ and $\varphi_\times(v_0, v_1, v_2)$ be the canonical $\in$-formulas that define addition and multiplication in $\mathrm{ZF} - \mathrm{Inf}$.

Then we have shown before that the interpretation χ^* of every axiom $\chi \in \mathrm{PA}$ is provable in $\mathrm{ZF} - \mathrm{Inf}$. ☐

We want to show the converse of this result. As a first step let us show that $\mathrm{ZF} - \mathrm{Inf}$ can be interpreted in a variant of Peano arithmetic which contains the exponentiation function $\exp(n) = 2^n$ as a basic notion. So let $S_{\exp} = \{+, \cdot, \exp, 0, 1\}$.

Definition 169. *The axiom system* $\mathrm{PA}^{\exp} \subseteq L^{S_{\exp}}$ *of* exponential PEANO arithmetic *consists of the following sentences*

- $\forall x \, x + 1 \neq 0$
- $\forall x \forall y \; x + 1 = y + 1 \rightarrow x = y$
- $\forall x \, x + 0 = x$
- $\forall x \forall y \; x + (y + 1) = (x + y) + 1$
- $\forall x \, x \cdot 0 = 0$

- $\forall x \forall y\, x \cdot (y+1) = x \cdot y + x$
- $\exp(0) = 1$
- $\forall x \exp(x+1) = \exp(x) \cdot 2$
- *Schema of induction: for every formula* $\varphi(x_0, \ldots, x_{n-1}, x_n) \in L^{S_{\exp}}$*:*

$$\forall x_0 \ldots \forall x_{n-1} (\varphi(x_0, \ldots, x_{n-1}, 0) \wedge \forall x_n (\varphi \rightarrow \varphi(x_0, \ldots, x_{n-1}, x_n + 1)) \rightarrow \forall x_n \varphi)$$

Theorem 170. $\mathrm{PA}^{\exp}$ *interprets* $\mathrm{ZF} - \mathrm{Inf}$.

Proof. We shall use the ideas for the coding of hereditarily finite sets that were introduced before in the definition of the decoding map $d: \mathbb{N} \leftrightarrow \mathrm{HF}$.

- $\varphi_{S_{\exp}}(v_0) = v_0 \equiv v_0$; every natural number is identified with a set;
- $\varphi_{\in}(v_0, v_1) = v_0\, \varepsilon\, v_1 = \exists a, b\, (a < 2^{v_0} \wedge 2^{v_0+1} | b \wedge v_1 = a + 2^{v_0} + b)$.

In $\mathrm{PA}^{\exp}$ one can now prove the axioms of $\mathrm{ZF} - \mathrm{Inf}$ translated into $S_{\exp}$-formulas. □

Theorem 171. *If* Φ *interprets* F

30 The first Gödel incompleteness theorem

Theorem 172. *If* $\mathrm{ZF} - \mathrm{Inf}$ *is consistent then* $\mathrm{ZF} - \mathrm{Inf}$ *is incomplete, i.e., there is an* $\in$*-sentence* φ *such that* $\mathrm{ZF} - \mathrm{Inf} \nvdash \varphi$ *and* $\mathrm{ZF} - \mathrm{Inf} \nvdash \neg\varphi$.

The basic idea of the proof is: if $\mathrm{ZF} - \mathrm{Inf}$ were complete then we could "decide" any $\in$-sentence by systematically running through all possible proofs from the axioms of $\mathrm{ZF} - \mathrm{Inf}$. Formalizing this idea in $\mathrm{ZF} - \mathrm{Inf}$ one gets a definition of truth within $\mathrm{ZF} - \mathrm{Inf}$: if one first finds a *formal proof* of φ then φ follows from $\mathrm{ZF} - \mathrm{Inf}$, and if one first finds a *formal proof* of $\neg\varphi$ then $\neg\varphi$ follows from $\mathrm{ZF} - \mathrm{Inf}$.

By the formalization of first-order logic within $\mathrm{ZF} - \mathrm{Inf}$ there is an $\in$-formula $\mathrm{Pf}(v_0, v_1)$ expressing that v_0 is a formal proof of v_1 from $\mathrm{ZF} - \mathrm{Inf}$. The predicate of *provability* can then be defined as

$$\mathrm{Pv}(v_1) = \exists v_0\, \mathrm{Pf}(v_0, v_1).$$

Note that a formal proof is a *finite* sequence of sequents, which are *finite* sequences of formulas, which are *finite* sequences of symbols, which are, in the case of $\in$-formulas, hereditarily finite objects. Therefore the provability predicate also satisfies:

$$\mathrm{Pv}(v_1) \leftrightarrow \exists v_0 \in \mathrm{HF}\, \mathrm{Pf}(v_0, v_1).$$

Any informal proof P of an informal $\in$-formula φ from $\mathrm{ZF} - \mathrm{Inf}$ can be Gödelized so that it appears in the above listing of heriditarily finite sets as the n-th element for some natural number n, and then

$$\mathrm{PA} - \mathrm{Inf} \vdash \mathrm{Pf}(d(n), \ulcorner \varphi \urcorner).$$

Conversely, if an informally hereditarily finite object Q is the m-th element of the above listing and is *not* a formal proof of φ form $\mathrm{ZF} - \mathrm{Inf}$ then

$$\mathrm{PA} - \mathrm{Inf} \vdash \neg\mathrm{Pf}(d(m), \ulcorner \varphi \urcorner).$$

Proof. (of the 1. incompleteness theorem)

Assume that $\mathrm{ZF} - \mathrm{Inf}$ is complete and consistent. We show that the formula

$$\psi(v_0) = \exists n \in \mathbb{N}\, (\mathrm{Pf}(d(n), v_0) \wedge \forall m < n \neg\mathrm{Pf}(d(m), \neg v_0))$$

is a definition of truth. $\psi(v_0)$ expresses that the *first* proof which proves v_0 or which proves $\neg v_0$ actually proves v_0.

Let θ be an $\in$-sentence.

Case 1. $\mathrm{ZF}-\mathrm{Inf}\vdash\theta$. Then there is a concrete natural number n such that $D(n)$ is a proof of θ from $\mathrm{ZF}-\mathrm{Inf}$. Since $\mathrm{ZF}-\mathrm{Inf}$ is consistent, $D(m)$ is not a formal proof of $\neg\theta$ for $m=0,1,\ldots,n-1$. Then

$$\mathrm{ZF}-\mathrm{Inf}\vdash\mathrm{Pf}(d(n),\ulcorner\theta\urcorner)$$

and for $m=0,1,\ldots,n-1$

$$\mathrm{ZF}-\mathrm{Inf}\vdash\neg\mathrm{Pf}(d(m),\neg\ulcorner\theta\urcorner)\,.$$

Since

$$\mathrm{ZF}-\mathrm{Inf}\vdash n=\{0,1,\ldots,n-1\},$$

we have

$$\mathrm{ZF}-\mathrm{Inf}\vdash\mathrm{Pf}(d(n),\ulcorner\theta\urcorner)\wedge\forall m<n\neg\mathrm{Pf}(d(m),\neg\ulcorner\theta\urcorner).$$

Thus $\mathrm{ZF}-\mathrm{Inf}\vdash\psi(\ulcorner\theta\urcorner)$.

Case 2. $\mathrm{ZF}-\mathrm{Inf}\vdash\neg\theta$. Take a concrete natural number m such that $D(m)$ is a proof of $\neg\theta$ from $\mathrm{ZF}-\mathrm{Inf}$. Since $\mathrm{ZF}-\mathrm{Inf}$ is consistent, $D(n)$ is not a formal proof of θ for $n=0,1,\ldots,m$. Work within the system $\mathrm{ZF}-\mathrm{Inf}$. Let $n<\omega$.

Case 2.1. $n\leqslant m$. Since $n=\{0,1,\ldots,n-1\}$, $\neg\mathrm{Pf}(d(n),\ulcorner\theta\urcorner)$.

Case 2.2. $n>m$. Then $P(m)$ witnesses that $\exists m<n\mathrm{Pf}(d(m),\neg\ulcorner\theta\urcorner)$.

By these cases

$$\forall n<\omega\neg(\mathrm{Pf}(d(n),\ulcorner\theta\urcorner)\wedge\forall m<n\mathrm{Pf}(d(m),\neg\ulcorner\theta\urcorner))$$

and $\neg\psi(\ulcorner\theta\urcorner)$.

By these cases

$$\mathrm{ZF}-\mathrm{Inf}\vdash(\theta\leftrightarrow\psi(\ulcorner\theta\urcorner)).$$

But then $\mathrm{ZF}-\mathrm{Inf}$ is inconsistent by the theorem on the undefinability of truth. □

31 The second GÖDEL incompleteness theorem

Definition 173. *Define the* $\in$*-formula*

$$\mathrm{Con}(\mathrm{ZF}-\mathrm{Inf})=\neg\mathrm{Pv}(\ulcorner\bot\urcorner).$$

$\mathrm{Con}(\mathrm{ZF}-\mathrm{Inf})$ formalizes that the system $\mathrm{ZF}-\mathrm{Inf}$ is consistent. The second incompleteness theorem states that $\mathrm{ZF}-\mathrm{Inf}$ cannot prove its own consistency, i.e., that finitary methods cannot prove the consistency of finitary methods, and therefore the consistency of mathematics cannot be proved by finitary methods.

Theorem 174. *If* $\mathrm{ZF}-\mathrm{Inf}$ *is consistent then* $\mathrm{ZF}-\mathrm{Inf}\nvdash\mathrm{Con}(\mathrm{ZF}-\mathrm{Inf})$.

Proof. By the fix point theorem there is an $\in$-sentence θ such that

$$\mathrm{ZF}-\mathrm{Inf}\vdash(\theta\leftrightarrow\neg\mathrm{Pv}(\ulcorner\theta\urcorner)).$$

The sentence θ formalizes the idea: "this sentence is not provable".

(1) If $\mathrm{ZF}-\mathrm{Inf}$ is consistent then $\mathrm{ZF}-\mathrm{Inf}\nvdash\theta$.

Proof. Assume $\mathrm{ZF}-\mathrm{Inf}\vdash\theta$. ..... Then $\mathrm{ZF}-\mathrm{Inf}\vdash\mathrm{Pv}(\theta)$. By the fix point property, $\mathrm{ZF}-\mathrm{Inf}\vdash\neg\theta$. Hence $\mathrm{ZF}-\mathrm{Inf}$ is inconsistent. *qed*(1)

The argument of (1) can be formalized within ZF:

(2) $\mathrm{ZF}-\mathrm{Inf}\vdash\mathrm{Con}(\mathrm{ZF}-\mathrm{Inf})\rightarrow\neg\mathrm{Pv}(\ulcorner\theta\urcorner)$.

Assume now that $\mathrm{ZF}-\mathrm{Inf}\vdash\mathrm{Con}(\mathrm{ZF}-\mathrm{Inf})$. By (2), $\mathrm{ZF}-\mathrm{Inf}\vdash\neg\mathrm{Pv}(\ulcorner\theta\urcorner)$. By the fix point property, $\mathrm{ZF}-\mathrm{Inf}\vdash\theta$. By (1), $\mathrm{ZF}-\mathrm{Inf}$ is inconsistent. □

Index