

Mathematical Logic. An Introduction

Summer 2006

BY PETER KOEPKE

Table of contents

Table of contents	1
1 Introduction	2
1.1 A simple proof	2
1.2 Formal proofs	3
1.3 Syntax and semantics	3
1.4 Set theory	4
1.5 Circularity	4
2 Set theoretic preliminaries	4
3 Symbols and words	7
4 Induction and recursion on calculi	9
5 Terms and formulas	10
6 Structures and models	11
7 The satisfaction relation	13
8 Logical implication and propositional connectives	15
9 Substitution and quantification rules	16
10 A sequent calculus	20
11 Derivable sequent rules	21
11.1 Auxiliary rules	21
11.2 Introduction and elimination of \forall, \wedge, \dots	22
11.3 Manipulations of antecedents	24
11.4 Examples of formal proofs	24
12 Consistency	25
13 Term models and HENKIN sets	26
14 Constructing HENKIN sets	30
15 The completeness theorem	33
16 Cardinalities of models	34
17 Groups	36
18 Fields	38
18.1 The characteristic of a field	38

18.2 Algebraically closed fields	39
19 Dense linear orders	39
20 Peano arithmetic	41
21 Nonstandard analysis	42
22 ZERMELO-FRAENKEL set theory	46
23 Relations and functions	49
24 Ordinal numbers	50
24.1 Induction	51
24.2 Natural numbers	52
24.3 Recursion	52
25 Cardinals	54
26 The axiom of choice	55
27 Logic in ZF	56
28 The undefinability of truth	57
29 The first GÖDEL incompleteness theorem	58
30 The second GÖDEL incompleteness theorem	59
31 Normal forms	59
32 HERBRAND's theorem	62
Index	65

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 occurring symbols as mathematical objects. Thus we let variables x, y, \dots range over some domain like the real numbers \mathbb{R} and let f and g stand for functions $F, G: \mathbb{R} \rightarrow \mathbb{R}$. Observe that the symbol or “name” f is not identical to the function F , and indeed f might also be interpreted 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, \dots and f, g, \dots 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.

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. The most basic mathematical objects seem to be *sets*. We briefly present some facts from set theory which are 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

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

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

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

The ordered pair $\{\{x\}, \{x, y\}\}$ is denoted by (x, y) . Ordered pairs allow to formalize (binary) relations and functions:

- a *relation* is a set 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 set a into a set b we write

$$f: a \rightarrow b.$$

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

It is natural to formalize the integer n by some set with n elements. We shall later see that the following formalization can be carried out uniformly in set theory:

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

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

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 $w_0 \dots w_{n-1}$. 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' . $w \hat{w}': m+n \rightarrow V$ can be defined by

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

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) $w \hat{w}' = w \hat{w}'' \rightarrow w' = w''$.
- 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 $w = w_0 \dots w_{n-1}$, $w' = w'_0 \dots w'_{n'-1}$, $w'' = w''_0 \dots w''_{n''-1}$. Then

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

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: $n \leq i < n + n'$. 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: $n + n' \leq i < n + n' + n''$. 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 $f: n \rightarrow x$. The smallest such n is called the *cardinality* of the finite set x and denoted by $n = \text{card}(x)$. The usual cardinality properties for finite sets follow from properties of finite sequences.

A set x is *denumerable* or *countable* if there is a surjective function $f: \mathbb{N} \rightarrow x$. If the set is not finite, it is *countably infinite*. Its cardinality is ω , written as $\omega = \text{card}(x)$. Under sufficient set theoretical assumptions, the union

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

where each x_n is countable is again countable.

If a set x 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 \leq be a binary relation. Define

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

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

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

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

So let (A, \leq) is be a partial order.

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

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

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

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

d) (A, \leq) 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 \leq 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, \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 $\text{Var} = \{v_n | n \in \mathbb{N}\}$ 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 $n \in \mathbb{N}$.

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, \dots , relation symbols by P, Q, R, \dots , functions symbols by f, g, h, \dots and constant symbols by c, c_0, c_1, \dots . 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

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

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 $S_{\text{Gr}} = \{(80, 1, 2), (87, 1, 0)\}$, e.g., but we shall not care much about such details. As usual in algebra, one also uses an *extended language of group theory*

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

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

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

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

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

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

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

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

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

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

Definition 9. Let \mathcal{C} be a calculus over S . A sequence $w^{(0)}, \dots, w^{(k-1)} \in S^*$ 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

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

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

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

Proof. The equality of sets can be proved by two inclusions.

(\subseteq) The set

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

satisfies the closure property $R[X] \subseteq X$ for all rules $R \in \mathcal{C}$. Since $\text{Prod}(\mathcal{C})$ is the intersection of all such sets, $\text{Prod}(\mathcal{C}) \subseteq X$.

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

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

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. 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

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

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

$$\text{Prod}(\mathcal{C}) \subseteq \{w \in S^* \mid \varphi(w)\}. \quad \square$$

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

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

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

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

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

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 $u \in \text{Prod}(\mathcal{C})$ with shorter derivation length. Let w have shortest derivation $w^{(0)}, \dots, w^{(l-1)}$. By the unique readability of \mathcal{C} there are $R \in \mathcal{C}$, $R \subseteq (S^*)^k \times S^*$ and $w^{(i_0)}, \dots, w^{(i_{k-1})}$ with $i_0, \dots, i_{k-1} < l-1$ such that

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

Then we can uniquely define

$$F(w) = G_R(F(w^{(i_0)}), \dots, F(w^{(i_{k-1})})). \quad \square$$

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 14. *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) $\frac{t_0 t_1 \dots t_{n-1}}{f t_0 \dots t_{n-1}}$ 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 15. *The formula calculus (for S) consists of the following rules:*

- a) $\frac{}{\perp}$ produces falsity;
- b) $\frac{}{t_0 \equiv t_1}$ for all S -terms $t_0, t_1 \in T^S$ produces equations;
- c) $\frac{}{R t_0 \dots t_{n-1}}$ for all n -ary relation symbols $R \in S$ and all S -terms $t_0, \dots, t_{n-1} \in T^S$ produces relational formulas;
- d) $\frac{\varphi}{\neg \varphi}$ produces negations of formulas;
- e) $\frac{\varphi \quad \psi}{(\varphi \rightarrow \psi)}$ 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 16. 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_{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, \dots 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 $\Phi_{Gr'} = \{\forall x \forall y \forall z x \circ (y \circ z) \equiv (x \circ y) \circ z, \forall x x \circ e \equiv x, \forall x x \circ x^{-1} \equiv e\}$ 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 17. For S -formulas φ and ψ and a variable x write

- \top (“true”) instead of $\neg \perp$;
- $(\varphi \vee \psi)$ (“ 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 18. An S -structure is a function $\mathfrak{A}: \{\forall\} \cup S \rightarrow V$ 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., $a(f): A^n \rightarrow A$.

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.,

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

Example 19. Formalize the *ordered field of reals* \mathbb{R} as follows. Define the language of ordered fields

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

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

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

This defines the standard structure $\mathbb{R} = (\mathbb{R}, <, +, \cdot, 0, 1)$. The multiple use of the letter \mathbb{R} corresponds to standard usage and should not lead to confusion.

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

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

Example 20. Define the language of *Boolean algebras* by

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

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 $\text{and} = \mathbb{B}(\wedge)$, $\text{or} = \mathbb{B}(\vee)$, and $\text{not} = \mathbb{B}(-)$ 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 21. 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 22. 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 23. 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 $a_0, \dots, a_{n-1} \in A$

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

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

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

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 $a_0, \dots, a_{n-1} \in A$

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

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 (occurring) variables.

Definition 24. Let S be a symbol set. An S -model is a function

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

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, \dots, x_{r-1} and $a_0, \dots, a_{r-1} \in |\mathfrak{M}|$ define

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

7 The satisfaction relation

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

Definition 25. 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 $t_0, \dots, t_{n-1} \in T^S$, let

$$\mathfrak{M}(ft_0 \dots t_{n-1}) = f^{\mathfrak{A}}(\mathfrak{M}(t_0), \dots, \mathfrak{M}(t_{n-1})).$$

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

Definition 26. 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) $\mathfrak{M}(\perp) = 0$;
- 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 $t_0, \dots, t_{n-1} \in T^S$

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

- 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 $\mathfrak{M} \models \varphi$ 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 $\mathfrak{M} \models \Phi$ iff $\mathfrak{M} \models \varphi$ for every $\varphi \in \Phi$.

Definition 27. 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 $\mathfrak{M} \models \Phi$.

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

Exercise 2. Prove:

- a) $\mathfrak{M} \models (\varphi \vee \psi)$ iff $\mathfrak{M} \models \varphi$ or $\mathfrak{M} \models \psi$;
- b) $\mathfrak{M} \models (\varphi \wedge \psi)$ iff $\mathfrak{M} \models \varphi$ and $\mathfrak{M} \models \psi$;
- c) $\mathfrak{M} \models (\varphi \leftrightarrow \psi)$ iff $\mathfrak{M} \models \varphi$ is equivalent to $\mathfrak{M} \models \psi$;
- d) $\mathfrak{M} \models \exists v_n \varphi$ iff there exists $a \in |\mathfrak{M}|$ such that $\mathfrak{M} \frac{a}{v_n} \models \varphi$.

With the notion of \models 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 occurring variables, and that satisfaction for a formula only depends on its free, non-bound variables.

Definition 28. For $t \in T^S$ define $\text{var}(t) \subseteq \{v_n | n \in \mathbb{N}\}$ by recursion on the term calculus:

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

Definition 29. Für $\varphi \in L^S$ define the set of free variables $\text{free}(\varphi) \subseteq \{v_n | n \in \mathbb{N}\}$ by recursion on the formula calculus:

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

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

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

Example 30.

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

Definition 31.

- a) For $n \in \mathbb{N}$ let $L_n^S = \{\varphi \in L^S \mid \text{free}(\varphi) \subseteq \{v_0, \dots, v_{n-1}\}\}$.
- b) $\varphi \in L^S$ is an S -sentence if $\text{free}(\varphi) = \emptyset$; L_0^S is the set of S -sentences.

Theorem 32. Let t be an S -term and let \mathfrak{I} and \mathfrak{I}' be S -models with the same structure $\mathfrak{I} \upharpoonright \{\forall\} \cup S = \mathfrak{I}' \upharpoonright \{\forall\} \cup S$ and $\mathfrak{I} \upharpoonright \text{var}(t) = \mathfrak{I}' \upharpoonright \text{var}(t)$. Then $\mathfrak{I}(t) = \mathfrak{I}'(t)$.

Theorem 33. Let φ be an S -formula, and let \mathfrak{I} and \mathfrak{I}' be S -models with the same structure $\mathfrak{I} \upharpoonright \{\forall\} \cup S = \mathfrak{I}' \upharpoonright \{\forall\} \cup S$ and $\mathfrak{I} \upharpoonright \text{free}(\varphi) = \mathfrak{I}' \upharpoonright \text{free}(\varphi)$. Then

$$\mathfrak{I} \models \varphi \text{ iff } \mathfrak{I}' \models \varphi.$$

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

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

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

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

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

$$\begin{aligned} \mathcal{J} \models \varphi & \text{ iff for all } a \in A \text{ holds } (\mathfrak{A}, \beta \frac{a}{v_n}) \models \psi \\ & \text{ iff for all } a \in A \text{ holds } (\mathfrak{A}, \beta' \frac{a}{v_n}) \models \psi \text{ by the inductive assumption,} \\ & \text{ iff } \mathcal{J}' \models \varphi. \end{aligned}$$

□

This allows further simplifications in notations for \models :

Definition 34. Let \mathfrak{A} be an S -structure and let (a_0, \dots, a_{n-1}) be a sequence of elements of A . Let t be an S -term with $\text{var}(t) \subseteq \{v_0, \dots, v_{n-1}\}$. Then define

$$t^{\mathfrak{A}}[a_0, \dots, a_{n-1}] = \mathcal{J}(t),$$

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

Let φ be an S -formula with $\text{free}(t) \subseteq \{v_0, \dots, v_{n-1}\}$. Then define

$$\mathfrak{A} \models \varphi[a_0, \dots, a_{n-1}] \text{ iff } \mathcal{J} \models \varphi,$$

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

In case $n=0$ also write $t^{\mathfrak{A}}$ instead of $t^{\mathfrak{A}}[a_0, \dots, a_{n-1}]$ and $\mathfrak{A} \models \varphi$ instead of $\mathfrak{A} \models \varphi[a_0, \dots, a_{n-1}]$. 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

$$\mathfrak{A} \models \Phi \text{ iff for all } \varphi \in \Phi \text{ holds: } \mathfrak{A} \models \varphi.$$

Example 35. 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

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

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

Definition 36. Let S be a language and let $\Phi \subseteq L_0^S$ be a set of S -sentences. Then

$$\text{Mod}^S \Phi = \{\mathfrak{A} \mid \mathfrak{A} \text{ is an } S\text{-structure and } \mathfrak{A} \models \Phi\}$$

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

Thus $\text{Mod}^{S_{Gr}} \Phi_{Gr}$ 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 $\text{Mod}^S \Phi$ is examined in subfields of mathematics: group theory, ring theory, graph theory, etc. Some typical questions are: Is $\text{Mod}^S \Phi \neq \emptyset$, i.e., is Φ satisfiable? Can we extend $\text{Mod}^S \Phi$ by adequate morphisms between models?

8 Logical implication and propositional connectives

Definition 37. For a symbol set S and $\Phi \subseteq L^S$ and $\varphi \in L^S$ define that Φ (logically) implies φ ($\Phi \models \varphi$) iff every S -model $\mathcal{J} \models \Phi$ is also a model of φ .

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

Theorem 38. *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 $\Gamma \models \varphi$ then $\Phi \models \varphi$.*
- b) (Assumption property) *If $\varphi \in \Gamma$ then $\Phi \models \varphi$.*
- c) (\rightarrow -Introduction) *If $\Gamma \cup \varphi \models \psi$ then $\Gamma \models \varphi \rightarrow \psi$.*
- d) (\rightarrow -Elimination) *If $\Gamma \models \varphi$ and $\Gamma \models \varphi \rightarrow \psi$ then $\Gamma \models \psi$.*
- e) (\perp -Introduction) *If $\Gamma \models \varphi$ and $\Gamma \models \neg\varphi$ then $\Gamma \models \perp$.*
- f) (\perp -Elimination) *If $\Gamma \cup \{\neg\varphi\} \models \perp$ then $\Gamma \models \varphi$.*
- g) (\equiv -Introduction) *$\Gamma \models t \equiv t$.*

Proof. f) Assume $\Gamma \cup \{\neg\varphi\} \models \perp$. Consider an S -model with $\mathfrak{I} \models \Gamma$. Assume that $\mathfrak{I} \not\models \varphi$. Then $\mathfrak{I} \models \neg\varphi$. $\mathfrak{I} \models \Gamma \cup \{\neg\varphi\}$, and by assumption, $\mathfrak{I} \models \perp$. But by the definition of the satisfaction relation, this is false. Thus $\mathfrak{I} \models \varphi$. Thus $\Gamma \models \varphi$. \square

9 Substitution and quantification rules

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

Definition 39. *For a term $s \in T^S$, pairwise distinct variables x_0, \dots, x_{r-1} and terms $t_0, \dots, t_{r-1} \in T^S$ define the (simultaneous) substitution*

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

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

- a) $x \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = \begin{cases} x, & \text{if } x \neq x_0, \dots, x \neq x_{r-1} \\ t_i, & \text{if } x = x_i \end{cases}$ for all variables x ;
- b) $c \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = c$ for all constant symbols c ;
- c) $(fs_0 \dots s_{n-1}) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = fs_0 \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} \dots s_{n-1} \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}}$ for all n -ary function symbols f .

Note that the simultaneous substitution

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

is in general different from a successive substitution

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

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

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

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

- a) $(s_0 \equiv s_1) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = s_0 \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} \equiv s_1 \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}}$ for all terms $s_0, s_1 \in T^S$;
- b) $(Rs_0 \dots s_{n-1}) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = R s_0 \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} \dots s_{n-1} \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}}$ for all n -ary relation symbols R and terms $s_0, \dots, s_{n-1} \in T^S$;

- c) $(\neg\varphi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = \neg(\varphi \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}})$;
- d) $(\varphi \rightarrow \psi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = (\varphi \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} \rightarrow \psi \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}})$;
- e) for $(\forall x\varphi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}}$ distinguish two cases:
- if $x \in \{x_0, \dots, x_{r-1}\}$, 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, \dots, t_{r-1} and x_0, \dots, x_{r-1} . Then set

$$(\forall x\varphi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = \forall u (\varphi \frac{t_1 \dots t_{r-1} u}{x_1 \dots x_{r-1} x}).$$
 - if $x \notin \{x_0, \dots, x_{r-1}\}$, choose $i \in \mathbb{N}$ minimal such that $u = v_i$ does not occur in $\forall x\varphi$, t_0, \dots, t_{r-1} and x_0, \dots, x_{r-1} and set

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

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

Theorem 41. Consider an S -model \mathfrak{M} , pairwise distinct variables x_0, \dots, x_{r-1} and terms $t_0, \dots, t_{r-1} \in T^S$.

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

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

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

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

Proof. By induction on the complexities of s and φ .

a) *Case 1:* $s = x$.

Case 1.1: $x \notin \{x_0, \dots, x_{r-1}\}$. Then

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

Case 1.2: $x = x_i$. Then

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

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

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

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

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

Assuming that the substitution theorem is proved for terms, we prove

- b) *Case 4:* $\varphi = s_0 \equiv s_1$. Then

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

Propositional connectives of formulas like \neg and \rightarrow behave similar to terms, so we only consider universal quantification:

Case 5: $\varphi = (\forall x \psi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}}$, 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 $\forall x \varphi, t_0, \dots, t_{r-1}$ and x_0, \dots, x_{r-1} . Then

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

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

$$\begin{aligned}
& (\forall x \varphi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} = \forall u (\varphi \frac{t_0 \dots t_{r-1} u}{x_0 \dots x_{r-1} x}). \\
\mathfrak{M} \models (\forall x \varphi) \frac{t_0 \dots t_{r-1}}{x_0 \dots x_{r-1}} & \text{ iff } \mathfrak{M} \models \forall u (\varphi \frac{t_0 \dots t_{r-1} u}{x_0 \dots x_{r-1} x}) \\
& \text{ iff for all } a \in M \text{ holds } \mathfrak{M} \frac{a}{u} \models \varphi \frac{t_0 \dots t_{r-1} u}{x_0 \dots x_{r-1} x} \\
& \quad (\text{definition of } \models)
\end{aligned}$$

iff for all $a \in M$ holds

$$\left(\mathfrak{M}_u^a\right) \frac{\mathfrak{M}_u^a(t_0) \dots \mathfrak{M}_u^a(t_{r-1}) \mathfrak{M}_u^a(u)}{x_0 \dots x_{r-1} x} \models \varphi$$

(inductive hypothesis for φ)

iff for all $a \in M$ holds

$$\left(\mathfrak{M}_u^a\right) \frac{\mathfrak{M}(t_0) \dots \mathfrak{M}(t_{r-1}) a}{x_0 \dots x_{r-1} x} \models \varphi$$

(since u does not occur in t_i)

iff for all $a \in M$ holds

$$\mathfrak{M} \frac{\mathfrak{M}(t_0) \dots \mathfrak{M}(t_{r-1}) a}{x_0 \dots x_{r-1} x} \models \varphi$$

(since u does not occur in φ)

iff for all $a \in M$ holds

$$\left(\mathfrak{M} \frac{\mathfrak{M}(t_0) \dots \mathfrak{M}(t_{r-1})}{x_0 \dots x_{r-1}}\right) \frac{a}{x} \models \varphi$$

(by simple properties of assignments)

iff $\left(\mathfrak{M} \frac{\mathfrak{M}(t_0) \dots \mathfrak{M}(t_{r-1})}{x_0 \dots x_{r-1}}\right) \models \forall x \varphi$

(definition of \models)

□

We can now formulate further properties of the \models relation.

Theorem 42. *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 $\Gamma \models \varphi_x^y$ and $y \notin \text{free}(\Gamma \cup \{\forall x \varphi\})$ then $\Gamma \models \forall x \varphi$.*
- b) (\forall -elimination) *If $\Gamma \models \forall x \varphi$ then $\Gamma \models \varphi_x^t$.*
- c) (\equiv -Elimination or substitution) *If $\Gamma \models \varphi_x^t$ and $\Gamma \models t \equiv t'$ then $\Gamma \models \varphi_x^{t'}$.*

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

$$\left(\mathfrak{J} \frac{a}{y}\right) \frac{\mathfrak{J}_y^a(y)}{x} \models \varphi \text{ and so } \left(\mathfrak{J} \frac{a}{y}\right) \frac{a}{x} \models \varphi$$

Case 1: $x = y$. Then $\mathfrak{J}_x^a \models \varphi$.

Case 2: $x \neq y$. Then $\mathfrak{J}_{yx}^a \models \varphi$, and since $y \notin \text{free}(\varphi)$ we have $\mathfrak{J}_x^a \models \varphi$.

Thus $\mathfrak{J} \models \forall x \varphi$. Thus $\Gamma \models \forall x \varphi$.

b) Let $\Gamma \models \forall x \varphi$. Consider an S -model \mathfrak{J} with $\mathfrak{J} \models \Gamma$. For all $a \in A = |\mathfrak{J}|$ holds $\mathfrak{J} \frac{a}{x} \models \varphi$. In particular $\mathfrak{J} \frac{\mathfrak{J}(t)}{x} \models \varphi$. By the substitution theorem, $\mathfrak{J} \models \varphi_x^t$. Thus $\Gamma \models \varphi_x^t$.

c) Let $\Gamma \models \varphi_x^t$ and $\Gamma \models t \equiv t'$. Consider an S -model \mathfrak{J} mit $\mathfrak{J} \models \Gamma$. By assumption $\mathfrak{J} \models \varphi_x^t$ and $\mathfrak{J} \models t \equiv t'$. By the substitution theorem

$$\mathfrak{J} \frac{\mathfrak{J}(t)}{x} \models \varphi.$$

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

$$\mathfrak{J} \frac{\mathfrak{J}(t')}{x} \models \varphi$$

and again by the substitution theorem

$$\mathfrak{J} \models \varphi_x^{t'}.$$

Thus $\Gamma \models \varphi_x^{t'}$.

□

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 43. 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 44. The sequent calculus consists of the following (*sequent-*)rules:

- *monotonicity* (MR)
$$\frac{\Gamma \quad \varphi}{\Gamma \quad \psi \quad \varphi}$$
- *assumption* (AR)
$$\frac{}{\Gamma \quad \varphi \quad \varphi}$$
- \rightarrow -*introduction* ($\rightarrow I$)
$$\frac{\Gamma \quad \varphi \quad \psi}{\Gamma \quad \varphi \rightarrow \psi}$$
- \rightarrow -*elimination* ($\rightarrow E$)
$$\frac{\Gamma \quad \varphi \quad \Gamma \quad \varphi \rightarrow \psi}{\Gamma \quad \psi}$$
- \perp -*introduction* ($\perp I$)
$$\frac{\Gamma \quad \varphi \quad \Gamma \quad \neg \varphi}{\Gamma \quad \perp}$$
- \perp -*elimination* ($\perp E$)
$$\frac{\Gamma \quad \neg \varphi \quad \perp}{\Gamma \quad \varphi}$$
- \forall -*introduction* ($\forall I$)
$$\frac{\Gamma \quad \varphi_x^y}{\Gamma \quad \forall x \varphi}, \text{ if } y \notin \text{free}(\Gamma \cup \{\forall x \varphi\})$$
- \forall -*elimination* ($\forall E$)
$$\frac{\Gamma \quad \forall x \varphi}{\Gamma \quad \varphi_x^t}, \text{ if } t \in T^S$$
- \equiv -*introduction* ($\equiv I$)
$$\frac{}{\Gamma \quad t \equiv t}, \text{ if } t \in T^S$$
- \equiv -*elimination* ($\equiv E$)
$$\frac{\Gamma \quad \varphi_x^t \quad \Gamma \quad t \equiv t'}{\Gamma \quad \varphi_x^{t'}}$$

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

Theorem 45. A formula $\varphi \in L^S$ is derivable from $\Gamma = \varphi_0 \dots \varphi_{n-1}$ ($\Gamma \vdash \varphi$) iff there is a derivation or a formal proof

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

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 $\Gamma_{i_0} \varphi_{i_0}, \dots, \Gamma_{i_{n-1}} \varphi_{i_{n-1}}$ with $i_0, \dots, i_{n-1} < i$.

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

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

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 46. *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*

$$\vdash \subseteq \vDash.$$

The converse inclusion corresponds to

Definition 47. *The sequent calculus is complete if $\vDash \subseteq \vdash$.*

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

Theorem 48. *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 \vDash .

11 Derivable sequent rules

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

Lemma 49. *Assume that*

$$\frac{\begin{array}{l} \Gamma \quad \varphi_0 \\ \vdots \\ \Gamma \quad \varphi_{k-1} \end{array}}{\Gamma \quad \varphi_k}$$

is a derived rule of the sequent calculus. Then

$$\frac{\begin{array}{l} \Gamma_0 \quad \varphi_0 \\ \vdots \\ \Gamma_{k-1} \quad \varphi_{k-1} \end{array}}{\Gamma_k \quad \varphi_k}, \text{ where } \Gamma_0, \dots, \Gamma_{k-1} \text{ are initial sequences of } \Gamma_k$$

is also a derived rule of the sequent calculus.

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

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.

$$\text{ex falsum libenter } \frac{\Gamma \perp}{\Gamma \varphi} :$$

$$\frac{\frac{1. \Gamma \quad \perp}{2. \Gamma \quad \neg\varphi \quad \perp}}{3. \Gamma \quad \varphi}$$

$$\neg\text{-Introduction } \frac{\Gamma \varphi \quad \perp}{\Gamma \quad \neg\varphi} :$$

$$\frac{\frac{1. \Gamma \quad \varphi \quad \perp}{2. \Gamma \quad \varphi \rightarrow \perp}}{\frac{3. \Gamma \quad \neg\neg\varphi \quad \neg\neg\varphi}{4. \Gamma \quad \neg\neg\varphi \quad \neg\varphi \quad \neg\varphi}{5. \Gamma \quad \neg\neg\varphi \quad \neg\varphi \quad \perp}}{\frac{6. \Gamma \quad \neg\neg\varphi \quad \varphi}{7. \Gamma \quad \neg\neg\varphi \quad \perp}}{8. \Gamma \quad \neg\varphi}$$

$$\frac{\frac{1. \Gamma \quad \neg\varphi}{2. \Gamma \quad \varphi \quad \varphi}}{3. \Gamma \quad \varphi \quad \perp}{4. \Gamma \quad \varphi \quad \psi}}{5. \Gamma \quad \varphi \rightarrow \psi}$$

$$\frac{\frac{1. \Gamma \quad \psi}{2. \Gamma \quad \varphi \quad \varphi}}{3. \Gamma \quad \varphi \quad \psi}}{4. \Gamma \quad \varphi \rightarrow \psi}$$

Cut rule

$$\frac{\frac{1. \Gamma \quad \varphi}{2. \Gamma \quad \varphi \quad \psi}}{3. \Gamma \quad \varphi \rightarrow \psi}}{4. \Gamma \quad \psi}$$

Contraposition

$$\frac{\frac{1. \Gamma \quad \varphi \quad \psi}{2. \Gamma \quad \neg\psi \quad \neg\psi}}{3. \Gamma \quad \neg\psi \quad \varphi \quad \varphi}{3. \Gamma \quad \neg\psi \quad \varphi \quad \varphi}}{4. \Gamma \quad \varphi \rightarrow \psi}$$

11.2 Introduction and elimination of \vee, \wedge, \dots

\vee -Introduction

$$\frac{\frac{1. \Gamma \quad \varphi}{2. \Gamma \quad \neg\varphi \quad \neg\varphi}}{3. \Gamma \quad \neg\varphi \quad \perp}{4. \Gamma \quad \neg\varphi \quad \psi}}{5. \Gamma \quad \neg\varphi \rightarrow \psi}}{6. \Gamma \quad \varphi \vee \psi}$$

\vee -Introduction

$$\begin{array}{l}
1. \Gamma \quad \psi \\
\hline
2. \Gamma \quad \neg\varphi \quad \psi \\
3. \Gamma \quad \neg\varphi \rightarrow \psi \\
\hline
4. \Gamma \quad \varphi \vee \psi
\end{array}$$
 \vee -Elimination

$$\begin{array}{l}
1. \Gamma \quad \varphi \vee \psi \\
2. \Gamma \quad \varphi \rightarrow \chi \\
3. \Gamma \quad \psi \rightarrow \chi \\
\hline
4. \Gamma \quad \neg\varphi \rightarrow \psi \\
5. \Gamma \quad \neg\chi \quad \neg\chi \\
6. \Gamma \quad \neg\chi \quad \varphi \quad \varphi \\
7. \Gamma \quad \neg\chi \quad \varphi \quad \chi \\
8. \Gamma \quad \neg\chi \quad \varphi \quad \perp \\
9. \Gamma \quad \neg\chi \quad \neg\varphi \\
10. \Gamma \quad \neg\chi \quad \psi \\
11. \Gamma \quad \neg\chi \quad \chi \\
12. \Gamma \quad \neg\chi \quad \perp \\
\hline
13. \Gamma \quad \chi
\end{array}$$
 \wedge -Introduction

$$\begin{array}{l}
1. \Gamma \quad \varphi \\
2. \Gamma \quad \psi \\
\hline
3. \Gamma \quad \varphi \rightarrow \neg\psi \quad \varphi \rightarrow \neg\psi \\
4. \Gamma \quad \varphi \rightarrow \neg\psi \quad \neg\psi \\
4. \Gamma \quad \varphi \rightarrow \neg\psi \quad \perp \\
5. \Gamma \quad \neg(\varphi \rightarrow \neg\psi) \\
\hline
6. \Gamma \quad \varphi \wedge \psi
\end{array}$$
 \wedge -Elimination

$$\begin{array}{l}
1. \Gamma \quad \varphi \wedge \psi \\
\hline
2. \Gamma \quad \neg(\varphi \rightarrow \neg\psi) \\
3. \Gamma \quad \neg\varphi \quad \neg\varphi \\
4. \Gamma \quad \neg\varphi \quad \varphi \rightarrow \neg\psi \\
5. \Gamma \quad \neg\varphi \quad \perp \\
\hline
6. \Gamma \quad \varphi
\end{array}$$
 \wedge -Elimination

$$\begin{array}{l}
1. \Gamma \quad \varphi \wedge \psi \\
\hline
2. \Gamma \quad \neg(\varphi \rightarrow \neg\psi) \\
3. \Gamma \quad \neg\psi \quad \neg\psi \\
4. \Gamma \quad \neg\psi \quad \varphi \rightarrow \neg\psi \\
5. \Gamma \quad \neg\varphi \quad \perp \\
\hline
6. \Gamma \quad \varphi
\end{array}$$
 \exists -Introduction

$$\begin{array}{l}
1. \Gamma \quad \varphi \frac{t}{x} \\
\hline
2. \Gamma \quad \forall x \neg\varphi \quad \forall x \neg\varphi \\
3. \Gamma \quad \forall x \neg\varphi \quad \neg\varphi \frac{t}{x} \\
4. \Gamma \quad \forall x \neg\varphi \quad \perp \\
5. \Gamma \quad \neg\forall x \neg\varphi \\
\hline
6. \Gamma \quad \exists x \varphi
\end{array}$$
 \exists -Elimination

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

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. $\Gamma \quad \varphi \quad \psi \quad \chi$
2. $\Gamma \quad \varphi \quad \psi \rightarrow \chi$
3. $\Gamma \quad \varphi \rightarrow (\psi \rightarrow \chi)$
4. $\Gamma \quad \psi \quad \psi$
5. $\Gamma \quad \psi \quad \varphi \quad \varphi$
6. $\Gamma \quad \psi \quad \varphi \quad \psi \rightarrow \chi$
7. $\Gamma \quad \psi \quad \varphi \quad \chi$

Doublication of premisses

1. $\Gamma \quad \varphi \quad \psi$
2. $\Gamma \quad \varphi \quad \varphi \quad \psi$

Elimination of double premisses

1. $\Gamma \quad \varphi \quad \varphi \quad \psi$
2. $\Gamma \quad \varphi \quad \varphi \rightarrow \psi$
3. $\Gamma \quad \varphi \rightarrow (\varphi \rightarrow \psi)$
4. $\Gamma \quad \varphi \quad \varphi$
5. $\Gamma \quad \varphi \quad \psi$

Iterated applications of these rules yield:

Lemma 50. *Let $\varphi_0 \dots \varphi_{m-1}$ and $\psi_0 \dots \psi_{n-1}$ be antecedents such that*

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

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

$$\frac{\varphi_0 \quad \dots \quad \varphi_{m-1} \quad \chi}{\psi_0 \quad \dots \quad \psi_{n-1} \quad \chi}$$

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 51. *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)

$$\begin{array}{l} x \equiv y \quad x \equiv y \\ x \equiv y \quad x \equiv x \\ x \equiv y \quad (z \equiv x) \frac{x}{z} \\ x \equiv y \quad (z \equiv x) \frac{y}{x} \\ x \equiv y \quad y \equiv x \\ x \equiv y \rightarrow y \equiv x \\ \forall y (x \equiv y \rightarrow y \equiv x) \\ \hline \forall x \forall y (x \equiv y \rightarrow y \equiv x) \end{array}$$

c)

$$\begin{array}{l} x \equiv y \wedge y \equiv z \quad x \equiv y \wedge y \equiv z \\ x \equiv y \wedge y \equiv z \quad x \equiv y \\ x \equiv y \wedge y \equiv z \quad (x \equiv w) \frac{y}{w} \\ x \equiv y \wedge y \equiv z \quad y \equiv z \\ x \equiv y \wedge y \equiv z \quad (x \equiv w) \frac{z}{w} \\ x \equiv y \wedge y \equiv z \quad x \equiv z \\ x \equiv y \wedge y \equiv z \rightarrow x \equiv z \\ \forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z) \\ \forall y \forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z) \\ \hline \forall x \forall y \forall z (x \equiv y \wedge y \equiv z \rightarrow x \equiv z) \end{array}$$

□

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

Theorem 52. *Let φ be an S -formula and $x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}$ be pairwise distinct variables. Then*

$$\vdash \forall x_0 \dots \forall x_{n-1} \forall y_0 \dots \forall y_{n-1} (x_0 \equiv y_0 \wedge \dots \wedge x_{n-1} \equiv y_{n-1} \rightarrow (\varphi \leftrightarrow \varphi \frac{y_0 \dots y_{n-1}}{x_0 \dots x_{n-1}})).$$

Proof. Choose pairwise distinct “new” variables u_0, \dots, u_{n-1} . Then

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

and

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

Thus the simultaneous substitutions can be seen as successive substitutions, and we may use the substitution rule repeatedly:

$$\begin{array}{ll} \varphi \frac{t_0 \dots t_{n-1}}{v_0 \dots v_{n-1}} & \varphi \frac{t_0 \dots t_{n-1}}{v_0 \dots v_{n-1}} \\ \varphi \frac{u_0 \dots u_{n-1} \ t_0}{v_0 \dots v_{n-1} \ u_0} \dots \frac{t_{n-1}}{u_{n-1}} & \varphi \frac{u_0 \dots u_{n-1} \ t_0}{v_0 \dots v_{n-1} \ u_0} \dots \frac{t_{n-1}}{u_{n-1}} \\ \varphi \frac{u_0 \dots u_{n-1} \ t_0}{v_0 \dots v_{n-1} \ u_0} \dots \frac{t_{n-1}}{u_{n-1}} \ t_{n-1} \equiv t'_{n-1} & \varphi \frac{u_0 \dots u_{n-1} \ t_0}{v_0 \dots v_{n-1} \ u_0} \dots \frac{t'_{n-1}}{u_{n-1}} \\ \vdots & \\ \varphi \frac{u_0 \dots u_{n-1} \ t_0}{v_0 \dots v_{n-1} \ u_0} \dots \frac{t_{n-1}}{u_{n-1}} \ t_{n-1} \equiv t'_{n-1} \dots t_0 \equiv t'_0 & \varphi \frac{u_0 \dots u_{n-1} \ t'_0}{v_0 \dots v_{n-1} \ u_0} \dots \frac{t'_{n-1}}{u_{n-1}} \\ \varphi \frac{t_0 \dots t_{n-1}}{v_0 \dots v_{n-1}} \ t_0 \equiv t'_0 \dots t_{n-1} \equiv t'_{n-1} & \varphi \frac{t'_0 \dots t'_{n-1}}{v_0 \dots v_{n-1}}. \end{array}$$

□

12 Consistency

Fix a language S .

Definition 53. A set $\Phi \subseteq L^S$ is consistent if $\Phi \not\vdash \perp$. Φ is inconsistent if $\Phi \vdash \perp$.

We prove some laws of consistency.

Lemma 54. 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 $\Phi, \Psi \in \mathcal{F}$ holds $\Phi \subseteq \Psi$ or $\Psi \subseteq \Phi$. Then

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

is consistent.

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

Conversely assume that $\Phi \vdash \psi$ and $\Phi \vdash \neg\psi$ for some $\psi \in L^S$. Then $\Phi \vdash \perp$ by \perp -introduction.

b) Assume $\Phi \vdash \varphi$. Take $\varphi_0, \dots, \varphi_{n-1} \in \Phi$ such that $\varphi_0 \dots \varphi_{n-1} \vdash \varphi$. Then we can extend a derivation of $\varphi_0 \dots \varphi_{n-1} \vdash \varphi$ as follows

$$\begin{array}{l} \varphi_0 \dots \varphi_{n-1} \quad \varphi \\ \varphi_0 \dots \varphi_{n-1} \quad \neg\varphi \quad \neg\varphi \\ \varphi_0 \dots \varphi_{n-1} \quad \neg\varphi \quad \perp \end{array}$$

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

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

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

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

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 55. Assume that $\Phi \subseteq L^S$ is satisfiable. Then Φ is consistent.

Proof. Assume that $\Phi \vdash \perp$. By the correctness of the sequent calculus, $\Phi \models \perp$. Assume that Φ is satisfiable and let $\mathcal{I} \models \Phi$. Then $\mathcal{I} \models \perp$. This contradicts the definition of the satisfaction relation. Thus Φ is not satisfiable. \square

Lemma 56. 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., $\Phi \not\vdash \perp$. By completeness, $\Phi \not\models \perp$, and we can take an S -interpretation $\mathcal{I} \models \Phi$ such that $\mathcal{I} \not\models \perp$. Thus Φ is satisfiable.

Conversely, assume that every consistent $\Phi \subseteq L^S$ is satisfiable. Assume $\Psi \not\models \psi$. Assume for a contradiction that $\Psi \not\vdash \psi$. Then $\Psi \cup \{\neg\psi\}$ is consistent. By assumption there is an S -interpretation $\mathcal{I} \models \Psi \cup \{\neg\psi\}$. $\mathcal{I} \models \Psi$ and $\mathcal{I} \not\models \psi$, which contradicts $\Psi \models \psi$. Thus $\Psi \vdash \psi$. \square

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 57. Let S be a language and let $\Phi \subseteq L^S$ be consistent. The term model \mathfrak{T}^Φ 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

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

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

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

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

The term model is well-defined:

Lemma 58. 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 $\bar{t}_0, \dots, \bar{t}_{n-1} \in T^\Phi$, $\bar{t}_0 = \bar{s}_0, \dots, \bar{t}_{n-1} = \bar{s}_{n-1}$ and $\Phi \vdash R t_0 \dots t_{n-1}$. Then $\vdash t_0 \equiv s_0, \dots, \vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule yield $\Phi \vdash R s_0 \dots s_{n-1}$. Hence $\Phi \vdash R t_0 \dots t_{n-1}$ implies $\Phi \vdash R s_0 \dots s_{n-1}$. By the symmetry of the argument, $\Phi \vdash R t_0 \dots t_{n-1}$ iff $\Phi \vdash R s_0 \dots s_{n-1}$.

c) Let $\bar{t}_0, \dots, \bar{t}_{n-1} \in T^\Phi$ and $\bar{t}_0 = \bar{s}_0, \dots, \bar{t}_{n-1} = \bar{s}_{n-1}$. Then $\vdash t_0 \equiv s_0, \dots, \vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule to $\vdash f t_0 \dots t_{n-1} \equiv f t_0 \dots t_{n-1}$ yield

$$\vdash f t_0 \dots t_{n-1} \equiv f s_0 \dots s_{n-1}$$

and $\overline{f t_0 \dots t_{n-1}} = \overline{f s_0 \dots s_{n-1}}$. □

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

Theorem 59.

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

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

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

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

$$\begin{aligned} \mathfrak{I}^\Phi(ft_0\dots t_{n-1}) &= f^{\mathfrak{I}^\Phi}(\mathfrak{I}^\Phi(t_0), \dots, \mathfrak{I}^\Phi(t_{n-1})) \\ &= f^{\mathfrak{I}^\Phi}(\bar{t}_0, \dots, \bar{t}_{n-1}) \\ &= \overline{ft_0\dots t_{n-1}}. \end{aligned}$$

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

$$\begin{aligned} \mathfrak{I}^\Phi \models Rt_0\dots t_{n-1} &\text{ iff } R^{\mathfrak{I}^\Phi}(\mathfrak{I}^\Phi(t_0), \dots, \mathfrak{I}^\Phi(t_{n-1})) \\ &\text{ iff } R^{\mathfrak{I}^\Phi}(\bar{t}_0, \dots, \bar{t}_{n-1}) \\ &\text{ iff } \Phi \vdash Rt_0\dots t_{n-1}. \end{aligned}$$

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

$$\begin{aligned} \mathfrak{I}^\Phi \models t_0 \equiv t_1 &\text{ iff } \mathfrak{I}^\Phi(t_0) = \mathfrak{I}^\Phi(t_1) \\ &\text{ iff } \bar{t}_0 = \bar{t}_1 \\ &\text{ iff } t_0 \sim t_1 \\ &\text{ iff } \Phi \vdash t_0 \equiv t_1. \end{aligned}$$

□

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

Definition 60. 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 61. Let $\Phi \subseteq L^S$ be a HENKIN set. Then for all $\chi, \psi \in L^S$ and variables x :

a) $\Phi \not\vdash \chi$ 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 $\Phi \not\vdash \chi$. 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 $\Phi \not\vdash \chi$.

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. $\Phi \not\vdash \chi$. 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 $\Phi \not\vdash \forall x\chi$. 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 62. *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 $\vec{t} \in T^S$*

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

b) $\mathfrak{F}^\Phi \models \Phi$.

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) $\chi = \perp$. Then $\perp \frac{\vec{t}}{\vec{x}} = \perp$. $\mathfrak{F}^\Phi \models \perp \frac{\vec{t}}{\vec{x}}$ is false by definition of the satisfaction relation \models , and $\Phi \vdash \perp \frac{\vec{t}}{\vec{x}}$ is false since Φ is consistent. Thus $\mathfrak{F}^\Phi \models \perp \frac{\vec{t}}{\vec{x}}$ iff $\Phi \vdash \perp \frac{\vec{t}}{\vec{x}}$.

ii.) $\chi = \neg\varphi \frac{\vec{t}}{\vec{x}}$ and assume that the claim holds for φ . Then

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

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

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

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

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

□

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 63. *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*

$$\Phi \cup \{\neg\forall x\varphi \rightarrow \neg\varphi_x^z\}$$

is consistent.

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

$$\varphi_0 \dots \varphi_{n-1} \neg\forall x\varphi \rightarrow \neg\varphi_x^z \vdash \perp.$$

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

1.	Γ	$\neg\forall x\varphi \rightarrow \neg\varphi_x^z$	\perp
2.	Γ	$\neg\neg\forall x\varphi$	$\neg\neg\forall x\varphi$
3.	Γ	$\neg\neg\forall x\varphi$	$\neg\forall x\varphi \rightarrow \neg\varphi_x^z$
4.	Γ	$\neg\neg\forall x\varphi$	\perp
5.	Γ	$\neg\forall x\varphi$	$\neg\forall x\varphi$
6.	Γ	$\neg\varphi_x^z$	$\neg\varphi_x^z$
7.	Γ	$\neg\varphi_x^z$	$\neg\forall x\varphi \rightarrow \neg\varphi_x^z$
8.	Γ	$\neg\varphi_x^z$	\perp
9.	Γ	φ_x^z	φ_x^z
10.	Γ	$\forall x\varphi$	$\forall x\varphi$
11.	Γ		\perp

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 64. *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*

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

is consistent.

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

$$\begin{array}{l} \Gamma_0\varphi_0 \\ \Gamma_1\varphi_1 \\ \vdots \\ \Gamma_{n-1}\varphi_{n-1} \\ \Gamma_n (\neg\forall x\varphi \rightarrow \neg\varphi_x^c) \perp \end{array} \tag{1}$$

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 occurrence of c by z , and for a sequence $\Gamma = (\psi_0, \dots, \psi_{k-1})$ of formulas let $\Gamma' = (\psi'_0, \dots, \psi'_{k-1})$. Replacing each occurrence of c by z in the derivation we get

$$\begin{array}{l} \Gamma'_0\varphi'_0 \\ \Gamma'_1\varphi'_1 \\ \vdots \\ \Gamma'_{n-1}\varphi'_{n-1} \\ \Gamma_n (\neg\forall x\varphi \rightarrow \neg\varphi_x^z) \perp \end{array} \tag{2}$$

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 quantifier 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 occurrences 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

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

which contradicts the preceding lemma. \square

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

Theorem 65. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^ω and $\Phi^\omega \subseteq L^{S^\omega}$ 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 $\psi \in L^S$:

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

Then set

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

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 $\forall x_0 \varphi_0, \dots, \forall x_{n-1} \varphi_{n-1} \in L^S$ of pairwise distinct universal formulas such that

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

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

$$\Phi \cup \left\{ \neg \forall x_0 \varphi_0 \rightarrow \neg \varphi_0 \frac{c_{\forall x_0 \varphi_0}}{x_0}, \dots, \neg \forall x_{n-1} \varphi_{n-1} \rightarrow \neg \varphi_{n-1} \frac{c_{\forall x_{i-1} \varphi_{i-1}}}{x_{i-1}} \right\}$$

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 $\{c_\psi \mid \psi \in L^S\}$; 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. \square

To get HENKIN sets we have to ensure derivation completeness.

Theorem 66. *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

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

$P \neq \emptyset$ 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 $\neg \varphi \in \Phi^*$. \square

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 $L^S = \{\varphi_n \mid n \in \mathbb{N}\}$ be an enumeration of L^S . Define a sequence $(\Phi_n \mid n \in \mathbb{N})$ 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. \square

According to Theorem 65 a given consistent set Φ can be extended to $\Phi^\omega \subseteq L^{S^\omega}$ containing witnesses. By Theorem 66 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 67. *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 67 and 62, we obtain a general and a countable model existence theorem:

Theorem 68. (HENKIN model existence theorem) *Let $\Phi \subseteq L^S$. Then Φ is consistent iff Φ is satisfiable.*

Theorem 69. (Downward LÖWENHEIM-SKOLEM theorem) *Let $\Phi \subseteq L^S$ be a countable consistent set of formulas. Then Φ possesses a model $\mathfrak{M} = (\mathfrak{A}, \beta) \models \Phi$, $\mathfrak{A} = (A, \dots)$ 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 56, Theorem 68 the model existence theorems imply the main theorem.

Theorem 70. (GÖDEL completeness theorem) *The sequent calculus is complete, i.e., $\models = \vdash$.*

Finally the equality of \models and \vdash and the compactness theorem 48 for \vdash imply

Theorem 71. (Compactness theorem) *Let $\Phi \subseteq L^S$ and $\varphi \in \Phi$. Then*

- a) $\Phi \models \varphi$ iff there is a finite subset $\Phi_0 \subseteq \Phi$ such that $\Phi_0 \models \varphi$.
- 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 infeasible.
- 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 72. 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 73. 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

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

where the big conjunction is defined by

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

For any model \mathfrak{M}

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

Now set

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

(1) Φ' has a model.

Proof. By the compactness theorem 71b 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

$$\Phi_0 \subseteq \Phi \cup \{\varphi_{\geq n} \mid n \leq n_0\}.$$

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

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

Theorem 74. (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 $(a_x \mid x \in X_0)$ 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

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

qed(1)

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

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

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

- a) \mathcal{K} is elementary or finitely axiomatizable if there is an S -sentence φ with $\mathcal{K} = \text{Mod}^S \varphi$.
- b) \mathcal{K} is Δ -elementary or axiomatizable, if there is a set Φ of S -sentences with $\mathcal{K} = \text{Mod}^S \Phi$.

We state simple properties of the Mod-operator:

Theorem 76. *Let S be a language. Then*

- a) For $\Phi \subseteq \Psi \subseteq L_0^S$ holds $\text{Mod}^S \Phi \supseteq \text{Mod}^S \Psi$.
- b) For $\Phi, \Psi \subseteq L_0^S$ holds $\text{Mod}^S(\Phi \cup \Psi) = \text{Mod}^S \Phi \cap \text{Mod}^S \Psi$.
- c) For $\Phi \subseteq L_0^S$ holds $\text{Mod}^S \Phi = \bigcap_{\varphi \in \Phi} \text{Mod}^S \varphi$.
- d) For $\varphi_0, \dots, \varphi_{n-1} \in L_0^S$ holds $\text{Mod}^S \{\varphi_0, \dots, \varphi_{n-1}\} = \text{Mod}^S(\varphi_0 \wedge \dots \wedge \varphi_{n-1})$.
- e) For $\varphi \in L_0^S$ holds $\text{Mod}^S(\neg \varphi) = \text{Mod}^S \emptyset \setminus \text{Mod}^S(\varphi)$.

c) explains the denotation Δ -elementary, since $\text{Mod}^S \Phi$ is the intersection (“Durchschnitt”) of all single $\text{Mod}^S \varphi$.

Theorem 77. *Let S be a language and \mathcal{K}, \mathcal{L} be classes of S -structures with*

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

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

Proof. Take axiom systems Φ_K and Φ_L such that $\mathfrak{K} = \text{Mod}^S \Phi_K$ and $\mathfrak{L} = \text{Mod}^S \Phi_L$. 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: $\text{Mod}^S \Phi_0 \supseteq \text{Mod}^S \Phi_K$. Since \mathfrak{K} is not finitely axiomatizable, $\text{Mod}^S \Phi_0 \neq \text{Mod}^S \Phi_K$. Then $\text{Mod}^S \Phi_0 \cap \mathfrak{L} \neq \emptyset$. Take a model $\mathfrak{A} \in \mathfrak{L}$, $\mathfrak{A} \in \text{Mod}^S \Phi_0$. Then $\mathfrak{A} \models \Phi_0 \cup \Phi_L$. *qed*(1)

(2) $\Phi_K \cup \Phi_L$ is satisfiable.

Proof: By the compactness theorem 71 it suffices to show that every finite $\Psi \subseteq \Phi_K \cup \Phi_L$ is satisfiable. 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), $\text{Mod}^S \Phi_K \cap \text{Mod}^S \Phi_L \neq \emptyset$. But the classes \mathfrak{K} and \mathfrak{L} are complements, contradiction. Thus \mathfrak{K} is finitely axiomatizable. \square

Theorem 78. *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 $\text{Mod}^S \Phi$ contains infinite structures. Then $\text{Mod}^S \Phi$ contains structures of arbitrarily high cardinalities, i.e., for any set X there is a model $\mathfrak{M} \models \Phi$ and an injective map from X into M .*

Proof. a) is immediate by Theorem 73.

b) The class of infinite S -structures is axiomatized by

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

If that class were *finitely* axiomatizable then the complementary class of finite S -structures would also be (finitely) axiomatizable, contradicting a).

c) Let $\{c_x \mid x \in X\}$ 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 $\mathfrak{M}_X \models \Phi_X$ and let $\mathfrak{M} = \mathfrak{M}_X \upharpoonright S \models \Phi$. Define $f: X \rightarrow M$ by

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

Then f is injective as required. \square

17 Groups

Definition 79. *The language of group theory is the language*

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

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

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

A group is an S_{Gr} -structure \mathfrak{G} with $\mathfrak{G} \models \Phi_{\text{Gr}}$.

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

$$- \quad \forall x, y, z (x \circ y) \circ z \equiv x \circ (y \circ z) \text{ (associativity)}$$

- $\forall x x \circ e \equiv x$ (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 80. $\Phi_{Gr} \vdash \forall v_0 (v_0 \circ e \equiv e \rightarrow v_0 \equiv e)$.

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 81. 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 82. The class \mathcal{T} of all torsion groups is not axiomatizable.

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

$$\Psi = \Phi \cup \left\{ \underbrace{\neg v_0 \circ \dots \circ v_0}_{n\text{-times}} \equiv e \mid n \in \mathbb{N} \setminus \{0\} \right\}.$$

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

$$\Psi_0 \subseteq \Phi \cup \left\{ \underbrace{\neg v_0 \circ \dots \circ v_0}_{n\text{-times}} \equiv e \mid 1 \leq n \leq n_0 \right\}.$$

The right-hand side can be satisfied in every torsion group which has an element of order $\geq n_0$, e.g., in the additive group of integers modulo n_0 . By the compactness theorem 71, Ψ is satisfiable. Take a model $\mathcal{G} \models \Psi$. Then \mathcal{G} is a group in which the element $\mathcal{G}(v_0)$ satisfies all formulas

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

Hence $\mathcal{G}(v_0)$ has infinite order in \mathcal{G} and \mathcal{G} is not a torsion group, although $\mathcal{G} \models \Phi$. 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 83. The extended language of group theory is the language

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

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

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

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

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 84. *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 fields in the *language of arithmetic*

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

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

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

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, \dots, z_{n-1}) is the *vector sum* of (x_0, \dots, x_{n-1}) and (y_0, \dots, y_{n-1}) can be expressed by the S_{Ar} -formula

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

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

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

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

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

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

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

and fields of characteristic 0 by

$$\Phi_{\text{Fd},0} = \Phi_{\text{Fd}} \cup \{\underbrace{1 + \dots + 1}_{n\text{-times}} \neq 0 \mid n \in \mathbb{N} \setminus \{0\}\}.$$

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

Theorem 86. *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

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

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

$$\Phi_0 \models \varphi_0 \text{ and } \{\varphi_0\} \models \Phi_0.$$

Without loss of generality, Φ_0 is of the form

$$\Phi_0 = \Phi_{\text{Fd}} \cup \{\underbrace{1 + \dots + 1}_{n\text{-times}} \neq 0 \mid n = 1, \dots, n_0\}.$$

This set is equivalent to $\Phi_{\mathbb{K}_p,0}$ 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 $\mathbb{K}_p \models \Phi_0$. But then Φ_0 does *not* axiomatize the class of fields of characteristic 0. Contradiction. \square

18.2 Algebraically closed fields

Definition 87. *A field \mathbb{K} is algebraically closed if every polynomial of degree ≥ 1 has a zero in \mathbb{K} .*

A polynomial

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

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

$$\Phi_{\text{acf}} = \Phi_{\text{Fd}} \cup \{\forall a_{n-1} \dots \forall a_0 \exists x x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \equiv 0 \mid n \in \mathbb{N} \setminus \{0\}\}.$$

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

19 Dense linear orders

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

Definition 88. *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 89. *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

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

and

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

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

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

and

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

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

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

We draw some logical consequences from this isomorphism result.

Definition 90. *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 $\varphi \in L_0^S$*

$$\Phi \vdash \varphi \text{ gdw. } \Phi \not\vdash \neg\varphi.$$

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 91. *Let \mathfrak{A} be an S -structure. Let*

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

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

Definition 92. *Let S be a language and $\Phi \subseteq L_0^S$. Then Φ is ω -categorical, if all countably infinite structures $\mathfrak{A} \models \Phi$ and $\mathfrak{B} \models \Phi$ are isomorphic.*

Theorem 93. *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 $\Phi \not\vdash \neg\varphi$ since Φ is consistent.

Conversely assume $\Phi \not\vdash \neg\varphi$. Assume for a contradiction that $\Phi \not\vdash \varphi$. Then $\Phi \cup \{\varphi\}$ und $\Phi \cup \{\neg\varphi\}$ are consistent. By the LÖWENHEIM-SKOLEM theorem 69 there are countable models $\mathfrak{A}_0 \models \Phi \cup \{\varphi\}$ and $\mathfrak{A}_1 \models \Phi \cup \{\neg\varphi\}$. 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 $\mathfrak{A}_0 \models \varphi$ and $\mathfrak{A}_1 \models \neg\varphi$. Contradiction. \square

As an immediate corollary of the previous theorems we obtain:

Theorem 94. *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 95. *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 96. *The axiom system $PA \subseteq L^{S_{AR}}$ 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 $\varphi(x_0, \dots, x_{n-1}, x_n) \in L^{S_{AR}}$:*

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

Then $\mathbb{N} \models PA$. 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 $0, 2, a, \dots$ 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 $\varepsilon, a + \varepsilon, \dots$. 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 $\text{st}: \mathbb{R} \rightarrow \mathbb{R}^*$ 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

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

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

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

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

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

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 97. \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 98.

- 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

$$\text{st}(u) = \sup_{\mathbb{R}} \{r \in \mathbb{R} \mid r < u\}$$

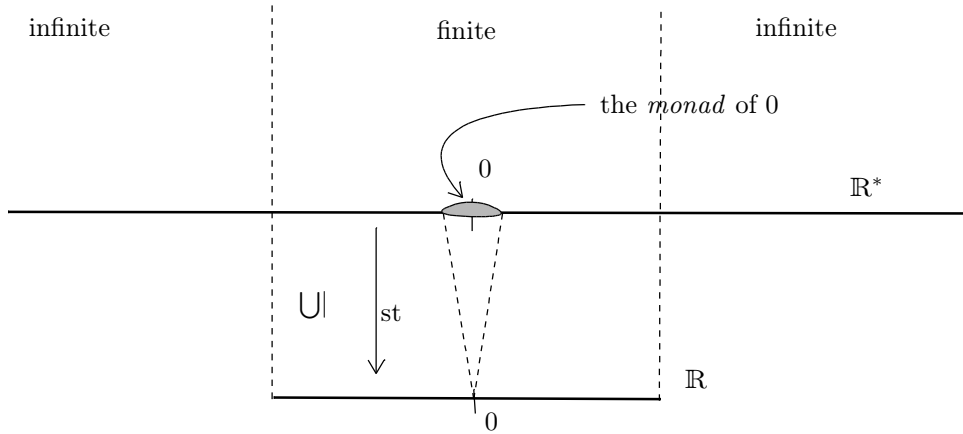
as a supremum in the standard numbers. Note that $\text{st}: \mathbb{R}^* \rightarrow \mathbb{R}$ is a partial function defined on the finite elements of \mathbb{R}^* .

- d) $u \in \mathbb{R}^*$ is infinitesimal if $\text{st}(u) = 0$.
- e) $u, v \in \mathbb{R}^*$ are infinitesimally near, $u \sim v$, if $u - v$ is infinitesimal.

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

$$\text{st}(\varepsilon^*) = \sup_{\mathbb{R}} \{r \in \mathbb{R} \mid r < \varepsilon^*\} = \sup_{\mathbb{R}} \{r \in \mathbb{R} \mid r \leq 0\} = 0.$$

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



Proposition 99.

- a) If $s \in \mathbb{R}$ then $\text{st}(s) = s$.
- 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) $\text{st}(s) = \sup_{\mathbb{R}} \{r \in \mathbb{R} \mid r < s\} = s$.

b) Let $\text{st}(u) = 0$. Let $s \in \mathbb{R}$, $s > 0$. Assume for a contradiction that $-s \geq u$. Then

$$\text{st}(u) \leq \text{st}(-s) = -s < 0,$$

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

$$\text{st}(u) \geq \text{st}(s) = s > 0,$$

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

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

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

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

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 $g: \mathbb{R} \rightarrow \mathbb{R}$ is the derivative f' of the function f .

Theorem 100. $g = f'$ iff the following criterion holds:

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

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

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

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 $g(x) \sim \frac{f(x + \delta) - f(x)}{\delta}$ let $\eta \in \mathbb{R}$, $\eta > 0$. Since $g(x) = f'(x)$ there exists $\delta \in \mathbb{R}$, $\delta > 0$ such that

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 101. *Let $f, g: \mathbb{R} \rightarrow \mathbb{R}$ 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. \square

The treatment of differentiation has demonstrated that the nonstandard theory allows different argumentations from the standard theory. The relation \sim of nearness allows 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 $\forall \varepsilon \exists \delta \dots$ can be replaced by properties of the form $\forall \xi \sim 0 \dots$.

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

Almost all mathematical notions can be defined set-theoretically. The notion of set is adequately formalized in an 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.

Definition 102. *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 *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 the frequent circularity in foundational theories.

Definition 103. *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 $\varphi(z, x_1, \dots, x_n)$:

$$\forall x_1 \dots \forall x_n \forall x \exists y \forall z (z \in y \leftrightarrow z \in x \wedge \varphi(z, x_1, \dots, x_n))$$

- 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 $\varphi(x, y, x_1, \dots, x_n)$:

$$\forall x_1 \dots \forall x_n (\forall x \forall y \forall y' ((\varphi(x, y, x_1, \dots, x_n) \wedge \varphi(x, y', x_1, \dots, x_n)) \rightarrow y \equiv y') \rightarrow \forall u \exists v \forall y (y \in v \leftrightarrow \exists x (x \in u \wedge \varphi(x, y, x_1, \dots, x_n))))$$

- v is the image of u under the map defined by φ .
- i) The foundation schema (Found) postulates for every \in -formula $\varphi(x, x_1, \dots, x_n)$:

$$\forall x_1 \dots \forall x_n (\exists x \varphi(x, x_1, \dots, x_n) \rightarrow \exists x (\varphi(x, x_1, \dots, x_n) \wedge \forall x' (x' \in x \rightarrow \neg \varphi(x', x_1, \dots, x_n))))$$
- if φ is satisfiable then there are \in -minimal elements satisfying φ .

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 104. A class term is of the form $\{x | \varphi\}$ where x is a variable and $\varphi \in L^\infty$. If $\{x | \varphi\}$ and $\{y | \psi\}$ are class terms then

- $u \in \{x | \varphi\}$ stands for φ_x^u ;
- $u = \{x | \varphi\}$ stands for $\forall v (v \in u \leftrightarrow \varphi_x^v)$;
- $\{x | \varphi\} = u$ stands for $\forall v (\varphi_x^v \leftrightarrow v \in u)$;
- $\{x | \varphi\} = \{y | \psi\}$ stands for $\forall v (\varphi_x^v \leftrightarrow \psi_y^v)$;
- $\{x | \varphi\} \in u$ stands for $\exists v (v \in u \wedge v = \{x | \varphi\})$;
- $\{x | \varphi\} \in \{y | \psi\}$ stands for $\exists v (\psi_y^v \wedge v = \{x | \varphi\})$.

In this notation, the separation schema becomes:

$$\forall x_1 \dots \forall x_n \forall x \exists y y = \{z | z \in x \wedge \varphi(z, x_1, \dots, x_n)\}.$$

We shall further extend this notation, first by giving specific names to important formulas and class terms.

Definition 105.

- a) $\emptyset := \{x | x \neq x\}$ is the empty set;
- b) $V := \{x | x = x\}$ is the universe.

We work in the theory ZF for the following propositions.

Proposition 106.

- 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 $y = \{z \mid z \in V \wedge z \notin z\}$. 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. \square

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 \in -formula. We also introduce *bounded quantifiers* to simplify notation.

Definition 107. 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 108. Let x, y, z, \dots be variables and X, Y, Z, \dots be class terms. Define

- a) $X \subseteq Y := \forall x \in X x \in Y$, X is a subclass of Y ;
- b) $X \cup Y := \{x \mid x \in X \vee x \in Y\}$ is the union of X and Y ;
- c) $X \cap Y := \{x \mid x \in X \wedge x \in Y\}$ is the intersection of X and Y ;
- d) $X \setminus Y := \{x \mid x \in X \wedge x \notin Y\}$ is the difference of X and Y ;
- e) $\bigcup X := \{x \mid \exists y \in X x \in y\}$ is the union of X ;
- f) $\bigcap X := \{x \mid \forall y \in X x \in y\}$ is the intersection of X ;
- g) $\mathcal{P}(X) = \{x \mid x \subseteq X\}$ is the power class of X ;
- h) $\{X\} = \{x \mid x = X\}$ is the singleton set of X ;
- i) $\{X, Y\} = \{x \mid x = X \vee x = Y\}$ is the (unordered) pair of X and Y ;
- j) $\{X_0, \dots, X_{n-1}\} = \{x \mid x = X_0 \vee \dots \vee x = X_{n-1}\}$.

One can prove the well-known boolean properties for these operations. We only give a few examples.

Proposition 109. $X \subseteq Y \wedge Y \subseteq X \rightarrow X = Y$.

Proposition 110. $\bigcup \{x, y\} = x \cup y$.

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 $u \in \bigcup \{x, y\}$. \square

We can now reformulate the ZF axioms using class terms.

- a) Extensionality: $\forall x \forall y (x \subseteq y \wedge y \subseteq x \rightarrow x = y)$.
- b) Set existence: $\emptyset \in V$.
- c) Separation schema: for all terms A with free variables x_0, \dots, x_{n-1}

$$\forall x_0 \dots \forall x_{n-1} \forall x x \cap A \in V.$$

- d) Pairing: $\forall x \forall y \{x, y\} \in V$.
- e) Union: $\forall x \bigcup x \in V$.
- f) Powerset: $\forall x \mathcal{P}(x) \in V$.
- g) Infinity: $\exists x (\emptyset \in x \wedge \forall u \in x u \cup \{u\} \in x)$.
- h) Replacement: see later.
- i) Foundation: for all terms A with free variables x_0, \dots, x_{n-1}

$$\forall x_0, \dots, x_{n-1} (A \neq \emptyset \rightarrow \exists x \in A x \cap A = \emptyset).$$

23 Relations and functions

Ordered pairs are the basis for the theory of relations.

Definition 111. $(x, y) = \{\{x\}, \{x, y\}\}$ is the ordered pair of x and y .

Proposition 112. $(x, y) \in V$.
 $(x, y) = (x', y') \rightarrow x = y \wedge x' = y'$.

Definition 113. Let A, B, R be terms. Define

- a) $A \times B = \{z \mid \exists a \in A \exists b \in B z = (a, b)\}$ 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 114.

- a) $\text{dom}(R) = \{x \mid \exists y (x, y) \in R\}$ is the domain of R .
- b) $\text{ran}(R) = \{y \mid \exists x (x, y) \in R\}$ is the range of R .
- c) $R \upharpoonright A = \{z \mid z \in R \wedge \exists x \exists y ((x, y) = z \wedge x \in A)\}$ is the restriction of R to A .
- d) $R[A] = \{y \mid \exists x \in A xRy\}$ is the image of A under R .
- e) $R^{-1} = \{z \mid \exists x \exists y (xRy \wedge z = (y, x))\}$ is the inverse of R .
- f) $R^{-1}[B] = \{x \mid \exists y \in B xRy\}$ is the preimage of B under R .

One can prove the usual properties for these notions in ZF. 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 115. Let F, A, B be terms. Then

- a) F is a function if $\forall x \forall y, y' (xFy \wedge xFy' \rightarrow y = y')$.
- b) $F: A \rightarrow B$ if F is a function $\wedge \text{dom}(F) = A \wedge \text{ran}(F) \subseteq B$. The sequence notions $(F(x) \mid x \in A)$ or $(F(x))_{x \in A}$ are just other ways to write $F: A \rightarrow V$.
- c) $F(x) = \{v \mid \exists y (xFy \wedge \forall y' (xFy' \rightarrow y = y')) \rightarrow \exists y (xFy \wedge v \in y)\}$ is the value of F at x .

Note that if $F: A \rightarrow B$ and $x \in A$ then $xFF(x)$. If there is no unique y such that xFy 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

It is natural to formalize the integer n by some set with n elements. This intuitive plan will be implemented in the sequel. We shall have

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

We note some properties of this informal presentation which will be the basis for the formalization of numbers:

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. On each "number", the \in -relation is a *strict linear order*: $4 = \{0, 1, 2, 3\}$ is strictly linearly ordered by \in .
3. "Numbers" are "complete" with respect to smaller "numbers"

$$i < j < m \rightarrow i \in m.$$

This can be written with the \in -relation as

$$i \in j \in m \rightarrow i \in m,$$

a property termed *transitivity*.

Definition 116.

- a) A is transitive, $\text{Trans}(A)$, iff $\forall y \in A \forall x \in y \ x \in A$.
- b) x is an ordinal (number), $\text{Ord}(x)$, if $\text{Trans}(x) \wedge \forall y \in x \ \text{Trans}(y)$.
- c) Let $\text{Ord} = \{x \mid \text{Ord}(x)\}$ be the class of all ordinal numbers.
- d) Set $0 = \emptyset$; for all x let $x+1 = x \cup \{x\}$.

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 ZF.

Theorem 117.

- a) $0 \in \text{Ord}$.
- b) $\forall x \in \text{Ord} \ x+1 \in \text{Ord}$.

Proof. a) $\text{Trans}(\emptyset)$ since formulas of the form $\forall y \in \emptyset \dots$ are tautologically true. Similarly $\forall y \in \emptyset \ \text{Trans}(y)$.

b) Assume $x \in \text{Ord}$.

(1) $\text{Trans}(x+1)$.

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) $\forall y \in x+1 \ \text{Trans}(y)$.

Proof. Let $y \in x+1 = x \cup \{x\}$.

Case 1. $y \in x$. Then $\text{Trans}(y)$ since x is an ordinal.

Case 2. $y = x$. Then $\text{Trans}(y)$ since x is an ordinal. □

Definition 118. Set $1 = 0 + 1$, $2 = 1 + 1$, $3 = 2 + 1$, etc.

By the previous result, $0, 1, 2, \dots \in \text{Ord}$. The class Ord shares many properties with its elements:

Theorem 119. Let $x \in \text{Ord}$ and $y \in x$. Then $y \in \text{Ord}$.

Proof. This follows immediately from the transitivity definition of Ord . \square

Theorem 120. The class Ord is strictly linearly ordered by \in , i.e.,

- a) $\forall x, y, z \in \text{Ord} (x \in y \wedge y \in z \rightarrow x \in z)$.
- b) $\forall x \in \text{Ord} x \notin x$.
- c) $\forall x, y \in \text{Ord} (x \in y \vee x = y \vee y \in x)$.

Proof. a) Let $x, y, z \in \text{Ord}$ and $x \in y \wedge y \in z$. Then z is transitive, and so $x \in z$.

b) follows immediately from Theorem 110.

c) Assume that there are “incomparable” ordinals. By the foundation schema choose $x_0 \in \text{Ord} \in$ -minimal such that $\exists y \in \text{Ord} \neg(x_0 \in y \vee x_0 = y \vee y \in x_0)$. Again, choose $y_0 \in \text{Ord} \in$ -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 . \square

Definition 121. Let $< = \in \cap \text{Ord} \times \text{Ord} = \{(x, y) | x \in \text{Ord} \wedge y \in \text{Ord} \wedge x \in y\}$ be the natural strict linear ordering of Ord by the \in -relation.

Theorem 122. Let $x \in \text{Ord}$. 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 $y < x$.

24.1 Induction

The ordinals satisfy an *induction theorem* which generalizes *complete induction* on the integers:

Theorem 123. Let $\varphi(x, v_0, \dots, v_{n-1}) \in L^\infty$ and $x_0, \dots, x_{n-1} \in V$. Assume that the property $\varphi(x, x_0, \dots, x_{n-1})$ is inductive, i.e.,

$$\forall x \in \text{Ord} (\forall y \in x \varphi(y, x_0, \dots, x_{n-1}) \rightarrow \varphi(x, x_0, \dots, x_{n-1})).$$

Then φ holds for all ordinals:

$$\forall x \in \text{Ord} \varphi(x, x_0, \dots, x_{n-1}).$$

Proof. Assume not. This means that there are x satisfying the property:

$$x \in \text{Ord} \wedge \neg \varphi(x, x_0, \dots, x_{n-1}).$$

According to the schema of foundation one can take an \in -minimal x with that property:

$$x \in \text{Ord} \wedge \neg \varphi(x, x_0, \dots, x_{n-1}) \wedge \forall y (y \in x \rightarrow \neg y \in \text{Ord} \wedge \neg \varphi(y, x_0, \dots, x_{n-1})).$$

The clause $y \in \text{Ord}$ is redundant since $x \subseteq \text{Ord}$:

$$x \in \text{Ord} \wedge \neg \varphi(x, x_0, \dots, x_{n-1}) \wedge \forall y (y \in x \rightarrow \varphi(y, x_0, \dots, x_{n-1})).$$

By the inductivity of φ the right-hand clause implies $\varphi(x, x_0, \dots, x_{n-1})$ and so

$$x \in \text{Ord} \wedge \neg\varphi(x, x_0, \dots, x_{n-1}) \wedge \varphi(x, x_0, \dots, x_{n-1}).$$

Contradiction. □

24.2 Natural numbers

We have $0, 1, \dots \in \text{Ord}$. We shall now define and study the set of *natural numbers/integers*. Recall the axiom of infinity:

$$\exists x (\emptyset \in x \wedge \forall u (u \in x \rightarrow u \cup \{u\} \in x)).$$

Or, with notations from the theory of ordinals:

$$\exists x (0 \in x \wedge \forall u \in x \ u + 1 \in x).$$

The set of natural numbers should be the \subseteq -smallest such x .

Definition 124. Let $\omega = \bigcap \{x \mid 0 \in x \wedge \forall u \in x \ u + 1 \in x\}$ be the set of natural numbers. Sometimes we write \mathbb{N} instead of ω .

We argue that this is an adequate formalization.

Theorem 125.

- a) $\omega \in V$.
- b) $\omega \subseteq \text{Ord}$.
- c) $(\omega, 0, +1)$ satisfy the second order PEANO axiom, i.e.,

$$\forall x \subseteq \omega (0 \in x \wedge \forall u \in x \ u + 1 \in x \rightarrow x = \omega).$$

- d) $\omega \in \text{Ord}$.

Proof. a) By the axiom of infinity take a set x_0 such that

$$0 \in x_0 \wedge \forall u \in x_0 \ u + 1 \in x_0.$$

Then

$$\omega = \bigcap \{x \mid 0 \in x \wedge \forall u \in x \ u + 1 \in x\} = x_0 \cap \bigcap \{x \mid 0 \in x \wedge \forall u \in x \ u + 1 \in x\} \in V$$

by the separation schema.

b) By a), $\omega \cap \text{Ord} \in V$. Obviously $0 \in \omega \cap \text{Ord} \wedge \forall u \in \omega \cap \text{Ord} \ u + 1 \in \omega \cap \text{Ord}$. So $\omega \cap \text{Ord}$ is one factor of the intersection in the definition of ω and so $\omega \subseteq \omega \cap \text{Ord}$. Hence $\omega \subseteq \text{Ord}$.

c) Let $x \subseteq \omega$ and $0 \in x \wedge \forall u \in x \ u + 1 \in x$. Then x is one factor of the intersection in the definition of ω and so $\omega \subseteq x$. This implies $x = \omega$.

d) By b), every element of ω is transitive and it suffices to show that ω is transitive. Let

$$x = \{n \mid n \in \omega \wedge \forall m \in n \ m \in \omega\} \subseteq \omega.$$

We show that the hypothesis of c) holds for x . $0 \in x$ is trivial. Let $u \in x$. Then $u + 1 \in \omega$. Let $m \in u + 1$. If $m \in u$ then $m \in \omega$ by the assumption that $u \in x$. If $m = u$ then $m \in x \subseteq \omega$. Hence $u + 1 \in x$ and $\forall u \in x \ u + 1 \in x$. By b), $x = \omega$. So $\forall n \in \omega \ n \in x$, i.e.,

$$\forall n \in \omega \forall m \in n \ m \in \omega. \quad \square$$

Recursion, often called induction, over the natural numbers is a ubiquitous method for defining mathematical object. We show a more general recursion theorem in the next subsection.

24.3 Recursion

We prove the following *recursion theorem*.

Theorem 126. *Let $G: V \rightarrow V$. Then there is a canonical class term F such that*

$$F: \text{Ord} \rightarrow V \text{ and } \forall \alpha \in \text{Ord } F(\alpha) = G(F \upharpoonright \alpha).$$

We then say that F is defined by recursion over the ordinals with the recursion rule G .

Proof. Let

$$\tilde{F} = \{f \mid \exists \delta \in \text{Ord } (f: \delta \rightarrow V \text{ and } \forall \alpha < \delta f(\alpha) = G(f \upharpoonright \alpha))\}$$

be the class of all *approximations* to the desired function F . We show properties of \tilde{F} using the induction theorem.

(1) Let $f, g \in \tilde{F}$. Then f, g are *compatible*, i.e., $\forall \alpha \in \text{dom}(f) \cap \text{dom}(g) f(\alpha) = g(\alpha)$.

Proof. We want to show that

$$\forall \alpha \in \text{Ord } (\alpha \in \text{dom}(f) \cap \text{dom}(g) \rightarrow f(\alpha) = g(\alpha)).$$

By the induction theorem it suffices to show that $\alpha \in \text{dom}(f) \cap \text{dom}(g) \rightarrow f(\alpha) = g(\alpha)$ is inductive, i.e.,

$$\forall \alpha \in \text{Ord } (\forall y \in \alpha (y \in \text{dom}(f) \cap \text{dom}(g) \rightarrow f(y) = g(y)) \rightarrow (\alpha \in \text{dom}(f) \cap \text{dom}(g) \rightarrow f(\alpha) = g(\alpha))).$$

So let $\alpha \in \text{Ord}$ and $\forall y \in \alpha (y \in \text{dom}(f) \cap \text{dom}(g) \rightarrow f(y) = g(y))$. Let $\alpha \in \text{dom}(f) \cap \text{dom}(g)$. Since $\text{dom}(f)$ and $\text{dom}(g)$ are ordinals, $\alpha \subseteq \text{dom}(f)$ and $\alpha \subseteq \text{dom}(g)$. By assumption

$$\forall y \in \alpha f(y) = g(y).$$

Hence $f \upharpoonright \alpha = g \upharpoonright \alpha$. Then

$$f(\alpha) = G(f \upharpoonright \alpha) = G(g \upharpoonright \alpha) = g(\alpha).$$

qed(1)

By the compatibility of the approximation functions the union

$$F = \bigcup \tilde{F}$$

is a function defined on a subclass of the ordinals. We show that F satisfies the recursion rule G where F is defined:

(2) $\forall \alpha \in \text{dom}(F) (\alpha \subseteq \text{dom}(F) \wedge F(\alpha) = G(F \upharpoonright \alpha))$.

Proof. Let $\alpha \in \text{dom}(F)$. Take some approximation $f \in \tilde{F}$ such that $\alpha \in \text{dom}(f)$. Since $\text{dom}(f)$ is an ordinal and transitive, we have

$$\alpha \subseteq \text{dom}(f) \subseteq \text{dom}(F).$$

Moreover

$$F(\alpha) = f(\alpha) = G(f \upharpoonright \alpha) = G(F \upharpoonright \alpha).$$

qed(2)

It remains to show that $\text{dom}(F) = \text{Ord}$, i.e.,

(3) $\forall \alpha \in \text{Ord } \alpha \in \text{dom}(F)$.

Proof. By induction on the ordinals. We have to show that $\alpha \in \text{dom}(F)$ is inductive in the variable α . So let $\alpha \in \text{Ord}$ and $\forall y \in \alpha y \in \text{dom}(F)$. Hence $\alpha \subseteq \text{dom}(F)$. Let

$$f = F \upharpoonright \alpha \cup \{(\alpha, G(F \upharpoonright \alpha))\}.$$

f is a function with $\text{dom}(f) = \alpha + 1 \in \text{Ord}$. Let $\alpha' < \alpha + 1$. If $\alpha' < \alpha$ then

$$f(\alpha') = F(\alpha') = G(F \upharpoonright \alpha') = G(f \upharpoonright \alpha').$$

if $\alpha' = \alpha$ then also

$$f(\alpha') = f(\alpha) = G(F \upharpoonright \alpha) = G(f \upharpoonright \alpha) = G(f \upharpoonright \alpha').$$

Hence $f \in \tilde{F}$ and $\alpha \in \text{dom}(f) \subseteq \text{dom}(F)$. □

We have now everything together to proceed with the further formalization of mathematics. The arithmetic operations on $\mathbb{N} = \omega$. This yields natural arithmetic, integers, and rationals. The real numbers can then be defined by DEDEKIND cuts or so.

25 Cardinals

The main focus of set theory is the study of *infinity*. We study some basic properties of cardinalities.

Definition 127.

- a) $\text{card}(x) = \bigcap \{ \alpha \mid \exists f (f: \alpha \rightarrow x \wedge f \text{ is surjective}) \}$ is the cardinality of x .
- b) x is finite if $\text{card}(x) < \omega$.
- c) x is infinite if $\text{card}(x) \not< \omega$.
- d) x is countable if $\text{card}(x) \leq \omega$.
- e) x is uncountable if x is not countable.

Theorem 128.

- a) $\forall n < \omega \text{ card}(n) = n$.
- b) $\text{card}(\omega) = \omega$.
- c) $\text{card}(\omega + 1) = \omega$.

Proof. a) By “complete induction” on $n < \omega$.
 $n = 0$: $\emptyset: \emptyset \rightarrow \emptyset$ is surjective. Hence

$$0 = \emptyset \subseteq \text{card}(0) = \bigcap \{ \alpha \mid \exists f (f: \alpha \rightarrow x \wedge f \text{ is surjective}) \} \subseteq \emptyset = 0.$$

$n = m + 1$, and assume that $\text{card}(m) = m$. Assume for a contradiction that $\text{card}(n) \leq m$. Take $f: m \rightarrow n$ surjective. Then $m \neq 0$ and we can take l such that $m = l + 1$.

Case 1. $f(l) = m$. Then $f \upharpoonright l: l \rightarrow m$ is surjective and $\text{card}(m) \leq l < m$. Contradiction.

Case 2. $f(l) < m$. Then define $f': l \rightarrow m$ by

$$f'(k) = \begin{cases} f(k), & \text{if } f(k) < m \\ f(l), & \text{if } f(k) = m \end{cases}$$

Then $f': l \rightarrow m$ is surjective and $\text{card}(m) \leq l < m$. Contradiction.

b) Obviously $\text{card}(\omega) \leq \omega$. Assume for a contradiction that $n = \text{card}(\omega) < \omega$. Then there is a surjection from n onto ω . This implies the existence of a surjection from n onto $n + 1$. Then $\text{card}(n + 1) \leq n$ contradicting a).

c) Define $f: \omega \rightarrow \omega + 1$ by

$$f(n) = \begin{cases} \omega, & \text{if } n = 0 \\ n - 1, & \text{if } n > 0 \end{cases}$$

$f: \omega \rightarrow \omega + 1$ is surjective and so $\text{card}(\omega + 1) = \omega$. □

We want to show that the set of finite sequences from a countable set is countable.

Theorem 129. *Let*

$$A^{<\omega} = \{ w \mid \exists n < \omega w: n \rightarrow A \}$$

be the class of all finite sequences from A . Let A be countable. Then $A^{<\omega}$ is countable.

Proof. We may assume that $A \neq \emptyset$. Let $f: \omega \rightarrow A$ be surjective. Define a map $g: \omega \rightarrow A^{<\omega}$ as follows. Let $n < \omega$, $n \neq 0$. Let $n = 2^{n_0} 3^{n_1} \dots p_{k-1}^{n_{k-1}+1}$ be the unique decomposition of n into prime factors. Then set

$$g(n) = (f(n_i))_{i \in k} \in A^{<\omega}.$$

Obviously, $g: \omega \rightarrow A^{<\omega}$ is surjective. □

Theorem 130. (Cantor) $\text{card}(\mathcal{P}(\omega)) \not\leq \omega$.

Proof. Assume that $\text{card}(\mathcal{P}(\omega)) \leq \omega$ and let $f: \omega \rightarrow \mathcal{P}(\omega)$ be surjective. Define

$$a = \{n \mid n < \omega \wedge n \notin f(n)\} \in \mathcal{P}(\omega).$$

Since f is surjective, take $n_0 < \omega$ such that $a = f(n_0)$. Then

$$n_0 \in a \leftrightarrow n_0 \notin f(n_0) = a.$$

Contradiction. □

This property is usually stated as: there are uncountably many real numbers. This leads immediately to questions like CANTOR's continuum hypothesis.

26 The axiom of choice

Many arguments in infinitary mathematics depend on the possibility of making infinitely many assignments or choices: "for every $n \in \omega$ let $f(n) = \dots$ ". Important examples are choices of sequences in analysis, the choice of bases for vector spaces, and many other places. It can be shown that infinitely many choices are in general not implied by the ZF-axioms, and one has to add *choice principles* or axioms. Probably the most popular such choice principle is ZORN's lemma which we already used in the proof of the general completeness theorem:

Every inductive partial order has a maximal element.

Let us define the axiom of choice.

Definition 131. *The axiom of choice, AC, is the following statement:*

$$\forall x(\forall u, v \in x(u \neq \emptyset \wedge (u \neq v \rightarrow u \cap v = \emptyset)) \rightarrow \exists z \forall u \in x \exists v u \cap z = \{v\}).$$

In ZF, the axiom of choice is equivalent to ZORN's lemma. Here we only prove one direction:

Theorem 132. *The lemma of ZORN implies AC.*

Proof. Let $x \in V$ such that $\forall u, v \in x(u \neq \emptyset \wedge (u \neq v \rightarrow u \cap v = \emptyset))$, i.e., the elements of x are non-empty and pairwise disjoint. To apply ZORN's lemma, define a partial order (Z, \subseteq) by

$$Z = \{z \mid z \subseteq \bigcup x \wedge \forall u \in x \text{card}(u \cap z) \leq 1\}.$$

$Z \subseteq \mathcal{P}(\bigcup x)$, and so $Z \in V$ by the axioms of union, power set, and separation. The relation \subseteq is always a partial order.

(1) (Z, \subseteq) is inductive.

Proof. Let $I \subseteq Z$ be a linear subset of Z , i.e., $\forall z, z' \in I(z \subseteq z' \vee z = z' \vee z' \subseteq z)$. Let $z^* = \bigcup I$. We have to show that $z^* \in Z$. Let $u \in x$ but assume that $\text{card}(u \cap z^*) \not\leq 2$. Choose elements $a, a' \in u \cap z^*$, $a \neq a'$. Choose $z, z' \in I$ such that $a \in z$ and $a' \in z'$. By the linearity of I we can assume that $z \subseteq z'$. Then $a, a' \in u \cap z'$, contradiction. *qed*(1)

By the lemma of ZORN, let z be an \subseteq -maximal element of Z . Let $u \in x$. We have to show that $\text{card}(u \cap z) = 1$. By the definition of Z , $\text{card}(u \cap z) \leq 1$. Assume for a contradiction that $\text{card}(u \cap z) = 0$, i.e., $u \cap z = \emptyset$. Take $v \in u$ and let

$$z' = z \cup \{v\}.$$

Then $z' \subseteq \bigcup x$ and $z \subseteq z'$, $z \neq z'$. We get a contradiction to the maximality of z by showing that (2) $z' \in Z$.

Proof. Let $u' \in x$. If $u' \neq u$ then $v \notin u'$ by pairwise disjointness and

$$\text{card}(u' \cap z') = \text{card}(u' \cap z) \leq 1.$$

If $u' = u$ then

$$u' \cap z' = u \cap z' = u \cap (z \cup \{v\}) = (u \cap z) \cup (u \cap \{v\}) = \emptyset \cup \{v\} = \{v\}. \quad \square$$

Definition 133. ZFC is the axiom system consisting of ZF together with the axiom of choice AC.

The system ZFC is generally assumed as a basis for ordinary mathematics since it implies the standard consequences of the axiom of choice or ZORN's lemma in the realms of analysis and linear algebra like choosing infinite sequences of reals with some properties or bases for arbitrary vector spaces.

Let us apply ZORN's lemma to get another proof of the SKOLEM paradoxon:

Theorem 134. Let S be a countable language and let \mathfrak{M} be an S -structure. Then there is an elementary substructure $\mathfrak{N} \prec \mathfrak{M}$ such that $N = |\mathfrak{N}'|$ is countable.

Proof. Let $M = |\mathfrak{M}|$. A function

$$h: L^S \times M^{<\omega} \rightarrow M$$

is called a SKOLEM function for \mathfrak{M} if for all $\varphi(v_0, \dots, v_n) \in L^S$ and all $(a_1, \dots, a_n) \in M^n$

$$\mathfrak{M} \models \exists v_0 \varphi[a_1, \dots, a_n] \text{ implies } \mathfrak{M} \models \varphi[h(\varphi, (a_1, \dots, a_n)), a_1, \dots, a_n].$$

We shall later show the existence of such a function using ZORN's lemma. We first show:

(1) If $\mathfrak{N} \subseteq \mathfrak{M}$ is a substructure of \mathfrak{M} which is closed with respect to a SKOLEM function h for \mathfrak{M} then $\mathfrak{N} \prec \mathfrak{M}$.

Proof. We show by induction on the complexity of $\psi(v_1, \dots, v_n) \in L^S$

$$\forall a_1, \dots, a_n \in |\mathfrak{N}| (\mathfrak{N} \models \psi[a_1, \dots, a_n] \leftrightarrow \mathfrak{M} \models \psi[a_1, \dots, a_n]).$$

This is clear for atomic formulas. The induction steps are trivial for propositional connectives. So let us finally consider $\psi(v_1, \dots, v_n) = \exists v_0 \varphi$ where the property already holds for $\varphi(v_0, v_1, \dots, v_n)$. Let $a_1, \dots, a_n \in |\mathfrak{N}|$.

Assume $\mathfrak{N} \models \psi[a_1, \dots, a_n]$. Take $a_0 \in |\mathfrak{N}|$ such that $\mathfrak{N} \models \varphi[a_0, a_1, \dots, a_n]$. By assumption, $\mathfrak{M} \models \varphi[a_0, a_1, \dots, a_n]$ and so $\mathfrak{M} \models \psi[a_1, \dots, a_n]$.

Conversely let $\mathfrak{M} \models \psi[a_1, \dots, a_n]$. Then $\mathfrak{M} \models \exists v_0 \varphi[a_1, \dots, a_n]$. Since h is a SKOLEM function, $\mathfrak{M} \models \varphi[h(\varphi, (a_1, \dots, a_n)), a_1, \dots, a_n]$. Since $|\mathfrak{N}|$ is closed under h , $h(\varphi, (a_1, \dots, a_n)) \in |\mathfrak{N}|$. By the inductive assumption on φ ,

$$\mathfrak{N} \models \varphi[h(\varphi, (a_1, \dots, a_n)), a_1, \dots, a_n].$$

Hence $\mathfrak{N} \models \exists v_0 \varphi[a_1, \dots, a_n]$. *qed*(1) ... □

The SKOLEM paradox revisited: If there is a model of ZF then there is a countable model \mathfrak{N} of ZF. Since the powerset of ω is uncountable in all models of ZF, the countable model \mathfrak{N} satisfies the sentence "there is an uncountable set". This goes against the intuition that ZF describes the universe of sets.

27 Logic in ZF

We have formulated the logical notions in a set theoretical framework:

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 $n \in \mathbb{N}$.

Every symbol, term, or formula can be represented canonically by some class term, just like the ordinary numbers "one, two, ..." are represented by class terms 0, 1, We use GÖDEL brackets $\ulcorner \varphi \urcorner$ to denote the class term corresponding to φ .

All the other notions introduced can also be GÖDELized.

28 The undefinability of truth

We prove a fix point theorem:

Theorem 135. *Let $\varphi(v_0)$ be an \in -formula. Then there is an \in -sentence θ without free variables such that*

$$\text{ZF} \vdash \theta \leftrightarrow \varphi(\ulcorner \theta \urcorner).$$

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 $\text{sub}(v_0, v_1, v_2)$ be a canonical \in -formula such that for all \in -formulas χ, χ'

$$\text{ZF} \models (\text{sub}(\ulcorner \chi \urcorner, \ulcorner \chi' \urcorner, z) \text{ iff } z = \ulcorner \chi(\ulcorner \chi' \urcorner) \urcorner = \ulcorner \exists v_0(v_0 = \ulcorner \chi' \urcorner \wedge \chi) \urcorner).$$

Then let

$$\psi(v_0) = \exists v_1(\text{sub}(v_0, v_0, v_1) \wedge \exists v_0(v_0 = v_1 \wedge \varphi)).$$

In ZF

$$\begin{aligned} \psi(\ulcorner \psi \urcorner) &= \exists v_0(v_0 = \ulcorner \psi \urcorner \wedge \psi) \\ &= \exists v_0(v_0 = \ulcorner \psi \urcorner \wedge \exists v_1(\text{sub}(v_0, v_0, v_1) \wedge \exists v_0(v_0 = v_1 \wedge \varphi))) \\ &\leftrightarrow \text{sub}(\ulcorner \psi \urcorner, \ulcorner \psi \urcorner, \ulcorner \exists v_0(v_0 = \ulcorner \psi \urcorner \wedge \psi) \urcorner) \wedge \exists v_0(v_0 = \ulcorner \exists v_0(v_0 = \ulcorner \psi \urcorner \wedge \psi) \urcorner \wedge \varphi) \\ &\leftrightarrow \exists v_0(v_0 = \ulcorner \exists v_0(v_0 = \ulcorner \psi \urcorner \wedge \psi) \urcorner \wedge \varphi) \\ &\leftrightarrow \varphi(\ulcorner \exists v_0(v_0 = \ulcorner \psi \urcorner \wedge \psi) \urcorner) \end{aligned}$$

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 136. *An \in -formula $\psi(v_0)$ is a definition of truth if for all \in -sentences θ :*

$$\text{ZF} \vdash (\theta \leftrightarrow \psi(\ulcorner \theta \urcorner)).$$

Using the fix point theorem we can easily show TARSKI’s theorem on the *undefinability of truth*:

Theorem 137. *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

$$\text{ZF} \vdash (\theta \leftrightarrow \neg \psi(\ulcorner \theta \urcorner)).$$

Since $\psi(v_0)$ is a definition of truth we also have

$$\text{ZF} \vdash (\theta \leftrightarrow \psi(\ulcorner \theta \urcorner)).$$

Together

$$\text{ZF} \vdash (\neg\psi(\ulcorner \theta \urcorner) \leftrightarrow \psi(\ulcorner \theta \urcorner)),$$

contradiction. □

29 The first GÖDEL incompleteness theorem

Theorem 138. *If ZF is consistent then ZF is incomplete, i.e., there is an \in -sentence φ such that $\text{ZF} \not\vdash \varphi$ and $\text{ZF} \not\vdash \neg\varphi$.*

The basic idea of the proof is: if ZF were complete then we could “decide” any \in -sentence by systematically running through all possible proofs from the axioms of ZF. Formalizing this idea in ZF one gets a definition of truth within ZF: if one first finds a *formal proof* of φ then φ follows from ZF, and if one first finds a *formal proof* of $\neg\varphi$ then $\neg\varphi$ follows from ZF. By the formalization of first-order logic within ZF there is an \in -formula $\text{Pf}(v_0, v_1)$ expressing that v_0 is a formal proof of v_1 from ZF. The predicate of *provability* can then be defined as

$$\text{Pv}(v_1) = \exists v_0 \text{Pf}(v_0, v_1).$$

Proof. We showed in the proof of Theorem 129 that any enumeration of A by ω induces a concrete and *definable* enumeration of $A^{<\omega}$ by ω .

A formal proof is a finite sequence of sequents, a sequent is a finite sequence of formulas, a formula is a finite sequence of symbols.

Defining natural enumerations for the sets of symbols, \in -formulas, sequents, and proofs in analogy with the techniques of the proof of Theorem 129 yields a list

$$P_0, P_1, \dots$$

of all proofs from the axioms of ZF.

This can be formalized within ZF: there is a class term $P(v_0)$ such that

$$\forall n < \omega \text{P}(n) \text{ is a formal proof from ZF.}$$

Furthermore, for all natural numbers $n = 0, 1, \dots$

$$\text{ZF} \vdash P(n) = \ulcorner P_n \urcorner.$$

Let us now assume that ZF is complete and consistent. We show that the formula

$$\psi(v_0) = \exists n < \omega (\text{Pf}(P(n), v_0) \wedge \forall m < n \neg \text{Pf}(P(m), \neg v_0))$$

is a definition of truth.

Let θ be an \in -sentence.

Case 1. $\text{ZF} \vdash \theta$. Then there is a natural number $n \in \{0, 1, \dots\}$ such that P_n is a proof of θ from ZF. Since ZF is consistent, P_m is not a formal proof of $\neg\theta$ for $m = 0, 1, \dots, n - 1$. Then

$$\text{ZF} \vdash \text{Pf}(P(n), \ulcorner \theta \urcorner)$$

and for $m = 0, 1, \dots, n - 1$

$$\text{ZF} \vdash \neg \text{Pf}(P(m), \neg \ulcorner \theta \urcorner).$$

Since

$$\text{ZF} \vdash n = \{0, 1, \dots, n - 1\},$$

we have

$$\text{Pf}(P(n), \ulcorner \theta \urcorner) \wedge \forall m < n \neg \text{Pf}(P(m), \neg \ulcorner \theta \urcorner).$$

Thus $\text{ZF} \vdash \psi(\ulcorner \theta \urcorner)$.

Case 2. $\text{ZF} \vdash \neg\theta$. Then there is a natural number $m \in \{0, 1, \dots\}$ such that P_m is a proof of $\neg\theta$ from ZF. Since ZF is consistent, P_n is not a formal proof of θ for $n = 0, 1, \dots, m$. Work within the system ZF. Let $n < \omega$.

Case 2.1. $n \leq m$. Since $n = \{0, 1, \dots, n-1\}$, $\neg\text{Pf}(P(n), \ulcorner \theta \urcorner)$.

Case 2.2. $n > m$. Then $P(m)$ witnesses that $\exists m < k \text{ Pf}(P(m), \neg\ulcorner \theta \urcorner)$.

By these cases

$$\forall n < \omega \neg(\text{Pf}(P(n), \ulcorner \theta \urcorner) \wedge \forall m < n \text{ Pf}(P(m), \neg\ulcorner \theta \urcorner))$$

and $\neg\psi(\ulcorner \theta \urcorner)$.

By these cases

$$\text{ZF} \vdash (\theta \leftrightarrow \psi(\ulcorner \theta \urcorner)).$$

But then ZF is inconsistent by the theorem on the undefinability of truth. □

30 The second GÖDEL incompleteness theorem

Definition 139. Define the \in -formula

$$\text{Con}(\text{ZF}) = \neg\text{Pv}(\ulcorner \perp \urcorner).$$

$\text{Con}(\text{ZF})$ formalizes that the system ZF is consistent. The second incompleteness theorem states that ZF cannot prove its own consistency, i.e., that mathematics cannot prove the consistency of mathematics.

Theorem 140. *If ZF is consistent then $\text{ZF} \not\vdash \text{Con}(\text{ZF})$.*

Proof. By the fix point theorem there is an \in -sentence θ such that

$$\text{ZF} \vdash (\theta \leftrightarrow \neg\text{Pv}(\ulcorner \theta \urcorner)).$$

The sentence θ formalizes the idea: “this sentence is not provable”.

(1) If ZF is consistent then $\text{ZF} \not\vdash \theta$.

Proof. Assume $\text{ZF} \vdash \theta$. Then $\text{ZF} \vdash \text{Pv}(\theta)$. By the fix point property, $\text{ZF} \vdash \neg\theta$. Hence ZF is inconsistent. *qed*(1)

The argument of (1) can be formalized within ZF:

(2) $\text{ZF} \vdash \text{Con}(\text{ZF}) \rightarrow \neg\text{Pv}(\ulcorner \theta \urcorner)$.

Assume now that $\text{ZF} \vdash \text{Con}(\text{ZF})$. By (2), $\text{ZF} \vdash \neg\text{Pv}(\ulcorner \theta \urcorner)$. By the fix point property, $\text{ZF} \vdash \theta$. By (1), ZF is inconsistent. □

Remark 141.

31 Normal forms

There are many motivations to transform formulas into equivalent *normal forms*. The motivation here will be that normal forms are important for *automated theorem proving* and for *logic programming*.

We are particularly interested in transforming formulas ψ into formulas ψ' such that ψ is consistent iff ψ' is consistent. This relates to provability as follows: $\Phi \vdash \varphi$ iff $\Phi \cup \{\neg\varphi\}$ is not satisfiable/inconsistent. So a check for provability can be based on inconsistency checks.

Work in some fixed language S .

Definition 142.

a) An S -formula is a literal if it is atomic or the negation of an atomic formula.

b) Define the dual of the literal L as

$$\bar{L} = \begin{cases} \neg L, & \text{if } L \text{ is an atomic formula;} \\ K, & \text{if } L \text{ is of the form } \neg K. \end{cases}$$

c) A formula φ is in disjunctive normal form if it is of the form

$$\varphi = \bigvee_{i < m} \left(\bigwedge_{j < n_i} L_{ij} \right)$$

where each L_{ij} is a literal.

d) A formula φ is in conjunctive normal form if it is of the form

$$\varphi = \bigwedge_{i < m} \left(\bigvee_{j < n_i} L_{ij} \right)$$

where each L_{ij} is a literal. Sometimes a disjunctive normal form is also written in set notation as

$$\varphi = \{ \{L_{00}, \dots, L_{0n_0-1}\}, \dots, \{L_{m-1,0}, \dots, L_{m-1,n_m-1}\} \}.$$

Theorem 143. Let φ be a formula without quantifiers. Then φ is equivalent to some φ' in disjunctive normal form and to some φ'' in conjunctive normal form.

Proof. By induction on the complexity of φ . Clear for φ atomic. The \neg step follows from the de Morgan laws:

$$\begin{aligned} \neg \bigvee_{i < m} \left(\bigwedge_{j < n_i} L_{ij} \right) &\leftrightarrow \bigwedge_{i < m} \neg \left(\bigwedge_{j < n_i} L_{ij} \right) \\ &\leftrightarrow \bigwedge_{i < m} \left(\bigvee_{j < n_i} \neg L_{ij} \right). \end{aligned}$$

The \wedge -step is clear for conjunctive normal forms. For disjunctive normal forms the associativity rules yield

$$\bigvee_{i < m} \left(\bigwedge_{j < n_i} L_{ij} \right) \wedge \bigvee_{i' < m'} \left(\bigwedge_{j' < n'_i} L'_{ij} \right) \leftrightarrow \bigvee_{i < m, i' < m'} \left(\bigwedge_{j < n_i} L_{ij} \wedge \bigwedge_{j' < n'_i} L'_{ij} \right)$$

which is also in conjunctive normal form. \square

Definition 144. A formula φ is in prenex normal form if it is of the form

$$\varphi = Q_0 x_0 Q_1 x_1 \dots Q_{m-1} x_{m-1} \psi$$

where each Q_i is either the quantifier \forall or \exists and ψ is quantifier-free. Then the quantifier string $Q_0 x_0 Q_1 x_1 \dots Q_{m-1} x_{m-1}$ is called the prefix of φ and the formula ψ is the matrix of φ .

Theorem 145. Let φ be a formula. Then φ is equivalent to a formula φ' in prenex normal form.

Proof. By induction on the complexity of φ . Clear for atomic formulas. If

$$\varphi \leftrightarrow Q_0 x_0 Q_1 x_1 \dots Q_{m-1} x_{m-1} \psi$$

with quantifier-free ψ then by the de Morgan laws for quantifiers

$$\neg \varphi \leftrightarrow \bar{Q}_0 x_0 \bar{Q}_1 x_1 \dots \bar{Q}_{m-1} x_{m-1} \neg \psi$$

where the dual quantifier \bar{Q} is defined by $\bar{\exists} = \forall$ and $\bar{\forall} = \exists$.

For the \wedge -operation consider another formula

$$\varphi' \leftrightarrow Q'_0 x'_0 Q'_1 x'_1 \dots Q'_{m'-1} x'_{m'-1} \psi'.$$

We may assume that the sets of bounded variables of the prenex normal forms are disjoint. Then

$$\varphi \wedge \varphi' \leftrightarrow Q_0 x_0 Q_1 x_1 \dots Q_{m-1} x_{m-1} Q'_0 x'_0 Q'_1 x'_1 \dots Q'_{m'-1} x'_{m'-1} (\psi \wedge \psi').$$

(semantic argument). □

Definition 146. A formula φ is universal if it is of the form

$$\varphi = \forall x_0 \forall x_1 \dots \forall x_{m-1} \psi$$

where ψ is quantifier-free. A formula φ is existential if it is of the form

$$\varphi = \exists x_0 \exists x_1 \dots \exists x_{m-1} \psi$$

where ψ is quantifier-free.

We show a quasi-equivalence with respect to universal (and existential) formulas which is not a logical equivalence but concerns the consistency or satisfiability of formulas.

Theorem 147. Let φ be an S -formula. Then there is a canonical extension S^* of the language S and a canonical universal $\varphi^* \in L^{S^*}$ such that

$$\varphi \text{ is consistent iff } \varphi^* \text{ is consistent.}$$

The formula φ^* is called the SKOLEM normal form of φ .

Proof. By a previous theorem we may assume that φ is in prenex normal form. We prove the theorem by induction on the number of existential quantifiers in φ . If φ does not contain an existential quantifier we are done. Otherwise let

$$\varphi = \forall x_1 \dots \forall x_m \exists y \psi$$

where $m < \omega$ may also be 0. Introduce a new m -ary function symbol f (or a constant symbol in case $m = 0$) and let

$$\varphi' = \forall x_1 \dots \forall x_m \psi \frac{f x_1 \dots x_m}{y}.$$

By induction it suffices to show that φ is consistent iff φ' is consistent.

(1) $\varphi' \rightarrow \varphi$.

Proof. Assume φ' . Consider x_1, \dots, x_m . Then $\psi \frac{f x_1 \dots x_m}{y}$. Then $\exists y \psi$. Thus $\forall x_1 \dots \forall x_m \exists y \psi$. *qed*(1)

(2) If φ' is consistent then φ is consistent.

Proof. If $\varphi \rightarrow \perp$ then by (1) $\varphi' \rightarrow \perp$. *qed*(2)

(3) If φ is consistent then φ' is consistent.

Proof. Let φ be consistent and let $\mathcal{M} = (M, \dots) \models \varphi$. Then

$$\forall a_1 \in M \dots \forall a_m \in M \exists b \in M \mathcal{M} \frac{\vec{a} \ b}{\vec{x} \ y} \models \psi.$$

Using the axiom of choice there is a function $h: M^m \rightarrow M$ such that

$$\forall a_1 \in M \dots \forall a_m \in M \mathcal{M} \frac{\vec{a} \ h(a_1, \dots, a_m)}{\vec{x} \ y} \models \psi.$$

Expand the structure \mathcal{M} to $\mathcal{M}' = \mathcal{M} \cup \{(f, h)\}$ where the symbol f is interpreted by the function h . Then $h(a_1, \dots, a_m) = \mathcal{M}' \frac{\vec{a}}{\vec{x}}(f x_1 \dots x_m)$ and

$$\forall a_1 \in M \dots \forall a_m \in M \mathcal{M}' \frac{\vec{a} \ \mathcal{M}' \frac{\vec{a}}{\vec{x}}(f x_1 \dots x_m)}{\vec{x} \ y} = \mathcal{M}' \frac{\vec{a}}{\vec{x}} \frac{\mathcal{M}' \frac{\vec{a}}{\vec{x}}(f x_1 \dots x_m)}{y} \models \psi.$$

By the substitution theorem this is equivalent to

$$\forall a_1 \in M \dots \forall a_m \in M \mathcal{M}' \frac{\vec{a}}{\vec{x}} \models \psi \frac{f x_1 \dots x_m}{y}.$$

Hence

$$\mathcal{M}' \models \forall x_1 \dots \forall x_m \psi \frac{f x_1 \dots x_m}{y} = \varphi'.$$

Thus φ' is consistent. □

32 HERBRAND'S theorem

By the previous chapter we can reduce the question whether a given finite set of formulas is inconsistent to the question whether some universal formula is inconsistent. By the following theorem this can be answered rather concretely.

Theorem 148. *Let S be a language which contains at least one constant symbol. Let*

$$\varphi = \forall x_0 \forall x_1 \dots \forall x_{m-1} \psi$$

be a universal S -sentence with quantifier-free matrix ψ . Then φ is inconsistent if there are variable-free S -terms ("constant terms")

$$t_0^0, \dots, t_{m-1}^0, \dots, t_0^{N-1}, \dots, t_{m-1}^{N-1}$$

such that

$$\varphi' = \bigwedge_{i < N} \psi \frac{t_0^i, \dots, t_{m-1}^i}{x_0, \dots, x_{m-1}} = \psi \frac{t_0^0, \dots, t_{m-1}^0}{x_0, \dots, x_{m-1}} \wedge \dots \wedge \psi \frac{t_0^{N-1}, \dots, t_{m-1}^{N-1}}{x_0, \dots, x_{m-1}}$$

is inconsistent.

Proof. All sentences φ' , for various choices of constant terms, are logical consequences of φ . So φ is consistent, all φ' are consistent.

Conversely assume that all φ' are consistent. Then by the compactness theorem

$$\Phi = \left\{ \psi \frac{t_0, \dots, t_{m-1}}{x_0, \dots, x_{m-1}} \mid t_0, \dots, t_{m-1} \text{ are constant } S\text{-terms} \right\}$$

is consistent. Let $\mathcal{M} = (M, \dots) \models \Phi$. Let

$$H = \{ \mathcal{M}(t) \mid t \text{ is a constant } S\text{-term} \}.$$

Then $H \neq \emptyset$ since S contains a constant symbol. By definition, H is closed under the functions of \mathcal{M} . So we let $\mathcal{H} = (H, \dots) \subseteq \mathcal{M}$ be the substructure of \mathcal{M} with domain H .

(1) $\mathcal{H} \models \varphi$.

Proof. Let $\mathcal{M}(t_0), \dots, \mathcal{M}(t_{m-1}) \in H$ where t_0, \dots, t_{m-1} are constant S -terms. Then $\psi \frac{t_0, \dots, t_{m-1}}{x_0, \dots, x_{m-1}} \in \Phi$, $\mathcal{M} \models \psi \frac{t_0, \dots, t_{m-1}}{x_0, \dots, x_{m-1}}$, and by the substitution theorem

$$\mathcal{M} \frac{\mathcal{M}(t_0), \dots, \mathcal{M}(t_{m-1})}{x_0, \dots, x_{m-1}} \models \psi.$$

Since ψ is quantifier-free this transfers to \mathcal{H} :

$$\mathcal{H} \frac{\mathcal{M}(t_0), \dots, \mathcal{M}(t_{m-1})}{x_0, \dots, x_{m-1}} \models \psi.$$

Thus

$$\mathcal{H} \models \forall x_0 \forall x_1 \dots \forall x_{m-1} \psi = \varphi.$$

qed(1)

Thus φ is consistent. □

In case that the formula ψ does not contain the equality sign \equiv checking for inconsistency of

$$\varphi' = \bigwedge_{i < N} \psi \frac{t_0^i, \dots, t_{m-1}^i}{x_0, \dots, x_{m-1}} = \psi \frac{t_0^0, \dots, t_{m-1}^0}{x_0, \dots, x_{m-1}} \wedge \dots \wedge \psi \frac{t_0^{N-1}, \dots, t_{m-1}^{N-1}}{x_0, \dots, x_{m-1}}$$

is in principle a straightforward finitary problem. φ' contains finitely many constant S -terms. φ' is consistent iff the relation symbols can be interpreted on appropriate tuples of the occurring S -terms to make φ' true. There are finitely many possibilities for the assignments of truth values of relations. This leads to the following (theoretical) algorithm for automatic proving for formulas without \equiv :

Let $\Omega \subseteq L^S$ be finite and $\chi \in L^S$. To check whether $\Omega \vdash \chi$:

1. Form $\Phi = \Omega \cup \{\neg \chi\}$ and let $\varphi = \forall (\bigwedge \Phi)$ be the universal closure of $\bigwedge \Phi$. Then $\Omega \vdash \chi$ iff $\Phi = \Omega \cup \{\neg \chi\}$ is inconsistent iff $(\bigwedge \Phi) \vdash \perp$ iff $\forall (\bigwedge \Phi) \vdash \perp$.

2. Transform φ into universal form $\varphi^\forall = \forall x_0 \forall x_1 \dots \forall x_{m-1} \psi$ (SKOLEMization).
3. Systematically search for constant S -terms

$$t_0^0, \dots, t_{m-1}^0, \dots, t_0^{N-1}, \dots, t_{m-1}^{N-1}$$

such that

$$\varphi' = \bigwedge_{i < N} \psi \frac{t_0^i, \dots, t_{m-1}^i}{x_0, \dots, x_{m-1}} = \psi \frac{t_0^0, \dots, t_{m-1}^0}{x_0, \dots, x_{m-1}} \wedge \dots \wedge \psi \frac{t_0^{N-1}, \dots, t_{m-1}^{N-1}}{x_0, \dots, x_{m-1}}$$

is inconsistent.

4. If an inconsistent φ' is found, output “yes”, otherwise carry on.

Obviously, if “yes” is output then $\Omega \vdash \chi$. This is the *correctness* of the algorithm. On the other hand, HERBRAND's theorem ensures that if $\Omega \vdash \chi$ then an appropriate φ' will be found, and “yes” will be output, i.e., the algorithm is *complete*.

Let us assume from now on, that the formulas considered do not contain the symbol \equiv .

We shall see that the search for those S -terms and the inconsistency-check can be further systematized. We can assume that the quantifier-free formula ψ is in conjunctive normal form, i.e., a conjunction of clauses $\psi = c_0 \wedge c_1 \wedge \dots \wedge c_{l-1}$. Then $\forall x_0 \forall x_1 \dots \forall x_{m-1} \psi$ is inconsistent iff the set

$$\{c_i \frac{t_0, \dots, t_{m-1}}{x_0, \dots, x_{m-1}} \mid t_0, \dots, t_{m-1} \text{ are constant } S\text{-terms}\}$$

is inconsistent.

The method of *resolution* gives an efficient method for showing the inconsistency of sets of clauses.

Definition 149. Let $c^+ = \{K_0, \dots, K_{k-1}\}$ and $c^- = \{L_0, \dots, L_{l-1}\}$ be clauses with literals K_i and L_j . Note that $\{K_0, \dots, K_{k-1}\}$ stands for the disjunction $K_0 \vee \dots \vee K_{k-1}$. Assume that K_0 and L_0 are dual, i.e., $L_0 = \neg K_0$. Then the disjunction

$$\{K_1, \dots, K_{k-1}\} \cup \{L_1, \dots, L_{l-1}\}$$

is a resolution of c^+ and c^- .

Resolution is related to the application of modus ponens: $\varphi \rightarrow \psi$ and φ correspond to the clauses $\{\neg\varphi, \psi\}$ and $\{\varphi\}$. $\{\psi\}$ is a resolution of $\{\neg\varphi, \psi\}$ and $\{\varphi\}$.

Theorem 150. Let C be a set of clauses and let c be a resolution of two clauses $c^+, c^- \in C$. Then if $C \cup \{c\}$ is inconsistent then C is inconsistent.

Proof. Let $c^+ = \{K_0, \dots, K_{k-1}\}$, $c^- = \{\neg K_0, L_1, \dots, L_{l-1}\}$, and $c = \{K_1, \dots, K_{k-1}\} \cup \{L_1, \dots, L_{l-1}\}$. Assume that $\mathcal{M} \models C$ is a model of C .

Case 1. $\mathcal{M} \models K_0$. Then $\mathcal{M} \models c^+$, $\mathcal{M} \models \{L_1, \dots, L_{l-1}\}$, and

$$\mathcal{M} \models \{K_1, \dots, K_{k-1}\} \cup \{L_1, \dots, L_{l-1}\} = c.$$

Case 2. $\mathcal{M} \models \neg K_0$. Then $\mathcal{M} \models c^-$, $\mathcal{M} \models \{K_1, \dots, K_{k-1}\}$, and

$$\mathcal{M} \models \{K_1, \dots, K_{k-1}\} \cup \{L_1, \dots, L_{l-1}\} = c.$$

Thus $\mathcal{M} \models C \cup \{c\}$. □

Theorem 151. Let C be a set of clauses closed under resolution. Then C is inconsistent iff $\emptyset \in C$. Note that the empty clause $\{\} \leftrightarrow \perp$.

Proof. If $\emptyset \in C$ then C is clearly inconsistent.

Conversely assume that C is inconsistent. By the compactness theorem there is a finite set of atomic formulas $\{\varphi_0, \dots, \varphi_{n-1}\}$ such that

$$C' = \{c \in C \mid \text{for every literal } L \text{ in } c \text{ there exists } i < n \text{ such that } L = \varphi_i \text{ or } L = \neg\varphi_i\},$$

the restriction of C to $\{\varphi_0, \dots, \varphi_{n-1}\}$ is inconsistent. Assume that the number n of atomic formulas with that property is chosen minimally.

Case 1. $n = 0$. Since the empty set of clauses is consistent, $C' \neq \emptyset$. On the other hand the only clause built from no atomic formulas is the clause $\{\} = \emptyset$. Thus $\emptyset \in C' \subseteq C$.

Case 2. $n = m + 1 > 0$. Assume for a contradiction that $\emptyset \notin C$. Let

$$C^+ = \{c \in C' \mid \neg\varphi_0 \notin c\}, C^- = \{c \in C' \mid \varphi_0 \notin c\}$$

and

$$C_0^+ = \{c \setminus \{\varphi_0\} \mid c \in C^+\}, C_0^- = \{c \setminus \{\neg\varphi_0\} \mid c \in C^-\}.$$

(1) C_0^+ and C_0^- are closed under resolution.

Proof. Let d'' be a resolution of d , $d' \in C_0^+$. Let $d = c \setminus \{\varphi_0\}$ and $d' = c' \setminus \{\varphi_0\}$ with $c, c' \in C^+$. The resolution d'' was based on some atomic formula $\varphi_i \neq \varphi_0$. Then we can also resolve c, c' by the same atomic formula φ_i . Let c'' be that resolution of c, c' . Since C is closed under resolution, $c'' \in C$, $c'' \in C^+$, and $d'' = c'' \setminus \{\varphi_0\} \in C_0^+$. *qed*(1)

(2) $\emptyset \notin C_0^+$ or $\emptyset \notin C_0^-$.

Proof. If $\emptyset \in C_0^+$ and $\emptyset \in C_0^-$, and since $\emptyset \notin C$ we have $\{\varphi_0\} \in C^+$ and $\{\neg\varphi_0\} \in C^-$. But then the resolution \emptyset of $\{\varphi_0\}$ and $\{\neg\varphi_0\}$ would be in C , contradiction. *qed*(2)

Case 1. $\emptyset \notin C_0^+$. By the minimality of n and by (1), C_0^+ is consistent. Let $\mathcal{M} \models C_0^+$. Let the atomic formula φ_0 be of the form $rt_0 \dots t_{s-1}$ where r is an n -ary relation symbol and $t_0, \dots, t_{s-1} \in T^S$. Since the formula $rt_0 \dots t_{s-1}$ does not occur within C_0^+ , we can modify the model \mathcal{M} to a model \mathcal{M}' by only modifying the interpretation $\mathcal{M}(r)$ exactly at $(\mathcal{M}(t_0), \dots, \mathcal{M}(t_{s-1}))$. So let $\mathcal{M}'(\mathcal{M}(t_0), \dots, \mathcal{M}(t_{s-1}))$ be *false*. Then $\mathcal{M}' \models \neg\varphi_0$. We show that $\mathcal{M}' \models C'$.

Let $c \in C'$. If $\neg\varphi_0 \in c$ then $\mathcal{M}' \models c$. So assume that $\neg\varphi_0 \notin c$. Then $c \in C^+$ and $c \setminus \{\varphi_0\} \in C_0^+$. Then $\mathcal{M} \models c \setminus \{\varphi_0\}$, $\mathcal{M}' \models c \setminus \{\varphi_0\}$, and $\mathcal{M}' \models c$. But then C' is consistent, contradiction.

Case 2. $\emptyset \notin C_0^-$. We can then proceed analogously to case 1, arranging that $\mathcal{M}'(\mathcal{M}(t_0), \dots, \mathcal{M}(t_{s-1}))$ be *true*. So we get a contradiction again. \square

This means that the inconsistency check in the automatic proving algorithm can be carried out even more systematically: produce all relevant resolution instances until the empty clause is generated. Again we have correctness and completeness for the algorithm with resolution.

Example 152. Already with a view towards logical applications of **Prolog** let us consider a theory about the recursive definition of formulas. Let

$$\begin{aligned} & \text{fm}(\text{psi}) \\ & \text{fm}(\text{phi}) \\ & \forall X, Y (\text{fm}(X) \wedge \text{fm}(Y) \rightarrow \text{fm}(\text{and}(X, Y))) \end{aligned}$$

be a small axiom system concerning the formation of formulas; here “psi” and “phi” are constant symbols, “and” is a binary function symbol, and “formula” is a unary relation symbol. To show that $\psi \wedge (\psi \wedge \psi)$ is a formula one has to derive

$$\text{fm}(\text{and}(\text{psi}, \text{and}(\text{psi}, \text{psi})))$$

from the axioms. This is equivalent to showing that

$$\begin{aligned} & \text{fm}(\text{psi}) \\ & \text{fm}(\text{phi}) \\ & \forall X, Y (\text{fm}(X) \wedge \text{fm}(Y) \rightarrow \text{fm}(\text{and}(X, Y))) \\ & \neg \text{fm}(\text{and}(\text{psi}, \text{and}(\text{psi}, \text{psi}))) \end{aligned}$$

is inconsistent. We can write the matrix of the conjunction of these formulas in conjunctive normal form as

$$C = \{\{\text{fm}(\text{psi})\}, \{\text{fm}(\text{psi})\}, \{\neg \text{fm}(X), \neg \text{fm}(Y), \text{fm}(\text{and}(X, Y))\}, \{\neg \text{fm}(\text{and}(\text{psi}, \text{and}(\text{psi}, \text{psi})))\}\}.$$

Obviously the universally quantified clause $\{\neg \text{fm}(X), \neg \text{fm}(Y), \text{fm}(\text{and}(X, Y))\}$ implies all its instantiations by constant terms. So we close the set C under such instantiations and under resolution. Deriving the empty clause $\{\}$ shows the desired inconsistency. We write the sequence of derived clauses in the format of a formal proof:

1	$\text{fm}(\text{psi})$	assumption
2	$\text{fm}(\text{phi})$	assumption
3	$\neg\text{fm}(X), \neg\text{fm}(Y), \text{fm}(\text{and}(X, Y))$	assumption
4	$\neg\text{fm}(\text{and}(\text{psi}, \text{and}(\text{psi}, \text{psi})))$	assumption
5	$\neg\text{fm}(\text{psi}), \neg\text{fm}(\text{and}(\text{psi}, \text{psi})), \text{fm}(\text{and}(\text{psi}, \text{and}(\text{psi}, \text{psi})))$	instance of 3
6	$\neg\text{fm}(\text{psi}), \neg\text{fm}(\text{and}(\text{psi}, \text{psi}))$	resolution of 4, 5
7	$\neg\text{fm}(\text{and}(\text{psi}, \text{psi}))$	resolution of 1, 6
8	$\neg\text{fm}(\text{psi}), \text{fm}(\text{and}(\text{psi}, \text{psi}))$	instance of 3
9	$\neg\text{fm}(\text{psi})$	resolution of 7, 8
10	$\{\}$	resolution of 1, 9

The choice of instances of the universal clause $\{\neg\text{fm}(X), \neg\text{fm}(Y), \text{fm}(\text{and}(X, Y))\}$ was directed by the desire to resolve certain clauses along the derivation. It is possible to find “fitting” instances by the method of *unification* which will be explained in the next chapter.

Index

PEANO arithmetic	41	contains witnesses	28
PEANO axiom, second order	52	contraposition	22
GÖDEL completeness theorem	33	correct sequent	20
HENKIN model existence theorem	33	countable	6
SKOLEM normal form	61	countable (set)	54
SKOLEM paradoxon	56	countable structure	34
HENKIN set	28	countably infinite	6
ZERMELO-FRAENKEL set theory	46	cut rule	22
+1	50	deduction	20
0	51	dense linear order	40
1	51	denumerable	6
2	51	derivable	20
<	51	derivation	8, 20
\vDash	13	derivation complete	28
ω	52	derived rule	21
\vdash	20	difference class	48
$A^{<\omega}$	54	disjunction	11
AC	55	disjunctive normal form	60
algebraically closed field	39	domain	49
antecedent	20	downward LÖWENHEIM-SKOLEM theorem	33
arithmetic	38	dual (literal)	60
atomic formula	10	elementary	35
axiomatizable	35	Δ -elementary	35
Boolean algebra	12	embedding	12
bounded quantifier	48	empty set	47
calculus	8	empty word	8
cardinality	6, 54	equivalence	11
cartesian product	49	<i>ex falsum libenter</i>	22
ω -categorical	41	existential formula	61
characteristic of a field	38	expansion	12
choice, axiom of	55	extended group	37
class term	47	extensionality	46, 48
compactness theorem	21, 33	field	38
complete set of sentences	40	finite (nonstandard analysis)	43
completeness	21	finite sequence	5
Con(ZF)	59	finite (set)	54
concatenation	5	finite structure	34
conjunction	11	finitely axiomatizable	35
conjunctive normal form	60	finiteness theorem	21, 33
consistent	26	first-order language	10
constant symbol	7	fix point theorem	57
constant term	62	formal proof	20

formula	10
\in -formula	46
foundation schema	47, 49
free variable	14
free(φ)	14
function	5, 49
function symbol	7
group	36
holds in a structure	13
homomorphism	12
image	49
implication	15
inconsistent	26
induction (for ordinals)	51
induction on a calculus	9
inductive	6, 51
infinite (nonstandard analysis)	43
infinite (set)	54
infinite structure	34
infinitesimal	43
infinitesimally near	43
infinity, axiom of	46, 49
infix operator	10
interpretation	13, 13
intersection	48, 48
inverse	49
language	7
language of arithmetic	38
language of group theory	7
language of group theory (extended)	7
language of set theory	46
length	5
linear	6
literal	59
logical implication	15
matrix (of a formula)	60
maximal element	6
model	13
model class	15
model of	15
model theory	15
natural numbers	52
nonstandard analysis	42
Ord	50
ordered field	11
ordered pair	5
ordinal (number)	50
pair, ordered	49
pair (unordered)	48
pairing axiom	46, 49
partial order	6
polish notation	10
postfix operator	10
power class	48
powerset axiom	46, 49
prefix (of a formula)	60
prefix operator	10
preimage	49
prenex normal form	60
product	8
product rule	45
propositional constant symbol	7
range	49
recursion equation	9
recursion (for ordinals)	53
recursion on a calculus	9
recursion rule	9, 53
reduct	12
reflexive	6
relation	5
relation, binary	49
relation symbol	7
replacement schema	46, 49
resolution	63
restriction	49
rule	8
RUSSELL's antinomy	47
GÖDEL's first incompleteness theorem	58
ZORN's lemma	7
GÖDEL's second incompleteness theorem	59
HENKIN's theorem	29
CANTOR's theorem	54
HERBRAND's theorem	62
satisfiable	13
satisfies	13
semantics	11
sentence	14
separation schema	46, 48
sequent	20
sequent rules	20
singleton set	48
standard part	43
strict linear order	39
strict order	39
structure	11
subclass	48
substitution	16, 16
substitution theorem	17
substructure	12
succedent	20
symbol set	7
term	10
term model	27
term (set theory)	48
$\text{Th}(\mathfrak{A})$	41
theory	40
S -theory	40
theory of a structure	41
torsion group	37
transfer	44
transitive	6, 50
true in	15
truth, definition of	57
truth, undefinability of	57
truth values	12
type	7
uncountable	6
uncountable (set)	54
uncountable structure	34
underlying set	11
union	48, 48
union axiom	46, 49
unique readability	9
universal formula	61
universally valid	13
universe	47
upper bound	6
upward LÖWENHEIM-SKOLEM theorem	35
$\text{var}(t)$	14
variable	7
word	7
ZF	46

ZFC 56