Einführung in die Mathematische Logik

by Peter Koepke

Bonn, Sommersemester 2015

Vorläufiges Skript zur Vorlesung

Wann sollte die Mathematik je zu einem Anfang gelangen, wenn sie warten wollte, bis die Philosophie über unsere Grundbegriffe zur Klarheit und Einmüthigkeit gekommen ist? Unsere einzige Rettung ist der formalistische Standpunkt, undefinirte Begriffe (wie Zahl, Punkt, Ding, Menge) an die Spitze zu stellen, um deren actuelle oder psychologische oder anschauliche Bedeutung wir uns nicht kümmern, und ebenso unbewiesene Sätze (Axiome), deren actuelle Richtigkeit uns nichts angeht. Aus diesen primitiven Begriffen und Urtheilen gewinnen wir durch Definition und Deduction andere, und nur diese Ableitung ist unser Werk und Ziel.
Felix Hausdorff, 12. Januar 1918

Table of contents

1 Deutsche Einleitung

Durch Einführung von logischen Verknüpfungen (“und”, “oder”, “nicht”) und Quantoren (“für alle”, “es existiert”) - oder entsprechenden Symbolen $\wedge, \vee, \neg, \forall, \exists$ - lassen sich alle mathematischen Aussagen in eine streng *formale* Form bringen. Z.B. werden in der Analysis Eigenschaften von Funktionen oft in Quantorenschreibweise definiert: $\forall\varepsilon\,\exists\delta\ldots$. Mathematische Beweise können als Folgen von Aussagen aufgefasst werden, die sich durch logische Schlüsse aus Grundannahmen ergeben. Dabei haben wichtige Schlussweisen einen rein *formalen*, kalkülartigen Charakter als schematische Umformungen von Symbolfolgen.

In dem Modul wird die formallogische Begründung der Mathematik anhand von Formulierungen von Aussagen, Theorien und Beweisen, die aus dem ersten Studienjahr bekannt sind, vorgestellt. Es wird ein vollständiger Beweiskalkül für die Prädikatenlogik (erster Stufe) angegeben, der dem üblichen mathematischen Schließen nahe steht. Durch die Formalisierung werden Aussagen und Beweise selbst zu mathematischen Objekten. Zentrales Ergebnis ist der Gödelsche Vollständigkeitssatz, der die formale Methode bestätigt: *jede* allgemeingültige mathematische Aussage kann im Beweiskalkül abgeleitet werden.

Die *Mengenlehre* ist die allgemein akzeptierte Grundlage der Mathematik. Die Zermelo-Fraenkelschen Axiome der Mengenlehre lassen sich in der Logik erster Stufe formulieren. Wir werden sehen, wie sich die üblichen Grundbegriffe der Mathematik wie Zahlen, Relationen, Funktionen usw. in diesem Axiomensystem entwickeln lassen.

Aus Sicht des reinen Formalismus wird die Frage “Was ist Mathematik?” daher beantwortet als:

$$\text{Mathematik} = \text{Prädikatenlogik} + \text{Zermelo-Fraenkelsche Axiome}.$$

Diese Sicht ist Grundlagen-theoretisch außerordentlich wichtig, aber sie abstrahiert von vielen Aspekten der tatsächlichen Mathematik wie der Anschaulichkeit mathematischer Objekte, den intellektuellen Herausforderungen mathematischer Probleme, der Anwendbarkeit der Mathematik in Wissenschaft und Technik, ihrer Ästhetik usw. Auch die formale Mathematik benötigt Kriterien für die Auswahl von interessanten Aussagen und Beweisen, die nicht im Formalismus selbst begründet sind.

In der Vorlesung und den Übungen wird besonderer Wert auf die Arbeit mit konkreten Formalisierungen gelegt. Die Vorlesung setzt Grundkenntnisse aus dem 1. Studienjahr Mathematik voraus.

Die Vorlesung ist ein in sich abgeschlossenes Modul und nicht Bestandteil des turnusmäßigen Logik-Mengenlehre-Zyklus. Sie wird evtl. im Wintersemester mit einem Seminar fortgesetzt.

Vorlesungsinhalte:

- Quantorensprachen
- Strukturen
- Interpretation von Termen und Formeln in Strukturen
- Formale Sprachen und Kalküle
- Beweiskalküle
- Konsistenz und Erfüllbarkeit von Theorien
- Der Gödelsche Vollständigkeitssatz

- Mengentheoretische Axiome
- Mengentheoretische Grundlegung der Mathematik
- Ordinalzahlen
- Zahlbereiche
- Kardinalzahlen
- Auswahlaxiom und Zornsches Lemma

2 The language of mathematics

Mathematical logic studies the language of mathematics with mathematical methods. So we first have to get some ideas about that language. We then begin to normalize or regulate the language, to consist of finite sequences of symbols which are built according to some simple rules. This will allow to apply mathematics to the language.

We shall use the language of *first-order predicate calculus* which resembles the quantifier notations known from calculus: f is continuous iff

$$\forall x \forall \varepsilon > 0 \exists \delta > 0 \forall x' (|x - x'| < \delta \rightarrow |f(x) - f(x')| < \varepsilon).$$

We shall demonstrate the move from informal mathematical statements to formal statements with examples from linear algebra.

2.1 Examples: vector spaces

Consider the definitions of a *vector space* in three standard textbooks.

Albrecht Beutelspacher: *Lineare Algebra - Eine Einführung in die Wissenschaft der Vektoren, Abbildungen und Matrizen*

> **3.1. Die Definition**
> Jedem Vektorraum liegt ein Körper K zugrunde. Welcher spezielle Körper das ist, wird meistens keine Rolle spielen; deshalb nennen wir den Körper neutral K. Wir werden die Elemente von K of auch **Skalare** nennen.
>
> Die Hauptsache eines Vektorraums sind aber seine Elemente, die Vektoren. Ein **Vektorraum** über dem Körper K (auch K-**Vektorraum** genannt) besteht aus einer Menge V von Elementen, die wir **Vektoren** nennen, die den folgenden Gesetzen genügt:
>
> **1. Verknüpfung von Vektoren:** Es gibt eine Verknüpfung $+$ auf V, die je zwei Vektoren v und w einen Vektor $v+w$ zuordnet, so dass für alle $u, v, w \in V$ die folgenden Eigenschaften erfüllt sind:
> *Assoziativität:*
> $$u + (v + w) = (u + v) + w$$
> *Existenz des Nullvektors:* Es gibt einen Vektor, den wir mit o bezeichnen, mit folgender Eigenschaft
> $$v + o = v.$$
> *Existenz negativer Vektoren:* Zu jedem Vektor v gibt es einen Vektor, den wir $-v$ nennen, mit
> $$v + (-v) = o.$$
> *Kommutativität:*
> $$u + v = v + u.$$

2. Verknüpfung von Skalaren und Vektoren: Für jeden Vektor $v \in V$ und jeden Skalar $k \in K$ ist ein Vektor $k \cdot v$ definiert (das Objekt $k \cdot v$ (für das wir auch kurz $k\,v$ schreiben) soll also ein Element von V sein). Diese Bildung des skalaren Vielfachen ist so, dass für alle $h, k \in K$ und für alle Vektoren $v, w \in V$ die folgenden Eigenschaften gelten:

$$\begin{aligned} (k+h)\,v &= k\,v + h\,v, \\ (k \cdot h) \cdot v &= k \cdot (h \cdot v), \\ 1 \cdot v &= v, \\ k \cdot (v+w) &= k \cdot v + k \cdot w. \end{aligned}$$

Egbert Brieskorn: *Lineare Algebra und analytische Geometrie*

Ein Vektorraum über einem Körper K ist eine Menge V zusammen mit zwei Operationen

$$\begin{array}{ll} V \times V \longrightarrow V & K \times V \longrightarrow V \\ (v,w) \longmapsto v+w & (a,v) \longmapsto a \cdot v \end{array}$$

für welche die folgenden Bedingungen erfüllt sind:

(A1) $\forall u, v, w \in V\ (u+v)+w = u+(v+w)$
(A2) $\exists 0 \in V\, \forall v \in V\, 0+v = v+0 = v$
(A3) $\forall v \in V\, \exists -v \in V\, -v+v = v+(-v) = 0$
(A4) $\forall v, w \in V\, v+w = w+v$
(V1) $\forall a, b \in K\, \forall v \in V\ (a\,b) \cdot v = a \cdot (b \cdot v)$
(V2) $\forall v \in V\, 1 \cdot v = v$
(V3) $\forall a, b \in K\, \forall v \in V\ (a+b) \cdot v = a \cdot v + b \cdot v$
(V4) $\forall a \in K\, \forall v, w \in V\, a \cdot (v+w) = a \cdot v + a \cdot w$

Serge Lang: *Linear Algebra*

A **vector space** V **over the field** K is a set of objects which can be added and multiplied by elements of K, in such a way that the sum of two elements of V is again an element of V, the product of an element of V by an element of K is an element of V, and the following properties are satisfied:

S1. *Given elements u, v, w of V, we have*

$$(u+v)+w = u+(v+w).$$

S2. *There is an element of V, denoted by 0, such that*

$$0+u = u+0 = u$$

for all elements u of V.

S3. *Given an element u of V, there exists an element $-u$ in V such that*

$$u+(-u) = 0.$$

S4. *For all elements u, v of V, we have*

$$u+v = v+u.$$

S5. *If c is a number, then $c\,(u+v) = c\,u + c\,v$.*

S6. *If a, b are two numbers, then $(a+b)\,v = a\,v + b\,v$.*

S7. *If a, b are two numbers, then $(a\,b)\,v = a\,(b\,v)$.*

S8. *For all elements u of V, we have $1 \cdot v = u$ (1 here is the number one).*

Notes about (these) mathematical texts:

1. Mathematical texts combine "exact" natural language and symbolic formulas in a particular style.
2. Like with ordinary natural language there may be many variants of texts which basically have the same mathematical content. Texts differ by individual "styles".
3. Superficially and in the general perception mathematical texts are perfectly exact and complete. This is, however, not true.
4. Texts leave out a lot of implicit assumptions: which addition $+$ and multiplication $\cdot$ is used where? Addition in the field, or between vectors? Do all vector spaces share the same $+$ and $\cdot$? Do all vector spaces have the same null vector 0?
5. Notions are incompletely specified: What is a vector space really: a *set* with operations?
6. Texts build on assumptions from other or earlier sources or some general expert knowledge: what is a field?
7. Considering vector spaces one uses notions and propositions from other domains like sets, operators, ...
8. A strictly formal system like a computer (program) would not be able to handle our vague definitions of vector spaces. We would obtain dozens of error messages.

To get an idea how a fully complete and exact version of the definition of vector space could look like, let us consider snippets from the MIZAR system for mathematics (`www.mizar.org`). `Mizar` is a system for writing and proof checking fully formalized mathematics ("formal mathematics"); it contains vast amounts of basic mathematical material.

```
::
::                      8. VECTOR SPACE STRUCTURE
::

definition let F be 1-sorted;
struct(LoopStr) VectSpStr over F (#
                   carrier -> set,
                    add -> BinOp of the carrier,
                    Zero -> Element of the carrier,
                   lmult -> Function of [:the carrier of F,the carrier:],
                                        the carrier #)
;

definition let F be add-associative right_zeroed right_complementable
Abelian associative left_unital distributive (non empty doubleLoopStr
);
mode VectSp of F is VectSp-like
add-associative right_zeroed right_complementable Abelian
(non empty VectSpStr over F);
end;

definition let F be non empty doubleLoopStr;
 let IT be non empty VectSpStr over F;
 attr IT is VectSp-like means
```

```
:: VECTSP_1:def 26
 for x,y being Element of F
         for v,w being Element of IT holds
               x*(v+w) = x*v+x*w &
               (x+y)*v = x*v+y*v &
               (x*y)*v = x*(y*v) &
               (1_F)*v = v;
end;
```

Notes on formal mathematics in MIZAR:

1. Notions have to be specified in detail; the zero of F is to be distinguished from the zero vector: (0_F)
2. *Types* of notions have to be specified. Like in a computer program the type of the scalar multiplication has to be introduced as
   `lmult -> Function of [:the carrier of F,the carrier:], the carrier #`
3. Most formal mathematics systems use idiosyncrasies like in programming languages: ASCII letters instead of common mathematical symbols; line endings with „ ; “; ...
4. There are many formal mathematics system, differing in their aims and in the language accepted.

3 Tranforming natural mathematical language into formalized language

We saw that the mathematical language used in textbook, lectures, and exams is *informal*. This informality is akin to the general informality of natural language. Natural language is usually incomplete and often inconsistent. But it allows to express facts and arguments briefly, geared towards human understanding. Natural language transports important natural intuitions. The common mathematical language is the main tool for mathematical thought, writing, and communication. Like in other fields, there are (informal) criteria when a text is accepted as sufficiently complete, exact, or even beautiful. These criteria are the result of mathematical history, culture, and education. As a mathematician you are required to acquire them and to adhere to them.

For the mathematical analysis of mathematical language, however, we shall move from informal mathematical language to formal language. Before we strictly define the formal language we shall demonstrate some normalizations and formalizations with the example of the definition of vector spaces.

3.1 Structures

In all the definitions above, F-vector spaces V are sets V with “extra operations“. This is captured by the notion of a *structure* $(V, ...)$ where V is the (non-empty) *underlying set*, and the extra components of the structure are explicitly listed. So an F-vector space is a structure $(V, +^V, \cdot^V, 0^V)$ where

- $+^V$ is the addition of vectors from V: $+^V : V \times V \to V$;
- $\cdot^V$ is the scalar multiplication: $\cdot^V : F \times V \to V$;
- 0^V is the zero-vector: $0^V \in V$.

Of course the field F has to be treated similarly: a field F is a structure of the form $(F, +^F, \cdot^F, 0^F, 1^F)$ where

- $+^F$ is the field addition: $+^F\colon F \times F \to F$;
- $\cdot^F$ is the field multiplication: $\cdot^F\colon F \times F \to F$;
- 0^F is additive neutral element of the field: $0^F \in F$;
- 1^F is multiplicative neutral element of the field: $1^F \in F$.

Now we can say exactly, which operations and constants are used in the axioms. The axioms of Serge Lang can now be written more exactly:

A structure $(V, +^V, \cdot^V, 0^V)$ is a **vector space** over a field $(F, +^F, \cdot^F, 0^F, 1^F)$, where the following properties are satisfied:

1. Given elements $u, v, w \in V$, we have
$$(u +^V v) +^V w = u +^V (v +^V w).$$
2. For all elements $u \in V$
$$0^V +^V u = u +^V 0^V = u.$$
3. Given an element $u \in V$ there exists an element $-u \in V$ such that
$$u +^V (-u) = 0^V.$$
4. For all elements $u, v \in V$, we have
$$u +^V v = v +^V u.$$
5. For all $c \in F$ and all $u, v \in V$, then
$$c \cdot^V (u +^V v) = c \cdot^V u +^V c \cdot^V v.$$
6. For all $a, b \in F$ and all $v \in V$, then
$$(a +^F b) \cdot^V v = a \cdot^V v +^V b \cdot^V v.$$
7. For all $a, b \in F$ and all $v \in V$, then
$$(a \cdot^F b) \cdot^V v = a \cdot^V (b \cdot^V v).$$
8. For all $u \in V$, we have
$$1 \cdot^V u = u.$$

This notation still has some problems:

1. To denote the order of operations, one uses brackets, but then some brackets are omitted according to the convention that multiplications of some kind have priority over addition of some kind. This has to be strictly regulated in a formal language.
2. The status of the $-u$ is unclear: is $-$ another operation, or is $-u$ just a variable like v or v'?
3. There are natural language variants which do not seem essential for the definition: sometimes "then" is used, and sometimes "we have".

3.2 Quantifiers

A lot of mathematics is of the "for all ... there exists ..." kind. The phrases "for all" and "there exists" are quantifying phrases. Language variants like "Given an ..." instead of "for all" are also common. These are often denoted by *quantifiers* $\forall$ and $\exists$ as in the Brieskorn.

Then the vector axioms become:

1. $\forall u, v, w \in V (u +^V v) +^V w = u +^V (v +^V w)$
2. $\forall u \in V\, 0^V +^V u = u +^V 0^V = u$
3. $\forall u \in V\, \exists v \in V u +^V v = 0^V$
4. $\forall u, v \in V u +^V v = v +^V u$
5. $\forall c \in F \forall u, v \in V c \cdot^V (u +^V v) = c \cdot^V u +^V c \cdot^V v$
6. $\forall a, b \in F \forall v \in V\, (a +^F b) \cdot^V v = a \cdot^V v +^V b \cdot^V v$
7. $\forall a, b \in F \forall v \in V (a \cdot^F b) \cdot^V v = a \cdot^V (b \cdot^V v)$
8. $\forall u \in V\, 1 \cdot^V u = u$

These axioms still involve set theory in the form of the $\in$-relation. For various reasons this should be pushed into the background. There are two "sorts" of quantiers, namely the $\in V$-quantifiers and the $\in F$-quantifiers. These appear less set-theoretical when we write $\forall^V u$ instead of $\forall u \in V$:

1. $\forall^V u, v, w (u +^V v) +^V w = u +^V (v +^V w)$
2. $\forall^V u . 0^V +^V u = u +^V 0^V = u$
3. $\forall^V u \exists^V v . u +^V v = 0^V$
4. $\forall^V u, v . u +^V v = v +^V u$
5. $\forall^F c \forall^V u, v . c \cdot^V (u +^V v) = c \cdot^V u +^V c \cdot^V v$
6. $\forall^F a, b \forall^V v\, (a +^F b) \cdot^V v = a \cdot^V v +^V b \cdot^V v$
7. $\forall^F a, b \forall^V v (a \cdot^F b) \cdot^V v = a \cdot^V (b \cdot^V v)$
8. $\forall^V u . 1 \cdot^V u = u$

3.3 Sorts

So far these axioms make use of two *sorts* of objects. An F-vector space V can be viewed as a two-sorted structure

$$(V, F, ...).$$

Our later logical analysis, however, will be easier if we can restrict to situations with *one* sort. This is also possible with vector spaces Vover the field F, when we take $V \cup F$ as a new underlying set. Such a vector space is a structure of the form

$$(V \cup F, R_V, R_F, +^V, \cdot^V, 0^V, +^F, \cdot^F, 0^F, 1^F)$$

where R_V and R_F are relations in one argument, that determine the subsets V and F of the underlying set $V \cup F$:

$$R_V(u) \text{ is true iff } u \in V, \quad R_F(u) \text{ is true iff } u \in F$$

the vector axioms now read:

1. $\forall u, v, w ((R_V(u) \wedge R_V(v) \wedge R_V(w)) \rightarrow (u +^V v) +^V w = u +^V (v +^V w))$
2. $\forall u\, (R_V(u) \rightarrow 0^V +^V u = u +^V 0^V = u)$
3. $\forall u (R_V(u) \rightarrow \exists v (\, R_V(v) \wedge u +^V v = 0^V))$
4. $\forall u, v\, ((R_V(u) \wedge R_V(v)) \rightarrow u +^V v = v +^V u)$

5. $\forall c(\, R_F(c) \to \forall u, v((R_V(u) \wedge R_V(v)) \to c \cdot^V (u +^V v) = c \cdot^V u +^V c \cdot^V v))$
6. $\forall a, b(\, (R_F(a) \wedge R_F(b)) \to \forall v(\, R_V(v) \to (a +^F b) \cdot^V v = a \cdot^V v +^V b \cdot^V v))$
7. $\forall a, b(\, (R_F(a) \wedge R_F(b)) \to \forall v(\, R_V(v) \to (a \cdot^F b) \cdot^V v = a \cdot^V (b \cdot^V v)))$
8. $\forall u(\, R_V(u) \to 1 \cdot^V u = u)$

Here we have also used the logical operators $\to$ (implies) and $\wedge$ (and), replacing $\forall^V u...$ by $\forall u(R_V(u) \to ...)$ and $\exists^V u...$ by $\exists u(R_V(u) \wedge ...)$.

3.4 Conclusion

After this example it appears conceivable to build an adequate mathematical language on the basis of symbols for

- variables, like $a, b, u, v, ...$
- relations, like $R_V, ...$
- operations, like $+^F, +^V, ...$
- constants, like $0^F, 1^F, 0^V, ...$
- propositional connectives, like $\wedge, \to$
- quantifiers, like $\forall, \exists$

Exercise 1. Consider the structure $(\mathbb{R}, +, \cdot, 0, 1, <, f, g)$ where f and g are functions from $\mathbb{R}$ to $\mathbb{R}$. Carry out formalizations similar to the above example for the following properties of f and g:

a) f is everywhere positive;

b) f is strictly monotoneously growing;

c) f is continuous;

d) f is *uniformly* continuous;

e) z is differentiable at x;

f) z is the derivative of f at x;

g) g is the derivative of f.

Exercise 2. Consider a two-sorted structure $(\mathcal{F}, \mathbb{R}, +, \cdot, 0, 1, <)$ where $\mathcal{F}$ is some collection of functions from $\mathbb{R}$ to $\mathbb{R}$. Formalize:

a) every function is continuous;

b) the sum of two continuous functions is continuous;

c) every positive function is the square of some positive function.

4 The Syntax of first-order logic: Symbols, terms, and formulas

The art of free society consists first in the maintenance of the symbolic code.
A. N. Whitehead

Formal mathematical statements will be finite sequences of symbols, like ordinary sentences are sequences of alphabetic letters. These sequences can be studied mathematically. We shall treat the sequences as mathematical objects, similar to numbers or vectors. This study will be carried out in the usual, *informal* mathematical language:

We shall use the common, informal *mathematical language to express properties of a* formal *mathematical language.*

This is not a contradiction in itself, but the natural state of affairs in foundational studies. Language is analysed within language. Physical experiments are carried out with apparatus build from physical material, following physical laws itself.

The study of the formal properties of symbols, words, sentence,... is called *syntax*. Syntax will later be related to the "meaning" of symbolic material, its *semantics*. The interplay between syntax and semantics is at the core of logic. A strong logic is able to present interesting semantic properties, i.e., properties of interesting mathematical structure, already in its syntax.

We build the formal language from atomic building blocks.

4.1 Symbols

A symbol has some basic information about its role within larger contexts like words and sentences. E.g., the symbol $\leqslant$ is usually used to stand for a *binary relation*. So we let symbols include information on its function, like "relation", together with further details, like "binary". We provide us with a sufficient collection of symbols.

Definition 1. *The* basic symbols *of first-order logic are*

a) $\equiv$ *for* equality,

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

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

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

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

Let $\mathrm{Var} = \{v_n | n \in \mathbb{N}\}$ *be the set of variables and let* S_0 *be the set of basic symbols.*

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

An n*-ary* function symbol*, for* $n \in \mathbb{N}$*, is (a set) of the form* $f = (x, 1, n)$ *where* 1 *indicates that the values of a function will be elements of a structure.*

0*-ary function symbols are also called* constant symbols*.*

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

We assume that the basic symbols are pairwise distinct and are distinct from any relation or function symbol. For concreteness one could for example set $\equiv = 0$*,* $\neg = 1$*,* $\to = 2$*,* $\bot = 3$*,* $(= 4$*,* $) = 5$*, 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 in some structure. 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 $x, y, z, \ldots$, relation symbols by $P, Q, R, \ldots$, functions symbols by $f, g, h, \ldots$ and constant symbols by $c, c_0, c_1, \ldots$ We shall also use other typographical symbols in line with standard mathematical practice. A symbol like $<$, e.g., usually denotes a binary relation, and we could assume for definiteness that there is some fixed set theoretic formalization of $<$ like $<=(999, 0, 2)$. Instead of the arbitrary 999 one could also take the number of $<$ in some typographical font as they are provided by mathematical typesetting systems.

Example 2. The *language of group theory* is the language

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

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

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

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

4.2 Words

Words:
A letter and a letter on a string
Will hold forever humanity spell-bound
The Real Group

Definition 3. *Let S be a language. A* word *over S is a finite sequence*

$$w\colon \{0,1,\ldots,n-1\} \to S_0 \cup S.$$

The number n is called the length *of w:* $\mathrm{length}(w) = n$. *The empty set $\emptyset$ is also called the* empty word. *Let S^* be the set of all words over S. A word $w\colon \{0,1,\ldots,n-1\} \to S_0 \cup S$ is usually written as a string of letters: $w(0)\,w(1)\ldots w(n-1)$.*

It is convenient to identify the natural number n with its set of predecessors:

$$n = \{0,1,\ldots,n-1\}.$$

This will be justified later in our treatment of set theory. Then

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

Definition 4. *If w and w' are words over the language S then their* concatenation $w^\frown w'$: $\mathrm{length}(w) + \mathrm{length}(w') \to S_0 \cup S$ *is defined by*

$$w^\frown w'(i) = \begin{cases} w(i), & \text{if } i < \mathrm{length}(w) \\ w'(i - \mathrm{length}(w)), & \text{else} \end{cases}$$

We also write ww' instead of $w^\frown w'$.

Exercise 3. The operation of concatenation satisfies some canonical laws:

a) $^\frown$ is associative: $(ww')w'' = w(w'w'')$.

b) $\emptyset$ is a neutral element for $^\frown$: $\emptyset w = w\emptyset = w$.

c) $^\frown$ has cancelation: if $uw = u'w$ then $u = u'$; if $wu = wu'$ then $u = u'$.

4.3 Terms

Fix a symbol set S for the remainder of this section.

Definition 5. *The set T^S of all S-*terms *is the smallest subset of S^* such that*

a) $x \in T^S$ for all variables x;

b) $ft_0...t_{n-1} \in T^S$ *for all* n*-ary function symbols* $f \in S$ *and all* $t_0, ..., t_{n-1} \in T^S$.

These terms are written in *Polish* notation, meaning that function symbols come first and that no brackets are needed. Indeed, terms in T^S have *unique readings* according to the following

Lemma 6. *For every term* $t \in T^S$ *exactly one of the following holds:*

a) t *is a variable;*

b) there is a uniquely defined function symbol $f \in S$ *and a uniquely defined sequence* $t_0, ..., t_{n-1} \in T^S$ *of terms, where* f *is* n*-ary, such that* $t = ft_0...t_{n-1}$.

Proof. Exercise. □

Remark 7. Unique readability is essential for working with terms. Therefore if this Lemma would not hold one would have to alter the definition of terms.

Example 8. For the language $S_{\mathrm{Gr}} = \{\circ, e\}$ of group theory, terms in $T^{S_{\mathrm{Gr}}}$ look like

$$e, v_0, v_1, ..., \circ ee, \circ e v_m\,, \circ v_m e\,, \circ ee\,, \circ e \circ ee\,, ..., \circ v_i \circ v_j v_k\,, \circ\circ v_i\, v_j v_k\,, ...$$

In standard notation we would have $\circ v_i \circ v_j v_k = (v_i \circ (v_j \circ v_k))$ and $\circ\circ v_i\, v_j v_k = ((v_i \circ v_j) \circ v_k)$. Later, if the operation $\circ$ should be seen to be associative, one might "leave out" brackets.

Exercise 4. Show that every term $t \in T^{S_{\mathrm{Gr}}}$ has odd length $2n+1$ where n is the number of $\circ$-symbols in t.

4.4 Formulas

Definition 9. *The set* L^S *of all* S-formulas *is the smallest subset of* S^* *such that*

a) $\bot \in L^S$ *(the false formula);*

b) $t_0 \equiv t_1 \in L^S$ *for all* S*-terms* $t_0, t_1 \in T^S$ *(equalities);*

c) $Rt_0...t_{n-1} \in L^S$ *for all* n*-ary relation symbols* $R \in S$ *and all* S*-terms* $t_0, ..., t_{n-1} \in T^S$ *(relational formulas);*

d) $\neg\varphi \in L^S$ *for all* $\varphi \in L^S$ *(negations);*

e) $(\varphi \to \psi) \in L^S$ *for all* $\varphi, \psi \in L^S$ *(implications);*

f) $\forall x \varphi \in L^S$ *for all* $\varphi \in L^S$ *and all variables* x *(universalisations).*

L^S *is also called the* first-order language *for the symbol set* S*. Formulas produced by conditions a) - c) only are called* atomic formulas *since they constitute the initial steps of the formula calculus.*

We restrict L^S to just the logical connectives $\neg$ and $\to$, and the quantifier $\forall$. We will later also use other connectives and quantifiers in convenient abbreviations for formulas in L^S. For theoretical considerations it is however advantageous to work with a "small" language.

Definition 10. *For* S*-formulas* φ *and* ψ *and a variable* x *write*

– $\top$ *("true") instead of* $\neg\bot$ *;*

- $(\varphi \vee \psi)$ *("φ or ψ") instead of* $(\neg\varphi \to \psi)$ *is the* disjunction *of* φ, ψ *;*
- $(\varphi \wedge \psi)$ *("φ and ψ") instead of* $\neg(\varphi \to \neg\psi)$ *is the* conjunction *of* φ, ψ *;*
- $(\varphi \leftrightarrow \psi)$ *("φ iff ψ") instead of* $((\varphi \to \psi) \wedge (\psi \to \varphi))$ *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 $(\varphi \vee \psi)$.

Exercise 5. Formulate and prove the unique readability of formulas in L^S.

Exercise 6. Formulate the standard axioms of group theory in $L^{S_{\mathrm{Gr}}}$.

5 Semantics

We shall *interpret* formulas like $\forall y \exists x\, y = g(f(x))$ in adequate *structures*. The interaction between language and structures is usually called *semantics*. Technically it will consist in mapping all syntactic material to semantic material centered around structures. We shall obtain a schema like:

$\forall$	structure $\mathfrak{A}$
variable	element of A
function symbol	function on A
relation symbol	relation on A
term	element of A
formula	truth value
...	...

Fix a symbol set S.

Definition 11. *An* S-structure *is a function* $\mathfrak{A}\colon \{\forall\} \cup S \to V$ *such that*

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

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

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

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

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

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

A 0-ary function symbol c is also called a constant symbol, and it is interpreted by a 0-ary function $\mathfrak{A}(c)\colon A^0 = \{0\} \to A$ which is defined for the single argument 0 and takes a single value $\mathfrak{A}(c)(0)$ in A. It is natural to identify the function $\mathfrak{A}(c)$ with the constant value $\mathfrak{A}(c)(0)$: $\mathfrak{A}(c) \in A$.

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

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

This "overloading" of notation is quite common in mathematics (and in natural language, "*pars pro toto*"). Usually a human reader is readily able to detect and "disambiguate" ambiguities introduced by multiple usage. There are also techniques in computer science to deal with overloading, e.g., by *typing* of notions. Another common overloading is given by a naive identification of syntax and semantics, i.e., by writing

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

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

Example 12. Formalize the *ordered field of reals* $\mathbb{R}$ as follows. Define the language of ordered fields

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

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

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

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

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

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

Example 13. Define the language of *Boolean algebras* by

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

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

Exercise 7. Show that every *truth-function* $F\colon B^n \to B$ can be obtained as a composition of the functions *and* and *not*.

The notion of structure leads to derived definitions.

Definition 14. *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 $\mathfrak{A}' \restriction (\{\forall\} \cup S) = \mathfrak{A}$.*

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

Definition 15. *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 $f^{\mathfrak{A}} = f^{\mathfrak{B}} \restriction A^n$.

Definition 16. *Let $\mathfrak{A}, \mathfrak{B}$ be S-structures and $h\colon |\mathfrak{A}| \to |\mathfrak{B}|$. Then h is a* homomorphism *from $\mathfrak{A}$ into $\mathfrak{B}$, $h\colon \mathfrak{A} \to \mathfrak{B}$, 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 $\mathfrak{B}$, $h\colon \mathfrak{A} \hookrightarrow \mathfrak{B}$, 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 (occuring) variables.

Definition 17. *Let S be a symbol set. An S-*model *is a function*

$$\mathfrak{M}\colon \{\forall\} \cup S \cup \mathrm{Var} \to V$$

such that $\mathfrak{M} \restriction \{\forall\} \cup S$ 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 or valuation *of the variable v_n in $\mathfrak{M}$.*

It will 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

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

6 The satisfaction relation

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

Definition 18. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation $\mathfrak{M}(t) \in |\mathfrak{M}|$ *of a term $t \in T^S$ by recursion on the term calculus:*

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

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

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

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

Definition 19. *Let $\mathfrak{M}$ be an S-model. Define the* interpretation $\mathfrak{M}(\varphi) \in \mathbb{B}$ *of a formula $\varphi \in L^S$, where $\mathbb{B} = \{0,1\}$ is the Boolean algebra of truth values, by recursion on the formula calculus:*

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

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

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

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

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

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

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

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

Definition 20. *Let S be a language and $\Phi \subseteq L^S$. Φ is* universally valid *if Φ holds in every S-model. Φ is* satisfiable *if there is an S-model $\mathfrak{M}$ such that $\mathfrak{M} \vDash \Phi$.*

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

Exercise 8. Prove:

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

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

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

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

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

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

Definition 21. *For $t \in T^S$ define* $\mathrm{var}(t) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on the term calculus:*

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

Definition 22. *Für $\varphi \in L^S$ define the set of* free variables $\mathrm{free}(\varphi) \subseteq \{v_n | n \in \mathbb{N}\}$ *by recursion on the formula calculus:*

- $\mathrm{free}(t_0 \equiv t_1) = \mathrm{var}(t_0) \cup \mathrm{var}(t_1)$*;*

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

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

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

Example 23.

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

Definition 24.

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

b) $\varphi \in L^S$ *is an* S-sentence *if* $\text{free}(\varphi) = \emptyset$; L^S_0 *is the set of* S*-sentences.*

Theorem 25. *Let* t *be an* S*-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be* S*-models with the same structure* $\mathfrak{M} \restriction \{\forall\} \cup S = \mathfrak{M}' \restriction \{\forall\} \cup S$ *and* $\mathfrak{M} \restriction \text{var}(t) = \mathfrak{M}' \restriction \text{var}(t)$. *Then* $\mathfrak{M}(t) = \mathfrak{M}'(t)$.

Theorem 26. *Let* t *be an* S*-term and let* $\mathfrak{M}$ *and* $\mathfrak{M}'$ *be* S*-models with the same structure* $\mathfrak{M} \restriction \{\forall\} \cup S = \mathfrak{M}' \restriction \{\forall\} \cup S$ *and* $\mathfrak{M} \restriction \text{free}(\varphi) = \mathfrak{M}' \restriction \text{free}(\varphi)$. *Then*

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

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

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

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

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

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

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

□

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

Definition 27. *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* $\mathrm{var}(t)\subseteq\{v_0,\dots,v_{n-1}\}$. *Then define*

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

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

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

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

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

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

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

Example 28. *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) $\forall v_0\forall v_1\forall v_2\ \circ v_0\circ v_1v_2\equiv\circ\circ v_0v_1v_2$;

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

c) $\forall v_0\exists v_1\ \circ v_0v_1\equiv e$.

This defines the axiom set

$$\Phi_{\mathrm{Gr}}=\{\forall v_0\forall v_1\forall v_2\ \circ v_0\circ v_1v_2\equiv\circ\circ v_0v_1v_2,\ \forall v_0\ \circ v_0\,e\equiv v_0,\ \forall v_0\exists v_1\ \circ v_0v_1\equiv e\}.$$

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

Definition 29. *Let S be a language and let $\Phi\subseteq L_0^S$ be a set of S-sentences. Then*

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

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

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

Exercise 9. One may consider $\mathrm{Mod}^S\Phi$ with appropriate morphisms as a category. In certain cases this category has closure properties like closure under products. One can give the categorial definition of cartesian product and show their existence under certain assumptions on Φ.

7 Logical implication and propositional connectives

Definition 30. *For a symbol set S and $\Phi\subseteq L^S$ and $\varphi\in L^S$ define that Φ* (logically) implies *φ ($\Phi\vDash\varphi$) iff every S-model $\mathfrak{I}\vDash\Phi$ is also a model of φ.*

Note that logical implication $\models$ is a relation between *syntactical* entities which is defined via the *semantic* notion of interpretation. The relation $\Phi \models ?$ can be viewed as the central relation in modern axiomatic mathematics: given the assumptions Φ what do they imply? The $\models$-relation is usually verified by mathematical *proofs*. These proofs seem to refer to the exploration of some domain of mathematical objects and, in practice, require particular mathematical skills and ingenuity.

We will however show that the logical implication $\models$ satisfies certain simple syntactical laws. These laws correspond to ordinary proof methods a a purely formal. Amazingly a finite list of methods will (in principle) suffice for all mathematical proofs: this is Gödel's completeness theorem that we shall prove later.

Theorem 31. *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 $\Gamma \models \varphi$.

c) ($\to$-Introduction) If $\Gamma \cup \varphi \models \psi$ then $\Gamma \models \varphi \to \psi$.

d) ($\to$-Elimination) If $\Gamma \models \varphi$ and $\Gamma \models \varphi \to \psi$ then $\Gamma \models \psi$.

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

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

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

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

Exercise 10. There are similar rules for the introduction and elimination of junctors like $\wedge$ and $\vee$ that we have introduced as abbreviations:

a) ($\wedge$-Introduction) If $\Gamma \models \varphi$ and $\Gamma \models \psi$ then $\Gamma \models \varphi \wedge \psi$.

b) ($\wedge$-Elimination) If $\Gamma \models \varphi \wedge \psi$ then $\Gamma \models \varphi$ and $\Gamma \models \psi$.

c) ($\vee$-Introduction) If $\Gamma \models \varphi$ then $\Gamma \models \varphi \vee \psi$ and $\Gamma \models \psi \vee \varphi$.

d) ($\vee$-Elimination) If $\Gamma \models \varphi \vee \psi$ and $\Gamma \vdash \neg\varphi$ then $\Gamma \models \psi$.

8 Substitution and term rules

To prove further rules for equality and quantification, we first have to consider the *substitution* of terms in formulas.

Definition 32. *For a term $s \in T^S$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$ define the* (simultaneous) substitution

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

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

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

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

Note that the *simultaneous* substitution

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

is in general different from a *succesive* substitution

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

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

Definition 33. *For a formula $\varphi \in L^S$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$ define the* (simultaneous) substitution

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

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

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

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

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

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

e) for $(\forall x\varphi)\,\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}}$ *we proceed in two steps: let $x_{i_0}, \ldots, x_{i_{s-1}}$ with $i_0 < \ldots < i_{s-1}$ be exactly those x_i which are "relevant" for the substitution, i.e., $x_i \in \mathrm{free}(\forall x\varphi)$ and $x_i \neq t_i$.*

- *if x does not occur in $t_{i_0}, \ldots, t_{i_{s-1}}$, then set*

$$(\forall x\varphi)\,\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = \forall x\,(\varphi\,\frac{t_{i_0}\ldots t_{i_{s-1}}}{x_{i_0}\ldots x_{i_{s-1}}}).$$

- *if x does occur in $t_{i_0}, \ldots, t_{i_{s-1}}$, then let $k \in \mathbb{N}$ minimal such that v_k does not occur in φ, $t_{i_0}, \ldots, t_{i_{s-1}}$ and set*

$$(\forall x\varphi)\,\frac{t_0\ldots t_{r-1}}{x_0\ldots x_{r-1}} = \forall v_k\,(\varphi\,\frac{t_{i_0}\ldots t_{i_{s-1}}v_k}{x_{i_0}\ldots x_{i_{s-1}}x}).$$

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

Theorem 34. *Consider an S-model $\mathfrak{M}$, pairwise distinct variables $x_0, \ldots, x_{r-1}$ and terms $t_0, \ldots, t_{r-1} \in T^S$.*

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

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

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

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

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

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

Case 1.2: $x = x_i$. Then

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

Case 2: $s = f s_0 \ldots s_{n-1}$ where $f \in S$ is an n-ary function symbol and the terms s_0, ..., $s_{n-1} \in T^S$ satisfy the theorem. Then

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

Assuming that the substitution theorem is proved for terms, we prove
b) *Case 4*: $\varphi = R s_0 \ldots s_{n-1}$. Then

$$\begin{aligned}
\mathfrak{M} \models (R s_0 \ldots s_{n-1}) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \quad &\text{iff} \quad \mathfrak{M} \models R s_0 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \ldots s_{n-1} \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}} \\
&\text{iff} \quad R^{\mathfrak{M}}\Big(\mathfrak{M}(s_0 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}), \ldots, \mathfrak{M}(s_1 \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}) \Big) \\
&\text{iff} \quad R^{\mathfrak{M}}\Big(\mathfrak{M} \frac{\mathfrak{M}(t_0) \ldots \mathfrak{M}(t_{r-1})}{x_0 \ldots x_{r-1}}(s_0), \\
&\qquad \ldots, \mathfrak{M} \frac{\mathfrak{M}(t_0) \ldots \mathfrak{M}(t_{r-1})}{x_0 \ldots x_{r-1}}(s_{n-1}) \Big) \\
&\text{iff} \quad \mathfrak{M} \frac{\mathfrak{M}(t_0) \ldots \mathfrak{M}(t_{r-1})}{x_0 \ldots x_{r-1}} \models R s_0 \ldots s_{n-1}
\end{aligned}$$

Equations $s_0 \equiv s_1$ can be treated as a special case of the relational *Case 4*. Propositional combinations of formulas by $\bot$, $\neg$ and $\to$ behave similar to terms; indeed formulas can be viewed as terms whose values are truth values. So we are left with universal quantification: *Case 5*: $\varphi = (\forall x \psi) \frac{t_0 \ldots t_{r-1}}{x_0 \ldots x_{r-1}}$, assuming that the theorem holds for ψ.

We proceed according to our definition of syntactic substitution. Let $x_{i_0}, \ldots, x_{i_{s-1}}$ with $i_0 < \ldots < i_{s-1}$ be exactly those x_i such that $x_i \in \text{free}(\forall x \psi)$ and $x_i \neq t_i$. Since

$$\mathfrak{M} \frac{\mathfrak{M}(t_0) \ldots \mathfrak{M}(t_{r-1})}{x_0 \ldots x_{r-1}} \models \varphi \text{ iff } \mathfrak{M} \frac{\mathfrak{M}(t_{i_0}) \ldots \mathfrak{M}(t_{i_{s-1}})}{x_{i_0} \ldots x_{i_{s-1}}} \models \varphi,$$

we can assume that $(x_0,...,x_{r-1}) = (x_{i_0},...,x_{i_{s-1}})$, i.e., every x_i is free in $\forall x\psi$, $x_i \neq x$, and $x_i \neq t_i$. Now follow the two cases in the definition of the substitution:

Case 5.1: The variable x does not occur in $t_0,....,t_{r-1}$ and

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

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

Case 5.2: The variable x occurs in $t_0,....,t_{r-1}$. Then

$$(\forall x\,\psi)\,\frac{t_0....t_{r-1}}{x_0...x_{r-1}} = \forall v_k\,(\psi\,\frac{t_{i_0}....t_{i_{s-1}}v_k}{x_{i_0}...x_{i_{s-1}}x}),$$

where $k \in \mathbb{N}$ is minimal such that v_k does not occur in φ, $t_{i_0},....,t_{i_{s-1}}$.

$$\begin{aligned}
\mathfrak{M} \vDash (\forall x\psi)\,\frac{t_0...t_{r-1}}{x_0...x_{r-1}} \;\text{ iff }\; & \mathfrak{M} \vDash \forall v_k\,(\psi\,\frac{t_0....t_{r-1}v_k}{x_0...x_{r-1}x}) \\
\text{iff }\; & \text{for all } a \in M \text{ holds } \mathfrak{M}\frac{a}{v_k} \vDash \psi\,\frac{t_0...t_{r-1}v_k}{x_0...x_{r-1}x} \\
\text{iff }\; & \text{for all } a \in M \text{ holds} \\
& (\mathfrak{M}\frac{a}{v_k})\frac{\mathfrak{M}\frac{a}{v_k}(t_0)...\mathfrak{M}\frac{a}{v_k}(t_{r-1})\mathfrak{M}\frac{a}{v_k}(v_k)}{x_0...x_{r-1}\,x} \vDash \psi \\
& \text{(inductive hypothesis for } \psi) \\
\text{iff }\; & \text{for all } a \in M \text{ holds} \\
& (\mathfrak{M}\frac{a}{x})\frac{\mathfrak{M}(t_0)...\mathfrak{M}(t_{r-1})a}{x_0...x_{r-1}x} \vDash \psi \\
& \text{(since } v_k \text{ does not occur in } t_i) \\
\text{iff }\; & \text{for all } a \in M \text{ holds}
\end{aligned}$$

$$\mathfrak{M}\,\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})\,a}{x_0\ldots x_{r-1}\,x} \vDash \psi$$

(since x is anyway sent to a)

iff for all $a \in M$ holds

$$(\,\mathfrak{M}\,\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})}{x_0\ldots x_{r-1}})\,\frac{a}{x} \vDash \psi$$

(by simple properties of assignments)

iff $\mathfrak{M}\,\frac{\mathfrak{M}(t_0)\ldots\mathfrak{M}(t_{r-1})}{x_0\ldots x_{r-1}} \vDash \forall x\,\psi$

□

We can now formulate properties of the $\vDash$ relation in connection with the treatment of variables.

Theorem 35. *Let S be a language. Let x, y be variables, $t, t' \in T^S$, $\varphi \in L^S$, and $\Gamma \subseteq L^S$. Then:*

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

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

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

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

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

Case 1: $x = y$. Then $\mathfrak{M}\frac{a}{x} \vDash \varphi$.

Case 2: $x \neq y$. Then $\mathfrak{M}\,\frac{aa}{yx} \vDash \varphi$, and since $y \notin \mathrm{free}(\varphi)$ we have $\mathfrak{M}\frac{a}{x} \vDash \varphi$.

Since $a \in M$ is arbitrary, $\mathfrak{M} \vDash \forall x\varphi$. Thus $\Gamma \vDash \forall x\varphi$.

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

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

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

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

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

and again by the substitution theorem

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

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

Note that in proving these proof rules we have used corresponding forms of arguments in the language of our discourse. This "circularity" was noted before and is a general feature in formalizations of logic. A particularly important method of proof is the $\forall$-introduction: to prove a universal statement $\forall x\varphi$ it suffices to consider an "arbitrary but fixed" y and prove the claim for y. Formally this corresponds to using a "new" variable $y \notin \mathrm{free}(\Gamma \cup \{\forall x\varphi\})$.

9 A sequent calculus

The only way to rectify our reasonings is to make them as tangible as those of the Mathematicians, so that we can find our error at a glance, and when there are disputes among persons, we can simply say: Let us calculate [calculemus], without further ado, to see who is right. G.W. Leibniz

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

Definition 36. *A finite sequence $(\varphi_0, ..., \varphi_{n-1}, \varphi_n)$ of S-formulas is called a* sequent. *The initial segment $\Gamma = (\varphi_0, ..., \varphi_{n-1})$ is the* antecedent *and φ_n is the* succedent *of the sequent. We usually write $\varphi_0 ... \varphi_{n-1} \varphi_n$ or $\Gamma \varphi_n$ instead of $(\varphi_0, ..., \varphi_{n-1}, \varphi_n)$. To emphasize the last element of the antecedent we may also denote the sequent by $\Gamma' \varphi_{n-1} \varphi_n$ with $\Gamma' = (\varphi_0, ..., \varphi_{n-2})$.*

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

Exercise 11. One could also define a sequent to be the concatenation of finitely many formulas

Definition 37. *The* sequent calculus *consists of the following (sequent-)rules:*

– *monotonicity* (MR) $\dfrac{\Gamma \quad \varphi}{\Gamma \quad \psi \quad \varphi}$

– *assumption* (AR) $\dfrac{}{\Gamma \quad \varphi \quad \varphi}$

– *$\to$-introduction* ($\to I$) $\dfrac{\Gamma \quad \varphi \quad \psi}{\Gamma \quad \varphi \to \psi}$

– *$\to$-elimination* ($\to E$) $\dfrac{\begin{array}{l}\Gamma \quad \varphi \\ \Gamma \quad \varphi \to \psi\end{array}}{\Gamma \quad \psi}$

– *$\bot$-introduction* ($\bot I$) $\dfrac{\begin{array}{l}\Gamma \quad \varphi \\ \Gamma \quad \neg\varphi\end{array}}{\Gamma \quad \bot}$

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

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

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

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

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

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

Remark 38. A calculus is a formal system for obtaining (mathematical) results. The usual algorithms for addition and multiplication of decimal numbers are calculi: the results are achieved by symbolic and systematic operations on the decimal symbols $0, \ldots, 9$. Such an addition is not an addition in terms of joining together line segments of certain lengths or forming the union of disjoint finite sets. The calculi are however correct in that the interpretation of the decimal numbers obtained correspond to the results of the intuitive operations of joining line segments or disjoint unions.

Mathematics has shown that far more sophisticated operations can also be described by *calculi*. The derivation of a polynomial function

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

can be obtained by formal manipulations of exponents and coefficients:

$$p'(x) = n\, a_n x^{n-1} + (n-1)\, a_{n-1} x^{n-2} + \ldots + a_1$$

without explicitly forming limits of difference quotients.

Since many basic results of analysis can be expressed as formal calculi, the word *calculus* is used for basic analysis courses in the English speaking world. Similarly in German one uses the words Differential*rechnung* and Integral*rechnung*. The words *derivation* or *Ableitung* also refer to derivations within a formal calculus.

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

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

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

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

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

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

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

Theorem 39. *The sequent calculus is* correct*, i.e., every rule of the sequent calculus leads from correct sequents to correct sequents. Thus every derivable sequent is correct. This means that*

$$\vdash \subseteq \models .$$

The converse inclusion corresponds to

Definition 40. *The sequent calculus is* complete *iff* $\models \subseteq \vdash$.

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

Theorem 41. *Let* $\Phi \subseteq L^S$ *and* $\varphi \in \Phi$. *Then* $\Phi \vdash \varphi$ *iff there is a finite subset* $\Phi_0 \subseteq \Phi$ *such that* $\Phi_0 \vdash \varphi$.

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

10 Derivable sequent rules

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

Lemma 42. *Assume that*

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

is a derived rule of the sequent calculus. Then

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

is also a derived rule of the sequent calculus.

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

We now list several derived rules.

10.1 Auxiliary rules

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

ex falso quodlibet $\dfrac{\begin{array}{ll}\Gamma & \bot\end{array}}{\begin{array}{ll}\Gamma & \varphi\end{array}}$:

1.	Γ		$\bot$
2.	Γ	$\neg\varphi$	$\bot$
3.	Γ		φ

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

1.	Γ	φ		$\bot$
2.	Γ			$\varphi\to\bot$
3.	Γ	$\neg\neg\varphi$		$\neg\neg\varphi$
4.	Γ	$\neg\neg\varphi$	$\neg\varphi$	$\neg\varphi$
5.	Γ	$\neg\neg\varphi$	$\neg\varphi$	$\bot$
6.	Γ	$\neg\neg\varphi$		φ
7.	Γ	$\neg\neg\varphi$		$\bot$
8.	Γ			$\neg\varphi$

1.	Γ		$\neg\varphi$
2.	Γ	φ	φ
3.	Γ	φ	$\bot$
4.	Γ	φ	ψ
5.	Γ		$\varphi\to\psi$

1.	Γ		ψ
2.	Γ	φ	ψ
3.	Γ		$\varphi\to\psi$

Cut rule

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

Contraposition

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

10.2 Introduction and elimination of $\vee, \wedge, ...$

The (abbreviating) logical symbols $\vee$, $\wedge$, and $\exists$ also possess (derived) introduction and elimination rules. We list the rules and leave their derivations as exercises.

$\vee$-*Introduction*

Γ	φ	
Γ	$\varphi\vee\psi$	

$\vee$-*Introduction*

$$\frac{\Gamma \quad \psi}{\Gamma \quad \varphi \vee \psi}$$

$\vee$-*Elimination*

$$\frac{\Gamma \quad \varphi \vee \psi \qquad \Gamma \quad \varphi \to \chi \qquad \Gamma \quad \psi \to \chi}{\Gamma \quad \chi}$$

$\wedge$-*Introduction*

$$\frac{\Gamma \quad \varphi \qquad \Gamma \quad \psi}{\Gamma \quad \varphi \wedge \psi}$$

$\wedge$-*Elimination*

$$\frac{\Gamma \quad \varphi \wedge \psi}{\Gamma \quad \varphi}$$

$\wedge$-*Elimination*

$$\frac{\Gamma \quad \varphi \wedge \psi}{\Gamma \quad \varphi}$$

$\exists$-*Introduction*

$$\frac{\Gamma \quad \varphi\frac{t}{x}}{\Gamma \quad \exists x \varphi}$$

$\exists$-*Elimination*

$$\frac{\Gamma \quad \exists x \varphi \qquad \Gamma \quad \varphi\frac{y}{x} \quad \psi}{\Gamma \quad \psi} \text{ where } y \notin \mathrm{free}(\Gamma \cup \{\exists x \varphi, \psi\})$$

10.3 Manipulations of antecedents

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

Transpositions of premisses

$$\frac{\begin{array}{lll} 1. & \Gamma \quad \varphi \quad \psi & \chi \end{array}}{\begin{array}{lll} 2. & \Gamma \quad \varphi & \psi \to \chi \\ 3. & \Gamma & \varphi \to (\psi \to \chi) \\ 4. & \Gamma \quad \psi & \psi \\ 5. & \Gamma \quad \psi \quad \varphi & \varphi \\ 6. & \Gamma \quad \psi \quad \varphi & \psi \to \chi \end{array}}{\begin{array}{lll} 7. & \Gamma \quad \psi \quad \varphi & \chi \end{array}}$$

Duplication of premisses

$$\frac{\begin{array}{lll} 1. & \Gamma \quad \varphi & \psi \end{array}}{\begin{array}{lll} 2. & \Gamma \quad \varphi \quad \varphi & \psi \end{array}}$$

Elimination of double premisses

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

Iterated applications of these rules yield:

Lemma 43. *Let $\varphi_0 ... \varphi_{m-1}$ and $\psi_0 ... \psi_{n-1}$ be antecedents such that*

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

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

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

is a derived rule.

10.4 Formal proofs about $\equiv$

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

Lemma 44. *We prove the following tautologies:*

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

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

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

Proof. a)

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

b)

$$\frac{\begin{array}{ll} x \equiv y & x \equiv y \\ x \equiv y & x \equiv x \\ x \equiv y & (z \equiv x)\frac{x}{z} \\ x \equiv y & (z \equiv x)\frac{y}{x} \\ x \equiv y & y \equiv x \\ & x \equiv y \to y \equiv x \\ & \forall y (x \equiv y \to y \equiv x) \end{array}}{\forall x \forall y (x \equiv y \to y \equiv x)}$$

c)

$$\frac{\begin{array}{ll} x \equiv y \wedge y \equiv z & x \equiv y \wedge y \equiv z \\ x \equiv y \wedge y \equiv z & x \equiv y \\ x \equiv y \wedge y \equiv z & (x \equiv w)\frac{y}{w} \\ x \equiv y \wedge y \equiv z & y \equiv z \\ x \equiv y \wedge y \equiv z & (x \equiv w)\frac{z}{w} \\ x \equiv y \wedge y \equiv z & x \equiv z \\ & x \equiv y \wedge y \equiv z \to x \equiv z \\ & \forall z (x \equiv y \wedge y \equiv z \to x \equiv z) \\ & \forall y \forall z (x \equiv y \wedge y \equiv z \to x \equiv z) \end{array}}{\forall x \forall y \forall z (x \equiv y \wedge y \equiv z \to x \equiv z)}$$

□

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

Theorem 45. *Let $\varphi \in L^S$ and $t_0, ..., t_{n-1}, t'_0, ..., t'_{n-1} \in T^S$. Then*

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

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

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

and

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

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

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

□

11 Consistency

Vor Allem aber möchte ich unter den zahlreichen Fragen, welche hinsichtlich der Axiome gestellt werden können, dies als das wichtigste Problem bezeichnen, zu beweisen, daß dieselben untereinander widerspruchslos sind, d.h. daß man auf Grund derselben mittelst einer endlichen Anzahl von logischen Schlüssen niemals zu Resultaten gelangen kann, die miteinander in Widerspruch stehen.
David Hilbert

Fix a language S.

Definition 46. *A set $\Phi \subseteq L^S$ is* consistent *if $\Phi \nvdash \bot$. Φ is* inconsistent *if $\Phi \vdash \bot$.*

We prove some laws of consistency.

Lemma 47. *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 $\Phi \vdash \bot$. Then by the *ex falso* rule, $\Phi \vdash \psi$ and $\Phi \vdash \neg\psi$.

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

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

$\varphi_0 \ \dots \ \varphi_{n-1} \qquad \varphi$
$\varphi_0 \ \dots \ \varphi_{n-1} \ \neg\varphi \ \ \neg\varphi$
$\varphi_0 \ \dots \ \varphi_{n-1} \ \neg\varphi \ \ \bot$

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

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

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

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

The proof of the completeness theorem will be based on the relation between consistency and satisfiability.

Lemma 48. *Assume that $\Phi \subseteq L^S$ is satisfiable. Then Φ is consistent.*

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

We shall later show the converse of this Lemma, since:

Theorem 49. *The sequent calculus is complete iff every consistent $\Phi \subseteq L^S$ is satisfiable.*

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

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

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

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

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

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

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

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

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

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

$$(\bar{t}_0, ..., \bar{t}_{n-1}) \in R^{\mathfrak{T}^\Phi} \text{ iff } \Phi \vdash Rt_0...t_{n-1} .$$

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

$$f^{\mathfrak{T}^\Phi}(\bar{t}_0, ..., \bar{t}_{n-1}) = \overline{ft_0...t_{n-1}} .$$

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

The term model is well-defined.

Lemma 51. *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 $\equiv$:

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

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 $\vdash t_0 \equiv t_1 \to t_1 \equiv t_0$, $\vdash t_1 \equiv t_0$, 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 $\bar{t}_0, ..., \bar{t}_{n-1} \in T^\Phi$, $\bar{t}_0 = \bar{s}_0, ..., \bar{t}_{n-1} = \bar{s}_{n-1}$ and $\Phi \vdash Rt_0...t_{n-1}$. Then $\vdash t_0 \equiv s_0$, ... , $\vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule yield $\Phi \vdash Rs_0...s_{n-1}$. Hence $\Phi \vdash Rt_0...t_{n-1}$ implies $\Phi \vdash Rs_0...s_{n-1}$. By the symmetry of the argument, $\Phi \vdash Rt_0...t_{n-1}$ iff $\Phi \vdash Rs_0...s_{n-1}$.

c) Let $\bar{t}_0, ..., \bar{t}_{n-1} \in T^\Phi$ and $\bar{t}_0 = \bar{s}_0, ..., \bar{t}_{n-1} = \bar{s}_{n-1}$. Then $\vdash t_0 \equiv s_0$, ... , $\vdash t_{n-1} \equiv s_{n-1}$. Repeated applications of the substitution rule to $\vdash ft_0...t_{n-1} \equiv ft_0...t_{n-1}$ yield

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

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

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

Theorem 52.

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

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

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

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

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

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

□

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

Definition 53. *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*

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

Lemma 54. *Let $\Phi \subseteq L^S$ be a* HENKIN *set. Then for all $\chi, \psi \in L^S$ and variables x:*

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

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

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

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

Conversely assume that $\Phi \vdash \chi \to \psi$. Assume that $\Phi \vdash \chi$. By $\to$-elimination, $\Phi \vdash \psi$. Thus $\Phi \vdash \chi$ implies $\Phi \vdash \psi$.
c) Assume that for all $t \in T^S$ holds $\Phi \vdash \chi\frac{t}{u}$. Assume that $\Phi \nvdash \forall x\chi$. By a), $\Phi \vdash \neg\forall x\chi$. Since Φ contains witnesses there is a term $t \in T^S$ such that $\Phi \vdash \neg\forall x\chi \to \neg\chi\frac{t}{u}$. By $\to$-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 55. *Let* $\Phi \subseteq L^S$ *be a* HENKIN *set. Then*

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

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

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

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

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

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

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

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

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

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

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

□

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

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

is consistent.

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

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

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

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

Hence Φ is inconsistent, contradiction. $\square$

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

Theorem 57. *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*

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

is consistent.

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

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

with $\Gamma_n \subseteq \Phi$. Choose a variable z, which does not occur in the derivation. For a formula ψ define ψ' by replacing each occurence of c by z, and for a sequence $\Gamma = (\psi_0, \ldots, \psi_{k-1})$ of formulas let $\Gamma' = (\psi'_0, \ldots, \psi'_{k-1})$. Replacing each occurence of c by z in the deriavation we get

$$\begin{array}{c} \Gamma'_0 \varphi'_0 \\ \Gamma'_1 \varphi'_1 \\ \vdots \\ \Gamma'_{n-1}\, \varphi'_{n-1} \\ \Gamma_n\ (\neg\forall x\,\varphi \to \neg\varphi\frac{z}{x})\ \bot \end{array} \tag{2}$$

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

So let

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

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

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

is a justified $\forall$-introduction.

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

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

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

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

is a justified $\forall$-elimination.

The derivation (2) proves that

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

which contradicts the preceding lemma. □

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

Theorem 58. *Let S be a language and let $\Phi \subseteq L^S$ be consistent. Then there is a language S^ω and $\Phi^\omega \subseteq L^{S^*}$ such that*

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

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

c) Φ^ω is consistent;

d) Φ^ω contains witnesses;

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

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

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

Then set

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

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

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

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

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

is consistent. Contradiction. *qed*(1)

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

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

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

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

To get HENKIN sets we have to ensure derivation completeness.

Theorem 59. *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 $\neg \varphi \in \Phi^*$. □

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

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

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

ii. Φ_n is consistent.

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

Let

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

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

According to Theorem 58 a given consistent set Φ can be extended to $\Phi^\omega \subseteq L^{S^\omega}$ containing witnesses. By Theorem 59 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 60. *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^*.

14 The completeness theorem

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

Combining Theorems 60 and 55, we obtain a general and a countable model existence theorem:

Theorem 61. (HENKIN model existence theorem) *Let $\Phi \subseteq L^S$. Then Φ is consistent iff Φ is satisfiable.*

By Lemma 49, Theorem 61 the model existence theorems imply the main theorem.

Theorem 62. (GÖDEL completeness theorem) *The sequent calculus is complete, i.e., $\models = \vdash$.*

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

- The completeness theorem gives an *ultimate correctness criterion* for mathematical proofs. A proof is correct if it can (in principle) be reformulated as a formal derivation. Although mathematicians prefer semi-formal or informal arguments, this criterion could be applied in case of doubt.
- Checking the correctness of a formal proof in the above sequent calculus is a syntactic task that can be carried out by computer. We shall later consider a prototypical *proof checker* `Naproche` which uses a formal language which is a subset of natural english.
- By systematically running through all possible formal proofs, *automatic theorem proving* is in principle possible. In this generality, however, algorithms immediately run into very high algorithmic complexities and become practically infeasable.
- Practical automatic theorem proving has become possible in restricted situations, either by looking at particular kinds of axioms and associated intended domains, or by restricting the syntactical complexity of axioms and theorems.

- Automatic theorem proving is an important component of *artificial intelligence* (AI) where a system has to obtain logical consequences from conditions formulated in first-order logic. Although there are many difficulties with artificial intelligence this approach is still being followed with some success.
- Another special case of automatic theorem proving is given by *logic programming* where programs consist of logical statements of some restricted complexity and a run of a program is a systematic search for a solution of the given statements. The original and 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.

15 The compactness theorem

The equality of $\models$ and $\vdash$ and the compactness theorem 41 for $\vdash$ imply

Theorem 63. (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.*

This theorem is often to construct (unusual) models of first-order theories. It is the basis of a field of logic called *Model Theory*.

We present a number theoretic application of the compactness theorem. The language of arithmetic can be naturally interpreted in the structure $\mathbb{N} = (\mathbb{N}, +, \cdot, 0, 1)$. This structure obviously satisfies the following axioms:

Definition 64. *The axiom system* $\mathrm{PA} \subseteq L^{S_{\mathrm{AR}}}$ *of* peano arithmetic *consists of the following sentences*

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

– *Schema of induction: for every formula* $\varphi(x_0,...,x_{n-1},x_n)\in L^{S_{\mathrm{AR}}}$*:*

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

The theory PA is allows to prove a lot of number theoretic properties, e.g., about divisibility and prime numbers. On the other hand the first *incompleteness theorem* of GÖDEL shows that there are arithmetic sentences φ which are not decided by PA although they are true in the standard model $\mathbb{N}$ of PA. Therefore PA is *not* complete.

If φ and $\neg\varphi$ are both not derivable from PA then $\mathrm{PA}+\neg\varphi$ and $\mathrm{PA}+\varphi$ are consistent. By the model existence theorem, there are models $\mathfrak{M}^-$ and $\mathfrak{M}^+$ such that $\mathfrak{M}^-\models\mathrm{PA}+\neg\varphi$ and $\mathfrak{M}^+\models\mathrm{PA}+\varphi$. $\mathfrak{M}^-$ and $\mathfrak{M}^+$ are not isomorphic. So there exist models of PA which are not isomorphic to the standard model $\mathbb{N}$.

We can also use the compactness theorem to obtain nonstandard models of theories. Define the S_{AR}-terms $\bar{n}$ for $n\in\mathbb{N}$ recursively by

$$\begin{aligned}\bar{0} &= 0,\\ \overline{n+1} &= (\bar{n}+1).\end{aligned}$$

Define divisibility by the S_{AR}-formula $\delta(x,y)=\exists z\; x\cdot z\equiv y$.

Theorem 65. *There is a model* $\mathfrak{M}\models\mathrm{PA}$ *which contains an element* $\infty\in M$ *such that* $\mathfrak{M}\models\delta(\bar{n}\,,\infty)$ *for every* $n\in\mathbb{N}\setminus\{0\}$ *(we use* $\mathfrak{M}\models\delta(\bar{n}\,,\infty)$ *as an intuitive abbreviation for* $\mathfrak{M}\models\delta(\bar{n}\,,v_0)[\infty]$*).*

So "from the outside", ∞ is divisible by every positive natural number. This implies that $\mathfrak{M}$ is a nonstandard model with $\mathfrak{M}\not\cong\mathbb{N}$.

Proof. Consider the theory

$$\Phi=\mathrm{PA}\cup\{\delta(\bar{n}\,,v_0)\mid n\in\mathbb{N}\setminus\{0\}\}.$$

(1) Φ is satisfiable.
Proof. We use the compactness theorem 63(b). Let $\Phi_0\subseteq\Phi$ be finite. It suffices to show that Φ_0 is satisfiable. Take a finite number $n_0\in\mathbb{N}$ such that

$$\Phi_0\subseteq\mathrm{PA}\cup\{\delta(\bar{n}\,,v_0)\mid n\in\mathbb{N},1\leqslant n\leqslant n_0\}.$$

Let $N=n!$. Then

$$\mathbb{N}\models\mathrm{PA}\text{ and }\mathbb{N}\models\delta(\bar{n}\,,N)\text{ for }1\leqslant n\leqslant n_0\,.$$

So $\mathbb{N}\frac{N}{v_0}\models\Phi_0$. *qed*(1)

By (1), let $\mathfrak{M}'\models\Phi$. Let $\infty=\mathfrak{M}'(v_0)\in|\mathfrak{M}'|$. Let $\mathfrak{M}$ be the S_{AR}-structure which extends to the model $\mathfrak{M}'$, i.e., $\mathfrak{M}=\mathfrak{M}'\restriction\{\forall\}\cup S_{\mathrm{AR}}$. Then $\mathfrak{M}$ is a structure satisfying the theorem. □

This indicates that the model class of PA is rather complicated and rich. Indeed there is a subfield of model theory which primarily studies models of Peano arithmetic.

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

Definition 66. *Let* S *be a language and* $\mathcal{K}$ *be a class of* S*-structures.*

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

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

We state simple properties of the Mod-operator:

Theorem 67. *Let S be a language. Then*

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

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

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

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

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

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

Theorem 68. *Let S be a language and $\mathcal{K}, \mathcal{L}$ be classes of S-structures with*

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

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

Proof. Take axiom systems Φ_K and Φ_L such that $\mathfrak{K} = \mathrm{Mod}^S\Phi_K$ and $\mathfrak{L} = \mathrm{Mod}^S\Phi_L$. Assume that $\mathfrak{K}$ is not finitely axiomatizable.
(1) Let $\Phi_0 \subseteq \Phi_K$ be finite. Then $\Phi_0 \cup \Phi_L$ is satisfiable.
Proof: $\mathrm{Mod}^S\Phi_0 \supseteq \mathrm{Mod}^S\Phi_K$. Since $\mathfrak{K}$ is not finitely axiomatizable, $\mathrm{Mod}^S\Phi_0 \neq \mathrm{Mod}^S\Phi_K$. Then $\mathrm{Mod}^S\Phi_0 \cap \mathfrak{L} \neq \emptyset$. Take a model $\mathfrak{A} \in \mathfrak{L}$, $\mathfrak{A} \in \mathrm{Mod}^S\Phi_0$. Then $\mathfrak{A} \vDash \Phi_0 \cup \Phi_L$. *qed*(1)
(2) $\Phi_K \cup \Phi_L$ is satisfiable.
Proof: By the compactness theorem 63 it suffices to show that every finite $\Psi \subseteq \Phi_K \cup \Phi_L$ is satsifiable. By (1), $(\Psi \cap \Phi_K) \cup \Phi_L$ is satisfiable. Thus $\Psi \subseteq (\Psi \cap \Phi_K) \cup \Phi_L$ is satisfiable. *qed*(2)
By (2), $\mathrm{Mod}^S\Phi_K \cap \mathrm{Mod}^S\Phi_L \neq \emptyset$. But the classes $\mathfrak{K}$ and $\mathfrak{L}$ are complements, contradiction. Thus $\mathfrak{K}$ is finitely axiomatizable. □

16 The Löwenheim-Skolem theorems

Definition 69. *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..*

If the language S is countable, i.e., finite or countably infinite, and it $\Phi \subseteq L^S$ is a *countable* consistent set of formulas then an inspection of the above construction of a term model for Φ shows the following theorem.

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

The word "downward" emphasises the existence of models of "small" cardinality. We shall soon consider an "upward" Löwenheim-Skolem theorem.

Theorem 71. *Assume that $\Phi \subseteq L^S$ has arbitrarily large finite models. Then Φ has an infinite model.*

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

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

where the big conjunction is defined by

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

For any model $\mathfrak{M}$

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

Now set

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

(1) Φ' has a model.
Proof. By the compactness theorem 63b it suffices to show that every finite $\Phi_0 \subseteq \Phi$ has a model. Let $\Phi_0 \subseteq \Phi$ be finite. Take $n_0 \in \mathbb{N}$ such that

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

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

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

Theorem 72. (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 $(c_x \,|\, x \in X)$ of pairwise distinct constant symbols which do not occur in S, e.g., setting $c_x = ((x, S), 1, 0)$. Let $S' = S \cup \{c_x \,|\, x \in X\}$ be the extension of S by the new constant symbols. Set

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

(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

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

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

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

qed(1)

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

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

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

Theorem 73. *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.

Proof. a) is immediate by Theorem 71.
b) The class of infinite S-structures is axiomatized by

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

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

17 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 74.

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*

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

where each L_{ij} is a literal.

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

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

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

$$\varphi = \{\{L_{00}, \ldots, L_{0n_0-1}\}, \ldots, \{L_{m-1,0}, \ldots, L_{m-1,n_{m-1}}\}\}.$$

Theorem 75. *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:

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

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

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

which is also in conjunctive normal form. □

Definition 76. *A formula φ is in* prenex normal form *if it is of the form*

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

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

Theorem 77. *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

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

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

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

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

For the $\wedge$-operation consider another formula

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

with quantifier-free ψ'. We may assume that the bound variables of of the prenex normal forms are disjoint. Then

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

(semantic argument). □

Definition 78. *A formula φ is* universal *if it is of the form*

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

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

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

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 79. *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

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

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

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

By induction it suffices to show that φ is consistent iff φ' is consistent.
(1) $\varphi' \to \varphi$.
Proof. Assume φ'. Consider $x_1, ..., x_m$. Then $\psi\frac{fx_1...x_m}{y}$. Then $\exists y\psi$. Thus $\forall x_1 ... \forall x_m \exists y \psi$. *qed*(1)
(2) If φ' is consistent then φ is consistent.
Proof. If $\varphi \to \bot$ then by (1) $\varphi' \to \bot$. *qed*(2)
(3) If φ is consistent then φ' is consistent.
Proof. Let φ be consistent and let $\mathcal{M} = (M, ...) \vDash \varphi$. Then

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

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

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

Expand the structure $\mathcal{M}$ to $\mathcal{M}' = \mathcal{M} \cup \{(f, h)\}$ where the symbol f is interpreted by the function h. Then $h(a_1, ..., a_m) = \mathcal{M}'\frac{\vec{a}}{\vec{x}}(fx_1...x_m)$ and

$$\forall a_1 \in M ... \forall a_m \in M \mathcal{M}'\frac{\vec{a}\ \mathcal{M}'\frac{\vec{a}}{\vec{x}}(fx_1...x_m)}{\vec{x}\ \ y} = \mathcal{M}'\frac{\vec{a}}{\vec{x}}\,\frac{\mathcal{M}'\frac{\vec{a}}{\vec{x}}(fx_1...x_m)}{y} \vDash \psi.$$

By the substitution theorem this is equivalent to

$$\forall a_1 \in M ... \forall a_m \in M \, \mathcal{M}'\frac{\vec{a}}{\vec{x}} \vDash \psi\frac{fx_1...x_m}{y}.$$

Hence

$$\mathcal{M}' \vDash \forall x_1 ... \forall x_m \, \psi\frac{fx_1...x_m}{y} = \varphi'.$$

Thus φ' is consistent. □

18 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 80. *Let S be a language which contains at least one constant symbol. Let*

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

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

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

such that

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

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

$$\Phi = \{\psi\frac{t_0,...,t_{m-1}}{x_0,...,x_{m-1}} \,|\, t_0,...,t_{m-1} \text{ are constant } S\text{-terms}\}$$

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

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

Then $H \neq \emptyset$ since S contains a constant symbol. By definition, H is closed under the functions of $\mathcal{M}$. So we let $\mathcal{H} = (H,...) \subseteq \mathcal{M}$ be the substructure of $\mathcal{M}$ with domain H.
(1) $\mathcal{H} \models \varphi$.
Proof. Let $\mathcal{M}(t_0)$, ..., $\mathcal{M}(t_{m-1}) \in H$ where t_0, ..., t_{m-1} are constant S-terms. Then $\psi\frac{t_0,...,t_{m-1}}{x_0,...,x_{m-1}} \in \Phi$, $\mathcal{M} \models \psi\frac{t_0,...,t_{m-1}}{x_0,...,x_{m-1}}$, and by the substitution theorem

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

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

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

Thus

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

qed(1)
Thus φ is consistent. □

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

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

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 occuring 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 $(\bigwedge\ \Phi) \vdash \bot$ iff $\forall(\bigwedge\ \Phi) \vdash \bot$.
2. Transform φ into universal form $\varphi^\forall = \forall x_0 \forall x_1 ... \forall x_{m-1}\, \psi$ (SKOLEMization).
3. Systematically search for constant S-terms
$$t_0^0,...,t_{m-1}^0,...,t_0^{N-1},...,t_{m-1}^{N-1}$$
such that
$$\varphi' = \bigwedge_{i<N} \psi\frac{t_0^i,...,t_{m-1}^i}{x_0,...,x_{m-1}} = \psi\frac{t_0^0,...,t_{m-1}^0}{x_0,...,x_{m-1}} \wedge ... \wedge \psi\frac{t_0^{N-1},...,t_{m-1}^{N-1}}{x_0,...,x_{m-1}}$$
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 $\psi = c_0 \wedge c_1 \wedge ... \wedge c_{l-1}$. Then $\forall x_0 \forall x_1 ... \forall x_{m-1} \psi$ is inconsistent iff the set

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

is inconsistent.

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

Definition 81. *Let $c^+ = \{K_0, ..., K_{k-1}\}$ and $c^- = \{L_0, ..., L_{l-1}\}$ be clauses with literals K_i and L_j. Note that $\{K_0, ..., K_{k-1}\}$ stands for the disjunction $K_0 \vee ... \vee K_{k-1}$. Assume that K_0 and L_0 are* dual*, i.e., $L_0 = \overline{K_0}$. Then the disjunction*

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

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

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

Theorem 82. *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 $c^+ = \{K_0, ..., K_{k-1}\}$, $c^- = \{\neg K_0, L_1 ..., L_{l-1}\}$, and $c = \{K_1, ..., K_{k-1}\} \cup \{L_1, ..., L_{l-1}\}$. Assume that $\mathcal{M} \vDash C$ is a model of C.
Case 1. $\mathcal{M} \vDash K_0$. Then $\mathcal{M} \vDash c^-$, $\mathcal{M} \vDash \{L_1 ..., L_{l-1}\}$, and

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

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

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

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

Theorem 83. *Let C be a set of clauses closed under resolution. Then C is inconsistent iff $\emptyset \in C$. Note that the empty clause $\{\} \leftrightarrow \bot$.*

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 $\{\varphi_0, ..., \varphi_{n-1}\}$ such that

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

the restriction of C to $\{\varphi_0, ..., \varphi_{n-1}\}$ 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 zero 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

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

and

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

(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 $rt_0...t_{s-1}$ where r is an n-ary relation symbol and $t_0, ..., t_{s-1} \in T^S$. Since the formula $rt_0...t_{s-1}$ 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 $(\mathcal{M}(t_0), ..., \mathcal{M}(t_{s-1}))$. So let $\mathcal{M}'(\mathcal{M}(t_0), ..., \mathcal{M}(t_{s-1}))$ 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 $\mathcal{M}'(\mathcal{M}(t_0), ..., \mathcal{M}(t_{s-1}))$ be *true*. So we get a contradiction again. □

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.

19 Logical programming

To give a small impression of the logical programming language `Prolog` let us consider a theory about the recursive definition of formulas. Let

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

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

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

from the axioms. This is equivalent to showing that

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

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

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

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

The choice of instances of the universal clause $\{\neg\mathrm{fm}(X), \neg\mathrm{fm}(Y), \mathrm{fm}(\mathrm{and}(X, Y))\}$ 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 finds substitutions to produce literals that are dual to each other. Indeed we did use informal and simple unification in the example:

- to make $3 = \neg\mathrm{fm}(X), \neg\mathrm{fm}(Y), \mathrm{fm}(\mathrm{and}(X, Y))$ and $4 = \neg\mathrm{fm}(\mathrm{and}(\mathrm{psi}, \mathrm{and}(\mathrm{psi}, \mathrm{psi})))$ resolve we chose substitutions for X and Y such that the literals $\mathrm{fm}(\mathrm{and}(X, Y))$ and $\neg\mathrm{fm}(\mathrm{and}(\mathrm{psi}, \mathrm{and}(\mathrm{psi}, \mathrm{psi})))$ became dual. This lead to setting X = psi and Y = and(psi,psi). The resolution then was $6 = \neg\mathrm{fm}(\mathrm{psi}), \neg\mathrm{fm}(\mathrm{and}(\mathrm{psi}, \mathrm{psi}))$.
- to make $1 = \mathrm{fm}(\mathrm{psi})$ and $6 = \neg\mathrm{fm}(\mathrm{psi}), \neg\mathrm{fm}(\mathrm{and}(\mathrm{psi}, \mathrm{psi}))$ resolve, no further substitution was required.
- to make $3 = \neg\mathrm{fm}(X), \neg\mathrm{fm}(Y), \mathrm{fm}(\mathrm{and}(X, Y))$ and $7 = \neg\mathrm{fm}(\mathrm{and}(\mathrm{psi}, \mathrm{psi}))$ resolve we chose the substitutions X = psi and Y = psi. The resolution then was $9 = \neg\mathrm{fm}(\mathrm{psi})$.
- to make $1 = \mathrm{fm}(\mathrm{psi})$ and $9 = \neg\mathrm{fm}(\mathrm{psi})$ resolve, no further substitution was required.

The above example can be viewed as the execution of a program in `Prolog`. `Prolog` systematically searches for unifications and keeps track of the required substitutions. The composition of all those substitutions is the computational result of the program.

To demonstrate how one can compute in `Prolog` let us consider the addition "2 + 2 = V?". We represent natural numbers by terms in a language with the constant symbol zero and the successor function succ. Addition is represented as a ternary predicate

$$\mathrm{add}(X, Y, Z) \leftrightarrow X + Y = Z.$$

The following program describes the recursive definition of add. To compute 2 + 2 one leads the assumption $\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})), \mathrm{succ}(\mathrm{succ}(\mathrm{zero})), X)$, which expresses that there is *no* solution to the addition problem, into a contradiction.

$$\begin{aligned}
&\mathrm{add}(X, \mathrm{zero}, X)\\
&(\mathrm{add}(X, Y, Z) \rightarrow \mathrm{add}(X, \mathrm{succ}(Y), \mathrm{succ}(Z)))\\
&\neg\mathrm{add}(\mathrm{succ}(\mathrm{succ}(\mathrm{zero})), \mathrm{succ}(\mathrm{succ}(\mathrm{zero})), V)
\end{aligned}$$

In `Prolog` notation, this can be written as

```
add(X,zero,X).
```

```
add(X,succ(Y),succ(Z) :- add(X,Y,Z).
?- add(succ(succ(zero)),succ(succ(zero)),V).
```

Execution of this program will lead to a substitution of V which makes the program inconsistent: we begin with the clauses

1. add(X,zero,X)
2. ¬add(X,Y,Z), add(X,succ(Y),succ(Z))
3. ¬add(succ(succ(zero)),succ(succ(zero)),V)

(The final literals of) 2 and 3 can be unified by the substitutions X:=succ(succ(zero)), Y:=succ(zero), V:=succ(Z). One obtains the resolvent:

4. ¬add(succ(succ(zero)),succ(zero),Z)

This should again resolve against 2. However to avoid variable clashes, we first rename the (universal) variables in 2:

5. ¬add(X1,Y1,Z1), add(X1,succ(Y1),succ(Z1))

4 and 5 can be unified by the substitutions X1:=succ(succ(zero)), Y1:=zero, Z:=succ(Z1). One obtains the resolvent:

6. ¬add(succ(succ(zero),zero,Z1)

This should resolve against 1. We first rename variables in 1:

7. add(X2,zero,X2).

6 and z can be unified by the substitutions X2:=succ(succ(zero)), Z1:=X2. As resolvent one obtains the desired contradiction

8. {}

A/the value for V which leads to this contradiction is obtained by chasing through the substitutions:

V=succ(Z)=succ(succ(Z1))=succ(succ(X2))=succ(succ(succ(succ(zero)))).

Thus 2+2=4!

20 ZERMELO-FRAENKEL set theory

Almost all mathematical notions can be defined set-theoretically. Georg Cantor the creator of set theory gave the following definition or description:

> Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten, wohlunterschiedenen Objekten m unsrer Anschauung oder unseres Denkens (welche die "Elemente" von M genannt werden) zu einem Ganzen.

Felix Hausdorff begins the *Grundzüge der Mengenlehre* with a concise description, which seems less dependent on human minds:

> Eine Menge ist eine Zusammenfassung von Dingen zu einem Ganzen, d.h. zu einem neuen Ding.

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 84. *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 85. *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* $\varphi(z, x_1, ..., x_n)$*:*

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

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

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

- v *is the image of* u *under the map defined by* φ*.*

i) *The* foundation schema (Found) *postulates for every* $\in$*-formula* $\varphi(x, x_1, ..., x_n)$*:*

$$\forall x_1 ... \forall x_n (\exists x \varphi(x, x_1, ..., x_n) \rightarrow \exists x (\varphi(x, x_1, ..., x_n) \wedge \forall x' (x' \in x \rightarrow \neg \varphi(x', x_1, ..., x_n))))$$

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

- $u \in \{x|\varphi\}$ *stands for* φ^u_x ;
- $u = \{x|\varphi\}$ *stands for* $\forall v\, (v \in u \leftrightarrow \varphi^v_x)$;
- $\{x|\varphi\} = u$ *stands for* $\forall v\, (\varphi^v_x \leftrightarrow v \in u)$;
- $\{x|\varphi\} = \{y|\psi\}$ *stands for* $\forall v\, (\varphi^v_x \leftrightarrow \psi^v_y)$;
- $\{x|\varphi\} \in u$ *stands for* $\exists v(v \in u \wedge v = \{x|\varphi\}$;
- $\{x|\varphi\} \in \{y|\psi\}$ *stands for* $\exists v(\psi^v_y \wedge v = \{x|\varphi\}$.

In this notation, the separation schema becomes:

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

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

Definition 87.

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 88.

a) $\emptyset \in V$.

b) $V \notin V$ *(*RUSSELL*'s antinomy).*

Proof. a) $\emptyset \in V$ abbreviates the formula

$$\exists v(v = v \wedge v = \emptyset).$$

This is equivalent to $\exists v\, v = \emptyset$ which again is an abbreviation for

$$\exists v\, \forall w\, (w \in v \leftrightarrow w \neq w).$$

This is equivalent to $\exists v \forall w\, w \notin v$ which is equivalent to the axiom of set existence. So $\emptyset \in V$ is another way to write the axiom of set existence.
b) Assume that $V \in V$. By the schema of separation

$$\exists y\, y = \{z|z \in V \wedge z \notin z\}.$$

Let $y = \{z | z \in V \wedge z \notin z\}$. Then

$$\forall z\ (z \in y \leftrightarrow z \in V \wedge z \notin z).$$

This is equivalent to

$$\forall z\ (z \in y \leftrightarrow z \notin z).$$

Instantiating the universal quantifier with y yields

$$y \in y \leftrightarrow y \notin y$$

which is a contradiction. □

We introduce further abbreviations. By a *term* we understand a class term or a variable, i.e., those terms which may occur in an extended $\in$-formula. We also introduce *bounded quantifiers* to simplify notation.

Definition 89. *Let A be a term. Then $\forall x \in A\, \varphi$ stands for $\forall x(x \in A \to \varphi)$ and $\exists x \in A\, \varphi$ stands for $\exists x\, (x \in A \wedge \varphi)$.*

Definition 90. *Let $x, y, z, \ldots$ be variables and $X, Y, Z, \ldots$ be class terms. Define*

a) $X \subseteq Y := \forall x \in X\ x \in Y$, *$X$ is a* subclass *of Y;*

b) $X \cup Y := \{x | x \in X \vee x \in Y\}$ *is the* union *of X and Y;*

c) $X \cap Y := \{x | x \in X \wedge x \in Y\}$ *is the* intersection *of X and Y;*

d) $X \setminus Y := \{x | x \in X \wedge x \notin Y\}$ *is the* difference *of X and Y;*

e) $\bigcup X := \{x | \exists y \in X\ x \in y\}$ *is the* union *of X;*

f) $\bigcap X := \{x | \forall y \in X\ x \in y\}$ *is the* intersection *of X;*

g) $\mathcal{P}(X) = \{x | x \subseteq X\}$ *is the* power class *of X;*

h) $\{X\} = \{x | x = X\}$ *is the* singleton set *of X;*

i) $\{X, Y\} = \{x | x = X \vee x = Y\}$ *is the* (unordered) pair *of X and Y;*

j) $\{X_0, \ldots, X_{n-1}\} = \{x | x = X_0 \vee \ldots \vee x = X_{n-1}\}$.

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

Proposition 91. $X \subseteq Y \wedge Y \subseteq X \to X = Y$.

Proposition 92. $\bigcup \{x, y\} = x \cup y$.

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 $u \in \bigcup \{x, y\}$. □

We can now reformulate the ZF axioms using class terms.

a) Extensionality: $\forall x \forall y\, (x \subseteq y \wedge y \subseteq x \to x = y)$.

b) Set existence: $\emptyset \in V$.

c) Separation schema: for all terms A with free variables $x_0, \ldots, x_{n-1}$

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

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 $x_0, \ldots, x_{n-1}$

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

21 Relations and functions

Ordered pairs are the basis for the theory of relations.

Definition 93. $(x, y) = \{\{x\}, \{x, y\}\}$ *is the* ordered pair *of* x *and* y.

Proposition 94. $(x, y) \in V$.
$(x, y) = (x', y') \to x = y \wedge x' = y'$.

Definition 95. *Let* A, B, R *be terms. Define*

a) $A \times B = \{z | \exists a \in A \exists b \in B \, z = (a, b)\}$ *is the* cartesian product *of* A *and* B.

b) R *is a* (binary) relation *if* $R \subseteq V \times V$.

c) If R *is a binary relation write* aRb *instead of* $(a, b) \in R$.

We can now introduce the usual notions for relations:

Definition 96.

a) $\mathrm{dom}(R) = \{x | \exists y \, (x, y) \in R\}$ *is the* domain *of* R.

b) $\mathrm{ran}(R) = \{y | \exists x \, (x, y) \in R\}$ *is the* range *of* R.

c) $R \restriction A = \{z | z \in R \wedge \exists x \exists y ((x, y) = z \wedge x \in A)\}$ *is the* restriction *of* R *to* A.

d) $R[A] = \{y | \exists x \in A \, xRy\}$ *is the* image *of* A *under* R.

e) $R^{-1} = \{z | \exists x \exists y \, (xRy \wedge z = (y, x))\}$ *is the* inverse *of* R.

f) $R^{-1}[B] = \{x | \exists y \in B \, xRy\}$ *is the* preimage *of* B *under* R.

One can prove the usual properties for these notions in ZF. 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 97. *Let* F, A, B *be terms. Then*

a) F *is a* function *if* $\forall x \forall y, y' (xFy \wedge xFy' \to y = y')$.

b) $F \colon A \to B$ *if* F *is a function* $\wedge \mathrm{dom}(F) = A \wedge \mathrm{ran}(F) \subseteq B$. *The sequence notions* $(F(x) | x \in A)$ *or* $(F(x))_{x \in A}$ *are just other ways to write* $F \colon A \to V$.

c) $F(x) = \{v | \exists y\,(xFy \wedge \forall y'\,(xFy' \to y = y') \to \exists y\,(xFy \wedge v \in y)\}$ *is the* value *of* F *at* x.

Note that if $F: A \to B$ 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 $\to F[x] \in V$.

22 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

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

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"
$$i < j < m \to i \in m.$$
This can be written with the $\in$-relation as
$$i \in j \in m \to i \in m,$$
a property termed *transitivity*.

Definition 98.

a) A *is* transitive, $\mathrm{Trans}(A)$, *iff* $\forall y \in A \forall x \in y\, x \in A$.

b) x *is an* ordinal (number), $\mathrm{Ord}(x)$, *if* $\mathrm{Trans}(x) \wedge \forall y \in x\, \mathrm{Trans}(y)$.

c) Let $\mathrm{Ord} = \{x | \mathrm{Ord}(x)\}$ *be the class of all ordinal numbers.*

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 99.

a) $0 \in \mathrm{Ord}$.

b) $\forall x \in \mathrm{Ord}\; x+1 \in \mathrm{Ord}$.

Proof. a) Trans($\emptyset$) since formulas of the form $\forall y \in \emptyset ...$ are tautologously true. Similarly $\forall y \in \emptyset\, \mathrm{Trans}(y)$.
b) Assume $x \in \mathrm{Ord}$.
(1) $\mathrm{Trans}(x+1)$.
Proof. Let $u \in v \in x+1 = x \cup \{x\}$.
Case 1. $v \in x$. Then $u \in x \subseteq x+1$, since x is transitive.
Case 2. $v = x$. Then $u \in x \subseteq x+1$. *qed*(1)
(2) $\forall y \in x+1\, \mathrm{Trans}(y)$.
Proof. Let $y \in x+1 = x \cup \{x\}$.
Case 1. $y \in x$. Then $\mathrm{Trans}(y)$ since x is an ordinal.
Case 2. $y = x$. Then $\mathrm{Trans}(y)$ since x is an ordinal. □

Definition 100. *Set* $1 = 0+1$, $2 = 1+1$, $3 = 2+1$, *etc.*

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

Theorem 101. *Let* $x \in \mathrm{Ord}$ *and* $y \in x$. *Then* $y \in \mathrm{Ord}$.

Proof. This follows immediately from the transitivity definition of Ord. □

Before we proceed in demonstrating that Ord satisfies further "number properties" we proof a convenient consequence of the foundation schema.

Lemma 102. *There is* no *finite sequence* $x_0, x_1, ..., x_n$ *which forms an* $\in$*-cycle with*

$$x_0 \in x_1 \in ... \in x_n \in x_0\,.$$

In particular $\forall x\, x \notin x$.

Proof. Assume that $x_0 \in x_1 \in ... \in x_n \in x_0$. Let $A = \{x_0, ..., x_n\}$. $A \neq \emptyset$ since $x_0 \in A$. By foundation, take $x \in A$ such that $x \cap A = \emptyset$.
Case 1. $x = x_0$. Then $x_n \in x \cap A \neq \emptyset$, contradiction.
Case 2. $x = x_i$ for some $1 \leqslant i \leqslant n$. Then $x_{i-1} \in x \cap A = \emptyset$, contradiction. □

Theorem 103. *The class* Ord *is strictly linearly ordered by* $\in$, *i.e.,*

a) $\forall x, y, z \in \mathrm{Ord}\, (x \in y \wedge y \in z \to x \in z)$.

b) $\forall x \in \mathrm{Ord}\, x \notin x$.

c) $\forall x, y \in \mathrm{Ord}\, (x \in y \vee x = y \vee y \in x)$.

Proof. a) Let $x, y, z \in \mathrm{Ord}$ and $x \in y \wedge y \in z$. Then z is transitive, and so $x \in z$.
b) by Lemma 102.
c) Assume that there are "incomparable" ordinals. By the foundation schema choose $x_0 \in \mathrm{Ord}$ $\in$-minimal such that $\exists y \in \mathrm{Ord}\, \neg(x_0 \in y \vee x_0 = y \vee y \in x_0)$. Again, choose $y_0 \in \mathrm{Ord}$ $\in$-minimal such that $\neg(x_0 \in y_0 \vee x_0 = y_0 \vee y_0 \in x_0)$. We obtain a contradiction by showing that $x_0 = y_0$:

Let $x \in x_0$. By the $\in$-minimality of x_0, x is comparable with y_0: $x \in y_0 \vee x = y_0 \vee y_0 \in x$. If $x = y_0$ then $y_0 \in x_0$ and x_0, y_0 would be comparable, contradiction. If $y_0 \in x$ then $y_0 \in x_0$ by the transitivity of x_0 and again x_0, y_0 would be comparable, contradiction. Hence $x \in y_0$.

For the converse let $y \in y_0$. By the $\in$-minimality of y_0 , y is comparable with x_0 : $y \in x_0 \vee y = x_0 \vee x_0 \in y$. If $y = x_0$ then $x_0 \in y_0$ and x_0, y_0 would be comparable, contradiction. If $x_0 \in y$ then $x_0 \in y_0$ by the transitivity of y_0 and again x_0, y_0 would be comparable, contradiction. Hence $y \in x_0$.

But then $x_0 = y_0$ contrary to the choice of y_0 . □

Definition 104. *Let* $<= \in \cap \mathrm{Ord} \times \mathrm{Ord} = \{(x, y) | x \in \mathrm{Ord} \wedge y \in \mathrm{Ord} \wedge x \in y\}$ *be the natural strict linear ordering of* Ord *by the* $\in$*-relation.*

Let us use small greek letters α, β, γ, ... as variables for ordinals. There are many parallels between the intuitive natural numbers and the ordinal numbers.

Lemma 105. *Let* $\alpha \in \mathrm{Ord}$. *Then* $\alpha + 1$ *is the immediate successor of* α *in the* $\in$*-relation:*

a) $\alpha < \alpha + 1$*;*

b) if $\beta < \alpha + 1$*, then* $\beta = \alpha$ *or* $\beta < \alpha$*.*

Lemma 106.

a) $\alpha + 1 \neq 0$ *;*

b) $\alpha + 1 = \beta + 1 \rightarrow \alpha = \beta$ *.*

Proof. *a)* $\alpha \in \alpha + 1$ whereas $\alpha \notin 0$. By extensionality, $\alpha + 1 \neq 0$.
b) Assume $\alpha + 1 = \beta + 1$ but $\alpha \neq \beta$. Then $\alpha < \beta + 1$ and by the previous Lemma $\alpha < \beta$. By symmetry we also get $\beta < \alpha$. But then $\alpha \in \beta \in \alpha$, contradicting Lemma 102. □

Theorem 107. (Burali-Forti) $\mathrm{Ord} \notin V$*, i.e., the class of ordinals is not a set.*

Proof. Assume that $\mathrm{Ord} \in V$. By Lemma 101, Trans(Ord). By the definition of ordinal number, $\forall x \in \mathrm{Ord}$ Trans(x). Thus Ord is an ordinal number and Ord $\in$ Ord. But this contradicts Lemma 102. □

This result was discovered by Cesare Burali-Forti and was seen as a paradox. Without the set/class distinction one wants to postulate the *set* of all ordinals which leads to a contradiction. On the other hand the result is very important since it expresses that there are "unboundedly" many ordinals, so that they can be used to "count" arbitrary sets.

22.1 Induction

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

Theorem 108. *Let* $\varphi(x, v_0, \ldots, v_{n-1}) \in L^{\in}$ *and* $x_0, \ldots, x_{n-1} \in V$*. Assume that the property* $\varphi(x, x_0, \ldots, x_{n-1})$ *is* inductive*, i.e.,*

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

Then φ *holds for all ordinals:*

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

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

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

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

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

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

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

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

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

Contradiction. □

22.2 Natural numbers

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

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

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

We will show that this is an adequate formalization.

Theorem 110.

a) $\omega \in V$.

b) $\omega \subseteq \mathrm{Ord}$.

c) $\omega \in \mathrm{Ord}$.

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

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

by the separation schema.
b) By a), $\omega \cap \mathrm{Ord} \in V$. Obviously $0 \in \omega \cap \mathrm{Ord} \wedge \forall u \in \omega \cap \mathrm{Ord}\ u + 1 \in \omega \cap \mathrm{Ord}$. So $\omega \cap \mathrm{Ord}$ is one factor of the intersection in the definition of ω and so $\omega \subseteq \omega \cap \mathrm{Ord}$. Hence $\omega \subseteq \mathrm{Ord}$.
c) By b), every element of ω is transitive and it suffices to show that ω is transitive. Let

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

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.,

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

□

Theorem 111. $(\omega, 0, +1)$ *satisfies the axioms of* second order PEANO axiom*, i.e.,*

a) $0 \in \omega$ *and* ω *is closed with respect to the* $+1$ *operation.*

b) $x + 1 \neq 0$ *;*

c) $x + 1 = y + 1 \to x = y$ *;*

d) $\forall x \subseteq \omega\, (0 \in x \wedge \forall u \in x\; u + 1 \in x \to x = \omega)$.

Proof. *a)* holds because ω is an intersection of sets with these closure properties. *b)* and *c)* follow from Lemma 106. For *d)* assume that $x \subseteq \omega$ such that $0 \in x \wedge \forall u \in x\; u + 1 \in x$. Then x is one of the factors in the intersection that defines ω. Hence $\omega \subseteq x$ and so $x = \omega$. □

22.3 Limit ordinals

We have seen that ω is an ordinal that is not a natural number. To study such numbers we define:

Definition 112. *Let* γ *be an ordinal.*

a) γ *is a* successor ordinal *if* $\gamma = \alpha + 1$ *for some* $\alpha \in \mathrm{Ord}$. *Let* $\mathrm{Succ} = \{\gamma \mid \gamma$ *is a successor ordinal*$\}$ *be the class of all successor ordinals.*

b) γ *is a* limit ordinal *if* $\gamma \neq 0$ *and* γ *is not a successor ordinal. Let* $\mathrm{Lim} = \{\gamma \mid \gamma$ *is a limit ordinal*$\}$.

Lemma 113. ω *is the smallest limit ordinal.*

Proof. Assume for a contradiction that ω was a successor ordinal, say $\omega = n + 1$. Then $n \in \omega$ and $n + 1 \in \omega$ since ω is closed under $+1$. But then $\omega \in \omega$, contradiction. Thus ω is a limit ordinal.

Assume that $\lambda < \omega$ is a smaller limit ordinal. If $u \in \lambda$ then $u + 1 \leqslant \lambda$ and so $u < \lambda$. Also $0 < \lambda$. But then λ was used in the intersection defining ω, and $\omega \subseteq \lambda$. This implies $\omega < \omega$, contracition. □

One can continue counting through the ordinals by defining

$$\begin{aligned} \omega + 2 &= (\omega + 1) + 1 \\ \omega + 3 &= (\omega + 2) + 1 \\ &\ldots \end{aligned}$$

so that the ordinals begin like

$$0, 1, 2, \ldots, \omega, \omega + 1, \omega + 2, \omega + 3, \ldots$$

Once we have introduced the principle of recursion, we shall see that there are many more limit ordinals above ω like the limit of the $\omega + n$.

22.4 Recursion

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

Theorem 114. *Let* $G : V \to V$*. Then there is a canonically defined class term* F *such that*

$$F : \mathrm{Ord} \to V \text{ and } \forall \alpha \in \mathrm{Ord}\; F(\alpha) = G(F \restriction \alpha).$$

We then say that F is defined by recursion *over the ordinals with the* recursion rule G. *Moreover, the function F is uniquely determined: if $F'\colon \mathrm{Ord} \to V$ with $\forall \alpha \in \mathrm{Ord}\ F'(\alpha) = G(F' \restriction \alpha)$ then $F = F'$.*

Proof. We begin by showing the compatibility of functions satisfying the recursion equation:
(1) Let F, F' be terms such that $\forall \alpha \in \mathrm{Ord} \cap \mathrm{dom}(F)\ \ F(\alpha) = G(F \restriction \alpha)$ and $\forall \alpha \in \mathrm{Ord} \cap \mathrm{dom}(F')\ F'(\alpha) = G(F' \restriction \alpha)$. Let $\alpha \in \mathrm{Ord}$ such that $\alpha + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F')$. Then $F(\alpha) = F'(\alpha)$.
Proof. By the induction theorem it suffices to show that the property

$$\alpha + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F') \to F(\alpha) = F'(\alpha)$$

is inductive, i.e.,

$\forall \alpha \in \mathrm{Ord}\ (\forall \beta \in \alpha\ \ (\beta + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F') \to F(\beta) = F'(\beta)) \to (\alpha + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F') \to F(\alpha) = F'(\alpha)))$.

So let $\alpha \in \mathrm{Ord}$ and $\forall \beta \in \alpha\ \ (\beta + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F') \to F(\beta) = F'(\beta))$. Let $\alpha + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F')$. For $\beta < \alpha$ we have $\beta + 1 \subseteq \mathrm{dom}(F) \cap \mathrm{dom}(F')$ and hence $F(\beta) = F'(\beta)$. Thus

$$F \restriction \alpha = F' \restriction \alpha.$$

By the recursion equation

$$F(\alpha) = G(F \restriction \alpha) = G(F' \restriction \alpha) = F'(\alpha).$$

qed(1)
Let

$$\tilde{F} = \{f \mid \exists \delta \in \mathrm{Ord}\ (f\colon \delta \to V \text{ and } \forall \alpha < \delta\ f(\alpha) = G(f \restriction \alpha)\}$$

be the class of all *approximations* to F. By (1), the elements of $\tilde{F}$ are pairwise compatible functions. Hence

$$F = \bigcup \{f \mid \exists \delta \in \mathrm{Ord}\ (f\colon \delta \to V \text{ and } \forall \alpha < \delta\ f(\alpha) = G(f \restriction \alpha)\}.$$

is a function defined on a subclass of the ordinals. We show that F also satisfies the recursion rule G where F is defined:
(2) $\forall \alpha \in \mathrm{dom}(F)\ (\alpha \subseteq \mathrm{dom}(F) \wedge F(\alpha) = G(F \restriction \alpha))$.
Proof. Let $\alpha \in \mathrm{dom}(F)$. Take some approximation $f \in \tilde{F}$ such that $\alpha \in \mathrm{dom}(f)$. Since $\mathrm{dom}(f)$ is an ordinal and transitive, we have

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

Moreover

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

qed(2)
It remains to show that $\mathrm{dom}(F) = \mathrm{Ord}$, i.e.,
(3) $\forall \alpha \in \mathrm{Ord}\ \alpha \in \mathrm{dom}(F)$.
Proof. By induction on the ordinals. We have to show that $\alpha \in \mathrm{dom}(F)$ is inductive in the variable α. So let $\alpha \in \mathrm{Ord}$ and $\forall \beta \in \alpha\ \beta \in \mathrm{dom}(F)$. Then $\alpha \subseteq \mathrm{dom}(F)$. Let

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

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

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

If $\alpha' = \alpha$ then

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

Hence $f \in \tilde{F}$ and $\alpha \in \mathrm{dom}(f) \subseteq \mathrm{dom}(F)$. *qed*(3)

The uniqueness of the function F follows from (1). □

There are various special cases of recursion in which the recursion rule G is determined in ways adequate for the application. Like in complete induction and recursion one often distinguishes 0-, successor and limit cases:

Theorem 115. *Let $G_0 \in V$, $G_{\mathrm{succ}}: V^2 \to V$, and $G_{\mathrm{lim}}: V \to V$. Then there is a canonically defined class term F such that*

$$F: \mathrm{Ord} \to V \text{ and } \forall \alpha \in \mathrm{Ord}\ F(\alpha) = \begin{cases} G_0, \text{ if } \alpha = 0 \\ G_{\mathrm{succ}}(F(\beta), \alpha), \text{ if } \alpha = \beta + 1 \\ G_{\mathrm{lim}}(F \restriction \alpha, \alpha), \text{ if } \alpha \in \mathrm{Lim} \end{cases}$$

We then say that F is defined by recursion *over the ordinals with the* recursion rules G_0, G_{succ}, *and* G_{lim}.

Proof. We have to combine the recursion rules G_0, G_{succ}, and G_{lim} into a single rule G: $V \to V$:

$$G(f) = \begin{cases} G_0, \text{ if } f = \emptyset \\ G_{\mathrm{succ}}(f(\beta), \alpha), \text{ if } \mathrm{Func}(f) \text{ and } \mathrm{dom}(f) = \alpha \\ G_{\mathrm{lim}}(f, \alpha), \text{ if } \mathrm{Func}(f) \text{ and } \mathrm{dom}(f) \in \mathrm{Lim} \\ 0, \text{ else} \end{cases}$$

Let $F: \mathrm{Ord} \to V$ be recursively defined by G. Then we have

for $\alpha = 0$: $F(0) = G(F \restriction 0) = G(\emptyset) = G_0$.

for $\alpha = \beta + 1$: $F(\alpha) = G(F \restriction \alpha) = G_{\mathrm{succ}}(F(\beta), \alpha)$.

for $\alpha \in \mathrm{Lim}$: $F(\alpha) = G(F \restriction \alpha) = G_{\mathrm{lim}}(F \restriction \alpha, \alpha)$. □

Note that class terms involved in recursion can also have extra parameters.

23 Ordinal arithmetic

We can now define arithmetical operations on the ordinals, using familiar recursive properties.

Definition 116. *Define the term* $\mathrm{add}(\delta, \alpha)$ *by ordinal recursion on the variable α (taking δ as a parameter) such that*

$$\mathrm{add}(\delta, \alpha) = \begin{cases} \delta, \text{ if } \alpha = 0 \\ \mathrm{add}(\delta, \beta) + 1, \text{ if } \alpha = \beta + 1 \\ \bigcup_{i<\alpha} \mathrm{add}(\delta, i), \text{ if } \alpha \in \mathrm{Lim} \end{cases}$$

$\mathrm{add}(\delta, \alpha)$ *is the* ordinal sum *of δ and α. We also write $\delta + \alpha$ instead of* $\mathrm{add}(\delta, \alpha)$. *Then the recursive equation can be written as*

$$\begin{aligned} \delta + 0 &= \delta \\ \delta + (\beta + 1) &= (\delta + \beta) + 1 \\ \delta + \alpha &= \bigcup_{i<\alpha} (\delta + i), \text{ if } \alpha \in \mathrm{Lim} \end{aligned}$$

One can show that ordinal addition satisfies several natural properties.

Proposition 117.

a) $\alpha+\beta\in\mathrm{Ord}$.

b) $\alpha+0=0+\alpha=\alpha$.

c) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$.

d) $\alpha,\beta\in\omega\to\alpha+\beta\in\omega$.

Proof. By induction. □

Note that ordinal addition is in general not commutative:

$$1+\omega=\bigcup_{n\in\omega}1+n=\omega\neq\omega+1$$

We have shown by the side that

Lemma 118. *There are limit ordinals* $>\omega$*:* $\omega+\omega\in\mathrm{Lim}$.

Proof. $\omega+\omega\in\mathrm{Ord}$ and $\omega+\omega>\omega$. Assume that

$$\beta<\omega+\omega=\bigcup_{n<\omega}\omega+n.$$

Let $\beta\in\omega+n_0$ for some $n_0\in\omega$. Then

$$\beta+1\in(\omega+n_0)+1=\omega+(n_0+1)\subseteq\bigcup_{n<\omega}\omega+n=\omega+\omega.$$

□

Definition 119. *Define the* ordinal product $\delta\cdot\alpha$ *of* δ *and* α *recursively:*

$$\begin{aligned}\delta\cdot 0 &= 0\\ \delta\cdot(\beta+1) &= (\delta\cdot\beta)+1\\ \delta\cdot\alpha &= \bigcup_{i<\alpha}(\delta\cdot i),\ \textit{if}\ \alpha\in\mathrm{Lim}\end{aligned}$$

Ordinal multiplication satisfies natural properties.

Proposition 120.

a) $\alpha\cdot\beta\in\mathrm{Ord}$.

b) $\alpha\cdot 0=0\cdot\alpha=0$.

c) $(\alpha\cdot\beta)\cdot\gamma=\alpha\cdot(\beta\cdot\gamma)$.

d) $\alpha\cdot(\beta+\gamma)=(\alpha\cdot\beta)+(\alpha\cdot\gamma)$.

e) $\alpha,\beta\in\omega\to\alpha\cdot\beta\in\omega$.

Proof. By induction. Let us prove *d)* by induction on γ. For $\gamma=0$

$$\alpha\cdot(\beta+0)=\alpha\cdot\beta=(\alpha\cdot\beta)+0=(\alpha\cdot\beta)+(\alpha\cdot 0).$$

For $\gamma=\delta+1$

$\alpha\cdot(\beta+(\delta+1))=\alpha\cdot((\beta+\delta)+1)=(\alpha\cdot(\beta+\delta))+\alpha=((\alpha\cdot\beta+\alpha\cdot\delta))+\alpha=(\alpha\cdot\beta)+((\alpha\cdot\delta)+\alpha)=(\alpha\cdot\beta)+(\alpha\cdot(\delta+1))$.

For $\gamma \in \mathrm{Lim}$

$$\alpha\cdot(\beta+\gamma)=\alpha\cdot\left(\bigcup_{i<\gamma}(\beta+i)\right)=\bigcup_{i<\gamma}(\alpha\cdot(\beta+i))=\bigcup_{i<\gamma}((\alpha\cdot\beta)+(\alpha\cdot i))=\bigcup_{j<\alpha\cdot\gamma}((\alpha\cdot\beta)+j)=$$

$(\alpha\cdot\beta)+(\alpha\cdot\gamma)$. □

Again, ordinal multiplication is not commutative:

$$2\cdot\omega=\bigcup_{n<\omega}2\cdot n=\omega\neq\omega+\omega=\omega\cdot 2.$$

Also "left-distributivity" does not hold:

$$(1+1)\cdot\omega=\bigcup_{n<\omega}((1+1)\cdot n)=\omega\neq\omega+\omega=(1\cdot\omega)+(1\cdot\omega).$$

Finally define ordinal exponentiation by

Definition 121. *Define the* ordinal power δ^α *of* δ *and* α *recursively:*

$$\begin{aligned}\delta^0 &= 1\\ \delta^{\beta+1} &= (\delta^\beta)\cdot\delta\\ \delta^\alpha &= \bigcup_{i<\alpha}\delta^i,\ \textit{if}\ \alpha\in\mathrm{Lim}\end{aligned}$$

Ordinal exponentiation satisfies natural properties.

Proposition 122.

a) $\alpha^\beta\in\mathrm{Ord}$.

b) $\alpha^0=1$, $\alpha^1=\alpha$, *and* $\alpha^2=\alpha\cdot\alpha$.

c) $(\alpha^\beta)^\gamma=\alpha^{\beta\cdot\gamma}$.

d) $\alpha^{\beta+\gamma}=(\alpha^\beta)\cdot(\alpha^\gamma)$.

e) $\alpha,\beta\in\omega\to\alpha^\beta\in\omega$.

24 Number systems

24.1 The structure $\mathbb{N}$

The arithmetical operations on $\mathbb{N}$ can be defined by restricting ordinal arithmetic to $\mathbb{N}$:

$$\mathbb{N}=(\omega,<,+,\cdot,0,1)$$

where $+=+\restriction(\omega\times\omega)$ and $\cdot=\cdot\restriction(\omega\times\omega)$. Then

Theorem 123. $\mathbb{N}$ *is a model of the first-order axiom system* PA *given in Definition 64. Hence* PA *is consistent.*

Note that we are proving the consistency of PA in the stronger system ZF so that we do not have a contradiction to Gödel's second incompleteness theorem.

Proof. It remains to check the schema of induction in $\mathbb{N}$:

for every formula $\varphi(x_0,\dots,x_{n-1},x_n)\in L^{S_{\mathrm{AR}}}$:

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

So let $\varphi(x_0,\dots,x_{n-1},x_n)\in L^{S_{\mathrm{AR}}}$ and $a_0,\dots,a_{n-1}\in\mathbb{N}$. Also assume that

$$\mathbb{N}\vDash\varphi(a_0,\dots,a_{n-1},0)\wedge\forall x_n(\varphi(a_0,\dots,a_{n-1},x_n)\to\varphi(a_0,\dots,x_{n-1},x_n+1)).$$

Define

$$X=\{u\in\mathbb{N}\mid\mathbb{N}\vDash\varphi(a_0,\dots,a_{n-1},u)\}\subseteq\mathbb{N}.$$

By assumption, $0\in X$ and $\forall u\in X\ u+1\in X$. Since $\mathbb{N}$ satisfies the second-order Peano axioms (see Theorem 111), $X=\mathbb{N}$. So

$$\mathbb{N}\vDash\forall x_n\,\varphi(a_0,\dots,a_{n-1},x_n).$$

□

The structure $\mathbb{N}=(\mathbb{N},<,+,\cdot,0,1)$ or indeed the structure $(\mathbb{N},+1,0)$ has a unique characterization up to isomorphism.

Theorem 124. *Let $N'=(N',S,Z)$ be a structure satisfying the axioms of second-order Peano arithmetic:*

a) $S(x)\neq Z$;

b) $S(x)=S(y)\to x=y$;

c) $\forall x\subseteq N'(Z\in x\wedge\forall u\in x\ S(u)\in x\to x=N')$.

Then $(\mathbb{N},+1,0)$ is isomorphic to (N',S,Z).

Proof. Define a map $h\colon\mathbb{N}\to N'$ by (complete) recursion:

$$\begin{aligned}h(0)&=Z\\h(n+1)&=S(h(n))\end{aligned}$$

(1) h is a homomorphism.
Proof. This is exactly expressed in the recursive definition of h. *qed*(1)
(2) h is injective.
Proof. Assume not. Let $n\in\mathbb{N}$ be minimal such that there is some $m\in\mathbb{N}$ such that $m\neq n$ and $h(m)=h(n)$.
Case 1. $n=0$. Then $m=l+1$ for some $l\in\mathbb{N}$.

$$S(h(l))=h(l+1)=h(m)=h(n)=h(0)=Z.$$

But this contradicts Peano axiom *a*).
Case 2. $n=k+1$ for some $k\in\mathbb{N}$. By the minimality of n we have $m>0$. Let $m=l+1$ for some $l\in\mathbb{N}$.

$$S(h(k))=h(k+1)=h(n)=h(m)=h(l+1)=S(h(l)).$$

By Peano axiom *b*) we get $h(k)=h(l)$. By the minimality of n we have that $k=l$. But then

$$m=l+1=k+1=n,$$

contradiction. *qed*(2)
(3) h is surjective.
Proof. Let $x=\mathrm{ran}(h)$. Then $Z=h(0)\in x$. If $u=h(n)\in x$ then

$$S(u)=S(h(n))=h(n+1)\in x.$$

By the Peano axiom c) we get $x = N'$. □

24.2 The structure $\mathbb{Q}_{\geqslant 0}$

(Non-negative) rational numbers are constructed as "quotients" of natural numbers. According to the laws of fractions, quotients like $\frac{1}{2}$ and $\frac{2}{4}$ can be identified. The identification proceeds via a canonical equivalence relation, hence rational numbers will be equivalence classes of quotients.

Definition 125. *A* quotient *is an ordered pair* (m, n) *where* $m \in \mathbb{N}$ *and* $n \in \mathbb{N} \setminus \{0\}$*;* $\mathbb{N} \times (\mathbb{N} \setminus \{0\})$ *is the set of all quotients. Define an equivalence relation* $\sim_{\mathbb{Q}}$ *on* $\mathbb{N} \times (\mathbb{N} \setminus \{0\})$ *by*

$$(m, n) \sim_{\mathbb{Q}} (m', n') \text{ iff } m \cdot n' = m' \cdot n.$$

For $(m, n) \in \mathbb{N} \times (\mathbb{N} \setminus \{0\})$ *let*

$$\frac{m}{n} = \{(m', n') \mid (m, n) \sim_{\mathbb{Q}} (m', n')\}$$

be the equivalence class of (m, n)*. Let*

$$\mathbb{Q}_{\geqslant 0} = \left\{ \frac{m}{n} \mid (m, n) \in \mathbb{N} \times (\mathbb{N} \setminus \{0\}) \right\}$$

be the set of non-negative rational numbers.

Define a binary addition operation $+_{\mathbb{Q}}$ *on* $\mathbb{Q}_{\geqslant 0}$ *by*

$$\frac{m}{n} +_{\mathbb{Q}} \frac{m'}{n'} = \frac{m \cdot n' + n \cdot m'}{n \cdot n'}.$$

Define a binary multiplication $\cdot_{\mathbb{Q}}$ *on* $\mathbb{Q}_{\geqslant 0}$ *by*

$$\frac{m}{n} \cdot_{\mathbb{Q}} \frac{m'}{n'} = \frac{m \cdot n'}{n \cdot n'}.$$

Define a relation $<_{\mathbb{Q}}$ *on* $\mathbb{Q}_{\geqslant 0}$ *by*

$$\frac{m}{n} <_{\mathbb{Q}} \frac{m'}{n'} \text{ iff } m \cdot n' < m' \cdot n.$$

Define a map $\pi \colon \mathbb{N} \to \mathbb{Q}_{\geqslant 0}$ *by*

$$\pi(n) = \frac{n}{1}.$$

***Lemma* 126.** *The preceding definition is correct, i.e.,*

a) $\sim_{\mathbb{Q}}$ *is an equivalence relation on* $\mathbb{N} \times (\mathbb{N} \setminus \{0\})$.

b) *Every rational* $\frac{m}{n}$ *is a set.*

c) $\mathbb{Q}_{\geqslant 0}$ *is a set.*

d) $+_{\mathbb{Q}}$ *and* $\cdot_{\mathbb{Q}}$ *are well-defined binary functions, and* $<_{\mathbb{Q}}$ *is a well-defined binary relation.*

e) $+_{\mathbb{Q}}$ *is associative and commutative on* $\mathbb{Q}_{\geqslant 0}$ *with neutral element* $\pi(0)$.

f) $\cdot_{\mathbb{Q}}$ *is a commutative group operation on* $\mathbb{Q}_{\geqslant 0} \setminus \{0\}$ *with neutral element* $\pi(1)$.

g) $<_{\mathbb{Q}}$ *is a strict linear order on* $\mathbb{Q}_{\geqslant 0}$.

h) The distributive law holds:

$$x \cdot_{\mathbb{Q}} (y +_{\mathbb{Q}} z) = x \cdot_{\mathbb{Q}} y +_{\mathbb{Q}} x \cdot_{\mathbb{Q}} z.$$

i) $\pi\colon (\mathbb{N}, <, +, \cdot, 0, 1) \to (\mathbb{Q}_{\geqslant 0}, <_{\mathbb{Q}}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, \pi(0), \pi(1))$ *is an embedding.*

Proof. *a)* $\sim_{\mathbb{Q}}$ is obviously reflexive and symmetric. For transitivity consider $(m,n) \sim_{\mathbb{Q}} (m', n')$ and $(m', n') \sim_{\mathbb{Q}} (m'', n'')$. Then

$$m \cdot n' = m' \cdot n \text{ and } m' \cdot n'' = m'' \cdot n'.$$

Then $m \cdot n' \cdot m' \cdot n'' = m' \cdot n \cdot m'' \cdot n'$, hence $m \cdot n'' = n \cdot m''$ and $(m,n) \sim_{\mathbb{Q}} (m'', n'')$.
b) $\mathbb{N} \times (\mathbb{N} \setminus \{0\})$ is a set, since V is closed under cartesian products. Then the equivalence class $\frac{m}{n} \subseteq \mathbb{N} \times (\mathbb{N} \setminus \{0\})$ is a set by separation.
c) Apply replacement to the function $(m,n) \mapsto \frac{m}{n}$. Then

$$\mathbb{Q}_{\geqslant 0} = \left\{ \frac{m}{n} \mid (m,n) \in \mathbb{N} \times (\mathbb{N} \setminus \{0\}) \right\}$$

is a set.
d) We have to show independence of representatives. Let $(a,b) \sim_{\mathbb{Q}} (a', b')$ and $(c,d) \sim_{\mathbb{Q}} (c', d')$. Then $a \cdot b' = a' \cdot b$ and $c \cdot d' = c' \cdot d$. This implies

$$(a \cdot d + c \cdot b) \cdot b' \cdot d' = a \cdot d \cdot b' \cdot d' + c \cdot b \cdot b' \cdot d' = a' \cdot d \cdot b \cdot d' + c' \cdot b \cdot b' \cdot d = (a' \cdot d' + c' \cdot b') \cdot b \cdot d$$

and

$$(a \cdot d + c \cdot b, b \cdot d) \sim (a' \cdot d' + c' \cdot b', b' \cdot d').$$

Also

$$a \cdot c \cdot b' \cdot d' = a' \cdot c \cdot b \cdot d' = a' \cdot c' \cdot b \cdot d$$

and

$$(a \cdot c, b \cdot d) \sim_{\mathbb{Q}} (a' \cdot c', b' \cdot d').$$

Finally

$$a\,d < c\,b \text{ iff } a\,d\,b'\,d' < c\,b\,b'\,d' \text{ iff } a'\,d\,b\,d' < c'\,b\,b'\,d \text{ iff } a'\,d' < c'\,b'$$

h)

$$\frac{a}{b}\left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b}\left(\frac{c\,f + e\,d}{d\,f}\right) = \frac{a\,(c\,f + e\,d)}{b\,d\,f} = \frac{a\,c\,f + a\,e\,d}{b\,d\,f} = \frac{a\,c\,b\,f + a\,e\,b\,d}{b\,d\,b\,f} = \frac{a\,c}{b\,d} + \frac{a\,e}{b\,f} = \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{e}{f}.$$

i) π is obviously injective. Now it suffices to see:

$$\pi(m+n) = \frac{m+n}{1} = \frac{m}{1} +_{\mathbb{Q}} \frac{n}{1} = \pi(m) +_{\mathbb{Q}} \pi(n)$$

and

$$\pi(m\,n) = \frac{m\,n}{1} = \frac{m}{1} \cdot_{\mathbb{Q}} \frac{n}{1} = \pi(m) \cdot_{\mathbb{Q}} \pi(n).$$

□

We can now identify the natural number n with the rational number $\frac{n}{1}$ and obtain

$$\mathbb{N} \subseteq \mathbb{Q}_{\geqslant 0}$$

and

$$<\restriction \mathbb{N}^2 = (<_{\mathbb{Q}}) \restriction \mathbb{N}^2 \text{ , } +\restriction \mathbb{N}^2 = (+_{\mathbb{Q}}) \restriction \mathbb{N}^2 \text{ , and } \cdot\restriction \mathbb{N}^2 = (\cdot_{\mathbb{Q}}) \restriction \mathbb{N}^2.$$

For simplicity we can now write n, $<$, $+$, and $\cdot$ instead of $\frac{n}{1}$, $<_{\mathbb{Q}}$, $+_{\mathbb{Q}}$, and $\cdot_{\mathbb{Q}}$.

24.3 The structure $\mathbb{R}_{\geqslant 0}$

(Non-negative) real numbers are constructed as (left halves of) Dedekind cuts in the (non-negative) rational numbers. If the cut determines a rational number, we require that that rational number is in the left-half of the cut.

Definition 127. *A non-negative* real (number) *is a subset $r \subseteq \mathbb{Q}_{\geqslant 0}$ such that*

a) $0 \in r$ *and* r *is* bounded*, i.e., there is a rational number $q \in \mathbb{Q}_{\geqslant 0}$ such that*

$$\forall p \in r\colon p < q;$$

b) r *is an* initial segment *of* $\mathbb{Q}_{\geqslant 0}$*, i.e.,*

$$\forall p \in r \forall p' \in \mathbb{Q}_{\geqslant 0}\colon p' < p \to p' \in r;$$

c) r *is* open above *0, i.e.,*

$$\forall p \in r \setminus \{0\}\, \exists p' \in r\colon p < p'.$$

Let

$$\mathbb{R}_{\geqslant 0} = \{r \subseteq \mathbb{Q}_{\geqslant 0} \mid r \text{ is a non-negative real}\}.$$

Define a binary addition operation $+_{\mathbb{R}}$ on $\mathbb{R}_{\geqslant 0}$ by

$$r +_{\mathbb{R}} r' = \{p + p' \mid p \in r, p' \in r'\}.$$

Define a binary multiplication $\cdot_{\mathbb{R}}$ on $\mathbb{R}_{\geqslant 0}$ by

$$r \cdot_{\mathbb{R}} r' = \{p \cdot p' \mid p \in r, p' \in r'\}.$$

Define a relation $<_{\mathbb{R}}$ on $\mathbb{R}_{\geqslant 0}$ by

$$r <_{\mathbb{R}} r' \text{ iff } r \subseteq r' \text{ and } r \neq r'.$$

Define a map $\pi'\colon \mathbb{Q}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ by $\pi'(0) = \{0\}$, and

$$\pi'(q) = \{p \in \mathbb{Q}_{\geqslant 0} \mid p < q\}$$

for $q \neq 0$.

Lemma 128. *The preceding definition is correct, i.e.,*

a) $\mathbb{R}_{\geqslant 0}$ *is a set.*

b) $+_{\mathbb{R}}$ *and* $\cdot_{\mathbb{R}}$ *are well-defined binary functions.*

c) $+_{\mathbb{R}}$ *is associative and commutative on* $\mathbb{R}_{\geqslant 0}$ *with neutral element* $\pi'(0)$*.*

d) $\cdot_{\mathbb{R}}$ *is a commutative group operation on* $\mathbb{Q}_{\geqslant 0} \setminus \{\{0\}\}$ *with neutral element* $\pi'(1)$*.*

e) $<_{\mathbb{Q}}$ *is a strict linear order on* $\mathbb{Q}_{\geqslant 0}$*.*

f) *The distributive law holds:*

$$x \cdot_{\mathbb{Q}} (y +_{\mathbb{Q}} z) = x \cdot_{\mathbb{Q}} y +_{\mathbb{Q}} x \cdot_{\mathbb{Q}} z.$$

g) $\pi'\colon (\mathbb{Q}_{\geqslant 0}, <, +, \cdot, 0, 1) \to (\mathbb{R}_{\geqslant 0}, <_{\mathbb{R}}, +_{\mathbb{R}}, \cdot_{\mathbb{R}}, \pi'(0), \pi'(1))$ *is an embedding.*

Proof. *a)* $\mathbb{R}_{\geqslant 0} \subseteq \mathcal{P}(\mathbb{Q}_{\geqslant 0})$ is a set by the powerset axiom and separation. □

By π' we can now identify the structure $\mathbb{Q}_{\geqslant 0}$ with a substructure of $\mathbb{R}_{\geqslant 0}$, and we can write q, $<$, $+$, and $\cdot$ instead of $\pi'(q)$, $<_{\mathbb{R}}$, $+_{\mathbb{R}}$, and $\cdot_{\mathbb{R}}$.

Dedekind cuts were introduced to obtain closure properties for certain irrational limit processes.

Definition 129. *Let $(L,<)$ be a strict linear order and $X \subseteq L$. Then*

a) $b \in L$ *is a* lower bound *of X if* $\forall x \in X\, b \leqslant x$.

b) $b \in L$ *is an* infimum *of X if b is a lower bound of X and for every lower bound b' of X we have $b' \leqslant b$.*

c) $b \in L$ *is an* upper bound *of X if* $\forall x \in X\, x \leqslant b$.

d) $b \in L$ *is a* supremum *of X if b is an upper bound of X and for every upper bound b' of X we have $b \leqslant b'$.*

Note that an infimum resp. supremum of X is uniquely determined if it exists.

Lemma 130. *Let $X \subseteq \mathbb{R}_{\geqslant 0}$ be non-empty and* bounded*, i.e, there is some $a \in \mathbb{R}_{\geqslant 0}$ such that*

$$\forall r \in X\, 0 \leqslant r < a.$$

Then the infimum and supremum of X both exist.

Proof. We show that

$$b = \bigcup X$$

is the supremum of X. The set $b \subseteq \mathbb{Q}_{\geqslant 0}$ is obviously bounded by a, and it is an initial segment of $\mathbb{Q}_{\geqslant 0}$ which is open above 0. So $b \in \mathbb{R}_{\geqslant 0}$. b is an upper bound for X since by construction $\forall r \in X\, r \leqslant b$. Assume that b' is another upper bound for X, i.e., $\forall r \in X\, r \leqslant b'$. Then $b = \bigcup X \subseteq b'$ and so $b \leqslant b'$. Hence b is the least upper bound of X.

For the infimum let $a' = \bigcap X$. a' is a bounded initial segment of $\mathbb{Q}_{\geqslant 0}$ with $0 \in a'$. If a' possesses a maximal element q then let $a = a' \setminus \{m\}$; otherwise set $a = a'$. It is easy to see that a is the infimum of X. □

Theorem 131. *Let $(\mathcal{R},\prec)$ be a strict linear order which densely contains $(\mathbb{Q}_{\geqslant 0},<)$ and which is complete with respect to suprema, i.e.,*

a) $(\mathbb{Q}_{\geqslant 0},<) \subseteq (\mathcal{R},\prec)$*;*

b) $\forall r \in \mathcal{R}\, \exists q \in \mathbb{Q}_{\geqslant 0}\, 0 \preccurlyeq r \prec q$*;*

c) $\forall r,s \in \mathcal{R}\, (r \prec s \to \exists q \in \mathbb{Q}_{\geqslant 0}\, r \prec q \prec s)$*;*

d) If $\emptyset \neq X \subseteq \mathcal{R}$ is bounded in $\mathcal{R}$, i.e., there is $r \in \mathcal{R}$ such that $\forall x \in X\, x \prec r$, then the supremum of X in $(\mathcal{R},\prec)$ exists.

Then under these hypotheses there is an isomorphism

$$\sigma\colon (\mathcal{R},\prec) \cong (\mathbb{R}_{\geqslant 0},<)$$

such that $\sigma \restriction \mathbb{Q}_{\geqslant 0} = \mathrm{id}$.

Proof. Define

$$\sigma\colon \mathcal{R} \to \mathbb{R}_{\geqslant 0}$$

by $\sigma \restriction \mathbb{Q}_{\geqslant 0} = \mathrm{id}$ and, for $r \in \mathcal{R} \setminus \mathbb{Q}_{\geqslant 0}$, by

$$\sigma(r) = \{q \in \mathbb{Q}_{\geqslant 0} \mid q \prec r\}.$$

It is straightforward to check that $\sigma(r) \in \mathbb{R}_{\geqslant 0}$.

(1) σ is order-preserving.

Proof. Let $r \prec s$. It suffices to check that case where $r, s \in \mathcal{R} \setminus \mathbb{Q}_{\geqslant 0}$. By hypothesis c) there is $q \in \mathbb{Q}_{\geqslant 0}$ such that $r \prec q \prec s$. Then $q \in \sigma(s) \setminus \sigma(r)$. So $\sigma(r) < \sigma(s)$. *qed*(1)

This implies immediately

(2) σ is injective.

(3) σ is surjective onto $\mathbb{R}_{\geqslant 0}$.

Proof. Let $r \in \mathbb{R}_{\geqslant 0} \setminus \mathbb{Q}_{\geqslant 0}$. Set $X = \{q \in \mathbb{Q}_{\geqslant 0} \mid q < r\}$. X is a non-empty bounded subset of $\mathcal{R}$. By the completeness assumption let r' be the supremum of X in $(\mathcal{R}, \prec)$. If $q \in \mathbb{Q}_{\geqslant 0}$ and $q < r$ then $q \prec r'$ since r' is an upper bound of X. Conversely if $q \prec r'$ then $q \in X$ and $q < r$. Hence

$$\sigma(r') = \{q \in \mathbb{Q}_{\geqslant 0} \mid q \prec r'\} = \{q \in \mathbb{Q}_{\geqslant 0} \mid q < r\} = r.$$

□

24.4 The structures $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$

The structures $\mathbb{N}$, $\mathbb{Q}_{\geqslant 0}$, and $\mathbb{R}_{\geqslant 0}$ are not closed under additive inverses. We complete $\mathbb{R}_{\geqslant 0}$ to the set of all real numbers and use this to also define $\mathbb{Z}$ and $\mathbb{Q}$. $\mathbb{R}$ is defined by formal *differences* from $\mathbb{R}_{\geqslant 0}$ like $\mathbb{Q}_{\geqslant 0}$ was defined by formal *quotients* from $\mathbb{N}$.

Definition 132. *A* difference *is an ordered pair (r, s) where $r, s \in \mathbb{R}_{\geqslant 0}$; $\mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0}$ is the set of all differences. Define an equivalence relation $\sim_{\mathbb{R}}$ on $\mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0}$ by*

$$(r, s) \sim_{\mathbb{R}} (r', s') \text{ iff } r + s' = r' + s.$$

For $(r, s) \in \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0}$ let

$$r - s = \{(r', s') \mid (r, s) \sim_{\mathbb{R}} (r', s')\}$$

be the $\sim_{\mathbb{R}}$equivalence class of (r, s). Let

$$\mathbb{R} = \{r - s \mid (r, s) \in \mathbb{R}_{\geqslant 0} \times \mathbb{R}_{\geqslant 0}\}$$

be the set of all real numbers.

Define a binary addition operation $+_{\mathbb{R}}$ on $\mathbb{R}$ by

$$(r - s) +_{\mathbb{R}} (r' - s') = (r + r') - (s + s').$$

Define a binary multiplication $\cdot_{\mathbb{R}}$ on $\mathbb{R}$ by

$$(r - s) \cdot_{\mathbb{R}} (r' - s') = (r\, r' + s\, s') - (r\, s' + r'\, s).$$

Define a relation $<_{\mathbb{R}}$ on $\mathbb{R}$ by

$$r - s <_{\mathbb{R}} r' - s' \text{ iff } r + s' < r' + s.$$

Define a map $\pi'' \colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ by

$$\pi''(r) = r - 0.$$

***Lemma* 133.** *The preceding definition is correct, i.e.,*

a) *$\sim_{\mathbb{R}}$ is an equivalence relation on $\mathbb{Q}^2_{\geqslant 0}$.*

b) *Every real number $r - s$ is a set.*

c) *$\mathbb{R}$ is a set.*

d) *$+_{\mathbb{R}}$ and $\cdot_{\mathbb{R}}$ are well-defined binary functions, and $<_{\mathbb{R}}$ is a well-defined binary relation.*

e) $+_{\mathbb{R}}$ *is a commutative group operation on* $\mathbb{R}$ *with neutral element* $\pi''(0)$.

f) $\cdot_{\mathbb{R}}$ *is a commutative group operation on* $\mathbb{R}\setminus\{0\}$ *with neutral element* $\pi''(1)$.

g) $<_{\mathbb{R}}$ *is a strict linear order on* $\mathbb{R}$.

h) The distributive law holds:

$$x\cdot_{\mathbb{R}}(y+_{\mathbb{R}}z)=x\cdot_{\mathbb{R}}y+_{\mathbb{R}}x\cdot_{\mathbb{R}}z.$$

i) $\pi\colon(\mathbb{R}_{\geqslant 0},<,+,\cdot,0,1)\to(\mathbb{R},<_{\mathbb{R}},+_{\mathbb{R}},\cdot_{\mathbb{R}},\pi''(0),\pi''(1))$ *is an embedding.*

j) For every real number $r-s$ *there is some* $t\in\mathbb{R}_{\geqslant 0}$ *such that*

$$r-s=t-0 \text{ or } r-s=0-t.$$

By i) one can identify $t-0\in\mathbb{R}$ *with* $t\in\mathbb{R}_{\geqslant 0}$. *For* $0-t\in\mathbb{R}$ *we simply write* $-t$.

Assuming that we have ensured that

$$\mathbb{N}\subseteq\mathbb{Q}_{\geqslant 0}\subseteq\mathbb{R}_{\geqslant 0}\subseteq\mathbb{R}$$

as substructures, we can now define

Definition 134.

a) The substructure $\mathbb{Z}\subseteq\mathbb{R}$ *of* integer numbers *is defined by* $\mathbb{Z}=\mathbb{N}\cup\{-n\mid n\in\mathbb{N}\}$.

b) The substructure $\mathbb{Q}\subseteq\mathbb{R}$ *of* rational numbers *is defined by* $\mathbb{Q}=\mathbb{Q}_{\geqslant 0}\cup\{-q\mid q\in\mathbb{Q}_{\geqslant 0}\}$.

On can show that the structure $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ can be characterized up to isomorphisms by 2nd-order properties.

24.5 On mathematical foundations

Mathematics is based on certain domains like numbers, functions, sets etc. with their basic properties. These domains have definite intuitive meanings and can be viewed as consisting of objects in space and time or in our (common) imagination. Despite intuitive insights, there has been a tendency since greek mathematics to express the basic properties exactly, in axiomatic form. This was partially necessitated by the wish for absolute exactness: the sum of angles in a triangle is *exactly* π and not just approximately; so what are the *exact* premisses for that result. Also one encountered unintuitive situations like in the beginnings of analysis where one uses the *infinite* to analyse situation in the finite.

Axiomatics in geometry led to questions of completeness and consistency of axioms. The consistency of mathematics as a whole appeared problematic, so that David Hilbert proposed a programme of proving the consistency of all of mathematics. This requires one unifying framework in which the standard mathematical domains can be explained. Set theory from its beginnings in the 19th century was used as an encompassing domain in which the other domains could be defined appropriately.

So how should we understand the formalization of domains like $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ within the theory ZF? Is the real number 3.1416 "really" a Dedekind cut, consisting of equivalence classes of ordered pairs of natural numbers? It is obviously better to "think" of real numbers as objects in their own right, which can be described categorically by some 1st and 2nd-order properties. Also it is natural to imagine that the number domains are included in each other as substructures:

$$\mathbb{N}\subseteq\mathbb{Z}\subseteq\mathbb{R}\subseteq\mathbb{C} \text{ and } \mathbb{N}\subseteq\mathrm{Ord}.$$

Sets form another domain, where e.g. $\mathbb{R} \in V$ but where $3.1416 \notin V$. This suggests a different but more "mathematical" setup of domains. Also the language of mathematics has a rich spectrum of notions to describe those domains in a comprehensive and varied system of axioms. The preceding constructions of number domains can be seen as providing a model for the mathematical axioms within ZF. We thus have a *relative* consistency result: if the axioms of ZF are consistent then the usual mathematical axiomatics is consistent.

In view of Gödel's second incompleteness theorem this is the best one can hope for. If one could prove the consistency of the usual axioms, this would include the axioms of ZF. Since ZF allows to carry out all mathematical proofs, ZF would prove its own consistency. But then, by Gödel's theorem, ZF would be *inconsistent*. So we have to *assume* the consistency of ZF as an empirical and intuitive fact and proceed from there.

25 Finite and infinite cardinalities

(Natural) numbers are mainly used to "count" the size of collections, i.e., sets. This leads to the notion of cardinal numbers.

Definition 135.

a) $\mathrm{card}(x) = \bigcap \{\alpha \mid \exists f\, (f: \alpha \to x \wedge f \text{ is surjective})\}$ *is the* cardinality *of* x.

b) $\kappa \in \mathrm{Ord}$ *is a* cardinal (number) *if* $\kappa = \mathrm{card}(x)$ *for some* $x \in V$; *let* $\mathrm{Card} = \{\mathrm{card}(x) \mid x \in V\}$ *be the class of all cardinals.*

c) x *is* finite *if* $\mathrm{card}(x) < \omega$.

d) x *is* infinite *if* $\mathrm{card}(x) \not< \omega$.

e) x *is* countable *if* $\mathrm{card}(x) \leqslant \omega$.

f) x *is* uncountable *if* x *is not countable.*

Lemma 136. *Let* $\kappa = \mathrm{card}(x)$. *Then there is a bijection* $\kappa \leftrightarrow x$.

Proof. Take a surjective $f: \kappa \to x$. Define $g: x \to \kappa$ by

$$g(z) = \text{ the smallest } \gamma \text{ such that } f(\gamma) = z.$$

Let $X = \mathrm{ran}(g) \subseteq \kappa$. Note that $f: X \to x$ is a bijection. Define $h: \kappa + 1 \to X \cup \{X\}$ recursively by

$$h(\alpha) = \begin{cases} \min\,(X \setminus \{h(\beta) \mid \beta < \alpha\}), \text{ if } X \setminus \{h(\beta) \mid \beta < \alpha\} \neq \emptyset \\ X, \text{ else} \end{cases}$$

One can show inductively:
(1) If $\beta < \alpha \leqslant \kappa$ and $h(\alpha) \neq X$ then $h(\beta) < h(\alpha)$ and $\alpha \leqslant h(\alpha)$.
(2) There is $\lambda \leqslant \kappa$ such that $h(\lambda) = X$.
Proof. Otherwise, by (1), $h(\kappa) \geqslant \kappa$. But by the definition of h, $h(\kappa) \in X \subseteq \kappa$ and $h(\kappa) < \kappa$. Contradiction. *qed*(2)

So assume that $\lambda \leqslant \kappa$ is the minimal ordinal such that $h(\lambda) = X$.
(3) $h \restriction \lambda: \lambda \leftrightarrow X$.
Proof. $h \restriction \lambda$ is injective by (1). Since $h(\lambda) = X$, we have $X \setminus \{h(\beta) \mid \beta < \lambda\} = \emptyset$ and so $X = \mathrm{ran}(h \restriction \lambda)$. So $h \restriction \lambda$ is bijective. *qed*(3)

$f \circ (h \restriction \lambda): \lambda \to x$ is a bijection. By the minimality of $\kappa = \mathrm{card}(x)$ we get $\lambda = \kappa$. □

So $\mathrm{card}(x)$ allows to enumerates x by a bijection.

Theorem 137.

a) $\forall n < \omega\ \mathrm{card}(n) = n$; *hence* $\forall n < \omega\ n \in \mathrm{Card}$.

b) $\mathrm{card}(\omega) = \omega$ *and so* $\omega \in \mathrm{Card}$.

c) $\mathrm{card}(\omega + 1) = \omega$.

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

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

$n = m + 1$, and assume that $\mathrm{card}(m) = m$. Assume for a contradiction that $\mathrm{card}(n) \leqslant m$. Take $f : m \to n$ surjective. Then $m \neq 0$ and we can take l such that $m = l + 1$.
Case 1. $f(l) = m$. Then $f \restriction l : l \to m$ is surjective and $\mathrm{card}(m) \leqslant l < m$. Contradiction.
Case 2. $f(l) < m$. Then define $f' : l \to m$ by

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

Then $f' : l \to m$ is surjective and $\mathrm{card}(m) \leqslant l < m$. Contradiction.
b) Obviously $\mathrm{card}(\omega) \leqslant \omega$. Assume for a contradiction that $n = \mathrm{card}(\omega) < \omega$. Then there is a surjection from n onto ω. This implies the existence of a surjection from n onto $n + 1$. Then $\mathrm{card}(n + 1) \leqslant n$ contradicting a).
c) Define $f : \omega \to \omega + 1$ by

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

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

By *c)* the infinite has paradoxical properties.

Lemma 138.

a) Let a, b *be finite sets. Then* $a \cup b$, $a \times b$, *and* $\mathcal{P}(a)$ *are finite.*

b) Let x, y *be countable sets. Then* $x \cup y$ *and* $x \times y$ *are countable.*

Proof. By constructing certain surjections. We only consider *b)*. Let $f : \omega \to x$ and $g : \omega \to y$ be surjective. Define a surjection $h : \omega \to x \cup y$ by

$$h(n) = \begin{cases} f(i), \text{ if } n = 2\,i \\ g(i), \text{ if } n = 2i + 1 \end{cases}$$

Define a surjection $h' : \omega \to x \times y$ by

$$h'(n) = \begin{cases} (f(i), g(j)), \text{ if } n = 2^i \cdot 3^j \\ (f(0), g(0)), \text{ else} \end{cases}$$

□

However:

Theorem 139. *(Cantor) The set* $\mathcal{P}(\omega)$ *is uncountable.*

Proof. Assume instead that $\mathrm{card}(\mathcal{P}(\omega)) \leqslant \omega$ and let $f : \omega \to \mathcal{P}(\omega)$ be surjective. Define

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

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. □

Let us generalize the argument to arbitrary cardinals.

Theorem 140. *Let α be an ordinal. Then there is no surjection from α onto $\mathcal{P}(\alpha)$.*

Proof. Assume instead that $f\colon \alpha \to \mathcal{P}(\alpha)$ were surjective. Define

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

Since f is surjective, take $\nu_0 < \alpha$ such that $a = f(\nu_0)$. Then

$$\nu_0 \in a \leftrightarrow \nu_0 \notin f(\nu_0) = a\,.$$

Contradiction. □

26 The axiom of choice

Consider the following commonly used proposition:

Lemma 141. *Assume* AC*. A countable union of countable sets is countable: let $(a_n)_{n<\omega}$ be a sequence of countable sets. Then $\bigcup_{n<\omega} a_n$ is countable.*

Proof. (1st attempt)We may assume without loss of generality that all a_n are nonempty. For $n \in \omega$ "choose" a surjection $f_n\colon \omega \to a_n$. Then define a surjection $h\colon \omega \to \bigcup_{n<\omega} a_n$ by

$$h(k) = \begin{cases} f_n(i), \text{ if } k = 2^n \cdot 3^i \\ f_0(0), \text{ else} \end{cases}$$ □

This argument is not complete. How should the "choices" of f_n be carried out? We cannot make these choices in some temporal succession. In a standard first-order proof, they have to be made instantaneouly at one step of the proof. Many arguments in infinitary mathematics depend on the possibility of making infinitely many assignments or choices: choices of sequences in analysis, choices of basis vectors in vector spaces, etc.. 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.

Definition 142. *The* axiom of choice*,* AC*, is the following statement:*

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

This says that the set x, consisting of pairwise disjoint non-empty elements possesses a choice set z which "chooses" exactly one element from each member of x.

Definition 143. *The axiom system* ZFC (Zermelo-Fraenkel with choice) *consists of the axiom of* ZF *together with the axiom of choice.*

The system ZFC is the usual foundational axiom system for mathematics. We are able to prove the above lemma:

Lemma 144. *Assume* AC. *A countable union of countable sets is countable: let* $(a_n)_{n<\omega}$ *be a sequence of countable sets. Then* $\bigcup_{n<\omega} a_n$ *is countable.*

Proof. We may assume without loss of generality that all a_n are nonempty. For $n \in \omega$ let

$$F_n = \{ f \mid f : \omega \to a_n \text{ is surjective} \} \neq \emptyset.$$

Each $F_n \subseteq \mathcal{P}(\omega \times a_n)$ is a set by the powerset axiom.

To choose surjections f_n from the F_n let

$$x = \{ \{n\} \times F_n \mid n < \omega \}.$$

x is a set by replacement. The elements $\{n\} \times F_n$ of x are nonempty and pairwise disjoint. By the axiom of choice take a set z such that for all $n < \omega$, the intersection

$$(\{n\} \times F_n) \cap z$$

contains just a single element (n, f_n). Hence $f : \omega \to V$ given by $n \mapsto f_n$ is a *choice function* which "chooses" $f_n \in F_n$ for all $n < \omega$.

We can now define a surjection $h : \omega \to \bigcup_{n<\omega} a_n$ by

$$h(k) = \begin{cases} f_n(i), \text{ if } k = 2^n \cdot 3^i \\ f_0(0), \text{ else} \end{cases}$$

□

One can show that one cannot prove this lemma in ZF alone - unless ZF is inconsistent.

26.1 Zorn's lemma

The most popular choice principle is ZORN's lemma which we already used in the proof of the general completeness theorem.

Definition 145. *Let* $(Z, \leqslant)$ *be a partial order. A* chain *in* Z *is a subset* $C \subseteq Z$ *such that*

$$\forall x, y \in C \, (x \leqslant y \vee y \leqslant x).$$

$u \in Z$ *is an* upper bound *of* Z *if*

$$\forall x \in C \, x \leqslant u.$$

$(Z, \leqslant)$ *is* inductive *if every chain in* Z *has an upper bound.*

$a \in Z$ *is a* maximal element *of* $(Z, \leqslant)$ *if*

$$\neg \exists x \in Z \, a < x.$$

The lemma of Zorn *is the statement "every inductive partial order which is a set has a maximal element".*

To prepare the proof of Zorn's lemma, we show another choice principle.

Lemma 146. *Assume* AC. *Let* x *be a set. Then there is a* choice function $f : x \setminus \{\emptyset\} \to \bigcup x$ *for* x*, i.e.,*

$$\forall u \in x \setminus \{\emptyset\} \, f(u) \in u.$$

Proof. Define $x' = \{ \{u\} \times u \mid u \in x, u \neq \emptyset \}$. x' is a set consisting of non-empty pairwise disjoint elements. By AC take a set z such that for all $u \in x, u \neq \emptyset$, the intersection

$$(\{u\} \times u) \cap z$$

is a singleton set $\{(u, f(u))\}$. Then f is a choice function for x. □

Theorem 147. AC *implies the lemma of* Zorn.

Proof. Let $(Z, \leqslant)$, $Z \in V$ be an inductive partial order. Let f be a choice function for $\mathcal{P}(Z)$. Define a function $h\colon \mathrm{Ord} \to Z \cup \{Z\}$ recursively:

$$h(\alpha) = \begin{cases} f(\{u \in Z \mid u \text{ is an upper bound for } \{h(\beta) | \beta < \alpha\} \text{ and } u \notin \{h(\beta) | \beta < \alpha\}\}), \text{ if this exists} \\ Z, \text{ else.} \end{cases}$$

By definition,
(1) If $\alpha < \beta$ and $h(\beta) \neq Z$ then $h(\alpha) < h(\beta) \in Z$.
(2) There exists $\lambda \in \mathrm{Ord}$ such that $h(\lambda) = Z$.
Proof. If not, then $h\colon \mathrm{Ord} \to Z$ would be an injection, contradiction. *qed*(2)
Let $\lambda \in \mathrm{Ord}$ be minimal such that $h(\lambda) = Z$.
(3) λ is a successor ordinal.
Proof. $h(0) \neq Z$: $\emptyset$ is a (trivial) chain in Z. Since Z is inductive, $\emptyset$ has an upper bound u in Z. Hence the set of upper bounds in the definition of $h(0)$ is non/empty and f chooses one such $u \in Z$.

Assume that λ were a limit ordinal. $\{h(\beta) | \beta < \lambda\}$ is a chain in Z. By inductivity it has an upper bound u. Since $(h(\beta) | \beta < \lambda)$ is strictly increasing in the partial order, $u \notin \{h(\beta) | \beta < \lambda\}$. Therefore $h(\lambda)$ is defined by an application of the choice function and $h(\lambda) \neq Z$. Contradiction. *qed*(3)

So let $\lambda = \kappa + 1$. $\{h(\beta) | \beta \leqslant \kappa\}$ is a strictly increasing chain in Z.
(4) $h(\kappa)$ is a maximal element of Z.
Proof. Assume not. Take some $u \in Z$ such that $h(\kappa) < u$. Then u is an upper bound of $\{h(\beta) | \beta \leqslant \kappa\}$ with $u \notin \{h(\beta) | \beta \leqslant \kappa\}$. But then $h(\lambda) \in Z$ would be defined, contradicting $h(\lambda) = Z$. □

Let us apply a similar argument to the study of cardinals.

Theorem 148. *Assume* AC. *Then* $\mathrm{card}(x) \in \mathrm{Ord}$ *for every* $x \in V$.

Proof. Let $x \in V$. Let f be a choice function for $\mathcal{P}(x)$. Define a function $h\colon \mathrm{Ord} \to x \cup \{x\}$ recursively:

$$h(\alpha) = \begin{cases} f(x \setminus \{h(\beta) | \beta < \alpha\}), \text{ if this exists,} \\ x, \text{ else.} \end{cases}$$

By definition,
(1) If $\alpha < \beta$ and $h(\beta) \neq x$ then $h(\alpha) \neq h(\beta) \in x$.
(2) There exists $\lambda \in \mathrm{Ord}$ such that $h(\lambda) = x$.
Proof. If not, then $h\colon \mathrm{Ord} \to x$ would be an injection, contradiction. *qed*(2)
Let $\lambda \in \mathrm{Ord}$ be minimal such that $h(\lambda) = x$. By the definition of h,

$$x \setminus \{h(\beta) | \beta < \lambda\} = \emptyset.$$

Hence $h \restriction \lambda\colon \lambda \to x$ is surjective, and $\mathrm{card}(x) \leqslant \lambda \in \mathrm{Ord}$. □

Theorem 149. *Assume* AC. *Let* κ *be a cardinal. Then there is a cardinal* $\lambda > \kappa$. *Let* κ^+ *be the least cardinal* $> \kappa$.

Proof. Let $\lambda = \mathrm{card}(\mathcal{P}(\kappa))$. If $\lambda \leqslant \kappa$. Then there is a surjection from κ onto $\mathcal{P}(\kappa)$ which is impossible. Hence $\lambda > \kappa$. □

Now we can define, in the system ZFC, the sequence of Alef's:

Definition 150. *Define recursively:*

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\alpha+1} &= \aleph_\alpha^+ \\ \aleph_\lambda &= \bigcup_{\alpha<\lambda} \aleph_\alpha \text{ , for limit ordinals } \lambda \end{aligned}$$

So there is a proper class of infinite cardinals. One can naturally define an arithmetic on cardinals.

Definition 151. *For* $\kappa, \lambda \in \mathrm{Card}$ *define*

a) the cardinal sum $\kappa + \lambda = \mathrm{card}((\{0\} \times \kappa) \cup (\{1\} \times \lambda))$*;*

b) the cardinal product $\kappa \cdot \lambda = \mathrm{card}(\kappa \times \lambda)$*;*

c) the cardinal power $\kappa^\lambda = \mathrm{card}(\{f \mid f\colon \lambda \to \kappa\})$.

Cardinal arithmetic shows unusual properties:

Theorem 152. *For* $\alpha, \beta \in \mathrm{Ord}$

$$\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max(\aleph_\alpha, \aleph_\beta).$$

On the other hand, already the value of $2^{\aleph_0}$ is not determined. Georg Cantor make the following conjecture:

Definition 153. Cantor's Continuum Hypothesis (CH) is the statement

$$2^{\aleph_0} = \aleph_1 .$$

This was generalized by Felix Hausdorff:

Definition 154. Hausdorff's Generalized Continuum Hypothesis (GCH) is the statement

$$\forall \alpha \; 2^{\aleph_\alpha} = \aleph_{\alpha+1} .$$

Axiomatic set theory has shown, that these hypotheses are independent of the ZFC axioms of set theory. If the axiom system ZFC is consistent, then so are the system ZFC+GCH and the system ZFC+$2^{\aleph_0} \neq \aleph_1$. So the simplest question about infinitary cardinal exponentiation cannot be resolved in the standard axioms.

Luckily such independencies seldomly affect usual mathematical questions. The axioms of ZFC are strong enough to decide most mathematical questions. If a proof does not yet exist this is in most cases due to the difficulty of finding a proof or disproof, but not to incompleteness.

So in ZFC together with 1st-order logic we are in a comfortable situation: ZFC is sufficient for all but a tiny minority of problems; at the fringes, axiomatic set theory exhibits exotic possibilities for the behaviour of infinities.

Index