Logik MN2

Anton Setzer

December 18, 1997

Contents

Chapter 0

Preliminaries

0.1 Preface

The following notes are course notes of a course LogikMN2 held at the Department of Mathematics, Uppsala University, October - December 1997.

Content of the Course We cite here from the course handbook [UU97]. The course is based on LogikMN1, which has the following content (English translation by the author):
Propositional logic: Truth, proof, completeness. Predicate logic: structure, semantic, proof, natural deduction, completeness. Introduction to model theory. orientation about incompleteness theorems, mathematical foundations (?, Swedish: matematikens grundvalar) and intuitionistic logic.
Literature for this course was van Dalen's book [vD94].
The content of the course LogikMN2 itself according to [UU97] is:
Gödel's incompleteness theorem. Recursion theory: recursive functions, second recursion theorem, universal functions, S-m-n-theorem, Rice's theorem, recursive enumerable sets, theorem of Rice and Shapiro, recursive inseparable sets, arithmetical hierarchy. Relative computability.
Selected topics from set theory: well-ordering, ordinals, cardinals, transfinite induction, equivalent formulations of the axiom of choice, continuum hypothesis.
Model theory: isomorphism, substructure, elementary equivalence, elementary substructure, compactness theorem, theorem of Löwenheim-Skolem, complete theories, categoricity. Nonstandard arithmetic and analysis. Tennenbaum's theorem.
Literature for the course was: [Men87] and for additional reading: [Cra91], [Cut80], [vD94] and [Sho67].

The plan for this lecture given in the first lecture was:

1. Model theory I Use of the completeness theorem, nonstandard structures.

2. Recursion theory I. Exploration of what "computable" means.

3. 1. Gödel's Incompleteness theorem

4. Representability and recursion theory II. Recursion theorem. Non recursive sets.

5. 2. Gödel's Incompleteness theorem "There is no 100% security in mathematics".

6. Set theory. The inconsistency of naïve set theory and how to define a system which is (hopefully) consistent. Ordinals, cardinals.

7. Model theory and higher cardinalities. If time permits. Incompleteness theorem for uncountable languages. κ-categoricity.

The material in 1 - 6 was actually covered, from 7. only κ-categoricity was mentioned in the appendix (chapter 10).

Sources The major source for this notes are the lecture notes by Buchholz, [Buc89], [Buc93a],[Buc93b] and [Buc97a], unbeatable in their technical precision and shortness. Large parts are translations of his notes.

Status Currently these notes are in the state as they were typed during the teaching period. Mistakes found during teaching and in the immediate revision afterwards have been corrected, but the author didn't have time yet to do a major proof check, which would be necessary in order to guarantee accuracy. Therefore the reader should be aware that there might be inaccuracies, typos, mistakes. The author appreciates very much hints about mistakes and inaccuracies.

0.2 Remarks for future versions of these course notes

We have made some decisions, some of them turned out not to be as good as we thought. Since we want to hand out these notes to the students, in the current version we are very close to the version taught and therefore haven't changed this. However we want to note here, what should be in later versions modified:

- We didn't choose equality to be part of the logic and therefore $=$ was in structures by definition not supposed to be interpreted standard. We regretted this choice very much, because practically in all theorems we had to add the statement: this holds if $=$ is interpreted standard (we might have overlooked some statements, where this has to be added).
- To introduce partial functions $f : A \to_{\mathrm{par}} B$ as strict functions $A_\perp \to B_\perp$, where $A_\perp := A \cup \{\perp\}$, would have been more natural.
- In the part of recursion theory it would have been better to introduce functions $\wedge, \vee, \ldots : \mathbb{N}^2 \to \mathbb{N}$ etc., which act as the boolean valued functions on $\{0, 1\}$ instead of simulating them with $+$ and $\cdot$.

- We defined Δ_0 formulas only as formulas with connectives $\rightarrow$, $\neg$, $\forall$ (no $\wedge$, $\vee$, $\exists$), and showed that they are essentially closed under $\wedge$, $\vee$, $\exists$. This didn't save us much time and was didactically not wise.

0.3 Notations

Since we are used to it and since it is easier to distinguish it from ordinary letters in handwriting, we will sometimes write symbols in (capital) Sütterlin letters. Only a few of them will be actually used. In print they will be represented by calligraphic letters. The transcription is as follows:

$\mathcal{A}$	$\mathfrak{A}$	$\mathcal{E}$	$\mathfrak{E}$	$\mathcal{I}$	$\mathfrak{I}$	$\mathcal{M}$	$\mathfrak{M}$	$\mathcal{P}$	$\mathfrak{P}$	$\mathcal{U}$	$\mathfrak{U}$	$\mathcal{X}$	$\mathfrak{X}$
$\mathcal{B}$	$\mathfrak{B}$	$\mathcal{F}$	$\mathfrak{F}$	$\mathcal{J}$	$\mathfrak{J}$	$\mathcal{N}$	$\mathfrak{N}$	$\mathcal{Q}$	$\mathfrak{Q}$	$\mathcal{V}$	$\mathfrak{V}$	$\mathcal{Y}$	$\mathfrak{Y}$
$\mathcal{C}$	$\mathfrak{C}$	$\mathcal{G}$	$\mathfrak{G}$	$\mathcal{K}$	$\mathfrak{K}$	$\mathcal{O}$	$\mathfrak{O}$	$\mathcal{R}$	$\mathfrak{R}$	$\mathcal{W}$	$\mathfrak{W}$	$\mathcal{Z}$	$\mathfrak{Z}$
$\mathcal{D}$	$\mathfrak{D}$	$\mathcal{H}$	$\mathfrak{H}$	$\mathcal{L}$	$\mathfrak{L}$	$\mathcal{P}$	$\mathfrak{P}$	$\mathcal{S}$	$\mathfrak{S}$	$\mathcal{X}$	$\mathfrak{X}$		

Quantification will be written in the form $\forall x(\phi)$, $\exists x(\phi)$, where the scope of the quantifier is what is within parenthesis. We omit the parenthesis if there is no confusion and write usually in this case $\forall x.\phi$, $\exists x.\phi$.
$\wedge$ and $\vee$ bind more than $\rightarrow$, for instance $5 = 10 \wedge 3 = 5 \rightarrow 2 = 7 \vee 9 = 9$ should be read as $(5 = 10 \wedge 3 = 5) \rightarrow (2 = 7 \vee 9 = 9)$.
We will write expressions like $\phi(x, y, z)$. Once we have used it, $\phi(r, s, t)$ means $\phi[x := r, y := s, z := t]$ where we assume that r, s, t are substitutable for x, y, z (which can always be achieved after renaming of bounded variables).
$\exists! x.\phi(x) := \exists x.(\phi(x)) \wedge \forall y, y'(\phi(y) \wedge \phi(y') \rightarrow y = y')$.

0.4 Equality

Definition 0.1 (a) If $\mathcal{L}$ is a language, then the equality axioms for $\mathcal{L}$ are

- $\forall x.x = x$.
- $\forall x, y(x = y \rightarrow y = x)$.
- $\forall x, y, z(x = y \wedge y = z \rightarrow x = z)$.
- $\forall x_1, \ldots, x_n.\forall y_1, \ldots, y_n.(x_1 = y_1 \wedge \cdots x_n = y_n \rightarrow f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n))$, f an n-ary function symbol of $\mathcal{L}$.
- $\forall x_1, \ldots, x_n \forall y_1, \ldots, y_n.(x_1 = y_1 \wedge \cdots x_n = y_n \rightarrow R(x_1, \ldots, x_n) \rightarrow R(y_1, \ldots, y_n))$, R an n-ary relation symbol of $\mathcal{L}$ which is not $=$.

(b) A theory with equality is a theory containing the equality axioms.

Lemma 0.2 *From the equality axioms for a language $\mathcal{L}$ follows*

- *If $t(y_1, \ldots, y_n)$ is a term (in $\mathcal{L}$), $\mathrm{FV}(t(y_1, \ldots, y_n)) \subseteq \{y_1, \ldots, y_n\}$, x_i, x'_i are distinct, then*

$$\begin{aligned}\forall x_1, \ldots, x_n, x'_1, \ldots, x'_n.\quad & x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n \\ & \rightarrow t(x_1, \ldots, x_n) = t(x'_1, \ldots, x'_n)\ .\end{aligned}$$

- *If* $A(y_1, \ldots, y_n)$ *is a formula (of* $\mathcal{L}$*),* $\mathrm{FV}(A(y_1, \ldots, y_n)) \subseteq \{y_1, \ldots, y_n\}$, x_i, x'_i *are distinct, then*

$$\forall x_1, \ldots, x_n, x'_1, \ldots, x'_n. \quad \begin{array}{l} x_1 = x'_1 \wedge \cdots \wedge x_n = x'_n \\ \to A(x_1, \ldots, x_n) \to A(x'_1, \ldots, x'_n) \ . \end{array}$$

Proof: Easy induction.

Chapter 1

Model theory

1.1 Structures and Models

We will follow in this chapter very closely [Buc97a], chapter 1 and 3.
In the following we will assume the completeness theorem for arbitrary (not only countable) languages. (Originally we planned to prove it, if possible, in a section Model theory II, but it turned out, that it wasn't possible.

Definition 1.1 (a) $\mathbb{B} := \{0, 1\}$. max and min will be considered with respect to the ordering $0 < 1$.

(b) Let $\mathcal{L}$ be language, i.e. a collection of function symbols f and relation symbols R together with the arities $\text{arity}(f)$ and $\text{arity}(R)$.
We assume here that formulas are built from prime formulas and $\perp$ using the connectives $\wedge$, $\vee$ and $\neg$.
A structure to $\mathcal{L}$ is a pair $\mathcal{M} = (M, (p^{\mathcal{M}})_{p \in \mathcal{L}})$, where M is a not empty set, called *domain* of the interpretation, and a family $(p^{\mathcal{M}})_{p \in \mathcal{L}}$ where

(i) $p^{\mathcal{M}} : M^n \to \mathbb{B}$ if p is an n-ary relation symbol;

(ii) $p^{\mathcal{M}} : M^n \to M$ if p is an n-ary function symbol, $n \geq 1$;

(iii) $p^{\mathcal{M}} \in M$ if p is an constant (i.e. a 0-ary function symbol).

If $\mathcal{M}$ is as above, $|\mathcal{M}| := M$.

(c) We define $\wedge^{\mathcal{M}}, \vee^{\mathcal{M}}, \to^{\mathcal{M}} : \mathbb{B}^2 \to \mathbb{B}$, $\neg^{\mathcal{M}} : \mathbb{B} \to \mathbb{B}$ and $\perp^{\mathcal{M}} \in \mathbb{B}$ by
$\wedge^{\mathcal{M}}(a, b) := \min\{a, b\}$, $\vee^{\mathcal{M}}(a, b) := \max\{a, b\}$, $\to^{\mathcal{M}} (a, b) := \max\{a, 1 - b\}$, $\neg^{\mathcal{M}}(a) := 1 - a$, $\perp^{\mathcal{M}} := 0$.

(d) If not mentioned differently, we will interpret $=$ by defining
$=^{\mathcal{M}} (a, b) := \begin{cases} 1 & \text{if } a = b \\ 0 & \text{otherwise} \end{cases}$.
This is called the standard interpretation of $=$.

(e) If $\mathcal{M}$ is a structure for $\mathcal{L}$, an $\mathcal{M}$-assignment is a function $\xi : \mathrm{Var} \to |\mathcal{M}|$. If ξ is an $\mathcal{M}$-assignment, $a \in |\mathcal{M}|$, $x \in \mathrm{Var}$, then $\xi_x^a : \mathrm{Var} \to |\mathcal{M}|$, $\xi_x^a(y) := \begin{cases} a & \text{if } x = y \\ \xi(y) & \text{otherwise.} \end{cases}$.

(f) An interpretation for a language $\mathcal{L}$ is a pair $\mathcal{I} = (\mathcal{M}, \xi)$ where $\mathcal{M}$ is an interpretation and ξ is an interpretation for $\mathcal{M}$. $\mathcal{I}_x^a := (\mathcal{M}, \xi_x^a)$.

(g) If $\mathcal{I} = (\mathcal{M}, \xi)$ is an interpretation for $\mathcal{L}$, we define for expressions (= terms or formulas) u in $\mathcal{L}$ $\mathcal{I}(u) \in \begin{cases} |\mathcal{M}| & \text{if } u \text{ is a term} \\ \mathbb{B} & \text{if } u \text{ is a formula} \end{cases}$ by induction on the definition of expressions u.
(If u is a term, $\mathcal{I}(u)$ is called the *value of* u *under interpretation* $\mathcal{I}$, if it is a formula, then $\mathcal{I}(u)$ is called the *interpretation of* u *under* $\mathcal{I}$).

- If u is a variable, $\mathcal{I}(u) := \xi(u)$.
- If $u = fu_1, \dots, u_n$, f a function- or relation symbol or $f \in \{\wedge, \vee, \to, \neg, \perp\}$, then

$$\mathcal{I}(t) := f^{\mathcal{M}}(\mathcal{I}(u_1), \dots, \mathcal{I}(u_n)) \ .$$

- $\mathcal{I}(\overset{\forall}{\exists} xA) :=\overset{\min}{\max} \{\mathcal{I}_x^a(A) \mid a \in |\mathcal{M}|\}$.

(h) Assume $\mathcal{I}$ is an interpretation, A is a formula, both of $\mathcal{L}$.
$\mathcal{I} \models A :\Leftrightarrow \mathcal{I}(A) = 1$.
If Γ is a set of formulas in $\mathcal{L}$, then
$\mathcal{I} \models \Gamma :\Leftrightarrow$ for every $A \in \Gamma$, $\mathcal{I} \models A$.
Γ is *satisfiable*, iff there exists an interpretation $\mathcal{I}$ such that $\mathcal{I} \models \Gamma$.
Such an interpretation is called a *model* of Γ.

(i) Assume Γ is a set of formulas, A a formula of the language $\mathcal{L}$.
$\Gamma \models A :\Leftrightarrow A$ holds in any model of Γ.
A is called *valid*, $\models A$, iff $\emptyset \models A$.
Two formulas A and B are *equivalent*, iff $\{A\}$ and $\{B\}$ have the same models.

Definition 1.2 (a) If u is an expression, $\mathrm{FV}(u) \subseteq \{x_1, \dots, x_n\}$ ($x_1, \dots, x_n$ distinct), $a_1, \dots, a_n \in |\mathcal{M}|$, then

$$u^{\mathcal{M}}[x_1 := a_1, \dots, x_n := a_n] := (\mathcal{M}, \xi)(u)$$

where ξ is an assignment with $\xi(x_i) = a_i$, $i = 1, \dots, n$.
If $u = A$ is a formula, then

$$\mathcal{M} \models A[x_1 := a_1, \dots, x_n := a_n] :\Leftrightarrow A^{\mathcal{M}}[x_1 := a_1, \dots, x_n := a_n] = 1$$

If the choice of variables is clear we write $u^{\mathcal{M}}[a_1, \dots, a_n]$ and $\mathcal{M} \models A[a_1, \dots, a_n]$.

(b) If $\mathcal{L}$ is finite, we sometimes write it as a tuple $(R_1, \ldots, R_n, f_1, \ldots, f_m)$. Then we will sometimes write structures $\mathcal{M}$ as
$(|\mathcal{M}|, R_1^{\mathcal{M}}, \ldots, R_n^{\mathcal{M}}, f_1^{\mathcal{M}}, \ldots, f_m^{\mathcal{M}})$.

Definition 1.3 (a) $\mathcal{L}(\Gamma)$ is the set of function- and relation symbols in a set of formulas Γ.

(b) A *sentence* is a closed formula.
$\mathrm{For}_{\mathcal{L}}^0$ is the set of $\mathcal{L}$-sentences.
The *universal closure* of the formula A is $\forall x_1 \cdots \forall x_n.A$ where $\mathrm{FV}(A) = \{x_1, \ldots, x_n\}$ and x_i are distinct.
An *axiom system* is a collection of sentences.

(c) For every $\mathcal{L}$-structure $\mathcal{M}$ let
$\mathrm{Th}(\mathcal{M}) := \{A \in \mathrm{For}_{\mathcal{L}}^0 \mid \mathcal{M} \models A\}$ (the *theory of* $\mathcal{M}$).

(d) If Σ is an axiom system let
$\mathrm{Th}_{\mathcal{L}}(\Sigma) := \{A \in \mathrm{For}_{\mathcal{L}}^0 \mid \Sigma \models A\}$ (the *theory derived by* Σ).
(Note the different use of $\mathrm{Th}(\mathcal{M})$ and $\mathrm{Th}_{\mathcal{L}}(\Sigma)$.

(e) $\mathrm{Mod}_{\mathcal{L}}(\Sigma)$ is the class of all $\mathcal{L}$-models of Σ.

Definition 1.4 (a) An axiom system Γ is called a *theory*, iff it is deductively closed, i.e. for every sentence $A \in \mathrm{For}_{\mathcal{L}(\Gamma)}^0$, if $T \vdash A$ then $A \in T$.

(b) If T is a theory and $\Sigma \subseteq T$, then Σ is called an *axiom system of* T if $T = \mathrm{Th}_{\mathcal{L}}(\Sigma)$.

(c) An axiom system Σ is called *complete*, iff for every $\mathcal{L}(\Sigma)$ sentence A follows $\Sigma \vdash A$ or $\Sigma \vdash \neg A$.

Lemma 1.5 *(a)* $\mathrm{Th}(\mathcal{M})$ *is a complete theory.*

(b) Is Σ an axiom system, $\mathcal{L}(\Sigma) \subseteq \mathcal{L}$, then $\mathrm{Th}_{\mathcal{L}}(\Sigma)$ *is a theory, and* $\mathrm{Th}_{\mathcal{L}}(\Sigma) = \{A \in \mathrm{For}_{\mathcal{L}}^0 \mid \Sigma \vdash A\}$.

(c) If T is a complete theory, T' is consistent, $T \subseteq T'$, then $T = T'$.

Proof: (a) $\mathrm{Th}(\mathcal{M}) \vdash A \Rightarrow \mathcal{M} \models A \Rightarrow A \in \mathrm{Th}(\mathcal{M})$. $\mathrm{Th}(\mathcal{M})$ is obviously complete.
(b) trivial.
(c) Exercise.

Definition 1.6 Let $\mathcal{L}$, $\mathcal{L}'$ be languages. $\mathcal{L}'$ is an extension of $\mathcal{L}$ iff $\mathcal{L} \subseteq \mathcal{L}'$. If $\mathcal{L} \subseteq \mathcal{L}'$, $\mathcal{M}$ is an $\mathcal{L}$-structure, $\mathcal{M}'$ is an $\mathcal{L}'$-structure, then $\mathcal{M}'$ is an *expansion of* $\mathcal{M}$ $:\Leftrightarrow$ $\mathcal{M}$ *is a reduct of* $\mathcal{M}'$ $:\Leftrightarrow$ $|\mathcal{M}| = |\mathcal{M}'|$ and for all $p \in \mathcal{L}'$ $p^{\mathcal{M}} = p^{\mathcal{M}'}$.
Let $\mathcal{M}' \restriction \mathcal{L}$ be the (unique) $\mathcal{L}$-reduct of $\mathcal{M}$.

Remark 1.7 *If $\mathcal{M}'$ is an expansion of the $\mathcal{L}$-structure $\mathcal{M}$, and ξ an $\mathcal{M}$-assignment, then for every expression u of the language $\mathcal{L}$ $(\mathcal{M}, \xi)(u) = (\mathcal{M}', \xi)(u)$. $\Gamma \models A$ and "T has a model" are therefore independent of the language $\mathcal{L} \supseteq \mathcal{L}(\Gamma \cup \{A\})$. Because of the completeness theorem, the same holds for "$\mathrm{T} \vdash A$" and "T is consistent".*

1.2 Compactness and Löwenheim-Skolem

Definition 1.8 A structure $\mathcal{M}$ is called finite (infinite, countable), iff this holds for $|\mathcal{M}|$.

Theorem 1.9 *(Compactness theorem) Let Γ be a set of formulas. Is every finite subset of Γ satisfiable, then Γ is satisfiable, too.*

Proof: Assume Γ is not satisfiable. Then by the completeness theorem Γ is not consistent. Therefore $\Gamma \vdash \perp$. Then for a finite subset Γ' of Γ follows $\Gamma' \vdash \perp$. Therefore Γ' is not satisfiable, a contradiction.

Theorem 1.10 *(Löwenheim-Skolem) A countable satisfiable set of formulas Γ has a countable model.*

Proof:
Let $C := \{c_n \mid n \in \omega\}$ new constants. With Γ are $\mathcal{L} := \mathcal{L}(\Gamma) \cup C$ and $T := \{t \mid t \text{ closed } \mathcal{L}\text{-term}\}$ countable. If Γ is satisfiable, it is as well consistent. In the proof of the completeness theorem, a model of Γ was constructed, with $|\mathcal{M}| = T$. Therefore Γ has a countable model.

Theorem 1.11 *If an axiom system Σ has arbitrary big finite models, then Σ has an infinite model, too.*

Proof: Let $\mathcal{L} := \mathcal{L}(\Sigma) \cup \{=\}$, where $=$ is a new binary relation, $x_1, x_2, \dots,$ different variables and

$$\Gamma := \Sigma \cup \{\neg(x_i = x_j) \mid i, j \in \mathbb{N}, i < j\} \ .$$

We show: Every finite subset of Γ can be satisfied. Proof: Let $\Delta \subseteq \Gamma$ be finite. Then $\Delta \subseteq \Sigma \cup \{\neg(x_i = x_j) \mid i, j \in \mathbb{N}, i < j \leq n\}$. Let $(\mathcal{M}', \xi')$ be a model of Σ having at least n distinct elements $a_1, \dots, a_n$. Let η be an assignment with $\eta(x_i) := a_i$. Then $(\mathcal{M}', \eta)$ is a model of Δ.
By the compactness-theorem Γ can be satisfied. If $(\mathcal{M}, \xi)$ is a model of Γ, then $i \mapsto \xi(x_i)$ is an injective map from $\mathbb{N}$ into $|\mathcal{M}|$, $\mathcal{M}$ is infinite.

1.3 Substructures, Isomorphisms and Elementary Equivalence

Definition 1.12 Let $\mathcal{M}$, $\mathcal{M}'$ two $\mathcal{L}$-structures ($\mathcal{L}$ a language).

(a) $\mathcal{M}$ is called *substructure of* $\mathcal{M}'$ ($\mathcal{M} \subseteq \mathcal{M}'$), if $|\mathcal{M}| \subseteq |\mathcal{M}'|$ and further:

  (i) $c^{\mathcal{M}} = c^{\mathcal{M}'}$ for every constant $c \in \mathcal{L}$.

  (ii) $p^{\mathcal{M}} = p^{\mathcal{M}'} \restriction |\mathcal{M}|^n$ for every n-ary function- or relation symbol $p \in \mathcal{L}$ (in case p a function symbol, $n \geq 1$).

(b) An isomorphic embedding $\pi : \mathcal{M} \to \mathcal{M}'$ is an injective function $\pi : |\mathcal{M}| \to |\mathcal{M}'|$ such that

(i) $\pi(f^{\mathcal{M}}(a_1, \dots, a_n)) = f^{\mathcal{M}'}(\pi(a_1), \dots, \pi(a_n))$ for very function symbol $f \in \mathcal{L}$ of arity $n \geq 0$, and every $a_1, \dots, a_n \in |\mathcal{M}|$.

(ii) $R^{\mathcal{M}}(a_1, \dots, a_n) = R^{\mathcal{M}'}(\pi(a_1), \dots, \pi(a_n))$ for very relation symbol $R \in \mathcal{L}$ of arity n, and every $a_1, \dots, a_n \in |\mathcal{M}|$.

An *isomorphism* $\pi : \mathcal{M} \to \mathcal{M}'$ is an isomorphic embedding $\mathcal{M} \to \mathcal{M}'$ such that $\pi : |\mathcal{M}| \to |\mathcal{M}'|$ surjective.

We write $\pi : \mathcal{M} \xrightarrow{\cong} \mathcal{M}'$ for π is an isomorphism from $\mathcal{M}$ to $\mathcal{M}'$.

$\mathcal{M} \cong \mathcal{M}' :\Leftrightarrow$ there exists an isomorphism $\pi : \mathcal{M} \xrightarrow{\cong} \mathcal{M}'$.

Remark 1.13 *A function $\pi : |\mathcal{M}| \to |\mathcal{M}'|$ is an isomorphic embedding from $\mathcal{M}$ into $\mathcal{M}'$ iff it is an isomorphism from $\mathcal{M}$ to a substructure of $\mathcal{M}'$.*

Definition 1.14

Two $\mathcal{L}$-structures $\mathcal{M}$, $\mathcal{M}'$ are *elementary equivalent*, $\mathcal{M} \equiv \mathcal{M}'$, if $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{M}')$.

Lemma 1.15 *(a) $\mathcal{M} \equiv \mathcal{M}' \Leftrightarrow \mathcal{M} \models \mathrm{Th}(\mathcal{M}')$.*

(b) If $\mathcal{L}$ is countable, then for every $\mathcal{L}$-structure $\mathcal{M}$ there exists a countable structure $\mathcal{M}'$ such that $\mathcal{M} \equiv \mathcal{M}'$.

(a) "$\Rightarrow$" $\mathrm{Th}(\mathcal{M}) = \mathrm{Th}(\mathcal{M}') \Rightarrow \mathcal{M} \models \mathrm{Th}(\mathcal{M}')$.
"$\Leftarrow$" Assume $\mathcal{M} \models \mathrm{Th}(\mathcal{M}')$. Then $\mathrm{Th}(\mathcal{M}') \subseteq \mathrm{Th}(\mathcal{M})$. By 1.5 (c) $\mathrm{Th}(\mathcal{M}') = \mathrm{Th}(\mathcal{M})$.
(b) $\mathrm{Th}(\mathcal{M})$ can be satisfied and is countable. Therefore there is a countable $\mathcal{M}'$ such that $\mathcal{M}' \models \mathrm{Th}(\mathcal{M})$.

Theorem 1.16 *Let T be a theory and $\mathcal{L} = \mathcal{L}(T)$. The following are equivalent:*

(i) T is complete

(ii) For every $\mathcal{M} \in \mathrm{Mod}_{\mathcal{L}}(T)$ we have $\mathrm{Th}(\mathcal{M}) = T$

(iii) If $\mathcal{M}, \mathcal{M}' \in \mathrm{Mod}_{\mathcal{L}}(T)$, then $\mathcal{M} \equiv \mathcal{M}'$.

Proof: Exercise.

Lemma 1.17 *Let π be an isomorphism from $\mathcal{M}$ to $\mathcal{M}'$ and ξ an $\mathcal{M}$-assignment. Then for every $\mathcal{L}$-term t and $\mathcal{M}$-formula A the following holds*

(a)
- $\pi((\mathcal{M}, \xi)(t)) = (\mathcal{M}', \pi \circ \xi)(t)$
- $(\mathcal{M}, \xi)(A) = (\mathcal{M}', \pi \circ \xi)(A)$

(b) If $\mathrm{FV}(t), \mathrm{FV}(A) \subseteq \{x_1, \dots, x_n\}$, x_i distinct, this can be written as

- $\pi(t^{\mathcal{M}}[x_1 := a_1, \dots, x_n := a_n]) = t^{\mathcal{M}'}[x_1 := \pi(a_1), \dots, x_n := \pi(a_n)]$

- $\mathcal{M} \models A[x_1 := a_1, \ldots, x_n := a_n] \Leftrightarrow \mathcal{M}' \models A[x_1 := \pi(a_1), \ldots, x_n := \pi(a_n)]$

(c) If t, A are closed, this can be simplified to:

- $\pi(\mathcal{M}(t)) = \mathcal{M}'(t)$.
- $\mathcal{M}(A) = \mathcal{M}'(A)$.

Proof: If we define $\pi : \mathbb{B} \to \mathbb{B}$, $\mathcal{I} := (\mathcal{M}, \xi)$, $\mathcal{I}' := (\mathcal{M}', \pi \circ \xi)$, then the above equation reads: $\pi(\mathcal{I}(u)) = \mathcal{I}'(u)$ for every expression u.
Induction on u, simultaneously for all $\mathcal{I}$.
u a variable x:
$\pi(\mathcal{I}(u)) = \pi(\xi(x)) = \mathcal{I}'(u)$.
$u = fu_1, \ldots, u_n$, f a relation-, function- or constant- symbol or
$f \in \{\wedge, \vee, \rightarrow, \neg, \bot\}$:

$$\begin{aligned} \pi(\mathcal{I}(fu_1, \ldots, u_n)) &= \pi(f^{\mathcal{M}}(\mathcal{I}(u_1), \ldots, \mathcal{I}(u_n))) \\ &= f^{\mathcal{M}'}(\pi(\mathcal{I}(u_1)), \ldots, \pi(\mathcal{I}(u_n))) \\ &\overset{\text{IH}}{=} f^{\mathcal{M}'}(\mathcal{I}'(u_1), \ldots, \mathcal{I}'(u_n)) \\ &= \mathcal{I}'(fu_1, \ldots, u_n) \end{aligned}$$

$u = \overset{\forall}{\exists}\, xA$:

$$\begin{aligned} \pi(\mathcal{I}(\overset{\forall}{\exists}\, x.A)) &= \mathcal{I}(\overset{\forall}{\exists}\, x.A) \\ &= \overset{\min}{\max} \{(\mathcal{M}, \xi^a_x)(A) \mid a \in |\mathcal{M}|\} \\ &\overset{\text{IH}}{=} \overset{\min}{\max} \{(\mathcal{M}', \pi \circ \xi^a_x)(A) \mid a \in |\mathcal{M}|\} \\ &= \overset{\min}{\max} \{(\mathcal{M}', (\pi \circ \xi)^{\pi(a)}_x)(A) \mid a \in |\mathcal{M}|\} \\ &\overset{\pi \text{ surjective}}{=} \overset{\min}{\max} \{(\mathcal{M}', (\pi \circ \xi)^{b}_x)(A) \mid b \in |\mathcal{M}'|\} \\ &= \mathcal{I}'(\overset{\forall}{\exists}\, xA) \end{aligned}$$

A corollary of the lemma is the following theorem:

Theorem 1.18 *If $\mathcal{M} \cong \mathcal{M}'$ then $\mathcal{M} \equiv \mathcal{M}'$*

Lemma 1.19 *For every structure $\mathcal{M}$ in which the equality axioms hold, there exists an elementary equivalent structure $\mathcal{M}'$ such that $=^{\mathcal{M}'}$ is standard and if $\mathcal{M}$ is countable (finite), then $\mathcal{M}'$ is countable (finite), too.*

Proof: Let $M := |\mathcal{M}|$, $\sim := \{(a,b) \in M \times M \mid =^{\mathcal{M}} (a,b) = 1\}$. $\sim$ is an equivalence relation. Let M' be the equivalence classes of M with respect to $\sim$ and define for n-ary functions f $f^{\mathcal{M}'}([a_1], \ldots, [a_n]) := [f^{\mathcal{M}}(a_1, \ldots, a_n)]$ and for n-ary relations R $R^{\mathcal{M}'}([a_1], \ldots, [a_n]) := R^{\mathcal{M}}(a_1, \ldots, a_n)$. By the congruence axioms, which are part of the equality axioms, follows that this definition is well-defined, $=^{\mathcal{M}'}$ is standard, and if π is the canonical map $M \to |\mathcal{M}'|$, then for any term t, formula A and assignment ξ with respect to $\mathcal{M}$, we get $\pi((\mathcal{M}, \xi)(t)) = (\mathcal{M}', \pi \circ \xi)(t)$ and $(\mathcal{M}, \xi)(A) = (\mathcal{M}', \pi \circ \xi)(A)$. $\mathcal{M} \equiv \mathcal{M}'$.

Theorem 1.20 *For every infinite structure $\mathcal{M}$ there exists an elementary equivalent structure $\mathcal{M}'$, which is not isomorphic to $\mathcal{M}$. If the language contains $=$ and $=^{\mathcal{M}}$ is standard, then $=^{\mathcal{M}'}$ can be chosen standard, too.*

Proof:
Let $\mathcal{L}$ be the language of $\mathcal{M}$.
Let $M := |\mathcal{M}|$, $\mathcal{P}(M)$ be the power set of M. For every $\alpha \in \mathcal{P}(M)$ let c_α be a new constant, further let, if $\mathcal{M}$ has not equality with standard interpretation, $=$ be a new binary relation symbol.
$\mathcal{L}' := \mathcal{L} \cup \{=\} \cup \{c_\alpha \mid \alpha \in \mathcal{P}(M)\}$.
$\Sigma' := \mathrm{Th}(\mathcal{M}) \cup \{\neg(c_\alpha = c_\beta) \mid \alpha, \beta \in \mathcal{P}(M), \alpha \neq \beta\}$.
Every finite subset of Σ' can be satisfied by a suitable expansion of $\mathcal{M}$. By the compactness theorem Σ' has a model $\mathcal{M}_1'$ (with standard interpretation of $=^{\mathcal{M}'}$, if $=^{\mathcal{M}}$ was standard). Let $\mathcal{M}' := \mathcal{M}_1' \upharpoonright \mathcal{L}$.
$\mathcal{M}_1' \models \Sigma' \Rightarrow \mathcal{M}_1' \models \mathrm{Th}(\mathcal{M}) \Rightarrow \mathcal{M}' \models \mathrm{Th}(\mathcal{M}) \Rightarrow \mathcal{M} \equiv \mathcal{M}'$.
$\mathcal{M}_1' \models \neg(c_\alpha = c_\beta) \Rightarrow c_\alpha^{\mathcal{M}_1'} \neq c_\beta^{\mathcal{M}_1'} \Rightarrow c_\alpha^{\mathcal{M}'} \neq c_\beta^{\mathcal{M}'}$.
Therefore $\mathcal{M}'$ has at least $\mathcal{P}(M)$ many different element, therefore it cannot be isomorphic to $\mathcal{M}$.

1.4 Nonstandard Structures

Definition 1.21 (a) Let $\mathcal{L}_\mathbb{N} := (=, 0, \mathrm{S})$ be the language of arithmetic, with $=$ being the 2-ary relation symbol for equality, 0 the constant 0 and S a unary function symbol for the successor.
$\mathcal{N}_0 := (\mathbb{N}, =, 0, \mathrm{S})$, where $\mathrm{S} : \mathbb{N} \to \mathbb{N}$, $n \mapsto n+1$.

(b) Let $\mathcal{L}_\mathbb{R} := (=, 0, 1, +, \cdot, <)$ the language of the real numbers, with the obvious arities, and $\mathcal{R}$ be the usual structure of the reals.

Remark By theorem 1.20 no infinite structure structure can be characterized by a first-order-axiom system up to isomorphism.
However, the Structure $\mathcal{N}_0$ is, if $=$ is interpreted standard, uniquely determined by the Peano-axioms (i.e. the equality axioms, $\forall x.0 \neq \mathrm{S}(x)$, $\forall x, y(\mathrm{S}(x) = \mathrm{S}(y) \to x = y)$, and the induction axiom: if $M \subseteq \mathbb{N}$, $0 \in M$ and $\forall x \in M.\mathrm{S}(x) \in M$ then $M = \mathbb{N}$).
But this does not cause a contradiction, since the Peano-axioms do not form a first order axiom system. The induction axiom can be precisely written as

$$\forall X(0 \in X \wedge (\forall x(x \in X \to \mathrm{S}(x) \in X) \to \forall x.x \in X)$$

and has a quantifier $\forall X$ ranging over all subsets of the natural numbers, therefore this formula is a 2nd order formula.

Definition 1.22 (a) A nonstandard model of the natural numbers is a structure of the language $\mathcal{L}_\mathbb{N}$ which is elementary equivalent, but not isomorphic to $\mathcal{N}_0$.

(b) A nonstandard model of the reals is a structure of the language $\mathcal{L}_{\mathbb{R}}$ which is elementary equivalent, but not isomorphic to $\mathcal{R}$.

In a nonstandard model of the natural numbers, the principal of complete induction does not hold, only, if it is restricted to (first-order-) definable subsets of the natural numbers.

Theorem 1.23 *There are countable nonstandard models of the natural numbers.*

Proof: $\Gamma := \mathrm{Th}(\mathcal{N}_0) \cup \{\neg(x = 0), \neg(x = \mathrm{S}(0)), \neg(x = \mathrm{S}(\mathrm{S}(0))), \dots\}$. Every finite subset of Γ and therefore Γ itself can be satisfied by a countable structure $\mathcal{N}_1$ and an assignment ξ. $\mathcal{N}_1 \models \mathrm{Th}(\mathcal{N}_0)$, therefore $\mathcal{N}_0 \equiv \mathcal{N}_1$. If $\pi : \mathcal{N}_0 \xrightarrow{\cong} \mathcal{N}_1$, then for every $n \in \mathbb{N}$ $\pi(n) = \pi(\mathcal{N}_0(\underbrace{\mathrm{S}(\cdots\mathrm{S}}_{n\text{ times}}(0)\cdots))) = \mathcal{N}_1(\mathrm{S}(\cdots\mathrm{S}(0)) \neq \xi(x)$, π is not surjective, a contradiction.

The structure $\mathcal{R}$ is up to isomorphism the unique complete ordered archimedean field with standard interpretation of $=$.
(The axioms of an ordered field (formulated in the language $\mathcal{L}_{\mathbb{R}}$ are the equality axioms, the field axiom, axioms stating the linearity of $<$ and $\forall x, y, z(x < y \to x + z < y + z)$, $\forall x, y, z(x < y \wedge 0 < z \to x \cdot z < y \cdot z)$.
An ordered field is archimedean, iff for every x there exists a natural number n such that $x < n$. This can be axiomatized by adding a predicate $\mathbb{N}$ (where we write $x \in \mathbb{N}$ for $\mathbb{N}(x)$ and axioms expressing, that $\mathbb{N}$ is the set of natural numbers, i.e. $0 \in \mathbb{N}$, $\forall x(x \in \mathbb{N} \to x+1 \in \mathbb{N})$, $\forall X.(0 \in \mathbb{N} \wedge \forall x \in X(x+1 \in \mathbb{N}) \to \forall x \in \mathbb{N}.x \in X)$.
The completeness axiom can be expressed by: every nonempty bounded set has a supremum), which is the 2^{nd}-order formula

$$\forall X(\emptyset \neq X \text{ bounded } \to \exists y. y = \sup(X))$$

as is the induction axiom for the predicate $\mathbb{N}$. In a nonstandard model of the reals not every bounded set $X \neq \emptyset$ has a supremum (however every in the language of$\mathcal{L}_{\mathbb{R}}$ definable has), or $\mathbb{N}$ is non standard.

Lemma 1.24 *For every archimedean ordered field there exists an elementary equivalent ordered field which is not archimedean.*

Proof:
Let $\mathcal{K}$ be an archimedean ordered field in the language $\mathcal{L}_{\mathbb{R}}$, $\Gamma := \mathrm{Th}(\mathcal{K}) \cup \{\underline{n} < x \mid 1 \leq n \in \mathbb{N}\}$, where $\underline{n} := \underbrace{1 + \cdots 1}_{n\text{ times}}$.
Every finite subset of Γ can be satisfied, therefore Γ can be satisfied. Let $(\mathcal{M}, \xi)$ be a model of Γ. $\mathcal{M} \equiv \mathcal{K}$, $\mathcal{M}$ is an ordered field. However $(\mathcal{M}, \xi) \models \underline{n} < x$, $\underbrace{1^{\mathcal{M}} +^{\mathcal{M}} \cdots +^{\mathcal{M}} 1^{\mathcal{M}}}_{n\text{ times}} <^{\mathcal{M}} \xi(x)$, $\mathcal{M}$ is not archimedean.

Corollary 1.25 *If a sentence A in the language $\mathcal{L}_{\mathcal{R}}$ holds in every non-archimedean ordered field, then it holds in every ordered field.*

Proof:
If $\mathcal{K}$ is archimedean, $\mathcal{K} \equiv \mathcal{M}$ where $\mathcal{M}$ is a non-archimedean ordered field. $\mathcal{M} \models A$, therefore $\mathcal{K} \models A$.

1.5 Axiomatizability

Definition 1.26 A class $\mathcal{S}$ of $\mathcal{L}$-structures is *(finitely) axiomatizable*, iff there exists a (finite) axiom system Σ such that $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\Sigma)$.

Remark 1.27 *(a) $\mathcal{S}$ is finitely axiomatizable iff there is an $\mathcal{L}$-sentence such that $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\{A\})$.*

(b) If there are structures $\mathcal{M}$, $\mathcal{M}'$ such that $\mathcal{M} \equiv \mathcal{M}'$, $\mathcal{M} \in \mathcal{S}$, $\mathcal{M}' \notin \mathcal{S}$, then $\mathcal{S}$ is not axiomatizable.

Lemma 1.28 *Let $\mathcal{S}$ be a class of $\mathcal{L}$-structures and Σ an axiom system.*

(a) $\mathcal{S}$ is finitely axiomatizable iff $\mathcal{S}$ and its complement are axiomatizable.

(b) Is $\mathrm{Mod}_{\mathcal{L}}(\Sigma)$ finitely axiomatizable, then there exists a finite $\Delta \subseteq \Sigma$ such that $\mathrm{Mod}_{\mathcal{L}}(\Sigma) = \mathrm{Mod}_{\mathcal{L}}(\Delta)$.

Proof:
Let $\mathcal{S}^{c}$ be the complement of $\mathcal{S}$. (a) "$\Rightarrow$": If $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\{A\})$ then $\mathcal{S}^{c} = \mathrm{Mod}_{\mathcal{L}}(\{\neg A\})$. "$\Leftarrow$" Let $\mathcal{S} = \mathrm{Mod}_{\mathcal{L}}(\Sigma)$, $\mathcal{S}^{c} = \mathrm{Mod}_{\mathcal{L}}(\Delta)$. $\Sigma \cup \Delta$ is not satisfiable. Therefore there exists a finite subset Σ' of Σ such that $\Sigma' \cup \Delta$ is unsatisfiable. $\mathcal{M} \in \mathcal{S} \Rightarrow \mathcal{M} \models \Sigma'$, and $\mathcal{M} \models \Sigma' \Rightarrow \mathcal{M} \not\models \Delta \Rightarrow \mathcal{M} \notin \mathcal{S}^{c} \Rightarrow \mathcal{M} \in \mathcal{S}$, therefore Σ' axiomatizes $\mathcal{S}$.
(b) Let Δ be an axiom system for $\mathcal{S}^{c}$. As in (a), "$\Leftarrow$" follows now Σ' axiomatizes $\mathrm{Mod}_{\mathcal{L}}(\Sigma)$ for some $\Sigma' \subseteq \Sigma$ finite.

Lemma 1.29 *(a) Is $\mathcal{S}$ a class of finite $\mathcal{L}$-structures, and $\mathcal{S}$ contains arbitrary big structures ($|\mathcal{M}|$ for $\mathcal{M} \in \mathcal{S}$ is arbitrary big), then $\mathcal{S}$ is not axiomatizable.*

(b) The class of all infinite $\mathcal{L}$-structures (or groups or rings or fields) is axiomatizable, but not finitely axiomatizable.

(c) The class of fields of characteristic 0 is axiomatizable, but not finitely axiomatizable.

(d) If a sentence A holds in all fields of characteristic 0, then there exists an $n_0 \in \mathbb{N}$ such that A holds in all fields of characteristic $p \geq n_0$.

(e) The class of all (non-)archimedean ordered fields is not axiomatizable.

Proof: Exercise.

1.6 An Example of a Theory with Unique Infinite Model (up to Isomorphism)

Definition 1.30 Let DO, the *theory of dense linear orderings without endpoints* be the deductive closure of the following axioms in the language $\mathcal{L} = \{<, =\}$:

(0) The equality axioms for $\mathcal{L}$;

(1) $\forall x.\neg(x < x) \wedge \forall x, y, z(x < y \wedge y < z \to x < z) \wedge \forall x, y(x < y \vee x = y \vee y < x)$

(2)$\forall x, y.(x < y \to \exists z(x < z \wedge z < y))$

(3) $\forall x.(\exists y(x < y) \wedge \exists y(y < x))$.

Lemma 1.31 *Every countable model of* DO *with standard interpretation of* $=$ *is isomorphic to the structure* $(\mathbb{Q}, =, <)$.

Proof:
Exercise.

Theorem 1.32 *The theory* DO *is complete and* $\mathrm{DO} = \mathrm{Th}(\mathbb{Q}, =, <)$.

Proof: It suffices to show, that every model of DO is elementary equivalent to $(\mathbb{Q}, =, <)$: If $\mathcal{M}$ is a model of DO, there exists a countable structure $\mathcal{M}_0$ such that $\mathcal{M} \equiv \mathcal{M}_0$. $\mathcal{M}_0 \cong (\mathbb{Q}, =, <)$, therefore $\mathcal{M} \equiv \mathcal{M}_0 \cong (\mathbb{Q}, =, <)$.

1.7 Nonstandard Analysis

In this section let r, s be real numbers.

Definition 1.33 (a) The language $\mathcal{L}_{\mathbb{R}}^{+}$ contains $=$, one constant $\widetilde{s}$ for every $s \in \mathbb{R}$, one n-ary function symbol $\widetilde{F}$ for every $F : \mathbb{R}^n \to \mathbb{R}$ $(n \geq 1)$ and one 2-ary relation symbol $<$.

(b) Let $\mathcal{R}^+$ be the standard structure in the language $\mathcal{L}_{\mathbb{R}}^{+}$, i.e. $|\mathcal{R}^+| = \mathbb{R}$, $\widetilde{s}^{\mathcal{R}^+} = s$, $\widetilde{F}^{\mathcal{R}^+} = F$, $<^{\mathcal{R}^+}(s_0, s_1) = 1 \Leftrightarrow s_0 < s_1$ and $=^{\mathcal{R}^+}$ is standard.

(c) Let $\mathcal{R}^*$ be an $\mathcal{L}_{\mathbb{R}}$-structure with standard interpretation of $=$, such that $\mathcal{R}^* \equiv \mathcal{R}^+$ and $\{a \in |\mathcal{R}^*| \mid \forall s \in \mathbb{R}.\widetilde{s}^{\mathcal{R}^*} <^{\mathcal{R}^*} a\} \neq \emptyset$.
$\mathbb{R}^* := |\mathcal{R}^*|$, $F^* := \widetilde{F}^{\mathcal{R}^*}$, $<^* := <^{\mathcal{R}^*}$. Further $\pi : \mathbb{R} \to \mathbb{R}^*$, $\pi(s) = \widetilde{s}^{\mathcal{R}^*}$.

Remark 1.34 $\pi : \mathcal{R}^+ \to \mathcal{R}^*$ *is an isomorphic embedding.*

Notation 1.35 (a) If $s \in \mathbb{R}$, we write s instead of $\pi(s)$ and consider $\mathcal{R}^+$ as a substructure of $\mathcal{R}^*$.

(b) Let $+_{\mathbb{R}} : \mathbb{R}^2 \to \mathbb{R}$ be the ordinary addition. We write $+$ for $+_{\mathbb{R}}$, $+_{\mathbb{R}}^*$ and the function symbol $\widetilde{+_{\mathbb{R}}}$. The same holds for 0 (zero), 1 (one), $\cdot$ (multiplication), $-$ (subtraction), and $|\cdot|$ (absolute value) and $/$. Further we write $\frac{r}{s}$ instead of r/s.

(c) In this chapter we write a, b, c, d for elements of $\mathbb{R}^*$.

(d) $\mathbb{R}_+ := \{s \in \mathbb{R} \mid 0 < s\}$.
$a \approx b :\Leftrightarrow \forall \epsilon \in \mathbb{R}_+ . |a - b| < \epsilon$. ($a$ and b are infinitely close).
a is finite $:\Leftrightarrow \exists s \in \mathbb{R}. |a| < s$.
a is infinitely small $:\Leftrightarrow s \approx 0$.
$[a] := \{d \in \mathbb{R}^* \mid a \approx d\}$. $[a]' := [a] \setminus \{a\}$.

Remark 1.36 $(\mathbb{R}^*, =, +, \cdot, 0, 1, <)$ *is an ordered field.*

Proof: $\mathcal{R}^* \equiv \mathcal{R}^+$ and the axiom system for ordered fields is a set of sentences in the language $\{=, +, \cdot, 0, 1, <\}$.

Remark 1.37 *For every $a \in \mathbb{R}^*$ there exists $b \in [a]'$ such that $a < b$.*

Proof: There exists $d \in \mathbb{R}^*$ such that $s < d$ for all $s \in \mathbb{R}_+$. By Remark 1.36 $0 < \frac{1}{d} < \frac{1}{s}$ for all $s \in \mathbb{R}_+$, $a < a + \frac{1}{d}$ and $|(a + \frac{1}{d}) - a| < \epsilon$ for all $\epsilon \in \mathbb{R}_+$.

Lemma 1.38 *Assume $F : \mathbb{R} \to \mathbb{R}$ and $r, s \in \mathbb{R}$.*

(a) $\lim_{x \to r} F(x) = s \Leftrightarrow$ *for every $a \in [r]'$ follows $F^*(a) \approx s$.*

(b) $F'(r) = s \Leftrightarrow$ *for every $d \in [0]'$ follows $\frac{F^*(r+d) - F(r)}{d} \approx s$.*

Proof:
"$\Rightarrow$" Let $a \in [r]'$ and $\epsilon \in \mathbb{R}_+$. By assumption there exists $\delta \in \mathbb{R}_+$ such that

$$\mathcal{R}^+ \models \forall x (0 < |x - \widetilde{r}| < \widetilde{\delta} \to |\widetilde{F}(x) - \widetilde{s}| < \widetilde{\epsilon}) \ ,$$

the same holds in $\mathcal{R}^*$ as well.
If $a \in [r]'$, then $0 < |a - r| < \delta$, $F^*(a) - s| < \epsilon$.
"$\Leftarrow$" Assume $\epsilon \in \mathbb{R}_+$, and let $0 < d \in [0]'$. For all $a \in \mathbb{R}^*$ such that $0 < |a - r| < d$ we have $a \in [r]'$, therefore $F^*(a) \approx s$ and therefore $|F^*(a) - s| < \epsilon$. Therefore

$$\mathcal{R}^* \models \exists y (0 < y \wedge \forall x (0 < |x - \widetilde{r}| < y \to |\widetilde{F}(x) - \widetilde{s}| < \widetilde{\epsilon})) \ .$$

By $\mathcal{R}^+ \equiv \mathcal{R}^*$, this formula holds as well in $\mathcal{R}^+$, and the assertion follows.
(b) $F'(r) = s \Leftrightarrow \lim_{d \to 0} G(d) = s$ where
$G : \mathbb{R} \to \mathbb{R}$, $G(s) := \begin{cases} \frac{F(r+s) - F(r)}{d} & \text{if } s \neq 0 \\ 0 & \text{otherwise.} \end{cases}$
If $d \in \mathbb{R}^* \setminus \{0\}$, $G^*(d) = \frac{F^*(r+d) - F(r)}{d}$ and by (a) follows now the assertion.

Example: Let $F : \mathbb{R} \to \mathbb{R}$, $F(r) := r^2$. Then for $d \in [0]'$,

$$\frac{F^*(r+d) - F(r)}{d} = \frac{(r+d)^2 - r^2}{d} = \frac{r^2 + 2rd + d^2 - r^2}{d} = 2r + d^2 \approx 2r \ ,$$

$F'(r) = 2r$.

Lemma 1.39 *(Chain rule) If $F, G : \mathbb{R} \to \mathbb{R}$, $r \in \mathbb{R}$, $G'(r)$ exists and $F'(G(r))$ exists. Then $(F \circ G)'(r) = F'(G(r)) \cdot G'(r)$.*

Proof:
Let $\Phi(d) := \frac{(F \circ G)^*(r+d) - (F \circ G)^*(r)}{d}$ for $d \in [0]'$. Show $\Phi(d) \approx F'(G(r)) \cdot G'(r)$.
Since $\frac{G^*(r+d) - G(r)}{d} \approx G'(r)$ and $G'(r)$ finite follows $G^*(r+d) - G(r) \approx 0$.
$\Phi(d) \overset{!}{=} \frac{F^*(G^*(r+d)) - F(G(r))}{d}$.
If $G^*(r+d) = G(r)$ follows $G'(r) \approx \frac{G^*(r+d) - G(r)}{d} = 0$, $G'(r) = 0$, $\Phi(d) = 0 = F'(G(r))G'(r)$, otherwise

$$\begin{aligned} \Phi(d) &= \frac{F^*(G^*(r+d)) - F(G(r))}{G^*(r+d) - G(r)} \cdot \frac{G^*(r+d) - G(r)}{d} \\ &\approx F'(G(r)) \cdot G'(r) \ . \end{aligned}$$

Chapter 2

Recursion Theory, part 1

2.1 Preliminaries: Partial functions

We will follow in this chapter very closely [Buc97a], chapter 1 and 3 and [Buc93b], section 14.
There is an attempt at the moment to rename this subject into computability theory.

Notation 2.1 In this chapter $a, b, c, d, i, j, k, l, m, n$ will be natural numbers and $\vec{a}, \vec{b}, \vec{c}, \vec{d}, \vec{i}, \vec{j}, \vec{k}, \vec{l}, \vec{m}, \vec{n}$ finite sequences (tuples) of natural numbers (the empty tuple is allowed as well).

In this chapter we are dealing with computability. Computer programs do not always terminate. Therefore the functions computed by a program will be in general partial. Partial functions will be needed not before section 2.4, however for systematic reason we introduce them now.

Definition 2.2 (a) An *n-ary partial function* ($n > 0$) is a function f such that $\mathrm{dom}(f) \subseteq \mathbb{N}^n$ and $\mathrm{rng}(f) \subseteq \mathbb{N}$. We define
$f(\vec{a}) \simeq e :\Leftrightarrow (\vec{a} \in \mathrm{dom}(f) \wedge f(\vec{a}) = e) \vee (\vec{a} \in \mathbb{N}^n \setminus \mathrm{dom}(f) \wedge e = \perp)$.
In case $f(\vec{a}) \simeq \perp$ we say, $f(\vec{a})$ *is undefined.*
We write $f : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$ for f is an n-ary partial function and identify partial functions with their graph.

(b) We extend the above notion to the case $n = 0$ by defining: a 0-ary partial function f, $f : \mathbb{N}^0 \to_{\mathrm{par}} \mathbb{N}$, is either a natural number or the undefined element $\perp$. We define
$f \simeq e :\Leftrightarrow (f$ is defined and $f = e) \vee f$ is undefined and $e = \perp)$.
The graph of f is $\{f\}$, if $f \not\simeq \perp$ and $\emptyset$ otherwise. If $\vec{a}$ is the empty tuple, we define $f(\vec{a}) \simeq e \Leftrightarrow f \simeq e$.

(c) A partial function $f : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$ is *total* iff $\mathrm{dom}(f) = \mathbb{N}^n$ (in case $n = 0$, if f is defined).

(d) n-ary functions are n-ary partial functions which are total.

(e) If f, g are partial functions, we define:
$f(\vec{a}) \simeq g(\vec{b}) \leftrightarrow \forall e \in \mathbb{N} \cup \{\perp\}. f(\vec{a}) \simeq e \Leftrightarrow g(\vec{a}) \simeq e$.

Example 2.3 The integer division div, the integer part of division of two natural numbers, is a partial function $\mathrm{div} : \mathbb{N}^2 \to_{\mathrm{par}} \mathbb{N}$, with $\mathrm{dom}(\mathrm{div}) = \mathbb{N}\times(\mathbb{N}\setminus\{0\})$.

Definition 2.4 (a) $0^n : \mathbb{N}^n \to \mathbb{N}$, $0^n(\vec{x}) := 0$. $(n > 0)$. $0^0 := 0$
$\mathrm{S} : \mathbb{N} \to \mathbb{N}$, $\mathrm{S}(a) := a + 1$.
$\mathrm{proj}_i^n : \mathbb{N}^n \to \mathbb{N}$, $\mathrm{proj}_i^n(a_1, \ldots, a_n) := a_i$. $(1 \leq i \leq n)$.

(b) If $1 \leq m$, $h : \mathbb{N}^m \to_{\mathrm{par}} \mathbb{N}$, $g_i : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$ $(i = 1, \ldots, m)$, then $h \circ (g_1, \ldots, g_m) : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$, $(h\circ(g_1, \ldots, g_m))(\vec{a}) \simeq b \Leftrightarrow \exists c_1, \ldots, c_m(g_1(\vec{a}) \simeq c_1 \wedge \cdots \wedge g_m(\vec{a}) \simeq c_m \wedge h(c_1, \ldots, c_m) \simeq b)$.

(c) If $g : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$, $h : \mathbb{N}^{n+2} \to_{\mathrm{par}} \mathbb{N}$, then $(\mathrm{R}gh) : \mathbb{N}^{n+1} \to_{\mathrm{par}} \mathbb{N}$,
$(\mathrm{R}gh)(\vec{a}, 0) :\simeq g(\vec{a})$,
$(\mathrm{R}gh)(\vec{a}, n+1) \simeq b :\Leftrightarrow \exists c((\mathrm{R}gh)(\vec{a}, n) \simeq c \wedge h(\vec{a}, n, c) \simeq b)$.

(d) If $g : \mathbb{N}^{n+1} \to_{\mathrm{par}} \mathbb{N}$, then $\mu g : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$,
$(\mu g)(\vec{a}) \simeq c \Leftrightarrow g(\vec{a}, c) \simeq 0 \wedge \forall i < c. \exists d \neq 0. g(\vec{a}, i) \simeq d$.

(e) If $g : \mathbb{N}^{n+1} \to_{\mathrm{par}} \mathbb{N}$, then $\overline{\mu} g : \mathbb{N}^{n+1} \to_{\mathrm{par}} \mathbb{N}$, $(\overline{\mu} g)(\vec{a}, b) \simeq (\mu h_b)(\vec{a})$, where
$h_b(\vec{a}, i) = \begin{cases} g(\vec{a}, i) & \text{if } i < b, \\ 0 & \text{otherwise.} \end{cases}$, i.e.
$(\overline{\mu} g)(\vec{a}, b) \simeq c \Leftrightarrow (g(\vec{a}, c) = 0 \vee c = b) \wedge \forall i < c. \exists d \neq 0. g(\vec{a}, i) \simeq d$.
(if g is total, $(\overline{\mu} g)(\vec{a}, b) = \min\{i \mid g(\vec{a}, i) = 0 \vee i = b\}$).

(f) If $R \subseteq \mathbb{N}^n$, the *characteristic function of* R $\chi_R : \mathbb{N}^n \to \mathbb{N}$, is defined by
$\chi_R(\vec{a}) := \begin{cases} 1 & \text{if } \vec{a} \in R \ , \\ 0 & \text{otherwise} \ . \end{cases}$
$(1 - \chi_R) : \mathbb{N}^n \to \mathbb{N}$, $(1 - \chi_R)(\vec{a}) := 1 - \chi_R(\vec{a})$

(g) If $R \subseteq \mathbb{N}^{n+1}$ is a $n+1$-ary relation, $\vec{a} \in \mathbb{N}^n$ then
$\mu y. R(\vec{a}, y) := (\mu(1 - \chi_R))(\vec{a})$;
$\mu y < b. R(\vec{a}, y) := (\overline{\mu}(1 - \chi_R))(\vec{a}, b)$

Remark 2.5 *(a) If $f, g, h_1, \ldots, h_m$ are total, then $f \circ (h_1, \ldots, h_m)$, $\mathrm{R}fg$ and $\overline{\mu} f$ are total, too (if they the operations are defined respectively). If R is a relation, χ_R is total. However μf might not be total, if f is total.*

(b) If g_i are 0-ary partial functions, h is an n-ary partial functions, then $h \circ (g_1, \ldots, g_m)$ is application, i.e.
$h \circ (g_1, \ldots, g_m) \simeq b \Leftrightarrow g_1, \ldots, g_m$ are defined and $h(g_1, \ldots, g_m) \simeq b$).
We write $h(g_1, \ldots, g_m)$ instead of $h \circ (g_1, \ldots, g_m)$.

Example 2.6 (a) If $f : \mathbb{N}^2 \to_{\mathrm{par}} \mathbb{N}$, $f(a,b) \simeq b+b$, then $(R1f) : \mathbb{N} \to \mathbb{N}$,
$(R1f)(0) = 1$,
$(R1f)(1) = f(0,(R1f)(0)) = 2$,
$(R1f)(2) = f(1,(R1f)(1)) = 4$,
$(R1f)(n) = 2^n$.

(b) Let $R(a,b) \Leftrightarrow (a \leq 5 \wedge b = 3)$.

$$(\mu R)(a) \simeq \begin{cases} 3 & \text{if } a \leq 5 \\ \perp & \text{otherwise.} \end{cases}.$$

$$(\overline{\mu} R)(a,b) \simeq \begin{cases} 3 & \text{if } a \leq 5 \wedge b \geq 3 \\ b & \text{otherwise.} \end{cases}.$$

(c) $f : \mathbb{N} \to_{\mathrm{par}} \mathbb{N}$, $f(0) \simeq \perp$, $f(n) \simeq 0$ for $n > 0$, then $(\mu f) \simeq \perp$.

2.2 Primitive Recursive functions

We start with the definition of primitive recursive functions. Primitive recursive functions are those which can be defined from some basic functions (constant, projection and successor function) using primitive recursion and composition. Primitive recursion is hereby the definition principle corresponding to the induction principle: If we have an initial value a and a function $g : \mathbb{N}^2 \to \mathbb{N}$, then we can introduce a new function $f : \mathbb{N} \to \mathbb{N}$ such that $f(0) = a$ and $f(n+1) = g(n, f(n))$. This can be generalized to having some additional arguments.

Definition 2.7 (a) The sets of n-ary primitive recursive function symbols $\widetilde{\mathrm{PR}}^n$ are defined simultaneously inductively by

($\widetilde{\mathrm{PR}}$ 1) $\widetilde{0^n} \in \widetilde{\mathrm{PR}}^n$, $\widetilde{\mathrm{S}} \in \widetilde{\mathrm{PR}}^1$ and if $1 \leq i \leq n$, $\widetilde{\mathrm{proj}_i^n} \in \widetilde{\mathrm{PR}}^n$.

($\widetilde{\mathrm{PR}}$ 2) If $1 \leq m \in \mathbb{N}$, $h \in \widetilde{\mathrm{PR}}^m$, $g_1, \dots, g_m \in \widetilde{\mathrm{PR}}^n$, then $h \widetilde{\circ} (g_1, \dots, g_m) \in \widetilde{\mathrm{PR}}^n$.

($\widetilde{\mathrm{PR}}$ 3) If $g \in \widetilde{\mathrm{PR}}^n$, $h \in \widetilde{\mathrm{PR}}^{n+2}$, then $\widetilde{\mathrm{R}} gh \in \widetilde{\mathrm{PR}}^{n+1}$.

(b) Let $\mathcal{L}_{\mathrm{PR}}$ be the language having the elements of $\widetilde{\mathrm{PR}}^n$ as n-ary function symbols and the binary relation $=$.

(c) We define the standard structure $\mathcal{N}$ with respect to the language $\mathcal{L}_{\mathrm{PR}}$ by $|\mathcal{N}| := \mathbb{N}$, $=$ is standard, $\widetilde{0^n}^{\mathcal{N}} := 0^n$, $\widetilde{\mathrm{S}}^{\mathcal{N}} := \mathrm{S}$, $\widetilde{\mathrm{proj}_n^i}^{\mathcal{N}} := \mathrm{proj}_n^i$, $(f \widetilde{\circ} (g_1, \dots, g_m))^{\mathcal{N}} := f^{\mathcal{N}} \circ (g_1^{\mathcal{N}}, \dots, g_m^{\mathcal{N}})$, $(\widetilde{\mathrm{R}} fg)^{\mathcal{N}} := \mathrm{R} f^{\mathcal{N}} g^{\mathcal{N}}$.

(d) $\mathrm{PR}^n := \{ f^{\mathcal{N}} \mid f \in \widetilde{\mathrm{PR}}^n \}$, $\mathrm{PR} := \bigcup_{n \in \mathbb{N}} \mathrm{PR}^n$. The elements of PR are called *primitive recursive functions*.

(e) A relation $R \subseteq \mathbb{N}^n$ is *primitive recursive*, if χ_R is primitive recursive.

Remark 2.8 *(a) Definition 2.7 (c) is well-defined, since $f^{\mathcal{N}}$ is total, if $f \in \widetilde{\mathrm{PR}}^n$.*

(b) $\mathrm{PR}^0 = \mathbb{N}$.

Proof of (b): "$\subseteq$" is trivial. "$\supseteq$": $n = \underbrace{\mathrm{S} \circ (\cdots \circ (\mathrm{S}}_{n\text{times}} \circ 0^0) \cdots)$.

An expression $\lambda x_1, \ldots, x_n.t$, where t is a term of the language $\mathcal{L}_{\mathrm{PR}}$ such that $\mathrm{FV}(t) \subseteq \{x_1, \ldots, x_n\}$ should represent the function, mapping $a_1, \ldots, a_n$ to $t^{\mathcal{N}}[x_1 := a_1, \ldots, x_n := a_n]$. We will show now, that the primitive recursive functions are closed under λ-abstraction in the following sense:

Lemma 2.9 *The primitive recursive functions are closed under λ-abstraction: For every* PR*-term t and pairwise distinct variables $x_1, \ldots, x_n$ $(n \geq 1)$ such that* $\mathrm{FV}(t) \subseteq \{x_1, \ldots, x_n\}$ *there exists an element $\widetilde{\lambda} x_1, \ldots, x_n.t$ of $\widetilde{\mathrm{PR}}^n$ such that*

$$\forall a_1, \ldots, a_n \in \mathbb{N}.(\widetilde{\lambda} x_1, \ldots, x_n.t)^{\mathcal{N}}(a_1, \ldots, a_n) = t^{\mathcal{N}}[x_1 := a_1, \ldots, x_n := a_n] \ .$$

$\widetilde{\lambda} x_1, \ldots, x_n.t$ can be effectively computed.

Definition 2.10 $\lambda x_1, \ldots, x_n.t := (\widetilde{\lambda} x_1, \ldots, x_n.t)^{\mathcal{N}}$.
We will usually not distinguish between elements of $\widetilde{\mathrm{PR}}$ and PR and omit usually the symbol tilde.
We will write 0 instead of 0^0.

Proof of Lemma 2.9: Induction on t.

(i) $t = c$, c a constant: Side induction on $c \in \mathrm{PR}^0$:
Subcase $c = \widetilde{0^0}$: $\widetilde{\lambda} x_1, \ldots, x_n.c := \widetilde{0}^n$.
$(\widetilde{\lambda} x_1, \ldots, x_n.c)^{\mathcal{N}}(a_1, \ldots, a_n) = 0 = (\widetilde{0^0})^{\mathcal{N}}[x_1 := a_1, \ldots, x_n := a_n]$
Subcase $c = f\widetilde{\circ}(g_1, \ldots, g_m)$: Let $\widetilde{\lambda}\vec{x}.g_i =: h_i$. $\widetilde{\lambda}\vec{x}.c := f\widetilde{\circ}(h_1, \ldots, h_m)$. $(\widetilde{\lambda}\vec{x}.c)^{\mathcal{N}}(\vec{a}) = f^{\mathcal{N}}(h_1^{\mathcal{N}}(\vec{a}), \ldots, h_m^{\mathcal{N}}(\vec{a})) = f^{\mathcal{N}}(g_1^{\mathcal{N}}[\vec{x} := \vec{a}], \ldots, g_m^{\mathcal{N}}[\vec{x} := \vec{a}]) = c^{\mathcal{N}}[\vec{x} := \vec{a}]$.

(ii) $\widetilde{\lambda} x_1, \ldots, x_n.x_i := \widetilde{\mathrm{proj}_i^n}$.
$(\widetilde{\lambda} x_1, \ldots, x_n.x_i)^{\mathcal{N}}(a_1, \ldots, a_n) = a_i = x_i^{\mathcal{N}}[x_1 := a_1, \ldots, x_n := a_n]$.

(iii) If $\widetilde{\lambda} x_1, \ldots, x_n.t_i = g_i$, $(i = 1, \ldots, m)$, then $\widetilde{\lambda} x_1, \ldots, x_n.ht_1, \ldots, t_m := h\widetilde{\circ}(g_1, \ldots, g_m)$, and

$$\begin{aligned}
(\widetilde{\lambda} x_1, \ldots, x_n.ht_1, \ldots, t_m)^{\mathcal{N}}(\vec{a}) &= h^{\mathcal{N}}(g_1^{\mathcal{N}}(\vec{a}), \ldots, g_m^{\mathcal{N}}(\vec{a})) \\
&= h^{\mathcal{N}}(t_1^{\mathcal{N}}[\vec{x} := \vec{a}], \ldots, t_m^{\mathcal{N}}[\vec{x} := \vec{a}]) \\
&= (ht_1, \ldots, t_m)^{\mathcal{N}}[\vec{x} := \vec{a}] \ .
\end{aligned}$$

Definition 2.11 (a) $+ := \mathrm{R}(\lambda x.x)(\lambda x, y', z.\mathrm{S}z)$. $+$ will be written infix. $\cdot :=$ $\mathrm{R}(\lambda x.0)(\lambda x, y', z.z + x)$. $\cdot$ will be written infix.
pred $:= \mathrm{R}0(\lambda y, z.y)$.
$\dot{-} := \mathrm{R}(\lambda x.x)(\lambda x, y', z.\mathrm{pred}(z))$. $\dot{-}$ will be written infix.

(b) If $f \in \mathrm{PR}^{n+1}$, then
$(\sum f) := (\mathrm{R}(\lambda x_1, \dots, x_n.0)(\lambda x_1, \dots, x_n, y', z.z + f(x_1, \dots, x_n, y')))(y)$.

Remark 2.12 *(a) $a + 0 = a$, $a + \mathrm{S}(b) = \mathrm{S}(a + b)$, therefore $+$ is ordinary addition.*

(b) $a \cdot 0 = 0$, $a \cdot (b + 1) = (a \cdot b) + a$, therefore $\cdot$ is multiplication.

(c) $\mathrm{pred}(0) = 0$, $\mathrm{pred}(b + 1) = b$.

(d) $a \dot{-} 0 = a$, $a \dot{-} (b + 1) = \mathrm{pred}(a \dot{-} b)$,
therefore $a \dot{-} b = \begin{cases} a - b & \textit{if } b \leq a \\ 0 & \textit{otherwise.} \end{cases}$

(e) $(\sum f)(\vec{a}, 0) = 0$, $(\sum f)(\vec{a}, b + 1) = (\sum f)(\vec{a}, b) + f(\vec{a}, b)$, therefore $(\sum f)(\vec{a}, b) = \sum_{i<b} f(\vec{a}, i)$.

Remark 2.13 *A relation $R \subseteq \mathbb{N}^n$ is primitive recursive, iff there exists an $f \in \mathrm{PR}^n$ such that $R = \{\vec{a} \in \mathbb{N}^n \mid f(\vec{a}) = 0\}$.*

Proof: $\lambda\vec{x}.1 \dot{-} g(\vec{x})$ switches between $g = \chi_R$ and $g = f$ as in the lemma.

Definition 2.14 of some formulas in the language $\mathcal{L}_{\mathrm{PR}}$.

(a) $s \leq t := s \dot{-} t = 0$;
$s < t := \mathrm{S}(s) \leq t$.

(b) $\forall x < t.A := \forall x.x < t \to A$,
$\exists x < t.A := \exists x.x < t \wedge A$ $(x \notin \mathrm{FV}(t))$.

(c) $\forall x \leq t.A := \forall x.x \leq t \to A$,
$\exists x \leq t.A := \exists x.x \leq t \wedge A$ $(x \notin \mathrm{FV}(t))$.

Definition 2.15 The set of Δ_0-formulas of the language $\mathcal{L}_{\mathrm{PR}}$, which is a subset of the formulas is inductively defined by:

1. Every prime formula of PR is a Δ_0-formula.
2. If A, B are Δ_0 formulas, so is $A \to B$.
3. If A is a Δ_0-formula and t is a PR-term such that $x \notin \mathrm{FV}(t)$, then $\forall x < t.A$ is a Δ_0-formula, too.

Remark 2.16 *If A, B are Δ_0-formulas, t is a term, $x \notin \mathrm{FV}(t)$, then $\neg A$, $A \wedge B$, $A \vee B$, $\exists x < t.A$, $\overset{\forall}{\exists}\, x \leq t.A$ are (in $\mathcal{N}$) equivalent to Δ_0-formulas. In this sense Δ_0-formulas are closed under $\neg$, $\wedge$, $\vee$ and bounded $\exists$.*

Proof: $\neg A \Leftrightarrow A \to \perp$, $A \vee B \Leftrightarrow (\neg A \to B)$, $A \wedge B \Leftrightarrow \neg(\neg(A) \vee \neg(B))$, $\exists x < t.A \Leftrightarrow \neg(\forall x < t.A)$, $\overset{\forall}{\exists} x \leq t.A \Leftrightarrow \overset{\forall}{\exists} x < \mathrm{S}(t).A$.

Lemma and Definition 2.17 *(a) If A is a Δ_0-formula of the language $\mathcal{L}_{\mathrm{PR}}$, $x_1, \ldots, x_n$ are distinct and $\mathrm{FV}(A) \subseteq \{x_1, \ldots, x_n\}$. Then the relation $\{(a_1, \ldots, a_n) \in \mathbb{N}^n \mid \mathcal{N} \models A[x_1 := a_1, \ldots, x_n := a_n]\}$ is primitive recursive. In this case we say, that R is* defined by the Δ_0-formula *A.*

(b) On the other hand, every primitive recursive relation can be defined by a Δ_0-formula.

Proof:
(a): We define by induction on the definition of A PR-terms r_A such that $\mathrm{FV}(r_A) = \mathrm{FV}(A)$ and if $\mathrm{FV}(A) \subseteq \{x_1, \ldots, x_n\}$, x_i distinct, then

$$(r_A)^{\mathcal{N}}[x_1 := a_1, \ldots, x_n := a_n] = 0 \Leftrightarrow \mathcal{N} \models A[x_1 := a_1, \ldots, x_n := a_n] \ .$$

Then with $f := \lambda x_1, \ldots, x_n.r_A$ according to Lemma 2.13 follows the assertion.
1. $A = \perp$: $r_A := \mathrm{S} \circ 0$.
2. $A = (s = t)$: $r_A := (s \dot{-} t) + (t \dot{-} s)$.
3. $A = B \to C$: $r_A := (1 \dot{-} r_B) \cdot r_C$.
4. $A = \forall y < t.B$, $y \notin \mathrm{FV}(t)$: Let $\mathrm{FV}(A) = \{x_1, \ldots, x_n\}$, x_i distinct. $f := \lambda x_1, \ldots, x_n, y.r_B$. $r_A := (\sum f)(\vec{x}, t)$.
(b): A primitive recursive relation R can be defined by the Δ_0-formula $\chi_R(\vec{x}) = S \circ 0$.

Corollary 2.18 *The set of primitive recursive relations is closed under $\cap$, $\cup$, $\setminus$ (difference), bounded quantification and replacement by primitive recursive functions (i.e. if $R \subseteq \mathbb{N}^k$ is a primitive recursive relation, $f_i : \mathbb{N}^n \to \mathbb{N}$ $(i = 1, \ldots, k)$, then the subset of $\mathbb{N}^n$ $\{(\vec{n}) \mid R(f_1(\vec{n}), \ldots, f_k(\vec{n}))\}$ is primitive recursive, too.*

Proof: The new relation can always be written as a Δ_0-formula.

Lemma 2.19 *If $f_1, \ldots, f_{k+1} \in \mathrm{PR}^n$ and $R_1, \ldots, R_k \subseteq \mathbb{N}^n$ are pairwise disjoint primitive recursive relations, then the function*

$$f : \mathbb{N}^n \to \mathbb{N},\ f(\vec{a}) := \begin{cases} f_1(\vec{a}) & \text{if } \vec{a} \in R_1, \\ \cdots & \cdots \\ f_k(\vec{a}) & \text{if } \vec{a} \in R_k, \\ f_{k+1}(\vec{a}) & \text{otherwise} \end{cases}$$

is primitive recursive.

Proof: Let $R_{k+1} := \mathbb{N}^n \setminus (R_1 \cup \cdots \cup R_k)$. $f := \lambda\vec{x}.(f_1(\vec{x})\chi_{R_1}(\vec{x}) + \cdots + f_{k+1}(\vec{x})\chi_{R_{k+1}}(\vec{x}))$.

Lemma 2.20 *Assume $g : \mathbb{N}^{n+1} \to \mathbb{N}$ primitive recursive. Then* *(a) $\overline{\mu}g$ is primitive recursive.*

(b) If there exists an $h \in \mathrm{PR}^{n+1}$ such that $\forall \vec{a} \in \mathbb{N}^n \, \exists i < h(\vec{a}).g(\vec{a}, i) = 0$, then (μg) is primitive recursive, too.

Proof:
(a) $p : \mathbb{N}^{n+1} \to \mathbb{N}$, $p(\vec{a}, c) := \begin{cases} c & \text{if } c < b \wedge g(\vec{a}, c) = 0 \wedge \forall i < c.g(\vec{a}, i) \neq 0 \\ b & \text{if } c = b \wedge \forall i < b.g(\vec{a}, i) \neq 0 \\ 0 & \text{otherwise} \end{cases}$ is primitive recursive. $(\overline{\mu}g)(\vec{a}, b) = (\sum p)(\vec{a}, \mathrm{S}(b))$.
(b) $(\mu g)(\vec{a}) = (\overline{\mu}g)(\vec{a}, h(\vec{a}))$.

Definition 2.21 Let $\pi : \mathbb{N}^2 \to \mathbb{N}$, $\pi(a, b) := (\sum_{i<a+b}(i+1)) + b = (\sum \mathrm{S})(a + b) + b$.

Lemma 2.22 *(a) $\pi : \mathbb{N}^2 \to \mathbb{N}$ is bijective.*

*(b) $a, b \leq \pi(a, b)$.
$0 < a \Rightarrow b < \pi(a, b)$.*

Remark: The picture is like this:

$$\begin{array}{ccccc} 0 = \pi(0,0) & 2 = \pi(0,1) & 5 = \pi(0,2) & 9 = \pi(0,3) & \cdots \\ 1 = \pi(1,0) & 4 = \pi(1,1) & 8 = \pi(1,2) & \cdots & \cdots \\ 3 = \pi(2,0) & 7 = \pi(2,1) & \cdots & \cdots & \cdots \\ 6 = \pi(3,0) & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array}$$

Proof:
(a): Let $f(c) := \sum_{i<c}(i+1)$. $f(c)$ is monotone, $f(0) = 0$, $f(c+1) = f(c)+c+1$. Assume $\pi(a, b) = \pi(a', b')$. Then $f(a+b) \leq \pi(a+b) < f(a+b+1)$, $f(a'+b') \leq \pi(a'+b') < f(a'+b'+1)$, $a+b = a'+b'$, $b = \pi(a, b) - f(a+b) = \pi(a', b') - f(a'+b') = b'$, $a = a'$.
Further if $n \in \mathbb{N}$, there exists some c such that $f(c) \leq n < f(c+1)$. $0 \leq b := n - f(c) < c+1$. $0 \leq a := c - b$, $\pi(a, b) = f(c) + b = n$.
(b) is clear.

Definition 2.23 $\pi_1(c) := \mu a < \mathrm{S}(c).\exists b \leq c.c = \pi(a, b)$.
$\pi_2(c) := \mu b < \mathrm{S}(c).c = \pi(\pi_1(c), b)$.

Remark 2.24 *π_1, π_2 are primitive recursive, $\pi_1(\pi(a, b)) = a$, $\pi_2(\pi(a, b)) = b$, $c = \pi(\pi_1(c), \pi_2(c))$.*

Proof: By 2.22.

Definition 2.25 (coding of finite sequences) $a * {<}b{>} := \pi(a, b) + 1$.
$\pi_i^-(a) := \pi_i(a \dot{-} 1)$ $(i = 1, 2)$.
$\tau(a, 0) := a$, $\tau(a, k+1) := \pi_1^-(\tau(a, k))$. (obviously $\tau(a, k) \neq 0 \Rightarrow \tau(a, k+1) <$

$\tau(a,k))$.
$\mathrm{lh}(a) := \mu k < \mathrm{S}(a).\tau(a,k) = 0$.

$$(a)_i := \begin{cases} \pi_2^-(\tau(a, \mathrm{lh}(a) \dot{-} (i+1))) & \text{if } i < \mathrm{lh}(a) \\ 0 & \text{otherwise.} \end{cases}$$

${<}{>} := 0$, ${<}a_1, \dots, a_{n+1}{>} := {<}a_1, \dots, a_n{>} * {<}a_{n+1}{>}$.

Lemma 2.26 *(a) The functions* $(a,b) \mapsto a * {<}b{>}$, π_i^-, τ, lh, $(a,i) \mapsto (a)_i$ *are obviously primitive recursive.*

(b) $\mathrm{lh}(a * {<}b{>}) = \mathrm{lh}(a) + 1$,
$(a * {<}b{>})_{\mathrm{lh}(a)} = b$, $(a * {<}b{>})_i = (a)_i$ *if* $i < \mathrm{lh}(a)$.

(c) $i < \mathrm{lh}(a) \Rightarrow (a)_i < a$.

(d) $(\mathrm{lh}(c) = \mathrm{lh}(c') \wedge \forall i < \mathrm{lh}(c).(c)_i = (c')_i) \Rightarrow c = c'$.

(e) $\mathrm{lh}({<}a_0, \dots, a_{n-1}{>}) = n$,
$({<}a_0, \dots, a_{n-1}{>})_i = a_i$ *(*$i < n$*).*
$a = {<}(a)_0, \dots, (a)_{n-1}{>}$ *with* $n := \mathrm{lh}(a)$.

Proof:
(a): clear.
(b): $c := a * {<}b{>}$. $\tau(c, i+1) = \tau(a,i)$, $\tau(c,0) \neq 0$. Therefore $\mathrm{lh}(c) = \mathrm{lh}(a) + 1$,
$(c)_{\mathrm{lh}(a)} = \pi_2^- \tau(c, \mathrm{lh}(c) \dot{-} (\mathrm{lh}(a)+1)) = \pi_2^-(\tau(c,0)) = \pi_2^-(c) = b$,
and if $i < \mathrm{lh}(a)$, $(c)_i = \pi_2^-(\tau(c, \mathrm{lh}(c) \dot{-} (i+1))) = \pi_2^-(\tau(c, \mathrm{lh}(a) - i + 1)) = \pi_2^-(\tau(a, \mathrm{lh}(a) \dot{-} i)) = (a)_i$.
(c) $(a)_i = \pi_2^-(\tau(a,j)) < \tau(a,j) \leq a$ for some j.
(d) Induction on $\mathrm{lh}(c)$:
If $\mathrm{lh}(c) = 0$, then $c = 0 = c'$.
$\mathrm{lh}(c) = k+1$: $c = a * {<}b{>}$, $c' = a' * {<}b'{>}$ for some a, b, a', b'. $b = (c)_{\mathrm{lh}(c)} = (c')_{\mathrm{lh}(c')} = b'$, $\mathrm{lh}(a) = \mathrm{lh}(c) \dot{-} 1 = \mathrm{lh}(a')$, $(a)_i = (c)_i = (c')_i = (a')_i$ for $i < \mathrm{lh}(a)$, by IH $a = a'$, $c = c'$.
(e) By (b) and (d).

Definition 2.27 If $f : \mathbb{N}^{n+1} \to \mathbb{N}$, then let $\overline{f} : \mathbb{N}^{n+1} \to \mathbb{N}$,
$\overline{f}(\vec{a}, b) := {<}f(\vec{a}, 0), \dots, f(\vec{a}, b){>}$.

Remark 2.28 $f \in \mathrm{PR}^{n+1}$ *iff* $\overline{f} \in \mathrm{PR}^{n+1}$.

Proof: "$\Rightarrow$": $\overline{f}(\vec{a}, 0) = {<}{>}$, $\overline{f}(\vec{a}, b+1) = \overline{f}(\vec{a}, b) * {<}f(\vec{a}, b){>}$. "$\Leftarrow$": $f(\vec{a}, n) = (\overline{f}(\vec{a}, n+1))_n$.

Lemma 2.29 *(Course of value recursion).*

(a) If $g \in \mathrm{PR}^{n+2}$*, then* $f : \mathbb{N}^{n+1} \to \mathbb{N}$, $f(\vec{a}, b) := g(\vec{a}, b, \overline{f}(\vec{a}, b))$ *is primitive recursive.*

(b) If $R \subseteq \mathbb{N}^{n+2}$ *is primitive recursive,* $Q \subseteq \mathbb{N}^{n+1}$ *such that*
$\forall (\vec{a}, b) \in \mathbb{N}^{n+1} [(\vec{a}, b) \in Q \Leftrightarrow (\vec{a}, b, \overline{\chi_Q}(\vec{a}, b)) \in R]$.
Then Q *is primitive recursive.*

Proof:
(a) $\overline{f}(\vec{a},0) = <>$, $\overline{f}(\vec{a},b{+}1) = \overline{f}(\vec{a},b) * <g(\vec{a},b,\overline{f}(\vec{a},b))>$, therefore $\overline{f}$ is primitive recursive, f is primitive recursive. (b) $\chi_Q(\vec{a},b) = \chi_R(\vec{a},b,\overline{\chi_Q}(\vec{a},b))$.

Lemma 2.29a *Assume $g \in \mathrm{PR}^k$, $h \in \mathrm{PR}^{k+1+l}$, $k_1,\dots,k_l \in \mathrm{PR}^{k+1}$,*
$\forall\vec{a},n.k(\vec{a},n) \le n$,
Let $f : \mathbb{N}^{k+1} \to \mathbb{N}$, $f(\vec{a},0) := g(\vec{a})$,
$f(\vec{a},n+1) := h(\vec{a},n,f(\vec{a},k_1(\vec{a},n)),\dots,f(\vec{a},k_l(\vec{a},n)))$.
Then $f \in \mathrm{PR}^{n+1}$.

Proof:
$$f(\vec{a},n) = \begin{cases} g(\vec{a}) & \text{if } n = 0 \\ h(\vec{a},n\dot{-}1,\overline{f}(\vec{a},n)_{k_1(\vec{a},n\dot{-}1)},\dots,\overline{f}(\vec{a},n)_{k_l(\vec{a},n\dot{-}1)}) & \text{otherwise .} \end{cases}$$

2.3 Recursive enumerable relations

Definition 2.30 A relation $Q \subseteq \mathbb{N}^n$ is called recursive enumerable, iff there exists a primitive recursive relation $R \subseteq \mathbb{N}^{n+1}$ such that $Q = \{\vec{a} \in \mathbb{N}^n \mid \exists b.(\vec{a},b) \in R\}$.

Remark 2.31 *(a) Every primitive recursive relation Q is recursive enumerable.*

(b) $\emptyset \ne Q \subseteq \mathbb{N}^k$ is recursive enumerable, iff $Q = \{(f_1(n),\dots,f_k(n)) \mid n \in \mathbb{N}\}$ for some $f_1,\dots,f_k \in \mathrm{PR}^1$.

Proof:
(a) $R := Q \times \mathbb{N}$.
(b) "$\Rightarrow$" Let R be as in the definition of recursive enumerable, $(a_1,\dots,a_k) \in Q$,
define $f_j : \mathbb{N} \to \mathbb{N}$, $f_j(n) := \begin{cases} (n)_j & \text{if } R((n)_0,\dots,(n)_k,(n)_{k+1}) \\ a_j & \text{otherwise.} \end{cases}$
One sees immediately $(f_1(n),\dots,f_k(n)) \in Q$, and if $(a_1,\dots,a_n) \in Q$, $R(a_1,\dots,a_n,b)$, then $f_j(<a_1,\dots,a_n,b>) = a_j$.
"$\Leftarrow$" $R(a,b) :\Leftrightarrow a = f(b)$.

Definition 2.32 Inductive definition of the *extended Σ_1-formulas*:

1. If A is Δ_0, then A is an extended Σ_1 formula.

2. If A, B are extended Σ_1-formulas, x a variable, t a term, $x \notin \mathrm{FV}(t)$, then $A \wedge B$, $A \vee B$, $\exists x.A$, $\forall x < t.A$ are extended Σ_1-formulas.

Lemma 2.33 *A relation $Q \subseteq \mathbb{N}^n$ is recursive enumerable, iff it can be defined by an extended Σ_1 formula, i.e. $Q = \{(a_1,\dots,a_n) \in \mathbb{N}^n \mid \mathcal{N} \models A[x_1 := a_1,\dots,x_n := a_n]\}$ for some distinct variables $x_1,\dots,x_n$ and extended Σ_1-formula A with $\mathrm{FV}(A) \subseteq \{x_1,\dots,x_n\}$.*

Proof:
A strict Σ_1-formula (often called just Σ-formula) is a formula $\exists z.C$ where C is Δ_0. By Lemma 2.17 the recursive enumerable relations are exactly those definable by a strict Σ_1-formula.
Therefore it suffices to show that for every extended Σ_1-formula A there exists a strict Σ_1 formula A' such that $\mathrm{FV}(A) = \mathrm{FV}(A')$ and if $\mathrm{FV}(A) \subseteq \{x_1, \dots, x_n\}$, $\mathcal{N} \models \forall x_1, \dots, x_n.(A \leftrightarrow A')$:
1. If A is Δ_0 let $A' := \exists z.A$ such that $z \notin \mathrm{FV}(A)$.
2. Let $A'_i := \exists x_i.A''_i$, $i = 1, 2$, $x \notin \mathrm{FV}(A_1) \cup \mathrm{BV}(A_1) \cup \mathrm{FV}(A_2) \cup \mathrm{FV}(t) \cup \{x_1\}$, w.l.o.g. $x_1 \notin \mathrm{BV}(A_1)$.
$(A_1 \overset{\wedge}{\vee} B_1)' := \exists x(A''_1[x_1 := \pi_1(x)] \overset{\wedge}{\vee} A''_2[x_2 := \pi_2(x)])$,
$(\exists z.A_1)' := \exists x.A''_1[z := \pi_1(x), x_1 := \pi_2(x)]$.
$(\forall z < t.A)' := \exists x.\forall z < t.\exists x_1 < x.A''_1$.

2.4 Recursive functions

Partial recursive functions will be what will be later referred to as the computable functions. At first sight it is not clear that they will capture the notion of computability. After some work we will be able to see, that programs can be represented by partial recursive functions.

Definition 2.34 (a) A function $f : \mathbb{N}^n \to_{\mathrm{par}} \mathbb{N}$ is *partial recursive*, iff the relation $\mathrm{Graph}(f) := \{(\vec{a}, b) \mid f(\vec{a}) \simeq b\}$ is recursive enumerable.

(b) A recursive function is a partial recursive function, which is total.

(c) A relation $R \subseteq \mathbb{N}^n$ is *recursive*, iff its characteristic function χ_R is recursive.

Lemma 2.34a *If f is primitive recursive, then it is recursive.*

Proof: f primitive recursive $\Rightarrow$ $\mathrm{Graph}(f)$ primitive recursive $\Rightarrow$ $\mathrm{Graph}(f)$ recursive enumerable $\Rightarrow$ f partial recursive, and since f is total, f is recursive.

Lemma 2.35 *(a) A relation $Q \subseteq \mathbb{N}^n$ is recursive, iff Q and $\mathbb{N}^n \setminus Q$ are recursive enumerable.*
Especially if Q is recursive, then it is recursive enumerable, too.

(b) $f : \mathbb{N}^n \to \mathbb{N}$ is recursive, iff $\mathrm{Graph}(f)$ is recursive.

(c) A relation $Q \subseteq \mathbb{N}^n$ is recursive enumerable, iff it is the domain of a n-ary partial recursive function.

(d) The set of n-ary partial recursive (recursive) functions is $\mathcal{R}^n_{\mathrm{par}}$ ($\mathcal{R}^n$). Here for $n \in \mathbb{N}$ $\mathcal{R}^n$ are simultaneously defined by

1. $0^n \in \mathcal{R}^n$, $\mathrm{S} \in \mathcal{R}^1$, $\mathrm{proj}^n_i \in \mathcal{R}^n$, ($1 \leq i \leq n$).

2. $h \in \mathcal{R}^m$, $m \geq 1$, $g_i \in \mathcal{R}^n$ $(i = 1, \ldots, m)$, then $h \circ (g_1, \ldots, g_m) \in \mathcal{R}^n$.

3. If $g \in \mathcal{R}^n$, $h \in \mathcal{R}^{n+2}$, then $(\mathrm{R}gh) \in \mathcal{R}^{n+1}$.

4. If $n \geq 1$, $g \in \mathcal{R}^{n+1}$, for all $\vec{a} \in \mathbb{N}^n$ there exists i such that $g(\vec{a}, i) = 0$, then $(\mu g) \in \mathcal{R}^n$.

Further $\mathcal{R}^n_{\mathrm{par}}$ is defined as $\mathcal{R}^n$, but without the condition on existence of an i such that $g(\vec{a}, i) = 0$ in 4.

$\mathcal{R} := \bigcup_{n \in \mathbb{N}} \mathcal{R}^n$, $\mathcal{R}_{\mathrm{par}} := \bigcup_{n \in \mathbb{N}} \mathcal{R}^n_{\mathrm{par}}$.

Proof:
(a) "$\Leftarrow$": $\chi_Q(\vec{a}) = b \Leftrightarrow (\vec{a} \in Q \wedge b = 1) \vee (\vec{a} \in \mathbb{N}^n \setminus Q \wedge b = 0)$, therefore $\mathrm{Graph}(\chi_Q)$ is recursive enumerable.
"$\Rightarrow$": $G := \mathrm{Graph}(\chi_Q)$ is recursive enumerable, $\vec{a} \in Q \Leftrightarrow (\vec{a}, 1) \in G$, $\vec{a} \in \mathbb{N}^n \setminus Q \Leftrightarrow (\vec{a}, 0) \in G$, Q, $\mathbb{N}^n \setminus Q$ are recursive enumerable.

(b) If f is recursive, then $\mathrm{Graph}(f)$ recursive enumerable, $\mathbb{N}^{n+1} \setminus \mathrm{Graph}(f) = \{(\vec{a}, b) \exists i((\vec{a}, i) \in \mathrm{Graph}(f) \wedge i \neq b\}$. If $\mathrm{Graph}(f)$ is recursive, then by (a) it is recursive enumerable, too.

(c) Let Q be recursive enumerable. Then $Q = \{\vec{a} \mid \exists b.R(\vec{a}, b)\}$ for some primitive recursive R. Let $f(\vec{a}) \simeq b \Leftrightarrow R(\vec{a}, b) \wedge \forall b' < b.\neg R(\vec{a}, b')$. $\mathrm{Graph}(f)$ is primitive recursive, therefore recursive enumerable and $\mathrm{dom}(f) = Q$.
Let $Q = \mathrm{dom}(f)$, f partial recursive, $\mathrm{Graph}(f) = \{(\vec{a}, b) \mid \exists c.R(\vec{a}, b, c)\}$, R primitive recursive. $Q = \{\vec{a} \mid \exists b.f(\vec{a}) \simeq b\} = \{\vec{a} \mid \exists b, c.R(\vec{a}, b, c)\}$, therefore recursive enumerable.

(d) Proof for "recursive". For "partial recursive" the proof is similar.
Every recursive function is in $\mathcal{R}$: If $f : \mathbb{N}^n \to \mathbb{N}$, $\mathrm{Graph}(f)$ is recursive enumerable. Let $f(\vec{a}) = b \Leftrightarrow \exists i.g(\vec{a}, b, i) = 0$, for some primitive recursive function g. Then $f(\vec{a}) = \pi_1(\mu z.g(\vec{a}, \pi_1(z), \pi_2(z)) = 0$, $f = \pi_1 \circ \mu h$, where let $h : \mathbb{N}^{n+1} \to \mathbb{N}$, $h(\vec{a}, z) := g(\vec{a}, \pi_1(z), \pi_2(z))$. h, π_1 are primitive recursive therefore in $\mathcal{R}$. $\forall \vec{a} \exists i.h(\vec{a}, i) = 0$, therefore f in $\mathcal{R}^n$.
In the other direction we have to show, that the set of recursive functions is closed under 1. - 4.:
1. the functions are primitive recursive, therefore its Graph is primitive recursive, therefore recursive enumerable.
2. $h \circ (g_1, \ldots, g_n)(\vec{a}) = c \Leftrightarrow \exists b_1, \ldots, b_n.g_1(\vec{a}) = b_1 \wedge \cdots \wedge g_n(\vec{a}) = b_n \wedge h(b_1, \ldots, b_n) = c$.
3. $(\mathrm{R}gh)(\vec{a}, b) = c \Leftrightarrow \exists c[(c)_0 = g(\vec{a}) \wedge \forall i < b.((c)_{i+1} = h(\vec{a}, i, (c)_i) \wedge c = (c)_b]$.
4. $(\mu g)(\vec{a}) = b \Leftrightarrow g(\vec{a}, b) = 0 \wedge \forall i < b.\exists c.(c \neq 0 \wedge g(\vec{a}, i) = c)$.

2.5 Computability

The goal is to define a mathematical structure which captures the notion of computability. More precisely we want to give mathematical precise notions for "decision procedure" and "effective procedure for a function f" as defined as follows:

Assume M is a set of "concrete objects" (like formulas, natural numbers), $X \subseteq M$.
A *decision procedure* for X relative to M is a method, which for every $a \in M$ after finitely many steps determines, whether a belongs to X or not. X is *decidable* (relative to M), iff a decision procedure for X relative to M exists.
Let $F : M \to N$, M, N sets of concrete objects.
An *effective procedure* for F is a method, which for every given $a \in M$ calculates the value $F(a)$ in finitely many steps. F is *computable*, iff an effective procedure for F exists.
Let F be a partial function from M to N, i.e. there exists $\mathrm{dom}(F) \subseteq M$, $F : \mathrm{dom}(F) \to N$.
An *effective procedure* for F is a method, which for $a \in M$ calculates, in case $a \in \mathrm{dom}(F)$, the value $F(a)$ in finitely many steps, for $a \notin M$ it might not terminate. F is *computable*, iff an effective procedure for F exists.
A *decision/computational problem* is the question, whether for a given set or relations/functions/partial functions there exists a decision procedure/effective procedure.
Remark: Every decision problem can be regarded as a computational problem for the function $\chi_X : M \to \{0, 1\}$, $\chi_X(a) := \begin{cases} 1 & \text{if } a \in X \\ 0 & \text{otherwise.} \end{cases}$
What is a method?
1. Mechanically (not using random procedure, oracles, intelligence, intuition).
2. Can be performed by an ideal machine (no upper bound on time and space available).

Church's Thesis A function $f : \mathbb{N}^n \to \mathbb{N}$ is computable iff it is recursive.
A n-ary partial function f is computable iff it is partial recursive.
A relation $Q \subseteq \mathbb{N}^n$ is decidable iff it is recursive.

It suffices to treat only the first of the two statements.
That every recursive/partial recursive function is computable can be seen by checking by induction on the definition of $\mathcal{R}$ in lemma 2.35 (c), that every function in $\mathcal{R}$ is computable. The other direction is a more sophisticated problem: Church's Thesis is not a mathematical theorem, but a philosophical statement, which can not be proved. Several machine models have been developed, which all compute the set of recursive/partial recursive functions. Therefore the theory of recursive functions is stable. More details will be given in a course on recursion theory, Turing machines etc.
We sketch, how a program in some programming language can be seen to be recursive (provided the program terminates on every input value). This should cover at least all possible assembler languages, in which higher programming languages are translated.
We assume that a program consists of a finite number of statements, numbered by natural numbers, and uses a finite number of registers containing natural numbers. A state of the program would then be a tuple $(a_1, \ldots, a_n, i)$, where i is the number of statement currently active and a_i is the content of the i-th register

(iff only these n registers are used). In a reasonable programming language, it should be possible to determine from $a_1, \ldots, a_n, i$ by an easy, therefore primitive recursive function, which is the next program statement and the content of the registers a_i, further to determine whether the program has stopped.
We code the state as above as a sequence $<a_1, \ldots, a_n, i>$, and we have now primitive recursive functions $f, g : \mathbb{N} \to \mathbb{N}$ an $f(<a_1, \ldots, a_n, i>)$ is the code for the next state and $g(<a_1, \ldots, a_n, i>) = 0$ if the program stops at state $(a_1, \ldots, a_n, i)$.
Let $h : \mathbb{N}^2 \to \mathbb{N}$, $h(a, 0) := a$, $h(a, n+1) := f(h(a, n))$. $h(a, n)$ is the code of the state of the program after n program steps.
Assume that the input of the program is contained in $a_1, \ldots, a_k$, the result in a_n, that at the beginning $a_{k+1} = \cdots = a_n = 0$ and that we start with program statement 1. Further assume that for every choice $a_1, \ldots, a_k$, the program starting as above eventually terminates. Let $f_0 : \mathbb{N}^k \to \mathbb{N}$ be the function calculated by the program.
Let $h_0 : \mathbb{N}^{k+1} \to \mathbb{N}$, $h_0(a_1, \ldots, a_k, n) := h(<a_1, \ldots, a_k, 0, \ldots, 0, 1>, n)$.
Then f_0 has the form $f_0(\vec{a}) = (h_0(\vec{a}, \mu x.g(h_0(\vec{a}, x)) = 0))_n$ and is therefore recursive.
If we drop the assumption that the program terminates, we get with the same argument that the partial function f_0 calculated by the program is partial recursive.

Chapter 3

Gödel's first incompleteness theorem

We will follow very closely [Buc93b].

3.1 Coding of Logic

Warning This chapter will be very formal. It is not necessary to understand every single detail, but it to get an understanding why in principle the coding we are going to do is possible and how to do it in this setting and in any other formalization of logic. There are of course many variations of codings, especially the concrete predicate calculus used can of course be replaced by any other complete standard calculus of predicate logic.

Gödel's incompleteness theorems are based on reasoning in a theory about the theory itself. The step from philosophical logic to mathematical logic was to start to reason about logic and mathematics using mathematical methods. Gödel pushed this further on by starting to reason about a theory in the theory itself, which naturally led to limitations. His incompleteness theorems are about the limits of what a theory can prove about itself.

In order to be able to reason about the theory itself we are working in, we need to have terms, formulas, proofs as objects of the language. Gödel showed that this can be done by coding these objects as natural numbers, if apart from some weak requirements we have natural numbers as basic objects. Before Gödel, the techniques were available, but most people thought that it is too complicated to carry this out. Gödel overcame this mental block.

We assume here, that we can have the natural numbers in our logical system. We then have to code terms, formulas, proofs etc. in our system and will do this by coding them as natural numbers. This will be done in a primitive recursive way.

Such a process of coding complicated structure as natural numbers is usually called Gödelization.

Definition 3.1 (a) The *Gödelization* of a set X is an injective function $\ulcorner\cdot\urcorner : X \to \mathbb{N}$, where we write $\ulcorner x\urcorner$ for $\ulcorner\cdot\urcorner(x)$, such that $\ulcorner X\urcorner := \{\ulcorner x\urcorner \mid x \in X\}$ is primitive recursive.
We will in most (but not all) cases write the same symbol $\ulcorner\cdot\urcorner$ for a Göelization.

(b) Let $X_1, \dots, X_n, X$ be sets with associated Gödelization $\ulcorner\cdot\urcorner$, $M \subseteq X_1 \times X_n$.
$\ulcorner M\urcorner := \{(\ulcorner u_1\urcorner, \dots, \ulcorner u_n\urcorner) \mid (u_1, \dots, u_n) \in M\}$.
If $f : M \to X$, then $f_{\ulcorner\cdot\urcorner} : \ulcorner M\urcorner \to \ulcorner X\urcorner$, $f_{\ulcorner\cdot\urcorner}(\ulcorner u_1\urcorner, \dots, \ulcorner u_n\urcorner) := \ulcorner f(u_1, \dots, u_n)\urcorner$. If the Gödelization is denoted by $\ulcorner\cdot\urcorner$, $\widetilde{f} := f_{\ulcorner\cdot\urcorner}$.
M, f are *primitive recursive*, (*recursive*, *recursive enumerable*) if $\ulcorner M\urcorner$, $\widetilde{f}$ are. If M, f are written infix, $\ulcorner M\urcorner$, $\widetilde{f}$ will be sometimes written infix, too.

(c) Let $\ulcorner n\urcorner := n$ for $n \in \mathbb{N}$. Obviously $\ulcorner\cdot\urcorner$ is a Gödelization for $\mathbb{N}$.

Definition 3.2 (a) Let $\underline{\text{Fun}}$, $\underline{\text{Rel}}$, $\underline{\text{Var}}$, $\underline{\text{Junc}}$, $\underline{\text{Quant}}$ be different natural numbers. (so $a \mapsto \underline{a}$ is a Gödelization on the finite set $\{\text{Fun}, \text{Rel}, \text{Var}, \text{Junc}\}$).

(b) A *primitive recursively represented language* is a pair $(\mathcal{L}, \text{enum})$ such that $\mathcal{L}$ is a language,
enum is a Gödelization of $\mathcal{L}$,
$\text{enum}(f) = \langle n, \underline{\text{Fun}}, i\rangle$ for some i, if f is an n-ary function symbol, and
$\text{enum}(R) = \langle n, \underline{\text{Rel}}, i\rangle$ for some $i \neq 0$, if R is an n-ary relation symbol.

(c) Let in the following $(\mathcal{L}, \text{enum})$ be a primitive recursively represented language, and assume that all function and relation symbols belong to $\mathcal{L}$, if not stated differently. Further term, formula etc. refers to $\mathcal{L}$ as well.
Abbreviation: $(a)_{i,j} := ((a)_i)_j$.

Definition 3.3 (a) A formula A is called *n-ary*, iff $\text{FV}(A) \subseteq \{v_1, \dots, v_n\}$ (v_i is the ith variable).
In this case we write $A(t_1, \dots, t_n)$ for $A[v_1 := t_1, \dots, v_n := t_n]$, and $\mathcal{M} \models A[a_1, \dots, a_n]$ for $\mathcal{M} \models A[v_1 := a_1, \dots, v_n := a_n]$.

(b) $\text{Junc} := \{\wedge, \vee, \to, \neg\}$.
$\text{Quant} := \{\forall, \exists\}$.
$\mathcal{L}^+ := \mathcal{L} \cup \{\perp\}$, $\mathcal{L}_{\text{Fun}}$ is the set of function symbols and $\mathcal{L}_{\text{Rel}}$ the set of relation symbols of $\mathcal{L}$.

(c) Var is the set of variables, Term the set of terms, Prim the set of prime formulas, For the set of formulas. $\text{For}_{\text{arity}} := \{(n, A) \mid A \text{ is an } n\text{-ary formula }\}$.
$\text{For}^n := \{A \mid (n, A) \in \text{For}_{\text{arity}}\}$.
$\text{FV} := \{(x, u) \mid u \text{ is an expression and } x \in \text{FV}(u)\}$.
$\text{subst} := \{(u, x, t) \mid t \text{ is substitutable for } x \text{ in } u, u \text{ a formula or term}\}$.

Definition 3.4 (omitted)

Definition 3.5 coding of all expressions of a language:

(a) We extend $\mathrm{enum} : \mathcal{L} \to \mathbb{N}$ to $\{\bot\} \cup \mathrm{Var} \cup \mathrm{Junc} \cup \mathrm{Quant}$ (i.e. all symbols used to built up terms and formulas) by defining

$$\begin{array}{rcl}
\mathrm{enum}(v_i) & := & <0, \underline{\mathrm{Var}}, i> (v_i \text{ being the } i\text{-th variable}) \\
\mathrm{enum}(\wedge) & := & <2, \underline{\mathrm{Junc}}, 0>, \\
\mathrm{enum}(\vee) & := & <2, \underline{\mathrm{Junc}}, 1>, \\
\mathrm{enum}(\to) & := & <2, \underline{\mathrm{Junc}}, 2>, \\
\mathrm{enum}(\neg) & := & <1, \underline{\mathrm{Junc}}, 3>, \\
\mathrm{enum}(\bot) & := & <0, \underline{\mathrm{Rel}}, 0>, \\
\mathrm{enum}(\forall) & := & <2, \underline{\mathrm{Quant}}, 0>, \\
\mathrm{enum}(\exists) & := & <2, \underline{\mathrm{Quant}}, 1>.
\end{array}$$

(Note that $\mathrm{enum}[\mathcal{L}^+]$, $\mathrm{enum}[\mathcal{L}_{\mathrm{Fun}}]$, $\mathrm{enum}[\mathcal{L}_{\mathrm{Rel}}]$ are primitive recursive).

(b) $\mathrm{arity}(a) := (a)_0$. (For $p \in \mathcal{L}^+ \cup \mathrm{Junc} \cup \mathrm{Quant} \cup \mathrm{Var}$, $\mathrm{arity}(\mathrm{enum}(p))$ is the arity of p, where variables have arity 0, quantifiers arity 2).

(c) A Gödelization of expressions is given by:
$\ulcorner v_i \urcorner := <\mathrm{enum}(v_i)>$,
$\ulcorner p(u_1, \dots, u_n) \urcorner := <\mathrm{enum}(p), \ulcorner u_1 \urcorner, \dots, \ulcorner u_n \urcorner>$. ($p \in \mathcal{L}^+ \cup \mathrm{Junc}$.
$\ulcorner \overset{\forall}{\exists} x A \urcorner := <\mathrm{enum}(\overset{\forall}{\exists}), \ulcorner x \urcorner, \ulcorner A \urcorner>$.

(d) To abstract from the notations we define:
$\mathrm{Op}(a) := (a)_0$, (so $\mathrm{Op}(\ulcorner p(u_1, \dots, u_n) \urcorner) = \mathrm{enum}(p)$).
If $p \in \mathcal{L}^+ \cup \mathrm{Junc} \cup \mathrm{Quant}$ of arity n, p can be regarded as a function of n-tuples of terms, formulas or variables and formulas into terms/formulas and therefore
$\widetilde{p}(a_1, \dots, a_n) := <\mathrm{enum}(p), a_1, \dots, a_n>$, which will be sometimes, following the conventions in Definition 3.1ab be written infix, if p is written infix.
$\mathrm{fst}(a) := (a)_1$, $\mathrm{snd}(a) = (a)_2$.
(So if $p \in \{\wedge, \vee, \to\}$, $\ulcorner A\, p\, B \urcorner = (\ulcorner A \urcorner\, \widetilde{p}\, \ulcorner B \urcorner)$,
$\mathrm{fst}(\ulcorner A\ j\ B \urcorner) = \ulcorner A \urcorner$, $\mathrm{snd}(\ulcorner A\ j\ B \urcorner) = \ulcorner B \urcorner$.
$\ulcorner \neg A \urcorner = \widetilde{\neg}(\ulcorner A \urcorner)$, $\mathrm{fst}(\ulcorner \neg A \urcorner) = \ulcorner A \urcorner$.
$\ulcorner \overset{\forall}{\exists} x.A \urcorner = \underset{\sim}{\overset{\forall}{\exists}}(\ulcorner x \urcorner, \ulcorner A \urcorner)$, $\mathrm{fst}(\ulcorner \overset{\forall}{\exists} x.A \urcorner) = \ulcorner x \urcorner$,
$\mathrm{snd}(\ulcorner \overset{\forall}{\exists} x.A \urcorner) = \ulcorner A \urcorner$).

(e) For $p \in \{\wedge, \vee, \to\}$, $\mathrm{For}_p(A) :\Leftrightarrow A$ is of the form $B\, p\, C$.
For $p \in \mathrm{Quant}$ $\mathrm{For}_p(A) :\Leftrightarrow A$ is of the form $px.B$.
$\mathrm{For}_\neg(A) :\Leftrightarrow A$ is of the form $\neg(A)$.

Lemma 3.6 *(a)* $\ulcorner \cdot \urcorner$ *is a Gödelization of* Var, Term *and* For *respectively. Especially* Var, Term, For *are primitive recursive (in the sense that* $\ulcorner \mathrm{Var} \urcorner$, $\ulcorner \mathrm{Term} \urcorner$, $\ulcorner \mathrm{For} \urcorner$ *are primitive recursive).*

(b) Prim, FV, $\mathrm{For}_{\mathrm{arity}}$, subst *and* For_p *for* $p \in \mathrm{Junc} \cup \mathrm{Quant}$ *are primitive recursive.*

Proof: $\ulcorner\cdot\urcorner$ is obviously injective.
The primitive recursiveness of the given sets and relations follows, since all Δ_0-definable relations are primitive recursive (Lemma 2.17, primitive recursive relations are closed under course-of-value-recursion (Lemma 2.29 (b)) and the following equivalences:
(it suffices to look only at the first 2 or 3 equivalences in order to see, that the others will work as well).

$$\begin{aligned}
a \in \ulcorner\mathrm{Var}\urcorner \quad &\Leftrightarrow \quad a = <<0, \underline{\mathrm{Var}}, (a)_{0,2}>> \\[1ex]
a \in \ulcorner\mathrm{Term}\urcorner \quad &\Leftrightarrow \quad a \in \ulcorner\mathrm{Var}\urcorner \vee \\
&\qquad [\mathrm{Op}(a) \in \mathrm{enum}[\mathcal{L}_{\mathrm{Fun}}] \wedge \mathrm{arity}(\mathrm{Op}(a)) = \mathrm{lh}(a) \dot- 1 \wedge \\
&\qquad\quad \forall i < \mathrm{lh}(a) \dot- 1((a)_{i+1} \in \ulcorner\mathrm{Term}\urcorner)] \\[1ex]
&\Leftrightarrow \quad a \in \ulcorner\mathrm{Var}\urcorner \vee \\
&\qquad [\mathrm{Op}(a) \in \mathrm{enum}[\mathcal{L}_{\mathrm{Fun}}] \wedge \mathrm{arity}(\mathrm{Op}(a)) = \mathrm{lh}(a) \dot- 1 \wedge \\
&\qquad\quad \forall i < \mathrm{lh}(a) \dot- 1.(\overline{\chi_{\ulcorner\mathrm{Term}\urcorner}}(a))_{(a)_{i+1}} = 1] \\[1ex]
a \in \ulcorner\mathrm{Prim}\urcorner \quad &\Leftrightarrow \quad \mathrm{lh}(a) > 0 \wedge \forall i < \mathrm{lh}(a) \dot- 1((a)_{i+1} \in \ulcorner\mathrm{Term}\urcorner) \wedge \\
&\qquad\quad \mathrm{Op}(a) \in \mathrm{enum}[\mathcal{L}_{\mathrm{Rel}}] \cup \{\mathrm{enum}(\perp)\} \wedge \\
&\qquad\qquad \mathrm{arity}(\mathrm{Op}(a)) = \mathrm{lh}(a) \dot- 1 \\[1ex]
a \in \ulcorner\mathrm{For}\urcorner \quad &\Leftrightarrow \quad a \in \ulcorner\mathrm{Prim}\urcorner \vee \\
&\qquad [\mathrm{lh}(a) = \mathrm{arity}(\mathrm{Op}(a)) + 1 \wedge \mathrm{Op}(a) \in \mathrm{enum}[\mathrm{Junc}] \\
&\qquad\quad \wedge \forall i < \mathrm{arity}(\mathrm{Op}(a)).(a)_{i+1} \in \ulcorner\mathrm{For}\urcorner] \vee \\
&\qquad [\mathrm{lh}(a) = 3 \wedge \mathrm{Op}(a) \in \mathrm{enum}[\mathrm{Quant}] \wedge \mathrm{fst}(a) \in \ulcorner\mathrm{Var}\urcorner \wedge \\
&\qquad\quad \mathrm{snd}(a) \in \ulcorner\mathrm{For}\urcorner] \\[1ex]
(x, a) \in \ulcorner\mathrm{FV}\urcorner \quad &\Leftrightarrow \quad x \in \ulcorner\mathrm{Var}\urcorner \wedge \\
&\qquad\quad [(a \in \ulcorner\mathrm{Var}\urcorner \wedge x = a) \vee \\
&\qquad\quad [a \in \ulcorner\mathrm{For}\urcorner \cup \ulcorner\mathrm{Term}\urcorner \wedge \\
&\qquad\qquad \exists i < \mathrm{lh}(\mathrm{Op}(a)).\ulcorner\mathrm{FV}\urcorner(x, (a)_{i+1}) \wedge \\
&\qquad\qquad\quad (\mathrm{Op}(a) \in \mathrm{enum}[\mathrm{Quant}] \to x \neq \mathrm{fst}(a))]] \\[1ex]
(n, a) \in \ulcorner\mathrm{For}_{\mathrm{arity}}\urcorner \quad &\Leftrightarrow \quad a \in \ulcorner\mathrm{For}\urcorner \wedge \forall i < a((i, a) \in \ulcorner\mathrm{FV}\urcorner \to 1 \leq (i)_{0,2} \leq n) \\[1ex]
(a, x, c) \in \ulcorner\mathrm{subst}\urcorner \quad &\Leftrightarrow \quad a \in \ulcorner\mathrm{For}\urcorner \wedge x \in \ulcorner\mathrm{Var}\urcorner \wedge c \in \ulcorner\mathrm{Term}\urcorner \wedge \\
&\qquad (a \in \ulcorner\mathrm{Prim}\urcorner \vee \\
&\qquad (\mathrm{Op}(a) \in \mathrm{enum}[\mathrm{Junc}] \wedge \forall i < \mathrm{arity}(\mathrm{Op}(a)). \\
&\qquad\qquad (((a)_{i+1}, x, c) \in \ulcorner\mathrm{subst}\urcorner)) \vee \\
&\qquad (\mathrm{Op}(a) \in \mathrm{enum}[\mathrm{Quant}] \wedge ((x, a) \in \ulcorner\mathrm{FV}\urcorner \to \\
&\qquad\qquad (\mathrm{fst}(a), c) \notin \ulcorner\mathrm{FV}\urcorner \wedge (\mathrm{snd}(a), x, c) \in \ulcorner\mathrm{subst}\urcorner)))))
\end{aligned}$$

$$a \in \ulcorner \mathrm{For}_p \urcorner \quad \Leftrightarrow \quad a \in \mathrm{For} \wedge \mathrm{Op}(a) = \mathrm{enum}(p)$$

Definition 3.7 Sub : $\mathbb{N}^3 \to \mathbb{N}$ is defined by:
$\mathrm{Sub}(a, b, c) :=$

$$\begin{cases} c & \text{if } a = b, \\ a & \text{if } (\mathrm{For}_\forall(a) \vee \mathrm{For}_\exists(a)) \wedge \mathrm{fst}(a) = b, \\ <\mathrm{Op}(a), \mathrm{Sub}((a)_1, b, c), \ldots , & \text{otherwise .} \\ \qquad \mathrm{Sub}((a)_{\mathrm{lh}(a) \dot{-} 1}, b, c)> & \end{cases}$$

Lemma 3.8 *(a)* Sub *is primitive recursive.*

(b) For $u \in \mathrm{Term} \cup \mathrm{For}$*,* $x \in \mathrm{Var}$*,* $t \in \mathrm{Term}$*,*
$\mathrm{Sub}(\ulcorner u \urcorner, \ulcorner x \urcorner, \ulcorner t \urcorner) = \ulcorner u[x := t] \urcorner$

Proof:
(a) Define $g(a, d, 0) := <\mathrm{Op}(a)>$, $g(a, d, m + 1) := g(a, d, m) * <(d)_{(a)_{m+1}}>$.
g is primitive recursive and $g(a, d, k) = <\mathrm{Op}(a), (d)_{(a)_1}, \ldots , (d)_{(a)_k}>$.
Let $h(b, c, a) := \mathrm{Sub}(a, b, c)$. Then

$$h(b, c, a) = \begin{cases} c & \text{if } a = b, \\ a & \text{if } (\mathrm{For}_\forall(a) \vee \mathrm{For}_\exists(a)) \wedge \mathrm{snd}(a) = b, , \\ g(a, \overline{h}(b, c, a), \mathrm{lh}(a) \dot{-} 1) & \text{otherwise.} \end{cases}$$

h is primitive recursive and $\mathrm{Sub}(a, b, c) = h(b, c, a)$ is primitive recursive.
(b): Induction on the definition of u. Let $\phi(u) := \mathrm{Sub}(\ulcorner u \urcorner, \ulcorner x \urcorner, \ulcorner t \urcorner)$.
If $u = x$, then $\phi(u) = \ulcorner t \urcorner = \ulcorner u[x := t] \urcorner$, and if u is a variable y, $y \neq x$, then $\ulcorner u \urcorner = <\mathrm{enum}(y)>$, $u \neq \ulcorner x \urcorner$, $\phi(u) = <\mathrm{Op}(u)> = u = \ulcorner u[x := t] \urcorner$.
If $u = f u_1, \ldots , u_n$, $f \in \mathcal{L}^+ \cup \mathrm{Junc}$. Then $\ulcorner u \urcorner = <\mathrm{enum}(f), \ulcorner u_1 \urcorner, \ldots , \ulcorner u_n \urcorner>$,

$$\begin{aligned} \phi(u) &= <\mathrm{enum}(f), \phi(u_1), \ldots , \phi(u_n)> \\ &\overset{\mathrm{IH}}{=} <\mathrm{enum}(f), \ulcorner u_1[x := t] \urcorner, \ldots , \ulcorner u_n[x := t] \urcorner> \\ &= \ulcorner u[x := t] \urcorner \end{aligned}$$

If $u = \overset{\forall}{\exists} y.A$ with $y \neq x$, then $\ulcorner u \urcorner = <\mathrm{enum}(\overset{\forall}{\exists}), \ulcorner y \urcorner, \ulcorner A \urcorner>$,

$$\begin{aligned} \phi(u) &= <\mathrm{enum}(\overset{\forall}{\exists}), \ulcorner y[x := t] \urcorner, \ulcorner A[x := t] \urcorner> \\ &= <\mathrm{enum}(\overset{\forall}{\exists}), \ulcorner y \urcorner, \ulcorner A[x := t] \urcorner> \\ &= \ulcorner \overset{\forall}{\exists} y.A[x := t] \urcorner = \ulcorner u[x := t] \urcorner \end{aligned}$$

and if $u = \overset{\forall}{\exists} x.A$, then $\phi(u) = \ulcorner u \urcorner = \ulcorner u[x := t] \urcorner$.

We are now going to formalize proofs as natural numbers. We will therefore first introduce natural deduction proofs in a sequent like formulation, since this is easier to be formalized. This will be just another way of organizing the derivations:

Definition 3.9 (a) In the following $\Gamma, \Gamma', \Gamma'', \Gamma''', \Delta$ denote finite sequences of formulas.
$\Gamma \subseteq \Delta$ iff all formulas in Γ occur in Δ,
$A \in \Gamma$ iff A occurs in Γ.
Γ, A, sometimes written as $\Gamma \cup A$, is the extension of the sequence of formulas Γ by one occurrence of the formula A.
$\Gamma \setminus A$ is the result of deleting all occurrences of A in Γ.
$\emptyset$ is the empty sequence of formulas.
$\mathrm{FV}_{\mathrm{seq}}(x, \Gamma) :\Leftrightarrow x$ is a free variable in one of the formulas in Γ.

(b) The sequence-like calculus of natural deduction SND derives assertions $\Gamma \Rightarrow A$ where Γ is a sequence of formulas and A is a formula (of a language $\mathcal{L}$). A statement $\Gamma \Rightarrow A$ should be read as: under assumptions Γ follows A.

The following are the rules of SND:

(Intro)	$\Gamma \Rightarrow A$	$(A \in \Gamma)$
$(\wedge^+)$	$\dfrac{\Gamma \Rightarrow A \qquad \Gamma \Rightarrow B}{\Gamma \Rightarrow A \wedge B}$	
$(\wedge_1^-)$	$\dfrac{\Gamma \Rightarrow A \wedge B}{\Gamma \Rightarrow A}$	
$(\wedge_2^-)$	$\dfrac{\Gamma \Rightarrow A \wedge B}{\Gamma \Rightarrow B}$	
$(\vee_1^+)$	$\dfrac{\Gamma \Rightarrow A}{\Gamma \Rightarrow A \vee B}$	
$(\vee_2^+)$	$\dfrac{\Gamma \Rightarrow B}{\Gamma \Rightarrow A \vee B}$	
$(\vee^-)$	$\dfrac{\Gamma \Rightarrow A \vee B \quad \Gamma' \Rightarrow C \quad \Gamma'' \Rightarrow C}{\Gamma''' \Rightarrow C}$	$(\Gamma \subseteq \Gamma'''; \Gamma' \subseteq \Gamma''', A$ $\Gamma'' \subseteq \Gamma''', B)$
$(\rightarrow^+)$	$\dfrac{\Gamma \Rightarrow A}{\Gamma' \Rightarrow B \rightarrow A}$	$(\Gamma \subseteq \Gamma', B)$
$(\rightarrow^-)$	$\dfrac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow A \rightarrow B}{\Gamma \Rightarrow B}$	
$(\forall^+)$	$\dfrac{\Gamma \Rightarrow A}{\Gamma \Rightarrow' \forall x.A}$	$(x \notin \mathrm{FV}(\Gamma),\ \Gamma \subseteq \Gamma')$
$(\forall^-)$	$\dfrac{\Gamma \Rightarrow \forall x.A}{\Gamma \Rightarrow A[x := t]}$	(t substitutable for x in A)
$(\exists^+)$	$\dfrac{\Gamma \Rightarrow A[x := t]}{\Gamma \Rightarrow \exists x.A}$	(t substitutable for x in A)
$(\exists^-)$	$\dfrac{\Gamma \Rightarrow \exists x A \quad \Gamma' \Rightarrow B}{\Gamma'' \Rightarrow B}$	$(x \notin \mathrm{FV}(\Gamma' \setminus A) \cup \mathrm{FV}(B)$ $\Gamma \subseteq \Gamma''; \Gamma' \subseteq \Gamma'', A)$
$(\neg^+)$	$\dfrac{\Gamma \Rightarrow \perp}{\Gamma' \Rightarrow \neg A}$	$(\Gamma \subseteq \Gamma', A)$
$(\neg^-)$	$\dfrac{\Gamma \Rightarrow A \quad \Gamma \Rightarrow \neg A}{\Gamma \Rightarrow \perp}$	
(EFQ)	$\dfrac{\Gamma \Rightarrow \perp}{\Gamma \Rightarrow C}$	
(Stab)	$\dfrac{\Gamma \Rightarrow \perp}{\Gamma' \Rightarrow A}$	$(\Gamma \subseteq \Gamma', \neg A)$

(c) Let Ruleset := $\{\text{Intro}, \wedge^+, \wedge_1^-, \wedge_2^-, \vee_1^+, \vee_2^+, \vee^-, \rightarrow^+, \rightarrow^-, \forall^+, \forall^-, \exists^+, \exists^-, \neg^+, \neg^-, \text{EFQ}, \text{Stab}\}$.
For $r \in$ Ruleset let premnum(r) be the number of premises of r.
If $n :=$ premnum(r), define
$\text{Rule}_r(\Gamma \Rightarrow A_1, \ldots, \Gamma_n \Rightarrow A_n, \Gamma \Rightarrow B) :\Leftrightarrow$
$\dfrac{\Gamma_1 \Rightarrow A_1 \quad \cdots \quad \Gamma_n \Rightarrow A_n}{\Gamma \Rightarrow B}$ is an instance of r.

(d) A proof in SND from a formulas Δ is a sequence $(D_1, \ldots, D_n)$ where $n \geq 1$, $D_i = \Gamma_i \Rightarrow A_i$ for some Γ_i, A_i, such that for each $i \in \{1, \ldots, n\}$, $A_i \in \Delta$ or there is a $r \in$ Ruleset and with $k :=$ premnum(r), $i_1, \ldots, i_k < i$ such that Rule$(D_{i_1}, \ldots, D_{i_k}, D_i)$. In this case D_n is called the *end sequence* of the proof.
Let $\text{Proof}_\Delta(D_1, \ldots, D_n)$ iff $(D_1, \ldots, D_n)$ is a proof. $(D_1, \ldots, D_n)$ is a proof of $\Gamma \Rightarrow A$ from formulas Δ iff it is proof from formulas Δ with end sequence $\Gamma \Rightarrow A$. $\Delta \vdash \Gamma \Rightarrow A :\Leftrightarrow \Gamma \Rightarrow A$ *is provable from formulas* Δ:$\Leftrightarrow$ there exists a proof of $\Gamma \Rightarrow A$ from formulas Δ. $\Delta \vdash A :\Leftrightarrow \Delta \vdash \emptyset \Rightarrow A$.

Remark 3.10 *A can be derived in ordinary natural deduction calculus from formulas Δ and assumptions contained in $\{A_1, \ldots, A_n\}$ iff $\Delta \vdash A_1, \ldots, A_n \Rightarrow A$.*

Proof: Both directions are immediate by induction on the derivation.

Definition 3.11 (a) The code of a sequence of formulas $A_1, \ldots, A_n$
$\ulcorner A_1, \ldots, A_n \urcorner := <\ulcorner A_1 \urcorner, \ldots, \ulcorner A_n \urcorner>$.
(especially $\ulcorner \emptyset \urcorner = <>$).

(b) $\ulcorner \Gamma \Rightarrow A \urcorner := \pi(\ulcorner \Gamma \urcorner, \ulcorner A \urcorner)$.
$\widetilde{\Gamma}_a := \pi_1(a)$, $\widetilde{\text{A}}_a := \pi_2(a)$.
(Therefore $\widetilde{\Gamma}_{\ulcorner \Gamma \Rightarrow A \urcorner} = \ulcorner \Gamma \urcorner$, $\widetilde{\text{A}}_{\ulcorner \Gamma \Rightarrow A \urcorner} = \ulcorner A \urcorner$).

(c) $\ulcorner (\Gamma_1 \Rightarrow A_1, \ldots, \Gamma_n \Rightarrow A_n) \urcorner := <\ulcorner \Gamma_1 \Rightarrow A_1 \urcorner, \ldots, \ulcorner \Gamma_n \Rightarrow A_n \urcorner>$.

(d) endseq$(D_1, \ldots, D_n) := D_n$.

Lemma 3.12 *(a) $\ulcorner \cdot \urcorner$ is a Gödelization of* Seq := $\{\Gamma \mid \Gamma$ *sequence of formulas* $\}$.
$\subseteq$, $\in$, FV_{seq} *are primitive recursive ($\ulcorner \subseteq \urcorner$, $\ulcorner \in \urcorner$ will be written infix).*
$\setminus$, $\cup$ *are primitive recursive (i.e. $\widetilde{\setminus}$, $\widetilde{\cup}$ are primitive recursive, written infix).*

(b) For every rule $r \in$ Ruleset Rule_r *is primitive recursive.*

(c) If Δ is primitive-recursive (recursive, recursive-enumerable), then Proof_Δ *is primitive recursive (recursive, recursive-enumerable) as well.*
endseq *is primitive recursive, i.e. there exists a unary primitive recursive function* $\widetilde{\text{endseq}}$ *such that* $\widetilde{\text{endseq}}(\ulcorner D_1, \ldots, D_n \urcorner) = \ulcorner D_n \urcorner$.

Proof:
(a): $\ulcorner : \urcorner \mathrm{Seq} \to \mathbb{N}$ is injective.
$\mathrm{Seq}(a) \Leftrightarrow \forall i < \mathrm{lh}(a).(a)_i \in \ulcorner \mathrm{For} \urcorner$.
$\ulcorner \subseteq \urcorner (a,b) \Leftrightarrow \mathrm{Seq}(a) \wedge \mathrm{Seq}(b) \wedge \forall i < \mathrm{lh}(a).\exists j < \mathrm{lh}(b).(a)_i = (b)_j$.
$\ulcorner \in \urcorner (a,b) \Leftrightarrow \mathrm{Seq}(b) \wedge \exists i < \mathrm{lh}(b).a = (b)_i$.
$\ulcorner \mathrm{FV}_{\mathrm{seq}} \urcorner (a,b) \Leftrightarrow \mathrm{Var}(a) \wedge \mathrm{Seq}(b) \wedge \exists i < \mathrm{lh}(b).\ulcorner \mathrm{FV} \urcorner (a,(b)_i)$.
For the verification of the primitive recursiveness of $\widetilde{\setminus}$ define first $\widetilde{\setminus}_0$ by:
$\widetilde{\setminus}_0(n,m,0) := <>$, $\widetilde{\setminus}_0(n,m,k+1) := \begin{cases} \widetilde{\setminus}_0(n,m,k) * <(n)_k> & \text{if } (n)_k \neq m, \\ \widetilde{\setminus}_0(n,m,k) & \text{otherwise.} \end{cases}$.
Now $n \mathbin{\widetilde{\setminus}} m := \widetilde{\setminus}_0(n,m,\mathrm{lh}(n))$.
$n \mathbin{\widetilde{\cup}} m := n * <m>$.
(b) If $n = \mathrm{premnum}(r)$, then $\mathrm{Rule}_r(a_1,\dots,a_n) \Leftrightarrow$
$\widetilde{\Gamma}_{a_1} \in \ulcorner \mathrm{Seq} \urcorner \wedge \cdots \widetilde{\Gamma}_{a_n} \in \ulcorner \mathrm{Seq} \urcorner \wedge$
$\widetilde{\mathrm{A}}_{a_1} \in \ulcorner \mathrm{For} \urcorner \wedge \cdots \widetilde{\mathrm{A}}_{a_n} \in \ulcorner \mathrm{For} \urcorner \wedge$
$\mathrm{rule}_r(\widetilde{\Gamma}_{a_1}, \widetilde{\mathrm{A}}_{a_1}, \dots, \widetilde{\Gamma}_{a_n}, \widetilde{\mathrm{A}}_{a_n})$,

where rule_r are defined and verified to be primitive recursive by the following equivalences (in these we use G, G', G'', G''' for natural numbers usually denoting sequences)

(not all cases have to be presented. Interesting are Intro, $\vee^-$, $\forall^+$, $\forall^-$).

$$
\begin{array}{rcl}
\mathrm{rule}_{\mathrm{Intro}}(G,a) & \Leftrightarrow & a \ulcorner \in \urcorner G. \\[1em]
\mathrm{rule}_{\wedge^+}(G,a,G',b, & \Leftrightarrow & G = G' = G'' \wedge c = a \mathbin{\widetilde{\wedge}} b. \\
G'',c) & & \\[1em]
\mathrm{rule}_{\wedge^-}(a,G,b,G') & \Leftrightarrow & G = G' \wedge a = b \mathbin{\widetilde{\wedge}} \mathrm{snd}(a). \\[1em]
\mathrm{rule}_{\wedge^-}(G,a,G',b) & \Leftrightarrow & G' = G \wedge a = \mathrm{fst}(a) \mathbin{\widetilde{\wedge}} b. \\[1em]
\mathrm{rule}_{\vee_1^+}(G,a,G',b) & \Leftrightarrow & G' = G \wedge b = a \mathbin{\widetilde{\vee}} \mathrm{snd}(b). \\[1em]
\mathrm{rule}_{\vee_2^+}(G,a,G',b) & \Leftrightarrow & G' = G \wedge b = \mathrm{fst}(b) \mathbin{\widetilde{\vee}} \mathrm{snd}(a). \\[1em]
\mathrm{rule}_{\vee^-}(G,a,G',b, & \Leftrightarrow & b = c = d \wedge \mathrm{For}_{\vee}(a) \wedge \\
G'',c,G''',d) & & G \ulcorner \subseteq \urcorner G''' \wedge G' \ulcorner \subseteq \urcorner G''' \mathbin{\widetilde{\cup}} \mathrm{fst}(a) \wedge \\
 & & G'' \ulcorner \subseteq \urcorner G''' \mathbin{\widetilde{\cup}} \mathrm{snd}(a). \\[1em]
\mathrm{rule}_{\to^+}(G,a,G',b) & \Leftrightarrow & \mathrm{For}_{\to}(b) \wedge a = \mathrm{snd}(b) \wedge \\
 & & G \ulcorner \subseteq \urcorner G' \mathbin{\widetilde{\cup}} \mathrm{fst}(b). \\[1em]
\mathrm{rule}_{\to^-}(G,a,G',b, & \Leftrightarrow & b = a \mathbin{\widetilde{\to}} c \wedge G = G' = G''. \\
G'',c) & &
\end{array}
$$

$$\begin{array}{rcl}
\mathrm{rule}_{\forall+}(G,a,G',b) & \Leftrightarrow & G \ulcorner\subseteq\urcorner G' \wedge b = \widetilde{\forall}(\mathrm{fst}(b),a) \wedge \neg\mathrm{FV}_{\mathrm{seq}}(\mathrm{fst}(b),G). \\[1em]
\mathrm{rule}_{\forall-}(G,a,G',b) & \Leftrightarrow & G = G' \wedge \mathrm{For}_{\forall}(a) \wedge \\
 & & \exists w \leq \max\{b, \ulcorner v_0 \urcorner\}.(\ulcorner\mathrm{subst}\urcorner(\mathrm{snd}(a),\mathrm{fst}(a),w) \wedge \\
 & & \quad b = \mathrm{Sub}(\mathrm{snd}(a),\mathrm{fst}(a),w)). \\[1em]
 & & (\text{possibly } w = \ulcorner v_0 \urcorner > b \text{ in case} \\
 & & \neg\ulcorner\mathrm{FV}\urcorner(\mathrm{fst}(a),\mathrm{snd}(a)) \text{ necessary}) \\[1em]
\mathrm{rule}_{\exists+}(G,a,G',b) & \Leftrightarrow & G = G' \wedge \mathrm{For}_{\exists}(b) \wedge \\
 & & \exists w \leq \max\{a, \ulcorner v_0 \urcorner\}.(\ulcorner\mathrm{subst}\urcorner(\mathrm{snd}(b),\mathrm{fst}(b),w) \wedge \\
 & & \quad a = \mathrm{Sub}(\mathrm{snd}(b),\mathrm{fst}(b),w)). \\[1em]
\mathrm{rule}_{\exists-}(G,a,G',b, & \Leftrightarrow & b = c \wedge \mathrm{For}_{\exists}(a) \wedge \\
G'',c) & & \neg\ulcorner\mathrm{FV}\urcorner_{\mathrm{seq}}(\mathrm{fst}(a), G' \mathbin{\widetilde{\setminus}} \mathrm{snd}(a)) \wedge \neg\ulcorner\mathrm{FV}\urcorner(\mathrm{fst}(a),b) \wedge \\
 & & G \ulcorner\subseteq\urcorner G'' \wedge G' \ulcorner\subseteq\urcorner G'' \mathbin{\widetilde{\cup}} \mathrm{snd}(a). \\[1em]
\mathrm{rule}_{\neg+}(G,a,G',b) & \Leftrightarrow & \mathrm{For}_{\neg}(b) \wedge a = \ulcorner\bot\urcorner \wedge \\
 & & G \ulcorner\subseteq\urcorner G' \mathbin{\widetilde{\cup}} \mathrm{snd}(b) \\[1em]
\mathrm{rule}_{\neg-}(G,a,G',b, & \Leftrightarrow & b = \widetilde{\neg}(a) \wedge c = \ulcorner\bot\urcorner \wedge \\
G'',c) & & G = G' = G'' \\[1em]
\mathrm{rule}_{\mathrm{EFQ}}(G,a,G',b) & \Leftrightarrow & G = G' \wedge a = \ulcorner\bot\urcorner. \\[1em]
\mathrm{rule}_{\mathrm{Stab}}(G,a,G',b) & \Leftrightarrow & a = \ulcorner\bot\urcorner \wedge G \ulcorner\subseteq\urcorner G' \mathbin{\widetilde{\cup}} \widetilde{\neg}(b).
\end{array}$$

(c)

$$\begin{array}{rcl}
\ulcorner\mathrm{Proof}_{\Delta}\urcorner(n) & \Leftrightarrow & \mathrm{lh}(n) \geq 1 \wedge \\
 & & \forall i < \mathrm{lh}(n)(\widetilde{\Gamma}_{(n)_i} \in \mathrm{Seq} \wedge \\
 & & \quad (\widetilde{\mathrm{A}}_{(n)_i} \in \ulcorner\Delta\urcorner \vee \\
 & & \quad \bigvee_{r \in \mathrm{Ruleset}} (\exists i_1, \ldots, i_{\mathrm{premnum}(r)} < i. \\
 & & \qquad \mathrm{Rule}_r((n)_{i_1}, \ldots, (n)_{i_{\mathrm{premnum}(r)}}, (n)_i))).
\end{array}$$

$\widetilde{\mathrm{endseq}}(n) := (n)_{\mathrm{lh}(n) \dot{-} 1}$.

Theorem 3.13 *Assume that Σ is a recursive enumerable axiom system. Then $\{A \mid \Sigma \vdash A\}$ is recursive enumerable.*

Proof: $a \in \{\ulcorner A \urcorner \mid \Sigma \vdash A\} \Leftrightarrow$ there exists a derivation $<D_0, \ldots, D_n>$ such that $\widetilde{\Gamma}_{D_n} = \ulcorner\emptyset\urcorner \wedge \widetilde{\mathrm{A}}_{D_n} = \ulcorner A \urcorner \Leftrightarrow \exists b(\mathrm{Proof}_{\Sigma}(b) \wedge \widetilde{\Gamma}_{\widetilde{\mathrm{endseq}}(b)} = \ulcorner\emptyset\urcorner \wedge \widetilde{\mathrm{A}}_{\widetilde{\mathrm{endseq}}(b)} = a)$.

3.2 Recursive Axiom Systems and Representation of Relations and Functions

Definition 3.14 A theory T is *recursively axiomatizable*, if $\mathcal{L}(T)$ is primitive recursively represented and T has a recursive axiom system.

Lemma 3.15 *Let T be a theory with primitive recursive represented language $\mathcal{L}(T)$. The following is equivalent:*

(i) *T is recursive enumerable*

(ii) *T has a primitive recursive axiom system.*

(iii) *T is recursive axiomatizable.*

(iii) *T has a a recursive enumerable axiom system.*

Proof: Let $\mathcal{L} := \mathcal{L}(T)$.
(i) $\Rightarrow$ (ii): Let $f \in \mathrm{PR}^1$ such that $\ulcorner T \urcorner = f(\mathbb{N})$, $g(n)$ the formula such that $f(n) = \ulcorner g(n) \urcorner$, $B_n := g(0) \wedge (g(1) \wedge \cdots (g(n-1) \wedge g(n)))$. $\Sigma := \{B_n \mid n \in \mathbb{N}\}$. Σ is an axiom system for T. Further $n \mapsto \ulcorner B_n \urcorner$ is primitive recursive, $n < \ulcorner B_n \urcorner$, therefore $a \in \ulcorner \Sigma \urcorner \Leftrightarrow \exists n < a(a = \ulcorner B_n \urcorner)$ is primitive recursive.
(ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv): trivial.
(iv) $\Rightarrow$ (i): theorem 3.13, For^0 is primitive recursive, $T = \{A \mid \Sigma \vdash A\} \cap \mathrm{For}^0$.

Theorem 3.16 *If a theory T is recursive axiomatizable and complete, then T is recursive.*

Proof: If T is inconsistent, $T = \mathrm{For}^0$. Otherwise $a \notin \ulcorner T \urcorner \Leftrightarrow (a \notin \ulcorner \mathrm{For}^0 \urcorner \vee \tilde{\neg}(a) \in \ulcorner T \urcorner$. By Lemma 3.15 and Lemma 2.35 (a) follows the assertion.

Definition 3.17 (a) A structure $\mathcal{N}_1$ in an extension of $\mathcal{L}_\mathbb{N}$ is $\mathcal{L}_\mathbb{N}$-*standard*, if it is an expansion of $\mathcal{N}_0$ (see Definitions 1.21 and 1.6).

(b) For $n \in \mathbb{N}$ we define the term $\underline{n}$: $\underline{0} := 0$, $\underline{n+1} := \mathrm{S}(\underline{n})$. These terms are called digits.

Remark 3.18 *If $\mathcal{N}_1$ is a $\mathcal{L}_\mathbb{N}$-standard structure, A an n-ary formula A, m_1, $\ldots, m_n \in \mathbb{N}$ then $\mathcal{N}_1 \models A[m_1, \ldots, m_n] \Leftrightarrow \mathcal{N}_1 \models A(\underline{m_1}, \ldots, \underline{m_n})$.*

Definition 3.19 Let $\mathcal{M}$ be a $\mathcal{L}$-structure. A relation $R \subseteq |\mathcal{M}|^n$ is *defined by an n-ary formula A in $\mathcal{M}$* iff $R = \{(a_1, \ldots, a_n) \mid \mathcal{M} \models A[a_1, \ldots, a_n]\}$. It is *definable*, iff it is defined by an n-ary formula A.
A function is in $\mathcal{M}$ *defined by A* or *definable*, iff this holds for its graph.

Definition 3.20 Let Σ be an axiom system in an extension of $\mathcal{L}_\mathbb{N}$ which proves the equality axioms.

(a) An n-ary formula A *represents in* Σ *the relation* $R \subseteq \mathbb{N}^n$, iff for all $a_1, \ldots, a_n \in \mathbb{N}$ we have

$$\begin{array}{rcl} R(a_1, \ldots, a_n) & \Rightarrow & \Sigma \vdash A(\underline{a_1}, \ldots, \underline{a_n}) \\ \neg R(a_1, \ldots, a_n) & \Rightarrow & \Sigma \vdash \neg A(\underline{a_1}, \ldots, \underline{a_n}). \end{array}$$

If only the first condition holds, then $\mathcal{R}$ *represents* R *weakly.*

(b) An $n+1$ ary formula A *represents in* Σ *the function* $f : \mathbb{N}^n \to \mathbb{N}$ iff for all $\vec{a} \in \mathbb{N}^n$, $b \in \mathbb{N}$ we have

$$\begin{array}{rcl} f(\vec{a}) = b & \Rightarrow & \Sigma \vdash A(\underline{\vec{a}}, \underline{b}) \land \forall y(A(\underline{\vec{a}}, y) \to y = \underline{b}). \\ f(\vec{a}) \neq b & \Rightarrow & \Sigma \vdash \neg A(\underline{\vec{a}}, \underline{b}). \end{array}$$

(If $\Sigma \vdash \neg(\underline{b} = \underline{c})$ for $b \neq c$, the first condition implies the second).

(c) $R \subseteq \mathbb{N}^n$ ($f : \mathbb{N}^n \to \mathbb{N}$) are *(weakly) representable in* Σ if they are (weakly) represented in Σ by some formula A.

Remark 3.21 *If* $\mathcal{N}_1$ *is* $\mathcal{L}_{\mathbb{N}}$*-standard, and every primitive recursive relation can be defined in* $\mathcal{N}_1$*, then every recursive enumerable relation can be defined in* $\mathcal{N}_1$*, too.*

Proof: Let R be n-ary, $R(\vec{a}) \Leftrightarrow \exists x.Q(\vec{a}, x)$, Q primitive recursive. Let $Q(\vec{a}, x)$ $\Leftrightarrow \mathcal{N}_1 \models A[\vec{a}, x]$. Then $R(\vec{a}) \Leftrightarrow \mathcal{N}_1 \models \exists v_{n+1}.A[\vec{a}]$.

3.3 Incompleteness

Definition 3.22 Let $\mathrm{s} \in \mathrm{PR}^2$, $\mathrm{s}(a, k) := \mathrm{Sub}(a, \ulcorner v_1 \urcorner, \ulcorner \underline{k} \urcorner)$. (If A is unary, $\mathrm{s}(\ulcorner A \urcorner, k) = \ulcorner A(\underline{k}) \urcorner$.)

Lemma 3.23 *(Fixed point lemma).*

(a) Let $\mathcal{N}_1$ *be a* $\mathcal{L}_{\mathbb{N}}$*-standard structure, in which the primitive recursive relation* $\{(k, b) \in \mathbb{N}^2 \mid s(k, k) = b\}$ *can be defined. Let* D *be a unary formula. Then there exists a sentence* G *such that* $\mathcal{N}_1 \models G \leftrightarrow D(\underline{\ulcorner G \urcorner})$.

(b) Let Σ *be an axiom system from which the equality axioms can be proved and in which* $\lambda a.\mathrm{s}(a, a)$ *is representable,* D *be a unary* $\mathcal{L}(\Sigma)$*-formula. Then there exists an* $\mathcal{L}(\Sigma)$*-sentence* G *such that* $\Sigma \vdash G \leftrightarrow D(\underline{\ulcorner G \urcorner})$.

Proof: (a) We give first a proof with some motivation and then the proof as a compact argument:
Assume first that a function $f : \mathbb{N} \to \mathbb{N}$ which is defined by a formula A in $\mathcal{N}_1$, i.e.

$$\mathcal{N}_1 \models A(\underline{k}, \underline{b}) \Leftrightarrow f(k) = b\ .$$

Let for this f, A, $C_A := \exists y(A(v_1, y) \land D(y))$. Then we have

$$\mathcal{N}_1 \models C_A(\underline{k}) \quad \Leftrightarrow \quad \exists b \in \mathbb{N}((\mathcal{N}_1 \models A(\underline{k}, \underline{b})) \land \mathcal{N}_1 \models D(\underline{b}))$$

$$\begin{aligned} &\Leftrightarrow \quad \exists b(f(k) = b \wedge \mathcal{N}_1 \models D(\underline{b})) \\ &\Leftrightarrow \quad \mathcal{N}_1 \models D(\underline{f(k)}) \ , \end{aligned}$$

i.e.

$$\mathcal{N}_1 \models C_A(\underline{k}) \leftrightarrow D(\underline{f(k)}) \ .$$

If we have now k such that $f(k) = \ulcorner C_A(\underline{k})\urcorner$, then we have

$$\mathcal{N}_1 \models C_A(\underline{k}) \leftrightarrow D(\underline{\ulcorner C_A(\underline{k})\urcorner})$$

and with $G := C_A(\underline{k})$ follows the assertion.
We cannot define $f(k) := \ulcorner C_A(\underline{k})\urcorner$, since C depends on A which defined f. However we can define $f(k)$ such that $f(\ulcorner B\urcorner) = \ulcorner B(\underline{\ulcorner B\urcorner})\urcorner$ for unary formulas B, namely $f(k) := \mathrm{s}(k,k)$. This specific f can be represented by assumption by some A and if we define $k := \ulcorner C_A\urcorner$, then we get $f(k) = f(\ulcorner C_A\urcorner) = \ulcorner C_A(\underline{\ulcorner C_A\urcorner})\urcorner = \ulcorner C_A(\underline{k})\urcorner$ and are done.

The compact proof is as follows:
Let $\{(k,b) \in \mathbb{N}^2 \mid s(k,k) = b\}$ be defined by the formula A, i.e. $\mathcal{N}_1 \models A(\underline{k},\underline{b}) \Leftrightarrow \mathrm{s}(k,k) = b$. Let $C := \exists y(A(v_1,y) \wedge D(y))$, y a new variable.
Then

$$\begin{aligned} \mathcal{N}_1 \models C(\underline{k}) \quad &\Leftrightarrow \quad \exists b \in \mathbb{N}((\mathcal{N}_1 \models A(\underline{k},\underline{b})) \wedge \mathcal{N}_1 \models D(\underline{b})) \\ &\Leftrightarrow \quad \exists b(\mathrm{s}(k,k) = b \wedge \mathcal{N}_1 \models D(\underline{b})) \\ &\Leftrightarrow \quad \mathcal{N}_1 \models D(\underline{\mathrm{s}(k,k)}). \end{aligned}$$

Let $k := \ulcorner C\urcorner$, $G := C(\underline{k})$.
$\ulcorner G\urcorner = \mathrm{Sub}(\ulcorner C\urcorner, \ulcorner v_1\urcorner, k) = \mathrm{s}(k,k)$.
Therefore

$$\begin{aligned} \mathcal{N}_1 \models G \quad &\Leftrightarrow \quad \mathcal{N}_1 \models C(\underline{k}) \\ &\Leftrightarrow \quad \mathcal{N}_1 \models D(\underline{\mathrm{s}(k,k)}) \\ &\Leftrightarrow \quad \mathcal{N}_1 \models D(\underline{\ulcorner G\urcorner}). \end{aligned}$$

(b) Similar to (a):
Assume A represents $\lambda x.\mathrm{s}(x,x)$ and $C := \exists y(A(v_1,y) \wedge D(y))$. Then for all $k \in \mathbb{N}$ $\Sigma \vdash C(\underline{k}) \leftrightarrow D(\underline{\mathrm{s}(k,k)})$.
[Let $b := \mathrm{s}(k,k)$. $\Sigma \vdash A(\underline{k},\underline{b}) \wedge \forall y(A(\underline{k},\underline{y}) \to \underline{b} = y)$. Therefore $\Sigma \vdash \exists y(A(\underline{k},y) \wedge D(y)) \leftrightarrow D(\underline{b})$.]
Let $k := \ulcorner C\urcorner$, $G := C(\underline{k})$. Then $\mathrm{s}(k,k) = \ulcorner C(\underline{k})\urcorner = \ulcorner G\urcorner$.
$\Sigma \vdash G \leftrightarrow D(\underline{\ulcorner G\urcorner})$.

Theorem 3.24 *(Tarski) Let $\mathcal{N}_1$ be $\mathcal{L}_{\mathbb{N}}$-standard and assume that every primitive recursive relation is definable in $\mathcal{N}_1$. Then $\ulcorner \mathrm{Th}(\mathcal{N}_1)\urcorner$ is not in $\mathcal{N}_1$ definable and therefore $\mathrm{Th}(\mathcal{N}_1)$ is not recursive enumerable and not recursive axiomatizable.*

Proof:

Assume $\mathrm{Th}(\mathcal{N}_1)$ can be defined by a unary formula D. By the fixed point lemma 3.23 exists a formula $G \in \mathrm{For}^0$ such that

$$\mathcal{N}_1 \models G \leftrightarrow \neg D(\underline{\ulcorner G \urcorner}) \ .$$

But then $\mathcal{N}_1 \models G \Leftrightarrow G \in \mathrm{Th}(\mathcal{N}_1) \Leftrightarrow \mathcal{N}_1 \models D(\underline{\ulcorner G \urcorner}) \Leftrightarrow \mathcal{N}_1 \not\models G$, a contradiction.

Theorem 3.25 *A consistent theory T, in which all recursive functions are representable and which contains the equality axioms, is undecidable (i.e. not recursive).*

Proof:
Assume T is recursive.
Then $\chi_{\ulcorner T \urcorner}$ and therefore as well the 1-ary relation $\ulcorner T \urcorner$ are representable in T. Therefore there exists a unary $\mathcal{L}(T)$-formula D, such that for every sentence A we have:

$$\begin{array}{lll} A \in T & \Rightarrow & T \vdash D(\underline{\ulcorner A \urcorner}) \\ A \notin T & \Rightarrow & T \vdash \neg D(\underline{\ulcorner A \urcorner}) \end{array}$$

By the fixed point lemma 3.23 there exists an $\mathcal{L}(T)$-sentence G such that

$$T \vdash G \leftrightarrow \neg D(\underline{\ulcorner G \urcorner}) \ .$$

If $G \in T$ follows $T \vdash D(\underline{\ulcorner G \urcorner})$, $T \vdash \neg G$, $T \vdash \perp$, contradicting the consistency of T.
If $G \notin T$ then $T \vdash \neg D(\underline{\ulcorner G \urcorner})$, $T \vdash G$, $G \in T$.
So in both cases we get a contradiction, T is not recursive.

Definition 3.26 An axiom system Σ in a language extending $\mathcal{L}_{\mathbb{N}}$ is *ω-consistent*, iff for every unary $\mathcal{L}(\Sigma)$-formula A we have:
If $\Sigma \vdash \neg A(\underline{n})$ for all $n \in \mathbb{N}$, then $\Sigma \not\vdash \exists x.A(x)$.

Remark 3.27 *ω-consistent implies consistent.*

Theorem 3.28 *(Gödel's first Incompleteness Theorem).*

(a) *Every consistent, recursively axiomatized theory T containing the equality axioms and in which all recursive functions are representable is incomplete.*

(b) *For every ω-consistent, recursive axiom system Σ, in which all recursive functions can be represented by an explicitly given formula and which proves the equality axioms, we can explicitly state an $\mathcal{L}(\Sigma)$-sentence G such that $\Sigma \not\vdash G$ and $\Sigma \not\vdash \neg G$.*

Proof:
(a): Theorems 3.25, 3.16.
(b): Of course we assume some explicitly given concrete definition of $\chi_{\ulcorner \Sigma \urcorner}$.
Let $\mathrm{Proof}^0_\Sigma(a,b) :\Leftrightarrow \ulcorner \mathrm{Proof}_\Sigma \urcorner(a) \wedge \widetilde{\Gamma}_{\widetilde{\mathrm{endseq}(a)}} = \ulcorner \emptyset \urcorner \wedge \widetilde{\mathrm{A}}_{\widetilde{\mathrm{endseq}(a)}} = b.$

($\mathrm{Proof}_\Sigma(a)$ iff a is a proof of the formula b from Σ).
By Lemma 3.12 (c), Proof^0_Σ is recursive and by the representability of recursive functions we can find a 2-ary $\mathcal{L}$ formula B such that

$$\begin{array}{rcl} \mathrm{Proof}^0_\Sigma(a,b) & \Rightarrow & \Sigma \vdash B(\underline{a},\underline{b}) \\ \neg\mathrm{Proof}^0_\Sigma(a,b) & \Rightarrow & \Sigma \vdash \neg B(\underline{a},\underline{b}) \end{array}$$

By the fixed point lemma 3.23 there exists an $\mathcal{L}$-sentence G such that

$$\Sigma \vdash G \leftrightarrow \neg\exists y B(y, \underline{\ulcorner G \urcorner}) \ .$$

Assume $\Sigma \vdash G$. Then there exists a a such that $\Sigma \vdash B(\underline{a}, \underline{\ulcorner G \urcorner})$. Therefore $\Sigma \vdash \exists y B(y, \underline{\ulcorner G \urcorner})$, $\Sigma \vdash \neg G$, contradicting the consistency of Σ.
Therefore $\Sigma \not\vdash G$. Then $\Sigma \vdash \neg B(\underline{a}, \underline{\ulcorner G \urcorner})$ for all $a \in \mathbb{N}$. By the ω-consistency of Σ follows $\Sigma \not\vdash \exists y . B(y, \underline{\ulcorner G \urcorner})$. Therefore $\Sigma \not\vdash \neg G$.

Chapter 4

Representation of the Recursive Functions in Number Theory

We will follow very closely [Buc97a].

4.1 Another Definition of the Recursive Functions

We want to show, that in some very simple theory we can represent all recursive functions. However the principle of primitive recursion is difficult to handle. So we show, that the recursive functions can be defined equivalently in a way which does not use this principle.

Definition 4.1 Inductive definition of the sets Rec^n of n-ary functions:

1. $0^n \in \mathrm{Rec}^n$ $(n \in \mathbb{N})$; $\mathrm{S} \in \mathrm{Rec}^1$; if $1 \leq i \leq n$ then $\mathrm{proj}_i^n \in \mathrm{Rec}^n$; $+, \cdot, \chi_< \in \mathrm{Rec}^2$.

2. If $h \in \mathrm{Rec}^m$, $g_1, \ldots, g_m \in \mathrm{Rec}^n$, $m \geq 1$, then $h \circ (g_1, \ldots, g_m) \in \mathrm{Rec}^n$.

3. If $g \in \mathrm{Rec}^{n+1}$, $\forall \vec{a} \in \mathbb{N}^n \, \exists i . g(\vec{a}, i) = 0$, then $(\mu g) \in \mathrm{Rec}^n$.

$\mathrm{Rec} := \bigcup_{n \in \mathbb{N}} \mathrm{Rec}^n$.

Theorem 4.2 *The set of recursive functions is exactly* Rec.

Proof:
Rec is obviously a subset of the recursive functions (by Lemma 2.35 (d)). In order to show that the recursive functions are a subset of Rec by Lemma 2.35

(d) it suffices to show that Rec is closed under primitive recursion. This will be done in the following lemmata and definitions.
Consider for simplicity the special case of f defined by primitive recursion by $f(0) = a$ and $f(n+1) = g(n, f(n))$. The idea for showing that f is in Rec[1] is to define, what it means for a sequence $<a_1, \ldots, a_n>$ to be in such a way such that $a_i = f(i)$, i.e. such that $a_0 = a \wedge \forall i < n.a_{i+1} = g(i, a_i)$. $f(i)$ is the ith element of the least such sequence which has length i, so f is in Rec if this can be carried out. Therefore we need to encode sequences in Rec. The coding we used is not suitable for this, instead one uses the Chinese Remainder Theorem:

Definition 4.3 (a) $\mathrm{Rest}_b^a(i)$ is the rest of the division of a by $b(i+1)+1$.

(b) $\beta(c, i) := \mathrm{Rest}_{\pi_2(c)}^{\pi_1(c)}(i)$.

(c) $|a - b| := \begin{cases} a - b & \text{if } a \geq b, \\ b - a & \text{otherwise.} \end{cases}$.

Lemma 4.4 (Chinese Remainder Theorem)
For arbitrary k, m_0, ..., $m_k \in \mathbb{N}$ there exist $a, b \in \mathbb{N}$ such that $\mathrm{Rest}_b^a(i) = m_i$ *for $i = 0, \ldots, k$.*
Therefore there exists a c such that for $i = 0, \ldots, k$ $\beta(c, i) = m_i$ (i.e. c represents the sequence $(m_0, \ldots, m_k)$).

Proof: Let $s := \max\{k, m_0, \ldots, m_k\} + 1$, $b := s!$, $b_i := b(i+1)+1$, $\prod b_i := b_0 \cdot \cdots \cdot b_n$. $m_i < b_i$ for $i = 0, \ldots, k$.

$$i < j \leq k \Rightarrow b_i, b_j \text{ are relative prime} \tag{1}$$

Proof: Assume p is a prime, $p \mid b_i$, $p \mid b_j$. Then $p \mid (b_i - b_j) = b(j - i)$, By $j - i < s$, $b = s!$, follows $j - i \mid s!$, $p \mid s!$, by $p \mid (b(j+1)+1)$ follows $p = 1$.

$$(0 \leq a, a' < \prod b_i \wedge a \neq a') \Rightarrow \exists i \leq k.\mathrm{Rest}_b^a(i) \neq \mathrm{Rest}_b^{a'}(i) \tag{2}$$

Proof: Assume $\mathrm{Rest}_b^a(i) = \mathrm{Rest}_b^{a'}(i)$ for $i = 0, \ldots, k$. Then $b_i \mid (a - b)$, and since b_i are relative prime, $\prod b_i \mid (a - b)$, $|a - b| < \prod b_i$, $a - b = 0$, contradicting the assumption.
Therefore $a \mapsto (\mathrm{Rest}_b^a(0), \ldots, \mathrm{Rest}_b^a(k))$ is an injective function form $\{a \in \mathbb{N} \mid a < \prod b_i\}$ into $\{j \mid j < b_0\} \times \cdots \times \{j \mid j < b_k\}$.
Since both sets have the same number of elements, the function is surjective, i.e. there exists an $a \in \mathbb{N}$ such that $(\mathrm{Rest}_b^a(0), \ldots, \mathrm{Rest}_b^a(n)) = (m_0, \ldots, m_k)$.

Lemma 4.5 *(a)* Rec *is closed under λ-abstraction, as is are the primitive recursive functions (where we refer to a language containing function symbols for all elements of* Rec *and a structure, in which all these are interpreted standard).*

(b) $\dot{-}$, π, π_1, π_2, $(a,b,i) \mapsto \mathrm{Rest}_b^a(i)$, $(a,i) \mapsto \beta(a,i)$ *and* $(a,b) \mapsto |a-b|$ *are in* Rec.

Proof:
(a): Similar to Lemma 2.9 (b): $a \dot{-} b = \min\{c \mid a \leq b + c\}$, $\dot{-} \in \mathrm{Rec}$.
$\pi(a,b) = \sum_{i<a+b}(i+1) + b = \frac{1}{2}(a+b)(a+b+1) + b = H((a+b)(a+b+1)) + b$, where $H(c) := \min\{i \mid c \leq 2i\} = \min\{i \mid \chi_<(2i, c) = 0\}$.
Therefore $\pi \in \mathrm{Rec}$.
Let $\mathrm{J}(i) := \frac{1}{2}i \cdot (i+1) = \sum_{i<c}(i+1)$. $\mathrm{J}(i) = H(i(i+1))$, therefore $\mathrm{J} \in \mathrm{Rec}$.
Then if $c = \pi(a,b)$, $a+b = \min\{i \mid \mathrm{J}(i) \leq c < \mathrm{J}(i+1)\} = \min\{i \mid c < \mathrm{J}(i+1)\} = \min\{i \mid \chi_<(\mathrm{J}(i+1), \mathrm{S}(c)) = 0\} =: \mathrm{J}_1(c)$.
$\pi_2(c) = b = c \dot{-} \mathrm{J}(\mathrm{J}_1(c))$,
$\pi_1(c) = a = \mathrm{J}_1(c) \dot{-} \pi_2(c)$.
$\mathrm{Rest}_b^a(i) = a \dot{-} f(a,b,i) \cdot (b(i+1)+1)$, where
$f(a,b,i) := \min\{k \mid a < (k+1)(b(i+1)+1)\}$.
$\beta(c,i) = \mathrm{Rest}_{\pi_2(c)}^{\pi_1(c)}(i)$.
$|a-b| = (a \dot{-} b) + (b \dot{-} a)$.

The following lemma completes the proof of Theorem 4.2:

Lemma 4.6 Rec *is closed under primitive recursion, i.e. if* $g \in \mathrm{Rec}^n$, $h \in \mathrm{Rec}^{n+2}$, *then* $\mathrm{R}gh \in \mathrm{Rec}^{n+1}$.

Proof:
Let $f := (\mathrm{R}gh)$.
Define $\mathrm{Correct}(\vec{a}, b, c) :\Leftrightarrow \beta(c, 0) = g(\vec{a}) \wedge \forall i < b.\beta(c, i+1) = h(\vec{a}, i, \beta(c,i))$.
If $\mathrm{Correct}(\vec{a}, b, c)$, then $\forall i \leq b.\beta(c,i) = f(\vec{a}, i)$, especially $f(\vec{a}, b) = \beta(c,b)$.
We define $G \in \mathrm{Rec}^{n+2}$ such that $G(\vec{a}, b, c) = 0 \Leftrightarrow \mathrm{Correct}(\vec{a}, b, c)$.
By Lemma 4.4 there exists for every $\vec{a}, b$ a natural number c such that $\beta(c,i) = f(\vec{a}, i)$ for $i = 0, \ldots, b$, especially $\mathrm{Correct}(\vec{a}, b, c)$. Therefore, if we can define the G as before, $f(\vec{a}, b) = \beta(\mu(G)(\vec{a}, b), b)$, $f \in \mathrm{Rec}^{n+1}$, and the assertion holds.
Let $G_0(\vec{a}, b, c) := \min\{i \leq b \mid i = b \vee h(\vec{a}, i, \beta(c,i)) \neq \beta(c, i+1)\}$,
$G(\vec{a}, b, c) := |g(\vec{a}) - \beta(c, 0)| + (b \dot{-} G_0(\vec{a}, b, c))$.
Then $G(\vec{a}, b, c) = 0 \Leftrightarrow \mathrm{Correct}(\vec{a}, b, c)$ and in order to show $G \in \mathrm{Rec}^{n+2}$ it suffices to show $G_0(\vec{a}, b, c)$.
But $G_0(\vec{a}, b, c) = \min\{i \mid (b \dot{-} i) \cdot (1 \dot{-} |h(\vec{a}, i, \beta(c,i)) - \beta(c, i+1)|) = 0$, and such an i always exists, (namely $i = b$), so $G_0 \in \mathrm{Rec}$.

4.2 Robinson's Q

Robinson's Q contains very few axioms. But it will allow still to represent the recursive functions, so in every recursively axiomatized consistent/ω-consistent theory, in which Robinson's Q can be embedded, Gödel's incompleteness theorem 3.28 holds and in the standard model of the natural numbers of a language containing at least 0, S, $+$, $\cdot$, $=$ Tarski's theorem 3.24 holds.

Definition 4.7 (Robinson's Q)

(a) Let $\mathcal{L}_{\mathrm{ar}} := \{=, 0, \mathrm{S}, +, \cdot\}$. Formulas in $\mathcal{L}_{\mathrm{ar}}$ are called arithmetical formulas. A structure $\mathcal{N}_1$ in an extension of $\mathcal{L}_{\mathrm{ar}}$ is called $\mathcal{L}_{\mathrm{ar}}$-standard, if $|\mathcal{N}_1| = \mathbb{N}$ and $=, 0, \mathrm{S}, +, \cdot$ are interpreted in a standard way.
$\mathcal{N}_{\mathrm{ar}}$ is the $\mathcal{L}_{\mathrm{ar}}$-standard structure in $\mathcal{L}_{\mathrm{ar}}$.
A relation $R \subseteq \mathbb{N}^n$ is called arithmetical, iff it is in $\mathcal{N}_{\mathrm{ar}}$ definable.

(b) The axiom system Q in the language $\mathcal{L}_{\mathrm{ar}}$ consists of the equality axioms and the following axioms:

(Q1) $\forall x(\neg(\mathrm{S}(x) = 0)) \wedge \forall x.\forall y(\mathrm{S}(x) = \mathrm{S}(y) \rightarrow x = y)$.

(Q2) $\forall x(x + 0 = x) \wedge \forall x.\forall y(x + \mathrm{S}(y) = \mathrm{S}(x + y))$.

(Q3) $\forall x(x \cdot 0 = 0) \wedge \forall x.\forall y(x \cdot \mathrm{S}(y) = (x \cdot y) + x)$.

(Q4) $\forall x(x = 0 \vee \exists y(x = \mathrm{S}(y)))$.

(c) Let in this section $s < t := \exists z.(\mathrm{S}(z) + s = t)$.

Lemma 4.8 *For all $a, b, k \in \mathbb{N}$ the following holds:*

(a) $\mathrm{Q} \vdash A[x := 0]$ *and* $\mathrm{Q} \vdash A[x := \mathrm{S}(y)]$, $y \notin \mathrm{FV}(A)$, *then* $\mathrm{Q} \vdash A$.

(b) $\mathrm{Q} \vdash \underline{a} + \underline{b} = \underline{a + b}$

(c) $\mathrm{Q} \vdash \underline{a} \cdot \underline{b} = \underline{a \cdot b}$

(d) $\mathrm{Q} \vdash 0 < \mathrm{S}(y)$.
$\mathrm{Q} \vdash \neg(x < 0)$.
$\mathrm{Q} \vdash \mathrm{S}(x) < \mathrm{S}(y) \leftrightarrow x < y$.

(e) $a < b \Rightarrow \mathrm{Q} \vdash \underline{a} < \underline{b}$.

(f) $a < b \Rightarrow \mathrm{Q} \vdash \neg(\underline{a} = \underline{b})$.

(g) $a \leq b \Rightarrow \mathrm{Q} \vdash \neg(\underline{b} < \underline{a})$.

(h) $\mathrm{Q} \vdash \mathrm{S}(z) + \underline{a} = z + \mathrm{S}(\underline{a})$.

(i) $\mathrm{Q} \vdash x < \underline{k} \rightarrow x = \underline{0} \vee \cdots \vee x = \underline{k - 1}$.

(j) $\mathrm{Q} \vdash x = \underline{0} \vee \cdots \vee x = \underline{k} \vee \underline{k} < x$.

Proof:
Abbreviation: $\vdash B :\Leftrightarrow \mathrm{Q} \vdash B$, $A \vdash B :\Leftrightarrow \mathrm{Q} \cup \{A\} \vdash B$.
(a): By (Q4).
(b): Induction on b:
$b = 0$: by (Q2) $\vdash \underline{a} + 0 = \underline{a}$.
$b \rightarrow b + 1$: $\vdash \underline{a} + \underline{b + 1} = \underline{a} + \mathrm{S}(\underline{b}) \overset{(\mathrm{Q2})}{=} \mathrm{S}(\underline{a} + \underline{b}) \overset{\mathrm{IH}}{=} \mathrm{S}(\underline{a + b}) = \underline{a + (b + 1)}$.
(c) similar to (b):
$b = 0$: by (Q3) $\vdash \underline{a} \cdot 0 = 0$.
$b \rightarrow b+1$: $\vdash \underline{a} \cdot \underline{b + 1} = \underline{a} \cdot \mathrm{S}(\underline{b}) \overset{(\mathrm{Q3})}{=} (\underline{a} \cdot \underline{b}) + \underline{a} \overset{\mathrm{IH}}{=} \underline{a \cdot b} + \underline{a} \overset{(\mathrm{b})}{=} \underline{a \cdot b + a} = \underline{a \cdot (b + 1)}$.

(d) $\vdash \mathrm{S}(y) + 0 = \mathrm{S}(y) \vdash 0 < \mathrm{S}(y)$.
In order to show $\neg(x < 0)$ by (a) it suffices to prove $\neg 0 < 0$ and $\neg \mathrm{S}(y) < 0$:
$\mathrm{S}(z) + 0 = 0 \vdash \mathrm{S}(z) = 0 \vdash \perp$. $\mathrm{S}(z) + \mathrm{S}(y) = 0 \vdash \mathrm{S}(\mathrm{S}(z) + y) = 0 \vdash \perp$.
$\vdash \mathrm{S}(x) < \mathrm{S}(y) \leftrightarrow \exists z(\mathrm{S}(z) + \mathrm{S}(x) = \mathrm{S}(y)) \leftrightarrow \exists z(\mathrm{S}(\mathrm{S}(z) + x) = \mathrm{S}(y))$
$\overset{\text{(Q1)+Equality axioms}}{\leftrightarrow} \exists z(\mathrm{S}(z) + x = y) \leftrightarrow x < y$.

(e) $a < b \Rightarrow ((b - (a+1)) + 1) + a = b \overset{\text{(b)}}{\Rightarrow} \vdash \mathrm{S}(\underline{b - (a+1)}) + \underline{a} = \underline{b} \Rightarrow \vdash \exists z.\mathrm{S}(z) + \underline{a} = \underline{b}$.

(f) Induction on a. Let $b = m + 1$.
$a = 0$: By (Q1) $\vdash \neg(0 = \mathrm{S}(\underline{m}))$, $\vdash \neg(0 = \underline{b})$.
$a \to a + 1$. If $a + 1 < b$, then $a < m \overset{\text{IH}}{\Rightarrow} \vdash \neg(\underline{a} = \underline{m}) \overset{\text{(Q1)}}{\Rightarrow} \vdash \neg(\mathrm{S}(\underline{k}) = \mathrm{S}(\underline{m}))$.

(g) Induction on b:
$b = 0$. Then $a = 0$. (d).
$b \to b + 1$. If $a = 0$ (d). Otherwise $a = a' + 1$, $a' < b$. $\underline{b+1} < \underline{a} \vdash \mathrm{S}(\underline{b}) < \mathrm{S}(\underline{a'}) \overset{\text{(d)}}{\vdash} \underline{b} < \underline{a'} \overset{\text{IH}}{\vdash} \perp$.

(h) Induction on a:
$a = 0$: $\vdash \mathrm{S}(z) + 0 = \mathrm{S}(z) = \mathrm{S}(z + 0) = z + \mathrm{S}(0)$.
$a \to a+1$: $\vdash \mathrm{S}(z)+\underline{a+1} = \mathrm{S}(z)+\mathrm{S}(\underline{a}) = \mathrm{S}(\mathrm{S}(z)+\underline{a}) \overset{\text{IH}}{=} \mathrm{S}(z+\mathrm{S}(\underline{a})) = z+\mathrm{S}(\underline{a+1})$.

(i) Let $A_k(x) := x < \underline{k} \to x = \underline{0} \vee \cdots \vee \underline{k-1}$.
Induction on k.
$k = 0$:
$\overset{\text{(d)}}{\vdash} \neg(x < \underline{0}) \vdash A_0(x)$.
$k \to k + 1$: By (a) show $\vdash A_{k+1}(0)$ and $\vdash A_{k+1}(\mathrm{S}(y))$.
$\vdash 0 = \underline{0} \vdash A_{k+1}(0)$.
$\mathrm{S}(y) < \underline{k+1} \overset{\text{(d)}}{\vdash} y < \underline{k} \overset{\text{IH}}{\vdash} y = \underline{0} \vee \cdots \vee y = \underline{\text{k-1}} \vdash \mathrm{S}(y) = \underline{1} \vee \cdots \vee y = \underline{\text{k}}$.

(j) Induction on k. Let $A_k(x) := x = \underline{0} \vee \cdots \vee x = \underline{k} \vee \underline{k} < x$. For each k we will show $A_k(0)$ and $A_k(\mathrm{S}(y))$ from which by (b) follows $A_k(x)$.
$k = 0$: $\vdash 0 = \underline{0} \vdash A_k(0)$. $\overset{\text{(d)}}{\vdash} \underline{0} < \mathrm{S}(y) \vdash A_k(\mathrm{S}(y))$.
$k \to k + 1$: $\vdash 0 = \underline{0} \vdash A_k(0)$. $\overset{\text{IH}}{\vdash} y = \underline{0} \vee \cdots \vee y = \underline{k} \vee \underline{k} < x \overset{\text{(d)}}{\vdash} \mathrm{S}(y) = \underline{1} \vee \cdots \vee \mathrm{S}(y) = \underline{k+1} \vee \underline{k+1} < \mathrm{S}(y) \vdash A_{k+1}(\mathrm{S}(y))$.

Definition 4.9 Let the set of extended Σ_1 formulas in $\mathcal{L}_{\mathrm{ar}}$ be defined as for the language $\mathcal{L}_{\mathrm{PR}}$, but $s < t$ is abbreviation for $\exists z(\mathrm{S}(z) + s = t)$ (instead of for $\mathrm{S}(s) \dot{-} t = 0$).

Theorem 4.10 *Every recursive function (and therefore every recursive relation) can be represented in* Q *by an arithmetic extended* Σ_1*-formula.*

Proof:
In this proof again $\vdash A :\Leftrightarrow \mathrm{Q} \vdash A$ and $B \vdash A \Leftrightarrow \mathrm{Q} \cup \{B\} \vdash A$. Further, if $\vec{a} = a_1, \ldots, a_n$, $\underline{\vec{a}} := \underline{a_1}, \ldots, \underline{a_n}$.

We show that every function $f \in \mathrm{Rec}^n$ can be represented in Σ by an $n+1$-ary extended Σ_1-formula A_f by induction on Rec. Note that since $\vdash \neg(\underline{a} = \underline{b})$ for $a \neq b$ by Lemma 4.8 (f) it suffices to show for all $\vec{a} \in \mathbb{N}^n$

$$\Sigma \vdash \forall y(A(\underline{\vec{a}}, y) \leftrightarrow y = \underline{f(\vec{a})}) \ .$$

$A_{0^n} := v_{n+1} = 0$.
$A_{\mathrm{S}} := v_2 = \mathrm{S}(v_1)$.
$A_{\mathrm{proj}_i^n} := v_{n+1} = v_i$.
$A_{\chi_<} := (v_1 < v_2 \wedge v_3 = \underline{1}) \vee (\neg(v_1 < v_2) \wedge v_3 = \underline{0})$: If $a_1 < a_2$, then $\vdash \underline{a_1} < \underline{a_2}$, $\vdash A_{\chi_<}(\underline{a_1}, \underline{a_2}, y) \leftrightarrow y = \underline{1} \leftrightarrow y = \underline{\chi(a_1, a_2)}$, and if $\neg(a_1 < a_2)$, then $\vdash \neg(\underline{a_1} < \underline{a_2})$ and similarly the assertion.
$A_{f\circ(g_1,\dots,g_m)}(\vec{v}, v_{n+1}) := \exists y_1, \dots, y_m(A_{g_1}(\vec{v}, y_1) \wedge \cdots \wedge A_{g_m}(\vec{v}, y_m) \wedge$ $A_f(y_1, \dots, y_m, v_{n+1}))$. The assertion is clear.
$A_{\mu g}(\vec{v}, v_{n+1}) := A_g(\vec{v}, v_{n+1}, \underline{0}) \wedge \forall y < v_{n+1}.\exists z(z \neq \underline{0} \wedge A_g(\vec{v}, y, z))$.
We argue in Q. Let $b := (\mu g)(\vec{a})$.
Assume $A_{\mu g}(\underline{\vec{a}}, y)$ and show $y = \underline{b}$.
$y = \underline{0} \vee \cdots \vee \underline{b} \vee \underline{b} < y$.
Case $y = \underline{i}$, $i < b$. By IH $\neg A_g(\underline{\vec{a}}, y, \underline{0})$, $\neg A_{\mu g}(\underline{\vec{a}}, y, \underline{0})$.
Case $y = \underline{b}$. The assertion follows.
Case $\underline{b} < y$. Then by $g(\vec{a}, b) = 0$ follows $A_g(\underline{\vec{a}}, \underline{b}, y) \leftrightarrow y = \underline{0}$, $\neg\exists z(A_g(\underline{\vec{a}}, \underline{b}, z) \wedge z \neq \underline{0})$, $\underline{b} < y$, $\neg A_{\mu g}(\underline{\vec{a}}, y)$.
Assume $y = \underline{b}$ and show $A_{\mu g}(\underline{\vec{a}}, y)$.
$A_g(\underline{\vec{a}}, y, \underline{0})$, and $z < y \to z = \underline{0} \vee \cdots \vee z = \underline{b-1}$, so if $z < y$, $z = \underline{i}$, then $A_g(\underline{\vec{a}}, y, \underline{g(\vec{a}, i)})$, $\neg(\underline{g(\vec{a}, i)} = \underline{0})$, $A_{\mu g}(\underline{\vec{a}}, y)$.

Theorem 4.11 *(a) Every recursive enumerable relation (and therefore every recursive function) can be defined in a $\mathcal{L}_{\mathrm{ar}}$-standard structure $\mathcal{N}_1$ by an extended Σ_1-formula.*

(b) Every recursive enumerable relation is arithmetical.

Proof: (a) $\mathcal{N}_1 \models \mathrm{Q}$, therefore, if A represents in a relation in Q, then it defines it in $\mathcal{N}_1$. (b) follows from (a).

4.3 Provability and Decidability in Theories extending Q

Theorem 4.12 $\ulcorner\mathrm{Th}(\mathcal{N}_{\mathrm{ar}})\urcorner$ *is not arithmetical.*

Proof: Theorem 3.24, Theorem 4.11 (b).

Corollary 4.13 $\mathrm{Th}(\mathcal{N}_{\mathrm{ar}})$ *is not recursive enumerable and therefore not recursive axiomatizable.*

Theorem 4.14 *Every consistent theory T with $\mathrm{Q} \subseteq T$ is undecidable.*

Proof: Theorem 3.25 and Theorem 4.11 (b).

Theorem 4.15 *(Gödel's first incompleteness Theorem).*

(a) Every consistent, recursively axiomatized theory T, in which all formulas in Q *and the equality axioms are provable, is incomplete.*

(b) For every ω-consistent, recursive axiom system Σ, in which all formulas of Q *and the equality axioms are provable, we can explicitly state an $\mathcal{L}(\Sigma)$-sentence G such that $\Sigma \nvdash G$ and $\Sigma \nvdash \neg G$.*

Theorem 4.16 *(Undecidability of first order predicate logic). The set of valid $\mathcal{L}_{\text{ar}}$-sentences is undecidable (not recursive).*

Proof: Let Th be the set of valid $\mathcal{L}_{\text{ar}}$-sentences and Th_{Q} the set of $\mathcal{L}_{\text{ar}}$-sentences, following from Q. By Theorem 4.14, Th_{Q} is not recursive. On the other hand we have $a \in \ulcorner\text{Th}_{\text{Q}}\urcorner \Leftrightarrow \ulcorner\bigwedge \text{Q}\urcorner \,\tilde{\to}\, a \in \ulcorner P\urcorner$, where $\bigwedge \text{Q}$ is the conjunction of the (finitely many) axioms in Q. Therefore P is not recursive.

Rosser showed, that in (b) of Gödel's first incompleteness theorem (3.28) we can get rid of the assumption Σ ω-consistent, as long as Σ proves Q:

Theorem 4.17 *(Rosser's strengthening of Gödel's first incompleteness theorem)*
For every consistent, recursive axiom system Σ such that $\Sigma \vdash \text{Q}$ we can explicitly state a true arithmetical sentence A such that $\Sigma \nvdash A$ and $\Sigma \nvdash \neg A$.

Proof:
Let Proof^0_Σ be as in the proof of Theorem 3.28. Proof^0_Σ is recursive. By Theorem 4.10 there exists a binary arithmetical formula B_{Proof} such that

$$\begin{aligned} \text{Proof}^0_\Sigma(a,b) \quad &\Rightarrow \quad \text{Q} \vdash B^0_{\text{Proof}}(\underline{a},\underline{b}) && (1)\\ \neg\text{Proof}^0_\Sigma(a,b) \quad &\Rightarrow \quad \text{Q} \vdash \neg B^0_{\text{Proof}}(\underline{a},\underline{b}) && (2)\end{aligned}$$

Define $\text{Refute}_\Sigma(a,b) :\Leftrightarrow \text{Proof}^0_\Sigma(a,\tilde{\neg}(b))$.
$\text{Refute}_\Sigma(a,b)$ is recursive, since Proof^0_Σ is recursive. Therefore there we can explicitly give a binary arithmetical formula B_{Refute} such that

$$\begin{aligned} \text{Refute}_\Sigma(a,b) \quad &\Rightarrow \quad \text{Q} \vdash B_{\text{Refute}}(\underline{a},\underline{b}) && (1')\\ \neg\text{Proof}^0_\Sigma(a,b) \quad &\Rightarrow \quad \text{Q} \vdash \neg B_{\text{Refute}}(\underline{a},\underline{b}) && (2')\end{aligned}$$

Let $C(z) := \forall y(B_{\text{Proof}}(y,z) \to \exists w < y.B_{\text{Refute}}(w,z))$.
$C(\underline{\ulcorner D\urcorner})$ expresses: for every proof of D there exists a shorter refutation of D.
By the fixed point lemma 3.23 we can explicitly define an arithmetical sentence A such that

$$\text{Q} \vdash A \leftrightarrow C(\underline{\ulcorner A\urcorner}) \qquad (*)$$

We show $\Sigma \nvdash A$ and $\Sigma \vdash \neg A$.
Assume, $\Sigma \vdash A$. Then there exists a b such that $\text{Proof}^0_\Sigma(b,\ulcorner A\urcorner)$, by (1)

$\mathrm{Q} \vdash B_{\mathrm{Proof}}(\underline{b}, \underline{\ulcorner A \urcorner})$. Since Σ is consistent, follows $\neg\mathrm{Refute}(n, \ulcorner A \urcorner)$ for all n, by (2') $\mathrm{Q} \vdash \neg B_{\mathrm{Refute}}(\underline{n}, \underline{\ulcorner A \urcorner})$. By Lemma 4.8 (i) follows therefore $\mathrm{Q} \vdash B_{\mathrm{Proof}}(\underline{b}, \underline{\ulcorner A \urcorner}) \wedge \forall z < \underline{b}.\neg B_{\mathrm{Refute}}(z, \underline{\ulcorner A \urcorner})$, $\mathrm{Q} \vdash \neg C(\underline{\ulcorner A \urcorner})$, $\mathrm{Q} \vdash \neg A$, $\Sigma \vdash \neg A$, $\Sigma \vdash \perp$, a contradiction.
Therefore $\Sigma \not\vdash A$, $\mathcal{N} \models C(\underline{\ulcorner A \urcorner})$, by $(*)$ $\mathcal{N} \models A$.
Assume $\Sigma \vdash \neg A$. Then there exists a $b \in \mathbb{N}$ such that $(b, \ulcorner A \urcorner) \in \mathrm{Refute}_\Sigma$, by $(1')$ $\mathrm{Q} \vdash B_{\mathrm{Refute}}(\underline{b}, \underline{\ulcorner A \urcorner})$. By the consistency of Σ follows $\neg\mathrm{Proof}^0_\Sigma(n, \ulcorner A \urcorner)$ for all $n \in \mathbb{N}$, and by (2) $\mathrm{Q} \vdash \neg B_{\mathrm{Proof}}(\underline{n}, \underline{\ulcorner A \urcorner})$ for all n.
We show $\mathrm{Q} \vdash B_{\mathrm{Proof}}(y, \underline{\ulcorner A \urcorner}) \rightarrow \exists w < y.B_{\mathrm{Refute}}(w, \underline{\ulcorner A \urcorner})$ and argue in Q.
Assume y. By Lemma 4.8 (j) we have $y = \underline{0} \vee \cdots y = \underline{b} \vee \underline{b} < y$. If $y = \underline{k}$ for $k \leq b$, then we get $\neg B_{\mathrm{Proof}}(y, \underline{\ulcorner A \urcorner})$. If $\underline{b} < y$, then by $\underline{b} < y$ follows $B_{\mathrm{Refute}}(\underline{b}, \underline{\ulcorner A \urcorner})$, therefore $\exists w < y.B_{\mathrm{Refute}}(w, \underline{\ulcorner A \urcorner})$.
Therefore $\mathrm{Q} \vdash C(\underline{\ulcorner A \urcorner})$, $\mathrm{Q} \vdash A$, $\Sigma \vdash A$, $\Sigma \vdash \perp$, a contradiction.

Definition 4.18 An arithmetical extended Π_1-formula is an arithmetical formula which is logically equivalent to the negation of an arithmetical extended Σ_1 formula.

The next theorem shows that we can reduce the complexity of the unprovable true formula to Π_1-formulas.

Theorem 4.19 *In every consistent, recursive axiom system Σ such that $\Sigma \vdash \mathrm{Q}$ we can explicitly define a true arithmetical Π_1-sentence A such that $\Sigma \not\vdash A$.*

Note that we don't get in general for this sentence A $\Sigma \not\vdash \not A$.

Remark 4.20 *(a) Every closed true arithmetical extended Σ_1-formula is provable in Q. (Therefore the complexity of the formula in Theorem theorepionefalse was optimal).*

(b) If Σ is ω-consistent, $\Sigma \vdash \mathrm{Q}$, A is a false closed true arithmetical extended Σ_1-formula, then $\Sigma \not\vdash A$. (Especially if Σ as in Theorem 4.19 is ω-consistent, and A is as there, then $\Sigma \not\vdash \neg A$).

Proof of Remark 4.20: Exercise.

Proof of Theorem 4.19: By Theorem 3.13 and Theorem 4.11 (a) we can explicitly define a binary arithmetical extended Σ_1-formula B such that

$$\mathrm{Proof}^0_\Sigma(a, b) \Leftrightarrow \mathrm{Q} \vdash B(\underline{a}, \underline{b}) \ .$$

By the fixed point lemma 3.23 we can explicitly define an arithmetical sentence A' such that

$$\mathrm{Q} \vdash A' \leftrightarrow \neg\exists z.B(z, \underline{\ulcorner A' \urcorner}) \qquad (3)$$

Let $A := \exists z.B(z, \underline{\ulcorner A' \urcorner})$.
Assume $\Sigma \vdash A$. Then $\Sigma \vdash A'$.
By (1) there is a b such that $\mathrm{Q} \vdash B(\underline{b}, \underline{\ulcorner A' \urcorner})$. Therefore $\mathrm{Q} \vdash \exists z.B(z, \underline{\ulcorner A' \urcorner})$ and by (3) and $\Sigma \vdash \mathrm{Q}$ follows $\Sigma \vdash \neg A'$, $\Sigma \vdash \perp$, a contradiction.
Therefore $\Sigma \not\vdash A$, i.e. A' and as well A are true, but by (3) and $\Sigma \vdash \mathrm{Q}$ not provable in Σ. A is extended Σ_1.

Chapter 5

Recursion Theory, part 2

We will follow very closely [Buc93b]. the value computed by it from this computation.
We will choose in the following a maybe not as intuitive way: we use the representability of primitive recursive functions in Q. Every primitive recursive relation R and therefore as well every recursive enumerable relation can be represented in Q by a formula A. Therefore as well for every partial recursive function f, Graph(f) can be represented, i.e.

$$\begin{array}{rcl} f(a_1,\dots,a_n)\simeq b & \Rightarrow & \mathrm{Q}\vdash A[\underline{a_1},\dots,\underline{a_n},\underline{b}] \\ f(a_1,\dots,a_n,b)\not\simeq b & \Rightarrow & \mathrm{Q}\vdash \neg A[\underline{a_1},\dots,\underline{a_n},\underline{b}]. \end{array}$$

So, if a is minimal such that $\pi_1(a)$ is a proof of $A[\underline{a_1},\dots,\underline{a_n},\underline{\pi_2(a)}]$ then (using the consistency of Q relative to the standard model) $f(a_1,\dots,a_n)\simeq\pi_2(a)$. If $(a_1,\dots,a_n)\notin\mathrm{dom}(f)$, such a proof doesn't exist.
If B is an arbitrary formula, we can define a function $f:\mathbb{N}^n\to_{\mathrm{par}}\mathbb{N}$ as follows: If $\vec{a}\in\mathbb{N}^n$, let a minimal such that $\pi_1(a)$ is a proof of $B[\underline{\vec{a}},\underline{\pi_2(a)}]$. If such a a exists, let $f(\vec{a}):\simeq\pi_2(a)$, $f(\vec{a}):\simeq\perp$ otherwise. We will see in the following that f will be partial recursive.
So the set of formulas can be used as names for all partial recursive functions.

Definition 5.1 (a) Let
$\mathrm{Sb}_0(e):=e$,
$\mathrm{Sb}_{n+1}(e,a_1,\dots,a_n):=\mathrm{Sb}_n(\mathrm{Sub}(e,\ulcorner v_{n+1}\urcorner,\ulcorner\underline{a_{n+1}}\urcorner),a_1,\dots,a_n)$.
(Note that $\mathrm{Sb}_n(\ulcorner A\urcorner,a_1,\dots,a_n)=\ulcorner A[v_1:=\underline{a_1},\dots,v_n:=\underline{a_n}]\urcorner$).

(b) $\mathrm{T}^n(e,a_1,\dots,a_n,c):\Leftrightarrow(\pi_2(c),\mathrm{Sb}_{n+1}(e,\pi_1(c),a_1,\dots,a_n))\in\ulcorner\mathrm{Proof}^0_{\mathrm{Q}}\urcorner$.
(Therefore $T^n(\ulcorner A\urcorner,a_1,\dots,a_n,c)\Leftrightarrow\pi_2(c)$ is a code for a proof of $A[v_1:=\pi_1(c),v_2:=a_1,\dots,v_{n+1}:=a_n]$.
$\mathrm{U}:=\pi_1$.
$\{e\}^n(a_1,\dots,a_n):=\mathrm{U}(\mu y.\mathrm{T}^n(e,a_1,\dots,a_n,y))$.

Theorem 5.2 *(a)* Sb_n*,* T^n*,* U *are primitive recursive.* $\{e\}^n$ *(*$e \in \mathbb{N}$*) and* $\{\cdot\}^n : \mathbb{N}^{n+1} \rightarrow_{\mathrm{par}} \mathbb{N}$*,* $\{\cdot\}^n(e, a_1, \ldots, a_n) \simeq \{e\}(a_1, \ldots, a_n)$ *are partial recursive.*

(b) (Kleene's Normal form Theorem) $\{\{e\}^n \mid e \in \mathbb{N}\}$ *is exactly the set of* n*-ary partial recursive functions*

Proof: (a): clear
(b): $\{e\}^n$ is partial recursive. If $f : \mathbb{N}^n \rightarrow_{\mathrm{par}} \mathbb{N}$ is partial recursive, Graph(f) represented by the $n+1$-ary formula A in Q, then $\{\ulcorner A(v_2, \ldots, v_{n+1}, v_1)\urcorner\}(\vec{a}) \simeq b \Leftrightarrow$ there exists a code c for a proof of $A[b, a_1, \ldots, a_n]$ such that $\pi(c, b)$ are minimal, and since A represents f this is equivalent to $f(\vec{a}) \simeq b$.

Definition 5.3 $\mathrm{W}^n_e := \mathrm{dom}(\{e\}^n)$.

Lemma 5.4 $\{\mathrm{W}^n_e \mid e \in \mathbb{N}\}$ *is the set of* n*-ary recursive enumerable relations.*

Proof: W^n_e are recursive enumerable. If R is recursive enumerable, $R = \mathrm{dom}(f)$ for some partial recursive function, $R = \mathrm{dom}(\{e\}^n) = \mathrm{W}^n_e$ for some $e \in \mathbb{N}$.

Theorem 5.5 (Turing-Halting problem). $\mathrm{K} := \{e \in \mathbb{N} \mid e \in \mathrm{W}^1_e\}$ *is recursive enumerable but not recursive.*

Remark: Intuitively $\{e\}$ is the partial function computed by the eth program. Then K is the set of e such that $\{e\}(e)$ is defined, i.e. program e applied to itself stops.

Proof of Theorem 5.5:
K is recursive enumerable: $e \in \mathrm{K} \Leftrightarrow e \in \mathrm{W}^1_e \Leftrightarrow \{e\}^1(e)$ is defined $\Leftrightarrow$ $\exists c.\mathrm{T}^1(e, e, c)$ is recursive enumerable, since T^1 is primitive recursive.
Assume K is recursive. Then $\mathbb{N} \setminus \mathrm{K}$ is recursive enumerable, $\mathbb{N} \setminus \mathrm{K} = \mathrm{W}^1_{e_0}$ for some $e_0 \in \mathbb{N}$. Now $e_0 \in \mathrm{K} \Leftrightarrow e_0 \in \mathrm{W}^1_{e_0} \Leftrightarrow e_0 \notin \mathrm{K}$, a contradiction.

Theorem 5.6 (s^m_n**-theorem or** s**-**m**-**n**-theorem)** *For every* $n, m \geq 1$ *there exists an* $m+1$*-ary primitive recursive function* s^m_n *such that for all* $e, c \in \mathbb{N}$*,* $\vec{a} \in \mathbb{N}^n$*,* $\vec{b} \in \mathbb{N}^m$ *we have:*

(a) $\mathrm{T}^{n+m}(e, \vec{a}, \vec{b}, c) \Leftrightarrow \mathrm{T}^n(\mathrm{s}^m_n(e, \vec{b}), \vec{a}, c)$.

(b) $\{e\}^{n+m}(\vec{a}, \vec{b}) \simeq \{\mathrm{s}^m_n(e, \vec{b})\}^n(\vec{a})$.

Proof:
Let $\mathrm{s}^0_n(e) := e$ and

$$\mathrm{s}^{m+1}_n(e, b_1, \ldots, b_{m+1}) := \mathrm{s}^m_n(\mathrm{Sub}(e, \ulcorner v_{n+m+2}\urcorner, \ulcorner \underline{b_{m+1}}\urcorner), b_1, \ldots, b_m) \ .$$

We show

$$\mathrm{Sb}_{n+m+1}(e, c, \vec{a}, \vec{b}) = \mathrm{Sb}_{n+1}(\mathrm{s}^m_n(e, \vec{b}), c, \vec{a}) \qquad (*)$$

Then

$$\begin{aligned}
\mathrm{T}^n(e,\vec{a},\vec{b},c) &\Leftrightarrow (\pi_2(c),\mathrm{Sb}_{n+m+1}(e,\pi_1(c),\vec{a},\vec{b}))\in \mathrm{Proof}_{\mathrm{Q}}\\
&\Leftrightarrow (\pi_2(c),\mathrm{Sb}_{n+1}(\mathrm{s}^m_n(e,\vec{b}),c,\vec{a}))\in \mathrm{Proof}_{\mathrm{Q}}\\
&\Leftrightarrow \mathrm{T}^n(\mathrm{s}^m_n(e,\vec{b}),\vec{a},c)
\end{aligned}$$

i.e. (a) and therefore as well (b).
Proof of $(*)$ by induction on m:
$m=0$ is trivial. $m\to m+1$:

$$\begin{aligned}
&\mathrm{Sb}_{n+m+2}(e,c,\vec{a},b_1,\dots,b_{m+1})\\
&\quad=\mathrm{Sb}_{n+m+1}(\mathrm{Sub}(e,\ulcorner v_{n+m+2}\urcorner,\ulcorner b_{m+1}\urcorner),c,\vec{a},b_1,\dots,b_m)\\
&\quad=\mathrm{Sb}_{n+1}(\mathrm{s}^m_n(\mathrm{Sub}(e,\ulcorner v_{n+m+2}\urcorner,\ulcorner b_{m+1}\urcorner),b_1,\dots,b_m),c,\vec{a})\\
&\quad=\mathrm{Sb}_{n+1}(\mathrm{s}^{m+1}_n(e,b_1,\dots,b_m,b_{m+1}),c,\vec{a})
\end{aligned}$$

Theorem 5.7 (Kleene's Recursion Theorem) *For every $n+1$ary partial recursive function g there exists an e such that $\{e\}^n(\vec{a})\simeq g(e,\vec{a})$ for all $\vec{a}\in\mathbb{N}^n$.*

Proof: As for the fixed point Lemma, we give first a proof with some motivation and then the short argument.
Let h be an arbitrary unary primitive recursive function. Then $f_h:\mathbb{N}^{n+1}\to_{\mathrm{par}}\mathbb{N}$, $f_h(\vec{a},e):\simeq g(h(e),\vec{a})$ is partial recursive. Let $f_h=\{e_h\}^{n+1}$. Then $\{\mathrm{s}^1_n(e_h,e)\}^n(\vec{a})\simeq\{e_h\}^{n+1}(e,\vec{a})\simeq f_h(\vec{a},e)\simeq g(h(e),\vec{a})$.
If now e, h are chosen, such that $\mathrm{s}^1_n(e_h,e)=h(e)$ then we are done. Now let, similarly as in the proof of the fixed point lemma $h(e):=\mathrm{s}^1_n(e,e)$. Then with $e:=e_h$ follows the assertion.
Compact argument: By Lemma 5.2 (b) there exists a k such that $\{k\}^{n+1}(\vec{a},e)\simeq g(\mathrm{s}^1_n(e,e),\vec{a})$ for all $\vec{a},e$. Let $e:=\mathrm{s}^1_n(k,k)$. Then $\{e\}^n(\vec{a})\simeq\{\mathrm{s}^1_n(k,k)\}^n(\vec{a})\simeq\{k\}^{n+1}(\vec{a},k)\simeq g(\mathrm{s}^1_n(k,k),\vec{a})\simeq g(e,\vec{a})$.

Corollary 5.8 *If $n\geq 1$, and f is a unary recursive function, then there exists an $e\in\mathbb{N}$ such that $\{f(e)\}^n=\{e\}^n$.*

Proof: $g(e,\vec{a}):\simeq\{f(e)\}^n(\vec{a})$ in Theorem 5.7.

Example of an application of the recursion theorem.
The Ackermann function $\mathcal{A}:\mathbb{N}^2\to\mathbb{N}$ is defined by
$\mathcal{A}_0(k):=k+1$, $\mathcal{A}_{m+1}(0):=\mathcal{A}_m(1)$, $\mathcal{A}_{m+1}(k+1):=\mathcal{A}_m(\mathcal{A}_{m+1}(k))$.
Define the partial recursive function g by

$$g(e,m,k):\simeq\begin{cases}k+1 & \text{if } m=0\\ \{e\}^2(m\dot{-}1,1) & \text{if} m>0\wedge k=0\,.\\ \{e\}^2(m\dot{-}1,\{e\}^2(m,k\dot{-}1)) & \text{otherwise.}\end{cases}$$

By the recursion theorem there exists an e such that $\{e\}^2(m,k)\simeq g(e,m,k)$ for all m,k.
By main induction on m and side induction on k one shows, that $\{e\}^2(m,k)\simeq\mathcal{A}(m,k)$. Therefore $\mathcal{A}(m,k)$ is recursive.

In general, for any function, which has recursion equations as the ones of $\mathcal{A}$ one can find a partial function which fulfills these equations. If the equations are in such a way, that one can prove that there exists a unique (partial or total) function which fulfills these equations, the function defined is shown to be partial recursive or recursive.

5.1 The theorems of Rice and Rice/Shapiro

We will now follow [Cut80].

Theorem 5.9 (Rice's Theorem) *If $\mathcal{F}$ is a set of n-ary partial recursive functions such that $\emptyset \neq \mathcal{F} \neq \{\{e\}^n \mid e \in \mathbb{N}\}$, then $\ulcorner\mathcal{F}\urcorner := \{e \in \mathbb{N} \mid \{e\}^n \in \mathcal{F}\}$ is not recursive.*

Proof: Let $e_0, e_1 \in \mathbb{N}$, $\{e_0\}^n \in \mathcal{F}$, $\{e_1\}^n \notin \mathcal{F}$.
Assume $\ulcorner\mathcal{F}\urcorner$ is recursive. Define $g : \mathbb{N}^{n+1} \to_{\text{par}} \mathbb{N}$,
$g(e,a) :\simeq \begin{cases} \{e_1\}^n(a) & \text{if } e \in \ulcorner\mathcal{F}\urcorner \\ \{e_0\}^n(a) & \text{if } e \notin \ulcorner\mathcal{F}\urcorner \end{cases}.$
By the recursion theorem, there exists an e such that $\forall a \in \mathbb{N}^n.\{e\}^n(a) \simeq g(e,a)$.
Then we get:
$e \in \ulcorner\mathcal{F}\urcorner \Rightarrow \forall a(\{e\}^n(a) \simeq g(e,a) \simeq \{e_1\}^n(a)) \Rightarrow \{e\}^n = \{e_1\}^n \Rightarrow e \notin \ulcorner\mathcal{F}\urcorner$.
$e \notin \ulcorner\mathcal{F}\urcorner \Rightarrow \forall a(\{e\}^n(a) \simeq g(e,a) \simeq \{e_0\}^n(a)) \Rightarrow \{e\}^n = \{e_0\}^n \Rightarrow e \in \ulcorner\mathcal{F}\urcorner$.
So we get a contradiction.

Definition 5.10 (a) If $f, f' : \mathbb{N}^n \to_{\text{par}} \mathbb{N}$,
$f \subseteq f' \Leftrightarrow \forall \vec{a} \in \text{dom}(f)(\vec{a} \in \text{dom}(f') \wedge f(\vec{a}) \simeq f'(\vec{a}))$
(or $\Leftrightarrow \text{Graph}(f) \subseteq \text{Graph}(f')$).

(b) A function $f : \mathbb{N}^n \to_{\text{par}} \mathbb{N}$ is finite, iff $\text{dom}(f)$ is finite (or equivalently $\text{Graph}(f)$ is finite).

Theorem 5.11 (Theorem of Rice/Shapiro) *Assume that $\mathcal{F}$ is a set of unary recursive functions such that $\{e \mid \{e\}^1 \in \mathcal{F}\}$ is recursive enumerable. Then for any unary partial recursive function f follows $f \in \mathcal{F}$ iff there exists a finite function $f' \subseteq f$ such that $f' \in \mathcal{F}$.*

Proof:
Let $\ulcorner\mathcal{F}\urcorner := \{e \mid \{e\}^1 \in \mathcal{F}\}$.
Suppose $f \in \mathcal{F}$, $f' \notin \mathcal{F}$ for all $f' \subseteq f$ finite.
K as in Theorem 5.5 is recursive enumerable. Let $a \in \text{K} \Leftrightarrow \exists b.R(a,b)$, R primitive recursive.
Define $g : \mathbb{N}^2 \to_{\text{par}} \mathbb{N}$,
$g(a,b) :\simeq \begin{cases} f(b) & \text{if } \forall c < b.\neg R(a,c) \\ \bot & \text{otherwise.} \end{cases}.$
By the s^m_n-theorem there exists a primitive recursive unary function s such that

$g(a, b) \simeq \{s(a)\}(b)$. (if $g(a, b) = \{e\}^2(b, a)$, $\{\mathrm{s}^1_1(e, a)\}(b) \simeq g(a, b)$, $s(a) := \mathrm{s}^1_1(e, a)$).
By definition $\{s(e)\} \subseteq f$ for every $e \in \mathbb{N}$. Further we have:

$$\begin{array}{lcl} e \in \mathrm{K} & \Rightarrow & \{s(e)\} \text{ is finite (therefore } \{s(e)\} \notin \mathcal{F}) \\ e \notin \mathrm{K} & \Rightarrow & \{s(e)\} = f \text{ therefore } \{s(e)\} \in \mathcal{F} \end{array} \quad (1)$$

Proof: If $e \in \mathrm{K}$, then $R(e, c)$ for some $c \in \mathbb{N}$, and for all $c > c_0$ we have $\{s(e)\}(c) \simeq g(e, c) \simeq \perp$, $\{s(e)\}$ is finite.
If $e \notin \mathrm{K}$, $\{s(e)\}(c) \simeq g(e, c) \simeq f(c)$ for all c, $\{s(e)\} = f$.
Therefore $e \in \mathbb{N} \setminus \mathrm{K} \Leftrightarrow s(e) \in \ulcorner\mathcal{F}\urcorner$, $\mathbb{N} \setminus \mathrm{K}$ is recursive enumerable, K is recursive, contradicting Theorem 5.5.
Assume $f \notin \mathcal{F}$, $f' \in \mathcal{F}$, $f' \subseteq f$, f' finite.
Define $g : \mathbb{N}^2 \to_{\mathrm{par}} \mathbb{N}$,

$$g(a, b) :\simeq \begin{cases} f(b) & \text{if } b \in \mathrm{dom}(f') \vee a \in \mathrm{K} \\ \perp & \text{otherwise.} \end{cases}.$$

Let using the s^m_n-theorem s be primitive recursive such that $\{s(e)\}(b) \simeq g(e, b)$.
$\{s(e)\} \subseteq f$.

$$\begin{array}{lcl} e \in \mathrm{K} & \Rightarrow & \{s(e)\} = f \text{ (therefore } \{s(e)\} \notin \mathcal{F}) \\ e \notin \mathrm{K} & \Rightarrow & \{s(e)\} = f' \text{ therefore } \{s(e)\} \in \mathcal{F} \end{array} \quad (1)$$

Again $e \in \mathbb{N} \setminus \mathrm{K} \Leftrightarrow s(e) \in \ulcorner\mathcal{F}\urcorner$ and as in the other direction follows again the assertion.

Definition 5.12 Assume $A, B \subseteq \mathbb{N}$. A and B are *recursively inseparable*, iff $A \cap B = \emptyset$ and there is no recursive set $C \subseteq \mathbb{N}$ such that $A \subseteq C$ and $B \subseteq \mathbb{N} \setminus C$.

Lemma 5.13 *Let $K_i := \{e \mid \{e\}^1(e) \simeq i\}$ for $i = 0, 1$. Then K_i are recursive enumerable and K_0 and K_1 are recursively inseparable.*

Proof: K_i are recursive enumerable is clear. Assume $K_0 \subseteq C \subseteq \mathbb{N}$, $K_1 \cap C = \emptyset$, C recursive, and let $\{e\}^1 = \chi_C$.
Assume $e \in C$. Then $\chi_C(e) = 1$, $\{e\}(e) = 1$, $e \in K_1$, $e \notin C$, a contradiction.
Assume $e \notin C$. Then $\chi_C(e) = 0$, $\{e\}(e) = 0$, $e \in K_0$, $e \in C$, a contradiction.

5.2 The Arithmetical Hierarchy

In this section we will follow very closely [Rat96].

Definition 5.14 (a) The *strict Σ_n and Π_n-formulas* in a language extending $\mathcal{L}_{\mathrm{ar}}$ are defined by:
Every Δ_0 formula (in the formulation of $\mathcal{L}_{\mathrm{ar}}$) is a strict Π_0- and Σ_0-formula.
If A is a strict Π_n-formula, then $\exists x.A$ is a strict Σ_{n+1}-formula.
If A is a strict Σ_n-formula, then $\forall x.A$ is a strict Π_{n+1}-formula.
In this section Σ_n-, Π_n-formula stands for strict Σ_n-, Π_n-formula. (Sometimes one defines Σ_n-formulas as extended Σ_n-formulas and therefore one sometimes writes strict Σ_n-formulas for what we are going to define)

(b) The Σ_n and Π_n relations are defined simultaneously inductively by: If R is recursive, then it is Σ_0 and Π_0.
If $R(\vec{x}, x)$ is Σ_n, $S(\vec{x}) \Leftrightarrow \forall x.R(\vec{x}, x)$, then S is Π_{n+1}.
If $R(\vec{x}, x)$ is Π_n, $S(\vec{x}) \Leftrightarrow \exists x.R(\vec{x}, x)$, then S is Σ_{n+1}.

Remark 5.15 *If $m \geq 1$, then $R \subseteq \mathbb{N}^n$ is Σ_m (Π_m) iff it can be defined by a Σ_m (Π_m)-formula A in $\mathbb{N}$ over the language $\mathcal{L}_{\text{ar}}$, i.e. for all $a_1, \dots, a_n \in \mathbb{N}$*

$$R(a_1, \dots, a_n) \Leftrightarrow \mathcal{N} \models A[x_1 := a_1, \dots, x_n := a_n]$$

Proof: It suffices to proof the assertion for $m = 1$. The Σ_1-relations are exactly the recursive enumerable relations which are exactly those definable by a (strict) Σ_1-formula The Π_1-relations are the complements of the Σ_1-relations, and the Π_1 formulas define exactly the relations which are complements of Σ_1-definable relations, so the assertion follows here again.

Lemma 5.16 *(a) If R is in $\Sigma_n \cup \Pi_n$, then R is in $\Sigma_m \cup \Pi_m$ for all $m > n$.*

(b) If R is an m-ary Σ_n (Π_n)-relation $f_1, \dots, f_m$ are recursive, then $Q' := \{\vec{x} \mid R(f_1(\vec{x}), \dots, f_m(\vec{x}))\}$ is Σ_n (Π_n), too

(c) If R is Σ_n, then $Q' := \{\vec{x} \mid \exists x.R(x, \vec{x})\}$ is Σ_n, too.
If R is Π_n, then $Q' := \{\vec{x} \mid \forall x.R(x, \vec{x})\}$ is Π_n, too.

(d) If R_0, R_1 are m-ary Σ_n (Π_n) relations, then $R_0 \cap R_1$, $R_0 \cup R_1$ are Σ_n (Π_n), too.

(e) If R is an m-ary Σ_n (Π_n) relation, then $\mathbb{N}^m \setminus R$ is Π_n (Σ_n).

(f) If R is Σ_n (Π_n), f is recursive, then $S := \{\vec{x} \mid \forall x < f(\vec{x})R(\vec{x}, x)\}$ and $T := \{\vec{x} \mid \exists x < f(\vec{x})R(\vec{x}, x)\}$ are Π_n (Σ_n), too.

Proof:
(a): If R is Σ_n, then by $R(\vec{x}) \Leftrightarrow \forall y.R(\vec{x})$ it is Π_{n+1}. Similar Π_n relations are Σ_{n+1}, too.
Every recursive relation is recursive enumerable, and since its complement is recursive as well, it is Σ_1 and Π_1. Therefore every Σ_0 or Π_0 relation is Σ_1 and Π_1 as well and from this follows that Σ_n (Π_n)-relations are Σ_{n+1} (Π_{n+1})-relations as well.
(b): trivial by induction on the definition of Π_n and Σ_n.
(c): First assertion If $R(x, \vec{x}) \Leftrightarrow \exists y.R'(x, y, \vec{x})$, R' Π_{n-1}, then $\exists x.R(x, \vec{x}) \Leftrightarrow \exists z.R'(\pi_1(z), \pi_2(z), \vec{x})$ for some new variable z. The second assertion follows similarly.
(d): Induction on n. $n = 0$ trivial. $n \to n+1$: Only for Σ_n. Let $R_i(\vec{x}) \Leftrightarrow \exists y S_i(\vec{x}, y)$, S_i Π_n. $(R_1 \overset{\cap}{\cup} R_2)(\vec{x}) \Leftrightarrow \exists y.(S_1(\vec{x}, \pi_1(y)) \overset{\wedge}{\vee} S_2(\vec{x}, \pi_2(y)))$ by IH Σ_n.
(e) trivial by induction on the definition.
(f) Proof simultaneously by induction on n. $n = 0$ follows, since recursive relations are closed under bounded quantification. $n \to n+1$. Consider only

the case Σ_{n+1}.
The second assertion follows from (c), (d) and since the $x < f(t)$ is recursive in the variables in t and x.
For the first assertion, let $R(\vec{x}, x) \Leftrightarrow \exists y.R'(\vec{x}, x, y)$ Then $\forall x < f(\vec{x}).R(\vec{x}, x) \Leftrightarrow \exists z.\forall x < f(\vec{x}).\exists y < z.R'(\vec{x}, x, y)$ and by IH follows the assertion.

Theorem 5.17 *For each $n, m > 0$ there exists an $m+1$-ary Σ_n (Π_n-)relation U_n^m ($\overline{\mathrm{U}}_n^m$), which enumerates the m-ary Σ_n (Π_n-)relations, i.e. for each m-ary Σ_n (Π_n-relation) R there exists an e such that*
$R(\vec{x}) \Leftrightarrow \mathrm{U}_n^m(e, \vec{x})$ and ($R(\vec{x}) \Leftrightarrow \overline{\mathrm{U}}_n^m(e, \vec{x})$) for all $\vec{x} \in \mathbb{N}^m$.

Proof:
$n = 1$: $\mathrm{U}_1^m(e, \vec{x}) :\Leftrightarrow W_e^n(\vec{x})$. U_1^m is recursive enumerable, therefore Σ_1 and enumerates by Lemma 5.4 all recursive enumerable, i.e. Σ_1-relations.
$\overline{\mathrm{U}}_1(e, \vec{x}) :\Leftrightarrow \neg\mathrm{U}_1(e, \vec{x})$ which enumerates all complements of recursive enumerable relations, i.e. Π_1-relations. $n \to n+1$: $\mathrm{U}_{n+1}^m(e, \vec{x}) \Leftrightarrow \exists y.\overline{\mathrm{U}}_n^{m+1}(e, y, \vec{x})$.
Similar for $\overline{\mathrm{U}}$.

Theorem 5.18 *Let Σ_n be the collection of all Σ_n-relations, similarly for Π_n. Then the following equations hold:*
$\Sigma_1 \overset{\subseteq}{\neq} \Sigma_2 \overset{\subseteq}{\neq} \cdots$.
$\Pi_1 \overset{\subseteq}{\neq} \Pi_2 \overset{\subseteq}{\neq} \cdots$
$\Sigma_n \not\subseteq \Pi_n$, $\Pi_n \not\subseteq \Sigma_n$.
$\Sigma_n \subseteq \Pi_{n+1}$, $\Pi_n \subseteq \Sigma_{n+1}$.

Proof:
$\Sigma_n \not\subseteq \Pi_n$: Let U_n^1 enumerate the Σ_n relations. $D(e) :\Leftrightarrow \mathrm{U}_n^1(e, e)$. D is Σ_n. If D were Π_n, then $D(e) \Leftrightarrow \neg\mathrm{U}_n^1(f, e)$ for some f, $D(f) \Leftrightarrow \neg\mathrm{U}_n^1(f, f) \Leftrightarrow \neg D(f)$, a contradiction.
$\Pi_n \not\subseteq \Sigma_n$: similarly.
$\Sigma_n \subseteq \Sigma_{n+1}$, $\Pi_n \subseteq \Pi_{n+1}$, $\Sigma_n \subseteq \Pi_{n+1}$, $\Pi_n \subseteq \Sigma_{n+1}$: already shown.
$\Sigma_{n+1} \not\subseteq \Sigma_n$: otherwise $\Sigma_{n+1} \subseteq \Sigma_n \subseteq \Pi_{n+1}$.

Chapter 6

Gödel's Second Incompleteness Theorem

We will follow very closely [Buc93b].

6.1 Proof of Gödel's and Löb's theorem

In this section we will prove Gödel's and Löb's theorem relative to some conditions on a theory T. We will later verify, that extension of a theory Z, which has primitive recursive functions, their defining axioms and full induction, fulfill these conditions.

Assumption 6.1 *In this section let T be a recursive axiom system in a recursive represented language $\mathcal{L}$ extending $\mathcal{L}_{\mathbb{N}}$ $(= \{=, 0, \mathrm{S}\})$, in which all primitive recursive functions are representable and which proves the equality axioms.*

Löb's theorem is relative to a predicate, expressed by a formula P. P usually stands for provability, and this instantiation is the original formulation of Gödel's second incompleteness theorem, which expresses that under some weak assumptions in an axiom system we can not prove its own consistency. However, the generalized form of both theorems is useful as well.
We will prove first the two theorems for arbitrary theories fulfilling some provability conditions. Then we will verify in section 6.3 that the ordinary provability predicate already in the relatively weak axiom system Z fulfills the conditions (D1) - (D3).

Definition 6.2

The following are provability conditions for a unary formula P in $\mathcal{L}$ and T:

(D1) $T \vdash A \Rightarrow T \vdash \mathrm{P}(\underline{\ulcorner A \urcorner})$ for every closed formula A.

(D2) $T \vdash \mathrm{P}(\underline{\ulcorner A \to B \urcorner}) \to \mathrm{P}(\underline{\ulcorner A \urcorner}) \to \mathrm{P}(\underline{\ulcorner B \urcorner})$ for every closed formula A, B.

(D3) $T \vdash \mathrm{P}(\underline{\ulcorner A \urcorner}) \to \mathrm{P}(\underline{\ulcorner \mathrm{P}(\underline{\ulcorner A \urcorner}) \urcorner})$.

Let $\mathrm{Provable}_\Sigma(b) := \exists a.\mathrm{Proof}^0_\Sigma(a, b)$, b is Gödelnumber of a formula provable in Σ.

If P is a unary formula in $\mathcal{L}$ let $\mathrm{Cons}_{T,\mathrm{P}} := \neg\mathrm{P}(\underline{\ulcorner \bot \urcorner})$. We write $\mathrm{Cons}_{T,\mathrm{Provable}_T}$ ("T is consistent").

(D1), (D2) can be shown in Z and for many other axiom systems easily. However, (D3) will require some effort.

Theorem 6.3 (Löb's theorem) *If* P *is a unary formula which fulfills (D1), (D2), (D3) relative to* T*. Then for every sentence* A *we have*

$$(T \vdash \mathrm{P}(\underline{\ulcorner A \urcorner}) \to A) \Rightarrow T \vdash A$$

Corollary 6.4 (Gödel's Second Incompleteness Theorem) *If* P *is a unary formula fulfilling (D1), (D2), (D3) relative to* T*,* T *is consistent. Then*

$$T \nvdash \mathrm{Cons}_{T,\mathrm{P}} \quad .$$

Proof of the corollary: Choose $A \equiv \bot$ in theorem 6.3.
Proof of Löb's theorem with Motivation:
Let $\vdash$ stand for provability in T.
First we will give a proof with motivation and then present the proof in a compact way.
It's easier to understand it, if we first consider the special case of Löb's theorem, namely Gödel's theorem (with $A :=\bot$. By the fixed point theorem there exists a formula C such that $\vdash C \leftrightarrow \neg\mathrm{P}(\underline{\ulcorner C \urcorner})$. ($C$ holds, iff it is not provable).
We show $\vdash \neg\mathrm{P}(\underline{\ulcorner C \urcorner})$:
$\vdash \mathrm{P}(\underline{\ulcorner C \urcorner}) \to \mathrm{P}(\underline{\ulcorner \mathrm{P}(\underline{\ulcorner C \urcorner}) \urcorner})$.
From $\vdash C \to \neg\mathrm{P}(\underline{\ulcorner C \urcorner})$ follows by D2 $\vdash \mathrm{P}(\underline{\ulcorner C \urcorner}) \to \mathrm{P}(\underline{\ulcorner \mathrm{P}(\underline{\ulcorner C \urcorner}) \urcorner}) \to \mathrm{P}(\underline{\ulcorner \bot \urcorner})$,
i.e. $\vdash \mathrm{P}(\underline{\ulcorner C \urcorner}) \to \mathrm{P}(\underline{\ulcorner \bot \urcorner})$,
and from $\mathrm{P}(\underline{\ulcorner \bot \urcorner}) \to \bot$ follows $\vdash \neg\mathrm{P}(\underline{\ulcorner C \urcorner})$.
Now we get $\vdash C$, $\vdash \mathrm{P}(\underline{\ulcorner C \urcorner})$, by $\vdash C \to \mathrm{P}(\underline{\ulcorner C \urcorner}) \to \bot$ therefore $\vdash \bot$.
Now we see that we haven't made use of the fact that $\bot$ was the falsum and can therefore replace A by an arbitrary sentence and yield Löb's theorem.
Short proof of Löb's theorem:
Abbreviation: $\Box A := \mathrm{P}(\underline{\ulcorner A \urcorner})$ (the binding is minimal, so $\Box A \to B$ should be read as $(\Box A) \to B$).
Further we write in this proof $\vdash$ for $T \vdash$.
Assume $A, \vdash \Box A \to A$. By the fixed point lemma 3.23 there exists an $\mathcal{L}$-sentence C such that $\vdash C \leftrightarrow (\Box C \to A)$. Then we get:
$\vdash C \to (\Box C \to A)$.
$\vdash \Box(C \to (\Box C \to A))$. (by (D1)).
$\vdash \Box C \to (\Box\Box C \to \Box A)$. (by (D2)).
$\vdash \Box C \to \Box\Box C$. (is (D3))
$\vdash \Box C \to \Box A$.

$\vdash \Box A \to A$ (assumption).
$\vdash \Box C \to A$.
$\vdash C$.
$\vdash \Box C$.
$\vdash A$.

6.2 The axiom system Z.

Notation 6.5 (a) We write in the following $\equiv$ for syntactical identity between two terms, formulas etc. By $T \vdash s \equiv t_0 = t_1 = \cdots = t_m \equiv t$ we mean that $s \equiv t_0$, $t_m \equiv t$ and $T \vdash t_0 = t_1$, $T \vdash t_1 = t_2, \dots, T \vdash t_{m-1} = t_m$. Statements like $T \vdash s = t \equiv t' = t''$ should be read similarly.

(b) Let in the following $\mathcal{L}$ be a primitive recursively represented language (with enumeration enum) such that $\mathcal{L}_{\mathrm{PR}} \subseteq \mathcal{L}$. Term, formula etc. means in this section $\mathcal{L}$-term, $\mathcal{L}$-term etc.

Definition 6.6 (a) The axiom system Z has the following axioms in the language $\mathcal{L}_{\mathrm{PR}}$ $(0 := 0^0)$:

(Z =) The equality axioms for $\mathcal{L}_{\mathrm{PR}}$.
(Z bas) $\forall x(\neg(\mathrm{S}(x) = 0)) \land \forall x.\forall y(\mathrm{S}(x) = \mathrm{S}(y) \to x = y)$.
(Z 0^n) $\forall x_1, \dots, x_n.0^n(x_1, \dots, x_n) = 0$.
(Z proj^i_n) $\forall x_1, \dots, x_n.\mathrm{proj}^i_n(x_1, \dots, x_n) = x_i$.
(Z $\circ$) $\forall x_1, \dots, x_n.(f \circ (g_1, \dots, g_m))(x_1, \dots, x_n) =$
$f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_m))$
$(g_i \in \mathrm{PR}^n,\ f \in \mathrm{PR}^m)$.
(Z R_0) $\forall x_1, \dots, x_n.(\mathrm{R}gh)(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n)$.
$(g \in \mathrm{PR}^n,\ h \in \mathrm{PR}^{n+2})$
(Z $\mathrm{R_S}$) $\forall x_1, \dots, x_n, y.(\mathrm{R}gh)(x_1, \dots, x_n, \mathrm{S}(y)) =$
$h(x_1, \dots, x_n, y, (\mathrm{R}gh)(x_1, \dots, x_n, y))$.
$(g \in \mathrm{PR}^n,\ h \in \mathrm{PR}^{n+2})$
(Z Ind) $A(0) \to \forall x(A(x) \to A(\mathrm{S}(x))) \to \forall x.A(x)$,
where $A(x)$ is an arbitrary formula of $\mathcal{L}_{\mathrm{PR}}$.

(b) Let $1 := \mathrm{S}(0)$, $x < y := \chi_<(x, y) = 1$.

(c) Let in this section $\mathcal{N}$ be the standard structure of $\mathcal{L}_{\mathrm{PR}}$.

Lemma 6.7 *(a) If $f \in \mathrm{PR}^n$, $a_1, \dots, a_n \in \mathbb{N}$, then $\mathrm{Z} \vdash f(\underline{a_1}, \dots, \underline{a_n}) = \underline{f(a_1, \dots, a_n)}$*

(b) If t is a term in $\mathcal{L}_{\mathrm{PR}}$, $\mathrm{FV}(t) \subseteq \{x_1, \dots, x_n\}$, $t^{\mathcal{N}}[x_1 := a_1, \dots, x_n := a_n] = b$, then $\mathrm{Z} \vdash t[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}] = \underline{b}$.

(c) If A is a Δ_0-sentence, then if $\mathcal{N} \models A$, then $\mathrm{Z} \vdash A$, and if $\mathcal{N} \models \neg A$, then $\mathrm{Z} \vdash \neg A$.

(d) *If A is an extended Σ_1-sentence, $\mathcal{N} \models A$, then* $\mathrm{Z} \vdash A$.

Proof:
(a): Induction on the definition of f:
$f = 0^n$: $\mathrm{Z} \vdash 0^n(\underline{a_1}, \ldots, \underline{a_n}) = 0 \equiv \underline{0^n(a_1, \ldots, a_n)}$.
$f = \mathrm{S}$: $\mathrm{Z} \vdash \mathrm{S}(\underline{a_1}) = \mathrm{S}(\underline{a_1}) \equiv \underline{\mathrm{S}(a_1)}$.
$f = \mathrm{proj}^i_n$: $b = a_i$, $\mathrm{Z} \vdash \mathrm{proj}^n_i(\underline{a_1}, \ldots, \underline{a_n}) = \underline{a_i} \equiv \underline{\mathrm{proj}^n_i(a_1, \ldots, a_n)}$.
$f = h \circ (g_1, \ldots, g_m)$: Let $c_i := g_i(\vec{a})$.
$\mathrm{Z} \vdash g_i(\underline{a_1}, \ldots, \underline{a_n}) = \underline{c_i}$,
$\mathrm{Z} \vdash h(\underline{c_1}, \ldots, \underline{c_m}) = \underline{h(c_1, \ldots, c_m)}$,

$$\begin{array}{rcl} \mathrm{Z} \vdash f(\underline{a_1}, \ldots, \underline{a_n}) & = & h(g_1(\underline{a_1}, \ldots, \underline{a_n}), \ldots, g_m(\underline{a_1}, \ldots, \underline{a_n})) \\ & = & h(\underline{c_1}, \ldots, \underline{c_m}) \\ & = & \underline{h(c_1, \ldots, c_m)} \\ & = & \underline{f(a_1, \ldots, a_n)} \ . \end{array}$$

$f = (\mathrm{R}gh)$: Show $\mathrm{Z} \vdash f(\underline{a_1}, \ldots, \underline{a_n}, \underline{c}) = \underline{f(a_1, \ldots, a_n, c)}$ by side-induction on c.
$c = 0$:
$\mathrm{Z} \vdash f(\underline{a_1}, \ldots, \underline{a_n}, \underline{0}) \equiv f(\underline{a_1}, \ldots, \underline{a_n}, 0) = g(\underline{a_1}, \ldots, \underline{a_n}) = \underline{g(a_1, \ldots, a_n)} = \underline{b}$.
$c \to c + 1$:

$$\begin{array}{rcl} \mathrm{Z} \vdash f(\underline{a_1}, \ldots, \underline{a_n}, \underline{c+1}) & \equiv & f(\underline{a_1}, \ldots, \underline{a_n}, \mathrm{S}(\underline{c})) \\ & = & h(\underline{a_1}, \ldots, \underline{a_n}, \underline{c}, f(\underline{a_1}, \ldots, \underline{a_n}, \underline{c})) \\ & \overset{\text{side IH}}{=} & h(\underline{a_1}, \ldots, \underline{a_n}, \underline{c}, \underline{f(a_1, \ldots, a_n, c)}) \\ & \overset{\text{main IH}}{=} & \underline{h(a_1, \ldots, a_n, c, f(a_1, \ldots, a_n, c))} \\ & \equiv & \underline{f(a_1, \ldots, a_n, c+1)} \end{array}$$

(b), (c): Exercise.

Lemma 6.8 (a) *If $A(x)$ is an $\mathcal{L}_{\mathrm{PR}}$-formula, then* $\mathrm{Z} \vdash \forall x(\forall y < x(A(y)) \to A(x)) \to \forall x.A(x)$.

(b) *If $R_1, \ldots, R_n$ are n-ary primitive recursive relations, $f_1, \ldots, f_{n+1}$ are primitive recursive functions, $R_n := \mathbb{N}^n \setminus (R_1 \cup \cdots \cup R_n)$, $f(\vec{x}) = \chi_{R_1}(\vec{x}) \cdot f_1(\vec{x}) + \cdots + \chi_{R_{n+1}}(\vec{x}) \cdot f_{n+1}(\vec{x})$, defined in the standard way, then* $\mathrm{Z} \vdash \forall \vec{x}(\bigwedge_{1 \le i < j \le n}(\neg(\chi_{R_i}(\vec{x}) = 1 \land \chi_{R_j}(\vec{x}) = 1)) \to \chi_{R_k}(\vec{x}) = 1 \to f(\vec{x}) = f_k(\vec{x}))$.

(c) *All the properties of* $+$, $\cdot$, $\dot{-}$, pred, $\sum(f)$, $\overline{\mu}(f)$, π, π_1, π_2, lh, $(\cdot)_\cdot$, $\cdot * <\cdot>$, $<\cdot, \ldots, \cdot>$, *which are statements in $\mathcal{L}_{\mathrm{PR}}$ like $\forall x, y(x + 0 = x \land x + \mathrm{S}(y) = \mathrm{S}(x + y))$ (i.e.* not *statements of the form f is primitive recursive) can be shown in* Z.

(d) *If t is a term of $\mathcal{L}_{\mathrm{PR}}$, $\mathrm{FV}(t) \subseteq \{x_1, \ldots, x_n\}$, $f := \widetilde{\lambda} x_1, \ldots, x_n.t$, then* $\mathrm{Z} \vdash f(x_1, \ldots, x_n) = t$.

(e) *If A is a Δ_0 formula* $\mathrm{FV}(A) \subseteq \{x_1, \dots, x_n\}$*, x_i distinct, R primitive recursive defined as in Lemma 2.17 such that* $R(\vec{a}) \Leftrightarrow \mathcal{N} \models A[x_1 := a_1, \dots, x_n := a_n]$*. Then* $\mathrm{Z} \vdash \forall \vec{x}((\chi_R(\vec{x}) = 1 \leftrightarrow A) \wedge (\chi_R(\vec{x}) = 0 \leftrightarrow \neg A))$.

(f) *If* $f \in \mathrm{PR}$*, then* $\mathrm{Z} \vdash (\overline{\mu} f)(\vec{a}, b) = y \leftrightarrow ((y = b \vee f(\vec{a}, b) = 0) \wedge \forall y' < y(y' \neq b \wedge f(\vec{a}, y') \neq 0))$.

Proof: (a): Note that $\chi_<(x, y) = \mathrm{sig}(y \dot{-} x)$, where $\mathrm{sig}(x) := 1 \dot{-} (1 \dot{-} x) = \begin{cases} 1 & \text{if } x > 0 \\ 0 & \text{if } x \leq 0 \end{cases}$. With this definition and a prove of elementary properties about $\dot{-}$ one can show $\mathrm{Z} \vdash \neg(x < 0)$ and $\mathrm{Z} \vdash (x < \mathrm{S}(y)) \leftrightarrow (x < y \vee x = y)$. Let $B(y) := \forall x < y.A(x)$. $\mathrm{Z} \vdash B(0)$, and Z proves that from $\forall y(\forall y' < y(A(y')) \rightarrow A(y))$ follows $\forall x(B(x) \rightarrow B(x+1))$, therefore by using Induction $\forall x.B(x)$, $\forall x.A(x)$.
(b) - (f): One verifies easily that all the proofs can be carried out using course of value induction. Some additional theorems like associativity of + or
$(\sum f)(\vec{a}, b) = 0 \Leftrightarrow \forall i < b.f(\vec{a}, i) = 0$ need to be proved as well, the proofs are tedious but easy.

6.3 Verification of conditions (D1) - (D3) in extensions of Z

We will show that extensions of Z with the standard provability predicate fulfill (D1) - (D3). (D1), (D2) will be shown easily, the main problem will be (D3).
In order to show (D3), we will prove more generally that for every extended Σ_1-sentence C we have $T \vdash C \rightarrow \mathrm{P}(\underline{\ulcorner C \urcorner})$. This will be done by using that every extended Σ_1-formula A is (in Z provable) equivalent to a formula $\exists x.f(x, \vec{x}) = 0$, where f is primitive recursive, so $f(x, \vec{x}) \rightarrow A$ and we need to show only the reflection principle for the (open!) formula $f(x, \vec{x}) = 0$. However, if P expresses provability in a theory Σ, then $f(x, \vec{x}) = 0 \rightarrow \mathrm{P}(\underline{\ulcorner f(x, \vec{x}) = 0 \urcorner})$ is in general not a valid formula, since the conclusion expresses $\Sigma \vdash f(x, \vec{x}) = 0$, therefore as well $\Sigma \vdash \forall x, \vec{x}.f(x, \vec{x}) = 0$ which does in general not follow from $f(x, \vec{x}) = 0$ for *some* $x, \vec{x}$.
The correct statement is $f(x, \vec{x}) = 0 \rightarrow \mathrm{P}([f(x, \vec{x}) = 0])$, where for formulas C with $\mathrm{FV}(C) = \{x_1, \dots, x_n\}$ $[C]$ is a term with $\mathrm{FV}([C]) \subseteq \mathrm{FV}(C)$ such that $([C])^{\mathcal{N}}[x_1 := a_1, \dots, x_n := a_n] = \ulcorner C[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}] \urcorner$. $C \rightarrow \mathrm{P}([C])$ expresses: "if C holds under assignment $x_i = a_i$, then $C[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}]$ is provable".
In case of quantifiers we have to deal with substitutability. However, it turns out that we never need to consider open quantified formulas, so we can restrict ourselves to simple formulas, as defined in the following.

Definition 6.9 (a) The set of *simple* formulas is inductively defined by:
If A is a prime formula, then A is simple.

If $\overset{\forall}{\exists} x.A$ is a closed formula, then A is simple.
If A, B are simple, then $\neg A$, $A \overset{\wedge}{\vee} B$, $A \to B$ are simple.

(b) A *simple expression* is a term or a simple formula.

(c) Let in the following (in this section only) $f \in \mathcal{L}^+ \cup \mathrm{Junc}$.

Definition 6.10 (a) Let $<\cdot, \dots, \cdot> \in \mathrm{PR}^n$,
$<\cdot, \dots, \cdot>(a_1, \dots, a_n) := <a_1, \dots, a_n>$.
If $t_1, \dots, t_n$ are terms, then $<t_1, \dots, t_n> := <\cdot, \dots, \cdot>(t_1, \dots, t_n)$ (a term, starting with a function symbol for $<\cdot, \dots, \cdot>$ applied to the terms $t_1, \dots, t_n$).

(b) Define $\nu : \mathbb{N} \to \mathbb{N}$, $\nu(n) := \ulcorner \underline{n} \urcorner$. Note, that $\nu(t)$ is a term, if t is a term (more precisely the application of the function symbol for ν to t).

Lemma 6.11 *(a)* $\mathrm{Z} \vdash \mathrm{Sub}(\underline{\ulcorner E \urcorner}, \underline{\ulcorner x \urcorner}, y) = \underline{\ulcorner E \urcorner}$ *for expressions* E *such that* $x \notin \mathrm{FV}(E)$.

(b) $\mathrm{Z} \vdash \mathrm{Sub}(\underline{\ulcorner x \urcorner}, \underline{\ulcorner x \urcorner}, y) = y$.

(c) $\mathrm{Z} \vdash \mathrm{Sub}(<\underline{\mathrm{enum}(f)}, z_1, \dots, z_n> \underline{\ulcorner x \urcorner}, y) =$
$<\underline{\mathrm{enum}(f)}, \mathrm{Sub}(z_1, \underline{\ulcorner x \urcorner}, y), \dots, \mathrm{Sub}(z_n, \underline{\ulcorner x \urcorner}, y)>$
(if n is the arity of f).

Proof: (a): Induction on the definition of E, using mainly Lemma 6.8 (d), (e). (b), (c): use Lemma 6.8 (e).

We will define $[u]$ for all simple expressions, and the obvious generalization of the condition would be: $[E]^{\mathcal{N}}[x_1 := a_1, \dots, x_n := a_n] = \ulcorner E[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}] \urcorner$. Therefore $[x]^{\mathcal{N}}[x := a] = \ulcorner \underline{a} \urcorner$, therefore we can define $[x] := \nu(x)$ $((\nu(x))^{\mathcal{N}}[x := a] = \nu(a) = \ulcorner \underline{a} \urcorner)$, $[f(E_1, \dots, E_n)] := <\underline{\mathrm{enum} f}, [E_1], \dots, [E_n]>$ and since, if E is simple and $E \equiv \overset{\forall}{\exists} xA$, then E is closed, $[\overset{\forall}{\exists} A] := \underline{\ulcorner \overset{\forall}{\exists} A \urcorner}$.
We need to prove $\mathrm{P}(\underline{\ulcorner A \urcorner}) \to \mathrm{P}([A])$, which expresses that, if A is provable, then $A[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}]$ is provable as well. For this step we need induction on the number of variables and therefore we will define more generally a term $[E]^U$ for every finite set of variables U such that, if $U = \{x_1, \dots, x_n\}$, $([E]^U)^{\mathcal{N}}[x_1 := a_1, \dots, x_n := a_n] = \ulcorner A[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}] \urcorner$. Now, in case $E = x \in U$, $[E]^U := \nu(x)$ and in case $E = x \notin U$, $[E]^U := \underline{\ulcorner x \urcorner}$ is a good definition. $[E]$ can now be defined as $[E]^{\mathrm{FV}(E)}$.

Definition 6.12 (a) For U being a finite set of variables, E a simple expression we define a $\mathcal{L}_{\mathrm{PR}}$-term $[E]^U$ by:

$$[x]^U := \begin{cases} \underline{\nu(x)} & \text{if } x \in U \\ \underline{\ulcorner x \urcorner} & \text{otherwise.} \end{cases}.$$

$[f(E_1, \dots, E_n)]^U := <\underline{\mathrm{enum}(f)}, [E_1]^U, \dots, [E_n]^U>$.
$[\overset{\forall}{\exists} xA]^U := \underline{\ulcorner \forall x.A \urcorner}$.

(b) $[E] := [E]^{\mathrm{FV}(E)}$.

Remark 6.13 *If A is a simple expression, $U \cap \mathrm{FV}(A) = \{x_1, \dots, x_n\}$, $\mathrm{FV}(A) \setminus U = \{y_1, \dots, y_m\}$, x_i, y_i are distinct, then $\mathrm{FV}([A]) = U \cap \mathrm{FV}(A)$ and*

$$([A]^U)^{\mathcal{N}}[x_1 := a_1, \dots, x_n := a_n] = \ulcorner A[x_1 := \underline{a_1}, \dots, x_n := \underline{a_n}]\urcorner$$

Remark 6.14 $[x] \equiv \nu(x)$
$[f(E_1, \dots, E_n)] \equiv <\underline{\mathrm{enum}(f)}, [E_1], \dots, [E_n]>$.

Lemma 6.15 *Let E be simple.*

(a) $\mathrm{Z} \vdash [E]^{\emptyset} = \underline{\ulcorner E \urcorner}$

(b) $\mathrm{Z} \vdash [t] = \nu(t) \to [E[y := t]] = [E][y := t]$

(c) $\mathrm{Z} \vdash [0] = \nu(0) \wedge [\mathrm{S}x] = \nu(\mathrm{S}(x)) \wedge [x] = \nu(x)$.

(d) For the terms $t \in \{0, x, \mathrm{S}(x)\}$, $\mathrm{Z} \vdash [E[y := t]] = [E][y := t]$.

Proof:
Let $\vdash$ stand for provability from axioms in Z.
(a): Induction on the definition of E:
$E = x$: $[x]^{\emptyset} \equiv \underline{\ulcorner x \urcorner}$.
$E = f(E_1, \dots, E_n)$:
By Lemma 6.7 $\vdash \underline{\ulcorner E \urcorner} = <\underline{\mathrm{enum}(f)}, \underline{\ulcorner E_1 \urcorner}, \dots, \underline{\ulcorner E_n \urcorner}>$,
by IH $\vdash \underline{\ulcorner E_i \urcorner} = [E_i]^{\emptyset}$,
further by definition $[E]^{\emptyset} \equiv <\underline{\mathrm{enum}(f)}, [E_1]^{\emptyset}, \dots, [E_n]^{\emptyset}>$.
$E \equiv \forall x A$: $[E]^{\emptyset} \equiv \underline{\ulcorner E \urcorner}$.
(b): Special case $E \equiv y$: $\mathrm{Z} \vdash [t] = \nu(t) \to [E[y := t]] \equiv [t] = \nu(y)[y := t] \equiv [E][y := t]$. Other cases: Easy induction on E.
(c): $\vdash [0] = \nu(0)$ follows by 6.7.
$\vdash [\mathrm{S}(x)] = <\underline{\mathrm{enum}(\mathrm{S})}, [x]> = <\underline{\mathrm{enum}(\mathrm{S})}, \nu(x)> = \nu(\mathrm{S}x)$.
$[x] \equiv \nu(x)$.
(d) By (b), (c).

Lemma 6.16 *(a)* $\mathrm{Z} \vdash \mathrm{Sub}(\nu(z), \underline{\ulcorner x \urcorner}, y) = \nu(z)$.

(b) If E is simple, then $\mathrm{Z} \vdash \mathrm{Sub}([E]^U, \underline{\ulcorner x \urcorner}, \nu(x)) = [E]^{U \cup \{x\}}$.

Proof:
Again we write $\vdash$ for provability in Z.
(a) $\vdash \mathrm{Sub}(\nu(0), \underline{\ulcorner x \urcorner}, y) \equiv \mathrm{Sub}(<\underline{\mathrm{enum}(0)}>, \underline{\ulcorner x \urcorner}, y) = \nu(0)$.

$$\begin{aligned}
\mathrm{Sub}(\nu(z), \underline{\ulcorner x \urcorner}, y) = \nu(z) \quad \vdash \quad & \mathrm{Sub}(\nu(\mathrm{S}(z)), \underline{\ulcorner x \urcorner}, y) \\
& = \mathrm{Sub}(<\underline{\mathrm{enum}(\mathrm{S})}, \nu(z)>, \underline{\ulcorner x \urcorner}, y) \\
& = <\underline{\mathrm{enum}(\mathrm{S})}, \mathrm{Sub}(\nu(z), \underline{\ulcorner x \urcorner}, y)> \\
& = <\underline{\mathrm{enum}(\mathrm{S})}, \nu(z)> \\
& = \nu(\mathrm{S}(z)) \ ,
\end{aligned}$$

therefore by the induction principle of Z follows the assertion.
(b): Induction on E. $U' := U \cup \{x\}$.
1. $E \equiv y \in U$:

$$\begin{aligned}\vdash \mathrm{Sub}([E]^U, \underline{\ulcorner x \urcorner}, \nu(x)) &= \mathrm{Sub}([y]^U, \underline{\ulcorner x \urcorner}, \nu(x))\\ &= \mathrm{Sub}(\nu(y), \underline{\ulcorner x \urcorner}, \nu(x))\\ &= \nu(y)\\ &= [E]^{U'} \quad .\end{aligned}$$

2. $E \equiv x \notin U$:

$$\begin{aligned}\vdash \mathrm{Sub}([E]^U, \underline{\ulcorner x \urcorner}, \nu(x)) &= \mathrm{Sub}([x]^U, \underline{\ulcorner x \urcorner}, \nu(x))\\ &= \mathrm{Sub}(\underline{\ulcorner x \urcorner}, \underline{\ulcorner x \urcorner}, \nu(x))\\ &= \nu(x)\\ &= [E]^{U'} \quad .\end{aligned}$$

3. $E \equiv y \notin U$, $y \not\equiv x$:

$$\begin{aligned}\vdash \mathrm{Sub}([E]^U, \underline{\ulcorner x \urcorner}, \nu(x)) &= \mathrm{Sub}([y]^U, \underline{\ulcorner x \urcorner}, \nu(x))\\ &= \mathrm{Sub}(\underline{\ulcorner y \urcorner}, \underline{\ulcorner x \urcorner}, \nu(x))\\ &= \underline{\ulcorner y \urcorner} = [E]^{U'} \quad .\end{aligned}$$

4. $E \equiv f(E_1, \ldots, E_n)$:

$$\begin{aligned}\vdash \quad & \mathrm{Sub}([E]^U, \underline{\ulcorner x \urcorner}, \nu(x))\\ & = \mathrm{Sub}(<\underline{\mathrm{enum}(f)}, [E_1]^U, \ldots, [E_n]^U>, \underline{\ulcorner x \urcorner}, \nu(x))\\ & = <\underline{\mathrm{enum}(f)}, \mathrm{Sub}([E_1]^U, \underline{\ulcorner x \urcorner}, \nu(x)), \ldots, \mathrm{Sub}([E_n]^U, \underline{\ulcorner x \urcorner}, \nu(x))>\\ & \stackrel{\mathrm{IH}}{=} <\underline{\mathrm{enum}(f)}, [E_1]^{U'}, \ldots, [E_n]^{U'}>\\ & = [E]^{U'} \quad .\end{aligned}$$

5. $E \equiv \forall x A$, $\mathrm{FV}(E) = \emptyset$:
$\vdash \mathrm{Sub}([E]^U, \underline{\ulcorner x \urcorner}, \nu(x)) = \mathrm{Sub}(\underline{\ulcorner E \urcorner}, \underline{\ulcorner x \urcorner}, \nu(x)) = \underline{\ulcorner E \urcorner} = [E]^{U'}$.

Assumption 6.17 *Let in the following Σ be a primitive recursive axiom system in a recursively represented language $\mathcal{L}$ such that $\mathcal{L} \supseteq \mathcal{L}_{\mathrm{PR}}$, which proves the equality axioms and* Z.

Lemma 6.18 *Let* P *be a unary formula in $\mathcal{L}_{\mathrm{PR}}$ such that:*

(P1) $(\Sigma \vdash A) \Rightarrow \Sigma \vdash \mathrm{P}(\underline{\ulcorner A \urcorner})$, *if A is simple.*

(P2) $\Sigma \vdash \mathrm{P}([A \to B]) \to \mathrm{P}([A]) \to \mathrm{P}([B])$ *for all simple formulas B.*

(P3) $\Sigma \vdash \mathrm{P}(z) \to \mathrm{P}(\mathrm{Sub}(z, \underline{\ulcorner x \urcorner}, \nu(y)))$.

Then

(P*) $(\Sigma \vdash A_1 \to \cdots \to A_m \to B) \Rightarrow \Sigma \vdash (\mathrm{P}([A_1]) \to \cdots \to \mathrm{P}([A_m]) \to \mathrm{P}([B]))$ *for all $m \geq 0$ and simple formulas $A_1, \ldots, A_m, B$.*

Proof:
We write $\vdash$ for $\Sigma\vdash$.
We show first

$$(\vdash A) \text{ and } A \text{ simple } \Rightarrow \vdash \mathrm{P}([A]^U) \ . \qquad (*)$$

by induction on the number of elements in U:
$U=\emptyset$: If $(\vdash A)$, then by (P1) $\vdash (\mathrm{P}(\underline{\ulcorner A \urcorner}))$, further $\vdash \underline{\ulcorner A \urcorner} = [A]^\emptyset$.
$U \to U \cup \{x\}$: If $\vdash A$, by IH $\vdash \mathrm{P}([A]^U)$, by (P3)
$\vdash \mathrm{P}([A]^U) \to \mathrm{P}(\mathrm{Sub}([A]^U, \underline{\ulcorner x \urcorner}, \nu(y)))$,
by Lemma 6.16 (b) $\vdash \mathrm{Sub}([A]^U, \underline{\ulcorner x \urcorner}, \nu(x)) = [A]^{U\cup\{x\}}$.
We show for $m \geq 0$, simple formulas $A_1, \ldots, A_m, B$:

$$\vdash \mathrm{P}([A_1 \to \cdots \to B]) \to \mathrm{P}([A_1]) \to \cdots \to \mathrm{P}([A_m]) \to \mathrm{P}([B]) \ . \qquad (**)$$

Proof by induction on m: $m=0$: trivial.
$m \to m+1$: Let $C := A_2 \to \cdots \to A_{m+1} \to B$.
By (P2) $\vdash \mathrm{P}([A_1 \to C]) \to \mathrm{P}([A_1]) \to \mathrm{P}([C])$, by IH
$\vdash \mathrm{P}([C]) \to \mathrm{P}([A_2]) \to \cdots \to \mathrm{P}([A_{m+1}]) \to \mathrm{P}([B])$ and therefore the assertion.
By $(*)$ and $(**)$ follows the assertion.

Lemma 6.19 *If* P *is a unary formula such that* (P^*) *(as in Lemma 6.18) holds. Then for every* n*-ary function symbol* $g \in \mathrm{PR}$ *we have*

$$\Sigma \vdash g(x_1, \ldots, x_n) = y \to \mathrm{P}([g(x_1, \ldots, x_n) = y]) \ .$$

Proof: We write $\vdash$ for $\Sigma\vdash$.
We will use for the operation $A \mapsto [A]$ only (P^*), Lemma 6.15 (c) and $[A]$ is an $\mathcal{L}_{\mathrm{PR}}$-term such that $\mathrm{FV}([A]) = \mathrm{FV}(A)$.
It suffices to prove

$$\vdash \mathrm{P}([g(\vec{x}) = y][y := g(\vec{x})]) \ . \qquad (*)$$

(note that $\mathrm{P}([E])[x := t] \equiv \mathrm{P}([E])[x := t])$.
Then follows by the equality axioms the assertion.
Induction on the definition of g:
Case $g \equiv 0^n, \mathrm{S}, \mathrm{proj}^i_n$: Let $t := 0, \mathrm{S}(x_1), x_i$ respectively.
$\vdash g(\vec{x}) = t$, (axiom of Z),
$\vdash \mathrm{P}([g(\vec{x}) = t])$ (P^*)
$\vdash [g(\vec{x}) = y][y := t] = [(g(\vec{x}) = y)[y := t]] \equiv [g(\vec{x}) = t]$ (by 6.15 (c))
$\vdash \mathrm{P}([g(\vec{x}) = y][y := t])$.
Case $g \equiv h \circ (g_1, \ldots, g_m)$.
Let $s_i := g_i(\vec{x})$, $s := h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$.
$\vdash g(\vec{x}) = s$. (axiom of Z)
$\vdash g_1(\vec{x}) = y_1 \to \cdots \to g_m(\vec{x}) = y_m \to h(y_1, \ldots, y_m) = z \to g(\vec{x}) = z$
(equality axioms).
$\vdash \mathrm{P}([g_1(\vec{x}) = y_1]) \to \cdots \to \mathrm{P}([g_m(\vec{x}) = y_m]) \to$

$\mathrm{P}([h(y_1,\dots,y_m)=z]) \to \mathrm{P}([g(\vec{x})=z])$ (by (P^*)).
$\vdash \mathrm{P}([g_1(\vec{x})=y_1][y_1:=s_1]) \to \cdots \to \mathrm{P}([g_m(\vec{x})=y_m][y_m:=s_m])$
$\to \mathrm{P}([h(y_1,\dots,y_m)=z][y_1:=s_1,\dots,y_m:=s_m,z:=s])$
$\to \mathrm{P}([g(\vec{x})=z][z:=s])$
(by equality axioms).
$\vdash \mathrm{P}([g_i(\vec{x})=y_i][y_i:=s_i])$ (IH).
$\vdash \mathrm{P}([h(\vec{y})=z][z:=h(\vec{y})])$ (IH).
$\vdash \mathrm{P}([h(\vec{y})=z][y_1:=s_1,\dots,y_m:=s_m,z:=s])$ (equality axioms).
$\vdash \mathrm{P}([g(\vec{x})=z][z:=s])$.
$\vdash s=g(\vec{x})$.
$\vdash \mathrm{P}([g(\vec{x})=z][z:=g(\vec{x})])$.
Case $g=\mathrm{R}g'h$.

Let $t(z,y):\equiv[g(\vec{x},z)=u][u:=y]$.
We show $\vdash \mathrm{P}(t(0,g(\vec{x},0)))$ and $\vdash \mathrm{P}(t(z,g(\vec{x},z)))\to\mathrm{P}(t(\mathrm{S}(z),g(\vec{x},\mathrm{S}(z))))$.
By formal induction in Σ (**OBS!** here is where full induction is needed — this complexity can however be reduced), follows
$\vdash \mathrm{P}(t(z,g(\vec{x},z)))$, i.e. the assertion.
1. $\vdash g(\vec{x},0)=g'(\vec{x})$. (axiom of Z).
$\vdash g'(\vec{x})=y\to g(\vec{x},0)=y$.
$\vdash \mathrm{P}([g'(\vec{x})=y])\to\mathrm{P}([g(\vec{x},0)=y])$.
$\vdash \mathrm{P}([g'(\vec{x})=y][y:=g'(\vec{x})])\to\mathrm{P}([g(\vec{x},0)=y][y:=g(\vec{x},0)])$.
$\vdash \mathrm{P}([g'(\vec{x})=y][y:=g'(\vec{x})]$ (IH).

2. $\vdash g(\vec{x},\mathrm{S}(y))=h(\vec{x},y,g(\vec{x},y))$.
$\vdash g(\vec{x},y)=z\to h(\vec{x},y,z)=u\to g(\vec{x},\mathrm{S}(y))=u$.
$\vdash \mathrm{P}([g(\vec{x},y)=z])\to\mathrm{P}([h(\vec{x},y,z)=u])\to\mathrm{P}([g(\vec{x},\mathrm{S}(y))=u])$ (P^*).
$\vdash \mathrm{P}([g(\vec{x},y)=z][z:=g(\vec{x},y)])$
$\to \mathrm{P}([h(\vec{x},y,z)=u][z:=g(\vec{x},y),u:=h(\vec{x},g(\vec{x},y))])$
$\to \mathrm{P}([g(\vec{x},\mathrm{S}(y))=u][u:=g(\vec{x},\mathrm{S}(y))])$
(by $\vdash h(\vec{x},g(\vec{x},y))=g(\vec{x},\mathrm{S}(y))$).
$\vdash \mathrm{P}([h(\vec{x},y,z)=u][u:=h(\vec{x},y,z)])$ (IH).
$\vdash \mathrm{P}([h(\vec{x},y,z)=u][z:=g(\vec{x},y),u:=h(\vec{x},g(\vec{x},y),z)])$.
$\mathrm{P}([g(\vec{x},y)=z][z:=g(\vec{x},y)]\vdash\mathrm{P}([g(\vec{x},\mathrm{S}(y))=u][u:=g(\vec{x},\mathrm{S}(y))])$

Lemma 6.20 *For every extended Σ_1-formula A in $\mathcal{L}_{\mathrm{PR}}$ and $x_1,\dots,x_n$ such that*
$\mathrm{FV}(A)\subseteq\{x_1,\dots,x_n\}$ *there exists $g\in\mathrm{PR}^{n+1}$ such that*

$$\mathrm{Z}\vdash A\leftrightarrow\exists z(g(x_1,\dots,x_n,z)=0)\ .$$

Proof:
First, $\mathrm{Z}\vdash A\leftrightarrow A'$ for some strict Σ_1-formula A' (see proof of Lemma 2.33) with $\mathrm{FV}(A')\subseteq\mathrm{FV}(A)$ by formalizing the argument in the proof of Lemma 2.33 in Z (use Meta-induction on the definition of extended Σ_1-formulas).
Let $A'\equiv\exists z.B$, B Δ_0. By Lemma 6.8 (d) there exists an $g\in\mathrm{PR}^{n+1}$ such that $\mathrm{Z}\vdash B\leftrightarrow g(\vec{x},z)=0$.

Lemma 6.21 *If* P *is a unary formula, which fulfills* (P*)*, then* $T \vdash C \to \mathrm{P}(\underline{\ulcorner C \urcorner})$ *for every extended* Σ_1*-sentence* C.

Proof:
Let $g \in \mathrm{PR}^1$ such that $\mathrm{Z} \vdash C \leftrightarrow \exists x.g(x) = 0$.
$\Sigma \vdash g(x) = 0 \to C$.
$\Sigma \vdash \mathrm{P}([g(x) = 0]) \to \mathrm{P}([C])$.
$\Sigma \vdash [g(x) = 0] = [g(x) = y][y := 0]$
$\Sigma \vdash g(x) = y \to \mathrm{P}([g(x) = y])$.
$\Sigma \vdash g(x) = 0 \to \mathrm{P}([g(x) = y][y := 0])$.
$\Sigma \vdash g(x) = 0 \to \mathrm{P}([g(x) = 0])$.
$\Sigma \vdash g(x) = 0 \to \mathrm{P}([C])$.
$\Sigma \vdash \exists x(g(x) = 0) \to \mathrm{P}([C])$.
$\Sigma \vdash C \to \mathrm{P}([C])$.

Lemma 6.22 *(a) If* P *is a unary extended* Σ_1*-sentence, which fulfills* (P*)*, then for all sentences* A, B *follow (D1), (D2), (D3).*

(b) Σ *fulfills (D1), (D2), (D3) with*
$\mathrm{P}(x) := \mathrm{Provable}_\Sigma(x) :=$
$\exists y.(\mathrm{Proof}_\Sigma(y, x) \wedge \widetilde{\Gamma}_{\widetilde{\mathrm{endseq}(b)}} = \underline{\ulcorner \emptyset \urcorner} \wedge \widetilde{\mathrm{A}}_{\widetilde{\mathrm{endseq}(b)}} = a)$.

Proof:
(a) Closed formulas are simple, so $\mathrm{Z} \vdash [A] = \underline{\ulcorner A \urcorner}$. (D1), (D2) follow directly from (P^*), and (D3) follows from 6.21 with $C :\equiv \mathrm{P}(\underline{\ulcorner A \urcorner})$.
(b) By Lemma 6.18 and (a) it suffices to show (P1) - (P3): (P1): If $\Sigma \vdash A$, then the (strict!) Σ_1-sentence $\mathrm{P}(\underline{\ulcorner A \urcorner})$ holds, therefore $\mathrm{Z}_1 \vdash \mathrm{P}(\underline{\ulcorner A \urcorner})$.
(P2): From a proof of $A \to B$ and a proof of A we get a proof of B by concatenating the two proofs and adding $\emptyset \Rightarrow B$, which follows from $(\to^-)$.
(P3) From a proof of A we get a proof of $A[x := \underline{y}]$ by using $\forall$-introduction and $\forall$-elimination. $\mathrm{FV}(\underline{y}) = \emptyset$, therefore $\underline{y}$ is substitutable for x in A. Formalization of this proof yields a proof of (P3).

Theorem 6.23 *Let* T *be a primitive recursive axiom system in a recursive presented language containing* $\mathcal{L}_{\mathrm{PR}}$*, which proves the equality axioms, induction for all* $\mathcal{L}(\Sigma)$ *formulas and all other axioms of* Z *and* P *the usual provability predicate.*

(a) **(Löb's theorem)**
$(T \vdash \mathrm{P}(\underline{\ulcorner A \urcorner}) \to A) \Rightarrow T \vdash A$.

(b) **(Gödel's second incompleteness theorem)**
If T *is consistent,* $T \nvdash \neg \mathrm{P}(\underline{\ulcorner \bot \urcorner})$.

6.4 Generalization of Gödel's 2^{nd} incompleteness theorem

Assumption 6.24 *(a) Let in this section $\mathcal{L}'$ be an arbitrary recursive represented language extending $\mathcal{L}_{\text{ar}}$. ($\mathcal{L}_{\text{PR}} \subseteq \mathcal{L}'$ is not required).*

(b) Let in this section Σ be a primitive recursive axiom system which proves the equality axioms in the language $\mathcal{L}'$. Let Provable_Σ *be defined as before.*

Definition 6.25 An interpretation of Z in Σ is a pair $(N, A \mapsto A^N)$, where N is a unary $\mathcal{L}'$-formula and $A \mapsto A^N$ is a function, which assigns to every PR-formula A a $\mathcal{L}'$-formula A^N such that

- $\bot^N \equiv \bot$.
- $(A\ s\ B)^N \equiv A^N\ s\ B^N$ $(s \in \{\wedge, \vee, \rightarrow\}$.
- $(\neg A)^N \equiv \neg(A^N)$.
- $(\overset{\forall}{\exists} xA)^N \equiv \overset{\forall}{\exists} x(N(x) \rightarrow A^N)$.
- $\text{FV}(A^N) = \text{FV}(A)$.
- $\text{Z} \vdash A \Rightarrow \Sigma \vdash A^*$, where, if $\text{FV}(A) = \{x_1, \ldots, x_n\}$, $A^* :\equiv N(x_1) \rightarrow \cdots \rightarrow N(x_n) \rightarrow A^N$.

Lemma 6.26 *If $(N, A \mapsto A^N)$ is an interpretation of* Z *in Σ, then for every* PR*-formula A follows*

$$\Sigma \vdash A^* \Rightarrow \Sigma \vdash (A[x := \underline{n}])^* \quad .$$

Proof:
For simplicity let $\text{FV}(A) = \{x, y\}$.
$\Sigma \vdash A^* \Rightarrow \Sigma \vdash N(y) \rightarrow N(x) \rightarrow A^N \Rightarrow \Sigma \vdash N(y) \rightarrow \forall x(N(x) \rightarrow A^N)$.
$\text{Z} \vdash \forall x(A) \rightarrow A[x := \underline{n}] \Rightarrow \Sigma \vdash (\forall x(A) \rightarrow A[x := \underline{n}])^* \Rightarrow \Sigma \vdash N(y) \rightarrow (\forall x(N(x) \rightarrow A^N) \rightarrow (A[x := \underline{n}])^N)$.
Therefore $\Sigma \vdash N(y) \rightarrow (A[x := \underline{n}])^N$, $\Sigma \vdash (A[x := \underline{n}])^*$.

Definition 6.27 An interpretation $(N, A \mapsto A^N)$ is strict, if there exists a function $g \in \text{PR}^1$ such that the following holds:

- $g(\ulcorner A \urcorner) = \ulcorner A^* \urcorner$ for every $\mathcal{L}_{\text{PR}}$-formula A,
- $g(n) = 0$, if n is not number of a $\mathcal{L}_{\text{PR}}$-formula,
- $\text{Z} \vdash g([A \rightarrow B]) = \langle \underline{\text{enum}(\rightarrow)}, g([A]), g([B]) \rangle$ for all simple $\mathcal{L}_{\text{PR}}$-formulas A, B,
- $\text{Z} \vdash \text{Provable}_\Sigma(g(z)) \rightarrow \text{Provable}_\Sigma(g(\text{Sub}(z, \underline{\ulcorner x \urcorner}, \nu(x))))$.

Theorem 6.28 *If Σ is a primitive recursive consistent axiom system and $(N, A \mapsto A^N)$ a strict interpretation of* Z *in Σ, then $\Sigma \nvdash (\mathrm{Cons}_\Sigma)^N$.*

Proof:
Let $T := \{A \mid A\mathcal{L}_{\mathrm{PR}}\text{-sentence and } \Sigma \vdash A^N\}$ and $\mathrm{P}(x) := \mathrm{Provable}_\Sigma(g(x))$.

$$((T \vdash A) \wedge A\ \mathcal{L}_{\mathrm{PR}}\text{-sentence } \Rightarrow \Sigma \vdash A^N) \tag{1}$$

Proof: By assumption there exist $A_1, \ldots, A_n \in T$ such that $\vdash A_1 \to \cdots \to A_n \to A$. Therefore $\mathrm{Z} \vdash A_1 \to \cdots \to A_n \to A$, $\Sigma \vdash (A_1 \to \cdots \to A_n \to A)^*$, $(A_1 \to \cdots \to A_n \to A)^* \equiv A_1^N \to \cdots \to A_n^N \to A^N$, $\Sigma \vdash A_1^N \to \cdots \to A_n^N \to A^N$ and $\Sigma \vdash A_i^N$ $(i = 1, \ldots, n)$, therefore $\Sigma \vdash A^N$.

$$T \text{ is consistent} \tag{2}$$

Proof: If $T \vdash \perp$, then $\Sigma \vdash \perp^N$, $\perp^N \equiv \perp$.

$$\mathrm{Z} \subseteq T \tag{3}$$

Proof: If $A \in \mathrm{Z}$, then $\Sigma \vdash A^N$, A is $\mathcal{L}_{\mathrm{PR}}$-sentence, $A \in T$.

$$\text{For } T \text{ and P hold (P1), (P2), (P3)} \tag{4}$$

Proof:
(P1): If A is an $\mathcal{L}_{\mathrm{PR}}$-formula, and $\forall A$ is the $\forall$-closure of A, then $T \vdash A \Rightarrow T \vdash \forall A \Rightarrow \Sigma \vdash (\forall A)^N \Rightarrow \Sigma \vdash A^* \Rightarrow \mathrm{Provable}_\Sigma(g(\underline{\ulcorner A \urcorner}))$ is a true extended Σ_1-sentence $\Rightarrow \mathrm{Z} \vdash \mathrm{Provable}_\Sigma(g(\underline{\ulcorner A \urcorner})) \Rightarrow T \vdash \mathrm{P}(\underline{\ulcorner A \urcorner})$.
(P2): Assume A, B are two simple $\mathcal{L}_{\mathrm{PR}}$-formulas.
Then

$$\mathrm{Z} \vdash \mathrm{Provable}_\Sigma(<\underline{\mathrm{enum}(\to)}, x, y>) \to \mathrm{Provable}_\Sigma(x) \to \mathrm{Provable}_\Sigma(y) \ .$$

Therefore

$$\mathrm{Z} \vdash \mathrm{Provable}_\Sigma(g([A \to B])) \to \mathrm{Provable}_\Sigma(g([A])) \to \mathrm{Provable}_\Sigma(g([B])) \ .$$

(P3) Last condition on "g is strict".
From Lemmata 6.18, 6.22 and Corollary 6.4 follows $T \nvdash \neg\mathrm{P}(\underline{\ulcorner \perp \urcorner})$. By Lemma 6.7 (a) follows $Z \vdash g(\underline{\ulcorner \perp \urcorner}) = \underline{\ulcorner \perp \urcorner}$ and therefore $T \nvdash \neg\mathrm{Provable}_\Sigma(\underline{\ulcorner \perp \urcorner})$. By Definition of T follows therefore $\Sigma \nvdash (\mathrm{Provable}_\Sigma(\underline{\ulcorner \perp \urcorner}))^N$.

Chapter 7

Set Theory

We will develop set theory in a minimal language. We can then show that several relations and functions can be defined by formulas. In order to make life easier we show, that if relations and functions can be done (in what sense will be made clear below) then we can add new function and relation symbols for the one defined by the formula and don't get any new theorems in the original language.

7.1 Adding new function and relation symbols

This section is very much based on [Men97], sect. 2.9.

Lemma 7.1 Let T be a set of formulas including the equality axioms, formulated in a language $\mathcal{L}$.

(a) Let $A^R(x_1, \ldots, x_n)$ be a formula in $\mathcal{L}$. Let $\mathcal{L}_R$ be the extension of $\mathcal{L}$ by one new n-ary relation symbol R and T_R the extension of T by adding the equality axioms for R and the axiom
(R^*) $\quad \forall y_1, \ldots, y_n.(A^R(y_1, \ldots, y_n) \leftrightarrow R(y_1, \ldots, y_n))$.
Then we have

  (i) T_R is a conservative extension of T, i.e. T_R proves the same $\mathcal{L}$-sentences as T.

  (ii) There exists a map $*$ from formulas in $\mathcal{L}_R$ into formulas of $\mathcal{L}$ such that
  - $(\psi \overset{\wedge}{\vee} \psi)^* \equiv \psi^* \overset{\wedge}{\vee} \psi^*$,
  - $(\overset{\forall}{\exists} x \psi)^* \equiv \overset{\forall}{\exists} x.(\psi^*)$,
  - $(\neg\psi)^* \equiv \neg(\psi^*)$
  - If $\mathrm{FV}(\psi) \subseteq \{x_1, \ldots, x_n\}$ then $T \vdash \forall x_1, \ldots, x_n.(\psi \leftrightarrow \psi^*)$.

(b) Let $A^f(x_1, \ldots, x_n, z)$ be a formula in $\mathcal{L}$, such that
$T \vdash \forall x_1, \ldots, x_n.\exists! z.A^f(x_1, \ldots, x_n, z)$. Let $\mathcal{L}_f$ be the extension of $\mathcal{L}$ by

one new n-ary relation symbol f and T_f the extension of T by adding the new equality axioms for f and the axiom

(f^*) $\quad \forall y_1, \ldots, y_n, z.A^f(y_1, \ldots, y_n, f(y_1, \ldots, y_n))$.

Then the same statement as for T_R can be proved for T_f mutatis mutandis.

Proof: (a) Let ψ^* be the result of replacing prime formulas $R(t_1, \ldots, t_n)$ in ψ by $A^R(t_1, \ldots, t_n)$. With this translation all axioms and rules of T_R translate immediately into axioms and rules of T.
(b) We show that T and T_f have the same models: To any model $\mathcal{M}$ of T exists a model $\mathcal{M}'$ of T_f with $\mathcal{M}' \restriction \mathcal{L} = \mathcal{M}$ and if $\mathcal{M}'$ is a model of T_f, then $\mathcal{M}' \restriction \mathcal{L}$ is a model of T:
The second statement is trivial, and if $\mathcal{M}$ is a model of T, let $\mathcal{M}'$ be the extension of $\mathcal{M}$ by defining $f^{\mathcal{M}'}(a_1, \ldots, a_n) := b$ for some b such that $b \in \mathcal{M}$ and $(\mathcal{M}, (x_1 \mapsto a_1, \ldots, x_n \mapsto a_n, y \mapsto b)) \models A(x_1, \ldots, x_n, y)$. Such a b exists and for any other b' we have $(b, b') \in =^{\mathcal{M}}$. One sees immediately that $=^{\mathcal{M}}$ is a congruence with respect to $f^{\mathcal{M}'}$ and $\mathcal{M}' \models (f^*)$, therefore $\mathcal{M}' \models T_f$.
Now (i) follows. For (ii), we replace in A first all prime formulas $R(t_1, \ldots, t_n)$ containing a t_i which is not a variable by $\forall x_1, \ldots, x_n(x_1 = t_1 \wedge \cdots \wedge x_n = t_n \to R(x_1, \ldots, x_n))$. Then replace prime formulas $s = t$ with s not a variable by $\forall x(x = s \to x = t)$. Finally we replace successively $x = g(t_1, \ldots, t_m)$ with one of the t_i not a variable by $\forall x_1, \ldots, x_m(x_1 = t_1 \wedge \cdots \wedge x_m = t_m \to x = g(x_1, \ldots, x_m))$. The resulting formula will be logically equivalent to the original formula and f occurs only in prime formulas of the form $x = f(x_1, \ldots, x_n)$. Now replace $x = f(x_1, \ldots, x_n)$ by $A(x_1, \ldots, x_n, x)$. The formula we get will be, by the assumption in T, in T equivalent to the original one.

7.2 The axioms of set theory

We will follow in this section very closely [Buc93b], section 7.
Set Theory is the main basis for mathematics. Most mathematical reasoning is carried out in set theory. However there are some problems ...
Sets Cantor: "Eine Menge ist eine Zusammenfassung von Objekten." (English: A set is a collection of objects).
However ...
Russell's paradox: Naïve set theory is inconsistent.
Let $a := \{x \mid x \notin x\}$. Case $a \in a$. Then $a \notin a$. Therefore in any case $a \notin a$. But then $a \in a$, contradiction.
Zermelo-Fraenkel-set theory ZF In order to avoid this inconsistency, restrict the introduction of new sets. The consistency of the resulting theory cannot be shown, but up to now no inconsistency has been found, therefore it seems very likely that the ZF is consistent.

We will first introduce abbreviations for classes, to make life easier.

Definition 7.2 (a) The language of *Zermelo-Fraenkel-Set Theory* (ZF) consists of one binary predicate symbol $\in$, written infix, and equality.

(b) A *class* is an expression $\{x \mid A\}$, where A is a formula and x a variable. In the following $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$, $\mathcal{F}$, $\mathcal{Q}$, $\mathcal{R}$ be classes.

(c) $a \in \{x \mid B\} := B[x := a]$ (where we assume that a can be substituted for x in A after some renaming of bounded variables.

(d) $\{x \in \mathcal{A} \mid B\} := \{x \mid x \in \mathcal{A} \wedge B\}$.

(e) We identify a set (i.e. a variable) a with the class $\{x \mid x \in a\}$. All the following abbreviations apply for classes as well (with exceptions in (f) and (i)).

(f) $\mathcal{A} = \mathcal{B} :\equiv \forall x(x \in \mathcal{A} \leftrightarrow x \in \mathcal{B})$. This definition holds as well with $\mathcal{A}$ or $\mathcal{B}$ replaced by sets, but not both (since $a = b$ is an atomic formula).

(g) $\forall x \in \mathcal{A}.B := \forall x(x \in \mathcal{A} \to B)$. $\exists x \in \mathcal{A}.B := \exists x(x \in \mathcal{A} \wedge B)$.

(h) $\mathcal{A} \subseteq \mathcal{B} := \forall x \in \mathcal{A}.x \in \mathcal{B}$.

(i) $\mathcal{A} \in \mathcal{B} := \exists x \in \mathcal{B}.x = \mathcal{A}$. This abbreviation applies for $\mathcal{B}$ replaced by a set b, but not with $\mathcal{A}$ replaced by set a.

(j) $\emptyset := \{\} := \{x \mid x \neq x\}$.
$\{x_1, \dots, x_n\} := \{x \mid x = x_1 \vee \cdots x = x_n\}$ $(n \geq 0)$.

(k) $\bigcup \mathcal{A} := \{x \mid \exists y \in \mathcal{A}.x \in y\}$.
$\bigcap \mathcal{A} := \{x \mid \forall y \in \mathcal{A}.x \in y\}$.

(l) $\mathcal{A} \cup \mathcal{B} := \{x \mid x \in \mathcal{A} \vee x \in \mathcal{B}\}$.
$\mathcal{A} \cap \mathcal{B} := \{x \mid x \in \mathcal{A} \wedge x \in \mathcal{B}\}$.
$\mathcal{A} \setminus \mathcal{B} := \{x \mid x \in \mathcal{A} \wedge x \notin \mathcal{B}\}$.

(m) $\mathcal{P}(\mathcal{A}) := \{x \mid x \subseteq \mathcal{A}\}$.

(n) $\mathrm{V} := \{x \mid x = x\}$.

(o) In the following $a, b, c, d, e, f, g, h, x, y, z, w$ are sets i.e. elements of V.

Remark 7.3 *(a)* $\forall x(x \neq \emptyset \leftrightarrow \exists y.y \in x)$.

(b) $\mathcal{A} \in \mathrm{V} \leftrightarrow \exists x.x = \mathcal{A}$.

Proof:
(a): $x = \emptyset \Leftrightarrow (\forall y(y \in x \leftrightarrow y \neq y) \Leftrightarrow \neg\exists y.y \in x$.
(b): $\mathcal{A} \in \mathrm{V} \Leftrightarrow \exists x \in V.x = \mathcal{A} \Leftrightarrow \exists x(x = x \wedge x = \mathcal{A}) \Leftrightarrow \exists x.x = \mathcal{A}$.

Definition 7.4 The universal closure of a formula A is the formula $\forall x_1.\dots\forall x_n.A$ where $x_1, \dots, x_n$ are the free variables in A and distinct.

Definition 7.5 The **axioms** of ZF are the equality axioms and the universal closure of the following formulas following:

(Ext) $x = y \leftrightarrow \forall z(z \in x \leftrightarrow z \in y)$. (Extensionality)

(Fun) $x \neq \emptyset \rightarrow \exists y(y \in x \wedge \forall z \in x.z \notin y)$. (Foundation axiom)

(Pair) $\{x, y\} \in \mathrm{V}$.

(Union) $\bigcup x \in \mathrm{V}$.

(Pow) $\mathcal{P}(x) \in \mathrm{V}$.

(Rep) $(\forall x, y, z(A(x, y) \wedge A(x, z) \rightarrow y = z) \rightarrow \{y \mid \exists x \in u.A(x, y)\} \in \mathrm{V}$. (Replacement axiom).

(Inf) $\exists x.(\emptyset \in x \wedge \forall y \in x.(y \cup \{y\}) \in x)$.

Note that (Rep) is an axiom schema rather than a simple axiom.

The Extensionality formalizes, that sets are determined by their elements.
The foundation axioms expresses that sets are well-founded in the sense (which means essentially that there are no infinite sequences $a_1 \ni a_2 \ni a_3 \ni \cdots$: $\{a_1, a_2, \ldots,\}$ would contradict the axiom).
The meaning of the replacement axioms is that, if a formula defines a function f, then for every set a $f[a]$ is a set.
Infinity guarantees the existence of infinite sets, without it there exists a model in which all sets are finite (the set of hereditarily finite sets, i.e. the finite sets, such that all its elements, the elements of its elements, the elements of its elements of its elements, etc. are finite).

Remark 7.6 *If we add to* ZF *new defined relation- and function symbols as in 7.1, then adding to the new theory instances of* (*Rep*) *in the extended language yields a conservative extension. We will therefore in the following add these symbols freely without mentioning it.*

Proof: The instance of R with respect to a formula A is equivalent to the instance with respect to the formula A^*.

Convention 7.7 In the following all formulas will be provable in ZF.

Remark 7.8 *(a) Every set a is a class i.e. there exists a class $\mathcal{A}$ such that $a = \mathcal{A}$.*

(b) There exists a class $\mathcal{A}$ which is not a set, i.e. $\neg\exists x.x = \mathcal{A}$.

Proof: (a) $\mathcal{A} := \{x \mid x \in a\}$. (b): $\mathcal{A} := \{x \mid x \notin x\}$. If $a = \mathcal{A}$, then we get Russell's paradox ($a \in a \leftrightarrow a \notin a$), a contradiction.
We can extend the language of set theory by adding relation symbols and function symbols in the following sense:

Definition 7.9 Assume t is a term, which is not a variable, in an extension of ZF.
$\{t \mid y_1 \in \mathcal{A}_1, \dots, y_n \in \mathcal{A}_n, A(y_1, \dots, y_n)\} :=$
$\{x \mid \exists y_1 \in \mathcal{A}_1, \dots, y_n \in \mathcal{A}_n.(x = t \wedge A(y_1, \dots, y_n))\}$ (x a new variable).
$\{t \mid y_1 \in \mathcal{A}_1, \dots, y_n \in \mathcal{A}_n\} := \{t \mid y_1 \in \mathcal{A}_1, \dots, y_n \in \mathcal{A}_n, \neg\perp\}$.

Lemma 7.10 *If t is some closed term in the extended language,* $\mathrm{FV}(t) \subseteq \{x_1, \dots, x_n\}$*. Then* $\forall y_1, \dots, y_n.\{t \mid x_1 \in y_1, \dots, x_n \in y_n\} \in \mathrm{V}$.

Proof: Induction on n. $n = 0$ $\{t \mid\} = \{t\} \in \mathrm{V}$.
$n \to n+1$. Let $A_{n+1}(x_{n+1}, u) := u = \{t \mid x_1 \in y_1, \dots, x_n \in y_n\}$. Then the premise of the replacement axiom is fulfilled, therefore $B := \{u \mid \exists x_{n+1} \in y_{n+1}.A_{n+1}(x_{n+1}, u)\}$ is a set. $\bigcup B = \{t \mid \exists x_1 \in y_1, \dots, x_{n+1} \in y_{n+1}\}$. ("$\subseteq$" is clear. "$\supset$": if $x_i \in y_i$, then by IH there exists u such that $A_{n+1}(x_{n+1}, u)$, and $t \in u \subseteq \bigcup B$).

Lemma 7.11 *(a)* $\mathrm{ZF} \vdash \forall x, y.x \cup y \in \mathrm{V}$.

(b) For every $n \in \mathbb{N}$ $n \geq 1$. $\mathrm{ZF} \vdash \forall x_1, \dots, x_n.\{x_1, \dots, x_n\} \in \mathrm{V}$.

(c) $\emptyset \in \mathrm{V}$.

Proof: (a) $z := \bigcup\{a, b\}$. (b) Induction on n. $n = 1$: $z := \{x_1, x_1\}$. $n \to n+1$: $z := \{x_1, \dots, x_n\} \cup \{x_{n+1}, x_{n+1}\}$.
(c) $\exists x.x = x$. (we have $\forall x.x = x$, therefore $x = x$, $\exists x.x = x$) Assume a, $a = a$. Let $A(x, y) :\equiv y \neq y$. The premise of the replacement axiom is fulfilled, therefore $\emptyset = \{y \mid \exists x \in a.y \neq y\}$ is a set.

Definition 7.12 $<a, b> := \{\{a\}, \{a, b\}\}$.

Lemma 7.13 $\forall x, x', y, y'(<x, y> = <x', y'> \to x = x' \wedge y = y')$.

Proof: Case $x = y$. Then $\{\{x\}\} = \{\{x'\}, \{x', y'\}\}$, $\{x\} = \{x'\} = \{x', y'\}$, $y = x = x' = y'$.
Case $x' = y'$. Similarly.
Otherwise $x \neq y$, $x' \neq y'$. $\{x, y\} \in \{\{x'\}, \{x', y'\}\}$, $\{x, y\} \neq \{x'\}$ (since $x \neq y$) therefore $\{x, y\} = \{x', y'\}$. Similarly $\{x\} = \{x'\}$, $x = x'$. $y' \neq y$, $y' \in \{x, y\}$, $y' = y$.

Definition 7.14 (a) $\mathcal{A} \times \mathcal{B} := \{<a, b> \mid a \in \mathcal{A}, b \in \mathcal{B}\}$.

(b) $\mathrm{Rel}_2(\mathcal{R}) := \mathcal{R} \subseteq V \times V$ (*$\mathcal{R}$ is a binary relation*). If $\mathcal{R}$ is a class term, $\mathcal{R}(x, y) := x \mathrel{\mathcal{R}} y := <x, y> \in \mathcal{R}$.

(c) $\mathrm{Fun}(F) := \mathrm{Rel}_2(\mathcal{F}) \wedge \forall x, y, z(<x, y> \in \mathcal{F} \wedge <x, z> \in \mathcal{F} \to y = z)$. (*$\mathcal{F}$ is a function*)

(d) $\mathrm{dom}(\mathcal{R}) := \{x \mid \exists y.\mathcal{R}(x, y)\}$ (the *domain of* $\mathcal{R}$)

(e) $\mathrm{rng}(\mathcal{R}) := \{y \mid \exists x.\mathcal{R}(x, y)\}$ (the *range of* $\mathcal{R}$).

(f) $\mathcal{R} \restriction \mathcal{A} := \mathcal{R} \cap (\mathcal{A} \times V)$ (the *restriction of* $\mathcal{R}$ *to* $\mathcal{A}$).

(g) $\mathcal{R}[\mathcal{A}] := \{y \mid \exists x \in \mathcal{A}.{<}x, y{>} \in \mathcal{R}\}$ (the *image of* $\mathcal{R}$ *under* $\mathcal{A}$).

(h) $\mathcal{Q} \circ \mathcal{R} := \{{<}x, z{>} \mid \exists y(\mathcal{R}(x, y) \wedge \mathcal{Q}(y, z))\}$. (Composition of relations).

(i) $\mathcal{R}^{-1} := \{{<}y, x{>} \mid \mathcal{R}(x, y)\}$ (the inverse of $\mathcal{R}$).

(j) $\mathcal{F}(x) := \bigcup\{y \mid {<}x, y{>} \in \mathcal{F}\}$ (which will be the application of a function to an element, if $\mathcal{F}$ is a function).

(k) $(\mathcal{F} : \mathcal{A} \to \mathcal{B}) := (\mathrm{Fun}(\mathcal{F}) \wedge \mathrm{dom}(\mathcal{F}) = \mathcal{A} \wedge \mathrm{rng}(\mathcal{F}) \subseteq \mathcal{B})$.

(l) $a^b := \{f \mid f : a \to b\}$.

(m) $\mathrm{injective}(\mathcal{F}) := \mathrm{Fun}(\mathcal{F}^{-1})$ ($\mathcal{F}$ *is injective*)

(n) $(\mathcal{F} : \mathcal{A} \rightarrowtail \mathcal{B}) := (\mathcal{F} : a \to \mathcal{B}) \wedge \mathrm{injective}(\mathcal{F})$. ($\mathcal{F}$ *is an injective function from* $\mathcal{A}$ *into* $\mathcal{B}$).

(o) $(\mathcal{F} : \mathcal{A} \twoheadrightarrow \mathcal{B}) := (\mathcal{F} : \mathcal{A} \to \mathcal{B}) \wedge \mathrm{rng}(\mathcal{F}) = \mathcal{B}$. ($\mathcal{F}$ *is a surjective function from* $\mathcal{A}$ *into* $\mathcal{B}$).

(p) $(\mathcal{F} : \mathcal{A} \xrightarrow{\cong} \mathcal{B}) := (\mathcal{F} : \mathcal{A} \rightarrowtail \mathcal{B}) \wedge (\mathcal{F} : \mathcal{A} \twoheadrightarrow \mathcal{B})$. ($\mathcal{F}$ *is an bijective function from* $\mathcal{A}$ *into* $\mathcal{B}$).

Lemma 7.15 *Assume* $\mathrm{Fun}(\mathcal{F})$, $\mathrm{Fun}(\mathcal{G})$, $\mathcal{A} \subseteq \mathrm{dom}(\mathcal{F}) \cap \mathrm{dom}(\mathcal{G})$.

(a) $\forall x \in \mathrm{dom}(\mathcal{F})(\mathcal{F}(x) \in \mathrm{V} \wedge {<}x, \mathcal{F}(x){>} \in \mathcal{F} \wedge \forall y({<}x, y{>} \in \mathcal{F} \leftrightarrow y = \mathcal{F}(x)))$.

(b) $\mathrm{Fun}(\mathcal{F} \restriction \mathcal{A}) \wedge \mathrm{dom}(\mathcal{F} \restriction \mathcal{A}) = \mathcal{A} \wedge \mathrm{rng}(\mathcal{F} \restriction \mathcal{A}) = \mathcal{F}[\mathcal{A}] \wedge \forall x \in \mathcal{A}(\mathcal{F}(x) = (\mathcal{F} \restriction \mathcal{A})(x))$.

(c) $\mathrm{rng}(\mathcal{F}) = \mathcal{F}[\mathrm{dom}(\mathcal{F})] \wedge \mathcal{F} = \mathcal{F} \restriction \mathrm{dom}(\mathcal{F})$.

(d) $(\forall x \in \mathcal{A}(\mathcal{F}(x) = \mathcal{G}(x)) \to \mathcal{F} \restriction \mathcal{A} = \mathcal{G} \restriction \mathcal{A})$.

(e) $\mathrm{dom}(\mathcal{F}) = \mathrm{dom}(\mathcal{G}) \wedge (\forall x \in \mathrm{dom}(\mathcal{F})(\mathcal{F}(x) = \mathcal{G}(x)) \to \mathcal{F} = \mathcal{G})$.

Proof: (a) Assume $x \in \mathrm{dom}(\mathcal{F})$. Then there exists z such that ${<}x, z{>} \in \mathcal{F}$. Assume $u \in \mathcal{F}(x)$. Then $u \in z'$ for some z' such that ${<}x, z'{>} \in \mathcal{F}$. $z' = z$. $u \in z$. Assume $u \in z$. Then $u \in \mathcal{F}(x)$. Therefore $\mathcal{F}(x) = z \in \mathrm{V}$, ${<}x, \mathcal{F}(x){>} \in \mathcal{F}$, ${<}x, y{>} \in \mathcal{F} \Leftrightarrow y = z = \mathcal{F}(x)$.

Lemma 7.16 *(Some conclusions from (Rep)*

(a) $\mathrm{Fun}(\mathcal{F}) \to \mathcal{F}[a] \in \mathrm{V}$.

(b) For every formula $A(x)$ $\{x \in a \mid A(x)\} \in \mathrm{V}$. *(*Principle of separation*).*
$\forall x(\mathcal{A} \cap x \in \mathrm{V})$.
$\mathcal{A} \subseteq \mathcal{B} \wedge \mathcal{B} \in \mathrm{V} \to \mathcal{A} \in \mathrm{V}$.

(c) $\mathcal{A} \neq \emptyset \to \bigcap \mathcal{A} \in \mathrm{V}$.

Remark: (b) will be the main basis for proving that some newly introduced classes are sets. One just needs to find a suitable a, for which usually some applications of $\mathcal{P}$ suffice.
Proof of the lemma:
(a) Let $A(x,y) := <x,y> \in \mathcal{F}$. By (Rep)

$$\begin{array}{lcl} \mathcal{F}[a] & = & \{\mathcal{F}(x) \mid x \in a\} \\ & \overset{\text{Lemma 7.15 (a)}}{=} & \{y \mid \exists x \in a. <x,y> \in \mathcal{F}\} \\ & = & \{y \mid \exists x \in a. A(x,y)\} \\ & \overset{\text{(Rep)}}{\in} & \mathrm{V} \end{array}$$

(b) Let $\mathcal{F} := \{<x,x> \mid A(x)\}$. $\mathrm{Fun}(\mathcal{F})$, $\mathcal{F}[a] = \{x \in a \mid A(x)\} \in \mathrm{V}$. The other assertions follow immediately from this.
(c) Assume $\mathcal{A} \neq \emptyset$. Therefore $x \in \mathcal{A}$ for some x. $\forall y \in \bigcap \mathcal{A}. y \in x$. $\bigcap \mathcal{A} \subseteq x \in \mathrm{V}$. $\mathcal{A} \subseteq \mathrm{V}$.

Lemma 7.17 *(a)* $a \cup b$, $a \cap b$, $a \setminus b$, $a \times b$, b^a, $\mathrm{dom}(r)$, $\mathrm{rng}(r)$, $r(b)$, $r[b]$, $r \restriction a$, r^{-1}, $r \circ s \in \mathrm{V}$.

(b) $\mathrm{Rel}(\mathcal{R}) \wedge \mathrm{dom}(\mathcal{R}) \in \mathrm{V} \wedge \mathrm{rng}(\mathcal{R}) \in \mathrm{V} \to \mathcal{R} \in \mathrm{V}$.

(c) $\mathrm{Fun}(\mathcal{F}) \to \mathcal{F} \restriction x \in \mathrm{V}$.

(d) $\mathrm{Fun}(\mathcal{F}) \wedge \mathrm{dom}(\mathcal{F}) \in \mathrm{V} \to \mathcal{F} \in \mathrm{V}$.

Proof:
(a) $a \cup b = \bigcup\{a, b\}$.
$a \cap b, a \setminus b \subseteq a$.
If $x \in a$, $y \in b$, then $<x,y> = \{\{x\}, \{x,y\}\} \in \mathcal{P}(\mathcal{P}(a \cup b))$, $a \times b \subseteq \mathcal{P}(\mathcal{P}(a \cup b)) \in \mathrm{V}$.
$b^a \subseteq \mathcal{P}(a \times b) \in V$.
$<x,y> \in r \Rightarrow \{x,y\} \in \bigcup r \Rightarrow x, y \in \bigcup\bigcup r$, $\mathrm{dom}(r), \mathrm{rng}(r), r[a] \subseteq \bigcup\bigcup r \in \mathrm{V}$, $r(a) = \bigcup r[\{a\}] \in \mathrm{V}$.
$r \restriction a \subseteq r$, $r^{-1} \subseteq \mathrm{rng}(r) \times \mathrm{dom}(r)$, $r \circ s \subseteq \mathrm{dom}(s) \times \mathrm{rng}(r)$.
(b) $\mathcal{R} \subseteq \mathrm{dom}(\mathcal{R}) \times \mathrm{rng}(\mathcal{R})$.
(c) $\mathcal{F} \restriction a \subseteq a \times \mathcal{F}[a]$.
(d) $\mathcal{F} = \mathcal{F} \restriction \mathrm{dom}(\mathcal{F})$.

Chapter 8

Ordinals

We will follow in this section very closely [Buc93b], section 8. We will work in ZF.

Motivation:

There are two induction principals for the natural numbers:

(i) $A(0) \to \forall x \in \mathbb{N}(A(x) \to A(x+1)) \to \forall x \in \mathbb{N}.A(x)$

(ii) $\forall x \in \mathbb{N}(\forall y < x(y \in \mathbb{N} \to A(y)) \to A(x)) \to \forall x \in \mathbb{N}.A(x)$

The second principal can be applied to bigger orderings as well. Let $M := \mathbb{N} \cup \{\omega\}$, ω a new element, for $x, y \in M$, $x \prec y \Leftrightarrow (x, y \in \mathbb{N} \wedge x < y) \vee (x \in \mathbb{N} \wedge y = \omega)$. We can visualize this order as follows:

$$0 \quad 1 \quad 2 \quad 3 \quad \cdots \quad \omega$$

(ii) holds with $\mathbb{N}, <$ replaced by $M, \prec$:

Under the assumptions of (ii) we get first $\forall n \in \mathbb{N}.A(n)$, and since $x \prec \omega \Rightarrow x \in \mathbb{N} \Rightarrow A(x)$ follows $A(\omega)$.

We can take now bigger orderings like

$$0 \quad 1 \quad 2 \quad 3 \quad \cdots \quad \omega \quad (\omega+1) \quad (\omega+2) \quad (\omega+3) \quad \cdots$$

and again the above principal holds: We get $A(x)$ for $x \preceq \omega$, then for $\omega + 1$, $\omega + 2, \ldots$.

For the ordering

$$0 \quad 1 \quad 2 \quad \cdots \quad \omega \quad (\omega+1) \quad (\omega+2) \quad \cdots \quad (\omega+\omega) = \omega \cdot 2$$

it holds again.

This scale can be extended further.

We start now with the development of orderings in general for which the above principle holds.

8.1 Well-founded relations

Definition 8.1 (a) $\forall x\, \mathcal{R}\, a.A(x) := \forall x(x\, \mathcal{R}\, a \to A(x))$, similar for $\exists$.

(b) $\mathrm{Prog}_{\mathcal{R}}(\mathcal{A}) := \forall x(\forall y\, \mathcal{R}\, x(y \in \mathcal{A}) \to x \in \mathcal{A})$. ($\mathcal{A}$ is *progressive with respect to* $\mathcal{R}$).

(c) $\mathrm{TI}_{\mathcal{R}}(\mathcal{A}) := \mathrm{Prog}_{\mathcal{R}}(\mathcal{A}) \to \forall x.x \in \mathcal{A}$. (*transfinite induction over* $\mathcal{R}$ *for* $\mathcal{A}$).

Lemma 8.2 *Assume* $\mathrm{Rel}(\mathcal{R})$. *The following principles are equivalent (i.e. the set of formulas of (i) and (ii) are over* ZF *equivalent)*

(i) Existence of minimal elements: For every class $\mathcal{C}$

$$\mathcal{C} \neq \emptyset \to \exists x \in \mathcal{C}.x_{\mathcal{R}} \cap \mathcal{C} = \emptyset \ .$$

(Such an x *is called a* minimal element in $\mathcal{C}$ with respect to $\mathcal{R}$*).*

(ii) For every class $\mathcal{C}$ $\mathrm{TI}_{\mathcal{R}}(\mathcal{C})$*. (*Induction over $\mathcal{R}$*).*

Proof:
(i) with $\mathcal{C} := \mathrm{V} \setminus \mathcal{D}$ is equivalent to

$$\begin{aligned}
& (\mathrm{V} \setminus \mathcal{D}) \neq \emptyset \to \exists x \in (\mathrm{V} \setminus \mathcal{D}).\forall y\, \mathcal{R}\, x.y \notin (\mathrm{V} \setminus \mathcal{D}) \\
\Leftrightarrow\ & \exists x.x \notin \mathcal{D} \to \exists x(x \notin \mathcal{D} \wedge \forall y\, \mathcal{R}\, x.y \in \mathcal{D}) \\
\Leftrightarrow\ & \neg(\exists x(x \notin \mathcal{D} \wedge \forall y\, \mathcal{R}\, x.y \in \mathcal{D})) \to \neg\exists x.x \notin \mathcal{D} \\
\Leftrightarrow\ & \forall x.(\forall y\, \mathcal{R}\, x.y \in \mathcal{D} \to x \in \mathcal{D}) \to \forall x.x \in \mathcal{D} \\
\equiv\ & \mathrm{TI}_{\mathcal{R}}(\mathcal{D})
\end{aligned}$$

Definition 8.3 (a) $\mathrm{trans}(\mathcal{R}) := \forall x, y, z(x\ \mathcal{R}\ y \wedge y\ \mathcal{R}\ z \to x\ \mathcal{R}\ z)$. ($\mathcal{R}$ *is transitive*).

(b) $\mathrm{irreflexive}(\mathcal{R}) := \forall x.\neg(x\, \mathcal{R}\, x)$. ($\mathcal{R}$ is *irreflexive*).

(c) $x_{\mathcal{R}} := \{y \mid y\, \mathcal{R}\, x\}(= \mathcal{R}^{-1}[\{x\}])$.

(d) $\mathrm{Found}(\mathcal{R}) := \forall u(u \neq \emptyset \to \exists x \in u.x_{\mathcal{R}} \cap u = \emptyset)$. ($\mathcal{R}$ is *founded*).

(e) $\mathrm{WFound}(\mathcal{R}) := \mathrm{Found}(\mathcal{R}) \wedge \forall x.x_{\mathcal{R}} \in \mathrm{V}$ ($\mathcal{R}$ is *well-founded*).

Remark 8.4 *(a) If (i) (or (ii)) of Lemma 8.2 holds for* $\mathcal{R}$*, then* $\mathrm{Found}(\mathcal{R})$*.*

(b) $\mathrm{Found}(\mathcal{R}) \to \mathrm{irreflexive}(\mathcal{R})$.

(c) $x_{\in} = x$ *(where we identify* $\in$ *with the relation* $\{< y, x >\mid y \in x\}$*).*

Proof: (b): Assume x. $\{x\} \neq \emptyset$, exists y in $\{x\}$ such that $y_{\mathcal{R}} \cap \{x\} = \emptyset$, $x_{\mathcal{R}} \cap \{x\} = \emptyset$, $\neg x\, \mathcal{R}\, x$.

Lemma 8.5 *Assume* $\mathrm{trans}(\mathcal{R})$, $\mathrm{WFound}(\mathcal{R})$*. Then (i) and (ii) of Lemma 8.2 hold.*

Proof: We show (i). Assume $\mathcal{C} \neq \emptyset$, $u \in \mathcal{C}$.
Case 1: $u_{\mathcal{R}} \cap \mathcal{C} = \emptyset$. Assertion holds.
Case 2: $u_{\mathcal{R}} \cap \mathcal{C} \neq \emptyset$. $a := (u_{\mathcal{R}} \cap \mathcal{C}) \in V$, $a \neq \emptyset$. By assumption exists $c \in a$ such that $c_{\mathcal{R}} \cap a = \emptyset$. $c \in \mathcal{C}$. By $c \in u_{\mathcal{R}}$ and trans$(\mathcal{R})$ follows $c_{\mathcal{R}} \subseteq u_{\mathcal{R}}$. Therefore $c \in \mathcal{C}$ and $c_{\mathcal{R}} \cap \mathcal{C} = \emptyset$.

Notation 8.5a $\mathcal{F}(a_1, \dots, a_n) := \mathcal{F}(<a_1, \dots, a_n>)$, if $n \geq 2$.

Theorem 8.6 *(Recursion theorem of set theory) Assume* WFound$(\mathcal{R})$, trans$(\mathcal{R})$, $\mathcal{G} : \mathcal{A} \times \mathrm{V} \to \mathrm{V}$. *Then there exists a unique function* $\mathcal{F} : \mathcal{A} \to \mathrm{V}$ *such that* $\mathcal{F}(x) = \mathcal{G}(x, \mathcal{F} \restriction x_{\mathcal{R}})$ *for all* $x \in \mathcal{A}$*)*.

Proof:
We define approximations of the resulting function $\mathcal{F}$ as follows:

$$\begin{aligned} \mathrm{Approx}(f) \quad := \quad & \mathrm{Fun}(f) \wedge \mathrm{dom}(f) \subseteq \mathcal{A} \wedge \\ & \forall x \in \mathrm{dom}(f)(\mathcal{A} \cap x_{\mathcal{R}} \subseteq \mathrm{dom}(f) \wedge f(x) = \mathcal{G}(x, f \restriction x_{\mathcal{R}})) \ . \end{aligned}$$

$\mathcal{C} := \{f \mid \mathrm{Approx}(f)\}$, $\mathcal{F} := \bigcup \mathcal{C}$. We show that $\mathcal{F}$ fulfills the assertion of the theorem.

$$\mathrm{Approx}(f_1) \wedge \mathrm{Approx}(f_2) \wedge x \in \mathrm{dom}(f_1) \cap \mathrm{dom}(f_2) \to f_1(x) = f_2(x) \tag{1}$$

Proof by induction over R. Assume $x \in \mathrm{dom}(f_1) \cap \mathrm{dom}(f_2)$ and the assertion for $y \ \mathcal{R} \ x$. Then $\mathcal{A} \cap x_{\mathcal{R}} \subseteq \mathrm{dom}(f_1) \cap \mathrm{dom}(f_2)$, by IH $\forall y \in \mathcal{A} \cap x_{\mathcal{R}}(f_1(x) = f_2(y))$, i.e. $f_1 \restriction x_{\mathcal{R}} = f_2 \restriction x_{\mathcal{R}}$. By Approx$(f_1)$, Approx$(f_2)$ follows $f_1(x) = \mathcal{G}(x, f_1 \restriction x_{\mathcal{R}}) = \mathcal{G}(x, f_2 \restriction x_{\mathcal{R}}) = f_2(x)$.

$$\mathrm{Fun}(\mathcal{F}) \wedge \mathrm{dom}(\mathcal{F}) = \bigcup \{\mathrm{dom}(f) \mid \mathrm{Approx}(f)\} \wedge \forall f \in \mathcal{C}. f = \mathcal{F} \restriction \mathrm{dom}(f) \tag{2}$$

Proof: By (1).

$$\forall x \in \mathrm{dom}(\mathcal{F})(\mathcal{A} \cap x_{\mathcal{R}} \subseteq \mathrm{dom}(\mathcal{F}) \wedge \mathcal{F}(x) = \mathcal{G}(x, \mathcal{F}(x_{\mathcal{R}}))) \tag{3}$$

Proof: If $x \in \mathrm{dom}(\mathcal{F})$, then $x \in \mathrm{dom}(f)$ for some f such that Approx(f), $\mathcal{A} \cap x_{\mathcal{R}} \subseteq \mathrm{dom}(f) \subseteq \mathrm{dom}(\mathcal{F})$, by (2) $\mathcal{F}(x) = f(x) = \mathcal{G}(x, f \restriction x_{\mathcal{R}}) = \mathcal{G}(x, \mathcal{F} \restriction x_{\mathcal{R}})$.

$$\mathcal{A} = \mathrm{dom}(\mathcal{F}) \tag{4}$$

Proof: $\mathrm{dom}(\mathcal{F}) \subseteq \mathcal{A}$ is clear. We show $\mathcal{A} \subseteq \mathrm{dom}(\mathcal{F})$ by induction on $\mathcal{R}$. Assume $x \in \mathcal{A}$, $a := x_{\mathcal{R}} \cap \mathcal{A} \subseteq \mathrm{dom}(\mathcal{F})$ (IH). We show $x \in \mathrm{dom}(\mathcal{F})$.
Let $f := \mathcal{F} \restriction a \cup \{<x, \mathcal{G}(x, \mathcal{F} \restriction x_{\mathcal{R}})>\}$.
We show Approx(f).
Fun(f) since $x \notin a$ (otherwise $x \ \mathcal{R} \ x$, contradicting the well-foundedness of $\mathcal{R}$).
Let now $y \in \mathrm{dom}(f)$.

If $y \in a$, then, by the transitivity of $\mathcal{R}$, $\mathcal{A} \cap y_{\mathcal{R}} \subseteq a \subseteq \mathrm{dom}(f)$ and $f(y) = \mathcal{F}(y) = \mathcal{G}(y, \mathcal{F} \restriction y_{\mathcal{R}}) = \mathcal{G}(y, f \restriction y_{\mathcal{R}})$.
If $y = x$, then $\mathcal{A} \cap x_{\mathcal{R}} = a \subseteq \mathrm{dom}(f)$ and $f(x) = \mathcal{G}(x, \mathcal{F} \restriction x_{\mathcal{R}}) = \mathcal{G}(x, f \restriction x_{\mathcal{R}})$.
The uniqueness of $\mathcal{F}$ follows immediately by induction on $\mathcal{R}$.

Definition 8.7 (a) $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{A}$ is called a linear ordering on $\mathcal{A}$, iff the following holds:

- $\forall x.\neg(x \mathcal{R} x)$.
- $\forall x, y, z(x \mathcal{R} y \wedge y \mathcal{R} z \rightarrow x \mathcal{R} z)$.
- $\forall x, y(x \mathcal{R} y \vee x = y \vee y \mathcal{R} x)$.

(b) A linear ordering $\mathcal{R}$ on $\mathcal{A}$ is called *well-ordering on* $\mathcal{A}$, iff $\mathcal{R}$ is well-founded.

(c) $\mathcal{A}$ is called *well-ordered* (*linearly ordered*) *by* $\mathcal{R}$, if $\mathcal{R} \cap (\mathcal{A} \times \mathcal{A})$ is a well-ordering (linear ordering) on $\mathcal{A}$.

(d) If $A \in \mathrm{V}$ and $\mathcal{R}$ is a well-ordering on $\mathcal{A}$, we call the pair $(\mathcal{A}, \mathcal{R})$ a *well-ordered set* or *well-ordering*

Remark 8.8 *Assume $\mathcal{A}$ is well-ordered by $\mathcal{R}$.*

(a) Every non-empty class $\mathcal{C} \subseteq \mathcal{A}$ has a (uniquely determined) minimal element $\min_{\mathcal{R}}(\mathcal{C})$.

(b) Every subclass $\mathcal{B} \subseteq \mathcal{A}$ is well-ordered by $\mathcal{R}$ as well

Proof of (a): Let $\mathcal{Q} := \mathcal{R} \cap (\mathcal{A} \times \mathcal{A})$. By Lemma 8.2 there exists $a \in \mathcal{C}$ such that $\mathcal{C} \cap a_{\mathcal{Q}} = \emptyset$. $\forall y \in \mathcal{C}(\neg(y \mathcal{R} a))$, $\forall y \in \mathcal{C}(y = a \vee a \mathcal{R} y)$, $a = \min_{\mathcal{R}}(\mathcal{C})$.
Uniqueness: If a, b are minima, then $a \mathcal{R} b \mathcal{R} a$, by well-foundedness of $\mathcal{R}$ $a = b$.

8.2 The class of Ordinals

Definition 8.9 (a) A class $\mathcal{A}$ is called *transitive*, if $\forall x \in \mathcal{A}.x \subseteq \mathcal{A}$.

(b) An *ordinal* is a transitive set, the elements of which are transitive as well.

(c) $\mathrm{Ord} := \{x \mid x \text{ is Ordinal}\}$.

(d) In the following $\alpha, \beta, \gamma, \delta, \rho, \xi, \eta, \zeta$ denote ordinals.
Therefore $\overset{\forall}{\exists} \alpha.A$ stands for $\overset{\forall}{\exists} \alpha \in \mathrm{Ord}.A$. $\alpha < \beta :\equiv \alpha \in \beta$, $\alpha \leq \beta :\equiv \alpha < \beta \vee \alpha = \beta$.

Lemma 8.10 *(a) If $\alpha \in \mathrm{Ord}$, $x \in \alpha$, then $x \in \mathrm{Ord}$.*

(b) $\in \cap(\mathrm{Ord} \times \mathrm{Ord})$ is transitive, well-founded and fulfills therefore (i) and (ii) of Lemma 8.4.

(c) $\in \cap(\text{Ord} \times \text{Ord})$ *is a linear order on* Ord.
(Especially by (a) Ord *is well-ordered by* $\in$*).*

(d) $\alpha \leq \beta \leftrightarrow \alpha \subseteq \beta$.

(e) $\text{Ord} \notin \text{V}$.

Proof:
(a): x is transitive. If $y \in x$, then $y \in x \in \alpha$, $y \in \alpha$, y is transitive. Therefore $x \in \text{Ord}$.
(b) $\mathcal{R} :=\in \cap(\text{Ord} \times \text{Ord})$. trans($\mathcal{R}$) (since $x \mathrel{\mathcal{R}} y \mathrel{\mathcal{R}} z$, then $x \in y \in z \in \text{Ord}$, $x \in z \in \text{Ord}$, $x \mathrel{\mathcal{R}} z$.
WFound($\mathcal{R}$): $y_{\mathcal{R}} = \emptyset$, if $y \notin \text{Ord}$, $y_{\mathcal{R}} = y$ otherwise, $y_{\mathcal{R}} \in \text{Ord}$. Further if $u \neq \emptyset$, then $v \in u$ s.t. $v \cap u = \emptyset$, $v_{\mathcal{R}} \cap u \subseteq v \cap u = \emptyset$. By Lemma 8.5 follow (i), (ii).
(c) $\alpha \notin \alpha$ by the foundation axiom (otherwise $\{\alpha\}$ contradicts it). $\in$ is transitive on Ord.
Proof of linearity: We show $\forall\alpha,\beta(\alpha < \beta \vee \alpha = \beta \vee \beta < \alpha)$. Induction on α, so assume α, Assertion for all $\alpha' < \alpha$ and show $\forall\beta((\alpha < \beta \vee \alpha = \beta \vee \beta < \alpha)$.
Induction on β, so assume assertion for $\beta' < \beta$.
Case 1: $\exists\alpha' < \alpha(\beta < \alpha' \vee \beta = \alpha')$. Then $\beta < \alpha$.
Case 2: Otherwise. Then by IH for α, $\forall\alpha' < \alpha.\alpha' < \beta$, $\alpha \subseteq \beta$.
Case 2.1 $\alpha < \beta' \vee \alpha = \beta'$ for some $\beta' < \beta$. Then $\alpha < \beta$.
Case 2.2 Otherwise. Then $\forall\beta' < \beta.\beta' < \alpha$, $\beta \subseteq \alpha$. Together with $\alpha \subseteq \beta$ therefore $\alpha = \beta$.
(d) If $\alpha \in \beta$ by transitivity of $\in$ on Ord, $\alpha \subseteq \beta$. If $\alpha = \beta$, $\alpha \subseteq \beta$. Assume now $\alpha \subseteq \beta$ and $\neg(\alpha \leq \beta)$. By the linearity of $\in$ follows then $\beta \in \alpha \subseteq \beta$, contradicting the foundation axiom.
(e) Ord is transitive and $\forall x \in \text{Ord}.\text{trans}(x)$. If $\text{Ord} \in \text{V}$, then $\text{Ord} \in \text{Ord}$, a contradiction.

Corollary 8.11 *(a) Every non empty class of ordinals has (exactly) on least element* $\min(\mathcal{C})$.

(b) $\forall\alpha(\forall\xi < \alpha(A(\xi)) \rightarrow A(\alpha)) \rightarrow \forall\alpha A(\alpha)$.

(c) For every $\mathcal{G} : \text{V} \rightarrow \text{V}$ *there exists a unique function* $\mathcal{F} : \text{Ord} \rightarrow \text{V}$ *such that* $\mathcal{F}(\alpha) = \mathcal{G}(\mathcal{F} \restriction \alpha)$ *for all* $\alpha \in \text{V}$.

Proof:
(b): Use principle (ii) with $\mathcal{C} := \{\alpha \in \text{Ord} \mid A(\alpha)\} \cup (\text{V} \setminus \text{Ord})$.
(c): Recursion theorem.

Lemma 8.12 *(a) If* $\mathcal{A} \subseteq \text{Ord}$ *is transitive, then* $\mathcal{A} \in \text{V} \Rightarrow \mathcal{A} \in \text{Ord}$ *and* $\mathcal{A} \notin \text{V} \rightarrow \mathcal{A} = \text{Ord}$.

(b) If $\mathcal{A} \subseteq \text{Ord}$ *is non empty, then* $\bigcap \mathcal{A} = \min(\mathcal{A})$, *i.e.* $c := \bigcap \mathcal{A} \in \mathcal{A} \wedge \forall\beta \in \mathcal{A}.c \leq \beta$

(c) *If* $a \in \mathrm{V}$, $a \subseteq \mathrm{Ord}$, *then* $\bigcup a \in \mathrm{Ord}$ *and* $\bigcup a = \sup(a)(:= \min\{\alpha \in \mathrm{Ord} \mid \forall \beta \in a.\beta \leq \alpha\})$.

(d) *For every class* $\mathcal{A} \subseteq \mathrm{Ord}$ *we have* $\mathcal{A} \in \mathrm{V} \leftrightarrow \exists \alpha \in \mathrm{Ord}.\forall \beta \in \mathcal{A}.\beta \leq \alpha$.

Proof:
(a) If $\mathcal{A} \subseteq \mathrm{Ord}$ is transitive, then $\mathcal{A}$ is transitive and its elements are transitive, so $\mathcal{A} \in \mathrm{V} \to \mathcal{A} \in \mathrm{Ord}$. If $\mathcal{A} \notin \mathrm{V}$, then $\alpha \in \mathrm{Ord} \to \mathcal{A} \not\subseteq \alpha \Rightarrow \exists \beta \in \mathcal{A}.\beta \notin \alpha \Rightarrow \exists \beta \in \mathcal{A}.\alpha \leq \beta \to \alpha \in \mathcal{A}$, $\mathcal{A} \subseteq \mathrm{Ord} \subseteq \mathcal{A}$.
(b) Let $\alpha := \min(\mathcal{A})$. then $\forall \beta \in \mathcal{A}.\alpha \subseteq \beta$, $\alpha \in \mathcal{A}$. Therefore $\alpha \subseteq \bigcap \mathcal{A} \subseteq \alpha$.
(c) Let $a \subseteq \mathrm{Ord} \wedge a \in \mathrm{V}$. One easily verifies $\bigcup a$ is a transitive set of ordinals. Therefore by (a) $\bigcup a \in \mathrm{Ord}$. Further, for all $\alpha \in \mathrm{Ord}$ we have $\bigcup a \leq \alpha \leftrightarrow \forall \beta \in a.\beta \leq \alpha$, i.e. $\bigcup a = \min\{\alpha \in \mathrm{Ord} \mid \forall \beta \in a.\beta \leq \alpha\}$.
(d): "$\to$": By $\mathcal{A} \in \mathrm{V}$ follows $\bigcup \mathcal{A} \in \mathrm{Ord}$, and $\forall \alpha \in \mathcal{A}.\alpha \leq \bigcup \mathcal{A}\}$.
"$\leftarrow$" From $\forall \beta \in \mathcal{A}.\beta \leq \alpha$ follows $\mathcal{A} \subseteq \alpha \cup \{\alpha\}$, $\mathcal{A} \in \mathrm{V}$.

Definition 8.13 Let $\mathcal{R}$ be a well-ordering on $\mathcal{A}$. An order function on $(\mathcal{A}, \mathcal{R})$ is a function $\mathcal{F}$ such that

- $\mathrm{dom}(\mathcal{F}) = \mathrm{Ord}$ or $\mathrm{dom}(\mathcal{F}) \in \mathrm{Ord}$.
- $\mathrm{rng}(\mathcal{F}) = \mathcal{A}$.
- $\forall \alpha, \beta \in \mathrm{dom}(\mathcal{F})(\beta < \alpha \to \mathcal{F}(\beta)\ \mathcal{R}\ \mathcal{F}(\alpha))$.

Theorem 8.14 *If* $\mathcal{R}$ *is a well-ordering on* $\mathcal{A}$, *then there exists exactly one order function* $\mathcal{F}$ *on* $(\mathcal{A}, \mathcal{R})$. *And we have* $\mathcal{F}(\alpha) = \min_{\mathcal{R}}\{x \in \mathcal{A} \mid \mathcal{F}[\alpha] \subseteq x_{\mathcal{R}}\}$ *for all* $\alpha \in \mathrm{dom}(\mathcal{F})$.
We call $\mathrm{dom}(\mathcal{F})$ *the* order type *of* $(\mathcal{A}, \mathcal{R})$.
Further we have $\mathcal{A} \in \mathrm{V} \to \mathrm{dom}(\mathcal{F}) \in \mathrm{Ord}$ *and* $\mathcal{A} \notin \mathrm{V} \to \mathrm{dom}(\mathcal{F}) = \mathrm{Ord}$.

Proof:
Uniqueness: Let $\mathcal{F}$ be an order function on $(\mathcal{A}, \mathcal{R})$. By transfinite induction on α we show: $\alpha \in \mathrm{dom}(\mathcal{F}) \to \mathcal{F}(\alpha) = \min_{\mathcal{R}}\{x \in A \mid \mathcal{F}[\alpha] \subseteq x_{\mathcal{R}}\}$. Then the uniqueness of $\mathcal{F}$ follows by the recursion theorem of set theory.
So assume $\alpha \in \mathrm{dom}(\mathcal{F})$. If $\beta \in \alpha$ then $\mathcal{F}(\beta)\ \mathcal{R}\ \mathcal{F}(\alpha)$, so $\mathcal{F}[\alpha] \subseteq \mathcal{F}(\alpha)_{\mathcal{R}}$. Let now $x \in \mathcal{A}$ such that $\mathcal{F}[\alpha] \subseteq x_{\mathcal{R}}$. By $\mathrm{rng}(\mathcal{F}) = \mathcal{A}$ there exists $\beta \in \mathrm{dom}(\mathcal{F})$ such that $\mathcal{F}(\beta) = x$. Then $\forall \xi \in \alpha.\xi < \beta$, $\alpha \leq \beta$, $\mathcal{F}(\alpha) \leq \mathcal{F}(\beta) = x$.
Existence: Define (using the recursion theorem of set theory) $\mathcal{F}_1 : \mathrm{Ord} \to \mathrm{V}$,

$$\mathcal{F}_1(\alpha) = \begin{cases} \min_{\mathcal{R}}\{x \in \mathcal{A} \mid \mathcal{F}_1[\alpha] \subseteq x_{\mathcal{R}}\} & \text{if } \exists x \in \mathcal{A}.\mathcal{F}_1[\alpha] \subseteq x_{\mathcal{R}} \\ 0 & \text{otherwise.} \end{cases}.$$

$\mathcal{D} := \{\alpha \in \mathrm{Ord}.\mathcal{F}_1[\alpha] \subseteq x_{\mathcal{R}}\}$ is obviously a transitive class of ordinals, therefore $\mathcal{D} \in \mathrm{Ord} \vee \mathcal{D} = \mathrm{Ord}$.
We show: $\mathcal{F} := \mathcal{F}_1 \restriction \mathcal{D}$ is an order function on $(\mathcal{A}, \mathcal{R})$.
Obviously $\mathrm{dom}(\mathcal{F}) = \mathcal{D}$, $\mathrm{rng}(\mathcal{F}) \subseteq \mathcal{A}$ and $\forall \alpha, \beta \in \mathcal{D}(\beta < \alpha \to \mathcal{F}(\beta)\ \mathcal{R}\ \mathcal{F}(\alpha))$.
We have to show: $x \in \mathcal{A} \to x \in \mathrm{rng}(\mathcal{F})$.
Proof by $\mathcal{R}$-induction: If $x \in \mathcal{A}$, then by IH $x_{\mathcal{R}} \subseteq \mathrm{rng}(\mathcal{F})$. $\mathcal{F}^{-1}[x_{\mathcal{R}}]$ is transitive. Since $\mathcal{F}$ is injective, follows $\mathcal{F}^{-1}[x_{\mathcal{R}}] \in \mathrm{V}$. Therefore $\alpha := \mathcal{F}^{-1}[x_{\mathcal{R}}] \in \mathrm{Ord}$. By

$x_{\mathcal{R}} \subseteq \operatorname{rng}(\mathcal{F})$ follows $\mathcal{F}[\alpha] = x_{\mathcal{R}}$. Further $\forall y \in \mathcal{A}(y \mathrel{\mathcal{R}} x \to \mathcal{F}[\alpha] \not\subseteq y_{\mathcal{R}})$, $\mathcal{F}(\alpha) = x$.

Corollary 8.15 *If $\mathcal{A}$ is a genuine class ($\mathcal{A} \notin \mathrm{V}$), and $\mathcal{R}$ a well-ordering on $\mathcal{A}$, then there exists a unique bijection $\mathcal{F} : \mathrm{Ord} \to \mathcal{A}$ such that $\forall \alpha, \beta.(\beta < \alpha \leftrightarrow \mathcal{F}(\beta) \mathrel{\mathcal{R}} \mathcal{F}(\alpha))$.*

Definition 8.16 (a) $0 := \emptyset$.
$S(x) := x \cup \{x\}$.

(b) $\omega := \bigcap\{u \mid 0 \in u \wedge \forall x \in u.\mathrm{S}(x) \in u\}$.

(c) α is called a *successor ordinal* iff $\exists \beta.\alpha = \mathrm{S}(\beta)$.
α is called a *limit ordinal*, if $\alpha \neq 0$ and α is not a successor ordinal.
Lim is the class of all limit ordinals.

Theorem 8.17 *(a) 0 is the least ordinal and $\forall \alpha.\mathrm{S}(\alpha) = \min\{\beta \in \mathrm{Ord}.\alpha < \beta\}$, $\mathrm{S}(\alpha) \in \mathrm{Ord}$.*

(b) $\alpha \in \mathrm{Lim} \leftrightarrow 0 < \alpha \wedge \forall \beta(\beta < \alpha \to \mathrm{S}(\beta) < \alpha)$.

(c) ω is the least limit ordinal.

(d) $0 \in \omega$, $\forall n \in \omega.\mathrm{S}(n) \in \omega$
For every class $\mathcal{C}$ follows $(0 \in \mathcal{C} \wedge \forall x \in \omega(x \in \mathcal{C} \to \mathrm{S}(x) \in \mathcal{C})) \to \forall x \in \omega.x \in \mathcal{C}$. (Therefore ω is the set of natural numbers).

(e) For every class $\mathcal{B}$, $a_0 \in \mathcal{B}$ and $\mathcal{G} : \omega \times \mathcal{B} \to \mathcal{B}$ there exists a unique function $\mathcal{F} : \omega \to \mathcal{B}$ such that $\mathcal{F}(0) = a_0$ and $\mathcal{F}(\mathrm{S}(x)) = \mathcal{G}(x, \mathcal{F}(x))$.

Proof:
By the infinity axiom follows that $\mathcal{J} := \{u \mid 0 \in u \wedge \forall x \in u.\mathrm{S}(x) \in u\}$ is not empty. Therefore:
$\omega = \bigcup J \in \mathrm{V} \wedge 0 \in \omega \wedge \forall x \in \omega.\mathrm{S}(x) \in \omega$.
(a): $0 \in \mathrm{V}$, and obviously $0 \in \mathrm{V}$. Further, if $\alpha \in \mathrm{V}$, then $\alpha \notin 0$, $0 \leq \alpha$, 0 is the least ordinal.
$\mathrm{S}(\alpha) \in \mathrm{Ord}$: Every element of $\mathrm{S}(\alpha)$ is an ordinal, therefore transitive. If $x \in y \in \mathrm{S}(\alpha)$, then $x \in y \in \alpha$, $x \in \alpha \subseteq \mathrm{S}(\alpha)$ or $x \in y = \alpha$, $x \in \mathrm{S}(\alpha)$, $\mathrm{S}(\alpha)$ is transitive. $\mathrm{S}(\alpha) \in \mathrm{V}$, therefore $\mathrm{S}(\alpha) \in \mathrm{Ord}$.
Further, if $\alpha < \beta$, then $\beta \neq \alpha$, $\neg(\beta < \alpha)$, $\mathrm{S}(\alpha) \subseteq \beta$. $\alpha < \mathrm{S}(\alpha)$, therefore $\mathrm{S}(\alpha) = \min\{\gamma \mid \alpha < \gamma\}$.
(b): Follows by $\forall \beta(\beta < \alpha \leftrightarrow \mathrm{S}(\beta) < \alpha)$.
(c): Let $a := \{\beta \in \omega \mid \beta \in \mathrm{Ord} \wedge \beta \subseteq \omega\}$. $0 \in a$ and if $\beta \in a$, then $\mathrm{S}(\beta) \in \omega$, $\mathrm{S}(\beta) \in \mathrm{Ord}$ and $S(\beta) \subseteq \omega$, therefore $\mathrm{S}(\beta) \in a$. Therefore $\omega \subseteq a$, ω is a transitive set of ordinals and therefore an ordinal.
$\omega \neq 0$, and if $\beta \in \omega$, then $\mathrm{S}(\beta) \in \omega$, therefore $\omega \in \mathrm{Lim}$. If $\beta < \omega$, $\beta \in \mathrm{Lim}$, then $0 \in \beta \wedge \forall \gamma \in \beta.\mathrm{S}(\gamma) \in \beta$, $\omega \subseteq \gamma \in \omega$, a contradiction. Therefore $\gamma \in \mathrm{Lim} \to \omega \leq \gamma$.
(d): Let $d := \omega \cap \mathcal{C}$. Then $d \in J$, $\omega \subseteq d \subseteq \mathcal{C}$.

(e) Define $\mathcal{G}_1 : \omega \times \mathrm{V} \to \mathrm{V}$,

$$\begin{array}{rcl}\mathcal{G}_1(x,f) & := & \mathrm{if}(x = 0 \vee \neg\mathrm{Fun}(f) \vee \bigcup x \notin \mathrm{dom}(f)) \text{ then } a_0 \\ & & \text{else } \mathcal{G}(\bigcup x, (f(\bigcup x))) \ ,\end{array}$$

i.e.

$$\mathcal{G}_1(x,f) = \{<x,z> \mid (\phi(x,f) \wedge z = a_0) \vee (\neg(\phi(x,f)) \wedge z = \mathcal{G}(\bigcup x, f(\bigcup x)))\} \ ,$$

where $\phi(x,f)$ is the condition in the if then else-clause.
There exists a unique function $\mathcal{F} : \omega \to \mathrm{V}$ such that $\forall x \in \omega.\mathcal{F}(x) = \mathcal{G}_1(x, \mathcal{F} \restriction x)$.
It follows $\mathcal{F}(0) = a_0$ and
$\mathcal{F}(\mathrm{S}(x)) = \mathcal{G}_1(\mathrm{S}(x), \mathcal{F} \restriction \mathrm{S}(x)) = \mathcal{G}(\bigcup \mathrm{S}(x), (\mathcal{F} \restriction \mathrm{S}(x))(\bigcup \mathrm{S}(x))) = \mathcal{G}(x, \mathcal{F}(x))$
for all $x \in \omega$.

Remark (e) can be extended to the case where we have additional parameters $x_1, \dots, x_n$ (i.e. if $\mathcal{G} : (\mathcal{A}_1 \times \cdots \times \mathcal{A}_n \times \omega) \to \mathcal{B}$, $\mathcal{H} : (\mathcal{A}_1 \times \cdots \times \mathcal{A}_n \times \omega \times \mathcal{B}) \to \mathcal{B}$, then there exists a unique $\mathcal{F} : (\mathcal{A}_1 \times \cdots \times \mathcal{A}_n \times \omega \to \mathcal{B}$ such that for all $a_1, \dots, a_n$ and $x \in \mathbb{N}$ $\mathcal{F}(a_1, \dots, a_n, 0) = \mathcal{G}(a_1, \dots, a_n)$, $\mathcal{F}(a_1, \dots, a_n, \mathrm{S}(x)) = \mathcal{H}(a_1, \dots, a_n, x, \mathcal{F}(a_1, \dots, a_n, x))$.)
This follows since first for every $a_1, \dots, a_n$ we can define $\mathcal{F}'_{a_0,\dots,a_n} : \omega \to \mathcal{A}$ such that $\mathcal{F}'_{a_1,\dots,a_n}(0) = \mathcal{G}(a_1, \dots, a_n)$ and $\mathcal{F}'_{a_1,\dots,a_n}(\mathrm{S}(x)) =$
$\mathcal{H}(a_1, \dots, a_n, x, \mathcal{F}'_{a_1,\dots,a_n}(x))$. This can be done explicitly, i.e. we can define $\mathcal{F}'_{a_1,\dots,a_n}$ as a class term depending on parameters $a_1, \dots, a_n$. Now define $\mathcal{F} :=$ $\{<<a_1, \dots, a_n, x>, y> \mid y = \mathcal{F}'_{a_1,\dots,a_n}(x)\}$.

8.3 The Axiom of Choice

Definition 8.18 (a) f is a *selection function for a* iff $\mathrm{Fun}(f) \wedge \forall x \in a(x \neq \emptyset \to x \in \mathrm{dom}(f) \wedge f(x) \in x)$. ($f$ selects out of every nonempty element of x an element).

(b) A relation $\mathcal{R}$ is called *partial order* iff $\mathcal{R}$ is irreflexive and transitive.

(c) A set K is called $\mathcal{R}$-chain, iff $\forall x, y \in K(x \mathrel{\mathcal{R}} y \vee x = y \vee y \mathrel{\mathcal{R}} x)$.

Theorem 8.19 *The following assertions are equivalent*

(AC) $\forall x.\exists f.(f$ *is selection function for* $x)$ *(*Axiom of Choice.

(WO) $\forall a.\exists r.(r$ *is well-ordering on* $a)$. *(*Well-ordering theorem*)*

(ZL) *For every non-empty partial ordered set* (a, r) *we have: If every* r*-chain* $K \subseteq a$ *has an upper bound in* a *(i.e.* $\forall x \in K(x\mathcal{R}b \vee x = b)$ *for some* $b \in K$*), then* a *has a maximum element (i.e.* $\exists p \in a.\neg\exists x \in a(p \ r \ x)$*). (*Zorn's Lemma*)*

Proof:
(AC) $\Rightarrow$ (ZL): Let (a, r) be a non-empty, partial ordered set such that every r-chain $K \subseteq a$ has an upper bound in a. By (AC) there exists a function $\mathcal{G} : \mathrm{V} \to \mathrm{V}$ such that $\forall x \in \mathcal{P}(a)(x \neq \emptyset \to \mathcal{G}(x) \in x)$.By transfinite induction we define $\mathcal{F} : \mathrm{Ord} \to \mathrm{V}$, $\mathcal{F}(\xi) := \mathcal{G}(\{x \in a \mid \mathcal{F}[\xi] \subseteq x_r\})$ for all $\xi \in \mathrm{Ord}$. (note $x_r = \{y \mid y\ r\ x\}$).
Let $\mathcal{D} := \{\xi \mid \{x \in a \mid \mathcal{F}[\xi] \subseteq x_r\} \neq \emptyset\}$.
Then we have obviously:
(1) $\mathcal{D}$ is transitive.
(2) $\mathcal{F}[\mathcal{D}] \subseteq a$.
(3) $\forall \eta, \xi \in \mathcal{D}(\eta < \xi \to \mathcal{F}(\eta) R \mathcal{F}(\xi))$.
By (2) and (3) $\mathcal{F}[\mathcal{D}] \in \mathrm{V}$, $\mathcal{F} \restriction \mathcal{D}$ is injective, therefore $\mathcal{D} \in \mathrm{V}$. By (1) follows $\mathcal{D} \in \mathrm{Ord}$. By $\mathcal{D} \in \mathrm{Ord} \setminus \mathcal{D}$ follows $\{x \in a \mid \mathcal{F}[\mathcal{D}] \subseteq x_r\} = \emptyset$. By (3), $\mathcal{F}[\mathcal{D}]$ is an r-chain. Let $p \in a$ be an upper bound for $\mathcal{F}[\mathcal{D}]$. Since r is transitive, $\neg \exists x \in a.p\ r\ x$.
(ZL) $\Rightarrow$ (WO): Let $c := \{s \subseteq a \times a \mid s$ is a well-ordering on some $b \subseteq a\}$.
Let for s arbitrary $\mathrm{field}(s) := \{x \in \bigcup\bigcup s. \exists y \in \bigcup\bigcup s.(<x, y> \in s \vee <y, x> \in s)\}$.
Define $s \sqsubset s' \Leftrightarrow s \neq s' \wedge s \subseteq s' \wedge \forall x \in \mathrm{field}(s). \forall y \in \mathrm{field}(s') \setminus \mathrm{field}(s). <y, x> \in s'$.
$\sqsubset$ is obviously a partial order on c.
Let $K \subseteq c$ be a $\sqsubset$-chain. We show $r := \bigcup K \in c$.
Since $\sqsubset$ is partial and K is a chain, $\sqsubset$ is linear on K. Therefore for $x, y, z \in \mathrm{field}(r)$ there exists $s \in c$ such that $x, y, z \in \mathrm{field}(s)$, and if $x\ s'\ y$ for some $s' \in c$, then $x\ s\ y$. One concludes easily now r is linear.
Further if a is a non-empty set, $b \in a$, then if $b_r \cap a \neq \emptyset$, $c \in b_r \cap a$, $c \in \mathrm{field}(s)$ for $s \in c$, $d \in c_s \cap a$ such that $d_s \cap a = \emptyset$, then $d_r \cap a = \emptyset$ (since if $u \in d_r \cap a$, then $u\ s'\ d$ for some $s' \in c$, $u\ s\ d$ a contradiction). Therefore $\bigcup K$ is founded, and therefore obviously well-founded.
Therefore $\bigcup K \in c$ and we see easily $\bigcup K$ is an upper bound of K.
Therefore c has a maximum element r. Assume $\mathrm{field}(r) \neq b$. Let $a \in b \setminus \mathrm{field}(r)$.
Let $r' := r \cup (\mathrm{field}(r) \times \{b\})$. $r' \in c$, $r \sqsubset r'$, a contradiction to r being maximum.
Therefore r is a well-ordering on a.
(WO) $\Rightarrow$ (AC): Let r be a well-ordering on $\bigcup a$. Define $f : a \setminus \{\emptyset\} \to \bigcup a$, $f(x) = \min_r(x)$. f is obviously a choice function for a.

8.4 Ordinal Arithmetic

We follow [Sch95].

Definition 8.20 (a) $1 := \mathrm{S}(0)$, $2 := \mathrm{S}(1)$.

(b) By recursion on β we define $\alpha + \beta$ by:
$\alpha + 0 := \alpha$,
$\alpha + \mathrm{S}(\beta) := \mathrm{S}(\alpha + \beta)$,
$\alpha + \lambda := \sup\{\alpha + \gamma \mid \gamma \in \lambda\}$, if $\lambda \in \mathrm{Lim}$.
(More precisely, define for α fixed, $\mathcal{F}_\alpha : \mathrm{Ord} \to \mathrm{V}$ by

$\mathcal{F}_\alpha(\beta) := \alpha$, if $\beta = 0$,
$\mathcal{F}_\alpha(\beta) := \mathrm{S}(\mathcal{F}_\alpha(\bigcup\beta))$, if β is a successor ordinal (and therefore $\bigcup\beta < \beta$),
$\mathcal{F}_\alpha(\beta) := \bigcup \mathrm{rng}\mathcal{F}_\alpha[\beta]$, otherwise.
$\alpha + \beta := \mathcal{F}_\alpha(\beta)$.

(c) By recursion on β we define $\alpha \cdot \beta$ by:
$\alpha \cdot 0 := 0$,
$\alpha \cdot \mathrm{S}(\beta) := (\alpha \cdot \beta) + \alpha$,
$\alpha \cdot \lambda := \sup\{\alpha \cdot \gamma \mid \gamma \in \lambda\}$, if $\lambda \in \mathrm{Lim}$.

(d) By recursion on β we define α^β by:
$\alpha^0 := \begin{cases} 0 & \text{if } \alpha = 0 \\ 1 & \text{otherwise,} \end{cases}$
$\alpha^{\mathrm{S}(\beta)} := \alpha^\beta \cdot \alpha$,
$\alpha^\lambda := \sup\{\alpha^\gamma \mid \gamma \in \lambda\}$, if $\lambda \in \mathrm{Lim}$.

Lemma 8.21 *(a)* $\alpha + \beta, \alpha \cdot \beta, \alpha^\beta \in \mathrm{Ord}$

(b) $0 + \beta = \beta$.

(c) If $n, m \in \omega$, *then* $n + m < \omega$.

(d) If $n \in \omega$, $n + \omega = \omega$.

(e) $\exists \alpha, \beta. \alpha + \beta \neq \beta + \alpha$.

(f) $\beta < \gamma \to \alpha + \beta < \alpha + \gamma$.

(g) There exists α, β, γ *such that* $\alpha < \beta$ *and* $\alpha + \gamma \not< \beta + \gamma$.

(h) $\alpha \leq \beta \to \alpha + \gamma \leq \beta + \gamma$.

(i) If $\lambda \in \mathrm{Lim}$, *then* $\alpha + \lambda \in \mathrm{Lim}$.

Proof:
(a): Easy induction on β.
(b): Induction on β.
(c): Induction on m.
(d): $n+m < \omega$, therefore $n+\omega = \sup\{n+m \mid m < \omega\} \leq \omega$. $m \leq n+m \leq n+\omega$, $\omega \leq n + \omega$.
(e): $\omega + 1 = \mathrm{S}(\omega) \neq \omega = 1 + \omega$.
(f) Induction on γ.
(g) $0 < 1$, but $0 + \omega = \omega = 1 + \omega$.
(h) Induction on γ.
(i) If $\gamma < \alpha + \lambda$, then $\gamma < \alpha + \beta$ for some $\beta < \lambda$, $\mathrm{S}(\gamma) < \mathrm{S}(\alpha + \beta) = \alpha + \mathrm{S}(\beta) \leq \alpha + \lambda$.

Lemma 8.22 *(a)* $0 \cdot \beta = 0$.

(b) $1 \cdot \beta = \beta$.

(c) *If* $n, m \in \omega$, *then* $n \cdot m < \omega$.

(d) *If* $1 \leq n \in \omega$, *then* $n \cdot \omega = \omega$.

(e) $\exists \alpha, \beta . \alpha \cdot \beta \neq \beta \cdot \alpha$.

(f) $0 < \alpha \wedge \beta < \gamma \rightarrow \alpha \cdot \beta < \alpha \cdot \gamma$.

(g) *There exists* α, β, γ *such that* $0 < \gamma$, $\alpha < \beta$ *and* $\alpha \cdot \gamma \not< \beta \cdot \gamma$.

(h) $\alpha \leq \beta \rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$.

(i) *If* $0 < \alpha$ *and* $\lambda \in \mathrm{Lim}$, *then* $\alpha \cdot \lambda \in \mathrm{Lim}$.

(j) $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$.

(k) *There exist* α, β, γ *such that* $(\alpha + \beta) \cdot \gamma \neq \alpha \cdot \gamma + \beta \cdot \gamma$.

(l) $\alpha \cdot \beta = 0 \rightarrow \alpha = 0 \vee \beta = 0$.

(m) $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$.

(n) *Is* $0 < \beta$, *then there are uniquely defined* γ, ρ *such that* $\alpha = \beta \cdot \gamma + \rho$ *and* $\rho < \beta$.

Proof:
(a), (b): Induction on β.
(c): Induction on m.
(d): As for $+$.
(e): $2 \cdot \omega = \omega < \mathrm{S}(\omega) = \omega + 1 \leq \omega + \omega = \omega \cdot 2$.
(f): Induction on γ.
(g): $1 < 2$, $1 \cdot \omega \not< \omega = 2 \cdot \omega$.
(h): Induction on γ.
(i): Similarly as for $+$.
(j): Induction on γ.
(k): $\alpha = \beta = 1$, $\gamma = \omega$ $(\alpha + \beta) \cdot \omega = 2 \cdot \omega = \omega$, $\alpha \cdot \omega + \beta \cdot \omega = \omega + \omega \neq \omega$.
(l): If $\alpha, \beta \neq 0$, then $0 < \alpha$, $1 \leq \beta$, $0 < 1 = 1 \cdot 1 \leq \alpha \cdot 1 \leq \alpha \cdot \beta$.
(m): Induction on γ.
(n): Uniqueness: γ is uniquely determined by $\beta \cdot \gamma \leq \alpha < \beta \cdot \mathrm{S}(\gamma)$, and since $+$ is monotone in the second argument follows uniqueness of ρ. Existence: Let $\mathcal{F} : \mathrm{Ord} \rightarrow \mathrm{Ord}$, $\mathcal{F}(\nu) := \beta \cdot \nu$, $\mathcal{F}$ is strictly monotone, therefore there exists γ, $\mathcal{F}(\gamma) \leq \alpha < \mathcal{F}(\mathrm{S}(\gamma))$. By monotonicity of $+$ in the second argument exists ρ such that $\mathcal{F}(\gamma) + \rho \leq \alpha < \mathcal{F}(\gamma) + \mathrm{S}(\rho) = \mathrm{S}(\mathcal{F}(\gamma) + \rho)$. $\beta \cdot \gamma + \rho = \alpha$. If $\rho \not< \beta$, then $\beta \cdot \mathrm{S}(\gamma) = (\beta \cdot \gamma) + \beta \leq \beta \cdot \gamma + \rho = \alpha < \mathcal{F}(\mathrm{S}(\gamma)) = \beta \cdot \mathrm{S}(\gamma)$, a contradiction.

Lemma 8.23 *(a)* $0^\alpha = 0$, $1^\alpha = 1$.

(b) $n, m < \omega \rightarrow n^m < \omega$.

(c) $2 \leq n < \omega \rightarrow n^\omega = \omega$.

(d) $1 < \alpha \wedge \beta < \gamma \rightarrow \alpha^\beta < \alpha^\gamma$.

(e) *There exist* α, β, γ *such that* $1 < \gamma$, $1 < \alpha < \beta$ *and* $\alpha^\gamma \nless \beta^\gamma$.

(f) $\alpha \leq \beta \to \alpha^\gamma \leq \beta^\gamma$.

(g) *If* $1 < \alpha$ *and* $\lambda \in \mathrm{Lim}$, *then* $\alpha^\lambda \in \mathrm{Lim}$.

(h) $\alpha^{\beta+\gamma} = \alpha^\beta + \alpha^\gamma$.

(i) $\alpha^{\beta \cdot \gamma} = (\alpha^\beta)^\gamma$.

(j) $1 < \alpha \to \beta \leq \alpha^\beta$.

Proof:
(a): Induction on α.
(b): Induction on m.
(c): As for $+$.
(d): Induction on γ.
(e): $\alpha := 2$, $\beta := 3 := \mathrm{S}(2)$, $\gamma := \omega$.
(f): Induction on γ.
(g): If $\gamma < \alpha^\lambda$, $\gamma < \alpha^\beta$ for some $\beta < \lambda$, $\mathrm{S}(\gamma) < \alpha^{\mathrm{S}(\beta)} \leq \alpha^\lambda$.
(h), (i): Induction on γ.
(j): Induction on β.

Chapter 9

Cardinals

We will follow in this section very closely [Buc93b], section 8. We will work in ZF.

9.1 Basics about Cardinals

We use natural numbers for two purposes: In order to enumerate (the first, the second, the third, the grammatical term is "ordinal number") and in order to give a measure for the size of a collection of objects (for instance "a woman has three children"). For finite sets, both notions coincide: independent of how we enumerate the elements of a finite set, the largest number we obtain will always be the number of elements of this sets.
For infinite sets these notions do not coincide: we can enumerate the set $\omega + 1$ in two ways: by the identity $(\omega+1) \to (\omega+1)$ and by $f : \omega \to \mathrm{S}(\omega)$, $f(0) := \omega$, $f(n+1) := n$. Therefore we could have two different sizes, ω and $\omega + 1$. We have to select one, and take the least one.
Cardinals will be ordinals of minimal size, i.e. those which cannot be mapped bijectively to a smaller ordinal. However, that every set has as size an ordinal, i.e. can be mapped bijectively to a ordinal, is equivalent to the well-ordering axiom (every set can be well-ordered), which is equivalent to the axiom of choice. So, in the development of the theory we will occasionally need the axiom of choice.

Definition 9.1 (a) $a \sim b :\Leftrightarrow \exists f(f : a \xrightarrow{\cong} b)$.

(b) $a \preceq b :\Leftrightarrow \exists f(f : a \rightarrowtail b)$.

Lemma 9.2 *(a) $\preceq$ is reflexive and transitive.*

(b) $a \subseteq b \to a \preceq b$.

(c) $\sim$ is an equivalence relation on V.

(d) *For every set a the following assertions are equivalent:*

(i) $\exists r$(r *is well-ordering on* a).

(ii) $\exists \alpha \in \mathrm{Ord}(\alpha \sim a)$.

(iii) $\exists \alpha \in \mathrm{Ord}.\exists f(f : \alpha \twoheadrightarrow a)$.

(iv) $\exists g(g : a \rightarrowtail \mathrm{Ord})$.

Proof:
(a) - (c): easy.
(d): (i) $\Rightarrow$ (ii): by theorem 8.14. (ii) $\Rightarrow$ (iii): trivial. (iii) $\Rightarrow$ (iv): $g(x) := \min\{\xi \in \alpha \mid f(\xi) = x\}$. (iv) $\Rightarrow$ (i): $r := \{(y, x) \in a \times a \mid g(y) < g(x)\}$.

Theorem 9.3 (Cantor-Bernstein) $a \preceq b \wedge b \preceq a \to a \sim b$.

Proof: W.l.o.g. $b \subseteq a$. Let $f : a \to b$ injective. We need to define $g : a \to b$ bijective.
Let $h : \omega \to \mathcal{P}(a)$, $h(0) := a \setminus b$, $h(\mathrm{S}(n)) := f[h(n)]$.

$$n < m \to h(n) \cap h(m) = \emptyset \tag{1}$$

Induction on n: $n = 0$. If $m > 0$, then $h(m) = f[h(m-1)] \subseteq b$, $h(m) \cap h(0) = h(m) \cap (a \setminus b) = \emptyset$.
$n \to n+1$: If $x \in h(n+1) \cap h(m)$, $m > n+1$, then $x = f(y) = f(y')$ for some $y \in h(n)$, $y' \in h(m-1)$, by injectivity and IH $y = y' \in h(n) \cap h(m-1) = \emptyset$, a contradiction.

$$f \restriction h(n) : h(n) \xrightarrow{\cong} h(n+1) \tag{2}$$

Clear.
Let $a_0 := \bigcup \mathrm{rng}(h) = \bigcup_{n \in \omega} h(n)$, $a_1 := a_0 \setminus h(0) = a_0 \setminus (a \setminus b) = a_0 \cap b$. By (1) $x \in a_0 \leftrightarrow \exists n \neq 0.x \in h(n)$.

$$f \restriction a_0 : a_0 \xrightarrow{\cong} a_1 \tag{3}$$

Let $a_2 := a \setminus a_0 = b \setminus a_1$. Let $g : a \to b$, $g(x) := \begin{cases} f(x) & \text{if } x \in a_0 \\ x & \text{otherwise.} \end{cases}$ $g \restriction a_0 = f \restriction a_0 : a_0 \to a_1$ bijective, $g \restriction (a \setminus a_0) = \mathrm{identity}_{a \setminus a_0} : (a \setminus a_0) \to (b \setminus a_1)$ bijective, where $\mathrm{identity}_c : c \to c$, $\mathrm{identity}(x) := x$. Further a is the disjoint union on a_0 and $a \setminus a_0$, b the disjoint union of a_1 and $b \setminus a_1$, and we get the assertion.

Theorem 9.4 $\mathcal{P}(a) \not\preceq a$.

Proof:
$a \preceq \mathcal{P}(a)$ ($f := \{<x, \{x\}> \mid x \in a\}$). If $\mathcal{P}(a) \preceq a$, then $\mathcal{P}(a) \sim a$, let $f : a \xrightarrow{\cong} \mathcal{P}(a)$, $b := \{x \in a \mid x \notin f(x)\} \in \mathcal{P}(a)$, c such that $f(c) = b$. Then $c \in f(c) \leftrightarrow c \notin f(c)$, a contradiction.

Definition 9.5 (a) A *cardinal* is an ordinal α such that $\neg\exists\beta < \alpha.\alpha \sim \beta$.

(b) Card is the class of cardinals.

(c) $|a| := \begin{cases} \min\{\xi \in \mathrm{Ord} \mid a \sim \xi\} & \text{if } \exists\xi.a \sim \xi \\ \{\{0\}\} & \text{otherwise.} \end{cases}$
(Note $\{\{0\}\} \notin \mathrm{Ord}$).
If $|a| \in \mathrm{Ord}$, then $|a|$ is called *the cardinality of* a.

Lemma 9.6 *(a) If $|a| \in \mathrm{Ord}$, then $|a|$ is a cardinal.*

(b) $\alpha \in \mathrm{Card} \leftrightarrow \neg\exists\xi < \alpha(\alpha \preceq \xi)$.

(c) $|a| \in \mathrm{Card} \leftrightarrow \exists\alpha.a \preceq \alpha$.

(d) $|a| \in \mathrm{Card} \to |a| = \min\{\xi \mid a \preceq \xi\}$.

(e) $|a| \in \mathrm{Card} \to (a \sim b \leftrightarrow |a| = |b|)$.

(f) $|a| \in \mathrm{Card} \to (b \preceq a \leftrightarrow |b| \leq |a|)$.

(g) $|a| \in \mathrm{Card} \wedge \mathrm{Fun}(\mathcal{F}) \to |\mathcal{F}[a]| \leq |a|$.

Proof:
(a) clear.
(b): if $\xi < \alpha$ then $\xi \preceq \alpha$, therefore $\alpha \preceq \xi \leftrightarrow \alpha \sim \xi$.
(c): by Lemma 9.2 (d), (iv) $\Rightarrow$ (ii).
(d) $\xi < |a| \Rightarrow |a| \not\preceq \xi \Rightarrow a \not\preceq \xi$. $|a| \leq \xi \Rightarrow a \preceq |a| \preceq \xi$.
(e) trivial.
(f) "$\leftarrow$" is trivial. "$\to$": $|b| = \min\{\xi \mid b \preceq \xi\} \leq \min\{\xi \mid a \preceq \xi\} = |a|$.
(g) Let r be a well-ordering on a (existing by Lemma 9.2 (d) (ii) $\Rightarrow$ (i)), $h : \mathcal{F}[a] \to a$, $h(y) := \min_r\{x \in a.\mathcal{F}(x) = y\}$. h is injective, $\mathcal{F}[a] \preceq a$, $|\mathcal{F}[a]| \leq |a|$.

The following theorem shows that we can come relatively far without using the axiom of choice. Note that, having the axiom of choice, it becomes trivial by defining $\alpha := |\mathcal{P}(a)|$.

Lemma 9.7 *(a)* **(Hartog, 1915)** $\forall x.\exists\alpha.\forall y \in \mathcal{P}(x).\alpha \not\sim y$.

(b) $\forall\alpha.\exists\beta > \alpha.\beta \in \mathrm{Card}$.

Proof:
(a) Assume x and $\forall\alpha.\exists y \in \mathcal{P}(x).\alpha \sim y$. Define a function $\mathcal{F}$ with $\mathrm{dom}(\mathcal{F}) = \mathrm{Ord}$ and $\mathcal{F}(\alpha) := w_\alpha$, where
$w_\alpha := \{<y, r> \mid y \subseteq x, <y, r> \text{ is a well-ordering of order-type } \alpha\}$.
($w_\alpha \subseteq \mathcal{P}(x) \times \mathcal{P}(x \times x)$, therefore w_α is a set).
By assumption $\mathcal{F}(\alpha) \neq \emptyset$ and since for $<y, r> \in \mathcal{F}(\alpha)$, α is the order type of $<y, r>$ follows $\mathcal{F}$ is injective, $\mathcal{F}[\mathrm{Ord}]$ is a set (since $\subseteq \mathcal{P}(\mathcal{P}(x) \times \mathcal{P}(x \times x))$), therefore $\mathrm{Ord} = \mathcal{F}^{-1}[\mathcal{F}[\mathrm{Ord}]]$ is a set, too, a contradiction.
(b) Let γ such that $\gamma \not\sim x$ for every $x \subseteq \alpha$. Let β be minimal s.t. $\gamma \sim \beta$. β is a cardinal. If $\beta \leq \alpha$, $\gamma \sim \beta \subseteq \alpha$, a contradiction, therefore $\alpha < \beta$.

Definition 9.8 $\alpha^+ := \min\{\mu \in \mathrm{Card} \mid \alpha < \mu\}$.

Lemma 9.9 *Let* $\kappa \in \mathrm{Card}$, $\alpha \in \mathrm{Ord}$.

(a) $|\alpha| < \kappa \leftrightarrow \alpha < \kappa$.

(b) $\kappa < |\alpha| \leftrightarrow \kappa^+ \leq \alpha$.

(c) $|\alpha| = \kappa \leftrightarrow \kappa \leq \alpha < \kappa^+$.

Proof: (a): $|\alpha| < \kappa \leftrightarrow \neg(\kappa \preceq \alpha) \leftrightarrow \alpha < \kappa$. (b) $\kappa < |\alpha| \leftrightarrow \kappa^+ \leq |\alpha| \leq \alpha$. (c) by (a), (b).

Definition 9.10 (a) a is *finite* $:\Leftrightarrow |a| < \omega$ (i.e. $\exists k \in \omega. a \sim k$).

(b) a is *D-finite* $:\Leftrightarrow \neg\exists f(f : a \rightarrowtail a \wedge f[a] \neq a)$.

Remark 9.11 *From a infinite does not follow in general* $\omega \leq |a|$*, since* $|a|$ *need not be an ordinal.*

Lemma 9.12 *(a)* $b \preceq a \wedge a$ *finite* $\rightarrow b$ *finite.*

(b) a *finite* $\rightarrow a = \emptyset \vee \exists x \in a(|a| = \mathrm{S}(|a \setminus \{x\}|))$.

(c) $a \subseteq \omega \rightarrow (a$ *finite* $\leftrightarrow \exists n \in \omega. a \subseteq n)$.

(d) ω *is the least infinite cardinal.*

(e) a *is D-infinite* $\leftrightarrow \omega \preceq a$.

(f) a *finite* $\rightarrow a$ *D-finite.*

(g) $\omega \subseteq \mathrm{Card}$.

(h) $(AC) \rightarrow (a$ *D-finite* $\leftrightarrow a$ *finite*$)$.

Proof:
(a): Lemma 9.6 (f).
(b): Let $f : k \rightarrow a$ bijective, $k \in \omega$. If $k = 0$, $a = \emptyset$. Otherwise $k = \mathrm{S}(k')$, and with $x := f(k)$ follows the assertion.
(c): "$\rightarrow$": Induction on $|a|$ using (b). "$\leftarrow$": Induction on n: If $a \subseteq 0$, $|a| = 0$. If $a \subseteq n+1$, then $a \subseteq n$ and by IH follows the assertion or $n \in a$, $a \setminus \{n\} \subseteq n$, $|a \setminus \{n\}| = k$ for some k $a \preceq k+1$.
(d): Assume ω is finite. Then by (c) $\omega \subseteq k$ for some $k \in \omega$, $k \in \omega = k$, a contradiction. ω is therefore infinite. Therefore $\neg\exists\alpha \in \omega.\alpha \sim \omega$, $\omega \in \mathrm{Card}$.
(e) "$\rightarrow$" Let $f : a \rightarrow a$ injective, $f[a] \neq a$. Let $x_0 \in a \setminus f[a]$ and define $g : \omega \rightarrow a$, $g(0) := x_0$, $g(\mathrm{S}(n)) := f(g(n))$. $\forall n \in \omega.\forall i(i > n \rightarrow g(n) \neq g(i))$: $n = 0$: $x_0 \notin f[a]$, $g(i) \in f[a]$. $n \rightarrow n+1$: $g(n+1) = g(i) \Rightarrow f(g(n)) = f(g(i-1)) \Rightarrow g(n) = g(i-1)$, contradicting the IH.
"$\leftarrow$: Let $g : \omega \rightarrowtail a$, define $f := \{<g(n), g(\mathrm{S}(n))> \mid n \in \omega\} \cup \{<x \mid x> \mid x \in a \setminus g[\omega]\}$. $f : a \rightarrow a$, f is obviously injective, $f[a] \neq a$.

(f): Assume $a \sim k$. If $\omega \preceq a$, then $\omega \preceq k$, contradicting that ω is a cardinal.
(g): Assume $n \in \omega$, $m \leq n$, $f : n \to m$ injective. n is D-finite (by (f)), $f[n] \subseteq m \subseteq n$, therefore $f[n] = n$, $m = n$.
(h): "$\to$": By (AC) there exists a well-ordering on a, therefore $|a| \in \mathrm{Card}$. If a is D-finite, then by (e) $\omega \not\preceq a$, $\omega = |\omega| \not\leq |a|$, $|a| < \omega$, $a \prec \omega$, a finite. "$\leftarrow$"; (f).

Lemma 9.13 $\omega \preceq \kappa \in \mathrm{Card} \to \kappa \in \mathrm{Lim}$.

Proof:
Assume $\omega \leq \mathrm{S}(\beta)$. Then

$$f : \mathrm{S}(\beta) \to \beta,\ f(\gamma) := \begin{cases} \mathrm{S}(\gamma) & \text{if } \gamma \in \omega \\ 0 & \text{if } \gamma = \beta \\ \gamma & \text{otherwise} \end{cases}$$

is bijective, $\mathrm{S}(\beta) \sim \beta < \mathrm{S}(\beta)$.

Definition 9.14 Let $\alpha \mapsto \aleph_\alpha$ [$\aleph$ is the Hebrew letter aleph] be defined recursively by: $\aleph_\alpha := \min\{\kappa \in \mathrm{Card} \mid \kappa \geq \omega \land \forall \beta < \alpha . \aleph_\beta < \kappa\}$.

Remark 9.15 $\alpha \mapsto \aleph_\alpha$ *is the order function of* $\mathrm{Card} \setminus \kappa$. *Especially it is well-defined (if* $\alpha \in \mathrm{Ord}$*, then there exists a cardinal bigger then* $\max\{\omega, \bigcup_{\beta<\alpha} \aleph_\beta\}$*).*

Lemma 9.16 Card *is closed, i.e.* $\forall u (u \subseteq \mathrm{Card} \to \sup(u) \in \mathrm{Card})$.

Proof: Let $\gamma := \sup(u)$, $f : \gamma \to \alpha$ injective. Then $\forall \xi \in u . \xi \preceq \alpha$, $\forall \xi \in u . \xi \leq \alpha$, $\gamma = \sup(u) \leq \alpha$.

9.2 Cardinal arithmetic

Definition 9.17 Let $\kappa, \mu \in \mathrm{Card}$.

(a) $\kappa \oplus \mu := |(\{0\} \times \kappa) \cup (\{1\} \times \mu)|$ $(1 := \mathrm{S}(0))$.

(b) $\kappa \odot \mu := |\kappa \times \mu|$.

Definition 9.18 Define the relation $\prec'$ on $\mathrm{Ord} \times \mathrm{Ord}$ by:
$<\alpha, \beta> \prec' <\alpha', \beta'> \leftrightarrow \max\{\alpha, \beta\} < \max\{\alpha', \beta'\} \lor ((\max\{\alpha, \beta\} = \max\{\alpha', \beta'\} \land (\alpha < \alpha' \lor (\alpha = \alpha' \land \beta < \beta'))))$.

Lemma 9.19 *(a)* $\prec'$ *is a well-ordering on* $\mathrm{Ord} \times \mathrm{Ord}$.

(b) If $\kappa, \mu \in \mathrm{Card}$*, then* $\kappa \oplus \mu, \kappa \odot \mu \in \mathrm{Card}$.

Proof:
(a): $\prec'$ is obviously linear. Further, if $\emptyset \neq a \subseteq \mathrm{Ord} \times \mathrm{Ord}$, then let α be minimal such that $\alpha = \max\{\beta, \gamma\}$ for some $<\beta, \gamma> \in a$, Then for all $<\beta, \gamma< \in a$ with $\max\{\beta, \gamma\} = \alpha$ let first β be minimal and then choose γ minimal such that $<\beta, \gamma> \in a \land \max\{\beta, \gamma\} = \alpha$. $<\beta, \gamma>$ is minimal in a.
(b): by (a)

Lemma 9.20 *Assume* $\kappa, \mu, \tau \in \mathrm{Card}$, $m, n \in \omega$.

(a) $\kappa \oplus 0 = \kappa$.

(b) $\kappa \odot 0 = 0$.

(c) $\kappa \odot 1 = \kappa$.

(d) $\oplus$, $\odot$ *are commutative, associative, and (together) distributive.*

(e) $m \oplus n = m + n$.

(f) $m \odot n = m \cdot n$.

(g) If $\kappa, \mu \neq 0$, $\omega \leq \max\{\kappa, \mu\} = \kappa \cup \mu$, *then* $\kappa \oplus \mu = \kappa \odot \mu = \kappa \cup \mu$.

Proof:
(a), (b), (c): trivial. (d): easy.
(e), (f) $m+n \sim (\{0\}\times m)\cup(\{1\}\times n)$, $m+n$ is a cardinal, therefore the assertion, similar for $\cdot$ and $\odot$.
(g): Obviously $\kappa\cup\mu \leq \kappa\oplus\mu \leq (\kappa\cup\mu)\odot(\kappa\cup\mu)$, $\kappa\cup\mu \leq \kappa\odot\mu \leq (\kappa\cup\mu)\odot(\kappa\cup\mu)$, so it suffices to show for $\omega \leq \kappa \in \mathrm{Card}$ that $\kappa \odot \kappa = \kappa$.
$\kappa \preceq \kappa \times \kappa$, therefore it suffices to show $\kappa \times \kappa \preceq \kappa$.
Let $\Gamma : \mathrm{Ord} \times \mathrm{Ord} \to \mathrm{Ord}$ the uniquely determined isomorphism $(\mathrm{Ord} \times \mathrm{Ord}, \prec'$ $) \to (\mathrm{Ord}, <)$ (the inverse of the order function of $(\mathrm{Ord}, <)$.
It suffices to show $\forall \kappa \in \mathrm{Card} \setminus \mathrm{Lim}.\Gamma[\kappa \times \kappa] = \kappa$. Induction on κ.
One easily verifies $\Gamma[\kappa \times \kappa] = \bigcup_{\beta<\kappa} \Gamma[\beta \times \beta]$ and therefore we have only to show $\forall \beta < \kappa.\Gamma[\beta \times \beta] < \kappa$.
If $\beta < \omega$ follows $\Gamma[\beta \times \beta] \sim \beta \times \beta \sim \beta \cdot \beta < \omega \leq \kappa$.
Otherwise $\beta < \kappa$, $\omega \leq |\beta| < \kappa$, $\Gamma[\beta \times \beta] \sim \Gamma[|\beta| \times |\beta|] = |\beta| < \kappa$.

Lemma 9.21 *Assume (AC),* $\mathrm{Fun}(\mathcal{F})$, $c \subseteq \mathrm{dom}(\mathcal{F})$.

(a) $|\bigcup \mathcal{F}[c]| \leq |c| \odot \sup\{|\mathcal{F}(x)| \mid x \in c\}$.

(b) Let $\omega \leq \kappa$ *such that* $|c| \leq \kappa \in \mathrm{Card} \wedge \forall x \in c(|\mathcal{F}(x)| \leq \kappa)$. *Then* $|\bigcup_{x\in c} \mathcal{F}(x)| \leq \kappa$.

Proof:
(a): W.l.o.g. $c = |c|$. Let $\kappa := \sup\{|\mathcal{F}(x)| \mid x \in c\}$. By (AC) there is a function $g : c \to \mathrm{V}$ such that $g(x) : \mathcal{F}(x) \to \kappa$ injective. Let $h : \bigcup \mathcal{F}[c] \to c \times \kappa$, $h(y) := <\xi, g(\xi)(y)>$ where $\xi := \min\{x \in c \mid y \in \mathcal{F}(x)\}$. h is injective, and therefore $\bigcup \mathcal{F}[c] \preceq c \times \kappa$.
(b): by (a). d

Definition 9.22 (a) ${}^{a}b := \{f : a \to b\}$.

(b) $\alpha^\beta := |{}^{\beta}\alpha|$.

Note that this is the same notation as for ordinal exponentiation, although these are quite different operations. In the literature this double-notation has been used since long time ago.

Remark 9.23 *Without (AC) we cannot prove in general* $\alpha^\beta \in \mathrm{Ord}$.

Lemma 9.24 *(AC) Let* $\kappa, \mu \in \mathrm{Card}$.

(a) $\kappa < 2^\kappa$.

(b) $(2 \leq \kappa \leq \mu \wedge \omega \leq \mu) \to 2^\mu = \kappa^\mu$.

(c) $(2^\kappa)^\mu = 2^{\kappa \odot \mu}$.

Proof:
(a): $2^\kappa \sim \{f : \kappa \to 2\} \sim \mathcal{P}(\kappa)$, $\kappa \not\sim \mathcal{P}(\kappa)$, $\kappa \preceq \mathcal{P}(\kappa)$.
(b) $2^\mu \leq \kappa^\mu$ is clear. Further $\kappa^\mu \leq \mu^\mu = |\{f : \mu \to \mu\}| \leq |\mathcal{P}(\mu \times \mu)| = |\mathcal{P}(\mu)| = 2^\mu$.
(c) Define $g :\ {}^\mu({}^\kappa 2) \to\ {}^{\mu \times \kappa}2$, $g(f)(<x, y>) = f(x)(y)$. g is bijective.

Definition 9.25 Let $\mathcal{P}^{<\omega}(a)$ be the set of finite subsets of a.

Lemma 9.26 *(AC) If a is infinite, then* $|\mathcal{P}^{<\omega}(a)| = a$.

Proof:
If $0 < n \in \omega$, then $a^n \sim a$ ($n = 1$: clear. $a^{n+1} \sim a^n \times a \sim a \times a \sim a$.). For every element of $\mathcal{P}^{<\omega}(a)$ there exists an $n \in \omega$ and a function $f : n \to a$ such that $f[n] = a$. Therefore there exists an injection $g : \mathcal{P}^{<\omega}(a) \to \bigcup_{n \in \omega} {}^n a$. Therefore $|\mathcal{P}^{<\omega}(a)| \leq |\bigcup_{n \in \omega} {}^n a| \leq \omega \odot |a| = |a|$. Further $a \to \mathcal{P}^{<\omega}(a)$, $x \mapsto \{x\}$ is injective, therefore $|a| \leq |\mathcal{P}^{<\omega}(a)|$.

9.3 The Continuum Hypothesis

Lemma 9.27 *(AC)* $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

Proof:
For every real number we can choose a Cauchy sequence in $\mathbb{Q}$. Therefore there exists by (AC) $g : \mathbb{R} \rightarrowtail \{f : \mathbb{N} \to \mathbb{Q}\}$. $\mathbb{Q} \sim \mathbb{N}$ therefore $|\mathbb{R}| \leq |\{f : \mathbb{N} \to \mathbb{N}\}| = |{}^\omega\omega| = |\mathcal{P}(\mathbb{N})|$.

In the other direction, let for $a \in \mathcal{P}(\omega)$, $f_a : \omega \to \omega$, $f_a(i) := \begin{cases} 1 & \text{if } i \in a \\ 0 & \text{otherwise,} \end{cases}$

and

$$g(a) := \begin{cases} \sum_{i=0}^\infty f_a(i)2^{-i} & \text{if} \forall i \in \omega . \exists j \in \omega (j > i \wedge f_a(j) = 0) \\ -\sum_{i=0}^\infty f_a(i)2^{-i} & \text{otherwise.} \end{cases}$$

(The case distinction is necessary, because in binary notation $a_0.a_1 \cdots a_n 0111 \cdots = a_0.a_1 \cdots a_n 1000 \cdots$). $g : \mathcal{P}(\omega) \to \mathbb{R}$ is injective.

The question is now: What is the cardinality of the reals in the $\aleph$-hierarchy, or, equivalently, what is the cardinality of $\mathcal{P}(\omega)$.

Continuum Hypothesis $|\mathcal{P}(\aleph_0)| = \aleph_1$.
Generalized Hypothesis $|\mathcal{P}(\aleph_\alpha)| = \aleph_{\alpha+1}$.

Equivalent to the (generalized) continuum hypothesis is the statement For $a := \omega$ (every infinite set a) there is no set b such that $|a| < |b| < |\mathcal{P}(a)|$.
Gödel (1939) and Cohen (1963) have shown that the continuum hypothesis is independent of set theory, i.e. it can neither be proved nor its negation can be proved in ZF, if ZF is consistent.
Many set theoreticians are looking for strong (and natural) axioms (usually existence of large cardinals), which, iff added to set theory, decide the continuum hypothesis.

Chapter 10

Appendix: Selected Topics

In this chapter we present the topics from the course description, we had no time to teach in detail:

10.1 Relative Computability

Definition 10.1 (a) **(Relative computability)**. The set of functions recursive in a function $f_0 : \mathbb{N}^k \to \mathbb{N}$ is the set of functions defined as $\mathcal{R}$ (Lemma 2.35 (d)), but with the additional clause $f_0 \in \mathcal{R}_k$.

(b) A set A is *recursive in a set* B or *Turing reducible to a set* B iff χ_A is recursive in χ_B. We write $A \leq_{\mathrm{T}} B$ for A is recursive in B.

(c) $A \equiv_{\mathrm{T}} B :\Leftrightarrow A \leq_{\mathrm{T}} B \wedge B \leq_{\mathrm{T}} A$.

(d) The equivalence classes of $\equiv_{\mathrm{T}}$ are called *Turing-degrees*.

Theorem 10.2 *(a)* $\leq_{\mathrm{T}}$ *is reflexive and transitive.*

(b) $\equiv_{\mathrm{T}}$ *is an equivalence relation.*

(c) $A \equiv_{\mathrm{T}} (\mathbb{N} \setminus A)$.

(d) If B *is recursive, then* $B \leq_{\mathrm{T}} A$ *for all* A.

(e) If B *is recursive,* $A \leq_{\mathrm{T}} B$*, then* A *is recursive*

(f) If A *is recursive enumerable, then* $A \leq_{\mathrm{T}} \mathrm{K}$.

Proof: (a)- (e) are easy.

(f): Let $f : \mathbb{N}^2 \to_{\mathrm{par}} \mathbb{N}$, $f(x, y) \simeq \begin{cases} 0 & \text{if } y \in A \\ \bot & \text{otherwise} \end{cases}$.
f is partial recursive. Let e be an index of f.

$$a \in A \quad \leftrightarrow \quad \forall a.\exists b.f(e, a) \simeq b$$

$$
\begin{aligned}
&\leftrightarrow \quad \exists b.\{e\}^2(e,a) \simeq b \\
&\leftrightarrow \quad \{\mathrm{s}^1_1(e,e)\}^2(b) \simeq b \\
&\leftrightarrow \quad \mathrm{s}^1_1(e,e) \in \mathrm{K}
\end{aligned}
$$

Theorem 10.3 (Friedberg, Muchnik) *There are recursive enumerable sets A, B such that $\neg(A{\leq_{\mathrm{T}}}B) \wedge \neg(B{\leq_{\mathrm{T}}}A)$.*

Proof: omitted.

Degree theory is the theory of the structure of Turing degrees. It is very well developed and extremely complex proof methods (i.e. so called "Monster proofs") are used in this area. Degree theory is the main part or recursion theory nowadays, and sometimes recursion theory (or in more modern terms computability theory) is identified with degree theory.

10.2 κ-categoricity

We cannot axiomatize (except for finite structures) the set of structure isomorphic to a given one $\mathcal{M}$, since for every infinite structure there exists an elementary equivalent structure of cardinality $|\mathcal{P}(\mathcal{M})|$ (Theorem 1.20). However, we could axiomatize the countable models of the structure of the rationals up to isomorphism (see Lemma 1.31). Therefore we get the following definition:

Definition 10.4 A theory T in a language $\mathcal{L}$ (with equality) IS κ-categorical, iff T has a model (with $=$ standard) of cardinality κ and every two models of T of cardinality κ are isomorphic.

Lemma 10.5 *The theory* DO *of dense linear orderings without endpoints is ω-categorical.*

Proof: Lemma 1.31

10.3 Tennenbaum's theorem

Definition 10.6 (a) Let PA be the extension of the theory Q in the language $\mathcal{L}_{\mathrm{ar}}$ by the induction axiom:

$$A(0) \to \forall x(A(x) \to A(\mathrm{S}(x))) \to \forall x(A(x))$$

(b) A set S is coded in a structure $\mathcal{M}$ of $\mathcal{L}_{\mathrm{ar}}$ iff there is an $a \in |\mathcal{M}|$ such that $S = \{n \in \mathbb{N} \mid \mathcal{M} \models \mathrm{Pr}_y \mid x[x := a, y := \underline{n}^{\mathcal{M}}]\}$. Here $\mathrm{Pr}_y \mid x$ is the formula $\exists z.z = \mathrm{Pr}_y {\wedge} z \mid y$ where $z = \mathrm{Pr}_y$ and $z \mid y$ are the formulas representing the corresponding primitive recursive function Pr. (Pr_y is the yth prime) and relation $\mid$ (for "divides"). Further as before $x < y := \exists z(z \neq 0 \wedge x + z = y)$.

(c) A nonstandard model of PA is a structure $\mathcal{M}$ in $\mathcal{L}_{\mathrm{ar}}$ such that $\mathcal{M} \models \mathrm{PA}$ and $\mathcal{M} \models \underline{n} \neq x[x := a]$ for some $x \in \mathcal{M}$.

(d) A recursive model of PA is a model of $\mathcal{M}$ such that $|\mathcal{M}| = \mathbb{N}$ and $+^{\mathcal{M}}$ and $\cdot^{\mathcal{M}}$ are recursive.

Lemma 10.7 *If* $\mathcal{M}$ *is a nonstandard model of* PA*, then* $\mathcal{M}$ *codes a non-recursive set.*

Sketch of Proof:
$\mathrm{PA} \vdash \forall x.\exists y.\forall z < x(\mathrm{Pr}_z \mid y \leftrightarrow z \in \mathrm{K})$,
where $z \in \mathrm{K}$ is the formula in PA representing the recursive enumerable relation K in Q (and therefore as well PA.
Let b be nonstandard, $b \in |\mathcal{M}|$. Then $\mathcal{M} \models \forall z < b(\mathrm{Pr}_z \mid a \leftrightarrow z \in \mathrm{K})$, for some $a \in |\mathcal{M}|$, i.e. a codes the non recursive set K.

Theorem 10.8 (Tennenbaum's theorem) *There is no recursive nonstandard model of* PA.

(One can show even, that in any nonstandard model $\mathcal{M}$ with $|\mathcal{M}| = \mathbb{N}$, neither $+^{\mathcal{M}}$ nor $\cdot^{\mathcal{M}}$ are recursive).

Sketch of Proof:
Assume $\mathcal{M}$ is such a model. $\mathrm{S}^{\mathcal{M}}(a) = a +^{\mathcal{M}} \mathrm{S}^{\mathcal{M}}(0^{\mathcal{M}})$, so $\mathrm{S}^{\mathcal{M}}$ and therefore as well $e \mapsto \underline{e}^{\mathcal{M}}$ are recursive, too.

Claim: It is decidable, whether $\mathcal{M} \models x < y[x := a, y := b]$.

Proof: Test whether $\mathcal{M} \models x + u = y[x := a, y := b, u := c]$ or $\mathcal{M} \models y + u = x[x := a, y := b, u := c]$ for all $c \in |\mathcal{M}|$. Such a c can be found, and once such a c is found, we conclude: If $c = 0^{\mathcal{M}}$ or $\mathcal{M} \models y + u = x[x := a, y := b, u := c]$, then $\mathcal{M} \not\models x < y[x := a, y := b]$, otherwise the formula holds.

Claim: It is decidable, whether $\mathcal{M} \models x \mid y[x := a, y := b]$ for $a, b \in |\mathcal{M}|$.

Proof: $\mathrm{PA} \vdash \forall x, y.x \neq 0 \to \exists! z.\exists! w(y = x \cdot z + w \wedge w < x)$.
This formula holds therefore in $\mathcal{M}$. In order to test whether $\mathcal{M} \models x \mid y[x := a, y := b]$ we have therefore to try for all $n \in \mathbb{N}$ whether $\mathcal{M} \models (y = x \cdot z + w \wedge w < x)[x := a, y := b, z := \pi_1(n), w := \pi_2(n)]$. We will find a unique n and if $\pi_2(n) = 0$, $\mathcal{M} \models x \mid y[x; = a, y := b]$, otherwise not.

Claim: It is decidable whether $\mathcal{M} \models \mathrm{Pr}_{\underline{n}} \mid y[y := a]$ for $a \in |\mathcal{M}|$.

Proof: $\mathcal{M} \models \forall z(\mathrm{Pr}_{\underline{n}} = z \leftrightarrow z = \underline{\mathrm{Pr}_n})$. Decide, whether $\mathcal{M} \models x \mid y[x := (\underline{\mathrm{Pr}_n})^{\mathcal{M}}, y := a]$.

Let $S \subseteq \mathbb{N}$ be non-recursive, S be coded in $\mathcal{M}$ by a. Then $e \in \mathrm{K} \Leftrightarrow \mathcal{M} \models \mathrm{Pr}_{\underline{e}^{\mathcal{M}}} \mid x[x := a]$, therefore K is recursive, a contradiction.

10.4 The second Recursion theorem

We follow [Cut80].
The intuitive meaning of the second recursion theorem is that for any program transformation there is a program invariant under it in the sense that the program and the transformed program compute the same function. If we consider

programs as natural numbers, the function associated with program e being $\{e\}^1$, and program transformations as unary total recursive functions (on $\mathbb{N}$), then the statement reads as follows:

Theorem 10.9 (2^{nd} Recursion theorem.) *If f is a unary (total) recursive function. Then there is an $e_0 \in \mathbb{N}$ such that $\{f(e_0)\}^1 = \{e_0\}^1$.*

Proof:
Let h be some unary partial recursive function. By the s_n^m theorem there exists a primitive recursive function g (depending on h) such that

$$\{g(e)\}^1 = \{f(h(e))\}^1 \ . \tag{$*$}$$

(If $\{e_1\}^2(y,e) \simeq \{f(h(e))\}^1(y)$, choose $g(e) := \mathrm{s}_1^1(e_1, e)$).
If e_2 is such that $g(e_2) \simeq h(e_2)$, (especially therefore $h(e_2)$ is defined), then with $e_0 := h(e_2) = g(e_2)$ follows the assertion.
Let now $h(e) :\simeq \{e\}^1(e)$, and for this specific h let g be chosen as above. Then $(*)$ reads as $g(e_2) = \{e_2\}^1(e_2)$, which is fulfilled by e_2 such that $g = \{e_2\}^1$.

Corollary 10.10 *(a) If f is a unary recursive function, then there are e such that $\mathrm{W}_{f(e)} = \mathrm{W}_e$.*

(b) If f is a unary recursive function, then there are arbitrarily big numbers e such that $\{f(e)\}^1 = \{e\}^1$.

(c) If f is a binary recursive function, then there is an e such that $\{e\}^1(y) \simeq f(e,y)$.

Proof:
(a): Let $\{f(e)\}^1 \simeq \{e\}^1$.
(b): Let $n \in \mathbb{N}$, $c \in \mathbb{N}$ such that, and $\{c\}^1 \neq \{0\}^0, \{1\}^1, \ldots, \{e\}^1$.
$\{f'(e)\}^1 = \begin{cases} c & \text{if } e \leq n \\ f(e) & \text{otherwise.} \end{cases}$ Assume $\{f'(e)\}^1 = \{e\}^1$. If we had $e \leq n$, then $\{c\}^1 \simeq \{e\}^1$, which is not possible. Therefore $e > n$, $\{f(e)\}^1 = \{e\}^1$.
(c) Let $\{g(e)\}^1(y) \simeq f(e,y)$ (s_n^m-theorem). Let e such that $\{g(e)\}^1 = \{e\}^1$, then the problem is solved.

Examples:

(a) There is a number n such that $\{e\}(n) = e^n$. [Corollary 10.10 (c) with $f(m,x) := x^m$].

(b) There is a number n such that $\mathrm{W}_e = \{e\}$.
[Let $f(e,y) \simeq \begin{cases} 0 & \text{if } x = y \\ \text{undefined} & \text{otherwise,} \end{cases}$ $\{e\}(y) \simeq f(e,y)$.]

Bibliography

[Buc89] W. Buchholz. Rekursionstheorie. Manuskript of a lecture held in Sommer Semester 1989 at the University of Munich, 1989.

[Buc93a] W. Buchholz. Mathematische Logik I. Manuskript of a lecture held in Winter Semester 1992/93 at the University of Munich, 1993.

[Buc93b] W. Buchholz. Mathematische Logik II. Manuskript of a lecture held in Sommer Semester 1993 at the University of Munich, 1993.

[Buc97a] W. Buchholz. Mathematische Logik I. Manuskript of a lecture held in Winter Semester 1996/97 at the University of Munich, 1997.

[Buc97b] W. Buchholz. Mathematische Logik II. Manuskript of a lecture held in Sommer Semester 1997 at the University of Munich, 1997.

[Cra91] S. Craig. *Logical Number theory I. An introduction.* Springer, Berlin, Heidelberg, New York, 1991.

[Cut80] N. Cutland. *Computability. An Introduction to recursive function theory.* Cambridge University Press, Cambridge, 1980.

[Men87] E. Mendelson. *Introduction to Mathematical Logic.* Chapman and Hall, London, third edition, 1987.

[Men97] E. Mendelson. *Introduction to Mathematical Logic.* Chapman and Hall, London, fourth edition, 1997.

[Pal91] E. Palmgren. Lecture notes in Logik 2. Manuskript of a lecture held October-December 91 at Uppsala University, 1991.

[Rat96] M. Rathjen. Logic MN2 HT96. Manuskript of a lecture held in 1996 at Uppsala University. Typed by Sara Eklund, 1996.

[Sch86] H. Schwichtenberg. Mathematische Logik. Manuskript of a lecture held in Winter Semester 1985/86 at the University of Munich, 1986.

[Sch95] H. Schwichtenberg. Mathematische Logik II. Manuskript of a lecture held in Sommer Semester 1995 at the University of Munich, 1995.

[Sho67] J. Shoenfield. *Mathematical Logic.* Addison-Wesley, Reading, Massachusetts, 1967.

[SS63] J. C. Sheperdson and H. E. Sturgis. Computability of recursive functions. *J. Assoc Computer Machinery*, 10:217 – 255, 1963.

[Tur36] A. Turing. On computable numbers with an application to the Entscheidungsproblem. *Proc. London Math. Soc.*, 2(42):230 – 265, 1936.

[UU97] Teknisk-natuvetenskapliga fakulteten Uppsala Universitet. *Studiehandbok 1997/98, Matematisk-naturvetenskaplig program*, 1997.

[vD94] D. van Dalen. *Logic and structure. Third ed.* Springer, Berlin, Heidelberg, New York, third edition, 1994.