LECTURE NOTES: INTRODUCTION TO MATHEMATICAL LOGIC

PHILIPP SCHLICHT

Contents

These are lecture notes from the University of Bonn in the summer of 2021. I would like to thank the participants for comments and for finding errors and typos, in particular Tom Stalljohann, Celina Teke, Lucas Valle Thiele and others.

Overview

In the first chapter, we study structures, formulas and introduce the Hilbert calculus.

In the second chapter, we give an introduction to set theory. We begin informally with ordinals and cardinals, and then study axiomatic set theory up to transfinite induction. This can be seen as a foundation on which all results in this course are built.

In the third chapter, we present the completeness of Hilbert's proof calculus. We then study the compactness theorem and applications, deriving finitary analogues of infinitary combinatorial statements such as the infinite Ramsey's theorem.

Date: July 20, 2021.

In the fourth chapter, the main goal is Gödel's first incompleteness theorem. It shows that no matter how one extends the theory of the natural numbers, assuming there is a reasonable listing of all axioms, some statements that can neither be proved nor disproved will always remain.

In the final chapter, we give an introduction to model theory. We aim for some applications in algebra, for instance the Lefschetz principle, which relates statements about the complex numbers to other algebraically closed fields.

1. Formal languages and structures

Lecture 1
12. April

Mathematical logic studies formal languages and proofs (syntax), structures such as groups, fields, graphs or linear orders, and the connection between languages and structures (semantics). Expressions in a formal language are themselves considered as mathematical objects. For instance, a word in a language is a finite sequence of symbols, i.e. a function.

1.1. **Structures and formulas.** We begin by introducing structures and formulas in *first-order logic.*[1] Many familiar mathematical structures consist of a set with additional structure, for example:

(a) A *graph* is a pair (G, E), where $G \neq \emptyset$ is the set of nodes and $E \subseteq G^2$ is the set of *edges*, a *symmetric* set of ordered pairs in G. (A subset E of G^2 is called symmetric if $\forall x, y \in G\ (x, y) \in E \leftrightarrow (y, x) \in E$.)

(b) A *partial order* is a pair $(P, \leq)$, where $P \neq \emptyset$ is a set and $\leq$ is a binary relation on P satisfying the following conditions:
   (i) (Reflexivity) $\forall x \in P\ x \leq x$
   (ii) (Antisymmetry) $\forall x \in P\ ((x \leq y \wedge y \leq x) \rightarrow x = y)$
   (iii) (Transitivity) $\forall x \in P\ ((x \leq y \wedge y \leq z) \rightarrow \leq z)$

In general, a structure is defined as follows:

Definition 1.1.1. A *structure* or *model* is a pair $\mathcal{M} = (M, \mathcal{F})$, where M is a nonempty set and $\mathcal{F} = \langle F_i \mid i \in I \rangle$ is a family of

(1) elements (constants) $F_i \in M$,
(2) functions $F_i \colon M^{k_i} \to M$ with $k_i \in \mathbb{N}$, and
(3) relations $F_i \subseteq M^{k_i}$ with $k_i \in \mathbb{N}$.

and I is a set. Note that in most cases, I will be finite or countable.

When we write $\mathcal{M}$ and $\mathcal{N}$, we will assume that $\mathcal{M} = (M, \mathcal{F})$ and $\mathcal{N} = (N, \mathcal{F})$ as above.

Here are some more examples. The superscript notation will be defined in Definition 1.1.5.

Example 1.1.2.

(1) A ring $(R, 0^R, 1^R, +^R, \cdot^R)$.
(2) A group $(G, 1^G, \cdot^G, (\cdot^{-1})^G)$.
(3) The structure of the natural numbers $(\mathbb{N}, 0^{\mathbb{N}}, S^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}}. <^{\mathbb{N}})$, where $S^{\mathbb{N}}$ denotes the successor function.
(4) The field $(\mathbb{Q}, 0^{\mathbb{Q}}, 1^{\mathbb{Q}}, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}})$.

All groups have a binary operation (multiplication), a neutral element and an inverse function. This is encoded in the language of groups.

[1] Second-order logic, which we won't study here, allows two kinds of objects, for instance natural numbers and sets of natural numbers.

Definition 1.1.3. A *language* or *alphabet* is a set of constant symbols, function symbols and relation symbols. Function and relation symbol have an *arity*, i.e. a number of arguments, $k \in \mathbb{N}$ with $k \geq 1$. For example, an k-ary function on a set M is of the form $f\colon M^k \to M$. A k-ary relation R on a set M is of the form $R \subseteq M^k$.

Here are some examples of languages.

Example 1.1.4.

1. The empty language $\mathcal{L}_\emptyset = \emptyset$.
2. The language $\mathcal{L}_R = \{0, 1, +, \cdot\}$ of rings and fields.
3. The language $\mathcal{L}_G = \{1, \cdot, {}^{-1}\}$ of groups.
4. The language $\mathcal{L}_O = \{<\}$ of strict linear ordes.
5. The language $\mathcal{L}_{OF} = \mathcal{L}_R \cup \mathcal{L}_O$ of linearly ordered fields.
6. The language $\mathcal{L}_\mathbb{N} = \{0, S, +, <\}$ of the natural numbers.
7. The language $\mathcal{L}_\in = \{\in\}$ of set theory.

Let always c, d denote constant symbols, f, g function symbols and R, S relation symbols.

Definition 1.1.5. Suppose that $\mathcal{L}$ is a language. An $\mathcal{L}$-structure is a structure $\mathcal{M} = (M, \mathcal{F})$, where M is a nonempty set and $\mathcal{F} = \langle s^M \mid s \in \mathcal{L} \rangle$ and

1. $s^\mathcal{M} \in M$ if $c \in \mathcal{L}$ is a constant symbol,
2. $f^\mathcal{M}\colon M^k \to M$ if $f \in \mathcal{L}$ is a k-ary function symbol, and
3. $R^\mathcal{M} \subseteq M^k$ if $R \in \mathcal{L}$ is a k-ary relation symbol.

So every symbol has an interpretation as an element, function or relation in the structure.

For example, let $\mathcal{R} = (\mathbb{R}, 0^\mathcal{R}, 1^\mathcal{R}, +^\mathcal{R}, \cdot^\mathcal{R})$ denote the field of real numbers, a structure in the language $\mathcal{L}_R = \{0, 1, +, \cdot\}$ of rings. Here an otherwise, we will often confuse the structure with its underlying set and write $(\mathbb{R}, 0^\mathbb{R}, 1^\mathbb{R}, +^\mathbb{R}, \cdot^\mathbb{R})$. One can further simplify the notation to $(\mathbb{R}, 0, 1, +, \cdot)$ when it is clear that one means constants and functions rather than symbols.

The familiar notions of homomorphisms, embeddings and isomorphism of (e.g.) groups, vector spaces etc. make sense in this general setting:

Definition 1.1.6. Suppose that $\mathcal{M} = (M, \langle s^\mathcal{M} \mid s \in \mathcal{L} \rangle)$ and $\mathcal{N} = N, \langle s^\mathcal{N} \mid s \in \mathcal{L} \rangle)$ are $\mathcal{L}$-structures. By a function $h\colon \mathcal{M} \to \mathcal{N}$, we mean a function $h\colon M \to N$ on the underlying sets.

1. h is a *homomorphism* if for all $n \in \mathbb{N}$ and all $a_0, \dots, a_{n-1} \in M$:
   - (a) $h(c^\mathcal{M}) = c^\mathcal{N}$ for all constant symbols c.
   - (b) $h(f^\mathcal{M}(a_0, \cdots, a_{k-1})) = f^\mathcal{N}(h(a_0), \cdots, h(a_{k-1}))$ for all k-ary function symbols f.
   - (c) $R^\mathcal{M}(a_0, \cdots, a_{k-1}) \implies R^\mathcal{N}(h(a_0), \cdots, h(a_{k-1}))$ for all k-ary relation symbols R.
2. h is an *embedding* if it is an injective homomorphism and for all k-ary relation symbols R and $a_0, \dots, a_{k-1} \in M$,
$$R^\mathcal{M}(a_0, \cdots, a_{k-1}) \iff R^\mathcal{N}(h(a_0), \cdots, h(a_{k-1})).$$
3. h is an *isomorphism* if it is a surjective embedding.
4. h is an *automorphism* if it is an isomorphism and $\mathcal{M} = \mathcal{N}$.

The notion of subgroup, subfield etc. make sense in this general setting.

Definition 1.1.7. Suppose that $\mathcal{M} = (M, \langle s^\mathcal{M} \mid s \in \mathcal{L} \rangle)$ and $\mathcal{N} = N, \langle s^\mathcal{N} \mid s \in \mathcal{L} \rangle)$ are $\mathcal{L}$-structures.

(1) $\mathcal{M}$ is a *substructure* of $\mathcal{N}$ if $M \subseteq N$ and the identity $\mathrm{id}\colon \mathcal{M} \to \mathcal{N}$ is an embedding, i.e. for all $n \in \mathbb{N}$ and all $a_0, \dots, a_{n-1} \in M$:
   (a) $c^{\mathcal{M}} = c^{\mathcal{N}}$ for all constant symbols $c \in \mathcal{L}$.
   (b) $f^{\mathcal{M}}(a_0, \cdots, a_{k-1}) = f^{\mathcal{N}}(a_0, \cdots, a_{k-1})$ for all k-ary function symbols $f \in \mathcal{L}$.
   (c) $R^{\mathcal{M}}(a_0, \cdots, a_{k-1}) \Longleftrightarrow R^{\mathcal{N}}(a_0, \cdots, a_{k-1})$ for all k-ary relation symbols $R \in \mathcal{L}$.
(2) $\mathcal{N}$ is a *superstructure* of $\mathcal{M}$ if $\mathcal{M}$ is a substructure of $\mathcal{N}$.

One can also change a structure by adding or removing constants, functions or relations.

Definition 1.1.8. Suppose that $\mathcal{K} \subseteq \mathcal{L}$ are languages and $\mathcal{M} = (M, \langle s^{\mathcal{M}} \mid s \in \mathcal{L}\rangle)$ is an $\mathcal{L}$-structure.

(1) $M{\restriction}\mathcal{K} = (M, \langle s^{\mathcal{M}} \mid s \in \mathcal{K}\rangle)$ is called a *reduct* of $\mathcal{M}$, more precisely the *reduct* of $\mathcal{M}$ to the language $\mathcal{K}$.
(2) $\mathcal{M}$ is called an *expansion* of $\mathcal{M}{\restriction}\mathcal{K}$. In other words, $\mathcal{M}$ is an expansion of a structure $\mathcal{N}$ if $\mathcal{N}$ is a reduct of $\mathcal{M}$.

Example 1.1.9.

(1) $\mathcal{M} = (\mathbb{R}, 0^{\mathbb{R}}, 1^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, <^{\mathbb{R}})$ is an $\mathcal{L}_{OF}$-structure (in fact it is an ordered field, i.e. it satisfies the axioms of ordered fields), and $\mathcal{M}{\restriction}\mathcal{L}_R = (\mathbb{R}, 0^{\mathbb{R}}, 1^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}})$ is its reduct to the language $\mathcal{L}_R$ of rings.
(2) Suppose that $\mathcal{M} = (M, \langle s^{\mathcal{M}} \mid s \in \mathcal{L}\rangle)$ is an is an $\mathcal{L}$-structure and $A \subseteq M$. Then $\mathcal{M}_A = (M, \langle s^{\mathcal{M}} \mid s \in \mathcal{L}\rangle \cup \langle a \mid a \in A\rangle)$ is an expansion of $\mathcal{M}$ to the language $\mathcal{L}_A = \mathcal{L} \cup A$.

The structure $\mathcal{M}_A$ has the property that every homomorphism $h\colon \mathcal{M}_A \to \mathcal{M}_A$ fixes A pointwise.

We now begin with building formulas from the language/alphabet. One first builds terms, and from those, formulas. The notion of *term* generalises the notion of polynomials over $(\mathbb{Z}, 0, 1, +, \cdot)$. The terms in the language of rings are the polynomials with coefficients in $\mathbb{Z}$ in an arbitrary number of variables.

We fix a sequence $\langle v_n \mid n \in \mathbb{N}\rangle$ of variables once and for all. We will still use the notation x, y, z for variables, but this will mean that they are among the v_n.

In the following, a word with n letters from a set S is formally a function $f\colon \{0, \dots, n-1\} \to S$. If S is countable, one can assume that S is a set of natural numbers, to realise words a partial functions on $\mathbb{N}$.

Definition 1.1.10. The following words are $\mathcal{L}$-terms:

(1) Every variable v_n
(2) Every constant symbol in $\mathcal{L}$
(3) $f(t_0, \dots, t_{n-1})$, if f is an n-ary function symbol and $t_0, \dots, t_{n-1}$ are $\mathcal{L}$-terms

The $\mathcal{L}$-terms are those words generated by the rules (1)-(3).

We next list the logical symbols, that are allowed independent of the language.

Definition 1.1.11. The following symbols are called *logical symbols*:

(1) Variables $v_n \in \mathrm{Var}$
(2) The equality symbol $\doteq$
(3) The negation symbol $\neg$
(4) The disjunction symbol $\vee$
(5) The existential quantifier $\exists$
(6) The left bracket (right bracket) and comma ,[2]

$\mathcal{L}$-formulas are, informally, those words that make sense. They are built as follows.

[2] Some authors call these *auxiliary* symbols instead of logical symbols.

Definition 1.1.12. The following words are $\mathcal{L}$-formulas:

(1) $s \doteq t$, if s, t are $\mathcal{L}$-terms.
(2) $R(t_0, \ldots, t_{k-1})$, if R is a k-ary relation symbol and $t_0, \ldots, t_{k-1}$ are terms
(3) $(\neg\varphi)$, if φ is an $\mathcal{L}$-formula
(4) $(\varphi \vee \psi)$, if φ, ψ are $\mathcal{L}$-formulas
(5) $(\exists x\varphi)$, if φ is an $\mathcal{L}$-formula and x is a variable

$\mathcal{L}$-formulas are those words generated by the rules (1)-(5). Moreover, a formula is called *quantifier-free* if it is generated using only (1)-(4), and *atomic* if it is generated only from (1) and (2).

While this is the formal definition of formulas, we will always allow the usual abbreviations to simplify the notation. For example, we write $x + y$ for $+(x, y)$ or abbreviate $((x < y) \wedge (y < z))$ by $x < y < z$. We also leave out brackets when there is no danger of confusion.

Note that in the previous definition, the brackets around $\varphi\wedge\psi$ are necessary, since one could otherwise not distinguish between $\exists x(\varphi \wedge \psi)$ and $(\exists x\ \varphi) \wedge \psi$. The brackets around $\neg\varphi$ and $\exists x\varphi$ are not strictly necessary:[3] one could still prove Lemma 1.1.17, but not Lemma 1.1.15.

We will often do induction on terms. This means that we show a statement for variables and constants in the beginning of the induction, and show that it holds for $f(t_0, \ldots, t_k)$ assuming it holds for $t_0, \ldots, t_k$ in the induction step. This is a valid induction on $n \in \mathbb{N}$, since the term $f(t_0, \ldots, t_k)$ has some length n, while the subterms $t_0, \ldots, t_k$ are strictly shorter.

Induction on formulas works similarly.

The disjunction $\vee$ and the universal quantifier $\forall$ are still missing. It is convenient to introduce them as notations, rather than as a part of the language itself, since this reduces the number of cases in proofs. We will call this the *extended language*, and will always use it from now on.

Notation 1.1.13. (Extended language)

(1) $(\varphi \wedge \psi) := (\neg(\neg\varphi \vee \neg\psi))$
(2) $(\varphi \rightarrow \psi) := ((\neg\varphi) \vee \psi))$
(3) $(\varphi \leftrightarrow \psi) := ((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi))$
(4) $(\forall x\ \varphi) := (\neg(\exists x\ \neg\varphi))$
(5) $(\varphi_0 \wedge \cdots \wedge \varphi_n) := \underbrace{((((}_{n} \varphi_0 \wedge \varphi_1) \wedge \varphi_2) \cdots \wedge \varphi_n)$
(6) $(\varphi_0 \vee \cdots \vee \varphi_n) := \underbrace{((((}_{n} \varphi_0 \vee \varphi_1) \vee \varphi_2) \cdots \vee \varphi_n)$
(7) $(\exists x_0 \ldots x_n\ \varphi) := \exists x_0(\exists x_1(\ldots(\exists x_n\varphi\ \underbrace{)))}_{n}$
(8) $(\forall x_0 \ldots x_n\ \varphi) := \forall x_0(\forall x_1(\ldots(\forall x_n\varphi\ \underbrace{)))}_{n}$

The following is the usual formulation of the group axioms in the extended language, using some abbreviations.

Example 1.1.14. The group axioms are the following formulas in the language $\mathcal{L}_G$:

(1) $\forall x, y, z\ (x \cdot y) \cdot z \doteq x \cdot (y \cdot z)$
(2) $\forall x\ (x \cdot 1 \doteq 1 \cdot x \doteq x)$
(3) $\forall x\ (x \cdot x^{-1} \doteq x^{-1} \cdot x \doteq 1)$

[3] For example, there are no brackets there in Martin Ziegler's book.

Formally, a word is a sequence of symbols in a set S, or in other words, a function $f\colon \{0,\dots,n\} \to S$. If $f\colon \{0,\dots,n\} \to S$ is a word, then an *initial segment* is a restriction $f{\upharpoonright}\{0,\dots,k\}$ for some $k \leq n$. An *end segment* is defined similarly.

Lemma 1.1.15.

(1) *An $\mathcal{L}$-term cannot be a proper inital segment or end segment of another $\mathcal{L}$-term.*
(2) *An $\mathcal{L}$-formula cannot be a proper initial segment or end segment of another $\mathcal{L}$-formula.*

Proof. (1): It is a bit easier than the following argument to see this by observing that the left and right brackets in a term cancel out, so given the beginning of a term, one can uniquely determine its end. So the next argument is not necessary, but I left it here.

Recall that in $f(t_0,\dots,t_m)$, f, (,), , are symbols and the t_i are themselves words. If $f(t_0,\dots,t_m)$ is an initial segment or end segment of $g(u_0,\dots,u_n)$, then it is easy to see from the inductive hypothesis that $m = n$, $t_i = u_i$ for all $i \leq m$ and $f = g$. We only consider one case in detail, since the other cases use similar steps.

Suppose that $s = f(s_0,\dots,s_k)$ and $u = g(u_0,\dots,u_l)$ are $\mathcal{L}$-terms and s is an initial segment of u. We will see that $s = t$. Since the first symbols of s and t agree, we have $f = g$, and since f is a k-ary function symbol, so is g, and hence $k = l$. We now show by induction that $s_i = t_i$ for all $i \leq k$. Write $u \sqsubseteq v$ if u is an initial segment of v, and $u \sqsubset v$ if it is a proper initial segment. Either $s_0 \sqsubset t_0$, $t_0 \sqsubset s_0$, or $s_0 = t_0$. The first two cases are impossible by the inductive hypothesis, so $s_0 = t_0$. Moving on to the next term, we have either $s_1 \sqsubset t_1$, $t_1 \sqsubset s_1$, or $s_1 = t_1$, etc.

(2): Suppose that ψ is a proper initial segment or end segment of θ. When θ is atomic, i.e. of the form $s \doteq t$ or $R(t_0,\dots,t_n)$, then the claim follows from (1). When θ equals $(\neg\varphi)$, $(\varphi \wedge \psi)$ or $(\exists x\ \varphi)$, it is easy to see that the claim follows from the inductive hypothesis (2). □

Lecture 2
14. April

Note that we often do an induction on the length of formulas. A more interesting notion of measuring the size of terms and formulas is their *depth*, where, informally, each step in the construction of a term of formula adds 1 to their depth. All proofs would work for induction on the depth as well.

A *segment* of a word $f\colon \{0,\dots,n\} \to S$ is a connected subword g of f, i.e., there are $k, l \in \mathbb{N}$ such that $g\colon \{0,\dots,k\} \to S$, $g(i) = f(l+i)$ for all $i \leq k$.

Definition 1.1.16. A *subformula* φ of an $\mathcal{L}$-formula ψ is a segment of ψ that is itself an $\mathcal{L}$-formula. It is a *proper subformula* if additionally $\varphi \neq \psi$.

Lemma 1.1.17. [4] *All subformulas of a formula φ appear in its construction, i.e.*

(1) *Atomic formulas $s \doteq t$ and $R(t_0,\dots,t_k)$ do not have any proper subformulas.*
(2) *Any proper subformula of*
    (a) *$(\neg\varphi)$ is a subformula of φ;*
    (b) *$(\varphi \vee \psi)$ is a subformula of φ or a subformula of ψ;*
    (c) *$(\exists x\ \varphi)$ is a subformula of φ.*

Therefore, for each nonatomic formula φ, there is a unique way in which φ is built from one or two other formulas.

Proof. This follows from Lemma 1.1.15. □

The previous lemma shows that one can recover the way in which the formula was built. In particular, this shows that one has avoided ambiguous formulas such as $\exists x\ \varphi \wedge \psi$, which could have meant either $\exists x\ (\varphi \wedge \psi)$ or $(\exists x\ \varphi) \wedge \psi$

[4] This also holds for the extended language, by the same argument.

The role of variables is relevant for formal derivations later on. It is important to distinguish between *free* and *bound* variables. For example, the variable x is free in $x < y$, but is bound by the quantifier $\forall x$ in $\forall x\ x < y$.

Definition 1.1.18. An occurence of a variable x in an $\mathcal{L}$-formula θ is *free* if this occurence is not bound by a quantifier, i.e.:

(a) If θ is an atomic formula, then every occurence of x is free.
(b) If θ is the formula $(\varphi \wedge \psi)$, then an occurence of x in φ is *free* in θ if it is free in φ; the same holds for ψ.
(c) If θ is the formula $(\exists y\ \varphi)$, then an occurence of x in φ is free in θ if it is free in φ and $x \neq y$.

An occurence of a variable x in an $\mathcal{L}$-formula is *bound* if it is not free.

1.2. **Semantics.** We now define when a formula is true in a structure, i.e. the *semantics*, or meaning, of the formula in the structure. The definition takes as inputs two objects, a structure $\mathcal{M}$ and a formula φ, and outputs whether the formula holds in the structure. One writes $\mathcal{M} \models \varphi$ if φ holds in $\mathcal{M}$, i.e. $\mathcal{M}$ is a model of φ.

Note that there is a difference between formal statements and their truth within a structure (defined formally by semantics), and informal mathematical statements that describe the structure from the outside. For example, the size of an infinite structure is a property that can be seen in the mathematical universe. E.g. the field $\mathbb{C}_{\text{alg}}$ of algebraic complex numbers is countable, but the field $\mathbb{C}$ of complex numbers is uncountable. However, this cannot be expressed within the structures, since $\mathbb{C}_{\text{alg}}$ and $\mathbb{C}$ satisfy precisely the same formulas ($\mathbb{C}_{\text{alg}} \prec \mathbb{C}$ is an elementary substructure, as we will see later).

The formula $\forall x, y, z\ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$ holds in an $\mathcal{L}_G$-structure $(G, 1, \cdot, ^{-1})$, if for all $a, b, c \in G$, the formula $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ holds with the values a, b, c assigned to x, y, z, respectively. We need such assignments for giving a recursive definition of validity of a formula in a structure.

Let $\text{Var} = \{v_n \mid n \in \mathbb{N}\}$ always denote our fixed set of variables.

Definition 1.2.1. An *assignment* (of variables) for a structure $\mathcal{M} = (M, \mathcal{F})$ is a function $\xi\colon \text{Var} \to M$.

Definition 1.2.2. Suppose $\mathcal{M} = (M, \mathcal{F})$ is an $\mathcal{L}$-structure and ξ is an assignment for $\mathcal{M}$. We define $t^{\mathcal{M},\xi}$ by induction on $\mathcal{L}$-terms:

(1) $c^{\mathcal{M},\xi} = c^{\mathcal{M}}$, if $c \in \mathcal{L}$ is a constant symbol
(2) $v_i^{\mathcal{M},\xi} = \xi(v_i)$ for all variables v_i
(3) $f(t_0, \ldots, t_{k-1})^{\mathcal{M},\xi} = f^{\mathcal{M}}(t_0^{\mathcal{M},\xi}, \ldots, t_{k-1}^{\mathcal{M},\xi})$ if f is a k-ary function symbol

Example 1.2.3. For $\mathcal{L} = \{0, 1, +, \cdot\}$, $(\mathbb{Q}, 0^{\mathbb{Q}}, 1^{\mathbb{Q}}, +^{\mathbb{Q}}, \cdot^{\mathbb{Q}})$, the polynomial $t = (v_0 \cdot v_0) + (v_1 \cdot v_2)$ and the assignment $\xi(v_i) = i + 2$, we have $t^{\mathcal{M},\xi} = 16$.

Lemma 1.2.4. *Suppose $\mathcal{M} = (M, \mathcal{F})$ is an $\mathcal{L}$-structure and t is an $\mathcal{L}$-term. Then $t^{\mathcal{M},\xi}$ depends only on the values $\xi(v_i)$ for variables v_i that appear in t.*

Proof. This is immediate, since the value $\xi(v_i)$ appears in the definition of $t^{\mathcal{M},\xi}$ only if v_i appears in t.

More formally, we show by induction on $\mathcal{L}$-terms t that for assignments ξ and ζ for $\mathcal{M}$ such that $\xi(v_i) = \zeta(v_i)$ for all variables v_i that appear in t, we have $t^{\mathcal{M},\xi} = t^{\mathcal{M},\zeta}$:

(1) For variables v_n, $v_n^{\mathcal{M},\xi} = \xi(v_n) = \zeta(v_n) = v_n^{\mathcal{M},\zeta}$.
(2) For constants c, $c^{\mathcal{M},\xi} = c^{\mathcal{M}} = c^{\mathcal{M},\zeta}$.
(3) If $f \in \mathcal{L}$ is a k-ary function symbol and $t_0, \ldots, t_{k-1}$ are terms, then $f(t_0, \ldots, t_{k-1})^{\mathcal{M},\xi} = f(t_0^{\mathcal{M},\beta}, \ldots, t_{k-1}^{\mathcal{M},\xi}) = f(t_0^{\mathcal{M},\zeta}, \ldots, t_{k-1}^{\mathcal{M},\zeta} = f(t_0, \ldots, t_{k-1})^{\mathcal{M},\zeta}$ by the inductive hypothesis.

□

Notation 1.2.5.

(1) If t is an $\mathcal{L}$-term, we write $t = t(x_0, \dots, x_{n-1})$ if $x_0, \dots, x_{n-1}$ lists all variables in t in the order of their first appearance in φ.

(2) For an $\mathcal{L}$-term $t = t(x_0, \dots, x_{n-1})$ and an assignment ξ for $\mathcal{M}$ with $\xi(x_i) = a_i$ for $i < n$, we write $t^{\mathcal{M}, a_0, \dots, a_{n-1}}$ for $t^{\mathcal{M}, \xi}$.

To define when a formula is true in a structure, we will need to inductively add more values to an assignment:

Definition 1.2.6. Suppose that ξ is an assignment for $\mathcal{M} = (M, \mathcal{F})$, x is a variable and $a \in M$. The assignment $\xi\frac{a}{x}$ is defined by

$$\xi\frac{a}{x}(y) = \begin{cases} a & \text{if } x = y \\ \xi(y) & \text{if } x \neq y. \end{cases}.$$

Here is the definition of truth in a structure, just as you would expect:

Definition 1.2.7. Suppose that ξ is an assignment for an $\mathcal{L}$-structure $\mathcal{M} = (M, \mathcal{F})$. We define the statement φ *holds in* $\mathcal{M}$ *for* ξ, written as $\mathcal{M} \models \varphi[\xi]$, by induction on $\mathcal{L}$-formulas φ:

(1) $\mathcal{M} \models s \doteq t\ [\xi] \iff s^{\mathcal{M}, \xi} = t^{\mathcal{M}, \xi}$.

(2) $\mathcal{M} \models R(t_0, \dots, t_k)[\xi] \iff R^{\mathcal{M}}(t_0^{\mathcal{M}, \xi}, \dots, t_k^{\mathcal{M}, \xi})$.

(3) $\mathcal{M} \models (\neg\psi)[\xi] \iff \mathcal{M} \not\models \psi[\xi]$.

(4) $\mathcal{M} \models (\psi \vee \theta)[\xi] \iff \mathcal{M} \models \psi[\xi]$ or $\mathcal{M} \models \theta[\xi]$.

(5) $\mathcal{M} \models (\exists x\ \psi)[\xi] \iff \exists a \in M\ \mathcal{M} \models \psi[\xi\frac{a}{x}]$.

1.3. **Elementary substructures.** The notion of substructure was introduced in Definition 1.1.7 above. The next lemma shows that every structure has a smallest substructure.

Lemma 1.3.1. *Suppose that $\mathcal{N} = (N, \langle s^{\mathcal{N}} \mid s \in \mathcal{L}\rangle)$ is an $\mathcal{L}$-structure and $A \subseteq M$. The following conditions are equivalent:*

(a) *There is a substructure $\mathcal{A}$ of $\mathcal{N}$ of the form $\mathcal{A} = (A, \langle s^{\mathcal{A}} \mid s \in \mathcal{L}\rangle)$.*

(b) *For any $a_0, \dots, a_n \in A$ and all $\mathcal{L}$-terms $t = t(x_0, \dots, x_n)$, we have $t^{\mathcal{N}, a_0, \dots, a_n} \in A$.*

Assuming that $\mathcal{L}$ contains at least one constant symbol,[5] *it follows that there is a ($\subseteq$-)least substructure of $\mathcal{N}$, and its domain is $\{t^{\mathcal{N}, a_0, \dots, a_n} \mid t(x_0, ..., x_n)$ is an $\mathcal{L}$-Term and $a_0, \dots, a_n \in A\}$.*

Proof. Exercise □

A substructure can have very different properties than the original structure. For instance $(\mathbb{Z}, 0^{\mathbb{Z}}, 1^{\mathbb{Z}}, +^{\mathbb{Z}}, \cdot^{\mathbb{Z}})$ is a substructure of $(\mathbb{R}, 0^{\mathbb{R}}, 1^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}})$, so a substructure of a field is not necessarily a field. The next definition describes a more useful notion.

We here already use the notation $\mathcal{M} \models \varphi[a]$ that is only introduced after Lemma 1.3.4 below.

Definition 1.3.2. Suppose that $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$-structures.

(1) $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$, written as $\mathcal{M} \prec \mathcal{N}$, if $M \subseteq N$ and for all $a_0, \dots, a_{n-1} \in M$ and all $\mathcal{L}$-formulas φ with n free variables

$$\mathcal{M} \models \varphi[a_0, \dots, a_{n-1}] \iff \mathcal{N} \models \varphi[a_0, \dots, a_{n-1}].$$

(2) An $\mathcal{L}$-*sentence* is an $\mathcal{L}$-formula without free variables.

[5] Recall that structures are by definition nonempty. If $\mathcal{L}$ does not contain constant symbols, then the following set is empty.

(3) $\mathcal{M}$ and $\mathcal{N}$ are called *elementary equivalent* if for all $\mathcal{L}$-sentences φ,

$$\mathcal{M} \models \varphi \iff \mathcal{N} \models \varphi.$$

Example 1.3.3.

(1) Every substructure of a complete graph (i.e., there is an edge between any two vertices) is itself a complete graph. If both are infinite, it is also an elementary substructure. (We will prove this later in the lecture.)
(2) $(\mathbb{Z}, \leq^{\mathbb{Z}})$ is a substructure of $(\mathbb{Q}, \leq^{\mathbb{Q}})$, but not an elementary substructure. (Consider the formula $\exists x\ \exists y\ (\forall z(x \not\leq z \wedge z \not\leq y) \wedge x \leq y \wedge x \neq y)$.)
(3) $(2\mathbb{N}, +^{\mathbb{N}}, 0^{\mathbb{N}})$ is not an elementary substructure of $(\mathbb{N}, +^{\mathbb{N}}, 0^{\mathbb{N}})$. (We can look at the notion of evenness $(\exists y\ x = y + y)$. In $\mathbb{N}$, $1 + 1$ is even, but this fails in $2\mathbb{N}$.)
(4) $(\mathbb{Q}, \leq^{\mathbb{Q}})$ is an elementary substructure of $(\mathbb{R}, \leq^{\mathbb{R}})$. (We will prove this later in the lecture.)

Lecture 3
19. April

The next lemma was already used in Definition 1.3.2.

Lemma 1.3.4. *If ξ, ζ are assignments for an $\mathcal{L}$-structure $\mathcal{M}$ such that $\xi(v_i) = \zeta(v_i)$ for all variables v_i that are free in φ, then*

$$\mathcal{M} \models \varphi[\xi] \iff \mathcal{M} \models \varphi[\zeta].$$

If $x_0, \dots, x_n$ are the free variables of φ and $\xi(x_i) = a_i$ for all $i \leq n$, we can therefore write $\mathcal{M} \models \varphi[a_0, \dots, a_n]$ instead of $\mathcal{M} \models \varphi[\xi]$. If φ has no free variables, we simply write $\mathcal{M} \models \varphi$.

Proof. This is immediate because only the values of variables occuring in φ appear in the inductive definition of $\mathcal{M} \models \varphi[\xi]$.

In more detail, we do an induction on formulas φ. The induction hypothesis states that the claim holds for φ for all assignments. If $R \in \mathcal{L}$ is an n-ary relation symbol, $t_0, \dots, t_n$ are $\mathcal{L}$-terms and $\varphi = R(t_0, \dots, t_n)$, then

$$\mathcal{M} \models \varphi[\xi] \iff R^{\mathcal{M}}(t_0^{\mathcal{M},\xi}, \dots, t_n^{\mathcal{M},\xi}) \iff R^{\mathcal{M}}(t_0^{\mathcal{M},\zeta}, \dots, t_n^{\mathcal{M},\zeta}) \iff \mathcal{M} \models \varphi[\zeta].$$

The cases $s \doteq t$, $(\neg\psi)$ and $(\psi \wedge \theta)$ are similar. If $\varphi = (\exists x\ \psi)$, then

$$\mathcal{M} \models \varphi[\xi] \iff \exists a \in M\ \mathcal{M} \models \psi[\xi\frac{a}{x}] \iff \exists a \in M\ \mathcal{M} \models \psi[\zeta\frac{a}{x}] \iff \mathcal{M} \models \varphi[\zeta].$$

□

Example 1.3.5. For each $n \in \mathbb{N}$, there is a sentence φ such that $\mathcal{M} = (M, \mathcal{F}) \models \varphi$ if and only if $|M| = n$. E.g. for $n = 3$, let φ be the sentence $\exists x_0, x_1, x_2\ (x_0 \neq x_1 \wedge x_0 \neq x_2 \wedge x_1 \neq x_2 \wedge \forall y\ (y \doteq x_0 \vee y \doteq x_1 \vee y \doteq x_2))$.

Hence a finite structure does not have proper elementary substructures.

Example 1.3.6. If $\mathcal{M} = (M, <^{\mathcal{M}})$ is an elementary substructure of $\mathcal{N} = (\mathbb{N}, <^{\mathbb{N}})$, then $\mathcal{M} = \mathcal{N}$.

Proof. We show $n \in M$ for all $n \in \mathbb{N}$ by induction on n.

To see that $0 \in M$, note that the statement $\exists y \neg\exists x\ (x < y)$ holds in $\mathcal{N}$ and thus it also holds in $\mathcal{M}$. So there is some $a \in M$ with $\mathcal{M} \models \neg\exists x\ (x < y)[a]$. Since $\mathcal{M} \prec \mathcal{N}$, we also have $\mathcal{N} \models \neg\exists x\ (x < y)[a]$. Thus a is the $<^{\mathbb{N}}$-least element of $\mathbb{N}$, i.e. $a = 0$. So $0 = a \in M$.

Now assume that $n \in M$. We have $\mathcal{N} \models \exists z > x\ \neg\exists y(x < y < z))[n]$ (this formula is an abbreviation for $\exists z(z > x \wedge \neg\exists y((x < y) \wedge (z < x)))$). A similar argument as for 0 shows that $n + 1 \in N$. □

Analogous to the notation for terms in Notation 1.2.5, we write $\varphi(x_0, \dots, x_n)$ if $x_0, \dots, x_n$ are precisely the free variables of φ, listed by the first appearance in φ.

Lemma 1.3.7 (Tarski's test). *Suppose that $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$-structures. The following conditions are equivalent:*

(1) *$\mathcal{M}$ is an elementary substructure of $\mathcal{M}$, i.e. $\mathcal{M} \prec \mathcal{N}$.*
(2) *$\mathcal{M}$ is a substructure of $\mathcal{N}$, and for all $\mathcal{L}$-formulas $\varphi(x, x_0, \ldots, x_n)$ and all $a_0, \ldots, a_n \in M$:*

If there is some $b \in N$ with $\mathcal{N} \models \varphi[b, a_0, \ldots, a_n]$,
then there is some $a \in M$ with $\mathcal{N} \models \varphi[a, a_0, \ldots, a_n]$.

Proof. (1)⇒(2): If $\mathcal{N} \models \varphi[b, a_0, \ldots, a_n]$, then $\mathcal{N} \models \exists x\ \varphi(x, x_0, \ldots, x_n)[a_0, \ldots, a_n]$. Since $M \prec N$, there is some $a \in M$ with $\mathcal{M} \models \varphi[a, a_0, \ldots, a_n]$. Since $M \prec N$, we have $\mathcal{N} \models \varphi[a, a_0, \ldots, a_n]$.

(2)⇒(1): By induction on formulas φ. The cases $\vee$ and $\neg$ are easy.

For the existential case, first suppose that $\varphi = \varphi(x, x_0, \ldots, x_n)$ and $\mathcal{M} \models \exists x\ \varphi[a_0, \ldots, a_n]$. Then there is some $a \in M$ with $\mathcal{M} \models \varphi[a, a_0, \ldots, a_n]$. By the inductive hypothesis for φ, $\mathcal{N} \models \varphi[a, a_0, \ldots, a_n]$.

Now suppose that $\mathcal{N} \models \exists x\ \varphi\ [a_0, \ldots, a_n]$. By (2), there is some $a \in M$ with $\mathcal{N} \models \varphi[a, a_0, \ldots, a_n]$. By the inductive hypothesis for φ, we have $\mathcal{M} \models \varphi[a, a_0, \ldots, a_n]$. So $\mathcal{M} \models \exists x\ \varphi\ [a_0, \ldots, a_n]$.

□

Homomorphisms (see Definition 1.1.6) preserve interpretations of terms:

Lemma 1.3.8. *Suppose that $\mathcal{M} = (M, \mathcal{F})$, $\mathcal{N} = (N, \mathcal{G})$ are $\mathcal{L}$-structures and $h \colon \mathcal{M} \to \mathcal{N}$ is a homomorphism. Then for any term $t = t(x_0, \ldots, x_n)$ and all $a_0, \ldots, a_n \in M$,*

$$h(t^{\mathcal{M}, a_0, \ldots, a_n}) = t^{\mathcal{N}, h(a_0), \ldots, h(a_n)}.$$

Proof. Exercise in the tutorials. □

Isomorphisms preserve the truth of formulas:

Lemma 1.3.9. *Suppose that $\mathcal{M} = (M, \mathcal{F})$, $\mathcal{N} = (N, \mathcal{G})$ are $\mathcal{L}$-structures and $h \colon \mathcal{M} \to \mathcal{N}$ is an isomorphism. Then for any formula $\varphi = \varphi(x_0, \ldots, x_n)$ and all $a_0, \ldots, a_n \in M$,*

$$\mathcal{M} \models \varphi[a_0, \ldots, a_n] \Longleftrightarrow \mathcal{N} \models \varphi[h(a_0), \ldots, h(a_n)].$$

Proof. Homework exercise. □

1.4. **Theories and axioms.**

One often wants to derive results about a structure from *axioms.* A set of $\mathcal{L}$-sentences (formulas with no free variables) is called a *theory.* The sentences in a theory T are often called axioms and T is called an axiom system.

Definition 1.4.1. One says that an $\mathcal{L}$-structure $\mathcal{M}$ *satisfies* an $\mathcal{L}$-theory T, or $\mathcal{M}$ is a *model* of T, in symbols $\mathcal{M} \models T$, if $\mathcal{M} \models \varphi$ for all $\varphi \in T$.

Given an axiom system T, we can ask:

(1) (Syntactic) Which formulas are provable from T? This will be made precise using a proof calculus in Section 1.5.
(2) (Semantic) Which formulas does T imply? (See Definition 1.4.7.) This is equivalent to the previous question by Gödel's proof of the completeness of the proof calculus in chapter 3.

Which models does T have? We study this question throughout the lecture. We have already looked at the notion of elementary substructure, where one has two structures with the same theory. The question how many models (of a given size) T has is also connected with incompleteness of T, since an axiom system that implies neither φ nor $\neg\varphi$ has some models that satisfy φ and some that don't.

We now look at some examples of theories. *Peano arithmetic* is an axiom system in the language $\mathcal{L}_{\text{Arith}} = \{0, S, +, \cdot\}$ of arithmetic that holds in the structure $(\mathbb{N}, 0^{\mathbb{N}}, S^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}})$ of the natural numbers, where $S^{\mathbb{N}}$ denotes the successor function.

Example 1.4.2. (Peano Arithmetic) PA consists of the axioms:

(1) $\forall x\ (S(x) \neq 0)$
(2) $\forall x, y\ (S(x) \doteq S(y) \to x \doteq y)$
(3) $\forall x, y\ (x + 0 \doteq x)$
(4) $\forall x, y\ (S(x + y) \doteq x + S(y))$
(5) $\forall x, y\ (x \cdot 0 \doteq 0)$
(6) $\forall x, y\ (x \cdot S(y) \doteq x \cdot y + x)$
(7) (Axiom scheme of induction) If $\varphi(x, \vec{y})$ is an $\mathcal{L}_{\text{Arith}}$-formula, then

$$\forall \vec{y}\ (\varphi(0, \vec{y}) \wedge \forall x\ [\varphi(x, \vec{y}) \to \varphi(S(x), \vec{y})]) \to \forall x\ \varphi(x, \vec{y}).$$

(The axioms (1)-(6) together with the axiom $\forall y\ (y = 0 \vee \exists x\ (S(x) = y))$, which follows from PA , are called Robinson Arithmetic.)

Note that PA consists of infinitely many axioms. (By a theorem of Ryll-Nardzewski, one cannot axiomatise PA with only finitely many axioms.)

Every model of PA satisfies statements about $+$ and $\cdot$ that can be proved by induction, for example division with remainder.

Example 1.4.3. The following statements hold in every model of PA:

(1) $\forall y\ (y = 0 \vee \exists x\ (S(x) = y))$
(2) $\forall x, y, z\ ((x + y) + z = x + (y + z))$
(3) $\forall x, y\ (x + y = y + x)$

In the case of PA, the axioms aim to describe a single structure. Other axioms, e.g. the group axioms, aim to describe a class of structures.

By a class, we mean the collection of all objects with a certain property, for example the class of all sets or the class of all groups. This will be studied in more detail in the next chapter.

Definition 1.4.4. For a class $\mathcal{C}$ of $\mathcal{L}$-structures, an $\mathcal{L}$-theory T is called an *axiomatisation* of $\mathcal{C}$ in $\mathcal{L}$ if $\mathcal{C}$ is the class of $\mathcal{L}$-structures $\mathcal{M}$ with $\mathcal{M} \models T$. If such a axiomatisation in $\mathcal{L}$ (resp., finite axiomatisation in $\mathcal{L}$) exists, $\mathcal{C}$ is called *axiomatisable in $\mathcal{L}$ (resp., finitely axiomatisable in $\mathcal{L}$)*

Note that some classes of $\mathcal{L}$-structures are not axiomatisable in $\mathcal{L}$, but axiomatisable as reducts by a theory T' in an extended language $\mathcal{L}' \supseteq \mathcal{L}$ in the following sense: The class $\mathcal{C}$ consist of precisely those $\mathcal{L}$-structures $\mathcal{M}$ such that there exists an expansion of $\mathcal{M}$ to an $\mathcal{L}'$-structure $\mathcal{M}'$ with $\mathcal{M}' \models T'$. In other words, the structures in $\mathcal{C}$ are precisely the reducts of those $\mathcal{L}'$-structures that satisfy the theory T'.

(14 June) To clarify, we will always say:
(1) A class $\mathcal{C}$ of $\mathcal{L}$-structures is axiomatisable in $\mathcal{L}$, or
(2) A class $\mathcal{C}$ of $\mathcal{L}$-structures is axiomatisable by language extension. This means that $\mathcal{C}$ is the class of reducts of models of an $\mathcal{L}'$-theory T' in some $\mathcal{L}' \supseteq \mathcal{L}$.

Here are examples of axiomatisations of various classes of structures.

Example 1.4.5.

(1) For any language $\mathcal{L}$ and any $n \in \mathbb{N}$ with $n \geq 1$, the class $\mathcal{C}_{\leq n}$ of $\mathcal{L}$-structures with at most elements is axiomatised by the axiom

$$\varphi_{\leq n} = \exists x_0 \ldots \exists x_{n-1}\ \forall y\ \bigvee_{i=0}^{n-1} y \doteq x_i.$$[6]

[6] This is an abbreviation for $y = x_0 \vee \cdots \vee y = x_n$.

Similarly, the class $\mathcal{C}_{\geq n}$ of $\mathcal{L}$-structures with at least elements can be axiomatised in the empty language by the axiom

$$\varphi_{\geq n} = \exists x_0 \dots \exists x_{n-1} \bigwedge_{i<j\leq n-1} \neg(x_i \doteq x_j).$$

(2) For any language $\mathcal{L}$, the class $\mathcal{C}_\infty$ of infinite $\mathcal{L}$-stuctures is axiomatised by the theory

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

We will see later that $\mathcal{C}_\infty$ has no finite axiomatisation in the empty language.

Let $\mathcal{C}_{\text{fin}}$ denote the class of finite $\mathcal{L}$-structures. We will see later that $\mathcal{C}_{\text{fin}}$ cannot be axiomatised in any language.

(3) The class of (symmetric) graphs $\mathcal{G} = (G, E^{\mathcal{G}})$ with no cycles is axiomatised in the language $\mathcal{L} = \{E\}$ with a single binary relation symbol by

$$T = \{\varphi\} \cup \{\varphi_n \mid n \in \mathbb{N}\},$$

where $\varphi = (\forall x, y\ (E(x,y) \to E(y,x)))$ and $\varphi_n = (\forall x_0, \dots, x_n(x_0 = x_n \to \neg \bigwedge_{i<n} E(x_i, x_{i+1}))$.

Lecture 4
21. April

Definition 1.4.6. The *theory* $\mathrm{Th}(\mathcal{M})$ of an $\mathcal{L}$-structure $\mathcal{M}$ is defined as the set of $\mathcal{L}$-sentences φ with $\mathcal{M} \models \varphi$.

We already introduced $\models$ for truth of a formula in a model (with an assignment). One also writes $\models$ for (semantical) implication:

Definition 1.4.7. Suppose that T is an $\mathcal{L}$-theory and φ is an $\mathcal{L}$-formula.

T (semantically) *implies* φ, written as $T \models_{\mathcal{L}} \varphi$, if every model of T, with any assignment, is a model of φ.

Moreover $\models_{\mathcal{L}} \varphi$ means that φ is *universally valid*, or *universally true*, i.e. φ holds in any $\mathcal{L}$-structure with any assignment.

A first observation is that implication does not depend on the language.

Lemma 1.4.8. *Suppose that $\mathcal{K} \subseteq \mathcal{L}$ are languages, T is a $\mathcal{K}$-theory and φ is a $\mathcal{K}$-formula. Then*

$$T \models_{\mathcal{K}} \varphi \Longleftrightarrow T \models_{\mathcal{L}} \varphi.$$

Proof. For any $\mathcal{K}$-structure $\mathcal{M}$ and any assignment ξ for $\mathcal{M}$, we have $\mathcal{M} \models \varphi[\xi] \Longleftrightarrow \mathcal{M}{\restriction}\mathcal{K} \models \varphi[\xi]$. This is because only symbols in $\mathcal{K}$ are actually used. It is an easy induction on formulas, similar to Lemma 1.3.4.

We can assume that φ is an $\mathcal{K}$-sentence by replacing a formula φ with free variables $x_0, \dots, x_n$ by $\forall x_0, \dots, x_n\ \varphi$.

First suppose that $T \models_{\mathcal{K}} \varphi$. If $\mathcal{M}$ is an $\mathcal{L}$-structure with $\mathcal{M} \models T$, then $\mathcal{M}{\restriction}\mathcal{K} \models T$ by the remark in the beginning of the proof. Hence $\mathcal{M}{\restriction}\mathcal{K} \models \varphi$ and $\mathcal{M} \models \varphi$

Now suppose that $T \models_{\mathcal{L}} \varphi$. If $\mathcal{M}$ is an $\mathcal{K}$-structure with $\mathcal{M} \models T$, take any $\mathcal{L}$-structure $\mathcal{N}$ expanding $\mathcal{M}$, i.e. with arbitrary interpretations of the new symbols. (Here we use that $M \neq \emptyset$, since all structures are nonempty by definition.) Then $\mathcal{N} \models T$ by the above remark. Hence $\mathcal{N} \models \varphi$ and $\mathcal{M} = \mathcal{N}{\restriction}\mathcal{K} \models \varphi$. □

Note that a formula $\varphi(x_0, \dots, x_n)$ is universally valid if and only if its universal closure $\forall x_0, \dots, x_n\ \varphi(x_0, \dots, x_n)$ is universally valid.

To study e.g. the class of all groups, one want to determine which $\mathcal{L}_G$-sentences are implied by the group axioms. It is useful to study universal truths, since the implication from φ to ψ is equivalent to universal truth of $\varphi \to \psi$.

1.5. **Universal truths and the Hilbert calculus.** A universal truth is an $\mathcal{L}$-formula that is true in any $\mathcal{L}$-structure for any assignment of variables. We will collect several kinds of universal truths and will then build up a proof calculus from them.

It is easy to check that $\varphi \to \varphi$ and $(\varphi \wedge \psi) \vee (\neg\varphi) \vee (\neg\psi)$ universally valid. More generally, for any *Boolean combination* of formulas $\varphi_0, \ldots, \varphi_n$ using $\vee, \neg, \wedge$ and $\to$, the truth of a combination in a model $\mathcal{M}$ depends only on the truth values of $\varphi_0, \ldots, \varphi_n$ in $\mathcal{M}$. (This is easy to see from the definition of $\mathcal{M} \models \varphi$.)

Propositional logic studies this. To define propositional formulas, we fix a countably infinite set $\mathbb{P}$, i.e. with one element for each natural number, whose elements we call *propositional variables*. For example, $p \to p$ for $p \in \mathbb{P}$ is a propositional formula and $\varphi \to \varphi$ is a $\mathcal{L}$-formula obtained by replacing p by φ in $p \to p$. A propositional formula can be understood as a string of symbols, but this does not fit into the framework of languages studied above, and propositional variables are not logical variables as studied above.

Definition 1.5.1.

(1) *Propositional formulas* are formal *Boolean combinations* of propositional variables $p \in \mathbb{P}$, i.e. they are generated as follows:
   (a) Each $p \in \mathbb{P}$ is a propositional formula.
   (b) If p and q are propositional formulas, then $(p \vee q)$ is a propositional formula.
   (c) If p is a propositional formula, then $(\neg p)$ is a propositional formula.

(2) A *propositional assignment* is an arbitrary function $\mu \colon \mathbb{P} \to \{0, 1\}$, where 1 stands for *true* and 0 for *false*. μ can be extended to a function on all propositional formulas by letting
   (a) $\mu(\neg q) = 1$ if $\mu(q) = 0$, and $\mu(\neg q) = 0$ otherwise;
   (b) $\mu(q \vee r) = 1$ if $(\mu(q) = 1$ or $\mu(r) = 1)$, and $\mu(q \vee r) = 0$ otherwise.

(3) A propositional formula p is called a *propositional tautology* if $\mu(p) = 1$ holds for all propositional assignments μ for p.

We also use the abbreviations $(p \wedge q) = \neg((\neg p) \vee (\neg q))$ and $(p \to q) = ((\neg p) \vee q)$. Using (2), one obtains

(a) $\mu(p \wedge q) = 1$ iff $(\mu(p) = 1$ and $\mu(q) = 1)$.
(b) $\mu(p \to q) = 1$ iff $(\mu(p) = 0$ or $\mu(q) = 1)$.

Example 1.5.2. For all propositional variables p and q, the propositional formulas $(p \to p)$ and $((p \wedge (p \to q)) \to q)$ are propositional tautologies.

Definition 1.5.3. A *tautology* is an $\mathcal{L}$-formula that is obtained from a propositional tautology p by replacing each propositional variable p_n in p by an $\mathcal{L}$-formula φ_n.

Lemma 1.5.4. *(Tautologies) All tautologies are universally valid.*

Proof. Suppose that φ is a tautology that arises from a Boolean combination p of propositional variables $p_0, \ldots, p_n$ by replacing p_i by the $\mathcal{L}$-formula φ_i for all $i \leq n$. Suppose further that $\mathcal{M}$ is an $\mathcal{L}$-structure and ξ is an assignment for $\mathcal{M}$.

We consider the truth values of subformulas of φ in $\mathcal{M}$ for ξ. If we choose the components p_i as true or false according to these truth values, the truth of subformulas of φ in $\mathcal{M}$ for ξ will correspond to the values of the corresponding propositional subformulas of p. This is because the inductive definition of μ corresponds to the inductive definition of $\mathcal{M} \models \varphi$.

In more detail, we define $\mu(p_i) = 1 \iff \mathcal{M} \models \varphi_i[\xi]$ for $i \leq n$ and let $\mu(q)$ be arbitrary for all other propositional variables q. Using Definitions 1.2.7 and 1.5.1, we see by induction on Boolean combinations that $\mathcal{M} \models \varphi[\xi] \iff \mu(p) = 1$. Since p is a propositional tautology, $\mathcal{M} \models \varphi[\xi]$. □

We will allow tautologies as basic steps in the proof calculus. Note that some authors fix a finite list of tautologies and derive all other ones from them using a proof calculus, see for instance [1, Page 11]. But then even proof of simple statements such as $\varphi \to \varphi$ can be quite complicated, see [1, Page 14].

We next consider universal truths about equality. The next lemma is immediate.

Lemma 1.5.5. *(Axioms of equality) The following $\mathcal{L}$-sentences are universally valid.*

(1) *(Reflexivity)* $\forall x\ x \doteq x$
(2) *(Symmetry)* $\forall x, y\ (x \doteq y \to y \doteq x)$
(3) *(Transitivity)* $\forall x, y\ (x \doteq y \wedge y \doteq z \to x \doteq z)$
(4) *(Congruence for functions) For all n-ary relation symbols f,*

$$\forall x_0, \dots x_n, y_0, \dots, y_n\ ((x_0 \doteq y_0 \wedge \cdots \wedge x_n \doteq y_n) \to f(x_0, \dots, x_n) \doteq f(y_0, \dots, y_n)).$$

(5) *(Congruence for relations) For all n-ary relation symbols R,*

$$\forall x_0, \dots x_n, y_0, \dots, y_n\ ((x_0 \doteq y_0 \wedge \cdots \wedge x_n \doteq y_n) \to (R(x_0, \dots, x_n) \leftrightarrow R(y_0, \dots, y_n))).$$

The next three lemmas collect ways to generate universal truths.

Lemma 1.5.6. *(Modus ponens) If φ and $\varphi \to \psi$ are universally valid formulas, then ψ is a universally valid formula.*

Proof. Suppose that ξ is an assignment for $\mathcal{M}$. Then both φ and $\varphi \to \psi$ hold in $\mathcal{M}$ for ξ. Recall that $\varphi \to \psi$ is defined as $(\neg\varphi) \vee \psi$, so we have $\mathcal{M} \not\models \varphi[\xi]$ or $\mathcal{M} \models \psi[\xi]$ □

The modus tollens states that if $\neg\psi$ and $\varphi \to \psi$ are universally valid, then $\neg\varphi$ is universally valid. This can be found by using the tautology $(\varphi \to \psi) \longrightarrow (\neg\psi \to \neg\varphi)$ and applying the modus ponens twice.

Lemma 1.5.7. *($\exists^{\to}$ introduction) If $\varphi \to \psi$ is a universally valid formula and x is not free in ψ, then $(\exists x \varphi) \to \psi$ is an universally valid formula.*

Proof. If $\mathcal{M} \models (\exists x \varphi)[\xi]$, then there is some $a \in M$ with $\mathcal{M} \models \varphi[\xi\frac{a}{x}]$. Since $\varphi \to \psi$ is universally valid, we have $\mathcal{M} \models \psi[\xi\frac{a}{x}]$, so $\mathcal{M} \models \psi[\xi]$ by Lemma 1.3.4. □

The next, and final, ${}^{\to}\exists$-*axiom* states that certain implications of the form

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

are universally valid. Here $\varphi\frac{s}{x}$ means that all free occurences of the variable x in φ are replaced by the term s. Although this definition is clear, we give the full recursive definition in the following, since this definition is used in the next lemmas.

Definition 1.5.8. Suppose that s, t are $\mathcal{L}$-terms and x is a variable. The term $t\frac{s}{x}$ is defined by replacing all occurences of x by s. More formally, define by induction on t:

(1) For $y \in \mathrm{Var}$, $y\frac{s}{x} = \begin{cases} s \text{ if } x = y \\ y \text{ otherwise} \end{cases}$
(2) For constants $c \in \mathcal{L}$, $c\frac{s}{x} = c$.
(3) If $f \in \mathcal{L}$ is an n-ary function symbol and $t_0, \dots, t_{n-1}$ are $\mathcal{L}$-terms, then $f(t_0, \dots, t_{n-1})\frac{s}{x} = f(t_0\frac{s}{x}, \dots, t_{n-1}\frac{s}{x})$.

Suppose that φ is an $\mathcal{L}$-formula, x is a variable and s is an $\mathcal{L}$-term. The formula $\varphi\frac{s}{x}$ is defined by replacing all free occurences of x by s. More formally, define by induction on φ:

(1) $(u \doteq v)\frac{s}{x} = (u\frac{s}{x} \doteq v\frac{s}{x})$ and $R(t_0, \dots, t_n)\frac{s}{x} = R(t_0\frac{s}{x}, \dots, t_n\frac{s}{x})$ for terms $u, v, t_0, \dots, t_n$.
(2) $(\neg\psi)\frac{s}{x} = (\neg(\psi\frac{s}{x}))$.
(3) $(\psi \wedge \theta)\frac{s}{x} = (\psi\frac{s}{x}) \wedge (\theta\frac{s}{x})$.

(4) $(\exists y\ \psi)\frac{s}{x} = \begin{cases} \exists y\ (\psi\frac{s}{x}) \text{ if } x \neq y \\ \exists y\ \psi \text{ if } x = y. \end{cases}$.

The next lemma shows that the interpretation of $t\frac{s}{x}$ can be found by interpreting t, but changing the value at x.

Lecture 5
26. April

Lemma 1.5.9. *(Substitution for terms) For any $\mathcal{L}$-term t and any assignment ξ for an $\mathcal{L}$-structure $\mathcal{M}$,*

$$(t\frac{s}{x})^{\mathcal{M},\xi} = t^{\mathcal{M},(\xi\frac{s^{\mathcal{M},\xi}}{x})}.$$

Proof. By induction on terms.

We have $(x\frac{s}{x})^{\mathcal{M},\xi} = s^{\mathcal{M},\xi} = x^{\mathcal{M},\xi\frac{s^{\mathcal{M},\xi}}{x}}$, if $y \neq x$ is a variable then $(y\frac{s}{x})^{\mathcal{M},\xi} = \xi(y) = y^{\mathcal{M},(\xi\frac{s^{\mathcal{M},\xi}}{x})}$ and if $c \in \mathcal{L}$ is a constant then $(c\frac{s}{x})^{\mathcal{M},\xi} = c^{\mathcal{M}} = c^{\mathcal{M},\xi\frac{s^{\mathcal{M},\xi}}{x}}$.

Moreover, $f(t_0\frac{s}{x},\dots,t_n\frac{s}{x})^{\mathcal{M},\xi} = f^{\mathcal{M}}((t_0\frac{s}{x})^{\mathcal{M},\xi},\dots,(t_n\frac{s}{x})^{\mathcal{M},\xi}) = f^{\mathcal{M}}(t_0^{\mathcal{M},\xi\frac{s^{\mathcal{M},\xi}}{x}},\dots,t_n^{\mathcal{M},\xi\frac{s^{\mathcal{M},\xi}}{x}})$
$= f(t_0,\dots,t_n)^{\mathcal{M},\xi\frac{s^{\mathcal{M},\xi}}{x}}$ □

When we substitute a variable in a formula, in some cases the formula does not have the intended meaning. This problem is prevented by the next condition.

Definition 1.5.10. The substitution $\varphi\frac{t}{x}$ is *allowed* if no variables of t are bound in the places where x is replaced by t, i.e. at free occurences of x.

(More formally, one should say that substituting t for x in φ is allowed, since the definition depends on the triple (φ, t, x).)

Here is a more detailed, recursive definition: the substitution is allowed if

(1) φ is atomic,
(2) $\varphi = (\neg\psi)$ and the substitution $\psi\frac{t}{x}$ is allowed,
(3) $\varphi = (\psi \vee \theta)$ and the substitutions $\psi\frac{t}{x}$ and $\theta\frac{t}{x}$ are allowed,
(4) $\varphi = (\exists y\ \psi)$ and (a) $x = y$ or (b) $x \neq y$, the substitution $\psi\frac{t}{x}$ is allowed and y does not occur in t.[7]

This always holds when t is a constant c. If t is a variable y, then the condition states that y is not bound in the relevant places. The next lemma shows that in this case, substitution works well.

Lemma 1.5.11. *(Substitution for formulas) Suppose that φ is an $\mathcal{L}$-formula and s is an $\mathcal{L}$-term. If the substitution $\varphi\frac{s}{x}$ is allowed, then*

$$\mathcal{M} \models (\varphi\frac{s}{x})[\xi] \iff \mathcal{M} \models \varphi[\xi\frac{s^{\mathcal{M},\xi}}{x}].$$

Proof. If x does not occur freely in φ, then the claim holds by Lemma 1.3.4.

Suppose that x occurs freely in φ. The atomic case follows from Lemma 1.5.9, and the cases $\varphi = (\neg\psi)$ and $\varphi = (\psi \vee \theta)$ are easy.

Suppose that $\varphi = (\exists y\ \psi)$. Since x appears freely in φ, this implies $x \neq y$. Since the substitution is allowed, y does not appear in s. Then:

[7] The previous version of this definition, taken from [3, page 14], did not distinguish the cases $x = y$ and $x \neq y$. Thanks to Tom Stalljohann for pointing out this mistake.

$$\begin{aligned}\mathcal{M} \models (\exists y\ \psi)\tfrac{s}{x}[\xi] \quad &\Longleftrightarrow \mathcal{M} \models \psi\tfrac{s}{x}[\xi\tfrac{a}{y}] \text{ for some } a \in M\\ &\Longleftrightarrow \mathcal{M} \models \psi[(\xi\tfrac{a}{y})\tfrac{s^{\mathcal{M},\xi\frac{a}{y}}}{x}] \text{ for some } a \in M \text{ [by the inductive hypothesis]}\\ &\Longleftrightarrow \mathcal{M} \models \psi[(\xi\tfrac{a}{y})\tfrac{s^{\mathcal{M},\xi}}{x}] \text{ for some } a \in M \text{ [since } y \text{ does not appear in } s]\\ &\Longleftrightarrow \mathcal{M} \models \psi[(\xi\tfrac{s^{\mathcal{M},\xi}}{x})\tfrac{a}{y}] \text{ for some } a \in M \text{ [since } x \neq y]\\ &\Longleftrightarrow \mathcal{M} \models (\exists y\ \psi)[\xi\tfrac{s^{\mathcal{M},\xi}}{x}]\end{aligned}$$

Note that the functions $(\xi\frac{a}{y})\frac{b}{x}\colon \mathrm{Var} \to M$ and $(\xi\frac{b}{x})\frac{a}{y}\colon \mathrm{Var} \to M$, where $b = s^{\mathcal{M},\xi}$, are identical since $x \neq y$. □

Lemma 1.5.12. *($^{\to}\exists$-axiom) Suppose that φ is an $\mathcal{L}$-formula, t is an $\mathcal{L}$-term and x is a variable. If the substitution $\varphi\frac{t}{x}$ is allowed, then the formula*

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

is universally valid.

Proof. Suppose that $\mathcal{M}$ is an $\mathcal{L}$-structure and ξ is an assignment for $\mathcal{M}$. By Lemma 1.5.11,

$$\mathcal{M} \models \varphi\frac{t}{x}[\xi] \Longleftrightarrow \mathcal{M} \models \varphi[\xi\frac{t^{\mathcal{M},\xi}}{x}] \Longrightarrow \mathcal{M} \models \exists x\ \varphi[\xi].$$

□

We now define the *Hilbert calculus* as the system of formal rules that consists of the above rules to generate universal truths.[8]

Definition 1.5.13. An $\mathcal{L}$-formula φ is called *$\mathcal{L}$-provable* (in the Hilbert calculus) in each of the following cases:

(1) φ is an equality axiom
(2) φ is a tautology
(3) φ is an $^{\to}\exists$-axiom
(4) φ is generated from two $\mathcal{L}$-provable $\mathcal{L}$-formulas using the modus ponens
(5) φ is generated from an $\mathcal{L}$-provable $\mathcal{L}$-formula using the $\exists^{\to}$-rule.

A *formal $\mathcal{L}$-proof* of φ is a list of $\mathcal{L}$-formulas, each of which is $\mathcal{L}$-provable from the previous formulas in the list, ending with φ. We write $\vdash_{\mathcal{L}}$ if such a proof exists.

Suppose that T is a set of $\mathcal{L}$-formulas. A *formal $\mathcal{L}$-proof* of φ from T is an $\mathcal{L}$-proof of $(\psi_0 \wedge \cdots \wedge \psi_n) \to \varphi$ for some $\psi_0, \ldots, \psi_n \in T$. We write $T \vdash_{\mathcal{L}} \varphi$ if such a proof exists.

To clarify, an $\mathcal{L}$-proof is always a list of formulas given by the rules of the calculus:
ψ_0
ψ_1
...
ψ_n

Here each ψ_j is either an axiom of the Hilbert calculus, or can be derived from the previous ψ_i using the modus ponens or the $\exists^{\to}$-rule.

Hilbert calculus:

Axioms of the calculus:

(1) Axioms of equality are $\mathcal{L}$-provable:
    (a) (Reflexivity) $\forall x\ x \doteq x$
    (b) (Symmetry) $\forall x, y\ (x \doteq y \to y \doteq x)$
    (c) (Transitivity) $\forall x, y\ (x \doteq y \wedge y \doteq z \to x \doteq z)$

[8] This calculus is used in [3] and many other books on mathematical logic.

(d) (Congruence for functions) For all n-ary relation symbols f,

$$\forall x_0, \dots x_n, y_0, \dots, y_n \; ((x_0 \doteq y_0 \wedge \cdots \wedge x_n \doteq y_n) \to f(x_0, \dots, x_n) \doteq f(y_0, \dots, y_n)).$$

(e) (Congruence for relations) For all n-ary relation symbols R,

$$\forall x_0, \dots x_n, y_0, \dots, y_n \; ((x_0 \doteq y_0 \wedge \cdots \wedge x_n \doteq y_n) \to (R(x_0, \dots, x_n) \leftrightarrow R(y_0, \dots, y_n))).$$

(2) All tautologies are $\mathcal{L}$-provable.

(3) (${}^{\to}\exists$-axiom) Suppose that φ is an $\mathcal{L}$-formula, t is an $\mathcal{L}$-term and x is a variable. If the substitution $\varphi\frac{t}{x}$ is allowed, then the formula

$$\varphi\frac{t}{x} \to \exists x \; \varphi$$

is $\mathcal{L}$-provable.

Rules of the calculus:

(1) (Modus ponens) If φ and $\varphi \to \psi$ are $\mathcal{L}$-provable formulas, then ψ is $\mathcal{L}$-provable.

(2) ($\exists^{\to}$ introduction) If $\varphi \to \psi$ is an $\mathcal{L}$-provable formula and x is not free in ψ, then $(\exists x \varphi) \to \psi$ is $\mathcal{L}$-provable.

Note that a proof of φ from a set T of formulas is defined as a proof of $(\psi_0 \wedge \cdots \wedge \psi_n) \to \varphi$ with $\psi_n \in T$.

One could naively think that in a proof from T, one can use formulas in T within the list of formulas, just like the axioms of the calculus. But this is not allowed, and in fact the $\exists^{\to}$-introduction would lead to problems.

The advantage of this calculus (and its variants) compared to e.g. the sequent calculus is that the rules are short and simple. But in any formal proof calculus, writing down actual formal proofs can be complicated and may involve many steps.

It will follow from the compactness theorem that $\vdash_{\mathcal{L}}$ is equivalent for differerent languages $\mathcal{L}$ (as long as the relevant formula φ is an $\mathcal{L}$-formula), so we will later write $\vdash$ instead of $\vdash_{\mathcal{L}}$.

Let $\top = (\varphi_0 \vee (\neg\varphi_0))$ (*true*) for a fixed formula φ_0 without free variables and $\bot := (\neg\top)$ (*false*).

Definition 1.5.14. An $\mathcal{L}$-theory is called

(1) *(syntactically) $\mathcal{L}$-consistent* if $T \nvdash_{\mathcal{L}} \bot$, i.e. one cannot prove a contradiction from T.

(2) *(syntactically) $\mathcal{L}$-complete* if for every ~~$\mathcal{L}$-formula~~ $\mathcal{L}$-sentence φ, $T \vdash_{\mathcal{L}} \varphi$ or $T \vdash_{\mathcal{L}} \neg\varphi$.

Proposition 1.5.15. *(Compactness for $\vdash$) An $\mathcal{L}$-theory T is $\mathcal{L}$-consistent if every finite subset of T is $\mathcal{L}$-consistent.*

Proof. By definition of $\vdash_{\mathcal{L}}$. □

Syntactic-semantic duality

	Syntactic (proof theoretic)	*Semantic (model theoretic)*
Implication	$T \vdash \varphi$	$T \models \varphi$
Consistency/Satisfiability	$T \nvdash \bot$	$T \not\models \bot$, i.e. T has a model
Completeness	For all φ, $T \vdash \varphi$ or $T \models \neg\varphi$	For all φ, $T \models \varphi$ or $T \models \neg\varphi$
Compactness	$T \vdash \varphi \Rightarrow$ there is a finite $T_0 \subseteq T$ with $T_0 \vdash \varphi$	$T \models \varphi \Rightarrow$ there is a finite $T_0 \subseteq T$ with $T_0 \models \varphi$

We will see in chapter 3 that the Hilbert calculus is complete, i.e. it can prove anything that can be proved by any other means. Moreover, $\vdash$ and $\models$ are equivalent. This will show that the left and right side in each box are equivalent.

We next give some examples how to construct formal proofs.

Example 1.5.16.

(1) ($\forall^{\rightarrow}$-axiom) Suppose that φ is an $\mathcal{L}$-formula, t is an $\mathcal{L}$-term and x is a variable. If the substitution $\varphi\frac{t}{x}$ is allowed, then the formula

$$\forall x\ \varphi \rightarrow \varphi\frac{t}{x}$$

is provable.

Proof. $\neg\varphi\frac{t}{x} \rightarrow \exists x\ \neg\varphi$ is an $^{\rightarrow}\exists$-axiom. Note that

$$(\neg\varphi\frac{t}{x} \rightarrow \exists x\ (\neg\varphi)) \ \longleftrightarrow\ (\forall x\ \varphi \rightarrow \varphi\frac{t}{x})$$

is a tautology obtained from the propositional tautology $(\neg p \rightarrow q) \leftrightarrow (\neg q \rightarrow p)$. (Recall that $\forall x\ \varphi$ is an abbreviation for $\neg\exists x\ (\neg\varphi)$.) Modus Ponens yields the required formula. □

(2) ($^{\rightarrow}\forall$-introduction) If $\varphi \rightarrow \psi$ is provable and x is not free in φ, then $\varphi \rightarrow \forall x\psi$ is provable.

Note that a special case $\varphi = (\theta \rightarrow \theta)$ (or any other tautology), $\varphi \rightarrow \psi$ is provable if and only if ψ is provable. We thus obtain the following special case of $^{\rightarrow}\forall$-introduction (for any variable x):

If ψ is provable, then $\forall x\psi$ is provable.

Proof. Note that $\neg\psi \rightarrow \neg\varphi$ is provable, since $(\varphi \rightarrow \psi) \leftrightarrow (\neg\psi \rightarrow \neg\varphi)$ is a tautology. Then $(\exists x\neg\psi) \rightarrow \neg\varphi$ holds by ($\exists^{\rightarrow}$ introduction) Using the tautology

$$((\exists x\neg\psi) \rightarrow \neg\varphi) \ \longrightarrow\ (\varphi \rightarrow \forall x\psi),$$

obtained from the propositional tautology $(p \rightarrow \neg q) \rightarrow (q \rightarrow \neg p)$, Modus Ponens yields $\varphi \rightarrow \forall x\psi$. □

Recall that $\mathcal{L}$-provability of ψ from T means that $\vdash_{\mathcal{L}} (\varphi_0 \wedge \cdots \wedge \varphi_n) \rightarrow \psi$ for some $\varphi_0, \ldots, \varphi_n \in T$. If T is a theory, then $\varphi_0, \ldots, \varphi_n$ do not contain free variables. Hence by the $\forall^{\rightarrow}$-axiom and $^{\rightarrow}\forall$-introduction, $T \vdash_{\mathcal{L}} \psi$ is equivalent to $T \vdash_{\mathcal{L}} \forall x_0, \ldots, x_k\ \psi$, if $x_0, \ldots, x_k$ are the free variables of ψ.

Lecture 6
28. April

(3) Next is a simple example of $\exists^{\rightarrow}$-introduction: to prove an existential formula, one provides a term witnessing it.

Suppose that $\mathcal{L}$ contains a unary function symbol S. Then $\forall x\ \exists y\ (S(x) = y)$ is provable.

Proof. $\forall x\ (S(x) \doteq S(x))$ is an equality axiom. By the $\forall^{\rightarrow}$-axiom and Modus Ponens, $S(x) \doteq S(x)$. $\exists^{\rightarrow}$-introduction yields $S(x) \doteq S(x) \rightarrow \exists y\ (S(x) = y)$. By Modus Ponens, $\exists y\ (S(x) = y)$ is provable as well. By $^{\rightarrow}\forall$-introduction, $\forall x\ \exists y\ (S(x) = y)$ is provable.

More precisely, we here use a consequence of $^{\rightarrow}\forall$-introduction ($\vdash_{\mathcal{L}} \varphi$ implies $\vdash_{\mathcal{L}} \forall x\varphi$) that is shown on Übungsblatt 3.

□

(4) In the next example, one needs to remove the quantifier $\forall$ before applying tautologies.

The formula $(\forall x\ (\varphi \wedge \psi)) \rightarrow (\forall x\ \varphi)$ is provable.

Note that it follows by tautologies that $(\exists x\ \varphi) \rightarrow (\exists x\ (\varphi \vee \psi))$ is provable.

Proof. Note that $(\forall x\ (\varphi \wedge \psi)) \rightarrow (\varphi \wedge \psi)$ is an $\forall^{\rightarrow}$-axiom and $(\varphi \wedge \psi) \rightarrow \varphi$ is a tautology. By tautologies, $(\forall x\ (\varphi \wedge \psi)) \rightarrow \varphi$ is provable. By $^{\rightarrow}\forall$-introduction, $(\forall x\ (\varphi \wedge \psi)) \rightarrow \forall x\ \varphi$ is provable □

(5) In the next example, one has to work backwards to construct a proof. Again we leave out several steps using tautologies.

The formula $(\forall x\ (\varphi \rightarrow \psi)) \rightarrow (\exists x\ \varphi \rightarrow \exists x\ \psi)$ is provable.

Proof. By tautologies and $\exists^{\rightarrow}$-introduction, it suffices to show that

$$\varphi \rightarrow (\forall x\ (\varphi \rightarrow \psi) \rightarrow \exists x\ \varphi)$$

is provable. Again by tautologies,

$$(\varphi \wedge \forall x\ (\varphi \rightarrow \psi) \rightarrow \exists x\ \varphi)$$

suffices. Note that $\forall x\ (\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \psi)$ is an $\forall^{\rightarrow}$-axiom and $\psi \rightarrow \exists x\ \psi$ is provable by $^{\rightarrow}\exists$-introduction. Tautologies yield the claim. □

The next lemma shows that the role of free variables in a provable formula is the same as the role of new constants in an extended language. This will be used in chapter 3 in the proof of the completeness of Hilbert's calculus.

Lemma 1.5.17. *Suppose that φ is an $\mathcal{L}$-formula, $x_0, \dots, x_n$ are (among the) free variables in φ, C is a set of new constants and $c_0, \dots, c_n \in C$ are distinct. Then*

$$\vdash_{\mathcal{L}\cup C} \varphi(\frac{c_0}{x_0}, \dots, \frac{c_n}{x_n}) \Longleftrightarrow \vdash_{\mathcal{L}} \varphi.$$

Proof. Suppose that P[9] is an $\mathcal{L} \cup C$-proof of $\varphi(\frac{c_0}{x_0}, \dots, \frac{c_n}{x_n})$, where $k \geq n$ and $c_0, \dots, c_k$ are distinct. We choose new variables $y_0, \dots, y_k$ that do not appear in the proof. By replacing c_i by y_i everywhere in P, we obtain a $\mathcal{L}$-proof $P\frac{y_0}{c_0}, \dots, \frac{y_k}{c_k}$[10] of $\varphi(\frac{y_0}{x_0}, \dots, \frac{y_n}{x_n})$. (One can easily check that each axiom and rule remains valid.) $^{\rightarrow}\forall$-introduction yields a proof of $\forall y_0, \dots, y_n\ \varphi(\frac{y_0}{x_0}, \dots, \frac{y_n}{x_n})$. By the $\forall^{\rightarrow}$-axiom $\forall y_0, \dots, y_n\ \varphi(\frac{y_0}{x_0}, \dots, \frac{y_n}{x_n}) \rightarrow \varphi$ (the x_i are not free in the formula on the left). By Modus Ponens, we obtain $\vdash_{\mathcal{L}} \varphi$.

Conversely, suppose that $\vdash_{\mathcal{L}} \varphi$ holds. By $^{\rightarrow}\forall$-introduction, we have $\vdash_{\mathcal{L}} \forall x_0, \dots, x_n\ \varphi$. By the $\forall^{\rightarrow}$-axiom and Modus Ponens, $\vdash_{\mathcal{L}\cup C} \varphi(\frac{c_0}{x_0}, \dots, \frac{c_n}{x_n})$. □

Note that the special case of the previous lemma where one chooses no variables at all shows that $\vdash_{\mathcal{L}} \varphi \Longleftrightarrow \vdash_{\mathcal{L}\cup C} \varphi$ holds for any $\mathcal{L}$-formula φ and a set C of constants. Hence the meaning of $\vdash_{\mathcal{L}}$ does not change when $\mathcal{L}$ is enriched by constants. will later see that this is also true for relation and function symbols.

Ending this chapter, we have a look at Hilbert's program, as paraphrased in [Kossak: Mathematical Logic (2018), page 180]:

(1) "Define a system based on a formal language in which all mathematical statements can be expressed, and in which proofs of theorems can be carried out according to well-defined, strict rules of proof.
(2) Show that the system is *complete*, i.e. all true mathematical statement can be proved in the formalism.
(3) Show that the system is *consistent*, i.e. it is not possible to derive a statement and its negation. The consistency should be carried out using finitistic means without appeal to the notion of actual infinity.
(4) Show that the system is *conservative*, i.e. if a statement about concrete objects of mathematics, such as natural numbers of geometric figures, has a proof involving infinitistic methods, then is also has an elementary proof in which those methods are not used.
(5) Show that the system is *decidable* by finding an algorithm for deciding the truth of falsity of any mathematical statement."

[9] A proof is a finite sequence of formulas.

[10] Up to now, we only defined substitution of variables by terms in formulas. If we were more precise here, we would define substitution of constants by variables in formulas, and thus in proofs, in precisely the same way.

We completed (1) in this chapter, and (2) is the completeness of Hilbert's calculus proved in chapter 3.

But the other items cannot be realised: (5) is false by (the proof of) Gödel's first incompleteness theorem; (3) and (4) are false by Gödel's second incompleteness theorem. The failure of (4) also follows from the unprovability in PA of the convergence of Goodstein sequences.

2. Sets and Axioms

Lecture 7
03. May

In this section, we study the framework of set theory.

We first study wellorders and ordinals informally. We then introduce the axioms of set theory and see how they are use to introduce ordinals and cardinals. We prove transfinite induction and recursion.

Up to now, we have worked informally in these settings:

- The world of (hereditarily) finite sets, i.e. finite sets whose elements, elements of elements etc. are finite. A word, i.e. a finite sequence of symbols, is again (hereditarily) finite, since we can assume that each symbol in our language is a (hereditarily) finite set.

  We have not yet said precisely which axioms we use in this setting. We will see that finite set theory, i.e. a version of the axioms of set theory without the axiom of infinity, suffices.

  In particular, we have done proofs by induction on the length of terms, or on the partial ordering *s is a subterm of t*. These are special cases of induction along *wellfounded relations*, which we study in this section.
- Arithmetic, i.e. PA (in exercise problems). In the set theoretic definition of natural numbers, any natural number is a (hereditarily) finite set, and PA can be proved from finite set theory.
- Set theory. We worked with infinite structures and need set theory to formalise those statements.

Set theory forms a basis for all of mathematics. Why do we need such a foundation? We want to have a formal system in which all common mathematical proofs and in which one can construct all mathematical objects, for instance the real and complex fields, function spaces, categories etc.

Some fields in mathematics have their own axiomatisations. For example, think of the theories of groups or fields. But to study these structures, one often goes beyond them, for example one studies fields with the help of their automorphism groups. Set theory is a unified framework in which all mathematical constructions can be done.

Example 2.0.1. This example explains how to construct the real ordered field. We will construct the structure $(\mathbb{N}, 0, 1, +, \cdot, <)$ of the natural numbers below. From this, one can easily construct the ordered field $(\mathbb{Q}, 0, 1, +, \cdot, <)$.

A *cut* in $(\mathbb{Q}, 0, 1, +, \cdot, <)$ is an downwards closed subset with respect to $<$ with an upper bound, but no maximum. $(\mathbb{R}, 0, 1, +, \cdot, <)$ is the set of cuts with pointwise operations induced by those of $\mathbb{Q}$.[11] So the reals are constructed via the power set of $\mathbb{Q}$.

It is not hard to show that $(\mathbb{R}, 0, 1, +, \cdot, <)$ is a *complete ordered field*, i.e. every bounded subset has a supremum. In analysis, one shows that there is a unique complete ordered field.

A central question in set theory is about size, the most basic property of mathematical objects. Why is this useful? For example, an obvious way to show that a structure G does not embed into a structure H is to show that G is strictly larger than H. Here is an example where it is not immediately obvious how two sets compare in size:

Example 2.0.2. Consider the set L of linear orders on $\mathbb{N}$ up to bi-embeddability $\sim$, where $(\mathbb{N}, <_0) \sim (\mathbb{N}, <_1)$ if $(\mathbb{N}, <_0)$ embeds into $(\mathbb{N}, <_1)$ and conversely.[12] We want to compare $L/{\sim}$ with $\mathbb{R}$. How do the sizes $|L/{\sim}|$ and $|\mathbb{R}|$ of these sets compare?

[11] Multiplication is first defined pointwise on $\mathbb{R}_{\geq 0}$ and then extended to $\mathbb{R}$ by cases for positive and negative numbers.

[12] This is strictly weaker then isomorphism.

It is not hard to show that $|L/{\sim}| = \aleph_1$, where $\aleph_1$ denotes the first uncountable cardinal. Thus $|L/{\sim}| \leq |\mathbb{R}|$. The axiom of choice is relevant: without it, one cannot show that these sets are comparable in size, i.e. that there exists an injection $L/{\sim} \to \mathbb{R}$ or an injection $\mathbb{R} \to L/{\sim}$.

Whether $|L/{\sim}| = |\mathbb{R}|$ cannot be decided on the basis of the axioms of set theory. Thus it is in general a highly nontrivial question to determine the size of a set.

The aim of this chapter is an introduction to set theory up to cardinals. The basic notion for comparing the cardinality of two sets is *wellordering*. We will therefore spend most of our efforts to study wellorders and recursion along wellorderings.

2.1. **Wellfounded relations and wellorders.** This section is an introduction to *wellorders*. They are used to count past the natural numbers.

We work informally as in usual mathematical proofs. This gives some of the flavour of working with ordinals and cardinals.

As any mathematical proof, these arguments can be fully formalised within the axiom system of set theory. We do this in the next section by developing basic results in set theory directly from the axioms.

One could develop most of the basic results of set theory informally.

Suppose that A is a set (later, classes will be allowed) an $(A, \leq)$ is a linear order. We will write $a < b$ for $(a \leq b \ \wedge \ a \neq b)$. We call $(A, <)$ a *strict linear order*.

Definition 2.1.1.

(1) A binary relation $<$ on a set A is called *wellfounded* if every nonempty subset of A has an $<$-minimal element.
(2) A *wellorder* $(A, <)$ is a wellfounded strict linear order.

Only this chapter, we also allow the empty set with a relation as a structure. In particular, the empty set with the empty relation is a wellorder. It is called 0.

The usual order of the natural numbers is an example of a wellorder. Its order type[13] is denoted by ω. Going beyond this, we obtain $\omega + 1$ by adding an element on top of ω, then $\omega + 2$, $\omega + 3$, $\dots \omega + \omega = \omega \cdot 2$, $\dots$, ω^2, ω^3, $\dots$, ω^ω etc.

Any wellfounded relation $(A, <)$ satisfies the following induction principle for all properties P:

> *Suppose that for all $b \in A$, if $P(a)$ holds for all $a < b$ then $P(b)$ holds. Then $P(a)$ holds for all $a \in A$.*

To see this, note that if $P(a)$ would fail for some $a \in A$, then it would fail for some $<$-minimal $a \in A$. This is because we assumed that $(A, <)$ is a wellorder. Thus $P(b)$ holds for all $b < a$. However, then $P(a)$ holds by the assumption on P. We will formally prove this below. P will be given by a first-order formula in the language of set theory.

The axiom of choice is not needed to prove the below results about wellorders. However, the next lemma clarifies the concept of wellorder with the use of the axiom of choice. It is not needed below.

Lemma 2.1.2. *Suppose that $<$ is a binary relation on a set A. The following conditions are equivalent:*

(1) *$(A, <)$ is wellfounded.*
(2) *There is no strictly decreasing infinite sequence $a_0 > a_1 > \dots$ in A.*

Proof. (1)⇒(2): Towards a contradiction, suppose that $\langle a_n \mid n \in \mathbb{N} \rangle$ is a strictly decreasing sequence in A. Then $\{a_n \mid n \in \mathbb{N}\}$ has no $<$-minimal element.

[13] By the order type, we mean the isomorphism class. The right definition of ω can only be introduced in the next section.

(2)⇒(1): Towards a contradiction, suppose that $(A,<)$ is not wellfounded. There is a subset B of A that contains no $<$-minimal element. We can therefore construct a sequence strictly decreasing sequence $\{a_n \mid n \in \mathbb{N}\}$ in A. Let $a_0 \in B$ be arbitrary. Choose an arbitrary $a_{n+1} < a_n$ in step $n+1$. More precisely, this argument uses the axiom of choice, which we will introduce below. One can find a_{n+1} by using a choice function that sends every nonempty subset of A to an element. □

We show next that any two wellorders are comparable. We define an *initial segment* of a wellorder $(A,<)$ to be either of the form $(A,<)$ or $(A_{<b}, <\restriction A_{<b})$, where $A_{<b} = \{a \in A \mid a < b\}$ for some $b \in A$. We will always use the notation $\mathcal{A} = (A, <_A)$, $\mathcal{B} = (B, <_B)$ and $\mathcal{C} = (C, <_C)$ for wellorders. We will write $\mathcal{A} < \mathcal{B}$ if $\mathcal{A}$ is isomorphic to a proper initial segment of $\mathcal{B}$.

The proof of the next lemma is an example of the following recursion principle for wellorders $\mathcal{A} = (A, <_A)$. Suppose that G is a function such that $G(f)$ is defined for any partial function f from A to a set B, and $G(f) \in B$ for all such functions f.

> *There is a unique function $F\colon A \to B$ such that for all $a \in A$, $F(a) = G(f\restriction A_{<a})$.*

A proof of this recursion principle will be added here. In the proof of the next lemma, the recursion is proved ad hoc.

Assumming the *wellordering principle*, i.e. the statement that every set can be wellordered, the next lemma shows that any two sets can be compared in size. The wellordering principle follows from the axioms of set theory.

Lemma 2.1.3. *For wellorders $\mathcal{A}$ and $\mathcal{B}$, exactly one of the following holds:*

(1) $\mathcal{A} \cong \mathcal{B}$.
(2) $\mathcal{A} < \mathcal{B}$.
(3) $\mathcal{B} < \mathcal{A}$.

Moreover, in each case the isomorphism is unique.[14]

Proof. By induction on $a \in A$ (by the induction principle above), we can assume that the statement of the lemma, including the uniqueness claim, already holds for all proper initial segments of $\mathcal{A}$.

We now prove that one of (1), (2) or (3) holds for $\mathcal{A}$.

First assume that for every $a \in A$, there is an isomorphism f_a from $A_{<a}$ to an initial segment of $\mathcal{B}$. By uniqueness of the f_a for $a \in A$, we have $f_b\restriction A_{<a} = f_a$ for all $a < b$ in A, i.e. f_b extends f_a. Then the union of the functions f_a for all $a \in A$ is an isomorphism from $\mathcal{A}$ to an initial segment of $\mathcal{B}$. Hence (1) or (2) holds.

Now assume that for some $a \in A$, there is no isomorphism f_a from $A_{<a}$ to an initial segment of $\mathcal{B}$. We can assume that a is the $<$-least such element of A.

First assume that $A_{<a}$ has a largest element a'. By our assumption, there is an isomorphism f from $A_{<a'}$ to an initial segment of $\mathcal{B}$. If its range is B, then (3) holds. Otherwise, its range is $B_{<b'}$ for some $b' \in B$. We can extend f to an isomorphism f' from $A_{<a}$ to an initial segment of $\mathcal{B}$ by defining $f(a') = b'$. but we assumed that such a map does not exist.

Now assume that $A_{<a}$ has no largest element. As in the the beginning of the proof of one of (1),(2) or (3), we can use the uniqueness of the isomorphisms $f_{a'}$ from $A_{<a'}$ to an initial segment of $\mathcal{B}$ for $a' < a$ to see that their union is an isomorphism from $A_{<a}$ to an initial segment of $\mathcal{B}$, contradicting the assumption on a.

It remains to prove uniqueness. Towards a contradiction, suppose that $f \neq g$ are isomorphisms in one of (1), (2). The proof of (3) is similar. It is easy to see that f cannot extend g or conversely. Hence there is some $a \in A$ with $f(a) \neq g(a)$. Suppose that a

[14] We mean the isomorphism from $\mathcal{A}$ to a proper initial segment of $\mathcal{B}$ in (2), and similarly in (3).

is $<_A$-least with $f(a) \neq g(a)$. But f and g are both isomorphisms to initial segments of $\mathcal{B}$, so $f(a)$ and $g(a)$ both equal the $<_B$-least element of B strictly above the range $\operatorname{ran}(f \restriction A_{<a}) = \operatorname{ran}(g \restriction A_{<a})$. □

We will now see that arithmetic can be extended to the ordinals. The definition of the operations is defined by glueing wellorders together.

When we work with wellorders $\mathcal{A} < \mathcal{B}$, we will assume that $\mathcal{A}$ is an initial segment of $\mathcal{B}$. We thus omit the isomorphisms in the following arguments. This can be justified by checking that the arguments still work with the necessary isomorphisms, or alternatively by noting that this property is actually true for ordinals introduced later in this chapter.

Now let $(A_i, <_{A_i})$ be wellorders for $i \in I$, where I is a set. By our assumption, each $(A_i, <_{A_i})$ is an initial segment of $(A_j, <_{A_j})$ or conversely, so we can form their union, denoted $\sup_{i \in I}(A_i, <_{A_i}) = (\bigcup_{i \in I} A_i, \bigcup_{i \in I} <_{A_i})$. It is easy to check that the isomorphism type of $\sup_{i \in I}(A_i, <_{A_i})$ depends only on the isomorphism types of $(A_i, <_{A_i})$ for $i \in I$.

We say that a wellorder $(A, <_A)$ has *successor length* if it has a largest element, and *limit length* otherwise. If $(A, <_A)$ has limit length, then it is the union of its proper initial segments.

Definition 2.1.4. (Addition of wellorders) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are wellorders. We assume that A and B are disjoint by replacing $\mathcal{B}$ by an isomorphic copy, if necessary. Let $\mathcal{A} + \mathcal{B} = (A \cup B, <)$, where $a < b$ if

- $a, b \in A$ and $a <_A b$,
- $a, b \in B$ and $a <_B b$, or
- $a \in A$ and $b \in B$.

Thus $\mathcal{B}$ is glued on top of $\mathcal{A}$. Note that addition is not commutative. What is $3 + \omega$?

Lemma 2.1.5. *Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ denote wellorders.*

(1) $\mathcal{A} + 0 \cong \mathcal{A}$.
(2) $\mathcal{A} + [\mathcal{B} + \mathcal{C}] \cong [\mathcal{A} + \mathcal{B}] + \mathcal{C}$.
(3) *If $\mathcal{C}$ has limit length, then*

$$\mathcal{A} + \mathcal{C} \cong \sup\{\mathcal{A} + \mathcal{B} \mid \mathcal{B} < \mathcal{C}\}.$$

Proof. These claims are easy to check directly from the definitions. (3) holds since the supremum is defined as the union. □

Lecture 8
05. May

Definition 2.1.6. (Multiplication of wellorders) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are wellorders. Let $\mathcal{A} \cdot \mathcal{B} = (A \times B, <_{\text{r-lex}})$, where $(a, b) <_{\text{r-lex}} (a', b')$ is the *right-lexicographical order* defined by

- $b <_B b'$ or
- $b = b'$ and $a <_A a'$.

Thus $\mathcal{A} \cdot \mathcal{B}$ glues $\mathcal{B}$ many copies of $\mathcal{A}$ together. For example, $\omega \cdot 3 = \omega + \omega + \omega$. Note that multiplication is not commutative. What is $3 \cdot \omega$?

Let 1 denote a wellorder with a single element.

Lemma 2.1.7. *Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ denote wellorders.*

(1) $\mathcal{A} \cdot 1 \cong \mathcal{A}$.
(2) $\mathcal{A} \cdot [\mathcal{B} \cdot \mathcal{C}] \cong [\mathcal{A} \cdot \mathcal{B}] \cdot \mathcal{C}$.
(3) $\mathcal{A} \cdot [\mathcal{B} + (\mathcal{C}] \cong [\mathcal{A} \cdot \mathcal{B}] + [\mathcal{A} \cdot \mathcal{C}]$.
(4) *If $\mathcal{C}$ has limit length, then*

$$\mathcal{A} \cdot \mathcal{C} \cong \sup\{\mathcal{A} \cdot \mathcal{B} \mid \mathcal{B} < \mathcal{C}\}.$$

Proof. These claims can be proved directly from the definitions are are left as exercises. □

One can further define exponentiation of wellorders as follows.

Definition 2.1.8. (Exponentiation of wellorders) Suppose that $\mathcal{A}$ and $\mathcal{B}$ are wellorders. Let $\mathcal{A}^{\mathcal{B}} = (A^{(B)}, <_{\text{r-lex}})$, where $A^{(B)}$ denotes the set of finite partial functions $f \colon B \to A$ and $f <_{\text{r-lex}} g$ is the *right-lexicographical order* defined by $f(b) < g(b)$ or $f(b)$ is not defined, where $b \in B$ is $<_B$-least such that either $f(b) \neq g(b)$ or one of them is defined and the other one ist not.

Exponentiation has the expected properties, see e.g. [2, Exercises 3.10 & 3.11].

We will get back to ordinal arithmetic later when we discuss ordinals.

2.2. **Axioms of set theory.** Before we begin to introduce the axioms, we begin with an example to illustrate how any mathematical object can be constructed as a set.

Example 2.2.1.

(1) A natural number is of the form $0 := \emptyset$, or $n+1 := n \cup \{n\}$ for a natural number n.[15] Thus n is itself a set with n elements.

(2) A rational number $q \in \mathbb{Q}$ is an equivalence class of triples (m,n,k)[16] of natural numbers, where (m,n,k) represents $\frac{m-n}{k+1}$.

(3) A real number $r \in \mathbb{R}$ is a nonempty set of rational numbers that is bounded from above, downwards closed (if $q \in r$ and $p \leq q$, then $p \in r$) and has no maximal element.

(4) A function $f \colon \mathbb{R} \to \mathbb{R}$ is a subset f of $\mathbb{R}^2$ such that for each $r \in \mathbb{R}$, there is a unique $s \in \mathbb{R}$ with $(r,s) \in f$.

In (3), we used the power set of the rationals $\mathbb{Q}$, i.e. the set of subsets of $\mathbb{Q}$. In (4), we used subsets of the reals.

Intuivitely, set formation is described as follows:

Georg Cantor:

> "Unter einer 'Menge' verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten in unserer Anschauung oder unseres Denkens (welche die 'Element' von M genannt werden) zu einem Ganzen."

Felix Hausdorff:

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

Can one form the set of objects with any given property (unrestricted separation)? Several *paradoxes* related to this emerged in work of Cantor, Burali-Forti and Russell, but it seems that they were not seen as paradoxes at that time. My impression from the literature is that unrestricted separation was never considered as an axiom scheme, but only emerged in the logical study of the foundations of set theory in Russell's work. When fixing the axioms in a logical setting, one has to make precise what kind of separation is allowed.

It was known to Cantor that some collections of sets are themselves not sets, for example *Cantor's paradox* states that the collection of all cardinal numbers does not form a set. Burali-Forti's paradox states that the collection of ordinals does not form a set. The difference between these and Russell's observation that the unrestricted principle of set

[15] This is an informal definition that will be made precise later. The set of natural numbers will be defined as the smallest set that is closed under the function $n \mapsto n \cup \{n\}$.

[16] Ordered pairs and tuples are defined below.

formation is contradictory is that Russell's paradox is purely logical and does not assume any other axioms.

Remark 2.2.2. (Russell's Paradox) Assume that there exists a set x that contains precisely those sets y with $y \notin y$ as elements. Then $x \in x$ holds if and only if $x \notin x$. Therefore, no such set can exist.

Actually, we will see that the axiom of foundation prohibits the existence of sets y with $y \in y$. Assuming the axiom of foundation, Russell's paradox says: there is no set of all sets, since it would contain itself as an element. However, Russell's formulation is more general and, as we will see, has counterparts in the proofs of Gödel's incompleteness theorems.

What is a possible solution to this paradox? As hinted, the collection of all sets is simply too large. Such collections are called *classes*. Classes are, for us, syntactical abbreviations of the form $\{x \mid \varphi(x)\}$, i.e. every class is given by a formula φ.

(An alternative is Bernays-Gödel class theory, where classes are objects by themselves.)

We now develop basic properties of sets and classes, introducing axioms when needed. The language of set theory is $\{\in\}$, where $\in$ is a binary relation symbol.

Axiom. (Existence) $\exists x\ (\forall y\ y \notin x)$.

One could alternatively work with the Existence Axiom $\exists x\ (x = x)$; the existence of the empty set would follow from the Separation Axiom below.

Two sets are equal if and only if they have the same elements.

Axiom. (Extensionality) $\forall x, x'\ (\forall y\ (y \in x \leftrightarrow y \in x') \rightarrow x = x')$.

We next define classes. One could formulate everything that follows using sets alone, but classes are quite convenient.

Definition 2.2.3. A *class term*

$$A = A(s_0, \ldots, s_n) = \{x \mid \varphi(x, s_0, \ldots, s_n)\}$$

is given by an $\mathcal{L}_\in$-formula φ and variables $s_0, \ldots, s_n$.

A *class* is a class term $A(s_0, \ldots, s_n)$ together with sets $s_0, \ldots, s_n$.[17] So a class term is variable, while a class is a fixed collection of sets. (Formally, this distinction means that we are in a context where the s_i are bound variables.)

Definition 2.2.4. Suppose that $A = \{x \mid \varphi(x, s_0, \ldots, s_n)\}$ is a class term and s is a variable. We define

(1) $s \in A$ to mean $\varphi(s, s_0, \ldots, s_n)$.
(2) $s \doteq A$[18] to mean $(\forall x \in s\ \varphi(x, s_0, \ldots, s_n)) \wedge (\forall x(\varphi(x, s_0, \ldots, s_n) \rightarrow x \in s)$.

One can thus regard classes as more general objects than sets. Some classes are equal to sets; the remaining ones are too large to be sets – by the separation axiom below, they are not a subset of any set – they are called *proper classes.*

A class is called a *proper class* if it is not equal to any set.

Definition 2.2.5. Suppose that A, B are classes.

(1) $A \subseteq B$ if $\forall x \in A\ (x \in B)$.
(2) $A \doteq B$ if $A \subseteq B$ and $B \subseteq A$.
(3) $A \in B$ if $\exists s\ (s \doteq A \wedge s \in B)$.

We will often simply write $=$ for $\doteq$.

[17] I.e. $s_0, \ldots, s_n$ are elements of the set theoretic universe V in Definition 2.2.7.

[18] We write $\doteq$ instead of $=$ here to make clear that $\doteq$ is used as a logical symbol in an extended language that allows abreviations. But one can always write $=$ instead of $\doteq$.

Lemma 2.2.6. *If A, B are classes and s, t are sets with $A \doteq s$ and $B \doteq t$, then $s \doteq t$ holds if and only if $A \doteq B$.*

Proof. By the Axiom of Extensionality. □

Definition 2.2.7.

(1) $\emptyset = \{x \mid x \neq x\}$.
(2) $V = \{x \mid x \doteq x\}$ (the *set-theoretic universe*).
(3) $\{x_0, \dots x_n\} = \{x \mid x \doteq x_0 \vee \dots \vee x \doteq x_n\}$.

Lemma 2.2.8. $\emptyset \in V$.

Definition 2.2.9. A class A is a *proper class* if there is no set s with $A = s$.

Definition 2.2.10. Suppose that $A, B, A_0, \dots A_n$ are classes.

(1) $A_0 \cup \dots \cup A_n = \{x \mid x \in A_0 \vee \dots \vee x \in A_n\}$.
(2) $A_0 \cap \dots \cap A_n = \{x \mid x \in A_0 \wedge \dots \wedge x \in A_n\}$.
(3) $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.
(4) $\bigcup A = \bigcup_{x \in A} x = \{y \mid \exists x \in A \ y \in x\}$.
(5) $\bigcap A = \bigcap_{x \in A} x = \{y \mid \forall x \in A \ y \in x\}$.

Lecture 9
10. May

Lemma 2.2.11. $\bigcup\{x, y\} = x \cup y$.

Proof. $\subseteq$: Suppose that $u \in \bigcup\{x, y\}$. Then $u \in v$ for some $v \in \{x, y\}$. Assume $v = x$. Then $u \in x$, so $u \in x \cup y$.

$\supseteq$: Suppose that $u \in x \cup y$. Assume $u \in x$. Then $u \in \bigcup\{x, y\}$. □

Axiom. (Pairing) $\forall x, y\ (\exists z\ (\forall u\ (u \in z) \leftrightarrow (u = x \vee u = y))$.

Note that the pair is unique by the Axiom of Extensionality.

Definition 2.2.12. (Kuratowski pair) Suppose that $s, t, s_0, \dots s_{n+1}$ are sets.

(1) $(s, t) := \{\{s\}, \{s, t\}\}$ is the *ordered pair* of s, t.
(2) $(s_0, \dots, s_{n+1}) := ((s_0, \dots, s_n), s_{n+1})$.[19]

Lemma 2.2.13.

(1) $\forall x, y\ \exists z\ (z = (x, y))$.
(2) $\forall x_0, \dots, x_n\ \exists z\ (z = (x_0, \dots, x_n))$.

Proof. (1) By the pairing axiom, $\{s\} = \{s, s\}$ and $\{s, t\}$ are sets, so $\{\{s\}, \{s, t\}\}$ is a set as well.

(2) By induction on n. □

Lemma 2.2.14. *$\forall x, y, x', y'\ ((x, y) = (x', y') \to (x = x') \wedge (x = y'))$, i.e. Definition 2.2.12 satisfies the fundamental property of ordered pairs.*

Proof. Suppose that $(x, y) = (x', y')$.

First suppose that $x = y$. Then $\{x\} = \{x, y\}$ and $(x, y) = \{\{x\}\}$. We have $(x', y') = \{\{x'\}, \{x', y'\}\} = \{\{x\}\}$. So $\{x'\} = \{x', y'\}$ and thus $x' = y'$. Then $(x, y) = \{\{x\}\} = \{\{y\}\}$ and $(x', y') = \{\{x'\}\} = \{\{y'\}\}$. So $x = x' = y = y'$.

Now suppose that $x \neq y$. By Extensionality, $x = x'$ or $x' = x = y$. Then $\{x, y\} = \{x', y'\}$, so $y = y'$. □

[19] Note that this is an induction in the metatheory. A weak fragment of PA would suffice for formalise the metatheory. However, this is not necessary: we could restrict ourselves to pairs here. No metatheory at all is needed to develop set theory, since every single theorem and proof consists of only finitely many formulas. The metatheory only comes into play when we define the full ZFC as a scheme and study its properties and its models.

Definition 2.2.15. If $A_0, \dots, A_n$ are class terms or classes, let

$$A_0 \times \cdots \times A_n = \{(x_0, \dots, x_n) \mid x_0 \in A_0 \wedge \cdots \wedge x_n \in A_n\}.$$

Definition 2.2.16.

(1) A class R is called a *binary relation* on a class A if $R \subseteq A \times A$.
(2) A relation F is called a *function* or *map* if

$$\forall x, y, y',\ ((x, y) \in F \wedge (x, y') \in F) \to y = y'.$$

Definition 2.2.17. Suppose that R is a relation.

(1) $\mathrm{dom}(R) = \{x \mid \exists y\ (x, y) \in R\}$.
(2) $\mathrm{ran}(R) = \{y \mid \exists x\ (x, y) \in R\}$.
(3) $\mathrm{field}(R) = \mathrm{dom}(R) \cup \mathrm{ran}(R)$.

Definition 2.2.18. Suppose that F is a function and A, B are classes.

(1) F is a *function from A to B* ($F\colon A \to B$) if $\mathrm{dom}(F) = A$ and $\mathrm{ran}(F) \subseteq B$.
(2) F is a *partial function from A to B* ($F\colon A \rightharpoonup B$) if $\mathrm{dom}(F) \subseteq A$ and $\mathrm{ran}(F) \subseteq B$.
(3) If B is a set, let ${}^{A}B = \{f \mid f\colon A \to B\}$.

Axiom. (Union) $\forall x\ \exists y\ \forall z\ (z \in y \leftrightarrow \exists u\ (u \in x \wedge z \in u))$.

Lemma 2.2.19. *$\forall x_0, \dots, x_n\ \{x_0, \dots, x_n\} \in V$ (i.e. $\exists z\ \forall u\ (u \in z \leftrightarrow (u = x_0 \vee \cdots \vee u = x_n))$).*

Proof. For $n = 0, 1$ this holds by the Pairing Axiom.

Suppose this holds for n. Then $\{x_0, \dots, x_{n+1}\} = \bigcup\{\{x_0, \dots, x_n\}, \{x_{n+1}\}$ is a set by the Pairing, Union and Extensionality Axioms. □

We now aim to define set of natural numbers. It will be defined as the smallest inductive set. The idea why one defines $s + 1$ as $s \cup \{s\}$ is that one wants to add a new element to the set s. Note that we will therefore also need to know that $s \notin s$. The Axiom of Foundation will ensure this.

Definition 2.2.20.

(1) For any set s, we define $s + 1 := s \cup \{s\} = \bigcup\{s, \{s\}\}$.
(2) A set s is called *inductive* if $\emptyset \in s$ and $\forall x \in s\ (x + 1) \in s$.

The Axiom of Infinity states that there is an inductive set.[20]

Axiom. (Infinity) $\exists y\ (\emptyset \in y \wedge \forall x\ (x \in y \to x + 1 \in y))$.

We need an axiom to ensure that an inductive set has infinitely many elements

Axiom. (Foundation) $\forall x \neq \emptyset\ \exists y\ (y \in x \wedge x \cap y = \emptyset)$.

Lemma 2.2.21. *There are no $\in$-cycles $x_0 \in x_1 \in \cdots \in x_n \in x_0$.*

Proof. $y = \{x_0, x_1, \dots, x_n\}$ is a set by Lemma 2.2.19. By the Foundation Axiom, y has an $\in$-minimal element x_k. If $k = 0$, then $x_0 \cap y = \emptyset$. But $x_n \in x_0 \cap y$, contradiction.

If $k > 0$, then $x_k \cap y = \emptyset$. But $x_{k-1} \in x_k \cap y$, contradiction. □

The Separation Scheme states that $\{z \in x \mid \varphi(z, x_0, \dots, x_n)\}$ is always a set. In other words, a subclass of a set is itself a set.

Axiom Scheme. (Separation) For any formula $\varphi(z, x_0, \dots, x_n)$,

$$\forall x\ \forall x_0, \dots, x_n\ \exists y\ \forall z\ (z \in y \leftrightarrow (z \in x \wedge \varphi(z, x_0, \dots, x_n))).$$

[20] Given all the other axioms and schemes of set theory, including the Axiom of Choice, one can show that this follows from the existence of an infinite, i.e. not finite, set. Here by a finite set, we mean a set x such that every injective function $f\colon x \to x$ is surjective.

Lemma 2.2.22. *V is not a set, i.e. $V \notin V$.*

Proof. By Lemma 2.2.21. □

Lemma 2.2.23. *There is a $\subseteq$-least inductive set.*

Proof. By the Axiom of Infinity, there is an inductive set x. The class

$$y = \{u \mid u \in x \text{ and for all inductive sets } z,\ u \in z\},$$

i.e. the intersection of all inductive sets, is a set by the Separation Scheme. Since $\emptyset \in y$, and for all $z \in y$ we have $z + 1 \in y$, y is in fact inductive. □

By the Axiom fo Extensionality, the $\subseteq$-least inductive set is unique. We will denote it by ω and call it the set of *natural numbers.*

Axiom Scheme. (Replacement) If F is a function, then $\forall x\ F[x] \in V$, where $F[x] = \{z \mid \exists y \in z\ (y, z) \in F\}$.

The Replacement Scheme lists infinitely many formulas. However, for any proof of a formula from the axioms of set theory, only finitely many instances of the Replacement Scheme are used. Thus for any specific result in set theory, we do not need to worry about issues such as: does one need to assume a certain theory such as PA, or the axioms of set theory without the axiom of infinity, to work with formulas? Such problems only arise when one studies the connection between structures and formulas as in the first chapter.

Definition 2.2.24. The axiom system ZF^- of

Zermelo-Fraenkel Set Theory without the Power Set Axiom

consists of the Axioms of Existence, Extensionality, Pairing, Union, Foundation, Infinity, and the Axiom Schemes of Separation and Replacement.

We work with ZF^- because this suffices to develop basic notions of set theory and to prove the recursion theorem. ZF consists ZF^- together with the Power Set Axiom. ZFC consists ZF together with the Axiom of Choice. These will be introduced later to prove properties of cardinals. For instance, without them one cannot prove that uncountable sets exist.

Lecture 10
12. May

Remark 2.2.25.

(1) The Axiom of Infinity and the Separation scheme imply the Axiom of Existence.
(2) The Axioms of Existence, Extensionality and the Replacement Scheme imply the Separation Scheme.
(3) The Axiom of Infinity and the Replacement Scheme imply the Axiom of Pairing.

Proof. (1) Given any set x, $\{y \in x \mid y \neq y\}$ is a set by the Separation Scheme.

(2) Suppose that $s, s_0, \ldots, s_n$ are sets and $\varphi(x, y_0, \ldots, y_n)$ is a formula.

If there is no $t \in s$ with $\varphi(t, s_0, \ldots, s_n)$, then $u = \{x \in s \mid \varphi(x, s_0, \ldots, s_n)\}$ is empty. By the Axiom of Existence, there is an empty set v and by the Axiom of Extensionality, $u = v$.

Now assume that there is some $t \in s$ with $\varphi(t, s_0, \ldots, s_n)$. Define a function $F\colon s \to s$ by letting $F(z) = z$ if $\varphi(z, y_0, \ldots, y_n)$ holds and $F(z) = t$ otherwise. Then $u = \{x \in s \mid \varphi(x, s_0, \ldots, s_n)\} = \operatorname{ran}(F)$ by the Axiom of Extensionality, and $\operatorname{ran}(F)$ is a set by the Replacement Scheme.

(3) This is left as an exercise. □

Remark 2.2.26. We aim to show later in the lecture:

(1) ZF^- is not *finitely axiomatisable*, i.e. there is no finite list of sentences which both follow from ZF^- and imply ZF^-. This means that the Separation Scheme and Replacement Scheme cannot be (both) replaced by finitely many axioms.
(2) Any consistent and sufficiently simple extension of ZF^- is incomplete by Gödel's first incompleteness theorem. (By sufficiently simple, we mean that the list of axioms can be generated by an algorithm. For example, any theory that consists of finitely many axioms and schemes.) Thus ZF^- (and ZF, ZFC) only determine the general rules how to work with sets, but do not provide a complete description of the set-theoretic universe.

We now study induction, recursion and ordinals using the axioms of ZF^-.

If $<$ is a relation and y is a set, we write $\mathrm{pred}_<(y) = \{x \mid x < y\}$. (Note that in general, this is a class.)

Definition 2.2.27. Suppose that $<$ is a relation (on V).

(1) $<$ is called *wellfounded* if any nonempy set contains a $<$-minimal element.
(2) $<$ is *wellfounded for classes* if every nonempty class contains a $<$-minimal element.
(3) $<$ is called *strongly wellfounded* if $<$ is wellfounded and for any $y \in \mathrm{field}(<)$, $\mathrm{pred}_<(y)$ is a set.
(4) A *wellorder* is a wellfounded linear order.

We will see below that strongly wellfounded implies wellfounded for classes.

The next theorems generalise induction and recursion on the natural numbers in two ways:

(1) To the transfinite, i.e. to ordinals beyond the natural numbers.
(2) To wellfounded partial orders.

The first one has a number of applications. One that can be found in most textbooks on set theory is to enumerate any given set, assuming the axiom of choice, and thus prove the wellordering theorem.

The second one is much more general. As an example, one can think of a *tree partial order*, i.e. a wellfounded partial order $<$ such that for all $x \in \mathrm{field}(<)$, $\mathrm{pred}_<(x)$ is linearly ordered by $<$. In such an example, one assumes a property to hold at the root of the tree and wants to prove it for all nodes.

Another example for induction along wellfounded partial orders is recursion for terms and formulas.

While one usually uses wellfoundedness to prove induction, the next theorem states that these two properties are in fact equivalent.

To formulate induction, we introduce the following notation. Suppose that $\varphi(u,v)$ is a formula and z is a set. We call φ *$<$-inductive* with parameter z if for all $y \in \mathrm{field}(<)$, we have $(\forall x < y\ \varphi(x,z)) \to \varphi(y,z)$. We further say that $<$ satisfies *induction* if for any $<$-inductive φ with parameter z, $\varphi(x,z)$ holds for all $x \in \mathrm{field}(<)$.

Lemma 2.2.28. *(Transfinite induction) The following conditions are equivalent for a relation $<$:*

(1) $<$ *is wellfounded for classes.*
(2) $<$ *satisfies induction.*

Proof. (1) $\Rightarrow$ (2): Suppose that $\varphi(x,z)$ fails for some $x \in \mathrm{field}(<)$. Since $<$ is wellfounded for classes, there is a $<$-minimal y for which $\varphi(y,z)$ fails. Then $\forall x < y\ \varphi(x,z)$ holds. But since φ is *$<$-inductive* with parameter z, this would imply $\varphi(y,z)$.

(2) $\Rightarrow$ (1): Assuming (1) fails, let $A = \{x \mid \varphi(x,z)\}$ be a nonempty class with no $<$-minimal element. Then (2) fails for $\neg\varphi$. □

Induction as in (2) also holds for strongly wellfounded relations, since such relations are wellfounded for classes by the proof of the next theorem. Note that $\mathrm{Ord} + \mathrm{Ord}$, $\mathrm{Ord} \cdot \omega$,

$\mathrm{Ord} \cdot \mathrm{Ord}$ are wellfounded for classes, where $\mathrm{Ord} \cdot \alpha$ means $\mathrm{Ord} \times \alpha$ ordered by $<_{\mathrm{r-lex}}$. So one can do induction far beyond Ord.

In the next theorem, we will use the following notation. Given a function $G\colon A \times V \to V$ and $B \subseteq A$, we say that a function $f\colon B \to V$ is *guided* by G if

(1) B is $\mathrm{pred}_<$-closed and
(2) $f(x) = G(x, f{\restriction}\mathrm{pred}_<(x))$ for all $x \in B$.

Condition (1) is necessary for the second condition to make sense. Condition (2) states that f satisfies the recursion defined by G.

Theorem 2.2.29. *(Transfinite recursion) Suppose that $<$ is a strongly wellfounded relation with* $\mathrm{field}(<) = A$. *(A is a class.) For any function $G\colon A \times V \to V$, there exists a unique function $F\colon A \to V$ that is guided by G.*

Proof. We first assume that $<$ is wellfounded for classes. We will eliminate this assumption in the end of the proof. An *approximation* is a set function guided by G.

Claim. *Suppose that f, g are approximations. Then* $v = \mathrm{dom}(f) \cap \mathrm{dom}(g)$ *is* $\mathrm{pred}_<$*-closed and* $f{\restriction}v = g{\restriction}v$.

Proof. It is clear that $v = \mathrm{dom}(f) \cap \mathrm{dom}(g)$ is $\mathrm{pred}_<$-closed. We show by induction that $f(x) = g(x)$ for all $x \in v$. Suppose $x \in v$ and for all $y < x$ (in v), we have $f(y) = g(y)$. So $f{\restriction}\mathrm{pred}_<(x) = g{\restriction}\mathrm{pred}_<(x)$. Then $f(x) = G(x, f{\restriction}\mathrm{pred}_<(x)) = G(x, g{\restriction}\mathrm{pred}_<(x)) = g(x)$. By Lemma 2.2.28, $\forall x \in v\ f(x) = g(x)$, as required. □

Lecture 11
17. May

For any set x, we call an approximation f with $x \in \mathrm{dom}(f)$ an *approximation at x*. The use of the next claim is to choose an approximation at x for each $x \in A$. Even the axiom of choice would not be useful here, since we need to make class many choices.

Claim. *Suppose that $x \in A$ and there is a approximation f at x. Then there is a (unique) $\subseteq$-least approximation f_x at x.*

Proof. It is easy to see that the intersection f of all approximations at x is a set by the Separation Scheme. The previous claim implies that f satisfies (1). To see that (2) holds for f, let g be any approximation at x. Then $f(y) = g(y) = G(y, g{\restriction}\mathrm{pred}_<(y)) = G(y, f{\restriction}\mathrm{pred}_<(y))$ for all $y \in \mathrm{dom}(f)$. □

A straightforward induction completes the proof.

Claim. *For any $x \in A$, there exists an approximation at x.*

Proof. By induction for $<$, we can assume that there exists an approximation at each $y < x$. By the Axiom of Union and the first claim, $f = \bigcup_{y<x} f_y$ is a set function. Moreover, it is easy to check that f is an approximation. If $x \in \mathrm{dom}(f)$, then we are done. Otherwise

$$g = f \cup \{(x, G(x, f{\restriction}\mathrm{pred}_<(x)))\}$$

is an approximation at x. □

By the first claim, $F = \bigcup_{y \in A} f_y\colon A \to V$ is a function, and one can easily check that it is guided by G.

It remains to show that any strongly wellfounded relation $(A, <)$ is wellfounded for classes. To see this, take some $x \in A$. By recursion for ω, we construct $g\colon \omega \to V$ with $g(0) = \{x\}$ and $g(n+1) = g(n) \cup \bigcup_{y \in g(n)} \mathrm{pred}_<(y)$. This is a set by the Replacement Scheme and the Axiom of Union. Then $\bigcup_{n \in \omega} g(n)$ is a $\mathrm{pred}_<$-closed set containing x. Apply wellfoundedness to this set to obtain a $<$-minimal element with respect to a given class. □

Exercise: Construct the least $\mathrm{pred}_<$-closed set by a direct recursion without the Axiom of Infinity.

There is no simple characterisation of those relations that allow recursion, as we have for induction. First of all, the reason why wellfoundedness for classes does not suffice in the proof is because the inductive hypothesis, i.e. the existence of class approximations, cannot be formulated in the language of set theory for wellorders beyond Ord. With the right formulation, one can prove recursion for $\mathrm{Ord} \cdot n$ for all $n \in \omega$.[21] However, it is independent of ZFC whether recursion of length $\mathrm{Ord} \cdot \omega$ holds.

This is no problem at all, since recursion for strongly wellfounded relations suffices for all purposes.

We now turn to ordinals and their basic properties.

Definition 2.2.30.

(1) (Transitive sets) A class A is called *transitive* if $\forall x, y\ (x \in y \in A \rightarrow x \in A)$, i.e. A is downwards closed with respect to $\in$.

(2) (Ordinals) A set x is called an *ordinal* if x is transitive and $(x, \in)$ is a strict linear order. Note that by the Axiom of Foundation, every ordinal is wellfounded. The point of taking transitive sets here is to have a unique ordinal for each order type.

(3) (Comparison of ordinals) For ordinals α, β, we write $\alpha < \beta :\Longleftrightarrow \alpha \in \beta$.

(4) (Successors and limits) An ordinal α is called a *successor ordinal* if $\alpha = \beta + 1 = \beta \cup \{\beta\}$ for some ordinal β. If $\alpha \neq 0$ is not a successor ordinal, then it is called a *limit ordinal.*

(5) Ord denotes the class of ordinals.

(6) ω denotes the (unique) $\subseteq$-least inductive set. Its elements are called *natural numbers.*

Recall that we define $0 := \emptyset$.

Lemma 2.2.31.

(1) Ord *is inductive.*

(2) Ord *is transitive.*

(3) *The relation* $<$ *is a strict linear order on* Ord*.*

(4) Ord *is a proper class.*

Proof.

(1) Clearly $0 \in \mathrm{Ord}$. Suppose that $\alpha \in \mathrm{Ord}$. To see that $\alpha + 1 \in \mathrm{Ord}$, suppose that $\gamma \in \beta \in \alpha + 1 = \alpha \cup \{\alpha\}$. We claim that $\gamma \in \alpha + 1$. There are two cases. If $\beta \in \alpha$, then $\gamma \in \alpha \subseteq \alpha + 1$, since α is transitive. If $\beta = \alpha$, then $\gamma \in \beta = \alpha \subseteq \alpha + 1$.

(2) Suppose that $\gamma \in \delta \in \mathrm{Ord}$. We claim that $\gamma \in \mathrm{Ord}$. Note that $(\gamma, \in)$ is a strict linear order, since $\gamma \subseteq \delta$ by transitivity of δ.

Call ordinals α, β *comparable* if the trichotomy $(\alpha < \beta) \vee (\alpha = \beta) \vee (\beta < \alpha)$ holds and *incomparable* otherwise.

To see that γ is transitive, take $\alpha \in \beta \in \gamma$. Since δ is transitive, $\alpha \in \delta$. Since $(\delta, \in)$ is a strict linear order, α and γ are comparable. Since $\alpha = \gamma$ and $\gamma \in \alpha$ contradict Lemma 2.2.21, we have $\alpha \in \gamma$ as required.

(3) Consider the strict partial order $(\alpha, \beta) < (\gamma, \delta) \Longleftrightarrow (\alpha < \gamma) \wedge (\beta < \delta)$ on $\mathrm{Ord} \times \mathrm{Ord}$. Clearly $(\mathrm{Ord} \times \mathrm{Ord}, <)$ is very strongly wellfounded and thus wellfounded for classes.

We show by induction along $(\mathrm{Ord} \times \mathrm{Ord}, <)$ that all pairs (α, β) are comparable. Suppose that there is an incomparable pair (α, β). Since $(\mathrm{Ord} \times \mathrm{Ord}, <)$ is wellfounded for classes, we can assume that (α, β) is $<$-minimal. It suffices to show that $\alpha = \beta$, since this would contradict the fact that α and β are incomparable. To see that $\alpha \subseteq \beta$, take any $\gamma \in \alpha$. By minimality of (α, β), β and γ are comparable. But $\beta = \gamma$ and $\beta \in \gamma$ would contradict the fact that α and β are incomparable. Thus $\gamma \in \beta$. Similarly, $\beta \subseteq \alpha$ and hence $\alpha = \beta$.

[21] We have not defined $\mathrm{Ord} \cdot n$ formally. We mean the product $\mathrm{Ord} \times n$ with the right-lexicographical order.

(4) Towards a contradiction, suppose that Ord is a set. Then by (3), Ord is an ordinal. We would then have Ord $\in$ Ord, contradicting the Axiom of Foundation.

□

The fact in (4) above that Ord is a proper class is called the Burali-Forti's paradoxon (1897). Burali-Forti showed that if there were a set Ω of all ordinals, then one could form its successor $\Omega + 1$, thus leading to the impossible inequality $\Omega < \Omega + 1 \leq \Omega$. This was known to Russell when he published his paradox in 1903.

Lemma 2.2.32.

(1) (Induction principle) *Any inductive subset x of ω equals ω*
(2) *ω is the least limit ordinal.*

Proof. (1) This is immediate, since ω is the $\subseteq$-least inductive set.

(2) We first show that ω is an ordinal. $(\omega, \in)$ is linearly ordered, since $\omega \subseteq \text{Ord}$. It remains to show that ω is transitive. Let $\varphi(x)$ denote the formula $x \subseteq \omega$. To show that $\varphi(n)$ holds for all $n \in \omega$, it suffices by (1) to show that $\{n \in \omega \mid \varphi(n)\}$ is inductive. Clearly $\varphi(0)$ holds. If $\varphi(n)$ holds, then $n+1 = n \cup \{n\} \subseteq \omega$ and hence $\varphi(n+1)$ holds.

We now show that ω is a limit ordinal. Otherwise, $\omega = \alpha + 1 = \alpha \cup \{\alpha\}$ for some $\alpha \in \text{Ord}$. Then $\alpha \in \omega$ and since ω is inductive, $\alpha + 1 \in \omega$, contradicting the Axiom of Foundation.

To see that all ordinals $\alpha < \omega$ are either successors or equal to 0, note that the set of these ordinals is inductive. By (1), this set equals ω. □

Let $\alpha \leq \beta$ denote $\alpha < \beta \vee \alpha = \beta$ for ordinals α, β.

Lecture 12
31. May

Lemma 2.2.33. *For ordinals α, β, we have $\alpha \leq \beta$ if and only if $\alpha \subseteq \beta$.*

Proof. $\Rightarrow$: If $\alpha \in \beta$, then $\alpha \subseteq \beta$ by transitivity of β. If $\alpha = \beta$, then the claim is obvious.

$\Leftarrow$: It suffices to show that $\beta < \alpha$ fails. But this would imply $\beta \in \beta$, contradicting the Axiom of Foundation. □

The next lemma is only included to show the existence of transitive closures. You can forget about it without losing anything essential.

If $<$ is a relation, we call a set x *$<$-closed* if for all $y \in x$, we have $\forall z\ (z < y \rightarrow z \in x)$. It is the same as $\text{pred}_<(x)$-closed.

Lemma 2.2.34.

(1) *If $<$ is a strongly wellfounded relation, then any $x \in \text{field}(<)$ is an element of some $<$-closed set.*
(2) *For any set x, there is a $\subseteq$-least transitive set that contains x as an element. This is called the* transitive closure $\text{tc}(x)$ *of x.*

Proof. (1) This was already done at the end of the proof of Theorem 2.2.29. By recursion for ω, we construct $g\colon \omega \rightarrow V$ with $g(0) = \{x\}$ and $g(n+1) = g(n) \cup \bigcup_{y \in g(n)} \text{pred}_<(y)$. Then $\bigcup_{n \in \omega} g(n)$ is a $<$-closed set containing x.

(2) It is easy to see that the intersection of (arbitarily many) transitive sets is again transitive. So the claim follows from (1). □

The next lemma shows that wellorders and ordinals are the same up to isomorphism. Every wellorder is represented by an ordinal.

It is easy to see that the following definitions can be done via the recursion theorem.

Definition 2.2.35.

(1) (a) $\alpha + 0 = \alpha$
(b) $\alpha + (\beta + 1) = (\alpha + \beta) + 1$

    (c) $\alpha+\gamma=\sup_{\beta<\gamma}(\alpha+\beta)$ for limits γ.
(2) (a) $\alpha\cdot 1=\alpha$
    (b) $\alpha\cdot(\beta+1)=(\alpha\cdot\beta)+\alpha$
    (c) $\alpha\cdot\gamma=\sup_{\beta<\gamma}(\alpha\cdot\beta)$ for limits γ.
(3) (a) $\alpha^0=1$
    (b) $\alpha^{\beta+1}=(\alpha^\beta)\cdot\alpha$
    (c) $\alpha^\gamma=\sup_{\beta<\gamma}(\alpha^\beta)$ for limits γ.

We already argued above that these definitions agree with the more intuitive definitions using sums and products of wellorders.

2.3. **Cardinals.** We will use the Power Set Axiom and the Axiom of Choice to prove that there are cardinals beyond ω.[22]

Axiom. (Power Set) $\forall x\ \exists y\ \forall z\ (z\in y\leftrightarrow z\subseteq x)$.

The set $\mathcal{P}(x)=\{z\mid z\subseteq x\}$ is called the power set of x.

A *choice function* for a set x is a function $f\colon x\to V$ with $f(y)\in y$ for all nonempty $y\in x$.

Axiom. (Axiom of Choice) Any set has a choice function.

Definition 2.3.1. ZF is the axiom system ZF^- with the Power Set Axiom. ZFC is the axiom system ZF with the Axiom of Choice.

From now on, we work in ZFC. The next lemma will allow us to associate a cardinal to any set.

Lemma 2.3.2. *For any set x, there is a bijection $f\colon\alpha\to x$ for some $\alpha\in\mathrm{Ord}$. If $(x,<)$ is a wellorder, then we can choose f as an isomorphism between $(x,<)$ and $(\alpha,<)$.*[23]

Proof. We write $\mathrm{ran}(x)=\{z\mid\exists y\ (y,z)\in x\}$ for any set x. (Previously, we had only defined this for relations.)

Let $g\colon(\mathcal{P}(x)\setminus\{\emptyset\})\to x$ be a choice function. Let x^* denote any set with $x^*\notin x$, for instance $x^*=x$.

Consider $G\colon\mathrm{Ord}\times V\to V$, where $G(\alpha,y)=g(x\setminus\mathrm{ran}(y{\restriction}\alpha))$ if $x\not\subseteq\mathrm{ran}(y{\restriction}\alpha)\neq\emptyset$ and $G(\alpha,y)=x^*$ otherwise.

By the recursion theorem, there is a unique function $F\colon\mathrm{Ord}\to V$ that is guided by G.

Claim. *Suppose that $\gamma\in\mathrm{Ord}$. If $x\not\subseteq\mathrm{ran}(F{\restriction}\alpha)$ for all $\alpha<\gamma$, then $(F{\restriction}\gamma)\colon\gamma\to x$ is injective.*

Proof. This follows from the fact that F is guided by G and from the definition of G. □

Note that $x\subseteq\mathrm{ran}(F{\restriction}\gamma)$ for some γ. Otherwise, $F\colon\mathrm{Ord}\to x$ is injective by the previous claim, contradicting the fact that Ord is a proper class and the Replacement Scheme. Let γ denote the least such ordinal.

By the previous claim, $(F{\restriction}\gamma)\colon\gamma\to x$ is injective. Thus $F{\restriction}\gamma\colon\gamma\to x$ is bijective.

For the second part of the lemma, let g be the choice function that picks the $<$-least element of a subset of x. It is easy to check that the function $F{\restriction}\gamma\colon\gamma\to x$ in the previous proof is an isomorphism between $(\gamma,<)$ and $(x,<)$. □

Recall that the ordinals are linearly ordered by inclusion. Hence by the previous lemma, for any two sets x and y there exists and injective function $f\colon x\to y$ or an injective function $g\colon y\to x$.

[22] The Power Set Axiom is necessary, while the Axiom of Choice could be avoided.

[23] It is easy to see there is a unique isomorphism.

Definition 2.3.3.

(1) A *cardinal* is an ordinal β such that for all $\alpha < \beta$, there is no bijective function $f\colon \alpha \to \beta$.
(2) Card denotes the class of cardinals.
(3) For any set x, the *size* (or *cardinality*) $|x|$ of x is the least $\alpha \in \mathrm{Ord}$ such that there exists a bijection $f\colon x \to \alpha$.

The next lemma is left as an exercise.

Lemma 2.3.4. *If there exists an injective function $f\colon \gamma \to \beta$ for some $\beta < \gamma$, then there exists an bijective function $g\colon \gamma \to \alpha$ for some $\alpha \leq \beta$. Hence $\gamma \notin \mathrm{Card}$.*

For a relation R, let $R^{-1} = \{(x,y) \mid (y,x) \in R\}$.

Lemma 2.3.5. *The following conditions are equivalent for sets x and y:*

(1) $|x| \leq |y|$.
(2) *There is an injective function $f\colon x \to y$.*
(3) *There is a surjective function $g\colon y \to x$.*

Proof. (1) ⇒ (2): This is clear.

(2) ⇒ (1): We can assume that y is a cardinal, i.e. $y = |y|$. By assumption, there is an injective function $f\colon |x| \to |y|$. If $|x| \leq |y|$, then we are done. If $|x| > |y|$, then we have a contradiction to the previous lemma.

(2) ⇒ (3): Suppose that $f\colon x \to y$ is an injective function. Fix any $x^* \in x$. Then $g\colon y \to x$,

$$g(z) = \begin{cases} f^{-1}(z) & \text{if } z \in \mathrm{ran}(f) \\ x^* & \textit{otherwise} \end{cases}$$

is surjective.

(3) ⇒ (2): Suppose that $g\colon y \to x$ is a surjective function. Let h be a choice function for $\mathcal{P}(y)$. Then $f\colon x \to y$, $f(z) = h(g^{-1}(z))$ is injective. □

Lemma 2.3.6. *For every $n \in \omega$, any injective function $f\colon n \to n$ is surjective. In particular, $n \in \mathrm{Card}$.*

Proof. We show this by induction. It is clear for $n = 0$.

Now suppose that claim holds for some $n \in \omega$. Suppose that $f\colon n+1 \to n+1$ is injective, but not surjective. We can assume that $f(n) = n$ by exchanging two values of f. In more detail, suppose first that $n \in \mathrm{ran}(f)$. Then $f(m) = n$ and $f(n) = k$ for some m, k. Then let $f(m) = k$ and $f(n) = n$, but leave the remaining values. Otherwise $n \notin \mathrm{ran}(f)$. Suppose that $f(n) = i$. Then let $f(n) = n$ and leave the remaining values.

A missing case has been added. (13. June)

Then $(f{\restriction}n)\colon n \to n$ is surjective by the induction hypothesis. It follows that f is surjective. □

The next lemma is left as an exercise:

Lemma 2.3.7. *For any set $x \subseteq \mathrm{Card}$, $\sup(x) \in \mathrm{Card}$. In particular, $\omega \in \mathrm{Card}$.*

Definition 2.3.8. A set x is called

(1) *finite* if $|x| < \omega$.
(2) *infinite* if x is not finite.
(3) *countable* if there is an injective function $f\colon x \to \omega$.
(4) *uncountable* if x is not countable.

Lemma 2.3.9. *(Cantor) $|\mathcal{P}(x)| > |x|$ holds for all sets x.*

Proof. We have $|x| \leq |\mathcal{P}(x)|$, since the function $f\colon x \to \mathcal{P}(x)$, $f(y) = \{y\}$, is injective by the Axiom of Extensionality.

Towards a contradiction, suppose that $|\mathcal{P}(x)| \leq |x|$. Note that there is a bijection between $\mathcal{P}(x)$ and $2^x = \{f \mid f\colon x \to 2\}$ by identifying sets with their characteristic functions. Using Lemma 2.3.5, we obtain exists a surjective function $g\colon x \to 2^x$. Let $f \in 2^x$ denote the unique function with $f(i) \neq g(i)(i)$ for all $i \in x$. Then $f \neq g(i)$ for all $i \in x$. This contradicts the fact that g is onto. □

Definition 2.3.10.

(1) For any $\alpha \in \mathrm{Ord}$, α^+ denotes the least cardinal $\lambda > \alpha$. (This is well defined by the previous lemma.)

(2) Cardinals of the form α^+ are called *successor cardinals*. The remaining cardinals $\lambda \neq 0$ are called *limit cardinals*.

(3) (The *Aleph-function*) We define $\aleph\colon \mathrm{Ord} \to \mathrm{Card}$ by recursion on $\alpha \in \mathrm{Ord}$:
   (a) $\aleph_0 = \omega$
   (b) $\aleph_{\alpha+1} = \aleph_\alpha^+$
   (c) $\aleph_\gamma = \sup_{\alpha<\gamma} \aleph_\alpha$ for limit ordinals γ.

The $\aleph$-function is strictly monotone, i.e. $\forall \alpha, \beta \in \mathrm{Ord}\ (\alpha < \beta \to \aleph_\alpha < \aleph_\beta)$. This can be proved easily by induction from the definition. In particular, the $\aleph$-function is injective. Since Ord is a proper class, by the Replacement Scheme, Card is a proper class as well.

$\aleph_\alpha$ is often denoted by ω_α.

Lecture 13
2. June

Lemma 2.3.11. *Every infinite cardinal κ equals $\aleph_\alpha$ for some $\alpha \in \mathrm{Ord}$.*

Proof. Let $\gamma = \sup\{\alpha \in \mathrm{Ord} \mid \aleph_\alpha \leq \kappa\}$.

We claim that $\aleph_\gamma \leq \gamma$. This is clear if γ is a successor ordinal. If γ is a limit ordinal, then $\aleph_\gamma = \sup_{\alpha<\gamma} \aleph_\alpha \leq \kappa$.

Hence $\aleph_\gamma \leq \kappa < \aleph_{\gamma+1} = \aleph_\gamma^+$, so $\kappa = \aleph_\gamma$. □

Definition 2.3.12.

(1) The *continuum hypothesis* CH states that $|\mathcal{P}(\aleph_0)| = \aleph_1$.

(2) The *generalised continuum hypothesis* GCH states that $|\mathcal{P}(\aleph_\alpha)| = \aleph_{\alpha+1}$ for all $\alpha \in \mathrm{Ord}$.

Definition 2.3.13.

(1) A function $f\colon \alpha \to \beta$ is called *cofinal* if $\mathrm{ran}(f)$ is unbounded in β, i.e. $\forall \beta' < \beta\ \exists \alpha' < \alpha\ (f(\alpha') > \beta')$.

(2) The *cofinality* $\mathrm{cof}(\kappa)$ of a cardinal κ is the least cardinal $\lambda \leq \kappa$ such that there exists a cofinal function $f\colon \lambda \to \kappa$.

(3) An infinite cardinal κ is called *regular* if $\mathrm{cof}(\kappa) = \kappa$ and *singular* otherwise.

For example, it is easy to see that $\mathrm{cof}(\aleph_\omega) = \omega$, so $\aleph_\omega$ is singular. On the other hand, one can show that $\aleph_n$ is regular for all $n \in \omega$. In fact all successor cardinals are regular.

Finally, we discuss Zorn's Lemma. This is useful for many applications, for instance that any vector space has a basis, any ring contains a maximal ideal. Many other similar results follow pretty directly from Zorn's Lemma.

Suppose that $(A, \leq)$ is a partial order. An element p of a subset B of A is called *maximal* in B if for any $q \geq p$ in B, $p = q$. ~~An element $q \in A$ is called *maximal* in $(A, \leq)$ if $p \leq q$ holds for all $p \in A$.~~ A subclass B of A is called a *chain* if it is linearly ordered by $\leq$. An element $q \in A$ is called an *upper bound* for a subclass B of A if $p \leq q$ holds for all $p \in B$. It is called *strict* if $p < q$ holds for all $p \in B$.

Lemma 2.3.14 (Zorn's Lemma). *Suppose that $(x, \leq)$ is a partially ordered set such that every linearly ordered subset has an upper bound. Then $(x, \leq)$ contains at least one maximal element.*

Proof. Towards a contradiction, suppose that $(x, \leq)$ has no maximal elements.

We claim that every chain y in $(x, \leq)$ has a strict upper bound. To see this, take any upper bound p for y. If this is not strict, then $p \in y$. Since p is not maximal in $(x, \leq)$, y has a strict upper bound.

Let $\mathrm{chain}(x, \leq)$ denote the set of chains in $(x, \leq)$. (This is a set by the Power Set Axiom and the Replacement Scheme.) By the Axiom of Choice, there exists a function $f\colon \mathrm{chain}(x, \leq) \to x$ such that for all $y \in \mathrm{chain}(x, \leq)$, $f(y)$ is a strict upper bound for y.

By recursion on $\alpha \in \mathrm{Ord}$, define

$$g(\alpha) = \begin{cases} f(g[\alpha]) & \text{if } g[\alpha] \text{ is a chain in } (x, \leq) \\ \emptyset & \text{otherwise.} \end{cases}$$

One can easily show by induction that for all $\alpha \in \mathrm{Ord}$, $g[\alpha]$ is a chain in $(x, \leq)$, so the second case in the definition never occurs, and that $g\colon \mathrm{Ord} \to x$ is injective. This contradicts the Replacement Scheme. □

2.4. **Tarski's undefinability of truth.** We now turn to metamathematical aspects of ZFC.

Why did we define truth $\mathcal{M} \models \varphi$ only for set models $\mathcal{M}$ and not for classes? Clearly, for any fixed formula φ and any class model $\mathcal{M}$, $\mathcal{M} \models \psi$ can be defined in the same way. But it is a different definition for each formula ψ. In fact, there is no uniform definition by the next result.

A *truth definition* is a formula $T(w, x, y, z)$ and a set parameter t such that for all formulas $\psi(x, y)$ and all sets r, s,

$$\psi(r, s) \iff T(\psi, r, s, t).$$

This is informal mathematical notation. More formally, one should write $(V, \in) \models \psi[r, s]$, and similiarly for $T(\psi, r, s, t)$.

It seems strange to plug in formulas into formulas. But that's posssible because the formulas are themselves elements of the class structure $(V, \in)$.

Theorem 2.4.1. *(Tarski) There is no truth definition.*

Proof. Suppose that $T(w, x, y, z)$ is a truth definition. Let $\psi(x, y)$ denote the formula $\neg T(x, x, y, y)$. Then

$$\psi(\psi, t) \iff \neg T(\psi, \psi, t, t).$$

This contradicts the assumption that T is a truth definition. □

A simpler case of the previous result is to show that there is no formula $T(x, y)$ such that for all formulas $\psi(x)$ and all words s,

$$\psi(s) \iff T(\psi, s).$$

Suppose that $T(x, y)$ is such a formula. Let $\psi(x)$ denote the formula $\neg T(x, x)$. Then $\psi(\psi) \iff \neg T(\psi, \psi)$, contradicting the assumption that T is a truth definition.

Informally, Tarski's result shows that one cannot express properties of classes by first-order formulas. One can also use the result to show that basic properties of classes such as $\{x \mid \varphi(x, y)\} = \emptyset$ cannot be expressed by a formula in φ and x.

An explanation of Tarski's undefinability of truth is given by the Levy hierarchy of formulas (see Wikipedia). Formulas with more quantifiers appear higher in the hierarchy. One can show that formulas with a certain number of quantifiers cannot be expressed by formulas with fewer quantifiers. This explains why a single formula such as T above does not suffice to express all formulas.

Undefinability of truth is also one of the main steps in the proof of Gödel's first incompleteness theorem.

3. Completeness and compactness

3.1. **Completeness of Hilbert's calculus.** In this section we prove that Hilbert's calculus is complete: if T is a set of $\mathcal{L}$-formulas and φ is an $\mathcal{L}$-formula with $T \models \varphi$, then $T \vdash_{\mathcal{L}} \varphi$. This theorem (in a slightly weaker variant) is originally due to Gödel. The proof that we present is essentially due to Henkin. We shall show that every $\mathcal{L}$-consistent $\mathcal{L}$-theory has a model. It is an easy exercise to show that this implies the completeness theorem.

To this end, we start with a consistent $\mathcal{L}$-theory and aim to build a model of T. To understand this task, think of the field axioms together with a set of first order conditions. If the conditions state e.g. that the field has characteristic 0, then such structures are already available. But in general, one does not know in advance how a model of the theory will look like. Roughly, the problem is that even for theories T of the form $\mathrm{Th}(\mathcal{M})$ for some structure $\mathcal{M}$, T often has less information than $\mathcal{M}$. For example, one cannot reconstruct the complex field from its theory in any sensible way.

However, such a reconstruction is possible if the structure is *canonical*. This means there is a constant symbol for each element. The following syntactical conditions suffice to ensure that a theory T equals the theory of a canonical model.

- T is complete (see Definition 1.5.14)
- T is *$\mathcal{L}$-deductively closed*, i.e. for all $\mathcal{L}$-sentences φ, $T \vdash_{\mathcal{L}} \varphi$ implies $\varphi \in T$.
- T is a *Henkin theory*, i.e. for any $\mathcal{L}$-formula φ and every free variable x in φ, it contains an $\mathcal{L}$-formula of the form
$$(\exists x \varphi) \to \varphi \frac{c}{x}.$$

Thus, we aim to extend T to a complete Henkin theory by recursion. We recursively expand both the language and the theory and thereby add more information about the structure that we aim to construct.

It is clear that any $\mathcal{L}$-complete $\mathcal{L}$-theory can be extended to an $\mathcal{L}$-deductively closed theory simply by adding all derivable sentences.

We first show how to extend any theory T to a complete theory.

Lemma 3.1.1. *Suppose that T is an $\mathcal{L}$-consistent $\mathcal{L}$-theory and φ is an $\mathcal{L}$-formula. Then $T \cup \{\varphi\}$ or $T \cup \{\neg\varphi\}$ is $\mathcal{L}$-consistent.*

Proof. Suppose that both theories are inconsistent. Then there are $\psi_0, \dots, \psi_n \in T$ with
$$\vdash_{\mathcal{L}} (\psi_0 \wedge \cdots \wedge \psi_n \wedge \neg\varphi) \to \bot$$
$$\vdash_{\mathcal{L}} (\psi_0 \wedge \cdots \wedge \psi_n \wedge \varphi) \to \bot.$$
By tautologies and the Modus Ponens, we have
$$\vdash_{\mathcal{L}} (\psi_0 \wedge \cdots \wedge \psi_n) \to \bot.$$
But then T would be $\mathcal{L}$-inconsistent, contrary to the assumption. □

Lemma 3.1.2. *Suppose that T is an $\mathcal{L}$-consistent $\mathcal{L}$-theory. Then there is an $\mathcal{L}$-consistent, $\mathcal{L}$-complete $\mathcal{L}$-theory $T' \supseteq T$.*

Proof. We assume that $\mathcal{L}$ is countable. The general case is proved similarly by transfinite recursion.

It is easy to see that there are only countably many $\mathcal{L}$-formulas. (This also follows from Exercise 26 (2).)

Suppose that $\langle \varphi_n \mid n \in \omega \rangle$ enumerates all $\mathcal{L}$-formulas. We construct a sequence $\langle T_n \mid n \in \omega \rangle$ of $\mathcal{L}$-consistent $\mathcal{L}$-theories by recursion. Let $T_0 = T$. Let $T_{n+1} = T_n \cup \{\varphi_n\}$ if $T_n \cup \{\varphi_n\}$ is consistent, and $T_{n+1} = T_n \cup \{\neg\varphi_n\}$. T_{n+1} is $\mathcal{L}$-consistent by Lemma 3.1.1. Then $T' = \bigcup_{n \in \omega} T_n$ is $\mathcal{L}$-consistent. Clearly, T' is complete. □

The second step is to extend T to a Henkin theory. It can be necessary to extend the language, since for example T might not contain any constant symbols.

Lemma 3.1.3. *Suppose that T is a consistent $\mathcal{L}$-theory, φ is an $\mathcal{L}$-formula, x is a free variable in φ*[24] *and c is a new constant. Then the $\mathcal{L}\cup\{c\}$-theory $T' := T\cup\{(\exists x\varphi)\to\varphi\frac{c}{x}\}$ is $\mathcal{L}\cup\{c\}$-consistent.*

Proof. Suppose that T' is inconsistent. Then there are $\psi_0,\dots,\psi_n \in T$ such that for $\psi=\psi_0\wedge\cdots\wedge\psi_n$,

$$\vdash_{\mathcal{L}\cup\{c\}} \psi\to\neg((\exists x\ \varphi)\to\varphi\frac{c}{x}).$$

By tautologies,

$$\vdash_{\mathcal{L}\cup\{c\}} (\neg\exists x\ \varphi)\to\neg\psi$$

and

$$\vdash_{\mathcal{L}\cup\{c\}} \varphi\frac{c}{x}\to\neg\psi.$$

By Lemma 1.5.17,

$$\vdash_{\mathcal{L}} (\neg\exists x\ \varphi)\to\neg\psi$$

and

$$\vdash_{\mathcal{L}} \varphi\to\neg\psi.$$

Note that ψ has no free variables, since T is a theory. By $\exists^{\to}$-introduction, we have

$$\vdash_{\mathcal{L}} (\exists x\varphi)\to\neg\psi.$$

By tautologies, $\vdash_{\mathcal{L}}\neg\psi$. But then T would be inconsistent. □

Lecture 14
7. June

Lemma 3.1.4. *Suppose that T is an $\mathcal{L}$-consistent $\mathcal{L}$-theory. Then there is a set C of new constants and an $\mathcal{L}\cup C$-consistent Henkin $\mathcal{L}\cup C$-theory T^+.*

Proof. We will define a sequence $\langle C_n \mid n\in\omega\rangle$ of disjoint sets of constants and write $\mathcal{L}_n=\mathcal{L}\cup C_0\cup\cdots\cup C_n$. We will define a $\subseteq$-increasing sequence $\langle T_n\mid n\in\omega\rangle$ of $\mathcal{L}_n$-consistent $\mathcal{L}_n$-theories.

Let $T_0=T$ and $C_0=\emptyset$. Now suppose that $\langle C_i,T_i\mid i\leq n\rangle$ are defined for some $n\geq 0$. Choose a set C_{n+1} of new constants which consists of a constant c_φ for each $\mathcal{L}$-formula $\varphi(x)\in T_n$ with a single free variable x. By Lemmas 3.1.3 and 1.5.17,

$$T_{n+1}:=T_n\cup\{(\exists x\varphi)\to\varphi\frac{c_\varphi}{x})\mid\ \varphi \text{ is an } \mathcal{L}\text{-formula, } x \text{ is a free variable in } \varphi\ \}$$

is $\mathcal{L}\cup\{c_\varphi\}$-consistent. More precisely, suppose that $T_{n+1}\vdash_{\mathcal{L}_{n+1}}\bot$. Then there are $\varphi_0,x_0,\dots,\varphi_k,x_k$ as above such that

$$T_n\cup\{(\exists x_i\varphi_i)\to\varphi_i\frac{c_{\varphi_i}}{x})\mid i\leq k\}\vdash_{\mathcal{L}_{n+1}}\bot.$$

By Lemma 1.5.17

$$T_n\cup\{(\exists x_i\varphi_i)\to\varphi_i\frac{c_{\varphi_i}}{x})\mid i\leq k\}\vdash_{\mathcal{L}_n\cup\{c_{\varphi_i}\mid i\leq k\}}\bot,$$

but this contradicts Lemma 3.1.3.

Thus $T^+=\bigcup_{n\geq 0}T_n$ is a consistent Henkin theory. □

[24] It suffices below to assume that x is the only free variable in φ. So one could also define the notion of Henkin theory only for such formulas.

Suppose that T is an $\mathcal{L}$-consistent $\mathcal{L}$-theory. By Lemma 3.1.4, we can extend T to an $\mathcal{L}_0$-consistent $\mathcal{L}_0$-Henkin theory T_0 for some $\mathcal{L}_0 \supseteq \mathcal{L}$. T_0 can be extended to an $\mathcal{L}_0$-complete $\mathcal{L}_0$-theory by Lemma 3.1.2. The theory of all $\mathcal{L}$-sentences $\mathcal{L}$-provable from this theory is $\mathcal{L}$-deductively closed.

Only the next step remains to prove the completeness theorem.

Lemma 3.1.5. *Suppose that T is an $\mathcal{L}$-consistent $\mathcal{L}$-theory. Then the following conditions are equivalent:*

(1) $T = \mathrm{Th}(\mathcal{M})$ *for some canonical $\mathcal{L}$-structure $\mathcal{M}$.*
(2) T *is an $\mathcal{L}$-complete Henkin theory.*

Proof. (1) $\Longrightarrow$ (2): This is clear.

(2) $\Longrightarrow$ (1): Since T is $\mathcal{L}$-complete, it is $\mathcal{L}$-deductively closed. We will use this throughout the proof.

One can construct the *term model* of T as follows. The underlying set is given by $\mathcal{L}$-constant symbols. Let $c \sim d :\Leftrightarrow (c \doteq d) \in T$ for constant symbols $c, d \in \mathcal{L}$ and let $[c]$ denote the $\sim$-equivalence class of c. The next claim shows that this is well-defined. Let $M = \{[c] \mid c \in \mathcal{L} \text{ is a constant}\}$ be the underlying set of the term model $\mathcal{M}$.

Claim. *$c \sim d :\Leftrightarrow (c \doteq d) \in T$ defines an equivalence relation on the set of constant symbols in $\mathcal{L}$.*

Proof. $\sim$ is reflexive: $(c \doteq c) \in T$ holds by the equality axioms and the $\forall^{\rightarrow}$-axiom.

$\sim$ is symmetric: If $(c \doteq d) \in T$, then $(d \doteq c) \in T$ holds by the equality axioms and the $\forall^{\rightarrow}$-axiom.

$\sim$ is transitive: Suppose that $(c \doteq d) \in T$ and $(d \doteq e) \in T$. Then $(c \doteq e) \in T$, since by the equality axioms $(c \doteq d \wedge d \doteq e \rightarrow c \doteq e) \in T$. □

Next, we define the interpretations of constant symbols, relation symbols and function symbols. Let $c^{\mathcal{M}} = [c]$ for constant symbols c.

For relation symbols R, let $R^{\mathcal{M}}([c_0], \dots, [c_n]) :\Longleftrightarrow R(c_0, \dots, c_n) \in T$. the next claim shows that this is well-defined.

Claim. *If $(c_0 \doteq d_0), \dots, (c_n \doteq d_n), R(c_0, \dots, c_n) \in T$, then $R(d_0, \dots, d_n) \in T$.*

Proof. By the equality axioms for relation symbols. □

For function symbols f, let $f^{\mathcal{M}}([c_0], \dots, [c_n]) = [c] :\Longleftrightarrow (f(c_0, \dots, c_{n-1}) = c) \in T$. This is well-defined by the next two claims.

Claim. *If $(c_0 \doteq d_0), \dots, (c_n \doteq d_n), f(c_0, \dots, c_n) = e, f(d_0, \dots, d_n) = e' \in T$, then $(e = e') \in T$.*

Proof. By the equality axioms for function symbols. □

Claim. *For any n-ary function symbol $f \in \mathcal{L}$ and constant symbols $c_0, \dots, c_{n-1} \in \mathcal{L}$, there is a constant symbol $c \in \mathcal{L}$ with $(f(c_0, \dots, c_{n-1}) = c) \in T$.*

Proof. Since $\vdash_{\mathcal{L}} f(c_0, \dots, c_n) \doteq f(c_0, \dots, c_n)$, the ${}^{\rightarrow}\exists$-axiom implies $\vdash_{\mathcal{L}} \exists x\, f(c_0, \dots, c_n) \doteq x$. Since T is a Henkin theory, there is a constant symbol $c \in \mathcal{L}$ such that

$$((\exists x\ f(c_0, \dots, c_n) \doteq x) \rightarrow f(c_0, \dots, c_n) \doteq c) \in T.$$

Therefore $f(c_0, \dots, c_n) \doteq c \in T$. □

Claim. *If t is an $\mathcal{L}$-term with no free variables, then $t^{\mathcal{M}} = [c] \Longleftrightarrow (t \doteq c) \in T$.*

Proof. By induction on terms.

Suppose that $t = d$ is a constant symbol. If $t^{\mathcal{M}} = [c]$, then $[c] = t^{\mathcal{M}} = [d]$, so $(c \doteq d) \in T$ by the definition of $\sim$.

Suppose that $t = f(t_0, \dots, t_n)$. By the previous claim, find constant symbols with $(t_i = c_i) \in T$ for $i \leq n$. Thus $(f(t_0, \dots, t_n) \doteq f(c_0, \dots, c_n)) \in T$. By the inductive hypothesis, $t_i^{\mathcal{M}} = [c_i]$ for $i \leq n$.

We have $f(c_0, \dots, c_n)^{\mathcal{M}} = [c] \iff (f(c_0, \dots, c_n) \doteq c) \in T$ by the definition of $f(c_0, \dots, c_n)^{\mathcal{M}}$. Since T is deductively closed, the claim follows. □

Claim. $\mathrm{Th}(\mathcal{M}) = T$.

Proof. We show by induction that for all $\mathcal{L}$-sentences φ,

$$\mathcal{M} \models \varphi \iff \varphi \in T.$$

First suppose that $\varphi = (s \doteq t)$. Suppose that $s^{\mathcal{M}} = [c]$ and $t^{\mathcal{M}} = [d]$. Then $(s \doteq c), (t \doteq d) \in T$ by the previous claim. Then

$$\mathcal{M} \models \varphi \Leftrightarrow [c] = [d] \Leftrightarrow (c \doteq d) \in T \Leftrightarrow (s \doteq t) \in T.$$

Suppose that $\varphi = (R(t_0, \dots, t_n))$. Suppose that $t_i^{\mathcal{M}} = [c_i]$ for $i \leq n$. Then

$$\mathcal{M} \models \varphi \Leftrightarrow R(t_0, \dots, t_n) \in T \Leftrightarrow (R(t_0, \dots, t_n)) \in T.$$

Suppose that $\varphi = (\neg\psi)$. Since T is complete,

$$\mathcal{M} \models \varphi \Leftrightarrow \mathcal{M} \not\models \psi \Leftrightarrow \psi \notin T \Leftrightarrow \varphi \in T.$$

Suppose that $\varphi = (\psi \wedge \theta)$. Then

$$\mathcal{M} \models \varphi \Leftrightarrow (\mathcal{M} \models \psi \text{ and } \mathcal{M} \models \theta) \Leftrightarrow (\psi \in T \text{ and } \theta \in T) \Leftrightarrow (\psi \wedge \theta) \in T.$$

Suppose that $\varphi = (\exists x\ \psi)$. Then

$$\begin{aligned} \mathcal{M} \models (\exists x\ \psi) &\iff \mathcal{M} \models \psi[[c]] \text{ for some constant symbol } c \in \mathcal{L} \\ &\iff \mathcal{M} \models \psi\tfrac{c}{x} \text{ for some constant symbol } c \in \mathcal{L} \\ &\iff (\psi\tfrac{c}{x} \in T) \text{ for some constant symbol } c \in \mathcal{L} \\ &\iff (\exists x\ \psi) \in T. \end{aligned}$$

The second equivalence holds by Lemma 1.5.11 (substitution for formulas). The third holds by the inductive hypothesis. □

This completes the proof of Lemma 3.1.5. □

Lecture 15
9. June

Theorem 3.1.6 (Completeness of Hilbert's calculus).

(1) *Any consistent $\mathcal{L}$-theory has a model.*
(2) *For any $\mathcal{L}$-theory T and any $\mathcal{L}$-sentence:*

$$(T \vdash_{\mathcal{L}} \varphi) \iff (T \models \varphi).$$

Proof. (1): By Lemmas 3.1.2, 3.1.4 and 3.1.5.

(2): $\Longrightarrow$: Suppose that $T \vdash_{\mathcal{L}} \varphi$. Then there are formulas $\psi_0, \dots, \psi_n \in T$ with $\vdash_{\mathcal{L}} (\psi_0 \wedge \cdots \wedge \psi_n) \to \varphi$. If $\mathcal{M} \models T$, then $\mathcal{M} \models \psi_0 \wedge \cdots \wedge \psi_n$ and hence $\mathcal{M} \models \varphi$, as required.

$\Longleftarrow$: Suppose that $T \not\vdash_{\mathcal{L}} \varphi$. Then $T \cup \{\neg\varphi\}$ is $\mathcal{L}$-consistent. By (1), there is a model $\mathcal{M}$ of $T \cup \{\neg\varphi\}$. Thus $T \not\models \varphi$. □

3.2. The Compactness Theorem and applications.

Definition 3.2.1.

(1) A theory T is called *satisfiable* if there is a model $M \models T$.
(2) A theory T is called *finitely satisfiable* if every finite $T_0 \subseteq T$ has a model.

Theorem 3.2.2 (Compactness theorem). *Every finitely satisfiable theory is satisfiable.*

Proof. Suppose that T is not satisfiable. Then $T \models \theta$ for all $\mathcal{L}$-sentences θ. Then $T \vdash_{\mathcal{L}} \theta$ for all $\mathcal{L}$-sentences θ by Theorem 3.1.6. By the definition of $\vdash_{\mathcal{L}}$, there are $\psi_0, \dots, \psi_n \in T$ with $\vdash_{\mathcal{L}} (\psi_0 \wedge \dots \wedge \psi_n) \to \bot$. Then $T_0 := \{\psi_0, \dots, \psi_n\}$ is not satisfiable. □

3.2.1. *From finite to infinite.*

Lemma 3.2.3. *If a theory T has models of size $\geq n$ for arbitrarily large $n \in \mathbb{N}$, then it has an infinite model.*

Proof. Recall the sentence

$$\varphi_{\geq n} = \exists x_0 \dots \exists x_{n-1} \bigwedge_{i<j\leq n-1} \neg(x_i \doteq x_j)$$

from Example 1.4.5, which axiomatises the class of structures with $\geq n$ elements in the empty language. Let

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

By assumption $T \cup T_\infty$ is finitely satisfiable. By the compactness theorem, it has a model $\mathcal{M}$. Then $\mathcal{M}$ is infinite. □

Definition 3.2.4. Suppose that $\mathcal{K} = (K, 0, 1, +, \cdot)$ is a field. The *characteristic* $\operatorname{char}(\mathcal{K})$ is the least $n \in \mathbb{N}$ such that $1 + 1 + \dots + 1$ (n times) $= 0$, if such an n exists. (One then says that $\mathcal{K}$ has *positive characteristic*.) Otherwise $\mathcal{K}$ has characteristic 0.

Let T_{field} denote the theory of fields.

Lemma 3.2.5. *If a theory $T \supseteq T_{\mathit{field}}$ has models of characteristic $\geq n$ for arbitrarily large $n \in \mathbb{N}$, then it has a model of characteristic* 0*.*

Proof. For primes p, let

$$\varphi_{\text{char}\neq p} = 1 + 1 + \dots + 1 \ (p \text{ times}) \neq 0$$

$$\varphi_{\text{char}\geq n} = \bigwedge_{1\leq p<n,\ p \text{ prime}} \varphi_{\text{char}\neq p}$$

and $T_{\text{char}=0} = \{\varphi_{\text{char}\geq n} \mid n \geq 1\}$. Note that the models of $T_{\text{char}=0}$ are precisely the fields of characteristic 0.

$T \cup T_{\text{char}}$ is finitely satisfiable by the assumption and hence it has a model $\mathcal{M}$. Then $\mathcal{M}$ has characteristic 0. □

If a property holds for all finite subsets of a given structure, one can often conclude via the Compactness Theorem that the property holds for the entire structure.

For example, a graph $\mathcal{G} = (G, E)$ consists of sets G and $E \subseteq [G]^2$. (Thus, by definition, $\mathcal{G}$ has no *loops*, i.e. edges connecting a vertex with itself.) $\mathcal{G}$ is called *k-colourable* if there is a function $f \colon G \to \{0, \dots, k-1\}$ such that $f(x) \neq f(y)$ whenever x, y are connected by an edge. By an *(induced) subgraph* of a graph $\mathcal{G}$ we mean the restriction of $\mathcal{G}$ to a subset of G.

Lemma 3.2.6. *If every finite subgraph of a graph $\mathcal{G} = (G, E)$ is k-colourable, then $\mathcal{G}$ is k-colourable.*

Proof. The language $\mathcal{L}$ of graphs consists of a single binary relation symbol R. Extend $\mathcal{L}$ to $\mathcal{L}'$ by adding a constant symbol d_i for each element $i \in G$ and a unary relation symbol C_i for each $i < k$. T is the $\mathcal{L}'$-theory that consists of the formulas:[25]

(1) $d_i \neq d_j$ for all $i \neq j$ in G.
(2) $R(d_i, d_j)$ if $(i, j) \in E$ and $\neg R(d_i, d_j)$ otherwise, for all $i \neq j$ in G.

[25] A variation of this proof still works if (3) and (4) are replaced with the relevant atomic formulas with constant symbols d_i instead of quantifying over x. Then the compactness theorem for propositional logic suffices.

(3) $\forall x \ \bigvee_{i<k} C_i(x)$.
(4) $\bigwedge_{i<k} \ \forall x, y \ (R(x,y) \to \neg(C_i(x) \wedge C_i(y)))$.

Since every finite subgraph of $\mathcal{G}$ is k-colourable, T is finitely satisfiable. By the compactness theorem, T has a model $\mathcal{H}$. Since $\mathcal{H}$ satisfies (1) and (2), it is easy to see that there is an embedding of $\mathcal{G}$ into $\mathcal{H}$ (i.e. an injective homomorphism, see Definition 1.1.6). Since $\mathcal{H}$ satisfies (3) and (4), there is a k-colouring of $\mathcal{H}$. The restriction to $\mathcal{G}$ is a k-colouring of $\mathcal{G}$. □

Write $[A]^n$ for the class of n-element subsets of A.

Lemma 3.2.7 (Infinite Ramsey's theorem). *Suppose that A is an infinite subset of $\mathbb{N}$, $k \geq 0$, $n \geq 1$ and $c \colon [A]^n \to \{0, 1, \ldots, k\}$ is a function. (We call c a* colouring*.) Then there is an infinite set $B \subseteq A$ with $|c[[B]^n]| = 1$. (B is called* homogeneous *or* monochromatic *for c.)*

Proof. The case for arbitrary $k \geq 1$ follow from the case $k = 1$ by iterated application of the case $k = 1$. We thus assume $k = 1$.

The case $n = 1$ is clear: if we split $\mathbb{N}$ into two sets, at least one of them is infinite. (This is called the *pigeonhole principle.*)

For the induction step, suppose that the claim holds for some $n \geq 1$. Suppose that $c \colon [A]^{n+1} \to \{0, 1\}$ is given.

We will inductively construct a $\subseteq$-decreasing sequence $\vec{B} = \langle B_j \mid j \in \mathbb{N} \rangle$ of subsets of A and a strictly increasing sequence $\vec{a} = \langle a_j \mid j \in \mathbb{N} \rangle$ in A with $a_j \in B_j$.

Let $B_0 = A$ and pick any $a_0 \in A$ (for instance, the least element of A). For the successor step, write

$$c_{a_0}(x) = c(\{a_0\} \cup x)$$

for $x \in [B_0]^n$ with $\min(x) > a_0$. by the induction hypothesis for n, there is an infinite subset $B_1 \subseteq B_0$ that is homogeneous for c_{a_0}. Then for some $i_0 \in \{0, 1\}$, $c(a_0 \cup x) = i_0 \leq 1$ for all $x \in [B_1]^n$. Since this property remains true for all subsets of B_1, we can assume that $a_0 < \min(B_1)$ by shrinking B_1. Pick $a_1 \in B_1$ and continue the construction of a_2, B_2 etc. similarly.

Once this has been completed, take $i \leq 1$ such that $J = \{j \in \mathbb{N} \mid i_j = i\}$ is infinite. Then $\{a_j \mid j \in J\}$ is homogeneous for c by the construction. □

Lecture 16
14. June

Next is a short proof of the finite Ramsey's theorem from the infinite Ramsey's theorem via the Compactness Theorem.

Lemma 3.2.8 (Finite Ramsey's theorem). *For all $k, l \in \mathbb{N}$ and $n \geq 1$, there is some $N \in \mathbb{N}$*[26] *such that for any colouring $c \colon [\{0, \ldots, N-1\}]^n \to \{0, \ldots, k-1\}$, there is a homogeneous set $H \subseteq \{0, \ldots, N-1\}$ for c of size l.*

Proof. We can assume that $l \geq k$. Let $\mathcal{L} = \{f\} \cup \{c_i \mid i \in \mathbb{N}\}$, where f is an n-ary function symbol and c_i is a constant symbol for $i \in \mathbb{N}$.

The next formula ψ_N holds in an $\mathcal{L}$-structure $\mathcal{M}$ if and only if there exists a homogeneous subset of size l for $f^{\mathcal{M}} \restriction \{c_i^{\mathcal{M}} \mid i \leq N\}$:

$$\psi_N := \bigvee_{I \in [\{0 \ldots, N\}]^l} \ \bigvee_{m<k} \ \bigwedge_{\{i_0, \ldots, i_{n-1}\} \in [I]^n} f(c_{i_0}, \ldots, c_{i_{n-1}}) = c_m$$

By the assumption, Let T be the theory that consists of the formulas $\neg\psi_N$ for $N \geq l$, the formulas $c_i \neq c_j$ for $i \neq j$, a formula θ asserting that $f(x_0, \ldots, x_{n-1})$ does not depend on

[26] We use an uppercase N to sugggest that N is very large compared to k and l. See the remark after the lemma.

the order of its arguments:

$$\theta := \forall x_0, \dots, x_{n-1} \ ((\bigwedge_{\pi \in \mathrm{Aut}_n} f(x_0, \dots, x_{n-1}) = f(x_{\pi(0}, \dots, x_{\pi(n-1)})\},$$

where Aut_n denotes the set of bijections $\pi \colon \{0, \dots, n-1\} \to \{0, \dots, n-1\}$, and a formula χ which states that f is a colouring:

$$\chi := \forall x_0, \dots, x_{n-1} \ ((\bigwedge_{i<j<n} x_i \neq x_j) \to \bigvee_{m<k} f(x_0, \dots, x_{n-1}) = c_m),$$

T is finitely satisfiable: for any $N \in \mathbb{N}$, there exists a colouring $g \colon [\{0, \dots, N\}]^n \to \{0, \dots, k-1\}$ with no homogeneous set of size l. Take this colouring on $\{c_0^{\mathcal{N}}, \dots, c_N^{\mathcal{N}}\}$ and extend it in an arbitrary way.

By the Compactness Theorem, there exists a model $\mathcal{M}$ of T. We can assume that $c_i^{\mathcal{N}} = i$ and $\mathbb{N}$ is the underlying set of $\mathcal{M}$, since the restriction of $\mathcal{M}$ to $\{c_i^{\mathcal{N}} \mid i \in \mathbb{N}\}$ is also a model of T.

Then there is no homogeneous set of size l for $f^{\mathcal{M}}$, and in particular no infinite one. This contradicts the infinite Ramsey's theorem. □

It is known that N grows extremely fast (exponentially) relative to l. For $k = 2$, the least such N is called the *Ramsey number* $R(l, l)$. (See the Wikipedia article on Ramsey's theorem.)

3.2.2. *(Finitely) axiomatisable classes.* The theory $T_{\mathrm{char}=0}$ in Lemma 3.2.5 axiomatises the class of fields with characteristic 0. Let $\mathcal{L}_{\mathrm{ring}}$ denote the language of rings and fields.

Lemma 3.2.9. *The class of fields of positive characteristic is not axiomatisable in $\mathcal{L}_{\mathrm{ring}}$.*

Proof. Towards a contradiction, suppose that T is an axiomatisation. For every prime p, $\mathbb{Z}/\mathbb{Z}p$ is a field wich characteristic p. (This is not hard to check.) Thus by Lemma 3.2.5, T has models of characteristic 0. □

The class of fields of characteristic 0 is not finitely axiomatisable in $\mathcal{L}_{\mathrm{ring}}$ by the next lemma. Otherwise, the class of fields of positive characteristic is axiomatisable in $\mathcal{L}_{\mathrm{ring}}$ by the next lemma, using the obvious fact that class of fields is axiomatisable.

Note that it is easy to see the class of fields of characteristic 0 is axiomatisable by language extension.

Lemma 3.2.10. *The following conditions are equivalent for any class $\mathcal{C}$ of $\mathcal{L}$-structures:*

(1) *$\mathcal{C}$ is finitely axiomatisable in $\mathcal{L}$.*
(2) *$\mathcal{C}$ is axiomatisable in $\mathcal{L}$ and its complement (i.e., the class of $\mathcal{L}$-structures not in $\mathcal{C}$)*[27] *is axiomatisable in $\mathcal{L}$.*

Proof. (1) ⇒ (2): Suppose that $T = \{\psi_0, \dots, \psi_n\}$ axiomatises $\mathcal{C}$. Let $\phi = (\psi_0 \wedge \dots \wedge \psi_n)$. Then $\{\phi\}$ axiomatises $\mathcal{C}$ and $\{\neg\phi\}$ axiomatises its complement.

(2) ⇒ (1): Suppose that T axiomatises $\mathcal{C}$ and T' axiomatises its complement. Then $T \cup T'$ is not satisfiable. By the Compactness Theorem 3.2.2, there are finite sets $S \subseteq T$ and $S' \subseteq T'$ such that $S \cup S'$ is not satisfiable.

We claim that S axiomatises $\mathcal{C}$. To see this, suppose that $\mathcal{M} \models S$. Since $S \cup S'$ is not satisfiable, $\mathcal{M} \not\models S'$ and hence $\mathcal{M} \not\models T'$. Thus $\mathcal{M} \in \mathcal{C}$. □

[27] For example, the complement of the class of fields with characteristic 0 in the class of $\mathcal{L}_{\mathrm{ring}}$-structures consists of fields with positive characteristic and those $\mathcal{L}_{\mathrm{ring}}$-structures that are not fields.

3.2.3. *The Löwenheim-Skolem theorems.*

Lemma 3.2.11. *For all infinite cardinals κ, we have $|\kappa \times \kappa| = \kappa$, $|[\kappa]^{<\omega}| = \kappa$.*

Proof. For $\kappa = \omega$, this was shown in exercise 26. We leave out the general case for time reasons (see Schimmerling: A course in Set Theory), although it is not difficult. □

The completeness theorem provides us with a model of any consistent theory. One can ask which sizes these models can have. The next theorem gives a complete answer by a direct application of the compactness theorem: an $\mathcal{L}$-theory with infinite models has models of all sizes $\geq |\mathcal{L}|$.

Theorem 3.2.12. *The following conditions are equivalent for any $\mathcal{L}$-theory T:*

(1) *For all $n \in \mathbb{N}$, T has a model of size $\geq n$*
(2) *T has an infinite model.*
(3) *T has models of size κ for any infinite cardinal $\kappa \geq |\mathcal{L}|$.*

Proof. It suffices to show (2)$\Longrightarrow$(3). Let $\mathcal{L}' = \mathcal{L} \cup \{c_\alpha \mid \alpha < \kappa\}$, where c_α are distinct new constant symbols. The theory $T' = T \cup \{c_\alpha \neq c_\beta \mid \alpha \neq \beta\}$ is finitely satisfiable. We constructed a model $\mathcal{M}$ of T' in the proof of the completeness theorem. In fact, in each step of the construction, only κ many new constant symbols were added, since there are precisely $|[\kappa]^{<\omega}| = \kappa$ (by Lemma 3.2.11) many new formulas. Therefore, the whole construction adds at most $|\kappa \times \omega| = \kappa$ (by Lemma 3.2.11) many constant symbols. So $\mathcal{M}$ has size κ. □

It remains to understand what are the sizes of elementary substructures and elementary superstructures of a given structure $\mathcal{M}$. (Recall the definition of elementary substructures in Section 1.3.) The Löwenheim-Skolem theorems fully answer this question.

The theory $\mathrm{Th}_{\mathcal{L}_A}(\mathcal{M}_A)$ (see Example 1.1.9) in the next lemma is also called the *elementary diagram* of $\mathcal{M}$. It is essentially a list of all tuples in $\mathcal{M}$ and the formulas true for these tuples in $\mathcal{M}$.

Lemma 3.2.13. *Suppose that $\mathcal{M}$ is an $\mathcal{L}$-structure with underlying set A. If $\mathcal{N}$ is a model of $\mathrm{Th}_{\mathcal{L}_A}(\mathcal{M}_A)$, then $\mathcal{M} \prec \mathcal{N}$.*

Proof. Suppose that $\mathcal{N}$ is a structure on a set B. Let $f\colon A \to B$ be the function $c \mapsto c^{\mathcal{N}}$. Since $\mathcal{N}$ is a model of $\mathrm{Th}_{\mathcal{L}_A}(\mathcal{M}_A)$, f is an elementary embedding. □

Theorem 3.2.14 (Upward Löwenheim-Skolem Theorem). *Any infinite $\mathcal{L}$-structure $\mathcal{M}$ on a set A has an elementary superstructure of any infinite size $\kappa \geq |A|, |\mathcal{L}|$.*

Proof. $|\mathcal{L}_A| = \kappa$ by Lemma 3.2.11. Thus $\mathrm{Th}_{\mathcal{L}_A}(\mathcal{M}_A)$ has models of any size $\geq \kappa$ by Theorem 3.2.12. These are superstructures of $\mathcal{M}$ by Lemma 3.2.13. □

Lecture 17
16. June

The construction of elementary substructures in the next result is direct and does not use the compactness theorem.

Suppose that $\mathcal{N}$ is an $\mathcal{L}$-structure on a set B. It follows from Exercise 5 that a subset A of B is the domain of a substructure of $\mathcal{N}$ if and only if A contains $c^{\mathcal{N}}$ and is closed under $f^{\mathcal{N}}$ for all constant symbols c and function symbols f in $\mathcal{L}$. To construct a substructure, one can start with a subset A_0 of A containing all $c^{\mathcal{N}}$ and obtain A_{n+1} from A_n by adding all $f^{\mathcal{N}}(a_0, \ldots, a_k)$ for $a_0, \ldots, a_k \in A_n$. Then $\bigcup_{n\in\omega} A_n$ is as required.

For an elementary substructure, we want to additionally satisfy the condition in Tarski's Test 1.3.7: *if there is some $b \in N$ with $\mathcal{N} \models \varphi[b, a_0, \ldots, a_n]$, then there is some $a \in M$ with $\mathcal{N} \models \varphi[a, a_0, \ldots, a_n]$.* So we want to add a witness to each such formula in every step of the construction. Functions providing such witnesses are called Skolem functions:

Definition 3.2.15. Suppose that $\mathcal{N}$ is an $\mathcal{L}$-structure on a set B and $\varphi(x_0, \dots, x_n, y)$ is an $\mathcal{L}$-formula. A *Skolem function* for φ is a partial function $f_\varphi^\mathcal{N} \colon B^{n+1} \to B$ such that for all $(b_0, \dots, b_n) \in B^{n+1}$: if $\mathcal{N} \models (\exists y\ \varphi)[b_0, \dots, b_n]$, then $\mathcal{N} \models \varphi(b_0, \dots, b_n, f^\mathcal{N}_{\varphi(b_0,\dots,b_n)})$.

Skolem functions exist by to the Axiom of Choice. (In fact, they cannot be constructed without it.)

Theorem 3.2.16 (Downward Löwenheim-Skolem Theorem). *Suppose that $\mathcal{N}$ is an $\mathcal{L}$-structure on a set C and $A \subseteq C$. Then there is an elementary substructure $\mathcal{M} \prec \mathcal{N}$ on an infinite set B with $A \subseteq B$ of size at most $\lambda := \max(|A|, |\mathcal{L}|)$.*

Proof. By the Axiom of Choice, find a Skolem function f_φ for any $\mathcal{L}$-formula $\varphi(x_0, \dots, x_n, y)$. Let $B_0 = A$ and

$$B_{n+1} = B_n \cup \bigcup_{n \in \mathbb{N},\ \varphi(x_0,\dots,x_k,y) \text{ is an } \mathcal{L}\text{-formula}} f_\varphi(B_n^{k+1}),$$

where $f_\varphi(B_n^{k+1})$ denotes the pointwise image. It is easy to check that $B := \bigcup_{n\in\omega} B_n$ passes Tarski's test as required.

There are $|\mathcal{L}| \leq \lambda$ (by Lemma 3.2.11) many $\mathcal{L}$-formulas, so in each step, only $|\bigcup_{n\in\omega}(\lambda \times \lambda^n)| \leq \lambda$ (by Lemma 3.2.11) many new elements are added. Hence $|B| \leq \lambda$. □

The downward Löwenheim-Skolem theorem provides us with many examples of elementary substructures. Before this, we did not have any examples besides Exercise 14.

Example 3.2.17. The field $(\mathbb{C}, 0, 1, +, \cdot)$ of complex numbers is uncountable (since the set $2^\mathbb{N}$ of infinite binary sequences is uncountable by Cantor's theorem). By the downward Löwenheim-Skolem theorem, it has a countable elementary subfield.

We aim to show later, using a technique called quantifier elimination, that the set of algebraic complex numbers forms an elementary subfield of the complex field.

By Theorem 3.2.12, or alternatively by the downward Löwenheim-Skolem theorem, we have the following striking consequence, called the **Skolem paradox**. If ZFC is consistent, then it has a countable model $(M, \in_M)$. This may seems contradictory at first sight.

One way to visualise such a model is to identify each element of M by a natural number and thus obtain a model $(\mathbb{N}, \in_\mathbb{N})$ of ZFC. Visualise $(\mathbb{N}, \in_\mathbb{N})$ as a direct graph with arrows that point to a set from its elements. Think of a statement true in $(\mathbb{N}, \in_\mathbb{N})$, for instance the existence of an uncountable set. This is just a statement about arrows.

The seeming paradox about uncountability is resolved by the difference by the internal and external meaning of *uncountable*. Assume that $\in_M$ equals the restriction of $\in$ to M.[28] We write $\mathbb{P}$ for $\mathcal{P}(\mathbb{N})$. Further assume:

- $\mathbb{N} \subseteq M$ and "$\mathbb{N}^M = \mathbb{N}$":
  let $\varphi(x)$ denote the $\mathcal{L}_\in$-formula stating that x is an element of ω. Then for all sets n, $\varphi(n)$ holds (i.e. $n \in \mathbb{N}$) if and only if $(M, \in) \models \varphi[n]$.[29]
- "$\mathbb{P}^M \subseteq \mathbb{P}$":
  Let $\psi(x)$ denote the $\mathcal{L}_\in$-formula stating that x is a subset of ω. Then for all $x \in M$ with $(M, \in) \models \psi[x]$, x is really a set of natural numbers, i.e. $\psi(x)$ holds.

Since $\mathbb{P}^M \subseteq M$ and this $\mathbb{P}^M$ is countable, there is a bijection $f \colon \mathbb{P}^M \to \mathbb{N}$, i.e. a subset of $\mathbb{P}^M \times \mathbb{N}$ with certain properties. Such a function cannot exist in M, since $(M, \in) \models \mathbb{P}^M$ is uncountable.. In other words, $(M, \in)$ cannot "see" the countability of $\mathbb{P}^M$.

[28] The downward Löwenheim-Skolem theorem implies that such a model exists if there is a set N of any size with $(N, \in) \models$ ZFC. The existence of such a set N follows from the existence of an inaccessible cardinal (which we do not study here).

[29] These properties of $\mathbb{N}$ and $\mathbb{P}$ can be realised by the Mostowski collapse (which we do not study here) applied to M.

3.2.4. *Nonstandard models for the natural numbers and for the reals.* In the first chapter, we asked:

- How can we axiomatise a given class of structures?

Conversely, one can ask:

- What is the class of models of a given theory?

Any countable theory with infinite models has models in many cardinalities by Theorem 3.2.12. It remains to classify the models of a fixed cardinality. Here we shall see that the theory of the natural numbers, and thus PA, has more than one countable model up to isomorphism. In fact, it is not hard to show that there are infinitely many isomorphism types. Thus PA does not say much about the structure of its models.

We will return to these questions in the last chapter, where we consider other theories.

The language of arithmetic is $\mathcal{L}_{\text{Arith}} = \{0, S, +, \cdot\}$. Recall the axiom system PA from Definition 1.4.2.

The model $(\mathbb{N}, 0^{\mathbb{N}}, S^{\mathbb{N}}, +^{\mathbb{N}}, \cdot^{\mathbb{N}})$[30] is called the *standard model* of PA. It is abbreviated by $\mathbb{N}$. All other models of PA, and extensions of PA, are called *nonstandard* models.

Lemma 3.2.18. *Suppose that $\mathcal{N} = (N, 0^{\mathcal{N}}, S^{\mathcal{N}}, +^{\mathcal{N}}, \cdot^{\mathcal{N}})$ is a model of* PA*. Then there is a unique homomorphism $i = i_{\mathcal{N}} \colon \mathbb{N} \to N$ from $\mathbb{N}$ to $\mathcal{N}$.*

Proof. We define by recursion $i(0) = 0^{\mathcal{N}}$, $i(S^{\mathbb{N}}(n)) = S^{\mathcal{N}}(f(n))$. Note that any homomorphism has to equal f.

We claim that $i(m +^{\mathbb{N}} n) = i(m) +^{\mathcal{N}} i(n)$. By induction, $i(m +^{\mathbb{N}} 0) = i(m) = i(m) +^{\mathcal{N}} 0$ and

$$\begin{aligned} i(m +^{\mathbb{N}} (n +^{\mathbb{N}} 1)) &= i(m +^{\mathbb{N}} S^{\mathbb{N}}(n)) = i(S^{\mathbb{N}}(m +^{\mathbb{N}} n)) = S^{\mathcal{N}}(i(m +^{\mathbb{N}} n)) \\ &= S^{\mathcal{N}}(i(m) +^{\mathcal{N}} i(n)) = i(m) + S^{\mathcal{N}}(i(n)) = i(m) +^{\mathcal{N}} (i(n+1). \end{aligned}$$

Similarly, $i(m \cdot^{\mathbb{N}} n) = i(m) \cdot^{\mathcal{N}} i(n)$. □

Suppose that $\mathcal{N} = (N, \dots)$ is a nonstandard model of PA. We identify $\mathbb{N}$ with a subset of N via $i_{\mathcal{N}}$. Note that $(\mathbb{N}, <^{\mathbb{N}})$ is an initial segment of $(N, <^{\mathcal{N}})$, since by induction on $n \in \mathbb{N}$, if $\mathcal{N} \models m < n$ then $m \in \mathbb{N}$. When $\mathcal{N}$ is clear from the context, we call all $n \in \mathbb{N}$ *standard* and all $n \in N \setminus \mathbb{N}$ *nonstandard.*

To construct a countable nonstandard model, we define terms Δ_n by induction for $n \in \mathbb{N}$: $\Delta_0 := 0$ and $\Delta_{n+1} = S(\Delta_n)$. Note that $i_{\mathcal{N}}$ maps each $n \in \mathbb{N}$ to $\Delta_n^{\mathcal{N}}$ by definition.

Lemma 3.2.19. *The theory* $\operatorname{Th}(\mathbb{N})$*, and hence also* PA*, has a countable nonstandard model.*

Proof. Let c be a new constant symbol and let $\mathcal{L} = \mathcal{L}_{\text{Arith}} \cup \{c\}$ Let

$$T := \operatorname{Th}(\mathbb{N}) \cup \{c \neq \Delta_n \mid n \in \mathbb{N}\}.$$

Since T is finitely satisfiable by the standard model $\mathbb{N}$, T has a model $\mathcal{N}$. To see that $\mathcal{N}$ is nonstandard, note that $i_{\mathcal{N}}$ is not surjective since $c^{\mathcal{N}} \neq \Delta_n^{\mathcal{N}}$ holds for all $n \in \mathbb{N}$. □

Suppose that $\mathcal{N} = (N, 0^{\mathcal{N}}, S^{\mathcal{N}}, +^{\mathcal{N}}, \cdot^{\mathcal{N}})$ is a nonstandard model of PA. We can define a relation $<$ from $+^{\mathcal{N}}$. Note that each element x of the nonstandard part has a successor $S^{\mathcal{N}}(x)$ and a predecessor y with $S^{\mathcal{N}}(y) = x$. Thus the nonstandard part of $(N, <)$ consists of "intervals" isomorphic to $(\mathbb{Z}, <^{\mathbb{Z}})$. One can easily show that the order or these "copies" of $(\mathbb{Z}, <^{\mathbb{Z}})$ is a dense linear order without end points.

Lecture 18
21. June

We now introduce the nonstandard reals.

[30] Formally, this is defined by restricting ordinal addition and multiplication to ω. Hence the full induction principle holds for all subsets of $\mathbb{N}$, and in particular PA holds.

An *ordered field* $(R, 0, 1, +, \cdot, <)$ a model of the field axioms, the axioms of strict linear orders, and the axioms stating that addition with a fixed number, and multiplication with a positive number, are strictly monotone functions:

- $\forall x, y, z\ (x < y \to x + z < y + z)$
- $\forall x, y, z\ (x < y \wedge z > 0 \to x \cdot z < y \cdot z)$

The language $\mathcal{L}$ consists of the language of ordered fields together with a set $\mathcal{S}$ consisting of:

- A constant symbol c_r for every $r \in \mathbb{R}$.
- An n-ary function symbol F_f for every function $f \colon \mathbb{R}^n \to \mathbb{R}$.
- An n-ary relation symbol R_A for every set $A \subseteq \mathbb{R}^n$.

We abbreviate the structure $(\mathbb{R}, 0^{\mathbb{R}}, 1^{\mathbb{R}}, +^{\mathbb{R}}, \cdot^{\mathbb{R}}, <^{\mathbb{R}}, \mathcal{S}^{\mathbb{R}})$ of the reals with the obvious interpretation of symbols in $\mathcal{S}$ as $\mathbb{R}$.

A *hyperreal field* is an $\mathcal{L}$-structure $(\mathbb{R}^*, 0^{\mathbb{R}^*}, 1^{\mathbb{R}^*}, +^{\mathbb{R}^*}, \cdot^{\mathbb{R}^*}, <^{\mathbb{R}^*}, \mathcal{S}^{\mathbb{R}^*})$, abbreviated as $\mathbb{R}^*$, with the following properties:

- (Transfer) $\mathbb{R} \prec \mathbb{R}^*$, i.e. $\mathbb{R}$ is an elementary substructure of $\mathbb{R}^*$.
- $\mathbb{R}^*$ is *not archimedean*, i.e. $\mathbb{R}^*$ contains a *positive infinitesimal* element ϵ with $0 < \epsilon < \frac{1}{n}$ for all $n \in \mathbb{N}$.

Every function $f \colon \mathbb{R}^n \to \mathbb{R}$ has a "version" $f^* \colon (\mathbb{R}^*)^n \to \mathbb{R}^*$. Similarly, every relation $A \subseteq \mathbb{R}^*$ has "version" $A^* \subseteq (\mathbb{R}^*)^n$. Sometime f^* and A^* are denoted by f and R, respectively.

Lemma 3.2.20. *There exists a hyperreal field.*

Proof. Let c be a new constant symbol and let $\mathcal{L}' = \mathcal{L} \cup \{c\}$ Let

$$T := \mathrm{Th}_{\mathcal{L}}(\mathbb{R}) \cup \{0 < c < c_{\frac{1}{n}} \mid n \in \mathbb{N}\}.$$

Since T is finitely satisfiable in $\mathbb{R}$, it has a model $\mathbb{R}^*$. We have $\mathbb{R} \prec \mathbb{R}^*$, since this holds for all models of $\mathrm{Th}_{\mathcal{L}}(\mathbb{R})$. Moreover, $\epsilon := c^{\mathbb{R}^*}$ witnesses that $\mathbb{R}^*$ is not archimedean. □

An alternative construction of a hyperreal field $\mathbb{R}^*$ goes essentially as follows. Consider all sequences $\vec{r} = \langle r_n \mid n \in \omega \rangle$ in $\mathbb{R}$. $\mathbb{R}^*$ is defined as the set of such sequences modulo an equivalence relation $\sim$. One defines $\vec{r} \sim \vec{s}$ if $r(n) = s(n)$ for "many" $n \in \mathbb{N}$, $\vec{r} < \vec{s}$ if $r(n) < s(n)$ for "many" $n \in \mathbb{N}$ etc. Thus the sequences $\vec{r} = \langle \frac{1}{2^n} \mid n \in \mathbb{N} \rangle$ and $\vec{s} = \langle \frac{1}{n+1} \mid n \in \mathbb{N} \rangle$ represent infinitesimals with $0 < \vec{r} < \vec{s} < \epsilon$ for all $\epsilon \in \mathbb{R}_{>0}$. More precisely, "many" $n \in \mathbb{N}$ means $\mathcal{U}$-many $n \in \mathbb{N}$ with respect to an ultrafilter $\mathcal{U}$ on $\mathbb{N}$.

Hyperreals allow elegant formulations of definitions and proofs from analysis. We shall give a few examples.

From now on, we fix a hyperreal field $\mathbb{R}^*$. We call its elements *hyperreals.*

We first describe some basic facts about the structure of $\mathbb{R}^*$.

Definition 3.2.21.

(1) The set of *finite* hyperreals is
$$\mathbb{R}_{\text{fin}} = \{x \in \mathbb{R}^* \mid \exists n \in \mathbb{N}\ |x| < n\}.$$
(2) The set of *infinite* hyperreals is
$$\mathbb{R}_{\text{inf}} = \mathbb{R}^* \setminus \mathbb{R}_{\text{fin}}.$$
(3) The set of *infinitesimals* is
$$\mu = \{x \in \mathbb{R}^* \mid \forall n \in \mathbb{N}\ |x| < \frac{1}{n}\}.$$

Lemma 3.2.22.

(1) $\mathbb{R}_{\text{fin}}$ *is a subring of* $\mathbb{R}^*$*: for all* $x, y \in \mathbb{R}_{\text{fin}}$*, we have* $x \pm y$*,* $x \cdot y \in \mathbb{R}_{\text{fin}}$.

(2) *μ is an ideal in $\mathbb{R}_{\text{fin}}$: it is a subring of $\mathbb{R}_{\text{fin}}$ and for all $x \in \mathbb{R}_{\text{fin}}$ and $y \in \mu$, we have $x \cdot y \in \mu$.*

Proof. (1) Suppose that $x, y \in \mathbb{R}_{\text{fin}}$. Find $r, s \in \mathbb{R}_{>0}$ with $|x| < r$ and $|y| < s$. Then $|x \pm y| \leq |x| + |y| \leq r + s \in \mathbb{R}_{>0}$ and $|x \cdot y| = |x| \cdot |y| \leq r \cdot s \in \mathbb{R}_{>0}$.

(2) Suppose that $x, y \in \mu$. We aim to show $x \pm y \in \mu$. Thus we fix any $r \in \mathbb{R}_{>0}$ and show $|x \pm y| < r$. Since $x, y \in \mu$, we have $|x|, |y| < \frac{r}{2}$, so $|x \pm y| \leq |x| + |y| < r$.

Suppose that $x \in \mathbb{R}_{\text{fin}}$ and $y \in \mu$. We aim to show $x \cdot y \in \mu$. We fix any $r \in \mathbb{R}_{>0}$ and show $|x \cdot y| < r$. Find some $s \in \mathbb{R}_{>0}$ with $|x| < s$. Since $y \in \mu$, we have $|y| < \frac{r}{s}$. Then $|x \cdot y| = |x| \cdot |y| < s \cdot \frac{r}{s} = r$. □

Definition 3.2.23. For $x, y \in \mathbb{R}^*$, $x \approx y$ means that $|x - y| \in \mu$. (x, y are *infinitely close.*)

Lemma 3.2.24.

(1) *$\approx$ is an equivalence relation on $\mathbb{R}^*$, i.e. for all $x, y, z \in \mathbb{R}^*$:*
   (a) *$x \approx x$.*
   (b) *If $x \approx y$, then $y \approx x$.*
   (c) *If $x \approx y$ and $y \approx z$, then $x \approx z$.*

(2) *$\approx$ is a* congruence relation *on $\mathbb{R}_{\text{fin}}$ with respect to $\pm$ and $\cdot$, i.e. for all $x, y, u, v \in \mathbb{R}_{\text{fin}}$: If $x \approx u$ and $y \approx v$, then $x \pm y \approx u \pm v$ and $x \cdot y \approx u \cdot v$.*

Proof. (1) follows from the definition of $\approx$, using that μ is additively closed.

(2) can be checked by first replacing x with u and then y with v. This uses the definition of $\approx$, the triangle inequality, and for the product, the fact that μ is an ideal in $\mathbb{R}_{\text{fin}}$. (See Lemma 3.2.22.) □

Note that $\mathbb{R}^*$ has its "version" $\mathbb{N}^*$ of the natural number by definition of hyperreal fields. This is a nonstandard model of PA. To see this, note that $\mathbb{R}^*$ contains an infinitesimal real ϵ. Since $\mathbb{R} \prec \mathbb{R}^*$, $\mathbb{N}^*$ is unbounded in $\mathbb{R}^*$, so there is some $N \in \mathbb{N}^*$ with $\frac{1}{\epsilon} <^{\mathbb{R}^*} N$. Since $0 <^{\mathbb{R}^*} \epsilon <^{\mathbb{R}^*} \frac{1}{n}$ for all $n \in \mathbb{N}$, we have $N > n$ for all $n \in \mathbb{N}$.

$\mathbb{R}^*$ not a complete ordered field, since it is easy to see that $\sup(\mathbb{N})$ does not exists in $\mathbb{R}^*$. If it did, $\sup(\mathbb{N}) - 1 \in \mathbb{R}_{\text{fin}}$, but then $\sup(\mathbb{N}) \in \mathbb{R}_{\text{fin}}$, since $\mathbb{R}_{\text{fin}}$ is a subring of $\mathbb{R}^*$. However, $\mathbb{R}_{\text{fin}}$ has no maximal element. Note that we already knew for abstract reasons that $\mathbb{R}^*$ not a complete ordered field: since $(\mathbb{N}^*, <^{\mathbb{N}^*}) \not\cong (\mathbb{N} <^{\mathbb{N}})$, we have $(\mathbb{R}^*, <^{\mathbb{R}^*}) \not\cong (\mathbb{R} <^{\mathbb{R}})$, but it follows from Problem 29 that there is a unique complete ordered field up to isomorphism.

Lemma 3.2.25. *(Existence of standard part) For any $r \in \mathbb{R}_{\text{fin}}$, there is a unique $s \in \mathbb{R}$ with $r \approx s$. s is called the* standard part *of r and is written as* $\text{st}(r) = s$*.*

Proof. To see that s is unique, suppose that $s_0, s_1 \in \mathbb{R}$ with $r \approx s_0$ and $r \approx s_1$. Since $\approx$ is an equivalence relation, we have $s_0 \approx s_1$. Thus $|s_0 - s_1| \in \mu \cap \mathbb{R} = \{0\}$ and hence $s_0 = s_1$.

To show that s exists, we can assume $r > 0$, since the case $r < 0$ is similar. Let

$$A := \{x \in \mathbb{R} \mid x < r\}.$$

A is nonempty, since $0 \in A$. A is bounded above, since it is bounded by $r \in \mathbb{R}_{\text{fin}}$ and hence by some $n \in \mathbb{N}$. by completeness of $\mathbb{R}$, $s := \sup(A)$ exists.

Take any $\delta \in \mathbb{R}_{>0}$. It suffices to show that $s - \delta < r < s + \delta$. We first claim that $r \leq s + \delta$. Since s is an upper bound for A, we have $s + \delta \notin A$. Hence $r \leq s_\delta$. We now claim that $r \geq s - \delta$. If $r < s - \delta$, then $s - \delta$ is an upper bound for A. This contradicts the fact that s is the least upper bound. □

Lemma 3.2.26. *Suppose that $x, y \in \mathbb{R}_{\text{fin}}$.*

(1) $x \approx y \iff \text{st}(x) = \text{st}(y)$.
(2) $x \leq y \implies \text{st}(x) \leq \text{st}(y)$, *but the converse fails.*
(3) $x \in \mathbb{R} \implies \text{st}(x) = x$.

Proof. This is easy to check and is left as an exercise. □

Lemma 3.2.27. *The map* $\mathrm{st}\colon \mathbb{R}_{\mathrm{fin}} \to \mathbb{R}$ *is a surjective ring homomorphism: for all* $x, y \in \mathbb{R}_{\mathrm{fin}}$, $\mathrm{st}(x \pm y) = \mathrm{st}(x) \pm \mathrm{st}(y)$ *and* $\mathrm{st}(x \cdot y) = \mathrm{st}(x) \cdot \mathrm{st}(y)$.

Proof. This follows from the fact that $\approx$ is a congruence relation. □

Lemma 3.2.28. $\mathbb{R}_{\mathrm{fin}}/\mu \cong \mathbb{R}$.

Proof. The kernel $\ker(\mathrm{st}) = \{x \in \mathbb{R}_{\mathrm{fin}} \mid \mathrm{st}(x) = 0\}$ of st equals μ. Thus the claim follows from the isomorphism theorem for rings that can be found in any introductory textbook on algebra. □

Recall the formal definition of convergence of sequences:

Definition 3.2.29. Suppose that $s_n \in \mathbb{R}^*$ for $n \in \mathbb{N}$ and $t \in \mathbb{R}^*$. $\vec{s} = \langle s_n \mid n \in \mathbb{N}\rangle$ *converges* to t, written as $\lim_{n\to\infty} s_n = t$, if

$$\forall \epsilon \in \mathbb{R}_{>0}\ \exists m \in \mathbb{N} \forall n \geq m\ |s_n - t| < \epsilon.$$

We now give elegant nonstandard characterisations of convergence and continuity.

In the next lemma, we write $N > \mathbb{N}$ if $N > n$ for all $n \in \mathbb{N}$. Recall that $\mathbb{R}^*$ associates a sequence $\vec{s}^*\colon \mathbb{N}^* \to \mathbb{R}^*$ to any sequence $\vec{s}\colon \mathbb{N} \to \mathbb{R}$. For any $N \in \mathbb{N}^*$, we write s^*_N for the N-th element $(\vec{s}^*)_N$ of this sequence. Note that by $\mathbb{R} \prec \mathbb{R}^*$, we have $F^* {\restriction} \mathbb{R}^n = F$ for any function $F\colon \mathbb{R}^n \to \mathbb{R}$.

Lemma 3.2.30. $\lim_{n\to\infty} s_n$ *hold if and only if for all* $N > \mathbb{N}$ *in* $\mathbb{N}^*$, $s^*_N \approx t$.

Proof. $\Longrightarrow$: Suppose that $\lim_{n\to\infty} s_n = t$. We fix some $N > \mathbb{N}$ in $\mathbb{N}^*$ and show $s^*_N \approx t$. To see this, fix any $\epsilon \in \mathbb{R}_{>0}$. It suffices to show $|s^*_N - t| < \epsilon$.

Since $\lim_{n\to\infty} s_n = t$, there is some $m \in \mathbb{N}$ such that

$$\mathbb{R} \models \forall n \geq m\ |s_n - t| < \epsilon.$$

Since $\mathbb{R} \prec \mathbb{R}^*$,

$$\mathbb{R}^* \models \forall n \geq m\ |s^*_n - t| < \epsilon.$$

In particular, $\mathbb{R}^* \models |s^*_N - t| < \epsilon$ as required.

$\Longleftarrow$: Suppose that for all $N > \mathbb{N}$ in $\mathbb{N}^*$, $s^*_N \approx t$. To show convergence, fix any $\epsilon \in \mathbb{R}_{>0}$. We are looking for some $m \in \mathbb{N}$ such that $\forall n \geq m\ |s_n - t| < \epsilon$. We have

$$\mathbb{R}^* \models \exists m\ \forall n \geq m\ |s^*_n - t| < \epsilon,$$

since this holds for any $N > \mathbb{N}$ in $\mathbb{N}^*$. Since $\mathbb{R} \prec \mathbb{R}^*$, this holds in $\mathbb{R}$ as required. □

Lemma 3.2.31. *Suppose* $f\colon A \to \mathbb{R}$ *and* $c \in A$. *The following conditions are equivalent:*

(1) f *is continuous at* c.
(2) *If* $x \in A^*$ *and* $x \approx c$, *then* $f(x) \approx f(c)$.
(3) *There is some* $\delta \in \mu_{>0}$ *such that for all* $x \in A^*$ *with* $|x - c| < \delta$, *we have* $f(x) \approx f(c)$.

Proof. This is left as an exercise. □

Definition 3.2.32. A function $f\colon A \to \mathbb{R}$ is called *uniformly continuous* if for any $\epsilon \in \mathbb{R}_{>0}$, there is some $\delta \in \mathbb{R}_{>0}$ such that

$$\forall x, y \in A\ (|x - y| < \delta \Longrightarrow |f(x) - f(y)| < \epsilon).$$

Lemma 3.2.33. *A function* $f\colon A \to \mathbb{R}$ *is uniformly continuous if and only if for all* $x, y \in A^*$ *with* $x \approx y$, *we have* $f(x) \approx f(y)$.

Added a missing star $*$

The proof is similar to the characterisation of continuity in Lemma 3.2.31. I might add this proof later, but it is not relevant for the exam. I might also add an elegant formulations of differentiability. The appeal of nonstandard analysis is that many basic and advanced result in analysis have short proofs that avoid calculations with ϵ's and δ's.

4. Incomplete theories

Lecture 19
23. June

4.1. **Finite set theory.** Recall from Definition 1.5.14 that a theory is called *complete* if for every formula φ, $T \vdash \varphi$ or $T \vdash \neg\varphi$. (It is easy to see that provability does not depend on the language by the completeness theorem.)

Let Fin denote the set of *hereditarily finite sets*, i.e. those with only finitely many elements, elements of elements etc. We assume $\mathcal{L} \subseteq \mathrm{Fin}$ for all languages studied below. Then any $\mathcal{L}$-formula is an element of Fin, since $\mathcal{L}$-formulas are functions $\{0, \ldots, n\} \to \mathcal{L}$.

We study circumstances in which an $\mathcal{L}$-theory T is incomplete.

We consider axiom systems T with the following properties:

- T is self-referential: it can prove sufficiently many facts about formulas and about provability in T.
- The axioms of T have an effective listing such as for PA or ZFC.

The second item ensures that provability in T can be expressed by a formula prov_T.

We will work with the following axiom system $\mathsf{ZF}_{\mathrm{Fin}}$. This is ZF except:

- The Axiom of Infinity is replaced by the Axiom of Finiteness.
- The Foundation Axiom is replaced with the Foundation Scheme.

Question while writing the lecture notes: does the Foundation Axiom imply the Foundation Scheme?

The proofs of transfinite induction in Lemma 2.2.28 and of transfinite recursion in Theorem 2.2.29 work in $\mathsf{ZF}_{\mathrm{Fin}}$. Note that the Axiom of Finiteness is not important for most proofs. However, with this axiom, there is a closed relationship between models of $\mathsf{ZF}_{\mathrm{Fin}}$ and models of PA.

Here are the axioms:

Axiom. (Existence) $\exists x\ (\forall y\ y \notin x)$.

Axiom. (Extensionality) $\forall x, x'\ (\forall y\ (y \in x \leftrightarrow y \in x') \to x = x')$.

Axiom. (Pairing) $\forall x, y\ (\exists z\ (\forall u\ (u \in z) \leftrightarrow (u = x \vee u = y))$.

Axiom. (Union) $\forall x\ \exists y\ \forall z\ (z \in y \leftrightarrow \exists u\ (u \in x \wedge z \in u))$.

The *Axiom of Finiteness* states that there is no inductive set and every set is in bijection with an ordinal.

Axioms marked in blue are different from ZF

Axiom. (Finiteness) $\neg\exists y\ (\emptyset \in y \wedge \forall x\ (x \in y \to x+1 \in y)) \wedge$
$\forall x\ \exists n \in \mathrm{Ord}\ \exists f \colon n \to x$ bijective.

Using the Foundation Scheme, it follows that every ordinal is 0 or a successor ordinal. We thus call the ordinals *natural numbers*.

Axiom. (Power Set) $\forall x\ \exists y\ \forall z\ (z \in y \leftrightarrow z \subseteq x)$.

We work with the *Foundation Scheme* instead of the *Axiom of Foundation*.

Axiom Scheme. (Foundation) For any formula $\varphi(z, x_0, \ldots, x_n)$,
$\forall x_0, \ldots, x_n\ (\exists z\ \varphi(z, x_0, \ldots, x_n) \to (\exists z\ \varphi(z, x_0, \ldots, x_n) \wedge \forall z' \in z\ \neg\varphi(z', x_0, \ldots, x_n))$.

Axiom Scheme. (Separation) For any formula $\varphi(z, x_0, \ldots, x_n)$,

$$\forall x\ \forall x_0, \ldots, x_n\ \exists y\ \exists z\ (z \in y \leftrightarrow (z \in x \wedge \varphi(z, x_0, \ldots, x_n))).$$

Axiom Scheme. (Replacement) If F is a function, then $\forall x\ F[x] \in V$, where $F[x] = \{z \mid \exists y \in z\ (y, z) \in F\}$.

We want to expand ZF_{Fin} by adding a constant symbol c_s for each $s \in \text{Fin}$ and adding their properties to the theory.

We first discuss how to extend an $\mathcal{L}$-theory without proving more $\mathcal{L}_\in$-sentences. Suppose that T is an $\mathcal{L}$-theory and T' is an $\mathcal{L}'$-theory with $\mathcal{L} \subseteq \mathcal{L}'$ and $T \subseteq T'$. T' is called a *conservative extension* of T if for all $\mathcal{L}$-sentences φ, $T \vdash \varphi$ holds if and only if $T' \vdash \varphi$ holds.

Language extensions, i.e. considering an $\mathcal{L}$-theory T as an $\mathcal{L}'$-theory, are always conservative. This follows from the completeness theorem.

A remark about language extension by definition: Suppose that $\mathcal{L}$ is a language and T is an $\mathcal{L}$-theory. Let R be a new n-ary relation symbol, $\mathcal{L}' = \mathcal{L} \cup \{R\}$ and

$$T' = T \cup \{\forall x_0, \dots, x_{n-1}\ (R(x_0, \dots, x_{n-1}) \longleftrightarrow \varphi(x_0, \dots, x_{n-1}))\}.$$

Every model $\mathcal{M} = (M, \mathcal{F})$ of T can be expanded to a model of T' by interpreting R as $\{(x_0, \dots, x_{n-1}) \in M^n \mid \mathcal{M} \models \varphi(x_0, \dots, x_{n-1}))\}$. Thus $\models_{\mathcal{L}} \varphi$ holds if and only if $\models_{\mathcal{L}'} \varphi$ for all $\mathcal{L}$-sentences φ. By the completeness theorem, the same holds for $\vdash$.

One can similarly add constant symbols and function symbols. We discuss only constant symbols, since function symbols work similarly. Let $\exists! x\ \varphi(x)$ state that a unique x with $\varphi(x)$ exists, i.e. it is an abbreviation for $\exists x \varphi(x) \wedge \forall y(\varphi(y) \to x = y)$. Suppose that $T \vdash \exists! x \varphi(x)$. Let c be a new constant symbol, $\mathcal{L}' = \mathcal{L} \cup \{c\}$ and $T' = T \cup \{\varphi(c)\}$. Then $\models_{\mathcal{L}} \varphi$ holds if and only if $\models_{\mathcal{L}'} \varphi$ for all $\mathcal{L}$-sentences φ.

We now expand ZF_{Fin} as follows. We add a new constant symbol c_s to $\mathcal{L}_\in$ for every set $s \in \text{Fin}$. For all $s \in t$ in Fin, we add the sentence

$$c_t = \{x \mid \bigvee_{s \in t} x = c_s\}.$$

As noted, this is a conservative extension of ZF_{Fin}. From now on, we identify this extension with ZF_{Fin}.

When we write $(\text{Fin}, \in) \models \psi$ for a sentence in the language extended by constants c_s, we always mean that $(\text{Fin}, \in)$ is the structure for the extended language where c_s has value s.

Recall that a subset A of a structure $\mathcal{M} = (M, \mathcal{F})$ is definable over $\mathcal{M}$ (with parameters, respectively) if $A = \{x \in M \mid \mathcal{M} \models \varphi(x)\}$ for some formula $\varphi(x)$ without parameters (with parameters, respectively).

Lemma 4.1.1. *ZF_{Fin} is incomplete. In fact, any $T \subseteq \text{Th}(\text{Fin}, \in)$ that is definable over $(\text{Fin}, \in)$ is incomplete.*

Proof. Let $\text{prov}_T(\varphi)$ denote an $\mathcal{L}_\in$-formula stating that $T \vdash \varphi$, i.e. there exists a finite sequence of formulas $\varphi_0, \dots, \varphi_n$ with $\varphi_n = \varphi$ such that each one is obtained from the previous ones by a rule of the Hilbert calculus. Recall that each formula φ_i is a function $\{0, \dots, n_i\}$ for some natural number n_i. Thus e.g. the statement "φ_j is derived from φ_i and φ_k by the Modus Ponens" can be expressed by an $\mathcal{L}_\in$-formula, and similarly for the other rules.

The following is a diagonalisation argument as we have seen in Cantor's proof of $|\mathcal{P}(x)| > |x|$ and in Tarski's undefinability of truth. Imagine a list of all formulas. A truth definition would allow us to write down a new formula by diagonalisation that is different from all formulas.

It T were complete, then for any formula $\psi(x)$ and any $s \in \text{Fin}$, we would have

$$(\text{Fin}, \in) \models \psi[s] \iff (\text{Fin}, \in) \models \text{prov}_T[\psi(c_s)] \iff (\text{Fin}, \in) \models \text{prov}_T(\text{sub}(c_\psi, c_s)),$$ [31]

[31] Here and elsewhere, $\varphi(t)$ is an abbreviation for the formula obtained by replacing φ's only free variable by the term t.
As a reminder: $[s]$ stands for an assignment of variables, the only relevant variable being mapped to the element s of the structure.

where $\text{sub}(\psi, x)$ denotes the recursive definition of the formula obtained from ψ by substituting x for its free variable. So $\mathsf{T}(\psi, s) = \text{prov}_T(\text{sub}(c_\psi, c_s))$ is a truth definition for $(\text{Fin}, \in)$. We now argue why this is contradictory.

Let $\psi(x)$ denote the formula $\neg\mathsf{T}(x, x) = \neg\text{prov}_T(\text{sub}(x, c_x))$ (it is not relevant what this formula means when x is not a formula). Then

$$(\text{Fin}, \in) \models \psi[\psi] \iff (\text{Fin}, \in) \models \neg\mathsf{T}[\psi, \psi] \iff (\text{Fin}, \in) \not\models \psi[\psi],$$

where $\text{sub}(\psi, x)$ denotes the recursive definition of the formula obtained from ψ by substituting x for its free variable.

The first equivalence holds by the definition of ψ. The second equivalence uses the fact that T is a truth definition: $(\text{Fin}, \in) \models \mathsf{T}[\psi, s] \iff (\text{Fin}, \in) \models \psi[s]$ as stated above. □

Gödel's first incompleteness theorem, in the form proved by Rosser, is a strengthening of Lemma 4.1.1: it does not assume that T is true, only that it is consistent. In this and the next sections, we work towards this goal.

We will need a syntactical version of the previous argument using sentences instead of formulas. Instead of $(\text{Fin}, \in) \models \chi[s]$ for a formula with one free variable and $s \in \text{Fin}$, we want to write $(\text{Fin}, \in) \models \chi(c_s)$.

The argument for the first equivalence can then be rewritten as follows. We assign to $\theta(x) := \text{prov}_T(x)$ the sentence $\psi(x) := \neg\theta(\text{sub}(x, c_x))$ and obtain $(\text{Fin}, \in) \models \psi(c_\psi) \iff (\text{Fin}, \in) \models \neg\theta(c_{\psi(c_\psi)})$, since clearly

$$(\text{Fin}, \in) \models \text{sub}(c_\psi, c_s) = c_{\psi(c_s)}.$$

In fact, one can show that for any formula $\varphi(x)$ and any $s \in \text{Fin}$, the equality $\text{sub}(c_\psi, c_s) = c_{\psi(c_s)}$ is provable in ZF_{Fin}, where sub is defined as substitution of variables by recursion. This will follow either from the fact that it can be checked from the formula defining sub, or from the fact that all Σ_1-formulas true in $(\text{Fin}, \in)$ are provable in ZF_{Fin} and its building on this that Σ_1-definable functions are representable in ZF_{Fin} (see Lemma 4.2.12).

Thus the equivalence $\psi(c_\psi) \longleftrightarrow \neg\theta(c_{\psi(c_\psi)})$ is provable in ZF_{Fin}. The existence of a sentence φ with $\mathsf{ZF}_{\text{Fin}} \vdash \varphi \longleftrightarrow \neg\theta(c_\varphi)$ is called the *Fixed point lemma* in the literature.

The argument for the second equivalence in the previous lemma does not work without the assumption $T \subseteq \text{Th}(\text{Fin}, \in)$. We only want to assume that T is consistent. Suppose we work with a model $\mathcal{M}$ of T instead of $(\text{Fin}, \in)$. We still have the first equivalence

$$\mathcal{M} \models \psi[\psi] \iff \mathcal{M} \models \neg\text{prov}[\psi(c_\psi)]$$

by the arguments above and the variant

$$(\text{Fin}, \in) \models \neg\text{prov}[\psi(c_\psi)] \iff \mathcal{M} \not\models \psi[\psi]$$

of the second equivalence, since T is complete. However, the argument breaks because $(\text{Fin}, \in)$ and $\mathcal{M}$ might not satisfy the same sentences, i.e. they might not be elementarily equivalent (see Definition 1.3.2).

A model $\mathcal{M}$ of $\mathsf{ZFC}_{\text{Fin}}$ different from $(\text{Fin}, \in)$ is called *nonstandard*. By the compactness theorem, such models exist. We note that in fact, some models of $\mathsf{ZFC}_{\text{Fin}}$ do not even satisfy the same Σ_1-sentences as $(\text{Fin}, \in)$ (see the next section on the Levy hierarchy for the definition of Σ_1-formulas); this follows for instance from Gödel's second incompleteness theorem.

In the following, we will see how to modify the argument to also make the second equivalence work. The point is that sufficiently simple statements (Σ_0-statements) hold in any model of $\mathsf{ZFC}_{\text{Fin}}$ if and only if they hold in $(\text{Fin}, \in)$. We will need that any Δ_1-definable set is *representable* by a Σ_1-formula (see Lemma 4.2.12).

Lecture 20
28. June

4.2. The Levy hierarchy.

We now study the complexity of formulas with respect to quantifiers. The complexity in the *Levy hierarchy* is determined by counting alternating blocks of quantifiers.

Can formulas with more quantifiers define more sets? For instance, can formulas of the form $\forall x\ \exists y\ \varphi(x, y, z)$ define more sets than formulas of the form $\exists y\ \varphi(y, z)$ or $\forall y\ \varphi(y, z)$, where φ is quantifier-free?

This depends on the structure. For some interesting structures such as the complex field, every definable subset can be defined without any quantifiers. We will come to this in the next chapter.

Here we will see that in the structure $(\mathrm{Fin}, \in)$ the number of quantifiers does matter. As the number of quantifiers increases, one can define more sets.

Definition 4.2.1. Work with the extension of $\mathcal{L}_\in$ defined above.

(1) We write $\exists x \in y\ \varphi$ for the formula $\exists x\ (x \in y \wedge \varphi)$, and $\forall x \in y\ \varphi$ for the formula $\forall x\ (x \in y \rightarrow \varphi)$ Any quantifier of this form is called *bounded.* Quantifiers of the form $\exists x$ and $\forall x$ are called *unbounded.*
(2) A Σ_0*-formula* (also called Π_0*-formula*) is a formula with non unbounded quantifiers.
(3) A Σ_1*-formula* is a formula of the form $\exists x_0 \dots \exists x_k\ \varphi$, where$\varphi$ is a Σ_0-formula.
(4) A Π_n*-formula* is a formula of the form $\neg\Sigma_n$, where φ is a Σ_n-formula
(5) A Σ_{n+1}*-formula* is a formula of the form $\exists x_0 \dots \exists x_k\ \varphi$, where$\varphi$ is a Π_n-formula.
(6) A set $A \subseteq \mathrm{Fin}^k$ with $k \geq 1$ is called Σ_n*-definable* if there is a Σ_n-formula $\varphi(x_0, \dots, x_{k-1})$ such that
$$A = \{(x_0, \dots, x_{k-1}) \in \mathrm{Fin}^k \mid (\mathrm{Fin}, \in) \models \varphi[x_0, \dots, x_{k-1}]\}.$$
Π_n-definable subsets of Fin^k are defined similarly.
(7) A set $A \subseteq \mathrm{Fin}^k$ with $k \geq 1$ is called Δ_n*-definable* if it is both Σ_n*-definable* and Π_n*-definable.*
(8) A function $f\colon (\mathrm{Fin})^k \to \mathrm{Fin}$ is called Σ_n-definable (Π_n-definable, Δ_n-definable, respectively) if its graph is Σ_n-definable (Π_n-definable, Δ_n-definable, respectively).

Definition 4.2.2. *Generalised* Σ_1-formulas arise from Σ_0-formulas by closing under $\exists x$, $\forall x \in y$, $\wedge$, and $\vee$.

For example, if φ is a Σ_0-formula, then $\forall x \in y\ \exists z\ \varphi$ is a generalised Σ_0-formulas.

There are various ways of bringing formulas into a simple form. One of them is prenex normal form (see Wikipedia). We need the following normal form, a variant of negation normal form for first order logic. It is used to avoid the negation case in inductive proofs.

Lemma 4.2.3 (Negation normal form). *Every formula is logically equivalent (i.e. provably equivalent in Hilbert's calculus) to a formula in which negations only appear at atomic formulas.*

Proof. This is easily proved by induction on formulas. For instance, $\neg\exists x\ \varphi$ is logically equivalent to $\forall x\ \neg\varphi$ and $\neg(\varphi \wedge \psi)$ is logically equivalent to $(\neg\varphi) \vee (\neg\psi)$. □

Lemma 4.2.4. *Every generalised* Σ_1*-formula* $\varphi(x_0, \dots, x_{k-1})$ *is in equivalent in* Fin *to a* Σ_1*-Formula* ψ*, i.e. for all* $(s_0, \dots, s_{k-1}) \in \mathrm{Fin}$,
$$\mathrm{Fin} \models \varphi[s_0, \dots, s_{k-1}] \Longleftrightarrow \mathrm{Fin} \models \psi[s_0, \dots, s_{k-1}].$$

Proof. By induction on formulas. Suppose that φ is the formula $\forall x \in y\ \psi(x, y, \vec{z})$, where ψ is a generalised Σ_1-formula. By the induction hypothesis, we can assume that ψ is a Σ_1-formula $\exists x_0, \dots, x_m\ \theta(x_0, \dots, x_m, x, y, \vec{z})$, where θ is a Σ_0-formula. Then φ is in $(\mathrm{Fin}, \in)$ equivalent to the Σ_1-formula $\exists z\ \forall x \in y\ \exists x_0 \in z \dots \exists x_m \in z\ \theta$. □

Lemma 4.2.5. *Every formula that arises by an $\in$-recursion guided by a Σ_1-formula is itself Σ_1. Moreover, given a Δ_1-definable language $\mathcal{L}$, the following statements are expressible by Σ_1-formulas:*

(1) *The k-th symbol of a word is x.*
(2) *The length of a word is $k \in \mathbb{N}$.*
(3) *v is a variable, constant symbol, function symbol, logical symbol etc.*
(4) *t is a term.*
(5) *$\varphi = (\forall x \psi)$, $\varphi = (\neg\psi)$.*
(6) *φ is a formula.*
(7) *x is a variable that occurs free (bound) at place $k \in \mathbb{N}$.*
(8) *φ is a sentence.*
(9) *$t = s\frac{r}{x}$, where r, s, t are terms.*
(10) *$\varphi = \psi\frac{t}{x}$, where φ, ψ are formulas, t is a term and x is a variable.*
(11) *φ is an axiom of Hilbert's calculus.*
(12) *$\varphi_0, \varphi_1, \dots, \varphi_n$ are formulas such that each φ_j arises from $\varphi_0, \dots, \varphi_{j-1}$ by rules of Hilbert's calculus.*

Proof. This is left as an exercise. For instance, suppose that $F\colon \mathrm{Fin} \to \mathrm{Fin}$ is defined by recursion guided by a Σ_1-definable function $G\colon \mathrm{Fin} \times \mathrm{Fin} \to \mathrm{Fin}$. Then $F(x) = y$ if there exists a transitive set z and a function $f\colon z \to \mathrm{Fin}$ such that for every $y \in z$, $f(y) = G(y, F{\restriction}y)$. Note that "for all $y \in z$" is a bounded quantifier. □

$\mathcal{L}$ always denotes a language that is a subset of Fin.

Definition 4.2.6. Suppose that $\varphi(x_0, \dots, x_{k-1})$ is an $\mathcal{L}$-formula and T is an $\mathcal{L}$-theory.

(1) φ *defines* a set $R \subseteq \mathrm{Fin}^k$ if for all $a_0, \dots, a_{k-1} \in \mathrm{Fin}$:
$$(a_0, \dots, a_{k-1}) \in R \iff (\mathrm{Fin}, \in) \models \varphi[a_0, \dots, a_{k-1}].$$
(2) T *decides* φ if for all $a_0, \dots, a_{k-1} \in \mathrm{Fin}$, one of the following holds:
   (a) $T \vdash \varphi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_{k-1}}}{x_{k-1}}$.
   (b) $T \vdash \neg\varphi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_{k-1}}}{x_{k-1}}$.
(3) φ *represents* a relation $R \subseteq \mathrm{Fin}^k$ *in* T if for all $a_0, \dots, a_{k-1} \in \mathrm{Fin}$:
   (a) If $(a_0, \dots, a_{k-1}) \in R$, then $T \vdash \varphi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_{k-1}}}{x_{k-1}}$.
   (b) If $(a_0, \dots, a_{k-1}) \notin R$, then $T \vdash \neg\varphi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_{k-1}}}{x_{k-1}}$.

The relationship between these notions is stated in the next lemma. This lemma is not actually needed below.

Lemma 4.2.7. *The following conditions are equivalent for any formula $\varphi(x_0, \dots, x_{k-1})$ and $R \subseteq \mathrm{Fin}^k$:*

(1) *φ represents R in $\mathsf{ZF}_{\mathrm{Fin}}$.*
(2) *φ defines R and $\mathsf{ZF}_{\mathrm{Fin}}$ decides φ.*

Proof. (1) ⇒ (2): It is clear that φ decides R. Since $\mathsf{ZF}_{\mathrm{Fin}}$ holds in Fin, φ defines R in Fin.

(2) ⇒ (1): Suppose that $(a_0, \dots, a_{n-1}) \in R$. Since φ defines R, $\varphi[a_0, \dots, a_{n-1}]$ holds in $(\mathrm{Fin}, \in)$ and hence $\mathsf{ZF}_{\mathrm{Fin}} \nvdash \neg\varphi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_{n-1}}}{x_{n-1}}$. Since $\mathsf{ZF}_{\mathrm{Fin}}$ decides φ, $\mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_{n-1}}}{x_{n-1}}$ as required. The case $(a_0, \dots, a_{n-1}) \in R$ is similar. □

Lemma 4.2.8.

(1) *Every Σ_0-formula φ true in $(\mathrm{Fin}, \in)$ is provable in $\mathsf{ZF}_{\mathrm{Fin}}$.*
(2) *Every Σ_0-definable set $R \subseteq \mathrm{Fin}^k$ is representable in $\mathsf{ZF}_{\mathrm{Fin}}$.*

Proof. (1) By induction on Σ_0-sentences in negation normal form (see Lemma 4.2.3). The claim holds for atomic sentences $c_s \in c_t$, $c_s = c_t$ and their negations by the choice of the extension of $\mathsf{ZF}_{\mathrm{Fin}}$ to the language extended by constant symbols c_s for $s \in \mathrm{Fin}$.

If $\varphi \wedge \psi$ holds, then both φ and ψ are provable by the induction hypothesis. Hence $\varphi \wedge \psi$ is provable.

The case $\varphi \vee \psi$ is similar.

Suppose that $\exists x \in c_t\ \varphi$ holds in $(\mathrm{Fin}, \in)$. Then for some $s \in t$, $\varphi\frac{c_s}{x}$ holds in $(\mathrm{Fin}, \in)$. The latter is provable in $\mathsf{ZF}_{\mathrm{Fin}}$ by the inductive hypothesis. Hence $\exists x \in c_t\ \varphi$ is provable in $\mathsf{ZF}_{\mathrm{Fin}}$.

Suppose that $\forall x \in c_t\ \varphi$ holds in $(\mathrm{Fin}, \in)$. Then for all $s \in t$, $\varphi\frac{c_s}{x}$ holds in $(\mathrm{Fin}, \in)$. Since $\varphi\frac{c_s}{x}$ is provable for each $s \in t$, their conjunction is provable. Hence $\forall x \in c_t\ \varphi$ is provable in $(\mathrm{Fin}, \in)$.

(2) This follows from (1). □

Lemma 4.2.9. *Every Σ_1-sentence φ true in $(\mathrm{Fin}, \in)$ is provable in $\mathsf{ZF}_{\mathrm{Fin}}$.*

Proof. Suppose that φ is the Σ_1-sentence $\exists x\ \psi(\vec{x})$, where ψ is a Σ_0-formula. If ψ holds in $(\mathrm{Fin}, \in)$, there are $a_0, \dots, a_n \in \mathrm{Fin}$ with $(\mathrm{Fin}, \in) \models \psi[a_0, \dots, a_n]$. By the previous lemma, $\psi\frac{c_{a_0}}{x_0} \dots \frac{c_{a_n}}{x_n}$ is provable in $\mathsf{ZF}_{\mathrm{Fin}}$. Hence ψ is provable as well. □

In fact, every Σ_0-definable set $R \subseteq \mathrm{Fin}^k$ is representable by the formula that defines it. This is not the case for Σ_1-definable sets.

Lecture 21
30. June

To show that Σ_1-definable functions are representable, we first want to simplify Σ_1-formulas.

Lemma 4.2.10. *For every Σ_{n+1}-formula $\theta(y_0, \dots, y_l)$, there is a Σ_{n+1}-formula of the form $\exists x\ \psi(x, y_0, \dots, y_l)$ that is equivalent to θ, provably in $\mathsf{ZF}_{\mathrm{Fin}}$, where ψ is Π_n.*

Proof. Consider the Σ_{n+1}-formula $\exists x_0 \dots \exists x_k\ \varphi(x_0, \dots, x_k, y_0, \dots, y_l)$. Then $\exists x \exists x_0 \in x \dots \exists x_k \in x\ \varphi(x_0, \dots, x_k, y_0, \dots, y_l)$ works. A similar argument as in the proof of Lemma 4.2.4 now shows that $\exists x_0 \in x \dots \exists x_k \in x\ \varphi(x_0, \dots, x_k, y_0, \dots, y_l)$ is a Π_n-formula. □

Definition 4.2.11. A function $f\colon \mathrm{Fin}^k \to \mathrm{Fin}$ is called Σ_1-*representable* in T if its graph is representable in T.

Lemma 4.2.12.

(1) *Every Σ_1-definable function $f\colon \mathrm{Fin}^k \to \mathrm{Fin}$ is Σ_1-representable in $\mathsf{ZF}_{\mathrm{Fin}}$.*
(2) *Every Δ_1-definable set $R \subseteq \mathrm{Fin}^k$ is Σ_1-representable in $\mathsf{ZF}_{\mathrm{Fin}}$.*

Moverover, we can choose the Σ_1-formula representing f in (1) such that $\mathsf{ZF}_{\mathrm{Fin}}$ proves $\forall z\ (\psi(\vec{x}, z) \rightarrow y = z)$.

Proof. (1) Note that the original Σ_1-definition does not always work. The idea is to consider a formula which asks for which value a witness appears first with respect to the V_n-hierarchy.

If one has a definable wellorder of the universe, then one can pick the first witness in this wellorder. $\mathsf{ZF}_{\mathrm{Fin}}$ actually proves that there is such a definable wellorder. But we give a direct proof of this lemma.

Let $\vec{V} = \langle V_n \mid n \in \omega \rangle$ denote the V-hierarchy, where $V_0 = \emptyset$ and $V_{n+1} = \mathcal{P}(V_n)$ for $n \in \omega$. We first claim that the statement $x \in V_n$ is definable in Fin by a Δ_1-definition in x and n. To see this, note that in Fin, we can define $\mathcal{P}(x) = y$ by the Σ_0-formula $\emptyset \in y$ and $\forall u \in x\ \forall v \in y\ (v \cup \{u\} \in y \wedge v \setminus \{u\} \in y)$. (For infinite sets, $\mathcal{P}(x) = y$ is only Π_1-definable.) Thus $\mathsf{ZF}_{\mathrm{Fin}}$ proves that $\vec{V}$ is definable by a Δ_1-recursion and is hence Δ_1-definable.

Suppose that the graph of f is defined by the Σ_1-formula $\exists z\ \varphi(\vec{x}, y, z)$, where φ is a Σ_0-formula.

Consider the Σ_0-formula $\theta(\vec{x}, y, v)$ stating that v is transitive, $\vec{x} \in v$, and in v, y is unique with $\exists z\ \varphi(\vec{x}, y, z)$. Note that in the last part, the quantifiers are restricted to v. Consider the Σ_1-statement $\psi(\vec{x}, y)$ stating the there is some n such that $\theta(\vec{x}, y, V_n)$ holds.

Claim. *If $\psi(x_0, \dots, x_k, y)$ holds in* Fin*, then $\psi(c_{x_0}, \dots, c_{x_k}, c_y)$ is provable in* $\mathsf{ZF}_{\mathrm{Fin}}$.

Proof. Recall that all true Σ_1-sentences are provable in $\mathsf{ZF}_{\mathrm{Fin}}$. □

The next claim implies that ψ represents f: if $\neg\psi(x_0, \dots, x_k, y)$ holds in Fin, then $\neg\psi(c_{x_0}, \dots, c_{x_k}, c_y)$ is provable in $\mathsf{ZF}_{\mathrm{Fin}}$.

Claim. *Suppose that $f(\vec{x}) = y$ holds in* Fin*. Then* $\mathsf{ZF}_{\mathrm{Fin}}$ *proves $\forall z\ (\psi(\vec{x}, z) \to y = z)$.*

Proof. Since $\psi(\vec{x}, y)$ holds, $\theta(\vec{x}, y, V_n)$ holds for some n. Since this is a true Σ_0-statement, it is provable in $\mathsf{ZF}_{\mathrm{Fin}}$.

Therefore for any $z \neq y$, $\theta(\vec{x}, z, v)$ fails for any transitive set v with $V_n \subseteq v$, since uniqueness of z fails, as witnessed by y. This is provable in $\mathsf{ZF}_{\mathrm{Fin}}$; more precisely, $\forall z\ (\psi(\vec{x}, z) \to y = z)$ is provable. □

(2) Let $f \colon \mathrm{Fin}^k \to \mathrm{Fin}$ denote the characteristic function of R, i.e. $f(\vec{x}) = 1$ if $\vec{x} \in R$ and $f(\vec{x}) = 0$ otherwise. Since R is Δ_1-definable, f is Σ_1-definable. By (1), let $\psi(\vec{x}, y)$ be a Σ_1-formula representing f. Then $\psi(\vec{x}, c_0)$ represents R: if $\vec{x} \notin R$, then $\psi(\vec{x}, c_1)$ is provable in $\mathsf{ZF}_{\mathrm{Fin}}$, since ψ represents f. By the previous claim, $\neg\psi(\vec{x}, c_0)$ is provable. □

The rest of this section is not used later. Its intention is to better understand truth definitions. In particular, we see that a truth definition for Σ_n-formulas exists.

We next want to show that not every Σ_{n+1}-definable set is Σ_n-definable. This provides another explanation of Tarki's undefinability of truth: a Σ_n-formula $\mathsf{T}(x, y)$ cannot define all Π_n-definable sets, so T is not a truth definition.

Definition 4.2.13. A formula $\mathsf{U}(x, y)$ is called a *universal* Σ_1-formula if it is a Σ_1-formula and for any Σ_1-formula $\varphi(y)$, there is some $s \in \mathrm{Fin}$ such that

$$\mathrm{Fin} \models \forall y\ (\varphi(y) \leftrightarrow \mathsf{U}(s, y)).$$

If $\mathsf{T}(x, y)$ is a Σ_1-formula that is a truth definition for Σ_1-formulas, then in particular T is a universal Σ_1-formula, since one can let $s = \varphi$ above.

Lemma 4.2.14. *There is a Σ_1-formula $\mathsf{T}_1(x, y)$ that is a truth definition for Σ_1-formulas.*

Proof. It suffices to find a Σ_1-formula $\mathsf{T}_1(x, y)$ that is equivalent to the statement: there is a set M such that $(M, \in) \models \varphi[y]$. (It is not relevant how $\mathsf{T}_1(\varphi, y)$ is defined if φ is not a formula.) Note that $(M, \in) \models \varphi[y]$ is defined by a Σ_1-recursion in Chapter 1, so it is Σ_1-definable by Lemma 4.2.5. In a bit more detail, $(M, \in) \models \varphi[y]$ says that there exists a function f that assigns truth values true/false to subformulas of φ and tuples in M such that (a) f satisfies the recursive definition, and (b) $f(\varphi, y) = \mathrm{true}$. □

If $\mathsf{T}_1(x, y)$ is a Σ_1 truth definition, then $\neg\mathsf{T}_1(x, y)$ is then a Π_1 truth definition. Using this and Lemma 4.2.10, one can inductively obtain a Σ_n-formula that is a truth definition for Σ_n-formulas for $n \geq 2$.

Lemma 4.2.15. *For each $n \geq 1$, there is a Σ_n-formula $\mathsf{T}_n(x, y)$ that is a truth definition for Σ_n-formulas.*

Proof. Suppose that $\mathsf{T}_1(\varphi, y, z)$ is a Σ_1 truth definition for formulas with two variables. This exists by an easy modification of the above argument. Consider Σ_2-formulas ψ of the form $\exists z\ \varphi_\psi(y,z)$, where φ_ψ a Π_1-formula. One can use Lemma 4.2.10 to see that this suffices. Then

$$\exists z \neg \mathsf{T}(\varphi, y, z)$$

is a Σ_2 truth definition. Similarly, we can construct a Σ_{n+1} truth definition from a Σ_n truth definition. □

Then next lemma shows that some Π_n-definable sets are not Σ_n-definable.

Lemma 4.2.16. *Suppose that $\mathsf{U}_n(\varphi, y)$ is a universal Σ_n-formula. Then $\neg\mathsf{U}_n(x,x)$ is a Π_n-formula that is not equivalent to any Σ_n-formula in $(\mathrm{Fin}, \in)$.*

Proof. Suppose that there is a Σ_n-formula $\varphi(x)$ such that

$$\forall x\ (\neg\mathsf{U}(x,x) \leftrightarrow \varphi(x))$$

holds in $(\mathrm{Fin}, \in)$. Since U_n is universal, there is some $s \in \mathrm{Fin}$ such that

$$\forall x\ (\mathsf{U}(x,s) \leftrightarrow \varphi(x))$$

holds in $(\mathrm{Fin}, \in)$. But the case $x = s$ yields a contradiction. □

4.3. **Incompleteness of extensions of finite set theory.**

Lecture 22
05. July

The next lemma is a provable version of the fact that there is no truth definition $\mathsf{T}(\varphi, x)$. To see this, let $\psi(x)$ be the formula $\neg\mathsf{T}(x,x)$.

Lemma 4.3.1 (Fixed point lemma). *For every formula $\psi(x)$, there is a sentence φ with $\mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi \longleftrightarrow \psi(c_\varphi)$. (Moreover, if $\psi(x)$ is a Σ_1-formula, then φ can be chosen as a Σ_1-sentence.[32])*

Proof. Recall from the proof of Lemma 4.1.1 that $\mathrm{sub}(\psi, x)$ denotes the recursive definition of the formula obtained from ψ by substituting x for its unique free variable. This is a Σ_1-definition by Lemma 4.2.5.

There are two ways to do the proof. One can either notice that $\mathsf{ZF}_{\mathrm{Fin}}$ proves that the recursive definition of sub is a (partial) function. Or one can apply Lemma 4.2.12 and obtain some other Σ_1-formula ν that defines sub in $(\mathrm{Fin}, \in)$ such that $\mathsf{ZF}_{\mathrm{Fin}}$ proves that ν defines a (partial) function. In any case, write $\nu(\varphi, x, \varphi')$ for such a Σ_1-formula, where φ' stands for the formula obtained by replacing the unique free variable of φ by x. Write $s(\varphi, x) = \varphi'$ if $\nu(\varphi, x, \varphi')$ holds.

Let $\theta(x)$ denote the formula $\psi(s(x,x))$, in more detail $\exists z\ \nu(x,x,z) \wedge \psi(z)$. Then

$$\mathsf{ZF}_{\mathrm{Fin}} \vdash \theta(c_\theta) \longleftrightarrow \psi(s(c_\theta, c_\theta)) \longleftrightarrow \psi(c_{\theta(c_\theta)}).$$

In more detail,

$$\mathsf{ZF}_{\mathrm{Fin}} \vdash \theta(c_\theta) \longleftrightarrow \exists z\ (\nu(c_\theta, c_\theta, z) \wedge \psi(z)) \longleftrightarrow \psi(c_{\theta(c_\theta)}).$$

The first equivalence holds by the definition of θ and since ν represents sub. The second equivalence holds since $\mathsf{ZF}_{\mathrm{Fin}}$ proves $s(c_\theta, c_\theta) = c_{\theta(c_\theta)}$, in more detail $\mathsf{ZF}_{\mathrm{Fin}}$ proves that $c_{\theta(c_\theta)}$ is the unique z with $\nu(c_\theta, c_\theta, z)$. This is because ν represents sub and $\mathsf{ZF}_{\mathrm{Fin}}$ proves that ν defines a function, as in the additional property in Lemma 4.2.12.

Let φ denote the formula $\theta(c_\theta)$. □

For the next theorem, note that for any Σ_1-definable theory T, the set

$$\{\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-sentence with } T \vdash \varphi\}$$

is ~~Δ_1-definable~~ Σ_1-definable. If T is additionally complete, then this set is in fact Δ_1-definable, since its complement

$$\{\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-sentence with } T \nvdash \varphi\} = \{\varphi \mid \varphi \text{ is an } \mathcal{L}\text{-sentence with } T \vdash \neg\varphi\}$$

[32] However, we will apply this to the Π_1-formula $\neg\mathrm{prov}_T(x)$.

is also Σ_1-definable.

The following is Rosser's stronger version of Gödel's incompleteness theorem, here in a version for $\mathsf{ZF}_{\mathrm{Fin}}$.

Theorem 4.3.2. *(A strong version of Gödel's first incompleteness theorem, in a version for* $\mathsf{ZF}_{\mathrm{Fin}}$*) Suppose that T is a consistent extension of* $\mathsf{ZF}_{\mathrm{Fin}}$ *that is Σ_1-definable over* $(\mathrm{Fin}, \in)$*. Then*

$$\{\varphi \mid \varphi \textit{ is an } \mathcal{L}\textit{-sentence with } T \vdash \varphi\}$$

is not Δ_1-definable. In particular, T is incomplete.

Proof. The idea is to apply the fixed point lemma to the formula $\neg\mathrm{prov}_T(x)$. In the actual proof, one works with a slightly modified formula.

Suppose that the set in the assumption is Δ_1-definable. Then it is represented in $\mathsf{ZF}_{\mathrm{Fin}}$ by some Σ_1-formula $\psi(x)$ by Lemma 4.2.12. By the previous Lemma 4.3.1, there is a ~~Σ_1~~ sentence φ such that

$$\mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi \longleftrightarrow \neg\psi(c_\varphi).$$

Then

$$T \vdash \varphi \iff \mathsf{ZF}_{\mathrm{Fin}} \vdash \psi(c_\varphi) \iff \mathsf{ZF}_{\mathrm{Fin}} \vdash \neg\varphi.$$

$$T \nvdash \varphi \iff \mathsf{ZF}_{\mathrm{Fin}} \vdash \neg\psi(c_\varphi) \iff \mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi.$$

The first equivalences hold by the choice of ψ. □

Added the assumption ω-consistent in the next corollary

Gödel's original proof of a weaker form of the incompleteness theorem avoids the use of Σ_1-representations and Lemma 4.2.12. (Note that the proof of the fixed point lemma does not need Lemma 4.2.12.) One still needs that true Σ_1-statements are provable as in Lemma 4.2.9.

Gödel used the notion of ω-consistency. It is a stronger form of consistency that is only of historical interest, as far as I know. A theory T extending $\mathsf{ZF}_{\mathrm{Fin}}$ is called *ω-consistent* if whenever $T \vdash \exists x\ \varphi(x)$, there exists some $t \in \mathrm{Fin}$ such that $T \nvdash \neg\varphi(c_t)$. Setting $\varphi = \bot$ shows that any ω-consistent theory is consistent.

Let $\mathrm{proof}(x, c_\varphi)$ denote a formula stating that x is a proof of c_φ. If one writes down such a formula in a straightforward way, one can see that it is decided in $\mathsf{ZF}_{\mathrm{Fin}}$, i.e. $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{proof}(x, c_\varphi)$ or $\mathsf{ZF}_{\mathrm{Fin}} \vdash \neg\mathrm{proof}(x, c_\varphi)$.

We claim that an ω-consistent theory T does not prove $\neg\mathrm{con}(T)$, where $\mathrm{con}(T) = \neg\mathrm{prov}_T(\bot) = \neg\exists x\ \mathrm{proof}(x, \bot)$. To see this, suppose towards a contradiction that $T \vdash \exists x\ \mathrm{proof}(x, \bot)$. Since T is ω-consistent, there is some $t \in \mathrm{Fin}$ such that $T \nvdash \neg\mathrm{proof}(c_t, \bot)$. As we remarked a few lines above, then $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{proof}(c_t, \bot)$. Hence t is actually a proof of $\bot$ and thus T is inconsistent. But every ω-consistent theory is consistent.

Also note that if $T \nvdash \neg\mathrm{con}(T)$, then T is consistent.

Corollary 4.3.3. *(Gödel's original first incompleteness theorem, in a version for* $\mathsf{ZF}_{\mathrm{Fin}}$*) Suppose that T is an ω-consistent extension of* $\mathsf{ZF}_{\mathrm{Fin}}$ *that is Σ_1-definable over* $(\mathrm{Fin}, \in)$*. Then T is incomplete.*

Proof. This follows from the previous theorem. Here is a shorter proof.

We do not actually use that T is ω-consistent, only that $T \nvdash \neg\mathrm{con}(T)$.

By the fixed point Lemma 4.3.1, there is a sentence φ such that

$$\mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi \longleftrightarrow \neg\mathrm{prov}_T(c_\varphi).$$

Since T is complete, one of the following two cases occurs:

Suppose that $T \vdash \varphi$. Since $\mathrm{prov}_T(c_\varphi)$ is a true Σ_1-sentence, $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{prov}_T(c_\varphi)$. Thus $\mathsf{ZF}_{\mathrm{Fin}} \vdash \neg\varphi$ by the choice of φ. This contradicts the case assumption.

Suppose that $T \vdash \neg\varphi$. Thus $T \vdash \mathrm{prov}_T(c_\varphi)$ by the choice of φ. Since $\mathrm{prov}_T(c_{\neg\varphi})$ is a true Σ_1-sentence, $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{prov}_T(c_{\neg\varphi})$ and thus $T \vdash \mathrm{prov}_T(c_{\neg\varphi})$. But $T \vdash \mathrm{prov}_T(c_\varphi)$

and $T \vdash \mathrm{prov}_T(c_{\neg\varphi})$ imply by tautologies that $T \vdash c_{\varphi\wedge\neg\varphi}$ and hence $T \vdash \neg\mathrm{con}(T)$. This contradicts the assumption that T is ω-consistent. □

Given the previous theorem, the question arises: is it possible that T is consistent and $T \vdash \neg\mathrm{con}(T)$? Gödel's second incompleteness theorem implies that this is indeed possible. An example of such a theory is $T = \mathsf{ZF}_{\mathrm{Fin}} + \neg\mathrm{con}(\mathsf{ZF}_{\mathrm{Fin}})$. How does a model $\mathcal{M}$ of such a theory T look like? $\mathcal{M}$ will have non-standard natural numbers, and proofs of non-standard length. From the viewpoint of $\mathcal{M}$, there exists a finite proof of $\perp$. But from the outside, we can see that the proof is an infinite object and thus not really a proof of $\perp$.

4.4. **An analysis of Gödel's sentence.** Suppose that T is a consistent theory extending $\mathsf{ZF}_{\mathrm{Fin}}$. In the arguments above, a Σ_1 sentence φ with

$$\mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi \longleftrightarrow \neg\mathrm{prov}_T(c_\varphi)$$

was used to show that a given extension of $\mathsf{ZF}_{\mathrm{Fin}}$ is incomplete. We will say *Gödel's sentence* when we mean any sentence with this property and write φ_T. The concrete sentence above was $\neg\mathrm{prov}_T(\mathrm{sub}(x, x))$.

We now know that T is incomplete. We would like to analyse Gödel's sentence, in particular we ask:

- Is φ_T true?
- What else can we say about φ_T?

We will see that φ is true, but not provable in T. (Incompleteness of T follows again, using that if φ were true, then it would be provable in $\mathsf{ZF}_{\mathrm{Fin}}$.) Moreover, we will use the analysis of ψ to prove that T cannot prove its own consistency. This is Gödel's second incompleteness theorem.

Lemma 4.4.1. *φ_T is not provable in T.*

Proof. Write φ for φ_T. Suppose that $T \vdash \varphi$. Then $(\mathrm{Fin}, \in) \models \mathrm{prov}_T(c_\varphi)$. Since true Σ_1-sentences are provable in $\mathsf{ZF}_{\mathrm{Fin}}$, we have that $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{prov}_T(c_\varphi)$. Since φ is a Gödel sentence for T, this implies $\mathsf{ZF}_{\mathrm{Fin}} \vdash \neg\varphi$. This contradicts the assumption. □

In the previous proof, we had the chain of implications:

$$T \vdash \varphi \Rightarrow (\mathrm{Fin}, \in) \models \mathrm{prov}_T(c_\varphi) \Rightarrow \mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{prov}_T(c_\varphi) \Rightarrow \mathsf{ZF}_{\mathrm{Fin}} \vdash \neg\varphi.$$

Thus $T \vdash \varphi$ yields a contradiction. We will show below that the formalised version $\mathrm{prov}_T(c_\varphi) \to \perp$ (equivalent to $\neg\mathrm{prov}_T(c_\varphi)$) of this implication is provable in $\mathsf{ZF}_{\mathrm{Fin}}$.

Lemma 4.4.2. *For formulas ψ and θ, the following sentences are provable in $\mathsf{ZF}_{\mathrm{Fin}}$:*

(1) $(\mathrm{prov}_T(c_\psi) \wedge \mathrm{prov}_T(c_\theta)) \to \mathrm{prov}_T(c_{\psi\wedge\theta})$.
(2) $(\mathrm{prov}_T(c_\psi) \vee \mathrm{prov}_T(c_\theta)) \to \mathrm{prov}_T(c_{\psi\vee\theta})$.
(3) $(\mathrm{prov}_T(c_\psi) \wedge \mathrm{prov}_T(c_{\psi\to\theta})) \to \mathrm{prov}_T(c_\theta)$.

Proof. (1) $\mathsf{ZF}_{\mathrm{Fin}}$ proves the stronger statement $\forall\psi, \theta\ (\mathrm{prov}_T(\psi) \wedge \mathrm{prov}_T(\theta) \to \mathrm{prov}_T(\psi \wedge \theta))$. This is because the concatenation of proofs of ψ and θ with the additional formula $\psi \wedge \theta$ yields a proof of $\psi \wedge \theta$. This is provable in any theory in which concatenations of arbitrary finite functions exist, for instance in $\mathsf{ZF}_{\mathrm{Fin}}$. (2) and (3) are similar. □

Lemma 4.4.3. *For every Σ_1-sentence, $\mathsf{ZF}_{\mathrm{Fin}}$ proves $\varphi \to \mathrm{prov}_T(c_\varphi)$.*

Proof. The proofs of Lemmas 4.2.8 and 4.2.9 are inductive and thus work in $\mathsf{ZF}_{\mathrm{Fin}}$. So we have the stronger fact: $\mathsf{ZF}_{\mathrm{Fin}}$ proves that for every Σ_1-sentence θ, $\theta \to \mathrm{prov}_T(c_\theta)$ holds. □

Let $\mathrm{con}(T)$ denote the sentence $\neg\mathrm{prov}_T(\bot)$ stating that T is consistent, i.e. that there is no proof of a contradiction from T. Note that this sentence is Π_1. It is not necessarily Σ_1. If it were Σ_1, then if true, it would be provable in $\mathsf{ZF}_{\mathrm{Fin}}$ and thus in any extension T. Hence $T \vdash \mathrm{con}(T)$ would hold for any such theory. This contradicts Gödel's second incompleteness theorem.

Theorem 4.4.4. *(Gödel's second incompleteness theorem) Suppose that T is a consistent extension of $\mathsf{ZF}_{\mathrm{Fin}}$ that is Σ_1-definable over $(\mathrm{Fin}, \in)$. Then $T \nvdash \mathrm{con}(T)$.*

Proof. The statement of Lemma 4.4.1 is provable in $\mathsf{ZF}_{\mathrm{Fin}}$ by Lemmas 4.4.2 and 4.4.3. Thus

$$\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{prov}_T(c_\varphi) \to \neg\mathrm{con}(T)$$

Now suppose towards a contradiction that $T \vdash \mathrm{con}(T)$. Since $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{con}(T) \to \neg\mathrm{prov}_T(c_\varphi)$, we have $T \vdash \neg\mathrm{prov}_T(\varphi)$. Since $\mathsf{ZF}_{\mathrm{Fin}} \vdash \varphi \longleftrightarrow \neg\mathrm{prov}_T(c_\varphi)$ by the choice of φ, we have $T \vdash \varphi$. But this contradicts Lemma 4.4.1. □

Lemma 4.4.5. *Suppose that T is a consistent extension of $\mathsf{ZF}_{\mathrm{Fin}}$ that is Σ_1-definable over $(\mathrm{Fin}, \in)$ and φ_T is a Gödel sentence for T. Then $T \vdash \varphi_T \longleftrightarrow \mathrm{con}(T)$.*

Proof. One direction was proved in the previous proof. The other direction is a simple exercise. □

Remark 4.4.6. The proof of the second incompleteness Theorem 4.4.4 also works of instead of prov_T we define φ_T by using a formula ψ representing provability as in Rosser's proof, if the conditions in Lemmas 4.4.2 and 4.4.3 are satisfied. Under these assumptions, $\mathsf{ZF}_{\mathrm{Fin}} \vdash \mathrm{con}(T) \to \varphi$ for Rosser's sentence φ.

The proof of Lemma 4.4.5 fails for φ if T is a theory with $T \vdash \neg\mathrm{con}(T)$. (Note that for any extension S of $\mathsf{ZF}_{\mathrm{Fin}}$ as above, $T = S \cup \{\mathrm{con}(S)\}$ is consistent by Theorem 4.4.4 and T has this property.)

It has been a well known open question for decades whether Rosser's sentences have a simple characterisation, in the same way that Gödel's sentence is provably equivalent to $\mathrm{con}(T)$. This would imply that all Rosser sentences are provably equivalent. Solovay and Guaspari (1979) showed that for a certain modification of prov_T, all Rosser sentences are provably equivalent, but this is open for the Rosser sentence for prov_T itself.

Lecture 23
07. July

4.5. Incompleteness of extensions of Peano arithmetic.

We already considered the notion of definable subsets of structures. We now look at the situation that one can define a structure in another one and this is provable with respect to a theory.

Definition 4.5.1.

(1) A structure $\mathcal{M} = (M, \mathcal{F})$ is called *interpretable* in a structure $\mathcal{N} = (N, \mathcal{G})$ if there exists a structure $\mathcal{M}' = (M', \mathcal{F}')$ isomorphic to $\mathcal{M}$ such that for some $k \in \mathbb{N}$:
   (a) M' is a subset of N^k definable over $\mathcal{N}$.
   (b) Each $R \in \mathcal{F}'$ is a definable over $\mathcal{N}$ subset of $N^{k \cdot l}$ for the appropriate $l \in \mathbb{N}$.

   If $k = 1$, then $\mathcal{M}$ is called *definable* in $\mathcal{N}$.

(2) An $\mathcal{L}$-theory S is called *interpretable* in a $\mathcal{K}$-theory T if for some $k \in \mathbb{N}$, there are $\mathcal{K}$-formulas $\varphi(x)$ and $\psi_s(\vec{x})$ for every $s \in \mathcal{L}$ such that for $k \in \mathbb{N}$, $M_\varphi = \{\vec{x} \in M^k \mid \varphi(\vec{x})\}$, $R_{\psi_s} = \{\vec{x} \mid \psi_s(\vec{x})\}$ and $\mathcal{G} = \langle R_{\psi_s} \mid s \in \mathcal{L}\rangle$:

$$T \vdash (M_\varphi, \mathcal{G}) \models S.$$

   More precisely, for each sentence $\theta \in S$, T proves that θ is true in this structure.

   If $k = 1$, then S is called *definable* in T.

An example for interpretability of structures is that the complex field $(\mathbb{C}, 0, 1, +, \cdot)$ is interpretable in the real field $(\mathbb{R}, 0, 1, +, \cdot)$. Conversely, one can show that $(\mathbb{R}, 0, 1, +, \cdot)$ is not interpretable in $(\mathbb{C}, 0, 1, +, \cdot)$.

Interpretability of theories in (2) above states that for all models $\mathcal{N} = (N, \mathcal{G})$ of T, one can define a model of S as a subset of N^k for some $k \in \mathbb{N}$, and this works uniformly, i.e. with fixed formulas.

It is clear that PA is definable in $\mathsf{ZF}_{\mathrm{Fin}}$. We will show that $\mathsf{ZF}_{\mathrm{Fin}}$ is definable in PA. In fact, the domain of the model of $\mathsf{ZF}_{\mathrm{Fin}}$ will be the same as the model of PA. Write $\in_{\mathsf{PA}}$ for the $\in$-relation defined in PA that we will define. The set of $\in_{\mathsf{PA}}$-formulas is defined by replacing $\in$ by $\in_{\mathsf{PA}}$ recursively in $\in$-formulas, so this set is Δ_1-definable over $(\mathrm{Fin}, \in)$.

We explain why the first incompleteness theorem for Δ_1 over $(\mathrm{Fin}, \in)$ definable extension of $\mathsf{ZF}_{\mathrm{Fin}}$ (Theorem 4.3.2) implies incompleteness of Δ_1 over $(\mathrm{Fin}, \in)$ definable extension T of PA. Towards a contradiction, suppose that T is complete. For any $\in$-formula φ, let φ_{PA} denote the $\in_{\mathsf{PA}}$-formula obtained by replacing $\in$ by $\in_{\mathsf{PA}}$ everywhere in φ. Let

$$T_{\in} = \{\varphi \mid \varphi \text{ is an } \in\text{-formula with } T \vdash \varphi_{\mathsf{PA}}\}.$$

Since T is a complete $\mathcal{L}_{\mathrm{Arith}}$-theory, $T_{\in}$ is a complete $\mathcal{L}_{\in}$-theory. $T_{\in}$ is Σ_1-definable. But this contradicts the first incompleteness Theorem 4.3.2.

We now work towards the definition of $\in_{\mathsf{PA}}$. It can be shown that one cannot define multiplication $\cdot$ in $(\mathbb{N}, +)$. Our aim is to show Gödel's result that one can define exponentiation $\exp(m, n) = m^n$ in PA. An intuition why this should be possible is that one can easily define very fast growing functions in PA, for example the product

$$f(n) = \prod_{p \text{ prime},\ p \leq n} p$$

of all primes $\leq n$.

Lemma 4.5.2.

(1) *(Division with remainder)* PA *proves* $\forall m, n\ m < n \to \exists k, l\ (n = k \cdot m_l \wedge l < m)$.
(2) PA *proves: for all primes with* $p | m \cdot n$*, we have* $p | m$ *or* $p | n$.

Proof. The proofs are by induction and are left as exercises. □

The idea for defining exponentiation is to code finite sequences by natural numbers. This allows recursive definitions, thus we can define exponentiation from multiplication, iterated exponentiation from exponentiation etc.

The following definition codes pairs of natural numbers by a single natural number.

Definition 4.5.3. Define $p(a, b) = (a + b)^2 + a + 1$.

Lemma 4.5.4. *If* $p(a, b) = p(a', b')$*, then* $a = a'$ *and* $b = b'$.

Proof. Note that $a + b < a' + b'$ implies that $p(a, b) \leq (a + b + 1)^2 < p(a', b')$. Therefore, $p(a, b) = p(a', b')$ implies that $a + b = a' + b'$. $a = a'$ and $b = b'$ follow. □

Lemma 4.5.5. *There is a definable partial function* $\rho \colon \mathbb{N}^2 \to \mathbb{N}$ *such that for all* $m \geq 1$ *and all* $0 < i < j \leq m$*, the numbers* $\rho(m, i)$ *and* $\rho(m, j)$ *are mutually prime.*

Proof. Suppose that B is least such that $\forall 0 < i \leq m\ i | b$. Define $\rho(m, i) = bi + 1$.

Suppose that p is a prime with $p | bi + 1$ and $p | bj + 1$, where $0 < i < j \leq m$. Then $p \nmid b$. Moreover, we have $p | (bj + 1) - (bi + 1) = b(j - i)$. Apply Lemma 4.5.2. If $p | j - i$, then $p | b$ by the definition of b. Hence $p | b$. However, we showed that $p \nmid b$. □

We use the previous lemma to code finite sets and finite sequences.

Someone remarked correctly during the lecture, the following lemma is not formulated in $\mathcal{L}_{\text{Arith}}$. I will correct this.
More precisely, the lemma should state that for any c, m and any $k > m$, one can find some c' that "outputs" the same values as c up to m, and outputs the only additional value k up to k.

Lemma 4.5.6.

(1) *There is a definable set $R \subseteq \mathbb{N}^3$ such that for all m and all $S \subseteq \{0, \dots, m\}$, there is some c such that for all i, $R(c, m, i) \Leftrightarrow i \in S$.*
(2) *(A variant of Gödel's β-function) There is a definable function $\beta\colon \mathbb{N}^3 \to \mathbb{N}$ such that for all m and all $c_0, \dots, c_m$, there is some c such that $\forall i \leq m\ \beta(c, m, i) = c_i$.*

Proof. (1) We define $c = \prod_{i \in S} \rho(m, i)$. Then $\forall i \leq m\ (i \in S \Leftrightarrow \rho(m, i) | c)$. We define $R(c, m, i) \Leftrightarrow \rho(m, i) | c$.

(2) Apply (1) to $\{p(i, c_i) \mid i \leq m\}$. □

One needs for formulate the previous lemma appropriately in $\mathcal{L}_{\text{Arith}}$. Then they are provable in PA.

Lemma 4.5.7. *Exponentiation* $\exp(m, n) = m^n$ *is definable in* PA.

Proof. More precisely, the claim is that one can define a function exp with $\exp(m, 0) = 1$ and $\exp(m, n+1) = \exp(m, n) \cdot m$ for all m, n.

We want to define $\exp(m, n) = k$ informally by the statement: *There are $c_1, \dots c_n$ with $c_1 = m$, for all $1 \leq i < n$, we have $c_{i+1} = m \cdot c_i$ and $c_n = k$.*. Formally, $\exists l, c\ \beta(c, l, 1) = m \wedge \forall 1 \leq i < n\ \beta(c, l, i+1) = m \cdot \beta(c, l, i) \wedge \beta(c, l, n) = k$. □

Note that one can show that exp is Δ_1-definable.

Using exp, we now define

$$m \in_{\mathsf{PA}} n \Leftrightarrow \exists k, r\ k > 0 \wedge r < \exp(2, m) \wedge n = (2 \cdot k + 1) \cdot \exp(2, m) + r].$$

Lemma 4.5.8. $\in_{\mathsf{PA}}$ *satisfies the axioms and schemes of* ZF_{Fin}.

Proof. See Problem 52 on sheet 12. □

In arithmetic, one defines bounded quantifiers of the form $\forall x \leq y$ and $\exists x \leq y$. this leads to a hierarchy of Σ_n, Π_n formulas and Δ_n sets. Using the above interpretations, one can show that the Σ_n-formulas of set theory are translated precisely to Σ_n-formulas of arithmetic and vice versa.

The first incompleteness theorem applies to all axiom systems listed by an algorithm.

This is because one can show that all sets listed by an algorithm are Σ_1-definable. The Σ_1-definition states that there exists a run of the algorithm that outputs the given number n at some stage.

Coversely, any Σ_1-definable subset of $(\mathbb{N}, +, \cdot)$ can be listed by an algorithm simply by search for a witness to the Σ_1-statement and then verifying the formula by running finite checks.

This chapter completes the solution of Hilbert's program at the end of Section 1: (5) is false by (the proof of) Gödel's first incompleteness theorem; (3) and (4) are false by Gödel's second incompleteness theorem.

5. Complete theories

Lecture 24
12. July

Contrary to the theories studied above, many interesting theories are actually complete. For instance, the theory of algebraically closed fields of fixed characteristic.

In this section, we study two techniques to prove completeness of a theory: quantifier elimination and categoricity.

5.1. **Quantifier elimination.** Suppose that T is an $\mathcal{L}$-theory and $\varphi(\vec{x})$, $\psi(\vec{x})$ are $\mathcal{L}$-formulas. We say that φ and ψ are *equivalent modulo* T and write $\varphi \sim_T \psi$ if $T \vdash \varphi \leftrightarrow \psi$.

Definition 5.1.1. An $\mathcal{L}$-theory T has *quantifier elimination* if for every $\mathcal{L}$-formula $\varphi(\vec{x})$, there is a quantifier-free $\mathcal{L}$-formula $\psi(\vec{x}) \sim_T \varphi(\vec{x})$.

Note that quantifier elimination depends on the choice of the language. In fact, one can extend any theory to a theory in an extended language with quantidier

We now want to see that it is sufficient to show absoluteness for a very restricted class of existential formulas.

Definition 5.1.2. A formula ψ is called *simple existential* if it is of the form $\exists x \varphi$ for some quantifier-free formula φ. If φ is moreover a conjunction of basic formulas (i.e. formulas of the form ψ or $\neg\psi$, where ψ is atomic), then ψ is called *primitive existential.*

The next lemma shows that primitive existential formulas are sufficient.

Lemma 5.1.3. *An $\mathcal{L}$-theory T has quantifier elimination if and only if every primitive existential formula is equivalent modulo T to a quantifier-free formula.*

Proof. Suppose that this condition holds. We show quantifier elimination by induction on formulas. The cases $\wedge$, $\vee$ and $\neg$ are obvious. Suppose that $\exists x \varphi(x)$ is an $\mathcal{L}$-formula. We can assume by the inductive hypothesis that $\varphi(x)$ is quantifier-free. Therefore, we can assume that φ is in disjunctive normal form, i.e. $\varphi = \bigvee_{i \leq n} \varphi_i$, where each is a conjunction of basic formulas (see Definition 5.1.2). Then $\exists x \varphi(x)$ is equivalent to the formula $\bigvee_{i<n} \exists x \varphi_i(x)$. By the assumption, this is equivalent modulo T to a quantifier-free formula. □

Example 5.1.4. The theory DLO of dense linear orders without end points consists of the axioms:

(1) $\forall x \; x \not< x$
(2) $\forall x, y, z \; (x < y \wedge y < z \rightarrow x < z)$
(3) $\forall x, y, z \; (x < y \vee y < x \vee x = y)$
(4) $\forall x, y \; (x < y \rightarrow \exists z \; x < y < z)$
(5) $\forall x \; \exists y, z \; (x < y \wedge z < x)$

Definition 5.1.5. From now on, we will use the logical constants $\top$, $\bot$. The definition of $\models$ is extended so that $\top$ is always true and $\bot$ is always false. Moreover, the definition of $\vdash$ is extended so that $\top$ is provable.

Lemma 5.1.6. DLO *satisfies quantifier elimination.*

Proof. We first show that negated atomic formulas are not needed. To see this, note that in DLO, $x \neq y \leftrightarrow x < y \vee y < x$, and $x \not< y \leftrightarrow y < x \vee x = y$. So in DLO, all quantifier-free formulas are equivalent to formulas in disjunctive normal form build only from atomic formulas.

Suppose that $\varphi(\vec{x}, y)$ is a conjunction of atomic formulas. We can write $\varphi(\vec{x})$ as $\varphi_0(\vec{x}) \wedge \varphi_1(\vec{x}, y)$, where each of φ_0 and φ_1 is a conjunction of atomic formulas and y appears in all atomic formulas in φ_1.

If $y < y$ appears in φ_1, then $\exists y \; \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \bot$. If $y = x_i$ appears in φ_1, then $\exists y \; \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \varphi(\vec{x}, x_i)$. So assume otherwise.

Then only formulas of the form $y = y$, $y < x_i$ and $x_i < y$ appear in φ_1. We can omit all formulas of the form $y = y$. If only formulas of the form $x_i < y$ appear, then $\exists y\ \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \top$. If only formulas of the form $y < x_i$ appear, then $\exists y\ \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \top$. So assume otherwise.

We define $\theta(\vec{x}) = \bigwedge\{x_i < x_j \mid x_i < y \text{ and } y < x_j \text{ appear in } \varphi_1\}$. We can assume that for all $i \neq j$ not both $x_i < x_j$ and $x_j < x_i$ appear in $\theta \wedge \varphi_1$, since otherwise $\exists y\ \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \bot$.

If $\theta \wedge \varphi_0$ is not compatible with a linear order of all x_i which appearing in $\theta \wedge \varphi_0$, then $\exists y\ \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \bot$.

Otherwise fix such a linear order. Let x_i be maximal such that $x_i < y$ appears and x_j minimal such that $y < x_j$ appears. Then $x_i < x_j$ by the previous assumption. So $\exists y\ \varphi(\vec{x}, y) \sim_{\mathsf{DLO}} \top$. □

Quantifier elimination is a useful tool to prove completeness. For instance, quantifier elimination holds if the theory has a prime structure.

Definition 5.1.7. Suppose that T is an $\mathcal{L}$-theory and $\mathcal{M}$ is a model of T.

(a) $\mathcal{M}$ is a *prime structure* for T if it can be embedded into every model of T.
(b) $\mathcal{M}$ is a *prime model* for T if it can be elementarily embedded into every model of T.

If a theory T has quantifier elimination and a prime structure $\mathcal{M}$, then $\mathcal{M}$ is a prime model by absoluteness of quantifier-free formulas. Then $\mathcal{M} \prec \mathcal{N}$ holds for any model $\mathcal{N}$ of T, so T is complete.

Example 5.1.8. $(\mathbb{Q}, <)$ is a prime model of DLO. To see this, note that it is easy to show that $(\mathbb{Q}, <)$ is embeddable into any dense linear order without end points. In fact, a simple back-and-forth construction shoes that $(\mathbb{Q}, <)$ is isomorphic to any countable dense linear order without end points.

We now see a useful model theoretic criterion for quantifier elimination.

The *atomic diagram* $\mathrm{Diag}(\mathcal{M})$ of an $\mathcal{L}$-structure $\mathcal{M} = (M, \dots)$ is defined as the set of basic $\mathcal{L}_M$-formulas that are true in $\mathcal{M}$. In the following proof, we will further write $\vec{x} = (x_0, \dots, x_n)$, $\vec{a} = (a_0, \dots, a_n)$.

The following is a useful test for quantifier elimination. Moreover, Lemma 5.1.3 shows that it is sufficient to check condition (b) only for primitive existential formulas (defined below).

These two paragraphs are new. They explain how quantifier-free formulas behave with respect to substructures.

Recall that for $\mathcal{L}$-structures $\mathcal{M} = (N, \mathcal{F})$ and $\mathcal{N} = (N, \mathcal{G})$ with $M \subseteq N$, $\mathcal{M}$ is a substructure of $\mathcal{N}$ if and only if the constant symbols have the same interpretations in $\mathcal{M}$ and $\mathcal{N}$, and the functions and relations of $\mathcal{M}$ are obtained by restricting those of $\mathcal{N}$. Thus by definition, $\mathcal{M}$ is a substructure of $\mathcal{N}$ if and only if the truth of atomic formulas is the same in $\mathcal{M}$ and $\mathcal{N}$.

Any quantifier-free statements are obtained by combining atomic formulas using $\wedge$, $\vee$ and $\neg$. by induction on formulas, for any substructure $\mathcal{M}$ of a structure $\mathcal{N}$, the truth of any quantifier-free formula is the same in $\mathcal{M}$ and $\mathcal{N}$.

Lemma 5.1.9. *If $\mathcal{M} = (M, \dots)$ is an $\mathcal{L}$-structure, T is an $\mathcal{L}$-theory and $\varphi(x_0, \dots, x_n)$ is an $\mathcal{L}$-formula, then the following statements are equivalent.*

(a) *There is a quantifier-free $\mathcal{L}$-formula $\psi(\vec{x})$ with $T \models \forall\vec{x}(\varphi(\vec{x}) \leftrightarrow \psi(\vec{x}))$.*
(b) *If $\mathcal{M} = (M, \dots)$ and $\mathcal{N} = (N, \dots)$ are models of T and $\mathcal{A} = (A, \dots)$ is a substructure of both $\mathcal{M}$ and $\mathcal{N}$, then $\mathcal{M} \models \varphi(a_0, \dots, a_n) \Leftrightarrow \mathcal{N} \models \varphi(a_0, \dots, a_n)$ for all $a_0, \dots, a_n \in A$.*

Proof. The first implication follows from the fact that quantifier-free statements about elements of $\mathcal{A}$ are absolute between $\mathcal{A}$, $\mathcal{M}$ and $\mathcal{N}$. We now assume that (b) holds. If $T \models \forall\vec{x}\varphi(\vec{x})$, then let $\psi = \top$ (the true statement) and if $T \models \forall\vec{x}\varphi(\vec{x})$, then let $\psi = \bot$

(the false statement). We can thus assume that both $T \cup \{\varphi(\vec{x})\}$ and $T \cup \{\neg\varphi(\vec{x})\}$ are consistent. We choose new constants and $(d_0, \dots, d_n)$ and write $\vec{d} = (d_0, \dots, d_n)$. Let

$$\Gamma(\vec{x}) = \{\psi(\vec{x}) \mid \psi(\vec{x}) \in \mathrm{Form}_{\mathcal{L}} \text{ is quantifier-free and } T \cup \{\varphi(\vec{x})\} \models \psi(\vec{x})\}$$

denote the set of quantifier-free consequences of $T \cup \{\varphi(\vec{x})\}$.

Claim 5.1.10. *$T \cup \Gamma(\vec{d}) \models \varphi(\vec{d})$.*

Proof. Assuming otherwise, there is a model $\mathcal{M}$ of $T \cup \Gamma(\vec{d}) \cup \{\neg\varphi(\vec{d})\}$. Let $\mathcal{A}$ be the substructure of $\mathcal{M}$ that is generated by $\vec{d}^{\mathcal{M}} = (d_0^{\mathcal{M}}, \dots, d_n^{\mathcal{M}})$. We now show that the theory $\Sigma = T \cup \mathrm{Diag}(\mathcal{A}) \cup \{\varphi(\vec{d})\}$ is consistent. Assuming that it is inconsistent, there are $\psi_0(\vec{d}), \dots, \psi_n(\vec{d}) \in \mathrm{Diag}(\mathcal{A})$ such that $T \models \bigwedge_{i \leq m} \psi_i(\vec{d}) \to \neg\varphi(\vec{d})$ and hence $T \models \varphi(\vec{d}) \to \bigvee_{i \leq m} \neg\psi_i(\vec{d})$. So $\bigvee_{i \leq m} \neg\psi_i(\vec{d}) \in \Gamma(\vec{d})$. Since $\mathcal{M} \models \Gamma(\vec{d})$ and $\Gamma(\vec{d})$ only contains quantifier-free formulas, we have $\mathcal{A} \models \Gamma(\vec{d})$. So $\mathcal{A} \models \bigvee_{i \leq m} \neg\psi_i(\vec{d})$ and thus there is some $i \leq m$ with $\mathcal{A} \models \neg\psi_i(\vec{d})$. But this contradicts the fact that $\psi_i(\vec{d}) \in \mathrm{Diag}(\mathcal{A})$. Since we have now shown that Σ is consistent, let $\mathcal{N}$ be a model of Σ. Then $\mathcal{N}$ is a model of $T \cup \{\neg\psi(\vec{d})\}$ and we can hence assume that it contains $\mathcal{A}$ as a substructure. Since $\mathcal{M}$ is a model of $T \cup \{\psi(\vec{d})\}$ that contains $\mathcal{A}$ as a substructure and $\vec{d}^{\mathcal{M}} = \vec{d}^{\mathcal{N}} \in \mathcal{A}$, this contradicts our assumption (b). □

By the completeness theorem, there are finitely many sentences $\theta_0(\vec{d}), \dots, \theta_k(\vec{d}) \in \Gamma(\vec{d})$ such that $\Gamma(\vec{d}) \models \theta(\vec{d})$ for $\theta(\vec{d}) = \bigwedge_{i \leq k} \theta_i(\vec{d})$. Then $T \models \theta(\vec{d}) \leftrightarrow \varphi(\vec{d})$ and hence $T \models \forall\vec{x}(\theta(\vec{x}) \leftrightarrow \varphi(\vec{x}))$. □

Lecture 25
14. July

We now show quantifier elimination for vector spaces and algebraically closed fields.

The language $\mathcal{L}_{V(K)}$ of vector spaces over a field K consists of the language $\mathcal{L}_{\mathrm{AddGroup}} = \{0, +\}$ of additive groups with an additional function symbol f_λ for scalar multiplication with each $\lambda \in K$.

Lemma 5.1.11. *The theory of infinite-dimensional vector spaces over a fixed field K has quantifier elimination.*

Proof. Suppose that V_0 and V_1 are K-vector spaces of infinite dimension that both contain a K-vector space V. Suppose that $\psi = \exists x \varphi(x, x_0, \dots, x_n)$ is a simple existential formula that holds in V_0 for some $a_0, \dots, a_n \in V$, witnessed by some $a \in V_0$. If $a \in V$ then ψ holds in V_1, so suppose that $a \in V_0 \setminus V$.

First suppose that $V \subsetneq V_1$ and let $b \in V_1 \subsetneq V$. Let $W_0 = \langle V \cup \{a\} \rangle^{V_0}$ and $W_1 = \langle V \cup \{b\} \rangle^{V_1}$ denote the subspaces generated by $V \cup \{a\}$ in V_0 and by $V \cup \{b\}$ in V_1, respectively. Pick an isomorphism $f \colon W_0 \to W_1$ with $f{\restriction}V = \mathrm{id}$ and $f(a) = b$. Since $W_0 \models \varphi(a, a_0, \dots, a_n)$ and isomorphisms preserve truth, we have $W_1 \models \varphi(b, a_0, \dots, a_n)$ and hence $V_1 \models \exists x \varphi(x, a_0, \dots, a_n)$.

If $V = V_1$, then V has infinite dimension. Let $V' \subsetneq V$ be a subspace with $a_0, \dots, a_n \in V'$. Applying the previous argument to V' instead of V yields $V_1 \models \exists x \varphi(x, a_0, \dots, a_n)$. □

This case was missing in the lecture

One can also be show this for arbitrary vector spaces over a fixed infinite field with a similar argument.

For both finite and infinite fields K, it is easy to see that the theory of infinite K-vector spaces has a prime model. Therefore it is complete.

Let ACF_p denote the theory of algebraically closed fields of characteristic p. The next result uses some facts from algebra about the existence and uniqueness of algebraic closures.

Theorem 5.1.12. *For any prime p or $p = 0$, the theory ACF_p has quantifier elimination.*

Proof. Suppose that L and M are algebraically closed fields of characteristic p and R is a substructure of both, i.e. a subring. Then the quotient fields of R in L and M are isomorphic and hence we can assume that they are equal and denote this field by K. Moreover the proof of uniqueness of algebraic closures shows that there is an isomorphism between the algebraic closures of K in L and M that is the identity on K. We can thus assume that there is an an algebraic closure $\bar{K}$ of K that is contained in both L and M.

We now assume that some primitive existential formula $\exists x \varphi(x, x_0, \dots, x_n)$ holds in L for some $a_0, \dots, a_n \in R$. Moreover assume that this is witnessed by some $a \in L$. If $a \in \bar{K}$, then $\varphi(a, a_0, \dots, a_n)$ holds in M, since φ is quantifier-free and hence absolute. We can thus assume that $a \notin \bar{K}$. Suppose that $\varphi(x) = (\bigwedge_{i<k} f_i(x) = 0) \wedge (\bigwedge_{j<l} g_j(x) \neq 0)$, where f_i and g_j are polynomials over R. Then $f_i(a) = 0$ for all $i < k$. Since a is not algebraic over K, each f_i is the zero polynomial.

Since $g_j \neq 0$ in $R[X]$ for all $j < l$, the polynomial $x \cdot \prod_{j<l} g_j(x) + 1$ is not constant and hence has a root b in M. Hence $g_j(b) \neq 0$ for all $j < l$ and thus $M \models \varphi(b, a_0, \dots, a_n)$.

Instead of arguing as in the last paragraph, one can also note that the set defined by $\varphi(x)$ is cofinite, i.e. its complement is finite. Note that any algebraically closed field K is infinite, since for finite $K = \{a_0, \dots, a_n\}$ the polynomial $1 + \prod_{i \leq n}(X - a_i)$ does not have roots in K. Therefore $M \models \exists x\ \varphi(x, a_0, \dots, a_n)$, as required. □

By the uniqueness of the algebraic closure up to isomorphism, ACF_p has a prime structure. Since it has quantifier elimination, this is a prime model. So ACF_p is complete.

Definition 5.1.13.

(1) A structure $\mathcal{M} = (M, \mathcal{F})$ is called *minimal* if it only every subset of M that is definable over $\mathcal{M}$ with parameters is either finite or cofinite.

(2) A *strongly minimal* theory is a complete theory all models of which are minimal.

It is easy to see that quantifier elimination implies the following result.

Lemma 5.1.14. *Every algebraically closed field is minimal.*

The ordered real field $(\mathbb{R}, 0, 1, +, \cdot, <)$ is not minimal, but it can be shown to satisfy the following property.

Definition 5.1.15. Suppose that $\mathcal{L}$ is a language that contains a binary relation symbol $<$.

(1) A structure $\mathcal{M} = (M, \mathcal{F})$ in which $<^{\mathcal{M}}$ is a strictly linear order is called *o-minimal*[33] if every subset of M that is definable over $\mathcal{M}$ with parameters is a finite union of intervals and points. (An interval can be open, half-open, and tend to ∞ or $-\infty$.)

(2) An *o-minimal* theory is a theory all models of which are *o*-minimal.

o-minimality can be understood as weak form of quantifier elimination. Moreover, in the case of the ordered real field, the definable sets are the semialgebraic sets. So the study of *o*-minimal structures generalises real algebraic geometry.

We now give some examples for using quantifier elimination for ACF_p to obtain elegant proofs of some results about polynomials.

Theorem 5.1.16. *(Hilbert's Nullstellensatz) Suppose that K is an algebraically closed field and $f_0, \dots, f_n \in K[X_0, \dots, X_k]$ such that $I = (f_0, \dots, f_n)$ is a proper ideal in $K[X_0, \dots, X_n]$ (i.e. $1 \notin I$). Then there are $a_0, \dots, a_k \in K$ such that $f_i(a_0, \dots, a_k) = 0$ for all $i \leq n$.*

Proof. The trick is to construct an algebraically closed extension $\bar{L}$ of K where such a root $(a_0, \dots, a_k)$ exists, and then use quantifier elimination to conclude that such a root exists in K. Recall that $K \prec \bar{L}$ by quantifier elimination.

[33] o stands for *order*.

By Zorn's Lemma applied to the set of proper ideals J in $K[X_0,\dots,X_k]$ which contain I, there is a maximal ideal J in $K[X_0,\dots,X_k]$ containing I. Since J is a maximal ideal, $L = K[X_0,\dots,X_k]/J$ is a field. Moreover we can identify K with a subfield of L by identifying $a \in K$ with $a+J$. For each $i \leq k$ we have $f_i(X_0+J,\dots,X_k+J) = f_i(X_0,\dots,X_n)+J = J$. The first equation holds by the definition of addition and multiplication in quotient rings and the second equation holds since $f_i(X_0,\dots,X_k) \in I$.

Therefore, the formula $\theta = \exists x_0,\dots,x_k \bigwedge_{i\leq n} f_i(x_0,\dots,x_k) = 0$ is true in L and hence also in its algebraic closure $\bar{L}$. The latter holds because the formula $\bigwedge_{i\leq n} f_i(x_0,\dots,x_k)$ is remains true in all large models, since it is quantifier-free. By quantifier elimination for ACF_p, θ is also true in $K \prec \bar{L}$. So $f_0,\dots,f_n$ have a common root $(a_0,\dots,a_k) \in K^{k+1}$, as required. □

If K is an algebraically closed field, then a subset S of K^n is called *constructible* if it is a finite Boolean combination of zero sets of polynomials in $K[X_0,\dots,X_{n-1}]$ and their complements.

By quantifier elimination, every definable subset of K^n is constructible (and conversely). In more detail, any definable subset is definable by some formula generated by $\wedge$ and $\vee$ from atomic formulas and negations of atomic formulas.

Lemma 5.1.17. *(Chevalley) If K is an algebraically closed field, S is a constructible subset of K^m and $f\colon K^m \to K^n$ is a polynomial function, then $f(S)$ is constructible.*

Proof. Suppose that f is given by the polynomials $g_0,\dots,g_{n-1} \in K[X_0,\dots,X_{m-1}]$. Then $(a_0,\dots,a_{n-1}) \in f(S) \Leftrightarrow \exists x_0,\dots,x_{m-1} \in K \bigwedge_{i<n} g_i(x_0,\dots,x_{m-1}) = a_i$. Thus $f(S)$ is definable and hence constructible. □

We now define the model-theoretic version of algebraic closure and show that quantifier elimination for ACF_0 and ACF_p implies that for these theories, the algebraic closures in the sense of algebra and of model theory are equal.

Definition 5.1.18. Suppose that $\mathcal{M} = (M,\mathcal{F})$ is an $\mathcal{L}$-structure, $\varphi(x)$ is an $\mathcal{L}$-formula and $A \subseteq M$.

(a) Let $\varphi(\mathcal{M}) = \{x \in M \mid \mathcal{M} \models \varphi(x)\}$.
(b) φ is called *algebraic over* $\mathcal{M}$ if $\varphi(\mathcal{M})$ is finite.
(c) An element $x \in M$ is called *algebraic over* A if $\mathcal{M} \models \varphi(x)$ for some algebraic $\mathcal{L}_A$-formula.
(d) The *algebraic closure* $\mathrm{acl}(A) = \mathrm{acl}^{\mathcal{M}}(A)$ of A in $\mathcal{M}$ is the set of all algebraic elements of M over A.
(e) A is *algebraically closed* in $\mathcal{M}$ if $\mathrm{acl}(A) = A$.

If A is a subset of an algebraically closed field K of characteristic p, then acl_K is equal to the standard algebraic closure (from algebra) by quantifier elimination for ACF_p. To see this, suppose that $a \in \mathrm{acl}(A)$ and $\varphi(x)$ is a quantifier-free formula with parameters in A and only finitely many solutions including a. By quantifier elimination, we can assume that it is quantifier-free and replace it by a logically equivalent formula $\bigvee_{i\in I} \bigwedge_{i\in J_i} \varphi_{i,j}(x)$ with basic formulas $\varphi_{i,j}$. Then a satisfies the formula $\psi(x) = \bigwedge_{i\in J_i} \varphi_{i,j}(x)$ for some $i \in I$ – the same is true when the basic inequalities $\varphi_{i,j}(x)$ are removed. This conjunction of polynomial equations can be rewritten as a single polynomial equation, showing that a is in the algebraic closure in the usual sense (as defined in field theory).

Lecture 26
19. July

5.2. **Categoricity.**

Definition 5.2.1. If κ is an infinite cardinal, a theory T is called *κ-categorical* if T has exactly one model of size κ up to isomorphism.

Lemma 5.2.2. *(Vaught's test) Suppose that κ is an infinite cardinal, $\mathcal{L}$ is a language with $|\mathcal{L}| \leq \kappa$ and T is a consistent theory with no finite models. If T is κ-categorical, then it is complete.*

Proof. We show that any two models $\mathcal{M}$ and $\mathcal{N}$ of T are elementarily equivalent. Since $\mathcal{M}$ and $\mathcal{N}$ are infinite and $|\mathcal{L}| \leq \kappa$, $\mathrm{Th}(\mathcal{M})$ and $\mathrm{Th}(\mathcal{N})$ have infinite models $\mathcal{M}'$ and $\mathcal{N}'$ of size κ by the Löwenheim-Skolem Theorem. By our assumption, $\mathcal{M} \equiv \mathcal{M}' \cong \mathcal{N}' \equiv \mathcal{N}$. □

If a theory is ω-categorical, is it necessarily κ-categorical for uncountable cardinals κ? The next theory is a simple counterexample.

Example 5.2.3. Consider the theory T of equivalence relations with exactly two classes, both of which are infinite. The language is $\mathcal{L} = \{E\}$, where E is a binary relation symbol. The theory T consists of the axioms for equivalence relations together with the axioms

$$\exists x, y\ \neg E(x, y)$$

$$\forall x, y, z\ (E(x, y) \vee E(x, z) \vee E(y, z)$$

$$\varphi_n = \forall x_0, \dots, x_n (\bigwedge_{i \leq n} E(x_0, x_i) \rightarrow \exists x \bigwedge_{i \leq n} (x \neq x_i \wedge E(x, x_i)))$$

for all $n \in \mathbb{N}$. It is easy to see that any two countable models of T are isomorphic. However T is not κ-categorical for any uncountable cardinal κ. To see this, let $\mathcal{M}$ be a model of T of size κ where both equivalence classes have size κ and let $\mathcal{N}$ be a model of size κ where one equivalence class has size κ and the other one has $\aleph_0$.

The theory DLO of dense linear orders without end points in Example 5.1.4 is another example of a complete theory that is ω-cateogrical, but not κ-categorical for uncountable cardinals κ.

Theorem 5.2.4. DLO *is $\aleph_0$-categorical.*

Proof. The following is a typical example of a *back-and-forth construction*; this is an iterative constructions that alternates between enumerations of two structures.

Suppose that $\mathcal{A} = (A, <_A)$ and $\mathcal{B} = (B, <_B)$ are countably infinite models of DLO and let $\langle a_n \mid n \in \mathbb{N} \rangle$ and $\langle b_n \mid n \in \mathbb{N} \rangle$ enumerate them without repetitions.

We construct a sequence of finite sets A_n, B_n of A, B and isomorphisms $f_n \colon A_n \to B_n$ by recursion. Let $A_0 = B_0 = f_0 = \emptyset$. Suppose that A_n, B_n and f_n are already defined.

We first extend the domain. If $a_n \in A_n$ (this will happen often), let $A'_n = A_n$, $B'_n = B_n$ and $f'_n = f_n$. If $a_n \notin A_n$, let $A'_n = A_n \cup \{a_n\}$. Since $\mathcal{B}$ is a model of DLO, there is some $b'_n \in B$ such that the extension f'_n of f_n with $f'_n(a_n) = b'_n$ is an isomorphism from A'_n to $B'_n = B_n \cup \{b'_n\}$.

We proceed similarly for the range. If $b_n \in B'_n$, let $A_{n+1} = A'_n$, $B_{n+1} = B'_n$ and $f_{n+1} = f'_n$. If however $b_n \notin B'_n$, we let $B_{n+1} = B_{n'} \cup \{b_n\}$ and choose some $a'_n \in A$ such that the extension f_{n+1} of f'_n with $f_{n+1}(a'_n) = b_n$ from $A_{n+1} = A'_n \cup \{a'_n\}$ to B_{n+1} is an isomorphism.

Finally, let f denote the union of the functions f_n for all $n \in \mathbb{N}$. By the construction, $f \colon A \to B$ is bijective. It is an isomorphism, since each f_n is an isomorphism. □

If $\mathcal{A} = (A, <_A)$ and $\mathcal{B} = (B, <_B)$ are strict linear orders, their *lexicographical order* $<_{\text{lex}}$ on $A \times B$ is defined by letting $(a, b) <_{\text{lex}} (a', b')$ if $a < a'$ or $(a = a' \wedge b < b')$. It is easy to check that this is always a linear order.

Theorem 5.2.5. DLO *is not κ-categorical for any uncountable cardinal κ.*

Proof. Let $<_{\mathbb{Q}}$ denote the usual linear order on $\mathbb{Q}$.

We first claim that for any linear order $(A, <_{\mathcal{A}})$, the lexicographical order $<_{\text{lex}}$ on $A \times \mathbb{Q}$ given by $<_{\mathcal{A}}$ and $<_{\mathbb{Q}}$ is dense and does not have end points. To show this, assume that

$(a,q) <_{\text{lex}} (b,r)$. If $a <_A b$, then we can pick any $q' \in \mathbb{Q}$ with $q <_{\mathbb{Q}} q'$ and have that $(a,q) <_{\text{lex}} (a,q') <_{\text{lex}} (b,r)$. If otherwise $a = b$ and $q <_{\mathbb{Q}} r$, then we choose some $q' \in \mathbb{Q}$ with $q <_{\mathbb{Q}} q' <_{\mathbb{Q}} r$ and have that $(a,q) <_{\text{lex}} (a,q') <_{\text{lex}} (b,r)$. Moreover $<_{\text{lex}}$ has no end points, since there are no end points in $<_{\mathbb{Q}}$.

As usual in set theory, κ equals the set of ordinals $\alpha < \kappa$ and is wellordered by the usual order $<$ on ordinals. We further let $<^*$ denote the reverse linear order on κ that is defined by $\alpha <^* \beta \iff \beta < \alpha$. Now let $<_{\text{lex}}$ and $<^*_{\text{lex}}$ denote the lexicographical orders on $\kappa \times \mathbb{Q}$ that are induced by $<$, $<_{\mathbb{Q}}$ and $<^*$, $<_{\mathbb{Q}}$, respectively. By the previous paragraph, $(\kappa \times \mathbb{Q}, <_{\text{lex}})$ and $(\kappa \times \mathbb{Q}, <^*_{\text{lex}})$ are dense linear orders without end points.

We show that $(\kappa \times \mathbb{Q}, <_{\text{lex}})$ and $(\kappa \times \mathbb{Q}, <^*_{\text{lex}})$ are not isomorphic. Note that $(\kappa \times \mathbb{Q}, <_{\text{lex}})$ contains strictly increasing sequences of length κ, for instance $\langle (\alpha, 0) \mid \alpha < \kappa \rangle$.

However, we claim that $(\kappa \times \mathbb{Q}, <^*_{\text{lex}})$ does not contain strictly increasing sequences of length κ. Towards a contradiction, suppose that $\langle (\alpha_\beta, q_\beta) \mid \beta < \kappa \rangle$ is such a sequence. Then the sequence $\langle \alpha_\beta \mid \beta < \kappa \rangle$ is a non-increasing sequence in κ by the definition of $<^*_{\text{lex}}$, i.e. $\alpha_\beta \geq \alpha_\gamma$ for all $\beta < \gamma < \kappa$. Since $(\kappa, <)$ is a well-order, there is some $\beta < \kappa$ such that $\alpha_\beta = \alpha_\gamma$ for all γ with $\beta \leq \gamma < \kappa$. By the definition of $<^*_{\text{lex}}$, it follows that the sequence $\langle q_\gamma \mid \beta \leq \gamma < \kappa \rangle$ is an uncountable strictly decreasing sequence in $\mathbb{Q}$. But $\mathbb{Q}$ is countable. Note that the proof shows there is no uncountable strictly decreasing sequence in $(\kappa \times \mathbb{Q}, <^*_{\text{lex}})$. □

Suppose that $\mathcal{K} = (K, 0, 1, +, \cdot)$ is a field. As above, $\mathcal{L}_{V(K)} = \mathcal{L}_{\text{Group}} \cup \{m_a \mid a \in K\}$ is the language of K-vector space, where m_a is interpreted as scalar multiplication with a. Let T denote the $\mathcal{L}$-theory of $\mathcal{K}$-vector spaces.

Example 5.2.6. The $\mathcal{L}_{V(K)}$-theory T of K-vector spaces is κ-categorical for all cardinals $\kappa > |K|$, since any two K-vector spaces are isomorphic if and only if their dimension is equal. Moreover, for any K-vector space V of size $|V| > |K|$, we have $|V| = \dim(V)$, by a counting argument.

Thus for finite fields K, T is κ-categorical for all infinite cardinals κ. For all countably infinite fields K, T it is not $\aleph_0$-categorical, but κ-categorical for all uncountable cardinals κ.

Lecture 27
21. July

We now turn to algebraically closed fields. Recall that a field is called *algebraically closed* if every polynomial $f(X) \in K[X]$ has a root in K. If moreover $K \subseteq L$ are fields, then an element $x \in L$ is called *algebraic* over K if it is the solution to some polynomial $f \neq 0$ in $K[X]$ and *transcendent* otherwise. Moreover L is called *algebraic* over K if each of its elements is algebraic over K.

Note that since for all $a, b \neq 0$ we have $a \cdot b \neq 0$, the characteristic n is necessarily a prime number; if $n = m \cdot k$ with $m, k > 1$, then $(m \cdot 1) \cdot (k \cdot 1) = 0$ in K and hence one of $m \cdot 1$ and $k \cdot 1$ is equal to 0, contradicting the minimality of n.

We use the following results from algebra without proofs.

Theorem 5.2.7. *Every field K has an algebraic closure $\bar{K}$ that is unique up to isomorphism.*

Lemma 5.2.8. *For every $n > 0$, there is a field $\mathbb{F}_{p^n}$ of characteristic p and size p^n that is unique up to isomorphism.*

We aim to define the transcendence degree of field extensions. To this end, we will assume that K, L and M are algebraically closed fields with $K \subseteq L, M$. A subset A of L is *algebraically independent* over K if for all $a_0, \ldots, a_n \in A$ and $f \in K[X_0, \ldots, X_n]$ with $f \neq 0$, we have $f(a_0, \ldots, a_n) \neq 0$. Moreover, a *trancendence base* of L over K is a maximal algebraically independent subset of L over K. If A is such a base, it follows that L is an algebraic extension of $K(A)$. So for every $x \in L$, there is a polynomial with coefficients in $K[A]$ with $f(x) = 0$.

We can use the next lemma to show that the size of transcendence bases is unique.

Lemma 5.2.9. *(Exchange property) Suppose that A and B are transcendence bases of L over K and $b \in B$, then there is some $a \in A$ such that $A' = (A \setminus \{a\}) \cup \{b\}$ is a transcendence base of L over K.*

By successively replacing elements of A with elements of B in a transfinite induction, we obtain that $|A| = |B|$. We can thus define the *transcendence degree* of L over K are unique size of a transcendence base. If K is the algebraic closure of $\mathbb{Q}$ or $\mathbb{F}_p$ (depending on the characteristic), then this is simply called the *transcendence degree* of L.

Lemma 5.2.10. *Any two algebraically closed fields of the same characteristic and transcendence degree are isomorphic.*

Proof. Suppose that A and B are transcendence bases of algebraically closed fields L and M over K and $F\colon A \to B$ is a bijection. It can be easily checked from the definition of transcendence base that F extends uniquely to a ring isomorphism $F\colon K(A) \to K(B)$. Hence F extends to an isomorphism between the fields of fractions $K(A)$ and $K(B)$. Then L is an algebraic closure of $K(A)$, M is an algebraic closure of $K(B)$ and hence they are isomorphic by the uniqueness of algebraic closures. □

Example 5.2.11. ACF_p is not $\aleph_0$-categorical, but κ-categorical for all uncountable cardinals κ. This follows from the fact that two algebraically closed fields with characteristic p are isomorphic if and only if their transcendence degree is equal.

By Vaught's test (Lemma 5.2.2), ACF_p is complete. We now derive some consequences of this fact.

Lemma 5.2.12. *(Lefschetz principle) The following conditions are equivalent for any sentence φ in the language $\mathcal{L}_{\mathrm{rings}}$ of rings and fields.*

(a) *φ holds in every algebraically closed field of characteristic 0.*
(b) *φ holds in the complex numbers.*
(c) *φ holds in some algebraically closed field of characteristic 0.*
(d) *There is some $n \in \mathbb{N}$ such that for all primes $p > n$, φ holds in all algebraically closed fields of characteristic p.*
(e) *There are arbitrarily large primes p such that φ holds in some algebraically closed field of characteristic p.*

Proof. The implications from (a) to (b) and from (b) to (c) are clear. Assuming (c) we have that φ holds in $\mathbb{C}$ and thus $\mathsf{ACF}_0 \models \varphi$, since ACF_0 is complete. Therefore there is a finite set $\Delta \subseteq \mathsf{ACF}_0$ with $\Delta \models \varphi$ and hence $\mathsf{ACF}_p \models \varphi$ if p is sufficiently large. The implication from (d) to (e) is again clear. If (e) holds, we assume towards a contradiction that $\mathsf{ACF}_0 \not\models \varphi$. Since ACF_0 is complete, we have $\mathsf{ACF}_0 \models \neg\varphi$. By the implication from (a) to (d) for $\neg\varphi$, we have that $\neg\varphi$ holds in all algebraically closed fields of sufficiently large characteristic, contradicting the assumption. □

Theorem 5.2.13. *Every injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.*

Proof. We first show this for the algebraic closure $\bar{\mathbb{F}}_p$ of $\mathbb{F}_p$ for all primes p. Suppose that $f\colon (\bar{\mathbb{F}}_p)^n \to (\bar{\mathbb{F}}_p)^n$ is given by polynomials $p_0, \dots, p_k$ with coefficients $a_0, \dots, a_l \in \bar{\mathbb{F}}_p$ and it is injective, but some $b \in \bar{\mathbb{F}}_p$ is not in its range. The subfield $K \subseteq \bar{\mathbb{F}}_p$ generated by $a_0, \dots, a_k, b$ is finite and the polynomials $p_0, \dots, p_k$ define an injective map $f'\colon K \to K$. Since K is finite f' is surjective, contradicting the assumption that $b \notin \mathrm{ran} f'$.

Suppose that there is a counterexample that is given by polynomials of degrees at most d. Let $\Phi_{n,d}$ be the first-order statement that every injective polynomial map with n

inputs and outputs that is given by polynomials of degrees at most d is surjective. Since $AFC_p \models \Phi_{n,d}$, this holds in $\mathbb{C}$ as well by Lemma 5.2.12. $\square$

References

[1] Lorenz Halbeisen and Regula Krapf. Gödel's Theorems & Zermelo's Axioms.

[2] Ernest Schimmerling. *A course on set theory.* Cambridge University Press, 2011.

[3] Martin Ziegler. *Mathematische Logik.* Springer, 2010.