Mathematical Logic & Foundations of Mathematics

John Hutchinson

Mathematical Sciences Institute
Australian National University

Primary website: https://johnehutchinson.github.io
ANU website: https://maths.anu.edu.au/people/john-hutchinson

February 28, 2026

Preface

These Notes are the text for a course on Mathematical Logic at the third and fourth year honours level, or first year graduate level, for students with a strong background in pure/theoretical mathematics.

I have tried to provide a clear route through to the major results. There are various optional asides and additional material, but this is indicated as such.

Mathematical logic grew out of the work by Hilbert, Gödel, Tarski, and others in the period 1930–1950 in order to address the paradoxes and problematic foundational issues raised previously by the work of Cantor, Frege and Russell.

The subject is one which is currently taught and researched in University Departments of Mathematics, Computer Science and Philosophy, with varying emphasis on topics and approach. The emphasis here is, naturally, mathematical! But we will also consider the broader insights and applications.

Pure/theoretical mathematics is an abstract discipline, extracting, analysing, extending and axiomatising the essence of ideas that may be common to a variety of disciplines, including the physical and biological sciences, computer science, economics and increasingly the social sciences.

Mathematical logic abstracts further from the reasoning itself which is used in mathematics, providing insight to the limits of human and machine cognition.

"Mathematical logic is the most abstract branch of mathematical thought, the most abstract human discipline.[1]

Artificial Intelligence [AI]

This has an impact on the way the course is taught and assessed, and on the future of mathematical research.

The assessment is discussed in detail on the course homepage. But in essence it will be approximately 20% class participation, 20% assignments, 15% midsemester and 45% final exams. Class participation and discussion is required and is an essential part of the course.

Regarding the future of mathematics research see the Talk by Terry Tao, including the interview in the second half. There is a series of AMS articles on AI, see in particular the articles by the Australian mathematicians Terry Tao, Akshay Venkatesh and Geordie Williamson.

"Our generation is witnessing the coming-of-age of automated theorem proving and proof assistants, which seem destined to transform mathematical practice. Mathematicians of the future may be commonly using proof assistants and automated proof verifiers, with large and growing databases of formally verified proofs, to undertake their mathematical investigations." (Hamkins, 2021, §5.4)

[1] Introduction (Goldstern and Judah, 1995).

Contents

Detailed Contents

Introduction

In mathematics we typically prove results from a set of axioms, as for example in the study of groups, fields, rings, topology or the real number system. In mathematical logic we formalise the methods of proof, and provide axioms for the underlying logic and rules of inference

The first emphasis in these notes is on the Completeness and Incompleteness Theorems for first-order logic. This is covered in Chapters 1–4 and I have provided a direct route through to these results. This is conceptually the most challenging part of the course.

You will find the material from Chapters 5 onwards, at least to the extent it is treated here, to be more similar to the mathematics you have previously learnt.

The beginning and introductory material from the later chapters is used in Chapters 1–4. You may already know some of this material. But I always point to this material explicitly when we proceed through the first four chapters, and we will cover it in class as it is needed. I have left a more complete (and yet still very incomplete!) development of model theory, computability, the axiom of choice, ordinals, cardinals and the Zermelo–Fraenkel axioms of set theory until Chapters 5 and beyond. Most of these chapters can be expanded into a book in their own right!

There are many *Exercises*. They are intended primarily to help you understand the material, and to check that you do indeed understand. Please attempt them all, and write out your solutions as you move through the text.

Chapter 1

Structures and Languages

1.1 Truth and Proof

What is the relationship between proof and truth? Does every truth have a proof?

The following introductory comments use terminology[1] that has not yet been defined. Hopefully it will be reasonably clear from the context what is intended. Defining these concepts carefully will be a major undertaking.

1.1.1 Truth

Suppose for example that $\mathfrak{G}$[2] is a mathematical structure (such as a group) and $\varphi(x_1, \ldots, x_n)$ is an assertion (i.e. formula, in standard logic terminology) in some appropriate language $\mathcal{L}$ (for groups in this case). Then $\varphi(x_1, \ldots, x_n)$ will be true or false in $\mathfrak{G}$ once we assign an element a_i of $\mathfrak{G}$ to each x_i.

We will define carefully what it means for $\varphi(x_1, \ldots, x_n)$ to be *true* in $\mathfrak{G}$ for such an assignment. We write this as

$$\mathfrak{G} \models \varphi[a_1, \ldots, a_n] \tag{1.1}$$

and read it as "$\varphi(x_1, \ldots, x_n)$ is *true* (or *is satisfied*) in $\mathfrak{G}$ at $(a_1, \ldots, a_n)$".

Suppose now that φ is a sentence (a formula with no free variables)[3], and Σ is a set of sentences. By

$$\Sigma \models \varphi, \tag{1.2}$$

which we read as "Σ semantically implies φ", it is meant that φ is true in every model in which all sentences from Σ are true.

Note that (1.2) does not indicate how one might establish that $\Sigma \models \varphi$, just that it *is* the case for some reason or other.

1.1.2 First-Order Logic

To define (1.1) and (1.2) carefully we first need to define the set of all possible formulas in the language $\mathcal{L}$. For us, this set of formulas in $\mathcal{L}$ is the set of formulae in the *first-order logic*[4] for $\mathcal{L}$. We carry out that program in this Chapter.

[1] In particular: Proof, truth, structure, language, formula, sentence.

[2] $\mathfrak{G}$ is the letter G in the Fraktur font. See Subsection 1.2.3

[3] Such as $\forall x\, \forall y\, (x \cdot y = y \cdot x)$. But not $x \cdot y = y \cdot x$, in which the variables x and y are free.

[4] "First-order" means that quantifiers $\forall$ and $\exists$ range over the elements of a structure, rather than over subsets of a structure.

First-order logic may seem to be too restrictive in the case of group theory since we cannot express the notion of an arbitrary subset or subgroup in first-order logic.

But all of mathematics can be developed in set theory, and set theory is most naturally developed in an appropriate first-order logic. *Much* more needs to be said about this matter, and this we will do as the course proceeds.

The notion of truth is a semantic[5] *notion.*
The notion of proof is a syntactic[6] *notion.*

In principle one can verify and analyze a proof as a purely syntactic object, without a concept of meaning and without interpreting the language in a model.

1.1.3 Proof

In comparison with (1.2), with Σ and φ as there, one defines

$$\Sigma \vdash \varphi \tag{1.3}$$

to mean there is a formal proof of φ from Σ, using some deductive calculus of logical rules and axioms. Equation (1.3) is read as "there is a (formal) proof from Σ to φ".

In Chapter 2 we develop the Hilbert proof system. We study formal proofs not with the intention of writing such proofs, but in order to understand the nature of proof and its capabilities and limits. This is currently significant in relation to proof checking and theorem proof assistant programs such as Lean.

1.1.4 "Truth = Proof"

Gödel's Completeness Theorem in Chapter 3 is the amazing result:

$$\Sigma \models \varphi \Longleftrightarrow \Sigma \vdash \varphi \tag{1.4}$$

In words: The sentence φ is true whenever all the sentences (think "axioms") in Σ are true, if and only if, there is a formal proof of φ from Σ.

The direction "$\Longleftarrow$" is straightforward, it just says that the logical rules and axioms preserve truth. But the direction "$\Longrightarrow$" is impressive: if we can deduce φ from Σ for whatever reason then there is a formal logical proof in (for example) the Hilbert system.

I need to clarify the statement "Truth = Proof". It is true in first-order logic. But all of mathematics can (essentially) be done in set theory, and set theory is done in first-order logic. I will elaborate as the course proceeds.

A Final Remark: We are interested in an analysis at the meta-logic level of formal proofs in first-order logic. Hilbert systems for first-order logic are particularly convenient since its formal proofs are linear sequences of strings of symbols, and are readily codeable arithmetically.

Gentzen natural deduction systems and Gentzen sequent calculus systems, both of which are tree-like, are more appropiate for proof construction and proof analysis.

[5] Semantic: adjective, relating to meaning in language or logic. Origin: mid 17th century, from French 'sémantique', from Greek sēmantikos 'significant'.

[6] Syntactic: adjective, relating to the arrangement and rules for words and phrases to create well-formed sentences in a language. Origin: mid 16th century: via late Latin from Greek 'suntaxis', from sun 'together' + tassein 'arrange'.

1.2 Mathematical Structures

1.2.1 What is a Structure?

A *(mathematical) structure* $\mathfrak{A}$ (for example, a group, field, vector space, set of complex numbers, etc.) can be represented as follows:

$$\mathfrak{A} = \langle A, R_i, F_j, C_k \rangle_{\ i \in I,\ j \in J,\ k \in K} \tag{1.5}$$

where:

(i) A is the universe under consideration (e.g., the set of group elements, the set of real numbers, etc.), and $A \neq \varnothing$ for technical reasons,

(ii) each R_i is an n_i-ary relation on A for some natural number $n_i \geq 1$, i.e. $R_i \subseteq A^{n_i}$,

(iii) each F_j is an n_j-ary function on A for some natural number $n_j \geq 1$, i.e. $F_j : A^{n_j} \to A$,

(iv) each C_k is a member of A, i.e. $C_k \in A$.

We shall try to be consistent in our notation. Thus the universe of a structure $\mathfrak{A}$ is A, of $\mathfrak{B}$ is B, of $\mathfrak{C}$ is C, etc. (See the following Notes regarding the Fraktur Font used here.)

1.2.2 Examples

1. The structure for a group with multiplication $\circ$ and identity element e might be written $\mathfrak{G} = \langle G, \circ, e \rangle$.

We could include a unary inverse operator denoted by the symbol ι or $^{-1}$, so the structure is then $\mathfrak{G} = \langle G, \circ, \iota, e \rangle$ or $\mathfrak{G} = \langle G, \circ, ^{-1}, e \rangle$. Alternatively we could treat the inverse as a defined operator via the axioms for group theory. There is considerable flexibility and we will not need to be concerned with this from a foundational perspective.

2. The structure for a linear ordering is of the form $\mathfrak{L} = \langle L, < \rangle$, where L is a set and $<$ is a linear ordering of L.

3. The structure for a simple undirected graph is $\mathfrak{G} = \langle V, E \rangle$, where V is the set of vertices and E is a binary relation interpreted by $E(v, w)$ iff there is an edge between v and w.

4. Zermelo–Frankel set theory is discussed in Chapter 13. The language is particularly simple as it has just a single binary relation symbol, interpreted as membership and usually written $\in$. If we want to distinguish between the symbol and its interpretation in a structure, we occasionally write E for the symbol.

What makes this impressive is that all of mathematics can be formulated in set theory. What makes this strange is that there are countable models of the axioms, by the Lowenheim–Skolem Theorem.

Exercise 1.1. If membership is just treated as a binary relation, what are some of the properties that it should have? □

5. The (first-order) structure for the real number system is $\mathfrak{R} = \langle \mathbb{R}, +, \cdot, <, 0, 1, \rangle$ where $+$ and $\cdot$ are binary operators on $\mathbb{R}$, $<$ is a binary relation, 0 and 1 are constants, all with their standard interpretation.

However, the completeness axiom for the real number system refers to arbitrary subsets of $\mathbb{R}$ and so is not a first-order concept. On the other hand, we can imbed $\mathfrak{R}$ within set theory, which *is* first-order. Again, we discuss this later.

1.2.3 Fonts & Alphabets – An Aside

1. *Fraktur Font*: For structures/models in mathematical logic and for Lie algebras, the Fraktur Font is standard usage. In LaTeX use `\mathfrak{ }`.

Here it is:

$$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}, \mathfrak{E}, \mathfrak{F}, \mathfrak{G}, \mathfrak{H}, \mathfrak{I}, \mathfrak{J}, \mathfrak{K}, \mathfrak{L}, \mathfrak{M}, \mathfrak{N}, \mathfrak{O}, \mathfrak{P}, \mathfrak{Q}, \mathfrak{R}, \mathfrak{S}, \mathfrak{T}, \mathfrak{U}, \mathfrak{V}, \mathfrak{W}, \mathfrak{X}, \mathfrak{Y}, \mathfrak{Z}.$$
$$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \mathfrak{d}, \mathfrak{e}, \mathfrak{f}, \mathfrak{g}, \mathfrak{h}, \mathfrak{i}, \mathfrak{j}, \mathfrak{k}, \mathfrak{l}, \mathfrak{m}, \mathfrak{n}, \mathfrak{o}, \mathfrak{p}, \mathfrak{q}, \mathfrak{r}, \mathfrak{s}, \mathfrak{t}, \mathfrak{u}, \mathfrak{v}, \mathfrak{w}, \mathfrak{x}, \mathfrak{y}, \mathfrak{z}.$$

The script version in Figure 1.1 is for handwritten notes, blackboard/whiteboard talk and discussion, or to impress your friends.

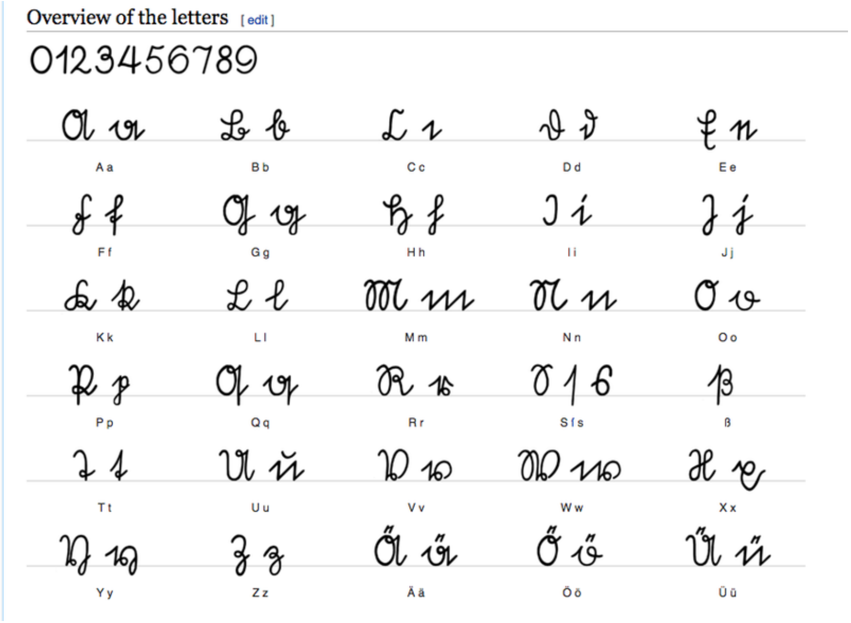


Figure 1.1: Handwritten version of the Fraktur font.

Only the capitals $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$ are commonly used in mathematical logic, while $\mathfrak{G}$, $\mathfrak{M}$, $\mathfrak{N}$ and $\mathfrak{L}$ are occasionaly used. This should not be a major stumbling block in your learning process.

2. *Greek Alphabet*: Used extensively.

α (alpha), β (beta), γ (gamma), δ (delta), ϵ (epsilon), ε (varepsilon), ζ (zeta), η (eta), θ (theta), ϑ (vartheta), ι (iota), κ (kappa), λ (lambda), μ (mu), ν (nu), ξ (xi), o (omicron), π (pi), ϖ (varpi), ρ (rho), ϱ (varrho), σ (sigma), ς (varsigma), τ (tau), υ (upsilon), φ (phi), φ (varphi), χ (chi), ψ (psi), ω (omega).

and

Γ (Gamma), Δ (Delta), Θ (Theta), Λ (Lambda), Ξ (Xi), Π (Pi), Σ (Sigma), Υ (Upsilon), Φ (Phi), Ψ (Psi), Ω (Omega).

Omicron is typeset the same as the roman letter o, and the missing capitals are typeset the same as their roman equivalents.

3. *Hebrew Alphabet*: Only need $\aleph$ (Aleph).

1.2.4 Variants for Structures

1. *Nonempty Universe*: The restriction that $A \neq \varnothing$ is standard in mathematical logic, although not universal in mathematical practice. See (Johnstone, 1987, page 24) for the price one must pay in terms of a modified version of modus ponens, if one allows an empty universe.

Exercise 1.2. How about $\forall x\, \varphi(x) \to \exists x\, \varphi(x)$? What if the universe is empty? □

2. *Many-Sorted Structure*: In the case of a vector space, the universe could be the (disjoint) union of the set of scalars and the set of vectors. Unary relations S, V could be used to single out these two sets/sorts.

3. *Relational Structure*: This is a structure in which there are only constants and relations. An n-ary function can be identified with an $(n+1)$-ary relation in the natural way.

One could restrict considerations to relational structures, with essentially no loss of generality, as it does make some details easier. But it is less convenient when working with functions.

Constants are also particular (unary) relations, or 0-ary functions. But it is inconvenient to work without constants.

1.2.5 Foundational Issues

In matters of a constructive and foundational nature we restrict I, J, K to be finite. The languages, formulas, etc. can then be coded up algorithmically by integers. We say more about this as we proceed.

Another useful situation is to restrict I and J to be finite while allowing the index K for constant symbols to be infinite (for example, having one constant symbol for *every* element in some non-finite structure). See Chapter 3.

The generalisation of results to higher cardinalities usually involves no significant new ideas, other than using ordinals[7] for enumeration/iteration purposes.

1.3 Language and Syntax

We will see in this Section how the symbols of a language $\mathcal{L}$ are used to construct terms, formulas, sentences, etc.

Syntax refers to the manner in which such meaningful expressions are built up in first-order logic, and to the notion and properties of formal proofs.

[7] See Chapter 11.

1.3.1 Symbols for a Language

A *language* $\mathcal{L}$ consists of a set of symbols. The language to describe the previous structure $\mathfrak{A}$ in (1.5) consists of:

- a set of relation symbols $\{r_i : i \in I\}$, each of some assigned arity,
- a set of function symbols $\{f_j : j \in J\}$, each of some assigned arity,
- a set of constant symbols $\{c_k : k \in K\}$.

1.3.2 Structures for a Language

The structure $\mathfrak{A} = \langle A, R_i, F_j, C_k \rangle_{i\in I, j\in J, k\in K}$ in (1.5) is an $\mathcal{L}$-*structure* if there is a one-one correspondence $r_i \leftrightarrow R_i$, $f_j \leftrightarrow F_j$ and $c_k \leftrightarrow C_k$, such that the arities match up.

The interpretation in $\mathfrak{A}$ of a relation symbol $r \in \mathcal{L}$ is often written $r^{\mathfrak{A}}$. Similarly the interpretation of a function symbol f is often written $f^{\mathfrak{A}}$. And the interpretation of a constant symbol c is often written $c^{\mathfrak{A}}$.

So we will often write instead of (1.5),

$$\mathfrak{A} = \langle A, r_i^{\mathfrak{A}}, f_j^{\mathfrak{A}}, c_k^{\mathfrak{A}} \rangle_{i\in I,\, j\in J,\, k\in K} \quad \text{or just} \quad \mathfrak{A} = \langle A, r^{\mathfrak{A}}, f^{\mathfrak{A}}, c^{\mathfrak{A}} \rangle, \tag{1.6}$$

if it is clear from context what is intended.

Remark 1.3.

1. *Important Distiction*: The relation/function/constant *symbols* in a formal language $\mathcal{L}$, and their *interpretation* as actual relations/functions/constants in a structure $\mathfrak{A}$, should not be confused with each other.

2. *Different Structures – Same Language*: Think of groups and the language of group theory.

   Even the *Peano Axioms* for arithmetic have infinitely many non-isomorphic models apart from the standard model. Their study can often tell us something significant about the standard model. See Chapter 8.

3. *Uncluttering*: Eventually we may just rely on context to distinguish between symbols in a language and their interpretations in a structure, and use the same notation in both cases.

   Some authors do not like this. But always making a distinction via notation between symbol and interpretation can lead to very cluttered writing. □

1.3.3 Logical Symbols

Besides the relation, function and constant symbols specific to the language $\mathcal{L}$, we also have the following *logical symbols* common to all first-order languages, and which are used to build up the terms and formulas of $\mathcal{L}$:

(,)	parentheses,
$v_0, v_1, v_2, \ldots$	variable symbols (usually just called variables),
$\neg$	not,
$\wedge$	and,
$\forall$	for all,
$=$	equals.

The intention, as we explain subsequently, is that variables will be interpreted as elements of the universe A of some structure $\mathfrak{A}$ under consideration.

Instead of taking $v_0, v_1, \ldots, v_n, \ldots$ as variables, we could take $v, v', v'', v''', \ldots$ if we wish to make do with a finite number of symbols.

We normally use $x, y, u, v, \ldots$ to denote variables.

Definition 1.4. The set of variables for any language $\mathcal{L}$ is denoted by $\mathcal{V}$.

The symbols "$\neg$" and "$\wedge$" are *connectives*, "$\forall$" is a *quantifier*, "$=$" is a binary relation symbol (which will always be interpreted in a structure with the meaning "is the same as", rather than as a more general equivalence relation).

We take these logical symbols as *primitive* and define other logic symbols from them, see Subsection 1.3.5.

1.3.4 MetaLanguage and MetaLanguage Symbols

We have a mathematical/formal language $\mathcal{L}$ to describe our mathematical structures $\mathfrak{A}$. But we also have to discuss $\mathcal{L}$ itself and its relationship with structures $\mathfrak{A}$, and that we do in our *metalanguage*, which is English.

Unless we are doing concrete foundational matters the symbols of $\mathcal{L}$ are often treated as *set-theoretic objects*. This is particularly the case if we have an infinite number of symbols in $\mathcal{L}$ and we expand $\mathcal{L}$ to a larger language $\mathcal{L}^*$ — as is the case when we are considering infinite structures and we add a new constant symbol for each element of the structure. See the proof of Gödel's Completeness Theorem 3.18.

Exercise 1.5. So we will regard symbols either as marks on a piece of papers (in Gödel's Incompleteness Theorem), or as more abstract mathematical objects (in Gödel's Completeness Theorem). Comment? □

It will be convenient to use the following symbols in our metalanguage: $\Longrightarrow$ or $\Rightarrow$ for "implies", $\Longleftrightarrow$ for "if and only if", & for "and".

Also, $A := B$ is an abbreviation for "A by definition equals B", $A =: B$ is an abbreviation for "B by definition equals A".

The symbol "$=$" is used in a number of different ways. It is a logical symbol in the language $\mathcal{L}$.

But it is also used in a metalinguistic manner, when we might write for example that $\varphi = \varphi_1 \wedge \varphi_2$ or $\varphi = \varphi(x_1, \ldots, x_n)$. This would indicate (perhaps depending on the context) that the formula φ is the conjunction of two formulas, or is a formula whose free variable are among $x_1, \ldots, x_n$, or just that we want to draw attention to the particular free variables $x_1, \ldots, x_n$ for some reason or other, although there may be other free variables in φ.

Hopefully it will be clear from context and accompanying explanations what is intended.

1.3.5 Defined Logical Symbols

Propositional Logic

In the following I will assume a little knowledge on your part of propositional logic. If you know what is a truth table and what is a tautology, you should be fine. If not, please read and understand Section 6.1.

Definition 1.6. Taking $\neg, \wedge, \forall$ as primitive, the following definitions/abbreviations are justified in terms of truth tables as in Section 6.1 or just their standard meaning, and the standard meaning of $\exists$.

- (or): $\varphi \vee \psi$ for $\neg(\neg\varphi \wedge \neg\psi)$
- (*implies*): $\varphi \to \psi$ for $\neg(\varphi \wedge \neg\psi)$
- (*if and only if*): $\varphi \leftrightarrow \psi$ for $(\varphi \to \psi) \wedge (\psi \to \varphi)$
- (*there exists*): $\exists v\, \varphi$ for $\neg\forall v\, \neg\, \varphi$

Brackets are dropped where possible, and also sometimes added for clarity.

The convention is that $\neg$ is less binding than $\wedge$ and $\vee$, which are less binding than $\to$ and $\leftrightarrow$. For example,

$$\neg\varphi \vee \psi \to \theta \wedge \varphi \quad \text{means} \quad \big(\neg\varphi \vee \psi\big) \to (\theta \wedge \varphi) \quad \text{means} \quad \big((\neg\varphi) \vee \psi\big) \to (\theta \wedge \varphi).$$

1.3.6 Terms

A finite sequence (or string) of symbols is a *term* of $\mathcal{L}$ if and only if it is one of the following forms:

(i) A variable v or constant symbol c;

(ii) $f(t_1, \ldots, t_n)$, where f is an n-ary function symbol of $\mathcal{L}$, and each t_i is a term.

Alternatively, we can define terms set-theoretically:

The set of terms of $\mathcal{L}$ is the least set S of finite sequences such that:

(i) each variable and constant symbol belongs to S;

(ii) if f is an n-ary function symbol of $\mathcal{L}$ and $t_1, \ldots, t_n \in S$, then $f(t_1, \ldots, t_n) \in S$.

Intuitively a *term* is a variable or a constant symbol, or is built from them by using function symbols. A term has a value in an $\mathcal{L}$-structure once the variables in the term are assigned values in the structure. See Definition 1.14 for the precise definition.

1.3.7 Atomic Formulas

A finite sequence (or string) of symbols is an *atomic formula* of $\mathcal{L}$ iff it is one of the following forms:

(i) $t_1 = t_2$, where t_1 and t_2 are terms;

(ii) $r(t_1, \ldots, t_n)$, where r is an n-ary relation symbol and the t_i are terms.

Intuitively an *atomic formula* is the simplest expression that will be either true or false in a $\mathcal{L}$-structure once values are assigned to the variables in the formula.

1.3.8 Formulas

A finite sequence of symbols is a *formula* of $\mathcal{L}$ iff it is one of the following forms:

(i) an atomic formula;

(ii) $(\neg\varphi)$, where φ is a formula;

(iii) $(\varphi_1 \wedge \varphi_2)$, $(\varphi_1 \vee \varphi_2)$, $(\varphi_1 \to \varphi_2)$, $(\varphi_1 \leftrightarrow \varphi_2)$, where φ_1 and φ_2 are formulas;

(iv) $\forall v\, \varphi$, $\exists v\, \varphi$, where v is a variable and φ is a formula.

As for terms, we can define the sets of atomic formulas and of formulas set theoretically.

Intuitively a *formula* is an expression that is either true or false in a $\mathcal{L}$-structure once values are assigned to the free[8] variables in the formula. See Definition 1.18.

Keep the following distinction in mind. The difference between $\mathcal{L}$-terms and $\mathcal{L}$-formulas is the following: once values in an $\mathcal{L}$-structure $\mathfrak{A}$ are assigned to (free) variables in a term or a formula, the term will represent an *element in* $\mathfrak{A}$ and the formula will be a *statement about* $\mathfrak{A}$ which will be either true or false.

See Subsections 1.4.2 and 1.4.3.

1.3.9 Complexity of Terms and Formulas

It is convenient to use a small number of logical symbols when proving results about formulas.

For this reason we will normally just prove results for formulas built up using the logical symbols $\neg, \wedge, \forall$, and regard $(\varphi_1 \vee \varphi_2)$, $(\varphi_1 \to \varphi_2)$, $(\varphi_1 \leftrightarrow \varphi_2)$ and $\exists v\, \varphi$ as convenient abbreviations.

It is convenient to assign an integer $h(t)$ to terms t, and $h(\varphi)$ to formulas φ, where h corresponds to the maximum number of "steps" required in their construction. If you think of the construction as being given by a finite tree, then h is the height/complexity of this tree. See Figure 1.2.

For terms define the *term complexity* function h by:

- $h(v) = h(c) = 1$, where v is a variable symbol and c is a constant symbol.[9]
- $h\big(f(t_1, \dots, t_n)\big) = 1 + \max\{h(t_1), \dots, h(t_n)\}$, where $f(t_1, \dots, t_n)$ is a term.

Similarly for formulas φ, define a (different) *formula height/complexity* function h by:

- $h(\varphi) = 1$ if φ is atomic,
- $h(\neg\varphi) = 1 + h(\varphi)$,
- $h(\varphi \wedge \psi) = 1 + \max\{h(\varphi), h(\psi)\}$,

[8] See Subsection 1.3.15.

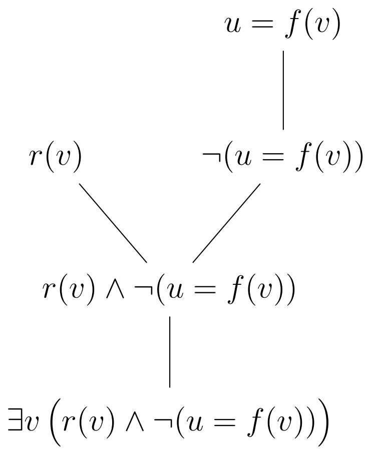
[9] Notice that "=" as used here is equality in the metalanguage. It is of course *not* the equality "=" for the formal language $\mathcal{L}$.

Some authors use a different symbol such as "≡" within the formal language. I think ambiguity and relying on context leads to a cleaner and less-cluttered exposition, but be careful!

- $h(\forall v\, \varphi) = 1 + h(\varphi)$.

Here we have taken $\neg, \wedge, \forall$ as primitive symbols.

See Figure 1.2.


$u = f(v)$
$r(v)$
$\neg(u = f(v))$
$r(v) \wedge \neg(u = f(v))$
$\exists v \left(r(v) \wedge \neg(u = f(v))\right)$

In the diagram the atomic formulas $r(v)$ and $u = f(v)$ both have (formula) complexity 1.

The formula $\neg(u = f(v))$ has complexity 2.

The formula $\exists v\,(r(v) \wedge \neg(u = f(v)))$ has complexity 4, corresponding to the 4 levels required for its construction.

The terms $v, u, f(v)$ have (term) complexity $1, 1, 2$ respectively.

Figure 1.2: Decomposition of a first-order formula into subformulas.

Exercise 1.7. What is the complexity of $r(v) \wedge \neg(u = f(v))$?

1.3.10 Proving Results about Terms and Formulas

Structural properties of terms and formulas can be established by induction on their complexity. To show every formula has some property P, we must establish four things:

1. Every atomic formula has property P;
2. If ψ is $\neg\varphi$ and φ has property P, then so does ψ;
3. If ψ is $\varphi_1 \wedge \varphi_2$ and both φ_1 and φ_2 have property P, then so does ψ;
4. If ψ is $\forall v\, \varphi$ and φ has property P, then so does ψ.

1.3.11 Uniqueness of Parsing

If terms or formulas are regarded as *concatenated strings* of symbols, uniqueness of parsing becomes an issue. Could a string of symbols be represented, say, as both $(\varphi_1 \wedge \varphi_2)$ and $(\varphi_1' \wedge \varphi_2')$, etc.? The answer is no, by a suitably induction on their complexity.

We will often drop, or sometimes add, brackets for the sake of readability and according to standard mathematical practice.

If we are interested in formulas primarily as concatenated strings, it is preferable to write $\wedge\varphi_1\varphi_2$ instead of $(\varphi_1 \wedge \varphi_2)$, $\neg\varphi$ instead of $(\neg\varphi)$, $\forall v\varphi$ instead of $(\forall v)\varphi$. This is known as *Polish notation*. We won't bother about doing this.

1.3.12 Other Logics

The language $\mathcal{L}$, the notions of term and formula of $\mathcal{L}$, the interpretation of these terms and formulas in structures for $\mathcal{L}$ (Section 1.4), and provability in $\mathcal{L}$ (Chapter 2), together determine what we refer to as the *first-order logic* over $\mathcal{L}$. Terminology is not universally consistent — often "language" and "logic" are used interchangeably.

Various other logics are possible over $\mathcal{L}$. If we add a second class of variables, interpreted as ranging over *subsets* of the interpretation, we obtain *second-order logic*. Likewise, higher-order logics.

Alternatively, new logical symbols can be added, such as a quantifier Q where $Qv \ldots$ is interpreted as meaning "there are uncountably many v such that $\ldots$", etc. Or, we may allow conjunctions and disjunctions of sets of formulas of certain infinite cardinalities. Also, various combinations of these ideas.

These and other logics have been studied extensively. Although they are not nearly as well-behaved as first-order logic, some of them do have nice properties.

From the perspective of studying the foundations of mathematics, first-order logic is the most important.

Moreover, all of mathematics can be done within set theory, and set theory has a first-order theory, as we discuss in Chapter 13.

1.3.13 Cardinality of a Language

The *cardinality* of a language $\mathcal{L}$ is

$$|\mathcal{L}| := \max\{\aleph_0, |I|, |J|, |K|\}, \tag{1.7}$$

where $|I|, |J|, |K|$ are the cardinalities of the sets I, J, K of relation, function and constant symbols respectively of $\mathcal{L}$. See (1.5), (1.6)

Exercise 1.8. $|\mathcal{L}|$ is the cardinality of the set of formulas of $\mathcal{L}$.

(If you have not at this stage studied any cardinality arithmetic, just treat the case where $|\mathcal{L}| = \aleph_0$.)

1.3.14 Subformulas

The set of *subformulas* of a given formula is defined inductively. In particular, the set of subformulas:

- of an atomic formula just contains the formula itself,
- of $\neg\varphi$ is $\{\neg\varphi\} \cup \{\text{subformulas of } \varphi\}$,
- of $\varphi \wedge \psi$ is $\{\varphi \wedge \psi\} \cup \{\text{subformulas of } \varphi\} \cup \{\text{subformulas of } \psi\}$,
- of $\forall v\, \varphi$ is $\{\forall v\, \varphi\} \cup \{\text{subformulas of } \varphi\}$.

And similarly for other logical symbols.

Exercise 1.9. What is the set of subformulas of $r(v) \wedge \neg(u = f(v))$? See Figure 1.2. □

1.3.15 Free and Bound Variables

Intuitively, the *free* variables of a formula φ are those variables that occur in φ but are not within the scope of a quantifier. They are the variables on whose values, in a given structure, the truth or falsity of φ depends (see Section 1.4).

The *bound* variables are those that occur within the scope of a quantifier.

Definition 1.10. The set $FV(\varphi)$ of *free variables* of a formula φ is defined inductively:

- If φ is an atomic formula then $FV(\varphi)$ is the set of all variables that occur in φ.
- $FV(\neg\varphi) = FV(\varphi)$.
- $FV(\varphi \wedge \psi) = FV(\varphi) \cup FV(\psi)$.
- $FV(\forall v\, \varphi) = FV(\varphi) \setminus \{v\}$.

The symbol "\" denotes set-theoretic subtraction.

Regarding defined logical symbols, it follows that

- $FV(\varphi \vee \psi) = FV(\varphi \to \psi) = FV(\varphi \leftrightarrow \psi) = FV(\varphi) \cup FV(\psi)$.
- $FV(\exists v\, \varphi) = FV(\varphi) \setminus \{v\}$.

The set $BV(\varphi)$ of *bound variables* of φ is similarly defined by induction on complexity, and is the set of variables of φ occurring within the scope of a quantifier.

Exercise 1.11. Look at the following examples. Then write out the definition for $BV(\varphi)$.
□

Example 1.12 *(Free and Bound variables).*

$$\begin{array}{lll}
\varphi_1 := r(u,v) \to u = w & FV(\varphi_1) = \{u,v,w\} & BV(\varphi_1) = \varnothing \\
\varphi_2 := \exists v \big(r(u,v) \to u = w\big) & FV(\varphi_2) = \{u,w\} & BV(\varphi_2) = \{v\} \\
\varphi_3 := \forall u\, \exists v \big(r(u,v) \to u = w\big) & FV(\varphi_3) = \{w\} & BV(\varphi_3) = \{u,v\} \\
\varphi_4 := \forall u\, \exists v \big(r(u,v) \to u = w\big) \vee (u = u) & FV(\varphi_4) = \{u,w\} & BV(\varphi_4) = \{u,v\} \\
\varphi_5 := \forall x\, \exists v \big(r(x,v) \to x = w\big) \vee (u = u) & FV(\varphi_5) = \{u,w\} & BV(\varphi_5) = \{x,v\}
\end{array}$$

It is often more convenient to speak of *free and bound occurrences* of a variable. In particular, for φ_4 as compared to φ_3, there are 2 additional occurrences of the symbol "u", both of which are free. The first 3 occurences of u in both cases are bound. The last two occurrences of u in φ_4 are free occurrences.

It is also conventional to say in φ_2 that the 2 occurrences of the symbol v are bound, in φ_3 the 3 occurrences of u are bound, etc.

Finally, note that φ_4 and φ_5 both have the same intended meaning. In fact, it is always possible and often convenient, to change the bound variables without changing any intended meaning. In this way one can ensure that no variable symbol in a formula has both free and bound occurrences.

1.3.16 Sentences

A *sentence* is a formula with no free variables.

So a sentence is always true or false in a structure, and this is independent of any assignment of values to variables.

1.3.17 Notation Regarding Free Variables

The expression $t(x_1, \ldots, x_n)$ is often used to denote a term t whose variables are a subset of $\{x_1, \ldots, x_n\}$.

But sometimes we will instead write, for example $t(v)$ or $t(u, v)$ etc., to denote a term t where u is *only one* of its free variables, or u and v are *only two* of its free variables, etc.

This will be convenient when we make substitutions. For example, if in the term $t(u)$ we replace all variables u by w, we might write $t(w)$ for the new term. It would be understood from context in this case that the free occurrences of u in t have been replaced throughout by w.

Similarly as for terms, the expression $\varphi(x_1, \ldots, x_n)$ denotes a formula φ whose *free* variables are a subset of $\{x_1, \ldots, x_n\}$.

Sometimes we write $\varphi(u)$ to draw attention to the fact that u is a free variable of φ, although there may also be other free variables in φ. This is again convenient if we wish to replace a free occurrence of u by another variable v or constant symbol c, in which case we write $\varphi(v)$ or $\varphi(c)$ respectively. If there is any danger of ambiguity I will be careful to explain what is intended.

1.3.18 Expansion of a Language

Sometimes we are interested in passing from a language $\mathcal{L}$ to a larger language $\mathcal{L}' \supseteq \mathcal{L}$. We say $\mathcal{L}'$ is an *expansion* of $\mathcal{L}$ and $\mathcal{L}$ is a *reduction* of $\mathcal{L}'$.

We will be particularly interested in the case where $\mathcal{L}' \setminus \mathcal{L}$ consists of new constant symbols, typically an infinite set of constant symbols, corresponding to a name for each element of some $\mathcal{L}$-structure. See the proof of Theorem 3.18.

1.4 Semantics

1.4.1 On Defining Truth in a Structure

The notion of truth of a sentence in a structure, and more generally of satisfaction of a formula for some assignment of values to its free variables, both of which are defined in this section, are *semantic* notions.

Unless mentioned otherwise, we consider a <u>*fixed*</u> *language $\mathcal{L}$. All formulas, sentences, and structures are for $\mathcal{L}$.*

Suppose φ is a *sentence*, and $\mathfrak{A}$ a structure for $\mathcal{L}$. In order to define

$$\mathfrak{A} \models \varphi, \tag{1.8}$$

which we read as "φ is true in $\mathfrak{A}$" or "$\mathfrak{A}$ satisfies φ", we need to more generally consider *formulas* with free variables.

The definition of $\mathfrak{A} \models \varphi$ proceeds by an induction on the complexity of φ. For example, to decide whether $\mathfrak{A} \models \forall v\, \varphi(v)$ we need to consider the truth value of $\varphi(v)$ in $\mathfrak{A}$ for *all* assignments of members of A (the universe of $\mathfrak{A}$) to the variable v.

The precise notion of *truth* as defined here is due to Tarski (Tarski, 1931; 1944). While it may appear relatively natural now, as Tarski remarks there are considerable difficulties in constructing *a materially adequate and formally correct definition of the term 'true sentence'*.

1.4.2 Interpretation of a Term in a Structure

Definition 1.13 (Variable Assignment). A *variable assignment* σ from the set of variables $\mathcal{V} = \{v_0, v_1, \ldots, v_n, \ldots\}$ into the structure $\mathfrak{A}$ is a function

$$\sigma : \mathcal{V} \to A, \tag{1.9}$$

mapping $\mathcal{V}$ into the universe A of $\mathfrak{A}$.

The value/interpretation of a term t under an assignment σ is defined in the natural way using the complexity of t.

Definition 1.14 (Interpretation of a Term). Let t be a term and let σ be a variable assignment into $\mathfrak{A}$. Then the interpretation $t^{\mathfrak{A}}[\sigma]$ of t in $\mathfrak{A}$ under the assignment σ is defined by induction on the complexity of t as follows:

(i) if t is a variable x, then $t^{\mathfrak{A}}[\sigma] = \sigma(x)$,

(ii) if t is a constant symbol c, then $t^{\mathfrak{A}}[\sigma] = c^{\mathfrak{A}}$,

(iii) if t is a term $f(t_1, \ldots, t_m)$, then

$$t^{\mathfrak{A}}[\sigma] = f^{\mathfrak{A}}\Big(t_1^{\mathfrak{A}}[\sigma], \ldots, t_m^{\mathfrak{A}}[\sigma]\Big).$$

Remark 1.15 *(Which assignment values matter?).* If $t = t(x_1, \ldots, x_n)$[10] is a term all of whose variables are in the set $\{x_1, \ldots, x_n\}$, then $t^{\mathfrak{A}}[\sigma]$ depends *only* on the values $\sigma(x_1), \ldots, \sigma(x_n)$ and *not* on $\sigma(u)$ for any other variable u.

That is, if $\sigma, \sigma' : \mathcal{V} \to A$ and $\sigma(x_i) = \sigma'(x_i)$ for $i = 1, \ldots, n$, then $t^{\mathfrak{A}}[\sigma] = t^{\mathfrak{A}}[\sigma']$.

If $\sigma(x_i) = a_i$ for $i = 1, \ldots, n$, then one often writes

$$t^{\mathfrak{A}}[a_1, \ldots, a_n] \quad \text{or} \quad t[a_1, \ldots, a_n] \tag{1.10}$$

for $t^{\mathfrak{A}}[\sigma]$, where the fact $x_i \mapsto a_i$ is understood from context, and where $\mathfrak{A}$ is also understood from context in the second case. □

Exercise 1.16. The proof that $t^{\mathfrak{A}}[\sigma] = t^{\mathfrak{A}}[\sigma']$ in the previous Remark is a simple induction on the complexity of t. Write out the proof in a succinct manner. □

Exercise 1.17. Is the "=" in the statement $t^{\mathfrak{A}}[\sigma] = t^{\mathfrak{A}}[\sigma']$ a symbol in the language $\mathcal{L}$ or a symbol in the metalanguage? Explain. □

[10] Once again, the "=" here is a symbol in the metalanguage, not in the formal language $\mathcal{L}$. The statement $t = t(x_1, \ldots, x_n)$ is a shorthand way of saying that the variables occurring in t belong to the set $\{x_1, \ldots, x_n\}$.

1.4.3 Satisfaction of a Formula in a Structure

Let $\varphi = \varphi(x_1, \ldots, x_n)$ be a formula of $\mathcal{L}$, where the set $\{x_1, \ldots, x_n\}$ contains all free variables from φ.

Let $\sigma : \mathcal{V} \to A$ be a variable assignment into the universe A of the $\mathcal{L}$-structure $\mathfrak{A}$, where $\sigma(x_i) = a_i$ for $i = 1, \ldots, n$. In Definition 1.18 we will define

$$\mathfrak{A} \vDash \varphi[\sigma] \quad \text{or equivalently} \quad \mathfrak{A} \vDash \varphi[a_1, \ldots, a_n], \tag{1.11}$$

so that it agrees with the informal idea that $\varphi(x_1, \ldots, x_n)$ is true in $\mathfrak{A}$ if each variable $x_i \in \mathcal{V}$ is interpreted as $a_i \in A$.

We read (1.11) as

$\mathfrak{A}$ *satisfies* φ *at (the assignment)* σ, or
$\mathfrak{A}$ *satisfies* φ *at* $(a_1, \ldots, a_n)$, or
something similar.

If two assignments $\sigma, \sigma' : \mathcal{V} \to A$ agree on all free variables in φ then it will follow from Definition 1.18 that

$$\mathfrak{A} \vDash \varphi[\sigma] \iff \mathfrak{A} \vDash \varphi[\sigma'] \tag{1.12}$$

This justifies the use of the notation $\mathfrak{A} \vDash \varphi[a_1, \ldots, a_n]$ in (1.11).

If φ is a sentence and so φ has no free variables, then from (1.12) the truth or falsity of $\mathfrak{A} \vDash \varphi[\sigma]$ is independent of the choice of assignment σ, and so we can simply write this as $\mathfrak{A} \vDash \varphi$.

We now give the formal definition of $\mathfrak{A} \vDash \varphi[\sigma]$ by induction on the complexity of φ. At each stage we will obtain either that $\mathfrak{A} \vDash \varphi[\sigma]$ is true or otherwise that $\mathfrak{A} \vDash \varphi[\sigma]$ is false. In the second case we write $\mathfrak{A} \nvDash \varphi[\sigma]$ and read it as "$\mathfrak{A}$ does not satisfy φ at (the assignment) σ".

In the following we are, as usual, taking $\neg, \wedge, \forall$ as the primitive logical symbols for the language $\mathcal{L}$.

Definition 1.18 (Satisfaction). Let $\mathfrak{A}$ be an $\mathcal{L}$-structure. We define for every variable assignment σ, by induction on the complexity of a formula φ, the relation $\mathfrak{A} \vDash \varphi[\sigma]$.

(i) $\mathfrak{A} \vDash (t_1 = t_2)[\sigma]$ iff $t_1^{\mathfrak{A}}[\sigma] = t_2^{\mathfrak{A}}[\sigma]$,[11]

(ii) $\mathfrak{A} \vDash r(t_1, \ldots, t_m)[\sigma]$ iff $(t_1^{\mathfrak{A}}[\sigma], \ldots, t_m^{\mathfrak{A}}[\sigma]) \in r^{\mathfrak{A}}$,

(iii) $\mathfrak{A} \vDash (\neg\varphi)[\sigma]$ iff $\mathfrak{A} \nvDash \varphi[\sigma]$,

(iv) $\mathfrak{A} \vDash (\varphi_1 \wedge \varphi_2)[\sigma]$ iff $\mathfrak{A} \vDash \varphi_1[\sigma]$ and $\mathfrak{A} \vDash \varphi_2[\sigma]$,

(v) $\mathfrak{A} \vDash \forall x\, \varphi[\sigma]$ iff $\mathfrak{A} \vDash \varphi[\sigma']$ for *all* σ' such that $\sigma(u) = \sigma'(u)$ whenever $u \neq x$. □

Remark 1.19 *(Universal Validity).*
If $\varphi = \varphi(x_1, \ldots, x_n)$ *is a formula, then by* $\mathfrak{A} \vDash \varphi$ *we mean that* $\mathfrak{A} \vDash \varphi[\sigma]$ *for* all *assignments* $\sigma : \mathcal{V} \to A$.

[11] This is yet another example of using notation, here "=", both in the formal language as in $t_1 = t_2$, and in the metalanguage as in $t_1^{\mathfrak{A}}[\sigma] = t_2^{\mathfrak{A}}[\sigma]$.

This is equivalent to $\mathfrak{A} \models \forall x_1 \ldots \forall x_n\, \varphi$. We say φ *is true/valid in* $\mathfrak{A}$.

We call $\forall x_1 \ldots \forall x_n\, \varphi$ the *universal closure* of φ. There is some ambiguity, depending on the order of the x_i, but it makes no difference to whether or not $\mathfrak{A} \models \forall x_1 \ldots \forall x_n\, \varphi$.

If $\mathfrak{A} \models \varphi[\sigma]$ for all $\mathfrak{A}$ and all σ, we say the formula φ is *universally valid.* □

Exercise 1.20. Explain why "…the order of the x_i …makes no difference to whether or not $\mathfrak{A} \models \forall x_1 \ldots \forall x_n\, \varphi$". □

Remark 1.21 *(Which assignment values matter?).* It is a straightforward induction, based on the complexity of φ, to show that the truth value of $\mathfrak{A} \models \varphi[\sigma]$ depends only on the assignments $\sigma(x_i)$ for the *free* variables $x_1, \ldots, x_n$ in φ. □

Exercise 1.22. Do this for (iii) and (v). (Assume we already know the result for the relevant subformulas.) □

Remark 1.23 *(Universal quantifiers).* Implicitly or explicitly inserting universal quantifiers is common mathematical practice. For example, we might write

$$u = v \to v = u,$$

where it is clear from the context that this is intended to apply to all interpretations of u and v in the relevant structures. □

1.4.4 Defined Logical Symbols

We took $\neg, \wedge, \forall$ as primitive and defined $\vee, \to, \leftrightarrow, \exists$ from them, see Section 1.3.5. It follows from Definition 1.6 that:

(vi) $\mathfrak{A} \models (\varphi_1 \vee \varphi_2)\,[\sigma]$ iff $\mathfrak{A} \models \varphi_1[\sigma]$ or $\mathfrak{A} \models \varphi_2[\sigma]$,

(vii) $\mathfrak{A} \models (\varphi_1 \to \varphi_2)\,[\sigma]$ iff $\mathfrak{A} \models \varphi_2[\sigma]$ whenever $\mathfrak{A} \models \varphi_1[\sigma]$,

(viii) $\mathfrak{A} \models (\varphi_1 \leftrightarrow \varphi_2)\,[\sigma]$ iff $\mathfrak{A} \models \varphi_2[\sigma]$ whenever $\mathfrak{A} \models \varphi_1[\sigma]$, and conversely,

(ix) $\mathfrak{A} \models \exists x\, \varphi[\sigma]$ iff $\mathfrak{A} \models \varphi[\sigma']$ for *some* σ' such that $\sigma(u) = \sigma'(u)$ whenever $u \neq x$.

Exercise 1.24. Prove (vii) and (ix) from Definition 1.6. □

1.4.5 Semantic Entailment

In the following you might think of Σ as being the axioms for a group[12] or for a field.

Definition 1.25 (Semantic Entailment). Suppose Σ is a set of formulas (possibly infinite) and φ is a formula from a language $\mathcal{L}$. Then

$$\Sigma \models \varphi \tag{1.13}$$

[12] Almost all interesting results in group theory are not expressible in the first-order logic corresponding to the language of group theory. But they *are* expressible and provable in Zermelo Fraenkel set theory, which in turn *is* a first-order theory.

if for every $\mathcal{L}$-structure, $\mathfrak{A} \models \Sigma \Longrightarrow \mathfrak{A} \models \varphi$.

Equivalently, by Definition 1.18, if $\mathfrak{A} \models \Sigma' \Longrightarrow \mathfrak{A} \models \varphi'$, where Σ' and φ' are the universal closures of the formulas in Σ, and of φ respectively.

We say Σ *semantically entails* or *logically implies* or *logically entails* φ.

If $\Sigma = \varnothing$ we write $\varnothing \models \varphi$ or $\models \varphi$, and say φ is *logically valid.* □

Remark 1.26 *(Semantic Deduction "Theorem").* For a set of sentences Σ, and for sentences φ and ψ,

$$\Sigma \models \varphi \quad \text{iff} \quad \Sigma \cup \{\neg\varphi\} \text{ has no models.} \tag{1.14}$$

Moreover,

$$\Sigma, \psi \models \varphi \quad \text{iff} \quad \Sigma \models \psi \to \varphi. \tag{1.15}$$

The analogous, deeper *Syntactic Deduction Theorem*, is Theorem 2.32.

Moreover, in analogy with the Syntactic Deduction Theorem, in (1.14) we can allow Σ and φ to be a set of formulas, and a formula, respectively. But ψ should be a sentence. □

Exercise 1.27. Justify (1.14). □

Exercise 1.28. Justify (1.15). □

1.4.6 Examples for Validity

Useful examples of logical validity and non-validity, are the following:

(i) $\models \forall v(\varphi \to \psi) \leftrightarrow (\varphi \to \forall v\, \psi)$, $\quad v$ not free in φ,

(ii) $\models \exists v(\varphi \to \psi) \leftrightarrow (\varphi \to \exists v\, \psi)$, $\quad v$ not free in φ,

(iii) $\models \forall v(\varphi \to \psi) \leftrightarrow (\exists v\, \varphi \to \psi)$, $\quad v$ not free in ψ,

(iv) $\models \exists v(\varphi \to \psi) \leftrightarrow (\forall v\, \varphi \to \psi)$, $\quad v$ not free in ψ,

(v) $\models \exists u\, \forall v\, \varphi(u, v) \to \forall v\, \exists u\, \varphi(u, v)$,

(vi) $\not\models \forall v\, \exists u\, \varphi(u, v) \to \exists u\, \forall v\, \varphi(u, v)$. □

Exercise 1.29. Give an argument to establish this in cases (iv), (v) and (vi). □

1.5 Other Material?

Chapter 2

Hilbert's Deductive System

The notions of *axioms, rules of inference and formal proof* discussed in this chapter, are *syntactic*. The notions of satisfaction and truth in a structure are *semantic*.

The axioms, the rules and the definition of proof were designed in such a way that it was hoped, and was later shown to be true, that $\Sigma \vDash \varphi$ if and only if $\Sigma \vdash \varphi$. See Chapter 3.

The deductive system we use here is one of many *Hilbert*-system variants. It is mathematically simple in that proofs are linear (rather than tree-like) and so well adapted to coding as sequences of natural numbers. See Chapter 5.

But from the perspective of computer science and proof theoretic studies the approach (using tree structues) due to Gentzen and others, in particular *natural deduction* and the *sequent calculus*, are much more useful.

2.1 Axioms

As usual, unless stated otherwise we work in a fixed language $\mathcal{L}$.

2.1.1 Preliminaries

Remark 2.1 *(Propositional Logic).* If you know a little about propositional logic, truth tables and tautologies, keep reading. If not, read and understand Subsections 6.1.1–6.1.6. □

Remark 2.2 *(Logical Axioms).* The *logical axioms* for first-order logic are divided into three groups. The propositional axioms, the quantifier axioms and the equality axioms.

If an instance of an axiom has free variables then *the axiom should be true for all interpretations of the free variables in the structure.* Equivalently, it means the same as its universal generalisation obtained by universally quantifying over all its free variables.

For example, if we take $u = v \to v = u$ as an axiom then we intend this to mean $\forall u\, \forall v\, (u = v \to v = u)$.

The intention is that the axioms should be true in every $\mathcal{L}$-structure for all assignments, and that the rules of inference should preserve truth. □

2.1.2 Propositional Axioms

Definition 2.3 (Propositional Axioms).

Suppose φ is a formula of $\mathcal{L}$ obtained from a *propositional tautology* ψ (see Definition 6.6), by substituting simultaneously and uniformly, formulas of $\mathcal{L}$ for the propositional symbols in ψ.

Then φ is a *propositional axiom* for first-order logic.

Remark 2.4 *(Examples).* In particular, $\varphi(v) \vee \neg\varphi(v)$ is a propositional axiom.

But $\forall v\,(\varphi(v) \vee \neg\varphi(v))$ is not a propositional axiom. However, it is immediately deducible by Universal Generalisation, see (2.7).

(Remember that in first-order logic, if a deduction gives a formula with free variables then the variables can be interpreted as being any element in the relevant structures.)

Remark 2.5 *(Possible Axiom Variations).* We could just take as propositional axioms the substitution instances of the three axioms for propositional logic in Section 6.2, rather than substitution instances for *all* tautologies.

However, for our purposes there is no need to be restrictive in this manner. The significant point is that truth tables provide an algorithmic procedure for determining if a formula in propositional logic is indeed a tautology. This can then be used to decide if a formula of $\mathcal{L}$ is a propositional axiom. □

2.1.3 Quantifier Axioms

Definition 2.6 (Quantifier Axioms).

1. Suppose φ and ψ are formulas of $\mathcal{L}$ and v *is a variable not free in* φ.

   Then
   $$\forall v(\varphi \to \psi) \to (\varphi \to \forall v\,\psi) \tag{2.1}$$
   is a *quantifier axiom*, sometimes called *distribution of* $\forall$ *over implication* (under the "variable not free" side condition on φ).

2. Suppose φ (written $\varphi(v)$ here, but it may have other free variables) is a formula of $\mathcal{L}$. Suppose $\varphi(t)$ is obtained from φ by substituting the term t for each *free occurrence* of v in φ, and that *no variable of t occurs bound in φ at the places where it is substituted.*[1]

   Then
   $$\forall v\,\varphi(v) \to \varphi(t) \tag{2.2}$$
   is the axiom of *universal instantiation* or of *specialisation.*

Remark 2.7 *(Restrictions on Quantifier Axioms).* These restrictions are necessary.

(a) For example, in (2.1) suppose φ and ψ are the same formula $s(v)$, where s is a unary relation symbol in the language $\mathcal{L}$.

Then
$$\forall v\,\big(s(v) \to s(v)\big) \to \big(s(v) \to \forall v\,s(v)\big)$$
cannot be an axiom as it is not logically valid.

This is so since
$$\mathfrak{A} \vDash \forall v\,\big(s(v) \to s(v)\big)$$

[1] This is often expressed as "t is substitutable for v in φ" or "*t is free for v in φ*".

for every $\mathcal{L}$-structure $\mathfrak{A}$. But it is *not* the case in general that

$$\mathfrak{A} \models \; s(v) \to \forall v \, s(v),$$

since the *free* occurrence of v could be assigned to some $a \in A$ such that $\mathfrak{A} \models s[a]$, while $\mathfrak{A} \not\models \forall v \, s(v)$.

(b) In (2.2) suppose φ (i.e. $\varphi(v)$) is the formula $\exists u \, r(u, v)$, where r is a binary relation symbol in the language $\mathcal{L}$..

Suppose the term t is the variable u. Then $\varphi(t)$ is $\exists u \, r(u, u)$ and (2.2) becomes

$$\forall v \, \exists u \, r(u, v) \to \exists u \, r(u, u),$$

which is *not* true in some $\mathcal{L}$-structures.

The problem is that the term t contains (and indeed is) the variable u, which become bound when substituted for v in φ.

(c) Note that in (2.2) it *is* acceptable that the term t is identical to v. So in particular, $\forall v \, \varphi \to \varphi$ (i.e. $\forall v \, \varphi(v) \to \varphi(v)$) is an axiom.

In particular, taking the example from (b) where $\varphi(v)$ is the formula $\exists u \, r(u, v)$, but now taking t to be the variable v, we get the formula

$$\forall v \, \exists u \, r(u, v) \to \exists u \, r(u, v).$$

This *is* true in all $\mathcal{L}$-structures, for all assignments of a value to the *free* occurrence of v. *Why?* □

2.1.4 Equality Axioms

Definition 2.8 (Equality Axioms).

1. Suppose u, v, w are variables. Then

$$\begin{gathered} u = u, \\ u = v \to v = u, \\ (u = v \wedge v = w) \to u = w, \end{gathered} \tag{2.3}$$

   are *equality axioms.*

2. Suppose $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ are variables and f is an n-ary function symbol. Then

$$\Big(u_1 = v_1 \wedge \cdots \wedge u_n = v_n\Big) \;\to\; f(u_1, \ldots, u_n) = f(v_1, \ldots, v_n) \tag{2.4}$$

   is an *equality axiom.*

3. Suppose $u_1, \ldots, u_n$ and $v_1, \ldots, v_n$ are variables and r is an n-ary relation symbol. Then

$$\Big(u_1 = v_1 \wedge \cdots \wedge u_n = v_n\Big) \;\to\; \Big(r(u_1, \ldots, u_n) \to r(v_1, \ldots, v_n)\Big) \tag{2.5}$$

   is an *equality axiom.*

Remark 2.9 *(Equality Axioms and the Interpretation of "=").* Axioms (2.3) ensure that *if* "=" is interpreted in a structure $\mathfrak{A} = \langle A, \dots \rangle$ just as a binary relation "$\sim$", then "$\sim$" is an equivalence relation.

Axioms (2.4) and (2.5) then ensure that the interpretations of the function and relation symbols in $\mathfrak{A}$ respect the equivalence classes corresponding to "$\sim$".

However, *we will require* that an $\mathcal{L}$-structure $\mathfrak{A}$ interprets "=" to mean "is the same element as". In other words, "=" is interpreted as equality in the standard sense, not just as an equivalence relation.

In particular, "=" is treated in a special manner, differently from any other binary relation. □

2.1.5 Universal Validity

Recall that an $\mathcal{L}$-formula φ is universally valid if $\mathfrak{A} \models \varphi[\sigma]$ for all $\mathcal{L}$-structures $\mathfrak{A}$ and all assignments $\sigma : \mathcal{V} \to A$. See Remark 1.19.

Theorem 2.10 (Universal Validity of the Logical Axioms). *The logical axioms are universally valid.*

Proof. Let $\mathfrak{A}$ be an $\mathcal{L}$-structure and $\sigma : \mathcal{V} \to A$ be an assignment of variables into the universe of $\mathfrak{A}$.

Suppose ψ is a propositional axiom, say $\theta \to (\chi \to \theta)$. This corresponds to a tautology in Propositional Logic and so is true in $\mathfrak{A}$ regardless of the truth or falsity of $\mathfrak{A} \models \theta[\sigma]$ and $\mathfrak{A} \models \chi[\sigma]$. Similarly for any propositional axiom.

Next suppose ψ is the quantifier axiom $\forall v(\theta \to \chi) \to (\theta \to \forall v\, \chi)$ where v is not free in θ.

We need to show[2] that $\mathfrak{A} \models \forall v(\theta \to \chi) \to (\theta \to \forall v\, \chi)[\sigma]$. $(*)$

For this we can assume $\mathfrak{A} \models \forall v(\theta \to \chi)[\sigma]$.

Then $\mathfrak{A} \models (\theta \to \chi)[\sigma']$ for every σ' agreeing with σ except possibly at v. $(**)$

We now have to prove $\mathfrak{A} \models (\theta \to \forall v\, \chi)[\sigma]$. For this we can assume $\mathfrak{A} \models \theta[\sigma]$.

But since v is not free in θ, it follows $\mathfrak{A} \models \theta[\sigma']$ for every σ' agreeing with σ except possibly at v.

From $(**)$ it now follows $\mathfrak{A} \models \chi[\sigma']$ for all such σ' and so $\mathfrak{A} \models \forall v\, \chi[\sigma]$.

So we have proved $\mathfrak{A} \models (\theta \to \forall v\, \chi)[\sigma]$. This was under the assumption that $\mathfrak{A} \models \forall v(\theta \to \chi)[\sigma]$. So we have proved $(*)$.

We next need to show $\mathfrak{A} \models \forall v\, \theta(v) \to \theta(t)\, [\sigma]$, where $\theta(t)$ is obtained from θ by substituting the term t for each free occurrence of v in θ, and no variable of t occurs bound in θ at the places where it is substituted.

For this we can assume $\mathfrak{A} \models \forall v\, \theta(v)\, [\sigma]$, and so $\mathfrak{A} \models \theta(v)\, [\sigma']$ for every σ' agreeing with σ except possibly at v. $(***)$

We need to show that $\mathfrak{A} \models \theta(t)[\sigma]$

But the conditions on t in $\theta(t)$ ensure that if $\sigma'(v) = t^{\mathfrak{A}}[\sigma]$ but otherwise σ' agrees with σ, then $\mathfrak{A} \models \theta(v)[\sigma']$ implies $\mathfrak{A} \models \theta(t)[\sigma]$.

From $(***)$ it follows that $\mathfrak{A} \models \theta(t)[\sigma]$. Hence $\mathfrak{A} \models \forall v\, \theta(v) \to \theta(t)\, [\sigma]$.

[2] The argument here, and for the next quantifier axiom, is not much more that a small formalisation of what I hope is your intuitive understanding of why the axiom is universally valid. The formal argument tends to obscure this fact.

The equality axioms are similarly true in any $\mathfrak{A}$ for any assignment to the (free) variables. I leave this for you to think about in the next Exercise 2.11.

□

Exercise 2.11. Explain why the equality axioms are universally valid. □

2.2 Rules of Inference

There are two rules of inference in this version of a Hilbert system.

2.2.1 Modus Ponens

Definition 2.12 (Modus Ponens). Suppose φ and ψ are formulas of $\mathcal{L}$, then

$$\text{from} \quad \varphi \quad \text{and} \quad \varphi \to \psi \quad \text{infer} \quad \psi. \tag{2.6}$$

Remark 2.13 *(Etymology).* From the Latin *modus ponendo ponens* – "method that by affirming affirms". Goes back to the ancient Greeks, perhaps Theophrastus (371–287 BC). □

Remark 2.14 *(Usage).* For example, one often establishes φ and then immediately claims ψ on the basis $\varphi \to \psi$ is a propositional axiom. □

2.2.2 Generalisation

Definition 2.15 (Generalisation). Suppose φ is a formula of $\mathcal{L}$, then

$$\text{from} \quad \varphi \quad \text{infer} \quad \forall v\, \varphi. \tag{2.7}$$

Remark 2.16 *(Universal Quantifiers).* A consequence of the Generalisation Rule is that we can put universal quantifiers in front of the propositional and identity axioms.

This accords with how we should think of free variables in the axioms — the axioms should hold in any structure independently of how the free variables are interpreted.

It also accords with standard mathematical practice: if we can prove a result $\varphi(v)$ about a variable v without any particular assumptions on v, we can deduce $\forall v\, \varphi(v)$. □

2.2.3 Preserving Validity

In the following, remember that $\mathfrak{A} \models \varphi$ means $\mathfrak{A} \models \varphi\,[\sigma]$ for every assignment $\sigma : \mathcal{V} \to A$, where A is the universe of $\mathfrak{A}$.

Theorem 2.17 (Inference Preserves Validity). *The two rules of inference preserve validity in the following sense:*

(i) if $\mathfrak{A} \models \varphi$ and $\mathfrak{A} \models \varphi \to \psi$ then $\mathfrak{A} \models \psi$,

(ii) if $\mathfrak{A} \models \varphi$ then $\mathfrak{A} \models \forall v\, \varphi$.

Proof. Suppose $\mathfrak{A} \models \varphi$ and $\mathfrak{A} \models \varphi \to \psi$. Then for each assignment σ, $\mathfrak{A} \models \varphi\,[\sigma]$ and $\mathfrak{A} \models \varphi \to \psi\,[\sigma]$. From Section 1.4.4(vii) and Exercise 1.24, $\mathfrak{A} \models \psi\,[\sigma]$. Since σ was arbitrary, $\mathfrak{A} \models \psi$. This proves (i).

Suppose $\mathfrak{A} \models \varphi$. Then for every $\sigma : \mathcal{V} \to A$, $\mathfrak{A} \models \varphi\,[\sigma]$. Since $\mathfrak{A} \models \forall v\, \varphi\,[\sigma]$ iff $\mathfrak{A} \models \varphi\,[\sigma']$ for all those σ' which agree with σ except on the variable v, it follows that $\mathfrak{A} \models \forall v\, \varphi\,[\sigma]$. This proves (ii). □

2.3 Syntactic Entailment

2.3.1 Derivations

Definition 2.18 (Derivation / Formal Proof). Suppose φ is a *formula* and Σ is a set of formulas in the language $\mathcal{L}$.

A *deduction/derivation/(formal) proof of φ from Σ*, or alternatively a Σ*-derivation of* φ, is a finite sequence $\varphi_1, \ldots, \varphi_n$ of *formulas* such that $\varphi_n = \varphi$ and such that each φ_i is a logical axiom or a member of Σ, or deducible from earlier φ_j's by means of one of the rules of inference. □

Definition 2.19 (Syntactic Entailment). Suppose Σ is a set of formulas (possibly infinite) and φ is a formula from the language $\mathcal{L}$. Then

$$\Sigma \vdash \varphi \tag{2.8}$$

means there is a formal proof from Σ to φ. We say Σ *syntactically entails/implies* φ.

If Σ is the empty set we write $\varnothing \vdash \varphi$ or $\vdash \varphi$, and say φ is a *logical theorem.* □

Exercise 2.20. Show $\Sigma \vdash \varphi \iff \Sigma \vdash \forall v\, \varphi$.

More generally, show that $\Sigma \vdash \varphi(v_1, \ldots, v_n) \iff \Sigma \vdash \forall v_1, \ldots, \forall v_n\, \varphi(v_1, \ldots, v_n)$.

(One direction uses repeated applications of (2.2). The other uses repeated applications of the rule for generalisation (2.7).) □

Remark 2.21 *(Finite Nature of Proofs).* Since derivations are finite, it is an important immediate consequence that $\Sigma \vdash \varphi$ iff $\Sigma_0 \vdash \varphi$ for some *finite* $\Sigma_0 \subseteq \Sigma$. □

Remark 2.22 *(Why these Axioms and Inference Rules?).* As noted previously, we are working within a Hilbert-style system.

Of course, the axioms should be true in any $\mathcal{L}$-structure under any assignment for the free variables, and the inference rules should preserve truth. This is so, and it is the main content of the *Soundness Theorem* 2.25. □

Exercise 2.23. For each axiom try to convince yourself that it is indeed the case that the axiom is true in every $\mathcal{L}$-structure under every assignment for the free variables, and the inference rules preserve this truth.

The proof of the Soundness Theorem 2.25 writes out the details. □

Remark 2.24. Just about every text has its own variant of the axioms and rules. The main point is that the axioms and rules should be sufficient to establish all other "valid" logical formulas. This requires that they should be sufficient to prove Gödel's *Completeness Theorem.* And this is what we will show in Section 3.4.

Showing that the Hilbert System is equivalent to any other standard system is not relatively difficult. In this way one has completeness for any reasonable first-order logic system. □

2.3.2 Soundness Theorem

Theorem 2.25 (Soundness Theorem). *If Σ is a set of formulas and φ is a formula (all in the same language $\mathcal{L}$), then $\Sigma \vdash \varphi$ implies $\Sigma \vDash \varphi$.*

Proof. Assume $\Sigma \vdash \varphi$ and $\varphi_1, \ldots, \varphi_{n-1}, \varphi_n (= \varphi)$ is a corresponding derivation.

To prove that $\Sigma \models \varphi$ we need to show that if $\mathfrak{A} \models \Sigma$ then $\mathfrak{A} \models \varphi$.
So assume $\mathfrak{A} \models \Sigma$.
We will show by induction on i that $\mathfrak{A} \models \varphi_i$ for $i = 1, \ldots, n$.

Since φ_1 is either a logical axiom or $\varphi_1 \in \Sigma$, it follows that $\mathfrak{A} \models \varphi_1$.

Suppose $i > 1$ and $\mathfrak{A} \models \varphi_j$ for all $j < i$.
If φ_i is a logical axiom or $\varphi_i \in \Sigma$, then as for φ_1, $\mathfrak{A} \models \varphi_i$.
If φ_i is obtained from previous φ_js by modus ponens or generalisation, then $\mathfrak{A} \models \varphi_i$ by Theorem 2.17.

It follows by induction that $\Sigma \models \varphi_n$, that is $\Sigma \models \varphi$. □

2.4 Properties of Derivations

We discuss just a few techniques for constructing formal derivations/proofs from the Hilbert axioms, with an emphasis on what is needed for the proof of Gödel's Completeness Theorem 3.12.

Once we have the Completeness Theorem (and the Soundness Theorem), it is usually easier to check $\Sigma \models \varphi$ than $\Sigma \vdash \varphi$. But of course, this is not a constructive argument for showing $\Sigma \vdash \varphi$.

Formal derivations of Hilbert type are discussed in great detail in various logic texts. See (Enderton, 2001; Hils and Loeser, 2019; Johnstone, 1987; Mendelson, 2015)

Contemporary developments of proof theory concentrate on different axiomatic systems, natural deduction and sequent calculus in particular.

2.4.1 An Equivalence Relation on Constant Symbols

With an eye to what will be needed in Step 4 of the proof of Gödel's Completeness Theorem 3.12, let $\mathcal{C}$ be the set of constant symbols (or some subset thereof) in the language $\mathcal{L}$. Let Σ be a set of sentences in $\mathcal{L}$. For $c_1, c_2 \in \mathcal{C}$ define

$$c_1 \sim c_2 \quad \Longleftrightarrow \quad \Sigma \vdash c_1 = c_2. \tag{2.9}$$

The formal deduction proving *reflexivity*, $c \sim c$, is

$u = u$	Equality axioms (2.3)
$\forall u\,(u = u)$	Generalisation (2.7)
$\forall u\,(u = u) \to c = c$	Quantifier axiom (2.2)
$c = c$	Modus Ponens (2.6)

Hence $\vdash c = c$, and in particular $\Sigma \vdash c = c$, and so $c \sim c$.

To show *symmetry*, $c \sim d \Rightarrow d \sim c$, suppose $c \sim d$. Then by definition $\Sigma \vdash c = d$.

Extend such a derivation to a derivation of $\Sigma \vdash d = c$ by *concatenating* at its end the following:

$u = v \to v = u$	Equality axioms (2.3)
$\forall u \forall v\,(u = v \to v = u)$	Generalisation (2.7), twice
$(c = d \to d = c)$	Quantifier axiom (2.2), twice
$d = c$	Modus Ponens (2.6) and using $\Sigma \vdash c = d$

Hence $\Sigma \vdash d = c$, and so $d \sim c$.

Exercise 2.26. So far we have seen that $\sim$ is reflexive and symmetric. The proof of *transivity*, that $(c \sim d \;\&\; d \sim e) \Longrightarrow c \sim e$, follows a similar pattern. Do it.

2.4.2 Existential Generalisation

The conditions on φ in the following are exactly as for universal instantiation, see (2.2).

Proposition 2.27. *(Existential Generalisation) Suppose $\varphi(v)$ is a formula of $\mathcal{L}$, $\varphi(t)$ is obtained from φ by substituting t for each free occurrence of v in φ, and no variable of t occurs bound in φ at the places where it is substituted. Then*

$$\vdash \varphi(t) \rightarrow \exists v\, \varphi(v). \tag{2.10}$$

Proof. From the definition of "$\exists$" we need to establish

$$\vdash \varphi(t) \rightarrow \neg\forall v\, \neg\varphi(v).$$

As in Remark 2.14 it is sufficient[3] to show

$$\vdash \forall v\, \neg\varphi(v) \rightarrow \neg\varphi(t).$$

But this is an instance of universal instantiation, quantifier axiom (2.2). □

2.4.3 Deduction Theorem

Remark 2.28 *(Why is σ a Sentence in the Deduction Theorem 2.32).*

Suppose $\mathcal{L}$ has a single unary relation symbol U and σ is the *formula* $U(x)$.

Then $U(x) \vdash \forall x\, U(x)$, since "$U(x), \forall x\, U(x)$" is a deduction of $\forall x\, U(x)$ from $U(x)$ according to Definitions 2.18 and 2.19. But if the Deduction Theorem were true with σ replaced by $U(x)$, it would follow that $\vdash U(x) \rightarrow \forall x\, U(x)$, and so by Generalisation

$$\vdash \forall x\Big(U(x) \rightarrow \forall x\, U(x)\Big). \tag{2.11}$$

However this is not the case by the Soundness Theorem (see Remark 2.22 and Exercise 2.23), because $\nvDash \forall x\Big(U(x) \rightarrow \forall x\, U(x)\Big)$ and so $\nvdash \forall x\Big(U(x) \rightarrow \forall x\, U(x)\Big)$.

To see that $\nvDash \forall x\Big(U(x) \rightarrow \forall x\, U(x)\Big)$ consider an $\mathcal{L}$-structure $\mathfrak{A}$ with universe A, for which $a, b \in A$, $a \in U^{\mathfrak{A}}$ and $b \notin U^{\mathfrak{A}}$. Then $\mathfrak{A} \nvDash \forall x\Big(U(x) \rightarrow \forall x\, U(x)\Big)$ by the following Exercise. □

Exercise 2.29. Explain why $\mathfrak{A} \nvDash \forall x\Big(U(x) \rightarrow \forall x\, U(x)\Big)$. □

[3] In propositional logic $\vdash (P \rightarrow \neg Q) \rightarrow (Q \rightarrow \neg P)$.
So in first-order logic $\vdash \big(\forall v\, \neg\varphi(v) \rightarrow \neg\varphi(t)\big) \;\rightarrow\; \big(\varphi(t) \rightarrow \neg\forall v\, \neg\varphi(v)\big)$.

Remark 2.30 *(But what If σ is <u>Not</u> a Sentence?).*

For simplicity suppose $\sigma \vdash \tau$, so Σ is $\varnothing$.

One *can* obtain a version of $\vdash \sigma \to \tau$ *provided* one restricts the class of allowable further deductions. In particular, generalisation has to be restricted to prevent (2.11). See (Mendelson, 2015, pp 70–72) for a careful analysis

While this might allow cleaner legitimate deductions in the Hilbert system, that is not our goal. And if formal deductions were the goal, then one should really be using sequent calculus or natural deduction. □

Remark 2.31 *(Connection between $\to$, $\vdash$ and $\vDash$).*

We will show for sentences φ and ψ that

$$\vdash \varphi \to \psi \quad \Longleftrightarrow \quad \varphi \vdash \psi \quad \Longleftrightarrow \quad \varphi \vDash \psi \quad \Longleftrightarrow \quad \vDash \varphi \to \psi. \tag{2.12}$$

The first $\Longleftrightarrow$ is the Deduction Theorem 2.32, the third $\Longleftrightarrow$ is Remark 1.26. The middle $\Longleftrightarrow$ is the Gödel Completeness Theorem 3.12 in Chapter 3.

One can also add Σ to the left side of each $\vdash$ and $\vDash$, where Σ is a set of sentences. □

Theorem 2.32 (Deduction Theorem). *If Σ is a set of formulas, σ a <u>sentence</u>, and τ a formula, then*

$$\Sigma \cup \{\sigma\} \vdash \tau \quad \Longleftrightarrow \quad \Sigma \vdash \sigma \to \tau.$$

Proof For the (easy) "$\Longleftarrow$" direction suppose $\Sigma \vdash \sigma \to \tau$ and let $\varphi_1, \dots, \varphi_n, \sigma \to \tau$ be a corresponding derivation.

Then, using modus ponens, $\varphi_1, \dots \varphi_n, \sigma \to \tau, \sigma, \tau$ is a derivation for $\Sigma \cup \{\sigma\} \vdash \tau$.

For the "$\Longrightarrow$" direction suppose $\Sigma \cup \{\sigma\} \vdash \tau$ and let $\varphi_1, \dots, \varphi_n (= \tau)$ be a derivation. We show by induction on i that there is a derivation of $\Sigma \vdash \sigma \to \varphi_i$.

(i) If φ_i is an axiom or $\varphi_i \in \Sigma$, then $\varphi_i,\ \varphi_i \to (\sigma \to \varphi_i),\ \sigma \to \varphi_i$ is such a derivation. (See Exercise 2.33)

(ii) If $\varphi_i = \sigma$, then $\sigma \to \sigma$ is such a derivation ($\sigma \to \sigma$ is a tautology of $\mathcal{L}$).

(iii) If φ_i is deduced by modus ponens from φ_j and from $\varphi_k = \varphi_j \to \varphi_i$, $(j, k < i)$, let $\theta_1, \dots, \theta_n,\ \sigma \to \varphi_j$ be the derivation for $\Sigma \vdash \sigma \to \varphi_j$,
and $\theta'_1, \dots, \theta'_m,\ \sigma \to (\varphi_j \to \varphi_i)$ be the derivation for $\Sigma \vdash \sigma \to (\varphi_j \to \varphi_i)$.

Then the following is a derivation for $\Sigma \vdash \sigma \to \varphi_i$.

$$\begin{aligned}
&\theta_1, \dots, \theta_n,\ \sigma \to \varphi_j,\ \theta'_1, \dots, \theta'_m,\ \sigma \to (\varphi_j \to \varphi_i), \\
&\quad \big(\sigma \to (\varphi_j \to \varphi_i)\big) \to \big((\sigma \to \varphi_j) \to (\sigma \to \varphi_i)\big), && \text{(propositional axiom, Exercise 2.34)} \\
&\qquad (\sigma \to \varphi_j) \to (\sigma \to \varphi_i), && \text{(modus ponens)} \\
&\qquad\quad \sigma \to \varphi_i. && \text{(modus ponens)}
\end{aligned}$$

(iv) If φ_i is deduced from φ_j by generalisation, i.e. $\varphi_i = \forall v\, \varphi_j$, let $\theta_1, \dots, \theta_n, \sigma \to \varphi_j$ be a derivation for $\Sigma \vdash \sigma \to \varphi_j$.

Then the following is a derivation for $\Sigma \vdash \sigma \to \varphi_i$.

(Note that in the application of quantifier axiom 1, v is not free in σ since σ is a sentence.)

$$\begin{array}{ll}
\theta_1, \ldots, \theta_n,\ \sigma \to \varphi_j, & \\
\quad \forall v\,(\sigma \to \varphi_j), & \text{(generalisation)} \\
\qquad \forall v\,(\sigma \to \varphi_j) \to (\sigma \to \forall v\,\varphi_j), & \text{(quantifier axiom 1)} \\
\qquad\quad \sigma \to \forall\,\varphi_j. & \text{(modus ponens)}
\end{array}$$

□

Exercise 2.33. (The following is used in (i) in the previous proof.)

Show for any two formulas φ and ψ, that $\varphi \to (\psi \to \varphi)$ is a propositional axiom. □

Exercise 2.34. (The following is used in (iii) in the previous proof.)

Show for any three formulas φ, ψ, χ, that $\big(\varphi \to (\psi \to \chi)\big) \to \big((\varphi \to \psi) \to (\varphi \to \chi)\big)$ is a propositional axiom. □

Remark 2.35 *(Using the Axioms and Rules of Inference).* Notice how certain propositional axioms, the first of the two quantifier axioms, and both rules of inference, were all used in the proof of the Deduction Theorem 2.32. Regarding the propositional axioms, two of the three axiom schemas for Propositional Logic itself were were used directly, see Section 6.2.

Proving the Deduction Theorem must surely have provided a strong incentive for the original axioms and rules of inference used in the Hilbert system. □

2.5 Material To Include

Chapter 3

Gödel's Completeness Theorem

3.1 Overview

The goal is to provide a system that is sound, verifiable and complete, such that

$$\Sigma \vdash \varphi \quad \Longleftrightarrow \quad \Sigma \models \varphi$$

> I find it incredible that we have formal proof systems for which semantic validity, a sweeping concept ranging across all possible semantic contexts, aligns exactly with provability in the system. Universal truth is thereby reduced to a finite reasoning process—every universal truth is true for a finite reason and this surely informs further philosophical questions and analysis.
>
> *David Hamkins* (Hamkins, 2021, Section 5.1)

3.2 Consistency

Remark 3.1 *(Fixed Countable Language).* In the following, unless otherwise clear from context, all formulas are in the same fixed language $\mathcal{L}$.

The cardinality of $\mathcal{L}$ is defined in (1.7)*, and prior to Section 3.5, is countable.* This implies that the set of formulas of $\mathcal{L}$ is also countable. However, the cardinality of the set of function and relation symbols, and often but not always of the set of constant symbols, will be finite.

The significant exception to this is Section 3.5 and beyond. □

The notions of a *consistent* set of sentences and of a *maximal consistent* set of sentences are syntactic. That is, they involve formal derivations from axioms.

Definition 3.2 (Absurdum). It is sometimes convenient to have a sentence, usually denoted by "$\bot$" and called *falsum*, *absurdity* or *contradiction*, and which is false in all structures for the language $\mathcal{L}$.

We define $\bot$ by

$$\bot \ := \ \varphi \wedge \neg\varphi$$

for any sentence φ.

The essential point is that $\bot$ is false in every $\mathcal{L}$-structure. On the other hand $\neg\bot$ is true in every $\mathcal{L}$-structure.

Definition 3.3 (Consistency). A set of sentences Σ is *consistent* if a contradiction cannot be derived from Σ. That is, if $\Sigma \nvdash \bot$.

Σ is *inconsistent* if $\Sigma \vdash \bot$.

Using this terminology we have the following version of the Soundness Theorem 2.25

Corollary 3.4 (Soundness). *If Σ has a model then Σ is consistent.*

Proof. If Σ is inconsistent then $\Sigma \vdash \bot$. Hence $\Sigma \models \bot$ by the Soundness Theorem, and so Σ has no model. □

The following gives three equivalent criteria for consistency, and the corresponding three criteria for inconsistency.

Proposition 3.5 (Consistency, Equivalent Versions). *Suppose Σ is a set of sentences in the language $\mathcal{L}$.*

Then

$$\begin{aligned} \Sigma \textit{ is consistent } &\iff \textit{for every sentence } \varphi,\ \Sigma \nvdash \varphi \textit{ or } \Sigma \nvdash \neg\varphi \\ &\iff \textit{for some sentence } \psi,\ \Sigma \nvdash \psi \\ &\iff \Sigma \nvdash \bot. \end{aligned}$$

The set Σ is inconsistent if it is not consistent. That is,

$$\begin{aligned} \Sigma \textit{ is inconsistent } &\iff \textit{for some sentence } \varphi,\ \Sigma \vdash \varphi \textit{ and } \Sigma \vdash \neg\varphi \\ &\iff \textit{for every sentence } \psi,\ \Sigma \vdash \psi \\ &\iff \Sigma \vdash \bot. \end{aligned}$$

Proof.

To prove that the three definitions of “inconsistent” are equivalent note that for any two sentences φ and ψ, $\vdash \varphi \to (\neg\varphi \to \psi)$ since it is a propositional tautology.

(a) So if for some sentence φ, $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$, it follows by juxtaposing the two deductions and using modus ponens twice that, for every ψ, $\Sigma \vdash \psi$.

(b) If $\Sigma \vdash \psi$ for every ψ, then in particular $\Sigma \vdash \bot$.

(c) If $\Sigma \vdash \bot$, since $\bot \to \varphi$ and $\bot \to \neg\varphi$ as each is a propositional axiom, it follows that $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$ (for every and hence for some φ).

The three definitions of “consistent” are also equivalent since Σ is consistent iff it is not inconsistent. But the first/second/third definitions for consistency are the negation of the first/second/third definitions for inconsistency. □

The following gives connections between consistency and derivability.

Theorem 3.6 (Properties of Consistency). *Suppose Σ is a set of sentences and σ is a sentence.*

1. *Σ is consistent iff every finite subset of Σ is consistent;*
2. *If $\Sigma \vdash \sigma$ then $\Sigma \cup \{\sigma\}$ is consistent, but not conversely.*
3. *$\Sigma \cup \{\sigma\}$ is inconsistent iff $\Sigma \vdash \neg\sigma$, $\Sigma \cup \{\sigma\}$ is consistent iff $\Sigma \nvdash \neg\sigma$;*
4. *$\Sigma \cup \{\neg\sigma\}$ is inconsistent iff $\Sigma \vdash \sigma$, $\Sigma \cup \{\neg\sigma\}$ is consistent iff $\Sigma \nvdash \sigma$.*

Proof.

1. Immediate, since proofs have finite length.
2. If $\Sigma \vdash \sigma$ then any proof from $\Sigma \cup \{\sigma\}$ (including a proof of an inconsistency) can be turned into a proof from Σ.
   (*Why* does the consistency of $\Sigma \cup \{\sigma\}$ not imply $\Sigma \vdash \sigma$?)
3. For the first statement:
   (a) If $\Sigma \cup \{\sigma\}$ is inconsistent, then $\Sigma \cup \{\sigma\} \vdash \neg\sigma$ and so $\Sigma \vdash \sigma \to \neg\sigma$ by the Deduction Theorem. But $\vdash (\sigma \to \neg\sigma) \to \neg\sigma$ as this is a propositional tautology.[1] Hence $\Sigma \vdash \neg\sigma$ by modus ponens.
   (b) If $\Sigma \vdash \neg\sigma$ then $\Sigma \cup \{\sigma\} \vdash \neg\sigma$ and $\Sigma \cup \{\sigma\} \vdash \sigma$, and so $\Sigma \cup \{\sigma\}$ is inconsistent.

   The second statement in 3 follows immediately.
4. This follows from 3, using $\Sigma \vdash \sigma$ iff $\Sigma \vdash \neg\neg\sigma$. □

Definition 3.7 (Maximal Consistency). A set of sentences Σ is *maximal consistent* in the language $\mathcal{L}$ iff Σ is consistent and has no proper consistent extension in $\mathcal{L}$.

That is, Σ is consistent and $\Sigma \cup \{\sigma\}$ is consistent iff $\sigma \in \Sigma$.

Theorem 3.8 (Maximal Consistency). *A set of sentences Σ is maximal consistent iff Σ is consistent and for each sentence σ either $\sigma \in \Sigma$ or $\neg\sigma \in \Sigma$.*

Proof. First suppose Σ is maximal consistent and so in particular is consistent.

For a sentence σ, if $\sigma \in \Sigma$ we are done.

If $\sigma \notin \Sigma$ then $\Sigma \cup \{\sigma\}$ is inconsistent by maximality. So $\Sigma \vdash \neg\sigma$ by Theorem 3.6.3. Hence $\Sigma \cup \{\neg\sigma\}$ is consistent and so $\neg\sigma \in \Sigma$ by maximality.

Next suppose Σ is consistent and for each sentence σ either $\sigma \in \Sigma$ or $\neg\sigma \in \Sigma$.

If $\Sigma \vdash \sigma$ then $\Sigma \cup \{\sigma\}$ is consistent, and so $\sigma \in \Sigma$ by maximality.

If $\Sigma \nvdash \sigma$ then $\Sigma \cup \{\neg\sigma\}$ is consistent by Theorem 3.6.4, and so $\neg\sigma \in \Sigma$ by maximality. □

Corollary 3.9. *If Σ is maximal consistent then for any sentences σ, τ:*

$$\sigma \in \Sigma \iff \Sigma \vdash \sigma \tag{3.1}$$

$$\sigma \notin \Sigma \iff \neg\sigma \in \Sigma \iff \Sigma \vdash \neg\sigma \tag{3.2}$$

$$\sigma \wedge \tau \in \Sigma \iff \sigma \in \Sigma \text{ and } \tau \in \Sigma. \tag{3.3}$$

Proof. Exercise. Keep is as brief as you can — just a few lines. □

The following result due to Lindenbaum will be applied in the proof of Gödel's Completeness Theorem in Section 3.4.

Lindenbaum's Theorem is easy to prove with the current set-up, it is essentially the same as for propositional logic and is just Theorem 6.18. But since that is in an optional section, let's prove it here.

Theorem 3.10 (Lindenbaum's Theorem). *Suppose Σ is a consistent set of sentences in the language $\mathcal{L}$. Then Σ can be extended to a maximal consistent set Σ^* in the same language $\mathcal{L}$.*

[1] This follows easily by truth tables. To motivate it, note that $\sigma \to \neg\sigma$, $\neg\sigma \vee \neg\sigma$ and $\neg\sigma$ are tautologically equivalent

Proof. Let $\varphi_1, \varphi_2, \varphi_3, \ldots$ be an enumeration of all sentences from $\mathcal{L}$. Define

$$\begin{aligned}
\Sigma_1 &= \Sigma, \\
\Sigma_{n+1} &= \begin{cases} \Sigma_n \cup \{\varphi_n\} & \text{if } \Sigma_n \cup \{\varphi_n\} \text{ is consistent,} \\ \Sigma_n & \text{otherwise,} \end{cases} \\
\Sigma^* &= \bigcup_{n \geq 1} \Sigma_n.
\end{aligned} \tag{3.4}$$

Each Σ_n is consistent by construction. Hence Σ^* is consistent since derivations are finite in length.

To see that Σ^* is *maximal* consistent, suppose $\Sigma^* \cup \{\varphi\}$ is consistent. We want to show $\varphi \in \Sigma^*$.

But $\varphi = \varphi_n$ for some n, and because $\Sigma_n \cup \{\varphi_n\}$ must also be consistent since $\Sigma_n \subset \Sigma^*$, it follows by construction that $\varphi_n \in \Sigma_{n+1}$. Hence $\varphi_n \in \Sigma^*$ and so Σ^* is maximal consistent. □

Remark 3.11 *("Construct" vs. "Constructivism").* The argument used in the proof of Lindenabum's theorem is called a *constructive* process in the following sense. At each stage in the construction, one of two (mutually exclusive) alternatives are available which determine whether or not to add φ_n to Σ_n. However, there is not normally an algorithm to decide which alternative is the case.[2]

While this usage of the word "construction" as here is standard mathematical practice, the proof of Lindenbaum's Theorem is not an acceptable process within the *Constructivism* view of mathematics. Similarly, the proof of Gödel's Theorem in Section 3.3 is *not* acceptable within the Constructivist program. □

3.3 Gödel's Completeness Theorem – Preliminaries

In Section 3.4 we prove the following major result due to Gödel.

Theorem 3.12 (Completeness Theorem, Version 1). *Suppose Σ is a set of sentences in the language $\mathcal{L}$, φ is a sentence in $\mathcal{L}$, and $\Sigma \vDash \varphi$. Then $\Sigma \vdash \varphi$.*

Remark 3.13 *(Significance of Completeness).* Suppose we know (by any means whatsoever) that φ is true whenever all sentences in Σ are true.

That is, we know φ is true in all models of Σ.

Then there is a formal first-order logic proof (in the sense previously discussed) of φ from Σ.

Although the theorem refers to first-order logic, its significance is enhanced by the fact that all of mathematics can be treated within (*first-order*) Zermelo Fraenkel set theory, perhaps with additional axioms such as the axiom of choice, the generalised continuum hypothesis, etc. □

Remark 3.14 *(An Important Case).* Suppose Σ has *no* models, i.e. Σ is not satisfiable.

This is the case iff $\Sigma \vDash \bot$. *Why?*

Then by Theorem 3.12, $\Sigma \vdash \bot$. That is, Σ is inconsistent. □

[2] See Chapter 7.

An equivalent, and equally important version of the Completeness Theorem, is the following.

Theorem 3.15 (Completeness Theorem, Version 2). *Suppose Σ is a consistent set of sentences in the language $\mathcal{L}$. Then Σ is satisfiable (i.e. has a model).*

Proposition 3.16 (Versions 1 & 2 are Equivalent).

Proof. Version 1 implies Version 2 by Remark 3.14.

Next assume Version 2 (Theorem 3.15).

To prove Version 1 (Theorem 3.12), suppose Σ is a set of sentences, φ is a sentence, and $\Sigma \vDash \varphi$.

$$\begin{aligned} &\therefore \quad \Sigma \cup \{\neg\varphi\} && \text{has no model.} \\ &\therefore \quad \Sigma \cup \{\neg\varphi\} && \text{is not consistent by Theorem 3.15.} \\ &\therefore \quad \Sigma \vdash \varphi && \text{by Theorem 3.6.} \end{aligned}$$

So Version 2 implies Version 1. □

Remark 3.17 *(Summary).* From Definition 3.5 and the Definition of satisfiability,

$$\Sigma \text{ is consistent} \iff \Sigma \nvdash \bot, \quad \Sigma \text{ is satisfiable} \iff \Sigma \nvDash \bot. \tag{3.5}$$

Theorems 3.12 and 3.15 respectively, together with the Soundness Theorem, can now be summarised as follows (using the contrapositive for Theorem 3.15):

$$\text{for all } \Sigma \text{ and } \varphi, \qquad \Sigma \vDash \varphi \iff \Sigma \vdash \varphi; \tag{3.6}$$

$$\text{for all } \Sigma, \qquad \Sigma \vDash \bot \iff \Sigma \vdash \bot. \tag{3.7}$$

□

3.4 Gödel's Completeness Theorem – Proof

In this Section, all languages are finite or countably infinite.

The ideas extend to uncountable languages, and this is important for applications to algebra. See Section 3.5.

We now prove the version of Gödel's Completeness Theorem given by Theorem 3.15. Namely:

Theorem 3.18 (Gödel's Completeness Theorem). *Suppose Σ is a consistent set of sentences in the language $\mathcal{L}$. Then Σ has a model $\mathfrak{A}$.*

Assuming the cardinality[3] $|\mathcal{L}| = \aleph_0$ *(as we do at this stage), then* $|\mathfrak{A}| \leq \aleph_0$ *where* $|\mathfrak{A}|$ *is the cardinality of the universe of* $\mathfrak{A}$.

Since all we have is the set Σ of consistent sentences, how do we go about building/constructing such a model $\mathfrak{A}$? In particular, what should we take for the universe A of $\mathfrak{A}$. The method here is due to Henkin and is somewhat different from that of Gödel, and is of broader applicability.

The proof is contained in the next 8 Steps.

Proof

[3] Recall the definition of the cardinality $|\mathcal{L}|$ of $\mathcal{L}$ in (1.7).

3.4.1 Step 1 Adding a Set $\mathcal{C}$ of New Constant Symbols to $\mathcal{L}$

Introduce a language $\mathcal{L}^* = \mathcal{L} \cup C$ which extends $\mathcal{L}$, by adding a countably infinite set $C = \{c_1, c_2, \dots\}$ of *new* constant symbols not in $\mathcal{L}$.

3.4.2 Step 2 Extend Σ to Σ^* with $\mathcal{C}$ a Set of Henkin Witnesses

This is the key result, due to Henkin. In the following Lemma, the constant c is called a *Henkin witness* for the formula $\exists v\, \varphi(v)$.

Lemma 3.19 (Henkin Witnesses). *There is a* consistent *extension* Σ^* *of* Σ *in the extended language* $\mathcal{L}^*$*, with the following property:*

For every *formula* $\varphi = \varphi(v)$ *of* $\mathcal{L}^*$ *(not just of* $\mathcal{L}$*) with at most one free variable depending on* φ *(here it is* v*), there is a constant* $c \in \mathcal{C}$ *(*c *depending on* φ*) such that*

$$\exists v\, \varphi(v) \to \varphi(c) \;\in\; \Sigma^*. \tag{3.8}$$

Proof. List all formulas of $\mathcal{L}^*$ (not just formulas of $\mathcal{L}$) with one free variable:

$$\varphi_1, \varphi_2, \dots, \varphi_n, \dots \tag{3.9}$$

Define a sequence of consistent extensions of Σ, in the language $\mathcal{L}^*$:

$$\Sigma =: \Sigma_0^* \subset \Sigma_1^* \subset \Sigma_2^* \subset \dots \subset \Sigma_n^* \subset \dots\ ,$$

by

$$\Sigma_n^* = \Sigma_{n-1}^* \cup \{\exists v\, \varphi_n(v) \to \varphi_n(c)\} \quad \text{for } n \geq 1, \tag{3.10}$$

where (depending on n), v is the free variable appearing in φ_n and c is the first constant symbol in C not already appearing in Σ_k^* for $k < n$. This is possible since only one new sentence is added at each stage, and so only a finite number of constant symbols from C have already been added at any (finite) stage in the process.

We claim that Σ_n^* is consistent for all n.[4]

This is true for $n = 0$ since $\Sigma_0^* = \Sigma$ and Σ is consistent.

Next assume Σ_{n-1}^* is consistent but Σ_n^* is not. Then:

$$\begin{array}{lll}
 & \Sigma_{n-1}^* \vdash \neg\big(\exists v\, \varphi_n(v) \to \varphi_n(c)\big) & \text{(Theorem 3.6.2)} \\
\therefore & \Sigma_{n-1}^* \vdash \exists v\, \varphi_n(v) \wedge \neg\varphi_n(c) & \text{(propositional logic and modus ponens)} \\
\therefore & \Sigma_{n-1}^* \vdash \exists v\, \varphi_n(v) \wedge \neg\varphi_n(w) & \text{(in previous derivation, replace } c \text{ everywhere} \\
 & & \quad \text{by a variable } w \text{ not used, free or bound)} \\
\therefore & \Sigma_{n-1}^* \vdash \exists v\, \varphi_n(v), \quad \Sigma_{n-1}^* \vdash \neg\varphi_n(w) & \text{(propositional logic and modus ponens)} \\
\therefore & \Sigma_{n-1}^* \vdash \exists v\, \varphi_n(v), \quad \Sigma_{n-1}^* \vdash \forall w\, \neg\varphi_n(w) & \text{(generalisation)} \\
\therefore & \Sigma_{n-1}^* \vdash \exists v\, \varphi_n(v), \quad \Sigma_{n-1}^* \vdash \neg\exists w\, \varphi_n(w) & \text{(definition of } \forall \text{ from } \exists)
\end{array}$$

[4] This consistency is not surprising. See "Plausibility Argument" in the following boxed discussion.

But $\vdash \exists v\, \varphi_n(v) \to \exists w\, \varphi_n(w)$[5] and so $\Sigma^*_{n-1} \vdash \exists w\, \varphi_n(w)$ by modus ponens. This is a contradiction.

Hence Σ^*_n is consistent for all n and so

$$\Sigma^* := \bigcup_{n \geq 0} \Sigma^*_n \tag{3.11}$$

is consistent.

Finally, C is a set of witnesses for Σ^*, since any formula φ from $\mathcal{L}^*$ with one free variable is φ_n for some n, and so a witnessing constant c for φ from C is introduced at the n-th stage in the previous procedure.

That is

$$\Sigma^* \vdash \exists v\, \varphi(v) \to \varphi(c), \tag{3.12}$$

where for each $\varphi \equiv \varphi(v)$, a formula with one free variable, the constant symbol c depends on the previous construction process. □

Plausibility Argument

It is natural to expect that we can consistently add $\exists v\, \varphi_n(v) \to \varphi_n(c)$ in (3.10) at the nth stage in the construction process. Here is a semantic argument.

(a) If we have a model for Σ^*_{n-1} in which $\exists v\, \varphi_n(v)$ is *true*, then interpreting the "new" symbol c as some such v, will make $\varphi_n(c)$ true and hence make the implication $\exists v\, \varphi_n(v) \to \varphi_n(c)$ true.

(b) If we have a model for Σ^*_{n-1} in which $\exists v\, \varphi_n(v)$ is *false*, then interpreting the "new" symbol c as any element in the model will make $\varphi_n(c)$ false, but the sentence $\exists v\, \varphi_n(v) \to \varphi_n(c)$ is again true. (*Why?*)

But of course we cannot argue semantically in this manner.

The correct argument is achieved by ensuring that there are enough axioms from first-order logic to justify the formal syntactic argument.

3.4.3 Step 3 Enlarge Σ^* to a Complete Theory

By Lindstrom's Theorem 3.10, the theory Σ^* in the language $\mathcal{L}^* = \mathcal{L} \cup \mathcal{C}$ has a *complete* consistent extension in the same language $\mathcal{L}^*$.

Henceforth, *we will use the same notation* Σ^* *to denote this complete extension.*

As in Lindstrom's Theorem in general, *the extension is neither unique nor canonical.*

[5] We need to be a little careful here. We passed from $\varphi_n(v)$ to $\varphi_n(c)$ to $\varphi_n(w)$. Moreover, c and v (as a free variable) do not occur in $\varphi_n(w)$. It follows that v is free for w in the sense of the universal instantiation axiom (2.2) and so

$\vdash \forall w \neg\varphi_n(w) \to \neg\varphi_n(v)$	by (2.1) as v not free in $\varphi_n(w)$
$\vdash \forall v \big(\forall w \neg\varphi_n(w) \to \neg\varphi_n(v)\big)$	generalisation (2.7)
$\vdash \forall w \neg\varphi_n(w) \to \forall v \neg\varphi_n(v)$	axiom (2.2)
$\vdash \neg\forall v \neg\varphi_n(v) \to \neg\forall w \neg\varphi_n(w)$	propositional axioms
$\vdash \exists v\, \varphi_n(v) \to \exists w\, \varphi_n(w)$	definition of $\exists$

3.4.4 Step 4 An Equivalence Relation on $\mathcal{C}$

Define a relation "$\sim$" on $\mathcal{C}$ by the first "$\iff$" in the following,

$$c \sim c' \iff (c = c') \in \Sigma^* \iff \Sigma^* \vdash c = c' \iff \Sigma^* \nvdash c \neq c', \tag{3.13}$$

where the second "$\iff$" is by the maximality of Σ^*, and the last "$\iff$" is from Theorem 3.8.

Taking the negation of these statements,

$$c \nsim c' \iff (c = c') \notin \Sigma^* \iff \Sigma^* \nvdash c = c' \iff \Sigma^* \vdash c \neq c'. \tag{3.14}$$

We will show "$\sim$" is an equivalence relation[6]. The essential point in the argument is to use the equality axioms in (2.3). Details are in Section 2.4.1.

Definition 3.20. The equivalence class corresponding to "$\sim$" and containing c is written $[c]$.

Exercise 3.21. It follows from the construction of Σ^* that each equivalence class contains a *countably infinite* set of constant symbols from $\mathcal{C}$. *Why?* □

3.4.5 Step 5 Constructing a Structure $\mathfrak{A}^*$ such that $\mathfrak{A}^* \models \Sigma^*$

The extension Σ^* of Σ is not canonical or uniquely determined. But once we have some such extension Σ^*, a structure $\mathfrak{A}^*$ for which $\mathfrak{A}^* \models \Sigma^*$ *is* uniquely determined from Σ^*, as we will see in this and the following Step.

In this Step we build the $\mathcal{L}^*$-structure $\mathfrak{A}^*$. In the next step we show $\mathfrak{A}^* \models \Sigma^*$.

The problem to be addressed in this Step is that the axioms for equality only ensure that the equality relation symbol "$=$" in an $\mathcal{L}^*$-structure will be interpreted as an equivalence relation, and not as the identity relation. So it is perhaps not so surprising that we will build the desired $\mathcal{L}^*$-structure by taking equivalence classes. But what will be critical is the use of the Henkin axioms from (3.8).

The universe A of $\mathfrak{A}^*$ is defined by

$$A := \{[c] : c \in \mathcal{C}\}, \tag{3.15}$$

where the relevant equivalence relation and the corresponding equivalence classes are from (3.13) and Definition 3.20.

The *interpretation* in $\mathfrak{A}^*$ of each constant symbol $c \in \mathcal{C}$ is, unsurprisingly, $[c]$.

$$c^{\mathfrak{A}^*} = [c]. \tag{3.16}$$

The *interpretation* of the remaining constant, function and relation symbols from $\mathcal{L}^* \setminus \mathcal{C} = \mathcal{L}$, are determined as follows:

1. *Constant Symbols in $\mathcal{L}$*: Let $d \in \mathcal{L}$ be a constant symbol.

We need to show there is an equivalence class $[c]$ as in (3.15) which, in a natural way, will be the interpretation of d.

[6] That is, $c \sim c$, $c \sim d \Longrightarrow d \sim c$, and $(c \sim d \;\&\; d \sim e) \Longrightarrow c \sim e$.

For this first note that $\vdash d = d$ by the same argument as in the "Details" box showing $\vdash c = c$.

But $\vdash d = d \to \exists v\,(v = d)$ from Proposition 2.27, existential generalisation.

Also $\Sigma^* \vdash \exists v\,(v = d) \to c = d$ for some (Henkin witness) $c \in \mathcal{C}$, by Lemma 3.19.

From two applications of modus ponens, $\Sigma^* \vdash c = d$ for some $c \in \mathcal{C}$.

It follows as in Section 2.4.1 that, if $c' \in \mathcal{C}$, then

$$\Sigma^* \vdash c' = d \quad\Longleftrightarrow\quad \Sigma^* \vdash c' = c \quad\Longleftrightarrow\quad [c] = [c'].$$

So we define

$$d^{\mathfrak{A}^*} = [c] \quad\Longleftrightarrow\quad \Sigma^* \vdash c = d, \tag{3.17}$$

and we have shown that the definition is independent of the equivalence class representative of $[c]$.

2. *Function Symbols in $\mathcal{L}$*: Let $f \in \mathcal{L}$ be an n-ary function symbol. Define the interpretation $f^{\mathfrak{A}^*} : A^n \to A$ of f in $\mathfrak{A}$ by

$$f^{\mathfrak{A}^*}([c_1], \dots, [c_n]) = [c] \quad\Longleftrightarrow\quad \Sigma^* \vdash f(c_1, \dots, c_n) = c, \tag{3.18}$$

where $c_1, \dots, c_n, c \in \mathcal{C}$.

To justify this we need to show:

(a) if $c_1, \dots, c_n \in \mathcal{C}$ then there exists $c \in \mathcal{C}$ such that $\Sigma^* \vdash f(c_1, \dots, c_n) = c$,

(b) if also $c'_1, \dots, c'_n \in \mathcal{C}$, $c_1 \sim c'_1, \dots, c_n \sim c'_n$ then $f(c_1, \dots, c_n) \sim f(c'_1, \dots, c'_n)$.

This then implies $f^{\mathfrak{A}^*} : A^n \to A$ is a total (i.e. everywhere defined) function, and that the definition of $f^{\mathfrak{A}^*}$ is independent of choice of equivalence class representatives.

The argument, similar to that for constant symbols, is as follows:

For (a) first note $\vdash f(c_1, \dots, c_n) = f(c_1, \dots, c_n)$ by a similar argument to that in Section 2.4.1 showing $\vdash c = c$.

But $\vdash f(c_1, \dots, c_n) = f(c_1, \dots, c_n) \to \exists v\,(v = f(c_1, \dots, c_n))$ from Proposition 2.27, existential generalisation.

Also $\Sigma^* \vdash \exists v\,(v = f(c_1, \dots, c_n)) \to c = f(c_1, \dots, c_n)$ for some (Henkin witness) $c \in \mathcal{C}$, by Lemma 3.19.

From two applications of modus ponens, $\Sigma^* \vdash c = f(c_1, \dots, c_n)$ for some $c \in \mathcal{C}$.

This establishes (a).

For (b) we have

$$\begin{aligned}
&c_1 \sim c'_1, \dots, c_n \sim c'_n \\
&\qquad\Longrightarrow\quad \Sigma^* \vdash c_1 = c'_1, \dots, \Sigma^* \vdash c_n = c'_n && \text{using (3.13)} \\
&\qquad\Longrightarrow\quad \Sigma^* \vdash c_1 = c'_1 \wedge \dots \wedge c_n = c'_n && \text{basic properties of “ $\vdash$ ”} \\
&\qquad\Longrightarrow\quad \Sigma^* \vdash f(c_1, \dots, c_n) = f(c'_1, \dots, c'_n) && \text{using equality axiom (2.4)} \\
&\qquad\Longrightarrow\quad f(c_1, \dots, c_n) \sim f(c'_1, \dots, c'_n) && \text{using (3.13)}
\end{aligned}$$

3. *Relation Symbols in $\mathcal{L}$*: Let $r \in \mathcal{L}$ be an n-ary relation symbol. Define the interpretation $r^{\mathfrak{A}^*} \subset A^n$ of r in $\mathfrak{A}^*$ by

$$\big([c_1], \ldots, [c_n]\big) \in r^{\mathfrak{A}^*} \quad \Longleftrightarrow \quad \Sigma^* \vdash r(c_1, \ldots, c_n), \tag{3.19}$$

where $c_1, \ldots, c_n \in \mathcal{C}$.

To show this is well defined we need to show the definition of $r^{\mathfrak{A}^*}$ is independent of choice of equivalence class representatives. But this is by essentially the same argument as for a function symbol.

$$\begin{array}{lll} c_1 \sim c_1', \ldots, c_n \sim c_n' & & \\ \quad\Longrightarrow \quad \Sigma^* \vdash c_1 = c_1' \wedge \cdots \wedge c_n = c_n' & & \text{(3.13), properties of “} \vdash \text{”} \\ \quad\Longrightarrow \quad \Sigma^* \vdash r(c_1, \ldots, c_n) \leftrightarrow r(c_1', \ldots, c_n') & & \text{using equality axiom (2.5)} \\ \quad\Longrightarrow \quad \Sigma^* \vdash r(c_1, \ldots, c_n) \text{ iff } \Sigma^* \vdash r(c_1', \ldots, c_n') & & \text{properties of “} \vdash \text{”} \\ \quad\Longrightarrow \quad \big([c_1], \ldots, [c_n]\big) \in r^{\mathfrak{A}^*} \text{ iff } \big([c_1'], \ldots, [c_n']\big) \in r^{\mathfrak{A}^*} & & \text{by (3.19)} \end{array}$$

3.4.6 Step 6 Proof that $\mathfrak{A} \vDash \Sigma^*$

Because *every* element in the universe A of $\mathfrak{A}^*$ is the interpretation of a constant symbol $c \in \mathcal{C}$ (in fact many such constant symbols, but all of which are equivalent via “$\sim$”), we will *not* need to consider free variables when interpreting terms in $\mathfrak{A}^*$, *nor* to consider formulas with free variables when defining the truth values of sentences in $\mathfrak{A}^*$.

Definition 3.22. Suppose t is a term in the language $\mathcal{L}^*$ (with no free variables). Then the interpretation $t^{\mathfrak{A}}$ ($\in A$) of t is defined by induction on the complexity of t as follows:

- If t is a constant symbol $c \in \mathcal{C}$ or $d \in \mathcal{L}$, then $c^{\mathfrak{A}^*}$ and $d^{\mathfrak{A}^*}$ have already been defined in (3.16) and (3.17). In particular
$$t^{\mathfrak{A}^*} = [c] \quad \Longleftrightarrow \quad \Sigma^* \vdash t = c.$$
- If t is $f(t_1, \ldots, t_n)$ then
$$t^{\mathfrak{A}^*} := f^{\mathfrak{A}^*}(t_1^{\mathfrak{A}^*}, \ldots, t_n^{\mathfrak{A}^*}).$$

Lemma 3.23. *If t is a term in $\mathcal{L}^*$ and $c \in \mathcal{C}$, then*

$$t^{\mathfrak{A}^*} = [c] \quad \Longleftrightarrow \quad \Sigma^* \vdash t = c. \tag{3.20}$$

Proof. We have already seen this for t a constant symbol.

Let t be $f(t_1, \ldots, t_n)$. Suppose $t^{\mathfrak{A}^*} = [c]$.

Assume (the inductive hypothesis) that the result corresponding to (3.20) holds with t replaced by $t_1, \ldots, t_n$.

Let $t_i^{\mathfrak{A}^*} = [c_i]$ and so $\Sigma^* \vdash t_i = c_i$, for $1 \leq i \leq n$.

Then

$$\begin{array}{rll} t^{\mathfrak{A}^*} = [c] \Longleftrightarrow & f^{\mathfrak{A}^*}(t_1^{\mathfrak{A}^*}, \ldots, t_n^{\mathfrak{A}^*}) = [c] & \text{Definition 3.22} \\ \Longleftrightarrow & f^{\mathfrak{A}^*}([c_1], \ldots, [c_n]) = [c] & \text{by assumption for each } t_i^{\mathfrak{A}^*} \\ \Longleftrightarrow & \Sigma^* \vdash f(c_1, \ldots, c_n) = c & \text{by (3.18)} \\ \Longleftrightarrow & \Sigma^* \vdash f(t_1, \ldots, t_n) = c & \text{by } \Sigma^* \vdash t_i = c_i \text{ and equality axiom (2.4)} \\ \Longleftrightarrow & \Sigma^* \vdash t = c & \text{definition of } t \end{array}$$

This establishes the result. □

Theorem 3.24. *For every sentence φ in the language $\mathcal{L}^*$,*

$$\mathfrak{A}^* \models \varphi \quad \Longleftrightarrow \quad \Sigma^* \vdash \varphi \quad \Longleftrightarrow \quad \varphi \in \Sigma^*. \tag{3.21}$$

That is,

$$\mathfrak{A}^* \models \Sigma^*. \tag{3.22}$$

Proof. The second $\Longleftrightarrow$ in (3.21) is by (3.1) in Corollary 3.9, since Σ^* is maximal consistent.

For the first $\Longleftrightarrow$ it will be more convenient to work with sentences built using $\exists$ rather than $\forall$ as a primitive logical symbol. So we consider $\forall$ as a defined symbol via $\forall := \neg\exists\neg$.

The proof of the first $\Longleftrightarrow$ will be by induction on the complexity of φ.

Moreover, unlike the situation with the definition and properties of "$\models$" for a general structure, since every element in A corresponds to a constant (in fact many) constant symbols in $\mathcal{C}$, we will be able to work just with sentences.

Atomic Sentences:

(a) $r(t_1, \ldots, t_n)$: We claim

$$\mathfrak{A}^* \models r(t_1, \ldots, t_n) \quad \Longleftrightarrow \quad \Sigma^* \vdash r(t_1, \ldots, t_n). \tag{3.23}$$

Since $t_i^{\mathfrak{A}^*} \in A$ for $1 \leq i \leq n$, let $t_i^{\mathfrak{A}^*} = [c_i]$.

Then

$$\begin{aligned}
\mathfrak{A}^* \models r(t_1, \ldots, t_n) &\Longleftrightarrow (t_1^{\mathfrak{A}^*}, \ldots, t_n^{\mathfrak{A}^*}) \in r^{\mathfrak{A}^*} && \text{Definition 1.18 (ii) for "}\models\text{"} \\
&\Longleftrightarrow ([c_1], \ldots, [c_n]) \in r^{\mathfrak{A}^*} \\
&\Longleftrightarrow \Sigma^* \vdash r(c_1, \ldots, c_n) && \text{definition in (3.19) of } r^{\mathfrak{A}^*}
\end{aligned}$$

(b) $t_1 = t_2$: We claim

$$\mathfrak{A}^* \models t_1 = t_2 \quad \Longleftrightarrow \quad \Sigma^* \vdash t_1 = t_2 \tag{3.24}$$

Let $t_1^{\mathfrak{A}^*} = [c_1]$, $t_2^{\mathfrak{A}^*} = [c_2]$.

Then $\Sigma^* \vdash t_1 = c_1$ and $\Sigma^* \vdash t_2 = c_2$ by Lemma 3.20.

Hence[7]

$$\begin{aligned}
\mathfrak{A}^* \models t_1 = t_2 &\Longleftrightarrow t_1^{\mathfrak{A}^*} = t_2^{\mathfrak{A}^*} && \text{Definition 1.18 (i) for } \models \\
&\Longleftrightarrow [c_1] = [c_2] \\
&\Longleftrightarrow c_1 \sim c_2 && \text{Definition 3.20 of } [\,\cdot\,] \text{ from } \sim \\
&\Longleftrightarrow \Sigma^* \vdash c_1 = c_2 && \text{definition of } \sim \text{ in (3.13)} \\
&\Longleftrightarrow \Sigma^* \vdash t_1 = t_2 && \text{see below}
\end{aligned}$$

The last equivalence uses

$$\begin{aligned}
&\vdash \ (c_1 = c_2 \wedge t_1 = c_1 \wedge t_2 = c_2) \ \rightarrow \ t_1 = t_2 \\
&\vdash \ (t_1 = t_2 \wedge t_1 = c_1 \wedge t_2 = c_2) \ \rightarrow \ c_1 = c_2
\end{aligned}$$

This, in turn, uses the logical axioms for equality.

[7] Note that the second "=" in the first line of the following display, and the "=" in the second line, are *not* equality symbols in the formal language $\mathcal{L}^*$. They are abbreviations in the metalanguage used to discuss the structure $\mathfrak{A}^*$. They are saying that $t_1^{\mathfrak{A}^*}$ and $t_2^{\mathfrak{A}^*}$ denote the same element in the universe A, and similarly that $c_1^{\mathfrak{A}^*}$ and $c_2^{\mathfrak{A}^*}$ denote the same element in A.

Exercise 3.25. Explain. □

Negation $\neg\varphi$: Assume (3.21) is true for φ. It follows that the analogue is true for $\neg\varphi$:

$$\begin{array}{rcll} \mathfrak{A}^* \models \neg\varphi & \iff & \mathfrak{A}^* \not\models \varphi & \\ & \iff & \Sigma^* \nvdash \varphi & \text{induction assumption} \\ & \iff & \Sigma^* \vdash \neg\varphi & \text{Corollary 3.9, since } \Sigma^* \text{ is maximal consistent} \end{array}$$

Conjunction $\varphi \wedge \psi$: Assume (3.21) is true for φ and ψ. It follows that the analogue is true for $\varphi \wedge \psi$:

$$\begin{array}{rclll} \mathfrak{A}^* \models \varphi \wedge \psi & \iff & \mathfrak{A}^* \models \varphi \quad \& \quad \mathfrak{A}^* \models \psi & & \text{Definition 1.18 (iv) for } \models \\ & \iff & \Sigma^* \vdash \varphi \quad \& \quad \Sigma^* \vdash \psi & & \text{induction assumption} \\ & \iff & \Sigma^* \vdash \varphi \wedge \psi & & \text{see below} \end{array}$$

The last equivalence uses

$$\vdash \varphi \wedge \psi \quad \iff \quad \vdash \varphi \;\&\; \vdash \psi$$

For $\Rightarrow$ use the propositional axioms $\varphi \wedge \psi \to \varphi$ and $\varphi \wedge \psi \to \psi$ and modus ponens. For $\Leftarrow$ concatenate deductions for $\vdash \varphi$ and $\vdash \psi$, follow this by the propositional axiom $\varphi \to (\psi \to \varphi \wedge \psi)$ and then two applications of modus ponens.

Existential Quantifier $\exists v\, \varphi$: Since $\exists v\, \varphi$ is a *sentence* in the language $\mathcal{L}^*$, it follows that φ has at most v as a free variable. For this reason we here write $\varphi(v)$ for φ, and by $\varphi(c)$ mean the sentence obtained by replacing all free occurrences of v in $\varphi(v)$ by c.

Then since *every* element in the universe of $\mathfrak{A}$ is $[c]$ for some $c \in \mathcal{C}$,

$$\begin{array}{rcll} \mathfrak{A}^* \models \exists v\, \varphi(v) & \iff & \mathfrak{A}^* \models \varphi(c) & \text{for some } c \in \mathcal{C}, \\ & \iff & \Sigma^* \vdash \varphi(c) & \text{by induction hypothesis, some } c \in \mathcal{C}, \\ & \iff & \Sigma^* \vdash \exists v\, \varphi(v), & \end{array}$$

where for "$\Rightarrow$" of the last $\iff$, use the first-order logic result $\vdash \varphi(c) \to \exists v\, \varphi(v)$, together with modus ponens; and for "$\Leftarrow$" use the Henkin Witness property (3.8) of $\mathcal{L}^*$, namely $\exists v\, \varphi(v) \to \varphi(c) \;\in\; \Sigma^*$, together with modus ponens.

This completes the proof of Theorem 3.21 and hence of Step 6. □

3.4.7 Step 7 Definition of $\mathfrak{A}$ & Proof that $\mathfrak{A} \models \Sigma$

This is now easy.

We have seen that

$$\mathfrak{A}^* \models \Sigma^*$$

Since $\Sigma \subset \Sigma^*$, it follows that

$$\mathfrak{A}^* \models \Sigma.$$

Since Σ is a set of sentences in the original language $\mathcal{L}$, Σ does not refer to the new constants $c \in \mathcal{C}$ which occur in the extended language $\mathcal{L}^* = \mathcal{L} \cup \mathcal{C}$.

We now *define* the structure $\mathfrak{A}$ to be the same as $\mathfrak{A}^*$, *except* that it is a structure just for the symbols in $\mathcal{L}$ and not for the new symbols in $\mathcal{C}$.

Since nothing else is changed, it is the case that

$$\mathfrak{A} \models \Sigma.$$

More precisely, we could argue by inducton on the complexity of formulas φ that $\Sigma \models \varphi[\sigma]$ iff $\Sigma^* \models \varphi[\sigma]$ for arbitrary assignments σ

3.4.8 Step 8 Proof that $|\mathfrak{A}| \leq \aleph_0$

We assumed that $|\mathcal{L}|$ is countable.

In particular the set of formulas with one free variable is countable, and hence so is the set of new constant symbols $\mathcal{C}$. But the universe of $\mathfrak{A}$ is given by equivalence classes from $\mathcal{C}$ and so is also countable.

This completes the proof of Gödel's Completeness Theorem 3.12. ∎

3.5 Uncountable Languages

In the proof of the Completeness Theorem we assumed the language $\mathcal{L}$ was countable.

But often we need to discuss an uncountable language, for example in the case which includes a (different) constant symbol for every element in some uncountable structure. Of course this moves us out of the finitistic realm, but to which we will return in Chapter 5.

So let us assume now that the cardinality $|\mathcal{L}|$ of $\mathcal{L}$ is some infinite cardinal κ.[8]

The general result is the following.

Theorem 3.26 (Completeness Theorem, General Version). *Suppose Σ is a consistent set of sentences in the language $\mathcal{L}$ with cardinality $|\mathcal{L}| = \kappa$.*[9]

Then Σ has a model $\mathfrak{A}$ with cardinality $|\mathfrak{A}| \leq \kappa$, where $|\mathfrak{A}|$ is the cardinality of the universe of $\mathfrak{A}$.

The proof of the Completeness Theorem in this more general setting is analogous to the proof in the countable case.

The difference is that instead of a sequence of new constants $\mathcal{C} = \{c_n : n < \omega\}$, one takes a transfinite sequence of new constants $\mathcal{C} = \{c_\alpha : \alpha < \kappa\}$. Instead of each proper initial segment of $\{n : n < \omega\}$ having (finite) cardinality $< \aleph_0$, each proper initial segment of $\{\alpha : \alpha < \kappa\}$ will have cardinality $< \kappa$, by a standard property of ordinals and cardinals.

*** I will include more details after we have treated ordinals and cardinals.

The treatment in (Chang and Keisler, 2012, pp 61–66) is essentially the same as here.

3.6 Consequences of Completeness

We discuss a number of examples in the following Chapter 4. They follow from the following the theorems which are immediate, but very powerful, consequences of the Completeness Theorem.

[8] I am going to now use some of the more elementary properies of ordinals and cardinals, but stick with it if you can.

[9] Recall the definition of the cardinality $|\mathcal{L}|$ of $\mathcal{L}$ in (1.7).

While they are stated here for arbitrary cardinalities, they are already very significant for $|\mathcal{L}|$ countably infinite.

Theorem 3.27 (Compactness Theorem). *A set of sentences Σ has a model if and only if every finite subset has a model.*

Proof. If Σ has a model, then this model is also a model of every finite subset of Σ.

If every finite subset of Σ has a model, then by the Soundness Theorem (version Corollary 3.4) every finite subset of Σ is consistent. Hence Σ is consistent and so has a model by the Completeness Theorem. □

Exercise 3.28. Why "Hence Σ is consistent"? □

Remark 3.29. It is perhaps surprising that this theorem, which says nothing about derivations (syntax) and is only concerned the models (semantics), uses the Completeness Theorem in its proof.

There is, however, a proof which combines the (usually different) models of each finite subset of Σ to obtain a model of Σ. This is called the ultraproduct construction, and it uses the notion of an ultrafilter.

See (Marker, 2015, pp 36–41) or (Chang and Keisler, 2012, Chapter 4), for example. □

Theorem 3.30 (Downward Lowenheim–Skolem–Tarski Theorem). *If a set of sentences Σ in the language $\mathcal{L}$ has a model then it has a model of cardinality at most $|\mathcal{L}|$.*

Proof. Since Σ has a model it is consistent. The Completeness Theorem then gives a model of cardinality at most $|\mathcal{L}|$. □

Theorem 3.31 (Upward Lowenheim–Skolem–Tarski Theorem). *If a set of sentences Σ in the language $\mathcal{L}$ has an infinite model then it has models of every cardinality $\kappa \geq |\mathcal{L}|$.*

Proof. Expand the language $\mathcal{L}$ by adding a set of new constant symbols $=\{c_j : j \in K\}$, where K is a set of cardinality κ.

Let $\mathcal{L}^*$ be the expanded language and note that $|\mathcal{L}^*| = \kappa$

Define

$$\Sigma^* = \Sigma \cup \{c_j \neq c_k : j \neq k\}. \tag{3.25}$$

Suppose F is an arbitrary finite subset of $\{c_j \neq c_k : j \neq k\}$. Since Σ has an infinite model, by interpreting the constant symbols in F as distinct elements in the universe of this model, we see $\Sigma \cup F$ has a model and so is consistent.

It follows that Σ^* is consistent.

By the Completeness Theorem, Σ^* has a model $\mathfrak{A}$ of cardinality at most κ, and by (3.25) the cardinality is at least κ.

Hence the cardinality of $\mathfrak{A}$ is precisely κ. By ignoring the interpretations of the new symbols c_k we obtain a model $\mathfrak{A}$ of Σ alone and of cardinality κ. □

3.7 Wrap-Up

An Interesting Journey

We began with a consistent set of sentences Σ in the language $\mathcal{L}$.
We then extended $\mathcal{L}$ to a language $\mathcal{L}^* = \mathcal{L} \cup \mathcal{C}$, by adding a countably infinite set $\mathcal{C}$ of new constant symbols. *Step 1*
We next extended Σ to Σ^*, a *consistent* set of sentences in $\mathcal{L}^*$, by consistently adding for *every* sentence in $\mathcal{L}^*$ of the form $\exists v\, \varphi(v)$, a Henkin sentence $\exists v\, \varphi(v) \to \varphi(c)$ for some $c \in \mathcal{C}$ depending on φ. *Step 2*
We then extended Σ^* to a *maximal consistent* set of sentences, which we also denoted by Σ^*. *Step 3*
We then defined an equivalence relation on $\mathcal{C}$ by $c \sim c'$ iff $(c = c') \in \Sigma^*$, and defined an $\mathcal{L}^*$-structure $\mathfrak{A}^*$ in which "$=$" was interpreted by "the same as" rather than as just an equivalence relation. This used the Henkin sentences in Σ^*. *Steps 4 and 5*
We next showed that $\mathfrak{A}^* \vDash \Sigma^*$ by again using the Henkin sentences in Σ^* and the maximal consistency of Σ^*. *Step 6*
Finally, by now *ignoring* the interpretation of the symbols in $\mathcal{C}$ we obtained the desired structure $\mathfrak{A}$ such that $\mathfrak{A} \vDash \Sigma$. *Step 7*

Alternative Approach

The approach in most texts is to iterate the production of Henkin Constants a countable number of times, take unions of the extended languages and extended sets of sentences thus obtained, and finally to iterate this iteration process itself a countable number of times. See (Johnstone, 1987; Leader, 2012; Zsák, 2025), and to a lesser extent (Enderton, 2001; Hils and Loeser, 2019; Leary and Kristiansen, 2015).

For the approach here see (Chang and Keisler, 2012) and comments in (Henkin, 1996, Observation C pp 156–157).[a]

[a] (Henkin, 1996) "The Discovery of My Completeness Proof" has an interesting historical discussion, comments on the nature of mathematical discovery, and on Henkin's own indirect route to his proof of the Completeness Theorem. Observation C on pages 156,157 discusses Henkin's improvements in his proof as a result of his teaching the material. This is the essentially the proof used here in the Notes.

Chapter 4

Consequences of Completeness: Compactness, Lowenheim–Skolem

[This chapter to be completed]

Chapter 5

Gödel's Incompleteness Theorem

[This chapter to be completed]

Chapter 6

Propositional Logic

6.1 The Basics of Propositional Logic

The methods and results in this section, up to but not including Subsection 6.1.7, are a precursor to the material in Subsection 1.3.5 and subsequently for first-order logic.

6.1.1 Propositional Symbols and Formulas.

We work with a *propositional language*

$$\mathcal{P} = \{p_1, p_2, p_3, \dots\},$$

which is just a countable collection of *propositional symbols* p_i.

These symbols are combined by means of "$\neg$" (not), "$\wedge$" (and) and parentheses to form *propositional formulas* (usually denoted $\varphi, \psi, \theta, \dots$) and defined inductively to be of the following form:

- a propositional symbol p_i, or
- $(\neg\varphi)$, where φ is a propositional formula, or
- $(\varphi \wedge \psi)$, where φ and ψ are propositional formulas.

Notice there are no quantifiers.

Parentheses are usually dropped where no ambiguity arises and for ease of readability.

Remark 6.1 *(Why* $\{\neg, \wedge\}$*?).* We could use many other combinations, for example $\{\neg, \rightarrow\}$ or $\{\neg, \vee\}$. What is chosen depends on what is convenient in the particular situation.

See also subsection 6.1.7

The particular utility of $\{\neg, \rightarrow\}$ is that $\rightarrow$ corresponds more directly to $\vdash$ (*syntactic implication* and $\vDash$ (*semantic implication*). □

6.1.2 Complexity of a Propositional Formula.

In order to prove results depending on the "complexity" of a formula it is often convenient to assign an integer $c(\varphi)$ to formulas as follows:

$$\begin{aligned} c(p_i) &= 1 \quad i = 1, 2, \dots \\ c(\neg\varphi) &= 1 + c(\varphi) \\ c(\varphi \wedge \psi) &= 1 + \max\{c(\varphi),\, c(\psi)\}. \end{aligned}$$

6.1.3 Truth Values.

The following table gives the truth values associated with the standard connectives.

φ	ψ	$\neg\varphi$	$\varphi \to \psi$	$\varphi \vee \psi$	$\varphi \wedge \psi$	$\varphi \leftrightarrow \psi$	$\varphi \uparrow \psi$
T	T	F	T	T	T	T	F
T	F	F	F	T	F	F	T
F	T	T	T	T	F	F	T
F	F	T	T	F	F	T	T

6.1.4 Defined Connectives.

Columns 5, 6, 7 justify the following *definitions* of $\vee, \wedge, \leftrightarrow$ in terms of $\neg$ and $\to$:

(i) $\varphi \vee \psi \;:= \neg(\neg\varphi \wedge \neg\psi)$,

(ii) $\varphi \to \psi \;:=\; \neg(\varphi \wedge \neg\psi)$,

(iii) $\varphi \leftrightarrow \psi \;:=\; (\varphi \to \psi) \wedge (\psi \to \varphi)$.

Exercise 6.2. Verify this via truth tables applied to each side of the ":=" symbols. □

The *Sheffer Stroke* symbol $\uparrow$, can be read as "not and" or "joint denial" or "neither nor", and corresponds to the logical/electronic gate NAND. It is defined by

$$\varphi \uparrow \psi \;:=\; \neg(\varphi \wedge \psi) \;=\; \varphi \to \neg\psi.$$

Moreover, $\neg$ and $\wedge$, and hence all connectives, can similarly be defined in terms of $\uparrow$:

$$\begin{aligned} \neg\varphi &:= \varphi \uparrow \varphi, \\ \varphi \wedge \psi &:= \neg(\varphi \uparrow \psi) := (\varphi \uparrow \psi) \uparrow (\varphi \uparrow \psi), \\ \varphi \to \psi &:= \varphi \uparrow (\psi \uparrow \psi).^{1} \end{aligned}$$

Exercise 6.3. Verify these via truth tables. □

6.1.5 Truth Tables

The truth values of a propositional formula can be computed in a systematic manner using the table in subsection 6.1.3. For example, see Table 6.1 for $\varphi \to \big((\psi \vee \theta) \to (\theta \to \neg\varphi)\big)$.

Definition 6.4 (Truth Valuation). A *(truth) valuation/assignment* v is a function

$$v : \mathcal{P} = \{p_1, p_2, p_3, \dots\} \to \{T, F\}.$$

In a similar manner to that in the previous Truth Table, v *extends to all propositional formulas* φ. The value of $v(\varphi)$ depends only on $v(p_i)$ for those p_i occurring in φ, as follows by a simple induction on the complexity of formulas.

Definition 6.5 (Models).

[1] I suppose somebody somewhere found this useful at sometime.

φ	ψ	θ	$\psi \vee \theta$	$\neg\varphi$	$\theta \to \neg\varphi$	$(\psi \vee \theta) \to (\theta \to \neg\varphi)$	$\varphi \to \big((\psi \vee \theta) \to (\theta \to \neg\varphi)\big)$
T	T	T	T	F	F	F	F
T	T	F	T	F	T	T	T
T	F	T	T	F	F	F	F
T	F	F	F	F	T	T	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	T	T	T	T	T
F	F	F	F	T	T	T	T

Table 6.1: Truth table for $\varphi \to ((\psi \vee \theta) \to (\theta \to \neg\varphi))$

- $v \vDash \varphi$ means φ is true under the valuation v.
  We say v *is a model for* φ.
- If Σ is a set of propositional formulas and $v \vDash \varphi$ for all $\sigma \in \Sigma$,
  we say v *is a model for* Σ.
- $\Sigma \vDash \varphi$ means every model of Σ is a model of φ.
  That is, if all formulas in Σ are true under a valuation v, then φ is also true under the valuation v.
- $\vDash \varphi$ means φ is true in all models, (i.e. is a *tautology*).

The above dot points are analogous in first-order logic to respectively: $\mathfrak{A} \vDash \varphi$, $\mathfrak{A} \vDash \sigma$ for every $\sigma \in \Sigma$, $\Sigma \vDash \varphi$ and $\vDash \varphi$ as in Section 1.4.

Here $\mathfrak{A}$ is a structure for a first-order language $\mathcal{L}$, φ is an $\mathcal{L}$-sentence and Σ is a set of $\mathcal{L}$-sentences.

6.1.6 Tautologies

Definition 6.6. A *propositional tautology* is a propositional formula φ which takes the value T for every valuation v.

If the propositional formula A contains n distinct propositional symbols, there are 2^n possible assignments to consider, or 2^n rows as in the previous table with $n = 3$.

The truth table technique gives an algorithm for deciding of any formula whether or not it is a tautology.

6.1.7 Disjunctive Normal Form

The following theorem shows that every truth table is truth-functionally equivalent to a formula built from $\wedge, \vee, \neg$ in a particularly nice manner.

The only "exception" is that if the truth table has output F for all inputs then one has the "empty disjunction", which is always false anyway (*Why?*). We could also use $\varphi \wedge \neg\varphi$ as the relevant formula.

Theorem 6.7 (Disjunctive Normal Form). *Corresponding to every truth table whose output is not identically false, and hence corresponding to every propositional formula* *which is not a contradiction, there is a truth-functionally equivalent formula which is a disjunction of conjunctions of atomic formulas or their negations.*

Proof. For example, consider Table 6.1.

Corresponding to the six rows 2 and 4–8, for which the (φ, ψ, θ) input gives output T, consider the following propositional formula:

$$\begin{gathered}(\varphi \wedge \psi \wedge \neg\theta) \vee (\varphi \wedge \neg\psi \wedge \neg\theta) \vee (\neg\varphi \wedge \psi \wedge \theta) \vee \\ (\neg\varphi \wedge \psi \wedge \neg\theta) \vee (\neg\varphi \wedge \neg\psi \wedge \theta) \vee (\neg\varphi \wedge \neg\psi \wedge \neg\theta).\end{gathered} \tag{6.1}$$

The first disjunct is true for the input (T, T, F) and *only* this input, the second similarly for the input (T, F, F), the third for (F, T, T), the fourth for (F, T, F), the fifth for (F, F, T) and the sixth for (F, F, F).

Thus the entire disjunction is true for each input in the Truth Table which gives output T, and is false for each input which gives output F.

This method for constructing a propositional formula corresponding to a given truth table, clearly works in general. □

Remark 6.8 *(Truth-Functional Completeness).* We saw in subsection 6.1.4 that the standard connectives, including $\vee$, are definable in terms of $\neg$ and $\wedge$. So it follows from the Theorem that the pair $\{\wedge, \neg\}$ alone is truth-functionally complete. But $\neg$ will no longer be applied only to atomic formulas. □

Exercise 6.9. Show that any formula φ can be put in "Conjunctive Normal Form".

1. Do this by first applying the previous theorem to $\neg\varphi$ and then apply $\neg$ to the result.

2. Explain what is meant by "Conjunctive Normal Form". □

6.2 *Optional:* A Deductive System

Axioms. Here is a set of *Axiom Schemas for Propositional Logic*:

(i) $\varphi \to (\psi \to \varphi)$,

(ii) $\big(\varphi \to (\psi \to \theta)\big) \to \big((\varphi \to \psi) \to (\varphi \to \theta)\big)$,

(iii) $(\neg\varphi \to \neg\psi) \to (\psi \to \varphi)$,

where φ, ψ, θ are arbitrary propositional formulas.

Exercise: Check the axioms are indeed tautologies.

Rule of Inference. The *sole* rule of inference here is *modus ponens.*

- From φ and $\varphi \to \psi$, infer ψ.

Exercise: Check that modus ponens preserves tautologies.

Formal Proofs. Suppose φ is a *propositional formula* and Σ is a set of *propositional formulas*.

A *proof* of φ from Σ is a finite sequence $\varphi_1, \ldots, \varphi_n$ of *formulas* such that $\varphi_n = \varphi$ and such that each φ_i is a propositional axiom, or a member of Σ, or deducible from earlier φ_j's by means of modus ponens.

We write $\Sigma \vdash \varphi$ in such a case, and say that φ is a *theorem* of Σ, or φ is *deducible* from Σ.

If Σ is the empty set we write $\vdash \varphi$, and say φ is a *propositional theorem*.

It is trivially true that if $\Sigma \vdash \varphi$ where Σ is infinite then $\Sigma_0 \vdash \varphi$ for some *finite* $\Sigma_0 \subset \Sigma$.

Soundness Theorem. It follows from the previous two *Exercises* regarding the axioms and the rule of inference for propositional logic, that all propositional theorems are tautologies.

More generally, if $\Sigma \vdash \varphi$ and all sentences in Σ have truth value T for some set of truth values assigned to the propositional symbols occurring in Σ, then φ also has truth value T for the same assignment.

This is called the *Soundness Theorem for Propositional Logic.* It is a trivial result – we would not choose axioms which were not tautologies, nor rules of inference that did not preserve tautologies!

Completeness Theorem. We show in Section 6.4 that the converse is also true: all tautologies are theorems, i.e. are logical consequences of Axioms (i), (ii) and (iii). This is called the *Completeness Theorem for Propositional Logic.* It is *not* trivial.

However...

All Tautologies as Axioms. *We will in future allow all tautologies as axioms for propositional logic.*

This is quite reasonable as it is a mechanical procedure to decide if a propositional formula is a tautology.

Moreover, there is little point in pursuing an axiomatic approach for Hilbert propositional logic, as indicated at the beginning of Section 2

*** "Simplifying" Axiom (iii).** In some older texts Axiom (iii) is replaced by $\neg\neg\varphi \to \varphi$. See (Johnstone, 1987, Pages 7,8,11,12), (Church, 1956, Chapter 1, §10).

But this only makes sense if $\neg\varphi$ is already defined in terms of other primitives, typically $\neg\varphi := \varphi \to \bot$, where $\bot$ is a propositional constant which is interpreted as "False".

Otherwise $\neg\neg\varphi$ only gives a property of the operator $\neg\neg$, and indeed $\neg\varphi$ could then consistently be interpreted as φ and the axiom would still be satisfied, which state of affairs is certainly not intended.

6.3 *Optional:* Deduction Theorem

As remarked previously, starred sections are not part of the main pathway through to the proofs of Gödel's Completeness and Incompleteness Theorems.

In this and the following section, despite the fact that we will take all tautologies as axioms, I do go through the details of deriving the tautologies from the axioms in Section 6.2. Because:

- It is (sort of) fun.
- It should be part of your training.
- Many texts do it.
- The ideas are useful in the proof of the Completeness Theorem for first-order logic.

Deductions from the Axioms. Here are some examples of proofs from the axioms of propositional logic.

Example 1. $\vdash \varphi \to \varphi$

$$\begin{array}{lll}
1. & \big(\varphi \to \big((\varphi \to \varphi) \to \varphi\big)\big) \to \big(\big(\varphi \to (\varphi \to \varphi)\big) \to (\varphi \to \varphi)\big) & \text{axiom (ii)} \\
2. & \varphi \to \big((\varphi \to \varphi) \to \varphi\big) & \text{axiom (i)} \\
3. & \big(\varphi \to (\varphi \to \varphi)\big) \to (\varphi \to \varphi) & \text{modus ponens on 1, 2} \\
4. & \varphi \to (\varphi \to \varphi) & \text{axiom (i)} \\
5. & \varphi \to \varphi & \text{modus ponens on 3, 4}
\end{array}$$

Example 2. $\varphi \to \psi,\ \psi \to \theta \vdash \varphi \to \theta$

$$\begin{array}{lll}
1. & \big(\varphi \to (\psi \to \theta)\big) \to \big((\varphi \to \psi) \to (\varphi \to \theta)\big) & \text{axiom (ii)} \\
2. & \psi \to \theta & \text{hypothesis} \\
3. & (\psi \to \theta) \to \big(\varphi \to (\psi \to \theta)\big) & \text{axiom (i)} \\
4. & \varphi \to (\psi \to \theta) & \text{modus ponens on 2, 3} \\
5. & (\varphi \to \psi) \to (\varphi \to \theta) & \text{modus ponens on 1, 4} \\
6. & \varphi \to \psi & \text{hypothesis} \\
7. & \varphi \to \theta & \text{modus ponens on 5, 6}
\end{array}$$

Remarks re the Deduction Theorem.

1. The Deduction Theorem (to follow) shows that syntactic provability ($\vdash$) "acts like" logical implication ($\to$).

2. The Deduction Theorem simplifies *formal* proofs from the axioms in propositional logic. Consider the previous two examples.

   Example 1. To show that $\vdash \varphi \to \varphi$, by the Deduction Theorem it is sufficient to show $\varphi \vdash \varphi$, which is immediate.

   Example 2. To show
   $$\varphi \to \psi,\ \psi \to \theta \vdash \varphi \to \theta,$$
   using the Deduction Theorem it is sufficient to show that
   $$\varphi \to \psi,\ \psi \to \theta,\ \varphi \vdash \theta.$$
   But this is immediate by two applications of modus ponens.

3. There is nothing very profound about the following proof of the Deduction Theorem. We simply made sure there were enough axioms for the proof, and for the proof of the Completeness Theorem which uses the Deduction Theorem, to go through.

4. Notice that the proof of the Deduction Theorem only uses Axioms (i) and (ii), and not Axiom (iii).

Deduction Theorem. If Σ is a set of propositional formulas, and φ and ψ are propositional formulas, then

$$\Sigma \cup \{\varphi\} \vdash \psi \quad \text{iff} \quad \Sigma \vdash \varphi \to \psi.$$

Proof

(a) Suppose $\Sigma \vdash \varphi \to \psi$, with proof

$$\theta_1\,, \ldots\,, \theta_n\,(=\varphi \to \psi).$$

Then, using modus ponens,

$$\theta_1\,, \ldots\,, \;\theta_{n-1}\,, (\theta_n =)\,\varphi \to \psi,\; \varphi\,,\; \psi\,,$$

is a proof for $\Sigma \cup \{\varphi\} \vdash \psi$.

(b) Suppose $\Sigma \cup \{\varphi\} \vdash \psi$, with proof

$$\psi_1\,, \ldots\,, \psi_n\,(=\psi).$$

We show by induction that there is a proof of $\Sigma \vdash \varphi \to \psi_i$ for each i .

(i) If ψ_i is an axiom or $\psi_i \in \Sigma$, then by Axiom (i) and modus ponens,

$$\psi_i,\; \psi_i \to (\varphi \to \psi_i),\; \varphi \to \psi_i$$

is a proof for $\Sigma \vdash \varphi \to \psi_i$.

(ii) If $\psi_i = \varphi$, then $\Sigma \vdash \varphi \to \psi_i$ since we saw a five line proof of $\vdash \varphi \to \varphi$ in the previous Example 1.

(iii) If ψ_i is deduced by modus ponens from ψ_j and from $\psi_k = \psi_j \to \psi_i$ $(j, k < i)$, let

$$S_1\,, S_2\,, \ldots\,, S_n,\; \varphi \to \psi_j$$

be the proof for $\Sigma \vdash \varphi \to \psi_j$, and let

$$S'_1\,, S'_2\,, \ldots\,, S'_m,\; \varphi \to (\psi_j \to \psi_i)$$

be the proof for $\Sigma \vdash \varphi \to (\psi_j \to \psi_i)$. Then the following is a proof for $\Sigma \vdash \varphi \to \psi_i$:

$$\begin{aligned}
&S_1, \ldots, S_n,\; \varphi \to \psi_j, \\
&S'_1, \ldots, S'_m,\; \varphi \to (\psi_j \to \psi_i), \\
&\big(\varphi \to (\psi_j \to \psi_i)\big) \to \big((\varphi \to \psi_j) \to (\varphi \to \psi_i)\big), && \text{(logical axiom (ii))} \\
&(\varphi \to \psi_j) \to (\varphi \to \psi_i), && \text{(modus ponens)} \\
&\varphi \to \psi_i. && \text{(modus ponens)}
\end{aligned}$$

More Deductions via the Deduction Theorem.

Example 3. $\vdash \neg\varphi \to (\varphi \to \psi)$, (equivalently by the Deduction Theorem) $\neg\varphi \vdash \varphi \to \psi$, and (again equivalently) $\{\varphi, \neg\varphi\} \vdash \psi$.

Take the hypothesis $\neg\varphi$.

1.	$\neg\varphi$	hypothesis
2.	$\neg\varphi \to (\neg\psi \to \neg\varphi)$	axiom (i)
3.	$\neg\psi \to \neg\varphi$	modus ponens on 1, 2
4.	$(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$	axiom (iii)
5.	$\varphi \to \psi$	modus ponens on 3, 4

Hence $\neg\varphi \vdash \varphi \to \psi$ and so $\vdash \neg\varphi \to (\varphi \to \psi)$.

Example 4. $\vdash \neg\neg\varphi \to \varphi$, or equivalently by the Deduction Theorem, $\neg\neg\varphi \vdash \varphi$.

Take the hypothesis $\neg\neg\varphi$.

1.	$\vdash \neg\varphi \to \neg\neg\neg\varphi$	previous example with $\varphi \mapsto \neg\varphi,\ \psi \mapsto \neg\neg\neg\varphi$
2.	$(\neg\varphi \to \neg\neg\neg\varphi) \to (\neg\neg\varphi \to \varphi)$	axiom (iii)
3.	$\neg\neg\varphi \to \varphi$	modus ponens on 1, 2
4.	$\neg\neg\varphi$	hypothesis
5.	φ	modus ponens on 3, 4

Hence $\neg\neg\varphi \vdash \varphi$ and so $\vdash \neg\neg\varphi \to \varphi$.

Example 5. $\vdash \varphi \to \neg\neg\varphi$, or equivalently by the Deduction Theorem, $\varphi \vdash \neg\neg\varphi$.

1.	$\vdash \neg\neg\neg\varphi \to \neg\varphi$	previous example with $\varphi \mapsto \neg\varphi$
2.	$(\neg\neg\neg\varphi \to \neg\varphi) \to (\varphi \to \neg\neg\varphi)$	axiom (iii)
3.	$\varphi \to \neg\neg\varphi$	modus ponens on 1, 2

Hence $\vdash \varphi \to \neg\neg\varphi$ and so $\varphi \vdash \neg\neg\varphi$.

6.4 *Optional:* Completeness Theorem

Overview Our goal in this section is to prove that syntactic implication is equivalent to semantic implication

That is,

$$\Sigma \vdash \varphi \quad \Longleftrightarrow \quad \Sigma \models \varphi.$$

"A propositional formula φ is deducible from a set Σ of propositional formulas, using just the logical axioms (i), (ii) and (iii) and modus ponens, iff φ is true in all models of Σ."

The direction $\Longrightarrow$ says that the logical axioms and modus ponens are not absurd. It is called the Soundness Theorem and was discussed in Section 6.2.

The direction $\Longleftarrow$ is much deeper and says that the logical axioms and modus ponens are sufficiently strong to prove from Σ *every* semantic consequence of Σ.

Falsum In the following we could take $\perp$ ("falsum" or "absurdity" or "contradiction") to be the negation of any of the axioms in Section 6.2, or one of their consequences. The truth table for any such formula has output F (false) for all truth value inputs.

For simplicity we define

$$\perp := \neg(p_1 \to p_1),$$

where p_1 was the first propositional symbol.

In the following $\varphi, \psi, \theta, \ldots$ are propositional formulas and Σ is a set of propositional formulas.

Definition 6.10. Σ is *consistent* if $\Sigma \nvdash \perp$. Σ is *inconsistent* if $\Sigma \vdash \perp$.

Theorem 6.11. *Σ is consistent iff every finite subset of Σ is consistent.*

Proof. Trivial, since proofs are finite. □

Theorem 6.12. *The following are equivalent:*

1. *Σ is inconsistent, i.e. $\Sigma \vdash \perp$,*
2. *There is some φ such that $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$,*
3. *For every φ, $\Sigma \vdash \varphi$.*

Proof. ($1 \implies 2$): Take $\varphi = p_1 \to p_1$. Then $\Sigma \vdash \varphi$ since $\vdash p_1 \to p_1$ from Example 1 in Section 6.3, and $\Sigma \vdash \neg\varphi$ by the definition of inconsistent.

($2 \implies 3$): Assume 2, and note from Example 3 in Section 6.3 that $\{\varphi, \neg\varphi\} \vdash \psi$ (for any ψ). Concatenating the proofs of $\Sigma \vdash \varphi$, $\Sigma \vdash \neg\varphi$ and $\{\varphi, \neg\varphi\} \vdash \psi$, gives a proof of $\Sigma \vdash \psi$.

($3 \implies 1$): Let $\varphi = p_1 \to p_1$. □

Corollary 6.13. *The following are equivalent:*

1. *Σ is consistent, i.e. $\Sigma \nvdash \perp$,*
2. *There is no φ such that $\Sigma \vdash \varphi$ and $\Sigma \vdash \neg\varphi$,*
3. *There is at least one φ such that $\Sigma \nvdash \varphi$.*

Proof. Immediate by the previous theorem. □

The following connects consistency and provability.

Theorem 6.14.

$$\begin{aligned} \Sigma \cup \{\neg\varphi\} \text{ \textit{is inconsistent} } &\iff \Sigma \vdash \varphi, \\ \Sigma \cup \{\varphi\} \text{ \textit{is inconsistent} } &\iff \Sigma \vdash \neg\varphi. \end{aligned}$$

Proof.

$$\begin{aligned} \Sigma \cup \{\neg\varphi\} \text{ inconsistent } &\implies \Sigma \cup \{\neg\varphi\} \vdash \neg(p_1 \to p_1) && \text{using } \perp := \neg(p_1 \to p_1) \\ &\implies \Sigma \vdash \neg\varphi \to \neg(p_1 \to p_1) && \text{deduction theorem} \\ &\implies \Sigma \vdash (p_1 \to p_1) \to \varphi && \text{axiom (iii)} \\ &\implies \Sigma \vdash \varphi && \text{example 1, modus ponens} \end{aligned}$$

Conversely, if $\Sigma \vdash \varphi$ then both $\Sigma \cup \{\neg\varphi\} \vdash \varphi$ and $\Sigma \cup \{\neg\varphi\} \vdash \neg\varphi$. By the previous Theorem this implies $\Sigma \cup \{\neg\varphi\}$ is inconsistent.

Replacing φ by $\neg\varphi$, $\Sigma \cup \{\neg\neg\varphi\}$ is inconsistent iff $\Sigma \vdash \neg\varphi$. But $\varphi \vdash \neg\neg\varphi$ and $\neg\neg\varphi \vdash \varphi$ by Examples 4 & 5 in Section 6.3, so $\Sigma \cup \{\neg\neg\varphi\}$ is inconsistent iff $\Sigma \cup \{\varphi\}$ is inconsistent.

This completes the proof. □

Corollary 6.15.

$$\begin{aligned} \Sigma \cup \{\neg\varphi\} \text{ is consistent } &\iff \Sigma \nvdash \varphi, \\ \Sigma \cup \{\varphi\} \text{ is consistent } &\iff \Sigma \nvdash \neg\varphi. \end{aligned}$$

Theorem 6.16. *Suppose Σ is a consistent set of propositional formulas and φ is any propositional formula. Then at least one of $\Sigma \cup \{\varphi\}$ and $\Sigma \cup \{\neg\varphi\}$ is consistent.*

Proof. If both $\Sigma \cup \{\varphi\}$ and $\Sigma \cup \{\varphi\}$ are inconsistent, then $\Sigma \vdash \neg\varphi$ and $\Sigma \vdash \varphi$ by Theorem 6.14. By Theorem 6.12, Σ is inconsistent. Contradiction. □

The following is a key concept for proving the Completeness Theorem.

Definition 6.17. Σ is *maximal consistent* if

- Σ is consistent,
- $\Sigma \subseteq \widetilde{\Sigma}$ and $\widetilde{\Sigma}$ consistent $\implies \Sigma = \widetilde{\Sigma}$.

Theorem 6.18. *Suppose Σ is a consistent set of propositional formulas. Then Σ can be extended to a maximal consistent set $\widetilde{\Sigma}$.*

Proof. Let $\varphi_1, \varphi_2, \varphi_3, \dots$ be an enumeration of all propositional formulas. Define

$$\begin{aligned} \Sigma_1 &= \Sigma, \\ \Sigma_{n+1} &= \begin{cases} \Sigma_n \cup \{\varphi_n\} & \text{if } \Sigma_n \cup \{\varphi_n\} \text{ is consistent,} \\ \Sigma_n & \text{otherwise,} \end{cases} \\ \widetilde{\Sigma} &= \bigcup_{n \geq 1} \Sigma_n. \end{aligned}$$

Each Σ_n is consistent by construction. Moreover $\widetilde{\Sigma}$ is consistent, since if $\widetilde{\Sigma} \vdash \bot$ then $\Sigma_n \vdash \bot$ for some n since derivations are finite in length. But this is a contradiction.

To see that $\widetilde{\Sigma}$ is *maximal* consistent, suppose $\widetilde{\Sigma} \cup \{\varphi\}$ is consistent. Then $\varphi = \varphi_n$ for some n, and because $\Sigma_n \cup \{\varphi_n\}$ must also be consistent it follows by construction that $\varphi_n \in \Sigma_{n+1}$. Hence $\varphi \in \widetilde{\Sigma}$ and so $\widetilde{\Sigma}$ is maximal consistent. □

The next result shows that a maximal consistent set of sentences is closed under deductions.

Theorem 6.19. *If Σ is maximal consistent, then $\Sigma \vdash \varphi$ implies $\varphi \in \Sigma$.*

Proof. If $\varphi \notin \Sigma$ then by definition of *maximal* consistent $\Sigma \cup \{\varphi\}$ is not consistent. Hence $\Sigma \vdash \neg\varphi$, and so Σ is inconsistent by Theorem 6.12. □

Theorem 6.20. *If Σ is maximal consistent, then for every φ exactly one of the following holds: $\varphi \in \Sigma$ or $\neg\varphi \in \Sigma$.*

Proof. They cannot both hold since Σ is consistent.

If $\varphi \notin \Sigma$ then $\Sigma \cup \{\varphi\}$ is inconsistent and so $\Sigma \vdash \neg\varphi$ by Theorem 6.12. But then $\neg\varphi \in \Sigma$ by Theorem 6.19. □

Theorem 6.21. *If Σ is maximal consistent then*

$$(\varphi \to \psi) \in \Sigma \quad \iff \quad (\varphi \in \Sigma \implies \psi \in \Sigma)$$

Proof. If $(\varphi \to \psi) \in \Sigma$ and $\varphi \in \Sigma$, then $\Sigma \vdash \varphi \to \psi$ and $\Sigma \vdash \varphi$.
Hence $\Sigma \vdash \psi$ by modus ponens, and so $\psi \in \Sigma$ by Theorem 6.19.

Conversely, suppose $\varphi \in \Sigma \Rightarrow \psi \in \Sigma$. Then $\Sigma \vdash \varphi \Rightarrow \Sigma \vdash \psi$.
Consider the two cases $\varphi \in \Sigma$ and $\varphi \notin \Sigma$

1. If $\varphi \in \Sigma$ then $\Sigma \vdash \varphi$, and so $\Sigma \vdash \psi$.
   But $\vdash \psi \to (\varphi \to \psi)$ by axiom (i).
   So $\Sigma \vdash \varphi \to \psi$ by modus ponens, and so $\varphi \to \psi \in \Sigma$ by Theorem 6.19
2. If $\varphi \notin \Sigma$ then $\neg\varphi \in \Sigma$ and so $\Sigma \vdash \neg\varphi$.
   Hence $\Sigma \vdash \neg\psi \to \neg\varphi$, again by axiom (i) and modus ponens.
   Hence $\Sigma \vdash \varphi \to \psi$ by axiom (iii) and modus ponens.
   Hence $(\varphi \to \psi) \in \Sigma$ by Theorem 6.19. □

Theorem 6.22. *Suppose Σ is maximal consistent. Let v be the valuation on propositional symbols p_n defined by*

$$v(p_n) = \begin{cases} T & \text{if } p_n \in \Sigma, \\ F & \text{if } p_n \notin \Sigma. \end{cases}$$

Using the primitive connectives "$\neg$" and "$\to$", extend v to a valuation V on all propositional formulas via induction on formula complexity and using truth tables.

Then

$$V(\chi) = \begin{cases} T & \text{if } \chi \in \Sigma, \\ F & \text{if } \chi \notin \Sigma. \end{cases}$$

Proof. The result is true by definition if χ is p_n for some n.

By Theorem 6.20, $\neg\varphi \in \Sigma$ iff $\varphi \notin \Sigma$. It follows from the truth table for $\neg\varphi$ that the result is true for $\neg\varphi$ if it is true for φ.

Assuming the result true for φ and ψ, and using Theorem 6.21

$$\begin{array}{llll} V(\varphi \to \psi) = T & \text{iff} & V(\varphi) = T \implies V(\psi) = T & \text{truth tables} \\ & \text{iff} & \varphi \in \Sigma \implies \psi \in \Sigma & \text{inductive hypothesis} \\ & \text{iff} & (\varphi \to \psi) \in \Sigma & \text{Theorem 6.21} \end{array}$$

The result now follows by induction on formula complexity. □

Theorem 6.23 (Model Existence Theorem). *Σ is consistent $\iff$ Σ has a model.*

Proof. For $\impliedby$ suppose Σ has a model, but Σ is inconsistent and so $\Sigma \vdash \bot$. By the Soundness theorem $\Sigma \models \bot$. But $\neg\bot$ must be true in the model since it is an axiom. Contradiction.

For $\implies$ suppose Σ is consistent and extend Σ to a maximal consistent set and apply the previous theorem. □

Theorem 6.24 (Completeness Theorem). *$\Sigma \models \varphi \iff \Sigma \vdash \varphi$.*

Proof. The $\Longleftarrow$ direction is just the Soundness Theorem.
For the opposite direction suppose $\Sigma \nvdash \varphi$.
Then $\Sigma \cup \{\neg\varphi\}$ is consistent by Theorem 6.14.
Therefore $\Sigma \cup \{\neg\varphi\}$ has a model by Theorem 6.23.
Therefore $\Sigma \not\models \varphi$ by the very meaning/definition of $\Sigma \models \varphi$.
This completes the proof. □

Chapter 7

Computability

7.1 Introduction

In this Introduction I discuss just enough material on computability to prove the various versions of Gödel's Incompleteness Theorems in Chapter 5.

The Introduction also serves as an introduction to the rest of this chapter.

7.1.1 Primitive Recursive Functions and Relations

We begin with a formal definition of a primitive recursive function, but soon move to a more convenient approach.

Definition 7.1. The following functions $f : \mathbb{N}^n \to \mathbb{N}$ $(n \geq 1)$ are *initial functions*:

- the *zero functions*, $O_n(x_1, \dots, x_n) = 0$ for $n \geq 1$,
- the *successor function* $S(x) = x + 1$,
- the *projection functions* $p_i^n(x_1, \dots, x_n) = x_i$ for $1 \leq i \leq n$.

The function $f : \mathbb{N}^n \to \mathbb{N}$ $(n \geq 1)$ is *obtained by composition* from $h, g_1, \dots, g_p$, if

$$f(x_1, \dots, x_n) = h\Big(g_1(x_1, \dots, x_n), \dots, g_p(x_1, \dots, x_n)\Big).$$

The function $f : \mathbb{N}^{n+1} \to \mathbb{N}$ $(n \geq 0)$ is *obtained by primitive recursion* from g and h if

$$\begin{aligned} &f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n), \\ &f(x_1, \dots, x_n, y) = h(x_1, \dots, x_n, y, f(x_1, \dots, x_n, y-1)) \quad \text{(for all } y \geq 1). \end{aligned} \tag{7.1}$$

Definition 7.2 (Primitive Recursive). A function $f : \mathbb{N}^n \to \mathbb{N}$ is *primitive recursive* if it is an initial function, or is obtained from primitive recursive functions by composition or by primitive recursion.

Equivalently, the function f is *primitive recursive* if there is a sequence of functions $f_1, f_2, \dots, f_k$ such that f is f_k and such that each f_j is an initial function or is obtained from previous f_i by composition or primitive recursion.

A set $R \subseteq \mathbb{N}^k$ is *primitive recursive* iff its characteristic function χ_R is primitive recursive.

Remark 7.3 *(Primitive Recursive and Computability).* Clearly a primitive recursive function is computable in the informal sense.

On the other hand, we can give an algorithm for listing all primitive recursive functions (e.g. first list all appropriate sequences of length 10 in which all functions are at most 10-ary, then those of length 20 in which all functions are at most 20-ary, etc.). From this we can effectively list all unary primitive recursive functions.

Let $\varphi(n) = \varphi_n(n) + 1$ where φ_n is the n^{th} unary primitive recursive function. Clearly φ is computable but not primitive recursive.

Thus the primitive recursive functions are a proper subset of the set of all computable functions. (Although we have yet to give a precise definition of this latter set.) □

Remark 7.4 *(Diagonalisation).* □

For simple examples see Proposition 7.6. Each of the functions $x + y$, $x \cdot y$, x^y, $x!$, and $x \dot{-} y$ is obtained from previous functions in the list by composition and primitive recursion.

In fact, it is difficult to define a function $f : \mathbb{N}^n \to \mathbb{N}$ which is not primitive recursive. (Although we will soon do so!). In particular, any built in function

The following Proposition provides a most convenient w

computed by a computer program which involves (bounded) for loops but does not involve (potentially) unbounded while loops.

When entering a loop of the form "for y do p", the value of the variable y is determined, and the program p is executed that many times. Assignment to the variable y within the body of the loop does not change the number of times the loop is executed, nor does execution of the body of the loop alone decrement y or change its value in any way except by explicit assignment.

7.1.2 The Programming Perspective on Recursive Functions

Both primitive recursive and general recursive functions can be cleanly formulated in terms of *for* loops and *while/until* loops. The idea seems to go back to the

7.1.3 Examples of Primitive Recursive Functions

Definition 7.5. Non-negative subtraction is defined by

$$x \dot{-} y = \max\{0, x - y\}. \tag{7.2}$$

Proposition 7.6. *The following functions are primitive recursive*

$$x + y,\ x \cdot y,\ x^y,\ x!,\ x \dot{-} y$$

7.2 Ackermann Function

7.2.1 History

The *Ackermann function* $A : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ is computable and is defined for *all* $m, n \in \mathbb{N} \times \mathbb{N}$, but it is *not* primitive recursive. It was introduced in 1928 by Ackermann, working on

Hilbert's program, in order to show the existence of a "computable" function which was not captured by the concept of primitive recursive. At that time the precise notion of a computable function was unknown.

The version of the Ackermann function which is essentially the one used here, was introduced independently by Rózsa Péter and Raphael Robinson in the early 1930s.

7.2.2 Applicatons

The Ackermann function $A(m,n)$ is the beginning of the theory of rapidly growing functions.

It occurs in term rewriting systems and termination proofs within the computer science study of algorithms, and arises in the ordinal analysis of hierarchies of consistency proofs for Peano Arithmetic and set theory.

The associated unary (diagonal) function is $A(n) := A(n,n)$. As we will see it is monotonically increasing and grows faster than any primitive recursive function.

Its (functional) inverse[1] is an extremely slowly growing function, essentially constant in any system of units, and is used in the analysis of disjoint-set data structures.

For a "light" discussion of computing $A(m,n)$ see "The Most Difficult Program to Compute?". For the program itself see Ackermann Function.

7.2.3 The Sequence of Unary Ackermann Functions

As discussed in the next two subsections, the two-variable Ackermann function $A(m,n)$ can be seen as a sequence of one-variable functions $A_m(n) := A(m,n)$ for $m,n \in \mathbb{N}$.

In Definition 7.12 we define the functions A_m independently of A, using the standard iterated function notation

$$f^{(n)}(x) \;:=\; \overbrace{f \circ f \circ \cdots \circ f}^{n \text{ times appy } f}(x). \tag{7.3}$$

The following definition is motivated by the Remark which follows it. See also Figure 7.1.

Definition 7.7 (Ackermann Sequence). The sequence of functions $A_m : \mathbb{N} \to \mathbb{N}$ is given by

$$A_1(0) = 2,\ A_2(0) = 0,\ A_m(0) = 1 \text{ if } m \geq 3 \tag{7.4}$$

$$A_0(n) = n + 1 \qquad n \geq 0 \tag{7.5}$$

$$A_m(n) = A_{m-1}^{(n)}(A_m(0)) \qquad m \geq 1,\ n \geq 1 \tag{7.6}$$

Remark 7.8 *(Notes on the Definition).*

- A_0 is the successor function.

[1] The functional inverse A^{-1} is defined by

$$A^{-1}(y) = \max\{x : A(x) \leq y\}, \quad \text{that is} \quad x \leq A^{-1}(y) \Longleftrightarrow A(x) \leq y.$$

If one computation where done every nanosecond, and since it can be shown that the number of computations needed for $A(x)$ is comparable to $A(x)$, the function A^{-1} would equal 5 from just after the big bang to far beyond the big crunch. See Figure 7.1.

- The conditions in (7.4) and (7.5) can be regarded as "boundary" conditions, see Figure 7.1.

- The values in (7.4) are chosen here so that A_1, A_2 and A_3 agree with addition, multiplication and exponentiation from the base 2 — see the following comments for these three functions.[2]

- For $m \geq 1$ and $n \geq 1$, $A_m(n)$ is defined by iterating n times the function A_{m-1} applied to $A_m(0)$.

- In particular, for $n \geq 1$, $A_1(n)$ is obtained by starting with $A_1(0) = 2$ and *iterating* n times the *successor* function A_0. So A_1 is the *add 2* function $n \mapsto n + 2$.

- For $n \geq 1$, $A_2(n)$ is obtained by starting with $A_2(0) = 0$ and *iterating* n times the *add 2* function A_1. So A_2 is the *multiply by 2* function $n \mapsto n \cdot 2$.

- For $n \geq 1$, $A_3(n)$ is obtained by starting with $A_3(0) = 1$ and *iterating* n times the *multiply by 2* function A_2. So A_3 is the *exponentiation from 2* function $n \mapsto 2^n$.

- For $n \geq 1$, $A_4(n)$ is obtained by starting with $A_4(0) = 1$ and *iterating* n times the *exponentiation from 2* function A_3. So A_4 is the *tetration from 2* function defined by $A_4(0) = 1$, and for $n \geq 1$, $A_4(n) := \left.2^{2^{\cdot^{\cdot^{\cdot^{2}}}}}\right\}$ (tower of 2's of height n).

- For $n \geq 1$, $A_5(n)$ is obtained by starting with $A_5(0) = 1$ and *iterating* n times the *tetration from 2* function A_4.

  To gain some idea of this, note that $A_4 \circ A_4(k)$ is the value of a tower of 2's whose height iself is given by the value of a further tower of 2's of height k. You might call this tower of towers a *power tower.*

- etc. (I think it impossible to wrap one's head around the size of these numbers – and this is barely the start of what is possible, that is, is "impossible"!) □

Remark 7.9 *(Explosive Blow-Up).* These functions grow faster and faster, with explosive blow-up quite soon. See Figure 7.1.

The growth behaviour of the A_m will become clearer after we discuss the Knuth Up-Arrow 7.2.5 notation .

Exercise 7.10. Explain in Figure 7.1 the following:

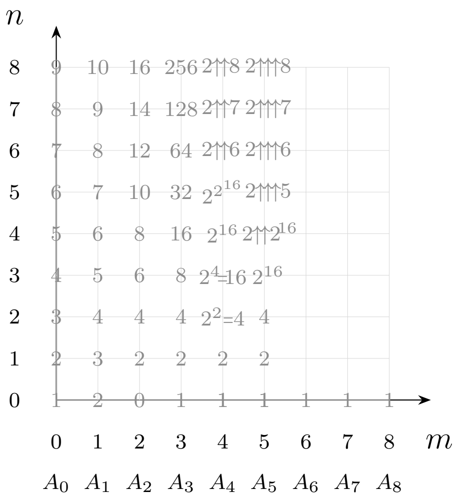
1. $A_4(6) = 2{\uparrow\uparrow}6 = 2^{2^{65{,}536}}$ has more than $0.3 \times 2^{65{,}536}$ *digits* written in base 10.

2. $A_5(5) = A_4^{(5)}(1) = 2 \uparrow\uparrow (2 \uparrow\uparrow 16)$ is inconceivable.

Proposition 7.11. *The A_m are Primitive Recursive.*

[2] You will find other conventions, but this does not any significant difference. In some cases it is just a matter of subtracting the number 3 from $A_m(n)$, which in the circumstances is about as trivial a change as possible!

Ackermann Function Table



n										
8	9	10	16	256	$2{\uparrow\uparrow}8$	$2{\uparrow\uparrow\uparrow}8$				
7	8	9	14	128	$2{\uparrow\uparrow}7$	$2{\uparrow\uparrow\uparrow}7$				
6	7	8	12	64	$2{\uparrow\uparrow}6$	$2{\uparrow\uparrow\uparrow}6$				
5	6	7	10	32	$2^{2^{16}}$	$2{\uparrow\uparrow\uparrow}5$				
4	5	6	8	16	2^{16}	$2{\uparrow\uparrow}2^{16}$				
3	4	5	6	8	$2^4=16$	2^{16}				
2	3	4	4	4	$2^2=4$	4				
1	2	3	2	2	2	2				
0	1	2	0	1	1	1	1	1	1	
	0	1	2	3	4	5	6	7	8	m
	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	

The values of the successor function $A_0(n) = S(n) = n + 1$ are in the column above A_0.
Similarly $A_1(n) = 2 + n$, $A_2(n) = 2 \cdot n$, $A_3(n) = 2^n$.

Using the Knuth up-arrow notation,
$A_3(n) = 2{\uparrow}n$, $A_4(n) = 2{\uparrow\uparrow}n$,
$A_5(n) = 2{\uparrow\uparrow\uparrow}n$, $A_6(n) = 2{\uparrow\uparrow\uparrow\uparrow}n$, $\ldots$

$A_4(6) = 2 \uparrow\uparrow 6 = 2^{2^{65,536}}$ has more than $0.3 \times 2^{65,536}$ *digits* written in base 10.

$A_5(5) = A_4^{(5)}(1) = 2 \uparrow\uparrow (2 \uparrow\uparrow 16)$, which is inconceivable.

Figure 7.1: Ackermann function $A_m(n) =: 2 \uparrow^{m-2} n$.

Proof. Following the format of (7.1), for $m \geq 1$,

$$A_m(0) = \begin{cases} 2 & m = 1 \\ 0 & m = 2 \\ 1 & m \geq 3 \end{cases}$$
$$A_m(n) = A_{m-1}(A_m(n-1)) \quad n \geq 1.$$

So A_m is defined by primitive recursion from A_{m-1} for $m \geq 1$. But A_0 is just the successor function and so is primitive recursive. Hence A_m is primitive recursive for each m.[3] □

By way of contrast, the functions $A(m, n) = A_m(n)$ and the diagonal function $A(n, n)$ are computable but *not* primitive recursive. We will prove this by examining the growth rates of primitive recursive functions and of the A_m.

Moreover, although there is not a primitive recursive definition of $A(m, n)$ there is a definition of $A(m, n)$ by a double/simultaneous recursion on (m, n). See Definition 7.7.

7.2.4 Computing the Ackermann Sequence

Each A_m is primitive recursive. Here is the high level program to compute A_5.

Note that the program consists of *nested primitive recursions*, three levels deep in this case, and $m - 2$ levels deep for A_m, if we take exponentiation as a built-in function.

Program	**Explanation**
Outer loop: calculate $A_5(n)$	

[3] We have already essentially seen this for $m = 1, 2, 3$ in Proposition 7.6.

Program | **Explanation**

```
Input $n$
  $x := 1$
For $i = 1, \dots, n$
  $x := A_4(x)$ (call subroutine)
$\Longrightarrow$ Output $x := A_5(n)$
```

Defines a sequence $(x_i)_{0 \le i \le n}$ by

$$x_0 = 1; \quad x_i = A_4^{(i)}(1) = A_5(i), \ 1 \le i \le n.$$

Middle loop: calculate $A_4(x)$

```
Input $x$
  $y := 1$
For $j = 1, \dots, x$
  $y := A_3(y)$ (call subroutine)
$\Longrightarrow$ Output $y := A_4(x)$
```

Defines a sequence $(y_j)_{0 \le j \le x}$ by

$$y_0 = 1; \quad y_j = A_3^{(j)}(1) = A_4(i), \ 1 \le j \le x.$$

$A_4(x)$ is a power tower of 2's of height x.

$$A_4(x) = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \Big\} \text{(tower of } x \text{ 2's)} =: 2 \uparrow\uparrow x$$

Innermost loop: calculate $A_3(y)$

```
Input $y$
  $z := 1$
For $k = 1, \dots, y$
  $z := 2 \cdot z$
$\Longrightarrow$ Output $z := A_3(y)$
```

Defines a sequence $(z_k)_{0 \le k \le y}$ by

$$z_0 = 1; \quad z_k = 2^k, \ 1 \le k \le y.$$

$A_3(y) = 2^y =: 2 \uparrow y$. (which is normally a built in function)

Output

```
return x
```

The output is $x_n = A_5(n) = 2 \uparrow\uparrow\uparrow n$.

7.2.5 Knuth Up-Arrow Notation

The up-arrow notation due to Knuth is very useful. In particular

$$\begin{aligned} 2 \uparrow n &:= 2^n = A_3(n) \\ 2 \uparrow\uparrow n &:= A_4(n) \\ 2 \uparrow\uparrow\uparrow n &:= A_5(n) \\ &\text{etc.} \end{aligned}$$

Note that

$$2 \uparrow\uparrow n = \overbrace{2 \uparrow (2 \uparrow \dots (2 \uparrow 2) \dots)}^{n \text{ copies of } 2}$$

$$2 \uparrow\uparrow\uparrow n = \overbrace{2 \uparrow\uparrow (2 \uparrow\uparrow \dots (2 \uparrow\uparrow 2) \dots)}^{n \text{ copies of } 2}$$

$$2 \uparrow\uparrow\uparrow\uparrow n = \overbrace{2 \uparrow\uparrow\uparrow (2 \uparrow\uparrow\uparrow \dots (2 \uparrow\uparrow\uparrow 2) \dots)}^{n \text{ copies of } 2}$$

and so on.

The role of 2 is not critical. Any integer $k \geq 2$ could be used, giving an Ackermann function with the additional parameter k. The growth rates are comparable.

See the Wiki article Knuth's Up-Arrow Notation.

7.2.6 Binary Function Formulation

The Ackermann Function is usually defined as a function $A(m, n)$ of two variables, (or with an additional parameter) even as a function of three variables, rather than as a sequence of unary functions A_m.

Whereas the individual A_m are primitive recursive from Proposition 7.11, the function $A(m, n)$ is computable but is *not* primitive recursive 7.2.7.

Definition 7.12 (Ackermann Function). For $m, n \in \mathbb{N}$, $A(m, n)$ is defined by

$$A(0, n) = \quad n + 1 \tag{7.7}$$

$$A(m, 0) = \begin{cases} 1 & m = 0 \\ 2 & m = 1 \\ 0 & m = 2 \\ 1 & m \geq 3 \end{cases} \tag{7.8}$$

$$A(m, n) = \quad A\big(m - 1, A(m, n - 1)\big) \qquad\qquad m, n \geq 1. \tag{7.9}$$

$A(m, n)$ is thus defined by double/simultaneous recursion on m and n, with the ordering

$$(m_1, n_1) \prec (m_2, n_2) \quad \iff \quad m_1 < m_2 \text{ or } (m_1 = m_2 \text{ and } n_1 < n_2). \tag{7.10}$$

This is the lexicographic well-ordering on $\omega \times \omega$, which in Figure 7.1 can be seen as first proceeding up the n-axis from $(0, 0)$, then up the parallel vertical line from $(1, 0)$, then up from $(2, 0)$, etc.

It should now be clear from Definition 7.7 that $A(m, n)$ is well-defined for all $m, n \in \mathbb{N}$.

Exercise 7.13. Why is $A(m, n) = A_m(n)$, using Definitions 7.7 and 7.12 respectively ?

Exercise 7.14. Why is "$\prec$" called "lexicographic" ?

Exercise 7.15. Explain why "$\prec$" is a well-ordering in terms of the "no infinite descending sequence" property.

Exercise 7.16. Fill in the missing values for A_6, A_7, A_8 in Figure 7.1.

7.2.7 The Ackermann Function is Not Primitive Recusive

[This chapter to be completed]

Chapter 8

Peano Axioms and Arithmetic

8.1 Formal Number Theory

Apart from the usual logical symbols, our language $\mathcal{L}$ will contain two binary function symbols $+$ (plus) and $\cdot$ (times), a unary function symbol $'$ (successor), and a constant symbol 0 (zero).

Terms and formulae are written in the conventional way, thus $x+y$ instead of $+(x,y)$, etc. For any natural number n, the numeral for n, written $\bar{n}$, is the term $0'''' \ldots '$ obtained by attaching n occurrences of $'$ to the right of 0. Thus $\bar{3}$ is $0'''$.

Robinson's Theory Q. Q has the following axioms

(i) $x' = y' \to x = y$

(ii) $x' \neq 0$

(iii) $x \neq 0 \to \exists y(x = y')$

(iv) $x + 0 = x$

(v) $x + y' = (x+y)'$

(vi) $x \cdot 0 = 0$

(vii) $x \cdot y' = (x \cdot y) + x$

In some sense Q is rather strong, in particular we can represent all recursive functions in Q (c. f., Section 4). On the other hand, the following are not theorems of Q: $x \neq x'$; $x + (y+z) = (x+y)+z$; $x+y = y+x$; $0+x = x$; $x < x'$; $\neg(x < y \land y < x)$; $x \cdot (y \cdot z) = (x \cdot y) \cdot z$; $x \cdot y = y \cdot x$; $0 \cdot x = x$; $x \cdot (y+z) = x \cdot y + x \cdot z$.

We take $x < y$ as an abbreviation for $\exists z(z \neq 0 \land x + z = y)$. If we are willing to accept the existence of the set of natural numbers with addition and multiplication defined in the usual way, these facts can be shown by considering the following model for Q. Here a and b are two objects distinct from the integers.

Models of Q. The best way to obtain an understanding of Q is to consider its possible models. Take an arbitrary model $\mathcal{O} \vDash Q$. There must be some element, 0 say, interpreting 0 in $\mathcal{O}$. Similarly for $\bar{n}$, and we call its interpretation n. These members of $\mathcal{O}$ are called *standard*. By axioms (i)–(iii) they are all distinct.

There may be other members of $\mathcal{O}$. If x is one such, then it must have a unique successor x' and by (i) and (iii) a unique predecessor. In this way we get

$$\dots x-3\; x-2\; x-1\; x\; x+1\; x+2\; x+3 \dots$$

This may be a finite loop, i.e. the ends join, as in the above example (in which the loops have only one member!), or have order type $\omega^* + \omega$ (where ω^* is the reverse ordering to ω). What is important is that no standard member of $\mathcal{O}$ can lead to a non-standard member (or conversely) by repeatedly applying either the successor or predecessor operations.

From (iv)–(vii) we see that addition and multiplication in the standard members of $\mathcal{O}$ are precisely the usual addition and multiplication on the natural numbers.

Clearly

$$\mathcal{O} \vDash \forall v(v < \bar{n} \leftrightarrow v = 0 \vee \cdots \vee v = \bar{n}),$$

$$\mathcal{O} \vDash \forall v \leq \bar{n}\; \varphi(v) \leftrightarrow \varphi(0) \wedge \cdots \wedge \varphi(\bar{n}).$$

Hence by the completeness theorem $Q \vdash$ the above sentences. But it is easy enough to construct a direct proof for $Q \vdash \dots$, and in fact the formal proof just mirrors the informal justification one gives for $\mathcal{O} \vDash \dots$.

Remark. There is a constructive proof of the consistency of Q (though not of P as we see later!). See Kleene, *Introduction to Metamathematics*, p. 470.

Peano's Theory P. The next theory P is usually referred to as first-order Peano arithmetic. Its axioms are (i)–(vii) of Q and the following schema ($\varphi(x)$ can have among its free variables both x and possibly other variables; $\varphi(0)$ and $\varphi(x')$ are the result of substituting 0 and x' for all free occurrences of x in $\varphi(x)$):

(viii) $\varphi(0) \wedge \forall x(\varphi(x) \to \varphi(x')) \to \forall x\, \varphi(x)$.

Thus (viii) gives induction for any property expressible in our language. Of course, induction for arbitrary sets of integers cannot be included, as this is not expressible in first-order logic. The formal development of P can be found in Kleene, *Introduction to Metamathematics*, pp. 181–194; Kleene, *Mathematical Logic*, pp. 201–213; Mendelson, *Introduction to Mathematical Logic*, pp. 102–116. The first reference also develops Q. (In all these treatments, some of the axioms given are particular cases of the equality axiom schemata of Chapter 1. It is more common practice, as we have done, to treat the equality axioms as logical axioms, rather than as particular axioms of the theory under consideration.)

It can be shown that P is not finitely axiomatisable.

We now informally indicate the roles of the axioms. (i) states that no two integers have the same successor. (ii) states that 0 is not the successor of any integer. (iii) states that every non-zero integer is a successor, and is actually a consequence of (viii) (as is easy enough to see informally—and is then a matter of patience to write out the formal proof). (iv)–(vii) give the usual recursive definitions of addition and multiplication.

We now outline the formal development of P. Certain functions and relations can be defined, or taken as abbreviations. Thus $x < y$ is an abbreviation for $\exists z(z \neq 0 \wedge x + z = y)$.

Transitivity etc. can be easily shown in P. Likewise $x - y = z$ is an abbreviation for $(x < y \wedge z = 0) \vee (x \geq y \wedge x = y + z)$. One can easily show

$$P \vdash \forall x \forall y \exists ! z (x - y = z).$$

Functions which are defined recursively, such as $x!$ or x^y, can also be defined in P, but this is trickier. We do it in Section 3. One can generally translate into P and prove the usual results of elementary number theory. Results such as the Prime Number Theorem, however, involve concepts such as the logarithmic function, and cannot even be formulated in P. Other results are proved, for example, using complex variable theory. Thus although they are formulated in P, they may not be provable in P (though one suspects they are!).

Models of P (and Q). By the compactness theorem, there are models of P and Q of every infinite cardinality (assuming they are consistent—in particular if we work in usual set theory and can thus show the existence of the standard model of natural numbers). There are also countable models besides the standard model. (Why?)

Models of P (continued). To form some idea of the possible models of P, we first note that under the previous definition of $x < y$, every model $\mathcal{O}$ is linearly ordered by $<$. Every member of $\mathcal{O}$, except 0, has a unique successor and predecessor. Thus the linear ordering induced on $\mathcal{O}$ is a linear ordering beginning with ω and followed by copies of $\omega^* + \omega$ (ω^* is the inverse ordering to ω, i.e. the order type of the negative integers).

Define an equivalence relation on members of $\mathcal{O}$ by $a_1 \sim a_2$ iff they differ by a standard integer (this definition cannot be expressed in $\mathcal{O}$ by a formula of the language of number theory, why?). Two members of $\mathcal{O}$ are thus equivalent iff they are both standard, or both in the same copy of $\omega^* + \omega$.

For any two members a_1 and a_2 of $\mathcal{O}$, there must be another member a_3 of $\mathcal{O}$ which satisfies in $\mathcal{O}$ that $a_3 = \frac{1}{2}(a_1 + a_2)$, or satisfies $a_3 = \frac{1}{2}(a_1 + a_2 + 1)$. If a_1 and a_2 are both non-standard, but lie in distinct copies of $\omega^* + \omega$, i.e. $a_1 \not\sim a_2$, then

$$a_1 < a_3 < a_2, \qquad a_1 \not\sim a_3, \qquad a_2 \not\sim a_3.$$

Hence between any two copies of $\omega^* + \omega$ there is another copy of $\omega^* + \omega$. Similarly, there is no first and no last copy of $\omega^* + \omega$. Thus the order type of $\mathcal{O}$ under $<$ is

$$\omega + (\omega^* + \omega) \times \alpha,$$

where α is a dense linear ordering without endpoints. (If A and B are linear orderings, $A \times B$ means B copies of A in the natural way.)

There is exactly one countable dense linear ordering without endpoints, namely η, the order type of the rationals. (Why?) Hence the order type of any non-standard countable model of P is

$$\omega + (\omega^* + \omega) \times \eta.$$

Notice that it is certainly not the case that all such models are isomorphic, only that their order types are isomorphic.

Every model of P is a model of Q but not conversely. In particular, the previous table gives a model of Q which is not even a linear ordering.

Later we show that there are sentences of L true in $\mathcal{O}$ (in the sense that they can be proved in our usual mathematics, more precisely in naive set theory, more precisely still from formal set theory), but are not provable in P. This is not simply due to the omission of some axiom, but as we will see the problem lies much deeper. In fact the same result can be proved for any extension of P which has an effectively enumerable set of axioms.

8.2 Representability of Functions and Relations

[This chapter to be completed]

Chapter 9

Model Theory

[This chapter to be completed]

Chapter 10

Axiom of Choice

We define in this chapter, and prove the equivalence of, the Axiom of Choice, the Well-Ordering Principle, and Zorn's Lemma.

> *To choose one sock from each of infinitely many pairs of socks*
> *requires the Axiom of Choice, but for shoes the Axiom is not needed.*
>
> Bertrand Russell

> *The Axiom of Choice is obviously true;*
> *the Well-Ordering Principle is obviously false;*
> *and who can tell about Zorn's Lemma?*
>
> Jerry Bona

10.1 Significance of the Axiom of Choice

The Axiom of Choice [AC] is different from most other axioms of set theory, which assert the existence of a set and give a rule for specifying membership of that set. Examples are the axiom of set theory asserting the existence of the union of a family of sets, or the axiom asserting the existence of the power set of a set, or the (replacement) axiom asserting that the range of a function whose domain is a set is also a set, etc. See Chapter 13.

The Axiom of Choice, however, asserts the existence of a function (and a function is just a set of ordered pairs[1]) with certain properties, without actually specifying which ordered pairs belong to the function.

The Axiom of Choice has some rather surprising consequences, as we discuss later. The philosophical issue is whether or not AC reflects physical reality, or indeed what "physical reality" actually means!

However, AC is now widely accepted within mathematics. But it is also considered good practice to note when it is used in a mathematical argument.

Despite the sometimes surprising consequences of AC we do know that it does not lead to an actual contradiction with the other axioms of set theory. The consistency of AC with the other axioms of set theory is due to Gödel. More surprisingly, the assertion that AC can be false for some infinite sets, is also consistent with the other axioms of set theory. This result is due to Paul Cohen. For these see results see (Jech, 2003).

So the situation regarding AC is not the same as with Russell's Paradox, where the "set" $\{x : x \notin x\}$ does lead to an actual contradiction.

[1] If $f : X \to Y$ then the set corresponding to f is just $\{(x, y) : f(x) = y\}$.

10.2 The Axiom of Choice

Assertion 10.1 (The Axiom of Choice [AC]). *Suppose $\{S_x : x \in I\}$ is a family of nonempty sets. Then there exists a function f with domain I such that $f(x) \in S_x$ for all $x \in I$.*

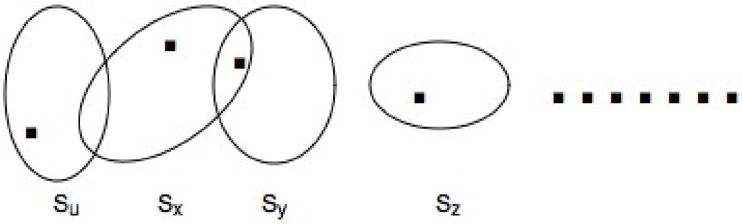


Figure 10.1: Axiom of Choice with choice function indicated by black dots.

Remark 10.2.

1. The axiom of choice as formulated here says that if S_x is nonempty for every $x \in I$ then the cartesian product $\prod_{x\in I} S_x$ is also nonempty. So it certainly seems to be a very harmless axiom!

2. If the index set I is finite, then the axiom of choice follows from the other axioms of set theory and the rules of first-order logic.

3. If there is a "rule" for selecting an object from each S_x then one does not need the axiom of choice. For example, if $S_x = \{0, 1\}$ for each x then one can take $f(x) = 0$ for all x, or $f(x) = 1$ for all x.

Exercise 10.3. Explain Russell's quote. □

Remark 10.4. The Axiom of Choice is often applied in the following form:

If F is a set of disjoint *nonempty sets then there is a set consisting of exactly one element from each set $S \in F$.* □

In the following we call f a *choice function* for the nonempty subsets of X.

Assertion 10.5 (AC*). *For every set X there exists a function $f : \mathcal{P}(X) \setminus \{\varnothing\} \to X$ such that $f(A) \in A$ for every nonempty $A \subseteq X$.*

Proposition 10.6. *AC is equivalent to AC*.*

Proof. (AC $\Longrightarrow$ AC*): AC* is the particular case of AC obtained by taking the index set $I = \mathcal{P}(X) \setminus \{\varnothing\}$ and $S_A = A$.

(AC* $\Longrightarrow$ AC): Assume AC*. Suppose $\{S_x : x \in I\}$ is a family of nonempty sets. Let $X = \bigcup_{i\in I} S_x$. See Figure 10.2

By AC*

$$\exists g : \mathcal{P}(X) \setminus \{\varnothing\} \to X \text{ such that } g(A) \in A \quad \forall A \subset X, A \neq \varnothing.$$

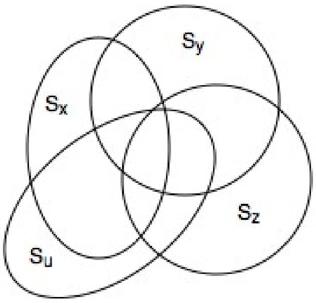


Figure 10.2: $X = \bigcup_{x \in I} S_x$. See Proposition 10.6.

Define

$$f(x) = g(S_x) \quad \forall x \in I. \qquad \square$$

Remark 10.7. In the following we will often write AC for either AC or AC*, and refer to both as the Axiom of Choice. □

10.3 Partial and Linear Orderings

Definition 10.8. $\langle X, \leqslant \rangle$ is a *partial ordering* if $\leqslant$ is a binary relation on X such that

1. $a \leqslant b$ and $b \leqslant c$ implies $a \leqslant c$ (transitive),
2. $a \leqslant a$ (reflexive),
3. $a \leqslant b$ and $b \leqslant a$ implies $a = b$ (antisymmetric).

We define $a < b$ if $a \leqslant b$ and $a \neq b$ (so we cannot have both $a < b$ and $b < a$).

Example 10.9. The following are partial orderings.

1. For any set X, $\langle \mathcal{P}(X), \subseteq \rangle$.
2. The usual $\leqslant$ ordering on $\mathbb{Z}$, $\mathbb{N}$ or $\mathbb{R}$.
3. $X = \{a, b, c, d, e, f, g\}$ with the partial ordering described in Figure 10.3.

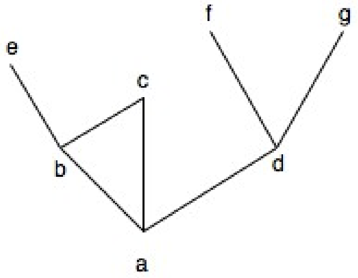


Figure 10.3: $x \leqslant y$ if $x = y$ or there is a "rising" path from x to y. For example, $a \leqslant b$, $a \leqslant c$ and $a \leqslant e$.

Definition 10.10. If $(X, \leqslant)$ is a partial ordering then $a \in X$ is a *maximal* element if there is no $b \in X$ such that $a < b$. We say a is a *greatest* element if $b \leqslant a$ for every $b \in X$.

Exercise 10.11. A greatest element is a maximal element, biut not conversely.

Definition 10.12. $\langle X, \leqslant \rangle$ is a *linear ordering* if it is a partial ordering such that for every $a, b \in X$ either $a \leqslant b$ or $b \leqslant a$ (note both are true precisely when $a = b$).

Equivalently, if for every $a, b \in X$ with $a \neq b$, either $a < b$ or $b < a$.

$L \subset X$ is an *initial segment* of X if $(y \in L \ \& \ x < y) \Longrightarrow x \in L$.

Idea: Think of a linear ordering as an ordering for which the elements of X are "in a line".

Example 10.13. In Example 10.9 only (2) is a linear ordering.

10.4 Zorn's Lemma

We will see in Section 10.6 that Zorn's Lemma is equivalent to the Axiom of Choice.

The Hahn–Banach Theorem in functional analysis, the Tychonoff Product Theorem in topology and the Maximal Ideal Theorem in algebra, all require in their proof the use of the Axiom of Choice, usually in the form of Zorn's Lemma.

And it not from lack of ingenuity that this is the case — it can be proved that they do not follow from the usual axioms of set theory without the Axiom of Choice. See (Jech, 2003).

Assertion 10.14 (Zorn's Lemma [ZL]). *Suppose $(X, \leqslant)$ is a partially ordered set such that every linearly ordered subset L has an upper bound in X. (That is, $\exists y \in X$ such that $x \leqslant y$ for all $x \in L$.)*

Then $(X, \leqslant)$ has a maximal element.

The following is a standard proposition which follows from ZL — every vector space has a basis. But it is not as obvious as one might think.

Consider the case where V is the vector space $\mathbb{R}$ over the field $\mathbb{Q}$. Then by the proposition there is a set of real numbers $B \subset \mathbb{R}$ such that for every nonzero $x \in \mathbb{R}$ there is a unique finite set of distinct real numbers $b_1, \ldots, b_n \in B$ and corresponding nonzero rational numbers $r_1, \ldots, r_n \in \mathbb{Q}$, such that

$$x = r_1 \cdot b_1 + \cdots + r_n \cdot b_n.$$

The following is a standard example of how Zorn's Lemma is used in a proof.

Proposition 10.15. *Every vector space V over a field F contains a basis $B \subset V$. That is, every finite subset of B is linearly independent and every $v \in V$ is a unique finite linear combination of elements from B with coefficients from F.*

We say B is a basis for V.

Nonexaminable Proof

Proof. (The point here is that this includes the case where V is not finite dimensional). Let

$$X = \{S : S \subset V \ \& \text{ every finite subset of } S \text{ is linearly independent}\}$$

Then $\langle X, \subseteq \rangle$ is a partial ordering.

If L is a linearly ordered subset of X then $\bigcup\{S : S \in L\}$ is itself a subset of V with the property that every finite subset is linearly independent (*why?*).
Hence $\bigcup\{S : S \in L\} \in X$ and is an upper bound for L (*why?*).

By Zorn's Lemma, $\langle X, \subseteq\rangle$ has a maximal element B (in fact many). Every element in V is a finite linear combination of elements of B, as otherwise we could enlarge B and contradict its maximality.
The fact this linear combination is unique follows from the fact that every finite subset of B is linearly independent (*why?*). □

10.5 Well-Orderings

Definition 10.16. $(X, \leqslant)$ is a *well-ordering* if it is a linear ordering such that every nonempty subset of X contains a least element.[2]

Example 10.17.

1. The only example of a well-ordering in Example 10.9 is $\mathbb{N}$ in (2).
2. $X = \mathbb{N} \cup \{\omega\}$ is a well-ordering if we use the standard ordering on $\mathbb{N}$ and set $n < \omega$ for all $n \in \mathbb{N}$.
3. $\mathbb{N}$ followed by another copy of $\mathbb{N}$ is a well-ordering.
4. Many more examples can be constructed this way.

Definition 10.18. Suppose $(X, \leqslant)$ is a well-ordering.

1. The *initial* element is the least element of X.
2. If $x \in X$ is any element then its *successor* is the least element y such that $x < y$, and is denoted by $s(x)$. Thus $s(x)$ exists unless x is the greatest element of $(X, \leqslant)$. A *successor* element is an element of the form $s(x)$.
3. A *limit* element $x \in X$ is an element which is not the initial element and is not a successor element.
   Equivalently, x is not the initial element and for every $y < x$ there is an element z such that $y < z < x$.

In Example 10.17(3) the "first" 0 is the initial element. The "second" 0 is a limit element. All other elements are successor elements.

Proposition 10.19. *If $(A, \leqslant)$ and $(B, \preccurlyeq)$ are well-orderings then one is isomorphic to an initial segment (and perhaps all) of the other.*

Proof. We don't need the result, and the proof is like that for the following Proposition. So I leave it as an exercise. □

We often define a function by induction over the natural numbers by first defining $f(0)$ and then defining $f(n)$ in terms of $f(0), \ldots, f(n-1)$. For example, the Fibonacci sequence is defined by

$$f(0) = 1,\ f(1) = 1,\ f(n) = f(n-2) + f(n-1) \text{ for } n \geq 2.$$

In general, we can define

$$f(n) = g\Big(f \restriction I(n)\Big),$$

[2] A *least* element of $A \subset X$ is of course an element $a \in A$ such that $a \leqslant b$ for all $b \in A$.

where g is a given function, $I(n)$ is the initial segment $\{k : k < n\}$, and $f \restriction I(n)$ is the restriction of f to $I(n)$.

It is useful here to think of a function as a set of ordered pairs, so $f \restriction I(n) = \{(k, f(k)) : k < n\}$.

We now generalise inductive definitions to well-ordered sets.

Proposition 10.20 (Definition by Recursion). *Suppose $(X, \leqslant)$ is a well-ordered set. Let $I(x) = \{y : y < x\}$ for each $x \in X$. Then given g with range T and appropriate domain, there is a unique function $f : X \to T$ such that*

$$f(x) = g\Big(f \restriction I(x)\Big). \tag{10.1}$$

Proof. The idea is straightforward.

Let $J(x) = \{y : y \leqslant x\}$.[3]

Let G be the set of those $z \in X$ such that there is a function of the form $f : J(z) \to T$ which satisfies (10.1) for all $x \in J(z)$.

For each $z \in G$ there can be at most one such function. If not, consider the first $x \leqslant z$ where two such functions differ and obtain an immediate contradiction, since by (10.1) they must agree at x.

If $y_1 < y_2$ and there exist corresponding such functions f_1 and f_2, then $f_2 \restriction I(y_1)$ is of the required form and so equals f_1.

It follows that G is an initial segment of X. Moreover, f is uniquely defined and satisfies (10.1) for all $x \in G$.

If $G \neq X$ let y be the least element in $X \setminus G$. Then we can use (10.1) to extend f from G to $G \cup \{y\}$. This contradicts the definition of G.

Hence $G = X$ and we are done. □

10.6 Equivalent versions of AC

Assertion 10.21 (WO: The Well-Ordering Principle). *Every set can be well-ordered.*

Assertion 10.22 (HMP: Hausdorff's Maximal Principle). *Suppose $(X, \leqslant)$ is a partially ordered set. Then X contains a maximal linearly ordered subset.*[4]

Proposition 10.23. *$\mathbb{R}^n$ can be well-ordered.*

Proof. By the well-ordering principle. □

Theorem 10.24. *AC $\iff$ AC* $\iff$ HMP $\iff$ ZL $\iff$ WO.*

Proof. We have already seen AC $\iff$ AC*.

We will show AC* $\Longrightarrow$ WO $\Longrightarrow$ HMP $\Longrightarrow$ ZL $\Longrightarrow$ AC*.

1: (AC* $\Longrightarrow$ WO): Suppose f is a "choice function" satisfying $f(A) \in A$ for all $\varnothing \neq A \subset X$.

The informal idea is to define the well ordering $x_1, x_2, \ldots, x_n, \ldots, x_\omega, \ldots$ by

$$x_1 = f(X),\ x_2 = f(X \backslash \{x_1\}),\ x_3 = f\Big(X \backslash \{x_1, x_2\}\Big),\ \ldots\ ,\ x_\omega = f\Big(X \backslash \{x_n : n \in \mathbb{N}\}\Big),\ \ldots\ .$$

[3] It is very convenient to work with initial segments of the form $J(x)$ as well as with $I(x)$.

[4] L is a *maximal* linearly ordered subset if it is linearly ordered by $\leqslant$ and if there is no larger linearly ordered subset containing L.

To make this precise consider all well orderings $(A, \leqslant)$ such that

1. $A \subset X$,
2. $x \in A \Longrightarrow x = f\Big(X \setminus \{y \in A : y < x\}\Big)$.

We have just seen there are indeed some such well orderings.

We *claim* if $(A, \leqslant)$ and $(B, \preccurlyeq)$ are two such well orderings then one is an initial segment of the other (with the same ordering).

Suppose neither $(A, \leqslant)$ nor $(B, \preccurlyeq)$ is an initial segment of the other.

Then it follows that for some $x \in A$, $\{y \in A : y \leqslant x\}$[5] is not an initial segment of $(B, \preccurlyeq)$.[6]

Take the first $x \in A$ such that $\{y \in A : y \leqslant x\}$ is *not* an initial segment of $(B, \preccurlyeq)$. It follows that $D := \{y \in A : y < x\}$ is an initial segment of both $(A, \leqslant)$ and $(B, \preccurlyeq)$.[7]

We will show $x \in B$ and that by "adding" x to the end of D we get $\{y \in A : y \leqslant x\}$ is an initial segment of both A and B, contradicting the definition of x.

By property (2) for the well ordering $(A, \leqslant)$, we have $x = f(X \setminus D)$.

On the other hand, since $B \setminus D$ is nonempty (as otherwise B is an initial segment of A) there is a least element x^* in $B \setminus D$. Then by property (2) for the well ordering $(B, \preccurlyeq)$, we have $x^* = f(X \setminus D)$.

Hence $x^* = x$ and so by "adding" $x = x^*$ to the end of D we see $\{y \in A : y \leqslant x\}$ is an initial segment of $(B, \preccurlyeq)$, contradicting the definition of x.

Thus for any two well orderings satisfying (1) and (2), one is an initial segment of the other. For this reason we can take the union of *all* such well orderings to get a well ordering of some $Y \subset X$. If $Y \neq X$ then we can enlarge the well ordering by adding $f(X \setminus Y)$ at the end, thus contradicting the fact we took the union of all such well orderings.

2: (WO $\Longrightarrow$ HMP): Suppose $(X, \leqslant)$ is a partial ordering and assume there is a well ordering $(X, \preccurlyeq)$.

The idea is to use the well ordering $\preccurlyeq$ to build up the maximal linearly ordered subset L for $\leqslant$. Let the well ordering be $x_1, x_2, \dots, x_n, \dots, x_\omega, \dots$. Set $x_1 \in L$. If $\leqslant$ gives a linear ordering on $\{x_1, x_2\}$ then include $x_2 \in L$, otherwise exclude it. If $\leqslant$ gives a linear ordering on $\{x_3\} \cup \{\text{elements already in } L\}$ then include $x_3 \in L$, otherwise exclude it. ... If $\leqslant$ gives a linear ordering on $\{x_\omega\} \cup \{\text{elements already in } L\}$ then include $x_\omega \in L$, otherwise exclude it. Etc.

To make this precise we define L, or more precisely the characteristic function $\mathcal{X}_L$, by recursion as in Proposition 10.20. That is

$$\mathcal{X}_L(x) = \begin{cases} 1 & \text{if } \leqslant \text{ is a linear ordering on } \{x\} \cup \{y : y \prec x \ \&\ \mathcal{X}_L(y) = 1\} \\ 0 & \text{otherwise} \end{cases}.$$

Then $\prec$ is a linear order on L and L is also maximal in this respect.[8]

3: (HMP $\Longrightarrow$ ZL): Assume HMP.

[5] It is important for the proof to take $\{y \in A : y \leqslant x\}$ and not $\{y \in A : y < x\}$. Note that doing this gives us more information, since not every initial segment is of the form $\{y \in A : y \leqslant x\}$.

[6] Since otherwise, if $\{y \in A : y \leqslant x\}$ is an initial segment of $(B, \preccurlyeq)$ for every $x \in A$, then taking the union one can check that this implies A is an initial segment of $(B, \preccurlyeq)$.

[7] Since $\{y \in A : y < x\} = \bigcup_{\{y \in A : y < x\}} \{z \in A : z \leqslant y\}$, and a union of initial segments is an initial segment. Similarly for B.

[8] Since if $\prec$ is a linear order on $L \cup \{x\}$ then the definition gives $\mathcal{X}_L(x) = 1$, and so $x \in L$.

Suppose $(X, \leqslant)$ is a partially ordered set such that every linearly ordered subset has an upper bound in X. By HMP there is a *maximal* linearly ordered subset L. Let y be an upper bound for L.

Then y is clearly a maximal element for $(X, \leqslant)$.[9]

4: (ZL $\Longrightarrow$ AC*): Assume ZL.

Given a set X, let F be the set of all choice functions f whose domain is a *subfamily* of the family of all nonempty subsets of X. By "choice" function it is meant as usual that $f(A) \in A$ for all A in the domain of f.

Define the partial order $\leqslant$ on F by $f \leqslant g$ if g is an extension of f. Then it is straightforward to check that $(F, \leqslant)$ is a partial ordering. Moreover, any linearly ordered subset has a greatest element, obtained by taking the union (regarding a function as a set of ordered pairs) of all functions in the linearly ordered subset.

By ZL there is a maximal element $f \in (F, \leqslant)$. The domain of f must be $\mathcal{P}(X) \setminus \{\varnothing\}$ as otherwise we could extend f by adding an ordered pair (x, A) for any nonempty set $A \subset X$ and $x \in A$.[10] □

10.7 Other Stuff

[This chapter to be completed]

[9] Since if $y < w$ then $L \cup \{w\}$ would be linearly ordered, contradicting the maximality of L.

[10] There is *not* a hidden application here of AC because of our "choosing" A and then choosing $x \in A$. *Why?*

Chapter 11

Ordinals

11.1 Linear Orderings

Definition 11.1 (Linear ordering). A linear ordering $<$ on a set A is a subset of $A \times A$ such that

(i) (Transitivity) for all $a, b, c \in A$, if $a < b$ and $b < c$ then $a < c$,

(ii) (Trichotomy) for all $a, b \in A$, exactly one of $a = b$, $a < b$, $b < a$ holds.

We often write $\mathcal{A} = \langle A, < \rangle$ and call $\mathcal{A}$ a linear ordering.

If $S \subset A$ and $x \in A$ then $x < S$ means $x < y$ for all $y \in S$. Similarly for $S < x$.

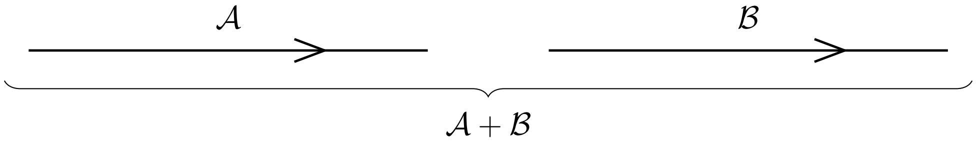
Exercise 11.2. Express the axioms for a linear ordering in an appropriate first-order language.

Definition 11.3 (Sum and product of linear orderings). If $\mathcal{A}$ and $\mathcal{B}$ are linear orderings, then:

(i) $\mathcal{A} + \mathcal{B}$ is the linear ordering obtained by following a copy of $\mathcal{A}$ with a copy of $\mathcal{B}$.

More precisely, let $\mathcal{A} = \langle A, <_1 \rangle$ and $\mathcal{B} = \langle B, <_2 \rangle$ where B is *disjoint*[1] from A. Then $\mathcal{A} + \mathcal{B} = \langle A \cup B, < \rangle$ where

$$u < v \quad \text{iff} \quad \begin{cases} u, v \in A \text{ and } u <_1 v, \\ \text{or } u \in A,\ v \in B, \\ \text{or } u, v \in B \text{ and } u <_2 v. \end{cases}$$



(ii) $\mathcal{B} \cdot \mathcal{A}$ is the linear ordering obtained by placing a copy of $\mathcal{B}$ at each $a \in A$, and ordering between different copies of $\mathcal{B}$ according to their position on A.

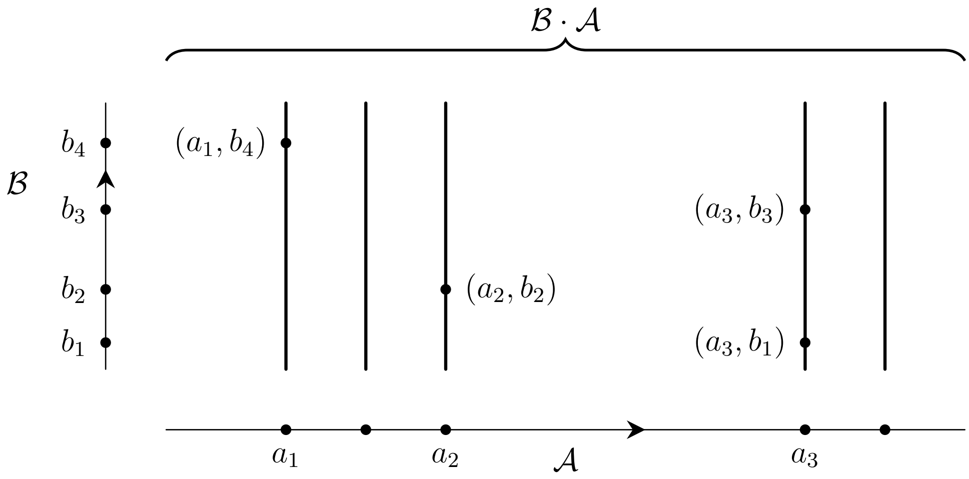
[1] There is clearly no loss of generality in assuming this.

We “read” $\mathcal{B} \cdot A$ from right to left according to the usual convention. Think of it as “$\mathcal{A}$ copies of $\mathcal{B}$”.

More precisely, let $\mathcal{A} = \langle A, <_1 \rangle$ and $\mathcal{B} = \langle B, <_2 \rangle$.

Then $\mathcal{B} \cdot \mathcal{A} = \langle A \times B,\ < \rangle$ where

$$(a_1, b_1) < (a_2, b_2) \quad \text{iff} \quad \begin{cases} a_1 <_1 a_2, \\ \text{or } a_1 = a_2 \text{ and } b_1 <_2 b_2. \end{cases}$$



Here: $(a_1, b_4) \ < \ (a_2, b_2) \ < \ (a_3, b_1) \ < \ (a_3, b_3)$

Remark 11.4. The ordering $<$ in $\mathcal{B} \cdot \mathcal{A}$ is also called the *lexicographic ordering* or *dictionary ordering* on $A \times B$. And is called the *antilexicographic ordering* on $B \times A$. □

Remark 11.5 *(Algebraic Properties of Addition and Multiplication).* It is straightforward to prove, that

$$\begin{aligned} \mathcal{A} + (\mathcal{B} + \mathcal{C}) &= (\mathcal{A} + \mathcal{B}) + \mathcal{C}, \\ \mathcal{A} \cdot (\mathcal{B} + \mathcal{C}) &= (\mathcal{A} \cdot \mathcal{B}) + (\mathcal{A} \cdot \mathcal{C}), \\ \mathcal{A} \cdot (\mathcal{B} \cdot \mathcal{C}) &= (\mathcal{A} \cdot \mathcal{B}) \cdot \mathcal{C}. \end{aligned}$$

But in general

$$(\mathcal{A} + \mathcal{B}) \cdot \mathcal{C} \neq \mathcal{A} \cdot C + \mathcal{B} \cdot \mathcal{C}$$

For example, let $\mathcal{A} = \{0\}$, $\mathcal{B} = \{1\}$ and $\mathcal{C} = \omega$, with the trivial order on the two singleton sets and $\omega = \{0, 1, 2, \dots\}$ with the standard ordering $0 < 1 < 2 < \dots$

Then $\mathcal{A} + \mathcal{B} = 2 :=$ [2] $\{0, 1\}$ with the ordering $0 < 1$. So

$$\begin{aligned} (\mathcal{A} + \mathcal{B}) \cdot \mathcal{C} &= 2 \cdot \omega \\ &\text{“=”}\ (0,0) < (0,1) < (1,0) < (1,1) < (2,0) < (2,1) < (3,0) < (3,1) < \dots \\ &\cong \omega. \end{aligned}$$

where “”$\cong$” means isomorphic as linear orderings.

[2] “:=” means “by definition equals”

On the other hand,

$$\mathcal{A} \cdot C + \mathcal{B} \cdot \mathcal{C} \;\cong\; \{0\} \cdot \omega + \{1\} \cdot \omega \;\cong\; \omega + \omega \;\not\cong\; \omega$$

The non-isomorphism is because every element in ω has an immediate predecessor, but this is this not the case for $\omega + \omega$. *Why?*

Definition 11.6 (Initial segment). I is an initial segment of the linear order $\mathcal{A} = (A, <)$ iff $I \subseteq A$ and

$$x \in I \;\wedge\; y < x \quad \Longrightarrow \quad y \in I.$$

Definition 11.7 (Finite orders and ω).

1. Besides denoting the respective integer, n also denotes the unique (up to isomorphism) linear ordering containing n elements. The domain of n is $\{0, 1, \ldots, n-1\}$ with $0 < 1 < \cdots < n-1$.

2. ω is the unique (up to isomorphism) linear ordering with infinite domain such that every proper initial segment is finite. The domain of ω is $\{0, 1, 2, \ldots\}$ with the usual order $0 < 1 < 2 < \cdots$.

11.2 Ordinals as Sophisticated Counting

In this and the next section I discuss the ideas behind ordinals in an informal manner. In many cases where ordinals are being used, this is about all that you will need.

Ordinals were introduced by Cantor in 1883 in his work on trigonometric series. See Aside/Cantor 11.3.

When we prove or define something by induction over ω (a "step by step" proof) we essentially know it works because ω has a first element, and because for every initial segment $I \subsetneq \omega$ there exists a first element $x > y$ for every $y \in I$.
Let's temporarily call this the *segment property* of ω.

By an informal argument (or formally by induction, but do not bother — it is all in Theorem 11.17) we see that any infinite linear order with the above *segment property* has an isomorphic copy of ω as a proper initial segment. Thus ω is the "smallest" linear ordering with the segment property, with domain and ordering as in Definition 11.7.2.

The next smallest such linear ordering has domain

$$\{0,\ 1,\ 2,\ \ldots\ ,\ \omega\}$$

with ordering

$$0\ <\ 1\ <\ 2\ <\ \ldots\ <\ \omega.$$

We write this as $\omega + 1$, consistent with Definitions 11.3 (and 11.7).

Then $\omega + 2$ is the next, $\omega + 3$ the next, $\ldots$. And after all these there is again a unique next, $\omega + \omega$ (i.e. $\omega \cdot 2$). Then $\omega \cdot 2 + 1$, $\omega \cdot 2 + 2$, $\ldots$, and after all these $\omega \cdot 2 + \omega$ (i.e. $\omega \cdot 3$).

These order types are called *ordinals.* Writing out part of the list we have

$$\begin{aligned}&0,1,2,3,\dots,\omega,\ \omega+1,\ \omega+2,\ \omega+3,\ \dots,\ \omega+\omega=\omega\cdot 2,\\ &\omega\cdot 2+1,\ \omega\cdot 2+2,\ \omega\cdot 2+3,\dots,\ \omega\cdot 3,\ \omega\cdot 3+1,\dots,\ \omega\cdot 4,\dots,\\ &\omega\cdot\omega=\omega^2,\ \omega^2+1,\dots,\ \omega^2+\omega,\ \omega^2+\omega+1,\dots,\ \omega^2+\omega\cdot 2,\\ &\omega^2+\omega\cdot 2+1,\dots,\ \omega^3,\dots,\ \omega^n,\dots,\ \omega^\omega,\dots,\omega^{\omega^\omega},\dots,\ \omega^{\omega^{\omega^\omega}},\dots,\ \omega^{\omega^{\cdot^{\cdot^{\cdot^\omega}}}},\dots,\ \epsilon_0,\dots\end{aligned}$$

Some ordinals α are *successor ordinals*, that is $\alpha=\beta+1$ for some β. Otherwise α is a *limit ordinal*, except that 0 is the *initial ordinal.* In the above list the explicitly displayed limit ordinals are

$$\omega,\ \omega\cdot 2,\ \omega\cdot 3,\ \omega\cdot 4,\ \omega^2,\ \omega^2+\omega,\ \omega^2+\omega\cdot 2,\ \omega^3,\omega^n,\ \omega^\omega,\omega^{\omega^\omega},\omega^{\omega^{\omega^\omega}},\omega^{\omega^{\cdot^{\cdot^{\cdot^\omega}}}},\epsilon_0.$$

The class of ordinals is ordered as in its construction, that is

$$0\ <\ 1\ <\ 2\ <\ 3\ <\ \dots\ <\ \omega\ <\ \omega+1\ <\ \omega+2\ <\ \dots<\ \omega\cdot 2\ <\ \dots\ <\ \omega^2\ <\ \dots\ ,$$

etc. Note that each ordinal has order type with domain its set of predecessors and ordering on this set as above.

The list of ordinals above does not even "scratch the surface" of the class of all ordinals. In fact, the class of all ordinals is too big to even be a set, as we see later.*** ref*** Informally: if there were such a set it would itself be a set which is an ordinal, in which case we could get an even larger ordinal by taking its successor. But this gives a contradiction.

11.3 Ordinals and Iterated Processes

Ordinals arise naturally in the context of *transfinite iteration* of various operations.

For example, take some fixed set X (in particular, X may be $\mathbb{R}$). Let

$$V_0(X)=X,\quad V_{n+1}(X)=V_n(X)\cup\mathcal{P}(V_n(X))\quad\text{for } n<\omega.$$

Then clearly

$$V_0(X)\subset V_1(X)\subset V_2(X)\subset\dots\subset V_n(x)\subset\dots$$

It is natural to extend this process up through the ordinals by defining

$$V_\omega(X)=\bigcup_{n<\omega}V_n(X),\quad V_{\omega+1}(X)=V_\omega(X)\cup\mathcal{P}\Big(V_\omega(X)\Big),\quad \dots\ .$$

More generally, define

$$V_\alpha(X)=\begin{cases}X & \text{if } \alpha=0,\\ V_\beta(X)\cup\mathcal{P}\Big(V_\beta(X)\Big) & \text{if } \alpha=\beta+1,\\ \bigcup\limits_{\beta<\alpha}V_\beta(X) & \text{if } \alpha \text{ is a limit ordinal.}\end{cases}$$

Then clearly

$$V_\beta(X)\subset V_\alpha(X)\quad\text{if}\quad \beta<\alpha.$$

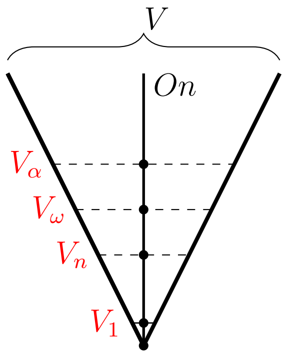
One surprising but useful observation is that one can, and it is standard to, take $X = \varnothing$ and build up all the sets used in set theory in this manner.

In this case

$$V_\alpha = \begin{cases} \varnothing & \text{if } \alpha = 0, \\ \mathcal{P}\big(V_\beta\big) & \text{if } \alpha = \beta + 1, \\ \bigcup\limits_{\beta<\alpha} V_\beta & \text{if } \alpha \text{ is a limit ordinal.} \end{cases}$$

Exercise: I claim that $V_\alpha \subset V_{\alpha+1}$ for all α. Note that $V_0 \subset V_1$, and convince yourself by a sort of induction that it is always true. We will make the argument more rigorous later by "transfinite induction", but it is good to think about it now with this straightforward example.

Use this result to show that $V_\alpha = V_\alpha(\varnothing)$, with $V_\alpha(\varnothing)$ as previously defined. □



- On: collection of ordinals
- Iterate power set along On
- $V_0 = \varnothing$, $V_{\alpha+1} = \mathcal{P}(V_\alpha)$, $V_\lambda = \bigcup_{\alpha<\lambda} V_\alpha$ (limit λ)
- The sets in V_1, V_n , V_ω, V_α, respectively are "points" below the corresponding dashed lines
- Black dots on the On line are ordinals $0, 1, n, \omega, \alpha$, respectively.
- $0 \in V_1$; $0, \dots, n-1 \in V_n$; $0, \dots, n, \dots \in V_\omega$; $\beta \in V_\alpha$ if $\beta < \alpha$. $\;\dots$

Remark 11.8 *(Tetrational Growth).* The size/cardinality of the V_n grows mind-bogglingly fast. Denoting by $|A|$ the number of elements in the set A, we have

- $|V_0| = 0$,
- $|V_1| = 1$,
- $|V_2| = 2$,
- $|V_3| = 2^2 = 4$,
- $|V_4| = 2^4 = 2^{2^2} =: 2 \upuparrows 3 = 16$,
- $|V_5| = 2^{16} = 2^{2^{2^2}} =: 2 \upuparrows 4 = 65,536$,
- $|V_6| = 2^{65,536} = 2^{2^{2^{2^2}}} =: 2 \upuparrows 5 > 10^{19728}$, ...

So $|V_6|$ is far, far greater than the $\approx 10^{17}$ seconds since the big bang, or the $\approx 10^{80}$ atoms in the observable universe. □

Cantor

Cantor introduced ordinals in the following similar setting for his analysis of trogonometric series.

If $A \subset \mathbb{R}$ then its derived set $A' \subseteq A$ is obtained by removing all isolated points and keeping the limit points. Repeating this operation gives a decreasing ordinal sequence of sets:

$$A_0 := A \;\supset\; A_1 := A_0' \;\supset\; A_2 := A_1' \;\supset\; \dots \;\supset A_\omega := \bigcap_{n<\omega} A_n \;\supset\; A_{\omega+1} := A_\omega' \;\supset\; \dots$$

The sequence is continued until it is no longer strictly decreasing.
See Wikipedia: Trigonometric Series

11.4 Equivalent Definitions of Well-Orderings

The next theorem gives three equivalent definitions for a well-ordered set, see Definition 11.10. The remark after Theorem 11.13 shows that well-ordered sets are precisely those linear orders over which one can do induction, and leads to yet a fourth definition.

Theorem 11.9. *If $\mathcal{A} = \langle A, < \rangle$ is a linearly ordered set, then the following are equivalent:*

(i) A contains no infinite descending sequences $a_1 > a_2 > a_3 > \dots$.

(ii) Every nonempty $S \subseteq A$ contains a least member.

(iii) Every initial segment $I \neq A$ has a least $\underline{\text{next}}$ element $a \in A$, that is

$$I < a \;\wedge\; (I < x \Longrightarrow a \leq x)$$

Proof.

(i)⇒(ii): Assume (i). If $\varnothing \neq S \subseteq A$ has no least member, construct a sequence

$$a_1 > a_2 > a_3 > \cdots > a_n > \dots$$

of elements from S as follows:
choose $a_1 \in S$ (possible as $S \neq \varnothing$)
choose $a_2 \in S$ so that $a_2 < a_1$ (possible as otherwise a_1 is a least member of S)
choose $a_3 \in S$ so that $a_3 < a_2$ (possible as otherwise a_2 is a least member of S)
etc.

(ii)⇒(i): Assume (i) is false. Then there exists an infinite descending sequences $a_1 > a_2 > a_3 > \dots$. Let $S = \{a_1, a_2, a_3, \dots\}$. Then S is nonempty and has no least member. So (ii) is false.

(ii)⇒(iii): Assume (ii). If $I \neq A$ is an initial segment then the least element of $A \setminus I$ is the least next element for I.

(iii)⇒(ii): Assume (iii). If $\varnothing \neq S \subseteq A$, let $I = \{x \in A : \; x < S\}$. Then $I \subsetneq A$ is an initial segment (perhaps $= \varnothing$). The least next element for I is the required least member of S. □

Definition 11.10 (Well-Ordered Set). A linearly ordered set $A = (A, <)$ is *well-ordered* iff it satisfies one (hence all) of the conditions of Theorem 11.9.

Use of the Axiom of Choice

The construction of an infinite sequence in the proof of (i)⇒(ii) uses a form of the axiom of choice – we discuss this axiom in Chaper 10.
The use of the axiom of choice here is NOT in the individual choices made in the proof of (i)⇒(ii). This is allowable by the axioms for set theory as we are choosing from a nonempty set in each individual case.
The problem arises in asserting that the countably infinite number of individual choices coresponds to a single (infinite) set. I will say more in Chapter 10.

Exercise 11.11. Every subset of a well-ordered set is well-ordered under the induced ordering.

Exercise 11.12. The sum and product of well-ordered sets are well-ordered.

Theorem 11.13 (Transfinite induction on well-ordered sets). *Suppose $\mathcal{A} = \langle A, < \rangle$ is a well-ordering, $S \subseteq A$, and*

$$\forall x \in A \Big(\forall u < x \, (u \in S) \implies x \in S \Big).$$

Then $S = A$.

Proof. If $A \setminus S \neq \varnothing$, take its least member and derive an immediate contradiction from Theorem 11.9(ii). □

Remark 11.14. Call a linear order $A = (A, <)$ *inductive* if every $S \subseteq A$ satisfies the hypothesis of Theorem 11.13. Then A is well-ordered: for if $I \subsetneq A$ is an initial segment with no least next element, then for every $x \in A$ we have $(\forall u < x \ (u \in I)) \Rightarrow x \in I$ (consider $x \in I$ and $x \notin I$ separately), hence $I = A$, a contradiction. Thus well-orders are precisely those linear orders over which we have proof by induction.

11.5 Properties of Well-Orderings

Remark 11.15. Equivalence classes of linear orders under order-isomorphism are called *ordinals* (ordinal numbers). Write $\alpha < \beta$ iff some representative of α is isomorphic to some proper initial segment of some representative of β. The next results show that $<$ is a well-order on ordinal numbers, and for every α the set of predecessors of α under $<$ is a representative of α.

Theorem 11.16 (No self-isomorphism to a proper intial segment). *If $A = (A, <)$ and $B \subsetneq A$ is an initial segment of A, then $B = (B, <)$ is not isomorphic to A. In fact, the only order-isomorphism from B to a segment of A is the identity.*

Proof. If $f : B \to B' \subseteq A$ is an order isomorphism and B' is a segment of A, then for the first element b of B (and hence of A) we must have $f(b) = b$. Then f fixes the second element, and so on. Formally, if $f(b) \neq b$ for some $b \in B$, consider the least $x \in B$ with $f(x) \neq x$; a contradiction arises immediately. □

Theorem 11.17 (Comparability of well-orders). *If $A = (A, <)$ and $B = (B, <)$ are well-ordered sets, then one is isomorphic to an initial segment of the other.*

Proof. *** See Theorem 12 proof, my old notes, p 115

Consider order-isomorphisms from segments of A onto segments of B. Any two agree on the smaller domain, so they paste to a largest one. If it is defined on all of A we are done. If not, its range must be all of B (else extend it), and we are still done. □

Corollary 11.18. *Given any two well-orderings, exactly one holds: they are isomorphic, or the first is isomorphic to a unique proper initial segment of the second, or the second to a unique proper initial segment of the first.*

It follows that $<$ is a linear ordering of ordinal numbers. More is true.

Theorem 11.19. $<$ *is a well-order of the class of ordinal numbers. Moreover, every ordinal has as a representative the set of ordinal numbers less than it together with the ordering induced from* $<$.

Proof. For the second claim: if $(A, <)$ represents α, then by Corollary 11.18 the set $\{\beta : \beta < \alpha\}$ is order-isomorphic to $(A, <)$ via the map taking each β to the corresponding proper initial segment of A.

See my old notes botom p115, top p 116

For the first claim: if S is a nonempty set of ordinals, take $\alpha \in S$. If α is least we are done; otherwise $S \cap \{\beta : \beta < \alpha\}$ has a least element because it is a subset of the well-ordered set $\{\beta : \beta < \alpha\}$. □

Definition 11.20. The well-ordered class of all ordinals is written On.

Definition 11.21 (Successor and limit). An ordinal $\alpha > 0$ is a *limit ordinal* iff it has no immediate predecessor. Otherwise (if $\alpha > 0$) it is a *successor* ordinal.

If α is a successor ordinal, then $\alpha = \beta + 1$ where β is the immediate predecessor of α.

Using Theorem 11.9(ii), one can see that every ordinal can be written (uniquely) in the form $\Lambda + n$ where Λ is a limit ordinal and $n \in \mathbb{N}$ (perhaps 0). For if β is a limit ordinal we are done. If not, let $\beta_0 = \beta + 1$, $\beta_1 = \beta_0 + 1$, and so on. Since $\beta > \beta_0 > \beta_1 > \cdots$ we must stop at some $\beta_m = \Lambda$, and $\beta = \Lambda + n$.

11.6 Transfinite induction and recursion

We give informal versions of these ideas, i.e. the versions used in everyday mathematics, as opposed to those formulated precisely in a specific set-theoretic language.

Definition 11.22 (Transfinite induction). Let S be an initial segment of the ordinals (the set of ordinals less than some ρ). Let $P(\alpha)$ be a property of ordinals. Suppose for every $\alpha \in S$,

$$\big(\forall \beta < \alpha \; P(\beta)\big) \;\Rightarrow\; P(\alpha)$$

(and in particular $P(0)$). Then $P(\alpha)$ holds for every $\alpha \in S$.

Idea. Consider the first $\alpha \in S$ (if any) where $P(\alpha)$ fails; this contradicts the hypothesis at α. □

Remark 11.23. In practice, verify separately:

(i) $P(0)$;

(ii) $P(\alpha) \Rightarrow P(\alpha+1)$ for successors;

(iii) if λ is a limit and $\forall \beta < \lambda \; P(\beta)$, then $P(\lambda)$.

Definition 11.24 (Transfinite recursion). Let S be an initial segment of the ordinals. Let G be a binary operation. There is a unique function F with domain S such that for every $\alpha \in S$,

$$F(\alpha) = G\Big(\alpha,\ F \restriction \alpha\Big).$$

Idea. Let $\mathcal{F}$ be the family of functions f with (i) $\mathrm{dom}(f)$ an initial segment of S, and (ii) $f(\alpha) = G\Big(\alpha, f \restriction \alpha\Big)$ for all $\alpha \in \mathrm{dom}(f)$. Any two are compatible (argue by the first place they differ). Their union F lies in $\mathcal{F}$ and must have domain S (else extend), giving existence; uniqueness is by the same minimum-counterexample argument. □

Remark 11.25 *(Typical format).* Often one specifies F by

$$F(0) = A, \qquad F(\alpha+1) = G\Big(F(\alpha)\Big), \qquad F(\lambda) = H\Big(\{F(\beta) : \beta < \lambda\}\Big)$$

for given A, unary G, and unary H, handling 0, successor, and limit stages separately.

[This chapter to be completed]

Chapter 12

Cardinals

12.1 Cardinal numbers

Definition 12.1. $A \sim B$ iff there is a bijection $f : A \to B$. This is an equivalence relation on sets. Each equivalence class is called a *cardinal number*. We write κ, or $|A|$, or $\mathrm{card}(A)$ for the cardinal associated with A. Cardinal numbers are often written $\aleph_0, \aleph_1, \aleph_2, \ldots$

Definition 12.2. Write $\kappa \leq \lambda$ iff there are sets A, B with $|A| = \kappa$, $|B| = \lambda$ and an injection $A \hookrightarrow B$. Write $\kappa < \lambda$ iff $\kappa \leq \lambda$ and $\kappa \neq \lambda$.

Remark 12.3. One shows easily: if $\kappa \leq \lambda$ and $\lambda \leq \mu$ then $\kappa \leq \mu$; and by Schröder–Bernstein, $\kappa \leq \lambda$ and $\lambda \leq \kappa$ imply $\kappa = \lambda$. Thus $\leq$ is a partial order on cardinals (no use of AC needed).

Remark 12.4. A cardinal number via equivalence classes is a proper class. Alternatively, identify cardinals with particular ordinals (initial ordinals); ordinals themselves can be identified with particular sets.

Remark 12.5 *(Cardinals as initial ordinals).* Identify each cardinal κ with the least ordinal α that well-orders some (hence every) set of size κ. By the Well-Ordering Principle this exists (here AC is used). Then the class Card of cardinals is a subclass of On and is well-ordered. It is not a set: for every ordinal α, $|\mathcal{P}(\alpha)|$ is a strictly larger cardinal (Theorem 12.14); also On is a proper class.

Remark 12.6 *(Counting ordinals).* It is conventional to enumerate the infinite cardinals as $\aleph_\alpha$ for ordinals α.

Remark 12.7. For each ordinal α, let $|\alpha|$ be the cardinality of the set of predecessors of α. Clearly $|\alpha| \leq \alpha$ and $|\alpha| = \alpha$ iff α is a cardinal. Hence if κ is a cardinal and $\alpha < \kappa$ then $|\alpha| < \kappa$.

In particular, every set has a well-order such that every initial segment has smaller cardinality than the whole set. If $|\alpha| = \aleph_0$ we say α is *countable*. All ordinals listed in §11.7–§11.17 are countable (or finite).

All ordinals listed in §§11.7–11.17 are countable (or finite).

Definition 12.8 (Cardinal addition and multiplication). Let $|A| = \kappa$, $|B| = \lambda$ and $A \cap B = \varnothing$. Then

$$\kappa + \lambda = |A \cup B|, \quad \kappa \cdot \lambda = |A \times B|.$$

Remark 12.9. Cardinal addition and multiplication differ from ordinal addition and multiplication; the context should make it clear which is intended.

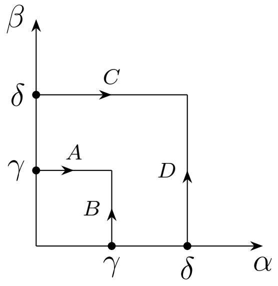
Lemma 12.10. *If κ is an infinite cardinal then $\kappa \cdot \kappa = \kappa$. (cardinal multiplication)*

Proof Idea. We will treat cardinals as particular ordinals.

We define a linear ordering on $On \times On$ as indicated in the diagram below and check that this is a well-ordering.

We then show by a cardinality argument that for any infinite cardinal κ, the restriction to $\kappa \times \kappa$ is isomorphic to the ordering on κ itself. Hence $\kappa \cdot \kappa = \kappa$.

The key idea is, assuming there is spme cardinal which does not have this property, to consider the *first* cardinal which does not have this property, and obtain a contradictoion.



Points in A, B, C, D are in the order shown. And $A \prec B \prec C \prec D$ in an obvious sense.
Points in $A \cup B$ are less than points in $C \cup D$ by condition (a) in the proof.
Points in A have their relative order determined by condition (b), as do points in C.
Points in B have their relative order determined by condition (c), as do points in D. □

Proof. (See the previous diagram and explanation)

Define a linear ordering $\prec$ on $On \times On$ by $(\alpha_1, \beta_1) \prec (\alpha_2, \beta_2)$ iff

$$\begin{array}{ll}
\text{(a)} & \max\{\alpha_1, \beta_1\} < \max\{\alpha_2, \beta_2\} \quad \text{or} \\
\text{(b)} & \max\{\alpha_1, \beta_1\} = \max\{\alpha_2, \beta_2\} \text{ and } \alpha_1 < \alpha_2 \quad \text{or} \\
\text{(c)} & \max\{\alpha_1, \beta_1\} = \max\{\alpha_2, \beta_2\} \text{ and } \alpha_1 = \alpha_2 \text{ and } \beta_1 < \beta_2.
\end{array}$$

It is immediate that $\prec$ is a linear ordering, and straightforward to show it is a well-ordering. *Exercise*

For any ordinal λ, the map $\gamma \mapsto (0, \gamma)$ for $0 \le \gamma < \lambda$, is an injection from $\langle \lambda, < \rangle$ into $\langle \lambda \times \lambda, \prec \rangle$. It follows that the well-ordering $\langle \lambda, < \rangle$ is isomorphic to an initial segment of $\langle \lambda \times \lambda, \prec \rangle$.

However, it need *not* be the case that $\langle \lambda, < \rangle$ is isomorphic to a *proper* initial segment of $\langle \lambda \times \lambda, \prec \rangle$. For example, $\langle \omega, < \rangle$ is isomorphic to $\langle \omega \times \omega, \prec \rangle$, that is to $\langle \aleph_0 \times \aleph_0, \prec \rangle$. *Exercise*

We claim that for *every (infinite) cardinal* κ the well-ordering $\langle \kappa, < \rangle$ is isomorphic to the well-ordering $\langle \kappa \times \kappa, \prec \rangle$, and so not to a *proper* initial segment.[1]

If the claim is false, let κ be the least cardinal such that the well-ordering $\langle \kappa, < \rangle$ is isomorphic to a *proper* initial segment of $\langle \kappa \times \kappa, \prec \rangle$ (and so not to $\langle \kappa \times \kappa, \prec \rangle$ itself).

[1] This is subtle. The well-orderings

$0, 1, 2, \ldots, n, \ldots$ $\qquad$ n an integer

$(0,0), (1,1), (2,2), \ldots, (n,n)$

Let the proper initial segment be $\{(\alpha,\beta) : (\alpha,\beta) \prec (\gamma,\delta)\}$, where $\gamma,\delta < \kappa$. Let $\xi = \max\{\gamma,\delta\}$. Then

$$\langle\kappa,<\rangle \cong \{(\alpha,\beta) : (\alpha,\beta) \prec (\gamma,\delta)\} \subseteq \xi \times \xi,$$

where $\cong$ denotes isomorphism of order types.

Taking cardinalities of $\langle\aleph_\zeta,<\rangle$ and $\xi \times \xi$, $\aleph_\zeta \leq |\zeta|^2$ (where $|\zeta|$ is the cardinality of ζ). □

Proposition 12.11. *There is a well-order of* On × On *such that, for each fixed* α*, the set* $\alpha \times \mathrm{On}$ *is an initial segment isomorphic to* On*. In particular,* $|\alpha \times \alpha| = |\alpha|$ *for every infinite ordinal* α*.*

Idea. Order pairs (α,β) by the maximum first, breaking ties by first then second coordinate. This is a well-order with the stated initial segment property. A minimal-counterexample argument yields a bijection $\alpha \times \alpha \cong \alpha$ for infinite α. □

Theorem 12.12 (Cardinal arithmetic for infinite cardinals). *If at least one of* κ,λ *is infinite, then*

$$\kappa \cdot \lambda = \kappa + \lambda = \max\{\kappa,\lambda\}.$$

Proof. Let $\mu = \max\{\kappa,\lambda\}$. Then $\mu \leq \kappa \cdot \lambda \leq \mu \cdot \mu = \mu$ by Proposition 12.11. For addition, $\mu \leq \mu + \mu \leq \mu \cdot 2 = \mu$; equivalently, partition μ into two disjoint subsets each equinumerous with μ. □

Definition 12.13. $2^\kappa := |\mathcal{P}(\kappa)|$.

Theorem 12.14 (Cantor). $\kappa < 2^\kappa$ *for every cardinal* κ*.*

Proof. If $f : \kappa \to \mathcal{P}(\kappa)$ were surjective, let $A = \{\alpha \in \kappa : \ \alpha \notin f(\alpha)\}$. Then $A = f(\gamma)$ for some γ, giving $\gamma \in A \iff \gamma \notin A$, a contradiction. □

Remark 12.15. Thus $|\mathbb{R}| = 2^{\aleph\_0}$. The Continuum Hypothesis asserts $2^{\aleph\_0} = \aleph\_1$; the Generalised Continuum Hypothesis asserts $2^\kappa = \kappa^+$ for all infinite κ.

Proposition 12.16. *If* A *is infinite with* $|A| = \kappa$*, then the set* S *of finite sequences of elements of* A *also has cardinality* κ*.*

Exercise. Show $\bigcup\_n < \omega A^n$ has size κ when κ is infinite. □

Chapter 13

Zermelo–Frankel Set Theory

Zermelo-Fraenkel set theory, usually ZF or ZFC, is a first-order theory with equality in the language $\mathcal{L}_\in$ having just the one non-logical binary relation $\in$, for membership. We discuss the axioms for set theory, and their models, in the following sections.

So how can there be a first-order theory for set theory, where we certainly *do have* quantifiers ranging over subsets? The idea is that in a model of set theory the sets will themselves be the individual members of the model of the axioms being considered.

The ZFC axioms for set theory are essentially sufficient to establish all of the properties of set theory needed in mathematics. And essentially all of mathematics *can* be described within set theory.

There is no "free lunch" however. The ZFC axioms for set theory do not fully mirror our informal intuition about what sets should be. There are infinitely many non-standard models of set theory also satisfying the ZFC axioms. Peano axioms for arithmetic and axioms for the real number system similarly have non-standard models. These non-standard models have some amazing and beautiful applications which are developed in the subject of non-standard analysis. For starters, you might look at (Keisler, 2000) and (Keisler, 2022)

GB Set Theory

There *are* extensions of the ZF and ZFC axioms which include variables ranging over classes of sets. This is known as Bernays-Gödel set theory and denoted BG and BGC respectively. All sets are classes but not conversely, and classes are describable by first-order formulae in the original ZF language. There is even a class of all sets, but classes cannot be elements of other sets or of other classes. See (Jech, 2003, p 70). The BG and BGC extensions are convenient but they do not introduce any profound new ideas.

13.1 Metatheory

DON'T

If you want to see detailed discussions of the metatheory, references are
I STRONGLY recommend against wasting time by doing so at this stage. It would be like exploring underground caves without a flashlight.
We will discuss models of ZF (and so in particular of ZFC) by using the same simple elementary set theory as we use to discuss models of group theory and models of linear

orderings.

However, it may seem paradoxical to discuss set theory by using set theory, the latter being called the *metatheory* in this context. But the metatheory is usually simple and constructive and does not use sophisticated notions from ZFC.

In particular, the discussion of proofs in Chapter 3 is finitistic. Basically it is all about marks on a piece of paper and allowable ways to manipulate them. The proof of Gödel's completeness theorem concerning the construction of a model is not finitistic, but in the case of a countable language (as for ZFC, for groups and for linear orderings) it is still fairly constructive and non-controversial philosophically. Although one proceeds through a countably infinite number of steps, each step is of a similar type, and is not unlike the notion of constructing the positive integers by adding one at each step. The proofs in Chapter 9 of the Gödel incompleteness theorems are constructive and finitistic.

13.2 Structures (V,in)

Just as there are many non-isomorphic models of the axioms for a linear ordering, and of the axioms for a group, there will be many different models for ZF and ZFC. But we are trying to capture in the ZFC axioms our intuitive idea of a universe of sets by means of a structure $\{V, \in\}$ where V is a (meta)set in the meta-universe in which we discuss models of various first-order theories, and $\in$ is a binary relation on V. We write $a \in b$ for $\in(a, b)$.

So $\{V, \in\}$ will be a model of (or occasionally just some of) the ZFC axioms. The axioms are discussed on pages 53-61 of (Johnstone, 1987) and will be discussed here.

As strange as it may seem, there will even be countable models $\{V, \in\}$ of ZFC, although within ZFC we can prove the existence of uncountable sets. The point is that a one-one correspondence that exists in the metatheory between the natural numbers and the members of V will not be represented by any member of V.

Along with the axioms themselves, it is helpful to simultaneously think of their intended interpretation in a fixed structure $\{V, \in\}$.

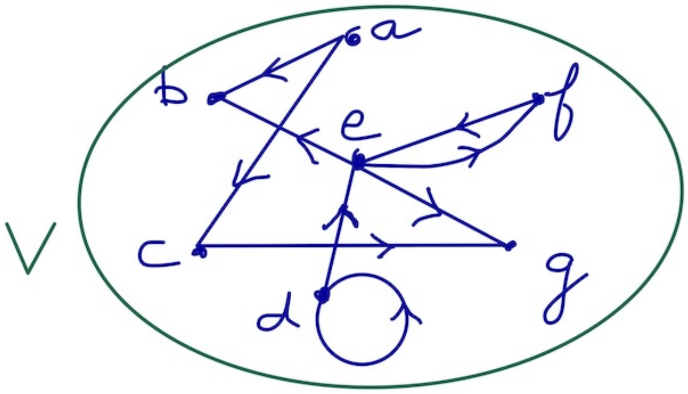


Figure 13.1: A very silly example of a $\{V, \in\}$ structure. Read the arrow from a to b as "b is a member of a". Probably no ZF axioms hold here.

Analogous to the situation for structures concerning the language of groups or the language of linear orderings, V *is a set in the metatheory* and $\in$ is a binary relation on V called the *membership relation*.

It is sometimes helpful to have a diagram in mind. In Figure 13.1,

$$b \in a, \quad c \in a.$$

We could write $\in ba$, but since we are humans and not computers we do not do so. Noting the direction of the relevant arrows, we do sometimes write $a \ni b$ and $a \ni c$.

Similarly,

$$b \in a,\ c \in a; \quad g \in c; \quad d \in d,\ e \in d; \quad b \in e,\ f \in e,\ g \in e; \quad f \in f \quad .$$

We can also write

$$a = \{b, c\}, \quad b = \varphi, \quad c = \{g\}, \quad d = \{d, e\}, \quad e = \{b, f, g\}, \quad f = \{f\}, \quad g = \varphi.$$

In particular, b and g have no members.

13.2.1 Notation for first-order language v. metalanguage

In the previous example, following the notation conventions of (Johnstone, 1987, page 53), a, b, c, d, e, f, g are *elements* of V and so are called *sets*.

We read $b \in a$ as b *belongs* to a, b is a *member* of a, b is an *element* of a, or a *contains* b. More precisely, $b \in a$ is the assertion that the first-order formula $v_1 \in v_2$ interpreted in $\{V, \in\}$ with v_1 assigned the value b and v_2 assigned the value a, is true.

On the other hand, we say a, b, c, d, e, f, g are *in* (the meta-set) V. Note this is a statement in the *metalanguage*, since in particular V is not a set in V.

Often we will not be so careful in terms of our terminology. It should be clear from context what is intended.

[This chapter to be completed]

Chapter 14

Extras

[This chapter to be completed]

References

The books and notes closest to the material in this course are (Leary and Kristiansen, 2015; Hils and Loeser, 2019; Johnstone, 1987; Leader, 2012; Zsák, 2025).

Of the first two books, (Leary and Kristiansen, 2015) is slower and perhaps best for a first introduction. However, in the first two chapters the excessive amount of notation and detail leads to rather tedious reading. It takes 86 pages to build up the necessary framework and prove Gödel's Completeness Theorem.

The book (Hils and Loeser, 2019) is a clean but succinct treatment and contains a lot of material — good for the second time around. It takes a mere 25 (and smaller) pages for the corresponding proof of Gödel's Completeness Theorem.

The treatment in the current notes, together with class lectures, is somewhere between these two books. Perhaps you could consider this treatment as motivation for the material in Hils and Loeser's book, or as an overview of Leary and Kristiansen's book!

*** Marker's book

(Johnstone, 1987) is the text for a Cambridge course but is not so clearly written. Chapters have no further divisions and they read more like a detailed transcription of the lectures.

The notes (Leader, 2012) and (Zsák, 2025) by subsequent lecturers for the Cambridge course are in most part closely based on Johnstone's book and are easier to follow.

The above five books/lecture notes are freely (and legally) available through the author's websites or otherwise, with links below.

Batzoglou, Serafim. 2024. *Introduction to Incompleteness: From Gödel's Theorems to Forcing and the Continuum Hypothesis*, Birkhäuser.

Lots of material. Similar approach to Chang and Keisler for Gödel's Completeness Theorem.

Chang, C. C. and H. Jerome Keisler. 2012. *Model Theory*, Dover. From 3rd ed Elsevier 1989

Well-written, the approach to Gödel's Completeness Theorem in these Notes is modelled on that in this book.

Church, Alonzo. 1956. *Introduction to Mathematical Logic*, Princeton University Press.

Primarily of historical interest.

Cunningham, Daniel W. 2023. *Mathematical Logic*, De Gruyter.

A more elementary approach with much detail.

Doxiadis, Apostolos and Christos H. Papadimitriou. 2009. *Logicomix: An Epic Search for Truth*, Bloomsbury.

A fun graphic novel in comic-book style about the life and work of Bertrand Russell and the foundations of logic.

Dudley, R. M. 2002. *Real analysis and probability*, Cambridge Studies in Advanced Mathematics, vol. 74, Cambridge University Press.

Revised reprint of the 1989 original.

Enderton, Herbert B. 2001. *A Mathematical Introduction to Logic*, 2nd ed., Academic Press.

A classic, somewhat dated.

Feferman, Anita Burdman. 1993. *From Trotsky to Gödel: The Life of Jean Van Heijenoort*, A.K. Peters.

With an Appendix by Solomon Feferman. The Fefermans knew Van Heijenoort professionally and socially.

Franzén, Torkel. 2005. *Gödel's Theorem: An Incomplete Guide to Its Use and Abuse*, A K Peters.

A well-written exposition at a mostly non-technical level.

______. 2006. *The Popular Impact of Gödel's Incompleteness Theorem*, Notices of the American Mathematical Society **53**, no. 4, 440–443.

Goldstern, Martin and Haim Judah. 1995. *The Incompleteness Phenomenon*, A K Peters. Corrected reprint, 2002.

Based on lectures given at Berkeley and Bar Ilan. Good informal exposition of various topics.

Hamkins, Joel David. 2021. *Lectures on the Philosophy of Mathematics*, MIT Press.

Henkin, Leon. 1949. *The completeness of the first-order functional calculus*, J. Symbolic Logic **14**, no. 3, 159–166.

______. 1996. *The discovery of my completeness proofs*, Bulletin of Symbolic Logic **2**, no. 2, 127–158.

Interesting historical discussion, comments on the nature of mathematical discovery, Henkin's indirect route to his proof of the Completeness Theorem. Observation C (pp. 156–157) gives improvements in the proof as a result of Henkin's course teaching, and which is the method used in these Notes.

Hils, Martin and François Loeser. 2019. *A First Journey Through Logic*, Springer.

Similar Hilbert system and completeness proof as for these notes.

Hinman, Peter G. 2005. *Fundamentals of Mathematical Logic*, A K Peters.

Mostly well-written, introductory graduate level, enough material for 4 courses at that level.

Jech, Thomas. 2003. *Set Theory: The Third Millennium Edition, Revised and Expanded*, 3rd ed., Springer.

Well written exensive treatment of modern set theory.

Johnstone, Peter T. 1987. *Notes on Logic and Set Theory*, Cambridge University Press.

Sometimes difficult to follow. No section breaks within chapters. Reads like a transcription of Johnstone's lectures at Cambridge.

Keisler, H. Jerome. 2000. *Elementary Calculus: An Infinitesimal Approach*, Dover Publications. `https://people.math.wisc.edu/~hkeisler/calc.html`.

First year calculus based on non-standard techniques.

______. 2022. *Foundations of Infinitesimal Calculus*, Prindle, Weber & Schmidt. `https://people.math.wisc.edu/~hkeisler/foundations.pdf`.

Well-written and rigorous treatment of the material in (Keisler, 2000).

Knuth, Donald E. 1976. *Mathematics and Computer Science: Coping with Finiteness*, Science **194**, no. 4271, 1235–1242.

Introduces the up-arrow $\uparrow\uparrow$ notation. Well-written, entertaining, for the non-expert.

Kozen, Dexter C. 1997. *Automata and Computability*, Undergraduate Texts in Computer Science, Springer.

For a Cornell computer science course. Discusses much of the material in these Notes.

Kunen, Kenneth. 2009. *The Foundations of Mathematics*, College Publications.

Well written, a lot of detail.

Leader, Imre. 2012. *Logic and Set Theory*.

Based on Johnstone's book, easier to follow.

Leary, Christopher C. and Lars Kristiansen. 2015. *A Friendly Introduction to Mathematical Logic*, 2nd ed., Milne Library.

Marker, David. 2015. *Metamathematics*.

For a first year graduate level course, extracts from his book.

______. 2024. *An Invitation to Mathematical Logic*, Springer.

Well written graduate level text.

Mendelson, Elliott. 2015. *Introduction to Mathematical Logic*, 6th ed., CRC Press.

A classic, but somewhat old-fashiuoned.

Meyer, Albert R. and Dennis M. Ritchie. 1967. *The complexity of loop programs*, Proceedings of the ACM National Meeting, 465–469.

The first to explicitly develop the connection between primitive/general recursive functions and for/while loops in a computer program.

Rathjen, Michael. *Proof Theory*, The Stanford Encyclopedia of Philosophy (Winter 2024 Edition).

See Section 2 for an overview discussion of Gentzen's Consistency Proof for Peano Arithmetic.

Potter, Michael. 2004. *Set Theory and Its Philosophy: A Critical Introduction*, Oxford University Press.

The interplay between mathematical results and philosophical reflection.

Rautenberg, Wolfgang. 2010. *A Concise Introduction to Mathematical Logic*, 3rd ed., Springer.

Rogers, Hartley Jr. 1987. *Theory of Recursive Functions and Effective Computability*, MIT Press.

A classic. The first four Sections in particular, are a very readable introduction.

Simpson, Stephen G. 2009. *Foundations of Mathematics*, Springer.

Smith, Peter. 2007. *An Introduction to Gödel's Theorems*, Cambridge University Press.

———. 2020. *Gödel Without (Too Many) Tears*, Cambridge University Press.

Soare, Robert I. 2016. *Turing Computability: Theory and Applications*, Springer.

An excellent readable text, with extensive motivation and history.

Srivastava, Shashi Mohan. 2013. *A Course on Mathematical Logic*, 2nd ed., Springer.

Tanaka, Kazuyuki. 2024. *Logic and Computation 1*.

Detailed slides from a lecture course.

Tarski, Alfred. 1931. *The concept of truth in formalized languages*, — Logic, Semantics, Metamathematics: Papers from 1923 to 1938 (edn 2, 1983), pp. 152–278.

A detailed analysis of truth from a philosophical and mathematical perspective.

———. 1944. *The Semantic Conception of Truth and the Foundations of Semantics*, Philosophy and Phenomenological Research **4**, no. 3, 341–376.

A readable summary of Tarski's previous work (Tarski, 1931).

Towsner, Henry. 2013. *Proof Theory Lecture Notes*.

Propositional and First-order Logic, Peano Arithmetic, Gentzen Sequent Calculus, Reverse Mathematics.

———. 2020a. *Goodstein's Theorem, Big Functions, and Unprovability*. Online Talks.

———. 2020b. *Goodstein's Theorem, ϵ_0, and Unprovability*.

Notes related to the online talks.

Uzquiano, Gabriel. 2022. *Quantifiers and Quantification*.

van Dalen, Dirk. 2013. *Logic and Structure*, 5th ed., Springer.

Wolf, Robert S. 2005. *A Tour Through Mathematical Logic*, Mathematical Association of America.

A user friendly survey.

Zach, Richard. 2016. *The Open Logic Text, available at* `https://openlogicproject.org/`.

Zsák, András. 2025. *Logic and Set Theory*.

Based on Johnstone's book, easier to follow.