## Contents

Chapter 1. First-order Structures 5  
1.1. Structures 5  
1.2. Homomorphisms, Substructures, Products 6  
1.3. First-Order Logic 8  
1.4. Compactness 11  

Chapter 2. Preservation Theorems 17  
2.1. The Homomorphism Preservation Theorem 17  
2.2. Saturation 20  
2.3. Proof of the Homomorphism Preservation Theorem 25  
2.4. The Theorem of Loś-Tarski 26  

Chapter 3. Algebras and Varieties 29  
3.1. Lattices 29  
3.2. Congruences 29  
3.3. Birkhoff’s Theorem 30  
3.4. Maltsev Conditions 38  

Chapter 4. Finite Model Theory 43  
4.1. Second-Order Logic 43  
4.2. Existential Second-Order Logic 45  
4.3. Least Fixed-Point Logic 50  
4.4. Non-Definability and Games 53  

Appendix A. Set Theory 57  
A.1. Sets and Classes 57  
A.2. Ordinals 58  
A.3. Cardinals 59  

Appendix B. Solutions to Exercises 63  
B.1. Exercise 7 (∗) 63  
B.2. Exercise 17 63  
B.3. Exercise 24 64  

Bibliography 65
CHAPTER 1

First-order Structures

This chapter is an introduction to first-order logic for mathematics students on bachelor level that have already followed courses in linear algebra, calculus, and algebra. We introduce first-order logic relatively quickly to then focus on constructions and results that are particularly important for applications of logic and model theory in mathematics. In particular, we treat ultraproducts and the compactness theorem. These concepts will also be important in the subsequent chapter on preservation theorems. More background in logic and model theory can be found in Hodges’ model theory [3]; a short version is also available [4]. A more recent textbook has been written by Tent and Ziegler [7]. A German text book on first-order logic is [2].

1.1. Structures

A signature $\tau$ is a set of relation and function symbols, each equipped with an arity $k \in \mathbb{N}$. A $\tau$-structure $A$ is a set $A$ (the domain of $A$) together with

- a relation $R^A \subseteq A^k$ for each $k$-ary relation symbol $R \in \tau$. Here we allow the case $k = 0$, in which case $R^A$ is either empty or of the form $\{()\}$, i.e., the set consisting of the empty tuple;
- a function $f^A : A^k \to A$ for each $k$-ary function symbol $f \in \tau$; here we also allow the case $k = 0$ to model constants from $A$.

Unless stated otherwise, $A, B, C, \ldots$ denotes the domain of the structure $A, B, C, \ldots$, respectively. We sometimes write $(A; R^A_1, R^A_2, \ldots, f^A_1, f^A_2, \ldots)$ for the structure $A$ with relations $R^A_1, R^A_2, \ldots$ and functions $f^A_1, f^A_2, \ldots$. We say that a structure is infinite if its domain is infinite. If all symbols in $\tau$ are function symbols, then a $\tau$-structure $A$ is also called an algebra (in the sense of universal algebra); in the other extreme, if all symbols in $\tau$ are relation symbols, then $A$ is called a relational structure.

Example 1.1.1. A group is a structure $(G, \circ)$ with a binary function symbol $\circ$ which satisfies the following axioms:

\begin{align*}
\forall x, y, z. (x \circ y) \circ z &= x \circ (y \circ z) & \text{(associativity)} \\
\exists e \forall y. e \circ y &= y \circ e = y & \text{(neutral element e)} \\
\forall y \exists z. y \circ z &= z \circ y = e & \text{(inverse elements)}
\end{align*}

Other examples of well-known structures from algebra are fields, vector spaces, rings, etc.

Example 1.1.2. A (simple, undirected) graph is a pair $(V, E)$ consisting of a set of vertices $V$ and a set of edges $E \subseteq \binom{V}{2}$, that is, $E$ is a set of 2-element subsets of $V$. Graphs can be modelled using relational structures $G$ using a signature that contains a single binary relation symbol $R$, putting $G := V$ and adding $(u, v)$ to $R^G$ if $\{u, v\} \subseteq E$. If we insist that a structure with this signature satisfies $(x, y) \in R^G \Rightarrow (y, x) \in R^G$ and $(x, x) \notin R^G$, then we can associate to such a structure an undirected graph and obtain a bijective correspondence between undirected graphs with vertices $V$ and structures $G$ with domain $V$ as described above.
1.2. Homomorphisms, Substructures, Products

1.2.1. Homomorphisms. In the following, let $A$ and $B$ be $\tau$-structures. A homomorphism $h$ from $A$ to $B$ is a mapping from $A$ to $B$ that preserves each function and each relation for the symbols in $\tau$; that is,

- if $(a_1, \ldots, a_k)$ is in $R^A$, then $(h(a_1), \ldots, h(a_k))$ must be in $R^B$;
- $f^B(h(a_1), \ldots, h(a_k)) = h(f^A(a_1, \ldots, a_k))$.

A homomorphism from $A$ to $B$ is called a strong homomorphism if it also preserves the complements of the relations from $A$. Injective strong homomorphisms are called embeddings. Surjective embeddings are called isomorphisms.

Example 1.2.1. Group homomorphisms, field endomorphisms, ring endomorphisms, linear maps between vector spaces.

Example 1.2.2. The graph colorability problem is an important problem in discrete mathematics, with many applications in theoretical computer science (it can be used to model e.g. frequency assignment problems). As a computational problem, the graph $n$-colorability problem has the following form.

**Given:** a finite graph $G = (V, E)$.

**Question:** can we colour the vertices of $G$ with $n$ colours such that adjacent vertices get different colours?

The $n$-colorability problem can be formulated as a graph homomorphism problem: is there a homomorphism from $G$ to $K_n := (\{1, \ldots, n\}; E_{K_n})$ where $E_{K_n} := \{(u, v) \in V^2 \mid u \neq v\}$.

We also refer to these homomorphisms as proper colourings of $G$, and say that $G$ is $n$-colourable if such a colouring exists. The chromatic number $\chi(G)$ of $G$ is the minimal natural number $n \in \mathbb{N}$ such that $G$ is $n$-colourable. For example, the chromatic number of $K_n$ is $n$.

Exercises.

1. We know that the neutral element in groups is unique. Show that any homomorphism from a group $G$ to a group $H$ maps the neutral element of $G$ to the neutral element of $H$.

Example 1.2.3. We present a concrete instance of a colouring problem from pure mathematics. Let $(V, E)$ the unit distance graph on $\mathbb{R}^2$, i.e., the graph has the vertex set $V := \mathbb{R}^2$ (we imagine the nodes as the points of the Euclidean plane) and edge set $E := \{(x, y) \in V^2 \mid |x - y| = 1\}$.

In other words, two points are linked by an edge if they have distance one. What is the chromatic number of this graph?

We claim that we need at least four colours. This follows easily from the following observations.

- The graph depicted in Figure 4.2, the so-called Golomb graph, appears as a subgraph $(V', E')$ of $(V, E)$, i.e., $V' \subseteq V$ and $E' \subseteq E \cap \binom{V}{2}$.
- To properly color this graph, we need at least four colours (this fact is easily verified by hand).
- If we need four colours to colour a subgraph of $(V, E)$, then we also need four colours for $(V, E)$.

The following statement follows from the compactness theorem of first-order logic, as we will see later in this chapter.
1.2. HOMOMORPHISMS, SUBSTRUCTURES, PRODUCTS

Figure 1.1. The 10-vertex Golomb Graph, drawn in the plane such that adjacent vertices are at distance one, along with a proper four-colouring.

Proposition 1.2.4. Let $G$ be a graph such that all finite subgraphs of $G$ are $k$-colourable. Then $G$ is $k$-colourable.

The problem to determine the chromatic number $\chi$ of this graph is known as the Hadwiger-Nelson problem. We have seen that $4 \leq \chi$. It is known that $\chi \leq 7$. The precise value of $\chi \in \{4, 5, 6, 7\}$ is not known.

1.2.2. Substructures. A $\tau$-structure $A$ is a substructure of a $\tau$-structure $B$ iff

- $A \subseteq B$,
- for each $R \in \tau$, and for all tuples $\bar{a}$ from $A$, $\bar{a} \in R^A$ iff $\bar{a} \in R^B$, and
- for each $f \in \tau$ we have that $f^A(\bar{a}) = f^B(\bar{a})$.

In this case, we also say that $B$ is an extension of $A$. Substructures $A$ of $B$ and extensions $B$ of $A$ are called proper if the domains of $A$ and $B$ are distinct.

Note that for every subset $S$ of the domain of $B$ there is a unique smallest substructure of $B$ whose domain contains $S$, which is called the substructure of $B$ generated by $S$, and which is denoted by $B[S]$.

Example 1.2.5. A group (compare with Example 1.2.5) can also be seen as a structure $G$ with a binary function symbol $\circ$ for composition, a unary function symbol $^{-1}$ for taking the inverse, and a constant denoted by $e$, satisfying the sentences

- $\forall x, y, z. x \circ (y \circ z) = (x \circ y) \circ z$,
- $\forall x. x \circ x^{-1} = 1$,
- $\forall x. e \circ x = x$, and $\forall x. x \circ e = x$.

In this signature, the subgroups of $G$ are precisely the substructures of $G$ as defined above. Note that all axioms are universal in the sense that all the variables are universally quantified (more on that comes later).

Example 1.2.6. When we view a graph as an $\{E\}$-structure $G$, then a subgraph is not necessarily a substructure of $G$. In graph theory, the substructures of $G$ are called induced subgraphs: the difference is that in an induced subgraph $(V', E')$ of $(V, E)$ the edge set must be of the form $E' := E \cap \binom{V'}{2}$ instead of an arbitrary subset of it.

1.2.3. Products. Let $\tau$ be a relational signature. Let $A$ and $B$ be $\tau$-structures. Then the (direct, or categorical) product $C = A \times B$ is the $\tau$-structure with domain $A \times B$, which has for each $k$-ary $R \in \tau$ the relation that contains a tuple $((a_1, b_1), \ldots, (a_k, b_k))$ if and only if $R(a_1, \ldots, a_k)$ holds in $A$ and $R(b_1, \ldots, b_k)$ holds in $B$. For each $k$-ary $f \in \tau$ the structure $C$ has the operation that maps $((a_1, b_1), \ldots, (a_k, b_k))$ to $(f(a_1, \ldots, a_k), f(b_1, \ldots, b_k))$. The direct product $A \times A$ is also denoted by $A^2$, and the $k$-fold product $A \times \cdots \times A$, defined analogously, by $A^k$. 
With the seemingly simple definitions of graph homomorphisms and direct products we can already formulate very difficult open combinatorial questions.

Conjecture 1.1 (Hedetniemi). Suppose that \( G \times H \rightarrow K_n \). Then \( G \rightarrow K_n \) or \( H \rightarrow K_n \).

This conjecture is easy for \( n = 1 \) and \( n = 2 \) (Exercise 2), and has been solved for \( n = 3 \) by N. Sauer and M. El-Zahar\(^1\). For \( n = 4 \) the conjecture is already open.

Exercises.
(2) Prove the Hedetniemi conjecture for \( n = 1 \) and \( n = 2 \).

1.3. First-Order Logic

To define the syntax of first-order logic, we first have to introduce terms, before we can define (first-order) formulas and (first-order) sentences, and finally (first-order) theories.

1.3.1. Terms. Let \( \tau \) be a signature. In this section we will see how to use the function symbols in \( \tau \) to build terms. Well-known examples of terms are polynomials: they are terms over a signature that contains a binary symbol + for addition and a binary symbol \( \ast \) for multiplication, together with constant symbols. Later, when we define the semantics of first-order logic, we will see how terms over a given \( \tau \)-structure describe functions (in the same way as polynomials describe polynomial functions over a given ring).

Definition 1.3.1. A (\( \tau \))-term is defined inductively:
- constants from \( \tau \) are \( \tau \)-terms;
- variables \( x_0, x_1, \ldots \) are \( \tau \)-terms;
- if \( t_1, \ldots, t_k \) are \( \tau \)-terms, and \( f \in \tau \) has arity \( k \), then \( f(t_1, \ldots, t_k) \) is a \( \tau \)-term.

We write \( t(x_1, \ldots, x_n) \) if all variables that appear in \( t \) come from \( \{x_1, \ldots, x_n\} \); we do not require that each variable \( x_i \) appears in \( t \).

1.3.2. Semantics of terms. Let \( \mathcal{A} \) be a \( \tau \)-structure and let \( x_1, \ldots, x_n \) be distinct variables. Every \( \tau \)-term \( t(x_1, \ldots, x_n) \) describes a function \( t^\mathcal{A} : \mathcal{A}^n \rightarrow \mathcal{A} \) as follows:
- if \( t \) equals \( c \in \tau \) then \( t^\mathcal{A} \) is the function \( (a_1, \ldots, a_n) \mapsto c^\mathcal{A} \);
- if \( t \) equals \( x_i \) then \( t^\mathcal{A} \) is the function \( (a_1, \ldots, a_n) \mapsto a_i \);
- if \( t \) equals \( f(t_1, \ldots, t_k) \) for a \( k \)-ary \( f \in \tau \) then \( t^\mathcal{A} \) is the function \( (a_1, \ldots, a_n) \mapsto f^\mathcal{A}(t_1^\mathcal{A}(a_1, \ldots, a_n), \ldots, t_k^\mathcal{A}(a_1, \ldots, a_n)) \).

Note that item 1 is a special case of item 3. The function described by \( t \) is also called the term function of \( t \) (with respect to \( \mathcal{A} \)).

1.3.3. First-order formulas. Let \( \tau \) be a signature. The relation symbols in the signature \( \tau \) did not play any role when defining \( \tau \)-terms, but they become important when defining \( \tau \)-formulas. Moreover, the equality symbol = is ‘hard-wired’ into first-order logic; we can use it to create formulas by equating terms. Finally, we can combine formulas using Boolean connectives, and quantify over variables.

Definition 1.3.2. An atomic (\( \tau \))-formula is an expression of the form
- \( t_1 = t_2 \) where \( t_1 \) and \( t_2 \) are \( \tau \)-terms;

---

\(^1\)The chromatic number of the product of two 4-chromatic graphs is 4, Combinatorica, 5(2):121-126, 1985.
• $R(t_1, \ldots, t_k)$ where $t_1, \ldots, t_k$ are $\tau$-terms and $R \in \tau$ is a $k$-ary relation symbol.

Formulas are defined inductively as follows:

• atomic formulas are formulas;
• if $\phi$ is a formula, then $\neg \phi$ is a formula (negation);
• if $\phi$ and $\psi$ are formulas, then $\phi \land \psi$ is a formula (conjunction);
• if $\phi$ is a formula, and $x$ is a variable, then $\exists x. \phi$ is a formula (existential quantification)

Atomic formulas and negations of atomic formulas are sometimes called literals. Similarly as for terms, we write $\neg \phi$ instead of ($\phi$)

1.3.4. Semantics of formulas. Every $\tau$-formula $\phi(x_1, \ldots, x_n)$ describes a relation $\phi^A \subseteq A^n$ as follows:

• if $\phi$ equals $t_1 = t_2$ then $\phi^A$ is the relation $
\{(a_1, \ldots, a_n) \mid t_1^A(a_1, \ldots, a_n) = t_2^A(a_1, \ldots, a_n)\}$
• if $\phi$ equals $R(t_1, \ldots, t_k)$ then $\phi^A := \{(a_1, \ldots, a_n) \mid (t_1^A(\bar{a}), \ldots, t_k^A(\bar{a})) \in R^A\}$
• if $\phi$ equals $\phi_1 \land \phi_2$ then $\phi^A := \phi_1^A \cap \phi_2^A$;
• if $\phi$ equals $\neg \psi$ then $\phi^A := A^n \setminus \phi^A$;
• if $\phi$ equals $\exists x. \psi(x, x_1, \ldots, x_n)$ then

$\phi^A := \{(a_1, \ldots, a_n) \mid \exists a \in A \text{ s.t. } (a, a_1, \ldots, a_n) \in \psi^A\}$

We freely use brackets to avoid ambiguities when writing down terms. The is, we write $\neg (x \land y)$ to distinguish it from $\neg x \land y$. If brackets are omitted, there is the convention that negation $\neg$ binds stronger than conjunction $\land$; that is, $\neg x \land y$ would stand for $(\neg x) \land y$.

For $\phi(x_1, \ldots, x_n)$ we write

$A \models \phi(a_1, \ldots, a_n)$

instead of $(a_1, \ldots, a_n) \in \phi^A$. In particular, if $\phi$ is a sentence, i.e., if $n = 0$, we write $A \models \phi$, and say that $A$ satisfies $\phi$, if $\langle \rangle \in \phi^A$ (that is, if $\phi^A \neq \emptyset$).

EXAMPLE 1.3.3. The following statements about well-known structures follow straightforwardly from the definitions.

• $(\mathbb{Z}; <) \models 0 < 1$
• $(\mathbb{Q}; <) \models \forall x, y \; (x < y \Rightarrow \exists z \; (x < z \land z < y))$ (density)
• $(\mathbb{Z}; <) \not\models \forall x, y \; (x < y \Rightarrow \exists z \; (x < z \land z < y))$

Shortcuts:

• Disjunction: $\phi \lor \psi$ is an abbreviation for $\neg (\neg \phi \land \neg \psi)$
• Implication: $\phi \Rightarrow \psi$ is an abbreviation for $\neg \phi \lor \psi$
• Equivalence: $\phi \Leftrightarrow \psi$ is an abbreviation for $\phi \Rightarrow \psi \land \psi \Rightarrow \phi$
• universal quantification: $\forall x. \phi(x)$ is an abbreviation for $\neg \exists x. \neg \phi(x)$
• inequality: $x \neq y$ is an abbreviation for $\neg (x = y)$
• false: $\bot$ is an abbreviation for $\exists x. x \neq x$.
• true: $\top$ is an abbreviation for $\neg \bot$ (the same as $\forall x. x = x$).

Moreover, when $A$ is a unary predicate, then we may write $\exists x \in A. \phi$ instead of $\exists x \; (x \in A \land \phi)$ and $\forall x \in A. \phi$ instead of $\forall x \; (x \in A \Rightarrow \phi)$.
1.3.5. **First-order sentences.** A *first-order* sentence is a formula without free variables, i.e., all variables that appear in the formula are quantified by some quantifier.

**Example 1.3.4.**
- Let $\tau = \{R\}$ where $R$ is a binary relation symbol.
  Then the following formula is an example of a first-order sentence
  $$\forall x_1, x_2, x_3 \left( R(x_1, x_2) \land R(x_2, x_3) \rightarrow R(x_1, x_3) \right)$$
  (expressing the transitivity of $R$).
- The group axioms that we have seen in Example 1.2.5 are examples of first-order sentences.

1.3.6. **First-order theories.** Let $\tau$ be a signature.

**Definition 1.3.5.** A $(\tau)$-theory is a set of first-order $\tau$-sentences.

**Example 1.3.6.** A famous example of a first-order theory is the set of axioms of Zermelo-Frankl set theory. Recall that this is an infinite set of first-order sentences over the signature $\tau = \{\in\}$. An example of a sentence in ZF is
  $$\exists x \forall y. \neg(y \in x)$$
  stating the existence of the empty set.

Let $A$ be a $\tau$-structure and $T$ a $\tau$-theory. Then $A$ is a model of $T$, in symbols $A \models T$, if $A \models \phi$ for all $\phi \in T$. A $\tau$-theory $T$ is called
- **satisfiable (or consistent)** if $T$ has a model.
- **complete** if for every $\tau$-sentence either $\phi \in T$ or $\neg \phi \in T$.

The *first-order theory* of $A$ is defined as the set of all first-order $\tau$-sentences that are satisfied by $A$. Note that $\text{Th}(A)$ is always a complete theory. We give some examples of first-order theories.

- $\text{Th}(\mathbb{Z}; <)$, $\text{Th}(\mathbb{Q}; <)$, etc.
- ZF and ZFC. Note that ZFC is not complete: for example the continuum hypothesis CH (which states that $\aleph_1 = 2^{\aleph_0}$) is independent in the sense that both ZFC $\cup \{\text{CH}\}$ and ZFC $\cup \{\neg \text{CH}\}$ have a model.

If $S$ and $T$ are $\tau$-theories then we write
  $$S \models T$$
if every model of $S$ is also a model of $T$. We also write $S \models \phi$ instead of $S \models \{\phi\}$.

1.3.7. **Vaught’s conjecture.** Let $T$ be a complete countable theory over a countable signature. How many countable models can $T$ have, up to isomorphism? Let $I(T)$ be the number of models of $T$ of cardinality $\aleph_0$, up to isomorphism, also called the spectrum of $T$. Examples:

- $I(\text{Th}(K_5)) = 0$
- $I(\text{Th}(\mathbb{Z}; <)) = \aleph_0$
- $I(\text{Th}(\mathbb{Q}; <)) = 1$
- $I(\text{Th}(\mathbb{R}; +, <)) = 2^{\aleph_0}$

Vaught’s theorem says that for any theory $T$ the spectrum $I(T)$ cannot be two. Morley showed that if $I(T)$ is infinite, then
  $$I(T) \in \{\aleph_0, \aleph_1, 2^{\aleph_0}\}$$

**Vaught’s Conjecture:** if $\kappa$ is infinite, then $I(T) \in \{\aleph_0, 2^{\aleph_0}\}$.

**Exercises.**
1.4. COMPACTNESS

(3) Write down the axioms of algebraically closed fields in first-order logic.

(4) A formula is in prenex normal form if it is of the form \( Q_1 x_1 \ldots Q_n x_n. \phi \) where \( Q_i \) is either \( \exists \) or \( \forall \) and \( \phi \) is without quantifiers. Show that every formula \( \phi(y_1, \ldots, y_n) \) is equivalent to a formula \( \psi(y_1, \ldots, y_n) \) in prenex normal form, that is, for every structure \( M \) we have \( M \models \forall \bar{y} (\phi(\bar{y}) \iff \psi(\bar{x})) \).

1.4. Compactness

A special case of the compactness theorem was already proved by Gödel; the general case below was proved by A. Maltsev in 1936.

**Theorem 1.4.1.** A theory \( T \) is satisfiable if \( T' \) is satisfiable for all finite \( T' \subseteq T \).

We will see below that Proposition 1.2.4 is an immediate corollary of this theorem.

In this section we present a proof of Theorem 1.4.1 based on ultraproducts, which are an important tool of model theory to build interesting structures; they have found many applications in mathematics, e.g. in topology, set theory, and algebra. But first we show a few consequences of compactness.

1.4.1. Applying Compactness.

**Corollary 1.4.2.** Let \( T \) be a first-order theory with arbitrarily large finite models. Then \( T \) has an infinite model.

**Proof.** By assumption, every finite subset of

\[
T' := T \cup \{ \exists x_1, \ldots, x_k \ \bigwedge_{1 \leq i < j \leq k} x_i \neq x_j \mid k \in \mathbb{N} \}
\]

has a model. By the compactness theorem, \( T' \) has a model, and every model of \( T' \) must be infinite. \( \Box \)

**Corollary 1.4.3.** A graph \( G = (V; E) \) is 3-colourable if and only if all its finite subgraphs are 3-colourable.

**Proof.** Let \( \tau \) be the signature \( \{ f, c_1, c_2, c_3 \} \cup \{ c_v \mid v \in V \} \) where \( f \) is a unary function symbol and all other symbols are distinct constant symbols. Consider the following \( \tau \)-theory \( T \).

\[
T := \{ f(c_u) \neq f(c_v) \mid (u, v) \in E \} \\
\cup \{ c_1 \neq c_2, c_2 \neq c_3, c_1 \neq c_3, \forall x (f(x) = c_1 \lor f(x) = c_2 \lor f(x) = c_3) \}
\]

By assumption, every finite subset of \( T \) is satisfiable. By the compactness theorem, \( T \) has a model \( M \), and \( f^M \) gives the desired 3-colouring of \( G \). \( \Box \)

**Exercises.**

(5) Let \( T \) be a first-order theory and \( \phi(x) \) a formula. Show that if \( T \) has for every \( n \in \mathbb{N} \) a model \( A \) with \( |\phi^A| \geq n \), then \( T \) has a model \( A \) such that \( \phi^A \) is infinite.

(6) Show that the compactness theorem does not hold if we allow infinite disjunctions as sentences.

(7) Show that the compactness theorem is equivalent to the following statement. If a first-order theory \( T \) has the same models as a single first-order sentence \( \phi \), there is already a finite subset of \( T \) which have the same models as \( \phi \).
1.4.2. Filter. Let $X$ be a set. A filter $\mathcal{F}$ on $X$ is a set of subsets of $X$ such that

1. $\emptyset \notin \mathcal{F}$ and $X \in \mathcal{F}$;
2. if $F \in \mathcal{F}$ and $G \subseteq F$ then $G \in \mathcal{F}$.
3. if $F_1, F_2 \in \mathcal{F}$ then $F_1 \cap F_2 \in \mathcal{F}$.

The idea is that the elements of $\mathcal{F}$ are (in some sense) ‘large’ (it helps thinking of $F \in \mathcal{F}$ being ‘almost all’ of $X$). Note that filters have the finite intersection property:

$$A_1, \ldots, A_n \in \mathcal{F} \Rightarrow A_1 \cap \cdots \cap A_n \neq \emptyset$$

(\text{FIP})

Lemma 1.4.4. Every subset $S \subseteq \mathcal{P}(X)$ with the FIP is contained in a smallest filter that contains $S$; this filter is called the filter generated by $S$.

Proof. First add finite intersections, and then all supersets to $S$. \hfill \Box

Examples:

- For non-empty subsets $Y \subseteq X$ let
  $$\mathcal{F} := \{Z \subseteq X \mid Y \subseteq Z\}$$
- The Fréchet filter: for an infinite set $X$ let
  $$\mathcal{F} := \{Y \subseteq X \mid X \setminus Y \text{ is finite}\}$$

1.4.3. Ultrafilter. A filter $\mathcal{F}$ is called a ultrafilter if $\mathcal{F}$ is maximal, that is for every filter $G \supseteq \mathcal{F}$ we have $G = \mathcal{F}$.

Lemma 1.4.5. Let $\mathcal{F}$ be a filter. Then the following are equivalent.

1. $\mathcal{F}$ is a ultrafilter.
2. For all $A \subseteq X$ either $A \in \mathcal{F}$ or $X \setminus A \in \mathcal{F}$.
3. For all $A_1 \cup \cdots \cup A_n \in \mathcal{F}$ there is an $i \leq n$ with $A_i \in \mathcal{F}$.

Proof. (1) $\Rightarrow$ (2): No $A \subseteq X$ can be added to $\mathcal{F}$. Hence, $\mathcal{F}$ is maximal. (2) $\Rightarrow$ (3): If there is an $i \leq n$ such that $\mathcal{F} \cup \{A_i\}$ has the FIP, then by Lemma 1.4.4 there is a filter that contains this set, and hence $\mathcal{F}$ was not maximal. Otherwise, there are $S_1, \ldots, S_n \subseteq \mathcal{F}$ with $A_i \cap S_i = \emptyset$. Then $S_i \in X \setminus A_i$ and thus $S_1 \cap \cdots \cap S_n \subseteq X \setminus (A_1 \cup \cdots \cup A_n) \notin \mathcal{F}$, a contradiction. \hfill \Box

Note that for every $a \in X$ the set

$$\mathcal{U} := \{Y \subseteq X \mid a \in Y\}$$

is an ultrafilter. The filters of this form are called the principal ultrafilter. Are there non-principal ultrafilters?

Lemma 1.4.6 (Ultrafilter Lemma). Every filter $\mathcal{F}$ is contained in a ultrafilter.

Proof. Let $\mathcal{M}$ be the set of all filters on $X$ that contain $\mathcal{F}$, partially ordered by containment. Note that unions of chains of filters in this partial order are again filters. By Zorn’s lemma, $\mathcal{M}$ contains a maximal filter. \hfill \Box

Non-principal ultrafilters are also called free ultrafilters. In particular the Fréchet filter is contained in an ultrafilter, which cannot be free.

Lemma 1.4.7. An ultrafilter is free if and only if it contains the Fréchet filter.

Proof. Let $\mathcal{U}$ be a free ultrafilter on $X$ and let $x \in X$. Either $\{x\} \in \mathcal{U}$ or $X \setminus \{x\} \in \mathcal{U}$. As $\mathcal{U}$ is free, $\{x\} \notin \mathcal{U}$. Hence, $X \setminus \{x\} \in \mathcal{U}$ for every $x \in X$. Let $F \subseteq X$ be finite. Then

$$X \setminus F = \bigcap_{x \in F} (X \setminus \{x\}) \in \mathcal{U}.$$
Let \( \mathcal{U} \) be a principal ultrafilter, i.e., there is \( x \in X \) with \( \{x\} \in \mathcal{U} \). Then the element \( X \setminus \{x\} \) of the Fréchet filters is not in \( \mathcal{U} \).

**1.4.4. Ultraproducts.** Let \( \tau \) be a signature, let \( \mathcal{U} \) be an ultrafilter on \( X \), and for each \( a \in X \) let \( M_a \) be a \( \tau \)-structure. The idea of ultraproducts is to define an "average" structure of all the structures \( M_a \).

**Definition 1.4.8.** We write

\[
\prod_{a \in X} M_a / \mathcal{U}
\]

for the \( \tau \)-structure \( M \) whose domain are the equivalence classes of the equivalence relation \( \sim \) defined on the set

\[
\prod_{a \in X} M_a := \{ g : X \to \bigcup_{a \in X} M_a \mid \forall a : g(a) \in M_a \}
\]

as follows:

\[
g \sim g' \iff \{ a \in X \mid g(a) = g'(a) \} \in \mathcal{U}
\]

The relations and functions of \( M \) are defined as follows:

- for constant symbols \( c \in \tau \):
  \[
c^M := [a \mapsto c^M_a]
\]
- for function symbols \( f \in \tau \) of arity \( k \):
  \[
f^M([g_1], \ldots, [g_k]) := [a \mapsto f^M_a(g_1(a), \ldots, g_k(a))]
\]
- for relation symbols \( R \in \tau \) of arity \( k \):
  \[
  R^M([g_1], \ldots, [g_k]) := \{ a \in X \mid (g_1(a), \ldots, g_k(a)) \in R^M_a \} \in \mathcal{U}
  \]

It is straightforward to verify that this is indeed well defined, because the interpretation of function and relation symbols is independent from the choice of the representatives\(^2\).

**1.4.5. The theorem of Loš.** Let \( \{ M_a \mid a \in X \} \) be a family of \( \tau \)-Structures, and let \( \mathcal{U} \) be an ultrafilter on \( X \).

**Theorem 1.4.9 (Loš).** Let \( \phi(X) \) be a first-order formula and \( \overline{g} \) be a tuple of elements of the ultraproduct \( M := \prod_{a \in X} M_a / \mathcal{U} \). Then

\[
\begin{align*}
M \models \phi(\overline{g}) & \iff \{ a \in X \mid M_a \models \phi(g(a)) \} \in \mathcal{U} \\
\end{align*}
\]

**Proof.** By induction over the syntactic form of first-order formulas.

- if \( \phi \) is atomic and of the form \( R(x_1, \ldots, x_n) \), then the statement follows from the definition of \( R^M \). If \( \phi \) contains terms then we have to do an additional induction over the recursive form of terms, which we omit.
- Suppose that the statement holds for \( \phi \) and for \( \psi \). Then

\[
\begin{align*}
M \models (\phi \land \psi)(\overline{g}) & \iff M \models \phi(\overline{g}) \land M \models \psi(\overline{g}) & \text{(semantics of conjunction)} \\
& \iff \{ a \in X \mid M_a \models \phi(g(a)) \} \in \mathcal{U} \land \{ a \in X \mid M_a \models \psi(g(a)) \} \in \mathcal{U} & \text{(inductive assumption)} \\
& \iff \{ a \in X \mid M_a \models \phi(g(a)) \} \cap \{ a \in X \mid M_a \models \psi(g(a)) \} \in \mathcal{U} & \text{(\( \mathcal{U} \) is filter)} \\
& \iff \{ a \in X \mid M_a \models (\phi \land \psi)(g(a)) \} \in \mathcal{U} & \text{(semantics of conjunction)} \\
\end{align*}
\]

\(^2\)Note that the same definition works even if \( \mathcal{U} \) is not an ultrafilter, just a filter: in this case the resulting structure is called a reduced product.
• Suppose that the statement holds for \( \phi \). Then
\[
\bar{M} \models \neg \phi([g])
\]
\[
\iff \bar{M} \not\models \phi([g])
\] (semantics of negation)
\[
\iff \{ a \in X \mid \bar{M}_a \models \phi(g(a)) \not\in \mathcal{U} \} \quad (\text{inductive assumption})
\]
\[
\iff \{ a \in X \mid \bar{M}_a \not\models \phi(g(a)) \} \subseteq \mathcal{U} \quad (\mathcal{U} \text{ is ultrafilter})
\]
\[
\iff \{ a \in X \mid \bar{M}_a \models \neg \phi(g(a)) \} \subseteq \mathcal{U} \quad (\text{semantics of negation})
\]

• Finally, suppose that the statement holds for the formula \( \phi(x, x_1, \ldots, x_k) \) and let \([g_1], \ldots, [g_k] \in \bar{M}\).
\[
\bar{M} \models (\exists x. \phi)([g_1], \ldots, [g_k])
\]
\[
\iff \text{there is } [g] \in M \text{ with } \bar{M} \models \phi([g], [g_1], \ldots, [g_k])
\]
\[
\iff \{ a \in X \mid \bar{M}_a \models \phi(g(a), g_1(a), \ldots, g_k(a)) \} \subseteq \mathcal{U}
\]
\[
\iff \{ a \in X \mid \bar{M}_a \models (\exists x. \phi)(g_1(a), \ldots, g_k(a)) \} \subseteq \mathcal{U}
\]

To see the final equivalence, note that for every \([g] \in \bar{M}\)
\[
\{ a \in X \mid \bar{M}_a \models \phi(g(a), g_1(a), \ldots, g_k(a)) \}
\]
\[
\subseteq \{ a \in X \mid \bar{M}_a \models (\exists x. \phi)(g_1(a), \ldots, g_k(a)) \}
\]

Conversely, there is \([g] \in \bar{M}\) with \( \exists x \): define \( g : X \to \bigcup_a \bar{M}_a \) as follows: for every \( a \in X \) with \( \bar{M}_a \models (\exists x. \phi)(\ldots) \) choose a witness \([h_a] \in \bar{M}\) for \( x \). Define \( g(a) := h_a \) if \( \bar{M}_a \models (\exists x. \phi)(\ldots) \) and otherwise \( g \) is defined arbitrarily. Then
\[
\{ a \in X \mid \bar{M}_a \models \phi(g(a), \ldots) \} = \{ a \in X \mid \bar{M}_a \models (\exists x. \phi)(\ldots) \}
\]
\[
\square
\]

The following can be obtained from the theorem of Loś by applying it to sentences instead of formulas, and to ultrapowers instead of ultraproducts.

**Corollary 1.4.10.**

\[
\text{Th}(\bar{M}^X/\mathcal{U}) = \text{Th}(\bar{M})
\]

The statement of the corollary is trivial if \( \mathcal{U} \) is a principal filter (why?). The statement is interesting if \( \mathcal{U} \) is free, as we see in the following example.

**Example 1.4.11.** Consider
\[
\bar{M} := (\mathbb{N}; +, *, 0, 1).
\]
There is an element \( u \) of \( \bar{M}' := \bar{M}^N/\mathcal{U} \) such that for all \( n \in \mathbb{N} \)
\[
\bar{M}' \models u > 1 + \cdots + 1 \quad \text{n times}
\]
for example \( u = [(1, 2, 3, \ldots)] \in \bar{M} \).
This distinguishes \( \bar{M}' \) from \( \bar{M} \). (Why is there no contradiction to Corollary 1.4.10?)

**Example 1.4.12.** Let \( \mathcal{U} \) be a free ultrafilter on \( \mathbb{N} \), and consider
\[
\bar{M} := (\mathbb{R}; 0, 1, +, *, \leq).
\]
Then
\[
\text{Th}(\bar{M}) = \text{Th}(\bar{M}^N/\mathcal{U})
\]

How big is \( \bar{M}^N/\mathcal{U} \)?
\[
|\bar{M}^N/\mathcal{U}| \leq |\mathbb{R}^\omega| = |(2^\mathbb{R})^\omega| = |2^{\mathbb{R}^\omega}|
\]
Note that $M^n/\mathcal{U}$ has ‘infinitesimal’ elements, i.e., elements $x$ such that for all $n \in \mathbb{N}$
\[
M \models 0 < x \wedge (1 + \cdots + 1)^n x < 1
\]
for example
\[
x = [(1,1/2,1/3,1/4,\ldots)]
\]
Abraham Robinson used this idea to develop a ‘nonstandard analysis’ which gives a formal interpretation to the reasoning with infinitely small positive entities à la Leibniz, Euler, and Cauchy.

**Exercises.**

(8) Let $n \in \mathbb{N}$ and let $M$ be a ultraproduct of finite structures each of which has at most $n$ elements. Then $M$ has at most $n$ elements, too.

(9) Show that if a first-order theory has infinite models, then it also has arbitrarily large models (for every set $X$ there is a model $M$ with $|M| \geq |X|$).

**1.4.6. Proof of the compactness theorem.** Let $T$ be a theory.

**Proof of the compactness theorem, Theorem 1.4.1.** Assume that every finite subset $S$ of $T$ has a model $M_S$. Let $X$ be the set of all finite subsets of $T$. For $\phi \in T$, let
\[
X_\phi := \{ S : X | M_S \models \phi \}.
\]
Then the set $\{ X_\phi \mid \phi \in T \}$ has the FIP: if $\phi_1, \ldots, \phi_n \in T$, let $S := \{ \phi_1, \ldots, \phi_n \} \in X$ and note that $M_S \models \phi_i$ for all $i$, and $S \in X_{\phi_i}$. Hence, $S \in X_{\phi_1} \cap \cdots \cap X_{\phi_n}$ shows that $X_{\phi_1} \cap \cdots \cap X_{\phi_n}$ is non-empty, proving the FIP.

By Lemma 1.4.4 and the ultrafilter lemma (Lemma 1.4.6) there is an ultrafilter $\mathcal{U}$ that contains $\{ X_\phi \mid \phi \in T \}$. Then $M := \prod_{S \in X} M_S/\mathcal{U}$ is a model of $T$: for $\phi \in T$ we have $X_{\phi} \in \mathcal{U}$ and $M \models \phi$ because of the theorem of Łoś.

**1.4.7. Proving the ultrafilter lemma with compactness.** Let $\mathcal{F}$ be a filter on a set $X$. We want to show that $\mathcal{F}$ is contained in an ultrafilter $\mathcal{U}$. Let $\tau = \{ P \} \cup \{ c_S \mid S \subseteq X \}$ be a signature with a unary relation symbol $P$ and constant symbols $c_S$. Informally, our idea is to construct a theory $T$ such that for every model $M$ of $T$ we have
\[
M \models P(c_S) \iff S \in \mathcal{U}.
\]
And here is such a theory.
\[
T := \{ P(c_S) \Rightarrow P(c_T) \mid S \subseteq X \}
\]
\[
\cup \{ (P(c_S) \land P(c_T)) \Rightarrow P(c_{S\cap T}) \mid S, T \subseteq X \}
\]
\[
\cup \{ P(c_S) \iff \neg P(c_{X\setminus S}) \mid S \subseteq X \}
\]
\[
\cup \{ P(c_S) \mid S \in \mathcal{F} \}
\]

**Claim:** Every finite $T' \subseteq T$ is satisfiable. In $T'$ there are only finitely many constant symbols $c_{S_1}, \ldots, c_{S_n}$. Then there is $x \in \bigcap_{P(c_{S_i}) \in T'} S_i$ because $\mathcal{F}$ has the FIP. Let $M$ be a $\tau$-structure with domain $\mathcal{P}(X)$ and
- $c_S := S$
- $P_M(S)$ iff $x \in S$.

Then we have
\[
M \models T'
\]
The compactness theorem asserts the existence of a model $M$ of $T$. Then
\[
\mathcal{U} := \{ S \subseteq X \mid P_M(S) \}
is an ultrafilter that extends $\mathcal{F}$. 
Preservation Theorems

There is a nice and fruitful interplay between syntactic restrictions of formulas and theories on the one hand, and semantic properties of formulas and theories on the other hand. Semantic properties are often expressed in terms of preservation under certain operations. In this chapter we will see preservation theorems for example for preservation under homomorphisms, under substructures, and under products. The following definition is central to formulate the precise statements of the respective theorems.

**Definition 2.0.1.** Let $M_1$ and $M_2$ be two $\tau$-structures, and $f : M_1 \to M_2$ be a function. We say that $f$ preserves a first-order $\tau$-formula $\phi(x_1, \ldots, x_n)$ if for all $a_1, \ldots, a_n \in M_1$ such that $M_1 \models \phi(a_1, \ldots, a_n)$ we have that $M_2 \models \phi(f(x_1), \ldots, f(x_n))$.

**Exercises.**

(10) True or false?
- Let $M_1$ and $M_2$ be two $\tau$-structures. Then $f : M_1 \to M_2$ is a homomorphism if and only if $f$ preserves all atomic $\tau$-formulas.
- Let $M$ be a $\tau$-structure. Then the identity map from $M$ to $M$ preserves all first-order $\tau$-formulas.
- Let $h$ be a bijective homomorphism between two finite $\tau$-structures. Then $h$ also preserves the formulas of the form $\neg \phi$ where $\phi$ is an atomic $\tau$-formula.
- The same statement when the two $\tau$-structures need not be finite.

**Definition 2.0.2.** Let $T$ be a first-order theory and $\phi(\bar{x})$ and $\psi(\bar{x})$ formulas. We say that $\phi$ and $\psi$ are (logically) equivalent modulo $T$ if $T \models \forall \bar{x}(\phi(\bar{x}) \Leftrightarrow \psi(\bar{x}))$.

**Exercises.**

(11) True or false?
- the formulas
  \[ \exists u, z (x = y + z \land u \ast u = z \land u \ast u \neq u) \]
  and
  \[ \forall u, z (u \ast u = z \Rightarrow y \neq x + z) \]
  are equivalent modulo $\text{Th}(\mathbb{R}; +, \ast)$.
- the same question modulo $\text{Th}(\mathbb{C}; +, \ast)$;
- the same question modulo $\text{Th}(\mathbb{Q}; +, \ast)$;
- the same question modulo $\text{Th}(\mathbb{Z}; +, \ast)$.

2.1. The Homomorphism Preservation Theorem

Our first example of a preservation theorem is the homomorphism preservation theorem, which captures an important syntactic restriction of first-order logic. A first-order formula is called
• **primitive positive** if it does not use the symbol $\neg$ (and therefore also not the abbreviations $\lor$ and $\forall$); additionally, we allow the 0-ary relation symbol $\bot$ which always denotes the empty set. Note that in first-order logic, $\bot$ was an abbreviation for $\exists x. x \neq x$.

• **existential positive** if $\neg$ and $\forall$ are forbidden, but $\lor$ is still allowed.

• **universal negative** if it is the negation of an existential positive formula.

Observe that

- every primitive positive formula is equivalent (that is, logically equivalent modulo the empty theory) to a formula of the form
  \[ \exists x_1, \ldots, x_n (\psi_1 \land \cdots \land \psi_m) \]
  where $\psi_1, \ldots, \psi_m$ are atomic formulas;
- every existential positive formula is equivalent to a disjunction
  \[ \phi_1 \lor \cdots \lor \phi_k \]
  where $\phi_1, \ldots, \phi_k$ are primitive positive formulas;
- every universal negative formula is equivalent to a conjunction of formulas of the form
  \[ \forall x_1, \ldots, x_n \neg (\psi_1 \land \cdots \land \psi_m) \]
  where $\psi_1, \ldots, \psi_m$ are atomic formulas.

Exercises.

(12) Prove the claims from the above observations.

**Example 2.1.1.** Hilbert’s 10th problem (one of the 23 problems posed by Hilbert in 1900 at the Sorbonne (Paris) conference of the International Congress of Mathematicians:

Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

The solution is negative: there cannot be such a process (now rather called *algorithm*).

The solution is via primitive positive definability: Matiyasevitch showed that in the structure $\langle \mathbb{N}; +, \ast \rangle$, the exponential function $(x, y) \mapsto x^y$ is primitive positive definable.

This was the last step in establishing a stronger result (with important contributions of Davis, Putnam, and Robinson), namely that every recursively enumerable subset of $\mathbb{N}$ is primitive positive definable in $\langle \mathbb{N}; +, \ast \rangle$, and such sets cannot be recognised algorithmically.

**Lemma 2.1.2.** Let $h$ be a homomorphism from a $\tau$-structure $M_1$ to a $\tau$-structure $M_2$. Then $h$ preserves all existential positive formulas.

**Proof.** By induction over the syntactic structure of existential positive formulas.

- if $\phi$ is atomic, the statement holds by definition of homomorphisms.
- if $\phi$ equals $\psi_1 \lor \psi_2$, then
  \[ M_1 \models \phi(\bar{a}) \iff M_1 \models \psi_1(\bar{a}) \text{ or } M_1 \models \psi_2(\bar{a}) \]
  \[ \Rightarrow M_2 \models \psi_1(h(\bar{a})) \text{ or } M_2 \models \psi_2(h(\bar{a})) \text{ (by IA)} \]
  \[ \iff M_2 \models \phi(h(\bar{a})) \]
- if $\phi$ equals $\psi_1 \land \psi_2$: analogous to the previous case.
• if \( \phi \) equals \( \exists x.\psi \) then
\[
\mathcal{M}_1 \models \phi(\bar{a}) \iff \text{there is } a' \in M_1 \text{ s.t. } \mathcal{M}_1 \models \psi(a', \bar{a})
\]
\[
\Rightarrow \text{ there is } a' \in M_1 \text{ s.t. } \mathcal{M}_2 \models \psi(h(a'), h(\bar{a})) \quad \text{(by I}\text{A)}
\]
\[
\Rightarrow \text{ there is } a'' := h(a') \in M_2 \text{ s.t. } \mathcal{M}_2 \models \psi(a'', h(\bar{a}))
\]
\[
\Leftrightarrow \mathcal{M}_2 \models \phi(h(\bar{a}))
\]
\[\square\]

**Corollary 2.1.3.** Suppose that \( \phi \) is equivalent to an existential positive formula \( \psi \) modulo \( T \). Then \( \phi \) is preserved by all homomorphisms between models of \( T \).

**Proof.** Let \( \mathcal{M}_1 \) and \( \mathcal{M}_2 \) be two models of \( T \), let \( h : M_1 \to M_2 \) be a homomorphism, and let \( \bar{a} \) be a tuple of elements of \( M_1 \). Then
\[
\mathcal{M}_1 \models \phi(\bar{a}) \iff \mathcal{M}_1 \models \psi(\bar{a})
\]
\[
\Rightarrow \mathcal{M}_2 \models \psi(h(\bar{a})) \quad \text{(Lemma 2.1.2)}
\]
\[
\Leftrightarrow \mathcal{M}_2 \models \phi(h(\bar{a}))
\]
\[\square\]

The lemma and its corollary are trivialities, but they are useful to prove that certain formulas are not equivalent to an existential positive formula modulo \( T \). For example, we claim that the formula \( x \neq y \) is not equivalent to an existential positive formula modulo \( \text{Th}(\mathbb{Q}; \leq) \). To see this, observe that the map \( h : \mathbb{Q} \to \mathbb{Q} \) defined by \( x \mapsto 0 \) is a homomorphism from \( (\mathbb{Q}; \leq) \) to \( (\mathbb{Q}; \leq) \). But it obviously does not preserve \( x \neq y \).

**Exercises.**

(13) Let \( \mathcal{M} \) be the \( \{<\} \)-structure with domain \( \{x \in \mathbb{Q} \mid 0 \leq x \} \) where \( <^\mathcal{M} \) is the usual order of the non-negative rational numbers. Which of the following formulas are equivalent to an existential positive formula modulo \( \text{Th}(\mathcal{M}) \):

• \( x \neq y \);
• \( \forall y. x < y \);
• \( \forall y (x = y \lor x < y) \)

Either find the existential positive formula, or prove that none exists.

(14) A formula \( \phi(x_1, \ldots, x_n) \) is called **produkttreu** if \( A \models \phi(a_1, \ldots, a_n) \) and \( B \models \phi(b_1, \ldots, b_n) \) imply \( A \times B \models \phi((a_1, b_1), \ldots, (a_n, b_n)) \). Show that

• \( t^A \times B((a_1, b_1), \ldots, (a_n, b_n)) = (t^A(a_1, \ldots, a_n), t^B(b_1, \ldots, b_n)) \) for every term \( t \);
• atomic formulas are produkttreu;
• if \( \phi \) and \( \psi \) are produkttreu, then so is \( (\phi \land \psi) \) and \( \forall x. \phi \).

Conclude that direct products of rings are rings. Show that one of the field axioms is not produkttreu (which one?).

A theory \( T \) is **existential positive** (or **universal negative**) if all sentences in \( T \) are existential positive (or universal negative, respectively).

**Example 2.1.4.** Let \( \tau = \{E\} \) be a signature with a single binary relation symbol. Then
\[
T := \{ \forall x_1, x_2, x_3 \neg(E(x_1, x_2) \land E(x_2, x_3) \land E(x_1, x_3)) \}
\]
is a universal negative theory; the models of \( T \) are precisely the directed graphs without a directed cycle of length three.

Two theories are called **(logically) equivalent** if they have the same models.
Theorem 2.1.5 (Homomorphism Preservation Theorem, Variant 1). Let $T$ be a first-order $\tau$-theory such that for every homomorphism between $\tau$-structures $M_1$ and $M_2$ we have

$$M_1 \models T \implies M_2 \models T.$$  

Then $T$ is equivalent to an existential positive theory.

Theorem 2.1.6 (Homomorphism Preservation Theorem, Variant 2). Let $T$ be a first-order theory. A first-order formula $\phi$ is equivalent to an existential positive formula modulo $T$ if and only if $\phi$ is preserved by all homomorphisms between models of $T$.

We present a proof of those theorems in Section 2.3; before, we have to introduce an important concept from model theory: saturated models.

2.2. Saturation

To define saturation, we have to introduce types. Loosely speaking, a type of a $\tau$-structure $M$ is a set of formulas that is satisfied by a real or by a 'virtual' element of $M$, that is, an element of some structure that has the same theory as $M$. A structure $M$ is saturated if 'as many types as possible' come from real elements of $M$.

2.2.1. Types. A (not necessarily finite) set $\Sigma$ of formulas with free variables $x_1, \ldots, x_n$ is called satisfiable over a structure $A$ if there are elements $a_1, \ldots, a_n$ of $A$ such that $A \models \Sigma(a_1, \ldots, a_n)$. We say that $\Sigma$ is satisfiable if there exists a structure $B$ such that $\Sigma$ is satisfiable over $B$.

Lemma 2.2.1. A set $\Sigma$ of formulas with free variables $x_1, \ldots, x_n$ is satisfiable if and only if all finite subsets of $\Sigma$ are satisfiable.

Proof. Introduce new constant symbols $c_1, \ldots, c_n$. Then $\Sigma$ is satisfiable if and only if $\Sigma(c_1, \ldots, c_n) := \{\phi(c_1, \ldots, c_n) \mid \phi(x_1, \ldots, x_n) \in \Sigma\}$ is satisfiable. Now apply the compactness theorem. $\square$

For $n \geq 0$, an $n$-type of a theory $T$ is a set $p$ of formulas with free variables $x_1, \ldots, x_n$ such that $p \cup T$ is satisfiable. An $n$-type of a structure $A$ is an $n$-type of the first-order theory of $A$.

Lemma 2.2.2. Let $A$ be a $\tau$-structure and $\Sigma$ a set of first-order $\tau$-formulas with free variables $x_1, \ldots, x_n$. Then the following are equivalent.

1. $\Sigma$ is an $n$-type of $A$;
2. every finite subset of $\Sigma$ is realised in $A$;
3. $A$ has an elementary extension that realises $\Sigma$.

Proof. (1) $\Rightarrow$ (2): If $\Sigma$ is an $n$-type of $A$, there exists a model $B$ of $\text{Th}(A)$ and $b \in B^n$ such that $B \models \Sigma(b)$. Hence, if $\Psi$ is a finite subset of $\Sigma$, then $B \models \exists x_1, \ldots, x_n \land \Psi$ and since $\text{Th}(A) = \text{Th}(B)$ we have $A \models \exists x_1, \ldots, x_n \land \Psi$, so $\Psi$ is realised in $A$.

(2) $\Rightarrow$ (3): if every finite subset $\Psi$ of $\Sigma$ is realised in $A$, then in particular every finite subset of $\Sigma \cup \text{Th}(A_A)$ is satisfiable, and hence $\Sigma \cup \text{Th}(A_A)$ is satisfiable by compactness. Let $B$ be a model of $\text{Th}(A_A)$ that satisfies $\Sigma$. Then the $\tau$-reduct of $B$ is an elementary extension of $A$ that realises $\Sigma$.

(3) $\Rightarrow$ (1): immediate. $\square$

Some more definitions for types.

- An $n$-type $p$ of $T$ is maximal if $T \cup p \cup \{\phi(x_1, \ldots, x_n)\}$ is unsatisfiable for any formula $\phi \notin T \cup p$. 

• An $n$-type $p$ is realised in $A$ if there exist $a_1,\ldots,a_n \in A$ such that $A \models \phi(a_1,\ldots,a_n)$ for each $\phi \in \Phi$.

• The set of all first-order formulas with free variables $x_1,\ldots,x_n$ satisfied by an $n$-tuple $\bar{a} = (a_1,\ldots,a_n)$ in $A$ is a maximal type of $A$, and called the type of $\bar{a}$ in $A$.

Let $A$ be a $\tau$-structure and $B \subseteq A$. We write $A_B$ for the expansion of $A$ by the constant symbol $b \in B$ for every element $b \in B$ (we set $bA := b$). We refer to the $n$-types of $A_B$ as the $n$-types of $A$ over $B$; the set of all maximal $n$-types of $A$ over $B$ is denoted by $S^n_B(A)$.

**Definition 2.2.3 (Saturation).** For an infinite cardinal $\kappa$, a structure $A$ is $\kappa$-saturated if $A$ realises all $I$-types over $B$ for all $B \subseteq A$ with $|B| < \kappa$. We say that an infinite structure $A$ is saturated if it is $|A|$-saturated.

**2.2.2. Chains.** We build saturated models using another important operation to build structures, namely the formation of limits of chains. Chains of $\tau$-structures are a fundamental concept from model theory. Let $I$ be a linearly ordered index set. Let $(A_i)_{i \in I}$ be a sequence of $\tau$-structures. Then $(A_i)_{i \in I}$ is called a chain if $A_i$ is a substructure of $A_j$ for all $i < j$.

**Definition 2.2.4.** The union of a chain $(A_i)_{i \in I}$ is a $\tau$-structure $B = \lim_{i \in I} A_i$, defined as follows.

- The domain of $B$ is $B := \bigcup_{i \in I} A_i$.
- For each relation symbol $R \in \tau$ we put $\bar{a} \in R^B$ if $\bar{a} \in R^{A_i}$ for some (or all) $A_i$ containing $\bar{a}$.
- For each function symbol $f \in \tau$ we set $f^B(\bar{a}) = a'$ if $f^{A_i}(\bar{a}) = a'$ for some (or all) $A_i$ containing $\bar{a}$.

**Example 2.2.5.** For each $n \in \mathbb{N}$, let $A_n := \{-n, -n+1, \ldots, 0, 1, 2, \ldots\} \subseteq \mathbb{Z}$ and let $A_n := (A_n; \leq)$ be the substructure of $(\mathbb{Z}; \leq)$ induced by $A_n$. Then $\text{Th}(A_n) = \text{Th}(A_0)$ for all $n \in \mathbb{N}$, but $\text{Th}(\lim_{i \in I} A_i)$ is different (why?).

Functions that preserve all first-order formulas are called elementary (they are necessarily embeddings). If $B$ is an expansion of $A$ such that the identity map from $A$ to $B$ is an elementary embedding, we say that $B$ is an elementary extension of $A$, and that $A$ is an elementary substructure of $B$, and write $A \prec B$. Note that $\prec$ is a transitive relation. A chain is called an elementary chain if $A_i \prec A_j$ for all $i < j$.

Note that the structure $A_{n+1}$ from Example 2.2.5 is not an elementary extension of $A_n$ (why?).

**Lemma 2.2.6 (Tarski’s elementary chain theorem).** Let $(A_i)_{i \in I}$ be an elementary chain of $\tau$-structures. Then $A_i \prec B := \lim_{i \in I} A_i$ for each $i \in I$.

**Proof.** We have to show that for each $i \in I$, every $\tau$-formula $\phi(x_1,\ldots,x_k)$, and every $\bar{a} \in (A_i)^k$ we have

$B \models \phi(\bar{a})$ if $A_k \models \phi(\bar{a})$

First consider the case that $\phi$ is atomic of the form $R(x_1,\ldots,x_k)$ for $R \in \tau$. We then have

$B \models R(\bar{a})$ if $\bar{a} \in R^B$

$$\begin{align*}
\text{if } \bar{a} \in R^{A_i} \\
\text{if } A_i \models R(\bar{a})
\end{align*}$$
Claim. If \( t(x_1, \ldots, x_k) \) is a \( \tau \)-term and \( \vec{a} \in (A_i)^k \), then \( t^A_\vec{a}(\vec{a}) = t^A_\vec{a}(\vec{a}) \). This can be shown by a straightforward induction on the structure of terms. Consequently, the statement is true for atomic formulas of the form \( t = s \), for \( \tau \)-terms \( t \) and \( s \).

Claim. If the statement is true for \( \phi \), then the statement is true for \( \neg \phi \):

\[
B \models \neg \phi(\vec{a}) \text{ iff not } B \models \phi(\vec{a})
\]

iff not \( A_\vec{a} \models \phi(\vec{a}) \) (by IA)

iff \( A_\vec{a} \models \phi(\vec{a}) \)

The verification for formulas of the form \( \phi \land \phi \) is similarly straightforward. Therefore we go straight to the existential quantifier.

Claim. If the statement is true for \( \phi \) then the statement is also true for \( \exists x_1. \phi \).

\[
A \models \exists x_1. \phi(x_1, \ldots, x_k)(b_2, \ldots, b_k)
\]

iff there is \( b_1 \in B \) s.t. \( B \models \phi(b_1, b_2, \ldots, b_k) \)

iff there is \( b_1 \in A_j \) s.t. \( A_j \models \phi(b_1, b_2, \ldots, b_k) \) for some \( j > i \)

iff \( A_j \models \exists x_1. \phi(b_1, b_2, \ldots, b_k) \)

iff \( A_j \models \exists x_1. \phi(b_1, b_2, \ldots, b_k) \) since \( A_i \prec A_j \).

\[\Box\]

Exercises.

(15) Let \( \kappa \) be an infinite cardinal. Show that if a structure \( A \) realises all 1-types over all \( B \subseteq A \) with \( |B| < \kappa \) if and only if \( A \) realises all \( n \)-types over all \( B \subseteq A \) with \( |B| < \kappa \).

(16) Let \( A, B \) sets with \( A \subseteq B \). Show that \( A := (A; =) \) is an elementary substructure of \( B := (B; =) \).

(17) Show that \( (\mathbb{Q}; <) \) is an elementary substructure of \( (\mathbb{R}; <) \). Is \( (\mathbb{Z}; <) \) an elementary substructure of \( (\mathbb{Q}; <) \)?

(18) Let \( A, B \) be a \( \tau \)-structures and \( f \) an isomorphism between \( A \) and \( B \). Then every tuple \( \vec{a} \in A^n \) has the same type in \( A \) as \( f(\vec{a}) \) in \( B \).

### 2.2.3. Building saturated models.

In this section we prove a general result about the existence of \( \kappa \)-saturated structures. We start with a lemma about realisation of types.

**Lemma 2.2.7.** Every \( \tau \)-structure \( A \) has an elementary extension \( B \) that realises all 1-types over \( A \).

**Proof. First proof:** Let \( (p_\alpha)_{\alpha \in \lambda} \) be an enumeration of \( S^A_1(A) \) where \( \lambda \) is an ordinal. We construct an elementary chain

\[
A_A := A_0 \prec \cdots \prec A_\beta \prec \cdots (\beta \leq \lambda)
\]

such that \( p_\alpha \) is realised in \( A_{\alpha+1} \). Suppose that \( (A_\alpha')_{\alpha<\beta} \) is already constructed.

- \( \beta \) is limit ordinal. Define \( A_\beta := \lim_{\alpha<\beta} A_\alpha \). Then \( (A_\alpha')_{\alpha<\beta} \) is an elementary chain, using Tarski’s chain lemma (Lemma 2.2.6).

- \( \beta = \alpha + 1 \). By Lemma 2.2.2, every finite subset \( \Psi \) of \( p_\alpha \) is realised in \( A_\alpha \), and therefore also in \( A_\alpha \). By Lemma 2.2.2 again, \( A_\alpha \) has an elementary extension \( A_{\alpha+1} \) that realises \( p_\alpha \).

\[\text{By Theorem A.2.4 there is a well-ordering of } S^A_1(A), \text{ and by Proposition A.2.2 there is an ordinal } \lambda \text{ and a sequence } (p_\alpha)_{\alpha<\lambda} \text{ that enumerates the elements of } S^A_1(A).\]
Second proof: For each 1-type $p$ of $A$ over $A$, we introduce a new constant symbol $c_p$. Let $T$ be the set of all atomic sentences of $A$ together with all the formulas $\phi(c_p)$ where $p$ is a 1-type of $A$ over $A$ and $\phi \in p$. We will show that finite subsets $F$ of $T$ are satisfiable. Let $p$ be a 1-type of $A$ over $A$. By definition, $\text{Th}(A) \cup p$ has a model $B$, which satisfies
\[
\psi := \exists x \bigwedge_{\phi(c_p) \in F} \phi(x).
\]
Therefore, $A \models \psi$, i.e., $A \models \bigwedge_{\phi(c_p) \in F} \phi(a)$ for some $a \in A$. Expanding $A$ by $c_p := a$ for all 1-types $p$ of $A$ over $A$, we obtain a model of $F$.

So by compactness, $T$ has a model $B$. Since $T$ contains the atomic sentences that hold in $A$, the structure $B$ is an elementary extension of $A$. Also, for each type $p$ of $B$ over $A$, the structure $B$ contains an element $c_p$ satisfying $p$, by choice of $T$. □

**Theorem 2.2.8.** Let $A$ be a structure and $\kappa$ an infinite cardinal. Then $A$ has a $\kappa$-saturated elementary extension.

**Proof.** Build a chain $(A_\alpha)_{\alpha < \kappa^+}$ of structures inductively as follows:
- $A_0 := A$.
- $A_{\alpha+1}$ is an elementary extension of $A_\alpha$, realising all 1-types over $A_\alpha$. Such a structure exists by Lemma 2.2.7.
- If $\beta$ is a limit ordinal then $A_\beta := \lim_{\alpha < \beta} A_\alpha$.

It follows by induction on $\alpha$ that $A_\alpha$ is an elementary extension of $A_\beta$ for all $\beta < \alpha$, using Tarski’s elementary chain lemma at the limit ordinals. So $(A_\alpha)_{\alpha < \kappa^+}$ is an elementary chain of models.

By Tarski’s elementary chain lemma again, $B := \lim_{\alpha < \kappa} A_\alpha$ is an elementary extension of $A$. We show that $B$ is even $\kappa^+$-saturated (which implies $\kappa$-saturated).

Let $S$ be a subset of $B$ of size less than $\kappa^+$. Then $S \subseteq A_\alpha$ for some $\alpha \leq \kappa$; otherwise, $S$ contains for every $\gamma < \kappa^+$ an element from $A_{\gamma+1} \setminus A_\gamma$, so $\text{cf}(\kappa^+) < \kappa^+$, in contradiction to Proposition 2.2.9. By construction, $A_{\alpha+1}$ realises all 1-types over $A_\alpha$. Consequently, $B$ realises all 1-types over $S$. □

By paying attention to the sizes of the structures that we build, one can show the following.

**Theorem 2.2.9.** Let $\tau$ be a signature and $\kappa \geq |\tau|$ an infinite cardinal. Then every $\tau$-structure of size $2^\kappa$ has a $\kappa^+$-saturated elementary extension of size $2^\kappa$.

**Proof.** We need the following observations:
- In the first proof of Lemma 2.2.2, the structure $B$ can be build to have cardinality $2^{|A|}$ (there are at most $2^\kappa$ many subsets of $A$ of cardinality at most $\kappa$).
- The union of a chain of length at most $\kappa^+$ of models of cardinality $2^\kappa$ has cardinality $2^\kappa$ (see Theorem A.3.2).

So if we assume the Generalised Continuum Hypothesis, then there are saturated models of size $\kappa^+$ for all cardinals $\kappa$. We particularly point out the following special case.

**Corollary 2.2.10.** Let $\tau$ be an at most countable signature, and $T$ be a satisfiable $\tau$-theory. Then $T$ has a $\aleph_1$-saturated model of cardinality $2^{\aleph_0}$.
Hence, assuming the continuum hypothesis, every satisfiable theory with a countable signature has a saturated model! The proposition above follows from a more general result (Theorem 2.2.9) that we will prove in Section 2.2.3. Note that for general $T$, some set-theoretic assumption is necessary for the existence of saturated models: if $T$ has $2^{\aleph_0}$ many 1-types (take for instance $(\mathbb{Q}; <)$ expanded by constants for all elements) then any $\aleph_0$-saturated model has size $2^{\aleph_0}$. Hence, if $\aleph_1 < 2^{\aleph_0}$, then there is no saturated model of size $\aleph_1$.

**Exercises.**

(19) Show that if $(A_\gamma)_{\gamma < \omega}$ is a sequence of $\tau$-structures and $\mathcal{U}$ a non-principal ultrafilter on $\omega$ then $\prod_{\gamma < \omega} A_\gamma / \mathcal{U}$ is $\aleph_1$-saturated.

**Lemma 2.2.11.** Let $A$ and $B$ be $\tau$-structures such that $B$ is $|A|$-saturated. Suppose that every primitive positive sentence that is true in $A$ is also true in $B$. Then there is a homomorphism from $A$ to $B$.

**Proof.** By Theorem A.2.4 there is a well-ordering of $A$, and by Proposition A.2.2 there is an ordinal $\alpha$ and a sequence $(a_\beta)_{\beta < \alpha}$ that enumerates the elements of $A$. We will identify $A$ with $\alpha$. We claim that for every ordinal $\beta < \alpha$ there exists an expansion $B(\beta)$ of $B$ such that every primitive positive sentence true on $A_\beta$ is true on $B(\beta)$. The proof is by induction on $\beta$.

- The base case, $\beta = 0$, follows from the hypothesis of the lemma.
- Inductive step: limit ordinals $\beta$. The claim holds since a sentence can only mention a finite collection of constants that must all be less than some $\gamma < \beta$.
- Inductive step: successor ordinals $\beta = \gamma + 1 < \alpha$. Let $\Sigma$ be the set of primitive positive formulas $\phi(x)$ such that $A_\gamma \models \phi(\beta)$. By induction assumption, $B(\gamma) \models \exists x. \phi(x)$ for every $\phi \in \Sigma$. By compactness, since $\Sigma$ is closed under conjunction, we have that $\Sigma$ is a 1-type of $B(\gamma)$. Then $\Sigma$ is realised by some element $b \in B$ because $B$ is $|A|$-saturated. Define $B(\beta)$ by setting $B(\beta) := b$. By construction we maintain that all primitive positive sentences true on $A_\beta$ are true on $B(\beta)$.

The function that maps $\beta \in A$ to $B(\beta)$ is a homomorphism from $A$ to $B$ since it preserves all atomic formulas.

The following proposition will not be needed for proving the homomorphism preservation theorem; but it is conceptually important, and moreover the proof contains a nice and powerful idea, called back and forth argument, so we present it here.

**Theorem 2.2.12.** Let $A$ and $B$ be two saturated models of the same theory and the same cardinality. Then $A$ and $B$ are isomorphic.

**Proof.** Let $(a_\alpha)_{\alpha < \kappa}$ be an enumeration of $A$ and $(b_\alpha)_{\alpha < \kappa}$ an enumeration of $B$. We inductively construct a sequence $(c_\alpha)_{\alpha < \kappa}$ of elements of $A$ and $(d_\alpha)_{\alpha < \kappa}$ of elements of $B$ such that for all $\beta < \kappa$

$$\text{Th}(A; (a_\alpha)_{\alpha < \beta}, (d_\alpha)_{\alpha < \beta}) = \text{Th}(B; (c_\alpha)_{\alpha < \beta}, (b_\alpha)_{\alpha < \beta}).$$

The base case $\beta = 0$ holds by the assumptions of the theorem. Suppose that $(c_\alpha)_{\alpha < \beta}$ and $(d_\alpha)_{\alpha < \beta}$ have already been constructed. If $\beta$ is a limit ordinal, there is nothing to be done. Otherwise, if $\alpha_\beta$ is not yet among the $\{c_\alpha | \alpha < \beta\}$, we use saturation of $B$ to find $c_\beta$ such that

$$\text{Th}(A; (a_\alpha)_{\alpha < \beta}, (d_\alpha)_{\alpha < \beta}) = \text{Th}(B; (c_\alpha)_{\alpha < \beta}, (b_\alpha)_{\alpha < \beta}).$$

Then we use saturation of $A$ to find $d_\beta$ such that

$$\text{Th}(A; (a_\alpha)_{\alpha < \beta}, (d_\alpha)_{\alpha < \beta}) = \text{Th}(B; (c_\alpha)_{\alpha < \beta}, (b_\alpha)_{\alpha < \beta}).$$
At the end of the day, the map \( f: A \to B \) defined by \( f(a_\alpha) := c_\alpha \) for all \( \alpha < \kappa \) is a homomorphism from \( A \) to \( B \), and the map \( b_\alpha \mapsto d_\alpha \) is a homomorphism from \( B \) to \( A \) which is the inverse of \( f \). \( \square \)

2.3. Proof of the Homomorphism Preservation Theorem

Recall that we want to prove two variants of the homomorphism preservation theorem. In both versions, we fix a \( \tau \)-theory \( T \).

1) \( T \) is equivalent to an existential positive theory if and only if the class of models of \( T \) is preserved under homomorphisms;

2) A first-order formula \( \phi \) is equivalent to an existential positive formula modulo \( T \) if and only if \( \phi \) is preserved by all homomorphisms between models of \( T \).

A common generalisation of these two theorems is:

**Theorem 2.3.1 (Homomorphism Preservation Theorem, Variant 3).** A set of first-order formulas \( \Sigma(\bar{x}) \) is equivalent\(^2\) to a set of existential positive formulas modulo \( T \) if and only if \( \Sigma(\bar{x}) \) is preserved by all homomorphisms between models of \( T \).

This theorem implies (1) by setting \( \Sigma(x) := T \) and \( T := \emptyset \). It also implies (2) by the compactness theorem (recall Exercise (7)). Here we employ an important trick, Lemma 2.3.2 below. Let \( \Psi(x_1, \ldots, x_n) \) and \( \Sigma(x_1, \ldots, x_n) \) be sets of first-order formulas. We write \( \Psi(\bar{x}) \models \Sigma(\bar{x}) \) if for every structure \( A \) and \( \bar{a} \in A^n \) we have that

\[ A \models \Psi(\bar{a}) \Rightarrow A \models \Sigma(\bar{a}). \]

**Lemma 2.3.2 (Constants lemma).** Let \( \Psi(x_1, \ldots, x_n) \) and \( \Sigma(x_1, \ldots, x_n) \) be sets of first-order \( \tau \)-formulas and \( c_1, \ldots, c_n \) be distinct constants that are not in \( \tau \). Then \( \Psi(\bar{x}) \models \Sigma(\bar{x}) \) if and only if \( \Psi(\bar{c}) \models \Sigma(\bar{c}) \).

We present the compactness argument to derive (2) from Theorem 2.3.1. We have to show that if a formula \( \phi(\bar{x}) \) is preserved by homomorphisms between models of \( T \), then \( \phi(\bar{x}) \) is equivalent modulo \( T \) to an existential positive formula. By (1), we know that \( \{\phi(\bar{x})\} \) is equivalent modulo \( T \) to a set of existential positive formulas \( \Psi(\bar{x}) \). Let \( \bar{c} \) be fresh constant symbols. Then Lemma 2.3.2 asserts that \( T \cup \{\phi(\bar{c})\} \) and \( T \cup \Psi(\bar{c}) \) have the same models. Then it can be shown as in the solution to Exercise 7 that there is a finite subset \( \Psi' \) of \( \Psi \) such that \( T \cup \Psi'(\bar{c}) \) and \( T \cup \Psi(\bar{c}) \) have the same models. The formula \( A \models \Psi' \) is the desired existential positive formula that is equivalent to \( \phi \).

**Proof of Theorem 2.3.1.** It is clear that homomorphisms preserve (sets of) existential positive formulas. For the converse, suppose that \( \Sigma(\bar{x}) \) is preserved by homomorphisms between models of \( T \). Let \( \Psi(\bar{x}) \) be the set of all existential positive formulas \( \psi(\bar{x}) \) such that \( T \cup \Sigma(\bar{x}) \models \psi(\bar{x}) \). We have to show that \( T \cup \Psi(\bar{x}) \models \Sigma(\bar{x}) \).

Let \( \bar{c} = (c_1, \ldots, c_n) \) be a sequence of constant symbols that are not contained in \( \sigma \). By Lemma 2.3.2, the theory \( \Psi(\bar{c}) \) consists of the set of all existential positive consequences of \( T \cup \Sigma(c) \), and that we have to show that \( T \cup \Psi(\bar{c}) \models \Sigma(\bar{c}) \). Let \( A \) be a model of \( T \cup \Psi(\bar{c}) \). Let \( U \) be the set of all primitive positive sentences \( \theta \) such that \( A \models \neg \theta \). We claim that

\[ T \cup \{-\theta \mid \theta \in U\} \cup \Sigma(\bar{c}) \]

is satisfiable. For otherwise, by compactness, there would be a finite subset \( U' \) of \( U \) such that \( T \cup \{-\theta \mid \theta \in U'\} \cup \Sigma(\bar{c}) \) is unsatisfiable. But then \( \psi := \bigvee U' \) is an existential positive sentence such that \( T \cup \Sigma(\bar{c}) \models \psi \), and hence \( \psi \in \Psi(\bar{c}) \). This is in contradiction to the assumption that \( A \models \neg \theta \) for all \( \theta \in U \). We conclude that there exists a model \( B \) of \( T \cup \{-\theta \mid \theta \in U\} \cup \Sigma(\bar{c}) \).

\(^2\)We say that \( \Sigma(\bar{x}) \) and \( \Psi(\bar{x}) \) are equivalent modulo \( T \) if for any \( \tau \)-structure \( A \) and \( \bar{a} \in A^n \) we have \( A \models \Sigma(\bar{a}) \) if and only if \( A \models \Psi(\bar{a}) \).
By Theorem 2.2.9, \( A \) has an elementary extension \( A' \) which is \(| B |\)-saturated. Every primitive positive \((\tau \cup \{ c_1, \ldots, c_n \})\)-sentence \( \theta \) that is true in \( B \) is also true in \( A' \); otherwise, if \( \theta \) were false in \( A' \), then it were also false in \( A \), and hence \( \theta \in U \) in contradiction to the assumption that \( B |_{c} = \{ \neg \theta \mid \theta \in U \} \). Hence, by Lemma 2.2.11, there exists a homomorphism from \( B \) to \( A' \). Since \( B |_{c} = \Sigma(c) \), and \( \Sigma \) is preserved by homomorphisms between models of \( T \), we have \( A' |_{c} = \Sigma(c) \). Since \( A' \) is an elementary extension of \( A \), we also have \( A |_{c} = \Sigma(c) \), which is what we wanted to show. \( \square \)

Note that here the assumption that \( \bot \) is always part of first-order logic is important: the first-order formula \( \exists x. x \neq x \) is preserved by all homomorphisms between models of \( T \), but without \( \bot \) it might not be equivalent to an existential positive formula modulo \( T \) (for instance if \( T \) is the empty theory).

### 2.4. The Theorem of Łoś-Tarski

The classical theorem of Łoś-Tarski characterises universal theories, and characterises equivalence of formulas to universal formulas modulo a theory.

**Definition 2.4.1.** A first-order formula is called

- **existential** if it is built from \( \exists, \lor, \land \), atomic formulas, and negated atomic formula. (Unrestricted use of negation \( \neg \) and in particular the quantifier \( \forall \) are forbidden.)
- **universal** if it is built from \( \forall, \lor, \land \), atomic formulas, and negated atomic formulas. (Unrestricted use of negation \( \neg \) and the quantifier \( \exists \) are forbidden.)

Note that

- a first-order formula is existential if and only if it is equivalent to a formula in prenex normal form without universal quantifiers (see Exercise 4);
- a first-order formula is universal if and only if it is equivalent to a formula in prenex normal form without existential quantifiers.

**Theorem 2.4.2 (Theorem of Łoś-Tarski, Version 1).** Let \( T \) be a first-order \( \tau \)-theory. Then \( T \) is equivalent to a universal theory if and only if the class of all models of \( T \) is closed under taking substructures.

**Theorem 2.4.3 (Theorem of Łoś-Tarski, Version 2).** Let \( T \) be a first-order theory. A first-order formula \( \phi \) is equivalent to an universal formula modulo \( T \) if and only if \( \neg \phi \) is preserved by all embeddings between models of \( T \).

We can derive both of these theorems from the following.

**Theorem 2.4.4 (Theorem of Łoś-Tarski, Version 3).** Let \( T \) be a first-order theory. A set of first-order formulas \( \Phi(\bar{x}) \) is equivalent to set of existential formulas \( \Psi(\bar{x}) \) modulo \( T \) if and only if \( \Phi \) is preserved by all embeddings between models of \( T \).

**Proof.** Add for each atomic formula \( \psi \) a new relation symbol \( N_\psi \) to the signature of \( T \), and add the sentence \( \forall \bar{x} (N_\psi(\bar{x}) \iff \neg \psi(\bar{x})) \); let \( T' \) be the resulting theory. Then every existential formula \( \phi \) is equivalent to an existential positive formula in \( T' \), which can be obtained from \( \phi \) by replacing negative literals \( \neg \psi(\bar{x}) \) in \( \phi \) by \( N_\psi(\bar{x}) \). Similarly, homomorphisms between models of \( T' \) must be embeddings. Hence, the statement follows from Theorem 2.3.1. \( \square \)

**Proof of Theorem 2.4.2.** The fact that substructures of a structure \( A \) satisfy all universal sentences that hold in \( A \) is straightforward. For the converse, suppose that \( T \) is a theory whose class of models is closed under substructures. This is
equivalent to saying that if $A$ is a model of $T' := \{\neg \phi \mid \phi \in T\}$, and $e$ is an embedding from $A$ to a structure $B$, then also $B$ is a model of $T'$. So we can apply Theorem 2.4.4 to $\Phi(\bar{x}) := T'$ and the empty theory, and obtain that $T'$ is equivalent to an existential theory $S$. But then $\{\neg \phi \mid \phi \in S\}$ is equivalent to a universal theory, and equivalent to $T$. □

Proof of Theorem 2.4.3. If is clear that if $\phi$ is a universal formula, then $\neg \phi$ is preserved by embeddings. Suppose now that $\neg \phi$ is preserved by all embeddings between models of $T$. By Theorem 2.4.4, $\neg \phi$ is equivalent to a set of existential formulas. By compactness, it is even equivalent to a finite set $F$ of existential formulas. Then $\neg \bigwedge F$ is equivalent to a universal formula that is equivalent to $\phi$. □
CHAPTER 3

Algebras and Varieties

An important goal of universal algebra is the classification of algebras, in a broad sense; we will see examples in this chapter of what ‘classification’ can mean specifically.

A very fruitful tool to classify algebras is the concept of a variety. The theorem of Birkhoff provides two distinct perspectives on varieties, and belongs to one of the most prominent basic results in universal algebra; it is in fact a preservation theorem in the sense of the previous chapter. A freely available textbook with an introduction to basic universal algebra is the book of Burris and Sankappanavar [1].

3.1. Lattices

See course notes by Henri Mühle, available on the course website.

3.2. Congruences

Algebras have been defined in Section 1.1: they are simply structures with a purely functional signature. When $A$ is an algebra with signature $\tau$ and domain $A$, then the functions $f^A$ are also called the (fundamental) operations of $A$. A term operation of $A$ is an operation of the form $t^A$ for a $\tau$-term $t$. We write $\text{Clo}(A)$ for the set of all term operations of $A$.

The set $\text{Clo}(A)$ is a function clone, that is, it is closed under compositions and contains the projections. As we will see later, many important properties of an algebra $A$ only depend on $\text{Clo}(A)$.

Definition 3.2.1. A congruence of an algebra $A$ is an equivalence relation that is preserved by all operations in $A$.

Proposition 3.2.2 (see [1]). Let $A$ be an algebra. Then $E$ is a congruence of $A$ if and only if $E$ is the kernel of a homomorphism from $A$ to some other algebra $B$.

When $A$ is a $\tau$-algebra, and $h: A \to B$ is a mapping such that the kernel of $h$ is a congruence of $A$, we define the quotient algebra $A/h$ of $A$ under $h$ to be the algebra with domain $h(A)$ where

$$f^A/h(h(a_1), \ldots, h(a_k)) = h(f^A(a_1, \ldots, a_k))$$

where $a_1, \ldots, a_k \in A$ and $f \in \tau$ is $k$-ary. This is well-defined since the kernel of $h$ is preserved by all operations of $A$. Note that $h$ is a surjective homomorphism from $A$ to $A/h$. The following is well known (see e.g. Theorem 6.3 in [1]).
3. ALGEBRAS AND VARIETIES

3.2.3. Let $\mathcal{A}$ and $\mathcal{B}$ be algebras with the same signature, and let $h : \mathcal{A} \to \mathcal{B}$ be a homomorphism. Then the image of any subalgebra $\mathcal{A}'$ of $\mathcal{A}$ under $h$ is a subalgebra of $\mathcal{B}$, and the preimage of any subalgebra $\mathcal{B}'$ of $\mathcal{B}$ under $h$ is a subalgebra of $\mathcal{A}$.

Proof. Let $f \in \tau$ be $k$-ary. Then for all $a_1, \ldots, a_k \in \mathcal{A}'$, $f^\mathcal{B}(h(a_1), \ldots, h(a_k)) = h(f^\mathcal{A}(a_1, \ldots, a_k)) \in h(\mathcal{A}')$, so $h(\mathcal{A}')$ is a subalgebra of $\mathcal{C}$. Now suppose that $h(a_1), \ldots, h(a_k)$ are in $\mathcal{B}'$; then $f^\mathcal{B}(h(a_1), \ldots, h(a_k)) \in B'$ and hence $\mu(f^\mathcal{A}(a_1, \ldots, a_k)) \in B'$. So, $f^\mathcal{A}(a_1, \ldots, a_k) \in h^{-1}(B')$ which shows that $h^{-1}(B')$ induces a subalgebra of $\mathcal{A}$. □

3.2.4. Let $\mathcal{A}$ be a subalgebra. Then the variety generated by $\mathcal{A}$ equals $HSP(\mathcal{A})$.

Proof. Clearly, $HSP(\mathcal{A})$ is contained in the variety generated by $\mathcal{A}$, and $HSP(\mathcal{A})$ is contained in the variety generated by $\mathcal{A}$. We have to verify that $HSP(\mathcal{A})$ is closed under $H, S,$ and $P$. It is clear that $H(HSP(\mathcal{A})) = HSP(\mathcal{A})$. Lemma 3.2.3 implies that $S(HSP(\mathcal{A})) \subseteq HS(SP(\mathcal{A})) = HSP(\mathcal{A})$. Finally, $P(HSP(\mathcal{A})) \subseteq HPS(P(\mathcal{A})) \subseteq HSP(P(\mathcal{A})) = HSP(\mathcal{A})$.

The proof that $HSP(\mathcal{A})$ is closed under $H, S,$ and $P$ is analogous. □

3.3. Birkhoff’s Theorem

Incomplete German version, to be completed.

3.3.0.1. Algebren. Eine Struktur $\mathcal{A}$ mit funktionaler Signatur $\tau$ (keine Relationssymbole) heißt Algebra.

- $f^\mathcal{A}$ heißt (fundamentale) Operation von $\mathcal{A}$.
- $t^\mathcal{A}$ für $\tau$-Term $t$ heißt Termoperation von $\mathcal{A}$.

Die Menge aller Termoperationen $t^\mathcal{A}(x_1, \ldots, x_n)$ ist

- abgeschlossen unter Komposition: wenn $l_0(x_1, \ldots, x_n), t_1(x_1, \ldots, x_m), \ldots, t_n(x_1, \ldots, x_m)$ Terme, dann auch $l_0(t_1, \ldots, t_n)(x_1, \ldots, x_m)$.
- enthält alle Projektionen: $(x_1, \ldots, x_n) \mapsto x_i$, für $i \in \{1, \ldots, n\}$. 


Mengen von Funktionen auf einer Menge $A$ die abgeschlossen sind unter Komposition
die die Projektionen enthalten heißen Klone $\text{Clo}(A)$: der Klon aller Termoperationen von $A$.

**Example 3.3.1.** Verbände: $\{\land, \lor, 0, 1\}$-Strukturen, die gewisse Eigenschaften erfüllen (Assoz., Komm., Idem., Abs., Einh.: siehe Skript von Henri Mühle).

**Example 3.3.2.** $A := \{0, 1\}$ wobei $\land$ die Funktion $(x, y) \mapsto \min(x, y)$. Wie sieht $\text{Clo}(A)$ aus? Sei $t(x_1, \ldots, x_n)$ ein $\{\land\}$-Term. Seien $x_1, \ldots, x_n$ die Variablen, die in $t$ auftauchen. Dann ist $t(A) = (x_1, \ldots, x_n) \mapsto \min(x_1, \ldots, x_n)$.

$\land$ ist eine Halbverbandsoperation:
\[
\forall x \quad \land(x, x) = x \quad (A)
\]
\[
\forall x, y \quad \land(x, y) = \land(y, x) \quad (C)
\]
\[
\forall x, y, z \quad \land(x, \land(y, z)) = \land(\land(x, y), z) \quad (I)
\]

Weitere Halbverbandsoperation: $\lor$, die Operation $(x, y) \mapsto \max(x, y)$.

**Example 3.3.3.** $A := \{0, 1\}; \land, \neg$ wobei $\neg$ die Funktion $x \mapsto 1 - x$.

$O^{(n)} := A^n = (A^n \to A)$. $O_A := \bigcup_{n \in \mathbb{N}} O^{(n)}$. Behauptung: $\text{Clo}(A) = O_A$. Beweis: Sei $f \in O^{(n)}$.

\[
t(x_1, \ldots, x_n) := \land_{(a_1, \ldots, a_n) \in A^n} \neg(\land_{a_i = 1} x_i)\]

Dann: $t(A) = f$.

**Example 3.3.4.** $A := \{0, 1\}; \text{minority}$ wobei minority $A$ die Funktion

$$(x_1, x_2, x_3) \mapsto x_1 + x_2 + x_3 \mod 2$$

ist eine Maltsevoperation $m$: sie erfüllt

$$\forall x, y, m(x, x, y) = m(y, x, x) = y$$

**Example 3.3.5.** $A := \{0, 1\}; +, \neg, 0$ wobei $A$ die Funktion $(x, y) \mapsto (x + y \mod 2) = x \oplus y$.

$A$ ist eine Gruppe; Jede Gruppe hat Maltsevterm $x \circ y^{-1} \circ z$.

**Example 3.3.6.** $A := \{0, 1\}; \text{majority}$ wobei $A$ die Funktion

$$(x, y) \mapsto \min(\max(x, y), \max(y, x), \max(x, z)) = \max(\min(x, y), \min(y, x), \min(x, z))$$

Eine Majoritätsoperation ist eine Operation $m$, die folgenden Axiomen genügt:

$$\forall x, y, m(x, y, y) = m(y, x, x) = m(y, x, x) = y$$

Auf der Grundmenge $\{0, 1\}$ gibt es nur eine Majoritätsfunktion.

**Universelle Algebra:** 
**Klassifikation** von Algebren und Klassen von Algebren.
- Klassifikation von $\text{Clo}(A)$ für alle 2-elementigen Algebren: Post’41.
- Es gibt überabzählbare viele Klone auf 3-elementiger Grundmenge: Yanov+Muchnik’59.

**3.3.1. Kongruenzen.** Sei $A$ eine $\tau$-Algebra und $E$ eine Äquivalenzrelation auf $A$. $E$ heißt Kongruenz von $A$ falls $E$ von allen Operationen in $A$ erhalten wird:
eine Funktion $f \in O^{(k)}_A$ erhält eine Relation $R$ falls für alle $t_1, \ldots, t_k \in R$ auch $f(t_1, \ldots, t_k) \in R$.

**Beispiele.** Kongruenzrelationen in Gruppen, in Ringen, in Körpern, etc.
- $N \triangleleft G$ dgd $\{(a, b) \mid ab^{-1} \in N\}$ ist Kongruenz.
• $E$ ist Kongruenzgdw $[1]_E$ ist normale Untergruppe.

**Lemma 3.3.7. Äquivalent:**

(1) $E$ ist Kongruenz von $A$.
(2) Es gibt einen Homomorphismus $h$ von $A$ in eine andere $\tau$-Algebra $B$ so dass $E$ der Kern $\{(a_1,a_2) \mid h(a_1) = h(a_0)\}$ ist von $h$.

**Proof.** (1) $\Rightarrow$ (2): Sei $A$ eine $\tau$-Algebra mit Kongruenz $E$. Definiere eine $\tau$-Algebra mit $B := A/E$ und

$$f_B([a_1]_E, \ldots, [a_k]_E) := [f(a_1, \ldots, a_k)]_E$$

Nachrechnen:

• ist wohldefiniert da $E$ Kongruenz;
• $h : A \to B$ mit $h(a) := [a]_E$ ist (surjektiver) Homomorphismus;
• $A/E := B$ heißt Faktoralgebra von $B$.

Umgekehrt: sei $h : A \to B$ ein Homomorphismus. Der Kern der Abbildung $h$ ist Äquivalenzrelation, und eine Kongruenz da $h$ Homomorphismus.

Falls $A \to B$ surjektiver Homomorphismus so heißt $B$ homomorphes Bild von $A$.

### 3.3.2. Subalgebren. Sei $A$ eine Algebra.

**Lemma 3.3.8.** $B \subseteq A$ wird genau dann von allen Operationen in $A$ erhalten, wenn $B$ Grundmenge einer Subalgebra von $A$ ist.

**Bem.** Wenn $\text{Clo}(A) = \text{Clo}(B)$, dann haben $A$ und $B$

• die gleichen Subalgebren
• die gleichen Kongruenzen

Übung:

• Was sind die Subalgebren von $A := \{0, 1\}; m$?
• Hat $A$ einen Halbverbandsterm?

### 3.3.3. Der Kongruenzverband. $A$: $\tau$-Algebra. $\text{Kon}(A)$: die Menge aller Kongruenzen von $A$.

**Lemma 3.3.9.** $(\text{Kon}(A), \subseteq)$ ist ein vollständiger Verband.

**Proof.** $\text{Kon}(A)$ ist unter beliebigen Schnitten abgeschlossen. Vereinigungen von Kongruenzen sind i.A. keine Kongruenzen! $R, S$ binäre Relationen $R \circ S := \{(x, z) \mid \exists y (R(x, y) \land R(y, z))\}$. Sei $(E_i)_{i \in I}$ eine Folge in $\text{Kon}(A)$. Definieren

$$E = \bigvee_{i \in I} E_i := \bigcup \{E_{i_1} \circ \cdots \circ E_{i_k} \mid i_1, \ldots, i_k \in I, k \in \mathbb{N}\}$$

Ist kleinste Äquivalenzrelation, die alle $E_i$ enthält. Seien nun $f \in \tau$ $n$-stellig und $(a_1, b_1), \ldots, (a_n, b_n) \in E$. Dann gibt es $i_1, \ldots, i_k \in I$ so dass für alle $j \in \{1, \ldots, n\}$

$$(a_j, b_j) \in E_{i_1} \circ \cdots \circ E_{i_k}$$

Also $(f(a_1, \ldots, a_n), f(b_1, \ldots, b_n)) \in E_{i_1} \circ \cdots \circ E_{i_k}$. Also $E \in \text{Kon}(A)$. □
3.3.4. Einfache Algebren. Letztes Mal: Kongruenzverband (Kon(\(A\)); \(\subseteq\)).
Spezielle Kongruenzen:
- \(\Delta_A\): die Diagonalrelation \(\{(a,a) \mid a \in A\}\)
- \(\nabla_A\): die Allrelation \(A^2\)
Algebren \(\underline{A}\), in denen \(\Delta_A\) und \(\nabla_A\) die einzigen Kongrenzen sind, heißen \emph{einfach}.
Beispiele:
(1) einfache Gruppen.
(2) Sei \(G\) eine Permutationsgruppe auf einer Menge \(A\).
Betrachte die Algebra \(\underline{A}\) mit Grundmenge \(A\) und Signatur \(G\), und definiere \(g^A := g\) für alle \(g \in G\). Dann heißt \(G\) \emph{primitiv} genau dann, wenn \(\underline{A}\) einfach ist.

3.3.5. Maltsev Bedingungen: Kongruenzdistributivität. Wiederholung VL Henri Mühle: Ein Verband \((P; \land, \lor, 0, 1)\) heißt \emph{distributiv} falls gilt
\[
\forall x, y, z \left( (x \land y) \lor z = (x \lor z) \land (y \lor z) \right) \\
\land \left( (x \lor y) \land z = (x \land z) \lor (y \land z) \right)
\]
Beispiele:
- Der Teilmengenverband \((P(M); \subseteq)\);
- Der Teilverband;
- Idealverbände (Darstellungssatz von Birkhoff);
- Jeder Verband ohne \(M_3\) und \(N_5\) als Unterverband (ohne Beweis).
Für welche Algebren \(\underline{A}\) ist \(\text{Kon}(\underline{A})\) distributiv? (\(\underline{A}\) ist ‘kongruenzdistributiv’).

3.3.6. Majoritäten und Kongruenzdistributivität.

\textbf{Lemma 3.3.10.} Sei \(\underline{A}\) eine Algebra mit einem Majoritästerm \(t\). Dann ist \(\underline{A}\) kongruenzdistributiv.

\textbf{Example 3.3.11.} Sei \(A\) durch \(<\) linear geordnet. Betrachte \(\underline{A} := (A; f)\) mit
\[
f^A(x, y, z) := \min(\max(x, y), \max(x, z), \max(y, z))
\]
(die \emph{Medianfunktion}).

\textbf{Example 3.3.12.} Sei \(A\) beliebige Menge. Betrachte \(\underline{A} := (A; f)\) mit
\[
f^A(x, y, z) := \begin{cases} 
  z & \text{falls } y = z \\
  x & \text{sonst}
\end{cases}
\]

\textbf{Proof.} Seien \(C, D, E \in \text{Kon}(\underline{A})\) und \((a, b) \in C \land (D \lor E)\).
Dann: \((a, b) \in C\) und es gibt \(c_1, \ldots, c_n\) mit \(aDc_1Ec_2Dc_3\ldots c_nEb\).
Für alle \(c \in A\) gilt
\[
m^A(a, c, b)Cm^A(a, c, a)
\]
Damit
\[
a = m^A(a, a, b)Cm^A(a, c_1, b) \quad (\text{zwei Mal Beobachtung})
\]
\[
(C \land E)m^A(a, c_2, b)
\]
\[
\ldots
\]
\[
(C \land D)m^A(a, c_n, b)
\]
\[
(C \land E)m^A(a, b, b) = b
\]
Also \((a, b) \in (C \land D) \lor (C \land E)\). \(\square\)
3.3.7. Maltsevbedingungen: Kongruenzpermutierbarkeit. $C_1, C_2 \in \text{Kon}(A)$ permutieren falls $C_1 \circ C_2 = C_2 \circ C_1$

$A$ heißt Kongruenzpermutierbar falls alle Paare von Kongruenzen von $A$ permutieren.

**Lemma 3.3.13.** Sei $A$ eine Algebra mit Maltsevterm $p$.

\[
\forall x, y. \quad p^A(y, x, x) = p^A(x, x, y) = y
\]

Dann ist der Kongruenzverband von $A$ kongruenzpermutierbar.

**Konsequenz.** Die Kongruenzen von den meisten klassischerweise betrachteten Algebren (Gruppen, Ringe, etc) permutieren.

**Proof.** Seien $C, E \in \text{Kon}(A)$. Es genügt zu zeigen:

\[
C \circ E \subseteq E \circ C.
\]

Sei $(a, b) \in C \circ E$. Also gibt es $c \in A$ mit $(a, c) \in C$ und $(c, b) \in E$.

\[
b = p^A(c, c, b) C p^A(a, c, b) E p^A(a, b, b) = a
\]

also $(b, a) \in C \circ E$ und $(a, b) \in E \circ C$. □


Benötigen dafür: Varietäten.

3.3.8. HSP. $K$: eine Klasse von Algebren mit Signatur $\tau$.

- $H(K)$: die Klasse aller homomorpher Bilder von Algebren in $K$.
- $S(K)$: die Klasse aller Subalgebren von Algebren in $K$.
- $P(K)$: die Klasse aller Produkte von Algebren in $K$.
- $I(K)$: die Klasse aller zu einer Algebra in $K$ isomorphen Algebren.
- $\text{Var}(K)$: die kleinste unter $H$, $S$, und $P$ abgeschlossene Klasse von Algebren, die $K$ enthält.

**Lemma 3.3.14.** $\text{Var}(K) = HSP(K)$.

**Proof.** $\supseteq$: klar.

$\text{Var}(K) \subseteq HSP(K)$:

Z.Z.: $HSP(K)$ unter $H$, $S$, und $P$ abgeschlossen.

- $H(HSP(K)) = HSP(K)$.
- $S(HSP(K)) \subseteq HS(SP(K)) = HSP(K)$.
- $P(HSP(K)) \subseteq HPSP(K) \subseteq HSPP(K) = HSP(K)$.

$K$ heißt **Varietät** falls $\text{Var}(K) = K = HSP(K)$.

**Beispiele.** Klasse aller Gruppen, Klasse aller Ringe.


$\text{Id}(K)$: Menge aller der Sätze der Gestalt (‘Identitäten’)

\[
\forall x. \quad t(x) = s(x)
\]

die in allen $A \in K$ gelten.

**Theorem 3.3.15** (Garet Birkhoff 1935). Sei $K$ eine Klasse von $\tau$-Algebren, und $A$ eine $\tau$-Algebra.

Dann ist $A \in HSP(K)$ genau dann wenn $\text{Id}(K) \subseteq \text{Id}(\{A\})$. 
**Konsequenz:** Eine Theorie $T$ ist zu einer Menge von Identitäten equivalent gdw. die Modelle von $T$ bilden eine Varietät.

**Beispiele.** Varietät aller Verbands, aller distributiven Verbands, aller Booleschen Algebren, etc

**Example 3.3.16.** Eine Boolesche Algebra ist eine Algebra der Gestalt

$$(B; \land, \lor, \neg, 0, 1)$$

wobei $(B; \land, \lor, 0, 1)$ ein distributiver Verband und $\neg$ eine einstellige Operation s.d.

$$\forall x. \neg(\neg(x)) = x$$

$$\forall x, y. \neg(x \land y) = \neg x \lor \neg y$$

$$\forall x, y. \neg(x \lor y) = \neg x \land \neg y$$

$$\forall x. \neg x \lor x = 1$$

$$\forall x. \neg x \land x = 0$$

**Beispiel.** $\{0, 1\}; \land, \lor, \neg, 0, 1$.

**Alternative Definition.** $B = (B; \land, \lor, \neg, 0, 1)$ ist Boolesche Algebra gdw $B \models \text{Id}\{\{0, 1\}; \land, \lor, \neg, 0, 1\}$.

**3.3.10. Beweis Birkhoff, einfache Richtung.** Let $\phi \in \text{Id}(K)$ be of the form

$\forall x_1, \ldots, x_n. s = t$. Let $A \in \text{HSP}(K)$.

- Sei $(B_i)_{i \in I}$ Folge in $K$ und $b^1, \ldots, b^n$ Elemente von $B := \prod_{i \in I} B_i$.

  $B \models s(b^1, \ldots, b^n) = t(b^1, \ldots, b^n)$

  $\Rightarrow s^B(b^1, \ldots, b^n) = t^B(b^1, \ldots, b^n)$

  $\Rightarrow s^B(b^1_i, \ldots, b^n_i) = t^B(b^1_i, \ldots, b^n_i)$ für alle $i \in I$

  $\Rightarrow B_i \models s(b^1_i, \ldots, b^n_i) = t(b^1_i, \ldots, b^n_i)$ für alle $i \in I$.

- Sei $B \in K$ und $A$ Subalgebra von $B$. Dann gilt $A \models \phi$ da $\phi$ universell.

- Sei $B \in K$ und $h: B \to A$ surjektiver Homomorphismus. Seien $a_1, \ldots, a_n \in A$. Dann gibt es $b_1, \ldots, b_n \in B$ mit $h(b_i) = a_i$.

  $s^B(b_1, \ldots, b_n) = t^B(b_1, \ldots, b_n)$ (da $B \models \phi$)

  $\Rightarrow h(s^B(b_1, \ldots, b_n)) = h(t^B(b_1, \ldots, b_n))$

  $\Rightarrow s^A(h(b_1), \ldots, h(b_n)) = t^A(h(b_1), \ldots, h(b_n))$ (h Homomorphismus)

  $\Rightarrow s^A(a_1, \ldots, a_n) = t^A(a_1, \ldots, a_n)$

**3.3.10.1. Die Termalgebra.** Sei $\tau$ eine funktionale Signatur und $X$ eine Menge.

**Definition 3.3.17 (Termalgebra).** Die Termalgebra $T(X)$ über $X$ mit Signatur $\tau$ ist folgende $\tau$-Algebra:

*Grundmenge ist die Menge aller $\tau$-Terme $T(X)$, und für $n$-stelliges $f \in \tau$ ist $f^{T(X)}(t_1, \ldots, t_n) := f(t_1, \ldots, t_n)$.*

**Bemerkungen.**

- $T(X)$ wird von $X$ erzeugt.

- Sei $\overline{A}$ eine $\tau$-Algebra. Dann hat jede Abbildung $f: X \to \overline{A}$ genau eine Erweiterung zu einem Homomorphismus von $T(X)$ nach $\overline{A}$.

  $f^A([t(x_1, \ldots, x_n)]) := t^A(f(x_1), \ldots, f(x_n))$

- $T(X)$ heißt frei über $X$ für die Klasse aller $\tau$-Algebren.
3.10.2. Die freie Algebra. Sei $K$ eine Klasse von $\tau$-Algebren.

**Definition 3.3.18.** Eine von $X \subset F$ erzeugte $\tau$-Algebra $F$ heißt frei über $X$ für $K$ falls für alle $A \in K$ und $f : X \rightarrow A$ eine Erweiterung von $f$ zu einem Homomorphismus von $F$ nach $A$ existiert.

**Eindeutigkeit:**
- Da $X$ ganz $F$ erzeugt, ist die Erweiterung von $f$ zu Homomorphismus von $F$ nach $A$ eindeutig.
- Falls $F_1$ frei über $X$ für $K$ und $F_2$ frei über $Y$ für $K$, und $|X| = |Y|$, dann ist $F_1 \cong F_2$.

3.10.3. Existenz der freien Algebra. Betrachte folgende Kongruenz von $T(X)

$$E := \bigcap \{ C \in \text{Kon}(T(X)) \mid T(X)/C \in IS(K) \}$$
Falls $X = \{ x_1, \ldots, x_n \}$ wird $T(X)/E$ erzeugt von $X/E := \{ [x_1]_E, \ldots, [x_n]_E \}$

**Lemma 3.3.19.** $FK(X) := T(X)/E$ ist frei über $X/E$ für $K$.

Zuerst: Minilemma. Seien $h : B \rightarrow A$ und $g : B \rightarrow C$ Homomorphismen, $\text{Kern}(g) \subseteq \text{Kern}(h)$, und $g$ ist surjektiv, dann gibt es einen Homomorphismus $f : C \rightarrow A$ mit $h = f \circ g$. Nämlich $x \mapsto h(g^{-1}(x))$.


Dann $E \subseteq \text{Kern}(h)$ da $T(X)/\text{Kern}(h) \in IS(|A|) \subseteq IS(K)$. Minilemma: $[t]_E \mapsto h(t)$ ist Homomorphismus $T(X)/E \rightarrow A$, der $f$ erweitert.

3.10.5. Die freie Algebra in ISP.

**Lemma 3.3.20.** $FK(X) \in ISP(K)$

**Proof.** Vorüberlegung: Seien $C_i \in \text{Kon}(B)$ für $i \in J$. Dann gilt $B/\bigcap_{i \in J} C_i \in IS(\prod_{i \in J} B/C_i)$.
3.3. BIRKHOFF’S THEOREM

3.3.10.6. Gleichungen, Terme, Homomorphismen. Sei \( X = \{x_1, \ldots, x_n\} \).

Lemma 3.3.21. \( \forall x_1, \ldots, x_n, s = t \) ist genau dann in \( \text{Id}(K) \) wenn
für alle \( A \in K \) und jeden Homomorphismus \( h : T(X) \to A \) gilt \( h(s) = h(t) \).

Proof. \( \Rightarrow \): Seien \( A \in K \) und \( h : T(X) \to A \).

\[
\begin{align*}
A &\models \forall x_1, \ldots, x_n, s = t & \text{(Nach Annahme)} \\
\Rightarrow s^A(h(x_1), \ldots, h(x_n)) &= t^A(h(x_1), \ldots, h(x_n)) & \text{(Definition von \( \models \))} \\
\Rightarrow h(s^A(x_1, \ldots, x_n)) &= h(t^A(x_1, \ldots, x_n)) & \text{(Definition \( T(X) \))} \\
\Rightarrow h(s) &= h(t) & \text{(h ist Homomorphismus)} \\
\end{align*}
\]

\( \Leftarrow \): seien \( A \in K \) und \( a_1, \ldots, a_n \in A \).

Dann gibt es Homomorphismus \( h : T(X) \to A \) mit \( h(x_1) = a_1, \ldots, h(x_n) = a_n \).

\[
\begin{align*}
s^A(a_1, \ldots, a_n) &= s^A(h(x_1), \ldots, h(x_n)) = h(s) \\
&= h(t) = t^A(h(x_1), \ldots, h(x_n)) = t^A(a_1, \ldots, a_n)
\end{align*}
\]

\[\square\]

3.3.10.7. Die Gleichungen der freien Algebra. \( K \): eine Klasse von \( \tau \)-Algebren und \( s, t \in T(X) \) für \( X = \{x_1, \ldots, x_n\} \). Äquivalent:

1. \( \forall x_1, \ldots, x_n, s = t \) \( \in \text{Id}(K) \)
2. \( F_K(X) \models \forall x_1, \ldots, x_n, s = t \)
3. \( [s]_E = [t]_E \) in \( F_K(X) = T(X)/E \)
4. \( (s, t) \in E = \bigcap \{C \in \text{Kon}(T(X)) \mid T(X)/C \in IS(K)\} \)

Insbesondere: falls \( \text{Id}(K) = \text{Id}(K') \), dann \( F_K(X) = F_K(X) \).

- Falls \( \forall \bar{x}. s = t \) \( \in \text{Id}(K) \) (1) dann \( E := F_K(X) \models \forall \bar{x}. s = t \) (2) da \( E \in ISP(K) \).
- Insbesondere \( [s]_E = [t]_E \) in \( F_K(X) \) (3) und damit \( s_E = t_E \) in \( F_K(X) \).
- Sei \( h : T(X) \to E \) der Homomorphismus \( h(t) := [t]_E \). Dann \( h(s) = s_E = t_E = h(t) \), also \( (s, t) \in \text{Kern}(h) = E \) (4).
- Sei \( A \in K \) und \( g : T(X) \to A \) Homomorphismus. Dann ist \( \text{Kern}(g) \supseteq E \), und es gibt Homomorphismus \( f : E \to A \) mit \( g = f \circ h \). Also: \( g(s) = f \circ h(s) = f \circ h(t) = g(t) \). Wegen Lemma: \( \forall \bar{x}. s = t \) \( \in \text{Id}(K) \).
3.10.8. Birkhoff Beweis. \( K \): eine Klasse von \( \tau \)-Algebren.
\( A \): \( \tau \)-Algebra so dass \( \text{Id}(K) \subseteq \text{Id}\{A\} \).
Sei \( K' \) die Klasse aller Modelle von \( \text{Id}(K) \).

Wissen:
- \( A \in K' \);
- \( K' \) ist Varietät;
- \( K \subseteq K' \);
- \( \text{Id}(K') = \text{Id}(K) \);
- \( F_K(X) = F_{K'}(X) \).

Wähle \( X \) mit \( |X| \geq |A| \). Da \( A \in K' \) gibt es Homomorphismus \( h : F_{K'}(X) \to A \).

Also:
\[ A \in H(F_{K'}(X)) = H(F_K(X)) \subseteq HSP(K) \]

3.11. Kochrezept Erhaltungssätze. Der Satz von Birkhoff als Erhaltungssatz:

<table>
<thead>
<tr>
<th>Logisches Konstrukt</th>
<th>Eigenschaft von Operationen</th>
<th>HPT</th>
<th>Birkhoff</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \neq )</td>
<td>injektiv</td>
<td>( \times )</td>
<td>( \times )</td>
</tr>
<tr>
<td>( \forall )</td>
<td>surjektiv</td>
<td>( \times )</td>
<td>( \sqrt{\checkmark} )</td>
</tr>
<tr>
<td>( \neg ) (atomare Negation)</td>
<td>stark</td>
<td>( \times )</td>
<td>( \times )</td>
</tr>
<tr>
<td>( \vee )</td>
<td>einstellig</td>
<td>( \sqrt{\checkmark} )</td>
<td>( \times )</td>
</tr>
<tr>
<td>( \exists )</td>
<td>(bei mehrstelligeren Operationen)</td>
<td>( \sqrt{\checkmark} )</td>
<td>( \times )</td>
</tr>
<tr>
<td>( \wedge )</td>
<td>(bei partiellen Operationen)</td>
<td>( \sqrt{\checkmark} )</td>
<td>( \sqrt{\checkmark} )</td>
</tr>
<tr>
<td>( = )</td>
<td>(bei ‘Hyperfunktionen’)</td>
<td>( \sqrt{\checkmark} )</td>
<td>( \sqrt{\checkmark} )</td>
</tr>
</tbody>
</table>

3.4. Maltsev Conditions

\( C_1, C_2 \in \text{Kon}(A) \) permutieren falls
\[ C_1 \circ C_2 = C_2 \circ C_1 \]
\( A \) heißt kongruenzpermütierbar falls alle Paare von Kongruenzen von \( A \) permutieren.

**Lemma 3.4.1** (Wiederholung). Sei \( A \) eine Algebra mit Maltsevterm \( p \).
\[ \forall x, y \quad p^A(y,x,x) = p^A(x,x,y) = y \]

Dann ist \( A \) kongruenzpermütierbar.

**Konsequenz.** Die Kongruenzen von den meisten klassischerweise betrachteten Algebren (Gruppen, Ringe, etc) permutieren.

**Exakte Charakterisierung der Existenz von Maltsevtermen?**

3.4.1. Kongruenzpermütierbarkeit, zweiter Besuch. Sei \( K \) eine Klasse von \( \tau \)-Algebren.

**Theorem 3.4.2** (Maltsev). Die Algebren in \( HSP(K) \) sind genau dann kongruenzpermütierbar, wenn es ein \( t \in T(\{x,y\}) \) gibt mit \( K \models \forall x, y. t(y,x,x) = t(x,x,y) = y \).

**Proof.** \( \Leftarrow \): folgt aus Lemma und einfacher Richtung von Birkhoff.
\( \Rightarrow \). **Schreibenweise**: Für \( E := F_K(X) \) und \( x, y \in X \),

schreiben \( C(x, y) \) für die kleinste Kongruenz von \( E \), die \( (x, y) \) enthält.

Sei \( F := F_K(\{x, y, z\}) \).

Sei \( C_1 := C(x, y) \in \text{Kon}(E) \) und \( C_2 := C(y, z) \in \text{Kon}(E) \).

Da \( (x, z) \in C_1 \circ C_2 = C_2 \circ C_1 \) gibt es \( b \in F \) mit \( (x, b) \in C_2 \) und \( (b, z) \in C_1 \).

Da \( F \) von \( \{x, y, z\} \) erzeugt wird, gibt es \( \tau \)-Term \( p(x, y, z) \) mit \( b = p^F(x, y, z) \).
3.4. MALTSEV CONDITIONS


\[ (D1) \quad x \land (y \lor z) = (x \land y) \lor (x \land z) \]

\[ (D2) \quad x \lor (y \land z) = (x \lor y) \land (x \lor z) \]

**Theorem 3.4.3 (Jónsson).** Die Algebren in \( HSP(K) \) sind genau dann kongruenzdistributiv, wenn es ein \( n \in \mathbb{N} \) und \( \tau \)-Terme \( p_0, \ldots, p_n \) gibt so dass

\[ K \models \forall x, y. p_i(x, y, x) = x \quad \text{für } i \in \{1, \ldots, n\} \]

\[ p_0(x, y, z) = x \]

\[ p_1(x, y, x) = p_{i+1}(x, y, y) \quad \text{für } i \text{ gerade} \]

\[ p_1(x, y, x) = p_{i+1}(x, y, y) \quad \text{für } i \text{ ungerade} \]

\[ p_n(x, y, z) = z \]

**Proof.** "⇒". Sei \( F := F_K(\{x, y, z\}) \).

\[ C(x, z) \land (C(x, y) \lor C(y, z)) = (C(x, z) \land C(x, y)) \lor (C(x, z) \land C(y, z)) \]

Also \((x, z) \in (C(x, z) \land C(x, y)) \lor (C(x, z) \land C(y, z))\) in \( F \).

Also gibt es \( p_1, \ldots, p_{n-1} \in F \) mit

\[ x(C(x, z) \land C(x, y))p_1 \]

\[ x = p_1(x, y, x) = p_1(x, y, y). \]

\[ p_2(C(x, z) \land C(y, z))p_2 \]

\[ p_1(x, y, x) = p_2(x, y, x), \]

\[ p_1(x, y, y) = p_2(x, y, y), \]

\[ \vdots \]

\[ p_{n-1}(C(x, z) \land C(y, z))z \]

\[ x = p_{n-1}(x, y, x) = p_{n-1}(x, y, y) = z \]

"⇐". Seien \( C_1, C_2, C_3 \in \text{Kon}(A) \) für \( A \in HSP(K) \). R.Z.Z:

\[ C_1 \land (C_2 \lor C_3) \subseteq (C_1 \land C_2) \lor (C_1 \land C_3) \]

\[ \supseteq \text{ gilt in jedem Verband} \]

Sei \((a, b) \in C_1 \land (C_2 \lor C_3)\). D.h., es gibt \( c_1, \ldots, c_t \) mit

\[ aC_2c_1C_3c_2C_3 \cdots c_tC_3b \]

Also für \( i \in \{1, \ldots, n\} \):

\[ p_i(a, a, b)C_2p_i(a, c_1, b)C_3p_i(a, c_2, b) \cdots C_3p_i(a, b, b) \]

und wegen \( p_i(a, c, b)C_1p_i(a, c, a) = a \):

\[ p_i(a, a, b)(C_1 \land C_2)p_i(a, c_1, b)(C_1 \land C_3)p_i(a, c_2, b) \cdots (C_1 \land C_3)p_i(a, b, b) \]

also

\[ p_i(a, a, b)((C_1 \land C_2) \lor (C_1 \land C_3))p_i(a, b, b) \]

Gleichungen liefern dann: \( a((C_1 \land C_2) \lor (C_1 \land C_3))b \).
3.4.3. Modularität. Ein Verband $V$ heißt modular falls gilt
\[ \forall x, y. \ x \leq y \Rightarrow (x \lor (y \land z) = y \land (x \lor z)) \]
äquivalent (da $x \leq y \Leftrightarrow (x = x \land y)$):
\[ \forall x, y, z. \ (x \land y) \lor (y \land z) = y \land ((x \land y) \lor z) \]

Lemma 3.4.4. Distributivität impliziert Modularität.

Sei $x \leq y$.
\[ x \lor (y \land z) = (x \lor y) \land (x \lor z) \] (D2)
\[ = y \land (x \lor z) \] (da $x \lor y = y$)

3.4.4. $N_5$.

$N_5$ ist nicht modular: $a \leq b$, aber
\[ a \lor (b \land c) = a \]
\[ \neq b = b \land (a \lor c) \]

Theorem 3.4.5 (Dedekind). $V$ ist genau dann modular, wenn es keine Einbettung $N_5 \to V$ gibt.

Proof. Angenommen, $a, b, c \in V$ mit $a \leq b$ und $a_1 := a \lor (b \land c) < b_1 := b \land (a \lor c)$. Nachrechnen: $c \land b_1 = c \land b$ und $c \lor a_1 = c \lor a$.

3.4.5. Kongruenzmodularität.

Proposition 3.4.6. Wenn $A$ kongruenzpermutierbar, dann ist $A$ kongruenzmodular.

Proof. Seien $C_1, C_2, C_3 \in \text{Kon}(A)$ mit $C_1 \subseteq C_2$. Z.Z.:
\[ C_2 \land (C_1 \lor C_3) \subseteq C_1 \lor (C_2 \land C_3) \]
Sei also $(a, b) \in C_2 \cap (C_1 \lor C_3)$.
Kongruenzpermutierbarkeit: $C_1 \lor C_3 = C_1 \circ C_3$.
Also gibt es $c$ mit $aC_1cC_3b$.
$(a, c) \in C_2$ da $C_1 \subseteq C_2$.
Da $(a, b) \in C_2$ gilt $(c, b) \in C_2$ da $C_2$ Äquivalenzrelation.
Also $(c, b) \in C_2 \cap C_3$.
Da $(a, c) \in C_1$ haben wir $(a, b) \in C_1 \circ (C_2 \cap C_3) \subseteq C_1 \lor (C_2 \land C_3)$.
3.4.6. Gummterme. Sei $\mathcal{K}$ eine Klasse von $\tau$-Algebren.

**Theorem 3.4.7 (Gumm).** Alle Algebren in $HPS(\mathcal{K})$ sind kongruenzmodular gdw es gibt $n \in \mathbb{N}$ und $\tau$-Terme $q_0, \ldots, q_n, p$ so dass für alle $i \in \{0, 1, \ldots, n\}$

$\mathcal{K} \models \forall x, y. q_i(x, y, x) = x$
$\quad \land q_0(x, y, z) = x$
$\quad \land q_i(x, y, y) = q_{i+1}(x, y, y)$ für gerade $i$
$\quad \land q_i(x, x, y) = q_{i+1}(x, x, y)$ für ungerade $i$
$\quad \land q_n(x, y, y) = p(x, y, y)$
$\quad \land p(x, x, y) = y$

**Exercises.**

(20) Show that $SH(\mathcal{K}) \subseteq HS(\mathcal{K}), PS(\mathcal{K}) \subseteq SP(\mathcal{K})$, and $PH(\mathcal{K}) \subseteq HP(\mathcal{K})$.

(21) Let $f: A \to \prod_{i \in I} A_i$ be a homomorphism. Show that

$\text{Kernel}(f) = \bigcap_{i \in I} \text{Kernel}(\pi_i \circ f)$

(22) Show that the variety of all lattices is congruence distributive, but not congruence permutable.

(23) Show that the variety of Boolean algebras is both congruence permutable and congruence distributive.

(24) Show that a lattice satisfies the identities

$\forall x, y, z. x \land (y \lor z) = (x \land y) \lor (x \land z)$
$\forall x, y, z. x \lor (y \land z) = (x \lor y) \land (x \lor z)$

if and only if it satisfies one of those identities.
CHAPTER 4

Finite Model Theory

Many important properties of structures cannot be expressed by first-order sentences. A large part of finite model theory is devoted to the study of extensions of first-order logic, often motivated by applications in database theory, graph theory, and complexity. We recommend the freely available textbook of Libkin [6] for background and additional material in finite model theory.

Proposition 4.0.1. There is no first-order sentence that holds on a graph if and only if the graph is connected.

Proof. Let $E$ be a binary relation symbol for the edge relationship in a graph, and suppose for contradiction that $\phi$ is a first-order formula that expresses connectedness as in the statement of the proposition. Let $u$ and $v$ be constant symbols and let $\psi_n$ be the sentence

$$\exists x_1, \ldots, x_n (E(u, x_1) \land \bigwedge_{i \in \{1, \ldots, n-1\}} E(x_i, x_{i+1}) \land E(x_n, v))$$

which states that there exists a path from $u$ to $v$. Note that the theory

$$\{\phi\} \cup \{\neg \psi_i \mid i \in \mathbb{N}\}$$

is unsatisfiable since $u$ and $v$ must be disconnected. But this contradicts compactness, since finite subsets of this theory are satisfied by graphs where $u$ and $v$ are at large enough distance.

Similarly, the following properties are not first-order:

- Graph $n$-colorability for any $n \geq 2$;
- Hamiltonicity of graphs;
- Existence of perfect matchings in graphs;
- The property of having an even number of vertices;
and most of the properties of graphs studied in discrete mathematics.

Exercises.

25) Show that Evenness of the number of elements of a finite structure over the empty signature is not a first-order property.

4.1. Second-Order Logic

A possible response to the weakness of first-order logic is to add expressive power via second-order quantification. We simply extend the syntax of first-order logic by adding the following item to the inductive definition:

- if $R \notin \tau$ is a relation symbol, and $\phi$ is a $\tau \cup \{R\}$-formula, then $\exists R.\phi$ is a $\tau$-formula.

In the definition of the semantics of $\tau$-formulas $\phi$, we treat second-order quantification as follows:
• if $\psi$ equals $\exists R. \phi$ then
  \[ \psi^A := \{ \bar{a} \mid \text{there exists a \((\tau \cup \{R\})\)-expansion} \ A' \text{ of} \ A \text{ s.t.} \ \bar{a} \in \phi^A' \}. \]

As for universal first-order quantification, universal second-order quantification $\forall R. \phi$ can be introduced as a shortcut for $\neg \exists R. \neg \phi$. Similarly as for first-order formulas, it can be shown that any second-order formula may be transformed into an equivalent formula with all second-order quantifiers in front.

**Example 4.1.1.** Clearly, connectivity of graphs can be expressed in second-order logic: viewing graphs as \{E\}-structures, we can e.g. use the formula

\[
\exists P \ \exists x, y \ (P(x) \land \neg P(y)) \\
\land \forall x', y' \ ((P(x') \land \neg P(y')) \Rightarrow \neg E(x', y'))
\]

Since the proof of Proposition 4.0.1 essentially only used compactness of first-order logic, this example shows that second-order logic does not satisfy the compactness theorem.

**Example 4.1.2.** The natural numbers with addition and multiplication have a second-order axiomatisation. By this we mean that there exists a second-order sentence $\phi$ such that every model of $\phi$ is isomorphic to $(\mathbb{N}; +, \cdot)$.

We will show the same statement for $(\mathbb{N}; s, 0)$ where $s$ is a unary function symbol for the successor function, and then show that addition and multiplication can be defined by universal second-order sentences over $(\mathbb{N}; s, 0)$, which implies the above claim. Our second-order axiomatisation for $(\mathbb{N}; s, 0)$ is known as the Peano axioms:

- $s$ is injective;
- $\forall n. s(n) \neq 0$.
- $\forall K \ (0 \in K \land \forall n(n \in K \Rightarrow s(n) \in K)) \Rightarrow \forall n n \in K$.

Now, addition has the following second-order definition\(^1\)

\[ x + y = z :\iff \forall f \ ((f(0) = x \land \forall k (f(s(k)) = s(f(k))) \Rightarrow f(y) = z). \]

Note that we then have that

\[ x + 0 = x \]

and \[ x + s(y) = s(x + y) \]

which is per se, however, not an explicit second-order axiomatisation. Multiplication can be defined similarly.

More generally, we will be interested in properties of structures that can be expressed in second-order logic or restricted versions of second-order logic. Here, by property we simply mean a class of structures of some fixed (typically relational and finite) signature $\tau$ (typically closed under isomorphism). A property of finite structures is a class of finite $\tau$-structures. We say that a property $P$ is expressed by a second-order sentence $\phi$ if and only if $\mathcal{A} \in P$ if and only if $\mathcal{A} \models \phi$. Expressibility of properties of finite structures is defined analogously, and belongs to the core concerns of finite model theory.

---

\(^1\)We use quantification over functions; this can be replaced by quantification over relations since we have a first-order characterisation of those relations that are graphs of functions.
4.2. Existential Second-Order Logic

We consider an important fragment of second-order logic obtained by restricting to formulas in prenex normal form where all second-order quantifiers are existential. The resulting logic is abbreviated by \( ESO \). We have already seen an ESO sentence in Example 4.1.1.

**Proposition 4.2.1.** For every \( k \in \mathbb{N} \) graph \( k \)-colorability (see Example 1.2.2) can be expressed in ESO.

**Proof.** Use the sentence
\[
\exists C_1, \ldots, C_k \forall x \left( C_1(x) \vee \cdots \vee C_k(x) \right) \\
\wedge \forall x \bigwedge_{i \neq j} (\neg C_i(x) \vee \neg C_j(x)) \\
\wedge \forall x, y \bigwedge_i (\neg E(x, y) \vee \neg C_i(x) \vee \neg C_i(y))
\]

\( \square \)

4.2.1. **Good characterisations.** If a property can be expressed in ESO, then in general we do not know whether the complement of the property is in ESO. Negating the formula syntactically would yield a universal second-order sentence, abbreviated by \( USO \). However, when we are interested in properties of finite structures, there are examples where the complement is expressible in ESO, too. An example of such a property is acyclicity of finite digraphs, i.e., the property of finite directed graphs not to contain a directed cycle.

**Proposition 4.2.2.** Acyclicity of finite digraphs is expressible both in ESO and in USO.

**Proof.** The ESO sentence
\[
\exists T \forall x, y, z \left( E(x, y) \Rightarrow T(x, y) \right) \\
\wedge (T(x, y) \wedge T(y, z) \Rightarrow T(x, z)) \\
\wedge \neg T(x, x)
\]
expresses that \( E \) has an irreflexive transitive extension \( T \), and hence is acyclic (this sentence would also work for expressing acyclicity of infinite digraphs).

On the other hand, the USO sentence
\[
\forall U \exists x \left( \forall y. \neg E(x, y) \right) \vee \left( \forall y. \neg E(y, x) \right)
\]
expresses acyclicity of finite digraphs: if \( C \) were a cycle, then \( U := C \) would contain neither sources nor sinks, so the sentence would be false; conversely, if the sentence is false, there exists a set \( U \) without sources and sinks, and such a set, for finite digraphs, must contain a cycle.  \( \square \)

The next example of a property that is expressible both in ESO and in USO illustrates an important trick when working with ESO on finite structures: introducing a linear order, and introducing the successor with respect to this linear order.

**Proposition 4.2.3.** The property of a finite structure to have an even number of elements is expressible in ESO and in USO.
Proof. Consider the ESO sentence
\[ \exists L, E \forall x, y, z \exists u (L(x, y) \land L(y, z) \Rightarrow L(x, z)) \]
\[ \land (\neg L(x, y) \lor \neg L(y, x)) \land \neg L(x, x) \]
\[ \land (S(x, y) \Rightarrow L(x, y)) \]
\[ \land (\neg L(x, y) \lor (L(x, u) \land L(u, y)) \lor S(x, y)) \]
\[ \land (E(x) \land S(x, y) \Rightarrow E(y)) \]
\[ \land (\neg E(x) \land S(x, y) \Rightarrow E(y)) \]
\[ \land (\neg F(x) \lor L(x, y) \land x = y) \land (F(x) \lor \neg L(x, y) \land x \neq y) \]
\[ \land (T(x) \lor L(y, x) \land x = y) \land (T(x) \lor \neg L(y, x) \land x \neq y) \]
\[ \land (F(x) \Rightarrow E(x)) \]
\[ \land (T(x) \Rightarrow \neg E(x)) \]

The sentence expresses that there exists a linear order \( L \) on the domain, that \( S \) is the successor relation with respect to \( L \), and that \( F \) holds on precisely on the first and \( T \) on the last element of \( L \). It then expresses that the elements are alternatingly in \( E \) and outside \( E \) along this order, that the first element is in \( E \) and the last element in outside \( E \). This is the case if and only if there is an even number of elements. It is straightforward to modify this to obtain a formula that expresses that there is an odd number of elements. \( \square \)

Properties of finite structures that are both in ESO and in USO (such as digraph acyclicity and evenness) are said to have a good characterisation (the term good characterisations goes back to Jack Edmonds who promoted them). Most of the fundamental questions one can ask about good characterisations are unresolved. We start with the following.

Question 4.1. Is 3-colorability of finite graphs in USO?

This is one of the most studied questions in all of mathematics. The reason is that Question 4.1 has countless equivalent formulations, each studied by many mathematicians and computer scientists in the last 70 years. Most notably, Question 4.1 is equivalent to the following question.

Question 4.2. Is the complement of every property of finite structures in ESO also in ESO?

In other words: we ask whether for every ESO sentence \( \phi \) there exists an ESO sentence \( \psi \) such that for all finite \( \tau \)-structures \( A \) we have
\[ A \models \phi \text{ if and only if } A \models \neg \psi. \]

Remark 4.2.4. It is quite common to say that a class of finite \( \tau \)-structures \( P \) is in ESO (or, analogously, is in USO) if there exists an ESO sentence \( \Phi \) that holds on precisely those \( \tau \)-structures that are in \( P \); that is, the logic is identified with the class of classes of structures that can be expressed by sentences in this logic. Hence, we have yet another equivalent formulation of Question 4.2: on finite structures, is ESO = USO?

If we drop the assumption about the finiteness of the structures in Question 4.2 the answer is negative (many thanks to Anuj Dawar for pointing out to me the proof of the following theorem).

Theorem 4.2.5. There are USO sentences that are not equivalent to ESO sentences (on infinite structures).
4.2. EXISTENTIAL SECOND-ORDER LOGIC

Proof. We have already seen in Example 4.1.2 that there exists a universal second-order sentence $\Phi$ such that every structure satisfying $\Phi$ is isomorphic to $(\mathbb{N}; +, \cdot)$. Suppose for contradiction that $\Psi$ is an ESO sentence that is equivalent to $\Phi$; we can choose $\Psi$ to be in prenex normal form. Then $(\mathbb{N}; +, \cdot)$ satisfies $\Psi$, and hence there exists an expansion $A$ of $(\mathbb{N}; +, \cdot)$ that satisfies the first-order part $\psi$ of $\Psi$. By Exercise 9, the sentence $\psi$ also has an uncountable model $B$. But then $B$ witnesses that $\Psi$ holds on an uncountable structure, too, contradicting the assumptions on the equivalent sentence $\Phi$. □

4.2.2. Complete Problems for ESO. To prove that a positive answer to Question 4.1 would imply a positive answer to Question 4.2, it is convenient to go via yet another equivalent problem, the 3-Sat problem. The Satisfiability Problem is the following problem:

• determine for a given $\{\land, \lor, \neg, 0, 1\}$-term (i.e., a term in the language of Boolean algebras) whether $t = 1$ is satisfiable in the two-element Boolean algebra.
• Equivalently: given a quantifier-free first-order sentence over a signature with relation symbols of arity zero, determine whether the sentence has a model.

We would like to code this problem as a property of finite structures. As we have seen in Section 3, every quantifier-free formula and every term in the language of Boolean algebras can be equivalently rewritten in conjunctive normal form. For 3-Sat, we additionally pose the restriction that each clause in this normal form consists of three literals only. That is, each clause can have one out of 8 possible shapes, depending on which literals are positive and negative, e.g.,

$$x_1 \lor x_2 \lor \neg x_3$$

We now view a 3-Sat instance as a relational structure where the elements are the variables of the term and where the signature $\tau_{3\text{-sat}}$ contains a ternary relation symbol for each of the 8 shapes of clauses. That is, we consider the signature

$$\tau_{3\text{-sat}} := \{C_{i,j,k} \mid i, j, k \in \{0, 1\}\}$$

and we are interested in the class of those $\tau_{3\text{-sat}}$-structures that homomorphically map to the structure $B_{3\text{-sat}}$ with domain $A = \{0, 1\}$ where

$$C_{i,j,k}^A := \{(a, b, c) \mid a +_2 i \lor b +_2 j \lor c +_2 k = 1\}$$

and $+_2$ denotes addition modulo 2.

Proposition 4.2.6. 3-Sat can be expressed in ESO.

Proof. Consider the ESO sentence

$$\exists T \forall x, y, z (\neg C_{000}(x, y, z) \lor T(x) \lor T(y) \lor T(z))$$

$$\land \neg C_{100}(x, y, z) \lor \neg T(x) \land T(y) \land T(z)$$

$$\land \ldots)$$

□

Definition 4.2.7 (First-order Interpretations). Let $\tau$ and $\sigma$ be two relational signatures and $d \in \mathbb{N}$.

• A (d-dimensional) first-order interpretation of $\tau$ in $\sigma$ consists of the formulas $\phi_\tau(x_1, \ldots, x_d)$, $\phi_\sigma(x_1, \ldots, x_{2d})$, and a sequence $(\phi_R)_{i \in \tau}$ of $\sigma$-formulas $\phi_R$ with free variables $x_1, \ldots, x_{d \cdot \text{ar}(R)}$. 

If $A$ is a $\sigma$-structure, then $I(A)$ denotes the $\tau$-structure $B$ whose universe is $\{ \bar{a} \in A^d \mid A \models \phi_\tau(\bar{a}) \}/E$ where $E := \{ (\bar{a}, \bar{b}) \mid A \models \phi_{=} (\bar{a}, \bar{b}) \}$ is an equivalence relation on $A^d$. For $R \in \tau$ of arity $k$, we have

$$R^B := \{ (e_1, \ldots, e_k) \in (A^d/E)^k \mid A \models \phi_R(\bar{a}^1, \ldots, \bar{a}^k) \text{ for some } \bar{a}^i \in e_i \}.$$ 

**Example 4.2.8.** Let $G$ be a graph. Then the line graph of $G$ is a graph whose vertices are the edges of $G$ and where two vertices are connected if they have non-empty intersection. Note that the line graph of $G$ equals $I(G)$ for the following 2-dimensional first-order order interpretation:

- $\phi_{=} (x_1, x_2) := E(x_1, x_2)$
- $\phi_{=} (x_1, x_2, y_1, y_2) := (x_1 = y_1 \land x_2 = y_2) \lor (x_1 = y_2 \land x_2 = y_1)$
- $\phi_E (x_1, x_2, y_1, y_2) := (x_1 = y_1 \lor x_2 = y_1) \lor (x_2 = y_1 \lor x_2 = y_2) \land (x_1 \neq y_1 \lor x_2 \neq y_2)$

**Definition 4.2.9 (First-order Reductions).** Let $\mathcal{P}$ and $\mathcal{S}$ be two properties of finite structures of signature $\tau$ and $\sigma$, respectively. A first-order reduction from $\mathcal{P}$ to $\mathcal{S}$ is a first-order interpretation $I$ of $\tau$ in $\sigma$ such that for all finite $\tau$-structures $A$ we have

$$A \in \mathcal{P} \text{ if and only if } I(A) \in \mathcal{S}.$$ 

**Example 4.2.10.** Consider the property $\mathcal{P}$ of finite graphs $G$ whether the edges of $G$ can be coloured by $\{1, \ldots, k\}$ such that edges that share a vertex get assigned
4.2. EXISTENTIAL SECOND-ORDER LOGIC 49

different colours. Then the interpretation \( I \) from Example 4.2.8 is a reduction from \( \mathcal{P} \) to the property of graph \( k \)-colorability, because \( G \in \mathcal{P} \) if and only if \( L(G) = I(G) \) is \( k \)-colourable.

The following lemma is not difficult to see, but tedious to work out in full detail, so that we do not present the proof at this point, but rather refer to [6] for details².

**Lemma 4.2.11.** Suppose that \( \mathcal{P} \) is in ESO, and that \( \mathcal{S} \) has a first-order reduction to \( \mathcal{P} \). Then \( \mathcal{S} \) is in ESO.

**Proposition 4.2.12.** 3-SAT has a first-order reduction to 3-colouring.

**Proof.** Let \( A \) be a finite \( \tau_{3\text{-sat}} \)-structure. We are looking for an interpretation \( I \) such that \( A \) homomorphically maps to \( B_{3\text{-sat}} \) if and only if \( I(A) \) is 3-colourable. If \( |A| \) has only one element (which is a first-order property), we choose \( I(A) \) to be either one vertex with a loop in case that there is no homomorphism from \( A \) to \( B_{3\text{-sat}} \), and one vertex without a loop otherwise. Otherwise, we construct \( I(A) \) as follows.

![Figure 4.2. Illustration for the construction of the first-order reduction from 3-Sat to 3-Colouring.](image)

- The graph \( I(A) \) has three distinguished vertices \( t, f, r \) that span a triangle.
- For each \( a \in A \) the graph \( I(A) \) contains two vertices \( p_a, n_a \) and the edges \((p_a, n_a), (n_a, r), (p_a, r)\).
- For each \( T = (a, b, c) \in C_{ijk} \) the graph \( I(A) \) has vertices \( u^1_T, \ldots, u^6_T \) and edges that form a triangle on \( u^1_T, u^2_T, u^3_T \), on \( u^4_T, u^5_T, u^6_T \), and edges \((u^3_T, r), (u^6_T, r), \) and \((u^6_T, f)\).
- If \( i = 1 \) then link \( u^1_T \) to \( n_a \), otherwise link \( u^2_T \) to \( p_a \). If \( j = 1 \) then link \( u^4_T \) to \( n_b \), otherwise link \( u^5_T \) to \( p_b \). If \( k = 1 \) then link \( u^3_T \) to \( n_c \), otherwise link \( u^6_T \) to \( p_b \).

The verification of the following is left to the reader:

1. If \( A \) is satisfiable, then \( I(A) \) is 3-colourable.
2. If \( I(A) \) is 3-colourable, then \( A \) is satisfiable.
3. There exists an interpretation \( I \) such that \( I(A) \) looks as described above.

\(\square\)

**Proposition 4.2.13.** Every problem in ESO has a first-order reduction to 3-SAT.

**Proof.** Let \( \Phi \) be an ESO \( \tau \)-sentence, and let \( \phi \) be the first-order part of \( \Phi \). We assume that \( \phi \) is in prenex normal form in conjunctive normal form. It is easy to see that two existentially quantified relation symbols of arity \( k \) and \( l \) can be replaced by

²The statement essentially follows from what is known as Fagin’s theorem.
one relation symbol of arity $k + l$ and that the formula can be adapted correspondingly so that the resulting formula is equivalent. By iterated application of this observation we can assume that $\Phi$ has a single existentially quantified $m$-ary relation symbol $R$.

Let $\mathcal{A}$ be a finite $\tau$-structure with domain $\mathcal{A} = \{a_1, \ldots, a_n\}$. We produce a 3-SAT instance that is satisfiable if and only if $\mathcal{A} \models \Phi$. Note that $\mathcal{A} \models \Phi$ if and only if $\mathcal{A}'$ has a $(\tau \cup \{R\})$-expansion such that $\mathcal{A}' \models \phi$. For each $\bar{a} \in \mathcal{A}$ our 3-SAT instance has a variable $x_{\bar{a}}$. The idea is that the variable $x_{\bar{a}}$ codes whether $R(\bar{a})$ holds in $\mathcal{A}'$. Note that $\forall x.\psi(x)$ holds in $\mathcal{A}'$ if and only if $\bigwedge_{b \in \mathcal{A}} \psi(b)$ holds. Similarly, $\exists x.\psi(x)$ holds in $\mathcal{A}'$ if and only if $\bigvee_{b \in \mathcal{A}} \psi(b)$ holds in $\mathcal{A}'$. However, in 3-SAT we are allowed 3 disjuncts only. But larger disjunctions $\bigvee_{i \in \{1, \ldots, n\}} \psi_i$ can be expressed in a 3-SAT instance by introducing additional variables $y_1, \ldots, y_n$ and using the formula

$$(\neg y_0 \lor \psi_1) \land \neg y_n \land \bigwedge_{i \in \{0, \ldots, n-1\}} (y_i \lor \psi_i \lor y_{i+1}).$$

Hence, we can assume in the following that all the variables of $\phi$ are instantiated by values from $\mathcal{A}$. Conjunctions and disjunctions in $\phi$ are translated similarly as above. Finally, an atomic formula in $\phi$ of the form $R(\bar{a})$ is translated by $x_{\bar{a}}$, and an atomic formula of the form $S(\bar{a})$ for $S \in \tau$ is translated by 0 if $\bar{a} \in S\mathcal{A}$ and by 1 otherwise.

It can be shown that the 3-SAT instance that we have described above can be computed from $\mathcal{A}$ via a first-order interpretation $I$. \hfill \Box

Note that in the proof, the assumption that the structure $\mathcal{A}$ is finite was crucial.

**Corollary 4.2.14.** Question 4.1 and Question 4.2 are equivalent.

**Useful terminology.** When $\mathcal{C}$ is a class of classes of finite structures (also called a complexity class) and $\mathcal{P}$ is a class of structures, then we say that

- $\mathcal{P}$ is **hard for $\mathcal{C}$ under first-order reductions** if every problem in $\mathcal{C}$ has a first-order reduction to $\mathcal{C}$.
- $\mathcal{P}$ is **complete for $\mathcal{C}$ under first-order reductions** if it is hard for $\mathcal{C}$ under first-order reductions and $\mathcal{P} \in \mathcal{C}$.

In this terminology, Proposition 4.2.13 shows that 3-Sat is ESO-hard, which together with Proposition 4.2.6 shows ESO-completeness of 3-Sat.

**Exercises.**

1. Show that 2-colorability of finite graphs is both in ESO and in USO.
2. Show that connectedness of finite graphs is both in ESO and in USO.
3. Show that Hamiltonicity of graphs is in ESO.
4. Show that every sentence in ESO is equivalent to a sentence of the form

$$\exists R \forall x \exists y. \psi$$

where $\psi$ is quantifier-free. Hint: use a linear order and the successor relation with respect to this linear order as in the proof of Proposition 4.2.3.

**4.3. Least Fixed-Point Logic**

In this section we learn about a powerful logic with the nice feature that every property of finite structures that can be expressed in this logic has a good characterisation in the sense of Section 4.2.1, that is, is both in ESO and in USO.
4.3.1. Knaster-Tarski. Given a set $U$. An operator on $U$ is a function from $\mathcal{P}(U) \to \mathcal{P}(U)$. A fixed point of an operator $F$ is a subset $V \subseteq U$ such that $F(V) = V$. A least fixed point of $F$ is a fixed point $X$ of $F$ such that for every other fixed point $Y$ of $F$ we have $X \subseteq Y$. Clearly, if $F$ has a least fixed point, it is unique, and denoted by $\text{LFP}(F)$.

An operator is said to be monotone if $X \subseteq Y$ implies $F(X) \subseteq F(Y)$. Consider the sequence $(X^i)_{i \in \mathbb{N}}$ defined by

$$X^i := \begin{cases} \emptyset & \text{if } i = 0 \\ F(X^{i-1}) & \text{otherwise} \end{cases}$$

Note that if $F$ is monotone then $X^i \subseteq X^{i+1}$ for all $i \in \mathbb{N}$, by induction on $i$.

**Theorem 4.3.1.** Every monotone operator $F : \mathcal{P}(U) \to \mathcal{P}(U)$ has a least fixed point, and

$$\text{LFP}(F) = \bigcap \{Y \mid Y = F(Y)\} = \bigcup_{i \in \mathbb{N}} X^i$$

**Proof.** Consider $S := \{Y \subseteq U \mid F(Y) \subseteq Y\}$. Then $S \neq \emptyset$ since $U \in S$.

**Claim.** $S := \bigcap S$ is a fixed point of $F$. Indeed, for every $Y \in S$ we have $S \subseteq Y$ and hence

$$F(S) \subseteq F(Y) \quad \text{(monotonicity)}$$

$$\subseteq Y \quad \text{(since } Y \in S).$$

Therefore, $F(S) \subseteq \bigcap S = S$. Moreover, $F(F(S)) \subseteq F(S)$ by monotonicity, and thus $F(S) \in S$. Hence, $S = \bigcap S \subseteq F(S)$, which concludes the proof that $S = F(S)$.

Let $S' := \{Y \subseteq U \mid F(Y) = Y\}$ and $S' := \bigcap S'$. Then $S \subseteq S'$ by the above, and hence $S' \subseteq S$. On the other hand, $S' \subseteq S$, so $S = \bigcap S \subseteq S' = S'$. Hence, $S = S'$ is a fixed point of $F$. Since $S'$ is the intersection of all fixed points of $F$, it is also the least fixed point of $F$. Thus,

$$\text{LFP}(F) = S = S' = \bigcap \{Y \mid Y = F(Y)\}.$$
4.3.3. LFP: Syntax and Semantics.

**Definition 4.3.4.** Least fixed point logic (LFP) extends the syntax of first-order logic with the following inductive rule:

- if $R \notin \tau$ is $k$-ary, $\phi(x_1, \ldots, x_k)$ is a $(\tau \cup \{R\})$-formula which is positive in $R \in \tau$, and $t_1, \ldots, t_k$ are $\tau$-terms, then

$$\text{LFP}_\phi^R(t_1, \ldots, t_k)$$

is a $\tau$-formula (whose free variables are those of $t$).

The semantics is defined as follows.

- $(\text{LFP}_\phi^R(t_1, \ldots, t_k))^A := \{ \bar{a} \mid (t_1(\bar{a}), \ldots, t_k(\bar{a})) \in \text{LFP}(F_\phi^R) \}$.

**Example 4.3.5.** The formula $\phi(x, y)$ given by

$$E(x, y) \land \exists z (E(x, z) \land R(z, y))$$

is positive in $R$. Let $A$ be an $\{E\}$-structure. Then $((\text{LFP}_\phi^R)(x_1, x_2))^A$ denotes the transitive closure of $E^A$. Hence, connectivity of graphs can be expressed by the LFP sentence

$$\forall u, v. \text{LFP}_\phi^R(u, v).$$

4.3.4. Example. Consider the following game played on a graph $G$ with a distinguished start note $a$ and a pebble which is initially placed on $a$. There are two players, $A$ and $B$, that play in turns, starting with player $A$. When the pebble is placed on a vertex $v$, then the players have to move the pebble along and edge $(v, w)$ to $w$. The player who cannot move any more (since there is no outgoing edge in the pebbled vertex) looses and the other wins. Of course, there are situations where no player can win and the game goes on forever.

Can we write down a first-order sentence $\phi$ such that a structure $(G, a)$ satisfies $\phi$ if and only if $B$ wins the game on $(G, a)$? Certainly not, but the proof has to wait until Section 4.4. Can we write down an LFP sentence? Yes, we can! Let $a$ be the $\{E, S\}$-formula

$$\forall y (E(x, y) \Rightarrow (E(y, z) \land S(z))).$$

Note that $F_{\alpha}^S(\emptyset)$ is the set of vertices with no outgoing edges; in all these vertices, player $A$ looses and player $B$ wins. In general, $F_{\alpha}^S(X)$ is the set of nodes $b$ such that no matter where player $A$ moves, player $B$ has no valid response from $X$. Hence, $(F_{\alpha}^S)^i(\emptyset)$ is the set of vertices where player $B$ can win with at most $i - 1$ rounds, and the sentence $\text{LFP}_{\alpha}^S(a)$ holds on $(G, a)$ iff player $B$ has a winning strategy.

4.3.5. LFP and ESO.

**Theorem 4.3.6.** Let $\Phi$ be an LFP sentence. Then there exist USO and ESO sentences that are equivalent to $\Phi$.

**Proof.** To obtain an ESO sentence, we quantify over a linear order $L$ and the corresponding successor relation $S$. For each subformula of the form $\text{LFP}_\phi^R(t_1, \ldots, t_k)$ we introduce a new $k$-ary existentially quantified predicate $S$, replace the formula by $S(t_1, \ldots, t_k)$, and add additional conjuncts to make sure that $S$ denotes precisely $\text{LFP}_\phi^R(t_1, \ldots, t_k)$. Here we use that $\text{LFP}(F_\phi^R)$ can be described inductively, starting from $\emptyset$, as in Theorem 4.3.1. Note that on a structure $A$, this induction reaches the fixed point in at most $|A|^k$ many steps. Suppose that $A = \{0, \ldots, |A|\}$ and that $L$ is the natural ordering of $A$. So we can identify the steps of the induction by $k$-tuples of Elements of $A$. Also note that there exists a first-order formula $\chi(y_1, \ldots, y_k, y_1', \ldots, y_k')$ that states that $y_1', \ldots, y_k'$ codes the successor step of $y_1, \ldots, y_k$.
4.4. Non-Definability and Games  

To simulate the induction, we existentially quantify over another relation $I$ of arity $2k$. The idea is that 

$$\{ (x_1, \ldots, x_k) \mid \{ x_1, \ldots, x_k, y_1, \ldots, y_k \} \in I \} = (F^R_{s_1})^i(\emptyset)$$

where $i$ is the state of the induction coded by $y_1, \ldots, y_k$. We now add the additional conjuncts:

- $\forall x_1, \ldots, x_k \neg I(x_1, \ldots, x_n, 0, \ldots, 0)$.
- the formula $\forall x_1, \ldots, x_k \forall y_1, \ldots, y_k, y'_1, \ldots, y'_k \ \chi(y_1, \ldots, y_k, y'_1, \ldots, y'_k) \Rightarrow$

$$I(s_1, \ldots, s_k, y'_1, \ldots, y'_k) \Leftrightarrow \phi'(s_1, \ldots, s_k, y_1, \ldots, y_k))$$

where $\phi'$ is the formula obtained from $\phi$ by replacing $R(s_1, \ldots, s_k)$ with $I(s_1, \ldots, s_k, y_1, \ldots, y_k)$.

Note that the syntax of LFP is closed under negation; so in order to obtain a USO sentence that is equivalent to $\phi$, we first build the ESO sentence $\psi$ equivalent to $\neg \phi$ as above; then $\neg \psi$ is the USO sentence that we were looking for. \hfill \square

Exercises.

(30) Show that connectedness of finite graphs is both in ESO and in USO.

4.4. Non-Definability and Games

4.4.1. Ehrenfeucht-Fraïssé Games. Das $q$-Runden Ehrenfeuchtspiel auf den relationalen $\tau$-Strukturen $A, B$:

- Es gibt zwei Spieler, Samson und Delila.
- In der $i$-ten Runde wählt Samson eine der Strukturen $A, B$ und ein Element $u_i$ dieser Struktur.
- Delilah antwortet mit einem Element $v_i$ der anderen Struktur.
- Falls nach $q$ Runden die Abbildung

$$f(x) = \begin{cases} v_i \text{ falls } x = u_i \in A \\ u_i \text{ falls } x = v_i \in A \end{cases}$$

ein Isomorphismus von endlicher Substruktur von $A$ auf endliche Substruktur von $B$ ist, so gewinnt Delila, sonst Samson.

Schreiben $A \simq B$ falls Delila eine Gewinnstrategie für das $q$-Runden Ehrenfeuchtspiel auf $A$ und $B$ hat (eine Äquivalenzrelation).

4.4.2. Quantorenrang. Der Quantorenrang $qr(\phi)$ einer $\tau$-Formel $\phi$ wird induktiv definiert:

- $qr(\phi) := 0$ für $\phi$ atomar;
- falls $\phi = \neg \psi$ so ist $qr(\phi) := qr(\psi)$;
- falls $\phi = \psi_1 \land \psi_2$ so ist $qr(\phi) := \max(qr(\psi_1), qr(\psi_2))$;
- falls $\phi = \exists x. \psi$ so ist $qr(\phi) := qr(\psi) + 1$.

Für endliche relationale Signatur $\tau$ gibt es für jedes $q \in \mathbb{N}$ nur endlich viele nicht äquivalente erststufige Sätze mit $qr(\phi) \leq q$.

Für zwei $\tau$-Strukturen $A, B$ definieren $A \equivq B$ falls für jeden Satz $\phi$ mit $qr(\phi) \leq k$ gilt:

$$A \models \phi \text{ gdw. } B \models \phi$$

Eine Äquivalenzrelation.
4.4.3. Der Satz von Ehrenfeucht-Fraïssé.

Theorem 4.4.1 (Fraïssé'54, Ehrenfeucht'61). \[A \sim_q A \text{ genau dann, wenn } A \equiv_q B.\]

Proof. \[A \sim_q A \Rightarrow A \equiv_q B.\]
Sei \(\phi\) mit \(qr(\phi) \leq q\) s.d. \(A|\phi\) und \(B \not\models \phi.\)

Z.b.: Samson hat Gewinnstrategie mit \(q\) Runden.
Beweis per Induktion nach \(q\) für den allgemeineren Fall, dass \(\phi(x_1, \ldots, x_m)\) freie Variablen hat, und es Konstanten \(\bar{a} \in A^m\) und \(\bar{b} \in B^m\) gibt mit
\[A|\phi(\bar{a})\text{ und } B \not\models \phi(\bar{b}).\]
und \(a_1, \ldots, a_m\) und \(b_1, \ldots, b_m\) im Spiel bereits ausgewählt.

Annahme: \(\phi\) ist in Negationsnormalform, d.h., alle Negationen in \(\phi\) sind vor atomaren Formeln.

Falls \(q = 0\) ist \(\phi\) quantorenfrei. Also gibt es atomare Formel \(\phi\) die \(\bar{a}\) von \(\bar{b}\) unterscheidet, und \(\bar{a} \mapsto \bar{b}\) ist kein Isomorphismus.

Wenn \(q = p + 1\), dann hat \(\phi\) eine Subformel \(\theta\) der Gestalt \(\exists x. \psi\) oder \(\forall x. \psi\) mit \(qr(\psi) \leq p\) und \(A|\theta(\bar{a})\) und \(B \not\models \theta(\bar{b}).\)

- Falls \(\theta = \exists x. \psi\) dann wählt Samson einen Zeugen für \(x\) in \(A\).
- Falls \(\theta = (\forall x. \neg \psi)(\bar{a})\), dann gilt \(B|((\forall x. \neg \psi)(\bar{b}),\)
und Samson wählt einen Zeugen für \(x\) in \(B\).

Rückrichtung: gilt ebenfalls, wird aber im folgenden nicht benötigt. \(\square\)

4.4.4. Ehrenfeucht-Fraïssé anwenden. \(S\): Klasse von \(\tau\)-Strukturen. \(S\) ist nicht in FOL ausdrückbar falls es für jedes \(q \in \mathbb{N}\) ein Paar von Strukturen \(A_q\) und \(B_q\) gibt so dass

- \(A_q \in S\) und \(B_q \notin S\), und
- Delila gewinnt das \(q\)-Runden E.F.-Spiel auf \(A_q\) und \(B_q\).

Denn: Angenommen es gibt \(\phi\) so, dass \(A \in S\) gw \(A|\phi.\)
Dann: \(A|q B_q\) für \(q := qr(\phi)\) und \(A_q \equiv_q B_q\) nach dem Satz von E.-F. Widerspruch zu \(A_q \in S\) und \(B_q \notin S\).
Sei \(A\) eine \(\emptyset\)-Struktur mit \(|A| = q\) und \(B\) eine \(\emptyset\)-Struktur mit \(|B| = q + 1\).

Einfach: \(A \sim_q B.\)
Also: Parität ist nicht in FOL ausdrückbar.

4.4.5. Parity. Sei \(L_n := ([1, \ldots, n], \leq).\) Dann gilt:
\[L_0 \neq_3 L_7 \quad L_0 \neq_3 L_7\]
\[L_7 \equiv_3 L_8 \quad L_7 \equiv_3 L_8\]

Allgemein: für \(m, n \geq 2^p - 1\)
\[L_m \equiv_p L_n\]

Delila’s Strategie: nach \(r\) Runden soll für alle \(1 \leq i < j \leq r\) gelten
- entweder \(a_i - a_j = b_i - b_j.\)
- oder \(a_i - a_j \geq 2^{p-r} - 1\) und \(b_i - b_j \geq 2^{p-r} - 1.\)

Beobachtung: die zwei Eigenschaften garantieren partiellen Isomorphismus.
Konsequenz: Parität bereits für lineare Ordnungen nicht in FOL ausdrückbar.


Proposition 4.4.2. Es gibt keinen erststufigen Satz \(\phi,\) der von einem endlichen Graphen \(G\) genau dann erfüllt wird, wenn \(G\) zusammenhängend ist.

Angenommen \(\phi\) ist so ein \(\{E\}\)-Satz. Sei \(\theta(u, v)\) eine \(\{\leq\}\)-Formel, die Nachfolgerrelation bzgl. \(\leq\) definiert. Sei \(\gamma(x, y)\) die Disjunktion
4.4. Connectivity of finite graphs. In the beginning of this chapter, we have used the compactness theorem to show that graph connectivity is not expressible by a first-order sentence. The same argument fails if we want to show that connectivity of finite graphs is not expressible by a first-order sentence. However, this can be shown using the fact that there is no first-order sentence expressing even parity of linear orders which we established earlier.

**Proposition 4.4.3.** There is no first-order sentence $\phi$ that holds on a finite graph $G$ if and only if the $G$ is connected.

**Proof.** Assume for contradiction that $\phi$ is an $\{E\}$-sentence expressing connectivity of finite graphs. Let $\theta(u,v)$ be the $\{\leq\}$-formula that defines the successor relation with respect to a linear order $\leq$. Let $\gamma(x,y)$ be the disjunction of the following first-order formulas:

- $\exists z (\theta(x,z) \land \theta(z,y))$, oder
- $\exists z (\theta(x,z) \land \forall u (u \leq z)) \land \forall u (y \leq u) \ (x$ ist vorletztes und $y$ erstes Element),
- $x$ ist letztes und $y$ ist zweites Element).

Let $G := ([1, \ldots, n]; \{(a, b) \mid (1, \ldots, n); \leq \models \gamma(a, b)\})$. Bild!

$G$ ist zusammenhängend gdw $n$ ist ungerade.

Ersetze $E$ in $\phi$ durch $\gamma$, und erhalten einen Satz, der genau dann auf endlicher linearer Ordnung gilt, wenn diese ungerade viele Elemente hat.

4.4.8. Games for Second-Order Logics. The SO Game between Spoiler and Duplicator on the $\tau$-structures $A$ and $B$ is similar to the Ehrenfeucht-Fraïssé game; here, the rounds are of either of the following two forms:

- **Point move:** as in the Ehrenfeucht-Fraïssé game, Spoiler chooses an element of either $A$ or $B$ and Duplicator responds with an element in the other structure.
- **Set move:** Spoiler chooses a subset of $A^k$ or of $B^k$, for some $k \in \mathbb{N}$. Duplicator responds with a subset of $B^k$ or $A^k$, respectively.

If $a_1, \ldots, a_p$ are the chosen elements in $A$ and $b_1, \ldots, b_p$ the corresponding elements of $B$ (such that $a_i$ and $b_i$ have been selected in the same round), and if $U_1, \ldots, U_r$ are the chosen relations over $A$ and $V_1, \ldots, V_r$ the correspondingly chosen relations over $B$, then Duplicator wins if $\bar{a} \mapsto \bar{b}$ is a partial Isomorphism between $(A, U_1, \ldots, U_r)$ and $(B, V_1, \ldots, V_r)$.

Similarly as with the Ehrenfeucht-Fraïssé game, if for every $p$ and $r$ we find structures $A$ and $B$ such that $A \in C$ and $B \notin C$, but Duplicator has a winning strategy for the SO game with $p$ point moves and $r$ set moves, then $C$ is not expressible in SO. This game can be adapted to ESO as follows. Samson must choose his relations over $A$, so Duplicator always plays relations in $B$. Then the game precisely characterises the expressive power of ESO. Analogously, we have a game for USO.
However, it is very difficult to come up with instances $A \in S$ and $B \notin S$ and winning strategies for duplicator and Question 4.1 remains wide open (already when Spoiler is only allowed to play a single binary relation).

**Exercises.**

(31) Show that acyclicity of finite undirected graphs is not first-order definable.

(32) Show that for every first-order formula $\phi$ the set

$$\{|A| \mid A \models \phi\}$$

is either finite or co-finite.

(33) Let $A$ be the $\{E\}$-structure with domain $A = \{0, 1\}$ and $E^A = \{(0, 1), (1, 0)\}$. Let $P$ be the class of finite $\{E\}$-structures that homomorphically map to $A$, and let $P_{}\text{fin}$ be the class of all finite $\tau$-structures in $P$. Fill the following table.

<table>
<thead>
<tr>
<th>in FO</th>
<th>$P$</th>
<th>$P_{}\text{fin}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>in ESO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in USO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>in LFP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(34) Sei nun $A$ die $\{E\}$-Struktur mit Grundmenge $A = \{0, 1\}$ und $E^A = \{0, 1\}$. Wieder betrachten wir die Menge aller $\{E\}$-Strukturen, die sich nach $A$ abbilden lassen. Wieder: Tabelle füllen.

(35) Do the same for the following structure. Here the signature $\tau = \{I, R_0, R_1\}$ contains a ternary relation symbol $I$ and unary relation symbols $R_0$ und $R_1$. Let $A$ be the $\tau$-structure with base set $A = \{0, 1\}$ and relations $I^A = A^3 \setminus \{(1, 1, 0)\}$, $R_0^A = \{0\}$, and $R_1^A = \{1\}$. 
APPENDIX A

Set Theory

In this appendix chapter we freely follow Appendix A of the book of Tent and Ziegler [7]. See [5] for a more detailed introduction to set theory.

A.1. Sets and Classes

We often speak of the class of all $\tau$-structures or the class of all ordinals, since we know that these things cannot be sets (as we will see in the next section, if the class of all ordinals were a set, we could derive a contradiction). Using first-order logic, we therefore want to give an axiomatic treatment of set theory that allows for the distinction between sets and (proper) classes. For this, we may work in Bernays-Gödel set theory (BG) which is formulated in a two-sorted language. One type of objects are sets and the other type of objects are classes; sets can be elements of sets, and sets can be elements of classes, but classes can’t be elements of sets or classes.

Here are the axioms of BG:

1. (a) Extensionality. Sets containing the same elements are equal:

   $$\forall x, y \in \text{Sets} \quad (\forall z (z \in x \iff z \in y) \Rightarrow x = y)$$

   (b) Empty set. There exists an empty set (denoted by $\emptyset$):

   $$\exists x \in \text{Sets} \quad \forall y \quad (\neg y \in x)$$

   (c) Pairing. For all sets $a$ and $b$ there is a set (denoted by $\{a, b\}$) which has exactly the elements $a$ and $b$:

   $$\forall a, b \in \text{Sets} \quad \exists c \in \text{Sets} \quad \forall x \quad (x \in c \iff x = a \lor x = b)$$

   (d) Union. For every set $a$ there is a set (denoted by $\bigcup a$) that contains precisely the elements of the elements of $a$:

   $$\forall a \in \text{Sets} \quad \exists b \in \text{Sets} \quad \forall x \quad (x \in b \iff \exists y \in a. x \in y)$$

   (e) Power set. For every set $a$ there is a set (denoted by $\mathcal{P}(a)$) that consists of all subsets of $a$:

   $$\forall a \in \text{Sets} \quad \exists b \in \text{Sets} \quad \forall x \quad (x \in b \iff x \subseteq a)$$

   (f) Infinity. There is an infinite set. One way to express this is to assert the existence of a set which contains the empty set and is closed under the successor operation $x \mapsto x \cup \{x\}$:

   $$\exists a \in \text{Sets} \quad (\emptyset \in a \land \forall x (x \in a \Rightarrow x \cup \{x\} \in a)$$

2. (a) Class extensionality: Classes containing the same elements are equal.

   (b) Comprehension: If $\phi(x, y_1, \ldots, y_m, z_1, \ldots, z_n)$ is a first-order formula in which only set-variables are quantified, and if $b_1, \ldots, b_m$ are sets, and $c_1, \ldots, c_n$ are classes, then there exists a class, denoted by

   $$\{x \in \text{Sets} \mid \phi(x, b_1, \ldots, b_m, c_1, \ldots, c_n)\}$$

57
containing precisely those sets $x$ that satisfy $\phi(x, b_1, \ldots, b_m, c_1, \ldots, c_n)$. This is in fact an infinite family of axioms (for every first-order formula $\phi$ we have one axiom).

(c) Replacement: If a class $c$ is a function, i.e., if for every set $a$ there is a unique set $b := c(a)$ such that $(a, b) := \{\{a\}, \{a, b\}\}$ belongs to $c$, then for every set $d$ the image $\{c(z) \mid z \in d\}$ is a set.

(3) Regularity (or Axiom of Foundation):

$$\forall x \in \text{Sets} \ (x \neq \emptyset \Rightarrow \exists y \in x (y \cap x = \emptyset))$$

Consequently: no set can be an element of itself. Moreover, there is no infinite sequence $(a_n)$ such that $a_{i+1}$ is an element of $a_i$ for all $i$. Most parts of mathematics can be practised without this axiom, but assuming this axiom simplifies some proofs of fundamental properties of ordinals.

(4) For BGC we add Global Choice: There is a function $c$ such that $c(a) \in a$ for every nonempty set $a$.

We mention that BG is a conservative extension of ZF: any set-theoretical statement provable in BG (BGC) is also provable in ZF (ZFC). (The substructure of a model of BG induced by sets is a model of ZF. Conversely, a model $M$ of ZF becomes a model of BG by taking the first-order definable subsets of $M$ as classes.)

### A.2. Ordinals

A well-ordering of a set $A$ is a linear order $<$ on $A$ such that any non-empty subset of $A$ contains a smallest element with respect to $<$. The usual ordering of the set $\mathbb{N}$ is an example of a well-ordering, and the usual ordering of $\mathbb{Z}$ and the positive rational numbers are non-examples. For $a \in A$, the predecessors of $a$ are the elements $b \in A$ with $b < a$.

**Definition A.2.1.** An ordinal is a well-ordered set in which every element equals its set of predecessors.

The well-ordering of an ordinal $\alpha$ is given by the relation $\in$: if $\beta, \gamma \in \alpha$, then

$$\beta < \alpha \iff \beta \text{ is a predecessor of } \alpha$$

$$\iff \beta \in \alpha$$

Hence, an ordinal is uniquely given by the set of its elements. Suppose that $\alpha$ is an ordinal, and $\gamma \in \beta \in \alpha$. Then $\gamma$ is a predecessor of $\beta$, and hence must be in $\alpha$. That is, ordinals $\alpha$ are transitive: if $\beta \in \alpha$ then $\beta \subseteq \alpha$.

An element $\beta$ of an ordinal $\alpha$ is again an ordinal number: Since $\beta \subseteq \alpha$, we obtain a well-ordering of $\beta$ by restricting the well-ordering of $\alpha$ to $\beta$. Moreover, if $\gamma, \gamma' \in \beta$, then $\gamma < \gamma'$ if $\gamma \in \gamma'$ so $\beta$ is indeed an ordinal.

**Proposition A.2.2.** Every structure $(A; <)$ where $A$ is well-ordered by $<$ is isomorphic to $(\alpha; \in)$ where $\alpha$ is an ordinal.

**Proof.** Define $f: A \to \alpha$ inductively by $f(y) := \{f(z) \mid z < y\}$. The image of $f$ is an ordinal $\alpha$ such that $(\alpha; \in)$ is isomorphic to $(A; <)$ via $f$. (Note that $f$ is the only isomorphism between $(A; <)$ and $(\alpha; \in)$.) \(\square\)

We denote the class of all ordinals by $\text{On}$.

**Proposition A.2.3.** $\text{On}$ is a proper class, i.e., a class which is not a set, and it is well-ordered by $\in$. 

A.3. CARDINALS

Proof. Let \( \alpha \) and \( \beta \) be different ordinals. We have to show that either \( \alpha \in \beta \)
or \( \beta \in \alpha \). If not, then \( x = \alpha \cap \beta \) would be a proper initial segment of \( \alpha \) and \( \beta \), and therefore itself an element of \( \alpha \) and \( \beta \), so \( x \in x \), a contradiction.

The class of all ordinals is not a set (the Burali-Forti Paradox): if it were a set, then it were an ordinal itself, and thus a member of itself, contradicting the Axiom of Foundation. \( \square \)

So every ordinal \( \alpha \) is a set having as elements precisely the smaller ordinals:

\[
\alpha = \{ \beta \in \text{On} \mid \beta < \alpha \}.
\]

In the following, for ordinals \( \alpha, \beta \) we write \( \alpha < \beta \) rather than \( \alpha \in \beta \).

For any ordinal \( \alpha \) its successor is defined as \( \alpha + 1 := \alpha \cup \{ \alpha \} \): it is the smallest ordinal greater than \( \alpha \). Starting from the smallest ordinal \( 0 = \emptyset \), its successor is \( 1 = \{0\} \), then \( 2 = \{0, 1\} \), and so on, yielding the natural numbers \( \mathbb{N} \). When we view \( \mathbb{N} \) as an ordinal, we denote it by \( \omega \). The next ordinal is \( \omega + 1 = \{0, 1, \ldots, \omega\} \), etc. By definition, a successor ordinal \( \beta \) contains a maximal element \( \alpha \) (so \( \beta = \alpha + 1 \)). Ordinals greater than \( 0 \) which are not successor ordinals are called limit ordinals. Any ordinal can be written uniquely as

\[
\lambda^{+1+\cdots+1}_{\text{n times}}
\]

where \( \lambda \) is a limit ordinal.

**Theorem A.2.4 (Well-ordering theorem).** Every set has a well-ordering.

Proof. Let \( A \) be a set. Fix a set \( B \) which does not belong to \( A \) and define a function \( f \) from the class of all ordinals to \( A \cup \{ B \} \) as follows:

- if \( A \setminus \{ \beta \mid \beta < \alpha \} \neq \emptyset \) then set \( f(\alpha) \) to be an element from this set (here we use the Axiom of Choice).
- Otherwise, \( f(\alpha) := B \).

Then \( \gamma := \{ \alpha \mid f(\alpha) \neq B \} \) is an ordinal and \( f \) defines a bijection between \( \gamma \) and \( A \). \( \square \)

In fact, the well-ordering theorem is equivalent to the Axiom of Choice. Note that the ordinal \( \gamma \) in the construction of the well-ordering of \( A \) is not unique, unless \( A \) is finite.

A.3. Cardinals

Two sets \( A \) and \( B \) have the same cardinality \( (|A| = |B|) \) if there exists a bijection between them. By the well-ordering theorem, every set has the same cardinality as some ordinal. We call the smallest such ordinal the cardinality \( |A| \) of \( A \). Ordinals occurring in this way are called cardinals. An ordinal \( \alpha \) is a cardinal if and only if all smaller ordinals do not have the same cardinality.

Notes.

- All natural numbers and \( \omega \) are cardinals.
- \( \omega + 1 \) is the smallest ordinal that is not a cardinal.
- The cardinality of a finite set is a natural number.
- A set of cardinality \( \omega \) is called countably infinite.
Sums, products, and powers of cardinals are defined as the cardinality of disjoint unions, Cartesian powers, and sets of functions:

\[ |x| + |y| := |x \uplus y| \quad \text{where } x \cap y = \emptyset \]
\[ |x| \cdot |y| := |x \times y| \]
\[ |x|^{|y|} := |x^y| \]

and likewise for infinite sums and products:

\[ \sum_{x \in I} |x| := | \bigcup_{x \in I} x | \]
\[ \prod_{x \in I} |x| := | \prod_{x \in I} x |. \]

Note that

\[ (\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}. \]

Cantor’s well-known diagonalization argument shows that

\[ 2^\kappa > \kappa. \]

In particular, there is no largest cardinal. Cantor’s result also follows from König’s theorem below for \( \kappa_i := 1 \) and \( \lambda_i := 2 \) for all \( i \in I := \omega \).

**Theorem A.3.1 (König’s theorem).** Let \((\kappa_i)_{i \in I}\) and \((\lambda_i)_{i \in I}\) be sequences of cardinals. If \( \kappa_i < \lambda_i \) for all \( i \in I \), then

\[ \sum_{i \in I} \kappa_i < \prod_{i \in I} \lambda_i. \]

**Proof.** We first show that \( \sum_{i \in I} \kappa_i \leq \prod_{i \in I} \lambda_i \). Choose pairwise disjoint sets \((A_i)_{i \in I}\) and \((B_i)_{i \in I}\) such that \( |A_i| = \kappa_i \), \( |B_i| = \lambda_i \), and \( A_i \subset B_i \) for all \( i \in I \). We will construct an injection \( f: \bigcup_{i \in I} A_i \rightarrow \prod_{i \in I} B_i \). Choose \( d_i \in B_i \setminus A_i \) for each \( i \in I \) (here we use the Axiom of Choice). For \( x \in A := \bigcup_{i \in I} A_i \), define

\[ f(x) := (a_i)_{i \in I} \text{ where } a_i := \begin{cases} x & \text{if } x \in A_i \\ d_i & \text{otherwise}. \end{cases} \]

To show the injectivity of \( f \), let \( x, y \in A \) be distinct. Let \( i \in I \) be such that \( x \in A_i \). If \( y \notin A_i \) then \( f(x)_i = x \neq y = f(y)_i \). If \( y \notin A_i \) then \( f(x)_i = x \neq d_i = f(y)_i \) since \( x \in A_i \) but \( d_i \in B_i \setminus A_i \). So in both cases, \( f(x) \neq f(y) \).

Suppose for contradiction that \( \sum_{i \in I} \kappa_i = \prod_{i \in I} \lambda_i \). Then we can find sets \((X_i)_{i \in I}\) with \(|X_i| = \kappa_i\) such that

\[ B := \prod_{i \in I} B_i = \bigcup_{i \in I} X_i. \]

For each \( i \in I \), define

\[ Y_i := \{a_i \mid a \in X_i\}. \]

For every \( i \in I \) there exists \( b_i \in B_i \setminus Y_i \) because \(|Y_i| \leq |X_i| = \kappa_i < \lambda_i = |B_i|\). Now define

\[ b := (b_i)_{i \in I} \in \prod_{i \in I} B_i. \]

Let \( j \in I \). Then \( b_j \notin Y_j \) by the choice of \( b_j \), and hence \( b \notin X_j \) by the definition of \( Y_j \). This shows that \( b \notin \bigcup_{i \in I} X_i \), a contradiction. \( \square \)
We write $\kappa^+$ for the smallest cardinal greater than $\kappa$, the *successor cardinal* of $\kappa$. Positive cardinals which are not successor cardinals are called *limit cardinals*. There is an isomorphism between the class of ordinals and the class of all infinite cardinals, which is denoted by

$$\alpha \mapsto \aleph_\alpha$$

and can be defined inductively by

$$\aleph_0 := \omega$$

$$\aleph_{\alpha + 1} := \aleph_\alpha^+$$

$$\aleph_{\beta} := \bigcup_{\alpha < \beta} \aleph_\alpha$$

if $\alpha$ is a limit ordinal.

Note that if $(\kappa_i)_{i \in I}$ is a family of cardinals, then $\kappa := \bigcup_{i \in I} \kappa_i$ is again a cardinal:

- if there is an $i \in I$ such that $\kappa_j \leq \kappa_i$ for all $j \in I$, then $\bigcup_{i \in I} \kappa_i = \kappa_i$ and the statement is true;
- otherwise, for every $i \in I$ there is a $j \in I$ with $\kappa_i < \kappa_j$. For each ordinal $\alpha$ with $\alpha < \kappa$ we have that $\alpha \in \kappa$ and hence $\alpha \in \kappa_i$ for some $i \in I$. By the above, there is a $j \in I$ such that $|\alpha| \leq \kappa_i < \kappa_j \leq |\kappa|$. Thus, every ordinal smaller than $\kappa$ has smaller cardinality than $\kappa$, and $\kappa$ is a cardinal.

**Theorem A.3.2.** Let $\kappa$ be an infinite cardinal. Then

1. $\kappa \cdot \kappa = \kappa$.
2. $\kappa + \lambda = \max(\kappa, \lambda)$.
3. $\kappa^\kappa = 2^\kappa$.

**Proof.** For ordinals $\alpha, \beta, \alpha', \beta'$, define $(\alpha, \beta) < (\alpha', \beta')$ iff

$$(\max(\alpha, \beta), \alpha, \beta) <_{\text{lex}} (\max(\alpha', \beta'), \alpha', \beta')$$

where $\text{lex}$ is the lexicographical ordering on triples of ordinals. Since this is a well-ordering, there is a unique order-preserving bijection $f$ between pairs of ordinals and ordinals by Proposition A.2.2.

**Claim.** If $\kappa$ is an infinite cardinal, then $f$ maps $\kappa \times \kappa$ to $\kappa$, and hence $\kappa \cdot \kappa = \kappa$.

The proof of the claim is by induction on $\kappa$. For $\alpha, \beta \in \kappa$ let $P_{\alpha, \beta}$ be the set of predecessors of $(\alpha, \beta)$. Note that:

- $P_{\alpha, \beta}$ is contained in $\delta \times \delta$ with $\delta = \max(\alpha, \beta) + 1$.
- Since $\kappa$ is infinite and $\alpha, \beta < \kappa$, the cardinality of $\delta$ is smaller than $\kappa$.
- By inductive assumption $|P_{\alpha, \beta}| \leq |\delta \times \delta| = |\delta| \cdot |\delta| \leq |\delta| < \kappa$.

Hence, $f(\alpha, \beta) < \kappa$ since $f$ is an order isomorphism and thus $f(\alpha, \beta) \in \kappa$.

Now (2) and (3) are simple consequences. Let $\mu := \max(\kappa, \lambda)$.

$$\mu \leq \kappa + \lambda \leq \mu + \mu \leq 2 \cdot \mu \leq \mu \cdot \mu = \mu$$

$$2^\kappa \leq \kappa^\kappa \leq (2^\kappa)^\kappa = 2^{\kappa \cdot \kappa} = 2^\kappa$$

The *Continuum Hypothesis (CH)* states that $\aleph_1 = 2^{\aleph_0}$, that is: there is no cardinal lying strictly between $\omega$ and the cardinality $|\mathbb{R}|$ of the continuum. The *Generalised Continuum Hypothesis (GCH)* states that $\kappa^+ = 2^\kappa$ for all infinite cardinals $\kappa$. As with CH, the GCH is known to be independent of ZFC, that is, there are models of ZFC where GCH is true, and models of ZFC where GCH is false (assuming that ZFC is consistent; see [5]).

Let $A$ be a set that is linearly ordered by $\prec$. A subset $B \subseteq A$ is called *cofinal* if for every $a \in A$ there is some $b \in B$ with $a \leq b$. Any linear order contains a well-ordered cofinal subset.
DEFINITION A.3.3. The cofinality \( \text{cf}(A) \) of \( A \) is the smallest ordinal that is order-isomorphic to a well-ordered cofinal subset of \( A \).

Examples:
- If \( A \) has a greatest element, then the cofinality is one since the set consisting only of the greatest element is cofinal and must be contained in any other cofinal subset of \( A \).
- A subset \( S \) of \( \mathbb{N} \) is cofinal if and only if \( S \) is infinite, and thus \( \text{cf}(\omega) = \omega \).
- \( \text{cf}(2^\omega) > \omega \); see Exercise 37.

LEMMA A.3.4. For linearly ordered \( A \) we have \( \text{cf}(\text{cf}(A)) = \text{cf}(A) \).

PROOF. If \( \{a_\alpha \mid \alpha < \beta\} \) is cofinal in \( A \) and \( \{\alpha(\nu) \mid \nu < \mu\} \) is cofinal in \( \beta \), then \( \{a_{\alpha(\nu)} \mid \nu < \mu\} \) is cofinal in \( A \). \( \square \)

LEMMA A.3.5. For linearly ordered \( A \) we have that \( \text{cf}(A) \) is a cardinal.

PROOF. Suppose for contradiction that \( \text{cf}(A) \) is not a cardinal. Choose a surjective map \( f \) from \( |\text{cf}(A)| \) to \( \text{cf}(A) \). This maps provides a cofinal sequence in \( \text{cf}(A) \) of length \( |\text{cf}(A)| \), and therefore \( \text{cf}(\text{cf}(A)) \leq |\text{cf}(A)| < \text{cf}(A) \). This is in contradiction to \( \text{cf}(\text{cf}(X)) = \text{cf}(X) \) from Lemma A.3.4. \( \square \)

A cardinal \( \kappa \) is regular if \( \text{cf}(\kappa) = \kappa \), and singular otherwise. As we have seen above, \( \aleph_0 \) is an example of a regular cardinal. Lemma A.3.5 and Lemma A.3.4 show that \( \text{cf}(A) \) is a regular cardinal. Assuming the axiom of choice, we also have the following.

PROPOSITION A.3.6. Successor cardinals \( \aleph_{\alpha+1} \) are regular.

PROOF. Suppose for contradiction that \( \text{cf}(\aleph_{\alpha+1}) \leq \aleph_\alpha \). Then \( \aleph_{\alpha+1} \) would be the union of at most \( \aleph_\alpha \) sets of cardinality at most \( \aleph_\alpha \), contradicting item (1) in Theorem A.3.2. \( \square \)

Exercises.

(36) Show that \( \aleph_\omega \) is singular.
(37) Show that \( \text{cf}(2^\omega) > \omega \).

Hint: write \( 2^\omega \) as \( \sum_{\nu<\mu} \kappa_\nu \) for \( \mu := \text{cf}(2^\omega) \), and apply König’s theorem (Theorem A.3.1) with \( (\kappa_\nu)_{\nu<\mu} \) and \( (\lambda_\nu)_{\nu<\mu} \) where \( \lambda_\nu := 2^\omega \) for all \( \nu < \mu \).
Solutions to Exercises

The solutions to exercises that will be used in the further course of the lecture are marked with an asterix (∗).

B.1. Exercise 7 (∗)

We restate Exercise 7 from Section 1.4. Show that the compactness theorem is equivalent to the following statement. If a first-order theory $T$ has the same models as a single first-order sentence $\phi$, there is already a finite subset of $T$ which have the same models as $\phi$.

We will show something more general: suppose that $S$ and $T$ are first-order theories and $\phi$ is a first-order sentence such that $S \cup \{\phi\}$ has the same models as $S \cup T$. Then there is a finite subset $T'$ of $T$ such that $S \cup \{\phi\}$ and $S \cup T'$ have the same models. By setting $S := \emptyset$ this is more general than the interesting direction of the exercise.

Proof. If $S \cup \{\phi\}$ has the same models as $S \cup T$, then $S \cup T \cup \{\neg\phi\}$ is unsatisfiable. The compactness theorem provides a finite unsatisfiable subset $F$ of $S \cup T \cup \{\neg\phi\}$. If $F \subseteq S \cup T$ then the statement is trivial, so $F$ is of the form $F' \cup \{\neg\phi\}$.

Claim: $S \cup F'$ has the same models as $S \cup \phi$. Let $M$ be any model of $S$.

- If $M \models \phi$, then $M \models T$ and $M \models F'$ since $F' \subseteq T$.
- If $M \not\models \phi$, then $M \models \neg\phi$. If $M \models F'$, then $F' \cup \{\neg\phi\}$ would be satisfiable, a contradiction. Hence, $M \not\models F'$.

□

B.2. Exercise 17

We have to show that $(\mathbb{Q}; <)$ is an elementary substructure of $(\mathbb{R}; <)$. In other words, the identity map from $\mathbb{Q}$ to $\mathbb{R}$ preserves every first-order formulas $\phi(x_1, \ldots, x_n)$. Let $a_1, \ldots, a_n \in \mathbb{Q}$ be such that $(\mathbb{Q}; <) \models \phi(a_1, \ldots, a_n)$. We have to show that $(\mathbb{R}; <) \models \phi(a_1, \ldots, a_n)$. It suffices to show that

$$Th(\mathbb{Q}; \leq, a_1, \ldots, a_n) \subseteq Th(\mathbb{R}; \leq, a_1, \ldots, a_n).$$

Note that $(a_i \leq a_j) \in Th(\mathbb{Q}; \leq, a_1, \ldots, a_n)$ if and only if $a_i \leq a_j$.

Let $T$ be the theory in the signature $\{\leq, a_1, \ldots, a_n\}$ which says that $\leq$ is a dense unbounded non-strict linear order, together with $\bigwedge_{i,j \leq n, a_i \leq a_j} a_i \leq a_j$. Note that $(\mathbb{R}; \leq, a_1, \ldots, a_n) \models T$. Any countable model of $T$ is isomorphic to $(\mathbb{Q}; <, a_1, \ldots, a_n)$. This can be shown by an easy back-and-forth argument which starts from the partial map that is defined on the constants, and preserves the constants. So let $\phi \in Th(\mathbb{Q}; \leq, a_1, \ldots, a_n)$. Then $T \models \phi$ by Exercise 18, and hence $(\mathbb{R}; \leq, a_1, \ldots, a_n) \models \phi$.
B.3. Exercise 24

Suppose that $L$ satisfies
\[ \forall x, y, z. x \land (y \lor z) = (x \land y) \lor (x \land z) \] (1)

We have to show that
\[ \forall x, y, z. x \lor (y \land z) = (x \lor y) \land (x \lor z). \]

For $x, y, z \in L$ we have
\[
(x \lor y) \land (x \lor z) = ((x \lor y) \land x) \lor ((x \lor y) \land z) \quad \text{(using (1))}
= (x \land (x \lor y)) \lor (z \land (x \lor y)) \quad \text{(commutativity of \land)}
= x \lor (z \land (x \lor y)) \quad \text{(absorption)}
= x \lor ((z \land x) \lor (z \land y)) \quad \text{(using (1))}
= (x \lor (z \land x)) \lor (z \land y) \quad \text{(associativity of \lor)}
= (x \lor (z \land z)) \lor (y \land z) \quad \text{(commutativity of \land)}
= x \lor (y \land z) \quad \text{(absorption)}
\]

The converse implication can be shown dually.
Bibliography