MATHEMATICAL LOGIC (MATH33021) 2025-26

GARETH O JONES AND MARCUS TRESSL

Lecture Notes

Contents

Date: December 9, 2025.

1. Partially Ordered Sets and Naïve Set Theory

1.1. Partially ordered sets.

1.1.1. **Definition.** A **partially ordered set** (**poset** for short) is a pair $(X, \leq)$ where X is a set and $\leq$ is a binary relation on X (in other words $\leq$ is a subset of $X \times X$) satisfying the following properties:

(i) $\leq$ is reflexive, i.e. $\forall x \in X : \ x \leq x$.
(ii) $\leq$ is anti-symmetric, i.e. $\forall x, y \in X : \ x \leq y \ \& \ y \leq x \Rightarrow x = y$.
(iii) $\leq$ is transitive, i.e. $\forall x, y, z \in X : \ x \leq y \ \& \ y \leq z \Rightarrow x \leq z$.

The relation $\leq$ is then called a **partial order** (on X) and X is called the **base set**, or **domain**, or **universe** of $(X, \leq)$.

Two elements $x, y \in X$ are called **comparable** if $x \leq y$ or $y \leq x$. We write $x \geq y$ for $y \leq x$ and $x < y$ for "$x \leq y$ and $x \neq y$". The relation $x < y$ is called a **strict partial order**; see also exercise 1(iii),(iv).

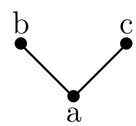
If in addition the **totality axiom**

(iv) $\forall x, y \in X : x \leq y$ or $y \leq x$

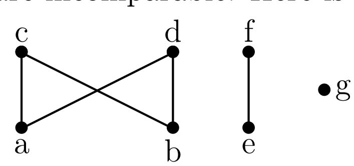
is satisfied (i.e. all elements are comparable), then we say that $(X, \leq)$ is a **chain** (aka **totally ordered set**, or **linearly ordered set**).

1.1.2. *Examples.*

(i) $(\mathbb{R}, \leq)$ with the **natural order** of real numbers is a chain. Similarly $(\mathbb{Q}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{N}, \leq)$ and $(\{1, \dots, n\}, \leq)$ in their natural order are chains.
(ii) Here is a poset with three elements that is not a chain:



The drawing indicates $X = \{a, b, c\}$ and the strict relations are precisely $a < b$ and $a < c$. Thus, b and c are incomparable. Here is another example:



So here $X = \{a, b, c, d, e, f, g\}$ and the strict relations are precisely $a < c$, $a < d$, $b < c$, $b < d$, and $e < f$. (Notice that g does not appear in that list.)
(iii) On every set X we have the **trivial partial order** defined by $x \leq y \iff x = y$. If X has three elements, then X with the trivial partial order just looks like this:

(iv) A prominent poset that is not a chain is the following: Let S be any set and let $\mathfrak{P}(S)$ be the **power set** of S (hence the set of all subsets of S). Then the inclusion $\subseteq$ of subsets of S is a partial order on $\mathfrak{P}(S)$. The axioms for posets are readily verified. If S has at least two elements, then $(\mathfrak{P}(S), \subseteq)$ is **not** a chain.

1.1.3**. Constructions on Posets** We now see methods on how to construct new posets from old ones. Starting with the examples in 1.1.2 one can actually show that all posets are obtained by applying these constructions several times.

(i) Let $(X, \leq)$ be a poset and let $T \subseteq X$. Then $\leq$ **induces a partial order** $\leq_0$ on T defined by $\leq \cap\, (T \times T)$. We write $\leq$ again for this partial order, if no confusion is caused. Then $(T, \leq_0)$ is called a **subposet** of $(X, \leq)$. Explicitly, a poset $(Y, \leq_0)$ is a subposet of a poset $(X, \leq)$ if and only if $Y \subseteq X$ and for all $y, y' \in Y$ we have $y \leq_0 y' \iff y \leq y'$.[1]

(ii) Consider the following construction. Suppose $(X, \leq_1)$ and $(Y, \leq_2)$ are partially ordered sets. We can form the **product of the two partially ordered sets** as follows: As the base set we take the cartesian product $X \times Y$ of the sets X and Y. Then the binary relation $\leq$ on $X \times Y$ defined as

$$(x, y) \leq (x', y') \iff x \leq_1 x' \text{ and } y \leq_2 y',$$

is a partial order on $X \times Y$. The poset $(X \times Y, \leq)$ is the product of $(X, \leq_1)$ and $(Y, \leq_2)$. Concrete examples of products will be done on the examples sheet.

(iii) We can also put other partial orders on the cartesian product. The following will be central for us. Suppose $(X, \leq_1)$ and $(Y, \leq_2)$ are partially ordered sets again. We can form the **lexicographic product of the two partially ordered sets** as follows: As the base set we take the cartesian product $X \times Y$ of the sets X and Y again. But this time we define a binary relation $\leq_{lex}$ on $X \times Y$ as

$$(x, y) \leq_{lex} (x', y') \iff x <_1 x' \text{ or } (x = x' \text{ and } y \leq_2 y').$$

Then $\leq_{lex}$ is a partial order on $X \times Y$. The poset $(X \times Y, \leq_{lex})$ is the lexicographic product of $(X, \leq_1)$ and $(Y, \leq_2)$ and is sometimes just denotes by $X \times_{lex} Y$.

The lexicographic product looks a bit more complicated than the product, however it is the lexicographic product that appears most in everyday life: Consider the following two letter words: it, me, by, in, on, as, up, at. If we order these alphabetically we get: as, at, by, in, it, me, on, up. These words are listed according to the lexicographic order of $\{a, b, c, \ldots, z\} \times_{lex} \{a, b, c, \ldots, z\}$.

More examples of lexicographic products will be done on the examples sheet.

(iv) The last example for now is a sort of "concatenation" of posets: Suppose $(X, \leq_1)$ and $(Y, \leq_2)$ are partially ordered sets again and assume that $X \cap Y = \emptyset$. We form the **ordered sum** of $(X, \leq_1)$ and $(Y, \leq_2)$ as follows: As the base set

[1]In order to understand precisely what this means you should do question 3(v)(d).

we take $X \cup Y$ and as partial order we take the relation $\leq$ defined as

$$\leq_1 \ \cup \ \leq_2 \ \cup (X \times Y).$$

This just means for $a, b \in X \cup Y$ that $a \leq b$ if and only if
(a) $a, b \in X$ and $a \leq_1 b$, or,
(b) $a, b \in Y$ and $a \leq_2 b$, or,
(c) $a \in X$ and $b \in Y$.
To visualize this: In the ordered sum, the original order of X and Y are unchanged and Y is stacked on top of X (or to the right of X if we think of orders going to the right), so that all elements of Y are greater than every element of X. If both $(X, \leq_1)$ and $(Y, \leq_2)$ are chains, then this ordered sum is again a chain. For example if $X = (\mathbb{N}, \leq)$ and $Y = (\{\frac{1}{2}, \frac{3}{2}\}, \leq)$ in their natural order, then the ordered sum looks like

$$1 — 2 — 3 — 4 — \ \ldots \quad — \tfrac{1}{2} — \tfrac{3}{2}$$

So here $n \leq \frac{1}{2} \leq \frac{3}{2}$ for all $n \in \mathbb{N}$. In general, the ordered sum of two chains can be pictured as

$$\underbrace{\cdots \overset{(X,\leq_1)}{\overline{\qquad\qquad\qquad}} \cdots \quad \cdots \overset{(Y,\leq_2)}{\overline{\qquad\qquad\qquad}} \cdots}_{\text{ordered sum of } (X,\leq_1) \text{ and } (Y,\leq_2)}$$

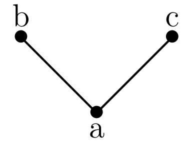
1.1.4. **Definition.** Let $(X, \leq)$ be a poset, let $S \subseteq X$ and let $x \in X$.
(i) We write $S \leq x$ for $\forall s \in S : s \leq x$. Similarly, $x \leq S$ means $\forall s \in S : x \leq s$, $S < x$ means $\forall s \in S : s < x$ and $x < S$ means $\forall s \in S : x < s$.
(ii) If $S \leq x$, then x is called an **upper bound** of S (in X). If $x \leq S$, then x is called a **lower bound** of S (in X).
(iii) If $S \leq x$ and $x \in S$, then x is the **largest element** of S. If $x \leq S$ and $x \in S$, then x is the **smallest element** of S. Notice that it is correct to say "the" largest/smallest element, i.e. these elements are unique (if they exist).
(iv) If x is the smallest upper bound of S, then x is called the **supremum** of S (in X); written as $x = \sup(S)$. If x is the largest lower bound of S, then x is called the **infimum** of S (in X); written $x = \inf(S)$. By the previous item, S can at most have one supremum and one infimum.
(v) If $x \in S$ and if there is no $s \in S$ with $x < s$, then x is called a **maximal element** of S. If $x \in S$ and if there is no $s \in S$ with $s < x$, then x is called a **minimal element** of S.

If $S = \{s_1, \ldots, s_n\}$ is finite then we also say upper bound, lower bound, supremum, infimum, etc., of $s_1, \ldots, s_n$.

These definitions are well known for the chain $(\mathbb{R}, \leq)$ but need some new thought for general posets. A common source of mistakes is the confusion of the notion "largest element" and "maximal element"; make sure you understand the difference by carefully studying the following

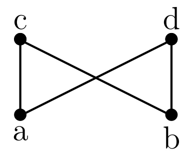
1.1.5. *Examples.*

(i) Consider the poset



(so here $X = \{a, b, c\}$ in the order indicated, cf. 1.1.2(ii)). Then b and c have no common upper bound, but a common lower bound, namely a, and $a = \inf\{b, c\}$. Furthermore, b and c are maximal elements of $S = \{a, b, c\}$ (which is equal to X here) but S does **not** have a largest element. On the other hand a is the smallest element of S.

(ii) In the poset



a and b have a common upper bound (both c and d are upper bounds), but a and b have no supremum.

1.1.6. **Definition.** An **initial segment** (aka **down-set**) of a poset $X = (X, \leq)$ is a subset Y of X such that for all $x, y \in X$ the following implication is true:

$$\text{If } x \leq y \text{ and } y \in Y, \text{ then } x \in Y.$$

We denote this property of Y by

$$Y \Subset X.$$

An important example is the following: Any $a \in X$ gives rise to the initial segment

$$X_{<a} := \{x \in X \mid x < a\} \text{ of } X.$$

1.1.7. **Observation.** *Let $X = (X, \leq)$ be a partially ordered set.*

(i) If I is an arbitrary index set and $Y_i \Subset X$ for each $i \in I$, then the union $\bigcup_{i \in I} Y_i$ and the intersection $\bigcap_{i \in I} Y_i$ are again an initial segment of X. This is left as an exercise in question 4.

(ii) If $Y, Z \Subset X$ and if X is a chain, then $Y \subseteq Z$ or $Z \subseteq Y$: To see this assume there are $y \in Y \setminus Z$ and $z \in Z \setminus Y$. Since X is a chain, y and z are comparable. Say $y \leq z$. But then also $y \in Z$ since Z is an initial segment of X, in contradiction to the choice of y.

1.1.8. **Definition.** Let $(X, \leq_1), (Y, \leq_2)$ be posets. A map $f : X \longrightarrow Y$ is called **monotone**, or a **poset-homomorphism** if f preserves the partial orders, i.e.,

$$\forall x, x' \in X : \; x \leq_1 x' \implies f(x) \leq_2 f(x').$$

Furthermore, f is called a **poset embedding** if

$$\forall x, x' \in X : \; x \leq_1 x' \iff f(x) \leq_2 f(x').$$

The map f is called an **isomorphism of posets** if f is bijective and an embedding. Two posets $(X, \leq_1), (Y, \leq_2)$ are called **isomorphic** is there is an isomorphism between them.

1.1.9. *Examples.*

(i) Let $(X, \leq)$ be a poset and let $T \subseteq X$ be a subposet, see 1.1.3(i). Then the inclusion map[2] $f : T \hookrightarrow X$ is a poset embedding.

(ii) Let $(X, \leq_1), (Y, \leq_2)$ be posets and let $f : X \longrightarrow Y$ be a poset embedding. Let $T = f(X)$ be the image of X under f. Then f induces an isomorphism $(X, \leq_1) \longrightarrow (T, \leq_2)$ onto the subposet $(T, \leq_2)$ of $(Y, \leq_2)$.

(iii) Let $(X, \leq_1), (Y, \leq_2)$ be posets and let $p_1 : X \times Y \longrightarrow X$, $p_2 : X \times Y \longrightarrow Y$ be the projections.

 (a) If we equip $X \times Y$ with the product order, then p_1 and p_2 are monotone.

 (b) If we equip $X \times Y$ with the lexicographic order, then p_1 is monotone, but in general p_2 is not monotone.

[2]For a subset A of a given set B, the **inclusion map** $A \longrightarrow B$ is the map $A \longrightarrow B$ that sends a to a. We also write $f : A \hookrightarrow B$ to indicate that $A \subseteq B$ and that f is the inclusion map $A \longrightarrow B$.

1.2. **Well ordered sets and the Lemma of Zorn.**
We will relax on the notation of the partial order whenever this is unambiguous. For example if $(X, \leq_1), (Y, \leq_2)$ are posets we will just write $(X, \leq)$ and $(Y, \leq)$. Keep in mind that $\leq$ on both sides should be considered as different objects. If the partial orders are clear from the context we will even drop $\leq$. The expression "Let $X = (X, \leq)$ be a poset" is a common shorthand for "Let $(X, \leq)$ be a poset, which we abbreviate as X". The convention here is similar to the one in group theory, where one denotes groups as $G, H, \ldots$ and the group operations are only specified when necessary.

1.2.1. **Definition.** A **well ordered set** is a poset $(X, \leq)$ such that every nonempty subset has a smallest element.

1.2.2. *Remark.* Observe that a well ordered set is a chain because any two element subset has a smallest element and therefore all elements are comparable.

Every finite chain is obviously well ordered. Further, the chain $(\mathbb{N}, \leq)$ is well ordered. Apart from these examples, you might have not seen any other well ordered sets yet. The chain $(\mathbb{Z}, \leq)$ is not well ordered. At this point the constructions from section 1.1 come in handy:

1.2.3. **Proposition.** *Let $(X, \leq)$ and $(Y, \leq)$ be well ordered sets. Then the ordered sum and the lexicographic product of $(X, \leq)$ and $(Y, \leq)$ are again well ordered.*

Proof. The proof that the ordered sum is well ordered is left as an exercise in question 8. We show that the lexicographic product is well ordered. So let $T \subseteq (X \times Y)$ be nonempty and let $p : X \times Y \longrightarrow X$ be the projection onto X. Then $p(T) \subseteq X$ is nonempty and as $(X, \leq)$ is well ordered by assumption, $p(T)$ has a smallest element x_0. Let $Y_0 = \{y \in Y \mid (x_0, y) \in T\}$. Since $x_0 \in p(T)$, there is some $y \in Y$ with $(x_0, y) \in T$, i.e. $y \in Y_0$ and so Y_0 is a nonempty subset of Y. As $(Y, \leq)$ is well ordered by assumption, Y_0 has a smallest element y_0. We now claim that (x_0, y_0) is the smallest element of T for the lexicographic order on $X \times Y$. By choice of y_0 we know that $(x_0, y_0) \in T$. Hence we only need to show that $(x_0, y_0) \leq (x, y)$ for all $(x, y) \in T$. Recall that this means

$$x_0 < x \quad \text{or} \quad (x_0 = x \text{ and } y_0 \leq y).$$

Since $x \in p(T)$ we have $x_0 \leq x$ by choice of x_0. If $x_0 < x$ then we are done. If $x_0 = x$, then $y \in Y_0$ and then $y_0 \leq y$ by choice of y. □

1.2.4. **Observation.** *If $(X, \leq)$ is well ordered then each initial segment Y of X with $Y \neq X$ is of the form $Y = X_{<a}$ for some $a \in X$. In fact the element a is uniquely determined by Y, namely*

$$a = \min(X \setminus Y).$$

Also observe that $X_{<a} = \emptyset$ if a is the smallest element of X.

1.2.5**. Lemma of Zorn.**
Let $X = (X, \leq)$ be a nonempty, partially ordered set, such that each subset W of X that is well ordered by $\leq$[3]*, has an upper bound in X. Then X possesses at least one maximal element.*

Proof. [This proof is not examinable]
Suppose X does not have maximal elements. Let $\mathscr{C}$ be the set of all well ordered subsets of X. Notice that $\mathscr{C} \neq \emptyset$, because the empty set is an element of $\mathscr{C}$.

Then, by the assumption of the theorem, for each $W \in \mathscr{C}$ there is some $x \in X$ with $W \leq x$. As we are assuming that X does not have maximal elements, x is not a maximal element, hence there is an element $u \in X$ with $x < u$. This shows that for each $W \in \mathscr{C}$, the set

$$U_W := \{u \in X \mid W < u\}$$

is non-empty (here $W < u$ stands for $\forall w \in W : w < u$).
By the *axiom of choice*, there is a map $a : \mathfrak{P}(X) \setminus \{\emptyset\} \longrightarrow X$ with the property $a(Y) \in Y$ for all non-empty subsets Y of X. Consequently, there is also a map $b : \mathscr{C} \longrightarrow X$ such that

$$W < b(W) \text{ for all } W \in \mathscr{C}$$

(define $b(W) = a(U_W)$).

Let

$$\mathscr{W} := \{W \in \mathscr{C} \mid \text{ for all } w \in W \text{ we have } b(W_{<w}) = w\}.$$

(Recall that $W_{<w} = \{x \in W \mid x < w\}$.)
Claim. For all $W, V \in \mathscr{W}$ we have $W \Subset V$ or $V \Subset W$.
Proof of the Claim. Define

$$K := \bigcup\{A \subseteq W \cap V \mid A \Subset W \text{ and } A \Subset V\}.$$

Then $K \subseteq W \cap V$ and by 1.1.7(ii) we have $K \Subset W$ and $K \Subset V$ (note that possibly $K = \emptyset$). Therefore it remains to show that $W \subseteq K$ or $V \subseteq K$.

Otherwise $K \subsetneq W$ and $K \subsetneq V$. So by 1.2.4 there are $w \in W$ and $v \in V$ with $K = W_{<w}$ and $K = V_{<v}$. Then

$$w = b(W_{<w}) = b(K) = b(V_{<v}) = v.$$

But now $K \cup \{w\} = K \cup \{v\}$ is an initial segment of W and V, which contradicts the definition of K and $w = v \notin K$. $\diamond$

The claim easily implies that

$$(*) \qquad M := \bigcup_{W \in \mathscr{W}} W$$

is a chain, well ordered by $\leq$ and that each $W \in \mathscr{W}$ is an initial segment of M. But then we get that $M \in \mathscr{W}$.

On the other hand $M \cup \{b(M)\}$ is well ordered, too. Since $M \cup \{b(M)\} \in \mathscr{W}$ and $b(M) \notin M$, this contradicts $(*)$. $\square$

[3]This means that the subposet of $(X, \leq)$ defined on the set $W \subseteq X$ is well ordered. In particular, W is totally ordered by $\leq$.

Zorn's lemma has a vast amount of applications in all parts of mathematics. We will make use of it now, but also in the chapters on predicate logic and model theory.

1.2.6. *Example.* Every vector space over any field has a basis. For example, the $\mathbb{Q}$-vector space $\mathbb{R}$ has a basis (each such basis is called a **Hamel basis**)

Proof. [This proof is not examinable] Let K be our field and let V be our K-vector space. By definition, a basis B of V is a linearly independent and generating subset of V. Recall from linear algebra: If $V = K^n$, then a subset B of K^n is a basis of K^n if and only if B is a maximally linear independent set (i.e., B is linearly independent and no proper superset of B is linearly independent).

The clue is that Zorn's lemma enables us to find a maximally independent subset B of V for any vector space (and they are in general not finite dimensional). Once we have shown this, the old proof from linear algebra can be copied verbatim to show that B is a generating set.

Hence we just need to find such a maximal independent set B: Let X be the set of linearly independent subsets of V, partially ordered by inclusion. We are looking for maximal elements in this poset and by Zorn's lemma we only need to show that any chain $Y \subseteq X$ has an upper bound in X. We let B be the union of all subsets $C \in Y$. Since any two sets $C, D \in Y$ are comparable for inclusion (Y is a chain!) the set B is also independent. This finishes the proof. □

1.2.7**. Well Ordering Principle.**
Every set can be well ordered, in other words, for every set M there is a well order with universe M.

Proof. We consider

$$\mathscr{W} := \{(A, \leq) \mid A \subseteq M \text{ and } \leq \text{ is a well ordering on } A\}.$$

and furnish it with the following relation: We define a binary relation $\sqsubseteq$ on $\mathscr{W}$ as follows:

$$\begin{aligned}(A_1, \leq_1) \sqsubseteq (A_2, \leq_2) \iff &(A_1, \leq_1) \text{ is a subposet of } (A_2, \leq_2)\\ &\text{and } A_1 \Subset A_2.\end{aligned}$$

Then $\sqsubseteq$ is a partial order on $\mathscr{W}$ (see questions 7 and 4 of the example sheets). By question 9, every chain in $\mathscr{W}$ has an upper bound. By Zorn's Lemma there are maximal elements $(A, \leq)$ in $\mathscr{W}$. But this is only possible if $A = M$, because for any $m \in M \setminus A$ the ordered sum of $(A, \leq)$ and $\{m\}$ would be an element of $\mathscr{W}$ strictly bigger than $(A, \leq)$ for $\sqsubseteq$. Hence $\leq$ is a well order on M. □

1.3. **Rigidity of well ordered sets.**

1.3.1. *Notation.* If X and Y are well ordered sets we write $X \sqsubseteq Y$, if there is a poset embedding $f : X \longrightarrow Y$ such that $f(X)$ is an initial segment of Y. In other words $X \sqsubseteq Y$ if and only if there is some $Z \Subset Y$ such that X and Z are isomorphic.

The rigidity of well ordered sets says the following:

1.3.2. **Theorem.**
If X and Y are well ordered sets and $X \sqsubseteq Y$, then there is a **unique** *poset-embedding $f : X \longrightarrow Y$ such that $f(X)$ is an initial segment of Y.*

Proof. Let $f, g : X \longrightarrow Y$ be poset embeddings with $f(X) \Subset Y$ and $g(X) \Subset Y$. We have to show that $f = g$. Since $f(X), g(X) \Subset Y$ we may assume $f(X) \subseteq g(X)$. Suppose there is some $a \in X$ with $f(a) \neq g(a)$. Since X is well ordered, there is a smallest $a \in X$ with $f(a) \neq g(a)$. Then

(a) $f(a) \neq g(a)$ by choice of a.
(b) $f(x) = g(x)$ for all $x < a$ by choice of a.
(c) $g(a) \leq f(a)$. To see this assume $f(a) < g(a)$. As $f(X) \subseteq g(X)$ we have $f(a) \in g(X)$ and we may apply g^{-1} to $f(a)$. Since g^{-1} is order preserving we get $g^{-1}(f(a)) < a$. By (b) applied to $x = g^{-1}(f(a))$ we have
$$f\Big(g^{-1}(f(a))\Big) = g\Big(g^{-1}(f(a))\Big) = f(a).$$
Now f is injective, hence $g^{-1}(f(a)) = a$, meaning $f(a) = g(a)$ in contradiction to (a).

Since $f(X) \Subset Y$, (c) implies that there must be some $b \in X$ with $f(b) = g(a)$. We will now derive a contradiction by considering two cases.

Case 1. $b < a$. Then $f(b) = g(b)$ by (b) and so $g(b) = f(b) = g(a)$, which contradicts $b < a$ and the injectivity of g.

Case 2. $a \leq b$. Since f is order preserving we have $f(a) \leq f(b) = g(a)$. By (a) we must have $f(a) < f(b) = g(a)$. But this contradicts (c). $\square$

1.3.3. **Theorem.** *If X and Y are well ordered sets, then*
(i) $X \sqsubseteq Y$ and $Y \sqsubseteq X \Rightarrow X \cong Y$.
(ii) $X \sqsubseteq Y$ or $Y \sqsubseteq X$.

Proof. (i). By assumption there are poset embeddings $g : X \longrightarrow Y$ and $h : Y \longrightarrow X$ such that $g(X) \Subset Y$ and $h(Y) \Subset X$.

Then also the composition $h \circ g : X \longrightarrow X$ is a poset embedding and $h \circ g(X) \Subset X$ (see question 4(ii) on the example sheets). By 1.3.2, $h \circ g$ is the identity on X. By symmetry, $g \circ h$ is the identity on Y. Hence g is a poset isomorphism and h is its compositional inverse.

(ii).[This part of the proof is not examinable] Let
$$\mathcal{C} := \{A \Subset X \mid A \sqsubseteq Y\}$$
be the set of all initial segments A of X such that $A \sqsubseteq Y$. By 1.1.7(ii), its union $K = \bigcup_{A \in \mathcal{C}} A$ itself is an initial segment of X.

Claim. There is a poset embedding $F : K \longrightarrow Y$ with $F(K) \Subset Y$. In particular $K \sqsubseteq Y$.

Proof of claim. For every $A \in \mathcal{C}$ let $f_A : A \longrightarrow Y$ be the unique (by 1.3.2) poset embedding with $f_A(A) \Subset Y$. If $A, B \in \mathcal{C}$ then $A, B \Subset X$ and so $A \subseteq B$ or $B \subseteq A$. Say $A \subseteq B$. Then the restriction of f_B to A is again a poset embedding whose image is an initial segment of Y. By uniqueness this restriction is f_A. Therefore there is a common extension $F : K \longrightarrow Y$ of all the f_A with $A \in \mathcal{C}$ and this extension is again a poset embedding. Since $F(K) = \bigcup_{A\in\mathcal{C}} f_A(A) \Subset Y$, F has the required property. $\diamond$

Now take F as in the claim. If $K = X$, then $X \sqsubseteq Y$ and we are done. So assume $K \neq X$. Let a be the smallest element of $X \setminus K$. As $K \Subset X$ we have $K = X_{<a}$. It suffices to show that $F(K) = Y$, since then F^{-1} is a poset embedding of Y with image $K \Subset X$ as required.

Suppose $F(K) \neq Y$. Let b be the smallest element of $Y \setminus F(K)$. As $F(K) \Subset Y$ we have $F(K) = Y_{<b}$. Since $K = X_{<a}$, F can be extended to a poset-isomorphism

$$K \cup \{a\} \longrightarrow f(K) \cup \{b\}$$

by mapping a to b. Since $K = X_{<a}$, we know $K \cup \{a\} \Subset X$ and similarly $F(K) = Y_{<b}$ entails $f(K) \cup \{b\} \Subset Y$. But then $K \cup \{a\} \in \mathcal{C}$ which is impossible as $a \notin K$ and K is the union of all sets in $\mathcal{C}$. $\square$

1.4. **Ordinal numbers.**
Loosely speaking, ordinal numbers are special well ordered sets and natural numbers will be the finite ordinal numbers. (We will actually define here what is a natural number!) The definition of ordinal numbers looks a bit awkward at first sight, but they have marvelous properties, as we will see in this section. First an auxiliary notion.

1.4.1. **Definition.**
A **transitive set** X is a set such that each of its elements is a subset of X.

Another way of saying this is that $X \subseteq \mathfrak{P}(X)$. Hence in a transitive set we know that for all $x \in X$ and all $y \in x$ we have $y \in X$, for short:

$$y \in x \in X \Rightarrow y \in X.$$

An **ordinal number**, or just **ordinal**, is a transitive set α such that the element relation is a strict well order on α.[4]This means that the relation $x \leq y$ defined as $x = y$ or $x \in y$ is a well order on α (thus $x < y$ reads as $x \in y$ in an ordinal).

Hence an ordinal is a special kind of well ordered set. Prominent examples of ordinals are:

$$0 := \emptyset,\ 1 := \{\emptyset\}, 2 := \{\emptyset, \{\emptyset\}\}, 3 := \{0, 1, 2\}, ...$$

and more generally

$$n + 1 := \{0, 1, 2, \dots, n\}.$$

This is in fact the rigorous definition of natural numbers. Working with ordinals feels a bit unusual at the beginning, in particular one needs to familiarize with the use of the $\in$-symbol as a partial order in ordinals. It is customary to write $x < y$ again instead of $x \in y$ inside an ordinal.

1.4.2. **Basic properties of ordinals** Let α be an ordinal.

(i) $\alpha^* := \alpha \cup \{\alpha\}$ is again an ordinal, called the **successor of** α.[5]
(ii) If $x \in \alpha$, then $x = \alpha_{<x}$ (see 1.1.6 for the definition of $\alpha_{<x}$).
(iii) If $K \Subset \alpha$ and $K \neq \alpha$, then K is the smallest element of $\alpha \setminus K$.
(iv) Every $x \in \alpha$ is itself an ordinal and at the same time an initial segment of α.
(v) If $x \in \alpha$, then $x^* = \alpha$ or x^* is the immediate successor[6] of x in the chain α.

Proof. Items (i)-(iii) follow quickly from the definition of an ordinal and are left as an exercise in question 12. In order to get used to ordinals it is vital that you attempt this exercise. We do the slightly more complicated (iv) and (v):

(iv). By (ii) we know that x is an initial segment of α and therefore x is also well ordered by $\in$. We still need to see that x is a transitive set. If $z \in y \in x$, then $y \in \alpha$

[4]Ordinals are usually denoted by small Greek letters $\alpha, \beta, \gamma, \dots$.

[5]In the literature, α^* is often denoted by α^+. However we will reserve the notation α^+ for cardinal successors later on.

[6]For elements x, y from a chain C, we say that y is the **immediate successor** of x in C if $x < y$ and if there is no element $z \in C$ with $x < z < y$. Notice that in general, not every element of a chain has an immediate successor.

(because α is transitive) and then for the same reason $z \in \alpha$. Since α is transitive for $\in$ we get $z \in x$. Hence $y \subseteq x$, and x is transitive.

(v). If x is the largest element of α, then $\alpha = \alpha_{<x} \cup \{x\}$. By (ii) this is just x^*.

If x is not the largest element of α, then the smallest $y \in \alpha$ that satisfies $x < y$ is $y = \min\{z \in \alpha \mid x < z\}$. By (iv), y is an ordinal. Since x is the largest element of y we get $x^* = y$ as we have seen just above for α. □

1.4.3. **Proposition.** *For ordinals α, β the following are equivalent:*

(i) $\alpha \sqsubseteq \beta$.
(ii) There is a poset embedding $\alpha \longrightarrow \beta$. [7]
(iii) $\alpha \subseteq \beta$. [8]
(iv) $\alpha \Subset \beta$.
(v) $\alpha = \beta$ *or* $\alpha \in \beta$.

Proof. (iii)⇒(iv). Let $x, y \in \beta$ with $x < y \in \alpha$, where $<$ is the order on β. We need to show that $x \in \alpha$. But the strict order relation on β is $\in$, hence $x \in y$. Hence $x \in y \in \alpha$ and as α is transitive we have $x \in \alpha$.

(iv)⇒(v) holds by 1.4.2(iii).

(v)⇒(i) holds by 1.4.2(ii).

(i)⇒(ii) is trivial.

(ii)⇒(iii).[this part of the proof is not examinable] Let $f : \alpha \longrightarrow \beta$ be a poset embedding and suppose $\alpha \nsubseteq \beta$. Let $y := \min(\alpha \setminus \beta)$. Then by 1.4.2(ii) we have $y = \alpha_{<y} \subseteq \beta$. By 1.4.2(iv), $y \Subset \alpha$ and y is an ordinal.

As we have already shown the implication (iii)⇒(iv) we get from $y \subseteq \beta$ that $y \Subset \beta$. By 1.4.2(iii), using $y \notin \beta$, we get $y = \beta$. Consequently, $f(y) \in \beta = y$, i.e. $f(y) < y$ in α. Since f is a poset embedding, it follows that $f(f(y)) < f(y)$, which shows that the set $\{x \in y \mid f(x) < x\}$ is not empty (it contains $f(y)$).

Let $x_0 \in y$ be minimal with $f(x_0) < x_0$. Then $f(x_0) \in x_0 \in y$ and so $f(x_0) \in y$. Hence the definition of x_0 implies $f(x_0) \leq f(f(x_0))$. On the other hand $f(x_0) < x_0$, thus $f(f(x_0)) < f(x_0)$ as f is a poset embedding. This is a contradiction. □

1.4.4. **Definition.** "Ordering on ordinals"
For ordinals α, β we will just write $\alpha \leq \beta$ instead of $\alpha \subseteq \beta$ and $\alpha < \beta$ instead of $\alpha \in \beta$. By 1.4.3, these relations can be interpreted in all plausible ways.

1.4.5. **Corollary.** *If α, β are ordinals, then $\alpha \Subset \beta$ or $\beta \Subset \alpha$. Hence also $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$, and $\alpha \leq \beta$ or $\beta \leq \alpha$.*

Proof. This follows from 1.3.3 and 1.4.3. □

1.4.6. **Corollary.** *If I is an index set and α_i is an ordinal for all $i \in I$, then also $\bigcup_{i \in I} \alpha_i$ is an ordinal.*

[7]The image of such an embedding does not need to be an initial segment of β.

[8]This inclusion is indeed meant as inclusion of sets, not as subposet relation. Hence we do a priori not ask that the order of α is the restriction of the order of β in this condition

Proof. By 1.4.5 we know that for all $i, j \in I$ we have $\alpha_i \Subset \alpha_j$ or $\alpha_j \Subset \alpha_i$. This easily implies that $\bigcup_{i\in I} \alpha_i$ is transitive and totally ordered by $\in$.

If $X \subseteq \bigcup_{i\in I} \alpha_i$ is non-empty, then $X \cap \alpha_i$ is non-empty for some $i \in I$. Let $x = \min(\alpha_i \cap X)$. Now, for every other index $j \in I$ we know that $\alpha_i \Subset \alpha_j$ or $\alpha_j \Subset \alpha_i$ by using 1.4.5. It now follows easily that x is in fact the smallest element of X. □

1.4.7. **Corollary.** *Every ordinal α is equal to the set of ordinals that are strictly less than α. In symbols:*

$$\alpha = \{\beta \mid \beta \textit{ is an ordinal and } \beta < \alpha\}.$$

(This generalises the identity $n + 1 = \{0, \dots, n\}$ from the beginning of the section to all ordinals.)

Proof. For ordinals the relation $\beta < \alpha$ is equivalent to $\beta \in \alpha$ by 1.4.3. Hence we know $\supseteq$. The other inclusion follows with 1.4.2(iv). □

1.4.8. **Definition.** There are two principle kind of ordinals: An ordinal α is called a **successor ordinal** if there is an ordinal β such that $\alpha = \beta^*$. Otherwise α is called a **limit ordinal**. Limit ordinals are frequently denoted by λ (resembling the "l" in "limit"). Notice that there is a unique finite limit ordinal, namely 0. We will be talking about these notions on the example sheets.

1.4.9. **Theorem.** *If W is a well ordered set, then there is a unique ordinal α that is isomorphic to W (and in fact, by 1.3.2, there is exactly one isomorphism $W \longrightarrow \alpha$).*

Proof. [this proof is not examinable] Uniqueness of α follows from 1.4.3(ii)⇔(iii). In order to find α let

$$\mathcal{K} := \{A \Subset W \mid A \text{ is isomorphic to some ordinal}\}.$$

For $A \in \mathcal{K}$ take an ordinal α_A and an isomorphism $f_A : A \longrightarrow \alpha_A$. We will show that $\alpha = \bigcup_{A\in\mathcal{K}} \alpha_A$ is an ordinal as required. By 1.4.6 we already know that α is an ordinal.

If $A \subseteq B$, then $A \Subset B$ and so $f_B(A) \Subset \alpha_B$. By the rigidity of well ordered sets we see that f_B is an extension of f_A. Since $\mathcal{K}$ is a chain for inclusion, it follows that there is a common extension f of all the f_A with $A \in \mathcal{K}$ and clearly f is an isomorphism

$$K := \bigcup_{A\in\mathcal{K}} A \longrightarrow \bigcup_{A\in\mathcal{K}} \alpha_A = \alpha.$$

It remains to show that $K = W$. Suppose this is not the case. Since K is a union of initial segments of W, K is itself an initial segment of W. As $K \neq W$, there is some $w \in W$ with $K = W_{<w}$. Hence $K \cup \{w\} \Subset W$ and f can be extended to an isomorphism $K \cup \{w\} \longrightarrow \alpha^* = \alpha \cup \{\alpha\}$ by mapping w to the element α of the ordinal α^* (see 1.4.2(i)). But this implies $K \cup \{w\} \in \mathcal{K}$, which contradicts $K = \bigcup_{A\in\mathcal{K}} A < w$. □

Combining 1.4.9 with the well ordering principle we get

1.4.10. **Corollary.** *Every set is in bijection with some ordinal.* □

Notice that an ordinal in 1.4.10 is in general **not** unique. More precisely: Every infinite set is in bijection with infinitely many ordinals; see question 15 from the example sheets.

1.4.11**. Ordinal Minimisation Principle.**
Let P be a property of ordinals and assume there is an ordinal with property P. Then there is a smallest ordinal with property P.

Proof. Take an ordinal β with property P. Since β is well ordered, there is a smallest ordinal $\alpha \leq \beta$ that has property P and we claim that α is the smallest ordinal with property P:

To see this, let γ be any ordinal with property P. If $\gamma \leq \beta$, then by choice of α we know $\alpha \leq \gamma$. If, on the other hand, $\gamma \nleq \beta$, then by 1.4.5 we know $\beta \leq \gamma$ and so again $\alpha \leq \gamma$. □

An easy example here is the following: There is a smallest infinite ordinal and this is denoted by ω. This follows from the ordinal minimisation principle for the property "α is infinite" for ordinals α.[9] Then ω is the set of all finite ordinals ($= \{0, 1, 2, 3, \ldots\}$): The set of all finite ordinals is the union λ of all finite ordinals. Note that this union is an ordinal by 1.4.6. This union is infinite and so $\omega \leq \lambda$. Since ω is infinite we have $n < \omega$ for all finite ordinals n, hence by definition of λ we see $\omega = \lambda$. More applications of 1.4.11 can be found in question 14

[9]We have actually not defined what it means that a set is finite, so we should specify this here: We say that a set S is **finite** if every injective function $S \longrightarrow S$ is surjective. Another formulation is: A set is infinite if it is in bijection with a nonempty limit ordinal.

1.5. **Cardinal numbers.**

Let X be any set. By 1.4.10, there is an ordinal that is in bijection with X. Hence by the ordinal minimisation principle 1.4.11 there is a smallest such ordinal and we can make the following

1.5.1. **Definition.** For a set X, the **cardinality of** X, or the **size of** X is the smallest ordinal α that is in bijection with X. In symbols

$$\mathrm{card}(X) = \alpha, \text{ or, } |X| = \alpha.$$

A **cardinal number**, or just a **cardinal**, is an ordinal α whose cardinality is α. In particular, the size of any set is a cardinal number.

Obviously all finite ordinals are cardinals. The **smallest infinite cardinal** is ω, since it is defined as the smallest infinite ordinal. This cardinal is also written as $\aleph_0$.[10]

1.5.2. **Proposition.** *Let X, Y be sets with $X \neq \emptyset$. The following are equivalent.*

(i) $\mathrm{card}(X) \leq \mathrm{card}(Y)$.
(ii) There is an injective map $X \longrightarrow Y$.
(iii) There is a surjective map $Y \longrightarrow X$.

Proof. We may assume that $X = \kappa$ and $Y = \lambda$ are cardinal numbers, just replace X, Y by their cardinals and recall that a set is in bijection with its cardinality.

(i)⇒(iii). Since $\kappa \leq \lambda$ and κ, λ are also ordinals we know that $\kappa \subseteq \lambda$. Hence we may define a surjective map $g : \lambda \longrightarrow \kappa$ by $g(y) = y$ if $y \in \kappa$ and $g(y) = 0$ otherwise. Notice that we need $\kappa \neq 0$ here, which is implied by $X \neq \emptyset$.

(iii)⇒(ii). Suppose $g : \lambda \longrightarrow \kappa$ is a surjective map. This is equivalent to saying that for each $x \in \kappa$, the fibre $g^{-1}(x)$[11] is nonempty. Then we may define $f(x) := \min(g^{-1}(x))$ and get an injective map $f : \kappa \longrightarrow \lambda$.

(ii)⇒(i). Let $f : \kappa \longrightarrow \lambda$ be injective. Then the image $f(\kappa)$ of f is a well ordered subset of λ and by 1.4.9 there is a unique ordinal number α which is isomorphic to $f(\kappa)$. By 1.4.3(ii)⇒(iii) we know $\alpha \subseteq \lambda$.

On the other hand, the function f, when considered as a map $\kappa \longrightarrow f(\kappa)$, is a bijection. Hence there is also a bijection $\kappa \longrightarrow \alpha$ and by definition of "cardinal" we then know $\kappa \leq \alpha$. Thus $\kappa \leq \alpha \leq \lambda$. □

Notice that by 1.4.5 we always have $\mathrm{card}(X) \leq \mathrm{card}(Y)$ or $\mathrm{card}(Y) \leq \mathrm{card}(X)$.

1.5.3**. Theorem of Bernstein.**
If X, Y are sets then the following are equivalent.

(i) $\mathrm{card}(X) = \mathrm{card}(Y)$.
(ii) There is a bijective map $X \longrightarrow Y$.
(iii) There are injective maps $X \longrightarrow Y$ and $Y \longrightarrow X$.
(iv) There are surjective maps $X \longrightarrow Y$ and $Y \longrightarrow X$.

---

[10]$\aleph$ is the first letter of the Hebrew alphabet and pronounced 'aleph'

[11]Recall from year 1 that $g^{-1}(x)$ is the set of all $y \in \lambda$ with $g(y) = x$.

Proof. By 1.5.2, item (iii) is equivalent to $\mathrm{card}(X) \leq \mathrm{card}(Y)$ and $\mathrm{card}(Y) \leq \mathrm{card}(X)$. But $\mathrm{card}(X) \leq \mathrm{card}(Y)$ and $\mathrm{card}(Y) \leq \mathrm{card}(X)$ means $\mathrm{card}(X) = \mathrm{card}(Y)$.[12], and therefore there is a bijection $X \longrightarrow Y$. The same argument shows the equivalence of (iv) and (i). Finally, the equivalence of (ii) and (i) is immediate from the definition of the cardinality of a set. □

1.5.4**. Size of the power set.**
For every set X we have $\mathrm{card}(X) < \mathrm{card}(\mathfrak{P}(X))$.

Proof. Since there is an injective function $X \longrightarrow \mathfrak{P}(X)$ we know $\mathrm{card}(X) \leq \mathrm{card}(\mathfrak{P}(X))$. Suppose $\mathrm{card}(X) = \mathrm{card}(\mathfrak{P}(X))$. Then there is a surjective map $f : X \longrightarrow \mathfrak{P}(X)$. Consider the set

$$Y = \{x \in X \mid x \notin f(x)\}. \tag{$*$}$$

Then $Y \subseteq X$ and as f is surjective there is some $y \in X$ with $f(y) = Y$. Consequently $(*)$ says that for every $x \in X$ we have

$$x \in f(y) \iff x \notin f(x).$$

But this is impossible when $x = y$. □

1.5.5. **Corollary.** *If X is a set, then there is a cardinal $\kappa >$* $\mathrm{card}(X)$.

Proof. Take $\kappa = \mathrm{card}(\mathfrak{P}(X))$ and apply 1.5.4. □

We will now study the size of cartesian products $X \times Y$ of sets. You have most likely seen in your first year that the product of two countable infinite sets is again countable. We record this again, but in a very explicit way, which is used at the very beginning of coding in Gödel style (cf. [Goedel]).

1.5.6. **Theorem and Definition.** *The* **Pairing Function**

$$\mathrm{Pair} : \omega \times \omega \longrightarrow \omega,$$

defined by

$$\mathrm{Pair}(x, y) := \frac{(x + y)(x + y + 1)}{2} + x$$

is bijective.

Proof. [this proof is not examinable] We first show that Pair is surjective. Take $n \in \omega$ and let $z \in \omega$ be maximal with $\frac{z(z+1)}{2} \leq n$. Then $n < \frac{(z+1)(z+2)}{2}$ and therefore

$$0 \leq n - \frac{z(z+1)}{2} < \frac{(z+1)(z+2)}{2} - \frac{z(z+1)}{2}.$$

Since $\frac{(z+1)(z+2)}{2} - \frac{z(z+1)}{2} = z + 1$ we have

$$0 \leq x := n - \frac{z(z+1)}{2} \leq z \text{ and so}$$
$$y := z - x \geq 0$$

[12]Make sure you understand why $\mathrm{card}(X) \leq \mathrm{card}(Y)$ and $\mathrm{card}(Y) \leq \mathrm{card}(X)$ implies $\mathrm{card}(X) = \mathrm{card}(Y)$

Now

$$\mathrm{Pair}(x,y)=\frac{(x+y)(x+y+1)}{2}+x=\frac{z(z+1)}{2}+x=n,$$

as required for surjectivity.

We now show that the preimage (x,y) of n under Pair constructed above is indeed unique; hence we show that Pair is injective.

Assume $\mathrm{Pair}(x',y')=n$. Then $\frac{(x'+y')(x'+y'+1)}{2}\leq n$ and so by choice of z above we know $x'+y'\leq z$. Suppose $x'+y'<z$. Then

$$\begin{aligned} n=\mathrm{Pair}(x',y')=\frac{(x'+y')(x'+y'+1)}{2}+x'\leq\frac{(z-1)z}{2}+z-1<\\ <\frac{z(z+1)}{2}\leq\mathrm{Pair}(x,y)=n,\ \text{ a contradiction.}\end{aligned}$$

Thus $x'+y'=z$, which implies $x'=n-\frac{(x'+y')(x'+y'+1)}{2}=n-\frac{(x+y)(x+y+1)}{2}=x$ and then $y'=(x'+y')-x'=(x+y)-x=y$. □

1.5.7. **Size of products.**
If X,Y are nonempty sets and at least one of them is infinite, then

$$\mathrm{card}(X\times Y)=\max\{\mathrm{card}(X),\mathrm{card}(Y)\}.$$

Proof. [this proof is not examinable] We may assume that $\mathrm{card}(Y)\leq\mathrm{card}(X)$, and so X is infinite. Since $\mathrm{card}(X)\leq\mathrm{card}(X\times Y)\leq\mathrm{card}(X\times X)$ it suffices to show that $\mathrm{card}(X\times X)=\mathrm{card}(X)$, i.e., we need to show that there is a bijection $X\times X\longrightarrow X$.

We will apply Zorn's lemma to the following poset. Let

$$\mathscr{S}:=\{(A,f)\mid A\subseteq X\text{ and }f:A\times A\longrightarrow A\text{ is a bijection}\}$$

and consider the relation

$$(A,f)\ \leqq (B,g):\Longleftrightarrow\ A\subseteq B\text{ and }g|_{A\times A}=f.$$

It is straightforward to see that $\leqq$ is a partial order on $\mathscr{S}$. Obviously $\mathscr{S}$ is not empty (consider singleton sets).

Now, if $\mathscr{K}\subseteq\mathscr{S}$ is a chain for $\leqq$, then $(\bigcup_{(A,f)\in\mathscr{K}}A,\bigcup_{(A,f)\in\mathscr{K}}f)$ is an upper bound for $\mathscr{K}$ in $\mathscr{S}$. Here $\bigcup_{(A,f)\in\mathscr{K}}f$ stands for the common extension of all the f when (A,f) runs through the elements of $\mathscr{K}$.[13] Notice that this common extension is indeed defined on the product $\bigcup_{(A,f)\in\mathscr{K}}A\times\bigcup_{(A,f)\in\mathscr{K}}A$.

Therefore, by Zorn's lemma, there is a maximal element $(A.f)$ in $(\mathscr{S},\leqq)$. The set A must be infinite, because otherwise A has to be a singleton and then we could use 1.5.6 to find a larger element in $\mathscr{S}$ above (A,f). [14]

Claim 1. If $n\in\mathbb{N}$ and $A_1,\ldots,A_n$ are sets with $\mathrm{card}(A_i)\leq\mathrm{card}(A)$ for all i, then $\mathrm{card}(A_1\cup\ldots\cup A_n)\leq\mathrm{card}(A)$.

[13]If we consider functions as sets by identifying a function with its graph, then the graph of the common extension is indeed the union of the graphs of the functions in the family.

[14]It should be remarked here that the maximality of (A,f) in $\mathscr{S}$ will not enable us to prove that $A=X$; for example, X could just have one more element than A. However, the maximality of (A,f) in $\mathscr{S}$ implies that A must be "big" in X, see claim 2.

Proof of claim 1. We have

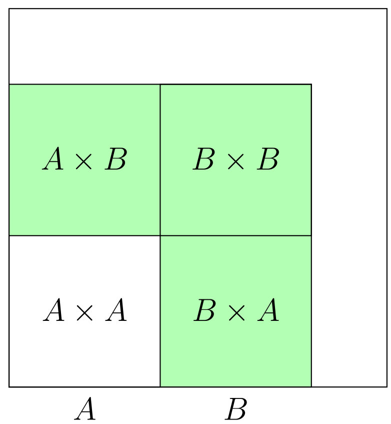
$$\begin{aligned}\operatorname{card}(A_1 \cup \ldots \cup A_n) &\leq \operatorname{card}(\{1,\ldots,n\} \times A), \text{ because there is an injective map} \\ &\qquad\qquad\qquad A_1 \cup \ldots \cup A_n \longrightarrow \{1,\ldots,n\} \times A \\ &\leq \operatorname{card}(A \times A), \text{ because } A \text{ is infinite, hence there} \\ &\qquad\qquad\qquad \text{is an injective map } \{1,\ldots,n\} \times A \longrightarrow A \times A \\ &= \operatorname{card}(A), \text{ because } f : A \times A \longrightarrow A \text{ is bijective.}\end{aligned}$$

We conclude that $\operatorname{card}(A_1 \cup \ldots \cup A_n) \leq \operatorname{card}(A)$. $\diamond$

We will now use the maximality of (A, f) in $\mathscr{S}$ to show that A is "big" in X:

Claim 2. $\operatorname{card}(X \setminus A) < \operatorname{card}(A)$.

Proof. Suppose for a contradiction that this is not the case. Then $\operatorname{card}(A) \leq \operatorname{card}(X \setminus A)$ and therefore there is a subset B of $X \setminus A$ with $\operatorname{card}(B) = \operatorname{card}(A)$; for example one can choose B as the image of an injective map $A \longrightarrow X \setminus A$. Now look at the following drawing of $X \times X$:



Since $\operatorname{card}(A \times A) = A$ and $\operatorname{card}(A) = \operatorname{card}(B)$ we also know $\operatorname{card}(B \times B) = \operatorname{card}(A \times B) = \operatorname{card}(B \times A) = \operatorname{card}(B)$. Let

$$C = (B \times B) \cup (A \times B) \cup (B \times A) \text{ (the green area).}$$

Using claim 1 (with $n = 3$) it follows that $\operatorname{card}(C) = \operatorname{card}(A) = \operatorname{card}(B)$. Hence there is a bijection $g : C \longrightarrow B$.

Since $(A \cup B) \times (A \cup B)$ is the disjoint union of $A \times A$ and C, we may define a map $h : (A \cup B) \times (A \cup B) \longrightarrow A \cup B$ by

$$h(x) := \begin{cases} f(x) & \text{if } x \in A \times A, \\ g(x) & \text{if } x \in C. \end{cases}$$

Since $f : A \times A \longrightarrow A$ and $g : C \longrightarrow B$ are bijections, also h is a bijection. But h extends f by definition. This shows that $(A, f) \leqslant (A \cup B, h)$, which contradicts the maximality of (A, f) in $(\mathscr{S}, \leqslant)$. $\diamond$

Hence by claim 2, the set $D = X \setminus A$ has cardinality $\leq \operatorname{card}(A)$. Since

$$X \times X = (A \times A) \cup (A \times D) \cup (D \times A) \cup (D \times D)$$

and each of the four sets on the right hand side has cardinality $\leq \mathrm{card}(A)$ we may use claim 1 again to deduce that $\mathrm{card}(X \times X) \leq \mathrm{card}(A) \leq \mathrm{card}(X)$. □

1.5.8. *Example.* $\mathrm{card}(\mathbb{C}) = \mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathfrak{P}(\mathbb{Q})) = \mathrm{card}(\mathfrak{P}(\mathbb{N}))$.

Proof. $\mathrm{card}(\mathbb{C}) = \mathrm{card}(\mathbb{R})$ follows from 1.5.7, since $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ (as sets). Since $\mathbb{Q}$ is countable (see level 1 material to find a bijection between $\mathbb{N}$ and $\mathbb{Q}$, or argue with a surjection $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Q}$) we know $\mathrm{card}(\mathfrak{P}(\mathbb{Q})) = \mathrm{card}(\mathfrak{P}(\mathbb{N}))$. Thus, by the Theorem of Bernstein, it suffices to show that

(a) $\mathrm{card}(\mathbb{R}) \leq \mathrm{card}(\mathfrak{P}(\mathbb{Q}))$ and
(b) $\mathrm{card}(\mathfrak{P}(\mathbb{N})) \leq \mathrm{card}(\mathbb{R})$.

(a). For $r \in \mathbb{R}$ let $f(r) = \{q \in \mathbb{Q} \mid q < r\}$. Then $f(r) \neq f(s)$ if $r \neq s \in \mathbb{R}$, because between two real numbers there is a rational number. Hence we have defined an injective map $f : \mathbb{R} \longrightarrow \mathfrak{P}(\mathbb{Q})$, which shows (a) (by 1.5.2).

(b) For an infinite subset S of $\mathbb{N}$ define

$$g(S) = \sum_{n=1}^{\infty} \frac{a_n}{3^n}, \text{ where } a_n = \begin{cases} 1 & \text{if } n \in S, \\ 0 & \text{if } n \notin S. \end{cases}$$

From real analysis we know that $g(S) \neq g(T)$ for all $S \neq T \subseteq \mathbb{N}$. Hence we have defined an injective map $g : \mathfrak{P}(\mathbb{N}) \longrightarrow \mathbb{R}$, which shows (a) (by 1.5.2).

Why did we choose the denominator 3^n in the definition of g and not 2^n? □

The most important application of 1.5.7 is the following.

1.5.9**. Size of arbitrary unions**
Let I be an index set and for each $i \in I$ let X_i be a set. Let κ be an infinite cardinal with $\mathrm{card}(X_i) \leq \kappa$ *for all i. Then*

$$\mathrm{card}(\bigcup_{i \in I} X_i) \leq \max\{\mathrm{card}(I), \kappa\}.$$

Proof. Since $\mathrm{card}(X_i) \leq \kappa$, there is a surjective map $f_i : \kappa \twoheadrightarrow X_i$ for each $i \in I$ (use 1.5.2 and observe that we may assume $X_i \neq \emptyset$). We define a map $f : I \times \kappa \longrightarrow \bigcup_{i \in I} X_i$ by $f(i, \alpha) := f_i(\alpha)$. Obviously f is surjective. By 1.5.2 again, we know

$$\mathrm{card}(\bigcup_{i \in I} X_i) \leq \mathrm{card}(I \times \kappa).$$

But now, 1.5.7 says $\mathrm{card}(I \times \kappa) = \max\{\mathrm{card}(I), \kappa\}$ showing the assertion. □

A particular case of 1.5.9 is

1.5.10. **Corollary.** *If X and Y are sets and at least one them is infinite, then* $\mathrm{card}(X \cup Y) = \max\{\mathrm{card}(X), \mathrm{card}(Y)\}$.

1.5.11. **Corollary.** *If X is an infinite set, then*

$$\mathrm{card}(\mathrm{Maps}(X, X)) = \mathrm{card}(\mathfrak{P}(X)),$$

where $\mathrm{Maps}(X, X)$ *denotes the set of all maps $X \longrightarrow X$.*

Remark: The important part here is the inequality $\leq$.

Proof. The inequality $\mathrm{card}(\mathrm{Maps}(X,X)) \geq \mathrm{card}(\mathfrak{P}(X))$ follows from the fact that every subset of a set is uniquely determined by its characteristic function $X \longrightarrow \{0,1\}$; hence we may construct an injective map $\mathfrak{P}(X) \longrightarrow \mathrm{Maps}(X,X)$.
For the converse, consider the map

$$\Gamma : \mathrm{Maps}(X,X) \longrightarrow \mathfrak{P}(X \times X)$$

that sends a function $f : X \longrightarrow X$ to its graph. Γ is obviously injective. Hence

$$\mathrm{card}(\mathrm{Maps}(X,X)) \leq \mathrm{card}\,\mathfrak{P}(X \times X) = \mathrm{card}\,\mathfrak{P}(X),$$

where we use 1.5.7 for the last equality (for the implication $\mathrm{card}(X \times X) = \mathrm{card}(X) \Longrightarrow \mathrm{card}\,\mathfrak{P}(X \times X) = \mathrm{card}\,\mathfrak{P}(X)$ take inspiration from the 4th question of the list of warm-up questions for Set Theory).

□

1.5.12. *Example.* Let F be a field.

(i) Let V be an infinite F-vector space and let B be a subsets of V that generates V as a vector space. Then

$$\mathrm{card}(V) = \max\{\mathrm{card}(F), \mathrm{card}(B)\}.$$

(ii) All infinite F-vector spaces of the same size strictly bigger than $\mathrm{card}(F)$ are isomorphic.

Proof. [this proof is not examinable] (i) Let S be the set

$$S = \bigcup_{E \subseteq B \text{ finite}} \mathrm{Maps}(E,F).$$

Consider the map $\Phi : S \longrightarrow V$ defined by

$$\Phi(\sigma) = \sum_{v \in E} \sigma(v) \cdot v$$

where $\sigma : E \longrightarrow F$ and $E \subseteq B$ is finite.

As B generates V as a vector space, every element of V is a finite linear combination of elements from B. This is equivalent to saying that the map Φ is surjective. In particular, the cardinality of V is at most the cardinality of the set S.

We estimate the cardinality of S: For $E \subseteq B$ finite, the cardinality of $Maps(E,F)$ is at most $\max\{\omega, \mathrm{card}(F)\}$ as follows from 1.5.7 (notice that $Maps(E,F)$ is in bijection with F^n, where n is the size of the finite set E). Hence by 1.5.9 we know

$$\mathrm{card}(S) \leq \max\Big\{\omega, \mathrm{card}(F), \mathrm{card}(\{E \subseteq B \mid E \text{ finite}\})\Big\}.$$

Now $\mathrm{card}\{E \subseteq B \mid E \text{ finite}\} \leq \max\{\omega, \mathrm{card}(B)\}$ by question 17 and so

$$\mathrm{card}(S) \leq \max\{\omega, \mathrm{card}(F), \mathrm{card}(B)\}.$$

Since V is infinite, either F or B must be infinite. Altogether it follows

$$\mathrm{card}(V) \leq \mathrm{card}(S) \leq \max\{\mathrm{card}(F), \mathrm{card}(B)\}.$$

Since the other inequality is obvious we get (i).

(ii). Now assume V, W are infinite F-vector spaces with $\mathrm{card}(V) = \mathrm{card}(W) > \mathrm{card}(F)$. By 1.2.6, both vector spaces have a basis. Let B be a basis of V and let C be a basis of W. By (i) we have $\mathrm{card}(V) = \max\{\mathrm{card}(F), \mathrm{card}(B)\}$. Since $\mathrm{card}(V) > \mathrm{card}(F)$ this is only possible when $\mathrm{card}(V) = \mathrm{card}(B)$. The same argument applies to W and C, thus $\mathrm{card}(W) = \mathrm{card}(C)$. But $\mathrm{card}(V) = \mathrm{card}(W)$, hence $\mathrm{card}(B) = \mathrm{card}(C)$ and there is a bijection $f_0 : B \longrightarrow C$. Since B is a basis of V, there is a unique F-vector space homomorphism $f : V \longrightarrow W$ extending f_0. Since C is a basis of W, f is an F-vector space isomorphism. □

1.5.13. *Example.* [This example is not examinable.]
Here is an application of some of the results about ordinals and cardinals. We claim that there is a subset S of $\mathbb{R}^2$ that intersects every line of $\mathbb{R}^2$ in exactly two points.

Before proving this, here is some discussion. One can decompose the property of S that is asked for into two pieces by saying that

(a) S intersects each line of $\mathbb{R}^2$ in at least 2 points, and
(b) S intersects each line of $\mathbb{R}^2$ in at most 2 points (equivalently: no three points of S are colinear).

Now, if S is a set with properties (a) and (b), then S is maximal among subsets of $\mathbb{R}^2$ having property (b), because for $p \in \mathbb{R}^2 \setminus S$ and any line ℓ through p, the set S contains already two points of S. One could therefore be tempted to apply Zorn's lemma and check whether a set S that is maximal with property (b) would also satisfy (a). However this is not true. For example the unit circle satisfies (b) and any point not on the unit circle is on a line that hits the unit circle twice; hence the unit circle is maximal with property (b), but still does not satisfy (a).

Proof. Let L be the set of all lines of $\mathbb{R}^2$. Since a line is determined by two points in the plane there is surjective map $\mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow L$. Obviously there is also an injective map $\mathbb{R} \longrightarrow L$. Hence we know that $\mathrm{card}(\mathbb{R}) \le \mathrm{card}(L) \le \mathrm{card}(\mathbb{R}^4)$. By 1.5.7 we know $\mathrm{card}(\mathbb{R}) = \mathrm{card}(\mathbb{R}^4)$ and therefore we have $\mathrm{card}(L) = \mathrm{card}(\mathbb{R})$. We write $\mathfrak{c}$ for this cardinal. We fix a bijection $\mathfrak{c} \longrightarrow L, i \mapsto \ell_i$ (which we think of an enumeration). For each $i < \mathfrak{c}$ we construct a set $S_i \subseteq \mathbb{R}^2$ with the following properties.

$(a)_i$ S_i intersects each line ℓ_j with $j < i$ in at least 2 points.
$(b)_i$ No three points of S_i are colinear.
$(c)_i$ $\mathrm{card}(S_i) < \mathfrak{c}$.
$(d)_i$ If $j < i$, then $S_j \subseteq S_i$.

To start with, we choose $S_0 = \emptyset$ (or in fact any subset S_0 of $\mathbb{R}^2$ of cardinality $< \mathfrak{c}$ not containing three colinear points). If $i < \mathfrak{c}$ is a limit ordinal and for all $j < i$ we have already defined S_j with properties $(a)_j$, $(b)_j$, $(c)_j$, $(d)_j$. then we may take $S_i = \bigcup_{j<i} S_j$ and see that the conditions also hold true for i (use 1.5.9 for $(c)_i$).

Now suppose $i < \mathfrak{c}$ and S_i is already constructed with the properties above. We define S_{i+1} such that conditions $(a)_{i+1}$, $(b)_{i+1}$, $(c)_{i+1}$, $(d)_{i+1}$ hold, as follows (here $i+1$ is the successor ordinal i^*). Let L' be the set of all lines passing through two points of S_i. If $\ell_i \in L'$ then we may take $S_{i+1} = S_i$.

Hence we may assume that $\ell_i \notin L'$. By $(c)_i$ the cardinality of L' is $< \mathfrak{c}$ (using a similar argument to the one used to calculate $\mathrm{card}(L) = \mathrm{card}(\mathbb{R})$ above). Now, each of the lines in L' and any of the lines ℓ_j with $j < i$ is different from ℓ_i, hence they can only have at most one point in common with ℓ_i. We obtain that the set

$$T = \ell_i \cap \left(\bigcup_{j<i} \ell_j \cup \bigcup_{\ell \in L'} \ell \right)$$

is of cardinality $< \mathfrak{c}$. Since every line is in bijection with $\mathbb{R}$ we know that $\mathrm{card}(\ell_i) = \mathfrak{c}$. In particular $\ell_i \setminus T$ has at least two elements.

Case 1. There is some $q \in \ell_i \cap S_i$.

Take $p \in \ell_i \setminus T$ with $p \neq q$ and set $S_{i+1} = S_i \cup \{p\}$. Then $(\mathrm{a})_{i+1}$ holds. Obviously $(\mathrm{d})_{i+1}$ holds and condition $(\mathrm{c})_{i+1}$ follows from the size of sums. It remains to show $(\mathrm{b})_{i+1}$, i.e. no three points of S_{i+1} are colinear. By $(\mathrm{b})_i$ one of these points would have to be p and the other two would have to be in S_i. But then p is on a line from L' and this contradicts the choice of p.

Case 2. $\ell_i \cap S_i = \emptyset$.

Take $p, q \in \ell_i \setminus T$ with $p \neq q$ and set $S_{i+1} = S_i \cup \{p, q\}$. Then $(\mathrm{a})_{i+1}$ holds. Again, $(\mathrm{d})_{i+1}$ holds and condition $(\mathrm{c})_{i+1}$ follows from the size of sums. It remains to show $(\mathrm{b})_{i+1}$, i.e. no three points of S_{i+1} are colinear. Suppose otherwise. If p and q are both among these points, then the third point would be in $\ell_i \cap S_i = \emptyset$ as ℓ_i is the line through p and q. This is excluded in case 2. By $(\mathrm{b})_i$ one of the three points would have to be p or q. Hence we may assume that p is among these three points and the other two points are in S_i. But as in case 1, this contradicts the choice of p.

The two cases finish the construction. But now we see that the set $S = \bigcup_{i<\mathfrak{c}} S_i$ satisfies condition (a) and (b). $\square$

1.6. **A first attempt at axiomatic set theory.**

So far, we have done set theory without much worry about ground assumptions; this is often referred to as *naïve set theory*. To motivate what is coming in the second part of the course, we briefly consider *axiomatic set theory*.

First, consider the question 'what is it that gives mathematics a certainty that other subjects might appear to lack?'. An answer might be that we prove our results. But this raises the question of what it means to give a proof. One possible answer to this is contained in the second half of the course. But even given that proofs 'preserve truth', that is, lead from true hypotheses to true conclusions, there remains the question of which hypotheses we should start from. Such hypotheses are called *axioms*.

Historically, the introduction of axioms for set theory was motivated by certain apparent paradoxes in the naïve approach, and by a desire to make clear exactly what the assumptions were underlying Zermelo's proof that every set could be well-ordered.

Perhaps the most famous of the paradoxes is *Russell's Paradox*, which goes as follows. Consider the collection

$$R = \{x : x \text{ is a set and } x \notin x\}.$$

If R is a set, we see that $R \in R$ if and only if $R \notin R$, which is impossible. So R cannot be a set. But it looks like one...

For a similar issue, consider

$$V = \{x : x \text{ is a set}\}.$$

If V is a set, then by Theorem 1.5.4 on the size of the powerset, there is no injective function $\mathfrak{P}(V) \to V$. But $\mathfrak{P}(V) \subseteq V$. So V cannot be a set.

Finally, let us consider the collection

$$\mathrm{On} = \{\alpha : \alpha \text{ is an ordinal }\}.$$

Suppose that On is a set. By 1.4.2, On is transitive and by the ordinal minimization principle 1.4.11 it is strictly well-ordered by membership. So On is itself an ordinal. But then $\mathrm{On} < \mathrm{On}$, contradicting $\mathrm{On} = \mathrm{On}$.

These examples have something in common: they consider 'very large' collections. Why should they be sets in the first place? When we think these examples are sets, it is perhaps because of something like the following:

Naïve comprehension axiom For any property Q of sets the collection

$$\{X : X \text{ has property } Q\}$$

is a set. So this axiom – a priori – cannot stand by Russell's paradox.

To try to avoid the problem with 'very large' collections, we could replace this with something like:

Restricted comprehension If X is a set and Q is a property of sets then the collection

$$\{x \in X : x \text{ has property } Q\}$$

is a set.

The difference here is that we are picking out a subcollection of a set X, rather than all sets satisfying some property. The idea is that if X is 'small enough' to be a set, then we should not get into trouble declaring some subcollection of X a set.

However, there is a second problem here. What exactly do we mean by 'a property of sets'. To see the issue with this, consider the property $Q(n)$ of sets saying that

n is a natural number, which can be defined
by using at most 1000 letters of the roman alphabet.

Let us consider the set $X = \{n : Q(n) \text{ holds}\}$. Since there are only finitely many natural numbers that can be defined using at most 1000 letters of the roman alphabet, the set X is finite. Hence $\mathbb{N} \setminus X$ is nonempty and thus there is a smallest element k of $\mathbb{N} \setminus X$. Is $k \in X$[15]? This is a version of *Berry's paradox*.

To avoid this issue, we may introduce logical formulas and say that our property has to be given by some such formula, in a certain language. We will start this process very soon. This will also allow us to be precise about so called *formal proofs*.

At the end of the course, we will see an axiomatisation of set theory. In addition to a version of the restricted comprehension axiom mentioned above, we will have various other axioms. The full list appears later, but it will include axioms such as 'If x is a set then so is its powerset', and 'there is an infinite set'. The most involved axiom will turn out to be the *Axiom of Replacement*. This allows us to build, for example, large ordinals. We secretly used this in the proof that every well-ordered set is isomorphic to an ordinal. Our axioms together will give us the system ZF (*Zermelo-Fraenkel set theory*). We will then add the *Axiom of Choice*, to get ZFC. See question 21 on the example sheet for more on the Axiom of Choice.

A further advantage of the axiomatic approach is that we can treat these formal set theories as topics for mathematical study, and prove theorems about these theories. For example,

Theorem. (Gödel) If ZF is consistent (that is, there is no contradiction provable from the axioms of ZF) then also ZFC is consistent.

But now we may also ask if we can prove in ZF that ZF is consistent.

Theorem. (Gödel, [GoedelStanford]) If ZF is consistent then ZF does **not** prove 'ZF is consistent'.

These theorems are (some way) beyond the scope of the course, but they might provide further motivation for the idea of axiomatising set theory, and for the upcoming development of formal logic leading to mathematical logic.

[15]Recall that natural numbers are sets: they are the finite ordinals

2. Predicate Logic

We begin by giving an overview, which is meant to give ideas, rather than to be precise.

Predicate logic deals with formal languages in which (in principle) all of mathematics can be formulated, together with their semantics (i.e. the meaning attached to certain expressions of such a language). Languages are designed with the intention of forming statements about "sets with structure" (which will be on the semantic side). We will prove rigorous statements about these languages and this is important to keep in mind.

To name two examples of such sets-with-structure one may think of a group (a set whose structure is given by the group operation), or a poset (a set whose structure is given by a partial order). In particular, we will be able to talk about elements of sets. We will have variables (or rather variable symbols) $x, y, x_1, x_2, \ldots, y_1, y_2, \ldots$ which, when meaning is attached to them, range over a given set. We will also have quantifiers $\forall, \exists$ ('for all' and 'there exists'). So a formula in Predicate Logic could, for example, begin with $\forall x \exists y \cdots$. What we are allowed to include in the formula will depend on the structure we are studying. We will have different languages for different types of structures. We give a language by choosing certain symbols which stand for *constants*, certain symbols standing for *relations* and certain symbols standing for *functions*.

Let us give some examples. Our sets-with-structure will always include $=$ (formally this is a 2-ary – aka *binary* – relation) and we will always have a binary relation **symbol** in our language, denoted by $\doteq$ (notice: the symbol $\doteq$ here should be understood as a letter only and no meaning is supposed to be attached to it - only when it comes to the interpretation of these symbols we will get to a binary relation). We might also have, for instance, an ordering, e.g. $\leq$ in the integers $\mathbb{Z}$ or the real numbers $\mathbb{R}$. This is another binary relation, and if we wanted to study it we could include another binary relation symbol in our language. If we wanted to talk about arithmetic in $\mathbb{Z}$ or $\mathbb{R}$ we could add binary function symbols $+$ and $\times$, to be interpreted as addition and multiplication, and perhaps constant symbols to be interpreted as 0 and 1.

Before getting onto these, we start by looking at the basic language, which is common to all languages and which serves here as a warmup for the general case (which starts in section 2.3).

2.1. **Warmup I: The Basic Language.**

The material here will be done in extended and rigorous form starting with section 2.3. Here we focus mainly on the syntactic side of the simplest language, which will also be present in the general case.

2.1.1. **Definition.** The **basic language** $\mathscr{L}_\emptyset$ has the following **letters**:

- The propositional connectives $\to, \neg$ as well as brackets $)$ and $($.
- The universal quantifier symbol $\forall$.
- Variable symbols $\ldots, v_0, v_1, v_2, \ldots$.
- The equality symbol $\doteq$.

Note that these letters are intended to have meaning later, but at the moment they should be read at a purely symbolic level. This can be compared to natural languages, which have letters making up an alphabet and have in the first place no meaning. (In our context the letters could also be understood as an object that one could feed to a computer.) In order to distinguish them from their use in the meta language we color them in red at the moment; this will stop at some point. The dot in $\doteq$ will remain later and remind us that this is the symbol of the language.

One might wonder why the propositional symbols $\wedge$, $\vee$ and the existential quantifier $\exists$ are not listed here. The reason is that these will be defined in terms of the above, but on a more practical side it is less work later in proofs to deal with a smaller language.

2.1.2. **Definition.** A **term** of $\mathscr{L}_\emptyset$ is just a variable[16], and the **free variable** of a term is the variable that makes up the term: We define $\mathrm{Fr}(x) = \{x\}$ for any variable x.

2.1.3. **Definition.** An **atomic formula** of $\mathscr{L}_\emptyset$ is an expression (formally: a finite sequence of letters) $s \doteq t$ where s, t are terms. We define

$$\mathrm{Fr}(s \doteq t) = \mathrm{Fr}(s) \cup \mathrm{Fr}(t).$$

Notice that $\doteq$ here is just a letter of our language, which has no other meaning (at the moment), whereas the symbol "$=$" here is used in the usual mathematical sense, i.e. we are expressing that $\mathrm{Fr}(s \doteq t)$ is equal to $\mathrm{Fr}(s) \cup \mathrm{Fr}(t)$ (by definition).

We define the **formulas** of $\mathscr{L}_\emptyset$, and their free variables, as follows:

- Every atomic formula is a formula.
- If φ is a formula then so is $(\neg\varphi)$, and $\mathrm{Fr}((\neg\varphi)) = \mathrm{Fr}(\varphi)$.

  Notice that in the expression $\mathrm{Fr}((\neg\varphi))$ the inner brackets are formal symbols of the language, whereas the outer brackets are meta theoretical brackets as used in mathematics all the time.
- If φ, ψ are formulas then so is $(\varphi \to \psi)$ and $\mathrm{Fr}((\varphi \to \psi)) = \mathrm{Fr}(\varphi) \cup \mathrm{Fr}(\psi)$.
- If φ is a formula and x is a variable symbol[17]. then $(\forall x\, \varphi)$ is a formula and $\mathrm{Fr}((\forall x \varphi)) = \mathrm{Fr}(\varphi) \setminus \{x\}$.

[16]This looks a bit strange at the moment, but for more complex languages this definition will be extended.

[17]So x stands for one of the v_0, v_1, v_2,.... This should be compared with the handling of objects in mathematics in general. For example when we want to prove a statement about integers

- Nothing else is a formula of $\mathscr{L}_\emptyset$.

The set of all $\mathscr{L}_\emptyset$-formulas is denoted by $\mathrm{Fml}(\mathscr{L}_\emptyset)$. A **sentence** of $\mathscr{L}_\emptyset$ is a formula without free variables and the set of all $\mathscr{L}_\emptyset$-sentences is denoted by $\mathrm{Sen}(\mathscr{L}_\emptyset)$:

$$\mathrm{Sen}(\mathscr{L}_\emptyset) = \{\sigma \in \mathrm{Fml}(\mathscr{L}_\emptyset) \mid \mathrm{Fr}(\sigma) = \emptyset\}.$$

We will drop brackets if the expression is unambiguous to help readability at the moment, but for formal proofs of statements about formulas one has to invoke brackets as defined above.

2.1.4. **Examples and Abbreviations** Here are some examples of formulas of $\mathscr{L}_\emptyset$ together with their free variables.

(i) $v_2 \doteq v_7$ is a formula, with free variables v_2, v_7. We could have also written: "$x \doteq y$ is a formula", with free variables x, y. So here we would use x, y as meta theoretic symbol for one of the v_0, v_1, v_2,… .

When we use x, y, z we always mean *distinct* variables.

(ii) $\forall x\, x \doteq y$ is a formula where x, y are variables; we have dropped outer brackets for readability. The only free variable is y.

(iii) Some abbreviations: For variables x, y we write $x \neq y$ instead of $\neg x \doteq y$.

For formulas φ, ψ we write

$$\varphi \vee \psi \text{ for } (\neg\varphi) \rightarrow \psi \qquad \text{("disjunction of } \varphi \text{ and } \psi\text{")}$$
$$\varphi \wedge \psi \text{ for } \neg(\varphi \rightarrow (\neg\psi)) \qquad \text{("conjunction of } \varphi \text{ and } \psi\text{"), and}$$
$$\varphi \leftrightarrow \psi \text{ for } (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$

In the meta theory we will use $\iff$ to indicate equivalence of statements, so again, $\leftrightarrow$ has to be understood as an abbreviation in the syntax of the language. In 2.2.6 we will make this explicit.

If φ is a formula and x is a variable we write

$$\exists x\, \varphi \text{ for } \neg(\forall x(\neg\varphi)).$$

For better readability we could have written (and we will write) $\neg\forall x \neg\varphi$.

Strictly speaking we should not color these abbreviations because they are not symbols of the language, but we still do it to alert the reader that this is just a syntactical expression and not a meta theoretic assertion.

(iv) For example $\forall x(x \doteq y \wedge y \neq z)$ is a formula with free variables y, z and $\exists x \forall y(x \doteq y \wedge y \neq z)$ is a formula with free variable z.

(v) $\forall x \forall y \forall z \exists u(\neg((u \neq x \wedge u \neq y) \rightarrow u \doteq z))$ is a formula with no free variables, that is, it is a sentence. Try to figure out what this sentence says. Although we have not yet defined meaning for formulas you can try to guess what the sentence expresses. See question 22 on the example sheet.

---

we say "Let x be an integer…", but no actual integer might appear in that proof. In our situation, the objects we are dealing with are the v_0, v_1, v_2,… and x ranges over them.

2.1.5**. How to understand the definition of a formula** The definition of formulas is inductive and each formula has a corresponding construction tree. Any formula that occurs in the tree for φ is called a **subformula** of φ. Each formula has a principle connective (and there is a unique readability theorem, to be formulated later). Here is an example. Consider the formula $\exists x \forall y(x \doteq y \rightarrow y \neq z)$. This is an abbreviation for $(\neg \forall x(\neg \forall y(x \doteq y \rightarrow y \neq z)))$. If we dismantle its construction we get the following tree.

- $\exists x \forall y(x \doteq y \rightarrow y \neq z)$
  - $\forall x(\neg \forall y(x \doteq y \rightarrow y \neq z))$
    - $\neg \forall y(x \doteq y \rightarrow y \neq z)$
      - $\forall y(x \doteq y \rightarrow y \neq z)$
        - $x \doteq y \rightarrow y \neq z$
          - $x \doteq y$
          - $(\neg y \doteq z)$
            - $y \doteq z$

We can see that for instance $y \doteq z$ and $\forall y(x \doteq y \rightarrow y \neq z)$ are subformulas of $\exists x \forall y(x \doteq y \rightarrow y \neq z)$ but that $\exists x(x \doteq y \rightarrow y \neq z)$ is not.

2.1.6. **Definition.** We define the **free occurrences** of a variable x in a formula as follows:

(1) Every occurrence of x in any atomic formula is free.
(2) The free occurrences of x in $(\neg \varphi)$ are the free occurrences of x in φ.
(3) The free occurrences of x in $(\varphi \rightarrow \psi)$ are the free occurrences of x in φ together with the free occurrences of x in ψ.
(4) There are no free occurrences of x in $\forall x \varphi$.

If ψ is a formula that has a subformula of the form $(Qx\varphi)$ where Q is either $\forall$ or $\exists$, we refer to $(Qx\varphi)$ as the **scope** of Qx. Any free occurrence of x in φ is said to be **bound** by Qx.

2.1.7. *Examples.*

(i) In the formula $\exists x(x \doteq y \wedge y \neq z) \wedge \forall z(x \doteq z)$ the variable y is free. The first occurrence of z is free, the second is bound by $\forall z$. The second occurrence of x is free, the first is bound by $\exists x$. The scope of the first $\exists x$ is the subformula $\exists x(x \doteq y \wedge y \neq z)$, the scope of $\forall z$ is $\forall z(x \doteq z)$ (dropping brackets for readability).
(ii) Consider the formula

$$\exists x((\forall x(x \doteq x)) \rightarrow x \doteq x).$$

The scope of the quantifier $\exists x$ is the entire formula. But the first $x \doteq x$ here lies in the scope of $\forall x$, so these xs are bound by $\forall x$, while the second $x \doteq x$ are bound by $\exists x$.

Instead of this formula, we could also write

$$\exists x(\forall y(y \doteq y) \rightarrow x \doteq x).$$

This formula is different, but it has the same meaning (it is logically equivalent, to be defined properly later). It is also much easier to read!

2.2. **Warmup II: Interpreting formulas in the basic language.**

We now come to the semantics of the basic language, i.e. we will give meaning to the formulas of $\mathscr{L}_\emptyset$. First some informal explanations.

2.2.1**.** Given a formula φ of the basic language, it does in general not make sense to ask whether it is true or false for two reasons:

(a) When φ has free variables, e.g. φ could be $x \doteq y$, then we need to know what x and y stand for. Hence at least we need to assume that φ has no free variables, i.e φ is a sentence.

(b) When φ is a sentence, e.g. φ could be $\forall x \forall y(x \doteq y)$, then we need to know the range of the quantifiers (we want to read "$\forall$" as "for all".)

In order to address (b) we need to a fix a **base set** (aka **universe** or **domain**) U. For example if U is the set $\mathbb{N}$ of natural numbers, then the formula $\forall x \forall y(x \doteq y)$ is false <u>in U</u> if we read the quantifier $\forall x$ as "For all $x \in \mathbb{N}$". If U is a set with exactly one element, then the formula $\forall x \forall y(x \doteq y)$ is true <u>in U</u>. Hence truth of a sentence depends on the chosen universe (at least). Of course one might also ask, whether a sentence is true in all universes (or in all universes that have some specific properties) and this will be addressed in great generality later.

When defining truth in (b) we are naturally lead to address the issue in (a). Suppose φ is a formula which has at most one free variable x and let ψ be the sentence $\forall x\, \varphi$. Now let U be a set. If we want to know whether ψ is true in U we want to interpret ψ in U as

$\varphi(x)$ is true in U when we "replace" x by a.[18]

This motivates the central definition of the semantics of Predicate Logic (for the basic language):

[18]Observe that $\varphi(a)$ does not belong to the basic language, because the element a of U is in general not a letter. Hence we cannot just literally replace x by a and say "$\varphi(a)$ is true in U" without defining what that means.

2.2.2. **Definition.** A **structure** of the basic language is a `nonempty` set $\mathscr{M}$.[19]

Given a structure $\mathscr{M}$ in the basic language and a formula φ of the basic language with at most free variables $x_1, \dots, x_n$ (hence $\mathrm{Fr}(\varphi) \subseteq \{x_1, \dots, x_n\}$), and elements $a_1, \dots, a_n$ of $\mathscr{M}$, we define

$$(\dagger) \qquad \varphi \text{ is true in } \mathscr{M} \text{ at } a_1, \dots, a_n\text{[20]},$$

and write this as

$$\mathscr{M} \models \varphi(a_1, \dots, a_n),$$

by induction on the construction of φ, following definition 2.1.3:

(i) If φ is an atomic formula of the form $x_1 \doteq x_2$ with variables x_1, x_2 then

$$\text{“}\mathscr{M} \models \varphi(a_1, a_2)\text{” is defined as } a_1 = a_2.$$

(ii) For the induction step we take $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$ and a variable x. Then

$$\text{“}\mathscr{M} \models (\neg\varphi)(a_1, \dots, a_n)\text{”}$$

is defined as

“$\mathscr{M} \not\models \varphi(a_1, \dots, a_n)$”, in other words “$\mathscr{M} \models \varphi(a_1, \dots, a_n)$ does not hold”

$$\text{“}\mathscr{M} \models (\varphi \rightarrow \psi)(a_1, \dots, a_n)\text{”}$$

is defined as

“If $\mathscr{M} \models \varphi(a_1, \dots, a_n)$ then $\mathscr{M} \models \psi(a_1, \dots, a_n)$”.

$$\text{“}\mathscr{M} \models (\forall x \varphi)(a_1, \dots, a_n)\text{”}$$

is defined as

$$\begin{cases} \mathscr{M} \models \varphi(a_1, \dots, a_n), & \text{in the case when } x \text{ is not among the } x_i \\ \mathscr{M} \models \varphi(a_1, \dots, \underbrace{b}_{i^{\text{th}} \text{ position}}, \dots, a_n) \text{ for all } b \in \mathscr{M}, & \text{if } x = x_i. \end{cases}$$

(iii) If φ is a sentence of $\mathscr{L}_\emptyset$, and φ is true in $\mathscr{M}$, then we say that $\mathscr{M}$ is a **model** of φ, in symbols: $\mathscr{M} \models \varphi$.

(iv) If T is a set of $\mathscr{L}$-sentences, then we say that $\mathscr{M} \models T$ if $\mathscr{M} \models \varphi$ for all $\varphi \in T$.

This definition is referred to as “truth definition in the basic language”.

---

[19]This definition again looks a bit strange but for general languages the notion of a structure is rather complex and central in the course; so here we are looking at the simplest instance. At the moment $\mathscr{M}$ just plays the role of the set U in the terminology of 2.2.1.

[20]We also say “φ holds/is true in $\mathscr{M}$ at $a_1, \dots, a_n$”, or, “$\mathscr{M}$ satisfies φ at $a_1, \dots, a_n$”.

2.2.3. *Remark.* The definition of "$\mathscr{M} \models (\forall x\varphi)(a_1, \ldots, a_n)$" in 2.2.2(ii) could have also been

$$\text{"}\mathscr{M} \models (\forall x_i\varphi)(a_1, \ldots, a_n)\text{"}$$
$$\text{is defined as}$$
$$\mathscr{M} \models \varphi(a_1, \ldots, \underbrace{b}_{i^{\text{th}} \text{ position}}, \ldots, a_n) \text{ for all } b \in |\mathscr{M}|$$

Why would that also cover the case "$\mathscr{M} \models (\forall x\varphi)(a_1, \ldots, a_n)$" for $x \notin \{x_1, \ldots, x_n\}$? For an answer, see the solution to the additional question in question 25 of the example sheet.

We will now drop the coloring of the letters (and the abbreviations) in formulas of the basic language. We also use brackets not in accordance to the formal definition in order to increase readability. After working through the material in section 2.1 you should be able to write down the formal expression in each case. Please keep in mind that we will develop mathematics of these formulas and in proofs we have to refer to the precise syntactic definitions.

2.2.4. *Examples.* Let φ be the formula $\forall x\, x \doteq y$, hence φ has exactly one free variable, namely y.

(i) Let $\mathscr{M}$ be a structure of the basic language and let $a \in \mathscr{M}$. Is φ true in $\mathscr{M}$ at a, in other words do we have

$$\mathscr{M} \models \varphi(a)\ ?$$

Answer: This depends on what $\mathscr{M}$ is. If $\mathscr{M}$ has exactly one element, then $\mathscr{M} \models \varphi(a)$ where a is the unique element of $\mathscr{M}$. The reason is that $\mathscr{M} \models \varphi(a)$ is defined in 2.2.2 by

$$\text{"For all } b \in \mathscr{M} \text{ we have } b = a\text{"},$$

which is clearly true since $\mathscr{M} = \{a\}$.

On the other hand if $\mathscr{M}$ has at least two elements, then $\mathscr{M} \models \varphi(a)$ fails, no matter what we choose for $a \in \mathscr{M}$: Since $\mathscr{M}$ has an element different from a we see that it is not the case that

$$\text{"For all } b \in \mathscr{M} \text{ we have } b = a\text{"}.$$

(ii) The reasoning in (i) shows that for every $\mathscr{L}_\emptyset$-structure $\mathscr{M}$, if there is some $a \in \mathscr{M}$ with $\mathscr{M} \models \varphi(a)$ then for any other element $a' \in \mathscr{M}$ we also have $\mathscr{M} \models \varphi(a')$. In other words, the truth of $\varphi(x)$ in a structure at some element is only dependent on the structure, not on the choice of the element. This will generally be an exceptional case. Formally the property says that every structure $\mathscr{M}$ is a model of the sentence

$$\forall y \forall z \Big(\forall x(x \doteq y) \leftrightarrow \forall x(x \doteq z)\Big).$$

Later we will show that every structure $\mathscr{M}$ is a model of this sentence for every choice of a formula φ of the basic language in at most one variable. Do you see a way to prove this?

2.2.5. *Example.* Let ψ be the formula $\forall x\,(x \neq y \to x \doteq z)$. Hence ψ has two free variables, namely y, z. Let $\mathscr{M}$ be a structure of the basic language and let $a, b \in \mathscr{M}$. When is ψ true in $\mathscr{M}$ at the tuple (a, b), in other words when do we have

$$\mathscr{M} \models \psi(a, b)\ ?$$

This again depends on the choice of $\mathscr{M}$, but this time it also depends on the choice of a and b. See question 24 of the example sheet for a guided discussion with examples.

2.2.6. **Meaning of the abbreviations** Let $\mathscr{M}$ be a structure in the basic language and let φ, ψ be formulas of the basic language with at most free variables $x_1, \ldots, x_n$ and elements $a_1, \ldots, a_n$ of $\mathscr{M}$. Then

(i) $\mathscr{M} \models (\varphi \vee \psi)(a_1, \ldots, a_n)$ if and only if the following condition holds:

$$\mathscr{M} \models \varphi(a_1, \ldots, a_n) \text{ or } \mathscr{M} \models \psi(a_1, \ldots, a_n).$$

(ii) $\mathscr{M} \models (\varphi \wedge \psi)(a_1, \ldots, a_n)$ if and only if the following condition holds:

$$\mathscr{M} \models \varphi(a_1, \ldots, a_n) \text{ and } \mathscr{M} \models \psi(a_1, \ldots, a_n).$$

(iii) $\mathscr{M} \models (\varphi \leftrightarrow \psi)(a_1, \ldots, a_n)$ if and only if the following condition holds:

$$\mathscr{M} \models \varphi(a_1, \ldots, a_n) \iff \mathscr{M} \models \psi(a_1, \ldots, a_n).$$

Notice that $\leftrightarrow$ is just a syntactic construction with no further meaning, whereas the symbol $\iff$ is the standard equivalence of mathematical statements (just like the expression "if and only if").

(iv) For $i \in \{1, \ldots, n\}$ we have $\mathscr{M} \models \exists x_i \varphi(a_1, \ldots, a_n)$ if and only if there is some $b \in \mathscr{M}$ such that

$$\mathscr{M} \models \varphi(a_1, \ldots, \underbrace{b}_{i^{\text{th}} \text{ position}}, \ldots, a_n)$$

Proof. This is done in question 25 of the example sheet. □

2.3. **Languages and formulas.**

In this section we define what is a first order language in full generality, usually denoted by $\mathscr{L}$. Such a language consists of an *alphabet* – extending the basic language – which will be used to form finite sequences (strings) of elements of that alphabet, built according to certain rules; these strings will be called *formulas*.

First a brief explanation how we want to extend the basic language. There is not a lot we can say with our basic language. For example consider the expression

$$\forall n\ 2 \leq n \to \exists p\ \Big(2 \leq p\ \wedge\ p|n\ \wedge\ \forall k \forall m\ (p = k \cdot m\ \to\ p = k\ \vee\ p = m)\Big).$$

When quantifiers are read as ranging over natural numbers, it expresses that every natural number greater or equal to 2 is divisible by a prime number. The symbols that are not in the basic language are

$$2 \quad \leq \quad | \quad \cdot$$

These symbols are thus interpreted as follows:

2 is a symbol for a an element, we will say 'constant symbol'.
$\leq$ is a symbol for a relation, we will say 'relation symbol'.
$|$ is a symbol for another relation.
$\cdot$ is a symbol for a function, we will say 'function symbol'.

Most of mathematics is expressed with naming elements (or 'constants'), relations and functions. Hence in order to get a more expressive logic and capture these objects in the language, we now add symbols for constants, relations and functions.

2.3.1**. Why do we set up languages?** The goal in this chapter – and the fundamental theorems of Predicate Logic – is to explain Soundness and Completeness, which says the following (in an informal way):

Using any language (as defined below), we can define an axiom system, consisting of sentences in the language, together with rules about what is a *formal* proof, such that

(1) all formal proofs produce true statements when fed with true statements (this is called "Soundness").
(2) the axioms system is complete in the sense that every mathematically true statement of our language is provable in the system (this is called "Completeness")

We then obviously also need to define what we mean by "truth", which will be done via "truth in $\mathscr{L}$-structures"; we have already defined this for the basic language.

One could respond to the two requirements above by declaring that the axioms is the set A of all true sentences and the rule is "being a member of A". But then the rule is – a priori – not even verifiable. Hence the axioms system will have to be as simple as possible (and consist of sentences that can be declared as obvious - we shall call them tautologies) and the rules should be so that even a computer is able to decide what is a formal proof and what is not.

The task has significant syntactic complexity so the setup of the language and the proof system will occupy us for a while, before we can realise the requirements (1) and (2) above.

The alphabet of a language

We reintroduce the red color to distinguish symbols of languages from any perceived meaning.

2.3.2. **Definition.** The **alphabet** of a language $\mathscr{L}$ consists of the following letters:

(I) A set of **logical symbols**, which are present in every language:
- $\neg$ ('not'), $\rightarrow$ ('implies'), $\forall$ ('for all')
- The equality symbol: $\doteq$
- Brackets: $)$ $($
- Comma: $,$
- Symbols to denote **variables**: $v_0, v_1, v_2, \ldots$ Notice that each v_i is considered as a single symbol (and not as a concatenation of two symbols).

Hence the letters of the basic language from section 2.1 are always present in any language. However in general there are more letters and this is where languages differ. These are recorded next.

(II)
- Three mutually disjoint sets $\mathscr{R}$ (called the set of **relation symbols** or **predicate symbols**), $\mathscr{F}$ (called the set of **function symbols**) and $\mathscr{C}$ (called the set of **constant symbols**). Further, none of these sets contains a logical symbol.
- Maps

$$\lambda : \mathscr{R} \longrightarrow \mathbb{N} \text{ called the "}\textbf{arity of relation symbols}\text{"}$$
$$\mu : \mathscr{F} \longrightarrow \mathbb{N} \text{ called the "}\textbf{arity of function symbols}''$$

For $R \in \mathscr{R}$ and $F \in \mathscr{F}$, the numbers $\lambda(R)$ and $\mu(F)$ are called the **arity** of R, F respectively. We say that R, F is n**-ary**, if $\lambda(R) = n$, $\mu(F) = n$, respectively; if $n = 1$ we say **unary** and if $n = 2$, we say **binary**.

2.3.3**. Terminology and Notation**

(a) Every logical symbol and every element from $\mathscr{R} \cup \mathscr{F} \cup \mathscr{C}$ is called an $\mathscr{L}$-symbol or simply a **symbol** whenever $\mathscr{L}$ is clear from the context. We shall also use the term **($\mathscr{L}$-)letter** instead of ($\mathscr{L}$)-symbol.

(b) We define the **set of variables** as

$$\mathrm{Vbl} := \{v_n \mid n \in \mathbb{N}_0\}.$$

(c) The (alphabet of a) language $\mathscr{L}$ is called **finite** if $\mathscr{R}$, $\mathscr{F}$ and $\mathscr{C}$ are finite. Otherwise the alphabet of $\mathscr{L}$ is called **infinite**

The (alphabet of a) language $\mathscr{L}$ is called **countable** if $\mathscr{R}$, $\mathscr{F}$ and $\mathscr{C}$ are countable or finite. Otherwise the alphabet of $\mathscr{L}$ is called **uncountable**. .

In general, the **cardinality of an alphabet of a language** $\mathscr{L}$ is the cardinality of $\mathscr{R} \cup \mathscr{F} \cup \mathscr{C}$.

(d) Obviously, the alphabet of a language is uniquely determined by the data in item II of definition 2.3.2. These data are called the **similarity type** of $\mathscr{L}$. Hence the similarity type of $\mathscr{L}$ is given by the triple

$$(\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$$

We will often communicate languages by stating the elements of $\mathscr{R} \cup \mathscr{F} \cup \mathscr{C}$ explicitly and then say the arity of relation symbols and function symbols. For example we could say, let $\mathscr{L}$ be the language $\{R, S, F, c, d)$, where R is a unary relation symbol, S is a relation symbol of arity 4, F is a binary function symbol and c, d are constant symbols; hence formally $\mathscr{R} = \{R, S\}$ with $\lambda(R) = 1, \lambda(S) = 4$, $\mathscr{F} = \{F\}$ with $\mu(F) = 2$ and $\mathscr{C} = \{c, d\}$.

If one of the sets $\mathscr{R}.\mathscr{F}$ or $\mathscr{C}$ is empty, we drop it.

2.3.4. **Real world examples**

(i) The empty language has similarity type $\mathscr{R} = \mathscr{F} = \mathscr{C} = \emptyset$. In the terminology of section 2.1, this language is just the basic language, which we also refer to as "the empty language" (explaining the notation $\mathscr{L}_\emptyset$).

(ii) The language of a composition (or of a "binary operation") has similarity $\{\cdot\}$, where $\cdot$ is a binary function symbol. Formally this reads as $\mathscr{R} = \mathscr{C} = \emptyset$, $\mathscr{F} = \{\cdot\}$ and $\mu(\cdot) = 2$ and $\mathscr{C} = \emptyset$.

(iii) The language of groups has similarity type $\{\cdot, ^{-1}, e\}$, where $\cdot$ is a binary function symbol, $^{-1}$ is a unary function symbol and e is a constant symbol. Formally this reads as $\mathscr{R} = \emptyset$, $\mathscr{F} = \{\cdot, ^{-1}\}$, $\mathscr{C} = \{e\}$ and $\mu(\cdot) = 2$, $\mu(^{-1}) = 1$.

(iv) The language of unital rings has similarity type $\{+, -, \cdot, 0, 1\}$, where $+, \cdot$ are binary function symbols, $-$ is a unary function symbol and $0, 1$ are constant symbols. Formally this reads as $\mathscr{R} = \emptyset$, $\mathscr{F} = \{+, -, \cdot\}$, $\mathscr{C} = \{0, 1\}$ and $\mu(+) = \mu(\cdot) = 2$, $\mu(-) = 1$.

(v) The language of set theory has similarity type $\{\in\}$, where $\in$ is a binary relation symbol. Formally this reads as $\mathscr{R} = \{\in\}$, $\mathscr{F} = \mathscr{C} = \emptyset$ and $\lambda(\in) = 2$.[21]

(vi) The language of posets has similarity type $\{\leq\}$ where $\leq$ is a binary relation symbol. Formally this reads as $\mathscr{R} = \{\leq\}$, $\mathscr{F} = \mathscr{C} = \emptyset$ and $\lambda(\leq) = 2$.

So this language is essentially the same as the language of set theory. We use different letters for the binary relation symbol, which will suit better to what we want to do with that language.

(vii) The language of ordered groups has similarity type $\{\leq, \cdot, ^{-1}, e\}$, where $\leq$ is a binary relation symbol, $\cdot$ is a binary function symbol, $^{-1}$ is a unary function symbol and e is a constant symbol. As an exercise, write out what this means following the patterns from the examples above.

[21]Some authors also use the similarity type $\{\in, \emptyset\}$, which also has a constant symbol $\emptyset$.

(viii) The language of ordered rings has similarity type $\{\leq, +, -, \cdot, 0, 1\}$, where $\leq$ is a binary relation symbol, $+$ and $\cdot$ are binary function symbols, $-$ is a unary function symbol and $0, 1$ are constant symbols. As an exercise, write out what this means following the patterns from the examples above.

We now build up the definition of formulas for a given signature of a language. These will be finite strings of letters of the language.

2.3.5. **Definition.** A **string** of an alphabet of a language $\mathscr{L}$ (or simply "a string of $\mathscr{L}$" or an "$\mathscr{L}$-string") is a finite sequence of logical symbols and elements from $\mathscr{R}$, $\mathscr{F}$ and $\mathscr{C}$. The **length of a string** is the length of that sequence. Every logical symbol and each element from $\mathscr{R}$, $\mathscr{F}$ and $\mathscr{C}$ is also considered to be a string (a sequence of length 1). We shall denote strings by simply concatenating letters, e.g. we write $v_0 \neg \forall, v_0 \to, \doteq v_0$ instead of the sequence $(v_0, \neg, \forall, ,, v_0, \to, ,, \doteq, v_0)$. (The string does not make any sense on the semantic side and only exemplifies the way of writing strings.)

In formal arguments we still make use of the notation of strings as sequences. Here is an example:

A **string** $(z'_1, ..., z'_m)$ **occurs in a string** $(z_1, ..., z_n)$ **at position** k if $m+k \leq n+1$ and $z_k = z'_1, ..., z_{k+m-1} = z'_m$ (i.e. $z_{k+i-1} = z'_i$ $(1 \leq i \leq m)$). In a picture:

$$\begin{array}{ccccccccc} z_1 & \dots & z_{k-1} & z_k & \dots & z_{k+m-1} & z_{k+m} & \dots & z_n \\ & & & \| & & \| & & & \\ & & & z'_1 & \dots & z'_m & & & \end{array}$$

In this case, $(z'_1, ..., z'_m)$ is called a **substring** of $(z_1, ..., z_n)$. If in addition $k = 1$, then $(z'_1, ..., z'_m)$ is called an **initial segment** or an **initial substring** of $(z_1, ..., z_n)$. Similarly, if $k = n - m + 1$, then $(z'_1, ..., z'_m)$ is called a **terminal segment** or a **terminal substring** of $(z_1, ..., z_n)$.

Before defining formulas we define

Terms

2.3.6. **Definition.** Given the similarity type $(\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ of a language $\mathscr{L}$, we define subsets $\mathrm{tm}_k(\mathscr{L})$ of strings (i.e. of finite sequences) of the alphabet of $\mathscr{L}$ by induction on $k \in \mathbb{N}_0$ as follows:

$$\mathrm{tm}_0(\mathscr{L}) = \mathrm{Vbl} \cup \mathscr{C} \text{ and}$$

$$\mathrm{tm}_{k+1}(\mathscr{L}) = \mathrm{tm}_k(\mathscr{L}) \cup \Big\{ F(t_1, t_2, ..., t_n) \mid n \in \mathbb{N}, F \in \mathscr{F}, \mu(F) = n, \text{ and } t_1, \dots, t_n \in \mathrm{tm}_k(\mathscr{L}) \Big\}.$$

The set of $\mathscr{L}$**-terms** is defined as

$$\mathrm{tm}(\mathscr{L}) := \bigcup_{k \in \mathbb{N}_0} \mathrm{tm}_k(\mathscr{L}).$$

The elements of $\mathrm{tm}(\mathscr{L})$ are called $\mathscr{L}$**-terms** or simply 'terms' if $\mathscr{L}$ is clear from the context. Observe that the terms of the basic language are terms of $\mathscr{L}$ as well.

Notice that by induction on k we see immediately that the number of opening brackets occurring in a term $t \in \mathrm{tm}_k(\mathscr{L})$, is equal to the number of closing brackets occurring in t.

The **complexity of an $\mathscr{L}$-term** t - denoted by $c(t)$ - is the least $k \in \mathbb{N}_0$ such that $t \in \mathrm{tm}_k(\mathscr{L})$. Notice that for $t \in \mathrm{tm}(\mathscr{L})$ and $k \in \mathbb{N}_0$ we have by definition $c(t) \leq k \iff t \in \mathrm{tm}_k(\mathscr{L})$.

Every variable that occurs in a term t is called a **free variable** of t and the set of these free variables is denoted by $\mathrm{Fr}(t)$. If $\mathrm{Fr}(t) = \emptyset$, then t is called a **closed term** or a **constant term**.

2.3.7**. Explanation of the definition of a term.** Each term is built up inductively, starting from variables and constant symbols, by creating expressions of the form $F(t_1, \ldots, t_n)$, where F is an n-ary function symbol and $t_1, \ldots, t_n$ are previously constructed terms. Notice that $F(t_1, \ldots, t_n)$ is (at the moment) just a list of symbols in our language - F is not a function and one cannot plug anything into it.

We do some examples.

(i) Suppose we have three constant symbols c_1, c_2, c_3 in our language as well as a a binary function symbol F and a function symbol G of arity 3 (i.e. $\mu(G) = 3$). We give some examples of terms of $\mathscr{L}$ and record their free variables and their complexity:

Term	Free variables	complexity
c_1	$\emptyset$	0
c_2	$\emptyset$	0
$G(c_1,c_2,c_3)$	$\emptyset$	1
$G(x,c_1,c_2)$	x	1
$G(x,y,z)$	x, y, z	1
$F(G(c_1,x,y),c_2)$	x, y	2
$F(G(x,y,c_1),F(x,c_2))$	x, y	2

The constant terms in this list are c_1, c_2 and $G(c_1,c_2,c_3)$.

(ii) The second example is from the real world. Suppose $\mathscr{L}$ is the language with similarity type $\{+, \cdot, 0, 1\}$, where $+$ and $\cdot$ are binary function symbols (hence, they are elements of $\mathscr{F}$ and their arity is $\mu(+) = \mu(\cdot) = 2$), and $0, 1$ are constant symbols (not the numbers 0,1). Here are a few terms in that language:

(a) $0, 1, v_7$. These are three terms of complexity 0.

(b) $+(0, v_2)$, $\cdot(1, 1)$, $+(v_1, v_3)$. These are three terms of complexity 1. In a human readable form we would write $0 + v_2$, $1 \cdot 1$, $v_1 + v_3$ (and we will do that), because in the intended structures (namely rings) where we deploy this language, the symbols will be interpreted as addition and multiplication. The only constant term among these three terms is $\cdot(1, 1)$.

(c) $+(1, \cdot(v_3, v_1))$, $\cdot(+(1, v_3), v_1)$. These are two terms of complexity 2. In a human readable form we might be tempted to write $1 + (v_3 \cdot v_1)$ and $(1 + v_3) \cdot v_1$.

(d) $\cdot(\cdot(+(1,1),v_2),v_2)$ is a term of complexity 3. In human readable form this would be $2v_2^2$.

We can see that in this language, terms (in human readable form) look like polynomials (with coefficients in $\mathbb{N}$). In fact, if you understand this example well, the general case is in essence not more complicated, just more general.

2.3.8**. Alternative definition of terms** Here is another way to define terms:

(1) Each variable symbol is a term and each constant symbol is a term.
(2) If F is an n-ary function symbol and $t_1,\dots,t_n$ are terms, then $F(t_1,\dots,t_n)$ is a term
(3) Nothing else is a term.

Proof. The equivalence of this definition with the definition of "term" in 2.3.6 is done in question 30 of the example sheet □

2.3.9**. The construction tree of a term** Yet another way of thinking about terms is in the form of a construction tree. This is not defined formally and is meant to build up intuition. So we do this in examples only:

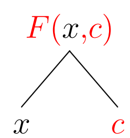
Suppose the similarity type of a language $\mathscr{L}$ is given by

- two constant symbols c,d,
- two binary function symbols F,G and
- a binary relation symbol R.

Then the terms of $\mathscr{L}$ are the strings of symbols formed by finitely many applications of the following rules:

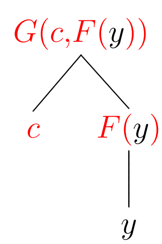
(1) all the variable symbols are terms and c,d are terms,
(2) if t_1,t_2 are terms, then $F(t_1,t_2)$ is a term and $G(t_1,t_2)$ are terms,
(3) nothing else is a term.

To see whether a string is a term, we can try to form a construction tree. For example,



At the bottom of the tree, we have x and c, both of which are terms. Then above, we have $F(x,c)$, which is formed by applying one of the rules. So we get a term.

Here is a non-example. We can see that $G(c,F(y))$ is *not* a term, by trying to draw a tree, and follow what happens:



At the bottom of the tree we have y which is a term, but above it we have $F(y)$, but F is binary, so $F(y)$ is not a term according to the rules. Hence we cannot use it to form other terms, and so $G(c, F(y))$ is not a term.

We need three results about terms later on, which require a rigorous proof. These proofs are not examinable and may be found in the appendix to this section. However, these results are very plausible if we think of how terms are constructed:

2.3.10**. Unique Readability Theorem for Terms** *If t is an $\mathscr{L}$-term, then either t is a variable or t is a constant symbol or there are uniquely determined $n \in \mathbb{N}$, $F \in \mathscr{F}$ of arity n and $t_1, \ldots, t_n \in \mathrm{tm}(\mathscr{L})$ such that*

$$t = F(t_1,t_2,...,t_n).$$

Proof. This proof is not examinable and may be found in 2.3.36 for the interested reader. □

The unique readability theorem is important when we make definitions or when we prove properties of terms by induction. Here is a first example.

2.3.11. **Corollary.** *For all $n \in \mathbb{N}$, all $\mathscr{L}$-terms $t_1, \ldots, t_n$ and each n-ary function symbol F of $\mathscr{L}$ we have*

$$c(F(t_1, \ldots, t_n)) = 1 + \max\{c(t_1), \ldots, c(t_n)\}.$$

Proof. This proof is not examinable and may be found in 2.3.37 for the interested reader. □

2.3.12. **Definition.** A term s is called a **subterm** of a term t, if s occurs in t; see 2.3.5 for the definition of "occurs in".

2.3.13. **Proposition.** *Let s be a subterm of a term t occurring at position p in t. Let r be another term. We define a new string u by replacing the substring s of t occurring at position p with the string r. Then u is again a term.*

Proof. This proof is not examinable and may be found in 2.3.41 for the interested reader. □

We now define the central object of the syntax of Predicate Logic.

Formulas

2.3.14. **Definition.** (formulas)
Given a similarity type $(\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ of a language $\mathscr{L}$, an **atomic $\mathscr{L}$-formula** is a string of the alphabet of $\mathscr{L}$ of the form

$$t_1 \doteq t_2,$$

where t_1, t_2 are $\mathscr{L}$-terms or a string of the form

$$R(t_1,...,t_n),$$

where R is a relation symbol of arity $n \in \mathbb{N}$ and $t_1, \ldots, t_n$ are $\mathscr{L}$-terms. The set of atomic $\mathscr{L}$-formulas is denoted by at-Fml($\mathscr{L}$).

We define

$$\begin{aligned}
\mathrm{Fml}_0(\mathscr{L}) &= \text{at-Fml}(\mathscr{L}) \text{ and inductively for each } k \in \mathbb{N}_0 : \\
\mathrm{Fml}_{k+1}(\mathscr{L}) &= \mathrm{Fml}_k(\mathscr{L}) \cup \{(\neg\varphi), (\varphi\to\psi), (\forall x\varphi) \mid \varphi, \psi \in \mathrm{Fml}_k(\mathscr{L}),\ x \in \mathrm{Vbl}\}.
\end{aligned}$$

The set of **$\mathscr{L}$-formulas** is defined as

$$\mathrm{Fml}(\mathscr{L}) := \bigcup_{k\in\mathbb{N}_0} \mathrm{Fml}_k(\mathscr{L}).$$

If the letter $\forall$ does not occur in the $\mathscr{L}$-formula φ, then φ is called **quantifier free**.

In the literature one can also find the expression **well formed formula** (abbreviated 'wff') instead of 'formula'.

Observe that every formula of the basic language is an $\mathscr{L}$-formula. As for terms, the number of opening brackets in a formula is equal to the number of closing brackets in that formula.

Warning. Not every formula that has (obvious) meaning in mathematics is a formula in our sense. This is in particular important after we have proved significant theorems involving formulas. Here is an example:

$$\forall n \in \mathbb{N}\ \exists r, q \in \mathbb{N}_0\ (n = q \cdot m + r\ \wedge\ r < m).$$

There is no language (according to our definition) such that the above is a formula in that language: Notice that the quantifier introduced in the definition of $\mathrm{Fml}_{k+1}(\mathscr{L})$ (cf. 2.3.14) is always applied in a nonrestricted way, e.g.

$$\forall n \exists r, q\ (n \doteq q \cdot m + r\ \wedge\ r < m)$$

will be a formula in the language of ordered rings; we introduce the appropriate abbreviations (concerning the symbols $\exists$ and $\wedge$) shortly, $r < m$ stands for $r \leq m \wedge r \neq m$.

The **language** or **signature** $\mathscr{L}$ is the triple consisting of the alphabet of $\mathscr{L}$, the set of $\mathscr{L}$-terms and the set of $\mathscr{L}$-formulas. Obviously, $\mathrm{tm}(\mathscr{L})$ and $\mathrm{Fml}(\mathscr{L})$ are uniquely determined by the similarity type of $\mathscr{L}$ and we shall simply communicate languages by their similarity type.

Hence the expression 'let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ be a language' stands for 'let $\mathscr{L}$ be the language with similarity type $(\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$'.

We say that a language is **finite**, **infinite**, **countable** or **uncountable** if the alphabet of that language has this property. In general, the cardinality of a language $\mathscr{L}$, denoted by $\mathrm{card}(\mathscr{L})$, is the cardinality of the alphabet of that language.

2.3.15. *Example.* Like in the case of formulas of the basic language and the case of $\mathscr{L}$-terms, the definition of an $\mathscr{L}$-formula is inductive and one can draw a construction tree for each formula. Here is an example. We work again in the language of example 2.3.9. Given variables u, x, y, z consider the $\mathscr{L}$-string

$$\forall x \forall y (R(z, u) \to F(c, y) \doteq G(x, F(z, u)))$$

We draw its construction tree following the definition of an $\mathscr{L}$-formula.

$$\forall x \forall y (R(z,u) \to F(c,y) \doteq G(x, F(z,u)))$$

$$\forall y (R(z,u) \to F(c,y) \doteq G(x, F(z,u)))$$

$$R(z,u) \to F(c,y) \doteq G(x, F(z,u))$$

$$R(z,u) \qquad F(c,y) \doteq G(x, F(z,u))$$

At the bottom we have atomic formulas. To be more precise, we should also check that $F(c{,}y)$ and $G(x{,}F(z{,}v))$ are terms. This can be done as in the term examples above. Then everything above is formed following the definitions, so what we get is a formula.

2.3.16. **Alternative definition of formulas** Here is another way to define $\mathscr{L}$-formulas: The formulas of $\mathscr{L}$ are defined as in the case of the basic language, but with the more general definitions of terms and atomic formulas. So

(1) Every atomic formula is a formula.
(2) If φ is a formula then so is $(\neg\varphi)$.
(3) If φ, ψ are formulas then so is $(\varphi{\to}\psi)$.
(4) If φ is a formula and x is a variable symbol then $(\forall x \varphi)$ is a formula.
(5) Nothing else is a formula of $\mathscr{L}$.

Proof. The equivalence of this definition with the definition of "$\mathscr{L}$-formula" in 2.3.14 is done in question 33 of the example sheet. □

As for terms we have a unique readability theorem:

2.3.17. **Unique Readability Theorem for Formulas** *Let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ be a language and let φ be an $\mathscr{L}$-formula. Then exactly one of the following conditions holds true:*

(i) φ is atomic and there are uniquely determined $t_1, t_2 \in \mathrm{tm}(\mathscr{L})$ such that φ is $t_1{\doteq}t_2$, or

(ii) φ is atomic and there are a unique $n \in \mathbb{N}$, a unique $R \in \mathscr{R}$ and uniquely determined $\mathscr{L}$-terms $t_1, \dots, t_n$ such that φ is $R(t_1{,}...{,}t_n)$, or

(iii) φ is equal to a string of the form $(\neg\psi)$ for a uniquely determined $\psi \in \mathrm{Fml}(\mathscr{L})$, or

(iv) φ is equal to a string of the form $(\varphi_1{\to}\varphi_2)$ for uniquely determined $\varphi_1, \varphi_2 \in \mathrm{Fml}(\mathscr{L})$, or

(v) φ is equal to a string of the form $(\forall x \psi)$ for uniquely determined $\psi \in \mathrm{Fml}(\mathscr{L})$ and $x \in \mathrm{Vbl}$.

Proof. This proof is not examinable and may be found in 2.3.44 for the interested reader. □

2.3.18. **Abbreviations and Domestication of the Notation**

- We will omit brackets if this increases readability and does not lead to ambiguity.
- We use the following abbreviation for $\mathscr{L}$-formulas φ, ψ: $\varphi \vee \psi := (\neg\varphi) \to \psi$, $\varphi \wedge \psi := \neg(\varphi \to (\neg\psi))$, $\varphi \leftrightarrow \psi := (\varphi \to \psi) \wedge (\psi \to \varphi)$ and $\exists x \varphi := \neg\forall x(\neg\varphi)$ where x is a variable.
- We shall generally not color the symbols of our languages anymore. We also will generally not use the logical symbols in the meta theory, hence in the meta theory we will write "forall" instead of $\forall$, "and" instead of "$\wedge$", etc.
- We write

  $\forall x_1, \ldots, x_n\ \varphi$ instead of $\forall x_1 ... \forall x_n \varphi$ and $\exists x_1, \ldots, x_n\ \varphi$ instead of $\exists x_1 ... \exists x_n \varphi$

  where each x_i is a variable. The strings $\forall x$ and $\exists x$ are called **quantifiers**. A string of quantifiers is a string of the form $Q_1 x_1 ... Q_n x_n$, where each Q_i is either $\forall$ or $\exists$ and each x_i is a variable.
- We write

  $$\bigwedge_{i=1}^{n} \varphi_i \text{ instead of } \overbrace{(...(}^{n\text{-times}}\ \varphi_1 \wedge \varphi_2) \wedge \varphi_3) ... \wedge \varphi_n) \text{ and}$$

  $$\bigvee_{i=1}^{n} \varphi_i \text{ instead of } \overbrace{(...(}^{n\text{-times}}\ \varphi_1 \vee \varphi_2) \vee \varphi_3) ... \vee \varphi_n).$$
- We write $t_1 \neq t_2$ instead of $(\neg t_1 \doteq t_2)$.
- If R is a binary relation, we write $t_1 R t_2$ instead of $R(t_1, t_2)$.

It should be understood that these conventions are meta theoretic conventions and they are meant to increase readability in the notes. When we are arguing about syntactic manipulations with terms and formulas we still refer to the rigorous definitions 2.3.6 and 2.3.14.

Complexity and subformulas

The unique readability theorems 2.3.10 and 2.3.17 allow us to define new objects from formulas, and to prove statements about formulas. This will be done via induction on the construction depth (or the 'complexity') of terms and formulas:

2.3.19. **Definition.** The **complexity of an $\mathscr{L}$-formula** φ - denoted by $c(\varphi)$ - is the least $k \in \mathbb{N}_0$ such that $\varphi \in \mathrm{Fml}_k(\mathscr{L})$.

Notice that this is not in conflict with the definition of the complexity of $\mathscr{L}$-terms (cf. 2.3.6), since the set of $\mathscr{L}$-terms is disjoint from the set of $\mathscr{L}$-formulas. Notice also that for any given terms $t_1, t_2, \ldots, t_n$ and each n-ary relation symbol R of $\mathscr{L}$, $c(R(t_1, \ldots, t_n)) = 0$. Similarly $c(t_1 \doteq t_2) = 0$.
By definition, for every $\mathscr{L}$-formula φ and each $k \in \mathbb{N}_0$ we have

$$c(\varphi) \leq k \iff \varphi \in \mathrm{Fml}_k(\mathscr{L}).$$

Here is a consequence of the Unique Readability Theorem for Formulas 2.3.17.

2.3.20. **Corollary.** *For all $\mathscr{L}$-formulas φ, ψ we have*

$$c(\neg\varphi) = 1 + c(\varphi),\ c(\varphi \to \psi) = 1 + \max\{c(\varphi), c(\psi)\} \text{ and } c(\forall x\varphi) = 1 + c(\varphi).$$

Proof. This proof is not examinable and may be found in 2.3.45 for the interested reader. □

2.3.21. **Definition.** We say that a formula φ is a **subformula** of a formula ψ if φ occurs in the string ψ; see 2.3.5 for the definition of "occurs in".

The next proposition can also be understood as the definition of "subformula", but is it less obvious that the two definitions are equivalent.

2.3.22. **Proposition.** *Suppose φ is a subformula of ψ.*

(i) If $c(\psi) = 0$ (equivalently: ψ is atomic), then $\varphi = \psi$.
(ii) Now suppose $c(\psi) = k + 1$.
  - *(a) If $\psi = (\forall x\vartheta)$ or $\psi = (\neg\vartheta)$, then φ is ψ or φ is a subformula of ϑ.*
  - *(b) If $\psi = (\psi_1 \to \psi_2)$, then $\varphi = \psi$, or φ is a subformula of ψ_1 or φ is a subformula of ψ_2.*

Proof. This proof is not examinable and may be found in 2.3.48 for the interested reader. □

2.3.23. **Theorem.** *Let ψ be a formula.*

(i) Let φ be a subformula of ψ occurring at position p in ψ. Let δ be another formula. We define a new string γ by replacing the substring φ of ψ occurring at position p with the string δ. Then γ is again a formula.
(ii) Let t be a term occurring in ψ at position p. Let s be another term. We define a new string γ by replacing the substring t of ψ occurring at position p with the string s. Then γ is again a formula.

Proof. This proof is not examinable and may be found in 2.3.49 for the interested reader. □

Free and bound occurrences of variables

We will write down formulas that we would like to consider as absolutely true (they will be called *axioms*). Instances of such formulas could be formulas of the form

$$(*) \qquad (\forall x\varphi) \to \varphi(x/y),$$

where φ is a formula of some language and $\varphi(x/y)$ stands for the formula obtained from φ by replacing x with y. It seems plausible that $(*)$ should be an axiom, because a priori $(\forall x\varphi)$ seems to say something stronger than $\varphi(x/y)$. However, there is a glitch here: For an example, consider the formula φ defined as $\exists y\ x \neq y$. If we replace x by y we obtain $\exists y\ y \neq y$ and hence $(*)$ is

$$(\forall x \exists y\ x \neq y) \to (\exists y\ y \neq y).$$

But obviously we do not want this formula to be a universal axiom. The problem here is that we replace x in a position of φ within the *scope of the quantifier* $\exists y$ and this has to be avoided if we want to include formulas of the shape $(*)$ as axioms. So we need to clarify the situation and first address the clause *scope of the quantifier.*

Let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ be a language.

2.3.24. **Definition.** (scope of a quantifier)
The **scope** of a quantifier $\forall x$ in an $\mathscr{L}$-formula φ is the set of all positions of letters in φ, which are captured in a subformula of the form $(\forall x\psi)$ of φ.

More formally: the scope of $\forall x$ in φ is the set of all $k \in \mathbb{N}$ such that there is a subformula of the form $(\forall x\psi)$ of φ, of length $l \in \mathbb{N}$ which occurs at a position p in φ with $p \leq k < p + l$.

2.3.25. *Example.* For example, look at the formula φ of the language of ordered groups (cf. 2.3.4) defined as

$$(\forall v_2((\forall v_1\ \ \cdot(e, v_1) \doteq v_5) \to\ \ ^{-1}(v_1) \leq e)).$$

Here is the scope of the quantifier $\forall v_1$:

$$(\forall v_2(\overbrace{(\forall v_1\ \ \cdot(e, v_1) \doteq v_5)}^{\text{scope of } \forall v_1} \to\ \ ^{-1}(v_1) \leq e)).$$

2.3.26. **Definition.** (free and bound occurrence of variables)
Let φ be an $\mathscr{L}$-formula and let x be a variable.

(i) If x occurs in φ at position $k \in \mathbb{N}$ and if k is *not* in the scope of the quantifier $\forall x$ in φ, then we say x occurs **free** in φ at position k.

(ii) If x occurs in φ at position $k \in \mathbb{N}$ and if k is in the scope of the quantifier $\forall x$ in φ, then we say x occurs **bound** in φ at position k.

(iii) x is a **free variable** of φ if there is some $k \in \mathbb{N}$ such that x occurs free in φ at position k.

The set of free variables of φ is denoted by $\mathrm{Fr}(\varphi)$. If $\mathrm{Fr}(\varphi) = \emptyset$, then φ is called an ($\mathscr{L}$-)**sentence** and the set of all $\mathscr{L}$-sentences is denoted by $\mathrm{Sen}(\mathscr{L})$, hence

$$\mathrm{Sen}(\mathscr{L}) = \{\varphi \in \mathrm{Fml}(\mathscr{L}) \mid \mathrm{Fr}(\varphi) = \emptyset\}.$$

(iv) Recall from 2.3.6 that the free variables of an $\mathscr{L}$-term are those that occur in the term. Notice that there are no variables which are possibly bound in a term.

Different occurrences of a given variable in a formula may be free or bound, depending on where they are. In example 2.3.25 above, v_1 occurs bound at two positions in φ and free at one position.

$$\varphi = (\forall v_2((\forall \overbrace{v_1}^{\text{bound occurrence}} \cdot(e, \overbrace{v_1}^{\text{bound occurrence}}) \doteq v_5) \to {}^{-1}(\overbrace{v_1}^{\text{free occurrence}}) \leq e))).$$

We have $\mathrm{Fr}(\varphi) = \{v_1, v_5\}$.

2.3.27. **Proposition.** *Let φ, ψ be $\mathscr{L}$-formulas.*

(i) If φ is quantifier free then $\mathrm{Fr}(\varphi)$ is the set of variables occurring in φ.
(ii) $\mathrm{Fr}(\neg\varphi) = \mathrm{Fr}(\varphi)$
(iii) $\mathrm{Fr}((\varphi \to \psi)) = \mathrm{Fr}(\varphi) \cup \mathrm{Fr}(\psi)$.
(iv) $\mathrm{Fr}(\forall x\varphi) = \mathrm{Fr}(\varphi) \setminus \{x\}$ *for all* $x \in \mathrm{Vbl}$.

Proof. This proof is not examinable and may be found in 2.3.50 for the interested reader. □

2.3.28**. Important Convention**

- The expressions '$t(x_1, \dots, x_n) \in \mathrm{tm}(\mathscr{L})$' or 'let $t(x_1, \dots, x_n)$ be an $\mathscr{L}$-term' are shorthand for

  "$t \in \mathrm{tm}(\mathscr{L}), x_1, \dots, x_n \in \mathrm{Vbl}$ with $x_i \neq x_j$ $(i \neq j)$ and $\mathrm{Fr}(t) \subseteq \{x_1, \dots, x_n\}$".

  This is common practice in mathematics, for example a polynomial in two variables is also considered as a polynomial in three variables.
- The expressions '$\varphi(x_1, \dots, x_n) \in \mathrm{Fml}(\mathscr{L})$' or 'let $\varphi(x_1, \dots, x_n)$ be an $\mathscr{L}$-formula' are shorthand for

  "$\varphi \in \mathrm{Fml}(\mathscr{L}), x_1, \dots, x_n \in \mathrm{Vbl}$ with $x_i \neq x_j$ $(i \neq j)$ and $\mathrm{Fr}(\varphi) \subseteq \{x_1, \dots, x_n\}$".

2.3.29. **Definition.** Let φ be an $\mathscr{L}$-formula.

(i) Let x, y be variables. We define

x is free in φ for y [22]

if no position of φ at which x occurs free in φ, is in the scope of the quantifier $\forall y$ in φ.

(ii) Let t be an $\mathscr{L}$-term. We define

x is free in φ for t

if x is free in φ for every variable that occurs in t.

---

[22]A more verbose expression would be "x is free in φ for a possible replacement by y". In the literature one also finds the expressions "x can be substituted by y in φ, or, "y is substitutable for x in φ", or, "x is substitutable in φ by y".

So by definition, each variable x is free for x in φ and each variable which does not occur in φ is free in φ for every term.

In example 2.3.25, i.e.

$$\varphi = (\forall v_2((\forall v_1 \ \circ(e, v_1) \doteq v_5) \to \ ^{-1}(v_1) \leq e)),$$

v_1 is free for v_5 but not free for v_2 in φ; v_5 is not free for the term $\circ(v_2, v_5)$.

2.3.30. **Definition.** Let $\varphi \in \mathrm{Fml}(\mathscr{L})$, $t_1, \ldots, t_n, t \in \mathrm{tm}(\mathscr{L})$ and let $x_1, \ldots, x_n$ be n distinct variables.

(i) The expression $t(x_1/t_1, \ldots, x_n/t_n)$ denotes the string obtained from t by replacing every occurrence of x_i in t with the string t_i $(1 \leq i \leq n)$.

(ii) If for each $i \in \{1, \ldots, n\}$ the variable x_i is free in φ for t_i then the expression $\varphi(x_1/t_1, \ldots, x_n/t_n)$ denotes the string obtained from φ by simultaneously replacing every *free* occurrence of x_i in φ with the string t_i $(1 \leq i \leq n)$. We call $\varphi(x_1/t_1, \ldots, x_n/t_n)$ the **substitution** of $x_1, \ldots, x_n$ by $t_1, \ldots, t_n$ in φ.

2.3.31**. Warning**

Notice that we replace the variables x_i by the terms t_i *simultaneously* and not consecutively: For example if φ is $x_1 \doteq x_2$ then $\varphi(x_1/t_1, x_2/t_2)$ is $t_1 \doteq t_2$ However, in general $\varphi(x_1/t_1, x_2/t_2)$ is *not* the same as $\varphi(x_1/t_1)(x_2/t_2)$ and in general these formulas also have a different interpretation of truth in structures. See question 36 of the example sheet.

2.3.32. **Proposition.** *Let $\varphi \in \mathrm{Fml}(\mathscr{L})$, $t_1, \ldots, t_n, t \in \mathrm{tm}(\mathscr{L})$ and let $x_1, \ldots, x_n$ be n distinct variables.*

(i) $t(x_1/t_1, \ldots, x_n/t_n)$ is an $\mathscr{L}$-Term and if $\mathrm{Fr}(t) \subseteq \{x_1, \ldots, x_n\}$, then

$$\mathrm{Fr}(t(x_1/t_1, \ldots, x_n/t_n)) \subseteq \mathrm{Fr}(t_1) \cup \ldots \cup \mathrm{Fr}(t_n).$$

(ii) If for each $i \in \{1, \ldots, n\}$ the variable x_i is free in φ for t_i then the string $\varphi(x_1/t_1, \ldots, x_n/t_n)$ is an $\mathscr{L}$-formula and in the case $\mathrm{Fr}(\varphi) \subseteq \{x_1, \ldots, x_n\}$ we have

$$\mathrm{Fr}(\varphi(x_1/t_1, \ldots, x_n/t_n)) \subseteq \mathrm{Fr}(t_1) \cup \ldots \cup \mathrm{Fr}(t_n).$$

Proof. This proof is not examinable and may be found in 2.3.51 for the interested reader. $\square$

Appendix to section 2.3

`None of the proofs in this appendix is examinable. Only statements that also occur outside of this appendix are examinable.`

2.3.33. *Remark.* Obviously the substring relation defined in 2.3.5 is transitive. In more detail: If r, s, t are strings such that

- r is a substring of s occurring at position p in s and
- s is a substring of t occurring at position k in t,

then r is a substring of t occurring at position $k+p-1$ in t.

2.3.34. **Lemma.** *Let t be an $\mathscr{L}$-term. Then*

(i) t is a variable if and only if the first letter of t is a variable.
(ii) t is a constant symbol if and only if the first letter of t is a constant symbol.
(iii) $t \in \mathrm{tm}(\mathscr{L}) \setminus \mathrm{tm}_0(\mathscr{L})$ if and only if the first letter of t is a function symbol.
(iv) $c(t) = 0 \iff t \in \mathrm{tm}_0(\mathscr{L})$.

Proof. (i). If t is a variable, then $t \in \mathrm{tm}_0(\mathscr{L}) \subseteq \mathrm{tm}(\mathscr{L})$, thus t is a term. If t is not a variable, then t is either a constant symbol, or, t starts with a function symbols (by definition of $\mathrm{tm}_{k+1}(\mathscr{L})$). In either case, the first letter of t is not a variable.

(ii). is similar to (i), just change swap the expressions "variable" and "constant symbols".

(iii). If the first letter of t is a function symbol, then $t \notin \mathrm{Vbl} \cup \mathcal{C} = \mathrm{tm}_0(\mathscr{L})$. Conversely, if $t \notin \mathrm{tm}_0(\mathscr{L})$, then $t \in \mathrm{tm}_{k+1}(\mathscr{L})$ for some k. By definition of $\mathrm{tm}_{k+1}(\mathscr{L})$ this implies that the first letter of t is a function symbol.

(iv). By definition, the complexity of t is 0 if and only if 0 is the smallest $k \in \mathbb{N}_0$ with $t \in \mathrm{tm}_k(\mathscr{L})$. But this is just the same as saying $t \in \mathrm{tm}_0(\mathscr{L})$. $\square$

2.3.35. **Lemma.** *If s, t are $\mathscr{L}$-terms and t is an initial segment of s then $s = t$.*

Proof. We pick $t \in \mathrm{tm}_k(\mathscr{L})$ for some $k \in \mathbb{N}_0$ and we show the following assertion by induction on k:

$(*)$ If s is an $\mathscr{L}$-term and t is an initial segment of s *or vice versa* then $s = t$.

If $k = 0$, then t is a variable or a constant symbol and $(*)$ follows immediately from 2.3.34.

If $t \in \mathrm{tm}_{k+1}(\mathscr{L})$ and $t \notin \mathrm{tm}_k(\mathscr{L})$, then pick $n \in \mathbb{N}$, $F \in \mathscr{F}$ and $t_1, ..., t_n \in \mathrm{tm}_k(\mathscr{L})$ with $t = F(t_1, t_2, ..., t_n)$. Suppose t is an initial segment of $G(s_1, s_2, ..., s_r)$ for some $G \in \mathscr{F}, r \in \mathbb{N}$ and $s_1, ..., s_r \in \mathrm{tm}(\mathscr{L})$ - or vice versa. Then obviously $F = G$, which implies $n = \mu(F) = \mu(G) = r$, and the string $t_1, t_2, ..., t_n)$ is an initial segment of $s_1, s_2, ..., s_n)$ or vice versa. Depending on the length of the strings t_1 and s_1, it follows that t_1 is an initial segment of s_1 or vice versa. Since $t_1 \in \mathrm{tm}_k(\mathscr{L})$ the induction hypothesis gives $t_1 = s_1$. It follows that $t_2, t_2, ..., t_n)$ is an initial segment of $s_2, s_2, ..., s_n)$ or vice versa.

Consequently t_2 is an initial segment of s_2 or vice versa. Since $t_2 \in \mathrm{tm}_k(\mathscr{L})$ the induction hypothesis gives $t_2 = s_2$. Continuing in this way we see that $t_1 = s_1, ..., t_n = s_n$. $\square$

2.3.36. **Theorem.** *(Unique readability theorem for terms) If t is an $\mathscr{L}$-term, then either t is a variable or t is a constant symbol or there are uniquely determined $n \in \mathbb{N}$, $F \in \mathscr{F}$ of arity n and $t_1, ..., t_n \in \mathrm{tm}(\mathscr{L})$ such that*

$$t = F(t_1,t_2,...,t_n).$$

Proof. That these cases are mutually exclusive follows by comparing the first letters. The uniqueness statement is clear if $t \in \mathrm{Vbl} \cup \mathscr{C}$. Suppose $t = F(t_1,t_2,...,t_n)$ and $t = G(s_1,s_2,...,s_r)$ for some $G \in \mathscr{F}, r \in \mathbb{N}$ and $s_1, ..., s_r \in \mathrm{tm}(\mathscr{L})$. Then $F = G$, hence $n = r$ and the string $t_1,t_2,...,t_n)$ is equal to $s_1,s_2,...,s_n)$. It follows that t_1 is an initial segment of s_1 or vice versa. By 2.3.35 we get $t_1 = s_1$ and so $t_2,...,t_n)$ is equal to $s_2,...,s_n)$. Continuing in this way we get $s_i = t_i$ for each $i \in \{1, ..., n\}$. $\square$

2.3.37. **Corollary.** *For all $n \in \mathbb{N}$, all $\mathscr{L}$-terms $t_1, ..., t_n$ and each n-ary function symbol F of $\mathscr{L}$ we have*

$$c(F(t_1, ..., t_n)) = 1 + \max\{c(t_1), ..., c(t_n)\}.$$

Proof. Let $t = F(t_1,...,t_n)$ and let $k = \max\{c(t_1), ..., c(t_n)\}$. Then $t_1, ..., t_n \in \mathrm{tm}_k(\mathscr{L})$ by definition of the complexity and so $t \in \mathrm{tm}_{k+1}(\mathscr{L})$. By definition of the complexity again, this means $c(t) \leq 1 + k$. Suppose $c(t) < 1 + k$. We write $l := c(t)$. Then $t \in \mathrm{tm}_l(\mathscr{L})$. Since the first letter of t is F, we know $c(t) > 0$, thus $l > 0$. By definition of $\mathrm{tm}_l(\mathscr{L})$ there are $G \in \mathscr{F}$, $r \in \mathbb{N}$ and $s_1, ..., s_r \in \mathrm{tm}_{l-1}(\mathscr{L})$ such that $t = G(s_1,...,s_r)$. By 2.3.36 we have $G = F$, $r = n$ and $s_i = t_i$ $(1 \leq i \leq n)$. It follows that $t_i = s_i \in \mathrm{tm}_{l-1}(\mathscr{L})$ $(1 \leq i \leq n)$, hence by definition of the complexity, $\max\{c(t_1), ..., c(t_n)\} \leq l-1$. Since $\max\{c(t_1), ..., c(t_n)\} = k$ we get the contradiction $k \leq l - 1 = c(t) - 1 < (1 + k) - 1 = k$. $\square$

Recall from 2.3.12 that a term s is called a **subterm** of a term t, if s occurs in t. We want to show that the subterm relation is reasonable, which means the following A term t is built up (or 'constructed') starting with constant symbols and variables by repeatedly concatenating function symbols with brackets, commas and previously build terms in the form $F(t_1, \dots, t_n)$. Every term that is used in this construction process, clearly is a subterm of t in the sense of definition 2.3.12. However, it is a priori not clear why a term s that occurs as a string in t was indeed used to construct t. This is the content of 2.3.40 and of 2.3.39. We need a preparation.

2.3.38. **Lemma.** *Let t be a term and let s be a nonempty substring of t with $s \neq t$.*

(i) If s is an initial substring of t, then either s is in $\mathcal{C} \cup \mathcal{F} \cup \mathrm{Vbl}$, or, the number of opening brackets occurring in s is greater than the number of closing brackets occurring in s.

In either case, the number of opening brackets occurring in s is greater than or equal to the number of closing brackets occurring in s.

(ii) If s is a terminal substring of t, then either $t = Fs$ for some function symbol F, or the number of opening brackets occurring in s is less than the number of closing brackets occurring in s.

In either case, the number of opening brackets occurring in s is less than or equal to the number of closing brackets occurring in s.

Proof. Recall that the number of opening brackets occurring in a term is equal to the number of closing brackets occurring in that term.

(i) By induction on $c(t)$, where $c(t) = 0$ is clear by 2.3.34(iv). So assume $t = F(t_1, \ldots, t_n)$ with $F \in \mathcal{F}$, $\lambda(F) = n$ and terms $t_1, \ldots, t_n$ of lower complexity than $c(t)$. Let s be an initial segment of t. If s is of length ≤ 2, the assertion is clear by 2.3.34. Let s_0 be the string obtained from s by removing the first two letters. Since $s \neq t$, s_0 is an initial segment of the string

$$t_1, \ldots, t_n$$

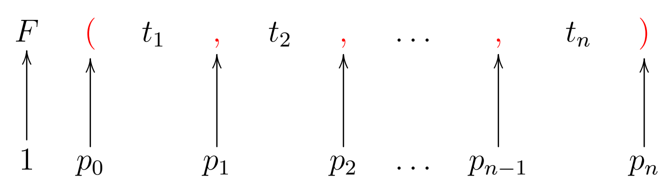
Using the induction hypothesis, we see that the number of opening brackets in s_0 is greater or equal to the the number of closing brackets in s_0. Since s is the string

$$F(s_0$$

we see that the number of opening brackets in s is bigger than the number of closing brackets in s.

(ii) follows from (i) applied to the initial substring s_0 of t for which t is $s_0 s$. $\square$

2.3.39. **Proposition.** *Let $t_1, \ldots, t_n$ be terms and let l_i be the length of t_i. Let F be a function symbol of arity n and suppose s is a subterm of $t = F(t_1, \ldots, t_n)$ occurring at position p. For $i \in \{1, \ldots, n-1\}$, let $p_i = l_1 + \ldots + l_i + i + 2$. Further, let $p_0 = 2$ and let p_n be the length of t. Here is a picture of the positions $p_0, \ldots, p_n$ in t.*



(Notice that the seemingly more intuitive definition of the $p_1, \ldots, p_n$ as the position "after" $t_1, \ldots, t_n$, would not be correct: for example, t_2 could occur in t_1, so "after t_2" is ambiguous) .

Then, either $p = 1$ and $s = t$, or, there is some $i \in \{1, \ldots, n\}$ such that $p_{i-1} < p < p_i$ and s is a subterm of t_i occurring at position $p - p_{i-1}$ in t_i.

Proof. If $p = 1$, then s is an initial segment of t and $s = t$ by 2.3.35.

So assume $p > 1$. Since the first letter of s is in $\mathrm{Vbl} \cup \mathcal{C} \cup \mathcal{F}$, we know $p \notin \{p_0, \ldots, p_n\}$. As $p > 1$, there is a unique $i \in \{1, \ldots, n\}$ with $p_{i-1} < p < p_i$ and it remains to show that s is a subterm of t_i occurring at position $p - p_{i-1}$ in t_i. Suppose this is not the case. Then the substring s_0 of t starting at position p and ending at position $p_i - 1$ is a nonempty, initial segment of s with $s_0 \neq s$. It follows that s is neither a variable nor a constant symbol, hence s_0 is neither a variable nor a constant symbol either. If s_0 were a function symbol, then this function symbol would be the last letter of t_i, which is impossible by the definition of 'term'. Thus, s_0 is not in $\mathcal{C} \cup \mathcal{F} \cup \mathrm{Vbl}$ and 2.3.38(i) implies that the number of opening brackets occurring in s_0 is greater than the number of closing brackets occurring in s_0. On the other hand, s_0 is also a terminal substring of t_i and this contradicts 2.3.38(ii). □

2.3.40. **Corollary.** *Let s be a subterm of t. Then $s = t$, or there are $n \in \mathbb{N}$, $F \in \mathscr{F}$ of arity n and $t_1, ..., t_n \in \mathrm{tm}(\mathscr{L})$ such that $t = F(t_1, t_2, ..., t_n)$ and s is a subterm of one of the t_i.*

Proof. This is an immediate consequence of 2.3.39. □

The assertion of corollary 2.3.40 could thus be used as an inductive definition of the subterm relation. Our reasoning in 2.3.39 and 2.3.38 would then prove that any term that is a substring of a term t, necessarily must be used in any construction of t. In fact, more is true. With the aid of 2.3.39 one can show easily that every occurrence of a term as a substring necessarily appears in any construction of t at some stage. The strength of 2.3.39 over its consequence 2.3.40 becomes apparent in the next proposition.

2.3.41. **Proposition.** *Let s be a subterm of a term t occurring at position p in t. Let r be another term. We define a new string u by replacing the substring s of t occurring at position p with the string r. Then u is again a term.*

Proof. By induction on the complexity of t: If $c(t) = 0$, then $s = t$ by 2.3.40 and therefore also $r = s$, thus $u = r = s = t$.

For the induction step we may assume that $t = F(t_1, \ldots, t_n)$. Choose the p_i as in 2.3.39. By 2.3.39, we know that for some i, we have $p_{i-1} < p < p_i$, and s occurs in t_i at position $p - p_{i-1}$. By induction, the string $\tilde{u}$ obtained from t_i by replacing the string s occurring at position $p - p_{i-1}$ with r, is again a term. consequently

$$u = F(t_1, \ldots, t_{i-1}, \tilde{u}, t_{i+1}, \ldots, n)$$

is a term, as required.

Notice that 2.3.40 alone would not suffice for a proof here, because we need to replace substrings at a prescribed position. The use of 2.3.40 would just give us that we may replace the subterm *at some occurrence*. □

Formulas

2.3.42. **Lemma.** *Let $\varphi \in \mathrm{Fml}(\mathscr{L})$. Then*

(i) φ is atomic if and only if the first letter of φ is in $\mathscr{R} \cup \mathscr{F} \cup \mathscr{C} \cup \mathrm{Vbl}$. Otherwise, the first letter of φ is an opening bracket.

(ii) Let $\varphi, \psi, \delta, \varepsilon \in \mathrm{Fml}(\mathscr{L})$ and let γ_1, γ_2 and γ_3 be defined as follows:

$$\gamma_1 \text{ is } (\neg\delta),$$
$$\gamma_2 \text{ is } (\varphi \rightarrow \psi) \text{ and}$$
$$\gamma_3 \text{ is } (\forall x \varepsilon) \text{ for some variable } x.$$

Furthermore, let $\gamma_0 \in$ at-$\mathrm{Fml}(\mathscr{L})$ be another formula.

If $i, j \in \{0, ..., 3\}$ with $i \neq j$, then γ_i is not an initial segment of γ_j.

Remark: For terms we had to prove a corresponding statement: see 2.3.34.

Proof. (i) If φ is atomic, then by inspection of the atomic formulas in definition 2.3.14, wee see that the first letter of φ is the first letter of a term, or it is in $\mathcal{R}$. By 2.3.34, we know that the first letter of any term is in $\mathscr{F} \cup \mathscr{C} \cup \mathrm{Vbl}$. Consequently, the first letter of φ is in $\mathscr{R} \cup \mathscr{F} \cup \mathscr{C} \cup \mathrm{Vbl}$.

If φ is not atomic, then φ is in $\mathrm{Fml}_{k+1}(\mathscr{L})$ for some $k \in \mathbb{N}$. By definition of $\mathrm{Fml}_{k+1}(\mathscr{L})$, we see that the first letter of φ is an opening bracket.

(ii) By (i), for every $i \in \{1, 2, 3\}$, the formula γ_0 and γ_i have a different first letter. Hence γ_0 is not an initial segment of γ_i and vice versa.

The formula γ_1 has a different letter than γ_3 in its second position. Hence γ_1 is not an initial segment of γ_3 and vice versa.

It remains to show that γ_2 is neither an initial segment of γ_1 nor of γ_3, and vice versa. To see this, it suffices to show that the first letter of φ is different from $\neg$ and different from $\forall$ (because these are the second letters of γ_1, γ_3 respectively). However, by (i), the first letter of φ is in $\mathscr{R} \cup \mathscr{F} \cup \mathscr{C} \cup \mathrm{Vbl}$, or it is an opening bracket. This proves the assertion. □

2.3.43. **Lemma.** *If $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$ and φ is an initial segment of ψ then $\varphi = \psi$.*

Remark: For terms the corresponding statement is 2.3.35.

Proof. We choose k such that $\varphi \in \mathrm{Fml}_k(\mathscr{L})$ and we show the following assertion by induction on $k \in \mathbb{N}_0$:

($*$) If $\psi \in \mathrm{Fml}(\mathscr{L})$ and φ is an initial segment of ψ or vice versa then $\varphi = \psi$.

If $k = 0$, then φ is atomic and by 2.3.42(i), also ψ is atomic. If φ is a term equality, i.e. of the form $t_1 \doteq t_2$, then also ψ has to be a term equality (compare the first letter). Then, using 2.3.35, we see that φ is equal to ψ. Hence φ and ψ both are of the form $R(t_1,...,t_n)$ and again by using 2.3.35, it follows easily that φ is equal to ψ.

For the induction step $k \Rightarrow k+1$ we may assume that $\varphi \in \mathrm{Fml}_{k+1}(\mathscr{L})$ is not atomic. By 2.3.42(ii) there are exactly three cases possible:

Case 1. $\varphi = (\neg\varphi_1)$ and $\psi = (\neg\psi_1)$, where $\varphi_1 \in \mathrm{Fml}_k(\mathscr{L})$ and $\psi_1 \in \mathrm{Fml}(\mathscr{L})$.

Case 2. $\varphi = (\varphi_1 \to \varphi_2)$ and $\psi = (\psi_1 \to \psi_2)$ where $\varphi_1, \varphi_2 \in \mathrm{Fml}_k(\mathscr{L})$ and $\psi_1, \psi_2 \in \mathrm{Fml}(\mathscr{L})$.

Case 3. $\varphi = (\forall x \varphi_1)$ and $\psi = (\forall y \psi_1)$, where $x, y \in \mathrm{Vbl}$, $\varphi_1 \in \mathrm{Fml}_k(\mathscr{L})$ and $\psi_1 \in \mathrm{Fml}(\mathscr{L})$.

In all three cases it is clear that φ_1 is an initial segment of ψ_1 or vice versa. As $\varphi_1 \in \mathrm{Fml}_k(\mathscr{L})$ the induction hypothesis implies $\varphi_1 = \psi_1$. Hence in case 1 and case 3 we get $\varphi = \psi$. In case 2 it follows that the string φ_2 is an initial segment of ψ_2 or vice versa. So again $\varphi_2 = \psi_2$ by induction and $\varphi = \psi$. □

2.3.44. **Theorem.** *(Unique readability theorem for formulas)*
Let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ be a language and let φ be an $\mathscr{L}$-formula. Then exactly one of the following holds true:

(i) φ is atomic and there are uniquely determined $t_1, t_2 \in \mathrm{tm}(\mathscr{L})$ such that φ is $t_1 \doteq t_2$, or

(ii) φ is atomic and there are a unique $n \in \mathbb{N}$, a unique $R \in \mathscr{R}$ and uniquely determined $\mathscr{L}$-terms $t_1, ..., t_n$ such that φ is $R(t_1,...,t_n)$, or

(iii) φ is equal to a string of the form $(\neg\psi)$ for a uniquely determined $\psi \in \mathrm{Fml}(\mathscr{L})$, or

(iv) φ is equal to a string of the form $(\varphi_1 \to \varphi_2)$ for uniquely determined $\varphi_1, \varphi_2 \in \mathrm{Fml}(\mathscr{L})$, or

(v) φ is equal to a string of the form $(\forall x \psi)$ for uniquely determined $\psi \in \mathrm{Fml}(\mathscr{L})$ and $x \in \mathrm{Vbl}$.

Proof. By 2.3.42(ii) it is clear that φ is equal to exactly one of the strings stated in (i)-(v). Now the uniqueness statements in (i)-(v) follow easily from 2.3.43. For example: Suppose φ is of the form $(\varphi_1 \to \varphi_2)$ as in (iv). If φ is also of the form $(\psi_1 \to \psi_2)$, then φ_1 is an initial segment of ψ_1 or vice versa. Hence by 2.3.43, $\varphi_1 = \psi_1$, which then implies $\varphi_2 = \psi_2$, thus $\varphi = \psi$. □

2.3.45. **Corollary.** *For all $\mathscr{L}$-formulas φ, ψ and every variable x we have*

$$c(\neg\varphi) = 1 + c(\varphi),\ c(\varphi \to \psi) = 1 + \max\{c(\varphi), c(\psi)\} \text{ and } c(\forall x \varphi) = 1 + c(\varphi).$$

Proof. We just show $c(\varphi \to \psi) = 1 + \max\{c(\varphi), c(\psi)\}$ the other two assertions are similar and easier.

Let δ be $(\varphi \to \psi)$ and let $k = \max\{c(\varphi), c(\psi)\}$. Then $\varphi, \psi \in \mathrm{Fml}_k(\mathscr{L})$ by definition of the complexity (for formulas) and so $\delta \in \mathrm{Fml}_{k+1}(\mathscr{L})$. By definition of the complexity again, this means $c(\delta) \leq 1 + k$. Suppose $c(\delta) < 1 + k$. We write $l := c(\delta)$. Then $\delta \in \mathrm{Fml}_l(\mathscr{L})$. Since the first letter of δ is an opening bracket we know $c(\delta) > 0$, thus $l > 0$. By definition of $\mathrm{Fml}_l(\mathscr{L})$ we know that δ is of the form $\neg(\delta_0)$, or, $(\forall x\ \delta_0)$, or, $(\delta_0 \to \delta_1)$ for some formulas $\delta_0, \delta_1 \in \mathrm{Fml}_{l-1}(\mathscr{L})$ and some variable x. Using 2.3.44 we know that δ_0 is φ and δ_1 is ψ. It follows that $\varphi, \psi \in \mathrm{Fml}_{l-1}(\mathscr{L})$, hence by definition of the complexity, $\max\{c(\varphi), c(\psi)\} \leq l - 1$. Since $\max\{c(\varphi), c(\psi)\} = k$ we get the contradiction $k \leq l - 1 = c(\delta) - 1 < (1 + k) - 1 = k$. □

As for terms, we need to verify that the subformula relation is reasonable, i.e. that every subformula of a formula φ is indeed used when φ is "constructed"; this is the content of 2.3.48. We need a preparation, similar to 2.3.38 for terms.

2.3.46. **Lemma.** *Let φ be a formula that is not atomic and let s be a nonempty substring of φ with $s \neq \varphi$.*

(i) If s is an initial substring of φ, then the number of opening brackets occurring in s is greater than the number of closing brackets occurring in s.

(ii) If s is a terminal substring of t, then the number of opening brackets occurring in s is less than the number of closing brackets occurring in s.

Proof. Recall that the number of opening brackets occurring in a formula is equal to the number of closing brackets occurring in that formula.

(i) By induction on $c(\varphi)$, where $c(\varphi) = 0$ is trivial. So assume φ is equal to $(\neg\psi)$, or equal to $(\forall x\ \psi)$, or equal to $(\psi \to \delta)$, where ψ, δ are of lower complexity than $c(\varphi)$. By the induction hypothesis we know the lemma for ψ and δ instead of φ.

Let s_0 be the substring of s obtained by removing the first letter.

Case 1. φ is equal to $(\neg\psi)$.

Since s is an initial segment of φ and s is different from φ, the string s_0 is an initial segment of the string $\neg\psi$. Hence the substring s_1 of s_0 obtained by removing the first letter is an initial substring of ψ. Since we have removed the opening bracket and the $\neg$ - symbol from s to obtain s_1 it is obviously enough to show that the number of opening brackets occurring in s_1 is greater than or equal to the number of closing brackets occurring in s_1.

However, either s_1 is ψ, in which case this is true, or, s_1 is an initial segment of ψ with $s_1 \neq \psi$ and we may use the induction hypothesis (when s_1 is empty, or when ψ is atomic we don't need induction of course).

This shows the lemma in case 1.

Case 2. φ is equal to $(\forall x\ \psi)$.

This is shown as in case 1; just work with s_1 as being the substring of s_0 obtained by removing the first two letters (observe that s_0 is an initial segment of $\forall x\ \psi$ in case 2).

Case 3. φ is equal to $(\psi \to \delta)$.

Since s is an initial segment of φ and s is different from φ, the string s_0 is an initial segment of the string $\psi \to \delta$. If the length of s_0 is less than or equal to the length of ψ, then using the induction hypothesis we know that the number of opening brackets occurring in s_0 is greater than or equal to the number of closing brackets occurring in s_0; this proves assertion (i).

If the length of s_0 is greater than the length of ψ, then let s_1 be the terminal segment of s_0 such that the string $\psi \to\ s_1$ is equal to $\psi \to \delta$. Then s_1 is an initial segment of δ and using the induction hypothesis we know that the number of opening brackets occurring in s_1 is greater than or equal to the number of closing brackets occurring in s_1. This again implies assertion (i).

(ii) follows from (i) applied to the initial substring s_0 of φ for which φ is $s_0 s$. □

2.3.47. **Lemma.** *Let ψ, δ be formulas and let φ be a subformula of $(\psi \to \delta)$ occurring at position p. Let l be the length of ψ. Then φ is $(\psi \to \delta)$, or, $2 \leq p \leq l+1$ and φ is a subformula of ψ occurring at position $p-1$, or, $l+3 \leq p$ and φ is a subformula of δ occurring at position $p-l-2$.*

Proof. If $l+3 \leq p$, then φ is a substring of the string

$$\delta)$$

Since φ is a formula, the number of opening brackets in φ is equal to the number of closing brackets in φ. Applying 2.3.46(ii) this entails that φ must be a subformula of δ.

Hence we may assume that $p \leq l+2$. Since φ is a formula, the first letter of φ is in $\mathcal{R} \cup \mathcal{F} \cup \mathcal{C} \cup \mathrm{Vbl}$, or it is an opening bracket. But this is not possible if p would be $l+2$ (which is the position of a $\to$ - symbol in $(\psi \to \delta)$).

Hence we may assume that $p \leq l+1$. If $p = 1$, then φ is an initial segment of $(\psi \to \delta)$ and φ is equal to $(\psi \to \delta)$ by 2.3.43.

Thus we may assume that $2 \leq p \leq l+1$ and it remains to show that φ is a subformula of ψ. Suppose this is not the case. Then the substring s of $(\psi \to \delta)$ starting at position p and ending at position $l-1$ is a nonempty initial segment of φ with $s \neq \varphi$. Further, φ is not atomic, since the symbol $\to$ occurs in φ. By 2.3.46(i), the number of opening brackets occurring in s is greater than the number of closing brackets occurring in s. On the other hand, s is also a terminal substring of ψ and this contradicts 2.3.46(ii) (ψ is not atomic since s contains an opening bracket). □

2.3.48. **Proposition.** *Suppose φ is a subformula of ψ.*

(i) If $c(\psi) = 0$ (equivalently: ψ is atomic), then $\varphi = \psi$.
(ii) Now suppose $c(\psi) = k+1$.
  (a) If $\psi = (\forall x \vartheta)$ or $\psi = (\neg \vartheta)$, then φ is ψ or φ is a subformula of ϑ.
  (b) If $\psi = (\psi_1 \to \psi_2)$, then $\varphi = \psi$, or φ is a subformula of ψ_1 or φ is a subformula of ψ_2.

Proof. (i). Firstly assume that ψ is atomic. Then no bracket appears in ψ. Hence no bracket appears in φ either and so φ is atomic, too. If φ is of the form $R(t_1, ..., t_n)$ then φ must occur at position 1 in ψ, since the only position at which a relation symbol can occur in an atomic formula is 1. By 2.3.43, we see that φ is ψ.

On the other hand if φ is of the form $t_1 \doteq t_2$, then also ψ is of this form (see the definition of "atomic formula"). Say ψ is $s_1 \doteq s_2$. Then, t_2 is an initial substring of s_2 and by 2.3.35 we know $t_2 = s_2$.

Further, t_1 is a terminal segment of s_1 and 2.3.38(ii) easily implies $s_1 = t_1$.

(ii)(a). Both cases a similar, we only do the case $\psi = (\forall x \vartheta)$. If φ is an initial segment of ψ, then φ is ψ by 2.3.43. Hence we may assume that φ is a substring of

$$\forall x \vartheta)$$

By 2.3.42(ii), the first letter of φ is in $\mathcal{R} \cup \mathcal{F} \cup \mathcal{C} \cup \mathrm{Vbl}$, or an opening bracket. Hence φ is a substring of

$$\vartheta)$$

and by 2.3.38(ii), φ cannot be a terminating segment of that string. Thus, φ is a substring of ϑ as required.

(ii)(b) is an immediate consequence of 2.3.47. ☐

2.3.49. **Theorem.** *Let ψ be a formula.*

(i) Let φ be a subformula of ψ occurring at position p in ψ. Let δ be another formula. We define a new string γ by replacing the substring φ of ψ occurring at position p with the string δ. Then γ is again a formula.

(ii) Let t be a term occurring in ψ at position p. Let s be another term. We define a new string γ by replacing the substring t of ψ occurring at position p with the string s. Then γ is again a formula.

Proof. (i) By induction on the complexity of ψ using 2.3.47: If $c(\psi) = 0$, then by 2.3.48(i), we know $\varphi = \psi$ and therefore also $\gamma = \delta$, which is a formula.

For the induction step we only do the difficult case, where ψ is $\psi_1 \to \psi_2$. Let l be the length of ψ_1. By 2.3.47, we know that φ is $(\psi_1 \to \psi_2)$, or, $2 \le p \le l+1$ and φ is a subformula of ψ_1 occurring at position $p-1$, or, $l+3 \le p$ and φ is a subformula of ψ_2 occurring at position $p-l-2$. If φ is $(\psi_1 \to \psi_2)$ then we are done and it remains to treat the other two cases.

Case 1. $2 \le p \le l+1$ and φ is a subformula of ψ_1 occurring at position $p-1$.

By induction, the string $\tilde{\gamma}$ obtained from ψ_1 by replacing the string φ at position $p-1$ with δ, is again a formula. consequently

$$\gamma = (\tilde{\gamma} \to \psi_2)$$

is a formula, as required.

Case 2. $l+3 \le p$ and φ is a subformula of ψ_2 occurring at position $p-l-2$.

By induction, the string $\tilde{\gamma}$ obtained from ψ_2 by replacing the string φ at position $p-l-2$ with δ, is again a formula. consequently

$$\gamma = (\psi_1 \to \tilde{\gamma})$$

is a formula, as required.

(ii) The only positions where a term can occur in ψ is within an atomic subformula φ of ψ (which follows from a trivial induction on the complexity of ψ). Let q be the position of the atomic subformula φ of ψ, such that $q \le p \le q+\text{length}(\varphi)$. Let $\tilde{\varphi}$ be the string obtained from φ by replacing t at position $q-p+1$ with s. Using 2.3.13 it follows easily that $\tilde{\varphi}$ is again formula.

It is clear that the string γ of 2.3.49(ii) is the string obtained from ψ by replacing φ at position q with $\tilde{\varphi}$. Thus by (i), γ is a formula. ☐

2.3.50. **Proposition.** *Let φ, ψ be $\mathscr{L}$-formulas.*

(i) If φ is quantifier free then $\mathrm{Fr}(\varphi)$ *is the set of variables occurring in φ.*

(ii) $\mathrm{Fr}(\neg\varphi) = \mathrm{Fr}(\varphi)$

(iii) $\mathrm{Fr}((\varphi \to \psi)) = \mathrm{Fr}(\varphi) \cup \mathrm{Fr}(\psi)$.

(iv) $\mathrm{Fr}(\forall x \varphi) = \mathrm{Fr}(\varphi) \setminus \{x\}$ *for all* $x \in \mathrm{Vbl}$.

Proof. (i). If φ is quantifier free, then by definition of 'free occurrence', every occurrence of a variable in φ is a free occurrence.

(ii). By definition of $\mathrm{Fr}(\varphi)$ it is enough to show for each $k \in \mathbb{N}$ and each variable x the following:

$$x \text{ occurs in } \varphi \text{ at position } k \text{ and } k \text{ is in the scope of } \forall x \text{ in } \varphi \text{ if and only if}$$
$$x \text{ occurs in } (\neg\varphi) \text{ at position } k+2 \text{ and } k+2 \text{ is in the scope of } \forall x \text{ in } (\neg\varphi).$$

$\Rightarrow$. If x occurs in φ at position k and k is in the scope of $\forall x$ in φ, then there is a subformula of the form $(\forall x\delta)$ of φ, of length $l \in \mathbb{N}$ that occurs at a position p in φ with $p \leq k < p+l$. Obviously x occurs in $(\neg\varphi)$ at position $k+2$ and by using 2.3.33 we see that $k+2$ is in the scope of $\forall x$ in $(\neg\varphi)$.

$\Leftarrow$. If x occurs in $(\neg\varphi)$ at position $k+2$ and $k+2$ is in the scope of $\forall x$ in $(\neg\varphi)$, then there is a subformula of the form $(\forall x\delta)$ of $(\neg\varphi)$, of length $l \in \mathbb{N}$ that occurs at a position p in $(\neg\varphi)$ with $p \leq k+2 < p+l$. Obviously $(\forall x\delta)$ is different from $(\neg\varphi)$ and so $(\forall x\delta)$ is a subformula of φ. This shows the assertion.

(iii) We first show $\mathrm{Fr}((\varphi \to \psi)) \subseteq \mathrm{Fr}(\varphi) \cup \mathrm{Fr}(\psi)$. Let x be a variable that occurs freely in $(\varphi \to \psi)$ at position k. Say $k \leq 2+$ length of φ. We claim that x occurs freely in φ at position $k-1$. Otherwise and because x occurs at position $k-1$ of φ, this occurrence is bound. I.e., there is a subformula of the form $(\forall x\delta)$ of φ occurring at a position p with $p \leq k-1 < p + \mathrm{length}(\forall x\delta)$. Using 2.3.33 we see that $(\forall x\delta)$ is a subformula of $(\varphi \to \psi)$ occurring at position $p+2$ and k is in the scope of $\forall x$ in $(\varphi \to \psi)$, contradicting our assumption that x occurs freely in $(\varphi \to \psi)$ at position k.

Now we show $\mathrm{Fr}((\varphi \to \psi)) \supseteq \mathrm{Fr}(\varphi) \cup \mathrm{Fr}(\psi)$. Let $x \in \mathrm{Fr}(\varphi) \cup \mathrm{Fr}(\psi)$. We do the case $x \in \mathrm{Fr}(\varphi)$, the case $x \in \mathrm{Fr}(\psi)$ is similar. Thus, x occurs freely in φ at a position k. We claim that x occurs freely in $(\varphi \to \psi)$ at position $k+1$. Otherwise and because x occurs at position $k+1$ of $(\varphi \to \psi)$, this occurrence is bound. I.e., there is a subformula of the form $(\forall x\delta)$ of $(\varphi \to \psi)$ occurring at a position p with $p \leq k+1 < p + \mathrm{length}(\forall x\delta)$. Since $(\forall x\delta)$ is a subformula of $(\varphi \to \psi)$, $(\forall x\delta)$ is equal to $(\varphi \to \psi)$, or $(\forall x\delta)$ is a subformula of φ, or $(\forall x\delta)$ is a subformula of ψ. Comparing the strings and taking into account the position of $(\forall x\delta)$ in $(\varphi \to \psi)$ this is only possible if $(\forall x\delta)$ is a subformula of φ. Using 2.3.33 we see that $(\forall x\delta)$ is a subformula of φ occurring at position $p-2$ and k is in the scope of $\forall x$ in φ, contradicting our assumption that x occurs freely in φ at position k.

(iv). By definition, x is not in $\mathrm{Fr}(\forall x\varphi)$. Hence it is enough to show for each variable $y \neq x$ and every $k \in \mathbb{N}$ the following:

$$y \text{ occurs in } \varphi \text{ at position } k \text{ and } k \text{ is in the scope of } \forall y \text{ in } \varphi \text{ if and only if}$$
$$y \text{ occurs in } (\forall x\varphi) \text{ at position } k+3 \text{ and } k+3 \text{ is in the scope of } \forall y \text{ in } (\forall x\varphi).$$

This is shown similarly to the proof of (ii) using $y \neq x$ for the implication "$\Leftarrow$":

$\Rightarrow$. If y occurs in φ at position k and k is in the scope of $\forall y$ in φ, then there is a subformula of the form $(\forall y\delta)$ of φ, of length $l \in \mathbb{N}$ that occurs at a position p in

φ with $p \leq k < p+l$. Obviously y occurs in $(\forall x\varphi)$ at position $k+3$ and by using 2.3.33 we see that $k+3$ is in the scope of $\forall y$ in $(\forall x\varphi)$.

$\Leftarrow$. If y occurs in $(\forall x\varphi)$ at position $k+3$ and $k+3$ is in the scope of $\forall y$ in $(\forall x\varphi)$, then there is a subformula of the form $(\forall y\delta)$ of φ, of length $l \in \mathbb{N}$ that occurs at a position p in $(\forall x\varphi)$ with $p \leq k+3 < p+l$. Since $y \neq x$, $(\forall y\delta)$ is different from $(\forall x\varphi)$ and so $(\forall y\delta)$ is a subformula of φ. Now we use 2.3.33 again to show the assertion. $\square$

2.3.51. **Proposition.** *Let $\varphi \in \mathrm{Fml}(\mathscr{L})$, $t_1, ..., t_n, t \in \mathrm{tm}(\mathscr{L})$ and let $x_1, ..., x_n$ be n distinct variables.*

(i) $t(x_1/t_1, ..., x_n/t_n)$ is an $\mathscr{L}$-Term and if $\mathrm{Fr}(t) \subseteq \{x_1, ..., x_n\}$, then

$$\mathrm{Fr}(t(x_1/t_1, ..., x_n/t_n)) \subseteq \mathrm{Fr}(t_1) \cup ... \cup \mathrm{Fr}(t_n).$$

(ii) If for each $i \in \{1, ..., n\}$ the variable x_i is free in φ for t_i then the string $\varphi(x_1/t_1, ..., x_n/t_n)$ is an $\mathscr{L}$-formula and in the case $\mathrm{Fr}(\varphi) \subseteq \{x_1, ..., x_n\}$ we have

$$\mathrm{Fr}(\varphi(x_1/t_1, ..., x_n/t_n)) \subseteq \mathrm{Fr}(t_1) \cup ... \cup \mathrm{Fr}(t_n).$$

Proof. (i) We proceed by induction on the complexity of t. If t is a constant symbol c, then $t(x_1/t_1, ..., x_n/t_n)$ is c and we are done. If t is a variable x, then $t(x_1/t_1, ..., x_n/t_n)$ is t_i if $x = x_i$ and $t(x_1/t_1, ..., x_n/t_n)$ is t otherwise. In both cases we are done.

For the induction step, assume $t = F(s_1, \ldots, s_k)$ and assume we know (i) already for the terms $s_1, \ldots, s_k$. Then

$$(*) \qquad t(x_1/t_1, ..., x_n/t_n) = F(s_1(x_1/t_1, ..., x_n/t_n), \ldots, s_k(x_1/t_1, ..., x_n/t_n))$$

is a term. Since all (free) variables of t are among $x_1, \ldots, x_n$, the free variables of $t = F(s_1, \ldots, s_k)$ are among $x_1, \ldots, x_n$, the free variables of each s_i are among $x_1, \ldots, x_n$. By induction, the free variables of $s_i(x_1/t_1, ..., x_n/t_n)$ are in $\mathrm{Fr}(t_1) \cup ... \cup \mathrm{Fr}(t_n)$. Thus, $(*)$ shows that

$$\mathrm{Fr}(t(x_1/t_1, ..., x_n/t_n)) \subseteq \mathrm{Fr}(t_1) \cup ... \cup \mathrm{Fr}(t_n).$$

(ii). By induction on the complexity of φ. If φ is atomic, then the assertion follows easily from (i); notice that any variable that occurs in an atomic formula, is a free variable of that formula.

For the induction step, we only do the case where φ is $\forall x\psi$. The other two cases are done similar to the proof of (i).

Claim. For each $i \in \{1, \ldots, n\}$ with $x_i \neq x$, the variable x_i is free in ψ for t_i.

To see this, assume p is the position of a free occurrence of x_i in ψ. As $x_i \neq x$, the variable x_i occurs freely in φ at position $p+3$ and by assumption x_i is not in the scope of a quantifier $\forall y$ in φ, where y is any variable occurring in t_i. Clearly then, x_i at position p in ψ is not in the scope of such a quantifier $\forall y$ in ψ either. This shows the claim.

Case 1. $x \neq x_i$ for all i.

By definition and using $x \neq x_i$, for each $p \in \mathbb{N}$ and all $i \in \{1, \ldots, n\}$, the variable x_i is free in ψ at position p if and only if x_i is free in φ at position $p+3$.

It follows that

$$\Big(\forall x \psi\Big)(x_1/t_1, ..., x_n/t_n) = \forall x \Big(\psi(x_1/t_1, ..., x_n/t_n)\Big).$$

Using induction we know that $\psi(x_1/t_1, ..., x_n/t_n)$ is a formula and its free variables are in in $\mathrm{Fr}(t_1) \cup ... \cup \mathrm{Fr}(t_n) \cup \{x\}$, provided the free variables of φ are among $x_1, \ldots, x_n$. But then $\varphi(x_1/t_1, ..., x_n/t_n)$ is a formula whose free variables are in $\mathrm{Fr}(t_1) \cup ... \cup \mathrm{Fr}(t_n)$, provided the free variables of φ are among $x_1, \ldots, x_n$.

Case 2. $x = x_i$.

W.l.o.g. $i = n$. Then x_1 is not a free variable of φ and we may apply case 1 to $x_2, t_2, \ldots, x_n, t_n$. □

2.4. **Structures and Tarski's Definition of Truth.**

Throughout, $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ denotes a formal language.

2.4.1. **Definition.** An **$\mathscr{L}$-structure** is a tuple

$$\mathscr{M} = \Big(M\ ,\ (R^{\mathscr{M}} \mid R \in \mathscr{R})\ ,\ (F^{\mathscr{M}} \mid F \in \mathscr{F})\ ,\ (c^{\mathscr{M}}, c \in \mathscr{C})\Big)$$

consisting of

(S1) A nonempty set M, called the **universe** or the **domain** or the **carrier** of $\mathscr{M}$. We shall also write $|\mathscr{M}|$ instead of M.

(S2) A family $(R^{\mathscr{M}} \mid R \in \mathscr{R})$ of relations of M such that for $R \in \mathscr{R}$, $R^{\mathscr{M}} \subseteq M^{\lambda(R)}$. Hence $R^{\mathscr{M}}$ is a $\lambda(R)$-ary relation of M, called the **interpretation of R in $\mathscr{M}$**. Observe that for different $R_1, R_2 \in \mathscr{R}$ we may have $R_1^{\mathscr{M}} = R_2^{\mathscr{M}}$.

Formally, $(R^{\mathscr{M}} \mid R \in \mathscr{R})$ is a map $\mathscr{R} \longrightarrow \bigcup_{n\in\mathbb{N}} \mathfrak{P}(M^n)$ such that the image $R^{\mathscr{M}}$ of $R \in \mathscr{R}$ under this map is a subset of $M^{\lambda(R)}$.

(S3) A family $(F^{\mathscr{M}} \mid F \in \mathscr{F})$ of functions, where for $F \in \mathscr{F}$, $F^{\mathscr{M}} : M^{\mu(F)} \longrightarrow M$. Hence $F^{\mathscr{M}}$ is a $\mu(F)$-ary function of M, called the **interpretation of F in $\mathscr{M}$**. Observe that for different $F_1, F_2 \in \mathscr{F}$ we may have $F_1^{\mathscr{M}} = F_2^{\mathscr{M}}$.

Formally, $(F^{\mathscr{M}} \mid F \in \mathscr{F})$ is a map $\mathscr{F} \longrightarrow \bigcup_{n\in\mathbb{N}} \mathrm{Maps}(M^n, M)$ such that the image $F^{\mathscr{M}}$ of $F \in \mathscr{F}$ under this map is a function $M^{\mu(F)} \longrightarrow M$.

(S4) A family $(c^{\mathscr{M}} \mid c \in \mathscr{C})$ of elements of M. Hence $c^{\mathscr{M}}$ is an element of M, called the **interpretation of c in $\mathscr{M}$**. Observe that for different $c_1, c_2 \in \mathscr{C}$ we may have $c_1^{\mathscr{M}} = c_2^{\mathscr{M}}$.

Formally, $(c^{\mathscr{M}} \mid c \in \mathscr{C})$ is simply a map $\mathscr{C} \longrightarrow M$.

$\mathscr{M}$ is called **finite**/**countable**/**uncountable**/**infinite** if its universe $|\mathscr{M}|$ is finite/countable/uncountable/infinite. More generally, the **size of a structure**, or **cardinality of a structure** $\mathscr{M}$ is the cardinality of its universe. In symbols: $\mathrm{card}(\mathscr{M})$ is defined as $\mathrm{card}(|\mathscr{M}|)$.

2.4.2. *Examples.* We give a list of examples of structures in various languages. Note that in order to state an example of a structure we have to do three things:

(a) First we have to specify the language we are working in.
(b) We need to specify what the universe of the structure is.
(c) We need to specify the interpretation in our structure of each of the non-logical symbols in the chosen language.

(1) An example (denoted by $\mathscr{M}$) in the language of a binary relation.
  (a) Here the language has exactly one binary relation symbol R and no other non-logical symbols.
  (b) We choose the universe of $\mathscr{M}$ to be the powerset of $\mathbb{C}$, hence $|\mathscr{M}| = \mathfrak{P}(\mathbb{C})$.

(c) We interpret R in $\mathscr{M}$ as the inclusion between subsets of $\mathbb{C}$. More formally we define

$$R^{\mathscr{M}} = \{(A, B) \in \mathfrak{P}(\mathbb{C}) \times \mathfrak{P}(\mathbb{C}) \mid A \subseteq B\}$$

Thus, $\mathscr{M}$ is really just the poset $(\mathfrak{P}(\mathbb{C}), \subseteq)$.

(2) Another example in the language of a binary relation.

(a) Again the language is the language of a binary relation symbol R.

(b) We choose the universe of $\mathscr{M}$ to be the set $\mathbb{Z}$ of integers.

(c) We interpret R in $\mathscr{M}$ as the set

$$R^{\mathscr{M}} = \{(k, k+1) \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

Note that in order to define an $\mathscr{L}$-structure $\mathscr{M}$ whose universe is $\mathbb{Z}$ we can in fact specify *any* set as being $\mathscr{R}^{\mathscr{M}}$, subject to only one restriction: $R^{\mathscr{M}}$ has to be a subset of $\mathbb{Z}^2$ (the '2' here is communicated by saying that R is 'binary', i.e the arity of R is $\lambda(R) = 2$.)

(3) An example in the language of a unary function symbol.

(a) Here the language has no relation symbols, no constant symbols and exactly one function symbol f and this is unary (i.e., $\mu(f) = 1$).

(b) We choose the universe of $\mathscr{M}$ to be the set $\mathbb{Z}$ of integers.

(c) We interpret f in $\mathscr{M}$ as the function $f^{\mathscr{M}} : \mathbb{Z} \longrightarrow \mathbb{Z}$ defined by

$$f^{\mathscr{M}}(k) = k + 1.$$

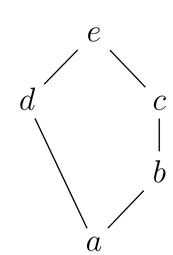
This structure is very similar to the structure in item **(2)**, but notice it is a structure in a different language, and so it is indeed different from the structure in the previous item.

(4) An example of a finite structure

(a) Here the language has the non-logical symbols $R, \top$ and $\perp$, where R is a binary relation symbol and $\top$ (called "top") and $\perp$ (called "bottom") are constant symbols.

(b) We choose five elements a, b, c, d, e (these could be the numbers 1,2,3,4,5) and let the universe of $\mathscr{M}$ consist of these 5 elements.

(c) We interpret $\top^{\mathscr{M}} = e$, $\perp^{\mathscr{M}} = a$ and we interpret R as the partially ordered set given by the diagram



Recall that by definition of a poset, this also forces the pairs $(a, c), (a, e)$ and (b, e) to be in $\mathscr{R}^{M}$. The structure $\mathscr{M}$ is a poset with a largest and a smallest element.

(5) An example of a group and a designated subgroup with a constant symbol.
  (a) Here the language "is" $\mathscr{L} = \{f, R, c\}$, where f is a binary function symbol, R is a unary relation symbol and c is a constant symbol.
  (b) We choose the universe of $\mathscr{M}$ to be the set $\mathbb{R}^{>0}$ of positive real numbers.
  (c) We interpret f in $\mathscr{M}$ as the multiplication function $f^{\mathscr{M}} : \mathbb{R}^{>0} \times \mathbb{R}^{>0} \longrightarrow \mathbb{R}^{>0}$. The relation symbol R is interpreted in $\mathscr{M}$ as $R^{\mathscr{M}} = \mathbb{Q}^{>0}$ The constant symbol c is interpreted in $\mathscr{M}$ as $c^{\mathscr{M}} = 1$.

Hence $R^{\mathscr{M}}$ is the (universe of) a subgroup of $(\mathbb{R}^{>0}, \cdot)$.

(6) An example of a field with two constant symbols and a designated subset.
  (a) Here the language $\mathscr{L}$ has similarity type $\{R, F, G, c, d\}$, where F, G are binary function symbols, R is a unary relation symbol and c, d are constant symbols.
  (b) We choose the universe of $\mathscr{M}$ to be the set $\mathbb{R}$ of real numbers.
  (c) We interpret F in $\mathscr{M}$ as the addition function $F^{\mathscr{M}} : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ and G as the multiplication function $G^{\mathscr{M}} : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$. The relation symbol R is interpreted in $\mathscr{M}$ as the nonnegative, rational numbers. The constant symbol c is interpreted in $\mathscr{M}$ as $c^{\mathscr{M}} = 0$ and d is interpreted as $d^{\mathscr{M}} = 1$.

(7) (a) Here the language is $\mathscr{L} = \{f, R\}$, where f is a unary function symbol and R is a ternary (i.e. "of arity 3") relation symbol.
  (b) We choose the universe of $\mathscr{M}$ to be the unit interval $[0, 1]$ of the real numbers.
  (c) We interpret f in $\mathscr{M}$ as the function $f^{\mathscr{M}} : [0, 1] \longrightarrow [0, 1]$ defined by

$$f^{\mathscr{M}}(t) = e^{t-1}.$$

(note that we may **not** define $f^{\mathscr{M}}(t) = e^t$ - why?) and the relation symbol R as the betweenness relation of $[0, 1]$:

$$R^{\mathscr{M}} = \{(a, b, c) \in [0, 1]^3 \mid b \text{ is between } a \text{ and } c\}$$

(8) In these examples we return to the language considered in 2.3.9, whose signature is $\{R, F, G, c, d\}$ where R is a binary relation symbol, F, G are binary function symbols and c, d are constant symbols. Then the following are examples of $\mathscr{L}$-structures (we are now expressing items (a),(b),(c) from the instruction at the beginning of 2.4.2 in a more compressed form):
  (i) Take $M = \mathbb{R}$, $R^{\mathscr{M}} = \{(a, b) \in \mathbb{R}^2 : a \leq b\}, F^{\mathscr{M}}(a, b) = a + b, G^{\mathscr{M}}(a, b) = a \cdot b, c^{\mathscr{M}} = 0, d^{\mathscr{M}} = 1$.
  (ii) Same as in (i), but this time with $M = \mathbb{Q}$ and addition and multiplication restricted to $\mathbb{Q}$.
  (iii) Or we could take $M = \mathbb{R}$, $R^{\mathscr{M}} = \{(a, b) \in \mathbb{R}^2 : a^2 + b^2 = 1\}, F^{\mathscr{M}}(a, b) = a^2 + b^2, G^{\mathscr{M}}(a, b) = a^3 + b^3, c^{\mathscr{M}} = -1, d^{\mathscr{M}} = 1$.

(iv) Or we could take a set M with six elements $M = \{a_1, a_2, a_3, b_1, b_2, b_3\}$ and choose $c^{\mathscr{M}} = a_1, d^{\mathscr{M}} = b_1,\ R^{\mathscr{M}} = \{(a_i, b_j) : i, j = 1, 2, 3\}$ and

$$F^{\mathscr{M}}(a,b) = \begin{cases} a_1 \text{ if } a \neq b \\ b_1 \text{ if } a = b \end{cases} \qquad G^{\mathscr{M}}(a,b) = \begin{cases} a_2 \text{ if } a \neq b \\ b_2 \text{ if } a = b \end{cases} .$$

Note how different these are. All they have in common is their property of having a 'structure' as prescribed by the similarity type of $\mathscr{L}$: Each has two distinguished elements, a distinguished subset of the square of the universe, and two distinguished binary functions.

Also compare the examples in **(8)** with example **(6)**: Is example **(6)** another example of the language used in **(8)**?

We now turn to the definition of truth of formulas in $\mathscr{L}$-structures and we first need to talk about

Interpreting terms in $\mathscr{L}$-structures

We can interpret terms of $\mathscr{L}$ (defined in 2.3.6) in our $\mathscr{L}$-structures. Informally, terms define functions simply by interpreting n-ary function symbols as functions $M^n \to M$ and constant symbols as elements of M, and by interpreting variable symbols as variables ranging over M.

For instance, suppose we have a language $\mathscr{L} = \{F, G, c\}$ where F is a unary function symbol, G is a binary function symbol and c is a constant symbol. Consider the $\mathscr{L}$-structure $\mathscr{M} = (\mathbb{N}, F^{\mathscr{M}}, G^{\mathscr{M}}, c^{\mathscr{M}})$, where $M = \mathbb{N}, F^{\mathscr{M}}(a) = a^2, G^{\mathscr{M}}(a,b) = a + b$ and $c^{\mathscr{M}} = 5$. Then the term

$$G(c, F(x))$$

gives the function $\mathbb{N} \to \mathbb{N}$ defined by

$$\begin{aligned} a \mapsto\ & G^{\mathscr{M}}(c^{\mathscr{M}}, F^{\mathscr{M}}(a)) \\ &= c^{\mathscr{M}} + F^{\mathscr{M}}(a) \\ &= 5 + a^2. \end{aligned}$$

That is, the interpretation of this term in this structure gives the function $a \mapsto 5+a^2$. For a second example, consider the term

$$F(G(c, G(x, F(y)))).$$

We can unravel this as follows:

$$\begin{aligned} F^{\mathscr{M}}(G^{\mathscr{M}}(c^{\mathscr{M}}, G^{\mathscr{M}}(a, F^{\mathscr{M}}(b)))) &= (G^{\mathscr{M}}(c^{\mathscr{M}}, G^{\mathscr{M}}(a, F^{\mathscr{M}}(b))))^2 \\ &= (c^{\mathscr{M}} + G^{\mathscr{M}}(a, F^{\mathscr{M}}(b)))^2 \\ &= (5 + a + F^{\mathscr{M}}(b))^2 \\ &= (5 + a + b^2)^2. \end{aligned}$$

So this term, interpreted in $\mathscr{M}$ gives the function $\mathbb{N}^2 \to \mathbb{N}$ defined by

$$(a, b) \mapsto F^{\mathscr{M}}(G^{\mathscr{M}}(c^{\mathscr{M}}, G^{\mathscr{M}}(a, F^{\mathscr{M}}(b)))).$$

Now we give the formal definition. The informal way above is the right way to think about it, but for proving statements about terms in general we need a robust notion:

2.4.3. **Definition.** Let $\mathscr{L}$ be a language and let $\mathscr{M}$ be an $\mathscr{L}$-structure with universe M.

(i) An **assignment** or a **valuation** of an $\mathscr{L}$-structure $\mathscr{M}$ is a map

$$h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|.$$

In the literature, also the pair (M, h) is called a valuation. Given an assignment h of $\mathscr{M}$, a variable x and an element $a \in |\mathscr{M}|$ we denote by $h\binom{x}{a}$ the assignment of $\mathscr{M}$ which differs from h only at the variable x, with value a at x:

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

(ii) We define by induction on the complexity of an $\mathscr{L}$-term t an element $t^{\mathscr{M}}[h] \in M$ for each assignment h of $\mathscr{M}$ as follows:

(a) If $c(t) = 0$, then

$$t^{\mathscr{M}}[h] = \begin{cases} t^{\mathscr{M}} & \text{if } t \in \mathscr{C} \\ h(t) & \text{if } t \in \mathrm{Vbl}\,. \end{cases}$$

(b) If $t_1, \ldots, t_n$ are $\mathscr{L}$-terms and $F \in \mathscr{F}$ with $\mu(F) = n$, then we define

$$F(t_1, \ldots, t_n)^{\mathscr{M}}[h] := F^{\mathscr{M}}(t_1^{\mathscr{M}}[h], \ldots, t_n^{\mathscr{M}}[h]).$$

This is a correct definition by 2.3.10 and is addressed further in question 40 of the example sheet.

Given a term t of $\mathscr{L}$, we may thus define a function

$$t^{\mathscr{M}} : M^{\infty} \to M,$$

where $M^{\infty} = \{\bar{m} : \bar{m} = (m_1, m_2, m_3, \ldots, m_p, \ldots), m_p \in M, p \geq 1\}$, that is M^{∞} is the set of all infinite sequences of elements of M. So here an assignment $h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|$ is denoted as a sequence $\bar{m} = (h(v_1), h(v_2), h(v_3), \ldots)$.

It is easy to show that $t^{\mathscr{M}}[h]$ only depends on those elements $h(v_i)$ for which the variable v_i occurs in t; this is done in question 41 of the example sheet. This means that in practice, we can think of $t^{\mathscr{M}}$ as a function of finitely many variables, rather than infinitely many variables.

Above is the formal definition of $t^{\mathscr{M}}$, but in practice we continue to work out examples as we did with the example above. Here is another one.

2.4.4. *Example.* Let $\mathscr{L}$ be the language $\{f, g, c, d\}$, with binary function symbols f, g [23] and constant symbols c, d. Consider the term t defined as

$$f(g(g(f(x, x), g(x, y)), c), d)\ .$$

Hence t has two free variables namely x, y and in any $\mathscr{L}$-structure $\mathscr{M}$ it defines a function $t^{\mathscr{M}} : |\mathscr{M}|^2 \longrightarrow |\mathscr{M}|$. For example:

(i) Suppose our $\mathscr{L}$-structure is given by $M = \mathbb{Z},\ f^{\mathscr{M}}(k, n) = k + n,\ g^{\mathscr{M}}(k, n) = k - n,\ c^{\mathscr{M}} = 17,\ d^{\mathscr{M}} = 19$. Then for $k, n \in M = \mathbb{Z}$ we have

$$\begin{aligned}
t^{\mathscr{M}}(k, n) =& f^{\mathscr{M}}(g^{\mathscr{M}}(g^{\mathscr{M}}(f^{\mathscr{M}}(k, k), g^{\mathscr{M}}(k, n)), c^{\mathscr{M}}), d^{\mathscr{M}}) \\
=& g^{\mathscr{M}}(g^{\mathscr{M}}(f^{\mathscr{M}}(k, k), g^{\mathscr{M}}(k, n)), c^{\mathscr{M}}) + d^{\mathscr{M}} \\
=& g^{\mathscr{M}}(f^{\mathscr{M}}(k, k), g^{\mathscr{M}}(k, n)) - c^{\mathscr{M}} + 19 \\
=& f^{\mathscr{M}}(k, k) - g^{\mathscr{M}}(k, n) - 17 + 19 \\
=& 2k - (k - n) + 2 \\
=& k + n + 2.
\end{aligned}$$

So the function $t^{\mathscr{M}} : M^2 \to M$ is the function

$$\mathbb{Z}^2 \longrightarrow \mathbb{Z},\ (k, n) \mapsto k + n + 2.$$

(ii) For another example, we continue with the same language and the same term, but this time we take $\mathscr{M}$ as the $\mathscr{L}$-structure given by $M = \mathbb{R},\ f^{\mathscr{M}}(r, s) = r + s,\ g^{\mathscr{M}}(r, s) = r \cdot s,\ c^{\mathscr{M}} = 0,\ d^{\mathscr{M}} = 1$. Then, in this new $\mathscr{M}$, we have

$$t^{\mathscr{M}}(r, s) = 1 \text{ for all } r, s \in M,$$

as you should work out in question 42 of the example sheet.

So in this structure, the term t is interpreted as the function $\mathbb{R}^2 \longrightarrow \mathbb{R}$ with constant value 1.

---

[23] In this example we are choosing small letters for function symbols. In previous examples we wrote F, G. In the future we write even $+, \cdot$ if we want to analyze a structure where the function symbols are interpreted as addition and multiplication, for example if we want to analyze the integers with addition and multiplication, or the set of polynomials $\mathbb{R}[x]$ with real coefficients, equipped with addition and multiplication of polynomials.

2.4.5. **Tarski's Definition of Truth** Let $\mathscr{L}$ be a language and let $\mathscr{M}$ be an $\mathscr{L}$-structure with domain M.

(A) We define by induction on the complexity of an $\mathscr{L}$-formula φ and each assignment h of $\mathscr{M}$, the expression φ **is true in** $\mathscr{M}$ **at** h, or φ **holds in** $\mathscr{M}$ **at** h, or $\mathscr{M}$ **satisfies** φ **at** h, denoted by

$$\mathscr{M} \models \varphi[h],$$

as follows:

(i) If φ is of the form $t_1 \doteq t_2$ with $\mathscr{L}$-terms t_1, t_2 then

$$\mathscr{M} \models t_1 \doteq t_2\ [h] \iff t_1^{\mathscr{M}}[h] = t_2^{\mathscr{M}}[h].$$

If φ is of the form $R(t_1, \ldots, t_n)$ with $R \in \mathscr{R}$ of arity n and $t_1, \ldots, t_n \in \mathrm{tm}(\mathscr{L})$ then

$$\mathscr{M} \models R(t_1, \ldots, t_n)\ [h] \iff (t_1^{\mathscr{M}}[h], \ldots, t_n^{\mathscr{M}}[h]) \in R^{\mathscr{M}}.$$

(ii) For the induction step we take $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$, $x \in \mathrm{Vbl}$ and define

- $\mathscr{M} \models (\varphi \to \psi)[h] \iff$ if $\mathscr{M} \models \varphi[h]$ then $\mathscr{M} \models \psi[h]$,

- $\mathscr{M} \models (\neg\varphi)[h] \iff \mathscr{M} \not\models \varphi[h]$, i.e. $\mathscr{M} \models \varphi[h]$ does not hold

and

- $\mathscr{M} \models (\forall x \varphi)[h] \iff$ for all $a \in |\mathscr{M}|$ we have $\mathscr{M} \models \varphi[h(\frac{x}{a})]$.

This is a correct definition by the Unique Readability Theorem for formulas 2.3.17. The issue of well-definedness here is parallel to the case of terms, see the discussion in question 40 of the example sheet.

(B) Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ and let h be an assignment of $\mathscr{M}$.
$\mathscr{M}$ is called a **model of** Σ **at** h if

$$\mathscr{M} \models \sigma[h] \text{ for all } \sigma \in \Sigma.$$

We denote this by

$$\mathscr{M} \models \Sigma[h].$$

Some authors also use $\mathscr{M} \models_h \Sigma$ instead of $\mathscr{M} \models \Sigma[h]$. We say that Σ has a model if it has a model at some assignment. In this case, Σ is called **satisfiable**.

In particular, if Σ is a set of $\mathscr{L}$-sentences, it makes sense to write

$$\mathscr{M} \models \Sigma$$

and to say that $\mathscr{M}$ is a **model** of Σ. This indeed contains the claim that for sentences, truth at some assignment is actually independent of the assignment - as one would expect in a correct setup of the matter. The proof of that may be found in 2.4.12.

2.4.6. **Explanation** As with the interpretation of terms, this looks like a complicated definition. But it is much easier to get the idea by looking at examples. This has to be understood as informal, but it will give the necessary intuition.

(i) For instance let $\mathscr{L} = \{R, f, c\}$ where f is a unary function symbol, c is a constant symbol and R is a binary relation symbol. Let $\mathscr{M}$ be given by $M = \mathbb{R}, R^{\mathscr{M}} = \{(r,s) \in \mathbb{R}^2 : r < s\}, f^{\mathscr{M}}(r) = r^2$ and $c^{\mathscr{M}} = 0$. Let φ be the sentence of $\mathscr{L}$ defined as

$$\forall x(R(c,x) \rightarrow \exists y(x \doteq f(y))).$$

Interpreting this in $\mathscr{M}$, truth of φ in $\mathscr{M}$ expresses

$\forall x \in \mathbb{R}(0 < x \rightarrow \exists y \in \mathbb{R}(x = y^2))$ - **which is not a formula in our language**, (or in any language), but a way to communicate to the reader what φ means in the chosen $\mathscr{M}$.

So this is true in the chosen $\mathscr{L}$-structure $\mathscr{M}$ and we say that φ is true in $\mathscr{M}$.

In the same language, if we instead consider $\mathscr{M}$ given by $M = \mathbb{Q}$ and $R^{\mathscr{M}} = \{(r,s) \in \mathbb{Q}^2 : r < s\}, f^{\mathscr{M}}(r) = r^2$ and $c^{\mathscr{M}} = 0$, then in this new $\mathscr{M}$ our sentence φ says

$\forall x \in \mathbb{Q}(0 < x \rightarrow \exists y \in \mathbb{Q}(x = y^2))$ (which is again not an $\mathscr{L}$-formula)

But now φ is false in $\mathscr{M}$, as for instance $0 < 2$ but $2 \neq r^2$ for any rational y.

Next, in the same language, consider $\mathscr{M}$ given by $M = \mathbb{Q}$, $R^{\mathscr{M}} = \{(r,s) \in \mathbb{Q}^2 : r < s\}$ and $c^{\mathscr{M}} = 0$ (as in the previous example), but now we choose $f^{\mathscr{M}}(r) = 2r$. Then in this $\mathscr{M}$ our sentence φ means

$\forall x \in \mathbb{Q}(0 < x \rightarrow \exists y \in \mathbb{Q}(x = 2y))$ (which not an $\mathscr{L}$-formula)

which is true, so we say that φ is true in this $\mathscr{M}$.

(ii) For another example, let $\mathscr{L}$ have a binary relation symbol R, a unary function symbol f and constant symbols c, d. Let $\mathscr{M}$ be given by $M = \mathbb{Q}, R^{\mathscr{M}} = \{(r,s) \in \mathbb{Q}^2 : r < s\}, f^{\mathscr{M}}(r) = r^2, c^{\mathscr{M}} = 0, d^{\mathscr{M}} = 1$. Let φ be the sentence of $\mathscr{L}$ defined as

$$\exists x(R(x, f(x)) \rightarrow (x \doteq c \wedge x \doteq d)).$$

Interpreted in $\mathscr{M}$ this says

$$\exists x \in \mathbb{Q}((x < x^2) \rightarrow (x = 0 \wedge x = 1)).$$

Now the $(x = 0 \wedge x = 1)$-part is always false. So the sentence will only be true if there is some $r \in \mathbb{Q}$ such that $r < r^2$ is false. (Then we will have 'false implies false', which is true.) There are such r, e.g. $r = 0$. So the sentence is true in $\mathscr{M}$.

(iii) If instead of a sentence φ, we consider an $\mathscr{L}$-formula φ with a free variable x, which we indicate by $\varphi(x)$, then φ doesn't make an assertion about a given $\mathscr{L}$-structure $\mathscr{M}$. However, if we are also given an element $m \in M$ $(= |\mathscr{M}|)$, then $\varphi(m)$, that is, "φ with m substituted for all free occurrences of x" does make an assertion, about m in $\mathscr{M}$.

For instance, continue with the language $\mathscr{L}$ from (i) that has a binary relation symbol R, a unary function symbol f and a constant symbols c. Let $M = \mathbb{Q}, R^{\mathscr{M}} = \{(r, s) \in \mathbb{Q} : r < s\}, f^{\mathscr{M}} = r^2$ and $c^{\mathscr{M}} = 0$. Consider the formula

$$R(c, x) \to \exists y(x \doteq f(y)).$$

Then if we interpret in $\mathscr{M}$ and "substitute 2 for the free occurrences of x" we get

$$0 < 2 \to \exists y \in \mathbb{Q}(2 = y^2) \text{ (which is not an } \mathscr{L}\text{-formula)}$$

And this is false (as $0 < 2$ and therefore $\exists y \in \mathbb{Q}(2 = y^2)$ is false), so we say $\varphi(2)$ is false in $\mathscr{M}$. On the other hand, if we interpret in $\mathscr{M}$ and "substitute 4 for the free occurrences of x" we get

$$0 < 4 \to \exists y \in \mathbb{Q}(4 = y^2). \text{ (which is not an } \mathscr{L}\text{-formula)}$$

And this is true. So we say that $\varphi(4)$ is true in $\mathscr{M}$.

2.4.7**. What is the role of "assignments" in the Truth Definition** The explanation in 2.4.6(iii) hints at the intended meaning of the assignment h in definition 2.4.5: The function $h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|$ takes on the role of "substituting elements of the universe for variables that occur freely in the formula". This is parallel to the role of assignments for terms, see 2.4.3. Like for evaluation of terms, for each fixed formula φ the truth of φ in $\mathscr{M}$ at some assignment h only depends on the values of h at the free variables of φ. For the interested reader this is shown in 2.4.12 of the appendix to this section.

An alternative definition of truth can then be read as follows (and you are welcome to use this definition throughout):

2.4.8. **The Truth Definition in different Form** Let $\mathscr{L}$ be a language and let $\mathscr{M}$ be an $\mathscr{L}$-structure with domain $M = |\mathscr{M}|$.

(A) (Compare with 2.4.5(A)) We define by induction on the complexity of an $\mathscr{L}$-formula $\varphi(x_1, \dots, x_n)$[24] and all $a_1, \dots, a_n \in M$ the expression "$\mathscr{M}$ satisfies φ at $(a_1, \dots, a_n)$"[25] and write

$$\mathscr{M} \models \varphi(a_1, \dots, a_n),$$

as follows:

(i) If φ is of the form $t_1 \doteq t_2$ with $\mathscr{L}$-terms t_1, t_2 then

$$\mathscr{M} \models \varphi(a_1, \dots, a_n) \iff t_1^{\mathscr{M}}(a_1, \dots, a_n) = t_2^{\mathscr{M}}(a_1, \dots, a_n).$$

If φ is of the form $R(t_1, \dots, t_k)$ with $R \in \mathscr{R}$ of arity k and $t_1, \dots, t_k \in \mathrm{tm}(\mathscr{L})$ then

$$\mathscr{M} \models \varphi(a_1, \dots, a_n) \iff (t_1^{\mathscr{M}}(a_1, \dots, a_n), \dots, t_k^{\mathscr{M}}(a_1, \dots, a_n)) \in R^{\mathscr{M}}.$$

(ii) For the induction step we take $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$, $x \in \mathrm{Vbl}$ and define

- $\mathscr{M} \models (\varphi \to \psi)(a_1, \dots, a_n) \iff$
  if $\mathscr{M} \models \varphi(a_1, \dots, a_n)$ then $\mathscr{M} \models \psi(a_1, \dots, a_n)$,

- $\mathscr{M} \models (\neg\varphi)(a_1, \dots, a_n) \iff$
  $\mathscr{M} \not\models \varphi(a_1, \dots, a_n)$ i.e. $\mathscr{M} \models \varphi(a_1, \dots, a_n)$ does not hold

and

- $\mathscr{M} \models (\forall y \varphi)(a_1, \dots, a_n) \iff$

$$\begin{cases} \mathscr{M} \models \varphi(a_1, \dots, a_n), & \text{if } y \text{ is not among the } x_i \\ \mathscr{M} \models \varphi(a_1, \dots, \underbrace{b}_{i^{\text{th}} \text{ position}}, \dots, a_n) \text{ for all } b \in |\mathscr{M}| & \text{, if } y = x_i. \end{cases}$$

(B) (Compare with 2.4.5(B)) Let Σ be a set of $\mathscr{L}$-formulas in at most n free variables $x_1, \dots, x_n$. Let $\bar{a} = (a_1, \dots, a_n) \in M$. The $\mathscr{L}$-structure $\mathscr{M}$ is called a **model of** Σ **at** $\bar{a}$ if

$$\mathscr{M} \models \sigma(\bar{a}) \text{ for all } \sigma \in \Sigma.$$

We denote this by

$$\mathscr{M} \models \Sigma(\bar{a}).$$

We say that Σ **has a model** (or that Σ is **satisfiable**) if it has a model $\mathscr{M}$ at some n-tuple with entries in $|\mathscr{M}|$.

---

[24]Recall that this is shorthand for saying that φ is an $\mathscr{L}$-formula with free variable in $\{x_1, \dots, x_n\}$; so for example every sentence is captured here, because a sentence does not have any free variables.

[25]We also say φ ia true/holds in $\mathscr{M}$ at $a_1, \dots, a_n$, or $\varphi(a_1, \dots, a_n)$ holds/is true in $\mathscr{M}$ or $\mathscr{M}$ satisfies $\varphi(a_1, \dots, a_n)$.

In particular, if Σ is a set of $\mathscr{L}$-sentences, so here $n = 0$, it makes sense to write

$$\mathscr{M} \models \Sigma$$

and to say that $\mathscr{M}$ is a **model** of Σ. This indeed contains the claim that for sentences, truth at some assignment is actually independent of the assignment - as one would expect in a correct setup of the matter. The proof of that may be found in 2.4.12.

2.4.9. *Example.* Let us work formally through an example of the Truth definition to see how it works. Normally, we proceed without it (as we did in the explanation 2.4.6). For the example, we may take $\mathscr{L} = \{P, f, g, c\}$ where P is a unary relation symbol, f, g are binary function symbols and c is a constant symbol. We take $\mathscr{M}$ to be given by $M = \{1, 2, 3, 4, \ldots,\}$, the positive integers, $P^{\mathscr{M}} = \{2, 3, 5, 7, 11, 13, \ldots\}$, the prime numbers, $f^{\mathscr{M}}(m, n) = m \cdot n$, $g^{\mathscr{M}}(m, n) = m + n$ and $c^{\mathscr{M}} = 2$. Let φ be the sentence

$$\forall x \exists y \exists z (g(f(c, x), c) \doteq g(y, z) \wedge P(y) \wedge P(z))$$

let $\vartheta(x, y, z)$ be the formula $g(f(c, x), c) \doteq g(y, z)$, let $\psi(y)$ be the formula $P(y)$ and let $\chi(z)$ be the formula $P(z)$. Note that the term $g(f(c, x), c)$ interpreted in $\mathscr{M}$ is the function $k \mapsto 2k + 2$.

Now let h be an assignment of $\mathscr{M}$, i.e., h is map $h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|$.

Then we have $\mathscr{M} \models \varphi[h] \iff$

$\iff$ for every $n \in M$ we have $\mathscr{M} \models (\exists y \exists z(\vartheta \wedge \psi \wedge \chi))[h\binom{x}{n}]$,

$\iff$ for every $n \in M$ there is $p \in M$ such that

$$\mathscr{M} \models (\exists z \vartheta \wedge \psi \wedge \chi)[h\binom{x}{n}\binom{y}{p}]$$

$\iff$ for every $n \in M$ there are $p, q \in M$ such that

$$\mathscr{M} \models (\vartheta \wedge \psi \wedge \chi)[h\binom{x}{n}\binom{y}{p}\binom{z}{q}]$$

$\iff$ for every $n \in M$ there are $p, q \in M$ such that

$$\mathscr{M} \models \vartheta[h\binom{x}{n}\binom{y}{p}\binom{z}{q}]$$

$$\text{and } \mathscr{M} \models \psi[h\binom{x}{n}\binom{y}{p}\binom{z}{q}]$$

$$\text{and } \mathscr{M} \models \chi[h\binom{x}{n}\binom{y}{p}\binom{z}{q}]$$

$\iff$ for every $n \in M$ there are $p, q \in M$ such that

$$2n + 2 = p + q \text{ and } p \text{ is prime and } q \text{ is prime}$$

$\iff$ every even natural number greater than 2 is the sum of two primes .

And this is Goldbach's conjecture. No one knows whether or not this is true.

We revisit some of the natural examples from 2.4.2.

2.4.10. *Examples.* We only indicate the languages and structures of these examples here, please have a look back at 2.4.2 if you want to see the full definition. In each of these examples we give a sentence that is true in the indicated structure. This can be verified formally, but it suffices that you informally can verify the truth of the sentence arguing like in 2.4.6 .

(1) Here $\mathscr{M}$ was $(\mathfrak{P}(\mathbb{C}), \subseteq)$ in the language of a binary relation R.
The sentence φ defined as

$$\forall x \forall y \forall z (R(x,y) \wedge R(y,z) \to R(x,z))$$

is true in $\mathscr{M}$ - this is just saying that the relation $R^{\mathscr{M}}$ on $\mathfrak{P}(\mathbb{C})$ is transitive. Recall that when we want to check if a sentence is true in a structure, all quantifiers range over the universe of that structure - in this case, the universe is the powerset of $\mathbb{C}$.

(2) Here $\mathscr{M}$ was the structure $(\mathbb{Z}, \{(k, k+1) \mid k \in \mathbb{Z}\})$ in the language of a binary relation R again. The sentence φ from the previous example is not true in $\mathscr{M}$. But the sentence

$$\Big(\forall x \exists y R(x,y)\Big) \wedge \Big(\forall x \forall y \forall z (R(x,y) \wedge R(x,z) \to y = z)\Big)$$

is true. It says that R is interpreted as the graph of a function from the universe of the structure to the universe of the structure.

(3) Here $\mathscr{M}$ was $(\mathbb{Z}, s)$, where $s(k) = k+1$ in the language of a unary function symbol f. The sentence

$$\forall x, y (f(x) \doteq f(y) \to x \doteq y)$$

is true in $\mathscr{M}$, because it says that the function s is injective. Note that this is not a sentence in the language of **(2)**, although the structures in **(3)** and **(2)** describe essentially the same mathematical object (in different cloths).

(4) This example was also a poset, but this time in the language whose non-logical symbols are $R, \top$ and $\bot$, where R is a binary relation symbol and $\top, \bot$ are constant symbols. We refer to 2.4.2**(4)** for structure $\mathscr{M}$ that we are considering here. In $\mathscr{M}$ the following sentence is true:

$$\forall x \forall y \exists z \Big(R(z,x) \wedge R(z,y) \wedge \forall u (R(u,x) \wedge R(u,y) \to R(u,z)) \Big)$$

This says that any two elements in the (universe of the) poset $\mathscr{M}$ have a greatest lower bound for the binary relation $R^{\mathscr{M}}$ (such posets are called "lattices").

We finish this section with a Proposition showing that our syntactic setup for replacing variables by terms in 2.3.30 is correct.

2.4.11. **Proposition.** *Let* $t, t' \in \mathrm{tm}(\mathscr{L})$, $\varphi \in \mathrm{Fml}(\mathscr{L})$ *and* $x \in \mathrm{Vbl}$. *Let* h *be an assignment of an* $\mathscr{L}$*-structure* $\mathscr{M}$ *and let* $a = t^{\mathscr{M}}[h]$.

(i) $(t'(x/t))^{\mathscr{M}}[h] = t'^{\mathscr{M}}[h\binom{x}{a}]$.
(ii) If x *is free in* φ *for* t *then* $\mathscr{M} \models \varphi(x/t)\ [h] \iff \mathscr{M} \models \varphi[h\binom{x}{a}]$.

Proof. This proof is not examinable and may be found in the appendix 2.4.13. □

Appendix to section 2.4

```
None of the proofs in this appendix is examinable. Only statements
that also occur outside of this appendix are examinable.
```

2.4.12. **Proposition.** *Let $\varphi(x_1, ..., x_n) \in \mathrm{Fml}(\mathscr{L})$, $t(x_1, ..., x_n) \in \mathrm{tm}(\mathscr{L})$ and let $\mathscr{M}$ be an $\mathscr{L}$-structure. If h and h' are assignments of $\mathscr{M}$ with $h(x_i) = h'(x_i)$ $(1 \leq i \leq n)$ then $t^{\mathscr{M}}[h] = t^{\mathscr{M}}[h']$ and*

$$\mathscr{M} \models \varphi[h] \iff \mathscr{M} \models \varphi[h'].$$

Proof. That $t^{\mathscr{M}}[h] = t^{\mathscr{M}}[h']$ has already been done in question 41 of the example sheets. We show that $\mathscr{M} \models \varphi[h] \ \Rightarrow \ \mathscr{M} \models \varphi[h']$. This also follows by a straightforward but lengthy induction on the complexity of φ using 2.3.27 to deal with the universal quantifier.

The base case: If the complexity of φ is zero, then φ is an atomic $\mathscr{L}$-formula, hence φ is of the form $t_1 \doteq t_2$ for some $\mathscr{L}$-terms t_1, t_2 or of the form $R(t_1, \ldots, t_n)$ for some relation symbol R of $\mathscr{L}$ of arity n and some terms $t_1, \ldots, t_n$ of $\mathscr{L}$. Now we know already that $t^{\mathscr{M}}[h] = t^{\mathscr{M}}[h']$ for all assignments h, h' that agree on the free variables of any term t, hence $\mathscr{M} \models \varphi[h]$ is immediate from its definition in 2.4.5(A)(i).

Now for the induction step. We need to deal with formulas of the form $(\neg\varphi)$, $(\varphi \to \psi)$ and $\forall y\, \psi$. So assume we know the assertion already for φ and ψ. Then

$$\begin{aligned} \mathscr{M} \models \neg\varphi[h] &\iff \mathscr{M} \not\models \varphi[h] \text{ by definition 2.4.5(A)(ii),} \\ &\iff \mathscr{M} \not\models \varphi[h'] \text{ by induction,} \\ &\iff \mathscr{M} \models \neg\varphi[h'] \text{ by definition again.} \end{aligned}$$

Further

$$\begin{aligned} \mathscr{M} \models (\varphi \to \psi)[h] &\iff \mathscr{M} \not\models \varphi[h] \text{ or } \mathscr{M} \models \psi[h] \text{ by definition 2.4.5(A)(ii),} \\ &\iff \mathscr{M} \not\models \varphi[h'] \text{ or } \mathscr{M} \models \psi[h'] \text{ by induction,} \\ &\iff \mathscr{M} \models (\varphi \to \psi)[h'] \text{ by definition again.} \end{aligned}$$

Finally suppose φ is $\forall y \psi$ and we know already the implication $\mathscr{M} \models \psi[h] \ \Rightarrow \ \mathscr{M} \models \psi[h']$ for all assignments h, h' of $\mathscr{M}$ that are identical on $\mathrm{Fr}(\psi)$. We show $\mathscr{M} \models \varphi[h] \ \Rightarrow \ \mathscr{M} \models \varphi[h']$ for assignments h, h' that are identical on $\{x_1, ..., x_n\}$. If $\mathscr{M} \models \varphi[h]$ then $\mathscr{M} \models \psi[h\binom{y}{a}]$ for all $a \in |\mathscr{M}|$ by definition 2.4.5(A)(ii). Now $h\binom{y}{a}(x_i) = h'\binom{y}{a}(x_i)$ $(1 \leq i \leq n)$ and both assignments are identical on y. Hence $h\binom{y}{a}(z) = h'\binom{y}{a}(z)$ for each free variable z of ψ (cf. 2.3.27, whose proof is done in 2.3.50(iv)) and from the induction hypothesis we get $\mathscr{M} \models \psi[h'\binom{y}{a}]$ for all $a \in |\mathscr{M}|$. This in turn shows $\mathscr{M} \models \varphi[h']$. □

2.4.13**. Proof of 2.4.11** Let $t, t' \in \mathrm{tm}(\mathscr{L})$, $\varphi \in \mathrm{Fml}(\mathscr{L})$ and $x \in \mathrm{Vbl}$. Let h be an assignment of an $\mathscr{L}$-structure $\mathscr{M}$ and let $a = t^{\mathscr{M}}[h]$.

(i) $(t'(x/t))^{\mathscr{M}}[h] = t'^{\mathscr{M}}[h\binom{x}{a}]$.

(ii) If x is free in φ for t then $\mathscr{M} \models \varphi(x/t)\ [h] \iff \mathscr{M} \models \varphi[h\binom{x}{a}]$.

Proof. (i) holds by a straightforward induction on the complexity of t':

With $a = t^{\mathscr{M}}[h]$ we show $(t'(x/t))^{\mathscr{M}}[h] = t'^{\mathscr{M}}[h(\binom{x}{a})]$ by induction on the complexity of t'.

If t' is a variable $y \neq x$, then $t'(x/t) = t'$ and

$$(t'(x/t))^{\mathscr{M}}[h] = t'^{\mathscr{M}}[h] = h(y) = h(\binom{x}{a})(y) = t'^{\mathscr{M}}[h(\binom{x}{a})]$$

If t' is x, then $t'(x/t) = t$ and

$$(t'(x/t))^{\mathscr{M}}[h] = t^{\mathscr{M}}[h] = a = h(\binom{x}{a})(x) = t'^{\mathscr{M}}[h(\binom{x}{a})]$$

If t' is a constant symbol c, then $t'(x/t) = c$ and

$$(t'(x/t))^{\mathscr{M}}[h] = c^{\mathscr{M}} = t'^{\mathscr{M}}[h(\binom{x}{a})].$$

Now for the induction step assume t' is $F(t'_1, \dots, t'_n)$ and we know the assertion already for $t'_1, \dots, t'_n$. Then

$$\begin{aligned}
(t'(x/t))^{\mathscr{M}}[h] &= (F(t'_1, \dots, t'_n)(x/t))^{\mathscr{M}}[h] \\
&= F(t'_1(x/t), \dots, t'_n(x/t))^{\mathscr{M}}[h] \\
&= F^{\mathscr{M}}(t'_1(x/t)^{\mathscr{M}}[h], \dots, t'_n(x/t)^{\mathscr{M}}[h]), \text{ by definition} \\
&= F^{\mathscr{M}}(t'^{\mathscr{M}}_1[h(\binom{x}{a})], \dots, t'^{\mathscr{M}}_n[h(\binom{x}{a})]), \text{ by induction} \\
&= F(t'_1, \dots, t'_n)^{\mathscr{M}}[h(\binom{x}{a})], \text{ by definition} \\
&= t'^{\mathscr{M}}[h(\binom{x}{a})],
\end{aligned}$$

as required.

(ii) is proved by induction on the complexity of φ. It is not very difficult, but lengthy.

For the base case, assume that φ is atomic. If φ is atomic and of the form $t_1 \doteq t_2$, then

$$\begin{aligned}
\mathscr{M} \models \varphi(x/t)[h] &\iff t_1(x/t)^{\mathscr{M}}[h] = t_2(x/t)^{\mathscr{M}}[h], \text{ by definition} \\
&\iff t_1^{\mathscr{M}}[h(\binom{x}{a})] = t_2^{\mathscr{M}}[h(\binom{x}{a})], \text{ by 2.4.11(i)} \\
&\iff \mathscr{M} \models \varphi[h(\binom{x}{a})], \text{ by definition}
\end{aligned}$$

If φ is $R(t_1, \dots, t_n)$, then

$$\begin{aligned}
\mathscr{M} \models \varphi(x/t)[h] &\iff (t_1(x/t)^{\mathscr{M}}[h], \dots, t_n(x/t)^{\mathscr{M}}[h]) \in \mathbb{R}^{\mathscr{M}}, \text{ by definition} \\
&\iff (t_1^{\mathscr{M}}[h(\binom{x}{a})], t_n^{\mathscr{M}}[h(\binom{x}{a})]) \in R^{\mathscr{M}}, \text{ by 2.4.11(i)} \\
&\iff \mathscr{M} \models \varphi[h(\binom{x}{a})], \text{ by definition}
\end{aligned}$$

For the induction step related to negation assume we know the assertion already for φ, then

$$\begin{aligned}
\mathscr{M} \models \neg\varphi(x/t)[h] &\iff \mathscr{M} \not\models \varphi(x/t)[h], \text{ by definition} \\
&\iff \mathscr{M} \not\models \varphi[h(\substack{x\\a})], \text{ by induction} \\
&\iff \mathscr{M} \models \neg\varphi[h(\substack{x\\a})], \text{ by definition.}
\end{aligned}$$

For the induction step related to implication, assume we know the assertion already for φ and ψ, then

$$\begin{aligned}
\mathscr{M} \models (\varphi \to \psi)(x/t)[h] &\iff \mathscr{M} \not\models \varphi(x/t)[h] \text{ or } \mathscr{M} \models \psi(x/t)[h], \text{ by definition} \\
&\iff \mathscr{M} \not\models \varphi[h(\substack{x\\a})] \text{ or } \mathscr{M} \models \psi[h(\substack{x\\a})], \text{ by induction} \\
&\iff \mathscr{M} \models (\varphi \to \psi)[h(\substack{x\\a})], \text{ by definition.}
\end{aligned}$$

Finally, suppose we know (ii) already for $\psi \in \mathrm{Fml}(\mathscr{L})$ and φ is $\forall y\psi$ with $y \in \mathrm{Vbl}$. We show (ii) for φ.

Case 1. x does not occur freely in φ.

Then $\varphi(x/t)$ is equal to φ and h is identical to $h(\substack{x\\a})$ at the free variables of φ. By 2.4.12 we have $\mathscr{M} \models \varphi(x/t)\ [h] \iff \mathscr{M} \models \varphi[h] \iff \mathscr{M} \models \varphi[h(\substack{x\\a})]$.

Case 2. x does occur freely in φ.

Since φ is $\forall y\ \psi$, we must have $x \neq y$.

Claim. x is free in ψ for t.

Proof. Let z be a variable occurring in t. We have to show that x is free in ψ for z. As x is free in φ for t and x occurs in φ by assumption, y does not occur in t, which shows that $z \neq y$. Since $x \neq y$, each free occurrence of x in ψ is also a free occurrence of x in φ (where the position is shifted by 3). Thus, as $z \neq y$ and x is free in φ for z, x is also free in ψ for z. $\diamond$

The claim implies that the formula $(\forall y\psi)(x/t)$ is equal to $\forall y(\psi(x/t))$ and we get

$$\begin{aligned}
\mathscr{M} \models \varphi(x/t)\ [h] &\iff \mathscr{M} \models (\forall y\psi)(x/t)\ [h] \\
&\iff \mathscr{M} \models \forall y(\psi(x/t))\ [h] \\
&\iff \mathscr{M} \models \psi(x/t)\ [h(\substack{y\\b})] \text{ for all } b \in M, \text{ by definition} \\
&\iff \mathscr{M} \models \psi\ [h(\substack{y\\b})(\substack{x\\a})] \text{ for all } b \in M, \text{ by the induction} \\
&\qquad\qquad\qquad\qquad \text{hypothesis using the claim} \\
&\iff \mathscr{M} \models \psi\ [h(\substack{x\\a})(\substack{y\\b})] \text{ for all } b \in M, \text{ since } x \neq y \\
&\iff \mathscr{M} \models (\forall y\psi)\ [h(\substack{x\\a})], \text{ by definition} \\
&\iff \mathscr{M} \models \varphi[h(\substack{x\\a})]
\end{aligned}$$

as desired. $\square$

2.5. **The Proof System.**

Recall from 2.3.1 that our proof system is supposed to have two components. An axiom system and the definition of what is a (formal) proof. Before doing that we first need to talk about Propositional Logic. Traditionally one would introduce a proof system for Propositional Logic and then extend this to Predicate Logic. However as the audience has seen Propositional Logic in an implicit way, we will take a shortcut. Those who are interested may read the appendix of this section exposing a proof system for Propositional Logic.

We are essentially skipping syntactic considerations for Propositional Logic as these are rather transparent for mathematicians. Still, we indicate what formulas are in Propositional Logic:

2.5.1. **Definition.** A **propositional formula** (we will often just call them **propositions** here) is an expression P built up from **propositional letters** $p_1, p_2, p_3, \ldots$ by successively applying the following rules:

If P and Q are propositions, then so are $(\neg P)$ and $(P \to Q)$. We will drop brackets if this is unambiguous.

2.5.2**. Deciding propositional truth** Since every particular proposition is built up from only finitely many of the $p_1, p_2, p_3, \ldots$ we can use truth tables[26] to verify whether a proposition is true for all possible assignments of truth values of the $p_1, p_2, p_3, \ldots$.

A proposition P is called a **tautology** (of Propositional Logic), or a **propositional tautology** if P is true for all possible assignments of truth values of the $p_1, p_2, p_3, \ldots$. For example $p_1 \to p_1$ is such tautology.

The method of using truth tables to decide whether a given proposition is a propositional tautology is straightforward and can even be performed by a computer. This means that there is a computer program that accepts as input a proposition (in form of a finite string of letters from $\{\neg, \to,), (, p_1, p_2, p_2, \ldots\}$) and outputs

- `YES` if the proposition is a propositional tautology and
- `NO` if the proposition is not a propositional tautology.

We will therefore consider every propositional tautology as universally true when we build our formal proof system for Predicate Logic in 2.5.6.

[26]We assume that the reader has seen truth tables before.

In order to import Propositional Logic into Predicate Logic one tool is needed:

2.5.3. **Import Lemma** Let $n \in \mathbb{N}$ and let P be a propositional formula build up using at most the propositional letters $p_1, \ldots, p_n$. Let $\mathscr{L}$ be a language and let $\varphi_1, \ldots, \varphi_n$ be $\mathscr{L}$-formulas. Let ψ be the string obtained from P by replacing simultaneously all occurrences of p_i with φ_i for each $i \in \{1, \ldots, n\}$. Then

(i) ψ is an $\mathscr{L}$-formula.

(ii) If $\mathscr{M}$ is an $\mathscr{L}$-structure and h is an assignment of $\mathscr{M}$, then we may define an assignment of truth values to the propositional letters $p_1, \ldots, p_n$ as follows: For $i \in \{1, \ldots, n\}$ we define

$$(*) \qquad p_i \text{ is true} \iff \mathscr{M} \models \varphi_i[h].$$

Then

$$(\dagger) \qquad \begin{array}{l} P \text{ is true under the as-} \\ \text{signment of truth val-} \\ \text{ues defined by } (*) \end{array} \iff \mathscr{M} \models \psi[h].$$

Proof. We show (i) and (ii) at the same time and we perform an induction on the construction of P.

For the base case, assume P is a propositional letter p_i. Then ψ is just φ_i, which is an $\mathscr{L}$-formula by assumption and $(\dagger)$ is explicitly stated in $(*)$. This shows (i) and (ii) in the base case.

Now for the induction step we have to consider two cases.

Case 1. Let P be $(\neg Q)$ and assume by induction we know (i) and (ii) for Q.

Then we know (by (i) for Q) that the string γ obtained from Q by replacing simultaneously all occurrences of p_i with φ_i for each $i \in \{1, \ldots, n\}$, is an $\mathscr{L}$-formula. Since ψ is equal to $(\neg\gamma)$, we see that ψ is an $\mathscr{L}$-formula.

Furthermore (ii) holds for Q by induction and by $(\dagger)$ for Q we know that Q is true under the given assignment of truth if and only of $\mathscr{M} \models \gamma[h]$. But then P is true under the given assignment of truth if and only of Q is false under the given assignment of truth if and only of $\mathscr{M} \not\models \gamma[h]$ if and only if $\mathscr{M} \models \psi[h]$.

Case 2. Let P be $(Q \to R)$ and assume by induction we know (i) and (ii) for Q and R.

Then we know (from (i) for Q and R) that the strings γ, δ obtained from Q, R respectively by replacing simultaneously all occurrences of p_i with φ_i for each $i \in \{1, \ldots, n\}$, are $\mathscr{L}$-formulas. As ψ is equal to $(\gamma \to \delta)$, it is an $\mathscr{L}$-formula.

Furthermore, by $(\dagger)$ for Q we know that Q is true under the given assignment of truth if and only of $\mathscr{M} \models \gamma[h]$, and by $(\dagger)$ for R we know that R is true under the given assignment of truth if and only of $\mathscr{M} \models \delta[h]$.

Now P is true under the given truth assignment if and only if Q is false or R is true under the given truth assignment. Consequently P is true under the given truth assignment if and only if $\mathscr{M} \not\models \gamma[h]$ or $\mathscr{M} \models \delta[h]$. But this is the same as $\mathscr{M} \models \psi[h]$. $\square$

By 2.5.3(i) we may define

2.5.4. **Definition.** A **tautology** (of Predicate Logic) is an $\mathscr{L}$-formula φ obtained from a tautology of Propositional Logic by replacing simultaneously all occurrences of propositional letters by $\mathscr{L}$-formulas.

2.5.5. *Example.* In the language with a unary relation symbol R the following $\mathscr{L}$-formula φ is a tautology:

$$R(x) \to ((\forall x\, x \doteq y) \to R(x)).$$

The reason is that φ is obtained from the propositional tautology P defined as

$$p_1 \to (p_2 \to p_1)$$

by replacing p_1 with $R(x)$ and p_2 with $(\forall x\, x \doteq y)$.
From 2.5.3(ii) we also know that for any $\mathscr{L}$-structure $\mathscr{M}$ and each assignment h of $\mathscr{M}$ we have $\mathscr{M} \models \varphi[h]$, because P is a propositional tautology (look at its truth table).

The reasoning in 2.5.5 applies to all tautologies: If φ is a tautology then $\mathscr{M} \models \varphi[h]$ for any $\mathscr{L}$-structure $\mathscr{M}$ and each assignment h of $\mathscr{M}$. This is done in question 50 of the example sheets.

We now get to our axiom systems for languages in Predicate Logic. Each axiom of a language $\mathscr{L}$ is a formula α of $\mathscr{L}$, which is supposed to be universally true, i.e. for each $\mathscr{L}$-structure $\mathscr{M}$ and every assignment h of $\mathscr{M}$ we require $\mathscr{M} \models \alpha[h]$. We list these axioms now and verify their universal validity a bit later, see 2.5.13.

2.5.6. **Definition.** Let $\mathscr{L}$ be a language. Each of the following $\mathscr{L}$-formulas are called **logical Axioms** (of $\mathscr{L}$), where φ, ψ and γ are $\mathscr{L}$-formulas and x is a variable:

(AxProp) Every tautology of Predicate Logic as defined in 2.5.4.
Examples are :
(a) $\varphi \to (\psi \to \varphi)$
(b) $(\varphi \to (\psi \to \gamma)) \to ((\varphi \to \psi) \to (\varphi \to \gamma))$
(c) $((\neg\varphi) \to (\neg\psi)) \to (\psi \to \varphi)$
[For those who are reading the proof system for Propositional Logic: It does actually suffice to just take these three schemes.]

(Ax$\forall\to$) $(\forall x(\varphi \to \psi)) \ \to \ ((\forall x\varphi) \ \to \ (\forall x\psi))$ [27]

(AxSubst) $(\forall x\varphi) \ \to \ \varphi(x/t)$, where x is free in φ for $t \in \mathrm{tm}(\mathscr{L})$.[27]

(AxGen) $\varphi \to \forall x\varphi$, where x is *not* free in φ.[27]

(AxEq) For every $\mathscr{L}$-term t, every n-ary relation symbol R and all (not necessarily distinct) variables $x_1, ..., x_n, x, y, z$ the axioms
(a) $x \doteq x$
(b) $x \doteq y \wedge y \doteq z \ \to \ z \doteq x$
(c) $x \doteq y \to t(z/y) \doteq t(z/x)$
(d) $x \doteq y \to \Big(R(x_1, ..., x_n)(z/x) \leftrightarrow (R(x_1, ..., x_n)(z/y))\Big)$

(Ax$\forall$) Any formula of the form

$$\forall x_1 \ldots \forall x_n \ \alpha$$

where α is one of the formulas introduced by the other logical axiom schemes above and $x_1, ..., x_n$ are variables.

[27]Notice that this is not just a single axiom, because for each choice of formula(s) and variables we obtain a formula of the form displayed here. In particular there are infinitely many axioms of this form and the expressions should rather be called an **axiom scheme**, which will be instantiated later. Axiom systems of this form are sometimes referred to as **Hilbert's style axiom system**.

2.5.7. **Definition.** Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$. A **formal proof** or a **deduction** from Σ (in $\mathscr{L}$) is a finite sequence $(\varphi_1, ..., \varphi_n)$ of $\mathscr{L}$-formulas such that for each $k \in \{1, ..., n\}$ one of the following conditions hold:

(PR1) φ_k is a logical axiom (of $\mathscr{L}$), or

(PR2) $\varphi_k \in \Sigma$, or

(PR3) (Modus Ponens) There are $i, j < k$ such that

$$\varphi_j \text{ is the formula } \varphi_i \to \varphi_k.$$

If $\Phi \subseteq \mathrm{Fml}(\mathscr{L})$, then we say Σ **proves** Φ and write

$$\Sigma \vdash_{\mathscr{L}} \Phi \text{ or } \Sigma \vdash \Phi \text{ when } \mathscr{L} \text{ is clear from the context,}$$

if every $\varphi \in \Phi$ is an entry of a proof from Σ. If $\Phi = \{\varphi\}$ we just write $\Sigma \vdash \varphi$. If $\Sigma = \emptyset$ we just write $\vdash \Phi$.
We say that $(\varphi_1, ..., \varphi_n)$ is a **proof of** φ **from** Σ if $(\varphi_1, ..., \varphi_n)$ is a proof from Σ and $\varphi = \varphi_n$.

2.5.8. *Remark.* The following are immediate consequences of definition 2.5.7:

(i) If $(\varphi_1, ..., \varphi_n)$ is a proof from Σ, then also $(\varphi_1, ..., \varphi_m)$ is a proof from Σ for every $m \leq n$. Moreover $\varphi_1 \in \Sigma$ or φ_1 is a logical axiom.

(ii) If $(\varphi_1, ..., \varphi_n)$ and $(\psi_1, ..., \psi_m)$ are proofs from Σ, then also $(\varphi_1, ..., \varphi_n, \psi_1, ..., \psi_m)$ is a proof from Σ.

(iii) $\Sigma \vdash \Phi \iff \Sigma \vdash \varphi$ for all $\varphi \in \Phi$.

(iv) $\Sigma \vdash \Phi$ for all $\Phi \subseteq \Sigma$.

Proof. To get used to definition 2.5.7, please carry this out; see Question 51 of the example sheets. □

2.5.9. **Corollary.** *(Modus Ponens for proofs)*

$$\text{If } \Sigma \vdash \varphi \to \psi \text{ and } \Sigma \vdash \varphi \text{ then } \Sigma \vdash \psi.$$

Proof. By 2.5.8(ii) and Modus Ponens. □

The next theorem follows again immediately from definition 2.5.7 of a formal proof. It is of central importance to Predicate Logic and used in many places later on.

2.5.10. **Theorem.** *"Proofs are Finite"*
For every $\varphi \in \mathrm{Fml}(\mathscr{L})$ and all subsets $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ the following are equivalent:

(i) $\Sigma \vdash \varphi$.
(ii) There is a finite subset $\Sigma_0 \subseteq \Sigma$ with $\Sigma_0 \vdash \varphi$.
(iii) There is a proof $(\varphi_1, ..., \varphi_n)$ of φ from Σ.

Proof. Again, please carry this out and use it for practicing definition 2.5.7; see Question 51 of the example sheets. □

2.5.11. **Lemma.** *(Transitivity of proofs)*

$$\textit{If } \Sigma, \Phi, \Psi \subseteq \mathrm{Fml}(\mathscr{L}) \textit{ with } \Sigma \vdash \Phi \textit{ and } \Phi \vdash \Psi \textit{ then } \Sigma \vdash \Psi.$$

Proof. Since $\Phi \vdash \Psi$, it suffices to show by induction on n the following:

$$\text{If } (\psi_1, ..., \psi_n) \text{ is a proof from } \Phi, \text{ then } \Sigma \vdash \psi_n.$$

If $n = 1$, then ψ_1 is a logical axiom or $\psi_1 \in \Phi$. In each case $\Sigma \vdash \psi_1$, using our assumption $\Sigma \vdash \Phi$.

For the induction step, suppose we are given a proof $(\psi_1, ..., \psi_{n+1})$ from Φ. If $\psi_{n+1} \in \Phi$ or ψ_{n+1} is a logical axiom then $\Sigma \vdash \psi_{n+1}$ again, using our assumption $\Sigma \vdash \Phi$. Otherwise there are $i, j \leq n$ such that ψ_j is $\psi_i \to \psi_{n+1}$. By the induction hypothesis and because $(\psi_1, ..., \psi_i)$ and $(\psi_1, ..., \psi_j)$ are proofs from Φ, we know $\Sigma \vdash \psi_i$ and $\Sigma \vdash \psi_j$. As ψ_j is $\psi_i \to \psi_{n+1}$ we may apply 2.5.9 to obtain $\Sigma \vdash \psi_{n+1}$. $\square$

2.5.12. *Example.* Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$.

(i) If $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$ and $\Sigma \vdash (\varphi \to \psi)$, then $\Sigma \cup \{\varphi\} \vdash \psi$.[28]

To see this take a proof $(\psi_1, \ldots, \psi_m)$ from Σ such that ψ_m is $(\varphi \to \psi)$. then $(\psi_1, \ldots, \psi_m, \varphi, \psi)$ is a proof from $\Sigma \cup \{\varphi\}$ and so $\Sigma \cup \{\varphi\} \vdash \psi$.

(ii) If $\varphi_1, ..., \varphi_n \in \mathrm{Fml}(\mathscr{L})$, then

$$\Sigma \vdash (\varphi_1 \wedge ... \wedge \varphi_n) \quad \iff \quad \Sigma \vdash \varphi_1 \text{ and ... and } \Sigma \vdash \varphi_n.$$

[See 2.3.18 for the definition of the formula $\varphi_1 \wedge ... \wedge \varphi_n$.]

The implication "$\Rightarrow$" here is obtained from 2.5.11 and the fact that $p_1 \wedge ... \wedge p_n \to p_i$ is a propositional tautology (hence $\varphi_1 \wedge ... \wedge \varphi_n \to \varphi_i$ is an axiom of $\mathscr{L}$).

"$\Leftarrow$": As $\Sigma \vdash \varphi_i$ for all $i \in \{1, \ldots, n\}$ we know that $\Sigma \vdash \{\varphi_1, \ldots, \varphi_n\}$. Hence by 2.5.11 it suffices to show $\{\varphi_1, \ldots, \varphi_n\} \vdash \varphi_1 \wedge \ldots \wedge \varphi_n$.

Consider the propositional variables $p_1, \ldots, p_n$ and let P be the proposition

$$p_1 \to (p_2 \to (\ldots \to (p_n \to (p_1 \wedge \ldots \wedge p_n)) \ldots)).$$

Then P is a tautology of Propositional Logic as one checks using truth tables. Let ψ be the $\mathscr{L}$-formula obtained from P by replacing, for each $i \in \{1, \ldots, n\}$, p_i by φ_i. Hence ψ is

$$\varphi_1 \to (\varphi_2 \to (\ldots \to (\varphi_n \to (\varphi_1 \wedge \ldots \wedge \varphi_n)) \ldots))$$

and ψ is a logical axiom. By (i) we get $\{\varphi_1\} \vdash (\varphi_2 \to (\ldots \to (\varphi_n \to (\varphi_1 \wedge \ldots \wedge \varphi_n)) \ldots))$. By (i) again we get $\{\varphi_1, \varphi_2\} \vdash (\varphi_3 \to (\ldots \to (\varphi_n \to (\varphi_1 \wedge \ldots \wedge \varphi_n)) \ldots))$. By induction we thus obtain

$$\{\varphi_1, \ldots, \varphi_n\} \vdash \varphi_1 \wedge \ldots \wedge \varphi_n,$$

as required.

[28]The converse here is also true, as we will see in 2.5.19

Correctness of logical axioms and formal proofs

We will now show that our logical axioms hold at all assignments of all structures (see 2.5.13). Furthermore the soundness theorem 2.5.16 shows that our logical proofs do not lead to contradictions. (Formally, 2.5.16 actually implies 2.5.13). This constitutes one part of a justification of our choice of axioms. The second part, namely that we did not state more axioms, will be justified later, by the so called *Completeness Theorem*: This theorem implies that, whenever φ is an $\mathscr{L}$-formula, which is valid in all assignments of all $\mathscr{L}$-structures, then $\vdash_{\mathscr{L}} \varphi$, in other words there is a formal proof of φ from our logical axioms. In this sense our choice of logical axioms, together with the rules of a formalized proof is *complete*. We start with a preparation:

2.5.13. **Lemma.** *For every logical axiom φ and each assignment h of every $\mathscr{L}$-structure $\mathscr{M}$ we have $\mathscr{M} \models \varphi[h]$.*

Proof. Tautologies are true in all structures at all assignments. This is worked out in question 50 of the example sheets and follows essentially from 2.5.3(ii). This settles the axioms in (**AxProp**).

For the axioms in (**Ax**$\forall \rightarrow$) and (**AxEq**) the assertion has a lengthy but not difficult proof; this is left as question 52 on the example sheet.

We show the universal validity of the logical axioms built by the schemes (**AxSubst**), (**AxGen**) and (**Ax**$\forall$). Let h be an assignment of an $\mathscr{L}$-structure $\mathscr{M}$.

Case 1. φ is an instance of (**AxSubst**), i.e. φ is of the form $(\forall x\psi) \rightarrow \psi(x/t)$, where x is free in ψ for $t \in \mathrm{tm}(\mathscr{L})$.

We have to assume $\mathscr{M} \models (\forall x\psi)[h]$ and we are supposed to show $\mathscr{M} \models \psi(x/t)[h]$. By 2.4.11(ii), it suffices to show $\mathscr{M} \models \psi[h\binom{x}{a}]$ with $a = t^{\mathscr{M}}[h]$. This clearly holds, as $\mathscr{M} \models (\forall x\psi)[h]$.

Case 2. φ is an instance of (**AxGen**), i.e. φ is of the form $\psi \rightarrow \forall x\psi$, where x is *not* free in ψ.

We have to assume $\mathscr{M} \models \psi[h]$ and we are supposed to show $\mathscr{M} \models \forall x\psi[h]$. This means we have to pick some $a \in |\mathscr{M}|$ and to prove $\mathscr{M} \models \psi[h\binom{x}{a}]$. Since x is assumed to be not free in ψ, the assignments h and $h\binom{x}{a}$ have the same values on all free variables of ψ. Hence with $\mathscr{M} \models \psi[h]$ we may apply 2.4.12 to obtain $\mathscr{M} \models \psi[h\binom{x}{a}]$.

Case 3. φ is an instance of (**Ax**$\forall$), i.e. φ is of the form $\forall x_1 ... x_n\ \psi$, where ψ is a logical axiom defined under one of the schemes (**AxProp**), (**Ax**$\forall \rightarrow$), (**AxEq**), (**AxSubst**) or (**AxGen**).

Since we have already shown the lemma for these logical axioms we know that $\mathscr{M} \models \psi[h']$ for all assignments h'. But now it is clear that $\mathscr{M} \models \forall x_1 ... x_n\ \psi[h]$. $\square$

2.5.14. **Definition.** Let $\Sigma, \Phi \subseteq \mathrm{Fml}(\mathscr{L})$. We say that Σ **logically implies** Φ (or Φ is a **logical consequence** of Σ) if for every assignment h of every $\mathscr{L}$-structure $\mathscr{M}$ we have:

$$\mathscr{M} \models \Sigma[h] \quad \Longrightarrow \quad \mathscr{M} \models \Phi[h].$$

If this is the case we write

$$\Sigma \models \Phi.$$

2.5.15. *Examples.*

(i) The notion $\Sigma \models \varphi$ indeed captures the format of standard mathematical theorems. For example consider the following assertion taken from group theory:

"If G is a group such that $g^2 = e$ for all $g \in G$, then G is commutative."

Here one could choose Σ to be a set of sentences in the language $\mathscr{L}$ of groups that define groups, i.e. such that for every $\mathscr{L}$-structure $\mathscr{M}$ we have $\mathscr{M} \models \Sigma$ if and only if $\mathscr{M}$ is a group. Furthermore one could choose φ to be the sentence

$$(\forall x\, x^2 \doteq e) \to (\forall x, y\ x \cdot y \doteq y \cdot x).$$

Then a proof of φ from Σ in group theory, would in fact show $\Sigma \models \varphi$ (rather than trying to show $\Sigma \vdash \varphi$): We would take a group, then we would assume that $g^2 = e$ for all $g \in G$ and then we would try to come up with an argument why G is commutative.

(ii) Here is an example of a meaningful logical implication $\Sigma \models \Phi$, where Σ is finite and Φ is (necessarily) infinite. Consider the following statement about posets:

"Every poset without maximal elements is infinite."

Here Σ could be the set of sentences in the language $\mathscr{L}$ of posets expressing reflexivity, anti-symmetry and transitivity of the binary relation, together with the sentence saying that the poset has no maximal element. What could Φ be here? See question 53 on the example sheet.

2.5.16. **Soundness Theorem** *Let $\mathscr{L}$ be a language. For all $\Sigma, \Phi \subseteq \mathrm{Fml}(\mathscr{L})$,*

$$\textit{if } \Sigma \vdash \Phi, \textit{ then } \Sigma \models \Phi.$$

Proof. It is enough to show by induction on n the following: If $(\varphi_1, ..., \varphi_n)$ is a proof from Σ then $\mathscr{M} \models \varphi_n[h]$ for every assignment h of every $\mathscr{L}$-structure $\mathscr{M}$ satisfying $\mathscr{M} \models \Sigma[h]$.

If $\varphi_n \in \Sigma$ or φ_n is a logical axiom, then this holds true by 2.5.13. In particular the claim holds for $n = 1$. Moreover for the induction step "$n - 1 \Rightarrow n$" it is clear that we only need to show the claim in the case where φ_n is the result of applying Modus Ponens to two entries of $(\varphi_1, ..., \varphi_{n-1})$. Hence there are $k, j < n$ such that $\varphi_k = \varphi_j \to \varphi_n$.

If h is an assignment of $\mathscr{M}$ with $\mathscr{M} \models \Sigma[h]$, then by induction we know $\mathscr{M} \models \varphi_j[h]$ and $\mathscr{M} \models \varphi_j \to \varphi_n\ [h]$. By 2.4.5(A)(ii) we get $\mathscr{M} \models \varphi_n[h]$ as desired. $\square$

Frequently the Soundness Theorem is used in its contrapositive form, e.g., when we want to show that $\Sigma \nvdash \varphi$ we can establish this by finding an $\mathscr{L}$-structure $\mathscr{M}$ and an assignment h of $\mathscr{M}$ such that $\mathscr{M} \models \Sigma[h]$ and $\mathscr{M} \nvDash \varphi[h]$.

2.5.17. **Definition.** A subset $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ is called **consistent** if there is no $\mathscr{L}$-formula φ with $\Sigma \vdash \varphi \wedge \neg\varphi$. Otherwise Σ is called **contradictory** or **inconsistent**. A formula φ is called consistent, inconsistent resp., if $\{\varphi\}$ has this property.

2.5.18. **Corollary.** *If $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ and if there is a model of Σ at some assignment, then Σ is consistent.*

Proof. This follows immediately from 2.5.16 since $\varphi \wedge \neg\varphi$ does not hold for any $\mathscr{L}$-formula φ in any $\mathscr{L}$-structure at any assignment. □

Deduction and Generalisation

2.5.19**. Deduction Theorem**

Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ and let $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$. Then

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

Proof. The implication $\Rightarrow$ has already been shown in 2.5.12(i).
In order to prove the implication $\Leftarrow$ it suffices to show by induction on n the following:

> If $(\varphi_1, ..., \varphi_n)$ is a proof from $\Sigma \cup \{\varphi\}$, then the sequence
> $(\varphi \to \varphi_1, ..., \varphi \to \varphi_n)$ can be completed to a proof from Σ.

If $n = 1$ and (φ_1) is a proof from $\Sigma \cup \{\varphi\}$, then φ_1 is a logical axiom or $\varphi_1 \in \Sigma \cup \{\varphi\}$. If $\varphi_1 = \varphi$, then $(\varphi_1 \to \varphi)$ is a logical axiom of $\mathscr{L}$ because $p_1 \to p_1$ is a propositional tautology, which implies the assertion. If φ_1 is a logical axiom or $\varphi_1 \in \Sigma$, then

$$(\varphi_1 \to (\varphi \to \varphi_1), \varphi_1, \varphi \to \varphi_1)$$

is a proof from Σ, since $\varphi_1 \to (\varphi \to \varphi_1)$ is an instance of 2.5.6, (**AxProp**)(a).

For the induction step, suppose $(\varphi_1, ..., \varphi_{n+1})$ is a proof from $\Sigma \cup \{\varphi\}$. By the induction hypothesis there is a proof $(\psi_1, ..., \psi_m)$ from Σ which contains $(\varphi \to \varphi_1, ..., \varphi \to \varphi_n)$ (in this order) as a subsequence.

Case 1. φ_{n+1} is a logical axiom or $\varphi_{n+1} \in \Sigma \cup \{\varphi\}$.

Then (φ_{n+1}) is already a proof from $\Sigma \cup \{\varphi\}$ and as seen in the case $n = 1$, $(\psi_1, ..., \psi_m)$ can be extended to a proof from Σ with last entry $\varphi \to \varphi_{n+1}$.

Case 2. There are $k, l \leq n$ such that φ_l is $\varphi_k \to \varphi_{n+1}$.

Then the sequence $(\psi_1, ..., \psi_m)$ has $\varphi \to \varphi_k$ and $\varphi \to (\varphi_k \to \varphi_{n+1})$ as entries. Let ϑ be the formula

$$(\varphi \to (\varphi_k \to \varphi_{n+1})) \;\to\; ((\varphi \to \varphi_k) \to (\varphi \to \varphi_{n+1})).$$

This is an instance of 2.5.6, (**AxProp**)(b). Hence ϑ is a logical axiom and

$$(\psi_1, ..., \psi_m, \vartheta, (\varphi \to \varphi_k) \to (\varphi \to \varphi_{n+1}), \varphi \to \varphi_{n+1})$$

is a proof from Σ (Modus Ponens is applied twice). □

2.5.20. *Remark.* The proof of 2.5.19 really belongs to Propositional Logic and this can be found explicitly in the appendix of this section, cf. 2.5.26. Note that we also have

$$\Sigma \models (\varphi \to \psi) \quad \iff \quad \Sigma \cup \{\varphi\} \models \psi$$

and this is much easier to prove than 2.5.19. You may want to have a go.

2.5.21**. Generalisation Theorem**

Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ *and* $\varphi \in \mathrm{Fml}(\mathscr{L})$*. If* $x \in \mathrm{Vbl}$ *does not occur freely in any formula from* Σ *then*

$$\Sigma \vdash \varphi \textit{ if and only if } \Sigma \vdash \forall x \varphi.$$

[Notice that x *may very well occur freely in* φ*.]*

Proof. The implication $\Leftarrow$ holds even without the assumption that x does not occur freely in any formula from Σ by 2.5.6 (**AxSubst**) applied with $x = t$ and Modus Ponens for proofs. The crucial statement here is the implication $\Rightarrow$, which we prove by induction on the length of a proof of φ from Σ:

If φ is a logical axiom, then by 2.5.6, (**Ax**$\forall$) we know that also $\forall x \varphi$ is a logical axiom, thus $\Sigma \vdash \forall x \varphi$. If $\varphi \in \Sigma$, then by assumption, x does not occur freely in φ. Hence by 2.5.6, (**AxGen**), $\varphi \to \forall x \varphi$ is a logical axiom. Applying Modus Ponens for proofs we get $\Sigma \vdash \forall x \varphi$.

For the induction step, suppose $(\varphi_1, ..., \varphi_{n+1})$ is a proof from Σ with $\varphi = \varphi_{n+1}$. From what we have seen above we may assume that φ is neither a logical axiom nor an element of Σ. Hence there are $i, j \leq n$ such that φ_j is $\varphi_i \to \varphi_{n+1}$. By 2.5.6, (**Ax**$\forall\!\to$) we have that

$$\forall x(\varphi_i \to \varphi_{n+1}) \ \to \ (\forall x \varphi_i \ \to \ \forall x \varphi_{n+1})$$

is a logical axiom. By the induction hypothesis we know $\Sigma \vdash \forall x \varphi_j$, in other words $\Sigma \vdash \forall x(\varphi_i \to \varphi_{n+1})$. So by Modus Ponens for proofs we get $\Sigma \vdash \forall x \varphi_i \ \to \ \forall x \varphi_{n+1}$. Since also $\Sigma \vdash \forall x \varphi_i$ by induction we may apply Modus Ponens for proofs again to obtain $\Sigma \vdash \forall x \varphi_{n+1}$. □

2.5.22. *Examples.* Let $\mathscr{L}$ be any language, $\varphi \in \mathrm{Fml}(\mathscr{L})$ and let x be a variable.

(i) If y is a variable that does not occur freely in φ and x is free for y in φ, then

$$\vdash \Big((\forall x \varphi) \to (\forall y\, \varphi(x/y)) \Big).$$

(ii) We have

$$\vdash \Big((\neg \forall x \ \varphi) \leftrightarrow (\exists x \ \neg \varphi) \Big).$$

Proof. (i) Since x is free in φ for y, axiom (**AxSubst**) implies $\vdash \big((\forall x \varphi) \to \varphi(x/y)\big)$, hence $\forall x \varphi \vdash \varphi(x/y)$, too. Since y does not occur freely in $\forall x \varphi$, the generalisation theorem 2.5.21 gives $\forall x \varphi \vdash \forall y\, \varphi(x/y)$. Applying the Deduction Theorem 2.5.19 yields the claim.

(ii)[29] By the generalisation theorem applied to the logical axiom $\varphi \leftrightarrow \neg\neg\varphi$ we know that $\vdash \forall x(\varphi \leftrightarrow \neg\neg\varphi)$. Using (**Ax**$\forall\to$) twice (together with 2.5.12(ii) and Modus Ponens for Proofs) we obtain $\vdash \Big((\forall x\ \varphi) \leftrightarrow (\forall x\ \neg\neg\varphi)\Big)$. Using the propositional tautology $(p_0 \leftrightarrow p_1) \leftrightarrow (\neg p_0 \leftrightarrow \neg p_1)$ we obtain

$$\vdash \Big((\neg\forall x\ \varphi) \leftrightarrow (\neg\forall x\ \neg\neg\varphi)\Big)$$

But this is the assertion (see the definition of $\exists x$). $\square$

[29]One can try to write out a formal proof, but this might be tedious. Note that the question is not asking for a formal proof, just that we prove why $\vdash \Big((\neg\forall x\ \varphi) \leftrightarrow (\exists x\ \neg\varphi)\Big)$ holds.

Appendix to section 2.5

None of the proofs in this appendix is examinable. Only statements that also occur outside of this appendix are examinable.

There is also a proof system for Propositional Logic, which is exhibited in this appendix. One can dream up various proof systems for propositions and many ideas that are exposed in Predicate Logic above can already be seen on that level. This alleviates the Predicate Logic material and can also be used directly (to some extent), an example is the proof of the Deduction Theorem 2.5.19, which is essentially a task of Propositional Logic.

If you read this appendix, you will therefore revise the entire section in a simplified context.

2.5.23. **Definition.** Given propositions P, Q, R, each of the following propositions is an axiom of Propositional Logic, or a **Propositional Axiom**. [30]

`Axiom 1:` $P \to (Q \to P)$

`Axiom 2:` $\Big(P \to (Q \to R)\Big) \to \Big((P \to Q) \to (P \to R)\Big)$

`Axiom 3:` $(\neg P \to \neg Q) \to (Q \to P)$

Notice that this is not just a list of three axioms, because for each choice of propositions P, Q, R we get a proposition out of each axiom above. In particular there are infinitely many axioms and the above three expressions should rather be called an **axiom scheme**, which we will instantiate below.

Axiom systems that are given in this form are called **Hilbert's style axiom system** (for Propositional Logic). The one above is by J. Łukasiewicz.

2.5.24. **Definition.** Let Σ be a set of propositions. A **formal proof in Propositional Logic** or a **deduction in Propositional Logic** from Σ is a finite sequence $(P_1, ..., P_n)$ of propositions such that for each $k \in \{1, ..., n\}$ one of the following conditions hold:

`PR1:` P_k is a propositional axiom, or

`PR2:` $P_k \in \Sigma$, or

`PR3:` (Modus Ponens) There are $i, j < k$ such that

$$P_j \text{ is the proposition } P_i \to P_k.$$ [30]

If Σ is a set of propositions and P is a proposition, then we say that Σ **proves** P and write

$$\Sigma \vdash P$$

if there is a formal proof $(P_1, \ldots, P_n)$ from Σ such that $P = P_i$ for some $i \in \{1, \ldots, n\}$. If $\Sigma = \emptyset$ we just write $\vdash P$.

[30] We drop brackets again according to standard mathematical conventions

2.5.25. **Lemma.** *Let P be a proposition. Then $\vdash (P \to P)$.*

Proof. Here is the formal proof:

(1) $P \to ((P \to P) \to P)$ by Axiom 1.[31]

(2) $(\underbrace{P}_{P} \to (\underbrace{(P \to P)}_{Q} \to \underbrace{P}_{R})) \;\to\; ((\underbrace{P}_{P} \to \underbrace{(P \to P)}_{Q}) \to (\underbrace{P}_{P} \to \underbrace{P}_{R}))$ by Axiom 2 [31] as indicated under the braces.

(3) $(P \to (P \to P)) \to (P \to P)$ by Modus Ponens applied to (1) and (2).

(4) $P \to (P \to P)$ by Axiom 1.

(5) $P \to P$ by Modus Ponens applied to (4) and (3). □

2.5.26**. Deduction Theorem for Propositional Logic**
If Σ is a set of propositions and P, Q are propositions, then

$$\Sigma \vdash (P \to Q) \iff \Sigma \cup \{P\} \vdash Q\,.$$

Proof. $\Rightarrow$. If $\Sigma \vdash P \to Q$, then we may append a proof from Σ of $P \to Q$ by (P, Q) to obtain a formal proof of Q from $\Sigma \cup \{P\}$:

(1) $P \to Q$ since $\Sigma \vdash P \to Q$, hence also $\Sigma \cup \{P\} \vdash P \to Q$
(2) P by $P \in \Sigma \cup \{P\}$
(3) Q by Modus Ponens for (2) and (1).

$\Leftarrow$. Assume $\Sigma \cup \{P\} \vdash Q$. It suffices to show by induction on n that for each proof $(P_1, \ldots, P_n)$ from $\Sigma \cup \{P\}$, the sequence $(P \to P_1, \ldots, P \to P_n)$ can be completed to a proof from Σ (i.e., it is a subsequence of a proof from Σ).

If $n = 1$, then P_1 is a logical axiom or $P_1 \in \Sigma \cup \{P\}$. If P_1 is a logical axiom or $P_1 \in \Sigma$, then $(P_1, P_1 \to (P \to P_1), P \to P_1)$ is a proof from Σ using Axiom 1. If $P_1 = P$, then $P \to P_1$ can be completed to a proof from $\emptyset$ by 2.5.25.

For the induction step, suppose $(P_1, ..., P_{n+1})$ is a proof from $\Sigma \cup \{P\}$. By the induction hypothesis there is a proof $(Q_1, ..., Q_m)$ from Σ which contains $(P \to P_1, ..., P \to P_n)$ (in this order) as a subsequence.

Case 1. P_{n+1} is a logical axiom or $P_{n+1} \in \Sigma \cup \{P\}$.
Then (P_{n+1}) is already a proof from $\Sigma \cup \{P\}$ and as seen in the case $n = 1$, $(Q_1, ..., Q_m)$ can be extended to a proof from Σ with last entry $P \to P_{n+1}$.

Case 2. There are $k, l \leq n$ such that P_l is $P_k \to P_{n+1}$.
Then the sequence $(Q_1, ..., Q_m)$ has $P \to P_k$ and $P \to (P_k \to P_{n+1})$ as entries. Now the proposition $\tilde{Q}$ defined as

$$(P \to (P_k \to P_{n+1})) \;\to\; ((P \to P_k) \to (P \to P_{n+1})).$$

is an instance of the logical axiom Axiom 2. Hence

$$(Q_1, ..., Q_m, \tilde{Q}, (P \to P_k) \to (P \to P_{n+1}), P \to P_{n+1})$$

is a proof from Σ (Modus Ponens is applied twice). □

[31]Or rather an instance of this axiom.

2.5.27. **Corollary.** *Let Σ be a set of propositions and let P, Q, R be propositions. Then*

(i) If $\Sigma \vdash Q$, then $\Sigma \vdash P \to Q$.

(ii) If $\Sigma \vdash P \to Q$ and $\Sigma \vdash Q \to R$, then $\Sigma \vdash P \to R$.

(iii) (a) $\vdash (P \to Q) \to ((Q \to R) \to (P \to R))$ and
(b) $\vdash (Q \to R) \to ((P \to Q) \to (P \to R))$.

(iv) If $\Sigma \vdash Q$, then $\Sigma \vdash (Q \to P) \to P$.

It is worth mentioning that the assertions above as well as 2.5.25 and 2.5.26 are proved from `Axiom 1` *and* `Axiom 2` *alone (and Modus Ponens of course); this is referred to as "Positive Implicational Calculus" and is part of "Intuitionistic Logic", which does not accept* `Axiom 3` *as universally true, but which has other axioms instead (all weaker than* `Axiom 3`*, given the first two axioms). For the remaining statements we will use* `Axiom 3`*.*

(v) $\vdash \neg\neg P \to P$ and $\vdash P \to \neg\neg P$.

(vi) $\vdash (P \to Q) \to (\neg Q \to \neg P)$.

(vii) If $\Sigma \vdash Q$, then $\Sigma \vdash (P \to \neg Q) \to \neg P$.

(viii) $\{P, \neg P\} \vdash Q$.

Proof. (i) follows from 2.5.26 and $\Sigma \cup \{P\} \vdash Q$.

(ii) By (i) we know that $\Sigma \vdash Q \to R$ implies $\Sigma \vdash P \to (Q \to R)$. Applying Modus Ponens twice using the axiom $(P \to (Q \to R)) \to ((P \to Q) \to (P \to R))$ we obtain $\Sigma \vdash P \to R$.

(iii). By (ii) we know that $\{P \to Q, Q \to R\} \vdash P \to R$. Now the Deduction Theorem applied in two different ways gives (a) and (b).

(iv) By Modus Ponens we have $\Sigma \cup \{Q \to P\} \vdash P$, hence by the Deduction Theorem we get $\Sigma \vdash (Q \to P) \to P$.

(v) Here is the justification why there is a formal proof of $\vdash \neg\neg P \to P$. Let $\mathbb{T}$ be any proposition with $\vdash \mathbb{T}$; for example $\mathbb{T}$ could be an axiom from 2.5.23.

(1) $\vdash \neg\neg P \to (\neg\neg\mathbb{T} \to \neg\neg P)$, which is an instance of `Axiom 1`.
(2) $\vdash (\neg\neg\mathbb{T} \to \neg\neg P) \to (\mathbb{T} \to P)$ by applying `Axiom 3` twice and then invoking (ii).
(3) $\vdash (\mathbb{T} \to P) \to P$ by (iv) using $\vdash \mathbb{T}$.
(4) $\vdash \neg\neg P \to P$ by applying (ii) to (1) and (2) and then again to (3).

We can now apply $\vdash \neg\neg P \to P$ to $\neg P$ and get $\vdash \neg\neg\neg P \to \neg P$. Applying `Axiom 3` and Modus Ponens gives $\vdash P \to \neg\neg P$.

(vi) We have

(1) $\vdash (P \to Q) \to (\neg\neg P \to Q)$ using $\vdash (\neg\neg P \to P) \to ((P \to Q) \to (\neg\neg P \to Q))$ by (iii)(a) and then invoking (v) and (ii) for $\Sigma = \emptyset$.
(2) $\vdash (\neg\neg P \to Q) \to (\neg\neg P \to \neg\neg Q)$ using $\vdash (Q \to \neg\neg Q) \to ((\neg\neg P \to Q) \to (\neg\neg P \to \neg\neg Q))$ by (iii)(b) and then proceeding as in (1).
(3) $\vdash (P \to Q) \to (\neg\neg P \to \neg\neg Q)$ using (ii) with (1) and (2)

(4) $\vdash (P \to Q) \to (\neg Q \to \neg P)$ using (ii) with `Axiom 3` and (3).

(vii) We have

(1) $\vdash (P \to \neg Q) \to (\neg\neg Q \to \neg P)$ by (vi)
(2) $\Sigma \vdash (\neg\neg Q \to \neg P) \to \neg P$ by (iv) as $\Sigma \vdash \neg\neg Q$ using (v).
(3) $\Sigma \vdash (P \to \neg Q) \to \neg P$ by (ii) for (1) and (2).

(viii) We have

(1) $\vdash P \to \neg\neg P$ by (v)
(2) $\vdash \neg\neg P \to (\neg Q \to \neg\neg P)$ by `Axiom 1`
(3) $\vdash (\neg Q \to \neg\neg P) \to (\neg P \to Q)$ by `Axiom 3`
(4) $\vdash P \to (\neg P \to Q)$ by (ii) applied twice using (1),(2),(3).
(5) $\{P, \neg P\} \vdash Q$ by using Modus Ponens twice using (4). □

2.5.28**. Soundness Theorem for Propositional Logic** Let Σ be a set of propositions and let P be a proposition with $\Sigma \vdash P$. Then P is true under all truth assignments of the $p_1, p_2, p_3, \ldots$ that make all propositions from Σ true.

Proof. It suffices to show by induction on n for every proof $(P_1, \ldots, P_n)$ from Σ that P_n is true under all truth assignments of the $p_1, p_2, p_3, \ldots$ that make all propositions form Σ true.

$n = 1$. According to the definition of "formal proof" in 2.5.24, P_1 is an axiom from 2.5.23, or, $P_1 \in \Sigma$. If $P_1 \in \Sigma$, then P_1 is true under the given truth assignments of the $p_1, p_2, p_3, \ldots$ by assumption on that truth assignments. If P_1 is an axiom from 2.5.23, then P_1 is in fact true under all truth assignments of the $p_1, p_2, p_3, \ldots$ as we see easily by using truth tables.

For the induction step take a proof $(P_1, \ldots, P_n)$ from Σ. Since $(P_1, \ldots, P_k)$ is also a proof from Σ for each $k < n$ we know by induction that $P_1, \ldots, P_{n-1}$ are all true under the given assignment of truth. We now examine how P_n can occur in the formal proof $(P_1, \ldots, P_n)$ from Σ following the definition of a formal proof in 2.5.24:

Case 1. P_n is a an axiom or $P_n \in \Sigma$. (This corresponds to `PR1` and `PR2` in 2.5.24.)

In this case we use the same reasoning as for P_1 in the case $n = 1$ and see that P_n is true under the given assignment.

Case 2. There are $i, j < n$ such that

$$P_j \text{ is the proposition } P_i \to P_n.$$

(This corresponds to `PR3` in 2.5.24.)

In this case we know by induction that P_i and $P_i \to P_n$ are true under the given assignment. But then the truth table of $P_i \to P_n$, written in terms of the possible truth values of P_i and P_n tells us that P_n is also true under the given assignment.

This finishes case 2 and the induction step. □

2.5.29. **Completeness Theorem of Propositional Logic** Let Σ be a set of propositions and let P be a proposition that is true under all truth assignments of the $p_1, p_2, p_3, \dots$ that make all $Q \in \Sigma$ true. Then $\Sigma \vdash P$.

Proof. Let $\mathbb{T}$ be any proposition with $\vdash \mathbb{T}$ and let $\mathbb{F}$ be $(\neg\mathbb{T})$. The crucial point is the following

Claim. Suppose Σ is a maximal set of propositions with the property that $\Sigma \nvdash \mathbb{F}$. Maximality here means that for every proposition P with $P \notin \Sigma$ we have $\Sigma \cup \{P\} \vdash \mathbb{F}$. We define an assignment of truth values by declaring p_i to be true if and only if $p_i \in \Sigma$. Then for every proposition P we have

$$(*) \qquad P \in \Sigma \iff P \text{ is true under the given assignment.}$$

Proof. If P is one of the p_i then $(*)$ is true by choice of the truth assignment. If $P = \neg Q$ and $(*)$ is true for Q, then it is also true for P, because

$\Rightarrow$. Suppose for a contradiction that $P \in \Sigma$ and P is false under the given assignment. Then $\neg P = \neg\neg Q$ is true under the given assignment using 2.5.28 and $\vdash \neg\neg Q \to Q$ (see 2.5.27(v)). But then $Q \in \Sigma$ as $(*)$ holds for Q by assumption. Hence $Q, \neg Q \in \Sigma$ and therefore $\Sigma \vdash \mathbb{F}$ (see 2.5.27(viii)) a contradiction.

$\Leftarrow$ If $P \notin \Sigma$, then $\Sigma \cup \{P\} \vdash \mathbb{F}$ by maximality of Σ. But then $\Sigma \vdash \neg Q \to \neg\mathbb{T}$ by the Deduction Theorem, hence $\Sigma \vdash \mathbb{T} \to Q$ using `Axiom 3` and so $\Sigma \vdash Q$ by 2.5.27(iv). By induction, Q is true under the given assignment and so P is false under the given assignment.

Finally assume P is $Q_1 \to Q_2$ and assume $(*)$ is true for Q_1, Q_2. We show $(*)$ for P.

$\Rightarrow$. Let $P \in \Sigma$. We need to show that $Q_1 \to Q_2$ is true under the given assignment. So we may assume that Q_1 is true under the given assignment. Then $Q_1 \in \Sigma$ by induction and by Modus Ponens then $\Sigma \vdash Q_2$. By maximality of Σ we get $Q_2 \in \Sigma$ and by induction then Q_2 is true under the given assignment, as required.

$\Leftarrow$. We assume P is true under the given assignment.

Case 1. $Q_1 \in \Sigma$ or $Q_2 \in \Sigma$.

If $Q_1 \in \Sigma$, then by induction, Q_1 is true under the given assignment and so also Q_2 is true under the given assignment, hence $Q_2 \in \Sigma$ by induction. Hence $Q_2 \in \Sigma$ in either case. But then $\Sigma \vdash Q_1 \to Q_2$ using the Axiom $Q_2 \to (Q_1 \to Q_2)$ and Modus Ponens. By maximality of Σ then $P \in \Sigma$.

Case 2. $Q_1 \notin \Sigma$ and $Q_2 \notin \Sigma$.

By maximality of Σ and the Deduction Theorem we get $\Sigma \vdash Q_1 \to \mathbb{F}$ and then $\Sigma \vdash \neg Q_1$ by 2.5.27(vii). Now $\vdash \neg Q_1 \to (Q_1 \to Q_2)$, because $\vdash \neg Q_1 \to (\neg Q_2 \to \neg Q_1)$. We conclude that $\Sigma \vdash (Q_1 \to Q_2)$ and by maximality of P then $P \in \Sigma$.

This finishes the proof of the claim. $\diamond$

Having proved the claim, we show the Theorem by contraposition. Hence we suppose $\Sigma \nvdash P$ and show that there is a truth assignment of the $p_1, p_2, p_3, \ldots$ making all $Q \in \Sigma$ true, but P false.

Since $\Sigma \nvdash P$ we know $\Sigma \cup \{\neg P\} \nvdash \mathbb{F}$, otherwise $\Sigma \vdash \neg P \to \mathbb{F}$ and so $\Sigma \vdash \neg\neg P$ by 2.5.27(vii), in contradiction to $\Sigma \nvdash P$ and $\vdash \neg\neg P \to P$.

Consequently $\Sigma \cup \{\neg P\}$ is in the set

$$\mathcal{S} = \{\Gamma \mid \Gamma \text{ is a set of propositions with } \Sigma \cup \{\neg P\} \subseteq \Gamma \text{ and } \Gamma \nvdash \mathbb{F}\}.$$

The set $\mathcal{S}$ is therefore a nonempty poset, ordered by inclusion. For every chain $\mathcal{C}$ of $\mathcal{S}$, the union $\hat{\Gamma} = \bigcup_{\Gamma \in \mathcal{C}} \Gamma$ is then again in $\mathcal{S}$, because proofs are finite. But then $\hat{\Gamma}$ is an upper bound of $\mathcal{C}$ in $\mathcal{S}$. Consequently, the lemma of Zorn applies and $\mathcal{S}$ possesses maximal elements. But a maximal element Γ of $\mathcal{S}$ is just the same thing as a maximal set of propositions in the sense of the claim. So the claim says that there is a truth assignment of the $p_1, p_2, p_3, \ldots$ such that all $Q \in \Gamma$ are true. Since $\Sigma \cup \{\neg P\} \subseteq \Gamma$ we get the assertion. □

2.5.30**. Conclusion** The Soundness Theorem 2.5.28 and the Completeness Theorem 2.5.29 of Propositional Logic can be summarized in the following form.

Let Σ be a set of propositions and let P be a proposition. The following conditions are equivalent.

(i) There is a formal proof of P from Σ.

(ii) Every truth assignment of the $p_1, p_2, p_3, \ldots$ that makes all $Q \in \Sigma$ true also makes P true. (One might think of this condition as saying "If Σ is true, then P is true".)

The implication (i)⇒(ii) holds by the Soundness Theorem and the the implication (ii)⇒(i) holds by the Completeness Theorem of Propositional Logic.

So here, condition (i) is a syntactic statement that asserts a formal property of propositions seen as strings, whereas (ii) is a semantic property, asserting a relation of truth of Σ and P.

The mathematical content of this equivalence may be viewed (and in fact proved) in terms of algebra and topology. This is explained in [StoneBool, section 3.3].

2.6. **Theories and Complete Theories.** Let $\mathscr{L}$ be a language.

2.6.1. **Definition.**

(i) An **$\mathscr{L}$-theory** is a consistent set of $\mathscr{L}$-sentences; we drop the letter $\mathscr{L}$, if the language is clear from the context.

(ii) A theory $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ is called a **complete theory** if for all $\varphi \in \mathrm{Sen}(\mathscr{L})$ we have

$$\varphi \notin \Sigma \quad \Longrightarrow \quad \neg\varphi \in \Sigma.$$

(Notice that the other implication also holds by the consistency requirement)

By the Soundness Theorem, every set of $\mathscr{L}$-sentences that are jointly true in a given $\mathscr{L}$-structure, is an $\mathscr{L}$-theory. For example the axioms of groups in the language of groups is an example of such a theory. Another example is the set of poset axioms in a language consisting of a binary relation symbol. In these notes, the notion of a theory is often intended to mean "axiom system of a naturally defined class of $\mathscr{L}$-structures" (like groups, rings, posets, graphs,...).

The main example of a complete theory is the following:

2.6.2**. Example and Definition** If $\mathscr{M}$ is an $\mathscr{L}$-structure, then the **theory of $\mathscr{M}$**, defined as

$$\mathrm{Th}(\mathscr{M}) = \{\varphi \in \mathrm{Sen}(\mathscr{L}) \mid \mathscr{M} \models \varphi\},$$

is a complete $\mathscr{L}$-theory. This follows from the Soundness Theorem and the definition of $\mathscr{M} \models \varphi$. Please do this in question 61 of the example sheets.

Indeed we shall see soon, that all complete sets are of this form (this is a version of the Completeness Theorem!)

2.6.3. **Lemma.** *Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ and let $\varphi \in \mathrm{Fml}(\mathscr{L})$. Then*

(i) $\Sigma \vdash \varphi \iff \Sigma \cup \{\neg\varphi\}$ is inconsistent.

(ii) If Σ is consistent, then $\Sigma \cup \{\varphi\}$ is consistent or $\Sigma \cup \{\neg\varphi\}$ is consistent.

Proof. (i). This has been done in question 56 of the example sheets.

(ii). If both $\Sigma \cup \{\varphi\}$ and $\Sigma \cup \{\neg\varphi\}$ are inconsistent, then by (i), $\Sigma \vdash \neg\varphi$ and $\Sigma \vdash \varphi$. Hence Σ is inconsistent as well. $\square$

2.6.4. **Proposition.** *For every theory $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ the following conditions are equivalent:*

(i) Σ is a complete theory, cf. 2.6.1.

(ii) For every $\mathscr{L}$-sentence φ we have $\varphi \in \Sigma$, or, $\neg\varphi \in \Sigma$.

(iii) The following two condistions hold.

*(a) Σ is **deductively closed**, i.e. for all $\varphi \in \mathrm{Sen}(\mathscr{L})$, if $\Sigma \vdash \varphi$, then $\varphi \in \Sigma$.*

(b) For every $\mathscr{L}$-sentence φ we have $\Sigma \vdash \varphi$, or, $\Sigma \vdash \neg\varphi$.

(iv) Σ is a maximally consistent set of $\mathscr{L}$-sentences, i.e. Σ is a consistent set of $\mathscr{L}$-sentences (which we know already as Σ is a theory) and each of its proper supersets of $\mathscr{L}$-sentences is inconsistent.

Remark: *In 2.7.4, more characterizations will be recorded, but for that we first need to show the Completeness Theorem.*

Proof. (i) is equivalent to (ii), because the implication "$\varphi \notin \Sigma \implies \neg\varphi \in \Sigma$" is equivalent to the disjunction "$\varphi \in \Sigma$ or $\neg\varphi \in \Sigma$".

(ii)⇒(iv). Let Σ' be a proper superset of Σ consisting of $\mathscr{L}$-sentences. Take $\varphi \in \Sigma' \setminus \Sigma$. By (ii) we get $\neg\varphi \in \Sigma$. Since $\Sigma \subseteq \Sigma'$ we get $\varphi, \neg\varphi \in \Sigma'$, which shows that Σ' is inconsistent, as required.

(iv)⇒(iii). If $\Sigma \vdash \varphi$, then $\Sigma \cup \{\varphi\}$ is consistent and the maximality property of Σ implies $\Sigma = \Sigma \cup \{\varphi\}$; hence $\varphi \in \Sigma$, showing (a). To see (b) assume $\Sigma \nvdash \varphi$. Then by 2.6.3, $\Sigma \cup \{\neg\varphi\}$ is consistent. The maximality property of Σ again implies $\Sigma = \Sigma \cup \{\neg\varphi\}$; hence $\neg\varphi \in \Sigma$.

(iii)⇒(ii). For every $\mathscr{L}$-sentence φ we know from (iii)(b) that $\Sigma \vdash \varphi$, or, $\Sigma \vdash \neg\varphi$. But now (iii)(a) entails $\varphi \in \Sigma$, or, $\neg\varphi \in \Sigma$. □

2.6.5. *Remark.* Every complete $\mathscr{L}$-theory Σ satisfies

$$\varphi \notin \Sigma \iff \neg\varphi \in \Sigma$$

for any $\mathscr{L}$-sentence φ. However, this equivalence alone does in general not imply that Σ is a complete theory: See question 62

2.6.6. **Theorem.** *Every consistent set of $\mathscr{L}$-sentences is contained in a complete $\mathscr{L}$-theory.*

Proof using the Lemma of Zorn. Let $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ be our consistent set. Let $\mathfrak{S}$ be the set of all consistent subsets of $\mathrm{Sen}(\mathscr{L})$ containing Σ. By 2.6.4 it is enough to show that $\mathfrak{S}$ contains elements that are maximal with respect to inclusion. However, the partial ordered set $(\mathfrak{S}, \subseteq)$ satisfies the requirement of Zorn's Lemma, because the union of a *chain* of $(\mathfrak{S}, \subseteq)$ is again in $\mathfrak{S}$ (as follows from the fact that formal proofs are finite, see 2.5.10). Hence by Zorn's lemma 1.2.5, $\mathfrak{S}$ indeed contains elements that are maximal with respect to inclusion. □

Proof in the countable case without Zorn. Let $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ be our consistent set. Suppose $\mathscr{L}$ is countable (or finite). Then the set of finite strings is also countable, in particular $\mathrm{Sen}(\mathscr{L})$ is countable. Let $\varphi_1, \varphi_2, \ldots$ be an enumeration of $\mathrm{Sen}(\mathscr{L})$. We define by induction a subset Σ_n of $\mathrm{Sen}(\mathscr{L})$ as follows: $\Sigma_0 = \Sigma$ and

$$\Sigma_{n+1} = \begin{cases} \Sigma_n \cup \{\varphi_{n+1}\} & \text{if } \Sigma_n \cup \{\varphi_{n+1}\} \text{ is consistent} \\ \Sigma_n \cup \{\neg\varphi_{n+1}\} & \text{otherwise.} \end{cases}$$

We claim that $T := \bigcup_{n \in \mathbb{N}_0} \Sigma_n$ is a complete theory (observe that $\Sigma = \Sigma_0 \subseteq T$). By definition of Σ_{n+1} we know that $\varphi_{n+1} \in \Sigma_{n+1}$ or $\neg\varphi_{n+1} \in \Sigma_{n+1}$. Since each $\varphi \in \mathrm{Sen}(\mathscr{L})$ is one of the φ_{n+1} for some $n \geq 0$ we see that $\varphi \notin T$ implies $\neg\varphi \in T$.

We still need to show that T is consistent. Since proofs are finite (2.5.10) it suffices to show that each Σ_n is consistent and we show this by induction on $n \in \mathbb{N}_0$. The base case $n = 0$ holds by assumption and the induction step holds by 2.6.3(ii). □

2.7. The Completeness Theorem and the Compactness Theorem.

2.7.1. **Theorem.** *(Completeness Theorem, Gödel, 1929)*
For all $\Sigma, \Phi \subseteq \mathrm{Fml}(\mathscr{L})$ *we have*

$$\Sigma \models \Phi \quad \Longrightarrow \quad \Sigma \vdash \Phi.$$

(Recall that the implication $\Leftarrow$ *also holds by the Soundness Theorem 2.5.16.)*

Proof. The proof is done in section 2.8 and is not examinable. ☐

2.7.2**. Warning on the terminology.**
In mathematics, the term "completeness" refers to many different things (e.g. complete space, complete graph, complete category, etc). "Completeness" in theorem 2.7.1 refers to completeness of the logical axiom system as explained in 2.3.1. It has nothing to do with completeness of a theory, defined in 2.6.1.

2.7.3. **Corollary.** *Every consistent set of* $\mathscr{L}$*-formulas is satisfiable (i.e. has a model at some assignment).*

Proof. Suppose Σ is a consistent set of $\mathscr{L}$-formulas, but Σ is not satisfiable. Then, trivially, $\Sigma \models \varphi \wedge \neg\varphi$ for every $\mathscr{L}$-formula φ. By the Completeness Theorem 2.7.1 we obtain $\Sigma \vdash \varphi \wedge \neg\varphi$, in contradiction to the assumption that Σ is consistent. ☐

We can now extend the characterizations in 2.6.4 of the completeness property of a theory.

2.7.4. **Corollary.** *The following conditions are equivalent for every theory* $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$*.*

(i) Σ *is a complete theory.*
(ii) There is an $\mathscr{L}$*-structure* $\mathscr{M}$ *with* $\Sigma = \mathrm{Th}(\mathscr{M})$*.*
(iii) Σ *is deductively closed for all models* $\mathscr{M}$ *and* $\mathscr{N}$ *of* Σ *we have* $\mathrm{Th}(\mathscr{M}) = \mathrm{Th}(\mathscr{N})$*.*

Proof. This is done in question 65 of the example sheets. ☐

2.7.5. **Theorem.** *(Compactness Theorem)*
If $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ *and every finite subset of* Σ *has a model at some assignment, then also* Σ *has a model at some assignment.*

Proof. By 2.7.3 it is enough to show that Σ is consistent. Since proofs are finite, this can be checked by looking into finite subsets of Σ. But our assumption and the Soundness Theorem imply that every finite subset of Σ is consistent. ☐

2.7.6**. Remark on the terminology.** Readers familiar with topology might wonder whether *compactness* here refers to compact topological spaces. This indeed is the case: The theorem says precisely that the following space S (called *type space* of $\mathscr{L}$) is compact: S is the set of all complete $\mathscr{L}$-theories, together with the topology generated by the sets $\{p \in S \mid \varphi \in p\}$, where φ runs through the $\mathscr{L}$-sentences.

The compactness theorem has remarkable consequences and is the foundation of Model Theory, to be studied in the next chapter. First applications are given right away:

2.7.7. *Examples.*

(A) *Finite and infinite structures.* Let $\mathscr{L}$ be any language. For $n \in \mathbb{N}$, let ε_n be the $\mathscr{L}$-sentence

$$\exists x_1 \dots x_n \, \forall y \bigvee_{1 \leq i \leq n} y \doteq x_i$$

and let σ_n be the $\mathscr{L}$-sentence

$$\exists x_1 \dots x_n \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j.$$

(i) An $\mathscr{L}$-structure $\mathscr{M}$ is a model of ε_n if and only if $\mathscr{M}$ has size at most n and $\mathscr{M}$ is a model of σ_n if and only if $\mathscr{M}$ has size at least n. We have discussed this at length in questions 27 and 48 of the example sheets. Consequently $\mathscr{M}$ is a model of $\varepsilon_n \wedge \sigma_n$ if and only if the size of $\mathscr{M}$ is n.

(ii) It follows from (i) that an $\mathscr{L}$-structure $\mathscr{M}$ is infinite if and only is $\mathscr{M}$ is a model of the set

$$\Sigma_\infty = \{\sigma_n \mid n \in \mathbb{N}\}.$$

(iii) In spite of (ii) there is no **single** sentence ψ in any language $\mathscr{L}$ such that the infinite $\mathscr{L}$-structures are **precisely** the models of ψ; informally: there is no way to express that a structure is infinite, using only a single sentence.

To see this we assume there is such a sentence ψ and we use the compactness theorem to derive a contradiction: Consider the set

$$\Gamma = \{\neg\psi\} \cup \Sigma_\infty.$$

Let $\Gamma_0 \subseteq \Gamma$ be finite and choose $n \in \mathbb{N}$ with

$$\Gamma_0 \subseteq \{\neg\psi, \sigma_1, \dots, \sigma_n\}$$

Then any finite $\mathscr{L}$-structure with at least n-elements (in its universe) satisfies Γ_0, because by assumption it satisfies $\neg\psi$ and the σ_i with $i \leq n$ hold in any structure of size n (see (i)). By the compactness theorem, Γ has a model $\mathscr{M}$. Since $\mathscr{M} \models \Sigma_\infty$, the structure $\mathscr{M}$ is infinite. However by assumption, every model of $\neg\psi$ is finite, a contradiction.

(iv) There are sentences in some languages that are consistent and that have only infinite models. One such example will be done in question 64.

(B) *Pseudo Finite Groups.* There is an **infinite** group G that has the following surprising property: Whenever φ is a sentence in the language of groups that is true in **all finite** groups, then φ is true in G.[32]

This can be seen with the aid of the compactness theorem. Let Σ be the set of all sentences in the language of groups that are true in all finite groups and let

$$\Gamma = \Sigma \cup \Sigma_\infty.$$

(Σ_∞ defined as in (A)) The example just claims that Γ has a model and by the compactness theorem we just need to show that every finite subset Γ_0 of Γ has a model. Since Γ_0 is finite, there is some $n \in \mathbb{N}$ such that

$$(*) \qquad \Gamma_0 \subseteq \Sigma \cup \{\sigma_1, \dots, \sigma_n\},$$

where σ_n is defined as in (A). The group $(\mathbb{Z}/n\mathbb{Z}, +, 0)$ is a model of Σ by definition of Σ. Since $\mathbb{Z}/n\mathbb{Z}$ has size n, this group also satisfies $\sigma_1, \dots, \sigma_n$. By $(*)$, this group is a model of Γ_0, as required.

We conclude this section with a theorem on how to write formulas in a natural way. This could have been proved earlier on a syntactic level (using formal proofs), instead we use the Completeness Theorem as this shortens the arguments:

The Prenex Normal Form Theorem

2.7.8. **Definition.** An $\mathscr{L}$-formula φ is said to be in **prenex normal form** if there are $n \in \mathbb{N}_0$, $x_1, ..., x_n \in \mathrm{Vbl}$, $Q_1, ..., Q_n \in \{\forall, \exists\}$ and a quantifier free formula χ such that φ is $Q_1 x_1 ... Q_n x_n\ \chi$.

We will show that every $\mathscr{L}$-formula is provably equivalent to a formula in prenex normal form.

2.7.9. **Lemma.** *If φ, ψ are $\mathscr{L}$-formulas and $x \notin \mathrm{Fr}\,\psi$, $y \notin \mathrm{Fr}\,\varphi$ then*

(i) $\vdash ((\forall x\varphi) \wedge (\forall y\psi)) \leftrightarrow \forall xy(\varphi \wedge \psi)$.
(ii) $\vdash ((\forall x\varphi) \vee (\forall y\psi)) \leftrightarrow \forall xy(\varphi \vee \psi)$.
(iii) $\vdash ((\exists x\varphi) \vee (\exists y\psi)) \leftrightarrow \exists xy(\varphi \vee \psi)$.
(iv) $\vdash ((\exists x\varphi) \wedge (\exists y\psi)) \leftrightarrow \exists xy(\varphi \wedge \psi)$.

Proof. In all statements we may assume that $x \neq y$. Otherwise, our assumption $x \notin \mathrm{Fr}\,\psi$ and $y \notin \mathrm{Fr}\,\varphi$ implies that neither x nor y occurs freely in any of the formulas under consideration; now observe that $\vdash \varphi \leftrightarrow \forall x\varphi$ for each formula φ and every variable $x \notin \mathrm{Fr}(\varphi)$.

(i) By the Completeness Theorem 2.7.1 it suffices to show $\models ((\forall x\varphi) \wedge (\forall y\psi)) \leftrightarrow \forall xy(\varphi \wedge \psi)$. Hence we have to take an $\mathscr{L}$-structure $\mathscr{M}$ and an assignment h of $\mathscr{M}$ and we have to show that $\mathscr{M} \models ((\forall x\varphi) \wedge (\forall y\psi))[h] \iff \mathscr{M} \models \forall xy(\varphi \wedge \psi)[h]$. The implication "$\Leftarrow$" is clear. For the implication "$\Rightarrow$" we use assumption $x \notin \mathrm{Fr}\,\psi$ and $y \notin \mathrm{Fr}\,\varphi$ and 2.4.12.

[32]Groups with these properties are called *pseudo finite*.

(ii). By the Completeness Theorem 2.7.1 it suffices to show $\models ((\forall x\varphi) \vee (\forall y\psi)) \leftrightarrow \forall xy(\varphi \vee \psi)$. Hence we have to take an $\mathscr{L}$-structure $\mathscr{M}$ and an assignment h of $\mathscr{M}$ and we have to show that

$$\mathscr{M} \models (\forall x\varphi) \vee (\forall y\psi)[h] \iff \mathscr{M} \models \forall xy(\varphi \vee \psi)[h].$$

"$\Rightarrow$": We may assume that $\mathscr{M} \models (\forall x\varphi)[h]$. Since y does not occur freely in φ we get $\mathscr{M} \models (\forall xy\varphi)[h]$ from 2.4.12. But then $\mathscr{M} \models \forall xy(\varphi \vee \psi)[h]$ as well.

"$\Leftarrow$": Suppose $\mathscr{M} \not\models (\forall x\varphi) \vee (\forall y\psi)[h]$. Hence there are $a, b \in |\mathscr{M}|$ with $\mathscr{M} \not\models \varphi[h\binom{x}{a}]$ and $\mathscr{M} \not\models \psi[h\binom{y}{b}]$. Since $x \notin \operatorname{Fr}\psi$ and $y \notin \operatorname{Fr}\varphi$ and $x \neq y$ and by using 2.4.12 again, we have $\mathscr{M} \not\models \varphi \vee \psi[h\binom{x}{a}\binom{y}{b}]$. Hence $\mathscr{M} \not\models \forall xy(\varphi \vee \psi)[h]$.

(iii) and (iv) follow from (i) and (ii) by contraposition. □

2.7.10. **Lemma.** *If φ is an $\mathscr{L}$-formula, $x, y \in \mathrm{Vbl}$ and x is free in φ for y then*

$$\vdash (\forall x\varphi) \leftrightarrow (\forall y\varphi(x/y)) \text{ and } \vdash (\exists x\varphi) \leftrightarrow (\exists y\varphi(x/y)).$$

Proof. From the Completeness Theorem 2.7.1 using 2.4.11. □

2.7.11. **Theorem.** *(Prenex Normal Form Theorem)*
Every $\mathscr{L}$-formula is provably equivalent to a formula in prenex normal form.

Proof. By induction on the complexity of φ, where φ is already in prenex normal form if φ is quantifier free.

If $\varphi = \neg\psi$ or $\varphi = \forall y\psi$ and ψ is provably equivalent to a formula in prenex normal form then clearly φ also is provably equivalent to a formula in prenex normal form.

It remains to show that $\varphi \wedge \psi$ is provably equivalent to a formula in prenex normal form provided φ and ψ have this property.

So assume $\vdash \varphi \leftrightarrow Q_1x_1...Q_nx_n\ \chi$ and $\vdash \psi \leftrightarrow P_1y_1...P_ky_k\ \delta$ with quantifier free formulas χ, δ and $Q_i, P_j \in \{\forall\exists\}$.

Using 2.7.10 n-times we may substitute all variables x_i in the string $Q_1x_1...Q_nx_n\ \chi$ by variables which do not occur in $P_1y_1...P_ky_k\ \delta$. Hence we may assume that no x_i occurs in $P_1y_1...P_ky_k\ \delta$. Applying this again to $P_1y_1...P_ky_k\ \delta$ we may also assume that no y_j occurs in $Q_1x_1...Q_nx_n\ \chi$. Moreover we may assume that $k = n$, otherwise fix this by placing quantifiers in front of one of the formulas containing a new variable. Now we can apply 2.7.9(i) and (iv) to obtain

$$\vdash Q_1x_1...Q_nx_n\ \chi \wedge P_1y_1...P_ky_n\ \delta \leftrightarrow Q_1x_1P_1y_1...Q_nx_nP_nx_n(\chi \wedge \delta).$$

Hence also $\varphi \wedge \psi$ is provably equivalent to $Q_1x_1P_1y_1...Q_nx_nP_nx_n(\chi \wedge \delta)$, which is in prenex normal form. □

2.7.12. *Example.* Let $\varphi = Q_1x_1...Q_nx_n\ \chi$ and $\varphi' = Q'_1y_1...Q'_ky_k\ \chi'$ be formulas in prenex normal form. We want to find a formula ϑ in prenex normal form such that $\vdash (\varphi \to \varphi') \leftrightarrow \vartheta$.

Let $u_1, ..., u_n$ be variables neither occurring in φ nor in φ' such that $u_i = u_j$ for all $i, j \in \{1, ..., n\}$ with $x_i = x_j$. Applying n-times 2.7.10 we see that $\vdash \varphi \leftrightarrow Q_1u_1...Q_nu_n\ \chi(x_1/u_1)...(x_n/u_n)$. Hence we may replace χ by $\chi(x_1/u_1)...(x_n/u_n)$ and x_i by u_i if necessary and so we may assume that no x_i occurs in φ'. By applying the same argument to φ' instead of φ we may also assume that no y_j occurs in φ.

For $i \in \{1, ..., n\}$, let $Q_i^* := \begin{cases} \forall & \text{if } Q_i \text{ is } \exists, \\ \exists & \text{if } Q_i \text{ is } \forall. \end{cases}$

Let

$$\vartheta := Q_1^*x_1...Q_n^*x_nQ'_1y_1...Q'_ky_k(\chi \to \chi').$$

By completeness, $\vdash \neg\varphi \leftrightarrow Q_1^*x_1...Q_n^*x_n\ \neg\chi$. Since $\vdash (\varphi \to \varphi') \leftrightarrow (\neg\varphi \vee \varphi')$ we obtain $\vdash (\varphi \to \varphi') \leftrightarrow \vartheta$ from the Completeness Theorem (keeping in mind that none of the x_i occurs in φ' and none of the y_j occurs in φ).

2.8. **Proof of the Completeness Theorem.**

`Except for the statements that occur outside of this section, the entire section is not examinable.`

The core problem in the proof of the Completeness Theorem is the "construction" of a model of a consistent set Σ of $\mathscr{L}$-sentences. Hence we need to use the information that Σ does not formally prove a contradiction in order to "construct" a model of Σ.

In subsection B. below we give an outline of the proof before we carry out the details. First we need to talk about a general method for building structures out of formulas:

A. Term Algebras

In this subsection we introduce a key tool for building structures, namely *term algebras* of (consistent) sets of formulas, which play a key role in the proof of the Completeness Theorem. Independently of this application, the construction of term algebras is omnipresent and highly important in mathematics.

2.8.1. *Notation.* Let $\mathscr{L}=(\lambda:\mathscr{R}\longrightarrow\mathbb{N},\mu:\mathscr{F}\longrightarrow\mathbb{N},\mathscr{C})$ be a language. The set of all closed terms of $\mathscr{L}$ is denoted by $\mathrm{ctm}(\mathscr{L})$. Recall from 2.3.26(iv) that an $\mathscr{L}$-term is closed (or constant) if no variable occurs in it.

Notice that $\mathscr{C}\subseteq\mathrm{tm}(\mathscr{L})$, in particular $\mathrm{ctm}(\mathscr{L})\neq\emptyset$ if $\mathscr{L}$ has a constant symbol.

Before we give the definition of term algebras, more precisely of the domain of a term algebra, we have to understand the following relation $\sim_\Sigma$ on $\mathrm{ctm}(\mathscr{L})$ for a given subset Σ of $\mathrm{Fml}(\mathscr{L})$. We define

$$t_1\sim_\Sigma t_2 \quad :\Longleftrightarrow \qquad \Sigma\vdash t_1\doteq t_2 \ \ (t_1,t_2\in\mathrm{ctm}(\mathscr{L})).$$

2.8.2. **Lemma.** *Let $\Sigma\subseteq\mathrm{Fml}(\mathscr{L})$.*

(i) $\sim_\Sigma$ is an equivalence relation on $\mathrm{ctm}(\mathscr{L})$.
(ii) If $F\in\mathscr{F}$ is a function symbol of arity n and $t_1,s_1,...,t_n,s_n\in\mathrm{ctm}(\mathscr{L})$ with $t_i\sim_\Sigma s_i$ for each i, then $F(t_1,...,t_n)\sim_\Sigma F(s_1,...,s_n)$.
(iii) If $R\in\mathscr{R}$ is a relation symbol of arity n and $t_1,s_1,...,t_n,s_n\in\mathrm{ctm}(\mathscr{L})$ with $t_i\sim_\Sigma s_i$ for each i, then $\Sigma\vdash R(t_1,...,t_n)\leftrightarrow R(s_1,...,s_n)$.

Proof. (i). If $t\in\mathrm{ctm}(\mathscr{L})$, then $t\sim_\Sigma t$: To see this, apply (**AxEq**)(a) and (**Ax**$\forall$) to obtain $\vdash\forall x\ x\doteq x$. Then using (**AxSubst**) and Modus Ponens shows $\vdash t\doteq t$.

Now let $t_1,t_2,t_3\in\mathrm{ctm}(\mathscr{L})$ with $t_1\sim_\Sigma t_2$ and $t_2\sim_\Sigma t_3$. We have to show $t_3\sim_\Sigma t_1$. Let x,y,z be three distinct variables. By (**AxEq**)(b) and (**Ax**$\forall$) we know $\vdash\forall xyz\ (x\doteq y\wedge y\doteq z\ \rightarrow\ z\doteq x)$. Applying (**AxSubst**) three times we get $\vdash(t_1\doteq t_2\wedge t_2\doteq t_3)\ \rightarrow\ t_3\doteq t_1$. Using a suitable tautology we obtain

$$\vdash t_1\doteq t_2\rightarrow(t_2\doteq t_3\rightarrow t_3\doteq t_1).$$

Now, using Modus Ponens and the assumption $\Sigma\vdash t_1\doteq t_2$ and $\Sigma\vdash t_2\doteq t_3$ shows $\Sigma\vdash t_3\doteq t_1$ as desired.

(ii). Let $x_1, y_1, ..., x_n, y_n$ be mutually distinct variables. The following are instances of (**AxEq**)(c):

$$\begin{array}{rcl} x_1 \doteq y_1 & \to & F(x_1, ..., x_n) \doteq F(y_1, x_2, ..., x_n) \\ x_2 \doteq y_2 & \to & F(y_1, x_2, ..., x_n) \doteq F(y_1, y_2, x_3, ..., x_n) \\ & \vdots & \\ x_n \doteq y_n & \to & F(y_1, ..., y_{n-1}, x_n) \doteq F(y_1, ..., y_n) \end{array}$$

Using a suitable tautology and (**AxEq**)(a),(b) then entail

$$\vdash (x_1 \doteq y_1 \land ... \land x_n \doteq y_n) \to F(x_1, ..., x_n) \doteq F(y_1, ..., y_n)$$

By the generalisation theorem 2.5.21 applied $2n$ times we get

$$\vdash \forall x_1 y_1 ... x_n y_n \left((x_1 \doteq y_1 \land ... \land x_n \doteq y_n) \to F(x_1, ..., x_n) \doteq F(y_1, ..., y_n) \right).$$

By applying (**AxSubst**) $2n$-times we obtain

$$\vdash (t_1 \doteq s_1 \land ... \land t_n \doteq s_n) \to F(t_1, ..., t_n) \doteq F(s_1, ..., s_n)$$

and using a suitable tautology we get

$$\vdash (t_1 \doteq s_1 \to (t_2 \doteq s_2 \to ...(t_n \doteq s_n \to F(t_1, ..., t_n) \doteq F(s_1, ..., s_n))...)$$

Since $\Sigma \vdash t_i \doteq s_i$ for all i we may now apply Modus Ponens for proofs n-times to obtain $F(t_1, ..., t_n) \sim_\Sigma F(s_1, ..., s_n)$.

(iii). Let $x_1, y_1, ..., x_n, y_n$ be mutually distinct variables. The following are instances of (**AxEq**)(d):

$$\begin{array}{rcl} x_1 \doteq y_1 & \to & (R(x_1, ..., x_n) \leftrightarrow R(y_1, x_2, ..., x_n)) \\ x_2 \doteq y_2 & \to & (R(y_1, x_2, ..., x_n) \leftrightarrow R(y_1, y_2, x_3, ..., x_n)) \\ & \vdots & \\ x_n \doteq y_n & \to & (R(y_1, ..., y_{n-1}, x_n) \leftrightarrow R(y_1, ..., y_n)) \end{array}$$

Using a suitable tautology we obtain

$$\vdash (x_1 \doteq y_1 \land ... \land x_n \doteq y_n) \to (R(x_1, ..., x_n) \leftrightarrow R(y_1, ..., y_n)).$$

By the generalisation theorem 2.5.21 applied $2n$ times we get

$$\vdash \forall x_1 y_1 ... x_n y_n \left((x_1 \doteq y_1 \land ... \land x_n \doteq y_n) \to (R(x_1, ..., x_n) \leftrightarrow R(y_1, ..., y_n)) \right).$$

By applying (**AxSubst**) $2n$-times we obtain

$$\vdash (t_1 \doteq s_1 \land ... \land t_n \doteq s_n) \to (R(t_1, ..., t_n) \leftrightarrow R(s_1, ..., s_n)).$$

Since $\Sigma \vdash t_i \doteq s_i$ for all i me may again use a suitable tautology and Modus Ponens for proofs n-times to obtain $R(t_1, ..., t_n) \leftrightarrow R(s_1, ..., s_n)$. □

2.8.3. **Definition of Term Algebras** Let $\mathscr{L}$ be a language with at least one constant symbol and let Σ be a set of $\mathscr{L}$-formulas. We will now define a certain $\mathscr{L}$-structure attached to Σ, called the **term algebra of** Σ and denoted by $\mathrm{TmAlg}(\Sigma)$.

Warning: Before giving the definition, it has to be mentioned that the term algebra of Σ will in general *not* be a model of Σ (at any assignment).

Now the definition of $\mathrm{TmAlg}(\Sigma)$.

(i) The domain of $\mathrm{TmAlg}(\Sigma)$ is defined to be the set of equivalence classes of constant $\mathscr{L}$-terms with respect to the equivalence relation $\sim_\Sigma$ (cf. 2.8.2(i)):
$$|\,\mathrm{TmAlg}(\Sigma)| := \mathrm{ctm}(\mathscr{L})/\sim_\Sigma .$$
We denote the equivalence class of $t \in \mathrm{ctm}(\mathscr{L})$ with respect to $\sim_\Sigma$ by $t/\sim_\Sigma$.

(ii) For $R \in \mathscr{R}$ of arity n we define
$$R^{\mathrm{TmAlg}(\Sigma)} = \{(t_1/\sim_\Sigma, ..., t_n/\sim_\Sigma) \mid t_i \in \mathrm{ctm}(\mathscr{L}) \text{ and } \Sigma \vdash R(t_1, ..., t_n)\}.$$
This is correct by 2.8.2(iii)

(iii) For $F \in \mathscr{F}$ of arity n we define the function $F^{\mathrm{TmAlg}(\Sigma)} : |\,\mathrm{TmAlg}(\Sigma)|^n \longrightarrow |\,\mathrm{TmAlg}(\Sigma)|$ by
$$F^{\mathrm{TmAlg}(\Sigma)}(t_1/\sim_\Sigma, ..., t_n/\sim_\Sigma) := F(t_1, ..., t_n)/\sim_\Sigma .$$
This is correct by 2.8.2(ii)

(iv) For $c \in \mathcal{C}$ we define
$$c^{\mathrm{TmAlg}(\Sigma)} := c/\sim_\Sigma \quad (\in |\,\mathrm{TmAlg}(\Sigma)|).$$

The **term algebra of a formula** σ is defined as the term algebra of $\{\sigma\}$.

2.8.4. *Example.* Here is an example of a consistent set Σ such that $\mathrm{TmAlg}(\Sigma)$ is not a model of Σ: Let $\mathscr{L}$ be a language that has exactly one constant symbol c and no function symbols. Let $\sigma = \exists x\ x \neq c$. Since every $\mathscr{L}$-structure with more than one element is a model of σ, σ is consistent (Soundness!). Moreover, the models of σ are precisely the $\mathscr{L}$-structures with more than one element. However, the term algebra of σ only has one element, since already $\mathrm{ctm}(\mathscr{L})$ only has one element!

2.8.5. *Example.* Let us compute another term algebra. This time, suppose $\mathscr{L}$ is a language that has exactly three constant symbols c, d, e and no function symbols (observe that $\mathscr{L}$ might have relation symbols). Let σ be the $\mathscr{L}$-sentence $c \doteq d \vee c \doteq e$. Since $\mathscr{L}$ does not have function symbols, $\mathrm{ctm}(\mathscr{L}) = \{c, d, e\}$. Hence $\mathrm{TmAlg}(\sigma)$ has *at most* three elements: $|\,\mathrm{TmAlg}(\sigma)| = \{c/\sim_\sigma, d/\sim_\sigma, e/\sim_\sigma\}$. What is the size of $\mathrm{TmAlg}(\sigma)$? We need to check which of the elements $c/\sim_\sigma, d/\sim_\sigma, e/\sim_\sigma$ of $|\,\mathrm{TmAlg}(\sigma)|$ are in fact different. By definition of the equivalence relation $\sim_\sigma$, this means we have to check whether or not $\sigma \vdash c \doteq d$, $\sigma \vdash c \doteq e$ and $\sigma \vdash d \doteq e$. Since σ is the sentence $c \doteq d \vee c \doteq e$ one could have a suspicion that $\sigma \vdash c \doteq d$ or $\sigma \vdash c \doteq e$. However, both fail and also $\sigma \vdash d \doteq e$ fails. In order to see that $\sigma \nvdash c \doteq d$, take an $\mathscr{L}$-structure $\mathscr{M}$ with universe $|\mathscr{M}| := \{1, 2\}$,
$$c^{\mathscr{M}} := 1,\ d^{\mathscr{M}} := 2 \text{ and } e^{\mathscr{M}} := 1.$$

The relation symbols of $\mathscr{L}$ can be assigned arbitrarily in $\mathscr{M}$. Then $\mathscr{M}$ is a model of σ, as $\mathscr{M} \models c \doteq d \vee c \doteq e$. But obviously $\mathscr{M}$ is not a model of $c \doteq d$. Hence by Soundness, we cannot have $\sigma \vdash c \doteq d$, i.e. we have $\sigma \nvdash c \doteq d$. Be aware, that this does NOT mean $\sigma \vdash \neg c \doteq d$, because every $\mathscr{L}$ structure with exactly one element satisfies σ and $c \doteq d$.

Thus $\sigma \nvdash c \doteq d$ and similarly $\sigma \nvdash c \doteq e$ and $\sigma \nvdash d \doteq e$. It follows that $\mathrm{TmAlg}(\sigma)$ has three elements and by definition

$$c^{\mathrm{TmAlg}(\sigma)} := c/\sim_\sigma,\ d^{\mathrm{TmAlg}(\sigma)} := d/\sim_\sigma \text{ and } e^{\mathrm{TmAlg}(\sigma)} := e/\sim_\sigma .$$

It remains to see, how the relation symbols of $\mathscr{L}$ are interpreted in $\mathrm{TmAlg}(\sigma)$: Let R be an n-ary relation symbol of $\mathscr{L}$. We claim that

$$(*) \qquad R^{\mathrm{TmAlg}(\sigma)} = \emptyset.$$

In order to see this, we pick $t_1, ..., t_n \in \mathrm{ctm}(\mathscr{L})$ and we have to show $\sigma \nvdash R(t_1, ..., t_n)$ (convince yourself that this is precisely the meaning of $(*)$). We may use the soundness theorem again and so it is enough to find a model $\mathscr{M}$ of σ with $\mathscr{M} \not\models R(t_1, ..., t_n)$. We choose $\mathscr{M}$ of size 1 (then we automatically have $\mathscr{M} \models \sigma$) and let $R^{\mathscr{M}} := \emptyset$.

2.8.6. **Proposition.** *Let $\mathscr{L}$ be a language with at least one constant symbol and let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$. Let $n \in \mathbb{N}_0$, $t_1, ..., t_n \in \mathrm{ctm}(\mathscr{L})$, $x_1, ..., x_n \in \mathrm{Vbl}$ pairwise distinct and let h be an assignment of $\mathrm{TmAlg}(\Sigma)$ with $h(x_i) = t_i/\sim$ $(1 \le i \le n)$.*

(i) If $t(x_1, ..., x_n) \in \mathrm{tm}(\mathscr{L})$ then $t^{\mathrm{TmAlg}(\Sigma)}[h] = t(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma$.

(ii) If $\varphi(x_1, ..., x_n) \in \mathrm{Fml}(\mathscr{L})$ is atomic then

$$\mathrm{TmAlg}(\Sigma) \models \varphi[h] \iff \Sigma \vdash \varphi(x_1/t_1, ..., x_n/t_n).$$

Proof. (i). We show $t^{\mathrm{TmAlg}(\Sigma)}[h] = t(x_1/t_1, ..., x_n/t_n)/\sim$ by induction on the complexity of t. If $t = x_i$ then $t^{\mathrm{TmAlg}(\Sigma)}[h] = h(x_i) = t_i/\sim_\Sigma$ as desired. If $t = c$ is a constant symbol then $t^{\mathrm{TmAlg}(\Sigma)}[h] = c^{\mathrm{TmAlg}(\Sigma)}$ and $t(x_1/t_1, ..., x_n/t_n) = c$ as desired.

For the induction step we may assume that

$$t = F(t_1'(x_1, ..., x_n), ..., t_k'(x_1, ..., x_n))$$

with $t_i' \in \mathrm{tm}(\mathscr{L})$ and $F \in \mathscr{F}$ of arity k. Then $t^{\mathrm{TmAlg}(\Sigma)}[h] =$

$$\begin{aligned}
&= F^{\mathrm{TmAlg}(\Sigma)}(t_1'^{\mathrm{TmAlg}(\Sigma)}[h], ..., t_k'^{\mathrm{TmAlg}(\Sigma)}[h]) \stackrel{\text{by ind. hyp.}}{=} \\
&= F^{\mathrm{TmAlg}(\Sigma)}(t_1'(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma, ..., t_k'(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma) \stackrel{\text{by def.}}{=} \\
&= F(t_1'(x_1/t_1, ..., x_n/t_n), ..., t_k'(x_1/t_1, ..., x_n/t_n))/\sim_\Sigma = t(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma .
\end{aligned}$$

(ii). In order to prove the equivalence we have two cases:

Case 1. φ is of the form $t \doteq s$ with $t(x_1, ..., x_n)$, $s(x_1, .., x_n) \in \mathrm{tm}(\mathscr{L})$.

Then

$$\begin{aligned}
\mathrm{TmAlg}(\Sigma) \models \varphi[h] &\stackrel{\text{by def.}}{\iff} t^{\mathrm{TmAlg}(\Sigma)}[h] = s^{\mathrm{TmAlg}(\Sigma)}[h] \\
&\stackrel{\text{by (i)}}{\iff} t(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma = s(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma \\
&\stackrel{\text{by def.}}{\iff} \Sigma \vdash t(x_1/t_1, ..., x_n/t_n) \doteq s(x_1/t_1, ..., x_n/t_n) \\
&\iff \Sigma \vdash \varphi(x_1/t_1, ..., x_n/t_n).
\end{aligned}$$

Case 2. φ is of the form $R(t'_1, ..., t'_k)$ with $t'_i(x_1, ..., x_n) \in \mathrm{tm}(\mathscr{L})$ and $R \in \mathscr{R}$ of arity k.
Then

$$\begin{aligned}
\mathrm{TmAlg}(\Sigma) \models \varphi[h] &\overset{\text{by def.}}{\iff} ({t'_1}^{\mathrm{TmAlg}(\Sigma)}[h], ..., {t'_k}^{\mathrm{TmAlg}(\Sigma)}[h]) \in R^{\mathrm{TmAlg}(\Sigma)} \\
&\overset{\text{by (i)}}{\iff} (t'_1(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma, ..., t'_k(x_1/t_1, ..., x_n/t_n)/\sim_\Sigma) \\
&\qquad\qquad \in R^{\mathrm{TmAlg}(\Sigma)} \\
&\overset{\text{by def.}}{\iff} \Sigma \vdash R(t'_1(x_1/t_1, ..., x_n/t_n), ..., t'_k(x_1/t_1, ..., x_n/t_n)) \\
&\iff \Sigma \vdash \varphi(x_1/t_1, ..., x_n/t_n).
\end{aligned}$$

□

2.8.7. **Corollary.** *If* $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ *and* $\varphi_1, ..., \varphi_n$ *are atomic* $\mathscr{L}$*-sentences (i.e. formulas from* $\mathrm{Sen}(\mathscr{L}) \cap \text{at-Fml}(\mathscr{L})$*), then*

$$\Sigma \vdash \varphi_1 \wedge ... \wedge \varphi_n \iff \mathrm{TmAlg}(\Sigma) \models \varphi_1 \wedge ... \wedge \varphi_n.$$

Proof. By 2.8.6(ii) using with 2.5.12(ii). □

2.8.8. **Proposition.** *Let* $\mathscr{L}$ *be a language with at least one constant symbol and let* $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$*. Let* $\varphi_1, ..., \varphi_n, \psi$ *be atomic* $\mathscr{L}$*-formulas with free variables among* $x_1, ..., x_k$*.*
If

$$\Sigma \vdash (\varphi_1 \wedge ... \wedge \varphi_n) \to \psi$$

then

$$\mathrm{TmAlg}(\Sigma) \models \forall x_1 ... x_k((\varphi_1 \wedge ... \wedge \varphi_n) \to \psi).$$

Proof. Take $t_1, ..., t_k \in \mathrm{ctm}(\mathscr{L})$ and let h be an assignment of $\mathrm{TmAlg}(\Sigma)$ with $h(x_i) = t_i/\sim$. Suppose $\mathrm{TmAlg}(\Sigma) \models \bigwedge_i \varphi_i[h]$. We have to show $\mathrm{TmAlg}(\Sigma) \models \psi[h]$. Define

$$\varepsilon_i := \varphi_i(x_1/t_1, ..., x_k/t_k) \text{ and } \delta := \psi(x_1/t_1, ..., x_k/t_k).$$

By 2.8.6 we know $\Sigma \vdash \varepsilon_i$ for each i, consequently $\Sigma \vdash \varepsilon_1 \wedge ... \wedge \varepsilon_n$ (cf. 2.5.12(ii)). Since $\Sigma \vdash (\varphi_1 \wedge ... \wedge \varphi_n) \to \psi$ and none of the x_i occurs freely in any formula from Σ we may apply the Generalisation Theorem 2.5.21 to obtain

$$\Sigma \vdash \forall x_1 ... x_k \ ((\varphi_1 \wedge ... \wedge \varphi_n) \to \psi).$$

Now (**AxSubst**) (applied k-times) and Modus Ponens gives

$$\Sigma \vdash (\varepsilon_1 \wedge ... \wedge \varepsilon_n) \to \delta.$$

Thus we get $\Sigma \vdash \delta$, which means $\mathrm{TmAlg}(\Sigma) \models \psi[h]$ by 2.8.6 again. □

B. Strategy for the proof of the Completeness Theorem

For a given consistent set Σ of $\mathscr{L}$-sentences we would like to "construct" a model of Σ. In fact we shall not construct such a model, instead we only show the existence of a model. In subsection A. we have introduced a method how to attach an $\mathscr{L}$-structure to Σ, namely the structure $\mathrm{TmAlg}(\Sigma)$. In general $\mathrm{TmAlg}(\Sigma)$ is not a model of Σ. In this subsection we show that under two assumptions on Σ, namely "Σ is a complete theory" (defined in 2.6.1) and "Σ possesses a system of witnesses" (defined in 2.8.10 below), the term algebra of Σ indeed is a model of Σ. In subsequent sections we will show how to use this fact for a general Σ. This is explained in more details in 2.8.12 below.

2.8.9. *Notation.* Given a language $\mathscr{L}$ we define $\mathrm{Fml}(\mathscr{L})(1)$ as the set of all $\mathscr{L}$-formulas with at most one free variable.

2.8.10. **Definition.** Let $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$. A **system of witnesses** for Σ is a map

$$\zeta : \mathrm{Fml}(\mathscr{L})(1) \longrightarrow \mathscr{C}$$

such that for all $x \in \mathrm{Vbl}$ and all $\varphi(x) \in \mathrm{Fml}(\mathscr{L})(1)$ we have

$$\Sigma \vdash (\exists x\varphi) \ \rightarrow \ \varphi(x/\zeta(\varphi)).$$

One can read this informally on the semantic side as saying that for each $\varphi \in \mathrm{Fml}(\mathscr{L})(1)$, if in a model $\mathscr{M}$ of Σ the formula φ has a solution in $\mathscr{M}$ (i.e. $\mathscr{M} \models \exists x\, \varphi$), then the language has a name for such a solution (namely $\zeta(\varphi)$). In this sense, $\zeta(\varphi)$ witnesses truth of $\exists x\, \varphi$ in *any* model of Σ.

2.8.11. **Proposition.** *If $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ is a complete theory and if Σ possesses a system of witnesses, then the term algebra of Σ is a model of Σ.*

Proof. It suffices to prove by induction on the complexity of $\varphi(x_1, ..., x_n) \in \mathrm{Fml}(\mathscr{L})$ the following:

For all $t_1, ..., t_n \in \mathrm{ctm}(\mathscr{L})$,

$$(\dagger) \qquad \Sigma \vdash \varphi(x_1/t_1, ..., x_n/t_n) \iff \mathrm{TmAlg}(\Sigma) \models \varphi(x_1/t_1, ..., x_n/t_n).$$

If φ is atomic, then we know this from 2.8.6 (without any assumption on Σ).

If $\varphi = \neg\psi$, then

$$\begin{aligned}
\Sigma \vdash \varphi(x_1/t_1, ..., x_n/t_n) &\iff \Sigma \vdash \neg\psi(x_1/t_1, ..., x_n/t_n) \\
&\overset{\text{as } \Sigma \text{ is complete}}{\iff} \Sigma \nvdash \psi(x_1/t_1, ..., x_n/t_n) \\
&\overset{\text{by ind. hypoth.}}{\iff} \mathrm{TmAlg}(\Sigma) \not\models \psi(x_1/t_1, ..., x_n/t_n) \\
&\iff \mathrm{TmAlg}(\Sigma) \models \varphi(x_1/t_1, ..., x_n/t_n)
\end{aligned}$$

If $\varphi = \varphi_1 \wedge \varphi_2$ then $(\dagger)$ holds if and only if $(\dagger)$ for both φ_1 and φ_2. Therefore, if φ is $\psi \rightarrow \gamma$, and $(\dagger)$ holds for ψ and γ, then $(\dagger)$ also holds for φ: φ is provably equivalent to $\neg(\psi \wedge \neg\gamma)$.

It remains to do the case $\varphi = \forall y\psi$, where $y \in \mathrm{Vbl}$ is arbitrary. As $\mathrm{Fr}(\varphi) \subseteq \{x_1, ..., x_n\}$ and $y \notin \mathrm{Fr}(\varphi)$ we may assume that $y \neq x_i$ $(1 \leq i \leq n)$.

"⇒": $\Sigma \vdash \varphi(x_1/t_1, ..., x_n/t_n)$ means $\Sigma \vdash \forall y\psi(x_1/t_1, ..., x_n/t_n)$, hence by **AxSubst** we have

$$\Sigma \vdash \psi(x_1/t_1, ..., x_n/t_n, y/t) \text{ for all } t \in \mathrm{ctm}(\mathscr{L}).$$

From the induction hypothesis we get $\mathrm{TmAlg}(\Sigma) \models \psi(x_1/t_1, ..., x_n/t_n, y/t)$ for all $t \in \mathrm{ctm}(\mathscr{L})$. By 2.4.11 this means

$$(+) \qquad \mathrm{TmAlg}(\Sigma) \models \psi(x_1/t_1, ..., x_n/t_n)[h]$$

for every assignment h of $\mathrm{TmAlg}(\Sigma)$ with $h(y) = t/\sim_\Sigma$ and all $t \in \mathrm{ctm}(\mathscr{L})$. Since $|\mathrm{TmAlg}(\Sigma)|$ is the set of all $t/\sim_\Sigma$ with $t \in \mathrm{ctm}(\mathscr{L})$, we get, as required,

$$\mathrm{TmAlg}(\Sigma) \models \forall y\ \psi(x_1/t_1, ..., x_n/t_n).$$

"⇐": Here and only here we need that Σ possesses a system of witnesses $\zeta : \mathrm{Fml}(\mathscr{L})(1) \longrightarrow \mathscr{C}$.

Suppose $\mathrm{TmAlg}(\Sigma) \models \forall y\psi(x_1/t_1, ..., x_n/t_n)$, but

$$\Sigma \nvdash \forall y\psi(x_1/t_1, ..., x_n/t_n).$$

Since Σ is complete we have

$$\Sigma \vdash \exists y\neg\psi(x_1/t_1, ..., x_n/t_n).$$

Let $c = \zeta(\neg\psi(x_1/t_1, ..., x_n/t_n))$.

Since ζ is a system of witnesses for Σ we have

$$\Sigma \vdash (\exists y\neg\psi(x_1/t_1, ..., x_n/t_n)) \ \rightarrow \ \neg\psi(x_1/t_1, ..., x_n/t_n)(y/c).$$

With Modus Ponens we get

$$\Sigma \vdash \ \neg\psi(x_1/t_1, ..., x_n/t_n, y/c).$$

In particular $\Sigma \nvdash \psi(x_1/t_1, ..., x_n/t_n, y/c)$. Using the induction hypothesis we obtain

$$\mathrm{TmAlg}(\Sigma) \not\models \psi(x_1/t_1, ..., x_n/t_n, y/c).$$

However, using 2.4.11 again, this contradicts our assumption

$$\mathrm{TmAlg}(\Sigma) \models \forall y\psi(x_1/t_1, ..., x_n/t_n). \qquad \square$$

2.8.12. *Strategy.* Let Σ be an arbitrary consistent set of $\mathscr{L}$-sentences. We will apply 2.8.11 to "construct" a model of Σ, in the following way:

In subsection C. we will show that there is a language $\mathscr{L}^*$ that has the same relation and function symbols as $\mathscr{L}$, but a huge set of constant symbols $\mathscr{C}^*$ (containing the constant symbols of $\mathscr{L}$), together with a consistent set Σ^* of $\mathscr{L}^*$-sentences containing Σ such that Σ^* possesses a system of witnesses (cf. 2.8.24).

In section 2.6 we have seen that every theory in every language is contained in a complete theory (cf. 2.6.6). Applying this to Σ^* gives a complete theory $\Sigma^\dagger$ of $\mathscr{L}^*$-sentences containing Σ^*. Now observe that any system of witnesses for Σ^* also is a system of witnesses of $\Sigma^\dagger$.

Hence $\Sigma^\dagger$ is a complete theory of $\mathscr{L}^*$-sentences containing Σ, and $\Sigma^\dagger$ possesses a system of witnesses. Thus we may apply 2.8.11 to obtain a model of $\Sigma^\dagger$, namely $\mathrm{TmAlg}(\Sigma^\dagger) \models \Sigma^\dagger$. Finally if we forget the interpretations of the new constants from $\mathscr{L}^*$ in $\mathrm{TmAlg}(\Sigma^\dagger)$ we obtain an $\mathscr{L}$-structure $\mathscr{M}$ which is a model of Σ (see 2.8.15).

C. Extensions by Constants

2.8.13. **Definition.** Let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ and $\mathscr{L}^+ = (\lambda^+ : \mathscr{R}^+ \longrightarrow \mathbb{N}, \mu^+ : \mathscr{F}^+ \longrightarrow \mathbb{N}, \mathscr{C}^+)$ be languages. $\mathscr{L}^+$ is called an **extension of** $\mathscr{L}$ and $\mathscr{L}$ is called a **sublanguage** of $\mathscr{L}^+$ if the following conditions hold:

- $\mathscr{R} \subseteq \mathscr{R}^+$ and $\lambda^+ \restriction \mathscr{R} = \lambda$.
- $\mathscr{F} \subseteq \mathscr{F}^+$ and $\mu^+ \restriction \mathscr{F} = \mu$.
- $\mathscr{C} \subseteq \mathscr{C}^+$.

If $\mathscr{L}^+$ is an extension of $\mathscr{L}$ with $\mathscr{R}^+ = \mathscr{R}$ and $\mathscr{F}^+ = \mathscr{F}$ (hence also $\lambda^+ = \lambda$ and $\mu^+ = \mu$), then $\mathscr{L}^+$ is called an **extension by constants** of $\mathscr{L}$. In this case we also write $\mathscr{L}^+ = \mathscr{L}(\mathscr{D})$, where $\mathscr{D} = \mathscr{C}^+ \setminus \mathscr{C}$. .

2.8.14. *Remark and Definition.* Let $\mathscr{L}^+ = (\lambda^+ : \mathscr{R}^+ \longrightarrow \mathbb{N}, \mu^+ : \mathscr{F}^+ \longrightarrow \mathbb{N}, \mathscr{C}^+)$ be an extension of the language $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$.

(i) The set of $\mathscr{L}$-terms is the set of all $\mathscr{L}^+$-terms that are $\mathscr{L}$-strings. The set of $\mathscr{L}$-formulas is the set of all $\mathscr{L}^+$-formulas that are $\mathscr{L}$-strings. Both assertion follow from a straightforward induction on the complexity of terms and formulas, respectively and are left to the reader.

(ii) If $\mathscr{M}^+$ is an $\mathscr{L}^+$-structure then there is obviously a unique $\mathscr{L}$ structure $\mathscr{M}$ with $|\mathscr{M}| = |\mathscr{M}^+|$, $R^{\mathscr{M}} = R^{\mathscr{M}^+}$ $(R \in \mathscr{R})$, $F^{\mathscr{M}} = F^{\mathscr{M}^+}$ $(F \in \mathscr{F})$ and $c^{\mathscr{M}} = c^{\mathscr{M}^+}$ $(c \in \mathscr{C})$. $\mathscr{M}$ is called the **restriction of** $\mathscr{M}^+$ **to** $\mathscr{L}$ and $\mathscr{M}^+$ is called an **expansion** of $\mathscr{M}$ to $\mathscr{L}^+$. The structure $\mathscr{M}$ is also called a **reduct of** $\mathscr{M}^+$. We write $\mathscr{M} = \mathscr{M}^+ \restriction \mathscr{L}$.

(iii) If $\mathscr{M}$ is an $\mathscr{L}$ structure then $\mathscr{M}$ can be expanded to $\mathscr{L}^+$ (in several ways if $\mathscr{L}^+ \neq \mathscr{L}$). Simply choose an arbitrary interpretation of the symbols from $\mathscr{L}^+$ that are not symbols of $\mathscr{L}$.

2.8.15. **Proposition.** *Let $\mathscr{L}^+$ be an extension of the language $\mathscr{L}$. If $\mathscr{M}$ is the restriction of the $\mathscr{L}^+$-structure $\mathscr{M}^+$ to $\mathscr{L}$, $t \in \mathrm{tm}(\mathscr{L})$, $\varphi \in \mathrm{Fml}(\mathscr{L})$ and $h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|$ (hence h is an assignment of $\mathscr{M}$ and of $\mathscr{M}^+$), then*

(i) $t^{\mathscr{M}}[h] = t^{\mathscr{M}^+}[h]$ *and*

(ii) $\mathscr{M} \models \varphi[h] \iff \mathscr{M}^+ \models \varphi[h]$.

Proof. (i) We show by induction on the complexity of t that $t^{\mathscr{M}}[h] = t^{\mathscr{M}^+}[h]$: If t is a variable, then $t^{\mathscr{M}}[h] = h(t) = t^{\mathscr{M}^+}[h]$ by definition 2.4.3(ii)(a). If t is a constant symbol $c \in \mathscr{C}$, then

$$t^{\mathscr{M}}[h] = c^{\mathscr{M}} = c^{\mathscr{M}^+} = t^{\mathscr{M}^+}[h],$$

by definition 2.4.3(ii)(a) and as $\mathscr{M}$ is the restriction of $\mathscr{M}^+$ to $\mathscr{L}$ (see 2.8.14(ii)).

If $F \in \mathscr{F}$ is an n-ary function symbol and $t_1, \ldots, t_n$ are $\mathscr{L}$-terms for which we already know our assertion, and t is $F(t_1, \ldots, t_n)$, then

$$\begin{aligned} t^{\mathscr{M}}[h] &= F^{\mathscr{M}}(t_1^{\mathscr{M}}[h], \ldots, t_n^{\mathscr{M}}[h]), \text{ by definition 2.4.3(ii)(b)} \\ &= F^{\mathscr{M}^+}(t_1^{\mathscr{M}}[h], \ldots, t_n^{\mathscr{M}}[h]), \text{ since } \mathscr{M} \text{ is the restriction of } \mathscr{M}^+ \text{ to } \mathscr{L} \\ &= F^{\mathscr{M}^+}(t_1^{\mathscr{M}^+}[h], \ldots, t_n^{\mathscr{M}^+}[h]), \text{ by induction} \\ &= t^{\mathscr{M}^+}[h], \text{ by definition 2.4.3(ii)(b).} \end{aligned}$$

(ii) We show $\mathscr{M} \models \varphi[h] \iff \mathscr{M}^+ \models \varphi[h]$ by induction on the complexity of the $\mathscr{L}$-formula φ. If φ is atomic of the form $s \doteq t$ for $\mathscr{L}$-terms s, t, then

$$\begin{aligned} \mathscr{M} \models \varphi[h] &\iff s^{\mathscr{M}}[h] = t^{\mathscr{M}}[h], \text{ by definition 2.4.5(A)(i)} \\ &\iff s^{\mathscr{M}^+}[h] = t^{\mathscr{M}^+}[h], \text{ by (i)} \\ &\iff \mathscr{M}^+ \models \varphi[h], \text{ by definition 2.4.5(A)(i)} \end{aligned}$$

If φ is atomic of the form $R(t_1, \ldots, t_n)$ for some n-ary relation symbol $R \in \mathscr{R}$ and some $t_1, \ldots, t_n \in \mathrm{tm}(\mathscr{L})$, then

$$\begin{aligned} \mathscr{M} \models \varphi[h] &\iff (t_1^{\mathscr{M}}[h], \ldots, t_n^{\mathscr{M}}[h]) \in R^{\mathscr{M}}, \text{ by definition 2.4.5(A)(i)} \\ &\iff (t_1^{\mathscr{M}}[h], \ldots, t_n^{\mathscr{M}}[h]) \in R^{\mathscr{M}^+}, \text{ since } \mathscr{M} = \mathscr{M}^+ \restriction \mathscr{L} \\ &\iff (t_1^{\mathscr{M}^+}[h], \ldots, t_n^{\mathscr{M}^+}[h]) \in R^{\mathscr{M}^+}, \text{ by (i)} \\ &\iff \mathscr{M}^+ \models \varphi[h], \text{ by definition 2.4.5(A)(i)} \end{aligned}$$

This shows (ii) when φ is atomic. For the induction step we have to process three cases, as usual.

Case 1. φ is $\neg\psi$. Then

$$\begin{aligned} \mathscr{M} \models \varphi[h] &\iff \mathscr{M} \not\models \psi[h], \text{ by definition 2.4.5(A)(ii)} \\ &\iff \mathscr{M}^+ \not\models \psi[h], \text{ by induction} \\ &\iff \mathscr{M}^+ \models \varphi[h], \text{ by definition 2.4.5(A)(ii)} \end{aligned}$$

Case 2. φ is $\psi \to \delta$. Then

$$\begin{aligned} \mathscr{M} \models \varphi[h] &\iff \text{if } \mathscr{M} \models \psi[h], \text{ then } \mathscr{M} \models \delta[h], \text{ by definition 2.4.5(A)(ii)} \\ &\iff \text{if } \mathscr{M}^+ \models \psi[h], \text{ then } \mathscr{M}^+ \models \delta[h], \text{ by induction} \\ &\iff \mathscr{M}^+ \models \varphi[h], \text{ by definition 2.4.5(A)(ii)} \end{aligned}$$

Case 3. φ is $\forall x\, \psi$. Then

$$\begin{aligned} \mathscr{M} \models \varphi[h] &\iff \mathscr{M} \models \psi[h(\tbinom{x}{a})] \text{ for all } a \in |\mathscr{M}|, \text{ by definition 2.4.5(A)(ii)} \\ &\iff \mathscr{M}^+ \models \psi[h(\tbinom{x}{a})] \text{ for all } a \in |\mathscr{M}|, \text{ by induction} \\ &\iff \mathscr{M}^+ \models \psi[h(\tbinom{x}{a})] \text{ for all } a \in |\mathscr{M}^+|, \text{ since } |\mathscr{M}^+| = |\mathscr{M}| \\ &\iff \mathscr{M}^+ \models \varphi[h], \text{ by definition 2.4.5(A)(ii)} \end{aligned}$$

□

2.8.16. **Corollary.** *Let $\mathscr{L}^+$ be an extension of $\mathscr{L}$ and let $\mathscr{M}$ be the restriction of the $\mathscr{L}^+$-structure $\mathscr{M}^+$ to $\mathscr{L}$. Let $t(x_1, ..., x_n) \in \mathrm{tm}(\mathscr{L})$, $\varphi(x_1, ..., x_n) \in \mathrm{Fml}(\mathscr{L})$ and let $d_1, ..., d_n$ be pairwise distinct constants of $\mathscr{L}^+$. If $h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|$ with $h(x_i) = d_i^{\mathscr{M}^+}$, then*

(i) $t^{\mathscr{M}}[h] = t(x_1/d_1, ..., x_n/d_n)^{\mathscr{M}^+}$.

(ii) $\mathscr{M} \models \varphi[h] \iff \mathscr{M}^+ \models \varphi(x_1/d_1, ..., x_n/d_n)$.

Proof. This follows from 2.8.15 and 2.4.11:

(i) We have

$$\begin{aligned} t^{\mathscr{M}}[h] &= t^{\mathscr{M}^+}[h], \text{ by 2.8.15(i)} \\ &= t(x_1/d_1, ..., x_n/d_n)^{\mathscr{M}^+}, \text{ by 2.4.11(i) applied } n \text{ times.} \end{aligned}$$

(ii) We have

$$\begin{aligned} \mathscr{M} \models \varphi[h] &\iff \mathscr{M}^+ \models \varphi[h], \text{ by 2.8.15(ii)} \\ &\iff \mathscr{M}^+ \models \varphi(x_1/d_1, ..., x_n/d_n), \text{ by 2.4.11(ii) applied } n \text{ times.} \end{aligned}$$ □

2.8.17. **Lemma.** *Let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ be a language and let $c \in \mathscr{C}$. Let $\mathscr{L}_0$ be the language $(\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C} \setminus \{c\})$, in other words $\mathscr{L}_0$ has the same alphabet as $\mathscr{L}$, except the constant symbol c is missing. In other words, $\mathscr{L}$ is the extension $\mathscr{L}_0(c)$ by constants of $\mathscr{L}_0$. Notice that by the very definition of terms and formulas we have $\mathrm{tm}(\mathscr{L}_0) \subseteq \mathrm{tm}(\mathscr{L})$ and $\mathrm{Fml}(\mathscr{L}_0) \subseteq \mathrm{Fml}(\mathscr{L})$.*

For each variable x and every $\mathscr{L}$-string s let s^c_x be the result of replacing the symbol c by the variable x. Then

(i) (a) If t is an $\mathscr{L}$-term, then t^c_x is an $\mathscr{L}_0$-term and $\mathrm{Fr}(t^c_x) \subseteq \mathrm{Fr}(t) \cup \{x\}$.
(b) If φ is an $\mathscr{L}$-formula, then φ^c_x is an $\mathscr{L}_0$-formula and $\mathrm{Fr}(\varphi^c_x) \subseteq \mathrm{Fr}(\varphi) \cup \{x\}$.

(ii) (a) If $\varphi \in \mathrm{Fml}(\mathscr{L}_0)$ then $\varphi(x/c)^c_x = \varphi$.
(b) If x does not occur in $\varphi \in \mathrm{Fml}(\mathscr{L})$ then $\varphi^c_x(x/c) = \varphi$.

(iii) If φ is a logical axiom of $\mathscr{L}$ and c does not occur in the scope of the quantifier $\forall x$ in φ then $\vdash_{\mathscr{L}_0} \varphi^c_x$.

(iv) If $\Sigma \subseteq \mathrm{Fml}(\mathscr{L}_0)$, c does not occur in the scope of the quantifier $\forall x$ in $\varphi \in \mathrm{Fml}(\mathscr{L})$ and if $\Sigma \vdash_{\mathscr{L}} \varphi$ then $\Sigma \vdash_{\mathscr{L}_0} \varphi^c_x$

Proof. (i) is a straightforward induction on the complexity of terms (to obtain (a)) and on the complexity of formulas (to obtain (b)).

(ii) is simply a statement about replacing letters in strings.

(a) It is obvious that the replacement operations $x \mapsto c$ and $c \mapsto x$ are inverse to each other, provided c does not occur in φ.

(b) It is obvious that the replacement operations $c \mapsto x$ and $x \mapsto c$ are inverse to each other, provided x does not occur in φ.

(iii). For the axiom schemes (**AxProp**) and (**Ax**$\forall\to$) this is immediate from (i) even if c occurs in the scope of the quantifier $\forall x$ in φ.

Suppose φ is an instance of (**AxSubst**). Hence there are $y \in \mathrm{Vbl}$, $t \in \mathrm{tm}(\mathscr{L})$ and $\psi \in \mathrm{Fml}(\mathscr{L})$ such that φ is $\forall y\psi \to \psi(y/t)$.

Case 1. $y = x$.

Then c does not occur in ψ since by assumption c does not occur in the scope of the quantifier $\forall x$ in φ. Clearly then $\psi(y/t)^c_x = \psi(y/t^c_x)$ (observe that $y = x$ is free in ψ for t^c_x, since this is true for all variables occurring in t by assumption and for

$x = y$ anyway). Hence φ^c_x is $\forall y\psi \to \psi(y/t^c_x)$ which is a logical axiom of $\mathscr{L}_0$ (and of $\mathscr{L}$) by (i).

Case 2. $y \neq x$.

Firstly, y is free in ψ^c_x for t^c_x, since either c does not occur in t and there is nothing to do, or c does occur in t and no free occurrence of y in ψ is in the scope of $\forall x$ in ψ (otherwise c would occur in the scope of $\forall x$ in $\psi(y/t)$). Clearly $\psi(y/t)^c_x = \psi^c_x(y/t^c_x)$ and so φ^c_x is $\forall y\psi^c_x \to \psi^c_x(y/t^c_x)$ which is a logical axiom of $\mathscr{L}_0$ (and of $\mathscr{L}$) by (i).

Suppose φ is an instance of (**AxGen**). Hence there are $\psi \in \mathrm{Fml}(\mathscr{L})$ and $y \in \mathrm{Vbl}$ which does not occur free in ψ such that φ is $\psi \to \forall y\psi$.

Case 1. $y = x$.

Then c does not occur in ψ since by assumption c does not occur in the scope of the quantifier $\forall x$ in φ. But then c does not occur in φ either and therefore $\varphi^c_x = \varphi$ is a logical axiom of $\mathscr{L}_0$ (and of $\mathscr{L}$) by (i).

Case 2. $y \neq x$.

Then y is not a free variable of ψ^c_x by (i)(b). Hence $\psi^c_x \to \forall y\ \psi^c_x$ is a logical axiom, too. Since $\psi^c_x \to \forall y\ \psi^c_x$ is φ^c_x this shows the claim.

Suppose φ is an instance of (**AxEq**). If φ is an instance of (a),(b) or (d) of (**AxEq**), then c does not occur in φ and there is nothing to do.

So we may assume that φ is an instance of (**AxEq**)(c). This means, φ is $y \doteq z \to t(w/z) \doteq t(w/y)$ for some $t \in \mathrm{tm}(\mathscr{L})$ and some $w, y, z \in \mathrm{Vbl}$.

Case 1. $x \neq w$.

Then $t(w/y)^c_x = t^c_x(w/y)$ and $t(w/z)^c_x = t^c_x(w/z)$. Using (i), φ^c_x is $y \doteq z \to t^c_x(w/z) \doteq t^c_x(w/y)$, which is a logical axiom of $\mathscr{L}_0$ (and of $\mathscr{L}$) by (i).

Case 2. $x = w$.

Let u be a variable, different from x, y, z which does not occur in t and let $s = t^c_u$. By (ii), s is an $\mathscr{L}_0$-term and as $u \notin \mathrm{Fr}(t)$, $t = s(u/c)$. Hence $t(w/z) = t(x/z) = s(u/c)(x/z) \overset{\text{as } u \neq z,x}{=} s(x/z)(u/c)$ and

$$(*) \qquad t(w/z)^c_x = s(x/z)(u/c)^c_x \overset{\text{as } c \text{ does not occur in } s(x/z)}{=} s(x/z)(u/x).$$

(observe that $s(x/z)(u/x)$ is not $s(u/x)(x/z)$ in general). The same reasoning with z replaced by y shows

$$(+) \qquad t(w/y)^c_x = s(x/y)(u/x).$$

By (**AxEq**)(c) and (**Ax**$\forall$) we have $\vdash \forall u\ y \doteq z \to s(x/z) \doteq s(x/y)$. Hence by (**AxSubst**) we obtain $\vdash y \doteq z \to s(x/z)(u/x) \doteq s(x/y)(u/x)$. Since φ^c_x is $y \doteq z \to t(w/z)^c_x \doteq t(w/y)^c_x$, $(*)$ and $(+)$ show that $\vdash_{\mathscr{L}_0} \varphi^c_x$.

Finally suppose φ is an instance of (**Ax**$\forall$), i.e. φ is of the form $\forall x_1...x_k\ \psi$ for some instance ψ of the other logical axioms of $\mathscr{L}$. We have shown that $\vdash_{\mathscr{L}_0} \psi^c_x$ (since c also is not in the scope of $\forall x$ in ψ). By the Generalisation Theorem 2.5.21 we get $\vdash_{\mathscr{L}_0} \forall x_1...x_n\ \psi^c_x$ as desired.

(iv) We start with a

Claim. If φ is a logical axiom of $\mathscr{L}$ or $\varphi \in \Sigma$, then $\Sigma \vdash_{\mathscr{L}_0} \varphi^c_x$.

Proof. If φ is a logical axiom of $\mathscr{L}$, then by (iii) $\vdash_{\mathscr{L}_0} \varphi^c_x$. If $\varphi \in \Sigma$, then as $\Sigma \subseteq \mathrm{Fml}(\mathscr{L}_0)$, $\varphi = \varphi^c_x$ and $\Sigma \vdash_{\mathscr{L}_0} \varphi^c_x$. $\diamond$

Now we prove (iv) by induction on the length k of a proof $(\psi_1, ..., \psi_k)$ of φ from Σ (recall that $\psi_k = \varphi$ By definition).

If $k = 1$, then we may apply the claim. For the induction step $k \Rightarrow k+1$ we also may apply the claim, provided ψ_{k+1} is a logical axiom of $\mathscr{L}$ or $\psi_{k+1} \in \Sigma$. It remains to show the assertion if ψ_{k+1} is obtained from $\psi_1, ..., \psi_k$ by Modus Ponens. Pick $i, j \leq n$ such that ψ_j is $\psi_i \to \psi_{k+1}$. Since $\Sigma \vdash_{\mathscr{L}} \psi_i$ and $\Sigma \vdash_{\mathscr{L}} \psi_j$ there is a finite subset Σ_0 of Σ with $\Sigma_0 \vdash_{\mathscr{L}} \psi_i$ and $\Sigma_0 \vdash_{\mathscr{L}} \psi_j$.

Let y be a variable, not occurring in $\Sigma_0, \psi_1, ..., \psi_{k+1}$. By the induction hypothesis we get $\Sigma_0 \vdash_{\mathscr{L}_0} (\psi_i)^c_y$ and $\Sigma \vdash_{\mathscr{L}_0} (\psi_j)^c_y$. Since $(\psi_j)^c_y$ is $(\psi_i)^c_y \to (\psi_{k+1})^c_y$ we may apply Modus Ponens to obtain $\Sigma_0 \vdash_{\mathscr{L}_0} (\psi_{k+1})^c_y$. Since y does not occur in Σ_0 we get $\Sigma_0 \vdash_{\mathscr{L}_0} \forall y (\psi_{k+1})^c_y$ from the Generalisation Theorem 2.5.21. Since c is not in the scope of $\forall x$ in $\varphi = \psi_{k+1}$, x is not in the scope of $\forall x$ in $\varphi = (\psi_{k+1})^c_x$. So the substitution axiom (**AxSubst**) gives $\Sigma_0 \vdash_{\mathscr{L}_0} (\psi_{k+1})^c_y(y/x)$. Since y does not occur in ψ_{k+1}, $(\psi_{k+1})^c_y(y/x)$ is $(\psi_{k+1})^c_x$ as desired. $\square$

2.8.18. **Proposition.** *Let $\mathscr{L}^+ = \mathscr{L}(\mathscr{D})$ be an extension by constants of $\mathscr{L}$, let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$, $\varphi(x_1, ..., x_n) \in \mathrm{Fml}(\mathscr{L})$ and suppose no x_i occurs freely in any formula from Σ. Let $d_1, ..., d_n \in \mathscr{D}$ with $d_i \neq d_j$ for all $i \neq j$. Then*

$$\Sigma \vdash_{\mathscr{L}} \varphi \iff \Sigma \vdash_{\mathscr{L}^+} \varphi(x_1/d_1, ..., x_n/d_n).$$

Proof. Since proofs are finite, we may assume that $\mathscr{L}^+ = \mathscr{L}(d_1, ..., d_n)$. The implication "$\Rightarrow$" follows from the generalisation theorem 2.5.21 and (**AxSubst**).

The implication "$\Leftarrow$" in the case $n = 1$ follows from 2.8.17. A trivial induction for $n > 1$ then shows the claim: Observe that $\mathscr{L}(d_1, ..., d_n) = \mathscr{L}(d_1)(d_2)...(d_n)$ and $\varphi(x_1/d_1, ..., x_n/d_n) = \varphi(x_1/d_1)...(x_n/d_n)$. $\square$

With the aid of 2.8.18 we can now translate deduction of formulas from formulas entirely into deduction of sentences from sentences:

2.8.19. **Theorem.** *Let $\mathscr{L}$ be language and let $\mathscr{D} = \{d_0, d_1, ...\}$ be a countable set of new constants. For $\varphi(v_0, ..., v_n) \in \mathrm{Fml}(\mathscr{L})$ let $\varphi_{\mathscr{D}}$ be the $\mathscr{L}(\mathscr{D})$-sentence*

$$\varphi_{\mathscr{D}} \ = \ \varphi(v_0/d_0, ..., v_n/d_n).$$

Let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ and $\varphi \in \mathrm{Fml}(\mathscr{L})$. Then

$$\Sigma \vdash_{\mathscr{L}} \varphi \iff \Sigma_{\mathscr{D}} \vdash_{\mathscr{L}(\mathscr{D})} \varphi_{\mathscr{D}},$$

where $\Sigma_{\mathscr{D}} = \{\sigma_{\mathscr{D}} \mid \sigma \in \Sigma\}$.

Proof. Since proofs are finite we may assume that $\Sigma = \{\sigma_1, ..., \sigma_k\}$. Then

$$\begin{aligned} \Sigma \vdash_{\mathscr{L}} \varphi & \overset{\text{Deduction Theorem}}{\iff} \vdash_{\mathscr{L}} (\sigma_1 \wedge ... \wedge \sigma_k) \to \varphi \\ & \overset{2.8.18}{\iff} \vdash_{\mathscr{L}(\mathscr{D})} ((\sigma_1)_{\mathscr{D}} \wedge ... \wedge (\sigma_k)_{\mathscr{D}}) \to \varphi_{\mathscr{D}} \\ & \overset{\text{Deduction Theorem}}{\iff} \Sigma_{\mathscr{D}} \vdash_{\mathscr{L}(\mathscr{D})} \varphi_{\mathscr{D}} \quad \square \end{aligned}$$

2.8.20. **Corollary.** *In the notation of 2.8.19, a set Σ of $\mathscr{L}$-formulas is consistent (in $\mathscr{L}$) if and only if $\Sigma_{\mathscr{D}}$ is a consistent set of $\mathscr{L}(\mathscr{D})$-sentences.*

Proof. Obvious from 2.8.19. □

2.8.21. **Lemma.**

(i) If y does not occur free in $\varphi \in \mathrm{Fml}(\mathscr{L})$ then $\vdash \forall x\varphi \to \forall y(\varphi(x/y))$.

(ii) If $\varphi, \psi \in \mathrm{Fml}(\mathscr{L})$ then

$$\vdash (\varphi \to \exists x\psi) \to \exists x(\varphi \to \psi).$$

Proof. (i) This has already been done as an example in 2.5.22.

(ii). By contraposition using a suitable tautology it suffices to show

$$\vdash \neg\neg\forall x\ \neg(\varphi \to \psi) \to \neg(\varphi \to \neg\forall x\ \neg\psi).$$

Now, using the propositional tautology

$$\Big(\neg\neg p_0 \ \to\ \neg(p_1 \to \neg p_2)\Big) \ \leftrightarrow\ \Big(p_0 \to (p_1 \wedge p_2)\Big)$$

it suffices to show

$$\vdash \forall x\ \neg(\varphi \to \psi) \to (\varphi \wedge \forall x\ \neg\psi).$$

By the deduction theorem 2.5.19 it suffices to show

$$(*) \qquad \forall x\ \neg(\varphi \to \psi) \vdash \varphi \wedge \forall x\ \neg\psi$$

By 2.5.12(ii) it remains to show

(a) $\forall x\ \neg(\varphi \to \psi) \vdash \varphi$ and

(b) $\forall x\ \neg(\varphi \to \psi) \vdash \forall x\ \neg\psi$.

Now by (**AxSubst**) applied to the term x we know $\forall x\ \neg(\varphi \to \psi) \vdash \neg(\varphi \to \psi)$. Furthermore we have the tautologies $\neg(\varphi \to \psi) \to \varphi$ and $\neg(\varphi \to \psi) \to \neg\psi$. Consequently, by Modus Ponens we get $\forall x\ \neg(\varphi \to \psi) \vdash \varphi$ (which shows (a)) and $\forall x\ \neg(\varphi \to \psi) \vdash \neg\psi$. Since x is not a free variable of $\forall x\ \neg(\varphi \to \psi)$ we can apply the generalisation theorem to obtain (b). □

2.8.22. **Proposition.** *Let $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ be a language and let $\zeta : \mathrm{Fml}(\mathscr{L})(1) \longrightarrow \mathscr{D}$ be a bijection onto a set $\mathscr{D}$ which is disjoint from the alphabet of $\mathscr{L}$. Let $\mathscr{L}'$ be the language $\mathscr{L}' = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C} \cup \mathscr{D})$.*

If $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ is consistent, then also

$$\Sigma' := \Sigma \cup \{(\exists x\varphi) \to \varphi(x/\zeta(\varphi)) \mid \varphi(x) \in \mathrm{Fml}(\mathscr{L}), x \in \mathrm{Vbl}\} \subseteq \mathrm{Sen}(\mathscr{L}')$$

is consistent.

Proof. Firstly, notice that by 2.8.18, it is not important to explicitly mention whether Σ is consistent in $\mathscr{L}$ or in $\mathscr{L}'$. We will make use of 2.8.18 in the proof below, without mentioning the language: If we say "is a proof" or "is inconsistent", then this always means w.r.t. $\mathscr{L}'$.

We have to show that no contradiction is provable from Σ' in $\mathscr{L}'$. Since every proof from Σ' is also a proof of a finite subset of Σ' we may assume that Σ is finite and it suffices to show by induction on $k \in \mathbb{N}_0$ the following:

If $\varphi_1(x_1), ..., \varphi_k(x_k) \in \mathrm{Fml}(\mathscr{L}), x_1, ..., x_k \in \mathrm{Vbl}$ (here we are not assuming that $x_i \neq x_j$ for $i \neq j$), then

$$\Sigma \cup \{(\exists x_i \varphi_i) \to \varphi_i(x_i/\zeta(\varphi_i)) \mid i \in \{1, ..., k\}\}$$

is consistent in $\mathscr{L}'$.

If $k = 0$ then this holds by assumption. For the induction step $k-1 \Rightarrow k$ we take $\varphi_1(x_1), ..., \varphi_k(x_k) \in \mathrm{Fml}(\mathscr{L})$ with $\varphi_i \neq \varphi_j$ for $i \neq j$. Let $d_i := \zeta(\varphi_i)$ $(1 \leq i \leq k)$. Since $\varphi_i \neq \varphi_j$ for $i \neq j$ we have $d_i \neq d_j$ for $i \neq j$, too. For $i \in \{1, ..., k\}$ let σ_i be the $\mathscr{L}'$-sentence

$$\sigma_i \ := \ (\exists x_i \varphi_i) \to \varphi_i(x_i/d_i).$$

We assume that $\Sigma \cup \{\sigma_1, ..., \sigma_k\}$ is inconsistent and we show that also $\Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\}$ is inconsistent.

We have $\Sigma \cup \{\sigma_1, ..., \sigma_k\} \vdash \gamma \wedge \neg\gamma$ for some $\gamma \in \mathrm{Fml}(\mathscr{L})$. By the deduction theorem 2.5.19 we have $\Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\} \vdash \sigma_k \to \gamma \wedge \neg\gamma$. As $\sigma_k \to \gamma \wedge \neg\gamma$ is provably equivalent to $\neg\sigma_k$ we obtain

$$(\dagger) \qquad \Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\} \vdash \neg\sigma_k.$$

Since Σ is finite there is a variable which does not occur in $\Sigma \cup \{\sigma_1, ..., \sigma_k\}$. We pick such a variable y and define

$$\psi := (\exists x_k \varphi_k(x_k)) \to \varphi_k(x_k/y).$$

Notice: since y does not occur in σ_k we have $(\sigma_k)^{d_k}_y = \psi$, hence $(\neg\sigma_k)^{d_k}_y = (\neg\psi)$ as well.

Since $\Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\} \subseteq \mathrm{Sen}(\mathscr{L}(d_1, ..., d_{k-1}))$ and y does not occur in σ_k, we may apply 2.8.17(iv) to obtain

$$(\ddagger) \qquad \Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\} \vdash (\neg\sigma_k)^{d_k}_y.$$

Since y does not occur in $\Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\}$, we may apply the generalisation theorem 2.5.21 to $(\ddagger)$ and obtain (using $(\neg\sigma_k)^{d_k}_y = (\neg\psi)$)

$$(*) \qquad \Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\} \vdash \forall y \neg\psi.$$

Thus, in order to reach our goal (i.e. to show that $\Sigma \cup \{\sigma_1, ..., \sigma_{k-1}\}$ is inconsistent) it suffices to prove $\vdash \exists y \psi$:

Since x_k does not occur free in $\neg\varphi_k(x_k/y)$ we may apply 2.8.21(i) and get $\vdash \forall y(\neg\varphi_k(x_k/y)) \to \forall x_k \neg\varphi_k$ (observe that $\varphi_k(x_k/y)(y/x_k)$ is φ_k). Applying contraposition we obtain

$$\vdash \exists x_k \varphi_k \to \exists y(\varphi_k(x_k/y)).$$

Applying 2.8.21(ii) to $\exists x_k \varphi_k$ and $\varphi_k(x_k/y)$ gives

$$\vdash \exists y(\exists x_k \varphi_k \to \varphi_k(x_k/y)).$$

But $\exists x_k \varphi_k \to \varphi_k(x_k/y)$ is ψ as desired. $\square$

2.8.23. **Theorem.** *Let* $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ *be a language. Then there is an extension by constants* $\mathscr{L}^*$ *of* $\mathscr{L}$ *by* $\operatorname{card}(\operatorname{Fml}(\mathscr{L}))$ *many constants and a subset* H^* *of* $\mathscr{L}^*$*-sentences such that*

(i) H^* *possess a system of witnesses (in* $\mathscr{L}^*$*), and*
(ii) For every consistent $\Sigma \subseteq \operatorname{Sen}(\mathscr{L})$ *the set* $\Sigma \cup H^*$ *is consistent (note that any system of witnesses for* H^* *is also a system of witnesses for* $\Sigma \cup H^*$*).*

Proof. By induction we define constant extensions $\mathscr{L}^n$ and a set $H^n \subseteq \operatorname{Sen}(\mathscr{L})^n$ as follows: $\mathscr{L}^0 := \mathscr{L}$ and $H^0 = \emptyset$. For the induction step we apply 2.8.22 to $\mathscr{L}^n$ and H^n to obtain

$$\mathscr{L}^{n+1} = (\mathscr{L}^n)' \text{ and } H^{n+1} = (H^n)'$$

in the notation of 2.8.22. Note that we have added $\operatorname{card}(\operatorname{Fml}(\mathscr{L}^n))$ many constants, hence by induction we have added $\operatorname{card}(\operatorname{Fml}(\mathscr{L}))$ many constants. By 2.8.22 we see inductively, that for every consistent $\Sigma \subseteq \operatorname{Sen}(L)$ the set $\Sigma \cup H^{n+1}$ is a consistent set of $\mathscr{L}^{n+1}$-sentences containing H^n.

Let $\mathscr{L}^*$ be the extension by constants of $\mathscr{L}$ obtained by adding all constants symbols from all languages $\mathscr{L}^n$ to $\mathscr{L}$. We see that $\operatorname{card}(\operatorname{Fml}(\mathscr{L}^*))$ still is equal to $\operatorname{card}(\operatorname{Fml}(\mathscr{L}))$.

Furthermore, $H^* := \bigcup_{n\in\mathbb{N}} H^n \subseteq \operatorname{Sen}(\mathscr{L}^*)$ has the property that for every consistent $\Sigma \subseteq \operatorname{Sen}(L)$ the set $\Sigma \cup H^*$ is a consistent set. By construction, H^* possess a system of witnesses (in $\mathscr{L}^*$). □

For the proof of the completeness theorem we only need the following corollary:

2.8.24. **Corollary.** *Let* $\mathscr{L} = (\lambda : \mathscr{R} \longrightarrow \mathbb{N}, \mu : \mathscr{F} \longrightarrow \mathbb{N}, \mathscr{C})$ *be a language and let* $\Sigma \subseteq \operatorname{Sen}(\mathscr{L})$ *be consistent. Then there is an extension by constants* $\mathscr{L}^*$ *of* $\mathscr{L}$ *and a consistent subset* Σ^* *of* $\mathscr{L}^*$*-sentences containing* Σ *such that* Σ^* *possess a system of witnesses (in* $\mathscr{L}^*$*).*

Proof. Take $\mathscr{L}^*$ and H^* as in 2.8.23 and define $\Sigma^* = \Sigma \cup H^*$. Now 2.8.23 gives the assertion. □

D. Finishing the Proof

The crucial assertion of the Completeness Theorem 2.7.1 is the following special case of its corollary 2.7.3:

2.8.25. **Theorem.** *Every consistent set of $\mathscr{L}$-sentences is satisfiable (i.e. has a model).*

Proof. This is done in 2.8.12. Now we have filled the missing gap in 2.8.24. $\square$

2.8.26. **Theorem.** *(Completeness Theorem)*
For all $\Sigma, \Phi \subseteq \mathrm{Fml}(\mathscr{L})$ we have

$$\Sigma \models \Phi \implies \Sigma \vdash \Phi.$$

(Recall that the implication $\Leftarrow$ also holds by the Soundness Theorem 2.5.16.)

Proof. Since proofs are finite, it is enough to show that

$$\Sigma \models \varphi \implies \Sigma \vdash \varphi$$

for every $\mathscr{L}$-formula φ. Firstly assume that $\Sigma \subseteq \mathrm{Sen}(\mathscr{L})$ and $\varphi \in \mathrm{Sen}(\mathscr{L})$. Suppose $\Sigma \nvdash \varphi$. By 2.6.3(i), $\Sigma \cup \{\neg\varphi\}$ is consistent. Hence by 2.8.25, $\Sigma \cup \{\neg\varphi\}$ has a model $\mathscr{M}$. So $\mathscr{M} \models \Sigma$ and $\mathscr{M} \nvDash \varphi$, which implies $\Sigma \nvDash \varphi$.

Now let $\Sigma \subseteq \mathrm{Fml}(\mathscr{L})$ and $\varphi \in \mathrm{Fml}(\mathscr{L})$ with $\Sigma \nvdash \varphi$. Let $\mathscr{D}$ be a countable (infinite) set of constant symbols, new w.r.t. $\mathscr{L}$. By 2.8.19 we know $\Sigma_{\mathscr{D}} \nvdash_{\mathscr{L}(\mathscr{D})} \varphi_{\mathscr{D}}$. By what we have shown above there is a model $\mathscr{N}$ of $\Sigma_{\mathscr{D}}$ with $\mathscr{N} \nvDash \varphi_{\mathscr{D}}$. Let $\mathscr{M}$ be the restriction of $\mathscr{N}$ to $\mathscr{L}$ and let $h : \mathrm{Vbl} \longrightarrow |\mathscr{M}|$ be defined by $h(v_i) = d_i^{\mathscr{N}}$. Then by 2.8.16, $\mathscr{M} \models \Sigma[h]$ and $\mathscr{M} \nvDash \varphi[h]$. Thus $\Sigma \nvDash \varphi$, too. $\square$

3. Models of Set Theory

Before we start with axiomatic set theory, it is beneficial to talk about so called definable sets in $\mathscr{L}$-structures.

3.1. **Definable sets.**

3.1.1. **Definition.** Let $\mathscr{M}$ be an $\mathscr{L}$-structure and let $n \in \mathbb{N}$. A subset S of $|\mathscr{M}|^n$ is called **definable in** $\mathscr{M}$ if there is some $\mathscr{L}$-formula $\varphi(x_1, ..., x_n, y_1, ..., y_k)$ and a k-tuple $\bar{a} \in |\mathscr{M}|^k$ such that

$$S = \{(m_1, ..., m_n) \in |\mathscr{M}|^n \ \mid \ \mathscr{M} \models \varphi(m_1, ..., m_n, a_1, ..., a_k)\}.$$

We then say that S is **defined by** $\varphi(\bar{x}, \bar{a})$ **(in** $\mathscr{M}$**)** and write $S = \varphi(\mathscr{M}^n, \bar{a})$. The elements $a_1, \ldots, a_k$ are called **parameters**. If there is such a formula with $k = 0$, then S is said to be **definable without parameters**.

3.1.2**. Discussion and Examples**

(i) One should think of a definable set S as the

"solution set of the formula $\varphi(x_1, ..., x_n, a_1, ..., a_k)$".

For example in the structure $\mathscr{M} = (\mathbb{R}, \leq, +, -, \cdot)$, the formula φ might be

$$x^8 + y_7 \cdot x^7 + ... + y_1 \cdot x + y_0 \geq y_8$$

and $\bar{a}$ might be $(\pi, 1, 2, 3, 4, 5, 6, \sqrt{2}, 0)$. So $\varphi(x_1, ..., x_n, a_1, ..., a_k)$ could be understood as the formula (in the ordinary sense of mathematics)

$$x^8 + \sqrt{2} \cdot x^7 + ... + 1 \cdot x + \pi \geq 0$$

and $S \subseteq \mathbb{R}$ is the solution set of this inequality. It is clear that we are interested in the analysis of such sets when we are studying the real numbers.

The elements $a_1, ..., a_k$ play the role of "coefficients" or "parameters" in this example and it is suitable to think of them in this way also in the general situation.

The formula φ in (i) is atomic, but many interesting definable sets are naturally given by formulas with quantifiers. Here are some examples.

(ii) Let S be the set of all $(a, b, c) \in \mathbb{R}^3$ such that the equation $ax^2 + bx + c = 0$ has a solution in $\mathbb{R}$. Then this set is defined in the structure $(\mathbb{R}, +, \cdot, 0)$ by the formula

$$\exists z \ x_1 \cdot z^2 + x_2 \cdot z + x_3 \doteq 0$$

of the language $\{+, \cdot, 0\}$. So here we do not need parameters.

(iii) Fix $n \in \mathbb{N}$. Let Z be the set of all $n \times n$-matrices over $\mathbb{R}$ that are invertible. If we identify an $n \times n$-matrix with an element of $\mathbb{R}^{n^2}$, then Z is a subset of $\mathbb{R}^{n^2}$.

In the structure $\mathscr{M} = (\mathbb{R}, +, -, \cdot, 0, 1)$, the set Z is defined by the following formula $\varphi(x_{11}, \ldots, x_{1n}, \ldots, x_{n1}, \ldots, x_{nn})$:

$$\exists u_{11} \ldots u_{1n} \ldots u_{n1} \ldots u_{nn} : \begin{pmatrix} x_{11} & \ldots & x_{1n} \\ \vdots & & \vdots \\ x_{n1} & \ldots & x_{nn} \end{pmatrix} \cdot \begin{pmatrix} u_{11} & \ldots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \ldots & u_{nn} \end{pmatrix} = I_n,$$

where I_n is the unit matrix. Again, the tuple $\bar{y}$ in 3.1.1 has length 0 (i.e., there are no variables for parameters).

(iv) Consider the polynomial

$$t(u, x_0, \ldots, x_n) = x_n \cdot u^n + x_{n-1} \cdot u^{n-1} \ldots + x_1 \cdot u + x_0$$

in the variable u with "general" coefficients $x_n, \ldots, x_0$. Look at the following formula $\varphi(x_0, \ldots, x_n, y)$ in the language $\{+, -, \cdot, \leq, 0, 1\}$:

$$\forall u_1, u_2 \Big(y \leq u_1 \leq u_2 \rightarrow t(u_1, x_0, \ldots, x_n) \leq t(u_2, x_0, \ldots, x_n) \Big).$$

Then the set defined by $\varphi(x_0, \ldots, x_n, \pi)$ in $\mathbb{R}^{n+1}$ is the set of all coefficient vectors of degree n polynomials that give increasing functions $[\pi, +\infty) \longrightarrow \mathbb{R}$. Here $k = 1$ and π is a parameter.

(v) Note that a definable set is defined by many formulas. For example the sets in (ii),(iii) and (iv) can also be defined by a quantifier free formulas in the structure $(\mathbb{R}, \leq, +, -, \cdot, 0, 1)$ of the language $\{\leq, +, -, \cdot, 0, 1\}$. For (ii) one may use the discriminant of the quadratic polynomial and for (iii) one may use the determinant of the given matrix, but for (iv) this is harder. A famous theorem by Tarski at the beginning of Model Theory says that indeed *every* set that is definable in $(\mathbb{R}, \leq, +, -, \cdot, 0, 1)$ without parameters is definable without parameters by a quantifier free formula in the language $\{\leq, +, -, \cdot, 0, 1\}$. For details we refer to [ModTh, section 4.3].

3.1.3. **Observation.** *In an arbitrary structure $\mathscr{M}$, the following sets are always definable:*

(i) The empty set and the set $|\mathscr{M}|^n$.
(ii) The diagonal $\{(a, a) \mid a \in |\mathscr{M}|\} \subseteq |\mathscr{M}|^2$.
(iii) For every $\bar{a} \in |\mathscr{M}|^n$, the set $\{\bar{a}\} \times |\mathscr{M}|^k \subseteq |\mathscr{M}|^n \times |\mathscr{M}|^k$.
(iv) Finite and cofinite subsets of $|\mathscr{M}|^n$ (recall that **cofinite** *means: the complement in $|\mathscr{M}|^n$ is finite)*

The proof is done left as question 69 of the example sheets.

A particularly interesting class of definable sets are graphs of functions. Well, not all functions:

3.1.4. **Definition.** Let $\mathscr{M}$ be an $\mathscr{L}$-structure with universe M and let $S \subseteq M^n$. A function $f : S \longrightarrow M^k$ is called **definable (in $\mathscr{M}$)** if its graph is a subset of $M^n \times M^k$ that is definable in $\mathscr{M}$.

3.1.5. *Example.* If F is an n-ary function symbol of $\mathscr{L}$, then $F^{\mathscr{M}}: M^n \longrightarrow M$ is definable in $\mathscr{M}$, because its graph is defined by the formula $F(x_1, \dots, x_n) \doteq x_{n+1}$. A bit more general, If $t(x_1, \dots, x_n)$ is an $\mathscr{L}$-term, then $t^{\mathscr{M}}: M^n \longrightarrow M$ is definable in $\mathscr{M}$, because its graph is defined by the formula $t(x_1, \dots, x_n) \doteq x_{n+1}$.

However, not every definable function is of this form. For example in the structure $\mathscr{M} = (\mathbb{R}, +, \cdot)$, the (graph of the) function $\frac{1}{\sqrt{1+x^2}}$ is defined without parameters by the formula

$$y^2 \cdot (1 + x^2) \doteq 1 \ \wedge \ \exists v \ y \doteq v^2.$$

(Note that in the language $\{+, \cdot\}$ we have no symbol to express $y \geq 0$, therefore we mimic this with the subformula $\exists v \ y = v^2$.)

Most of the basic set theoretic operations on definable sets and functions are again definable:

3.1.6. **Proposition.** *Let $\mathscr{M}$ be an $\mathscr{L}$-structure with universe $M = |\mathscr{M}|$.*

(i) If S, T are definable subsets of M^n, then also $S \cap T$, $S \cup T$ and $S \setminus T$ are definable.

(ii) For $k \leq n$, the projection $p: M^n \longrightarrow M^k$ onto some k coordinates is a definable function and for each definable set $S \subseteq M^n$, the set $p(S)$ is a definable subset of M^k.

Now let $S \subseteq M^n$ and let $f: S \longrightarrow M^k$ be a function.

(iii) If f is definable, then S and the image of f are definable.

(iv) The composition of definable maps (when well-defined) is definable, hence if f is definable, $T \subseteq M^k$ and $g: T \longrightarrow M^l$ is definable with $f(S) \subseteq T$, then also $g \circ f: S \longrightarrow M^l$ is definable.

(v) f is definable if and only if each component of f is a definable map $S \longrightarrow M$.

Proof. (i) If S is defined by $\varphi(\bar{x}, \bar{a})$ and T is defined by $\psi(\bar{x}, \bar{a})$, then $S \cap T$, $S \cup T$ and $S \setminus T$ are definable by $\varphi(\bar{x}, \bar{a}) \wedge \psi(\bar{x}, \bar{a})$, $\varphi(\bar{x}, \bar{a}) \vee \psi(\bar{x}, \bar{a})$ and $\varphi(\bar{x}, \bar{a}) \wedge \neg\psi(\bar{x}, \bar{a})$ respectively.

Notice, that we can actually assume here that S and T are defined by using the same parameters: Suppose φ has free variables in $x_1, \dots, x_n, y_1, \dots, y_k$ and ψ has free variables in $u_1, \dots, u_n, v_1, \dots, v_l$. Further suppose $S = \varphi(\mathscr{M}^n, \bar{b})$ and $T = \psi(\mathscr{M}^n, \bar{c})$. Then let $\bar{w} = (w_1, \dots, w_{k+l})$ be a tuple of $k+l$ distinct new variables and let $\bar{a}$ be the concatenation of $\bar{b}$ and $\bar{c}$. We see that S is defined by $\tilde{\varphi}(\bar{x}, \bar{a})$ where $\tilde{\varphi}$ denotes the formula $\varphi(\bar{x}, w_1, \dots, w_k)$ and T is defined by $\tilde{\psi}(\bar{x}, \bar{a})$ where $\tilde{\psi}$ denotes the formula $\psi(\bar{x}, w_{k+1}, \dots, w_{k+l})$.

(ii) That p is a definable map is left as an exercise. If S is defined by $\varphi(x_1, ..., x_n, a_1, \dots, a_l)$ and p is the projection $M^n \longrightarrow M^k$ onto the first k coordinates, then $p(S)$ is defined by $\exists x_{k+1} ... x_n \ \varphi(x_1, ..., x_n, a_1, \dots, a_l)$. For projections onto other coordinate we just quantify over the remaining variables instead of $x_{k+1} ... x_n$.

(iii) If $f: S \longrightarrow M^k$ is definable, then S is definable because S is the projection of the graph of f onto the first n coordinates, hence (ii) applies. The image of f is definable, because the image of f is the projection of the graph of f onto the last k coordinates, hence (ii) applies again.

(iv) To see that $g \circ f$ is definable, take $\mathscr{L}$-formulas (with parameters $\bar{a}, \bar{b}$ inserted) $\gamma_f(x_1, ..., x_n, y_1, ..., y_k, \bar{a})$ and $\gamma_g(y_1, ..., y_k, z_1, ..., z_l, \bar{b})$ defining the graph of f, g in $\mathscr{M}$, respectively. Then the graph of $g \circ f$ is defined by

$$\exists y_1 ... y_k \; (\gamma_f(x_1, ..., x_n, y_1, ..., y_k) \wedge \gamma_g(y_1, ..., y_k, z_1, ..., z_l)).$$

Hence the composition $g \circ f : S \longrightarrow M^l$ is definable, which shows the assertion.[33]

(v) $\Rightarrow$. If f is definable, then the i-th component of f is the composition of f with the i-th coordinate function $M^k \longrightarrow M$; hence this coordinate of f is definable by (ii) and (iv).

$\Leftarrow$ Conversely, if the graph of the i-th coordinate of f is defined by $\gamma_i(x_1, ..., x_n, y, \bar{a}_i)$ (with parameters $\bar{a}_i$ inserted), then f is defined by

$$\bigwedge_{i=1}^{k} \gamma_i(x_1, ..., x_n, y_i, \bar{a}_i).$$

$\square$

3.1.7. *Convention.* Let $\mathscr{M}$ be an $\mathscr{L}$-structure with universe M, $S \subseteq M^n$ and let $f = (f_1, \ldots, f_k) : S \longrightarrow M^k$ be a function that is definable in $\mathscr{M}$ by $\gamma(x_1, \ldots, x_n, y_1, \ldots, y_k)$ without parameters. If $\varphi(x_1, \ldots, x_k)$ is an $\mathscr{L}$-formula then we write $\varphi(f_1, \ldots, f_k)$ for the formula $\exists y_1, \ldots, y_k \varphi(y_1, \ldots, y_k) \wedge \gamma(x_1, \ldots, x_n, y_1, \ldots, y_k)$.

For example if $T \subseteq M^m$ and $g : T \longrightarrow M$ is definable in $\mathscr{M}$, then $g(x_1, \ldots, x_m) \doteq x_{m+1}$ just stands for a formula defining the graph of g (here $k = 2$, φ is $x_1 \doteq x_2$, $n = m+1$, $S = T \times M$, $f_1(x_1, \ldots, x_{m+1}) = g(x_1, \ldots, x_m)$, $f_2(x_1, \ldots, x_{m+1}) = x_{m+1}$).

3.1.8. *Example.* Look at $\mathscr{M} = (\mathbb{R}, +, \cdot)$ and a definable map $f : \mathbb{R}^n \longrightarrow \mathbb{R}^k$. The definition from Real Analysis of continuity at a point of such a function can be used to show that the set of all points where f is continuous, is again definable in $\mathscr{M}$; see question 71. Similarly, the set of all points where f is differentiable, is definable in $\mathscr{M}$.

[33] Alternatively, we could have used the formula $\forall y_1 ... y_k \; (\gamma_f(x_1, ..., x_n, y_1, ..., y_k) \wedge \gamma_g(y_1, ..., y_k, z_1, ..., z_l))$.

3.2. **Zermelo-Fraenkel Set Theory (with choice).**

Named after Ernst Zermelo and Abraham Fraenkel.

We can now carry out what has been announced in section 1.6, namely we can give an introduction to axiomatic set theory. This means we will write out a set of sentences in the language of set theory, which is abbreviated as "ZFC" and argue that most of mathematics is a consequence of these axioms (we will also comment on what lies outside).

Another aim is to show how the paradoxes in section 1.6 are resolved, and how Gödels's theorems can be understood. Finally we will deploy the completeness theorem and the compactness theorem to prove some surprising facts about these axioms, or rather models of those.[34]

Throughout, $\mathscr{L}$ denotes the language $\{\,\varepsilon\,\}$ of set theory, where ε is a binary relation symbol. We write $x \mathrel{\varepsilon} y$ for $\varepsilon\,(x, y)$.

[34]The attentive reader will have noticed that this introduction does not talk about theories.

3.2.1. **The Zermelo-Fraenkel Axioms** Consider the following $\mathscr{L}$-sentences. The text in square brackets indicates the intended meaning (and only this part is examinable). You should think that all elements range over "sets".

Existence [There is an empty set x, denoted by $\emptyset$.]

$$\exists x \forall y (y \not\varepsilon x)$$

Extensionality [Two sets with the same elements are equal.]

$$\forall x \forall y \ \big(x \doteq y \longleftrightarrow \forall z \ (z \,\varepsilon\, x \leftrightarrow z \,\varepsilon\, y)\big)$$

Pairing [For all sets x, y there is a set "$z = \{x, y\}$".]

$$\forall x \forall y \exists z \forall u \big(u \,\varepsilon\, z \leftrightarrow (u \doteq x \vee u \doteq y)\big).$$

Powerset [Every set x has a power set $y = \mathfrak{P}(x)$.]

$$\forall x \exists y \forall z \Big(z \,\varepsilon\, y \longleftrightarrow (\forall u \ u \,\varepsilon\, z \to u \,\varepsilon\, x)\Big)$$

Union [For each set x the "union" $y = \bigcup x$ of all the $z \in x$ exists.]

$$\forall x \exists y \forall u \big(u \,\varepsilon\, y \longleftrightarrow \exists z (u \,\varepsilon\, z \wedge z \varepsilon x)\big)$$

Foundation [The relation ε is well-founded: Every nonempty set contains an element that is disjoint from x.]

$$\forall x \Big((\exists y \ y \,\varepsilon\, x) \to (\exists y \ y \,\varepsilon\, x \wedge \forall z \ z \,\varepsilon\, x \to z \not\varepsilon\, y)\Big)$$

Separation [35] [Every definable subset of a set defines a set.]
This is an axiom scheme: Given an $\mathscr{L}$-formula $\varphi = \varphi(x, z, u_1, ..., u_n)$, an instance of this axiom scheme is the sentence

$$\forall z \forall u_1 ... \forall u_n \exists y \forall x \Big(x \,\varepsilon\, y \longleftrightarrow (\varphi \wedge x \,\varepsilon\, z)\Big).$$ [36]

Replacement [The image of a set under a definable function is a set.]
This is an axiom scheme: Given an $\mathscr{L}$-formula $\varphi = \varphi(x, y, u_1, ..., u_n)$, an instance of this axiom scheme is the sentence

$$\forall u_1 ... \forall u_n \Big((\forall x \exists! y \, \varphi) \to \forall v \exists w \forall y \ (y \,\varepsilon\, w \longleftrightarrow \exists x \ x \,\varepsilon\, v \wedge \varphi)\Big).$$

Infinity [There is an infinite set.]

$$\exists x \Big((\exists y \, y \,\varepsilon\, x) \wedge \forall y \, y \,\varepsilon\, x \to \exists z \, (z \,\varepsilon\, x \wedge \forall u \, (u \,\varepsilon\, z \leftrightarrow u \doteq y \vee u \,\varepsilon\, y))\Big)$$

ZF denotes the set consisting of the $\mathscr{L}$-sentences above. In the literature, there are slight variations on these axioms, but they all prove the same $\mathscr{L}$-sentences.

---

[35] also called **restricted comprehension**

[36] Here the $z, u_1, \ldots, u_n$ should be thought of as placeholders for parameters. The axiom then says that for each choice of the $c, a_1, \ldots, a_n$ in a model $\mathscr{M}$, the set defined by $\varphi(x, c, a_1, ..., a_n)$ in $\mathscr{M}$ (in the sense of 3.1.1), intersected with the set defined by $x \,\varepsilon\, c$ in $\mathscr{M}$, is equal to the set defined by $x \,\varepsilon\, b$ in $\mathscr{M}$ for some $b \in |\mathscr{M}|$. In this explanation the word "set" refers to the meta theory.

3.2.2. Examples of definable sets and functions in ZF

Let $\mathscr{M}$ be a model of ZF with universe M.

(1) We write $x \subseteq y$ as abbreviation of the formula $\forall v(v \,\varepsilon\, x \to v \,\varepsilon\, y)$

(2) We write $z = \{x, y\}$ for the formula $\forall v(v \,\varepsilon\, z \longleftrightarrow (v \doteq x \vee v \doteq y))$. By Pairing and Extensionality, this formula defines the graph of a function in $\mathscr{M}$, namely the function $\{\_, \_\} : M \times M \longrightarrow M,\ (x, y) \mapsto \{x, y\}$. (Compare this with 3.1.7).

If $x = y$ we just write $\{x\}$ instead of $\{x, x\}$, which makes sense by Extensionality.

(3) We write $z = \langle x, y\rangle$ for the formula $z = \{\{x\}, \{x, y\}\}$. By (2) this defines the graph of a function in $\mathscr{M}$, namely the function $\langle \_, \_\rangle : M \times M \longrightarrow M,\ (x, y) \mapsto \langle\{x\}, \{x, y\}\rangle$, which captures the ordered pair with first entry x and second entry y in $\mathscr{M}$.

(4) We write $z = x \times y$ for the formula $\forall u\big(u \,\varepsilon\, z \longleftrightarrow \exists v \exists w(v \,\varepsilon\, x \wedge w \,\varepsilon\, y \wedge u \doteq \langle v, w\rangle)\big)$. By (3) this defines the graph of a function in $\mathscr{M}$, namely the function $\_ \times \_ : M \times M \longrightarrow M,\ (x, y) \mapsto x \times y$, which captures the cartesian product of x and y in $\mathscr{M}$.

(5) We write $\mathrm{FUNC}(x, y, z)$ for the formula $z \subseteq x \times y \wedge \forall u(u \,\varepsilon\, x \to \exists! v\langle u, v\rangle \,\varepsilon\, z)$. By (4) this captures the notion of a function $x \to y$ with graph z in $\mathscr{M}$. Furthermore we define $\mathrm{Graph}(z)$ as the formula $\exists x \exists y\, \mathrm{FUNC}(x, y, z)$ expressing that z is the graph of a function in $\mathscr{M}$.

(6) We write $y = \mathfrak{P}(x)$ for the formula $\forall z\Big(z \,\varepsilon\, y \longleftrightarrow z \subseteq x\Big)$. By Powerset and Extensionality this formula defines the graph of a function in $\mathscr{M}$, namely the function $\mathfrak{P} : M \longrightarrow M,\ x \mapsto \mathfrak{P}(x)$, capturing the operation of taking the powerset in $\mathscr{M}$.

We are now able to formally write out the following further axiom in a human readable form:

Axiom of Choice [Every set of nonempty sets has a choice function.]

$$\forall x\Bigg(\emptyset \not\varepsilon\, x \to \exists y \exists z\Big(\mathrm{FUNC(x, y, z)} \wedge \forall u \forall v(u \,\varepsilon\, x \wedge \langle u, v\rangle \,\varepsilon\, z \to v \,\varepsilon\, u)\Big)\Bigg).$$

Hence this axiom says that for every $x \in M$ with $\emptyset \not\varepsilon\, x$ (you should think of x as a set of nonempty sets), there is a function f (with domain x and graph z) such that $f(u) \in u$ for all $u \,\varepsilon\, x$.

In most part of mathematics one also uses the axiom of choice. For example we have used it in the proof of Zorn's lemma and therefore many of the vast amount of consequences of Zorn's lemma also make use of the axiom of choice.

We write ZFC for the set ZF together with the Axiom of Choice.

3.2.3. *Remark.* The axiom of choice says, in a colloquial way, that for every collection of nonempty subsets X_i of a given set X, where i is from some index set I, there is a function $f : I \longrightarrow X$ with $f(i) \in X_i$ for all $i \in I$. This seems to be obvious: since $X_i \neq \emptyset$ we could just define

$$f : I \longrightarrow X,\ f(i) = \text{ some element of } X_i.$$

However, this claims the existence of an object (namely the graph of f) and the choice that one has to make for each i is not expressible within the axioms of ZF.

To understand this better, consider another structure $\mathscr{M}$ in the language $\{\,\varepsilon\,\}$ of set theory with universe $\mathbb{Z}$, which interprets the binary relation symbol ε as

$$k\,\varepsilon^{\mathscr{M}}\,n \iff k \neq n \text{ and } k, n \in \{3m, 3m+1, 3m+2\} \text{ for some } m \in \mathbb{Z}.$$

Then for each n there are two elements $k \in \mathbb{Z}$ with $k\,\varepsilon^{\mathscr{M}}\,n$. However there is no way to "pick one out" uniformly for all choices of n only by a single $\mathscr{L}$-formula (even with using parameters). In fact we will prove in question 78 that there is no function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ that is definable in $\mathscr{M}$ with the property that $f(n)\,\varepsilon^{\mathscr{M}}\,n$ holds for all n. Note that there are many functions $g : \mathbb{Z} \longrightarrow \mathbb{Z}$ with the property that $g(n)\,\varepsilon^{\mathscr{M}}\,n$ holds for all n. But none of them is definable in $\mathscr{M}$.

Observe that the Axiom of Choice is also claiming the existence of certain definable functions (using a parameter) of its models; this is clarified in question 73 of the example sheets.

3.3. Elementary equivalence and the Skolem-Löwenheim Theorems.

We return to general languages and import some fundamental results from Model Theory. Throughout, $\mathscr{L}$ is a first order language. We are mainly interested in the following relation between $\mathscr{L}$-structures:

3.3.1. **Definition.** Two $\mathscr{L}$-structures $\mathscr{M}$ and $\mathscr{N}$ are called **elementary equivalent** if they satisfy the same $\mathscr{L}$-sentences. This is usually denoted by $\mathscr{M} \equiv \mathscr{N}$. In other words $\mathscr{M} \equiv \mathscr{N}$ if and only if $\mathrm{Th}(\mathscr{M}) = \mathrm{Th}(\mathscr{N})$.

Elementary equivalence is very hard to verify in general as it says something about all $\mathscr{L}$-sentences that are true in the given structures.

3.3.2**. Non-examples.**

(i) The posets $(\mathbb{Z}, \leq)$ and $(\mathbb{Q}, \leq)$ are not elementary equivalent.
(ii) The fields $(\mathbb{R}, +, \cdot, -, 0, 1)$ and $(\mathbb{C}, +, \cdot, -, 0, 1)$ are not elementary equivalent.
(iii) The fields $(\mathbb{R}, +, \cdot, -, 0, 1)$ and $(\mathbb{Q}, +, \cdot, -, 0, 1)$ are not elementary equivalent.

There are two theoretical instances that we will be considering.

3.3.3. **Definition.** Let $\mathscr{M}, \mathscr{N}$ be $\mathscr{L}$-structures. An isomorphism $f : \mathscr{M} \longrightarrow \mathscr{N}$ is a bijective map $f : |\mathscr{M}| \longrightarrow |\mathscr{N}|$ satisfying the following conditions:

(a) If R is an n-ary relation symbol of $\mathscr{L}$, and $a_1, \ldots, a_n \in |\mathscr{M}|$, then
$$\mathscr{M} \models R(a_1, \ldots, a_n) \iff \mathscr{N} \models R(f(a_1), \ldots, f(a_n)).$$
(b) If F is a k-ary function symbol of $\mathscr{L}$ and $a_1, \ldots, a_k \in |\mathscr{M}|$, then
$$f(F^{\mathscr{M}}(a_1, \ldots, a_k)) = F^{\mathscr{N}}(f(a_1), \ldots, f(a_k)).$$
(c) If c is a constant symbol of $\mathscr{L}$, then $f(c^{\mathscr{M}}) = c^{\mathscr{N}}$.

Clearly if f is an isomorphism $\mathscr{M} \longrightarrow \mathscr{N}$, then its compositional inverse f^{-1} is an isomorphism $\mathscr{N} \longrightarrow \mathscr{M}$. Two $\mathscr{L}$-structures $\mathscr{M}$ and $\mathscr{N}$ are called **isomorphic**, in symbols $\mathscr{M} \cong \mathscr{N}$, if there is an isomorphism $\mathscr{M} \longrightarrow \mathscr{N}$.

3.3.4. *Examples.*

(i) An isomorphism between to structures in the basic language is just a bijection.
(ii) An isomorphism between two groups in the language of groups in the sense of 3.3.3 is just the same thing as an isomorphism between two groups in the sense of group theory.
(iii) An isomorphism between two posets in the language of posets in the sense of 3.3.3 is just the same thing as an isomorphism between posets in the sense of definition 1.1.8.

3.3.5. **Proposition.** *Let $f : \mathscr{M} \longrightarrow \mathscr{N}$ be an $\mathscr{L}$-isomorphism. If h is an assignment of $\mathscr{M}$ and φ is an $\mathscr{L}$-formula, then*

$$\mathscr{M} \models \varphi[h] \iff \mathscr{N} \models \varphi[f \circ h].$$

A more natural formulation of this statement reads as follows: For every $\varphi(x_1, \dots, x_n) \in \mathrm{Fml}(\mathscr{L})$ and each $\bar{a} \in |\mathscr{M}|^n$ we have

$$\mathscr{M} \models \varphi(a_1, \dots, a_n) \iff \mathscr{N} \models \varphi(f(a_1), \dots, f(a_n)).$$

In particular $\mathscr{M}, \mathscr{N}$ are elementary equivalent.

Proof. [This proof is long but is straightforward. Please read it or better try to do it yourself by induction on the complexity of φ.]

We show the assertion by induction on the complexity of φ. For the induction start assume that φ has complexity 0, i.e. φ is an atomic formula.

Claim. If t is an $\mathscr{L}$-term, then $f(t^{\mathscr{M}}[h]) = t^{\mathscr{N}}[f \circ h])$.

Proof. This is true by definition 3.3.3 when t is of the form $F(x_1, \dots, x_n)$ for some $F \in \mathscr{F}$ and then a straightforward induction on the complexity of the term t shows the claim. $\diamond$

The claim implies that $\mathscr{M} \models \varphi[h] \iff \mathscr{N} \models \varphi[f \circ h]$ if φ is an equality of terms. If φ is of the form $R(t_1, \dots, t_k)$ with $R \in \mathscr{R}$, then the claim together with the definition 3.3.3 shows that $\mathscr{M} \models \varphi[h] \iff \mathscr{N} \models \varphi[f \circ h]$. This covers the case of an atomic formula φ.

For the induction step it suffices to show the equivalence when φ is $\neg\psi$, and when φ is $\psi \wedge \gamma$ and when φ is $\forall x \psi$, assuming the equivalence already for $\psi$and γ (consult question 55 if you are wondering why we are dealing with the case $\psi \wedge \gamma$ instead of $\psi \rightarrow \gamma$). The cases when φ is $\neg\psi$, and when φ is $\psi \wedge \gamma$ are clear. We deal with the case when φ is $\forall x \psi$.

We choose variables $y_1, \dots, y_n$ with $\mathrm{Fr}(\psi) \subseteq \{x, y_1, \dots, y_n\}$, hence ψ should be understood as $\psi(x, y_1, \dots, y_n)$ and $\mathrm{Fr}(\varphi) = \mathrm{Fr}(\forall x \psi) \subseteq \{y_1, \dots, y_n\}$. For $a_1, \dots, a_n \in |\mathscr{M}|$ we need to show

$$\mathscr{M} \models \forall x \psi(a_1, \dots, a_n) \iff \mathscr{N} \models \forall x \psi(f(a_1), \dots, f(a_n)).$$

By symmetry it suffices to just show $\Longrightarrow$ (for the other implication use f^{-1}). So assume $\mathscr{M} \models \forall x \psi(a_1, \dots, a_n)$. In order to show $\mathscr{N} \models \forall x \psi(f(a_1), \dots, f(a_n))$ we need to show that for all $c \in |\mathscr{N}|$ we have $\mathscr{N} \models \psi(c, f(a_1), \dots, f(a_n))$. Take an element $c \in |\mathscr{N}|$. Since f is surjective, there is some $b \in |\mathscr{M}|$ with $f(b) = c$. As we assume $\mathscr{M} \models \forall x \psi(a_1, \dots, a_n)$ we know that $\mathscr{M} \models \psi(b, a_1, \dots, a_n)$. By the assumption on ψ we know that $\mathscr{N} \models \psi(f(b), f(a_1), \dots, f(a_n))$. But $f(b) = c$, hence $\mathscr{N} \models \psi(c, f(a_1), \dots, f(a_n))$ as required. $\square$

3.3.6. **Corollary.** *Let $\mathscr{M}$ be an $\mathscr{L}$-structure with universe $M = |\mathscr{M}|$. If $f : \mathscr{M} \longrightarrow \mathscr{N}$ is an isomorphism between $\mathscr{L}$-structures and $S \subseteq M^n$ is defined by $\varphi(\bar{x}, \bar{a})$, then $f(S)$ is defined by $\varphi(\bar{x}, f(\bar{a}))$ (here we also consider f as a map $M^n \longrightarrow |\mathscr{N}|^n$ obtained from f by applying f coordinate wise; thus $f(S) \subseteq |\mathscr{N}|^n$ and $f(\bar{a}) \in |\mathscr{N}|^n$).*

Proof. Let T be the subset of $|\mathscr{N}|^n$ defined by $\varphi(\bar{x}, f(\bar{a}))$. The assertion says that $f(S) = T$. But this follows from 3.3.5. $\square$

3.3.7. **Definition.** Let $\mathscr{N}$ be an $\mathscr{L}$-structure.

(i) A **substructure** of $\mathscr{N}$ is an $\mathscr{L}$-structure $\mathscr{M}$ with $|\mathscr{M}| \subseteq |\mathscr{N}|$ such that the interpretations of the relation, function and constant symbols of $\mathscr{L}$ in $\mathscr{M}$ are restrictions of those in $\mathscr{N}$. This means concretely
  (a) If R is an n-ary relation symbol of $\mathscr{L}$, then $R^{\mathscr{M}} = M^n \cap R^{\mathscr{N}}$,
  (b) If F is a k-ary function symbol of $\mathscr{L}$, then $|\mathscr{M}|$ is closed under $F^{\mathscr{N}}$, i.e. $F^{\mathscr{M}}(a_1, \dots, a_k) = F^{\mathscr{N}}(a_1, \dots, a_k) \in M$ for all $a_1, \dots, a_k \in |\mathscr{M}|$.
  (c) If c is a constant symbol of $\mathscr{L}$, then $c^{\mathscr{M}} = c^{\mathscr{N}} \in |\mathscr{M}|$.

  If this is the case we also say that $\mathscr{N}$ is an **extension of a structure** of $\mathscr{M}$.

(ii) If $\mathscr{M}$ is a substructure of $\mathscr{N}$, then $\mathscr{M}$ is called an **elementary substructure** of $\mathscr{N}$ and $\mathscr{N}$ is an **elementary extension** of $\mathscr{M}$ if for every $\mathscr{L}$-formula $\varphi(x_1, \dots, x_n)$ and all all $a_1, \dots, a_n \in |\mathscr{M}|$ we have

$$\mathscr{M} \models \varphi(a_1, \dots, a_n) \iff \mathscr{N} \models \varphi(a_1, \dots, a_n)$$

  This property is denoted by $\mathscr{M} \prec \mathscr{N}$.

Clearly $\mathscr{M} \prec \mathscr{N}$ implies $\mathscr{M} \equiv \mathscr{N}$, however this is not the same as saying that $\mathscr{M}$ is a substructure of $\mathscr{N}$ and $\mathscr{M} \equiv \mathscr{N}$. An example is given in question 76.

The following two theorems are the most important consequences of the completeness and the compactness theorem for Mathematics and for Set Theory. The proofs are not examinable and may be found in the appendix to this section.

3.3.8**. Skolem-Löwenheim downwards.**
Let $\mathscr{M}$ be an $\mathscr{L}$-structure and let $A \subseteq |\mathscr{M}|$. Then there is an elementary substructure $\mathscr{N}$ of $\mathscr{M}$ with $A \subseteq |\mathscr{N}|$ such that $\mathrm{card}(\mathscr{N}) \leq \max\{\aleph_0, \mathrm{card}(A), \mathrm{card}(\mathscr{L})\}$.

Proof. This proof is not examinable and may be found in the appendix, 3.3.14 □

3.3.9**. Skolem-Löwenheim upwards.**
Let $\mathscr{M}$ be an infinite $\mathscr{L}$-structure and let κ be a cardinal $\geq \mathrm{card}(\mathscr{M}), \mathrm{card}(\mathscr{L})$. Then there is an elementary extension $\mathscr{N} \succ \mathscr{M}$ of cardinality κ. (So in particular, every infinite $\mathscr{L}$-structure in any language has **proper** elementary extensions.)

Proof. This proof is not examinable and may be found in the appendix, 3.3.16 □

3.3.10**. Example - Sets** Let $\mathscr{L} = \emptyset$ be the language of sets. If $\mathscr{M}$ and $\mathscr{N}$ are infinite sets, then they are elementary equivalent as $\mathscr{L}$-structures. Another way of saying this is: The set of logical consequences of the theory of infinite sets is complete (cf. 2.7.4).

Proof. Choose a cardinal κ of at least the cardinality of $\mathscr{M}$ and $\mathscr{N}$. By Skolem-Löwenheim upwards 3.3.9, there are elementary extensions $\mathscr{M}' \succ \mathscr{M}$ and $\mathscr{N}' \succ \mathscr{N}$ both of cardinality κ. In particular $\mathscr{M}'$ and $\mathscr{N}'$ are of the same cardinality and there is a bijective map $f : \mathscr{M}' \longrightarrow \mathscr{N}'$. So we are in the following situation:

$$\begin{tikzcd} \mathscr{M}' \arrow[r, "f"] & \mathscr{N}' \\ \mathscr{M} \arrow[u, hook, "\prec"] & \mathscr{N} \arrow[u, hook', "\prec"'] \end{tikzcd}$$

where the vertical maps are the inclusion (they are elementary). Since the vertical maps are elementary we get $\mathscr{M} \equiv \mathscr{M}'$ and $\mathscr{N} \equiv \mathscr{N}'$. Since f is a bijection and $\mathscr{L}$ has no non-logical symbols, f is an isomorphism $\mathscr{M}' \longrightarrow \mathscr{N}'$. By 3.3.5 we know that $\mathscr{M}' \equiv \mathscr{N}'$ in this case. Altogether we get $\mathscr{M} \equiv \mathscr{M}' \equiv \mathscr{N}' \equiv \mathscr{N}$ as desired. $\square$

We will not use the following proposition later on, but it shows how strong elementary equivalence is.

3.3.11. **Proposition.** *Let $\mathscr{L}$ be any language (not necessarily finite). If $\mathscr{M}, \mathscr{N}$ are $\mathscr{L}$-structures with $\mathscr{N} \equiv \mathscr{M}$ and $\mathscr{M}$ is finite, then $\mathscr{M}$ is even isomorphic to $\mathscr{N}$.*

Proof. [This proof is not examinable] Let n be the size of $\mathscr{M}$ and let $a_1, \ldots, a_n$ be the list of all elements of $|\mathscr{M}|$. We write $\bar{a} = (a_1, \ldots, a_n)$. Since $\mathscr{N} \equiv \mathscr{M}$ the structure $\mathscr{N}$ is also of size n (see question 48 from the example sheets). It suffices to find some n-tuple $\bar{b} = (b_1, \ldots, b_n)$ of $|\mathscr{N}|$ such that for all formulas $\varphi(\bar{x})$, $\bar{x} = (x_1, \ldots, x_n)$ we have

$$\mathscr{M} \models \varphi(\bar{a}) \Rightarrow \mathscr{N} \models \varphi(\bar{b}).$$

(Then the map $f : \mathscr{M} \longrightarrow \mathscr{N}$ defined by $f(a_i) = b_i$ is easily seen to be an isomorphism.) Suppose there is no such n-tuple. Then for each $\bar{b} \in |\mathscr{N}|^n$ there is a formula $\varphi_{\bar{b}}(\bar{x})$ such that $\mathscr{M} \models \varphi_{\bar{b}}(\bar{a})$ and $\mathscr{N} \models \neg\varphi_{\bar{b}}(\bar{b})$. Since $\mathscr{N}$ is finite, the set $|\mathscr{N}|^n$ is finite as well and therefore we may form the conjunction $\psi(\bar{x})$ of all the $\varphi_{\bar{b}}(\bar{x})$ with $\bar{b} \in |\mathscr{N}|^n$. Then $\mathscr{M} \models \psi(\bar{a})$ and as $\mathscr{N} \equiv \mathscr{M}$ there is some $\bar{b} \in |\mathscr{N}|^n$ with $\mathscr{N} \models \psi(\bar{b})$. But this contradicts $\mathscr{N} \models \neg\varphi_{\bar{b}}(\bar{b})$ and $\models \psi(\bar{x}) \to \varphi_{\bar{b}}(\bar{x})$. $\square$

Appendix to section 3.3

`None of the proofs in this appendix is examinable. Only statements that also occur outside of this appendix are examinable.`

3.3.12. **Tarski-Vaught Test.**
Let $\mathscr{M}$ be an $\mathscr{L}$-structure and let $A \subseteq |\mathscr{M}|$. The following are equivalent:

(i) A is the universe of an elementary substructure of $\mathscr{M}$.
(ii) For every $\mathscr{L}$-formula $\varphi(x, \bar{y})$ and all $\bar{a} \in A^{\bar{y}}$ [37], if $\mathscr{M} \models \exists x\, \varphi(x, \bar{a})$ (to be correct we should actually write $\mathscr{M} \models (\exists x\, \varphi)(\bar{a})$), then there is some $b \in A$ with $\mathscr{M} \models \varphi(b, \bar{a})$.

Proof. (i)$\Rightarrow$(ii) is immediate from the definition of "elementary substructure". For the converse we first observe that under assumption (ii), A is closed under all $F^{\mathscr{M}}$ ($F \in \mathscr{F}$) and A contains all $c^{\mathscr{M}}$ with $c \in \mathscr{C}$: To see this, take an n-ary function symbol F. Applying condition (ii), where $\varphi(x, \bar{y})$ is the formula $F(\bar{y}) \doteq x$ we see that $F^{\mathscr{M}}(\bar{a}) \in A$ for all $\bar{a} \in A^{\bar{y}}$. Similarly, using the formula $x \doteq c$ (so, no other variables $\bar{y}$ are present in φ), we see that $c^{\mathscr{M}} \in A$ for all $c \in \mathscr{C}$.

Hence we know that A together with the structure induced from $\mathscr{M}$ is a substructure of $\mathscr{M}$ which we denote by $\mathscr{A}$. We now show (and this will prove (i)) by induction on the complexity of an $\mathscr{L}$-formula $\varphi(x_1, ..., x_k)$:

$$\text{For all } \bar{a} \in A^k \text{ we have } \mathscr{A} \models \varphi(\bar{a}) \overset{(*)}{\iff} \mathscr{M} \models \varphi(\bar{a}).$$

If φ is quantifier free this certainly holds true, since $\mathscr{A}$ is a substructure of $\mathscr{M}$. Moreover $(*)$ holds for $\neg\varphi$ if it holds for φ and $(*)$ holds for $\varphi \wedge \psi$ if it holds for φ and for ψ. Thus, for the induction step, it is enough to assume that $\varphi(x_1, ..., x_k)$ is $\exists y\ \psi(y, x_1, ..., x_k)$ where $\psi(y, x_1, ..., x_k) \in \mathrm{Fml}(\mathscr{L})$ and $(*)$ holds for ψ and all $(k+1)$-tuples from A. Take $\bar{a} \in A^k$.

"$\Rightarrow$". If $\mathscr{A} \models \varphi(\bar{a})$, then there is some $b \in A$ with $\mathscr{A} \models \psi(b, \bar{a})$ and by the induction hypothesis we have $\mathscr{M} \models \psi(b, \bar{a})$, thus $\mathscr{M} \models \varphi(\bar{a})$.

"$\Leftarrow$". If $\mathscr{M} \models \varphi(\bar{a})$ then $\mathscr{M} \models \exists y\ \psi(y, \bar{a})$. By (ii), there is some $b \in A$ with $\mathscr{M} \models \psi(b, \bar{a})$. By the induction hypothesis we get $\mathscr{A} \models \psi(b, \bar{a})$, thus $\mathscr{A} \models \varphi(\bar{a})$. $\square$

3.3.13. **Lemma.**
For any language $\mathscr{L}$, the cardinality of $\mathrm{Fml}(\mathscr{L})$ *is* $\max\{\aleph_0, \mathrm{card}(\mathscr{L})\}$.

Proof. The set $\mathrm{Fml}(\mathscr{L})$ consists of finite $\mathscr{L}$-strings, hence it is enough to show that the set of $\mathscr{L}$-strings has cardinality at most $\max\{\aleph_0, \mathrm{card}(\mathscr{L})\}$. The set X of all letters of $\mathscr{L}$ has cardinality $\kappa = \max\{\aleph_0, \mathrm{card}(\mathscr{L})\}$ Hence an $\mathscr{L}$-string, by its very definition, is a member of X^n for some $n \in \mathbb{N}$. From question 17 on the example sheets we know that $\bigcup_{n\in\mathbb{N}} X^n$ has size κ as required. $\square$

[37] $A^{\bar{y}}$ stands for A^m, where m is the length of the tuple of variables $\bar{y}$. In order not to overload notation we use this convention (in particular when we never really need the integer m).

3.3.14. **Skolem-Löwenheim downwards.**
Let $\mathscr{M}$ be an $\mathscr{L}$-structure and let $A \subseteq |\mathscr{M}|$. Then there is an elementary substructure $\mathscr{N}$ of $\mathscr{M}$ with $A \subseteq |\mathscr{N}|$ such that $\operatorname{card}(\mathscr{N}) \leq \max\{\aleph_0, \operatorname{card}(A), \operatorname{card}(\mathscr{L})\}$.

Proof. The strategy is the following: We want to apply the Tarski-Vaught test 3.3.12. By this test, the only thing we need to do is to add elements to A so that condition (ii) of the test is satisfied for the resulting set. We then have to count the number of elements we have added to get the cardinality estimates. Here are the details.

We use the following ad-hoc notation for each $\mathscr{L}$-formula $\varphi(x, y_1, \ldots, y_n)$ and all $\bar{a} \in |\mathscr{M}|^n$: If $\mathscr{M} \models \exists x\ \varphi(x, \bar{a})$, choose an element $b_{\varphi,\bar{a}} \in |\mathscr{M}|$ with

$$\mathscr{M} \models \varphi(b_{\varphi,\bar{a}}, \bar{a}).$$

If $\mathscr{M} \not\models \exists x\ \varphi(x, \bar{a})$, then choose $b_{\varphi,\bar{a}} \in |\mathscr{M}|$ arbitrarily.

For an arbitrary subset S of $|\mathscr{M}|$ we denote by S^* the following subset of $|\mathscr{M}|$:

$$S^* = \{b_{\varphi,\bar{a}} \mid n \in \mathbb{N}, \varphi(x, y_1, \ldots, y_n) \in \operatorname{Fml}(\mathscr{L}) \text{ and } \bar{a} \in S^n\}.$$

Observe that S^* contains S (if we choose φ as $x \doteq y$ and $a \in S$, then $b_{\varphi,a} = a$). Moreover, S^* is the image under the map

$$D \longrightarrow |\mathscr{M}|;\ (\varphi, \bar{a}) \mapsto b_{\varphi,\bar{a}},$$

where

$$D = \{(\varphi(x, \bar{y}), \bar{a}) \mid n \in \mathbb{N},\ \varphi(x, y_1, \ldots, y_n) \in \operatorname{Fml}(\mathscr{L}) \text{ and } \bar{a} \in S^n\}.$$

Since $D \subseteq \operatorname{Fml}(\mathscr{L}) \times \bigcup_{k\in\mathbb{N}} S^k$. We see that the cardinality of S^* is at most

$$(\dagger) \qquad \operatorname{card}(\operatorname{Fml}(\mathscr{L}) \times \bigcup_{n\in\mathbb{N}} S^n) \leq \max\{\aleph_0, \operatorname{card}(S), \operatorname{card}(\mathscr{L})\}.$$

By choice of all the $b_{\varphi,\bar{a}}$ we know that all tests performed on S in condition (ii) of the Tarski-Vaught test are solvable in S^*. However, we have introduced new elements and so the test does not give an elementary substructure on S^*.

The trick now is to iterate the construction. So we define (and return to our set A) $A_0 := A$ and by induction on $n \in \mathbb{N}$: $A_n = (A_{n-1})^*$. Finally we take $B := \bigcup_n A_n$ and claim that B satisfies the Tarski-Vaught test: Take $\varphi(x, \bar{y}) \in \operatorname{Fml}(\mathscr{L})$ and $\bar{a} \in B^{\bar{y}}$. Since $\bar{a}$ is a finite tuple it is contained in some A_n. But then $b_{\varphi,\bar{a}} \in A_{n+1} \subseteq B$ and so B satisfies condition (ii) of the Tarski-Vaught test.

Finally we take $\mathscr{N}$ as the structure on B given by the Tarski-Vaught test and we need to estimate the cardinality of B: By induction on n using $(\dagger)$, we see that $\operatorname{card} A_n \leq \max\{\aleph_0, \operatorname{card}(A), \operatorname{card}(\mathscr{L})\}$. Then the countable union B of these sets also has cardinality $\leq \max\{\aleph_0, \operatorname{card}(A), \operatorname{card}(\mathscr{L})\}$. □

We now turn to the proof of the Skolem-Löwenheim upwards theorem 3.3.9. Let $\mathscr{L}$ be a language. A crucial application of the compactness theorem says that any infinite structure has proper elementary extensions. A refined formulation is given in 3.3.9. We first show how to create proper elementary extensions.

3.3.15. **Lemma.** *Let $\mathscr{M}$ be an infinite $\mathscr{L}$-structure and let κ be any cardinal. Then there is an elementary extension $\mathscr{N}$ of $\mathscr{M}$ such that* $\operatorname{card}(|\mathscr{N}|) \geq \kappa$.

Proof. [this proof is not examinable] The proof uses the "method of diagrams" in combination with the compactness theorem. Let $M = |\mathscr{M}|$ be the universe of $\mathscr{M}$.

Firstly, we will enlarge our language $\mathscr{L}$ to include more constant symbols, naming all elements of M. So, for each $a \in M$, choose a new constant symbol c_a such that $c_a \neq c_b$ for $a \neq b$. We write $\mathscr{L}(M)$ for the resulting language; hence $\mathscr{L}(M)$ is the same as $\mathscr{L}$ except that it has more constant symbols, namely all the c_a.

Now in the new language $\mathscr{L}(M)$, consider the structure $(\mathscr{M}, M)$, with universe M, which interprets the non-logical symbols of $\mathscr{L}$ just like $\mathscr{M}$ and the new constant symbol c_a as a. Formally this says $(c_a)^{(\mathscr{M},M)} = a$. Informally one should think of $(\mathscr{M}, M)$ as being the same as $\mathscr{M}$, but we have introduced names for each element of M in the language. This looks like a tedious undertaking, but has remarkable applications as we shall see now.

Next, we introduce even more new constant symbols: Let $\mathscr{D}$ be any set of new (for $\mathscr{L}(M)$) constant symbols of size $\geq \kappa$ and add these constant symbols to the language $\mathscr{L}(M)$. Call the resulting language $\mathscr{L}^*$.

We now look at the following $\mathscr{L}^*$-theory

$$T = \Big\{\varphi(c_{a_1}, \ldots, c_{a_n}) \mid \varphi(x_1, \ldots, x_n) \in \operatorname{Fml}(\mathscr{L}),\ a_1, \ldots, a_n \in |\mathscr{M}| \text{ and } \mathscr{M} \models \varphi(a_1, \ldots, a_n)\Big\} \cup \Big\{\neg(d \doteq e) \mid d, e \in \mathscr{D}, d \neq e\Big\}.$$

Claim. T has a model, hence there is an $\mathscr{L}^*$-structure $\mathscr{N}^*$ with $\mathscr{N}^* \models T$.
Proof. By the Compactness Theorem it suffices to show that every finite subset of T has a model. But for every finite subset T_0 of T there is a finite subset $\mathscr{D}_0 \subseteq \mathscr{D}$ such that

$$\begin{aligned} T_0 \subseteq T_1 :=& \{\varphi(c_{a_1}, \ldots, c_{a_n}) \mid \varphi(x_1, \ldots, x_n) \in \operatorname{Fml}(\mathscr{L}) \text{ with } \mathscr{M} \models \varphi(a_1, \ldots, a_n)\} \\ &\cup \{\neg(d \doteq e) \mid d, e \in \mathscr{D}_0, d \neq e\}. \end{aligned}$$

Now T_1 has the following $\mathscr{L}^*$-structure $\mathscr{M}_1$ as a model:

We choose the universe and the interpretations of the $\mathscr{L}(M)$-symbols as given by $(\mathscr{M}, M)$; in particular c_a in $\mathscr{M}_1$ is interpreted as $a \in M$.

For the constants $d \in \mathscr{D}$ we do the following. Enumerate the constants in $\mathscr{D}_0$ as $d_1, \ldots, d_k$. Since $\mathscr{M}$ is infinite, there are distinct $a_1, \ldots, a_k \in M$. Then we interpret the d_i in $\mathscr{M}_1$ as a_i and all other constants in $\mathscr{D}$ arbitrarily.

Then we see that $\mathscr{M}_1$ is a model of T_1 as required. $\diamond$

Now take a model $\mathscr{N}^*$ of T as claimed to exist. Let $\mathscr{N}$ be the $\mathscr{L}$-structure underlying $\mathscr{N}^*$, thus $\mathscr{N}$ is just the same as $\mathscr{N}^*$ but we forget the interpretation of the constant symbols c_a and $d \in \mathscr{D}$. We define a map $f : M \longrightarrow |\mathscr{N}| = \mathscr{N}^*|$ as follows:

$$f(a) = (c_a)^{\mathscr{N}^*}.$$

Then f is an elementary embedding:

If $\varphi(x_1,\dots,x_n) \in \mathrm{Fml}(\mathscr{L})$ with $\mathscr{M} \models \varphi(a_1,\dots,a_n)$, then $\varphi(c_{a_1},\dots,c_{a_n}) \in T$ and as $\mathscr{N}^*$ is a model of T we know $\mathscr{N}^* \models \varphi(c_{a_1},\dots,c_{a_n})$. But in $\mathscr{N}^*$, the c_{a_i} are by definition interpreted as $f(a_i)$. Hence $\mathscr{N}^* \models \varphi(f(a_1),\dots,f(a_n))$ and so $\mathscr{N} \models \varphi(f(a_1),\dots,f(a_n))$ as required.

Further, the size of $|\mathscr{N}|$ is at least κ because for distinct constant symbols $d,e \in \mathscr{D}$ we have $\mathscr{N}^* \models d \neq e$. Consequently the map $\mathscr{D} \longrightarrow |\mathscr{N}|$ that sends d to $d^{\mathscr{N}^*}$ is injective.

In summary, we know that there is an elementary embedding $f : \mathscr{M} \longrightarrow \mathscr{N}$ such that $\mathscr{N}$ is of size $\geq \kappa$. Finally we identify $\mathscr{M}$ with the image of f and get an elementary extension $\mathscr{N}$ of $\mathscr{M}$ as required. □

3.3.16**. Skolem-Löwenheim upwards.**
Let $\mathscr{M}$ be an infinite $\mathscr{L}$-structure and let κ be a cardinal $\geq \mathrm{card}(\mathscr{M}), \mathrm{card}(\mathscr{L})$. Then there is an elementary extension $\mathscr{N} \succ \mathscr{M}$ of cardinality κ.

Proof. By 3.3.15, there is an elementary extension $\mathscr{N}_1 \succ \mathscr{M}$ of size $\geq \kappa$. Since $\kappa \geq \mathrm{card}(\mathscr{M})$ there is a subset $A \subseteq |\mathscr{N}_1|$ containing $|\mathscr{M}|$ of size κ. By Skolem-Löwenheim downwards there is en elementary substructure $\mathscr{N} \prec \mathscr{N}_1$ containing A, of size $\leq \max\{\kappa, \mathrm{card}(\mathscr{L})\}$. As $\kappa \geq \mathrm{card}(\mathscr{L})$ by assumption we see that $\mathscr{N}$ has size $\leq \kappa$. Since A has already size κ it follows that $\mathrm{card}(\mathscr{N}) = \kappa$.

Finally, as $\mathscr{M} \prec \mathscr{N}_1$ and $\mathscr{M} \subseteq \mathscr{N} \prec \mathscr{N}_1$ we get $\mathscr{M} \prec \mathscr{N}$ (see question 77). □

3.3.17**. Example: Infinitesimal elements in Analysis** [This example is not examinable] Let $f : \mathbb{R} \longrightarrow \mathbb{R}$ be a function and let $\mathscr{L}$ be the language $\{\leq, +, \cdot, -, 0, 1, F\}$, where F is a unary function symbol and the other symbols are relation symbols, function symbols and constant symbols with arity as you might guess by now (I chose the symbol "$-$" to be a unary function symbol). Let $\mathscr{M}$ be the $\mathscr{L}$-structure $(\mathbb{R}, \leq, +, -, \cdot, 0, 1, f)$, hence $F^{\mathscr{M}} = f$. By Skolem-Löwenheim upwards there is a proper elementary extension $\mathscr{N}$ of $\mathscr{M}$.

Claim. There are positive infinitesimal elements in $\mathscr{N}$, i.e., there is some $\mu \in |\mathscr{N}|$ such that for all $r \in \mathbb{R}$ with $0 < r$ we have $0 < \mu < r$ (in $\mathscr{N}$). (Notice that μ is not unique, e.g. $2{\cdot}\mu$ is also infinitesimal.)

Proof. Since $\mathscr{N}$ is a proper extension of $\mathscr{M}$, there is some $\alpha \in |\mathscr{N}| \setminus \mathbb{R}$. If $r < \alpha$ (in $\mathscr{N}$) for all $r \in \mathbb{R}$, then we may take $\mu = \frac{1}{\alpha}$. If $\alpha < r$ (in $\mathscr{N}$) for all $r \in \mathbb{R}$, then we may take $\mu = -\frac{1}{\alpha}$. In the remaining case we know that the set $S = \{r \in \mathbb{R} \mid r < \alpha \text{ (in } \mathscr{N})\}$ is nonempty and bounded from above. By the completeness axiom of $\mathbb{R}$ from Real Analysis we know that S has a supremum s in $\mathbb{R}$. Then either $s < \alpha$ (in $\mathscr{N}$) and we may take $\mu = \alpha - s$, or, $\alpha < s$ (in $\mathscr{N}$) and we may take $\mu = s - \alpha$. To fill the details here use the property $\mathscr{M} \prec \mathscr{N}$. $\diamond$

With the presence of infinitesimal elements we can now talk about them rigorously. For example:

Pick $a \in \mathbb{R}$. Then the function f is differentiable at a with derivative $f'(a) = b$ if and only if for every non-zero infinitesimal element μ, the Newton quotient (formed in $\mathscr{N}$)

$$\frac{F^{\mathscr{N}}(a+\mu) - F^{\mathscr{N}}(a)}{\mu},$$

is infinitesimally close to b. One may think of $F^{\mathscr{N}}$ as an extension of f (which is $F^{\mathscr{M}}$) and $\mu =$ "dx", so this characterization of differentiability shows that the intuitive one given to you elsewhere - is correct.

The proof of the equivalence is left as an advanced exercise to the interested reader: Use the fact that $\mathscr{N}$ is an elementary extension of $\mathscr{M}$.

3.4. **Foundations of axiomatic set theory.**

Here we give a brief overview of some of the highlights of axiomatic set theory. Most of these statements have long and complicated proofs and we will only give references to these. However, with the build up of Predicate Logic and the material in chapter 3 above, we are now able to understand the meaning of the results.

Note that we have not yet assumed that ZF is consistent, as a matter of fact, Gödel has shown that one cannot prove this at all in ZF (as axiom system of the meta theory). We'll talk about this in more detail in 3.4.9 below. However if we assume that ZF is consistent, then it has many models as follows from the Skolem-Löwenheim theorems 3.3.8, 3.3.9:

3.4.1. **Theorem.** *Every model of ZF is infinite. If ZF is consistent, then for every cardinal κ there is a model $\mathscr{M}$ of ZF with* $\operatorname{card}(|\mathscr{M}|) = \kappa$.

In particular, if ZF is consistent, then ZF has a countable model!

Proof. Let $\mathscr{M}$ be a model ZF. Then $\mathscr{M}$ is infinite as follows from the Axiom of Infinity, or by induction from the Pairing Axiom starting from the empty set according to Existence.

Now assume that ZF is consistent. By the completeness theorem (or rather its consequence 2.7.3) ZF has a model $\mathscr{M}$. We have just seen that $\mathscr{M}$ is infinite. We may now apply Skolem-Löwenheim downwards (3.3.8) to $\mathscr{M}$ (and the empty set) and see that there is an elementary restriction $\mathscr{N} \prec \mathscr{M}$ such that $\mathscr{N}$ is countable (and infinite). Finally by Skolem-Löwenheim upwards (3.3.9) applied to $\mathscr{N}$ and κ there is an elementary extension $\mathscr{M}^*$ of $\mathscr{N}$ of cardinality κ. Since elementary extensions preserve truth of sentences we see that $\mathscr{M}^* \equiv \mathscr{M}$. Hence $\mathscr{M}^*$ is a model of ZF of cardinality κ. □

How on earth can ZF have a countable model? A countable model $\mathscr{M}$ of ZF looks like a unicorn, because one could make the following argument. By the Axiom of Infinity there is an element $b \in |\mathscr{M}|$ such that $A := \{a \in |\mathscr{M}| : \mathscr{M} \models a \,\varepsilon\, b\}$ is infinite, e.g. by checking that the function $f : A \longrightarrow A, f(a) = a \cup \{a\}$ is injective but not surjective.[38]. Now the Powerset Axiom seems to say that the powerset of A exists in $\mathscr{M}$, which would contradict that the powerset of any infinite set is uncountable. However, this axiom only says that there is some $p \in |\mathscr{M}|$ such that

$$\mathscr{M} \models \forall y(y \,\varepsilon\, p \leftrightarrow y \subseteq b).$$

This implies that for an element $d \in |\mathscr{M}|$ with $d \,\varepsilon^{\mathscr{M}}\, p$, the set defined by $x \,\varepsilon\, d$ in $\mathscr{M}$ is a subset of A, but it does not imply that every subset of A comes from some $d \in |\mathscr{M}|$ in this form.

Note that in $\mathscr{M}$ the element p above is still uncountable in the sense of $\mathscr{M}$ (use the proof of 1.5.4 inside $\mathscr{M}$), however the set defined by $x \,\varepsilon\, p$ in $\mathscr{M}$ is countable, because $|\mathscr{M}|$ is countable.

[38]Observe that the existence of such an element b is a much stronger statement than just saying that $\mathscr{M}$ itself is infinite. In fact one can explicitly construct a model of ZF$\setminus\{$Axiom of Infinity$\}$ with countable universe, namely $(V_\omega, \in)$ defined in 3.4.3.

3.4.2. **Recursion Theorem** Let $\mathscr{M}$ be a model of ZF with universe M and let $g : M \longrightarrow M$ be a function that is definable in $\mathscr{M}$. Then there is a definable function $f : M \longrightarrow M$ such that for every ordinal α of $\mathscr{M}$ we have

$$f(\alpha) = g(f|_\alpha).$$

Here $f|_\alpha$ stands for the graph of the restriction of f to α, which indeed is a set and so we can plug it into g. For a more formal definition see question 82.

Proof. [Kunen2009, p. 225 and 244] □

The recursion theorem allows induction not only over natural numbers but over all ordinals; it is then called **transfinte induction**. It is often used to justify infinite definitions, like the **von Neumann hierarchy of sets**:

3.4.3. **Proposition.** *We define $V_0 = \emptyset$ and for every ordinal α, $V_{\alpha+1} = \mathfrak{P}(V_\alpha)$. For limit ordinals λ we define $V_\lambda = \bigcup_{\alpha\in\lambda} V_\alpha$. Then in any model of ZF, every element is in at least one of the V_α.*

Proof. This follows from the foundation axiom. Sketch. Suppose there is some set x that is not in any V_α. By the foundation axiom there is some set x that is not in any of the V_α such that no $y \in x$ has this property. But then each $y \in x$ is in some α and as y is a set there is some β such that for all $y \in x$ we have $y \in V_\beta$. Since $x = \{y \mid y \in x\}$ we get $x \subseteq V_\beta$. But then $x \in V_{\beta+1}$, a contradiction. □

3.4.4. **Equivalences of the Axiom of Choice** Each of the following statements are equivalent to the Axiom of Choice, assuming ZF.

(i) The Lemma of Zorn, see 1.2.5
(ii) The Well Ordering Principle, see 1.2.7.
(iii) Given any sets X, Y, either there is a surjective function $X \longrightarrow Y$, or there is a surjective function $Y \longrightarrow X$.
(iv) Every vector space has a basis.
(v) Tychonoff's theorem: The product of arbitrary many compact spaces is compact.

There are very many other conditions.

Proof. All this can be found in [Rubin1985, I.3]. □

All statements in 3.4.4 have significant impact in various parts of mathematics (Algebra, Topology, Analysis) and so most mathematician accept the Axiom of Choice. However, the Axiom of Choice also has undesirable consequences. The most famous one is maybe the so called "pea and sun paradox", which goes as follow:

3.4.5. **The Banach-Tarski Paradox** (Here we are assuming ZFC, i.e. ZF+Axiom of Choice.)

Let P be the closed ball of radius 0.5cm of $\mathbb{R}^3$. Let's think of P as a pea. Let S be the closed ball of radius 700000 kilometers in $\mathbb{R}^3$. Let's think of S as the sun.

Then there is a partitioning $P = P_1 \dot\cup \ldots \dot\cup P_5$ of P and a partitioning $S = S_1 \dot\cup \ldots \dot\cup S_5$ of S such that for each $i \in \{1, \ldots, 5\}$ there is a distance preserving map $\sigma_i : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ (also called isometry) with $\sigma_i(P_i) = S_i$.

Informally: The pea can be chopped up into 5 pieces such that these pieces can be put together[39] to the sun.

Proof. This is proved in much bigger generality in [Wagon1993]. □

Independence results

By the first incompleteness theorem 3.4.7 there are many sentence that we may want to add to ZF in order to get a stronger base. The most famous one is the Axiom of Choice, which is widely accepted. A second famous one is the so-called continuum hypothesis:

(**CH**) Every uncountable subset of $\mathbb{R}$ is in bijection with $\mathbb{R}$.

This also exists in a more general from, as generalised continuum hypothesis:

(**GCH**) If κ is an infinite cardinal, then the cardinality of $\mathfrak{P}(\kappa)$ is the smallest cardinal strictly bigger than κ.

3.4.6. **Theorem.** *Suppose* ZF *is consistent. Then*

(i) ZF + *Axiom of Choice* + *(*GCH*) is consistent (Gödel).*
(ii) ZFC + $\neg$*(*GCH*) is consistent (Cohen).*
(iii) ZF + $\neg$ *Axiom of Choice is consistent (Cohen).*

Hence the Axiom of Choice is independent of ZF*, i.e. it can neither be proved nor refuted in* ZF*. Similarly (*GCH*) is independent of* ZFC*.*

Cohen's proof introduced a completely new method to construct models of ZF *called* **forcing** *and this is one of the pillars of modern axiomatic set theory.*

Proof. This and much more independent results can all be found in [Jech2003]. □

It is not too difficult to show that ZF+GCH proves the Axiom of Choice. For those who want to dive into the topic, this could be even and advanced exercise.

[39]only moving the pieces around and applying orthogonal transformations

Incompleteness and Decidability

3.4.7. **Incompleteness I** (Gödel's first incompleteness theorem)
If Σ is any finite set of $\{\,\varepsilon\,\}$ sentences, then the deductive closure of $\mathrm{ZF} \cup \Sigma$ is **not** a complete theory. In fact a much stronger result is true with a scope even outside of set theory, but we don't have the means to express this rigorously. For set theory we have (informally) the following:

There is no algorithm which computes **any** complete theory containing ZF.

Proof. The required rigorous statement and the rigorous definition of what an algorithm can possible compute, as well as the proof may be found in [Goedel]. □

3.4.8. The assertion in 3.4.7 implies that we have no access to all true statements and one might wonder what we actually can access in a more restricted context. There are various structures that are in principle accessible. Most prominently, consider the structure $\mathscr{M} = (\mathbb{R}, +, -, \cdot, \leq, 0, 1)$ in the language of ordered rings. Then there is a computer program which accepts as input any sentence φ in that language (in form of a string of letters from the alphabet) and outputs

- YES if φ is true in $\mathscr{M}$.
- NO if φ is false in $\mathscr{M}$.

This has been proved by Alfred Tarski and is often labeled as the beginning of Model Theory, cf. [ModTh]. Structures (in a finite language), for which such an algorithm exist are called **decidable** and the question about which structures are decidable is a major driving force in contemporary logic and computer science.

3.4.9. **Incompleteness II** (Gödel's second incompleteness theorem)
If Σ is any finite set of $\{\,\varepsilon\,\}$-sentences, such that $\mathrm{ZF} \cup \Sigma$ is consistent, then $\mathrm{ZF} \cup \Sigma$ **cannot** prove its own consistency. Again there is a much stronger statement and we refer to [Goedel] again.

Here is an informal explanation what is asserted here. Let $\mathscr{M}$ be a model of $\mathrm{ZF} \cup \Sigma$. Then we can write out all the definitions and statements of predicate logic from chapter 2 inside $\mathscr{M}$. Hence we can do predicate logic inside $\mathscr{M}$ by *coding* all objects and notions (like sentence from $\mathrm{ZF} \cup \Sigma$ and proofs from that set) into $\mathscr{M}$. Then there is an $\{\,\varepsilon\,\}$-sentence φ such that

$\mathscr{M} \models \varphi$ if and only if the coded version of $\mathrm{ZF} \cup \Sigma$ in $\mathscr{M}$ is consistent in $\mathscr{M}$.

All this can be done independently of the chosen model $\mathscr{M}$, so φ will not be dependent on $\mathscr{M}$. Now the theorem says

$$\mathrm{ZF} \cup \Sigma \nvdash \varphi.$$

`Addon:` Since $\mathrm{ZF} \cup \Sigma$ is assumed to be consistent, the assertion $\mathrm{ZF} \cup \Sigma \nvdash \varphi$ is equivalent to saying that $\mathrm{ZF} \cup \Sigma \cup \{\neg\varphi\}$ is consistent, as we have seen in question 56 of the example sheets. Hence $\mathrm{ZF} \cup \Sigma \cup \{\neg\varphi\}$ then is a proper consistent strengthening of $\mathrm{ZF} \cup \Sigma$ (which has a model by the completeness theorem) and so we may feed 3.4.9 again with $\Sigma \cup \{\neg\varphi\}$.

++

References

[Ciesie1997] Krzysztof Ciesielski. Set theory for the working mathematician, volume 39 of London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1997.

[CorLas2000] René Cori and Daniel Lascar. Mathematical logic. Oxford University Press, Oxford, 2000. A course with exercises. Part I, Propositional calculus, Boolean algebras, predicate calculus, Translated from the 1993 French original by Donald H. Pelletier, With a foreword to the original French edition by Jean-Louis Krivine and a foreword to the English edition by Wilfrid Hodges.

[CorLas2001] René Cori and Daniel Lascar. Mathematical logic. Oxford University Press, Oxford, 2001. A course with exercises. Part II, Recursion theory, Gödel's theorems, set theory, model theory, Translated from the 1993 French original by Donald H. Pelletier, With a foreword to the original French edition by Jean-Louis Krivine and a foreword to the English edition by Wilfrid Hodges.

[Devlin1984] Keith J. Devlin. Constructibility. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1984.

[Endert2001] Herbert B. Enderton. A mathematical introduction to logic. Harcourt/Academic Press, Burlington, MA, second edition, 2001.

[Goedel31] Kurt Gödel. Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. Monatsh. Math. Phys., 38(1):173–198, 1931.

[Goedel1938] Kurt Gödel. The consistency of the axiom of choice and of the generalized continuum-hypothesis. Proceedings of the National Academy of Sciences, 24(12):556–557, 1938.

[Goedel63] Kurt Gödel. On formally undecidable propositions of *Principia Mathematica* and related systems. Translated by B. Meltzer, with an introduction by R. B. Braithwaite. Basic Books Inc. Publishers, New York, 1963.

[Goldre2005] Derek Goldrei. Propositional and predicate calculus. A model of argument. London: Springer, 2005.

[Hamilt1988] A. G. Hamilton. Logic for mathematicians. Cambridge University Press, Cambridge, second edition, 1988.

[Jech2003] Thomas Jech. Set theory. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2003. The third millennium edition, revised and expanded. 134

[Kirby2019] Jonathan Kirby. An invitation to model theory. Cambridge University Press, Cambridge, 2019.

[Kunen2009] Kenneth Kunen. The foundations of mathematics, volume 19 of Studies in Logic (London). College Publications, London, 2009. Mathematical Logic and Foundations. 133

[PreDel2011] Alexander Prestel and Charles N. Delzell. Mathematical logic and model theory. Universitext. Springer, London, 2011. A brief introduction, Expanded translation of the 1986 German original.

[GoedelStanford] Panu Raatikainen. Gödel's Incompleteness Theorems `https://plato.stanford.edu/archives/spr2022/entries/goedel-incompleteness/`. In Edward N. Zalta, editor, The Stanford Encyclopedia of Philosophy. Metaphysics Research Lab, Stanford University, Spring 2022 edition, 2022. 24

[Rubin1985] Herman Rubin and Jean E. Rubin. Equivalents of the axiom of choice. II, volume 116 of Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Co., Amsterdam, 1985. 133

[Goedel] Marcus Tressl. Gödel's Incompleteness Theorems. Notes from an MSc course 2018. , December 2025. 16, 135

[ModTh] Marcus Tressl. Introduction to Model Theory. Notes from an MSc course 2011. , December 2025. 116, 135

[StoneBool] Marcus Tressl. Stone Duality for Boolean Algebras. A self contained introduction. , December 2025. 91

[Wagon1993] Stan Wagon. The Banach-Tarski paradox. Cambridge University Press, Cambridge, 1993. With a foreword by Jan Mycielski, Corrected reprint of the 1985 original. 134

Index

Homepage: https://personalpages.manchester.ac.uk/staff/Gareth.Jones-3/

Homepage: http://personalpages.manchester.ac.uk/staff/Marcus.Tressl/