1. Monday

We start with two algebraic results whose easiest and most natural proofs have model-theoretic content.

1.1. **Ax's Theorem.** A polynomial $f \in \mathbb{C}[X]$ defines the polynomial function $f : \mathbb{C} \to \mathbb{C}$ denoted by the same symbol. If $f \notin \mathbb{C}$, then f has a zero. Let $z \in \mathbb{C}$. Replacing f with $f - z$, we see that z is in the image of f, so f is onto. In particular we have:

$$\text{if } f \text{ is 1-1, then } f \text{ is onto.}$$

Ax proved a theorem generalizing the above fact to several variables. Let us take $f_1, \ldots, f_n \in \mathbb{C}[X_1, \ldots, X_n]$ and define

$$F : \mathbb{C}^n \to \mathbb{C}^n, \quad F(z_1, \ldots, z_n) := (f_1(z_1, \ldots, z_n), \ldots, f_n(z_1, \ldots, z_n)).$$

Theorem 1.1 (Ax)**.** *If F is 1-1, then F is onto.*

We will say that a field K satisfies Ax's theorem if Theorem 1.1 holds for K in place of $\mathbb{C}$. (Note that e.g. $\mathbb{Q}$ does not satisfy Ax's theorem, since the polynomial function X^3 is 1-1, but it is not onto.)

Step 1
Any finite field satisfies Ax's theorem.

Proof of Step 1. For self-functions on finite sets, 1-1 is equivalent to onto. □

Step 2
Let p be a prime number and $\mathbb{F}_p^{\text{alg}}$ the algebraic closure of $\mathbb{F}_p$. Then $\mathbb{F}_p^{\text{alg}}$ satisfies Ax's theorem.

Proof of Step 2. Let $f_1, \ldots, f_n \in \mathbb{F}_p^{\text{alg}}[X_1, \ldots, X_n]$. Since $\mathbb{F}_p^{\text{alg}}$ is the union of its finite subfields, there is $m \in \mathbb{N}$ such that for each $k \in \mathbb{N}$ we have $f_1, \ldots, f_n \in \mathbb{F}_{p^{km}}[X_1, \ldots, X_n]$. Therefore, by Step 1, for k, m as above $F(\mathbb{F}_{p^{km}}^n) = \mathbb{F}_{p^{km}}^n$. Since we can also represent $\mathbb{F}_p^{\text{alg}}$ as the following union

$$\mathbb{F}_p^{\text{alg}} = \bigcup_{k \in \mathbb{N}} \mathbb{F}_{p^{km}},$$

$F(\mathbb{F}_p^{\text{alg}}) = \mathbb{F}_p^{\text{alg}}$, so $\mathbb{F}_p^{\text{alg}}$ satisfies Ax's theorem. □

Step 3
$\mathbb{C}$ satisfies Ax's theorem.

Proof of Step 3. For any $d, n \in \mathbb{N}$ there is a sentence $\phi_{d,n}$ in the language of rings (formal definitions later) expressing Ax's theorem for polynomials in n variables of degree at most d. It is enough now to use the following model-theoretic theorem (to be proved later). □

Theorem 1.2. *For any sentence ϕ in the language of rings, ϕ is true in $\mathbb{C}$ if and only if ϕ is true in $\mathbb{F}_p^{\text{alg}}$ for infinitely many prime numbers p.*

1.2. **Nullstellensatz.** Let $f \in \mathbb{C}[X] \setminus \{0\}$. Then $f \in \mathbb{C}$ if and only if $(f) = \mathbb{C}[X]$. Therefore we have:

$$\text{if } (f) \neq C[X], \text{ then } f \text{ has a zero.}$$

Hilbert's Nullstellensatz generalizes the above fact to several variables.

Theorem 1.3 (**Hilbert's Nullstellensatz**)**.** *Let $f_1, \ldots, f_m \in \mathbb{C}[X_1, \ldots, X_n]$. If $(f_1, \ldots, f_m) \neq \mathbb{C}[X_1, \ldots, X_n]$, then there is $\bar{z} \in \mathbb{C}^n$ such that*

$$f_1(\bar{z}) = 0, \ldots, f_m(\bar{z}) = 0.$$

Proof. Let $I := (f_1, \ldots, f_m)$. Since $I \neq \mathbb{C}[X_1, \ldots, X_n]$, I extends to a maximal ideal $\mathfrak{m}$. Let $K := \mathbb{C}[X_1, \ldots, X_n]/\mathfrak{m}$. Let $\Phi : \mathbb{C} \to K^{\mathrm{alg}}$ denote the following composition:

$$\mathbb{C} \xrightarrow{\subseteq} \mathbb{C}[X_1, \ldots, X_n] \longrightarrow \mathbb{C}[X_1, \ldots, X_n]/\mathfrak{m} = K \xrightarrow{\subseteq} K^{\mathrm{alg}}.$$

Then Φ is a non-zero homomorphism of fields, so it is an embedding. Hence we can identify $\mathbb{C}$ with a subfield of K^{alg}. Let as consider a sentence ϕ in the language of rings with parameters from $\mathbb{C}$ saying that

$$\exists x_1, \ldots, x_n \quad f_1(x_1, \ldots, x_n) = 0 \wedge \ldots \wedge f_m(x_1, \ldots, x_n) = 0.$$

Then ϕ holds in K^{alg}, since we can take $X_i + \mathfrak{m}$ for x_i (Exercise 1). Nullstellensatz follows now from another model-theoretic theorem. □

Theorem 1.4. *Any extension of algebraically closed fields $F \subseteq M$ is* elementary, *i.e. for any sentence ϕ in the language of rings with parameters from F, ϕ holds in F if and only if ϕ holds in M.*

1.3. **Basic definitions: the case of fields.** We start with a concrete example. The notion of *language of rings* appeared above. It is

$$L_{\mathrm{r}} = \{+, \cdot, -, 0, 1\},$$

where $+$ and $\cdot$ are *binary function symbols*, $-$ is a *unary function symbols* and $0, 1$ are *constant symbols.*
An L_{r}-formula is a formula "obtained in a meaningful way" using:

- variables x_i, y_i for $i \in \mathbb{N}$ (occasionally other symbols may appear);
- constant symbols $0, 1$;
- binary function symbols $+, \cdot$, a unary function symbol $-$, and the equality symbol $=$;
- parentheses), (and logical connectives $\wedge, \vee, \neg$;
- quantifiers $\forall, \exists$.

The formal definition of a formula is inductive (induction on the "complexity of a formula") and a bit cumbersome, so we skip it. Note that using the logical connectives $\wedge, \vee, \neg$ we can also define other logical connectives as $\rightarrow, \leftrightarrow$ in the standard way.

Examples of L_{r}-formulas

$$\phi_1 : \quad \exists x \; x \cdot x = -1 \qquad \text{"a square root of } -1 \text{ exists"}$$
$$\phi_2 : \quad \forall x \; \exists y \; x = y \cdot y \qquad \text{"all square roots exist"}$$
$$\phi_3 : \quad \forall x \; \exists y \; x = (y \cdot y) \cdot y \qquad \text{"cube roots exist"}$$
$$\phi : \quad \exists y \; x = y \cdot y.$$

We will write the formula $\phi_{d,n}$ which appeared in the proof of Ax's theorem. For simplicity we take $d = 1, n = 2$ and skip some of the brackets below:

$$\forall a_0, a_1, a_2, b_0, b_1, b_2 \quad (\forall x_1, y_1, x_2, y_2 \quad (a_0 + a_1 \cdot x_1 + a_2 \cdot y_1 = a_0 + a_1 \cdot x_2 + a_2 \cdot y_2$$
$$\wedge \; b_0 + b_1 \cdot x_1 + b_2 \cdot y_1 = b_0 + b_1 \cdot x_2 + b_2 \cdot y_2) \quad \rightarrow \quad (x_1 = x_2 \wedge y_1 = y_2))$$
$$\rightarrow$$
$$(\forall z, v \; \exists x, y \quad a_0 + a_1 \cdot x + a_2 \cdot y = z \;\; \wedge \;\; b_0 + b_1 \cdot x + b_2 \cdot y = v).$$

In the formula ϕ above the variable x is *free* (i.e. not quantified) and in the formulas $\phi_1, \phi_2, \phi_3, \phi_{d,n}$ there are no free variables. It is better to denote the formula ϕ above by $\phi(x)$ pointing out the free variable x. If a formula has no free variables it is called a *sentence.* Any set of sentences is called a *theory.*

Examples of L_{r}-theories

- the theory of rings;
- the theory of fields;
- the theory of domains of characteristic 5;
- the theory of algebraically closed fields (infinitely many sentences required!).

Exercise 2: Write (the sentences in) the last two theories.

An L_r-*structure* is a set M together with two binary functions one unary function and two specified elements:

$$+^M, \cdot^M : M \times M \to M; \quad -^M : M \to M; \quad 0^M, 1^M \in M.$$

If ϕ is an L_r-sentence, then we can check whether ϕ *holds* (or is *satisfied*) in

$$\mathbf{M} := (M, +^M, \cdot^M, -^M, 0^M, 1^M)$$

or not. If T is an L_r-theory and each sentence of T holds in an L_r-structure $\mathbf{M}$, then we say that $\mathbf{M}$ is a *model* of T.

Examples

- If T is the theory of rings, then an L_r-structure $\mathbf{M}$ is a model of T if and only if $\mathbf{M}$ is a ring. Similarly for the other theories in the example above. (This looks tautological and reminds Tarski's example: "The sentence 'Snow is white' is true if and only if snow is white".)
- The sentence ϕ_1 does not hold in $\mathbb{R}$.
- The sentence ϕ_3 holds in $\mathbb{R}$.

Again it is cumbersome to write the formal definition of the satisfaction of an L_r-sentence in an L_r-structure (Tarski's definition of truth) but it conforms to common sense as in the examples above.

Notation
If ϕ is an L_r-sentence, T is an L_r-theory and $\mathbf{M}$ is an L_r-structure, then we write $\mathbf{M} \models \phi$ if ϕ holds in $\mathbf{M}$ and $\mathbf{M} \models T$ if $\mathbf{M}$ is a model of T.

1.4. **Basic definitions: the general case.** A *language* L consists of:

- a set of function symbols $\mathcal{F}$ and positive integers n_f (called the *arity* of f) for any $f \in \mathcal{F}$;
- a set of relation symbols $\mathcal{R}$ and positive integers n_R (called the *arity* of R) for any $R \in \mathcal{R}$;
- a set of constant symbols $\mathcal{C}$.

Examples

- language of rings above L_r (two function symbols of arity 2, one function symbol of arity 1 and two constants),
- language of orderings $L_\mathrm{o} = \{<\}$ (one relation symbol of arity 2),
- language of ordered rings $L_\mathrm{or} = \{+, -, \cdot, <, 0, 1\}$ (two function symbols of arity 2, one function symbol of arity 1 and two constant symbols)

Let us fix a language $L = (\mathcal{F}, \mathcal{R}, \mathcal{C})$. As in Section 1.3, we can produce L-formulas, L-sentences and L-theories from L.
By the cardinality of L, denoted $|L|$, we mean $|\mathcal{F}| + |\mathcal{R}| + |\mathcal{C}|$. We notice an easy result.

Lemma 1.5. *The set of L-formulas has cardinality $|L| + \aleph_0$.*

If we have an L-formula $\phi(x_1, \ldots, x_n)$ (as in Section 1.3, $x_1, \ldots, x_n$ are all the free variables in ϕ) and $c_1, \ldots, c_n \in \mathcal{C}$, then we can define an L-sentence $\phi(c_1, \ldots, c_n)$ plugging for each free

variable x_i the constant symbol c_i.
For any set A, we have the new language $L_A = (\mathcal{F}, \mathcal{R}, \mathcal{C}_A)$, where

$$\mathcal{C}_A = \mathcal{C} \cup \{c_a | a \in A\}.$$

The L_A-formulas are usually called *L-formulas with parameters from A.*

An *L-structure* is a set M together with:

- a function $f^M : M^{n_f} \to M$ for each $f \in \mathcal{F}$;
- a subset $R^M \subseteq M^{n_R}$ for each $R \in \mathcal{R}$;
- an element $c^M \in M$ for each $c \in \mathcal{C}$.

We denote

$$\mathbf{M} := (M, f^M, R^M, c^M)_{f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C}}$$

and call M the *universe* of the L-structure $\mathbf{M}$, and f^M, R^M, c^M the *interpretations* of the language symbols f, R, c in the structure $\mathbf{M}$.
As in Section 1.3, if we have an L-sentence ϕ (resp. an L-theory T), we can check whether ϕ holds in an L-structure $\mathbf{M}$ (resp. whether $\mathbf{M}$ is a *model* of T).

Examples

- $(\mathbb{Q}, <)$ is an L_{o}-structure. It satisfies for example the following L_{o}-sentence (density):
$$\forall x, y\ \exists z \quad x < y \ \to \ (x < z \ \wedge z < y).$$
- $(\mathbb{R}, +, -, \cdot, <, 0, 1)$ is an L_{or}-structure. It satisfies for example the following sentence (squares are non-negative)
$$\forall x, y \quad x = y \cdot y \ \to \ (x > 0 \ \vee \ x = 0).$$

If $\mathbf{M}$ is an L-structure and $A \subseteq M$, then $\mathbf{M}$ is also naturally an L_A-structure. We define:

$$\mathrm{Th}(\mathbf{M}) := \{\phi \mid \phi \text{ is an } L\text{-sentence and } \mathbf{M} \models \phi\},$$
$$\mathrm{Th}_A(\mathbf{M}) := \{\phi \mid \phi \text{ is an } L_A\text{-sentence and } \mathbf{M} \models \phi\}.$$

Definition 1.6. We say that two L-structures $\mathbf{M}$ and $\mathbf{N}$ are *elementarily equivalent* (denoted $\mathbf{M} \equiv \mathbf{N}$), if $\mathrm{Th}(\mathbf{M}) = \mathrm{Th}(\mathbf{N})$.

2. Tuesday

We will prove today the Compactness Theorem, which is the starting point of any model-theoretic considerations. Let us fix a language $L = (\mathcal{F}, \mathcal{R}, \mathcal{C})$, an L-theory T and an L-sentence ϕ.

Theorem 2.1 (Compactness Theorem). *Let $\kappa := \aleph_0 + |L|$. If each finite subset of T has a model, then T has a model of cardinality at most κ.*

Before the proof we need several definitions:

- ϕ is a *logical consequence* of T, denoted $T \models \phi$, if for any L-structure $\mathbf{M}$, $\mathbf{M} \models T$ implies $\mathbf{M} \models \phi$.
- T is *maximal* if for any L-sentence α either $\alpha \in T$ or $\neg\alpha \in T$.
- T is *finitely satisfiable* if each finite subset of T has a model.
- T has the *witness property* if whenever $\alpha(x)$ is an L-formula with one free variable, then there is $c \in \mathcal{C}$ such that
$$[(\exists x\ \alpha(x)) \ \to \ \alpha(c)] \in T.$$

Note that for any L-structure $\mathbf{M}$, the theory $\mathrm{Th}(\mathbf{M})$ is maximal.

Lemma 2.2. *Let T be finitely satisfiable and maximal. If $\Delta \subseteq T$ is finite and $\Delta \models \phi$, then $\phi \in T$.*

Proof. Assume not, i.e. $\phi \notin T$. Since T is maximal, $\neg\phi \in T$. For any L-structure $\mathbf{M}$, if $\mathbf{M} \models \Delta$ then $\mathbf{M} \models \phi$ (since $\Delta \models \phi$). Hence $\Delta \cup \{\neg\phi\}$ is a finite subset of T without a model, which contradicts the finite satisfability of T. □

Lemma 2.3. *If T is finitely satisfiable, maximal, and has the witness property, then T has a model of cardinality at most $|\mathcal{C}|$.*

Proof. For $c_1, c_2 \in \mathcal{C}$ let us define:

$$c_1 \sim c_2 \quad \text{iff} \quad \text{the formula } c_1 = c_2 \text{ belongs to } T.$$

Claim 1
The relation $\sim$ is an equivalence relation on $\mathcal{C}$.

Proof of Claim 1. Let $c_1, c_2, c_3 \in \mathcal{C}$ and assume that $c_1 \sim c_2, c_2 \sim c_3$. Then the sentences $c_1 = c_2$ and $c_2 = c_3$ belong to T, which we write for example "$[c_1 = c_2] \in T$". Clearly we have:

$$\{[c_1 = c_2], [c_2 = c_3]\} \models [c_1 = c_3].$$

By 2.2, the sentence $c_1 = c_3$ belongs to T. Hence $c_1 \sim c_3$.
Similarly we show that $c_1 \sim c_1$, and that $c_1 \sim c_2$ implies $c_2 \sim c_1$. □

Let $M := \mathcal{C}/\sim$. Clearly $|M| \leqslant |\mathcal{C}|$. We need to define the interpretations of the elements of $\mathcal{F}, \mathcal{R}$ and $\mathcal{C}$ in the set M to obtain the structure $\mathbf{M}$ with universe M.
For $c \in \mathcal{C}$, we define $c^M := c/\sim$.
Let $R \in \mathcal{R}$, $n := n_R$ and $c_1, d_1, \ldots, c_n, d_n \in \mathcal{C}$.

Claim 2
If $c_1 \sim d_1, \ldots, c_n \sim d_n$, then $R(c_1, \ldots, c_n) \in T$ iff $R(d_1, \ldots, d_n) \in T$.

Proof of Claim 2. It is enough to show one implication. Assume that $R(c_1, \ldots, c_n)$ belongs to T. The sentences $c_1 = d_1, \ldots, c_n = d_n$ also belong to T. Clearly:

$$\{R(c_1, \ldots, c_n), [c_1 = d_1], \ldots, [c_n = d_n]\} \models R(d_1, \ldots, d_n).$$

By 2.2, the sentence $R(d_1, \ldots, d_n)$ belongs to T. □

By Claim 2, we can define

$$(c_1/\sim, \ldots, c_n/\sim) \in R^M \quad \text{iff} \quad R(c_1, \ldots, c_n) \in T.$$

Let $f \in \mathcal{F}$, $n := n_f$ and $c_1, \ldots, c_n \in \mathcal{C}$. Since T has the witness property, there is $c \in \mathcal{C}$ such that

$$[(\exists x\ f(c_1, \ldots, c_n) = x) \ \rightarrow\ f(c_1, \ldots, c_n) = c] \in T.$$

Claim 3
The sentence $f(c_1, \ldots, c_n) = c$ belongs to T

Proof of Claim 3. Suppose not and we will reach a contradiction. Since T is maximal and $[f(c_1, \ldots, c_n) = c] \notin T$, then $\neg[f(c_1, \ldots, c_n) = c] \in T$. Since

$$[(\exists x\ f(c_1, \ldots, c_n) = x) \ \rightarrow\ f(c_1, \ldots, c_n) = c] \in T$$

and T is finitely satisfiable, there is an L-structure $\mathbf{M}$ such that:

$$\mathbf{M} \models \{\neg[f(c_1, \ldots, c_n) = c], [(\exists x\ f(c_1, \ldots, c_n) = x) \ \rightarrow\ f(c_1, \ldots, c_n) = c]\}.$$

But it means that

$$f^M\left(c_1^M, \ldots, c_n^M\right) \neq c^M \quad \text{and} \quad f^M\left(c_1^M, \ldots, c_n^M\right) = c^M,$$

which is a contradiction. □

Using 2.2 one proves (similarly as in Claims 1 and 2) that for any $d, d_1, \ldots, d_n \in \mathcal{C}$ if $c_1 \sim d_1, \ldots, c_n \sim d_n$ and sentences $f(c_1, \ldots, c_n) = c$, $f(d_1, \ldots, d_n) = d$ belong to T, then $c \sim d$. Hence, we define for $c, c_1, \ldots, c_n \in \mathcal{C}$ the following

$$f^M(c_1/\sim, \ldots, c_n/\sim) = c/\sim \quad \text{iff} \quad [f(c_1, \ldots, c_n) = c] \in T.$$

By Claim 3, for any $c_1, \ldots, c_n \in \mathcal{C}$, there is $c \in \mathcal{C}$ such that $[f(c_1, \ldots, c_n) = c] \in T$. Therefore, the function f^M is well-defined.

We have defined an L-structure $\mathbf{M}$. Let $\psi(x_1, \ldots, x_n)$ be an L-formula. Using 2.2 again, it can be shown by induction on the complexity of the formula $\psi(x_1, \ldots, x_n)$ that for any $c_1, \ldots, c_n \in \mathcal{C}$ we have

$$\mathbf{M} \models \psi(c_1/\sim, \ldots, c_n/\sim) \quad \text{iff} \quad \psi(c_1, \ldots, c_n) \in T.$$

In particular $\mathbf{M} \models T$. □

We proceed to show that without loss we can assume T is maximal and has the witness property.

Lemma 2.4. *If T is finitely satisfiable, then there is a language $L' \supseteq L$ such that $|L'| = |L| + \aleph_0$ and an L'-theory $T' \supseteq T$ such that T' is finitely satisfiable and has the witness property.*

Proof. Let us define a new language

$$\mathcal{C}_1 := \mathcal{C} \cup \{c_\phi \mid \phi(x) \text{ is an } L\text{-formula}\}, \quad L_1 := (\mathcal{F}, \mathcal{R}, \mathcal{C}_1),$$

and an L_1-theory

$$T_1 := T \cup \{(\exists x\ \phi(x)) \to \phi(c_\phi) \mid \phi(x) \text{ is an } L\text{-formula}\}.$$

Claim
T_1 is finitely satisfiable.

Proof of Claim. Take Δ, a finite subset of T_1, and let $\Delta_0 := \Delta \cap T$. Since T is finitely satisfiable, there is an L-structure $\mathbf{M}$ which is a model of Δ_0. We will expand $\mathbf{M}$ to an L_1-structure which will be a model of Δ. For any L-formula $\phi(x)$ we need to find a right $c_\phi^M \in M$. If $\mathbf{M} \models \exists x \phi(x)$, then we set $c_\phi^M \in M$ such that $\mathbf{M} \models \phi(c_\phi^M)$. If $\mathbf{M} \models \neg\exists x \phi(x)$, then we set $c_\phi^M \in M$ arbitrarily. □

Now we define a language L_2 and an L_2-theory T_2 such that T_2 is finitely satisfiable and "witnesses L_1-formulas". We continue inductively this process and take $L' := \bigcup L_n$ and $T' := \bigcup T_n$. By Lemma 1.5, $|L'| = |L| + \aleph_0$. By Claim, T' is finitely satisfiable and by the construction, T' has the witness property. □

Lemma 2.5. *If T is finitely satisfiable, then there is $T^* \supseteq T$, a finitely satisfiable and maximal L-theory.*

Proof. Let ϕ be an L-sentence.
Claim
$T \cup \{\phi\}$ is finitely satisfiable or $T \cup \{\neg\phi\}$ is finitely satisfiable.

Proof of Claim. Assume $T \cup \{\phi\}$ is not finitely satisfiable. Then, there is a finite $\Delta \subseteq T$ such that $\Delta \cup \{\phi\}$ has no model. Therefore, for any L-structure $\mathbf{M}$, if $\mathbf{M} \models \Delta$, then $\mathbf{M} \models \neg\phi$. Let us take a finite subset $\Sigma \subseteq T$. Since T is finitely satisfiable, there is an L-structure $\mathbf{M}$ such that $\mathbf{M} \models \Sigma \cup \Delta$. By the above considerations, $\mathbf{M} \models \neg\phi$. Hence $\mathbf{M} \models \Sigma \cup \{\neg\phi\}$, so $T \cup \{\neg\phi\}$ is finitely satisfiable. □

Exercise 3: Lemma 2.5 follows from Claim and Zorn's lemma. □

Proof of Compactness Theorem. By Lemma 2.4, there is a language $L' \supseteq L$ of cardinality κ and an L'-theory $T' \supseteq T$ such that T' is finitely satisfiable and has the witness property. By Lemma 2.5, there is an L'-theory $T^* \supseteq T'$ which is finitely satisfiable and maximal. Since T' has the witness property, T^* has the witness property as well (as a larger theory). By Lemma 2.3, T^* has a model $\mathbf{M}$ of cardinality at most κ. Then $\mathbf{M}$ (or formally its restriction to the language L) is also a model of T. □

We say that T *proves* ϕ, denoted $T \vdash \phi$, if there is a "finite logical proof" showing that ϕ follows from a finite subset of T (for example $\{\alpha, \phi\} \vdash \alpha \wedge \phi$). The following famous result is closely related to the Compactness Theorem.

Theorem 2.6 (**Gödel's Completeness Theorem**). *$T \vdash \phi$ if and only if $T \models \phi$.*

Gödel proved the Compactness Theorem using the Completeness Theorem.

Exercise 4: Assuming the Completeness Theorem prove that the following are equivalent:

(1) T has a model.
(2) T does not prove a contradictory statement, i.e. it is not true that $T \vdash \phi \wedge \neg\phi$.

T is *consistent*, if it satisfies the equivalent conditions above. By Compactness Theorem, T is consistent if and only if it is finitely satisfiable.
T is *complete*, if T is consistent and for any L-sentence ϕ we have $T \models \phi$ or $T \models \neg\phi$. Of course maximal theories are complete, but completeness is a more meaningful notion.

Exercise 5: Prove that the following are equivalent:

(1) T is complete;
(2) For any L-structures $\mathbf{M}, \mathbf{N}$ if $\mathbf{M} \models T$ and $\mathbf{N} \models T$, then $\mathbf{M} \equiv \mathbf{N}$.

Exercise 6: Assume that T is complete and ϕ is a sentence. Show that:

(1) If $M \models T$, then $M \models \phi$ iff $T \models \phi$;
(2) $T \models \phi$ iff $T \cup \{\phi\}$ is consistent.

3. Wednesday

Today we prove the model-theoretic theorems from Monday which were necessary for Ax's theorem and the Nullstellensatz.
Let $L = (\mathcal{F}, \mathcal{R}, \mathcal{C})$ be a language,

$$\mathbf{M} = (M, f^M, R^M, c^M)_{f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C}}, \ \ \mathbf{N} = (N, f^N, R^N, c^N)_{f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C}}$$

be L-structures and $\Phi : M \to N$. We say that Φ is an *L-monomorphism* between $\mathbf{M}$ and $\mathbf{N}$, denoted $\Phi : \mathbf{M} \to \mathbf{N}$, if it is a one-to-one function preserving the interpretations of all the function, relation and constant symbols of L, i.e.

- for each $f \in \mathcal{F}$ of arity n and all $m_1, \ldots, m_n \in M$ we have:
$$\Phi(f^M(m_1, \ldots, m_n)) = f^N(\Phi(m_1), \ldots, \Phi(m_n));$$
- for each $R \in \mathcal{F}$ of arity n and all $m_1, \ldots, m_n \in M$ we have:
$$(m_1, \ldots, m_n) \in R^M \quad \text{iff} \quad (\Phi(m_1), \ldots, \Phi(m_n)) \in R^N;$$
- for each $c \in \mathcal{C}$ we have:
$$\Phi(c^M) = c^N.$$

We say that Φ is an *L-isomorphism* between $\mathbf{M}$ and $\mathbf{N}$ if Φ is a bijection and an L-monomorphism (then Φ^{-1} is an L-monomorphism as well). As usual, if there is an L-isomorphism between $\mathbf{M}$ and $\mathbf{N}$, we denote $\mathbf{M} \cong \mathbf{N}$ (or $\mathbf{M} \cong_L \mathbf{N}$) and this is an "equivalence relation".

The following lemma (saying that "isomorphisms preserve the truth") can be proven by induction on the complexity of formulas.

Lemma 3.1. *Let $\phi(x_1, \ldots, x_n)$ be an L-formula and $m_1, \ldots, m_n \in M$. If $\Phi : \mathbf{M} \to \mathbf{N}$ is an isomorphism, then we have*

$$\mathbf{M} \models \phi(m_1, \ldots, m_n) \quad \textit{iff} \quad \mathbf{N} \models \phi(\Phi(m_1), \ldots, \Phi(m_n)).$$

$\mathbf{M}$ is an *L-substructure* of $\mathbf{N}$ if $M \subseteq N$ and the inclusion is an L-monomorphism, i.e. we have $f^M \subseteq f^N, R^M = R^N \cap M^{n_R}, c^M = c^N$ for all $f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C}$.

Remark 3.2. Let $M_0 \subseteq M$. We say that M_0 is *closed under $\mathcal{F}$ and $\mathcal{C}$*, if for all $f \in \mathcal{F}$ we have $f^M(M_0^{n_f}) \subseteq M_0$ and for all $c \in \mathcal{C}$, we have $c^M \in M_0$. If M_0 is closed under $\mathcal{F}$ and $\mathcal{C}$, then M_0 together with the restrictions of all the interpretations of elements of L is an L-substructure of $\mathbf{M}$. Abusing the language (the one we speak) a little bit, we sometimes say that a subset $M_0 \subseteq M$ is an L-substructure of $\mathbf{M}$ if it is closed under $\mathcal{F}$ and $\mathcal{C}$ (compare with group theory, ring theory, etc.). If $\Phi : \mathbf{M} \to \mathbf{N}$ is an L-monomorphism, then $\Phi(M)$ is closed under $\mathcal{F}$ and $\mathcal{C}$, so $\Phi(M)$ becomes an L-substrucutre of $\mathbf{N}$. Clearly, Φ becomes than an L-isomorphism between $\mathbf{M}$ and $\Phi(M)$. If L is a purely relational language, then a substructure is the same as a subset.

Example

- $(\mathbb{N}, <)$ is an L_{o}-substructure of $(\mathbb{Q}, <)$, $(\mathbb{Q}, <)$ is an L_{o}-substructure of $(\mathbb{R}, <)$;
- $(\mathbb{Q}, +, -, \cdot)$ is an L_{r}-substructure of $(\mathbb{R}, +, -, \cdot)$.
- If $\mathbf{N}$ is a ring and $\mathbf{M}$ is an L_{r}-substructure of $\mathbf{N}$, then $\mathbf{M}$ is a (sub)ring as well. (This is the reason why we have also included the unary symbol "$-$" in the language L_{r}.)

Definition 3.3. We say that $\mathbf{M}$ is an *elementary substructure* of $\mathbf{N}$ (denoted $\mathbf{M} \preccurlyeq \mathbf{N}$), if $\mathbf{M}$ is a substructure of $\mathbf{N}$ and for any L-sentence ϕ with parameters from M, $\mathbf{M} \models \phi$ iff $\mathbf{N} \models \phi$.

The above definition can be rephrased. If $\mathbf{M}$ is a substructure of $\mathbf{N}$, then the following are equivalent:

(1) $\mathbf{M} \preccurlyeq \mathbf{N}$;
(2) $\mathrm{Th}_M(\mathbf{M}) = \mathrm{Th}_M(\mathbf{N})$.

In particular, if $\mathbf{M} \preccurlyeq \mathbf{N}$, then $M \equiv N$. We will see below that the converse need not hold.

Non-examples

- $\mathbb{R}$ is not an elementary substructure $\mathbb{C}$, since the sentence ϕ_1 from Section 1.3 holds in $\mathbb{C}$ but it does not hold in $\mathbb{R}$. Hence these structures are not even elementarily equivalent.
- $(\mathbb{N}, <)$ is not an elementary substructure of $(\mathbb{Q}, <)$ since the ordering on $\mathbb{N}$ is not dense. Hence these structures are not even elementarily equivalent.
- $(\mathbb{N}_{>0}, <)$ is not an elementary substructure of $(\mathbb{N}, <)$ (1 is the smallest element in the substructure) but we even have

  $$(\mathbb{N}_{>0}, <) \cong (\mathbb{N}, <),$$

  so, by 3.1, we also have $(\mathbb{N}_{>0}, <) \equiv (\mathbb{N}, <)$.

It is difficult now to give examples of elementary substructures. The following theorem provides many such in a general context.

Theorem 3.4 (**Upward Löwenheim-Skolem Theorem**)**.** *Let $\mathbf{M}$ be an infinite L-structure and $\kappa \geqslant |M| + |L|$. Then there is $\mathbf{N} \succcurlyeq \mathbf{M}$ such that $|N| = \kappa$.*

Proof. Let us expand the language L_M to L' by adding new constant symbols $\{c_i | i < \kappa\}$ and define an L'-theory:

$$T := \mathrm{Th}_M(\mathbf{M}) \cup \{c_i \neq c_j | i < j < \kappa\}.$$

Since M is infinite, we can easily make $\mathbf{M}$ a model of any finite subset of T. By the compactness theorem, T has a model $\mathbf{N}$ of cardinality at most κ. Hence $|N| = \kappa$ (new constants!) and $\mathbf{N}$ (or rather its restriction to the language L) is an elementary extension of $\mathbf{M}$. $\square$

We will sometimes denote a structure by the same symbol as its universe, for example in the proof below.

Proof of Theorem 1.4. Let us take $\kappa > |M|$. By Theorem 3.4, there are elementary extensions $F \preccurlyeq F', M \preccurlyeq M'$ such that $|F'| = |M'| = \kappa$. Hence we have extensions of algebraically closed fields $F \subseteq F', F \subseteq M'$. By the choice of κ, we have:

$$\mathrm{trdeg}_F\, F' = \mathrm{trdeg}_F\, M'.$$

Exercise 7: There is an F-isomorphism $\Phi : F' \to M'$.
Hence we have a commutative diagram:

$$\begin{array}{ccc} F' & \xrightarrow{\Phi} & M' \\ {\scriptstyle\preccurlyeq}\uparrow & & {\scriptstyle\preccurlyeq}\uparrow \\ F & \xrightarrow{\subseteq} & M. \end{array}$$

Let us take an L_{r}-formula $\phi(x_1, \ldots, x_n)$ and $t_1 \ldots, t_n \in F$. Since $F \preccurlyeq F'$, "Φ preserves the truth" (3.1) and $\Phi(t_1) = t_1, \ldots, \Phi(t_n) = t_n$ (Φ is over F), we get that:

$$F \models \phi(t_1 \ldots, t_n) \quad \text{iff} \quad M' \models \phi(t_1 \ldots, t_n).$$

Since $M \preccurlyeq M'$, we get that:

$$M \models \phi(t_1 \ldots, t_n) \quad \text{iff} \quad M' \models \phi(t_1 \ldots, t_n).$$

Therefore $F \preccurlyeq M$. $\square$

Let ACF denote the L_{r}-theory of algebraically closed fields and for p, a prime number or 0, ACF_p denote the L_{r}-theory of algebraically closed fields of characteristic p.

Theorem 3.5. ACF_p *is complete.*

Proof. Let us take two algebraically closed fields K_1, K_2 of characteristic p and their prime subfields F_1, F_2. Clearly, $F_1^{\mathrm{alg}} \cong F_2^{\mathrm{alg}}$. By 1.4, $F_1^{\mathrm{alg}} \preccurlyeq K_1$ and $F_2^{\mathrm{alg}} \preccurlyeq K_2$. In particular we have (using 3.1):

$$\mathrm{Th}(K_1) = \mathrm{Th}(F_1^{\mathrm{alg}}) = \mathrm{Th}(F_2^{\mathrm{alg}}) = \mathrm{Th}(K_2).$$

Hence any two models of ACF_p are elementarily equivalent, so ACF_p is complete (see Exercise 5). $\square$

We can now state and prove an extended version of Theorem 1.2.

Theorem 3.6 (**Lefschetz Principle**). *Let ϕ be an L_r-sentence. The following are equivalent:*

1. *For almost all prime numbers p, $\mathbb{F}_p^{\mathrm{alg}} \models \phi$;*
2. *For infinitely many prime numbers p, $\mathbb{F}_p^{\mathrm{alg}} \models \phi$;*
3. $\mathrm{ACF}_0 \models \phi$;
4. $\mathbb{C} \models \phi$.

Proof. The implication (1) $\Rightarrow$ (2) is obvious.
We will prove (2) $\Rightarrow$ (3). By Exercise 6(2), it is enough to show that $\mathrm{ACF}_0 \cup \{\phi\}$ is consistent. Let T_0 be a finite subset of $\mathrm{ACF}_0 \cup \{\phi\}$. For $n \in \mathbb{N}_{>0}$, let ϕ_n be the following L_{r}-sentence:

$$\neg(1 + \ldots + 1 = 0) \quad (+ \text{ taken } n \text{ times}).$$

Since $\mathrm{ACF}_0 = \mathrm{ACF} \cup \{\phi_n | n \in \mathbb{N}_{>0}\}$, there is $N \in \mathbb{N}$ such that

$$T_0 \subset \mathrm{ACF} \cup \{\phi_n | n < N\} \cup \{\phi\}.$$

Let us take a prime number p such that $p > N$ and $\mathbb{F}_p^{\mathrm{alg}} \models \phi$. Then $\mathbb{F}_p^{\mathrm{alg}} \models T_0$, so $\mathrm{ACF}_0 \cup \{\phi\}$ is finitely satisfiable.
The equivalence (3) $\Leftrightarrow$ (4) is given by Exercise 6(1).
We will prove (3) $\Rightarrow$ (1). Assume that (1) does not hold, i.e. there are infinitely many prime numbers p such that $\mathbb{F}_p^{\mathrm{alg}} \models \neg\phi$. By the already proven implication (2) $\Rightarrow$ (3), we get that $\mathrm{ACF}_0 \models \neg\phi$, so (3) does not hold (since ACF_0 is consistent). $\square$

4. Friday

Today we will find a criterium under which formulas have a particularly simple form. Let us fix a language $L = (\mathcal{F}, \mathcal{R}, \mathcal{C})$ and an L-structure $\mathbf{M}$. First we look at a notion which is somehow dual to the notion of a formula. Let $n > 0$ and $\bar{x} := (x_1, \ldots, x_n)$.

Definition 4.1. For an L_M-formula $\phi(\bar{x})$ let

$$\phi(\bar{x})^{\mathbf{M}} := \{\bar{m} \in M^n \mid \mathbf{M} \models \phi(\bar{m})\}.$$

A subset $X \subseteq M^n$ is called *definable* (in $\mathbf{M}$ over M), if there is an L_M-formula $\phi(\bar{x})$ such that $X = \phi(\bar{x})^M$.

Remark 4.2. In the definition above, there is a *subset of M^n definable in the structure* $\mathbf{M}$ *with parameters from M*. It is not good to confuse those three difference appearances of M.

Before seeing examples, let us note some basic properties of definable sets. If we have L_M-formulas $\phi(\bar{x}), \alpha(\bar{x})$, then:

$$(\phi(\bar{x}) \vee \alpha(\bar{x}))^{\mathbf{M}} = \phi(\bar{x})^{\mathbf{M}} \cup \alpha(\bar{x})^{\mathbf{M}};$$

$$(\phi(\bar{x}) \wedge \alpha(\bar{x}))^{\mathbf{M}} = \phi(\bar{x})^{\mathbf{M}} \cap \alpha(\bar{x})^{\mathbf{M}};$$

$$(\neg\phi(\bar{x}))^{\mathbf{M}} = M^n \setminus \phi(\bar{x})^{\mathbf{M}};$$

$$(\exists x_{k+1}, \ldots, x_n \ \phi(\bar{x}))^{\mathbf{M}} = \pi^n_k(\phi(\bar{x})^{\mathbf{M}}),$$

where $\pi^n_k : M^n \to M^k$ is the projection on the first k coordinates.
Hence the conjunction corresponds to the intersection, the disjunction to the union, the negation to the complement, and the existential quantifier to the coordinate projection.
Basic definable sets are the graphs of f^M for $f \in \mathcal{F}$, the subsets R^M for $R \in \mathcal{R}$, the points c^M for $c \in \mathcal{C}$ and a bit more complicated sets as

$$\{(a, b) \in M^2 \mid \mathbf{M} \models R^M(f_1^M(f_2^M(a)), f_3^M(b))\}.$$

(I skip the technical definition of the notion of *term* here.) Other definable sets come from these basic ones after applying Boolean combinations (i.e. unions, intersections and complements) and projections. The following question arises: how many of these operations (most importantly projections) have to be taken to obtain all the definable sets?

Examples

- If K is a field (considered as an L_{r}-structure), then any set of solutions of a system of polynomial equations in n variables is a definable subset of K^n (e.g. for $n = 2$ we have parabolas, hyperbolas, etc.). Such a set of solutions is called a *Zariski closed set*. A Boolean combination of Zariski closed sets is still a definable set, such a set is called a *constructible set*.
- For any L_{o}-structure $(X, <)$ and $x, y \in X$, the interval (x, y) is a definable set.
- The order $<^{\mathbb{R}}$ is definable in the L_{r}-structure $\mathbb{R}$. Hence in a way, the L_{or}-structure $\mathbb{R}$ is definable in the L_{r}-structure $\mathbb{R}$.
- $\mathbb{N}$ is definable in $\mathbb{Z}$.
- $\mathbb{Z}$ is definable in $\mathbb{Q}$.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are not definable in $\mathbb{C}$.
- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ are not definable in $\mathbb{R}$.

Theorem 4.3 (**Chevalley's Theorem**). *If K is an algebraically closed field, then a projection of a constructible set is again a constructible set.*

The above theorem (to be proved later) says that in the case of algebraically closed fields the above-mentioned process terminates very quickly, actually no projections are needed at all! In such a case we say that the theory of an algebraically closed field, ACF_p, has quantifier elimination (definition below).

Definition 4.4. An L-theory T has *quantifier elimination* if any L-formula $\phi(\bar{x})$ is *equivalent modulo* T with a quantifier-free formula, i.e. there is a formula $\alpha(\bar{x})$ having no quantifiers such that

$$T \models \forall \bar{x}\ (\phi(\bar{x}) \leftrightarrow \alpha(\bar{x})).$$

We proceed to find a checkable criterium for quantifier elimination, which will serve to prove Chevalley's theorem. We will need some more notions.

Definition 4.5. Let $\mathbf{M}$ be an L-structure and $\bar{m} \in M^n$.

- An (L-)*type* $q(\bar{x})$ is any set of formulas with free variables $\bar{x}$.
- If $q(\bar{x})$ is a type, then the *set of realizations* of $q(\bar{x})$ in $\mathbf{M}$ is

$$q(\bar{x})^{\mathbf{M}} := \bigcap_{\phi(\bar{x}) \in q(\bar{x})} \phi(\bar{x})^{\mathbf{M}}.$$

- A type $q(\bar{x})$ is *finitely satisfiable* in $\mathbf{M}$, if for any finite $q_0(\bar{x}) \subseteq q(\bar{x})$, the set $q_0(\bar{x})^{\mathbf{M}}$ is non-empty.
- The *quantifier-free type* of $\bar{m}$ in $\mathbf{M}$ is the following collection of L-formulas:

$$\mathrm{qftp}^{\mathbf{M}}(\bar{m}) := \{\phi(\bar{x}) \mid \mathbf{M} \models \phi(\bar{m}) \text{ and } \phi(\bar{x}) \text{ is quantifier-free}\}.$$

- The *complete type* of $\bar{m}$ in $\mathbf{M}$ is the following collection of L-formulas:

$$\mathrm{tp}^{\mathbf{M}}(\bar{m}) := \{\phi(\bar{x}) \mid \mathbf{M} \models \phi(\bar{m})\}.$$

Remark 4.6. Let $\mathbf{M}$ be an L-substructure of $\mathbf{N}$ and $\bar{a} \in M^n$.

(1) It can be shown by induction on the complexity of formulas that $\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{N}}(\bar{a})$, e.g. for any $f_1, f_2 \in \mathcal{F}; R_1, R_2 \in \mathcal{R}$ we clearly have

$$f_1^M(\bar{a}) = f_2^M(\bar{a}) \quad \text{iff} \quad f_1^N(\bar{a}) = f_2^N(\bar{a}),$$
$$\bar{a} \in R_1^M \quad \text{iff} \quad \bar{a} \in R_2^M.$$

(2) If $\mathbf{M} \preccurlyeq \mathbf{N}$, then $\mathrm{tp}^{\mathbf{M}}(\bar{a}) = \mathrm{tp}^{\mathbf{N}}(\bar{a})$, but in general the complete types need not be equal. For example $\mathrm{tp}^{\mathbb{R}}(-1) \neq \mathrm{tp}^{\mathbb{C}}(-1)$.

(3) Actually, if $\mathbf{M}$ is a substructure of $\mathbf{N}$, then $\mathbf{M} \preccurlyeq \mathbf{N}$ if and only if for all $\bar{a} \in M^n$ (and all $n > 0$) we have $\mathrm{tp}^{\mathbf{M}}(\bar{a}) = \mathrm{tp}^{\mathbf{N}}(\bar{a})$.

We can formulate now an intuitive (but still not easy to check) criterium for quantifier elimination.

Lemma 4.7. *An L-theory T has quantifier elimination if and only if, for all models $\mathbf{M}$ of T, all $n \in \mathbb{N}$ and $\bar{a}, \bar{b} \in M^n$ we have:*

$$\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{M}}(\bar{b}) \quad \Rightarrow \quad \mathrm{tp}^{\mathbf{M}}(\bar{a}) = \mathrm{tp}^{\mathbf{M}}(\bar{b}).$$

Proof. Exercise 8: The (easy) left-to-right implication.
Assume that T does not have quantifier elimination and take an L-formula $\phi(\bar{x})$ which is not equivalent modulo T with a quantifier free formula. We will find in two steps $\mathbf{M} \models T$ and $\bar{a}^M, \bar{b}^M \in M^n$ such that

$$\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{M}}(\bar{b}) \ \text{ and } \ \mathrm{tp}^{\mathbf{M}}(\bar{a}) \neq \mathrm{tp}^{\mathbf{M}}(\bar{b}).$$

Let L' be L expanded by new constant symbols $\bar{a}, \bar{b}$. Since $\phi(\bar{x})$ is not equivalent modulo T to a quantifier free formula, the following L'-theory is consistent:

$$T \cup \{\phi(\bar{a}) \wedge \neg\alpha(\bar{a}) \mid T \models \forall \bar{x}\ (\alpha(\bar{x}) \to \phi(\bar{x})) \text{ and } \alpha(\bar{x}) \text{ is quant.-free}\}.$$

Let $(\mathbf{N}, \bar{a}^N) \models T_{\bar{a}}$, where $T_{\bar{a}}$ is the above L'-theory. The first step is completed, in the second one we will find an appropriate $\bar{b}$. Since $(\mathbf{N}, \bar{a}^N) \models T_{\bar{a}}$, the following L'-theory is consistent:

$$T_{\bar{a}} \cup \{\alpha(\bar{b}) \wedge \neg\phi(\bar{b}) \mid \alpha(\bar{x}) \in \mathrm{qftp}^{\mathbf{N}}(\bar{a}^N)\}.$$

Let $(\mathbf{M}, \bar{a}^M, \bar{b}^M)$ be a model of this theory, so $\mathrm{qftp}^{\mathbf{M}}(\bar{a}^M) = \mathrm{qftp}^{\mathbf{M}}(\bar{b}^M)$. However, $\mathbf{M} \models \phi(\bar{a})$ and $\mathbf{M} \models \neg\phi(\bar{b})$, hence $\mathrm{tp}^{\mathbf{M}}(\bar{a}^M) \neq \mathrm{tp}^{\mathbf{M}}(\bar{b}^M)$. □

In the next lemma we find a general (independent from any complete theory T) criterium for checking equality of quantifier-free types.

Lemma 4.8. *Let $\mathbf{M}, \mathbf{N}$ be L-structures, $\bar{a} \in M^n$ and $\bar{b} \in N^n$. The following are equivalent:*

1. *there is an L-substructure $\mathbf{M}_0 \subseteq \mathbf{M}$ containing $\bar{a}$ and an L-monomorphism $\Phi : \mathbf{M}_0 \to \mathbf{N}$ such that $\Phi(\bar{a}) = \bar{b}$;*
2. $\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{N}}(\bar{b})$.

Proof. Let us assume (1) and set $N_0 := \Phi(M_0)$. Then $\mathbf{N}_0$ (i.e. N_0 with the restrictions of all f^N, R^N, c^N) is an L-substructure of $\mathbf{N}$ and Φ is an L-isomorphism between $\mathbf{M}_0$ and $\mathbf{N}_0$. By Remark 4.6 and 3.1, we have:

$$\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{M}_0}(\bar{a}) = \mathrm{qftp}^{\mathbf{N}_0}(\bar{b}) = \mathrm{qftp}^{\mathbf{N}}(\bar{b}).$$

Let us assume (2). We define $\mathbf{M}_0$ inductively. (It will be the substructure of $\mathbf{M}$ *generated* by $\bar{a}$.) Let $A_0 := \mathcal{C}^M \cup \{a_1, \ldots, a_n\}$, where $\bar{a} = (a_1, \ldots, a_n)$. For $k \in \mathbb{N}$, we define:

$$A_{k+1} := A_k \cup \bigcup_{f \in \mathcal{F}} \{f^M(A_k^{n_f})\}.$$

Finally, let $M_0 := \bigcup_k A_k$. Then M_0 is closed under all the f^M, so it gives $\mathbf{M}_0$, an L-substructure of $\mathbf{M}$. We define now inductively a monomorphism $\Phi : \mathbf{M}_0 \to \mathbf{N}$ taking $\bar{a}$ to $\bar{b}$. On A_0 we define:

$$\Phi_0(a_1) := b_1, \ldots, \Phi_0(a_n) := b_n, \quad \Phi_0(c^M) := c^N \text{ for } c \in \mathcal{C}.$$

Since $\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{N}}(\bar{b})$ we get that:

- for $i, j \leqslant n$, $a_i = a_j$ if and only if $b_i = b_j$;
- for $c_1, c_2 \in \mathcal{C}$, $c_1^M = c_2^M$ if and only $c_1^N = c_2^N$. (Note that the "quantifier-free theory of $\mathbf{M}$" is a part of $\mathrm{qftp}^{\mathbf{M}}(\bar{a})$!)

Hence Φ_0 is well-defined and injective on A_0.
We will define one more step. For any $f \in \mathcal{F}$ and $\bar{s} \in A_0^{n_f}$ let

$$\Phi_1(f^M(\bar{a})) := f^N(\Phi_0(\bar{a})).$$

As above, Φ_1 is well-defined and injective on A_1. Similarly, we can see that Φ_1 satisfies the definition of L-monomorphism "wherever it makes sense". We continue to define $\Phi_2 : A_2 \to N$ etc. and set $\Phi := \bigcup \Phi_n$. □

Remark 4.9. As in the proof of the implication (2) ⇒ (1) above, for any $A \subseteq M$ we can define a substructure of $\mathbf{M}$ *generated* by A. Hence we also get the notion of a *finitely generated* substructure of $\mathbf{M}$. If $\mathbf{M}_0$ is a substructure of $\mathbf{M}$, then $\mathbf{M}_0\langle A\rangle$ denotes the substructure of $\mathbf{M}$ generated by $\mathbf{M}_0 \cup A$. The L_{r}-substructure of a ring R generated by $A \subseteq R$ is exactly the subring of R generated by A.

To formulate the main criterium for quantifier elimination, we need to define one more property of structures which is called saturation. Existence of saturated structures allows to work in one model of a complete theory, rather than in all of them.

Definition 4.10. An L-structure $\mathbf{M}$ is $\aleph_0$-*saturated*, if for any finite $A \subseteq M$ and any finitely satisfiable L_A-type $q(x)$ (one variable!), $q(x)^{\mathbf{M}}$ is non-empty.

Exercise 9: Show that if $\mathbf{M}$ is $\aleph_0$-*saturated*, then for any finite $A \subseteq M$ and any finitely satisfiable L_A-type $q(x_1, \ldots, x_n)$ (finitely many variables!), $q(x_1, \ldots, x_n)^{\mathbf{M}}$ is non-empty.

Examples

- The field $\mathbb{R}$ (considered as an L_{r}-structure) is *not* $\aleph_0$-saturated. To see this, consider for each $n \in \mathbb{N}$ the following L_{r}-formula:

$$\phi_n(x): \quad \exists y\ y^2 + 1 + \ldots + 1 = x \quad (\text{"+" taken } n \text{ times}),$$

  and let $q(x) := \{\phi_n(x) \mid n \in \mathbb{N}\}$. Any finite subset of $q(x)$ is satisfiable by a large enough real number, however $q(x)^{\mathbb{R}} = \emptyset$. Intuitively, "$+\infty$" satisfies $q(x)$.
- The field $\mathbb{C}$ (considered as an L_{r}-structure) *is* $\aleph_0$-saturated. We will see it later as a consequence of quantifier elimination.

The following existence result can be proved similarly as the Upper Löwenheim-Skolem Theorem.

Lemma 4.11. *Let* $\mathbf{M}$ *be an infinite* L*-structure. Then there is* $\mathbf{N} \succcurlyeq \mathbf{M}$ *which is* $\aleph_0$*-saturated.*

We can finally formulate and show our desired criterion for quantifier elimination. See Remark 4.9 for some of the terminology used below.

Theorem 4.12 (**Schoenfield-Blum Criterion**). *Let* T *be an* L*-theory without finite models. The following are equivalent:*

(1) *If* $\mathbf{M}_1, \mathbf{M}_2 \models T$*,* $\mathbf{M}_2$ *is* $\aleph_0$*-saturated,* $\mathbf{U} \subseteq \mathbf{M}_1, \mathbf{M}_2$ *is a common finitely generated* L*-substructure and* $c \in M_1$*, then there is an* L*-monomorphism* $\Phi : \mathbf{U}\langle c\rangle \to \mathbf{M}_2$ *which is the identity on* U*.*
(2) T *has quantifier elimination.*

Proof of Theorem 4.12. Exercise 10: Prove the (not so easy) implication (2) ⇒ (1) (how the saturation is used?).
Let us assume (1). To show (2) we will check the criterion for quantifier elimination from Lemma 4.7. Let us take $\mathbf{M} \models T$ and $\bar{a}, \bar{b} \in M^n$ such that $\mathrm{qftp}^{\mathbf{M}}(\bar{a}) = \mathrm{qftp}^{\mathbf{M}}(\bar{b})$. We aim to show that $\mathrm{tp}^{\mathbf{M}}(\bar{a}) = \mathrm{tp}^{\mathbf{M}}(\bar{b})$. By 4.11, there is $\mathbf{M} \preccurlyeq \mathbf{N}$ such that $\mathbf{N}$ is $\aleph_0$-saturated. Since for any $\bar{s} \in M^n$ we have $\mathrm{tp}^{\mathbf{M}}(\bar{s}) = \mathrm{tp}^{\mathbf{N}}(\bar{s})$ (Remark 4.6), we may assume that $\mathbf{M}$ is already $\aleph_0$-saturated.

By 4.8, there are finitely generated (see Remark 4.9) substructures $\mathbf{M}_{\bar{a}}, \mathbf{M}_{\bar{b}} \subseteq \mathbf{M}$ such $\bar{a} \in M_{\bar{a}}^n, \bar{b} \in M_{\bar{b}}^n$ and an L-isomorphism $\Psi : \mathbf{M}_{\bar{a}} \to \mathbf{M}_{\bar{b}}$ such that $\Psi(\bar{a}) = \bar{b}$.
Let us take an L-formula $\phi(\bar{x})$ such that $\mathbf{M} \models \phi(\bar{a})$. We will show that $\mathbf{M} \models \phi(\bar{b})$. For simplicity we assume that $\phi(\bar{x})$ is *existential*, i.e. that there is a quantifier-free formula $\psi(\bar{x}, \bar{y})$, where $\bar{y} = (y_1, \ldots, y_k)$, such that

$$\phi(\bar{x}) \ = \ \exists \bar{y} \ \psi(\bar{x}, \bar{y}).$$

Since $\mathbf{M} \models \phi(\bar{a})$, there is $\bar{s} = (s_1, \ldots, s_k) \in M^k$ such that $\mathbf{M} \models \psi(\bar{a}, \bar{s})$.
We will inductively extend Ψ to an L-monomorphism

$$\Psi_k : \mathbf{M}_{\bar{a}}\langle s_1, \ldots, s_k \rangle \to \mathbf{M}.$$

Let us take $0 \leqslant l < k$, set $\mathbf{U} := \mathbf{M}_{\bar{a}}\langle s_1, \ldots, s_l \rangle$ and assume that we have an L-monomorphism $\Psi_l : \mathbf{U} \to \mathbf{M}$ extending Ψ. We will define Ψ_{l+1} using the condition (1). We first extend Ψ_l to an L-isomorphism (denoted also Ψ_l) between $\mathbf{M}$ and $\mathbf{M}'$, an L-superstructure of $\mathbf{M}_{\bar{b}}$. The existence of such an extension is left as Exercise 11. We apply (1) for $\mathbf{U}$ as above and

$$\mathbf{M}_1 := \mathbf{M}', \ \mathbf{M}_2 := \mathbf{M}, \ c := \Psi(s_{l+1}).$$

We get an L-monomorphism $\Phi : \mathbf{U}\langle \Psi(s_{l+1}) \rangle \to \mathbf{M}$ which is the identity on $\mathbf{U}$. Let

$$\Psi_{l+1} : \mathbf{M}_{\bar{b}}\langle s_1, \ldots, s_l, s_{l+1} \rangle \to \mathbf{M}, \quad \Psi_{l+1}(t) := \Phi(\Psi_l(t)).$$

Since Φ is identity on $\mathbf{U}$, Φ_{l+1} extends Φ_l. Therefore, we have inductively defined an extension of Ψ to $\Psi_k : \mathbf{M}_{\bar{a}}\langle \bar{s} \rangle \to \mathbf{M}$.
Let $\bar{t} := \Psi_k(\bar{s})$. Since $\mathbf{M} \models \psi(\bar{a}, \bar{s})$ and $\psi(\bar{x}, \bar{y})$ is quantifier-free, we get by Remark 4.6 that $\mathbf{M}_{\bar{a}}\langle \bar{s} \rangle \models \psi(\bar{a}, \bar{s})$. Clearly Ψ_k is an L-isomorphism between $\mathbf{M}_{\bar{a}}\langle \bar{s} \rangle$ and $\mathbf{M}_{\bar{b}}\langle \bar{t} \rangle$. By 3.1, we have $\mathbf{M}_{\bar{b}}\langle \bar{t} \rangle \models \psi(\bar{b}, \bar{t})$. Again by Remark 4.6, we get $\mathbf{M} \models \psi(\bar{b}, \bar{t})$. Hence $\mathbf{M} \models \phi(\bar{b})$ indeed. □

5. Saturday

Today we will apply the Schoenfield-Blum Criterion for quantifier elimination to several theories. To do that, we need to understand the "isomorphism type" of an element over a finitely generated substructure.

Theorem 5.1. *The theory* ACF *has quantifier elimination.*

Proof. We will use the criterion from Theorem 4.12. Let us take algebraically closed fields M_1, M_2 such that M_2 is $\aleph_0$-saturated, a common finitely generated subring (an L_{r}-substructure) $R \subseteq M_1, M_2$ and $c \in M_1$. Let K be the fraction field of R. Then K naturally embedds both in M_1 and M_2, so we may assume that $R = K$.

Case 1 c is algebraic over K (the saturation will not be used)

Let $f \in K[X]$ be the minimal polynomial of c over K. Then we have:

$$(*) \qquad K(c) = K[c] \cong_K K[X]/(f).$$

Since M_2 is algebraically closed, there is $d \in M_2$ such that $f(d) = 0$. Again we have:

$$(**) \qquad K(d) = K[d] \cong_K K[X]/(f).$$

Composing the isomorphisms from $(*)$ and $(**)$, we get a monomorphism $K(c) \to M_2$ over K.

Case 2 c is transcendental over K (the saturation will be used)

Let $\bar{a}$ be a finite tuple generating K, and $q(x)$ be an $L_{\bar{a}}$-type expressing that x is transcendental over K. The type $q(x)$ is finitely satisfiable in M_2, since every polynomial has only finitely many zeroes and M_2 is infinite being algebraically closed. Since M_2 is $\aleph_0$-saturated, there is $d \in q(x)^{M_2}$. Then d is transcendental over K and we have:

$$K(c) \cong_K K(X) \cong_K K(d).$$

Composing the above isomorphisms we get a monomorphism $K(c) \to M_2$ over K. □

Exercise 12: Let K be any field and $V \subseteq K^n$. Show that V is constructible if and only if, there is a quantifier-free L_K-formula $\phi(\bar{x})$ such that $V = \phi(\bar{x})^K$.

Corollary 5.2. *If K is an algebraically closed fields and $X \subseteq K$ is definable, then X is finite or cofinite.*

Proof. By Exercise 12 and quantifier elimination for ACF. □

Note that we would not be able to check the condition (1) from the Schoenfield-Blum test, if M_2 were not $\aleph_0$-saturated. For example take $K = \mathbb{Q}$, $M_1 = \mathbb{Q}(X)^{\text{alg}}$, $M_2 = \mathbb{Q}^{\text{alg}}$ and $c = X$.

Exercise 13: Show that an algebraically closed field is saturated if an only if it has infinite transcendence degree over its prime subfield.

Definition 5.3. Let $\mathbf{M}$ be an L-structure and T be an L-theory.

1. $\mathbf{M}$ is *minimal*, if any definable subset of $\mathbf{M}$ is either finite or cofinite.
2. T is *strongly minimal*, if for any $\mathbf{M} \models T$, $\mathbf{M}$ is minimal.
3. $\mathbf{M}$ is *strongly minimal*, if $\text{Th}_M(\mathbf{M})$ is strongly minimal, i.e. for any $\mathbf{M} \preccurlyeq \mathbf{N}$, $\mathbf{N}$ is minimal.

Examples

1. ACF is strongly minimal.
2. Let $L_E = \{E\}$, where E is a binary relation symbol. An L_E-structure (M, E^M) such that E^M is an equivalence relation having one E^M-class of size n for each $n \in \mathbb{N}_{>0}$ and no infinite classes is minimal and not strongly minimal. Quantifier elimination necessary for minimality. Bounds...

Let K be a field. We know that if K is algebraically closed, then K is strongly minimal. Actually, the converse also holds. But if K is minimal, then we know that K is algebraically closed only if K has finite characteristic.

Let DLO be the L_o-theory of dense linear orders without endpoints.

Theorem 5.4. DLO *has quantifier elimination.*

Proof. Let $\mathbf{M}_1, \mathbf{M}_2 \models$ DLO, where $\mathbf{M}_2$ is $\aleph_0$-saturated (the saturation actually will not be used here) and $\mathbf{M}_i = (M, <^i)$ for $i = 1, 2$. Since the language L_o is purely relational, any subset of an L_o-structure is an L_o-substructure. In particular, a finitely generated substructure is just a finite subset. Let us take a finite substructure $\mathbf{U} \subseteq \mathbf{M}_1, \mathbf{M}_2$ and $c \in M_1 \setminus U$. Since the order $<^1$ is linear, the order $<^U$ is linear as well, so $\mathbf{U} = \{u_1, \ldots, u_n\}$, where $u_1 <^U \ldots <^U u_n$.

Case 1 $c <^1 u_1$

Since $<^2$ has no end-points, there is $d \in M_2$ such that $d <^2 u_1$. We define an L_o-monomorphism

$$\Psi : \mathbf{U}\langle c\rangle \to M, \quad \Psi(c) = d, \ \Psi|_U = \text{id}_U .$$

Case 2 there is $1 \leqslant i < n$ such that $u_i <^1 c <^1 u_{i+1}$

Since $<^2$ is dense, there is $d \in M_2$ such that $u_i <^2 d <^2 u_{i+1}$ and we define Ψ as in Case 1.

Case 3 $u_n <^1 c$

This is analogous to Case 1. □

Let R be a ring and define the following language

$$L^R := (+, -, 0, \lambda_r)_{r \in R},$$

where $+$ is a binary function symbol, $-$ and all λ_r are unary function symbol and 0 is a constant symbol. Then any (left,right) R-module is naturally an L^R-structure and in this case an L^R-substructure os the same as R-submodule.

Theorem 5.5. *Let K be a field. The L^K-theory of infinite K-vector spaces has quantifier elimination*

Proof. Exercise 14: check that the (very easy here) Shoenfield-Blum test holds. □

Let us consider now the real field.

Fact 5.6. *The L_r-theory* $\mathrm{Th}(\mathbb{R})$ *does not have quantifier elimination.*

Proof. Assume that the L_{r}-theory $\mathrm{Th}(\mathbb{R})$ has quantifier elimination. As in 5.2, we conclude that each L_{r}-definable subset of $\mathbb{R}$ is either finite or cofinite. But $[0, \infty)$ is definable by the formula $\exists y \; x = y^2$, a contradiction. □

We can also consider $\mathbb{R}$ as an L_{or}-structure and this is the right language for quantifier elimination.

Theorem 5.7 (Tarski)**.** *The L_{or}-theory* $\mathrm{Th}(\mathbb{R})$ *has quantifier elimination.*

We have no time for the proof. We will just write an L_{or}-theory RCF whose models are exactly the same as models of $\mathrm{Th}(\mathbb{R})$. Such models are called *real closed fields*

Axioms for RCF

(1) $<$ is a total order;
(2) $\forall x, y, z \; x \leqslant y \rightarrow x + z \leqslant y + z$;
(3) $\forall x, y, z \; (x \leqslant y \wedge z > 0) \rightarrow x \cdot z \leqslant y \cdot z$;
(4) $\forall x, y \;\; (x \leqslant y \leftrightarrow \exists z \; y - x = z \cdot z)$;
(5) Each polynomial of odd degree has a root.

By checking the shape of subsets of $\mathbb{R}$ definable by quantifier-free formula, it is easy to see (*having* quantifier elimination) that finite union of intervals are all the definable subsets or $\mathbb{R}$.

Definition 5.8. Let L be a language containing L_{o} and $\mathbf{M}$ be an L-structure. $\mathbf{M}$ is *o-minimal* ("o" stands for order) if any definable subset of M is a finite union of ($<^M$-)intervals.

We know that $\mathbb{R}$ is o-minimal. We quote a remarkable theorem of Wilkie:

Theorem 5.9. *The structure* $(\mathbb{R}, <, +, -, \cdot, \exp, 0, 1)$ *is o-minimal.*

Many other o-minimal structures are known and there is a rich theory of o-minimal structures.