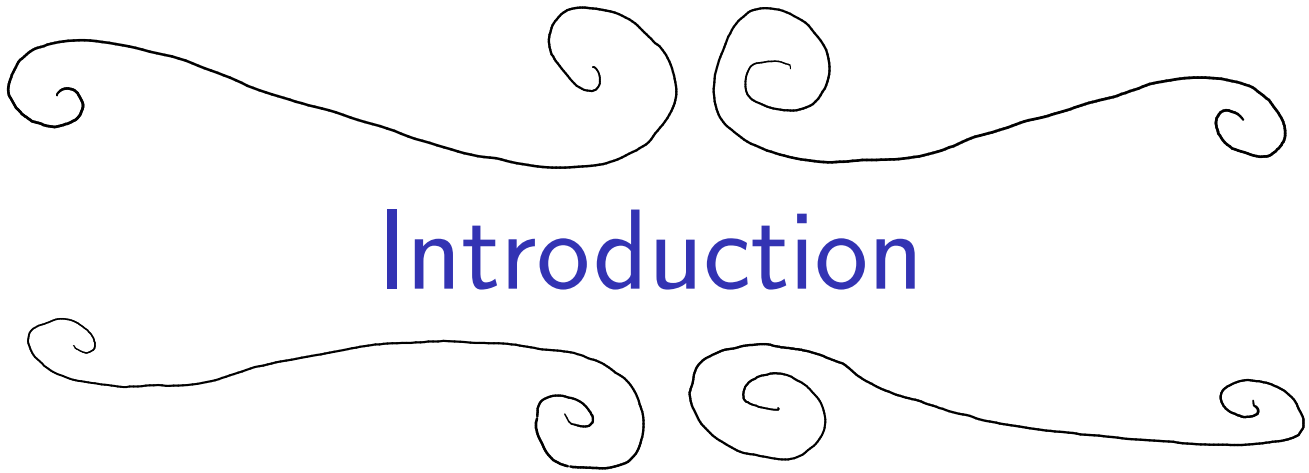
Applications of Model Theory to Algebra and Geometry

Immi Halupczok

University of Leeds

Spring 2016



Introduction

What is model theory?

- Model theory = study of *definable sets*.
- Definable set = set defined by a *first order formula*
  Example: $\{x \in \mathbb{Q} \mid \underbrace{x \neq 0 \wedge \exists y : y^2 = x}_{\text{First order formula}}\}$ is a definable set in $\mathbb{Q}$.
- Work in many different kind of structures: fields, rings, groups, vector spaces, ordered sets, graphs, etc.
- Usefulness #1: Results about definable sets are very general.
  - Wish: describe *all* definable sets in a given structure
  - Hopeless in general; instead: identify classes of "tame" structures where one has some control over definable sets
  - Typical results in tame structures:
    - All definable sets can be defined using only simple formulas.
    - Definable sets have invariants, like dimension.
    - Existence of algorithms (e.g. to decide whether a definable set is empty)
- Usefulness #2: Transfer results between different structures:
  - Certain structures cannot be distinguished by first order formulas.
  - Thus: If a result has been proven in one of them, it also holds in the other one, provided the result can be expressed by a first order formula.

In this lecture

- Content:
  - First part: Introduction to model theory and central results
  - Second part:
    - various classes of "tame" structures
    - applications

    (less formal)
- Exam:
  - Take-home exam
  - Only about the first part of the lecture
  - Do 4 out of 5 questions (all carrying equal marks)
- Exercise Sheets:
  - Available on the MAGIC site of this course (under "Files").
  - Intended to be roughly similar to exam questions (but no guarantee)
  - I can give feedback on solutions: `i.halupczok@leeds.ac.uk`
- Literature:
  - Tent, Ziegler: *A Course in Model Theory*
  - Marker: *Model Theory: An Introduction*

Basic Definitions

Languages

- Not every formula makes sense in every structure.
  Example: $\exists y : y^2 = x$ makes sense in a field (or in a ring), but not in a vector space.
- A *language* specifies which symbols are defined in a given structure and hence may appear in a formula.

Definition

A **language** *is a set L of* **function symbols**, **relation symbols**, *and* **constant symbols**. *Each function symbol and each relation symbol has an* **arity** $\in \{1, 2, 3, \dots\}$.

- **Some Standard-examples:**
  - $L_{\mathrm{ag}} = \{0, +, -\}$, the language of abelian groups;
    0 is a constant symbol, $+$ is a binary function symbol,
    $-$ is a unary function symbol.
  - $L_{\mathrm{ring}} = L_{\mathrm{ag}} \cup \{1, \cdot\}$, the language of rings;
    1 is a constant symbol, $\cdot$ is a binary function symbol.
  - $L_{\mathrm{ord}} = \{<\}$, the language of ordered sets;
    $<$ is a binary relation symbol.
  - $L_{\mathrm{oring}} = L_{\mathrm{ring}} \cup L_{\mathrm{ord}}$, the language of ordered rings.

Formulas, informally

- **Examples:**
  - "$x = 0 \vee \neg\exists y : y + y = x$" is an L_{ag}-formula. ($L_{\mathrm{ag}} = \{0, +, -\}$)
    This is a statement about x. For example, in $\mathbb{Z}$ (i.e., if $x, y \in \mathbb{Z}$), it says: x is either 0 or odd.
  - "$\forall x : (x > 0 \underset{\uparrow}{\rightarrow} \exists y : y \cdot y = x)$" is an L_{oring}-formula. ($L_{\mathrm{oring}} = L_{\mathrm{ag}} \cup \{1, \cdot, <\}$)

    Notation for implication

    This formula does not depend on a variable; it is either true or false. For example, it is true in $\mathbb{R}$ but false in $\mathbb{Q}$.
- Informally, a (first order) *L-formula* is a syntactically correct expression build using:
  - the symbols from L
  - $=$, $\wedge$, $\vee$, $\neg$, $\forall$, $\exists$, parenthesis
  - symbols for variables (e.g. $x, y, \ldots$)

Formulas, formally

Definition

Let L be a language, and let $\underline{x} = (x_1, \ldots, x_n)$ be variables.

- *The following are L-**terms in** $\underline{x}$:*
  - *x_i for any $i = 1, \ldots, n$*
  - *any constant symbol from L*
  - *$f(t_1, \ldots, t_\ell)$, where $t_1, \ldots, t_\ell$ are L-terms in $\underline{x}$; f is an ℓ-ary function symbol in L*
- *The following are L-**formulas in** $\underline{x}$:*
  - *$t_1 = t_2$, where t_1 and t_2 are L-terms in $\underline{x}$*
  - *$R(t_1, \ldots, t_\ell)$, where $t_1, \ldots, t_\ell$ are L-terms; R is an ℓ-ary relation symbol in L*
  - *$\neg\phi_1$, $\phi_1 \wedge \phi_2$ and $\phi_1 \vee \phi_2$, where ϕ_1 (and ϕ_2) are L-formulas in $\underline{x}$*
  - *$\forall y\, \phi$ and $\exists y\, \phi$, where if ϕ is an L-formula in $\underline{x}, y$.*
- *Formulas of the form $t_1 = t_2$ or $R(t_1, \ldots, t_\ell)$ are called* **atomic**.
- *A formula in no variables (i.e., $n = 0$) is called a* **sentence**.

- Instead of "formula in $\underline{x}$", one often says "formula with free variables $\underline{x}$".

More notation concerning Formulas

- If ϕ is a formula in $\underline{x}$, one often writes $\phi(\underline{x})$. (And similarly for terms.)
- We will often use informal notation in formulas. In particular:
  - We write "$\rightarrow$" for "implies"; i.e., $\phi_1 \rightarrow \phi_2$ stands for $\neg\phi_1 \vee \phi_2$.
  - $\phi_1 \leftrightarrow \phi_2$ stands for $(\phi_1 \rightarrow \phi_2) \wedge (\phi_2 \rightarrow \phi_1)$.
  - $t_1 \neq t_2$ means $\neg t_1 = t_2$.
  - $\top$ is any formula which is always true, e.g., $\forall x\colon x = x$
  - $\bot = \neg\top$ is always false.
  - For various symbols that may be in L, we use the "usual" notation. E.g.:
    - If $+ \in L$, then we write $x + y$ (and not something like $+(x, y)$).
    - If $< \in L$, then $x \leq y$ means $x < y \vee x = y$, and $x > y$ means $y < x$.
  - We may use other informal shortcuts:
    - If $\cdot \in L$, then we write x^2 for $x \cdot x$, and similarly $x^3, \ldots$. (but *not* x^y)
    - If $+ \in L$ but not $\cdot \in L$, $2x$ means $x + x$; similarly $3x$, etc.

Structures

- Formulas per se have no meaning; they only get a meaning in a *structure*. An L-structure specifies what the symbols of L stand for.

Definition

*Let L be a language. An L-**structure** is a set M together with the following:*

- *For each ℓ-ary function symbol f in L, a function $f^M : M^\ell \to M$.*
- *For each ℓ-ary relation symbol R in L, a subset $R^M \subseteq M^\ell$. (Intention: R^M is the set of tuples for which the relation holds.)*
- *For each constant symbol c in L, an element $c^M \in M$.*

*f^M and R^M are called the **interpretation** of f and M in M.*

Most of the time, we write f and R instead of f^M and R^M.

Example: $\mathbb{Z}$ is an L_{oring}-structure: ($L_{\mathrm{oring}} = \{0, 1, +, -, \cdot, <\}$.)

- The interpretation of the symbol $0 \in L_{\mathrm{ag}}$ is the element 0 of $\mathbb{Z}$.
- The interpretation of the symbol $+ \in L_{\mathrm{ag}}$ is addition, i.e., the map $\mathbb{Z}^2 \to \mathbb{Z}, (x, y) \mapsto x + y$.
- The interpretation of $- \in L_{\mathrm{ag}}$ is the map $x \mapsto -x$
- 1, $\cdot$: similarly
- The interpretation of $<$ is the set $\{(a, b) \in \mathbb{Z}^2 \mid a < b\}$.

(In very formal notation: $+$ is the *symbol* in L_{ag}; $+^{\mathbb{Z}}$ is the *function* $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.)

Structures, cont'd

- More generally:
  Any abelian group is naturally an L_{ag}-structure.
  Any ring with unit is naturally an L_{ring}-structure. ($L_{\mathrm{ring}} = L_{\mathrm{ag}} \cup \{1, \cdot\}$.)
  Any ordered set in an L_{ord}-structure. ($L_{\mathrm{ord}} = \{<\}$.)
  etc.
- Note: Up to now, nothing prevents us from interpreting the above languages in a completely different way than what the symbols suggest.

Interpretation of formulas, informally

- An L-formula can be *interpreted* in any L-structure M; this works as the notation would suggest.
  Example: Consider the L_{ag}-formula $\phi(x) = \exists y : y + y = x$.
  We can interpret in $\mathbb{Z}$ and ask for which $n \in \mathbb{Z}$ it holds.
  Answer: $\phi(n)$ holds iff n is even.
- Notation: Given an L-structure M,
  an L-formula $\phi(x_1, \ldots, x_n)$,
  elements $a_1, \ldots, a_n \in M$,
  we write $M \models \phi(a_1, \ldots, a_n)$ to say:
  "ϕ holds in M if one plugs in $a_1, \ldots, a_n$ for $x_1, \ldots, x_n$"
- Note: If ϕ is a sentence (no free variables), then no a_i are needed; we write $M \models \phi$ if ϕ holds in M.

Interpretation of formulas, formal definition

Definition

- *Fix: a language L, an L-structure M, a tuple $\underline{a} \in M^n$.*
- *Given an L-term $t(x_1, \ldots, x_n)$, define its* **interpretation** *$t^M(\underline{a})$ by:*
  - *If $t = x_i$:* $t^M(\underline{a}) := a_i$
  - *If $t = c$:* $t^M(\underline{a}) := c^M$ *(for $c \in L$ a constant symbol)*
  - *If $t = f(t_1, \ldots, t_\ell)$:* $t^M(\underline{a}) := f^M(t_1^M(\underline{a}), \ldots, t_\ell^M(\underline{a}))$
- *Given an L-formula $\phi(x_1, \ldots, x_n)$, define $M \models \phi(\underline{a})$ by:*
  - *If $\phi = (t_1 = t_2)$:* $M \models \phi(\underline{a}) :\iff t_1^M(\underline{a}) = t_2^M(\underline{a})$
  - *If $\phi = R(t_1, \ldots, t_\ell)$:* $M \models \phi(\underline{a}) :\iff (t_1^M(\underline{a}), \ldots t_\ell^M(\underline{a})) \in R^M$
  - *If $\phi = \neg\psi$:* $M \models \phi(\underline{a}) :\iff M \not\models \psi(\underline{a})$
  - *$\phi = \psi_1 \wedge \psi_2$, $\phi = \psi_1 \vee \psi_2$: similarly*
  - *If $\phi(\underline{x}) = \exists y\, \psi(\underline{x}, y)$:* $M \models \phi(\underline{a}) :\iff$ *there exists an $b \in M$ such that $M \models \psi(\underline{a}, b)$*
  - *$\phi(\underline{x}) = \forall y\, \psi(\underline{x}, y)$: similarly*
- *"$M \models \phi(\underline{a})$" is pronounced as: "$\phi(\underline{a})$* **holds in** *$M$" or "$\underline{a}$* **satisfies** *$\phi$ (in M)" or, if ϕ is a sentence, "M is a* **model** *of ϕ".*
- *Notation: $\phi(M) := \{\underline{a} \in M^n \mid M \models \phi(\underline{a})\}$ is the* **set defined by** *ϕ (in M). Such a set $\phi(M) \subseteq M^n$ is called L-***definable (in** *M)**.***

Example: For $\phi(x) = \exists y : y + y = x$: $\phi(\mathbb{Z}) = 2\mathbb{Z}$, $\phi(\mathbb{Q}) = \mathbb{Q}$

Examples/Exercises

- How to define the units of a ring by an L_{ring}-formula?
  I.e. want $\phi(x)$ such that for any ring R, $\phi(R) = R^{\times}$.
- Express "there exists exactly one y such that $\psi(y)$ holds" as a formula (assuming that ψ is a formula).
  (This allows us to use "$\exists^{=1} y$" as a shortcut in formulas.)
- Express "there exists exactly two y such that $\psi(y)$ holds" as a formula. (Notation: $\exists^{=2} y$.)
- Is there an L_{ag}-sentence ϕ such that $M \models \phi$ iff M is an abelian group?
- Let $L = L_{\mathrm{oring}} \cup \{f\}$, where f is a unary function. Suppose that $\mathbb{R}$ is an L-structure, with the usual interpretation of L_{oring}. Find a sentence expressing that f is continuous.
- Consider $\mathbb{R}$ as an L_{ring}-structure (i.e., without "$<$"). Is there a formula $\phi(x, y)$ such that for $a, b \in \mathbb{R}$, we have $\mathbb{R} \models \phi(a, b)$ iff $a < b$?

Some definable sets in fields

- Fix a field K; work in $L_{\mathrm{ring}} = \{0, 1, +, -, \cdot\}$.
- Some L_{ring}-definable sets:
  - The zero set $\{\underline{a} \in K^n \mid f(\underline{a}) = 0\}$ of a polynomial $f \in \mathbb{Z}[\underline{x}]$.
    (Note that $n \in \mathbb{N}$ can be written as $\underbrace{1 + \cdots + 1}_{n}$ in a formula.)
  - Boolean combinations of the above.

  Note: These are *all* sets that are L_{ring}-definable without quantifiers.
- Sometimes, one wants to allow polynomials with coefficients in K (instead of $\mathbb{Z}$). In other words, we want to allow elements of K in formulas.
  Formalism/notation for this:

Definition

Suppose M is an L-structure and $A \subseteq M$. Then

- *$L(A)$ consists of the language L, together with one constant symbol for each $a \in A$.*
- *M is considered as an $L(A)$-structure in the obvious way.*

*Instead of "$L(A)$-definable", one often writes A-***definable***.*

Thus: For $f \in K[\underline{x}]$, $\{\underline{a} \in K^n \mid f(\underline{a}) = 0\}$ is $L_{\mathrm{ring}}(K)$-definable (or K-definable).

Theories

- For many kinds of algebraic structues (groups, fields, rings, ordered sets), the axioms can be written as (first order) sentences. We make this formal.

Definition

Fix a language L.

- *An L-**theory** T is a set of L-sentences.*
- *A **model** of a theory T is an L-structure M such that $M \models \phi$ for all $\phi \in T$.*

Examples:

- The theory of abelian groups is the L_{ag}-theory consisting of the axioms for abelian groups: $\mathrm{AG} = \{$
  $\forall x, y, z : (x + y) + z = x + (y + z)$ (associativity)
  $\forall x, y : x + y = y + x$ (commutativity)
  $\forall x : x + 0 = x$ (neutral element)
  $\forall x : x + (-x) = 0$ (inverse element)
  $\}$. Thus: An L_{ag}-structure is a model of AG iff it is an abelian group.
- Similarly, one defines the L_{ring}-theory of rings, the L_{ring}-theory of fields, L_{ord}-theory of ordered sets, the L_{oring}-theory of ordered rings (or fields) etc.

- Note: For fields, one only uses L_{ring} (without symbol for division), since division by 0 is not defined.

More examples of theories

- The theory ACF of algebraically closed fields consists of:
  - the field axioms
  - "Every non-constant polynomial has a 0."
    Q: Can this be expressed by an L_{ring}-formula?
    A: Not by one, but by many: For each $n \geq 1$, take the axiom:
    $\forall a_0, \ldots, a_{n-1} : \exists x : x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0 = 0$
- For a prime p, the theory of algebraically closed fields of characteristic p is:
  $\text{ACF}_p = \text{ACF} \cup \{\underbrace{1 + 1 + \cdots + 1}_{p} = 0\}$
- The theory of algebraically closed fields of characteristic 0 is:
  $\text{ACF}_0 = \text{ACF} \cup \{1 + 1 \neq 0, 1 + 1 + 1 \neq 0, 1 + 1 + 1 + 1 + 1 \neq 0, \text{etc.}\}$
- What about axiomatizing $\mathbb{R}$ (in L_{oring})?
  - $\mathbb{R}$ is the unique ordered field such that each bounded subset has a supremum.
  - Thus need to say: $\forall X \subseteq \mathbb{R} : (X \text{ bounded} \rightarrow X \text{ has a supremum})$.
  - This is not an L_{oring}-formula: Only quantifiers over elements are allowed, not over subsets!
  - We will see: $\mathbb{R}$ cannot be uniquely characterized by L_{oring}-axioms.

More about theories

Definition

Fix a language L.

- *An L-theory T is* **consistent** *if models of T exist.*
- *Two L-theories are* **equivalent** *if they have the same models.*
- *An L-sentence ϕ* **follows** *from an L-theory T if for ϕ holds in every model of T. In that case, we write $T \vdash \phi$.*

Examples:

- All examples from the previous slides (e.g. $\mathrm{ACF}, \mathrm{ACF}_0, \mathrm{ACF}_p, \dots$) are consistent.
- The L_{ag}-theory $\{0 \neq 0\}$ is not consistent.
- In every algebraically closed field, any monic polynomial of degree 2 has exactly two solutions. Thus: $\mathrm{ACF} \vdash \forall a_1, a_0 : \exists^{=2} x \colon x^2 + a_1 x + a_0 = 0$.

Note: We will usually not distinguish between equivalent theories.

Exercise: Prove that the following are equivalent:

- T is inconsistent.
- $T \vdash \bot$. (Recall: $\bot$ is the always-false sentence.)
- There exists a sentence ϕ s.t. $T \vdash \phi$ and $T \vdash \neg\phi$.

Complete theories

- We added more and more axioms to the theory of fields: algebraically closed fields (ACF), and then e.g. algebraically closed fields of characteristic 0 (ACF_0). Could we say even more?
- Answer: No!
  - For any L_{ring}-sentence ϕ, we have $\mathrm{ACF}_0 \vdash \phi$ or $\mathrm{ACF}_0 \vdash \neg\phi$.
  - Thus $\mathrm{ACF}_0 \cup \{\phi\}$ is either equivalent to ACF_0 or it is inconsistent.

  Formalism for that:

Definition

A consistent L-theory T is **complete** *if for every L-sentence ϕ, either $T \vdash \phi$ or $T \vdash \neg\phi$.*

Theorem

ACF_0 *and* ACF_p *(for every prime p) are complete.*

(Partial proof: later.)

Elementary equivalence

- An easy way to obtain complete theories: For any L-structure M, take all sentences that hold in M:

Definition

Let M be an L-structure. The **theory of** M *is* $\mathrm{Th}(M) := \{\phi \text{ } L\text{-sentence} \mid M \models \phi\}$.

- $\mathrm{Th}(M)$ is a complete theory.
  Proof: For any L-sentence ϕ, either $M \models \phi$ or $M \models \neg\phi$.
  This is defined as one would expect. ↓
- Q: Does $\mathrm{Th}(M) = \mathrm{Th}(M')$ imply that M and M' are "isomorphic"? A: No!
- That ACF_0 is complete means: For any two algebraically closed fields K_1, K_2 of characteristic 0, we have $\mathrm{Th}(K_1) = \mathrm{Th}(K_2)$. (Proof: Exercise.)
  This is an important phenomenon, so we define:

Definition

Two L-structures M_1, M_2 are **elementarily equivalent** *if* $\mathrm{Th}(M_1) = \mathrm{Th}(M_2)$.
Notation: $M_1 \equiv_L M_2$.

- Thus: Any two algebraically closed fields of the same characteristic are elementarily equivalent.
- We will see many other such situations.

Quantifier elimination

Quantifier elimination: definition, motivation

- How can one possibly prove that ACF_0 is complete? Need understanding of *everything* that can be expressed by an L_{ring}-sentence.
- For this, need understanding of *all* definable sets.
- Philosophy: Only quantifiers make things complicated. (Sets definable without quantifiers are easy to understand.) Thus: Q: Are quantifiers really necessary?

Definition

Fix an L-theory T.

- *Two formulas $\phi(\underline{x})$, $\psi(\underline{x})$ are* **equivalent modulo** *T if for every $M \models T$, we have $\phi(M) = \psi(M)$.*
  Equivalently: ... if $T \vdash \forall \underline{x} : (\phi(\underline{x}) \leftrightarrow \psi(\underline{x}))$.
- *An L-theory T has* **quantifier elimination** *(**q.e.**) if every L-formula is equivalent modulo T to a quantifier-free L-formula (i.e., a formula containing neither $\forall$ or $\exists$).*

Exercise: For any structure M, we have:

- $\phi(\underline{x})$, $\psi(\underline{x})$ are equivalent modulo $\mathrm{Th}(M)$ iff $\phi(M) = \psi(M)$.
- $\mathrm{Th}(M)$ has q.e. iff every definable set in M can be defined by a quantifier-free formula.

Quantifier elimination: a proof strategy

Fix a theory T. How can one prove that T has q.e.?

Proposition

T has q.e. iff every formula of the form
$\exists y : \psi(\underline{x}, y)$, *where ψ is quantifier free*
is equivalent modulo T to a quantifier free formula.

Proof:

- ▷ Let an arbitrary L-formula ϕ be given. (Goal: Get rid of quantifiers in ϕ.)
- ▷ Get rid of all "$\forall$" using that $\forall y : \phi(\underline{x}, y)$ is equivalent to $\neg\exists y : \neg\phi(\underline{x}, y)$.
- ▷ Assume that any sub-formula is already quantifier free (by an induction over the "length" of ϕ).
- ▷ We consider the various possibilies for ϕ from the definition of formulas:
  - ▷ If ϕ is atomic, it is quantifier-free.
  - ▷ If $\phi = \psi_1 \vee \psi_2$ or $\phi = \psi_1 \wedge \psi_2$ or $\phi = \neg\psi_1$:
    The sub-formulas ψ_1, ψ_2 are quantifier free, so ϕ is, too.
  - ▷ If $\phi(\underline{x}) = \exists y : \psi(\underline{x}, y)$:
    This is equivalent to a quantifier free formula by assumption. □

Example: Q.e. in dense linear orders without endpoints

- DLO is the L_{ord}-theory of dense linear orders without endpoints.
  - "Dense" means: for any $a < b$ there exists c in between, i.e. $a < c < b$.
  - "Without endpoints" means: There is no minimal and no maximal element.
- **Example:** $\mathbb{Q} \models \mathrm{DLO}$, $\mathbb{R} \models \mathrm{DLO}$

Proposition

DLO *has quantifier elimination.*

Proof:

- By the previous slide, it suffices to consider formulas of the form
  $\exists y : \psi(\underline{x}, y)$ where ψ is quantifier free.
- Thus ψ is a boolean combination of $t_1 = t_2$ and $t_1 < t_2$, where each t_j is one of $x_1, \ldots, x_n, y$.
- Now get rid of the quantifier using the following ideas:
  - Get rid of disjunctions: $\exists y : (\psi_1(\underline{x}, y) \vee \psi_2(\underline{x}, y))$ is equivalent to $\exists y : \psi_1(\underline{x}, y) \vee \exists y : \psi_2(\underline{x}, y)$. (Treat both parts separately.)
  - $\exists y : (y = x_\ell \wedge \psi_1(\underline{x}, y))$ is equivalent to $\psi_1(\underline{x}, x_\ell)$.
  - $\exists y : (y < x_1 \wedge \cdots \wedge y < x_n)$ is always true, since the order has no minimum.
  - $\exists y : (x_1 < y \wedge y < x_2)$ is equivalent to $x_1 < x_2$, since the order is dense. □

Q.e. in ACF; completeness of ACF_0, ACF_p

Using a similar strategy (but more work), one proves:

Theorem

ACF *(the theory of algebraically closed fields) has quantifier elimination.*

From this, we deduce:

Corollary

ACF_0 *and* ACF_p *are complete.*

Proof:

- Let ϕ be any L-sentence.
- By quantifier elimination in ACF, we may assume without loss that ϕ is quantifier free.
- Thus ϕ only consists of $0, 1, +, -, \cdot, =$ and boolean combinations. (No variables!)
- Fixing the characteristic of K determines whether such a ϕ holds, i.e.:
  - Either $\mathrm{ACF}_0 \vdash \phi$ or $\mathrm{ACF}_0 \vdash \neg\phi$
  - And similarly for ACF_p, for each prime p.

□

Real closed fields

Definition

An ordered field R is called **real closed** *if every polynomial of odd degree has a zero. We denote the L_{oring}-theory of real closed fields by* RCF*.*

Exercise: Show that real closed fields can indeed be axiomatized by L_{oring}-sentences.

Examples: $\mathbb{R}$ is real closed; the relative algebraic closure $\tilde{\mathbb{Q}} \cap \mathbb{R}$ is real closed.

Theorem

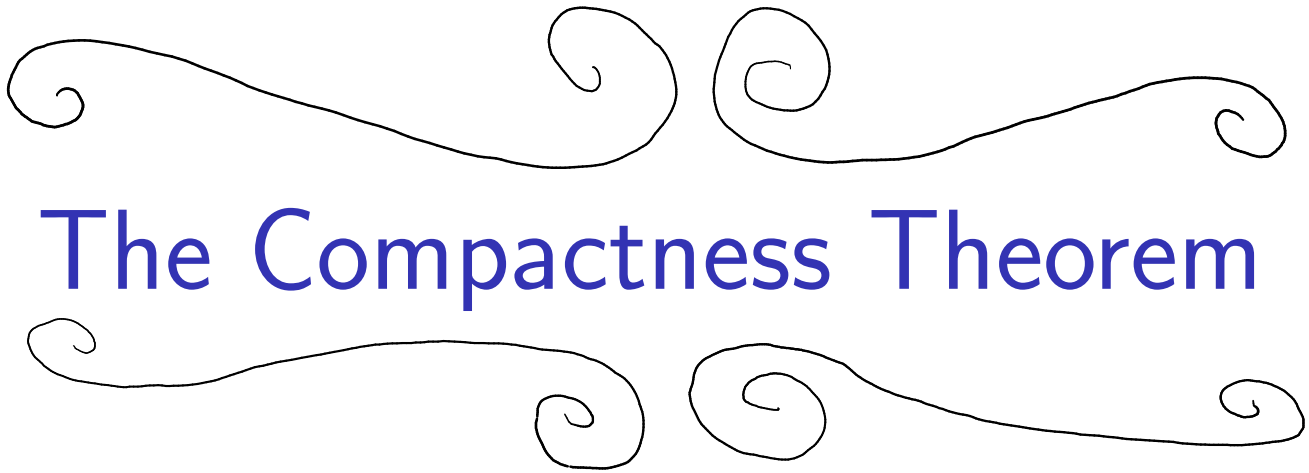
RCF *has quantifier elimination.*

As for ACF, one deduces:

Theorem

RCF *is complete.*

(Note: The characteristic of ordered fields is always 0.)
This proves our claim that $\mathbb{R}$ cannot be characterized by L_{ring}-axioms:
$\mathbb{R} \equiv_{L_{\mathrm{oring}}} (\tilde{\mathbb{Q}} \cap \mathbb{R})$.



The Compactness Theorem

Statement of the Compactness Theorem

Fix a language L.

Theorem (Compactness Theorem, 1st version)

For any L-theory T and any L-sentence ϕ:
If $T \vdash \phi$ then there exists a finite subset $T_0 \subseteq T$ such that $T_0 \vdash \phi$.

Definition

T is **finitely consistent** *if every finite subset is consistent.*

Theorem (Compactness Theorem, 2nd version)

If T is finitely consistent, then it is consistent.

- Implication 1st $\Rightarrow$ 2nd version: Use $\phi = \bot$. □
- Implication 2st $\Rightarrow$ 1nd version: $T \vdash \phi \quad \Rightarrow \quad T \cup \{\neg\phi\}$ is inconsistent $\Rightarrow \quad T_0 \cup \{\neg\phi\}$ is inconsistent for some finite $T_0 \quad \Rightarrow \quad T_0 \vdash \phi$. □
- Note: There exists a 3rd version stating that some topological space is compact (hence the name).

Compactness: sketch of proof (assuming $|L| \leq \aleph_0$)

- Given: T finitely consistent. Goal: Construct $M \models T$.
- Let $C = \{c_i \mid i \in \mathbb{N}\}$ be new constant symbols and $L_C := L \cup C$.
- We enlarge T to an L_C-theory T' with the following properties:
  (1) T' is still finitely consistent.
  (2) For every L_C-sentence ϕ, either $\phi \in T'$ or $\neg\phi \in T'$
  (3) If $(\exists x\colon \psi(x)) \in T'$, then there is a $c_i \in C$ such that $\psi(c_i) \in T'$.

  Strategy for this: Repeat the following:
  - If (2) is violated, add one of ϕ or $\neg\phi$ to T'. (At least one of them won't make T' finitely inconsistent.)
  - If (3) is violated, then add $\psi(c_i)$ to T', where c_i is a constant not yet used before. (This won't make T' finitely inconsistent.)

  Doing this carefully and using Zorn's lemma, this yields T' as desired.
- Now set $M := C/\!\sim$, where $c_1 \sim c_2$ iff $(c_1 = c_2) \in T'$.
- T' says how to turn M into an L_C-structure; for example, if f is a binary function and $(f(c_1, c_2) = c_3) \in T'$, then $f^M(c_1/\!\sim, c_2/\!\sim) = c_3/\!\sim$.
- It remains to prove: $M \models T'$. (Then we are done since $T \subseteq T'$.)
- Given $\phi \in T'$, do an induction over the length of ϕ. Difficult cases:
  - $\phi = \exists x\, \psi(x)$: By (3), $\psi(c_i) \in T'$, so $M \models \psi(c_i)$, so $M \models \phi$.
  - $\phi = \forall x\, \psi(x)$: Then $\neg\psi(c_i) \notin T'$ for all c_i, so $\psi(c_i) \in T'$, so $M \models \phi$. □

Remarks: $|M| \leq |C| = \aleph_0$. If $|L| > \aleph_0$, modify the proof using $|C| = |L|$.

Application: Transfer between different characteristics

- We have seen that one can transfer sentences between algebraically closed fields of the same characteristic. Using the compactness theorem, we can also change the characteristic, as follows:

Theorem

Let ϕ be any L_{ring}-sentence. Then the following are equivalent:

(1) $\mathrm{ACF}_0 \vdash \phi$ *(i.e.: ϕ holds in algebraically closed fields of characteristic 0)*

(2) For every sufficiently big prime p, $\mathrm{ACF}_p \vdash \phi$.

(3) There exist arbitrarily large p such that $\mathrm{ACF}_p \vdash \phi$.

Proof:

- Recall: $\mathrm{ACF}_p = \mathrm{ACF} \cup \{\underbrace{1+\cdots+1=0}_{p} \text{ times}\}$ and $\mathrm{ACF}_0 = \mathrm{ACF} \cup \{2 \neq 0, 3 \neq 0, \dots\}$
- (1) $\Rightarrow$ (2): $\mathrm{ACF}_0 \vdash \phi \Rightarrow T_0 \vdash \phi$ for some finite $T_0 \subseteq \mathrm{ACF}_0$. T_0 contains only finitely many "$p \neq 0$", so for big p, $\mathrm{ACF}_p \vdash \phi$.
- (2) $\Rightarrow$ (3): trivial.
- (3) $\Rightarrow$ (1): Suppose $\mathrm{ACF}_0 \nvdash \phi$. Since ACF_0 is complete, $\mathrm{ACF}_0 \vdash \neg\phi$. Apply (1) $\Rightarrow$ (2) to $\neg\phi$. This yields: $\mathrm{ACF}_p \vdash \neg\phi$ for all big p, contradicting the assumption. $\square$

Application of the application: "injective $\Rightarrow$ surjective"

- In particular, for L_{ring}-sentences ψ: $\quad \tilde{\mathbb{F}}_p \models \psi$ for all $p \quad \Rightarrow \quad \mathrm{ACF} \vdash \psi$. $\quad (*)$.
  Here is a concrete application of this:

Theorem

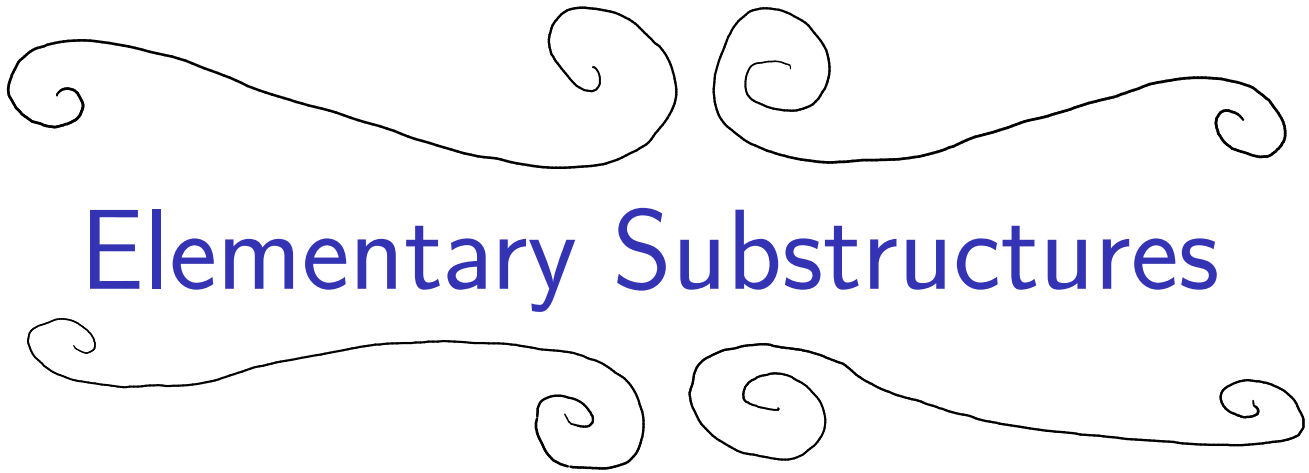
Given: an algebraically closed field K;
an $L_{\mathrm{ring}}(K)$-definable set $X \subseteq K^n$; *(Recall: $L_{\mathrm{ring}}(K) = L_{\mathrm{ring}} \cup K$)*
a rational map $f : X \to X$ (i.e. $f = g_1/g_2$ for $g_i \in K[x_1, \ldots, x_n]$, with $0 \notin g_2(X)$).
If f is injective then it is surjective.

Proof in the case $K = \tilde{\mathbb{F}}_p$ (the algebraic closure of $\mathbb{F}_p$):

- Let $\underline{b} \in X$ be given. We need to find $\underline{a} \in X$ with $f(\underline{a}) = \underline{b}$.
- Choose $L = \mathbb{F}_{p^r} \subseteq K$ containing $b_1, \ldots, b_n$ and the coefficients of g_1, g_2
- Set $X_L := X \cap L^n$. Then $\underline{b} \in X_L$ and $f(X_L) \subseteq X_L$.
- This map $X_L \to X_L$ is injective (by assumption), and hence surjective, since X_L is finite. In particular, there exists $\underline{a} \in X_L \subseteq X$ with $f(\underline{a}) = \underline{b}$.

Deducing the general case:

- The theorem becomes an L_{ring}-sentence if we fix:
  - the degrees $d_1 = \deg g_1$, $d_2 = \deg g_2$;
  - an L_{ring}-formula $\phi(\underline{x}, \underline{y})$ and only consider $X = \phi(K, \underline{c})$ for $\underline{c} \in K^m$.
- Apply $(*)$ for each d_1, d_2, ϕ separately. $\square$



Elementary Substructures

Substructures

Substructures of L-structures are defined in a natural way:

Definition

A subset M_0 of an L-structure M is a **substructure** *if M_0 it contains c^M for all constant symbols $c \in L$ and if it is closed under f^M for all function symbols $f \in L$. Such an M_0 is in a natural way an L-structure.*

- **Example:**
  - A substructure of a group (in L_{ag}) is a subgroup.
  - A substructure of a field (in L_{ring}) is a subring.
- Given $M_0 \subseteq M$ and a formula $\phi(\underline{x})$, compare $\phi(M_0)$ and $\phi(M) \cap M_0$.

  Sloppy notation; should be M_0^n (↓)
- In general, we have neither $\subseteq$ nor $\supseteq$.

  Example:
  - Consider $2\mathbb{Z} \subseteq \mathbb{Z}$ as L_{oag}-structures ($L_{\mathrm{oag}} = \{0, +, -, <\}$).
  - And consider $\phi(x) = \exists^{=1} y \colon 0 < y < x$
  - Then $\phi(\mathbb{Z}) \cap 2\mathbb{Z} = \phi(\mathbb{Z}) = \{2\}$ but $\phi(2\mathbb{Z}) = \{4\}$.
- Introduce a notion for substructures where this does not happen...

Elementary substructures

Definition

Let $M_0 \subseteq M$ be L-structures (i.e., M_0 is a substructure of M).

- ▷ *We call M_0 an* **elementary substructure** *of M if for every L-formula $\phi(\underline{x})$, we have: $\phi(M_0) = \phi(M) \cap M_0$.*
- ▷ *Equivalently: if $M_0 \equiv_{L(M_0)} M$.*
- ▷ *M is called* **elementary extension** *of M_0. Notation: $M_0 \prec M$ or $M_0 \prec_L M$.*

Proof of equivalence: Both conditions are equivalent to:
For all L-formulas $\phi(\underline{x})$ and all $\underline{a} \in M_0$: $M \models \phi(\underline{a}) \iff M_0 \models \phi(\underline{a})$. □

Non-Example: We have seen: $2\mathbb{Z} \not\prec_{L_{\mathrm{oag}}} \mathbb{Z}$.

Proposition

If $K_1 \subseteq K_2$ are algebraically closed fields, then $K_1 \prec_{L_{\mathrm{ring}}} K_2$.

Proof:

- ▷ Let $\phi(\underline{x})$ be an L_{ring}-formula and $\underline{a} \in K_1$. Goal: $K_1 \models \phi(\underline{a}) \iff K_2 \models \phi(\underline{a})$.
- ▷ By q.e., without loss $\phi(\underline{x})$ has no quantifiers.
- ▷ Then the goal is trivially true. □

Analogously, for real closed fields $R_1 \subseteq R_2$, one obtains $R_1 \prec_{L_{\mathrm{oring}}} R_2$.

Application: Hilbert's Nullstellensatz

An important result from algebraic geometry:

Theorem (Hilbert's Nullstellensatz)

Given: an algebraically closed field K;
polynomials $f_1, \ldots, f_k \in K[\underline{x}]$ with $1 \notin I := (f_1, \ldots, f_k)$.
Then there exists $\underline{a} \in K^n$ such that $f_1(\underline{a}) = \cdots = f_k(\underline{a}) = 0$. $(*)$

An easy proof using model theory:

- Denote the conclusion $(*)$ by ϕ; this is an $L_{\mathrm{ring}}(K)$-sentence.
- Instead of proving $K \models \phi$, it suffices to prove $K' \models \phi$ for any $K' \succ K$...
- ...i.e., for any algebraically closed $K' \supseteq K$.
- Choose a maximal ideal $M \supseteq I$.
- We obtain a field extension $K'' := K[\underline{x}]/M \supseteq K$. Set $K' := \tilde{K}''$.
- Write $q\colon K[\underline{x}] \to K''$ for the quotient map.
- Then for all i, we have $f_i(q(x_1), \ldots, q(x_n)) = q(f_i(x_1, \ldots, x_n)) = 0$ (since $f_i \in M$).
- Thus $K' \models \phi$, namely with $\underline{a} = (q(x_1), \ldots, q(x_n))$. □

Tarski's test

To check that something is an elementary substructure, use the following.

Proposition (Tarski's test)

Given: L-structures $M_0 \subseteq M$. The following are equivalent:

(1) $M_0 \prec M$

(2) For every $L(M_0)$-formula $\phi(x)$, we have:
If there exists $a \in M$ such that $M \models \phi(a)$,
then there exists $a_0 \in M_0$ such that $M \models \phi(a_0)$.

Proof of (1) $\Rightarrow$ (2): $M \models \phi(a) \quad \Rightarrow \quad M \models \exists x\colon \phi(x) \quad \overset{(1)}{\Rightarrow} \quad M_0 \models \exists x\colon \phi(x)$

$\Rightarrow \quad M_0 \models \phi(a_0)$ for some $a_0 \in M_0 \quad \overset{(1)}{\Rightarrow} \quad M \models \phi(a_0)$ □

Proof of (2) $\Rightarrow$ (1):

- Given a sentence $\phi \in L(M_0)$, we need to prove: $M_0 \models \phi \iff M \models \phi$
- We do an induction over the length of ϕ.
- Only the case $\phi = \exists x\colon \psi(x)$ is non-trivial. In that case:
  - $M \models \phi \iff$ Ex. $a \in M$ s.t. $M \models \psi(a)$
  - By assumption: $\iff$ Ex. $a_0 \in M_0$ s.t. $M \models \psi(a_0)$
  - By induction: $\iff$ Ex. $a_0 \in M_0$ s.t. $M_0 \models \psi(a_0)$
  - $\iff M_0 \models \phi$ □

The Löwenheim–Skolem Theorem

The Löwenheim–Skolem Theorem

Elementary extensions and elementary substructures "always exist":

Theorem (Löwenheim–Skolem)

Given: an infinite L-structure M; a cardinal $\kappa \geq \max\{|L|, \aleph_0\}$.

- ▷ *"Upwards": If $\kappa > |M|$, then there exists $M' \succ M$ with $|M'| = \kappa$.*
- ▷ *"Downwards": If $\kappa < |M|$, there exists $M_0 \prec M$ with $|M_0| = \kappa$.*

Proof of "downwards":

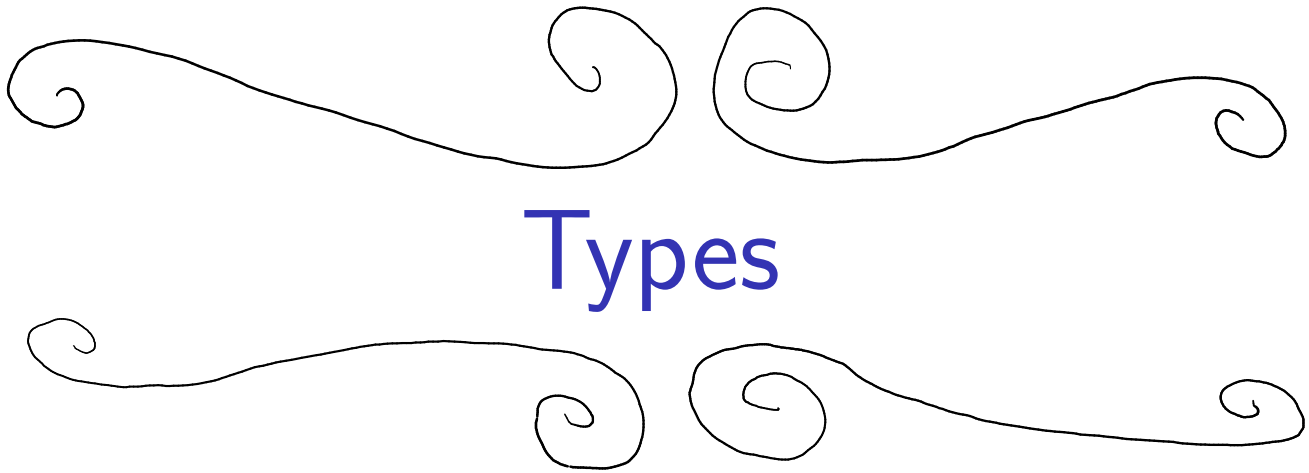
- ▷ Choose any substructure $M_0 \subseteq M$ of cardinality κ.
- ▷ According to Tarski's test, we need, for every $L(M_0)$-formula $\phi(x)$:
  If $M \models \phi(a)$ for some $a \in M$, then one can find such an a even in M_0.
- ▷ To achieve this: For each such $\phi(x)$, put a corresponding a into M_0.
- ▷ Now $L(M_0)$ became bigger, so do this again; repeat this ω many times. □

Proof of "upwards":

- ▷ Let C be a new set of κ many constant symbols and set $L'' := L(M) \cup C$.
- ▷ Consider the L''-theory $T := \mathrm{Th}(M) \cup \{\text{all constants from } C \text{ are different}\}$.
- ▷ T is finitely consistent, so by compactness, we find a model $M'' \models T$;
  in particular $M'' \succ_L M$, and all constants being different implies $|M''| \geq \kappa$.
- ▷ If $|M''| > \kappa$, use "downards", with M as initial M_0, to find $M' \prec M''$ with
  $|M'| = \kappa$ and $M \subseteq M'$. Now $M \prec M'' \succ M'$ implies $M \prec M'$. □

Consequences of Löwenheim–Skolem

- Let M be an L-structure.
- We already saw: $\mathrm{Th}(M)$ does not always determine M.
  Examples: $M = \mathbb{R}$ as L_{oring}-structure;
  M algebraically closed field as L_{ring}-structure
- The Löwenheim–Skolem says that $\mathrm{Th}(M)$ never determines M if M is infinite.
- And even more: $\mathrm{Th}(M)$ has models of every cardinality $\geq \max\{|L|, \aleph_0\}$.
- **Example:**
  - For any infinite cardinal κ, there exists a $K \models \mathrm{ACF}_0$ with $|K| = \kappa$.
  - Direct proof: Take $\mathbb{Q}$; adjoin κ many transcendental elements; take the algebraic closure of that. The resulting field has cardidinality κ.
- One can also prove: Given M_1, M_2 with $M_1 \equiv M_2$, there exists M with $M_1 \prec M$, $M_2 \prec M$.
- Common application: Suppose T is a complete theory.
  Often, one works in one huge $M \models T$ which contains all the $M_i \models T$ one might ever be interested in as elementary substructues. (Such a huge M is called a "monster model".)



Types

Types, informally

- To understand a structure M, it can be useful to pass to some $M^* \succ M$ since M^* contains "idealized elements".

  Example:
  - In $\mathbb{R}$, there exist arbitrarily small positive numbers:
    For every $n \in \mathbb{N}$, there exists $a \in \mathbb{R}$ with $0 < a < \frac{1}{n}$.
  - In a (suitable) $\mathbb{R}^* \succ \mathbb{R}$, there exist infinitesimal positive numbers:
    There exists $a \in \mathbb{R}^*$ such that $0 < a < \frac{1}{n}$ for every $n \in \mathbb{N}$.
  - Some proofs in $\mathbb{R}$ can be simplified by working in $\mathbb{R}^*$, using such infinitesimal a.
- The idealized elements in M^* are described by infinitely many $L(M)$-formulas.

  Example (cont'd):
  - The infinitesimal positive elements $x \in \mathbb{R}^*$ are those satisfying:
    $x > 0$, $x < 1$, $x < \frac{1}{2}$, $x < \frac{1}{3}$, $x < \frac{1}{4}$, ...
- Sets of formulas like this are called *types*.

Types, formally

Formally, a type is similar to a complete theory, but using formulas with free variables instead of sentences.
Fix a language L, an L-theory T and $n \in \mathbb{N}$. Below, all tuples $\underline{x}$, $\underline{a}$ are n-tuples.

Definition

Consider a set $p(\underline{x})$ of L-formulas $\phi(\underline{x})$ (in n variables).

- *A* **realization** *of $p(\underline{x})$ in some $M \models T$ is a tuple $\underline{a} \in M^n$ such that $M \models \phi(\underline{a})$ for all $\phi(\underline{x}) \in p(\underline{x})$. Notation: $M \models p(\underline{a})$.*
- *$p(\underline{x})$ is* **consistent** *(with T) if realizations exist.*
- *$p(\underline{x})$* **implies** *a formula $\psi(\underline{x})$ if for every $M \models T$ and $\underline{a} \in M^n$, we have: $M \models p(\underline{a}) \Rightarrow M \models \psi(\underline{a})$. Notation: $p \vdash \psi$.*
- *$p(\underline{x})$ is* **complete** *(modulo T) if for every $\psi(\underline{x})$, either $p \vdash \psi$ or $p \vdash \neg\psi$.*
- *$p(\underline{x})$ is an (n-)***type** *of T if it is consistent and complete.*

(n: *length of tuple*)

Example:

- $p(x) = \{x > 0, x < 1, x < \frac{1}{2}, x < \frac{1}{3}, \dots\}$ is a 1-type of RCF.
  (Note: $x < \frac{1}{3}$ can be expressed as $(1+1+1) \cdot x < 1$.)
- Any infinitesimal element of $\mathbb{R}^* \succ \mathbb{R}$ is a realization of $p(x)$.

Note: We do not distinquish between "equivalent" types.

Consistency of types

As before, fix a language L and an L-theory T.

Proposition

A set of formulas $p(\underline{x})$ is consistent iff it is finitely consistent, i.e., iff every finite subset $\Sigma \subseteq p$ is consistent.

Proof:

- Set $L' := L \cup \{\underline{c}\}$, where $\underline{c}$ is an n-tuple of constants.
- Set $T' := T \cup p(\underline{c})$, where $p(\underline{c}) := \{\phi(\underline{c}) \mid \phi(\underline{x}) \in p(\underline{x})\}$.
- Using that $p(\underline{x})$ is finitely consistent, deduce that T' is finitely consistent. (A realization $M \models \Sigma(\underline{a})$ yields a model of $T \cup \Sigma(\underline{c})$ by setting $\underline{c}^M = \underline{a}$.)
- By the Compactness Theorem, T' is consistent, i.e., there exists $M' \models T'$.
- Then $M' \models p(c^{M'})$. □

Example:

- Consider again $L = L_{\mathrm{oring}}$, $T = \mathrm{RCF}$, $p(x) = \{x > 0, x < 1, x < \frac{1}{2}, x < \frac{1}{3}, \dots\}$.
- Any finite subset of $p(x)$ has a realization $a \in \mathbb{R}$: just take a small enough.
- Thus $p(x)$ is consistent.

Completeness of types

- Proving completeness of sets of formulas is often hard.
  Example: Completeness of $p(x) = \{x > 0, x < 1, x < \frac{1}{2}, x < \frac{1}{3}, \dots\}$ can be proven using quantifier elimination.
- An easy way to obtain types: "analogue of $\mathrm{Th}(M)$ for types":

Definition

Given a structure M and $\underline{a} \in M^n$, set $\mathrm{tp}(\underline{a}) := \{\phi(\underline{x}) \mid M \models \phi(\underline{a})\}$ *(the* **type of** $\underline{a}$*).*

- Note: Every consistent set $\Sigma(\underline{x})$ of formulas is contained in a type.
  Proof: $\Sigma(\underline{x}) \subseteq \mathrm{tp}(\underline{a})$ for any realization $M \models \Sigma(\underline{a})$. □

Types over a set

Most of the time, one fixes an L-structure M, a set $B \subseteq M$ (often $B = M$) and considers types in the language $L(B)$ of the $L(B)$-theory $T = \mathrm{Th}(M)$.
Notation for that:

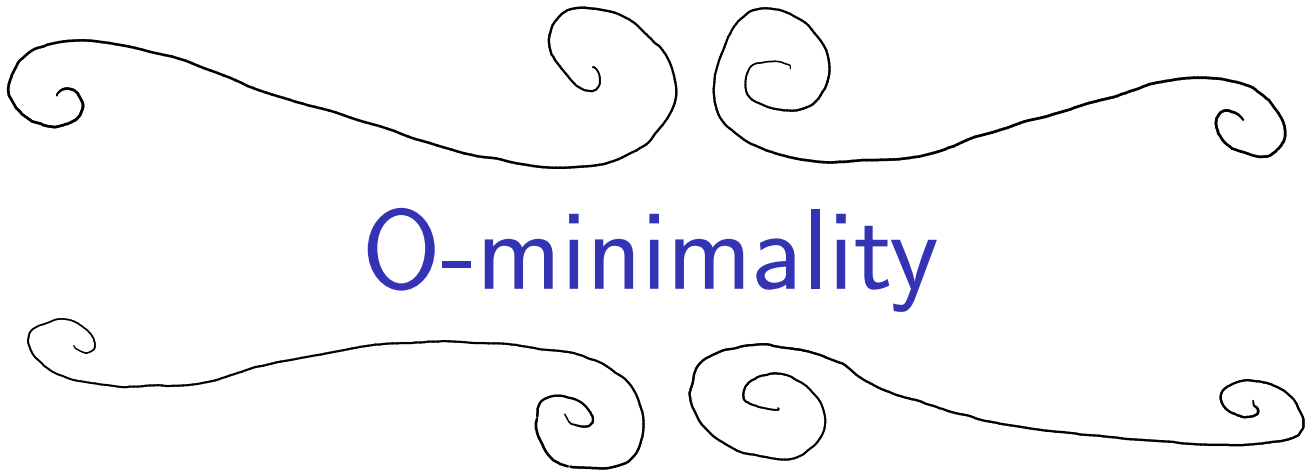
Definition

Fix L, M, B as above.

- *A* **type over** B *is a type in the language $L(B)$ of the $L(B)$-theory $\mathrm{Th}(M)$.*
- *For $M' \succ M$ and $\underline{a} \in (M')^n$ the* **type of** $\underline{a}$ **over** B $\mathrm{tp}(a/B)$ *is the type of a in the language $L(B)$.*

Example: Consider $L = \{<\}$, $M = \mathbb{Q}$ (and $T = \mathrm{Th}(\mathbb{Q}) = \mathrm{DLO}$).

- Any real number $r \in \mathbb{R}$ yields a type $p_r(x) := \mathrm{tp}(r/\mathbb{Q})$.
  Example: $p_\pi(x)$ contains $x > 3$, $x > 3.1$, $\ldots$, $x < 4$, $x < 3.2$, $\ldots$
- For $r < r'$, we have $p_r \neq p_{r'}$, since for $q \in \mathbb{Q}$ with $r < q < r'$, we have $(q < x) \in p_{r'}$ but $(q < x) \notin p_r$.
- But there exist even more 1-types over $\mathbb{Q}$, e.g. $\{x > 0\} \cup \{x < q \mid q \in \mathbb{Q}, q > 0\}$.



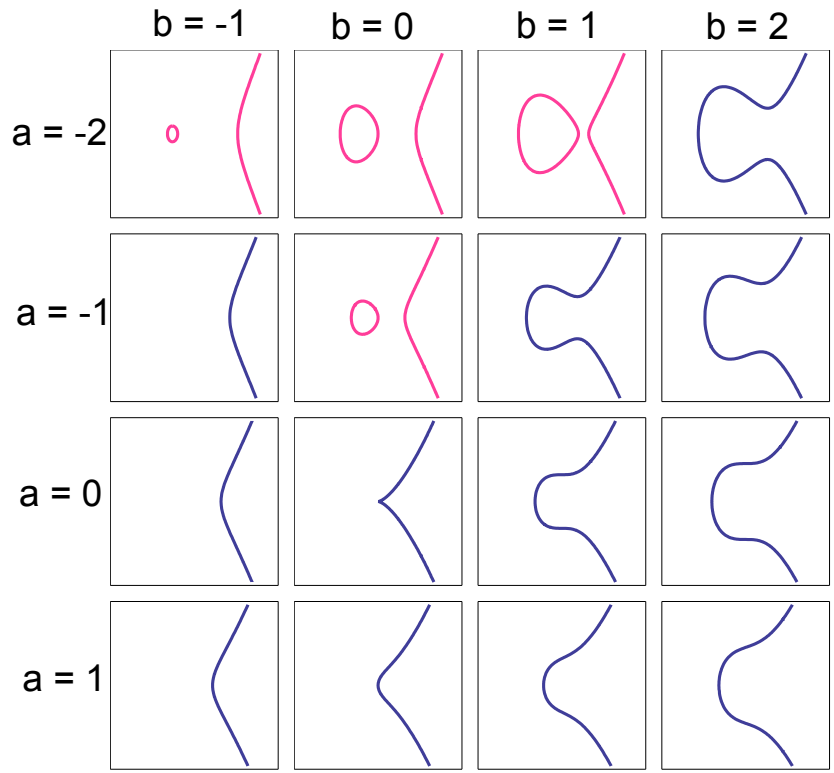
O-minimality

Motivation: homeomorphism types of zero sets

Consider $f(x, y) = x^3 + ax + b - y^2$.

What homeomorphism types can the zero set have, depending on a, b?

There are only finitely many different homeomorphism types.



Theorem (Fixed degree)

Fix $n, d \in \mathbb{N}$.
Consider polynomials $f \in \mathbb{R}[\underline{x}]$ in n variables of degree at most d.
For each such f, consider its zero-set $X := \{\underline{x} \in \mathbb{R}^n \mid f(\underline{x}) = 0\}$.
All those X have only finitely many different homeomorphism types.

Motivation: homeomorphism types of zero sets

Improvement of the theorem:

- ▷ What about $f_i(x, y) = x^i + ax + b - y^2$, for $i \in \mathbb{N}$?
- ▷ There are still only finitely many homeomorphism types (for all $i \in \mathbb{N}$ and $a, b \in \mathbb{R}$).

Theorem (Fixed number of monomials)

Fix $n, r \in \mathbb{N}$.
Consider polynomials $f \in \mathbb{R}[\underline{x}]$ in n variables which are sums of at most r monomials.
For each such f, consider its zero-set $X := \{\underline{x} \in \mathbb{R}^n \mid f(\underline{x}) = 0\}$.
All those X have only finitely many different homeomorphism types.

This has been proven using model theory.

O-minimal structures: definition

- ▷ Recall: One goal of model theory: identify classes of "tame" structures. ("Tame" = one has some control over all definable sets)
- ▷ One such class: "o-minimal structures" (o = "order")
- ▷ Fix a language $L \supseteq L_{\mathrm{ord}} = \{<\}$ and an L-structure M.
- ▷ By "definable" we mean M-definable (which means $L(M)$-definable).

Definition

We call M **o-minimal** *if:*

(1) $<$ defines a dense linear order without endpoints on M; and

(2) every definable subset of M can be defined by an $L_{\mathrm{ord}}(M)$-formula.

- ▷ Since DLO has quantifier elimination:
  (2) $\iff$ Definable subsets of M are finite unions of points and intervals (possibly unbounded).
- ▷ Note: No conditions imposed about definable subsets of M^n for $n \geq 2$.

Example: $\mathbb{Q}$ or $\mathbb{R}$ in the language L_{ord}

Example: $\mathbb{R}$ in the language L_{oring} (use quantifier elimination)

Non-example: $\mathbb{R}$ in the language $L_{\mathrm{oring}} \cup \{\sin\}$.

($\sin x = 0$ defines a set which is not a finite union of points and intervals.)

O-minimal structures: cell decomposition

For M o-minimal, any definable set $Z \subseteq M^n$ is a finite unions of "cells":

Definition

A definable $Z \subseteq M^n$ is a **cell** *if:*

- *Case $n = 1$: Z is a point or an interval (unbounded intervals allowed)*
- *Case $n \geq 2$: There exists a cell $X \subseteq M^{n-1}$ and*
  - *either Z is the graph of a continuous function $f : X \to M$*
  - *or Z is an "interval between two continuous functions $f_1, f_2 : X \to M$", i.e.:*
    - *we assume $f_1(\underline{x}) < f_2(\underline{x})$ for all $\underline{x} \in X$;*
    - *$Z = \{(\underline{x}, y) \in X \times M \mid f_1(\underline{x}) < y < f_2(\underline{x})\}$*
  - *Unbounded intervals allowed: can remove "$f_1(\underline{x}) < y$" and/or "$y < f_2(\underline{x})$"*

Example: There are 4 types of cells in M^2: points, vertical lines, graphs and "intervals between functions".

Note: "Continuous" refers to the interval topology.

Theorem (Cell decomposition)

Every definable subset of M^n can be written as a finite disjoint union of cells.

O-minimal structures: homeomorphism types

- ▷ For our motivating goal, we need to understand homeomorphism types of definable sets.
- ▷ We continue assuming that M is an o-minimal L-structure.

Theorem

Fix a definable set $Z \subseteq M^{m+n}$. *This is called a* **definable family** *of sets.*
For each $\underline{a} \in M^m$, we obtain a definable set $Z_{\underline{a}} = \{\underline{b} \mid (\underline{a}, \underline{b}) \in Z\}$.
Those $Z_{\underline{a}}$ have only finitely many different homeomorphism types (for varying $\underline{a}$).

Proof: In general: lots of work; but easy if Z is a cell:

- ▷ Any cell is homeomorphic to $(0,1)^k$ for some $k \leq n$.
- ▷ If Z is a cell, each $Z_{\underline{a}}$ is either empty or a cell. □

(In fact, $Z_{\underline{a}}$ is homeomorphic to $(0,1)^k$ for some k independent of $\underline{a}$.)

Recall:

- Our original goals were: Prove that among a certain family of sets, there are only finitely many homeomorphism types.
- Now it suffices to show: that family of sets is a *definable* families of sets...
- ...in *any* o-minimal structure.

Proof for fixed degree

Recall the 1st version of our goal:

Theorem (Fixed degree)

Fix $n, d \in \mathbb{N}$.
Consider polynomials $f \in \mathbb{R}[\underline{y}]$ in n variables of degree at most d.
For each such f, consider its zero-set $Y := \{\underline{y} \in \mathbb{R}^n \mid f(\underline{y}) = 0\}$.
All those Y have only finitely many different homeomorphism types.

We need to check that those Y form a definable family of sets.

- ▷ Work in $\mathbb{R}$ as an L_{oring}-structure.
- ▷ Consider the coefficients of f as variables, which we denote by $\underline{x}$. Let $\phi(\underline{x}, \underline{y})$ be the formula expressing "$f(\underline{y}) = 0$".
  (If e.g. $n = 1$, then $\phi(\underline{x}, y) = (x_d y^d + \cdots + x_1 y + x_0 = 0)$)
- ▷ Set $Z := \phi(\mathbb{R})$. Then the sets $Z_{\underline{a}}$ are exactly the zero sets Y of polynomials f as above. □

Proof for fixed number of monomials

Now recall the 2nd version of our goal:

Theorem (Fixed number of monomials)

Fix $n, r \in \mathbb{N}$.
Consider polynomials $f \in \mathbb{R}[\underline{y}]$ in n variables which are sums of at most r monomials.
For each such f, consider its zero-set $Y := \{\underline{y} \in \mathbb{R}^n \mid f(\underline{y}) = 0\}$.
All those Y have only finitely many different homeomorphism types.

- ▷ To obtain that those Y form a definable family, we need ay^m to be definable when not only a and x are considered as variables, but also m.
- ▷ This is not the case in L_{oring}. However:

Theorem

$\mathbb{R}$ *is o-minimal when considered as an L-structure for $L = L_{\mathrm{ring}} \cup \{\exp\}$.*

- ▷ In this language, $(x, y) \mapsto x^y$ is definable: $x^y = \exp(y \cdot \log(x))$.
- ▷ (Note: This is only true for $x \geq 0$. One needs a small trick to treat $x < 0$.)
- ▷ Also note: The family of sets we obtain is even bigger than required: it allows "polynomials" with any positve real exponents.

Non-standard Analysis

Non-standard Analysis: the idea

- Choose a "sufficiently big" elementary extension $\mathbb{R}^* \succ \mathbb{R}$.
- Idea: Statements can be simplified by:
  - using infinitesimal elements in $\mathbb{R}^*$ instead of small elements in $\mathbb{R}$;
  - using infinite elements of $\mathbb{R}^*$ instead of big elements in $\mathbb{R}$.
- As language L, we use "everything", i.e.:
  - For every element of $\mathbb{R}$, put a constant symbol into L.
  - For every subset of $\mathbb{R}^n$, put an n-ary relation symbol into L.
  - For every function $\mathbb{R}^n \to \mathbb{R}$, put an n-ary function symbol into L.
- Consequence: For every $X \subseteq \mathbb{R}^n$ and every $f : \mathbb{R}^n \to \mathbb{R}$, we obtain "corresponding" objects in $\mathbb{R}^*$, defined by the same symbol of L:
  - $X \subseteq \mathbb{R}^n$ yields $X^* \subseteq (\mathbb{R}^*)^n$ (with $X^* \cap \mathbb{R}^n = X$).
  - A function $f : \mathbb{R}^n \to \mathbb{R}$ extends to $f : (\mathbb{R}^*)^n \to \mathbb{R}$.
- Properties expressible by L-sentences transfer from $\mathbb{R}$ to $\mathbb{R}^*$.

  Examples:
  - We have $\mathbb{N}^* \subseteq \mathbb{Z}^* \subseteq \mathbb{Q}^* \subseteq \mathbb{R}^*$; $\mathbb{Q}^*$ is a field, $\mathbb{Z}$ a ring, etc.
  - Any mathematical operations defined in $\mathbb{R}$ (or on subsets) extend.
    Example: "$x \mapsto 2^x$" is defined for $x \in \mathbb{Z}^*$; it satisfies $2^{x+1} = 2 \cdot 2^x$.
    Other example: $\sin(x)$ is defined on $\mathbb{R}^*$; it is continuous, differentiable, etc.
- Note: Every subset or $\mathbb{R}^n$ is definable, but not every subset of $(\mathbb{R}^*)^n$.
  (For example, $\mathbb{R}^* \setminus \mathbb{R}$ is not definable.)

How big is $\mathbb{R}^*$?

- The previous slide says: Choose $\mathbb{R}^* \succ \mathbb{R}$ "sufficiently big". What does this mean?
- For many applications, it suffices to have:
  $$\text{For every infinite } X \subseteq \mathbb{R}^n,\ X^* \supsetneq X. \qquad (\star)$$
- Existence of such $\mathbb{R}^*$ follows from compactness.
- Note: For finite $X \subseteq \mathbb{R}^n$, one always has $X^* = X$.
- $(\star)$ implies: $\mathbb{N}^*$ contains infinite elements; $\mathbb{Q}^*$ contains infinite and infinitesimal elements.

Definition

- $\omega \in \mathbb{R}^*$ *is* **infinite** *if* $|\omega| > r$ *for all* $r \in \mathbb{R}$
- $\epsilon \in \mathbb{R}^*$ *is* **infinitesimal** *if* $|\epsilon| < r$ *for all* $r \in \mathbb{R}_{>0}$

- Actually, all elements of $\mathbb{N}^* \setminus \mathbb{N}$ are infinite.
- We can deduce that $\mathbb{R}^*$ is pretty big:
  Example: Take $\omega \in \mathbb{R}^*$ infinite. Some elements of $\mathbb{R}^*$:
  $\omega^5,\ \frac{1}{\omega},\ 2^\omega \in \mathbb{R}^*,\ \underbrace{2^{2^{2^{\cdots}}}}_{\omega \text{ times}},\ \sqrt{\omega},\ \log(\omega),\ \sqrt[\omega]{2}$

Simplifying statements about bounds

Lemma

For any set $X \subseteq \mathbb{R}$, we have the following equivalences:

(1) For every $r \in \mathbb{R}$ there exists $x \in X$ with $x > r$ *(X is unbounded from above)*
$\iff$ *X^* contains (some) positive infinite elements*

(2) There exists an $r \in \mathbb{R}$ such that $x \in X$ for all $x > r$
$\iff$ *X^* contains all positive infinit elements*

(3) Similar statements about X containing elements near 0 and infinitesimal elements of X^*.

Proof of (1):

- Set $Y := \{n \in \mathbb{N} \mid \text{There exists an } x \in X \text{ with } x > n\}$.
- X unbounded $\iff$ Y infinite $\iff$ $Y^* \supsetneq Y$
  $\iff$ Y^* contains infinite elements $\iff$ X^* contains infinite elements. □

Note: $Y^* \setminus Y \subseteq \mathbb{N}^* \setminus \mathbb{N}$

Note: $Y^* := \{n \in \mathbb{N}^* \mid \text{There exists an } x \in X^* \text{ with } x > n\}$

Computing limits

Elements of $\mathbb{R}^*$ are either infinite, or infinitesimally close to elements of $\mathbb{R}$:

Lemma

For every non-infinite $\alpha \in \mathbb{R}^*$, there exists exactly one $a \in \mathbb{R}$ with $a - \alpha$ infinitesimal.
Set $\mathrm{st}(\alpha) := a$ (the **standard part** *of a).*

This is handy to compute limits:

Lemma

Given: $f : \mathbb{N} \to \mathbb{R}$. Then:
$\lim_{n\to\infty} f(n) = b$ *iff, for every infinite $\omega \in \mathbb{N}^*$, $\mathrm{st}(f(\omega)) = b$.*

So: To compute a limit, plug in an infinite natural number.
Example: $\lim_{n\to\infty} \frac{2n^2+1}{n^2} = \mathrm{st}(\frac{2\omega^2+1}{\omega^2}) = \mathrm{st}(2 + \frac{1}{\omega^2}) = 2$

More limits and derivatives

For a function f defined on a suitable subsets of $\mathbb{R}$:

Lemma

$\lim_{x\to a} f(x) = b$ *iff, for every* α *with* $\mathrm{st}(\alpha) = a$, $\mathrm{st}(f(\alpha)) = b$.

Example: Computing the derivative of $f(x) = x^3$:

$f'(x) = \lim_{t\to 0} \frac{(x+t)^3 - x^3}{t} = \mathrm{st}(\frac{(x+\tau)^3 - x^3}{\tau})$ for τ infinitesimal

$= \mathrm{st}(\frac{x^3+3x^2\tau+3x\tau^2+\tau^3 \ - \ x^3}{\tau}) = \mathrm{st}(3x^2 + 3x\tau + \tau^2) = 3x^2.$

Example: The derivative of an arbitrary f: $f'(x) = \lim_{x'\to x} \frac{f(x')-f(x)}{x'-x}$.

- ▷ Choose $x' - x$ infinitesimal. Set $dx := x' - x$ and $df := f(x') - f(x)$.
- ▷ Then $f'(x) = \mathrm{st}(\frac{df}{dx})$.
- ▷ From this, one deduces the composition law for derivatives:
  If $y = f(x), z = g(y)$, $h = g \circ f$, then
  $h'(x) = \mathrm{st}(\frac{dz}{dx}) = \mathrm{st}(\frac{dz}{dy} \cdot \frac{dy}{dx}) = \mathrm{st}(\frac{dz}{dy}) \cdot \mathrm{st}(\frac{dy}{dx}) = g'(y) \cdot f'(x)$.

Some non-standard topology

Instead of considering $\mathbb{R} \prec \mathbb{R}^*$, can consider the same construction $M \prec M^*$ for an arbitrary set M.

- Let M be any Hausdorff topological space.
- Generalization of the standard part:
  - Given $\alpha \in M^*$, we define the **standard part** $\mathrm{st}(\alpha)$ as the element of M infinitesimally close to α if it exists.
  - α is **infinitesimally close** to a means: for every open $U \supseteq a$, $\alpha \in U^*$.
  - Note: if $\mathrm{st}(\alpha)$ exists, it is unique (since M is Hausdorff).

The results about limits in $\mathbb{R}$ generalize; for example, for a function f defined on a subset of M:

Lemma

$\lim_{x \to a} f(x) = b$ *iff, for every* α *with* $\mathrm{st}(\alpha) = a$, $\mathrm{st}(f(\alpha)) = b$.

Lemma

f *is continuous at* $a \in M$ *iff*
for all α *with* $\mathrm{st}(\alpha) = a$, *we have* $\mathrm{st}(f(\alpha)) = f(a)$.

Tychonoff's Theorem

Some properties of the topological space M can also easily be expressed:

Lemma

M is compact iff st *is defined on all of M^*.*

Example: $M = [a, b] \subseteq \mathbb{R}$ yields $M^* = \{x \in \mathbb{R}^* \mid a \leq x \leq b\}$
Non-example: $M = (a, b) \subseteq \mathbb{R}$ yields $M^* = \{x \in \mathbb{R}^* \mid a < x < b\}$;
For $\alpha \in \mathbb{R}^*$ with $\alpha - a$ infinitesimal, $\mathrm{st}(\alpha)$ is not defined (in M)
Recall that the following is not so easy to prove classically:

Theorem (Tychonoff)

If T_i are compact topological spaces, for $i \in I$, then $T := \prod_{i \in I} T_i$ is also compact.

Proof:

- Consider $T \cup \bigcup_i T_i =: M \prec M^*$.
- Let $\pi_i \colon T \to T_i$ be the projection (for every i).
- Given $\alpha \in T^* \subseteq M^*$, we find $\alpha_i := \pi_i(\alpha) \in T_i^*$; $\mathrm{st}(\alpha_i)$ exists.
- An easy computation shows: $a := (\mathrm{st}(\alpha_i))_{i \in I} \in T$ infinitesimally close to α.
- So $\mathrm{st}(\alpha) = a$. □

Some non-standard number theory

A (probably) useless curiosity:
Recall:

Conjecture (Twin Prime Conjecture)

There exist infinitely many $n \in \mathbb{N}$ such that both, n and $n+2$ are prime.

- The set of primes $\mathbb{P} \subseteq \mathbb{N}$ yields "non-standard primes" $\mathbb{P}^* \subseteq \mathbb{N}^*$.
- These are indeed primes in the following sense:
  $\forall x \in \mathbb{N}^* : \big(x \in \mathbb{P}^* \leftrightarrow \forall y \in \mathbb{N}^* : (y \mid x \rightarrow (y = 1 \vee y = x))\big)$
- It makes sense to ask whether "infinite twin primes" exists, i.e., $n \in \mathbb{N}^* \setminus \mathbb{N}$ such that $n, n+2 \in \mathbb{P}^*$.
- By a previous lemma, to prove the Twin Prime Conjecture, it suffices to find a single infinite pair of twin primes.

An algebraic application

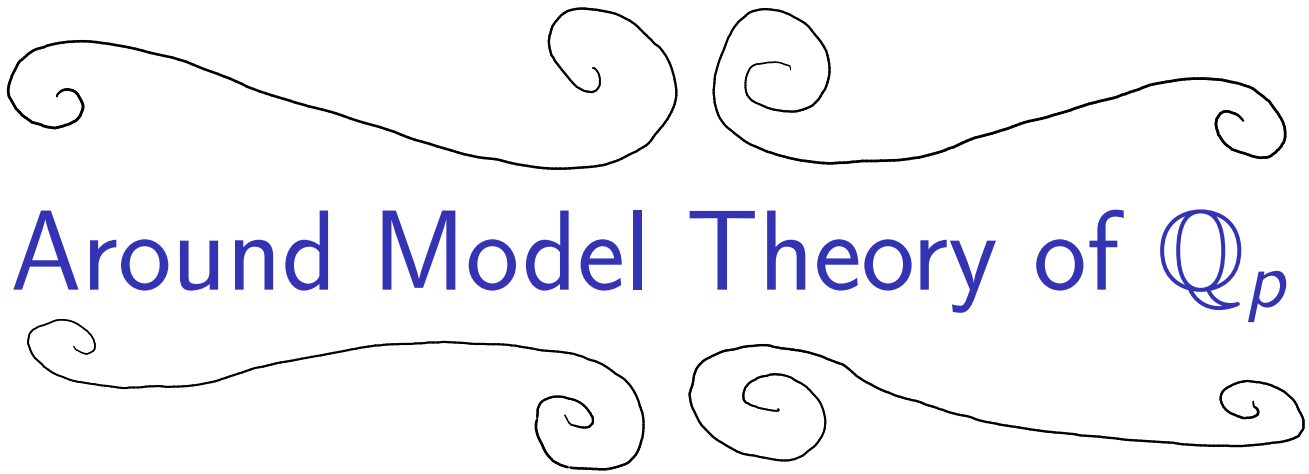
Theorem

For every $n, d \in \mathbb{N}$ there exists $\alpha \in \mathbb{N}$ such that the following holds:

- *Given: a field K; polynomials $f, f_1, \ldots, f_m \in K[\underline{x}]$ in n variables of degree $\leq d$.*
- *Suppose that $f \in (f_1, \ldots, f_m)$, i.e., $f = g_1 f_1 + \cdots + g_m f_m$ $(\star)$ for some polynomials $g_1, \ldots, g_m \in K[\underline{x}]$.*
- *Then there exist g_i of degree at most α satisfying $(\star)$.*

Proof:

- Suppose otherwise: For some fixed n, d, no α works in general.
- For each $\alpha \in \mathbb{N}$, fix a counter-example: K_α and $f_\alpha, f_{1,\alpha}, \ldots, f_{m,\alpha}$
- One can show: Without loss, m is the same for all counter-examples.
- Put all K_α and $K_\alpha[\underline{x}]$ into M and consider $M^* \succ M$.
- In M^*, we find a counter-example with α infinite:
  (1) $K_\alpha \subseteq M^*$ is a field; $f, f_1, \ldots, f_m \in K_\alpha[\underline{x}]$ are of degree at most d.
  (2) There exist g_i satisfying $(\star)\ldots$; the g_i might have infinite degree!
  (3) There exist no g_i of degree $\leq \alpha$ satisfying $(\star)$.
- However, one can show: (2) implies that there also exist g_i of finite degree.
- This contradicts (3). □



Around Model Theory of $\mathbb{Q}_p$

Norms on fields

- As you know, $\mathbb{R}$ is the completion of $\mathbb{Q}$...
- ...with respect to the usual metric, coming from the absolute value on $\mathbb{Q}$.
- But there exist other norms on $\mathbb{Q}$ inducing other metrics:

Definition

A **norm** *on a field K is a map $|\cdot|: K \to \mathbb{R}_{\geq 0}$ such that*

- $|0| = 0$, $|1| = 1$.
- $|a \cdot b| = |a| \cdot |b|$
- *Triangle inequality:* $|a + b| \leq |a| + |b|$

"Usual" norm on $\mathbb{Q}$: the absolute value

Other norms on $\mathbb{Q}$: For each prime p, the p-**adic norm** $|\cdot|_p$:

- Given $q \in \mathbb{Q}^\times$, consider the prime factor decomposition $q = \prod_i p_i^{r_i}$ $(r_i \in \mathbb{Z})$. Set $|q|_{p_i} := p_i^{-r_i}$.
- **Examples:** $|17|_3 = 1$, $|18|_3 = \frac{1}{9}$, $\frac{1}{100} = 1$, $|\frac{1}{3}|_3 = 3$;

"close to 0" ↑ (under $|18|_3$)

"far away from 0" ↑ (under $|\frac{1}{3}|_3$)

The p-adic numbers

Definition

The p-adic numbers $\mathbb{Q}_p$ is the field obtained as the completion of $\mathbb{Q}$ with respect to the metric induced by $|\cdot|_p$.

How do elements of $\mathbb{Q}_p$ look like?

- For each $i \in \mathbb{N}$, fix some $a_i \in \{0, \ldots, p-1\}$.
- Consider $b_n = \sum_{i=0}^{n-1} a_i p^i$ (in base p, b_n has digits $a_{n-1}, \ldots, a_0$)
- For $m < n$, we have $b_n - b_m = \sum_{i=m}^{n-1} a_i p^i$.
  This is divisible by p^m, so $|b_n - b_m|_p \leq p^{-m}$.
- Thus $(b_n)_n$ is a Cauchy-sequence with respect to $|\cdot|_p$.
- Its limit is an element of $\mathbb{Q}_p$. We write it as a formal sum $\sum_{i=0}^{\infty} a_i p^i$.
  (a "number in base p with infinitely many digits before the decimal point".)
- In general, we have: $\mathbb{Q}_p = \{\sum_{i=N}^{\infty} a_i p^i \mid N \in \mathbb{Z}, a_i \in \{0, 1, \ldots, p-1\}\}$,
  i.e., also allow finitely many digits after the decimal point.

  Examples in $\mathbb{Q}_5$:
  - $\ldots 44444_5 + 1_5 = \ldots 00000_5$, so $\ldots 44444_5 = -1$
  - $\ldots 22223_5 \cdot 2_5 = \ldots 00001_5$, so $\ldots 22223_5 = \frac{1}{2}$

Motivation: a hard problem

- Problem (P): Given $f(\underline{x}) \in \mathbb{Z}[\underline{x}]$, find out whether $f = 0$ has an integer solution.
  I.e.: Does there exist an $\underline{a} \in \mathbb{Z}^n$ such that $f(\underline{a}) = 0$?
- This is very difficult in general.
  Example: Fermat's Last Theorem: $f(x, y, z) = x^k + y^k - z^k$ has no solution for each $k \geq 3$.

Theorem (Hilbert's 10th problem)

There exists no algorithm solving problem (P).

Side remarks:

- Since $\exists \underline{x}\colon f(\underline{x}) = 0$ is a L_{ring}-sentence, this means:
  There exists no algorithm deciding whether an L_{ring}-sentence holds in $\mathbb{Z}$.
  Thus, model theoretically, the ring $\mathbb{Z}$ is "wild".
- Similarly:
  There exists no algorithm deciding whether an L_{ring}-sentence holds in $\mathbb{Q}$.
- Open question:
  Does there exist an algorithm for Problem (P) in $\mathbb{Q}$?

Motivation: how $\mathbb{Q}_p$ helps

- Suppose $f \in \mathbb{Z}[\underline{x}]$ (or $f \in \mathbb{Q}[\underline{x}]$) is given.
- If f has no solution: how to prove that?
- One technique: check for solutions in $\mathbb{R}$
  - If there's no solution in $\mathbb{R}$, there's no one in $\mathbb{Q}$ either.
  - Checking for solutions in $\mathbb{R}$ is much easier (there exists an algorithm)...
    ...because it's complete and hence analytic methods can be used.
    ...and/or/equivalently: because model theory of $\mathbb{R}$ is well understood.
- Instead of $\mathbb{R}$, can also use any other completion of $\mathbb{Q}$, e.g. $\mathbb{Q}_p$.
  - Again, there exists an algorithm to check for solutions in $\mathbb{Q}_p$...
    ...because it's complete and hence analytic methods can be used.
    ...and/or/equivalently: because model theory of $\mathbb{Q}_p$ is well understood.
- Combining several completions of $\mathbb{Q}$ yields more information about f. The best thing to do: look at all completions.

Theorem (Ostrowski)

$\mathbb{R}$ and $\mathbb{Q}_p$ (for all primes p) are all completions of $\mathbb{Q}$.

Quantifier elimination in $\mathbb{Q}_p$

- How to decide whether $f = 0$ has a solution in K (for $K = \mathbb{R}$ or $K = \mathbb{Q}_p$)?
- A general approach: use q.e. (= quantifier elimination):
  - Find a quantifier free sentence ϕ equivalent to $\exists \underline{x}\colon f(\underline{x}) = 0$.
  - ϕ quantifier free $\Rightarrow$ easy to see whether it holds.

  Note: This needs "effective q.e.", i.e., an algorithm to find the quantifier-free formula.
- We already saw: $\mathbb{R}$ has (effective) q.e. in the language L_{oring}

Theorem (Macintyre)

$\mathbb{Q}_p$ has effective q.e. in a suitable language L_{Mac}.

Definition

- $L_{\mathrm{Mac}} = L_{\mathrm{ring}} \cup \{P_2, P_3, P_4, P_5, \dots\}$.
- *P_ℓ is a unary predicate: $P_\ell(a)$ iff a has an ℓ-th root in $\mathbb{Q}_p$.*

Thus, to find out whether $f = 0$ has a solution in $\mathbb{Q}_p$:

- Find an equivalent, quantifier free L_{Mac}-sentence ϕ.
- This is a boolean combination $m = n$ and $P_\ell(m)$ for integers m.
- Checking whether m has an ℓ-th root in $\mathbb{Q}_p$ is not very difficult.

Local-global principles

- ▷ We know: If $f = 0$ has a solution in $\mathbb{Q}$, then it has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all p.
- ▷ Sometimes, one has an equivalence:
  XXX is true in $\mathbb{Q}$ iff XXX is true in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all p.
  Such a result is called a "local-global principle".
  ($\mathbb{Q}$ is a "global field", $\mathbb{R}$ and $\mathbb{Q}_p$ are "local fields".)

An important example of a local-global principle:

- ▷ Suppose $f \in \mathbb{Q}[\underline{x}]$ is a quadratic form, i.e., all monomials have degree 2.
- ▷ Such an f always has the trivial solution $\underline{x} = 0$.
- ▷ A non-trivial solution in $\mathbb{Q}$ also yields one in $\mathbb{R}$ and $\mathbb{Q}_p$.

Theorem (Hasse–Minkowski)

A quadratic form $f \in \mathbb{Q}[\underline{x}]$ has a non-trivial solution in $\mathbb{Q}$ iff it has a non-trivial solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all p.

An algorithm for quadratic forms

How to decide whether a quadratic form f has a non-trivial solution in $\mathbb{Q}$?

- ▷ In $\mathbb{R}$ and in each $\mathbb{Q}_p$, we have an algorithm:
  Apply q.e. to $\exists \underline{x}\colon (\underline{x} \neq 0 \wedge f(\underline{x}) = 0)$.
- ▷ But we'd have to check this for infinitely many fields ($\mathbb{R}$ and all $\mathbb{Q}_p$)...
- ▷ An ingredient for this:
  There exists a language $L_{\mathrm{DP}} \supseteq L_{\mathrm{ring}}$ in which all fields $\mathbb{Q}_p$ *uniformly* have q.e.... more or less.
  - ▷ "Uniformly" means: Given $\phi(\underline{x})$, there exists a quantifier free $\psi(\underline{x})$ such that $\phi(\mathbb{Q}_p) = \psi(\mathbb{Q}_p)$ for every p.
  - ▷ "More or less" means: In reallity, there are still some quantifiers left, but they are harmless enough.
- ▷ This yields an algorithm deciding whether a sentence ψ holds in $\mathbb{Q}_p$ for all p.

Thus, to decide whether f has a non-trivial solution in $\mathbb{Q}$:

- ▷ Check whether $\mathbb{R} \models \exists \underline{x}\colon (\underline{x} \neq 0 \wedge f(\underline{x}) = 0)$
- ▷ Check whether for all $\exists \underline{x}\colon (\underline{x} \neq 0 \wedge f(\underline{x}) = 0)$ holds in all $\mathbb{Q}_p$ using L_{DP}.

Remark: If it's just about quadratic forms, there are simpler algorithms than using q.e.; however, using q.e. works very generally.

Remark: The Hasse–Minkowski Theorem cannot be true for all polynomials, since it yields an algorithm, but there is no algorithm for all polynomials.

And now for something completely different: a field similar to $\mathbb{Q}_p$

Recall: $\mathbb{Q}_p = \{\sum_{i=N}^{\infty} a_i p^i \mid N \in \mathbb{Z}, a_i \in \{0, 1, \ldots, p-1\}\}$

A very similar field: $\mathbb{F}_p((t))$

- $\mathbb{F}_p((t))$ consists of formal power series over the finite field $\mathbb{F}_p$ with finitely many negative powers of t allowed.
- Formally: $\mathbb{F}_p((t)) = \{\sum_{i=N}^{\infty} a_i t^i \mid N \in \mathbb{Z}, a_i \in \mathbb{F}_p\}$, where the sum is a formal sum.
- Since $\mathbb{F}_p = \{0, \ldots, p-1\}$, the only difference between $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ is:
  - In $\mathbb{Q}_p$, addition and multiplication is with carry.
  - In $\mathbb{F}_p((t))$, addition and multiplication is without carry.

"Theorem:" The bigger p is, the more similar $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are.
This can be made precise using model theory...

$\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are similar

Theorem (The "Transfer Principle" by Ax–Kochen/Ershov, 60s)

Given: an L_{ring}-sentence ϕ.
Then, for all sufficiently big prime p:

$$\mathbb{Q}_p \models \phi \iff \mathbb{F}_p((t)) \models \phi$$

- There are various generalizations of this theorem, to sentences in a bigger language, and even to sentences which are not really first order.
- This had several applications:
  - Some results could be proven only in $\mathbb{Q}_p$. (The proofs needed that $\mathbb{Q}_p$ has characteristic 0.)
  - Other results could be proven only in $\mathbb{F}_p((t))$. (The proofs only worked for power series fields.)
  - By the Transfer principle, for big p, all those results are valid for both, $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.

Classes of Tame Structures

Many classes of tame structures

- Recall: There is no chance of understanding all definable structures; so try to find classes "tame" structures.
  "M is tame" could mean, in the best possible case:
  - (1) One can classify the definable sets.
  - (2) One can classify all $M' \equiv M$.
  - (3) One can classify all types.
- (3) is very useful for (1) and (2).
- Up to now, we have seen
  - some specific examples of tame structures (e.g. $\mathbb{R}$, $\mathbb{C}$)
  - one class of tame structures: o-minimal structures.
- There exists a whole zoo of notions of tameness.
  Today, I will present a few more of them.
- Note: Since one often wants to be able to replace M by some $M' \succ M$, one usually requires not only M to be tame (in some given sense), but all $M' \equiv M$.

Independence of the language

Another general remark (about good notions of tameness):

- ▷ Different languages on a structure M can yield the same definable sets.
  Example: Definable sets in $\mathbb{R}$ are the same with the language L_{ring} as with the language L_{oring}, since "$x < y$" can be expressed as $x \neq z \wedge \exists z \colon x + z^2 = y$.
- ▷ Good notions of tameness should only depend on what's definable (and not on the actual language).
- ▷ For this reason: q.e. (quantifier elimination) is not considered.
  - ▷ Whether one has q.e. depends on the language.
    Example: $\mathbb{R}$ does *not* have q.e. in the language L_{ring}.
  - ▷ Even worse: By changing the language, *any* structure can be made to have q.e. (without changing which sets are definable):
    Add a relation symbol for every definable set.

O-minimal structures

Recall: M is **o-minimal** if there's an order on M (dense, without endpoints) and every definable subset of M is a finite union of points and intervals.

Examples:

- ▷ any dense linear order
- ▷ any real closed field in the language L_{oring}, e.g. $\mathbb{R}$
- ▷ $\mathbb{R}_{\exp}$, i.e, $\mathbb{R}$ in the language $L_{\mathrm{oring}} \cup \{\exp\}$

Note the following non-trivial fact:

Proposition

If M is o-minimal and $M' \equiv M$, then M' is o-minimal, too.

There are several other notions of tameness (all called "XXX-minimality") which are defined by specifying the definable subsets of M.

Strongly minimal structures

Definition

- M *is* **minimal** *if every definable subset of* M *is either finite or co-finite.*
- M *is* **strongly minimal** *if every* $M' \equiv M$ *is minimal.*

Example: $\mathbb{N}$ in the language $L_{\mathrm{ord}} = \{<\}$ is minimal but not strongly minimal.

Strongly minimal examples:

- the infinite set, in the empty language
- any algebraically closed field K in the language L_{ring}
  Indeed:
  - A polynomial equation $f(x) = 0$ defines a finite set.
  - A polynomial inequation $f(x) \neq 0$ defines a co-finite set.
- vector fields over any field K, in the language $L = \{0, +\} \cup \{\lambda_a \mid a \in K\}$, where λ_a is scalar multiplication by a.
  Note: No quantification over K possible (so no subspaces definable).

An independence relation

Definition

Given: Any structure M, a set $A \subseteq M$, an element $b \in M$.
We call b **algebraically independent** *of A if it is not contained in any finite, A-definable set.*

Example: In an algebraically closed field K:
If $L \subseteq K$ is a subfield then b is algebraically independent of L
in the model theoretic sense $\iff$ in the algebra sense.
Example: In a vector space V:
b is algebraically independent of $A \iff b$ is linearly independent of A.
Now suppose M is strongly minimal. Then:

- ▷ Any two maximal algebraically independent subsets of M have the same cardinality.
- ▷ This yields a notion of "dimension of M".
  Example: If M is a vector space, this is the usual dimension.
  Example: If M is an algebraically close field, this is the transcendence degree.
- ▷ $\{M' \mid M' \equiv M\}$ are classified by their dimension (up to isomorphism).

Stable structures

- ▷ Philosophy: An independence relation is very useful.
  In which structures does one exist?
- ▷ One answer: in "stable structures"
- ▷ In some (vague) sense, stable is the opposite of o-minimal:
  o-minimal = "on M, there is (essentially) only an order"
  stable = "on M there is no order at all".

Formally:

Definition

M is stable if the following does not exist:

- ▷ *a formula $\phi(\underline{x}, \underline{y})$*
- ▷ *a structure $M' \equiv M$*
- ▷ *elements $\underline{a}_i \in (M')^n$ for $i \in \mathbb{N}$*
- ▷ *... such that $M' \models \phi(\underline{a}_i, \underline{a}_j)$ iff $i < j$*

Examples of stable structures:

- ▷ any strongly minimal structure
- ▷ any abelian group in the language $L_{\mathrm{ag}} = \{0, +, -\}$
- ▷ the free (non-abelian) group in n generators (This is a big theorem!)

More about stability

There exist various equivalent characterisations of stable structures:

- stable $\iff$ there exists an independence relation satisfying certain axioms (but much weaker ones than in strongly minimal structures):
  - Notation: $A \mathop{\smile\!\!\!\!\!\!|}_C B$ means "A is independent of B over C"
  - Example axiom: $A \mathop{\smile\!\!\!\!\!\!|}_B C$ and $A \mathop{\smile\!\!\!\!\!\!|}_{B \cup C} D$ implies $A \mathop{\smile\!\!\!\!\!\!|}_B C \cup D$
- stable $\iff$ "There do not exist too many types."
  - Formally: M is stable iff there exists a cardinal κ such that: For any $A \subseteq M' \equiv M$ with $|A| \leq \kappa$, there exist $\leq \kappa$ many types over A
  - **Non-example:**
    - Consider $\mathbb{Q}$ in the language $\{<\}$.
    - $|\mathbb{Q}| = \aleph_0$, but there exist $2^{\aleph_0}$ types over $\mathbb{Q}$ (each $r \in \mathbb{R} \setminus \mathbb{Q}$ yields one)
    - This roughly explains: When there is an order around, one gets lots of types.

Further generalizations

There exist various generalizations of stability:

- The definitions are similar to stability:
  "There exists no formula ϕ defining some kind of thing"
- Several of these generalizations also imply:
  - there exists an independence relation satisfying certain axioms
  - certain forms of "there do not exist too many types"
- One such generalization: **NIP structures**
  Examples:
  - any o-minimal structure
  - the p-adic numbers $\mathbb{Q}_p$
  - $\mathbb{Z}$ in the language $L_{\mathrm{oag}} = \{0, +, -, <\}$
- Another such generalization: **simple structures**
  Examples:
  - the random graph
  - any pseudo-finite field

Overview


$\mathbb{Z}$ as a ring
$\mathbb{Q}$
NTP$_2$
simple
random graph
pseudo-finite fields
NIP
stable
abelian groups
$\mathbb{Q}_p$
$\mathbb{Z}$ as an ordered group
free non-abelian groups
o-minimal
$\mathbb{R}_{\exp}$
real closed fields
strongly minimal
vector spaces
algebraically closed fields
dense orders without endpoints
infinite sets