Model Theory in algebra

Guo Haoyang

March 2025

Contents

1 Introduction

Siegel's theorem of function field

Theorem 1.1: Siegel's theorem

Let K be a function field over a constant field k, R be a subring generated by finitely elements in K, E/K be an elliptic curve over K that is not a base change from k and $\varphi \in K(E)$ be a non-constant function. Then, $\left|\{P \in E(K) | \varphi(P) \in R\}\right| < \infty$

Now we are using Siegel's theorem. Suppose that S was finite and let $R' := R\left[\prod\right]$. Then, R' is a ring of finite type over $\mathbb{Q}$. Then, $P, 2P, \cdots \in \mathscr{E}(K)$ are infinitely many

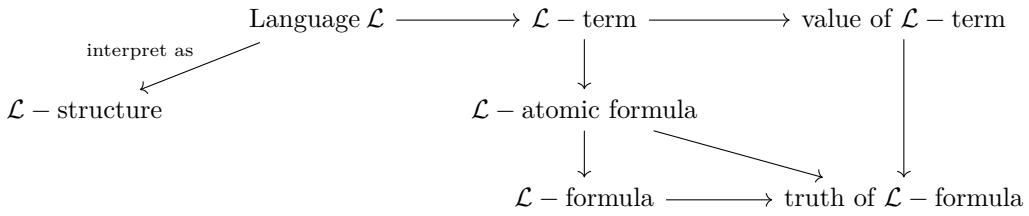
The special subvarieties of $\mathscr{E}$:
(1) $\mathscr{E}$ (2) $\mathscr{E}_\lambda$, such that λ is special (3) Torsion sections (4) torsion points of special $\mathscr{E}_\lambda$ What is special variety?
One has an 'inherited' notion of special subvarieties. $\mathscr{E}^2 = \mathscr{E} \times_{\mathbb{P}-\{0,1,\infty\}} \mathscr{E} = \mathscr{E}_\lambda \times \mathscr{E}_\lambda$

2 O-minimality and model theory

2.1 Basic definitions in logic

2.1.1 Languages and models

This theory is part of mathematical logic. Pertaining to logic and mathematical logic, although this topic is partial mathematical logic, there is a parlance I really like to mention: 'Logic is the study of reasoning; and mathematical logic is the study of the type of reasoning done by mathematicians.' [Sho67]
The follows are some concepts modeling structures we met in different fields, such as sets, rings, ordered rings and so on. Relations between those concepts are in the following chart. All contents mainly come from [02] and [WD15].



Definition 2.1: Language

A language $\mathcal{L} = \left\{\mathcal{F}, \{n_f\}_{f\in\mathcal{F}}, \mathcal{R}, \{n_R\}_{R\in\mathcal{R}}, \mathcal{C}\right\}$ is given by the following data:
(1) A set of function symbols $\mathcal{F}$ and a set of positive integers $\{n_f\}$ by assigning each $f \in \mathcal{F}$ an n_f [a].
(2) A set of function relation $\mathcal{R}$ and a set of positive integers $\{n_R\}$ by assigning each $R \in \mathcal{R}$ an n_R [b].
(3) A set of constant symbols $\mathcal{C}$.

[a] n_f indicates the arity(number of variables) of the functions
[b] n_R indicates the number of elements the relation involves

Remark The number n_f tells us f is a function of n_f variables and the number n_R tells us R is an n_R-ary relations.
Any one or all of $\mathcal{F}, \mathcal{R}, \mathcal{C}$ may be empty. (1) The language of rings $\mathcal{L}_\mathrm{r} = \left\{\{+,-,\cdot\}, \{2 = n_+, 2 = n_-, 2 = n_\cdot\}, \varnothing, \varnothing, \{\mathbf{0}, \mathbf{1}\}\right\}$
(2) The language of ordered rings $\mathcal{L}_\mathrm{or} = \left\{\{+,-,\cdot\}, \{2 = n_+, 2 = n_-, 2 = n_\cdot\}, \{<\}, \{2 = n_<\}, \{\mathbf{0}, \mathbf{1}\}\right\}$
(3) The language of pure sets $\mathcal{L} = \varnothing$

(4) The language of graphs $\mathcal{L}$ what is the language of graphs?
Overall, we choose the language that is closed related to the structure we wish to study ([02]).

Definition 2.2: $\mathcal{L}$-structure/Model

Let $\mathcal{L}$ be a language. A $\mathcal{L}$-structure $\mathcal{M}$ can be simply given by $(M, \mathcal{I})$:
• A set $M \neq \varnothing$, called the universe, domain or the underlying set of $\mathcal{M}$
• An interpretation function $\mathcal{I}$, which interprets $\mathcal{F}, \mathcal{R}, \mathcal{C}$ inside $\mathcal{L}$ as:
(1) $\forall f \in \mathcal{F}$, a function with notation $\mathcal{I}(f) = f^{\mathcal{M}} : M^{n_f} \to M$
(2) $\forall R \in \mathcal{R}$, a set with notation $\mathcal{I}(R) = R^{\mathcal{M}} \subseteq M^{n_R}$
(3) $\forall c \in \mathcal{C}$, an element with notation $\mathcal{I}(c)$ or $c^{\mathcal{M}}$

Remark So, $\mathcal{M} = M \cup \{f^{\mathcal{M}}\}_{f\in\mathcal{F}} \cup \{R^{\mathcal{M}}\}_{R\in\mathcal{R}} \cup \{c^{\mathcal{M}}\}_{c\in\mathcal{C}}$
An $\mathcal{L}$-structure gives an abstract language an interpretation to make it concrete.
A structure for $\mathcal{L}_{\mathrm{r}}$ consists of a non-empty set R; operations $+, -, \cdot$ $(+ = +^{\mathcal{M}}, - = -^{\mathcal{M}}, \cdot = \cdot^{\mathcal{M}})$; identity elements $0 = \mathbf{0}^{\mathcal{M}}, 1 = \mathbf{1}^{\mathcal{M}}$.

Usually we choose the language that is closely related to the model we study.

As a routine, after introducing some objects, we establish the morphism between them. So, the next concept is to introduce the morphism between two $\mathcal{L}$-structures.

Definition 2.3: $\mathcal{L}$-embedding

Let $\mathcal{L}$ be a language and let $\mathcal{M}, \mathcal{N}$ be $\mathcal{L}$-structures, with universe M and N respectively. An $\mathcal{L}$-embedding is a injective map $\eta : M \to N$ that **preserves the interpretation of all symbols of** $\mathcal{L}$, i.e.
(1) $\forall f \in \mathcal{F}$, $\forall (a_1, \ldots, a_{n_f}) \in M^{n_f}$, $\eta \circ f^{\mathcal{M}} = f^{\mathcal{N}} \circ \eta^{n_f}$, i.e. the following diagram commutes:

$$\begin{array}{ccc} M^{n_f} & \xrightarrow{\eta^{n_f}} & N^{n_f} \\ {\scriptstyle f^{\mathcal{M}}}\downarrow & & \downarrow{\scriptstyle f^{\mathcal{N}}} \\ M & \xrightarrow{\eta} & N \end{array}$$

(2) $\forall R \in \mathcal{R}$, $\forall a_1, \ldots, a_{n_f} \in M$, $(a_1, \ldots, a_{n_f}) \in M^{n_f} \Leftrightarrow (\eta(a_1), \ldots, \eta(a_{n_f})) \in N^{n_f}$
(3) $\forall c \in C$, $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$
A bijective $\mathcal{L}$-embedding is an $\mathcal{L}$-isomorphism.
$\mathcal{M}$ is a substructure of $\mathcal{N}$, or $\mathcal{N}$ is an extension of $\mathcal{M} \Leftrightarrow M \subseteq N$ and $M \hookrightarrow N$ is an $\mathcal{L}$-embedding.

2.1.2 Terms and formulae

To describe $\mathcal{L}$-structures/models, the goal is to develop $\mathcal{L}$-terms and $\mathcal{L}$-formulae.
There are two ways to define the $\mathcal{L}$-terms and $\mathcal{L}$-formula. One is a recursive definition and another one is up-side-down: without defining what is an $\mathcal{L}$-term explicitly, make an anticipation on the collection of all $\mathcal{L}$-terms [02]. A similar trick is applied to $\mathcal{L}$-formulae.

Definition 2.4: $\mathcal{L}$-term

Let $\mathcal{L}$ be a language.
Top-down definition: (instead of saying what is an $\mathcal{L}$-term, we say what is the set of $\mathcal{L}$-terms.
The set of $\mathcal{L}$-terms is the smallest set $\mathcal{T}$ such that:
•(Constant symbol) $\forall c \in \mathcal{C}$, $c \in \mathcal{T}$
•(Variable symbol) each variable symbol: $\forall i$, $v_i \in \mathcal{T}$
•(Recursively) $\forall f \in \mathcal{F}$, $\forall t_1, \ldots, t_{n_f} \in \mathcal{T}$, then $f(t_1, \ldots, t_{n_f}) \in \mathcal{T}$

Remark An observation of $\mathcal{L}$-terms is it has the same hierarchy as Language $\mathcal{L}$, although it is defined using $\mathcal{L}$.
For the top-down version definition, the third one is saying that: to see if something is an $\mathcal{L}$-term, we just need to peel off the shell made of function symbols to see if the core consists of elements either constant or variable symbols.
Can we put terms on the places of variables of a function or a relation?
In [Cal13], the definition of a term does not use words like 'the smallest', it consists of four things: the first three

and one more: 'a string of symbols is a term if it can be shown to be a term by a finite number of applications from (i) to (iii)'. Are these two definitions equivalent? Then is a similar definition true for formula?

Do not forget that our goal is to express statements on $\mathcal{L}$-structures (using elements of an $\mathcal{L}$-structure/model $\mathcal{M}$) mentioned at the beginning of this chapter. Since $\mathcal{L}$-term is in the same hierarchy as $\mathcal{L}$, we require interpretations on $\mathcal{L}$-term $\mathcal{T}$[1] as what we did for $\mathcal{M}$:

Definition 2.5: Interpretation of $\mathcal{L}$-terms

Let $\mathcal{L}$ be a language, $\mathcal{T}$ be an $\mathcal{L}$-term and $\mathcal{M}$ be an $\mathcal{L}$-structure/model. Then, for a given $\overline{a} = (a_1, a_2, \dots, a_{n_f}) \in M^{n_f}$, where each $a_i \in M$, and a given $t \in \mathcal{T}$, we can define the **value** of t at $\overline{a}$ or the **interpretation** of t(as a function $t^{\mathcal{M}} : M^{n_f} \to M$), denoted $t^{\mathcal{M}}(\overline{a})$, to be
•(variable symbol) $t = v_i$ for some v_i: $t^{\mathcal{M}}(\overline{a}) = a_i$
•(constant symbol) $t = c$: $t^{\mathcal{M}}(\overline{a}) = c^{\mathcal{M}}$
•(recursively) $t = f(t_1, \dots, t_{n_f})$, where $t_1, \dots, t_{n_f}$ are terms: $t^{\mathcal{M}}(\overline{a}) = f^{\mathcal{M}}(t_1^{\mathcal{M}}(\overline{a}), \dots, t_{n_f}^{\mathcal{M}}(\overline{a}))$
So, $t^{\mathcal{M}} : M^{n_f} \to M$ is defined to be $\overline{a} \mapsto t^{\mathcal{M}}(\overline{a})$

The atomic $\mathcal{L}$ formulae are directly defined but $\mathcal{L}$-formulae are up-side-down. Is the subterm here actually necessary here?

The definition of a formula is hierarchical.

Definition 2.6: $\mathcal{L}$-formula

Let $\mathcal{L}$ be a language and $\mathcal{T}$ be an $\mathcal{L}$-term.
Atomic $\mathcal{L}$-formula: An atomic $\mathcal{L}$-formula is any one of the followings:
• $t_1 = t_2$, where $t_1, t_2 \in \mathcal{T}$ are $\mathcal{L}$-terms
• $R(t_1, \dots, t_{n_R})$, where $R \in \mathcal{R}$ and $t_1, \dots, t_{n_R} \in \mathcal{T}$ are $\mathcal{L}$-terms.
$\mathcal{L}$-formula: The set of all $\mathcal{L}$-atomic formulae is the smallest set $\mathcal{W}$ such that:
• $\mathcal{W}$ contains all atomic $\mathcal{L}$-formulae
• $\phi \in \mathcal{W} \Rightarrow \neg\phi \in \mathcal{W}$
• $\phi, \psi \in \mathcal{W} \Rightarrow \phi \wedge \phi, \phi \vee \psi \in \mathcal{W}$
• $\phi \in \mathcal{W} \Rightarrow \forall v_i\, \phi, \exists v_i\, \phi \in \mathcal{W}$, where v_i is a variable symbol (then $v_i \in \mathcal{T}$)

For a variable symbol v, we say it is **bound** if there is appearance in the scope of an $\exists$ and $\forall$ quantifier the formula ϕ. Otherwise it is said to be **free**. In our context here, formulae are frugal with variables. More precisely, we assume that each formula has each variable either bound or free. [2]
Some shorthand for a formula: [3]

Definition 2.7: Sentence

A formula ϕ is called a sentence $\Leftrightarrow \forall$ variable appearing in ϕ, ϕ is bounded, appearing in the scope of $\forall$ or $\exists$ quantifiers.

Remark $\phi(v_1, v_2)$ $v_1 = v_2^2$ is a formula, not a sentence.
$\exists v_1 : v_1 = v_2^2$ $\phi(v_2)$
What is the number here, an arbitrary n or just n_R w.r.t. R?

Given a formula, we care about the truth of that formula. Assign a formula a value ($\overline{a} \in M^{n_R}$, is the formula true or false. The following definition helps us answer this question.

[1] some author prefer to call it 'give a value to $t \in \mathcal{T}$' [WD15]
[2] A good example to be frugal with variables in [02] is consider $v_1 > 0 \vee \exists v_1\, v_1 \cdot v_1 = v_2$ (here it is actually $\cdot(v_1, v_1) = v_2$), it is equivalent to $v_1 > 0 \vee \exists v_3\, v_3 \cdot v_3 = v_2$.
[3] for $p \to q$ there are many natural language expressions:
• q whenever p/ q if p/ q when p/ q follows from p/ p only if q/ if p, (then) q
• q is sufficient for p/ p is necessary for q
• q unless p

Definition 2.8: Truth of a formula

Let ϕ be a formula with free variable $\overline{v} = (v_1, \ldots, v_{n_f})$ and $\overline{a} = (a_1, \ldots, a_{n_f}) \in M^{n_f}$.
$\mathcal{M}$ satisfies $\phi(\overline{a})$ or $\phi(\overline{a})$ is true in $\mathcal{M}$, denoted $\mathcal{M} \vDash \phi(\overline{a})$, is inductively defined as:
- $\phi = (t_1 = t_2)$ [a] $\mathcal{M} \vDash \phi(\overline{a}) := (t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}))$
- $\phi = R(t_1, \ldots, t_{n_R})$, where $R \in \mathcal{R}$ and $t_1, \ldots, t_{n_R} \in \mathcal{T}$, then $\mathcal{M} \vDash \phi(\overline{a}) := \left((t_1^{\mathcal{M}}(\overline{a}), \ldots, t_{n_R}^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}}\right)$

Inductive cases:
- $\phi = \neg\psi$, $\mathcal{M} \vDash \phi(\overline{a}) := \left(\mathcal{M} \nvDash \psi(\overline{a})\right)$
- $\phi = \psi \vee \theta$, $\mathcal{M} \vDash \phi(\overline{a}) := \left(\mathcal{M} \vDash \psi(\overline{a}) \vee \mathcal{M} \vDash \theta(\overline{a})\right)$
- $\phi = \psi \wedge \theta$, $\mathcal{M} \vDash \phi(\overline{a}) := \left(\mathcal{M} \vDash \psi(\overline{a}) \wedge \mathcal{M} \vDash \theta(\overline{a})\right)$
- $\phi = \exists v_j\, \phi(\overline{v}, v_j)$, then $\mathcal{M} \vDash \phi(\overline{a}) := \left(\exists b \in M, \mathcal{M} \vDash \phi(\overline{a}, b)\right)$
- $\phi = \forall v_j\, \phi(\overline{v}, v_j)$, then $\mathcal{M} \vDash \phi(\overline{a}) := \left(\forall b \in M, \mathcal{M} \vDash \phi(\overline{a}, b)\right)$

[a] the first $=$ serves for the common notion of equality and the second $=$ serves as a logic symbol

For any $\mathcal{L}$-structure $\mathcal{M}$, every sentence is either true or false. But, a formula is not necessarily has a truth value, in other words, sometimes true and sometimes false [4].
Is it the case that only one of $\mathcal{M} \vDash \phi$ and $\mathcal{M} \vDash \neg\phi$ is true? Why? and where?

2.1.3 Theories and Axioms

From now on, by abusing notation, $\mathcal{T}$ is assigned a new meaning, $\mathcal{L}$-theory.

Definition 2.9: $\mathcal{L}$-theory and Satisfiability

Let $\mathcal{L}$ be a language. An $\mathcal{L}$-**theory** is a set $\mathcal{T}$ of $\mathcal{L}$-sentences.
An $\mathcal{L}$-structure is a **model** of $\mathcal{T}$, written as $\mathcal{M} \vDash \mathcal{T} \Leftrightarrow \forall \phi \in \mathcal{T}, \mathcal{M} \vDash \phi$
An $\mathcal{L}$-formula ϕ is **satisfiable** $\Leftrightarrow \exists$ $\mathcal{L}$-model $\mathcal{M}$, $\mathcal{M} \vDash \phi$
An $\mathcal{L}$-theory $\mathcal{T}$ is **satisfiable** $\Leftrightarrow \exists$ $\mathcal{L}$-model $\mathcal{M}$, such that $\mathcal{M} \vDash \mathcal{T} \Leftrightarrow \forall \phi \in \mathcal{T}$, ϕ is satisfiable.

Definition 2.10: Axioms

Still $\mathcal{L}$ is a language. Let Δ be an $\mathcal{L}$-theory. Δ is an axiom $\Leftrightarrow \{\phi : \mathcal{T} \vDash \phi\} = \{\phi : \triangle \vDash \phi\}$ In other words, Δ has the same set of consequences as the theory $\mathcal{T}$ itself.

Remark Axioms and theories
(1) Linear orders: Let $\mathcal{L} = \{<\}$, and $<$ is the binary relation symbol. The axioms for linear orders consist of the following $\mathcal{L}$-sentences:
- (Not self-contradicting) $\forall x \quad \neg(x < x)$
- (Transitivity) $\forall x \forall y \forall z \quad ((x < y \wedge y < z) \to x < z)$
- (Trichotomy) $\forall x \forall y \quad (x < y \vee x = y \vee y < x)$

(5) Ordered fields:
- Axioms for fields
- Axioms for linear orders
- $\forall x \forall y \forall z \quad (x < y \to x + z < y + z)$
- $\forall x \forall y \forall z \quad ((x < y \wedge z > 0) \to x \cdot z < y \cdot z)$

Definition 2.11: Elementary Class and Full theory

Let $\mathcal{K}$ be a class of $\mathcal{L}$-structures. $\mathcal{K}$ is an **elementary class** $\Leftrightarrow \exists$ an $\mathcal{L}$-theory $\mathcal{T}$, $\mathcal{K} = \{\mathcal{M} : \mathcal{M} \vDash \mathcal{T}\}$
There is a dual concept, **full theory** of an $\mathcal{L}$-structure $\mathcal{M}$, denoted $\mathrm{Th}(\mathcal{M})$. $\mathrm{Th}(\mathcal{M}) = \{\mathcal{T} : \mathcal{M} \vDash \mathcal{T}\}$

In every structure M, a sentence is either true or not write accordingly $\mathcal{M}$ be an $\mathcal{L}$-structure with underlying set M. M is definable (in $\mathcal{L}$) $\Leftrightarrow \exists$ an $\mathcal{L}$-formula $\phi(\overline{v}, \overline{w}) = \phi(v_1, \ldots, v_n, w_1, \ldots, w_m)$, where $m, n \geq 0$ and $b \in M^m$ such that

$$X = \{\overline{a} \in M^n | \mathcal{M} \vDash \phi(\overline{a}, \overline{b})\}$$

[4] An example is in the $\mathcal{L}_{\mathrm{or}}$-structure $\mathbb{R}$: $\exists v_2 v_2 \cdot v_2 = v_1$ is true when v_1 is non-negative and false when v_1 is negative, $\forall v_1 \exists v_2 v_2 \cdot v_2 = v_1$ is false

Definition 2.12: Definable sets

Let $\mathcal{L}$ be a language and $\mathcal{M}$ be an $\mathcal{L}$-structure with underlying universe M. Let $X \subseteq M^n$ for some n.
X is **definable** $\Leftrightarrow \exists$ an $\mathcal{L}$-formula $\phi(\overline{v}, \overline{w}) = \phi(v_1, \ldots, v_n, w_1, \ldots, w_m)$ and $\exists \overline{b} \in M^m$, such that

$$X = \{\overline{a} \in M^n | \mathcal{M} \vDash \phi(\overline{a}, \overline{b})\}$$

In this case, it is said that $\phi(\overline{v}, \overline{b})$ **defines** X.
X is A-**definable** or **definable over** $A \Leftrightarrow \exists$ an $\mathcal{L}$-formula $\phi(\overline{v}, \overline{w}) = \phi(v_1, \ldots, v_r, w_1, \ldots, w_l)$ and $\exists \overline{b} \in A^l$, such that $\phi(\overline{v}, \overline{b})$ defines X.

Remark The difference between definability and A-definability is the scope of $\overline{b}$ is restricted to A.
What is the requirement of the number of variables? In each examples, we let the language be $\mathcal{L}_{\mathrm{r}}$
(1) Let the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{R, +, -, 0, 1\}$ be a ring. Let $p(y) \in R[y]$ be a polynomial and consider the set

$$Y = \{x \in R : p(x) = 0\}$$

which is the solution of $p(y)$ in the ring R, and it is definable and A-definable for some certain A. Why? Suppose that $p(y) = \sum_{i=0}^{n} a_i y^i$, so we could consider the $\mathcal{L}$-formula $\phi(v, w_0, \ldots, w_n)$ to be

$$\phi(v, w_0, \ldots, w_n) := \quad w_n \cdot v^n + \cdots + w_1 \cdot v_1 + w_0 = \mathbf{0}^{5}$$

The left hand side is linear combination of variables, hence it is a term. On the right hand side, there is only one identity symbol, so it is also a term. Therefore, this ϕ is an atomic formula. If picking $\overline{w} = (w_0, \ldots, w_n)$ to be $\overline{a} = (a_0, \ldots, a_n)$, then $\phi(v, \overline{a})$ defines Y. In particular, Y is A-definable for any $A \supseteq \{a_0, \ldots, a_n\}$
(2) Let the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{\mathbb{R}, +, -, 0, 1\}$ be the real numbers.
(3) Let the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{\mathbb{Z}, +, -, 0, 1\}$ be the ring of integers.
(4) Let F be a field Is F a set or a structure? and the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{F[x], +, -, 0, 1\}$ be the ring of polynomials.
(5) Let the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{\mathbb{C}(x), +, -, 0, 1\}$ be the field of complex rational functions in one variable.
(6) Let the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{\mathbb{Q}_p, +, -, 0, 1\}$ be the field of p-adic numbers.
(7) Let the $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M} = \{\mathbb{Q}, +, -, 0, 1\}$ be the field of rational numbers.
Now we give a characterisation of definable sets which makes the prediction of whether a set is definable easier:

Proposition 2.1: Characterisation of definable sets

Let $\mathcal{L}$ be a language and $\mathcal{M}$ be an $\mathcal{L}$-structure. $\forall n \geq 1$, let D_n be a collection of subsets of M^n such that

$$D = (D_n | n \geq 1)$$

is the smallest collection with the properties listed below:
(1) (total space) $\forall n$, $M^n \in D_n$
(2) (graphs) $\forall$ n-ary function symbol f, $\Gamma_f \mathcal{M} = \{(\overline{x}, f(\overline{x})) | \overline{x} \in M^n\}$
(3) (relation) $\forall$ n-ary relation symbol R, $R^{\mathcal{M}} \in D_n$
(4) (diagonals) $\forall i, j \leq n$, $\{(x_1, \ldots, x_n) \in M^n : x_i = x_j\} \in D_n$
(5) (product) if $X \in D_n$, then $M \times X \in D_{n+1}$
(6) (Boolean) Each D_n is closed under complement union and intersection
(7) (projection) if $X \in D_{n+1}$, and π is defined as $\pi : M^{n+1} \to M^n \quad (x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n)$, then $\{a \in M^n : (a, b) \in X\} \in D_n$
(8) (truncation) if $X \in D_{n+m}$ and $b \in M^m$, then $\{a \in M^n : (a, b) \in X\} \in D_n$
Then, for some n, $X \subseteq M^n$ is definable $\Leftrightarrow X \in D_n$

What does the bracket mean here? D is the collection of definable sets in $\mathcal{L}$?

Proof: □
There are two kinds of consequences: syntactic consequence and semantic consequence.
How to motivate the following defintion?

[5] here v^n is a shorthand of $\underbrace{v \cdot \cdots \cdot v}_{n-\text{times}}$. From now on, we will abbreviate products if no confusion arises.

Definition 2.13: Semantic consequence

Let $\mathcal{L}$ be a language, $\mathcal{T}$ be an $\mathcal{L}$-theory and ϕ be an $\mathcal{L}$-formula.
ϕ is a logical consequence of $\mathcal{T} \Leftrightarrow \forall$ $\mathcal{L}$-structure $\mathcal{M}$, $\mathcal{M} \vDash \mathcal{T} \Rightarrow \mathcal{M} \vDash \phi$

Remark The book [EFT21] provides a clearer description of the definition.
The definition says that for every model $\mathcal{M}$ of $\mathcal{L}$-theory $\mathcal{T}$, [6] $\mathcal{M}$ is also a model for ϕ

What's true in $\mathbb{R}$ should be true in any real fields

Example. Let $c : \mathbb{C} \to \mathbb{C}$ be taking complex conjugate, and $\sigma : \mathbb{C} \to \mathbb{C}$be any field automorphism with, $\tau := \sigma c \sigma^{-1}$, then $R = \mathbb{C}^{\tau}$ is a real closed field and
$T \vDash \phi$ is Emperical truth? and $T \vdash \phi$ is Formal proof?

Theorem 2.1: Gödel's completeness theorem

Let $\mathcal{L}$ be a language, T be an $\mathcal{L}$-theory and ϕ be an $\mathcal{L}$-sentence. Then,

$$T \vDash \phi \Leftrightarrow T \vdash \phi$$

Theorem 2.2: Consistency and Satisfiablility

Let $\mathcal{L}$ be a language, T be an $\mathcal{L}$-theory. T is consistent $\Leftrightarrow$ T is satisfiable.

Theorem 2.3: Compactness theorem

Let $\mathcal{L}$ be a language, T be an $\mathcal{L}$-theory. T is satisfiable $\Leftrightarrow \forall$ finite subset of T is satisfiable.

Remark To make this statement shorter, introduce **finitely satisfiable**: An $\mathcal{L}$-theory is finitely satisfiable $\Leftrightarrow \forall$ finite subset $\Delta \subseteq \mathcal{T}$, Δ is satisfiable.
Then this theorem is rephrased as: a theory $\mathcal{T}$ is satisfiable $\Leftrightarrow$ $\mathcal{T}$ is finitely satisfiable.
Although the compactness theorem is a consequence of , it is still the
This theorem is often used in the contrapositive form: if $\mathcal{T}$ is unsatisfiable $\Leftrightarrow \exists$ a finite subset $\Delta \subseteq \mathcal{T}$ that is unsatisfiable.
It is true for both propositional logic and first order logic.

Proof: Here is the proof in propositional logic. The case of countably many propositions is considered. For a larger cardinality, it is almost the same proof, but in conjunction with the axiom of choices. □

Some applications of the compactness theorem [Var]
• 4-color problem
The compactness theorem proves this theorem. Combining this theorem and the classic Four color theorem, one can deduce an infinite version of the four color theorem.

Theorem 2.4: Characterisation of k-colourability

A graph Γ is k-colorable $\Leftrightarrow$ every finite subgraph of Γ is k-colorable.

Proof: □

Theorem 1 (Four color theorem) *Every finite planar graph is* 4*-colorable.*

Theorem 2 (Infinite four color theorem) *Every infinite planar graph is* 4*-colorable.*

Proof: Fix an infinite planar graph Γ. We want every finite subgraph of Γ to be 4 colorable so that Γ is also 4 colorable. Every subgraph of a planar graph is planar, so is every finite subgraph of Γ. Then, theorem 2.4 suggests that every finite subgraph of Γ is 4-colorable. □
• König's Lemma

[6] whether $\mathcal{T}$ is satisfiable or not is ok, when it is not, then this is vacuously true

Theorem 2.5: König's lemma

Every finitely-branching infinite tree has an infinite path.

• Extension of partial order

Theorem 2.6: Extending partial orders

Every partial order can be extended to a total order.

Definition 2.14: Complete theory

Let $\mathcal{L}$ be a language and $\mathcal{T}$ be an $\mathcal{L}$-theory. $\mathcal{T}$ is **complete** $\Leftrightarrow \forall$ $\mathcal{L}$-sentence ϕ, either $T \vDash \phi$ or $T \vDash \neg\phi$

A tacit question: Is it possible that both cases happen?

2.2 Quantifier Elimination

Why do we care about quantifier elimination? Informally speaking, given a logical statement with some variables being quantified. We want to get rid of those quantifiers. For example, given a formula in the language $\mathcal{L}_{\mathrm{r}}$

$$\exists x(ax^2 + bx + c = 0 \wedge a \neq 0)$$

there is an elimination $a \neq 0 \wedge b^2 - 4ac \geq 0$ (here $b^2 - 4ac \geq 0$ is an abbreviation of $b^2 - 4ac > 0 \wedge b^2 - 4ac = 0$). This gives us some feelings on this concept. So, first, quantifier elimination is a concept of simplification. In addition, the input quantified formula can be viewed as a question, and the output free formula is a solution or an answer to that question. [Bro02]

Definition 2.15: Quantifier elimination

Let $\mathcal{T}$ be an $\mathcal{L}$-theory, with $\mathcal{L}$ a language.
$\mathcal{T}$ has a quantifier elimination $\Leftrightarrow \forall$ $\mathcal{L}$-formula ϕ, $\exists$ quantifier-free formula ψ such that $T \vDash (\phi \leftrightarrow \psi)$

Remark This means that in every model, ϕ holds $\Leftrightarrow \psi$ holds. And $\phi \leftrightarrow \psi$ is a shorthand for $(\neg\phi \vee \psi) \wedge (\neg\psi \vee \phi)$

2.3 Algebraically closed fields

Two ACFs are isomorphic $\Leftrightarrow$ they have the same characteristics and the same transcendence degree over their prime fields.

Corollary 2.1: Cardinality of definable sets

A definable set is either finite or cofinite.

If F is such a field and F_0 is its prime field then

$$|F| = \aleph_0 + \operatorname{tr\,deg}_{F_0}(F) \overset{\dagger}{=} \operatorname{tr\,deg}_{F_0}(F)$$

†: if $|F| > |F_0|$ ACF_p is κ-categorical for all $\kappa > \aleph_0$
Both $\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}(t)}$ have cardinality $\aleph_0$ and are not isomorphic as fields.

2.4 Real fields

2.4.1 Basic notions of real fields

Definition 2.16: Formally real field

This could be worked on either the field in algebra or some $\mathcal{L}_{\mathrm{r}}$-structure $\mathcal{M}$ with the universe being interpreted as a field.
Let F be a field. F is **(formally) real** $\Leftrightarrow -1$ is not a sum of squares.
Let $\sum F^2$ denote the set of all sum of squares of F. A rephrase is: F is **formally real** $\Leftrightarrow -1 \notin \sum F^2$

Remark Usually, this definition is used in its contraposition: a field is not real $\Leftrightarrow \exists f_1, \ldots, f_n \in F$, $-1 \in \sum_{i=1}^{n} f_i^2$
• This definition captures some properties of the real numbers. Also, a very straightforward example of (formally) real is the real number $\mathbb{R}$ itself, since $-1 \notin \sum \mathbb{R}^2$

Definition 2.17: Real closed field

A real closed field is a real field that has no formally real proper algebraic field extension.

There are many examples of real closed fields:
(1) Field of real algebraic numbers
(2) Field of Puiseux series with real coefficients: We will shed some light on this field on the following subsubsection. This is not only an example for real algebraic geometry, but also an important tool in classical and real algebraic geometry.
(3)Levi-Civita field
and so on

2.4.2 Orders and real fields

In this little section, we study the connection between the (formally) real fields and the orders. Since at the very beginning, for the sake of generality, the language we put is the language og rings $\mathcal{L}_{\mathrm{r}}$, not the language of ordered rings $\mathcal{L}_{\mathrm{or}}$. Here, we will reveal that ordered fields are (formally) real and a field is real is equivalent to put an order on it:

Theorem 2.7: Order implying real

An ordered field is a (formally) real field.

Proof: □

Theorem 2.8: Orders on real fields

Any real field is orderable. Moreover, if $a \in F$ but $-a \notin \sum F^2$, then $\exists$ an ordering that makes $a > 0$.

Proof: The core is to construct an ordering on F. But, we first consider the real closure of F, R. Define an 'order' on R to be: $\forall x \forall y$, $x < y \Leftrightarrow$ their difference $y - x$ is a sum of squares of non-zero elements in R, i.e.

$$x < y := y - x \in \sum R^{\times 2}$$

We are going to check this is an order on R. First it is a linear order:
• $\forall x \in R$, $x - x = 0 \notin \sum R^{\times 2}$, so $\neg(x < x)$.
• $\forall x \forall y \forall z$, $x < y$ and $y < z$ imply that $y - x = \sum_i a_i^2 \in \sum R^{\times 2}$ and $z - y \sum_j b_j^2 \in \sum R^{\times 2}$. Then, $z - x = \sum_{i,j} a_i^2 + b_j^2 \in \sum R^{\times 2} \Leftrightarrow x < z$.
• $\forall x \forall y$, if $x = y$,done. If $x \neq y$, then let $a := y - x$. We are going to show that either $a \in \sum R^{\times 2}$ or $-a \in \sum R^{\times 2}$. Suppose otherwise, neither is inside $\sum R^{\times 2}$. Then, $R(\sqrt{a})$ is a real algebraic field extension of R. Since R is already algebraic closed, $R(\sqrt{a}) = R$. But, this means $a \in \sum R^{\times 2}$, contradicting to the assumption that neither of a and $-a$ is in $\sum R^{\times 2}$. So, in the case of $x \neq y$, we have $x < y \vee y < x$.
They other two are as follows:
• $\forall x \forall y \forall z$, the definition of 'order' in R implies that $x < y \to x + z < y + z$.

• $\forall x \forall y \forall z$, $x < y$ equals to $y - x = \sum_i a_i^2 \in \sum R^{\times 2}$, and $z > 0$ equals to $z \overset{\dagger}{=} z - 0 = \sum_j b_j^2$. So, $z \cdot y - z \cdot x \overset{\dagger}{=} z \cdot (y - x) = \sum_{i,j} (a_i b_j)^2 \in \sum R^{\times 2}$, then $x \cdot z < y \cdot z$.

†: from field axioms

Then,we showed that this is an order on R. Restricting this order to the field F, we get an order on F.

For the second part, assume there is already an order on F and $\exists a \in F$, $-a \notin \sum F^2$. Notice that for every order on F, the sum of squares of non-zero element is positive: (1) for $t > 0$, $t \cdot t > t \cdot 0 = 0$ (2) for $t < 0$, $0 = t + (-t) < 0 + (-t) = -t$, then by (1), $t^2 = (-t)^2 > 0$. a is a square in the real field $F(\sqrt{a})$[7], so $\forall$ order on F, $a > 0$. Not to mention the order on $F(\sqrt{a})$ extending the order we fixed on F. □

Remark The definition of order can be modified as: $x < y \Leftrightarrow y - x$ is a square of non-zero element of R. The proof that this is an order is almost the same as above. [8]

Lemma 2.1 (Algebraic extension of real is real) *If F is real and $-a \in F - \sum F^2$, then $F(\sqrt{a})$ is real (where if a is a square in F we understand $F(\sqrt{a})$ as F). Thus, if F is real, either $F(\sqrt{a})$ or $F(\sqrt{-a})$ is real.* [9]

Proof: Suppose otherwise, $F(\sqrt{a})$ is not real when F is real and $-a \in F \setminus \sum F^2$. Since elements of $F(\sqrt{a})$ are of the form $b + c\sqrt{a}$, where $b, c \in F$, then we can write -1 as a sum of squares of elements of $F(\sqrt{a})$:

$$-1 = \sum_{i=1}^{n} (b_i + c_i\sqrt{a})^2 = \sum_{i=1}^{n} (b_i^2 + ac_i^2 + 2b_i c_i \sqrt{a}) \quad (*)$$

There are two cases to consider:
(1) If $\sqrt{a} \in F$, then $F(\sqrt{a}) = F$, so the right hand side of $(*)$ belongs to F, meaning that F is not real, contradiction.
(2) If $\sqrt{a} \notin F$, then we can write $\sqrt{a} = -\dfrac{\sum_{i=1}^{n} (b_i^2 + ac_i^2) + 1}{2\sum_{i=1}^{n} b_i c_i}$, implying that $\sqrt{a} \in F$, again a contradiction.
Both cases are impossible. Hence, $F(\sqrt{a})$ must be real. □

Theorem 2.9: Conditions making extension of real fields with i ACF

Let F be a (formally) real closed field with the two properties as follows:
• $\forall a \in F$, either $\sqrt{a}$ or $\sqrt{-1} \in F$
• $\forall f(x) \in F[x]$ with odd degree, $\exists a \in F$, $f(a) = 0$ ($f(x)$ has a root in F)
Let i be a root of $x^2 + 1$ in an extension of F, then $F(i)$ is an algebraically closed field.

Theorem 2.10: Characterisation of real closed field

Let F be a real field. TFAE:
(1) F is a real closed field
(2) $F(i)$ is algebraically closed
(3) Every positive element is a square and every $f(x) \in F[x]$ has a root in F.

As an $\mathcal{L}_{\mathrm{r}}$-theory, $\mathrm{RCF_r}$ does not have quantifier elimination [10]. However, recall from theorem 2.8, every real field is orderable, and we can also put the order as mentioned in the proof of theorem 2.8 to make F a real ordered field. Thus we have a 'model' for some theory(axioms). So, what should be the theory? We can combine the theory of ordered field and real field. The language we study should be converted from $\mathcal{L}_{\mathrm{r}}$ to $\mathcal{L}_{\mathrm{or}}$:

[7] This fact comes from the preceding lemma

[8] The only part needs take care is the transitivity: if $y - x = a^2$ and $z - y = b^2$, then $z - x = a^2 + b^2$. It remains to show that $a^2 + b^2$ is a square of non-zero elements of R, which is equal to show that $w^2 = a^2 + b^2$ has solution in R. This is true since R is real closed (mainly because it is algebraically closed).

[9] Assume -1 is a sum of squares and develop $\sum (b_i + c_i\sqrt{a_i})^2$.

[10] Suppose $\mathrm{RCF_r}$ admits a quantifier elimination, then by corollary 2.1, every definable set as a model of $\mathrm{RCF_r}$ is finite or co-finite. Consider the real numbers $\mathbb{R}$, and $\mathbb{R}_{\geq 0}$. $\mathbb{R}_{\geq 0}$ is definable by the formula $\phi(y) := \exists y \quad x = y^2$. However, $\mathbb{R}_{\geq 0}$ is neither finite or co-finite.

Definition 2.18: Theory of real ordered field

Let RCF be the $\mathcal{L}_{\text{or}}$-theory axiomatized by axioms of real closed field and axioms of ordered fields, i.e. by following formulae:
- Axioms of ordered fields
- $\forall n \geq 1, \forall x_1 \forall x_2 \dots \forall x_n \quad ((\sum_{i=1}^{n} x_i^2) + 1 \neq 0)$
- $\forall x \exists y \quad (x = y^2 \vee x + y^2 = 0)$
- $\forall n \geq 0, \forall x_1 \dots \forall x_{2n} \quad (y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$

In the new $\mathcal{L}_{\text{or}}$-theory RCF we made, we are going to show that it has quantifier elimination.
This is because the order relation, say the $\mathcal{L}_{\text{or}}$-formula $x < y$, can be defined by $y \neq x \wedge \exists z \ z^2 = y - x$, which is a formula in the language $\mathcal{L}_{\text{or}}$. So, this shows the definable sets over $\mathcal{L}_{\text{r}}$ and over $\mathcal{L}_{\text{or}}$ are the same.
What is the connection? $\forall$ ordered field $(F, <)$, $\exists$ real closure K of F such that the canonical ordering on K extends the ordering of F.
From what, $\text{RCF}_\forall$ is the theory of ordered integral domains.

Theorem 2.11: Quantifier elimination in the new theory

The $\mathcal{L}_{\text{or}}$-theory RCF has quantifier elimination.

2.4.3 Puiseux series

$\mathbb{C}[[z]]$ is the ring of formal power series with complex coefficients. $\forall n \in \mathbb{Z}$, there is a ring $\mathbb{C}[[z^{\frac{1}{n}}]]$ such that $\mathbb{C}[[z^{\frac{1}{n}}]] \cong \mathbb{C}[[z]]$ by $z^{\frac{1}{n}} \mapsto z$. Whenever $m|n$, $\exists$ an natural isomorphism

$$\mathbb{C}[[z^{\frac{1}{m}}]] \hookrightarrow \mathbb{C}[[z^{\frac{1}{n}}]] \quad z^{\frac{1}{m}} \mapsto z^{\frac{1}{m}}$$

Them, define **formal Puiseux series**, denoted as $\mathbb{C}[[z^*]]$ to be the ring

$$\mathbb{C}[[z^*]] = \varinjlim \mathbb{C}[[z^{\frac{1}{m}}]]$$

Explicitly, the ring $\mathbb{C}[[z^*]]$ can be written as

$$\mathbb{C}[[z^*]] := \left\{ \sum_{i=0}^{\infty} a_i z^{\frac{i}{n}} : \forall i, a_i \in \mathbb{C}, n \geq 1, n \in \mathbb{Z} \right\}$$

Quotient field and valuation on it
(1) Quotient field: The quotient field $\mathbb{C}((z^*))$ of $\mathbb{C}[[z^*]]$, which can be written explicitly as

$$\mathbb{C}((z^*)) = \left\{ \sum_{i=N}^{\infty} a_i z^{\frac{i}{n}} : N \in \mathbb{Z}, \forall i, a_i \in \mathbb{C}, n \geq 1, n \in \mathbb{Z} \right\}$$

(2) Discrete valuation: We can put a valuation ν on this quotient field by

$$\nu : \mathbb{C}((z^*)) \to \mathbb{Q} \cup \{\infty\} \qquad \nu\left(\sum_{i=N}^{\infty} a_i z^{\frac{i}{n}} \right) = \frac{N}{n}, \text{if } a_N \neq 0$$

i.e. this valuation takes the first non-zero a_k to the fraction $\frac{k}{n}$ which relates to its place of index k.
This is indeed a valuation. Let $A := \sum_{s=N}^{\infty} a_s z^{\frac{s}{n}}$ and $B := \sum_{s=M}^{\infty} b_t z^{\frac{t}{m}}$
- $\nu(A) = +\infty \Leftrightarrow$ the first non-zero term has index $\infty \Leftrightarrow$ every term of A of coefficient $0 \Leftrightarrow A = 0$
- Write AB into $\sum_{i=D}^{\infty} c_i z^{\frac{i}{mn}}$, where $D = nM + mN$. Then, $\nu(AB) = \frac{D}{mn} = \frac{mN+nM}{mn} = \nu(A) + \nu(B)$
- $\nu(A + B) = \frac{\min\{Nm, Mn\}}{mn} = \min\{\frac{Nm}{mn}, \frac{Mn}{mn}\}$ Since the term in A, B with lower index determines $\nu(A + B)$.

(3) Completion: Let $\mathbb{C}\{z\}$ be the subring of $\mathbb{C}[[z]]$ consisting of series that converges in some open neighbourhood of 0, and $\mathbb{C}(\{z\}) := \text{Frac}(\mathbb{C}\{z\})$. Similarly, let $\mathbb{C}\{z^*\}$ be the subring of $\mathbb{C}[[z^*]]$ consisting of series that converges in some open neighbourhood of 0, and $\mathbb{C}(\{z^*\}) := \text{Frac}(\mathbb{C}\{z^*\})$.

2.5 Semialgebraic sets

2.6 Hilbert's 17

Definition 2.19: Positive semi-definite polynomial

Let F be a real field and $f(\overline{x}) \in F(x_1, \ldots, x_n)$ be a rational function.
f is **positive-semidefinite** $\Leftrightarrow \forall \overline{a} \in F^n$, $f(\overline{a}) \geq 0$

Theorem 2.12: Hilbert's 17th Problem

Let F be a real closed field. If f is a semidefinite polynomial over F, then $f(\overline{x}) = \sum_{i=0}^{n} f_i^2(\overline{x})$, where $\forall i$, $f_i(\overline{x}) \in F(x_1, \ldots, x_n)$. i.e. f is a sum of squares of rational functions.

Definition 2.20: Semialgebraic sets

Corollary 2.2: Semialgebraic sets and definability

Let F be an ordered field. $\{\text{semialgebraic sets for } F\} = \{\mathcal{L}_{\text{or}} - \text{definable sets for } F\}$

Geometric interpretation of quantifier elimination:

Theorem 2.13: (Tarski) theoerm

Theorem 2.14: O-minimality of RCF

The theory of RCF is O-minimal.

References

[Sho67] Joseph Robert Shoenfield. *Mathematical Logic*. Reading, Mass., Addison-Wesley, 1967.

[Bro02] Christopher W Brown. *What is Quantifier Elimination?* 2002. URL: https://www.usna.edu/Users/cs/wcbrown/qepcad/B/QE.html (visited on 02/17/2025).

[02] "Structures and Theories". In: *Model Theory: An Introduction*. New York, NY: Springer New York, 2002, pp. 7–32. ISBN: 978-0-387-22734-4. DOI: 10.1007/0-387-22734-2_2. URL: https://doi.org/10.1007/0-387-22734-2_2.

[Cal13] Ben Call. *The compactness theorem and applications*. https://math.uchicago.edu/~may/REU2013/REUPapers/Call.pdf. 2013.

[WD15] William Weiss and Cherie D'Mello. *Fundamentals of Model Theory*. https://www.math.toronto.edu/weiss/model_theory.pdf. 2015.

[EFT21] Heinz-Dieter Ebbinghaus, Jörg Flum, and Wolfgang Thomas. "Semantics of First-Order Languages". In: *Mathematical Logic*. Cham: Springer International Publishing, 2021, pp. 25–54. ISBN: 978-3-030-73839-6. DOI: 10.1007/978-3-030-73839-6_3. URL: https://doi.org/10.1007/978-3-030-73839-6_3.

[Var] Moshe Y. Vardi. *The compactness theorem*. https://www.cs.rice.edu/~vardi/comp409/lec23.pdf.