DECIDABILITY OF TARSKI GEOMETRY

BATYRKHAN SAKENOV

ABSTRACT. Tarski geometry, which is a big part of Euclidean geometry, is actually decidable. It means that there exists an algorithm that can check whether a statement in Euclidean geometry is true in a finite number of steps. We show that the Euclidean space axiomatized by Tarski's axioms is decidable through mathematical logic and model theory in particular.

1. Introduction to logic symbols and definitions

1.1. **Logic symbols.** In logic we always use formal languages that have precise formulation rules. Sentences in formal languages can be translated to English, though with a limited degree of expressiveness. First, we consider some examples of translation to build up an understanding of logic symbols.

The English sentence "A bag of potatoes was found" can be translated into the formal language as, say, the symbol P. Then a closely related sentence "A bag of potatoes was not found," can be translated as $\neg P$. Here $\neg$ is our negation symbol, read as "not."

Now suppose we have a sentence "Peels of potato were all over the floor" translated as F. Then the following compound sentences in English can be translated as formulas

"A bag of potatoes was found and peels of potato were all over the floor": $(P \wedge F)$
"If peels of potato were all over the floor, then a bag of potatoes was found": $(F \to P)$
"Either a bag of potatoes was not found, or peels of potato were not all over the floor:"

$$((\neg P) \vee (\neg F))$$

We are now ready to introduce the table of logic symbols and their meanings in English.

Symbol	**Verbose name**	**Remarks**
(	left parenthesis	punctuation
)	right parenthesis	punctuation
$\neg$	negation symbol	English: not
$\wedge$	conjunction symbol	English: and
$\vee$	disjunction symbol	English: or (inclusive)
$\to$	conditional symbol	English: if , then
$\leftrightarrow$	biconditional symbol	English: if and only if
A_1	first sentence symbol	
A_2	second sentence symbol	
A_3	third sentence symbol	
...		
A_n	n-th sentence symbol	
...		

Date: June 6–July 8, 2022.

Here the five symbols $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ are called *connective symbols*. Their meanings (and English translations) do not change in any logical language. Meanwhile the symbols $A_1, A_2, \ldots, A_n$ are called *sentence symbols*. They can be considered as parameters, and their meanings are not fixed.

1.2. **Well-formed formulas.** In logic an *expression* is a finite sequence of symbols. However, some expressions might not make sense; for example $((\rightarrow A$ is one of such sentences. Therefore, as we want to work with sentences and formal languages that make sense, we need to define "grammatically correct sentences". We want a gramatically correct sentence to satisfy the following rules:

(1) Every sentence symbol is a grammatically correct sentence.
(2) If α and β are grammatically correct sentences, then so are $(\neg\alpha), (\alpha\wedge\beta), (\alpha\wedge\beta), (\alpha \rightarrow \beta)$, and $(\alpha \leftrightarrow \beta)$
(3) No expression is a grammatically correct sentence unless it is compelled to be one by (1) and (2).

Now we introduce a formal definition of a grammatically correct sentence.

Definition 1.1. A *well-formed formula* (or simply *wff*) is an expression that can be built from sentence symbols by applying five *formula building operations* finitely many times. Formula building operations are defined by the following equations.

$$\begin{aligned} \mathcal{E}_{\neg}(\alpha) &= (\neg\alpha) \\ \mathcal{E}_{\wedge}(\alpha, \beta) &= (\alpha \wedge \beta) \\ \mathcal{E}_{\vee}(\alpha, \beta) &= (\alpha \vee \beta) \\ \mathcal{E}_{\rightarrow}(\alpha, \beta) &= (\alpha \rightarrow \beta) \\ \mathcal{E}_{\leftrightarrow}(\alpha, \beta) &= (\alpha \leftrightarrow \beta) \end{aligned}$$

For example, A_1, A_2, A_3, A_4 are sentence symbols and wffs. Hence, $\mathcal{E}_{\rightarrow}(A_1, A_2) = (A_1 \rightarrow A_2)$, $\mathcal{E}_{\vee}(A_3, A_4) = (A_3 \vee A_4)$, and $\mathcal{E}_{\leftrightarrow}((A_1 \rightarrow A_2), (A_3 \vee A_4)) = ((A_1 \rightarrow A_2) \leftrightarrow (A_3 \vee A_4))$ are also wffs.

As a matter of fact, there is an algorithm that can check whether an expression is a wff. However, this algorithm is not needed for the purpose of this paper, so we do not discuss it here. Instead, we provide some properties of wffs that and can provide reader with more insight of a what grammatically correct sentence can and should look like.
Property 1. In any wff the number of "(" (left parentheses) equals to the number of ")" (right parentheses).
Property 2. There are no wffs of length of 2, 3, or 6. Any other length is possible.
Property 3. Let α be a wff. Let $C(\alpha)$ denote the number of places at which binary connective symbols $(\wedge, \vee, \rightarrow, \leftrightarrow)$ occur in α. Also let $S(\alpha)$ denote number of places at which sentence symbols $(A_1, A_2, \ldots)$ occur in α. Then $S(\alpha) = C(\alpha) + 1$. For example if $\alpha = ((A_1 \rightarrow A_2) \leftrightarrow (A_3 \vee A_4))$, then $S(\alpha) = 4$, while $C(\alpha) = 3$.

1.3. **Truth assignments.** We now talk about assigning values to our parameters. In particular, we are interested in assigning two values - *False* and *True*. First off all we fix a set F, T of *truth values* consisting of two points

F, called a *falsity*
T, called a *truth.*

Definition 1.2. A *truth assignment* for a set $\mathcal{S}$ of sentence symbols is a function

$$v : \mathcal{S} \to \{F, T\}$$

assigning either T or F to each symbol in $\mathcal{S}$.

Now we consider the set $\overline{\mathcal{S}}$ of wffs that are formed by five formula building operations on sentence symbols of $\mathcal{S}$. Then $\overline{v}$, an extension of v, is a function

$$\overline{v} : \overline{\mathcal{S}} \to \{F, T\}$$

which assigns a truth value to each wff in $\overline{\mathcal{S}}$.

1.4. **Tautological implication.** This is the final subsection of the introduction to logic. At the end of this subsection there is a note on definitions of the whole section.

Definition 1.3. We say that a truth assignment v *satisfies* a wff ϕ iff $\overline{v}(\phi) = T$. We also say that a truth assignment v *satisfies* a set $\mathcal{S}$ of wffs if for any α in $\mathcal{S}$ we have $\overline{v}(\alpha) = T$.

We are now ready to define one of the key definitions in logic.

Definition 1.4. We say that a set of wffs Σ *tautologically implies* a wff τ (written as $\Sigma \vDash \tau$) iff for any truth assignment on the set of sentence symbols of $\Sigma \cup \{\tau\}$ that satisfies Σ also satisfies τ.

For example if we have $\mathcal{S} = \{A, (A \to B)\}$, then $\mathcal{S} \vDash B$.

Another interesting example can be seen when $\mathcal{S} = \{A, B\}$. It is known that $(\neg(A \wedge B)) \vDash ((\neg A) \vee (\neg B))$. Moreover, the converse is also true: $((\neg A) \vee (\neg B)) \vDash (\neg(A \wedge B))$. In such cases we say that $(\neg(A \wedge B))$ and $((\neg A) \vee (\neg B))$ are *tautologically equivalent* (written as $(\neg(A \wedge B)) \vDash\!\dashv ((\neg A) \vee (\neg B))$).

Truth assignments do not appear later in the paper, but their main reason for being here was to define what tautological implication is. Tautological implication is extensively used to define main terminology and tools of model theory. Therefore, a reader is advised to get a good understanding of what tautological implication is before properly diving into the next section.

2. Languages and structures.

Model theory is an area of mathematical logic that studies relationships between formal theories and their models. This might essentially say nothing to the reader if they do not know what are formal definitions of *theories* and *models*. In this section we are going to define what languages and structures are to prepare reader for the introduction of *models, theories, and axioms* in section 3.

We start off with the definition of *relations*.

Definition 2.1. An n-ary *relation* R is a set of of n-tuples.

Usually relations describe a connection between the elements of the n-tuple. For example, we can say that (x, y, z) is in 3-ary relation R if $x \mid y \mid z$, and $x < y < z \leq 6$. Then triples such as $(1, 2, 4), (1, 3, 6)$ can be in relation R. Functions are relations too.

Now we can start with basic definitions of model theory.

Definition 2.2. A *language* $\mathcal{L}$ is specified by the following data:

(1) a set of function symbols $\mathcal{F}$ and positive integers n_f for each $f \in \mathcal{F}$,

(2) a set of relation symbols $\mathcal{R}$ and positive integers n_R for each $R \in \mathcal{R}$, and
(3) a set of constant symbols $\mathcal{C}$.

Essentially a language $\mathcal{L}$ provides us with a set of symbols to which we can assign particular functions, relations, and constants. Here n_f, denotes the number of variables a function with the symbol f should have. Analogously, n_R, denotes the number of elements a relation with the symbol R should have.

Example. Below are some examples of languages:

- The language of rings $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$.
- The language of ordered rings $\mathcal{L}_{or} = \mathcal{L}_r \cup \{<\}$.

Here $+, -, \cdot, <$ are binary function symbols.

Definition 2.3. An $\mathcal{L}$-*structure* $\mathcal{M}$ is specified by the following data:

(1) a non-empty set M called *the universe* or *domain*,
(2) a function $f^{\mathcal{M}} : M^{n_f} \to M$ for each $f \in \mathcal{F}$,
(3) a relation $R^{\mathcal{M}} \subseteq M^{n_R}$ for each $R \in \mathcal{R}$, and
(4) an element $c^{\mathcal{M}} \in M$ for each $c \in \mathcal{C}$

In structure $\mathcal{M}$, the function $f^{\mathcal{M}}$, relation $R^{\mathcal{M}}$, and constant $c^{\mathcal{M}}$ are called the *interpretations* of symbols f, R and c respectively. We will denote a structure $\mathcal{M}$ by $(M, f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}} : f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C})$.

Example. Rings are structures in the language $\mathcal{L}_r$, where addition interprets $+$, subtraction interprets $-$, multiplication interprets $\cdot$, additive identity interprets 0, and multiplicative identity interprets 1.

Definition 2.4. Suppose $\mathcal{M}$ and $\mathcal{N}$ are $\mathcal{L}$-structures with universes M and N respectively. An $\mathcal{L}$-*embedding* is a injective function $\sigma : \mathcal{M} \to \mathcal{N}$ that preserves the interpretation of all symbols of $\mathcal{L}$. Precisely:

(1) $\sigma(f^{\mathcal{M}}(a_1, a_2, \ldots, a_{n_f})) = f^{\mathcal{N}}(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_{n_f}))$ for all $f \in \mathcal{F}$ and $a_1, a_2, \ldots, a_{n_f} \in M$
(2) $(a_1, a_2, \ldots, a_{R_n}) \subseteq R^{\mathcal{M}}$ iff $(\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_{R_n})) \subseteq R^{\mathcal{N}}$ for all $R \in \mathcal{R}$ and $a_1, a_2, \ldots, a_{n_R} \in M$
(3) $\sigma(c^{\mathcal{M}}) = c^{\mathcal{N}}$ for all $c \in \mathcal{C}$

If the function σ is bijective, then σ is called an $\mathcal{L}$-isomorphism. If $M \subseteq N$ and there exists and embedding from $\mathcal{M}$ to $\mathcal{N}$, then $\mathcal{M}$ is called a *substructure* of $\mathcal{N}$, while $\mathcal{N}$ is called an *extension* of $\mathcal{M}$.

Example. $(\mathbb{R}, \cdot, \leq, 1)$ is a substructure of $(\mathbb{C}, \cdot, 1)$. That is because the function $\sigma(x) = x$ is an embedding from $(\mathbb{R}, \cdot, 1)$ to $(\mathbb{C}, \cdot, 1)$. Indeed, the function σ is injective, and it satisfies the following properties:

(1) The only function in $(\mathbb{R}, \cdot, \leq, 1)$ is $\cdot$, and $\sigma(a_1 \cdot a_2) = a_1 \cdot a_2 = \sigma(a_1) \cdot \sigma(a_2)$
(2) The only relation in $(\mathbb{R}, \cdot, \leq, 1)$ is $\leq$, and $a_1 \leq a_2$ iff $\sigma(a_1) \leq \sigma(a_2)$.
(3) $\sigma(1) = 1$.
(4) $\mathbb{R} \subset \mathbb{C}$.

$\sigma(x) = x + 1$ is an isomorphism from $(\mathbb{Z}, +, 0)$ to $(\mathbb{Z}, +, 1)$.

We will now proceed to the introduction of the analogue of *wffs* in language $\mathcal{L}$.

Definition 2.5. A set of $\mathcal{L}$-*terms* is a set $\mathcal{T}$ such that:

(1) If $c \in \mathcal{C}$, then $c \in \mathcal{T}$,
(2) if v_i is a variable symbol, then $v_i \in \mathcal{T}$, and
(3) if $f \in \mathcal{F}$, and $t_1, t_2, \ldots, t_{n_f} \in \mathcal{T}$, then $f(t_1, t_2, \ldots, t_{n_f}) \in \mathcal{T}$.

An element of $\mathcal{T}$ is called an $\mathcal{L}$-*term*.

Thus, the set of terms contains only constants, variables, and expressions achieved by applying functions on terms.

Definition 2.6. We say that ϕ is an $\mathcal{L}$ -*atomic formula* if either:

(1) $\phi = (t_1 = t_2)$ for some terms t_1 and t_2 , or
(2) $\phi = R(t_1, t_2, \ldots, t_{n_R})$ for some $R \in \mathcal{R}$ and terms $t_1, t_2, \ldots, t_{n_R}$.

Therefore, atomic formulas are expressions achieved by applying relations on some terms.

Definition 2.7. The set of $\mathcal{L}$-*formulas* is a set $\mathcal{W}$ that contains all atomic formulas and such that:

(1) if $\phi \in \mathcal{W}$, then $\neg\phi \in \mathcal{W}$,
(2) if $\phi, \psi \in \mathcal{W}$, then $(\phi \wedge \psi)$ and $(\phi \vee \psi)$ are in $\mathcal{W}$, and
(3) if $\phi \in \mathcal{W}$, then $\exists v\ \phi$ and $\forall v\ \phi$ are in $\mathcal{W}$.

In other words, the set of $\mathcal{L}$-formulas is the set of atomic formulas closed under operations $\neg, \wedge, \vee, \exists v, \forall v$. $\mathcal{L}$-formulas are the wffs of the language $\mathcal{L}$.

Example. In the language $\mathcal{L}_{or}$ of ordered rings examples of $\mathcal{L}_{or}$-formulas can be:

- $v = 0 \vee v > 0$,
- $\neg(v_1 = v_2)$, and
- $\exists v_2\ v_2 \cdot v_2 = v_1$.

Definition 2.8. We say that a variable v occurs *freely* in a formula if it is not inside a quantifier $\exists v$ or $\forall v$. Otherwise, we say that v is *bound*.

There is a particular type of $\mathcal{L}$-formulas that is of a special interest in model theory.

Definition 2.9. An $\mathcal{L}$-*sentence* is an $\mathcal{L}$-formula in which none of the variables occurs freely.

In other words, in a sentence each variable occurs with a quantifier.

Example. Here are examples of a formula that is a sentence and a formula that does not qualify to be a sentence.

- Formula $\forall y\ \exists x\ (x^2 = y)$ is a sentence, because both x and y have quantifiers.
- Formula $\exists x\ (x^2 = y)$ is not a sentence, because y does not have a quantifier.

Now, we will talk about sentences and formulas being *true* in a structure. Let $\mathcal{M}$ be an $\mathcal{L}$-structure and ϕ an $\mathcal{L}$-formula. Suppose that $v_1, v_2, \ldots, v_n$ are free variables of ϕ, then denote $\overline{v} = (v_1, v_2, \ldots, v_n)$ to be an n-tuple of variables of ϕ. We write $\phi(\overline{v}) = \phi(v_1, v_2, \ldots, v_n)$ to make explicit the free variables in ϕ. We will now rigorously define what it means $\mathcal{M} \vDash \phi$, or in other words, what it means for ϕ to be true in $\mathcal{M}$.

Definition 2.10. Let $\phi(v_1, v_2, \ldots, v_n)$ be a formula with n free variables, and $\overline{a} = \{a_1, a_2, \ldots, a_n\} \in \mathcal{M}^n$. Then $\mathcal{M} \vDash \phi(\overline{a})$ is inductively defined in the following way:

(1) If ϕ is an atomic formula and:

   (a) If $\phi = (t_1 = t_2)$, then $\mathcal{M} \vDash \phi(\overline{a})$ iff $t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a})$.
   (b) If $\phi = R(t_1, t_2, \ldots, t_{n_R})$, then $\mathcal{M} \vDash \phi(\overline{a})$ iff $t_1(\overline{a}), t_2(\overline{a}), \ldots, t_{n_R}(\overline{a})) \in R^{\mathcal{M}}$.
(2) If ϕ is another $\mathcal{L}$-formula:
   (a) If $\phi = \neg\psi$, then $\mathcal{M} \vDash \phi$ iff $\mathcal{M} \nvDash \psi$.
   (b) If $\phi = (\psi \wedge \omega)$, then $\mathcal{M} \vDash \phi$ iff $\mathcal{M} \vDash \psi$ and $\mathcal{M} \vDash \omega$.
   (c) If $\phi = (\psi \vee \omega)$, then $\mathcal{M} \vDash \phi$ iff $\mathcal{M} \vDash \psi$ or $\mathcal{M} \vDash \omega$.
   (d) If $\phi = \exists v_j\ \psi(\overline{v}, v_j)$, then $\mathcal{M} \vDash \phi$ iff there exists $b \in M$ such that $\mathcal{M} \vDash \psi(\overline{a}, b)$.
   (e) If $\phi = \forall v_j\ \psi(\overline{v}, v_j)$, then $\mathcal{M} \vDash \phi$ iff $\mathcal{M} \vDash \psi(\overline{a}, b)$ for all $b \in M$.

If $\mathcal{M} \vDash \phi(\overline{a})$ we can either say that $\mathcal{M}$ *satisfies* $\phi(\overline{a})$ or that $\phi(\overline{a})$ is *true* in $\mathcal{M}$. Now, note that if ϕ is an $\mathcal{L}$-sentence, then ϕ does not have free variables, and thus $\mathcal{M} \vDash \phi$ or $\mathcal{M} \nvDash \phi$. This means that an $\mathcal{L}$-sentence is either true or false in a structure $\mathcal{M}$.

Proposition 2.11. *Suppose that $\mathcal{M}$ is a substructure of $\mathcal{N}$, $\phi(\overline{v})$ is a quantifier-free formula, and $\overline{a} \in \mathcal{M}^m$. Then $\mathcal{M} \vDash \phi(\overline{a})$ iff $\mathcal{N} \vDash \phi(\overline{a})$.*

Proof. Before we use induction on formulas, we prove the proposition for terms.

Claim 2.12. *If $t(\overline{v})$ is a term, and $\bar{b} \in \mathcal{M}$, then $t^{\mathcal{M}}(\bar{b}) = t^{\mathcal{N}}(\bar{b})$.*

This can be proved by induction on formulas:
Case 1. t is the constant symbol $c \in \mathcal{C}$, then $t^{\mathcal{M}}(\bar{b}) = c^{\mathcal{M}} = c^{\mathcal{N}} = t^{\mathcal{N}}(\bar{b})$.
Case 2. t is the variable v_i, then $t^{\mathcal{M}}(\bar{b}) = b_i = t^{\mathcal{N}}(\bar{b})$.
Case 3. t is the n-ary function symbol $f(t_1, t_2, \ldots, t_n)$, where $t_1, t_2, \ldots, t_n$ are terms. Then from $\mathcal{M} \subseteq \mathcal{N}$ we know that $t_i^{\mathcal{M}}(\bar{b}) = t_i^{\mathcal{N}}(\bar{b})$ for $i = 1, 2, \ldots, n$, and $f^{\mathcal{M}} = f^{\mathcal{N}}$. Thus,

$$\begin{aligned} t^{\mathcal{M}}(\bar{b}) &= f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{b}), t_2^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^(\mathcal{N})(t_1^{\mathcal{M}}(\bar{b}), t_2^{\mathcal{M}}(\bar{b}), \ldots, t_n^{\mathcal{M}}(\bar{b})) \\ &= f^(\mathcal{N})(t_1^{\mathcal{N}}(\bar{b}), t_2^{\mathcal{N}}(\bar{b}), \ldots, t_n^{\mathcal{N}}(\bar{b})) \\ &= t^{\mathcal{N}}(\bar{b}). \end{aligned}$$

Hence, we proved the claim. Now, we prove the proposition for atomic-formulas.
Case 1. $\phi = (t_1 = t_2)$, then

$$\mathcal{M} \vDash \phi(\overline{a}) \Leftrightarrow t_1^{\mathcal{M}}(\overline{a}) = t_2^{\mathcal{M}}(\overline{a}) \Leftrightarrow t_1^{\mathcal{N}}(\overline{a}) = t_2^{\mathcal{N}}(\overline{a}) \Leftrightarrow \mathcal{N} \vDash \phi(\overline{a}).$$

Case 2. $\phi = R(t_1, t_2, \ldots, t_n)$, then from our claim

$$\begin{aligned} \mathcal{M} \vDash \phi(\overline{a}) &\Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), t_2^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{M}} \\ &\Leftrightarrow (t_1^{\mathcal{M}}(\overline{a}), t_2^{\mathcal{M}}(\overline{a}), \ldots, t_n^{\mathcal{M}}(\overline{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow (t_1^{\mathcal{N}}(\overline{a}), t_2^{\mathcal{N}}(\overline{a}), \ldots, t_n^{\mathcal{N}}(\overline{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow \mathcal{N} \vDash \phi(\overline{a}). \end{aligned}$$

Thus, the proposition is true for all atomic formulas. Now, we are ready to prove that it is true for other formulas by induction. *Case 1.* $\phi = \neg\psi$ and the proposition is true for ψ, then

$$\mathcal{M} \vDash \phi(\overline{a}) \Leftrightarrow \mathcal{M} \nvDash \psi(\overline{a}) \Leftrightarrow \mathcal{N} \nvDash \psi(\overline{a}) \Leftrightarrow \mathcal{N} \vDash \phi(\overline{a}).$$

Case 2. $\phi = \psi_0 \wedge \psi_1$ and the proposition is true for ψ_0, ψ_1, then

$$\mathcal{M} \vDash \phi(\overline{a}) \Leftrightarrow (\mathcal{M} \vDash \psi_0(\overline{a})) \wedge (\mathcal{M} \vDash \psi_1(\overline{a})) \Leftrightarrow (\mathcal{N} \vDash \psi_0(\overline{a})) \wedge (\mathcal{N} \vDash \psi_1(\overline{a})) \Leftrightarrow \mathcal{N} \vDash \phi(\overline{a}).$$

Because, the set of quantifier-free formulas is closed under $\neg$ and $\wedge$ (see (2) in 2.13 below), the proposition is true for all quantifier-free formulas. ■

The proposition we just proved can be interpreted as "a quantifier-free formula is true in $\mathcal{M}$ iff it is true in its extension $\mathcal{N}$".

Remark 2.13.
1. Note that in formulas and sentences quantifiers only range over elements of structures and not sets of elements. This limitation of formulas to elements is exactly what makes our logic *first-order*. Our specification to only *first-order logic* is important in the context of geometry. This is explained in the last section of this paper.
2. From truth tables it can be seen that some formulas involving symbols $\vee, \rightarrow, \leftrightarrow, \forall$ are the same as formulas that do not have these symbols in them:
   - $\phi \rightarrow \psi$ is an abbreviation for $\neg\phi \vee \psi$,
   - $\phi \leftrightarrow \psi$ is an abbreviation for $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$,
   - $\phi \vee \psi$ is an abbreviation for $\neg(\neg\phi \wedge \neg\psi)$,
   - $\forall\phi$ is an abbreviation for $\neg(\exists v \neg\phi)$.

   Therefore, instead of considering formulas formed by all $\neg, \wedge, \vee, \exists, \forall$ we can only consider the formulas formed by $\neg, \wedge, \exists$. We will be using this fact in proofs, to reduce the number of cases needed to be considered in induction on formulas.

Definition 2.14. We say that structures $\mathcal{M}$ and $\mathcal{N}$ are *elementary equivalent* (written $\mathcal{M} \equiv \mathcal{N}$) if

$$\mathcal{M} \vDash \phi \text{ iff } \mathcal{N} \vDash \phi,$$

for all $\mathcal{L}$-sentences ϕ.

Proposition 2.15. *If there is an isomorphism from $\mathcal{M}$ to $\mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$.*

Definition 2.16. Let T be a theory and ϕ be a sentence. We say that ϕ is a *logical consequence* of T and write $T \vDash \phi$ if $\mathcal{M} \vDash \phi$ whenever $\mathcal{M} \vDash T$.

3. Theories and models.

"*Model theory* is a study of relationship between theories and their models."
To understand the statement above we define theories and models.

Definition 3.1. An $\mathcal{L}$-*theory* T is a set of $\mathcal{L}$-sentences.

Definition 3.2. We say that $\mathcal{M}$ is a *model* of a theory T (written $\mathcal{M} \vDash T$) iff $\mathcal{M} \vDash \phi$ for all $\phi \in T$.

Some theories do not have models. For example the theory $T = \{\forall x\ x = 0, \exists x > 0\}$ has two contradictory sentences, which is why it does not have a model. We say that theories that have models are *satisfiable*.

Definition 3.3. We say that a class $\mathcal{K}$ of $\mathcal{L}$-structures is an *elementary class* if there is a theory T such that $\mathcal{K} = \{M : M \vDash T\}$.

Often in model theory we are given a set of structures, which we want to describe by some properties. In other words, we want to find a common theory of these structures. We call the sentences of such theory *axioms*.

Example (Linear orders). Let $\mathcal{L} = \{<\}$, where $<$ is a binary relation symbol. The class of linear orders is axiomatized by the sentences:

- $\forall x \neg(x < x)$,
- $\forall x \neg(x < x)$,
- $\forall x \forall y \forall z\ ((x < y \wedge y < z) \rightarrow x < z)$,
- $\forall x \forall y\ (x < y \vee x = y \vee x > y)$.

The class of dense linear orders includes all the axioms above and

$$\forall x \forall y\ (x < y \rightarrow (\exists z\ (x < z \wedge z < y))).$$

Example (Graphs). Let $\mathcal{L} = \{R\}$, where R is a binary relation which means that two vertices are connected. We can axiomatize the class of irreflexible graphs (i.e. no vertex is connected to itself) by two axioms.

- $\forall x\ \neg R(x, x)$,
- $\forall x \forall y\ (R(x, y) \rightarrow R(y, x))$.

4. Main tools of model theory.

Some theorems play an important role in the whole model theory, and they are applied to prove many results not only in logic, but in abstract algebra, computer science, and geometry. To name a few of such theories, we have *Godel's Completeness theorem* and the *Compactness theorem.* Though, of the main interest to us is one of the results that says that if a theory T satisfies certain conditions, then T is decidabile.

4.1. Main theorems of model theory.

We start with the formal definition of proof.

Definition 4.1. A *proof* of ϕ from theory T is a finite sequence of $\mathcal{L}$-formulas $\psi_1, \psi_2, \ldots, \psi_m$ such that $\psi_m = \phi$ and $\psi_i \in T$ or ψ_i follows from $\psi_1, \psi_2, \ldots, \psi_{i-1}$ by a simple logical rule for each i. We write $T \vdash$ if there is a proof of ϕ from T and say that ϕ is *deducible* from T.

Some important points about proofs:

- Proofs are finite.
- (Soundness) If $T \vdash \phi$, then $T \vDash \phi$
- If T is a finite set of sentences, then there is an algorithm that, when given a sequence of $\mathcal{L}$-formulas σ and an $\mathcal{L}$-sentence ϕ, will decide whether σ is a proof of ϕ from T.

We now, get to a very surprising and important result in model theory.

Theorem 4.2 (Godel's Completeness theorem)**.** *Let T be an $\mathcal{L}$-theory and ϕ be an $\mathcal{L}$-sentence. Then $T \vDash \phi$ iff $T \vdash \phi$.*

One direction of this theorem is intuitively true: if ϕ is deducible from T, then ϕ is true whenever T is true. However, the other direction is not that obvious, and it informally says that, if you look at a truth table of a theory and see that a sentence is true whenever the theory is true, then the statement should be deducible from the theory.

The Completeness theorem provides us with a criterion that checks whether a theory T is satisfiable. But for that criterion we need another important definition in model theory.

Definition 4.3. We say that theory T is *inconsistent* if there is a sentence ϕ such that $T \vdash \{\phi \wedge \neg\phi\}$. If there is no such sentence ϕ, we say that T is *consistent.*

Corollary 4.4. *T is satisfiable iff T is consistent.*

Proof. Suppose we have a satisfiable theory T and a sentence ϕ such that $T \vDash \phi$, then note that we cannot have that $T \vDash \neg\phi$ from the definition of logical consequence (there is no $\mathcal{M}$ such that $\mathcal{M} \vDash \phi$ and $\mathcal{M} \vDash \neg\phi$). Hence, from soundness of proofs there does not exists a sentence ϕ such that $T \vdash \phi$ and $T \vdash \neg\phi$, because otherwise from soundness we would get that $T \vDash \phi$ and $T \vDash \neg\phi$. Hence, if T is satisfiable, then T is consistent.

Now, suppose we have a consistent theory T. We will prove by contradiction that T should be satisfiable. Suppose T is not satisfiable, then there is a sentence ϕ such that every model of T is a model of $\phi \wedge \neg\phi$. Hence, $T \vDash (\phi \wedge \neg\phi)$, but by the completeness theorem it would mean that $T \vdash (\phi \wedge \neg\phi)$, i.e. that T is inconsistent. This is a contradiction. Hence, if T is consistent, then T is satisfiable. ■

Completeness theorem also proves one of the main theorems in model theory.

Theorem 4.5 (Compactness theorem)**.** *T is satisfiable iff every finite subset of T is satisfiable.*

Proof. It is obvious that if T is satisfiable, then its finite subsets are satisfiable too. Now suppose that every finite subset of T is satisfiable, while T is not. Then by 4.4 T is inconsistent, and there exists a sequence of formulas σ, which is a proof of $\phi \wedge \neg\phi$ for some sentence ϕ (i.e. a proof of a contradiction). Since σ is finite, all the formulas of it are derived from a finite set of assumptions (sentences) which we will denote as T_0. Hence, σ is a proof of contradiction from T_0, which means that T_0 is inconsistent. But then from the 4.4, T_0 is not satisfiable, which is a contradiction to our assumption. Thus, if all finite subsets of T are satisfiable, then T is satisifable too. ■

Definition 4.6. We say that an $\mathcal{L}$-theory T is *complete* if for any $\mathcal{L}$-sentence ϕ either $T \vDash \phi$ or $T \vDash \neg\phi$.

Definition 4.7. An $\mathcal{L}$-language is called *recursive* if there exists an algorithm that decides whether a sequence of symbols is an $\mathcal{L}$-formula.

We say that an $\mathcal{L}$-theory T is *recursive* if there is an algorithm that, when given an L-sentence ϕ as input, decides whether $\phi \in T$.

Proposition 4.8. *If $\mathcal{L}$ is a recursive language and T is a recursive $\mathcal{L}$-theory, then the set $\{\phi : T \vdash \phi\}$ is recursively enumerable. This means that there is an algorithm, that given ϕ as input will stop accepting $T \vdash \phi$ and not stop if $T \nvdash v$.*

Proof. There is $\sigma_0, \sigma_1, \ldots$, a computable listing of all finite sequences of $\mathcal{L}$-formulas. At stage i of our algorithm, we check to see whether σ_i is a proof of ϕ from T. This involves checking that each formula either is in T (which we can check because T is recursive) or follows by a logical rule from earlier formulas in the sequence σ_i and that the last formula is ϕ. If σ_i is a proof of ϕ from T, then we halt accepting; otherwise we go on to stage $i + 1$. ■

Now, we can get to a result which will be very important for the decidability of Tarski's geometry. But before that let's define what it means for a theory to be decidable.

Definition 4.9. We say that an $\mathcal{L}$-theory T is *decidable* if there is an algorithm such, that when given an $\mathcal{L}$-sentence ϕ as input, decides whether $T \vDash \phi$.

Then, we have the following lemma

Lemma 4.10. *If T is a recursive complete satisfiable theory in a recursive language $\mathcal{L}$, then T is decidable.*

Proof. Because T is satisfiable, $A = \{\phi : T \vDash \phi\}$ and $B = \{\phi : T \vDash \neg\phi\}$ are disjoint. Because T is consistent, $A \cup B$ is the set of all $\mathcal{L}$-sentences. By 4.4, $A = \{\phi : T \vdash \phi\}$ and $B = \{\phi : T \vdash \neg\phi\}$. By 4.8 A and B are recursively enumerable. But any recursively enumerable set with a recursively enumerable complement is recursive.

To decide whether ϕ is a logical consequence of complete satisfiable recursive theory T, we begin searching through possible proofs from T until we find either a proof of ϕ or a proof of $\neg\phi$. Because T is satisfiable, we will not find proofs of both. Because T is complete, we will eventually find a proof of one or the other. ■

4.2. **Elementary embeddings.** In 2.4 we talked about functions that preserve interpretations of languages. Now, we will work a particular type of useful embeddings.

Definition 4.11. We say that an embedding $j : \mathcal{M} \to \mathcal{N}$ is an *elementary embedding* iff

$$\mathcal{M} \vDash \phi(a_1, a_2, \ldots, a_n) \Leftrightarrow \mathcal{N} \vDash \phi(j(a_1), j(a_2), \ldots, j(a_n))$$

for all $\mathcal{L}$-formulas $\phi(v_1, v_2, \ldots, v_n)$ and all $a_1, a_2, \ldots, a_n \in \mathcal{M}$.

Notation. If $\mathcal{M}$ is a substructure of $\mathcal{N}$ and there exists an elementary embedding $j : \mathcal{M} \to \mathcal{N}$, then we say that $\mathcal{M}$ is an *elementary substructure* of $\mathcal{N}$ and write $\mathcal{M} \prec \mathcal{N}$. We also say that $\mathcal{N}$ is an *elementary extension* of $\mathcal{M}$.

Corollary 4.12. *Isomorphisms are elementary embeddings.*

Proof. The proof of 2.15 shows that the corrolary is true. ■

Now, we are going to show how we can construct elementary embeddings.

Definition 4.13. Suppose $\mathcal{M}$ is an $\mathcal{L}$-structure. Let $\mathcal{L}_M$ be the language where we add to L constant symbols m for each element of M (the universe of $\mathcal{M}$). The *atomic diagram* of $\mathcal{M}$ is

$$\{\phi(m_1, m_2, \ldots, m_n) : \phi \text{ is either an atomic } \mathcal{L}\text{-formula} \\ \text{or the negation of an atomic } \mathcal{L}\text{-formula and } \mathcal{M} \vDash \phi(m_1, m_2, \ldots, m_n)\}.$$

We denote the atomic diagram of $\mathcal{M}$ by $Diag(\mathcal{M})$.

The *elementary diagram* of $\mathcal{M}$ is

$$\{\phi(a_1, a_2, \ldots, a_n) : \mathcal{M} \vDash \phi(a_1, a_2, \ldots, a_n) \text{ and } \phi \text{ is an } \mathcal{L}\text{-formula}\}.$$

We denote the elementary diagram of $\mathcal{M}$ by $Diag_{el}(\mathcal{M})$.

This way, formula in language $\mathcal{L}$ can be expressed as an $\mathcal{L}_{\mathcal{M}}$-sentence.

We have the following lemma:

Lemma 4.14. *Suppose that $\mathcal{N}$ is an $\mathcal{L}_{\mathcal{M}}$-structure.*

(1) *If $\mathcal{N} \vDash Diag(\mathcal{M})$, then, if we view $\mathcal{N}$ as an $\mathcal{L}$-structure, there is an embedding $j : \mathcal{M} \to \mathcal{N}$.*
(2) *If $\mathcal{N} \vDash Diag_{el}(\mathcal{M})$, then, if we view $\mathcal{N}$ as an $\mathcal{L}$-structure, there is an elementary embedding $j : \mathcal{M} \to \mathcal{N}$.*

Proof. ■

5. Elimination of Quantifiers.

Definition 5.1. An $\mathcal{L}$-theory T has *elimination of quantifiers* if for every formula ϕ there is a quantifier-free formula ψ such that

$$T \vDash \phi \leftrightarrow \psi.$$

Example. Let $\phi(a, b, c)$ be the formula

$$\exists x \; ax^2 + bx + c = 0.$$

Then from quadratic equations we know that

$$\mathbb{R} \vDash \phi \leftrightarrow [(a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge (b \neq 0 \vee c = 0)].$$

Thus, we managed to find a quantifier free formula equivalent to $\mathbb{R} \vDash \phi$.

We will now provide a model-theoretic criterion for quantifier elimination.

Theorem 5.2. *Suppose $\mathcal{L}$ is a language that contains a constant symbol c, T is an $\mathcal{L}$-theory, and $\phi(\overline{v})$ is an $\mathcal{L}$-formula. The following statements are equivalent:*

1. *There is a quantifier-free $\mathcal{L}$-formula $\psi(\overline{v})$ such that $T \vDash \forall \overline{v} \; (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$.*
2. *If $\mathcal{M}$ and $\mathcal{N}$ are models of T, $\mathcal{A}$ is an $\mathcal{L}$-structure, $\mathcal{A} \subseteq \mathcal{M}$, and $\mathcal{A} \subseteq \mathcal{N}$ then $\mathcal{M} \vDash \phi(\overline{a})$ iff $\mathcal{N} \vDash \phi(\overline{a})$ for all $\overline{a} \in \mathcal{A}$.*

Proof. (1) $\Rightarrow$ (2), Suppose that there exists quantifier-free $\psi(\overline{v})$ such that $T \vDash \forall \overline{v} \; (\phi(\overline{v}) \leftrightarrow \psi(\overline{v}))$. Let $\overline{a} \in \mathcal{A}$, where $\mathcal{A}$ is a common substructure of $\mathcal{M}$ and $\mathcal{N}$, which are models of theory T. In 2.11 we saw that quantifier-free formulas are preserved under substructure and extension. Thus,

$$\begin{gathered}\mathcal{M} \vDash \phi(\overline{a}) \Leftrightarrow \mathcal{M} \vDash \psi(\overline{a}) \\ \Leftrightarrow \mathcal{A} \vDash \psi(\overline{a}) \text{ (because } \mathcal{A} \subseteq \mathcal{M}) \\ \Leftrightarrow \mathcal{N} \vDash \psi(\overline{a}) \text{ (because } \mathcal{A} \subseteq \mathcal{N}) \\ \Leftrightarrow \mathcal{N} \vDash \phi(\overline{a}).\end{gathered}$$

(2) $\Rightarrow$ (1),

Claim 5.3. *We may assume that both $T \cup \{\phi(\overline{v})\}$ and $T \cup \{\neg\phi(\overline{v})\}$ are satisfiable. In other words, there exists a model $\mathcal{K}$ such that $\mathcal{K} \vDash T \cup \{\phi(\overline{v})\}$.*

Proof. First, if $T \vDash \forall \overline{v} \; \phi(\overline{v})$, then $T \vDash \forall \overline{v} \; (\phi(\overline{v}) \leftrightarrow c = c)$. If $T \vDash \forall \overline{v} \; \neg\phi(\overline{v})$, then $T \vDash \forall \overline{v} \; (\phi(\overline{v}) \leftrightarrow c \neq c)$. ∎

Let $\Gamma(\overline{v}) = \{\psi(\overline{v}) : \psi$ is a quantifier-free formula and $T \vDash \forall \overline{v} \; (\phi(\overline{v}) \rightarrow \psi(\overline{v}))\}$.

Claim 5.4. *Let $d_1, d_2, \ldots, d_m$ be new constant symbols. Then $T \cup \Gamma(\overline{d}) \vDash \phi(\overline{d})$.*

Proof. Suppose the claim is not true. Then let $\mathcal{M} \vDash T \cup \Gamma(\overline{v}) \cup \{\neg\phi(\overline{d})\}$. Now, let A be a substructure of $\mathcal{M}$ generated by $\overline{d}$. (I.e. the smallest substructure of $\mathcal{M}$ which contains constant symbols $d_1, d_2, \ldots, d_m$).

Let $\Sigma = T \cup Diag(A) \cup \{\phi(\overline{d})\}$. If Σ is unsatisfiable, we note that $T \cup Diag(A)$ and $T \cup \{\phi(\overline{d})\}$ are both satisfiable. Then by the Compactness theorem, there exists a finite set of quantifier-free formulas $\{\psi_1(\overline{d}), \psi_2(\overline{d}), \ldots, \psi_k(\overline{d})\} \subseteq Diag(\mathcal{A})$ such that the theory $\{\psi_1(\overline{d}), \psi_2(\overline{d}), \ldots, \psi_k(\overline{d})\} \cup \phi(\overline{d})$ is unsatisfiable. But this means that

$$T \vDash (\bigwedge_{i=1}^{m} \psi_i(\overline{d}) \rightarrow \neg\phi(\overline{d})).$$

Now, because $d_1, d_2, \ldots, d_n$ are newly added constants, which do not appear in T we have,

$$T \models \forall \overline{v}\ (\bigwedge_{i=1}^{m} \psi_i(\overline{v}) \to \neg\phi(\overline{v})).$$

But then

$$T \models \forall \overline{v}\ (\phi(\overline{v}) \to \bigvee_{i=1}^{m} \neg\psi_i(\overline{v})),$$

so $\bigvee_{i=1}^{m} \neg\psi_i(\overline{v}) \in \Gamma$, and $A \models \bigvee_{i=1}^{m} \neg\psi_i(\overline{v})$, which is a contradiction. Thus, Σ is satisfiable.

Since Σ is satisfiable, there exists a model of Σ, which we will denote as $\mathcal{N}$. Then $\mathcal{N} \models \Sigma \models \phi(\overline{d})$. Also $\mathcal{N} \models \Sigma \models diag(A)$, and so by 4.14 $\mathcal{N}$ is an extension of $\mathcal{A}$. But then $\mathcal{M} \models \neg\phi(\overline{d})$ and $\mathcal{N} \models \phi(\overline{d})$, while both $\mathcal{M}$ and $\mathcal{N}$ are extensions of $\mathcal{A}$, which is a contradiction to our initial assumption of. Hence, $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$.

Now, since $T \cup \Gamma(\overline{d}) \models \phi(\overline{d})$, by the Compactness theorem, there exist a finite set of quantifier-free formulas $\{\psi_1(\overline{d}), \psi_2(\overline{d}), \ldots, \psi_k(\overline{d})\} \cup \phi(\overline{d}) \in \Gamma$ such that

$$T \models (\bigwedge_{i=1}^{m} \psi_i(\overline{d}) \to \phi(\overline{d})).$$

Since $d_1, d_2, \ldots, d_m$ are newly added constant symbols, which are not in T, we have that

$$T \models \forall \overline{v}\ (\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \to \phi(\overline{v})).$$

Thus,

$$T \models \forall \overline{v}\ (\bigwedge_{i=1}^{n} \psi_i(\overline{v}) \leftrightarrow \phi(\overline{v})),$$

and $\bigwedge_{i=1}^{n} \psi_i(\overline{v})$ is quantifier-free. ■

If T is a theory, then $T_\forall$ is the set of all universal consequences of T. It is known that $\mathcal{A} \models T_\forall$ iff there exists $\mathcal{M} \models$ with $\mathcal{A} \subseteq \mathcal{M}$.

Definition 5.5. We say that a theory T has *algebraically prime models* if for any $\mathcal{A} \models T_\forall$ there is $\mathcal{M} \models T$ and an embedding $i : \mathcal{A} \to \mathcal{M}$ such that for all $\mathcal{N} \models T$ and embeddings $j : \mathcal{A} \to \mathcal{N}$ there is $h : \mathcal{M} \to \mathcal{N}$ such that $j = h \circ i$.

Definition 5.6. If $\mathcal{M}, \mathcal{N} \models T$ and $\mathcal{M} \subseteq \mathcal{N}$, then we say that $\mathcal{M}$ is *simply closed* in $\mathcal{N}$ and write $\mathcal{M} \prec_s \mathcal{N}$ if for any quantifier-free formula $\phi(\overline{v}, w)$ and $\overline{a} \in M$, $\mathcal{N} \models \exists w\ \phi(\overline{a}, w)$ then so does $\mathcal{M}$.

Corollary 5.7. *Suppose that T is an $\mathcal{L}$-theory such that*

(1) *T has algebraically prime models and*
(2) *$\mathcal{M} \prec_s \mathcal{N}$ whenever $\mathcal{M} \subseteq \mathcal{N}$ are models of T.*

Then, T has quantifier elimination.

Definition 5.8. An $\mathcal{L}$-theory T is *model-complete* if $\mathcal{M} \prec \mathcal{N}$ whenever $\mathcal{M} \subseteq \mathcal{N}$ and $\mathcal{M}, \mathcal{N} \models T$.

Proposition 5.9. *If T has quantifier elimination, then T is model-complete.*

Proof. ■

Proposition 5.10. *Let T be a model-complete theory. If there is $\mathcal{M}_0 \models T$ and $\mathcal{M}_0$ embeds in every model of T, then T is complete.*

Proof. ■

6. Algebraic background

To prove that Tarski's system of geometry is decidable, we will need to work with the theory of *Real closed fields* (written as RCF). To understand RCF, we need to have some background knowledge about groups, rings, fields, and ordered fields.

6.1. **Axioms of groups.** The classes of groups and different types of groups such as rings, ordered rings, and fields are of the most importance for our paper. Note that almost all of the following axioms are used to define the structures when we first read about them.

Let $\mathcal{L} = \{*, e\}$, where $*$ is a binary function symbol, and e is a constant symbol. The class of *groups* is axiomatized by

- $\forall x\ x * e = e * x$,
- $\forall x \forall y \forall z\ x * (y * z) = (x * y) * z$,
- $\forall x \exists y\ x * y = y * x = e$.

For the class of *Abelian (commutative) groups* we should add $\forall x \forall y\ x * y = y * x$.

We will often deal with the class of *additive groups*, which are axiomatized by replacing $*$ with $+$ and e with 0.

Now, we can axiomatize the class of ordered additive commutative groups. Let $\mathcal{L} = \{+, <, 0\}$, then the axioms for ordered commutative groups are

- axioms for additive groups,
- axioms for linear orders, and
- $\forall x \forall y \forall z (x < z \to x + z < y + z)$.

In the section 2, we already talked about the language rings as an example of language. Now we will axiomatize the class of rings.

Let $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$ be the language of rings, then the axioms for the class of *rings* are given by

- axioms for additive commutative groups
- $\forall x\ x \cdot 0 = 0$
- $\forall x\ x \cdot 1 = x$
- $\forall x \forall y \forall z\ (x - y = z \leftrightarrow x = y + z)$
- $\forall x \forall y \forall z\ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$
- $\forall x \forall y \forall z\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)$
- $\forall x \forall y \forall z\ (x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

It is important to notice that rings are commutative under $+$, but not necessarily under $\cdot$.

The *class of fields* is axiomatized by

- axioms for rings,
- $\forall x \forall y\ x \cdot y = y \cdot x$, and
- $\forall x (x \neq 0 \to \exists y\ x \cdot y = 1)$.

Let $\mathcal{L}_{or} = \{+, -, \cdot, <, 0, 1\}$ be the language of ordered rings. Then the class of *ordered fields* is axiomatized by:

- axioms for fields,
- axioms for linear orders,

- $\forall x \forall y \forall z\ (x < y \rightarrow x + z < y + z)$, and
- $\forall x \forall y \forall z\ ((x < y \wedge z > 0) \rightarrow x \cdot z < y \cdot z)$.

6.2. **Axioms of real numbers.** Let $\mathcal{L} = \{\mathbb{R}, +, \cdot, <\ 0, 1\}$. The class of *real numbers* is axiomatized by:

- axioms for fields,
- axioms for linear orders, and
- Dedekind completeness.

Definition 6.1. An element a is *algebraic over a field* K, if there exists a polynomial $p(x) \in K[x]$ (in other words, a polynomial with coefficients in K) such that $p(a) = 0$.

Example. Let $\mathbb{Q}$ be the field of rational numbers. $\phi = \frac{1+\sqrt{5}}{2}$ is algebraic over Q. That is because ϕ is a root of $(x - \frac{1+\sqrt{5}}{2})(x - \frac{1-\sqrt{5}}{2}) = x^2 - x - 1$, which has rational coefficients.

Definition 6.2. An extension of field K is called algebraic, if all its elements are algebraic over K.

Example. Let $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$, and $\mathbb{Q}(i) = \{a + ib | a, b \in \mathbb{Q}\}$, where $i = \sqrt{-1}$. Then $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(i)$ are algebraic extensions of $\mathbb{Q}$. It can be clearly seen from considering polynomials $P(x) = (x - (a + b\sqrt{2}))(x - (a - b\sqrt{2}))$ and $R(x) = (x - (a + ib))(x - (a - ib))$, which have rational coefficients.

Now, we will introduce some terminology related to real closed fields.

Definition 6.3. We say that a field F is *orderable* if there is a linear order $<$ of F making $(F, <)$ an ordered field.

Definition 6.4. We say that a field F is *formally real* if -1 is not a sum of squares of elements of F.

Theorem 6.5. *F is formally real iff F is orderable.*

Proof. Suppose F is orderable. Then all squares in F are non-negative, which implies that their sums is also non-negative and thus is not equal to -1.

Suppose F is formally real. If $a \in F$ and $-a$ is not a sum of squares in F, then there is an ordering of F in which a is positive. ■

Definition 6.6. A field F is *real closed* if it is formally real with no proper formally real algebraic extensions.

The class of real closed fields can be axiomatized by the following theorems:

- axioms for fields,
- for each $n \geq 1$, the axiom
$$\forall x_1,\ \forall x_2,\ \ldots, \forall x_n\ x_1^2 + x_2^2 + \ldots + x_n^2 \neq -1,$$
- $\forall x\ \exists y\ (y = x^2 \vee y + x^2 = 0)$,
- for each $n \geq 0$, the axiom
$$\forall x_0,\ \forall x_2,\ \ldots, \forall x_{2n}\ \exists y\ y^{2n+1} + \sum_{i=0}^{2n} y^i x_i = 0.$$

Definition 6.7. We let RCF be the $\mathcal{L}_{or}$t-heory axiomatized by the axioms above for real closed fields and the axioms for ordered fields.

Definition 6.8. If F is a formally real field, a *real closure* of F is a real closed algebraic extension of F.

By Zorn's lemma, for every formally real field F there is a maximal formally real extension of F.

7. Real closed fields

Note that all $\mathcal{L}_{or}$-terms in the RCF are polynomials.

Definition 7.1. *Basic formulas* are atomic formulas or their negation.

Definition 7.2. A *primitive existential formula* is a formula of a form $\exists x\ \phi(x)$, where $\phi(x)$ is a conjunction of basic formulas.

It is known that an $\mathcal{L}$-theory has quantifier elimination if for every primitive existential formula $\exists x\ \phi(x)$ is equivalent to a quantifier-free formula.

Claim 7.3. *In in the theory RCF of language $\mathcal{L}_{or}$, every primitive existential formula is equivalent to a disjunction of formulas of the form $\exists x\ (\wedge_{i=1}^{n} f_i(x) = 0 \wedge_{j=1}^{m} g_j(x) > 0)$, where f_i, g_j are polynomials.*

Proof. Note that a primitive existential formula $\exists x\ \phi(x)$ is of the form $\wedge_{i=1}^{n}\psi_i \wedge_{j=1}^{m} \neg\theta_j$, where ψ_i, θ_j are atomic formulas. Since in the language $\mathcal{L}_{or}$ atomic formulas are of the form $p = q$ or $p < q$, their negations are equivalent to

$$\neg(p = q) \leftrightarrow (p < q \vee q < p),$$

$$\neg(p < q) \leftrightarrow (p = q \vee q < p),$$

in which p, q are $\mathcal{L}_{or}$-terms. Note that these negations are disjunctions of atomic formulas. Therefore, ϕ can be rewritten as $\vee_{k=1}^{l}\sigma_k$, where σ_k is a conjuction of atomic formulas.

Thus, we have

$$\exists x\ \phi(x) \leftrightarrow \exists x\ \ \vee_{k=1}^{l} \sigma_k(x) \leftrightarrow \vee_{k=1}^{l}(\exists x\ \sigma_k(x)).$$

Now, each atomic formula in the conjunction σ_k is of the form $p(x) = q(x)$ or $p(x) < q(x)$, where $p(x), q(x)$ are $\mathcal{L}_{or}$-terms, and thus polynomials. Then note that these atomic formulas are equivalent to

$$f(x) = p(x) - q(x) = 0, \quad g(x) = q(x) - p(x) > 0.$$

Therefore

$$\sigma_k(x) = (\wedge_{i=1}^{n} f_i(x) = 0 \wedge_{j=1}^{m} g_j(x) > 0),$$

and

$$\exists x\ \phi(x) \leftrightarrow \vee_{k=1}^{l}(\exists x\ \sigma_k(x)).$$

■

Now, from the claim, to show that RCF has quantifier elimination it is sufficient to prove that each of the σ_k has an equivalent quantifier-free formula. We will do that using 5.2.

Theorem 7.4 (Tarski-Seidenberg)**.** *The L_{or}-theory RCF admits quantifier elimination.*

Proof. Suppose $\mathcal{M}, \mathcal{N}$ are models of RCF with a common substructure $\mathcal{A}$. Let $\psi(\overline{a}) = \exists b\ \phi(b, \overline{a})$ be a primitive existential, where $\overline{a} \in A$. As already mentioned we will be using 5.2 to prove that $\sigma(\overline{a}) = \exists b\ (\wedge_{i=1}^{n} f_i(b) = 0 \wedge_{j=1}^{m} g_j(b) > 0)$ is equivalent to some quantifier-free formula. Thus, we need to show that $\mathcal{M} \vDash \sigma(\overline{a})$ iff $\mathcal{N} \vDash \sigma(\overline{a})$ for all $\overline{a} \in A$.

Suppose there exists $\mathcal{M}$ such that $\mathcal{M} \vDash \sigma(\overline{a})$ for all $\overline{a} \in A$, then there are functions $f_i, g_j \in \mathcal{M}$ and $b \in M$ such that $\wedge_{i=1}^{n} f_i(b) = 0 \wedge_{j=1}^{m} g_j(b) > 0$ holds. Since $\mathcal{A}$ is a substructure of both $\mathcal{M}$ and $\mathcal{N}$, the interpretations of f_i and g_j are the same in $\mathcal{A}, \mathcal{M}$, and $\mathcal{N}$.

If $f_i(x)$ is non-zero for some i, then b is a root of f_i, which means that b is algebraic over $\mathcal{A}$. Because $\mathcal{A}$ has no proper algebraic extensions, b should be in $\mathcal{A}$. Thus, $b \in \mathcal{M}$ and $b \in \mathcal{N}$, and

$$\mathcal{N} \vDash \sigma(\overline{a}).$$

Now we may assume that $f_i(x)$ is zero for all i, then

$$\sigma(\overline{v}) \leftrightarrow \exists b\ (\wedge_{j=1}^{m} g_j(b) > 0).$$

Note that

Note that this argument works the same way if we take $\mathcal{N} \vDash \sigma(\overline{a})$ and want to prove that $\mathcal{M} \vDash \sigma(\overline{a})$.

■

8. Tarski's system of geometry

9. Acknowledgements

The author would like to thank Maxim Gilula and Simon Rubinstein-Salzedo for their advice on the topic. This project would not have been possible without the help of Euler Circle community.

References