# Logic and Foundation II

## Part 6. Real-closed ordered fields: completeness and decidability

Kazuyuki Tanaka

BIMSA

April 2, 2024

北京雁栖湖应用数学研究院
Beijing Institute of Mathematical Sciences and Applications

## Logic and Foundations II

- Part 5. Models of first-order arithmetic (continued)
- Part 6. Real-closed ordered fields: completeness and decidability
- Part 7. Theory of reals and reverse mathematics
- Part 8. Second order arithmetic and non-standard methods

## Part 6. Schedule

- March 28, (1) Basic properties of one-variable polynomials
- Apr. 2, (2) Real closed ordered fields and the Artin-Schreier theorem
- to be continued

# Real closed ordered field

## Definition

The theory AF of **fields** consists of the following axioms in the language $\mathcal{L}_{\mathrm{AF}} = \{+, -, \bullet, /, 0, 1\}$: (note $x/0 = 0$ for convenience)

$$x + 0 = x, \quad x + y = y + x, \quad x + (y + z) = (x + y) + z, \quad x + (-x) = 0,$$
$$x \bullet 0 = 0, \quad x \bullet 1 = x, \quad x \bullet y = y \bullet x, \quad x \bullet (y \bullet z) = (x \bullet y) \bullet z,$$
$$x/0 = 0, \quad x \neq 0 \to x \bullet (y/x) = y, \quad 1 \neq 0, \quad x \bullet (y + z) = (x \bullet y) + (x \bullet z).$$

The theory OF of **ordered fields** is AF added with the following axioms in the language $\mathcal{L}_{\mathrm{OF}} = \{+, -, \bullet, /, 0, 1, <\}$: $<$ is a linear order and $0 < 1$,

$$(x > 0 \wedge y > 0) \to (x + y > 0 \wedge xy > 0).$$

The theory RCOF of **real-closed ordered fields** is OF added with the following axioms:

$$\forall x_0 \forall x_1 \cdots \forall x_n \forall y \forall z ((y < z \wedge x_0 + x_1 y + \cdots + x_n y^n < 0 < x_0 + x_1 z + \cdots + x_n z^n)$$
$$\to \exists u (y < u < z \wedge x_0 + x_1 u + \cdots + x_n u^n = 0)) \quad (n > 0).$$

- In the above definition, we define "real closed property" in the form of the Intermediate Value Theorem. For the theory $\mathrm{RCF}$ of (unordered) **real-closed fields**, there is an alternative definition that demands the existence of square roots and roots of odd-degree polynomials as axioms.

## Lemma

In any ordered field, if a polynomial $P(a) > 0$, then there exists some $\epsilon > 0$ such that $P(x) > 0$ in the interval $(a - \epsilon, a + \epsilon)$.

**Proof.**

- It is clear when $P(x)$ is a constant. So we may assume its degree $N > 0$.
- $P(x + a) - P(a)$ is a polynomial that does not contain a constant term. Let $M$ be the maximum of absolute values of its coefficients Then, for $|x| \leq 1$, we have $|P(x + a) - P(a)| \leq NM|x|$
- So, setting $\epsilon = \min\{1, |P(a)|/NM\}$, if $|x| < \epsilon$, then we have $|P(x + a) - P(a)| < |P(a)|$.
- Since $P(a) > 0$, this inequality does not hold unless $P(x + a) > 0$. □

# The Artin-Schreier theorem

- In the previous semester (Problem 9 in part 3), we show that all fields can be embedded in an algebraically closed field and that they also have an algebraic closure.
- Similarly, every ordered field can be embedded in a real closed ordered field, and it has a real closure. However, it is difficult to create a real closed field directly.
- In the following, we will construct a real closed field within an algebraically closed field. The final trick by Zorn's lemma is quite brilliant.

**Theorem (Artin-Schreier)**

*All ordered fields can be embedded in a real closed ordered field.*

**Proof.**

- Let $\mathfrak{K}$ be an ordered field, and suppose the intermediate value theorem does not hold in $\mathfrak{K}$. Then let $P(x)$ be a polynomial over $\mathfrak{K}$ (with coefficients in $K$) of the minimal degree such that there exist $a < b \in K$ such that $P(a)P(b) < 0$ and for all $c \in (a, b)$ $P(c) \neq 0$.

Then, we show

**Claim 1**

$P(x)$ is irreducible.

**Proof of Claim 1**

- Assume $P(x)$ is not irreducible. So it can be decomposed as $P(x) = Q(x)R(x)$. Since $P(a)P(b) < 0$, we have $Q(a)Q(b) < 0$ or $R(a)R(b) < 0$.
- If $Q(a)Q(b) < 0$, there exists $c \in (a, b)$ such that $Q(c) = 0$, because $P(x)$ is a polynomial of the minimal degree such that the intermediate value theorem does not hold. However, $Q(c) = 0$ implies $P(c) = 0$, which reaches a contradiction.
- Similarly for $R(a)R(b) < 0$.

- Let $\mathfrak{K}[x]$ be a commutative ring of polynomials over $\mathfrak{K}$.
- We define an equivalence relation $\approx$ modulo $P(x)$ on it. That is,

$$Q(x) \approx R(x) \Leftrightarrow \text{“}Q(x) - R(x) \text{ is a multiple of } P(x).\text{”}$$

- Let $\mathfrak{K}[x]/P(x)$ be the quotient algebra of the equivalence classes. Obviously, $\mathfrak{K}[x]/P(x)$ is also a commutative ring.

**Claim 2**

$\mathfrak{K}[x]/P(x)$ is a field.

**Proof of Claim 2**

Let $[Q(x)]_{\approx} \neq 0 = [P(x)]_{\approx}$. Since $P(x)$ is irreducible, $Q(x)$ and $P(x)$ are mutually prime. Therefore, by mutual division method, there exist $R(x)$ and $S(x)$ such that

$$R(x)Q(x) + S(x)P(x) = 1.$$

Then, since $[R(x)]_{\approx}[Q(x)]_{\approx} = 1$, $[Q(x)]_{\approx}$ has a multiplicative inverse $[R(x)]_{\approx}$.

- Without loss of generality, we may assume $P(a) < 0,\ P(b) > 0$, and then we set

$$A = \{a' \in [a, b] : \exists x \in [a', b]\ P(x) < 0\},$$

$$B = \{a' \in [a, b] : \forall x \in [a', b]\ P(x) > 0\} = [a, b] - A.$$

  By the previous lemma, $A$ has no maximum value and $B$ has no minimum value.

- We may assume that for any element $[Q(x)]_{\approx}$ of $\mathfrak{K}[x]/P(x)$, the representative element $Q(x)$ has a small order than $P(x)$. Then, the intermediate value theorem holds for $Q(x)$.

- The number of real roots of $Q(x)$ is less than or equal to the degree of $Q(x)$. So, we can take sufficiently close $a' \in A$, $b' \in B$ such that $(a', b')$ does not include a real root of $Q(x)$. Thus, $Q(x)$ does not change its sign in the interval. Then, we define the sign of $[Q(x)]_{\approx}$ by the sign of $Q(x)$ on $(a', b')$.

- Then we will show that $\mathfrak{K}[x]/P(x)$ is an extension of $\mathfrak{K}$ as an ordered field with this order.

## Claim 3

$\mathfrak{K}[x]/P(x)$ is an extension of $\mathfrak{K}$ as an ordered field.

## Proof of Claim 3

- First, it is clear that $\mathfrak{K}[x]/P(x)$ includes $\mathfrak{K}$ as a substructure. It is easy to see that the order of $\mathfrak{K}[x]/P(x)$ is linear and that the positive part is closed under $+$.
- Next, we will show that the positive part is closed under $\cdot$, i.e.,

$$[Q(x)]_{\approx} > 0 \wedge [R(x)]_{\approx} > 0 \to [Q(x)R(x)]_{\approx} > 0.$$

- Here, we may assume the degrees of $Q(x)$ and $R(x)$ are less than that of $P(x)$. Then suppose $Q(x)R(x) = S(x)P(x) + T(x)$ where the degrees of $S(x)$ and $T(x)$ are also less than that of $P(x)$, i.e., $[Q(x)R(x)]_{\approx} = [T(x)]_{\approx}$.
- Now, take $a' \in A$, $b' \in B$ so that $Q(x)$, $R(x)$, $S(x)$, and $T(x)$ all have constant sign in $(a', b')$. Then, $Q(x)R(x)$ is always positive and $S(x)P(x)$ changes sign, so $T(x)$ must be always positive. Therefore, $[Q(x)R(x)]_{\approx} = [T(x)]_{\approx} > 0$.

We show that $\mathfrak{K}[x]/P(x)$ without order can be embedded in the algebraic closure $\overline{\mathfrak{K}}$ of $\mathfrak{K}$.

**Claim 4**

$\mathfrak{K}[x]/P(x)$ without order can be embedded in the algebraic closure $\overline{\mathfrak{K}}$ of $\mathfrak{K}$.

**Proof of Claim 4**

- Suppose that $P(u) = 0$ holds for some element $u$ of $\overline{\mathfrak{K}}$. Let $I = \{Q \in K[x] : Q(u) = 0\}$. Then, it is easy to see that this is an ideal. That is, for any $Q_1, Q_2 \in I$, $Q_1 + Q_2 \in I$; for any $R \in K[x]$ and $Q \in I$, $R \cdot Q \in I$.
- $P(x)$ belongs $I$, and any polynomial with a smaller degree than $P(x)$ does not belong to it. Hence, $P(x)$ is its generator. In other words, if $Q(u) = 0$, we can write $Q(x) = R(x)P(x)$.
- Now, we define a homomorphism $f : \mathfrak{K}[x] \to \mathfrak{K}[u]$ by $f(Q(x)) = Q(u)$. Since $I = \mathrm{Ker}(f) = \{Q : f(Q(x)) = 0\}$, by the homomorphism theorem, we have

$$\mathfrak{K}[x]/P(x) \cong \mathfrak{K}[x]/\mathrm{Ker}(f) \cong \mathfrak{K}[u].$$

  Since $\mathfrak{K}[x]/P(x)$ is a field, $\mathfrak{K}[u]$ is also a field. Hence, $\mathfrak{K}[u]$ coincides with the extension field $\mathfrak{K}(u)$, which is a subfield of $\overline{\mathfrak{K}}$. So, $\mathfrak{K}[x]/P(x)$ can be embedded in $\overline{\mathfrak{K}}$. (That is, $\overline{\mathfrak{K}}$ is also the algebraic closure of $\mathfrak{K}[x]/P(x)$.)

- Now consider the class of subfields of $\overline{\mathfrak{K}}$ that becomes an extended ordered field of $\mathfrak{K}$ with an appropriate "order". By Zorn's lemma (Axiom of choice), we obtain the maximal ordered field $\mathfrak{L}$ in this class.
- If $\mathfrak{L}$ does not satisfy the intermediate value theorem, by the above argument, $\mathfrak{L}$ can be extended further, which contradicts the maximality.
- Therefore, $\mathfrak{L}$ is a real closed ordered field. $\square$

**Problem 1**

Using the above theorem, show the following.
For any open formula $\varphi$ in the language $\mathcal{L}_{\mathrm{OF}}$,

$$\mathrm{RCOF} \vdash \varphi \Leftrightarrow \mathrm{OF} \vdash \varphi.$$

Let $\mathfrak{K} \subseteq \mathfrak{L}$ be two fields. We construct a substructure of $\mathfrak{L}$ by collecting its elements algebraic over $\mathfrak{K}$ (i.e., which are roots of polynomials over $\mathfrak{K}$). Then, we can easily see that it is a field, and so we denote it by $\overline{\mathfrak{K}}^{\mathfrak{L}}$.
Obviously, we have $\overline{\mathfrak{M}}^{\mathfrak{L}} = \overline{\mathfrak{K}}^{\mathfrak{L}}$ for a field $\mathfrak{M}$ such that $\mathfrak{K} \subseteq \mathfrak{M} \subseteq \overline{\mathfrak{K}}^{\mathfrak{L}}$.

## Lemma (Isomorphic condition)

*Let $\mathfrak{K}_1 \cong \mathfrak{K}_2$ be two ordered fields, and $f : \mathfrak{K}_1 \to \mathfrak{K}_2$ an isomorphism. If we take a real closed field $\mathfrak{L}_i$ such that $\mathfrak{K}_i \subseteq \mathfrak{L}_i$ for each $i = 1, 2$, then $f$ can be uniquely extended to an isomorphism between $\overline{\mathfrak{K}_1}^{\mathfrak{L}_1}$ and $\overline{\mathfrak{K}_2}^{\mathfrak{L}_2}$.*

**Proof.**

- If $\overline{\mathfrak{K}_1}^{\mathfrak{L}_1} = \mathfrak{K}_1$, then also $\overline{\mathfrak{K}_2}^{\mathfrak{L}_2} = \mathfrak{K}_2$ and so the claim of the theorem is trivial.
- Hence, we suppose $\overline{\mathfrak{K}_1}^{\mathfrak{L}_1} \neq \mathfrak{K}_1$. Let $P(x)$ be a polynomial over $\mathfrak{K}_1$ of the smallest degree among those with roots in $|\overline{\mathfrak{K}_1}^{\mathfrak{L}_1}| - |\mathfrak{K}_1|$, and $u$ be one of its roots.
- $\mathfrak{K}_1(u)$ inherits an order as a substructure of $\mathfrak{L}_1$. On the other hand, it coincides with the order of $\mathfrak{K}_1[x]/P(x)$ defined in the proof of the above theorem. This is because the sign of an element $[Q(x)]_{\approx}$ in $\mathfrak{K}_1[x]/P(x)$ is defined by the sign of $Q(x)$ in the neighborhood of $u$, and so when $Q(u)$ exists, its sign must be the same.

- By the minimality of the degree of $P(x)$, $P'(u) \neq 0$. In particular, we assume $P'(u) > 0$.
- Therefore, by the previous lemma, there exist $a, b \in |\mathfrak{K}_1|$ such that $a < u < b$ and $P'(x) > 0$ on the interval $(a, b)$.
- Then by the contrapositive of Rolle's Theorem, $P(x)$ is strictly increasing on this interval, and so the root $u$ is uniquely determined in the interval by $P(x)$.
- Hence, if $P(x)$ is mapped to $R(x)$ by the isomorphism $f : \mathfrak{K}_1 \to \mathfrak{K}_2$, then $R(x)$ uniquely determines an element $v$ of $\overline{\mathfrak{K}_2}^{\mathfrak{L}_1}$ in the interval $(f(a), f(b))$. Then, as ordered fields, the following isomorphisms hold (cf. Claim 4 of the last theorem):

$$\mathfrak{K}_1(u) \cong \mathfrak{K}_1[x]/P(x) \cong \mathfrak{K}_2[x]/R(x) \cong \mathfrak{K}_2(v).$$

- Therefore, we can extend $f : \mathfrak{K}_1 \to \mathfrak{K}_2$ by mapping $u$ to $v$, resulting in an isomorphism from $\mathfrak{K}_1(u)$ to $\mathfrak{K}_2(v)$.

- Consider all isomorphisms between ordered fields $\mathfrak{M}_1 \subseteq \overline{\mathfrak{K}_1}^{\mathfrak{L}_1}$ and $\mathfrak{M}_2 \subseteq \overline{\mathfrak{K}_2}^{\mathfrak{L}_2}$ that extend $f : \mathfrak{K}_1 \to \mathfrak{K}_2$. By Zorn's Lemma, we can choose a maximal ordered field $\mathfrak{M}_1$.
- If $\mathfrak{M}_1 \subsetneqq \overline{\mathfrak{M}_1}^{\mathfrak{L}_1} = \overline{\mathfrak{K}_1}^{\mathfrak{L}_1}$, then we can extend $\mathfrak{M}_1$, which contradicts its maximality.
- Hence, $\mathfrak{M}_1 = \overline{\mathfrak{K}_1}^{\mathfrak{L}_1}$. Then, it's clear that $\mathfrak{M}_2$ is also identical to $\overline{\mathfrak{K}_2}^{\mathfrak{L}_2}$.
- Finally, since each $u$ in $\overline{\mathfrak{K}_1}^{\mathfrak{L}_1}$ is uniquely determined as the $n$-th root of a polynomial, the corresponding element $v$ in $\overline{\mathfrak{K}_2}^{\mathfrak{L}_2}$ is also uniquely determined as the $n$-th root of the corresponding polynomial, and thus the extension of the isomorphism is unique. $\square$

By the above theorem and the lemma for isomorphism condition, any ordered field $\mathfrak{K}$ has a unique real closed ordered field which is an algebraic extension (up to isomorphisms). Such a real closed ordered field is called the **real closure** of $\mathfrak{K}$.

In the following lectures, we will prove the quantifier elimination of real closed ordered fields. Now, we prove one more lemma necessary for this purpose.

### Lemma (1-model completeness)

*Let $\mathfrak{K} \subseteq \mathfrak{L}$ be two real closed ordered fields. For any open formula $\varphi(\vec{x}, y)$ and elements $\vec{a}$ of $\mathfrak{K}$,*

$$\mathfrak{L}_{\{\vec{a}\}} \models \exists y \varphi(\vec{a}, y) \;\Rightarrow\; \mathfrak{K}_{\{\vec{a}\}} \models \exists y \varphi(\vec{a}, y).$$

**Proof.**

- We express the open formula $\varphi(\vec{x}, y)$ in disjunctive normal form. Since we have

  $$u \neq v \leftrightarrow u < v \vee v < u$$

  and

  $$u \not< v \leftrightarrow u = v \vee v < u$$

  $\varphi(\vec{x}, y)$ can be expressed as a disjunction ($\vee$) of a conjunction ($\wedge$) of atomic formulas without using negation.

- Therefore, $\exists y \varphi(\vec{x}, y)$ is expressed by a disjunction of formulas in the form:

  $$\exists y(\alpha_1(\vec{x}, y) \wedge \cdots \wedge \alpha_k(\vec{x}, y))$$

  where $\alpha_i$ is an atomic formula.

- Now, assuming that $\exists y(\alpha_1(\vec{a}, y) \wedge \cdots \wedge \alpha_k(\vec{a}, y))$ holds in $\mathfrak{L}_{\{\vec{a}\}}$, it suffices to show that it holds in $\mathfrak{K}_{\{\vec{a}\}}$. In what follows, we write $\mathfrak{L}, \mathfrak{K}$ for $\mathfrak{L}_{\{\vec{a}\}}, \mathfrak{K}_{\{\vec{a}\}}$, respectively

- First, $\alpha_1(\vec{a}, y) \wedge \cdots \wedge \alpha_k(\vec{a}, y)$ consists of equations and inequalities. Since atomic formulas not involving $y$ can be moved outside $\exists y$, we may assume each $\alpha_i(\vec{a}, y)$ is expressed as $P(y) = 0$ or $Q(y) > 0$.
- Suppose it contains a equation $P(y) = 0$. Since any $y = b$ satisfying $P(y) = 0$ in $\mathfrak{L}$ is also algebraic over $\mathfrak{K}$, it belongs to the real closed field $\mathfrak{K}$. Furthermore, if $\alpha_1(\vec{a}, b) \wedge \cdots \wedge \alpha_k(\vec{a}, b)$ holds in $\mathfrak{L}$, it obviously holds in $\mathfrak{K}$.
- Next, suppose that $\alpha_1(\vec{a}, y) \wedge \cdots \wedge \alpha_k(\vec{a}, y)$ contains only inequalities $Q_i(y) > 0$.
- Let $S$ denote the set of all real roots of $Q_i(y) = 0$ for $i$ $(1 \leq i \leq k)$, which is the same set whether it is considered in $\mathfrak{L}$ or $\mathfrak{K}$.
- In $\mathfrak{L}$, $\exists y(Q_1(y) > 0 \wedge \cdots \wedge Q_k(y) > 0)$ implies, by the Intermediate Value Theorem the existence of adjacent points $a$ and $b$ in $S$ such that for any point $z$ in $(a, b)$, $Q_1(z) > 0 \wedge \cdots \wedge Q_k(z) > 0$ holds, or for the maximum or minimum $c$ in $S$, for any point $z$ in $(c, +\infty)$ or $(-\infty, c)$, $Q_1(z) > 0 \wedge \cdots \wedge Q_k(z) > 0$ holds.
- Thus, $z = (a + b)/2$ or $z = c \pm 1$ in $\mathfrak{K}$ satisfies $Q_1(z) > 0 \wedge \cdots \wedge Q_k(z) > 0$. $\square$

# Thank you for your attention!