Quantifier-elimination in algebraically closed fields

Introductory Model Theory

November 18–25, 2021

Recommended reading: Poizat's *Course in Model Theory*, Chapter 6.1.

Definition 1. A *field* is a structure $(K, +, \cdot, -, 0, 1)$ satisfying the axioms

$$\forall x, y, z \Big(x + y = y + x \ \wedge \ x \cdot y = y \cdot x \ \wedge \ x \cdot 1 = x \ \wedge \ x + 0 = x \ \wedge \ x + (-x) = 0$$
$$\wedge \ x + (y + z) = (x + y) + z \ \wedge \ x \cdot (y \cdot z) = (x \cdot y) \cdot z \ \wedge \ x \cdot (y + z) = (x \cdot y) + (x \cdot z)\Big)$$
$$0 \neq 1 \ \wedge \ \forall x \ (x \neq 0 \to \exists y \ (x \cdot y = 1)).$$

A *ring* is defined similarly, without the last line.

For example, $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are fields, and $\mathbb{Z}$ is a ring.

Fact 2. *In a ring,* $(x = 0 \ \vee \ y = 0) \to xy = 0$*. In a field,* $xy = 0 \to (x = 0 \ \vee \ y = 0)$*.*

1 Polynomials

If K is a field, a *polynomial* is a formal expression

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

where $a_0, \ldots, a_n \in K$. The degree of P is $\deg P = n$ (assuming $a_n \neq 0$). We say P is *monic* if $a_n = 1$. The ring of polynomials is written $K[x]$.

Lemma 3 (Polynomial division)**.** *If* $P(x) \in K[x]$ *is monic and* $A(x) \in K[x]$*, then there are* $Q(x), R(x) \in K[x]$ *such that* $A(x) = Q(x)P(x) + R(x)$*, and* $\deg R < \deg P$*.*

Proof. By induction on $\deg A$. If $\deg A < \deg P$ take $R = A$ and $Q = 0$. Otherwise, let $A = a_n x^n + \cdots$, where $n = \deg A \geq \deg P$. Let $P = x^m + p_{m-1} x^{m-1} + \cdots$, where $m = \deg P$. Then $A - a_n x^{n-m} P = (a_n x^n + \cdots) - (a_n x^n + a_n p_{m-1} x^{n-1} + \cdots)$, a polynomial of lower degree. By induction, there are Q' and R such that

$$A - a_n x^{n-m} P = Q'P + R$$
$$A = (a_n x^{n-m} + Q')P + R.$$

□

Lemma 4. *Suppose $P(x) \in K[x]$ and $P(a) = 0$ for some $a \in K$. Then $P(x) = (x-a)Q(x)$ for some $Q(x) \in K[x]$.*

Proof. Apply the Division Lemma to write $P(x) = (x-a)Q(x) + R(x)$ where $\deg R(x) < \deg(x-a) = 1$. Then $R(x) = c$ for some $c \in K$. But

$$0 = P(a) = (a-a)Q(a) + R(a) = R(a) = c,$$

so $R(x) = c = 0$, and then $P(x) = (x-a)Q(x)$. $\square$

The set of *roots* of $P(x)$ is $\{a \in K : P(a) = 0\}$. Note that $roots(P \cdot Q) = roots(P) \cup roots(Q)$, by Fact 2.

Lemma 5. *Let $P(x)$ be a non-zero polynomial of degree n. Then $P(x)$ has at most n roots in K.*

Proof. If $P(x)$ has no roots we are done. Otherwise $P(a) = 0$ for some a. Then $P(x) = (x-a)Q(x)$. We have $\deg P = 1 + \deg Q$, so $\deg Q = n-1$. By induction, $Q(x)$ has at most $n-1$ roots. The roots of P are a and the roots of Q, so P has at most n roots. $\square$

Theorem 6. *The following are equivalent for a field K:*

1. *Every polynomial of degree n factors as $c \cdot \prod_{i=1}^{n}(x-a_i)$.*
2. *Every polynomial of degree $n > 0$ has a root.*

Proof. (1) $\implies$ (2): Given $P(x)$ of degree $n > 0$, write $P(x) = c \cdot \prod_{i=1}^{n}(x-a_i)$. Then a_1 is a root of $P(x)$.

(2) $\implies$ (1): Let $P(x)$ have degree n. If $n = 0$, then $P(x)$ is a constant $c \in K$, so $P(x) = c \cdot 1$. If $n > 0$, then $P(x)$ has a root b, so $P(x) = (x-b)Q(x)$. By induction on degree, $Q(x) = c \cdot \prod_{i=1}^{n-1}(x-a_i)$, so $P(x) = c \cdot (x-b) \cdot \prod_{i=1}^{n-1}(x-a_i)$. $\square$

Definition 7. A field K is *algebraically closed* if the equivalent conditions of Theorem 6 hold.

Fact 8 (Fundamental theorem of algebra)**.** *$\mathbb{C}$ is an algebraically closed field.*

Algebraically closed fields are axiomatized by the field axioms plus the axiom schema

$$\forall y_0, \ldots, y_n \left(y_n \neq 0 \to \exists x \sum_{i=0}^{n} y_i x^i = 0 \right)$$

for $n > 0$. This theory is denoted ACF. We will show ACF has quantifier elimination.

Lemma 9. *If $K \models$ ACF, then K is infinite.*

Proof. If $K = \{a_1, \ldots, a_n\}$, then $P(x) = 1 + \prod_{i=1}^{n}(x-a_i)$ has no root in K. $\square$

2 Fields of fractions

Theorem 10. *Let K be a field and R be a subring. Define* $\mathrm{Frac}(R) = \{a/b : a, b \in R,\ b \neq 0\}$. *Then* $\mathrm{Frac}(R)$ *is a subfield of K.*

Proof sketch. We must show $\mathrm{Frac}(R)$ is closed under addition, multiplication, subtraction, and division. This is straightforward. For example, $\mathrm{Frac}(R)$ is closed under addition because

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}. \qquad \square$$

$\mathrm{Frac}(R)$ is called the *field of fractions* of R, and is the subfield of K generated by R. As an example, $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.

Theorem 11. *Let K_1, K_2 be fields. Let R_1, R_2 be subrings, respectively. Let $f : R_1 \to R_2$ be an isomorphism. Then f extends to an isomorphism $g : \mathrm{Frac}(R_1) \to \mathrm{Frac}(R_2)$.*

Proof sketch. Define by $g(a/b) = f(a)/f(b)$. Then g is a well-defined isomorphism from F_1 to F_2 extending f. For example, g is well-defined because

$$a/b = c/d \implies ad = bc \implies f(a)f(d) = f(b)f(c) \implies f(a)/f(b) = f(c)/f(d).$$

The map g preserves addition because

$$\begin{aligned} g\left(\frac{a}{b} + \frac{c}{d}\right) &= g\left(\frac{ad+bc}{bd}\right) = \frac{f(ad+bc)}{f(bd)} = \frac{f(a)f(d) + f(b)f(c)}{f(b)f(d)} \\ &= \frac{f(a)}{f(b)} + \frac{f(c)}{f(d)} = g\left(\frac{a}{b}\right) + g\left(\frac{c}{d}\right). \end{aligned} \qquad \square$$

3 Prime ideals

Definition 12. An *ideal* in a ring R is a subset $I \subseteq R$ such that

- $x, y \in I \implies x + y \in I$.
- $0 \in I$.
- $x \in I, y \in R \implies xy \in I$.

I is a *prime ideal* if $1 \notin I$ and for $x, y \in R$ we have $x, y \notin I \implies xy \notin I$.

Example. The even numbers $2\mathbb{Z}$ are a prime ideal in the ring $\mathbb{Z}$.

Theorem 13. *Let R be a ring and K be a field and $f : R \to K$ be a map satisfying*

$$\begin{gathered} f(x+y) = f(x) + f(y) \\ f(xy) = f(x)f(y) \\ f(1) = 1. \end{gathered}$$

Let $I = \{x \in R : f(x) = 0\}$. Then I is a prime ideal.

Such a map is called a *homomorphism* and I is called the *kernel*.

Proof. Note that $f(0) + 1 = f(0 + 1) = f(1) = 1 = 0 + 1$. Add -1 to both sides, simplify, and see $f(0) = 0$. We verify the definition of a prime ideal.

- If $f(x) = 0$ and $f(y) = 0$, then $f(x + y) = f(x) + f(y) = 0 + 0 = 0$.
- $f(0) = 0$.
- If $f(x) = 0$ and $y \in R$, then $f(xy) = f(x)f(y) = 0 \cdot f(y) = 0$.
- $f(1) = 1 \neq 0$.
- Suppose $f(x) \neq 0$ and $f(y) \neq 0$. Then $f(xy) = f(x)f(y) \neq 0$. $\square$

Lemma 14 (Division)**.** *If $n > 0$ and $a \in \mathbb{Z}$, there are $q, r \in \mathbb{Z}$ such that $a = qn + r$, and $r \in \{0, \ldots, n-1\}$.*

Proof. Let $q = \lfloor a/n \rfloor$, and $r = a - qn$. Then $r/n = a/n - q = a/n - \lfloor a/n \rfloor$, so $0 \leq r/n < 1$, and $0 \leq r < n$. $\square$

Theorem 15. *Let I be an ideal in $\mathbb{Z}$.*

1. *$I = n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$ for some $n \geq 0$.*
2. *If I is a prime ideal, then n is 0 or a prime number.*

Proof.

1. Note $\{0\} \subseteq I$. If $I = \{0\}$, take $n = 0$. Otherwise, take $n \in I \setminus \{0\}$ minimizing $|n|$. If $n < 0$, replace n with $-n = n \cdot (-1) \in I$. Then $n\mathbb{Z} \subseteq I$ because I is an ideal. We claim $n\mathbb{Z} = I$. Otherwise, take $a \in I \setminus n\mathbb{Z}$. Then $a = qn + r$ for some $r \in \{0, \ldots, n-1\}$. But $r = a - qn = a + n(-q) \in I$. This contradicts the choice of n unless $r = 0$, in which case $a = qn \in n\mathbb{Z}$, contradicting the choice of a.
2. If $n = 1$, then $1 \in n\mathbb{Z}$, and I is not prime. If $n = ab$ where $a, b > 1$, then $a \notin n\mathbb{Z}$ and $b \notin n\mathbb{Z}$, but $ab = n \in n\mathbb{Z}$, and I is not prime. $\square$

Theorem 16. *Let I be an ideal in $K[x]$.*

1. *$I = P \cdot K[x]$ for some polynomial P that is monic or zero.*
2. *If I is a prime ideal, then P is 0 or an irreducible polynomial.*

Proof. Similar to Theorem 15. $\square$

4 Algebraic and transcendental elements

Fix a field L and a subfield K.

Definition 17. An element $a \in L$ is *algebraic over* K if there is a non-zero polynomial $P(x) \in K[x]$ such that $P(a) = 0$. Otherwise, a is *transcendental over* K.

Example. $\sqrt{2}$ is algebraic over $\mathbb{Q}$ because it's a root of $x^2 - 2 = 0$.

Fact 18 (Lindemann)**.** *π is transcendental over $\mathbb{Q}$.*

Definition 19. $I_{a/K} = \{P(x) \in K[x] : P(a) = 0\}$.

Lemma 20. *$I_{a/K}$ is a prime ideal in $K[x]$.*

Proof. $I_{a/K}$ is the kernel of the homomorphism

$$\begin{aligned} K[x] &\to L \\ P(x) &\mapsto P(a). \end{aligned}$$

□

Theorem 21. *If a is transcendental over K, then $I_{a/K} = 0 \cdot K[x] = \{0\}$.*

If a is algebraic over K, then $I_{a/K} = P(x) \cdot K[x] = \{P(x)Q(x) : Q(x) \in K[x]\}$ for some irreducible monic polynomial $P(x) \in K[x]$, called the minimal polynomial *of a over K.*

If $M \models \mathrm{ACF}$ and K is a subfield, then K^{alg} denotes the set of $a \in M$ algebraic over K.

Remark 22. If $M \models \mathrm{ACF}$ and K is a countable subfield, then K^{alg} is countable. (This uses Lemma 5.)

5 Quantifier elimination in ACF

Recall from November 11,

Fact 23. *Suppose M, N are $\mathcal{L}$-structures. Suppose $\bar{a} \in M^n$ and $\bar{b} \in N^n$. If $\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b})$, then there is an isomorphism $f : \langle \bar{a} \rangle_M$ to $\langle \bar{b} \rangle_N$ such that $f(\bar{a}) = \bar{b}$.*

Lemma 24. *Suppose M, N are uncountable models of ACF. Suppose $\bar{a} \in M^n$ and $\bar{b} \in N^n$ and $\mathrm{qftp}^M(\bar{a}) = \mathrm{qftp}^N(\bar{b})$. Suppose $\alpha \in M$. Then there is $\beta \in N$ such that $\mathrm{qftp}^M(\bar{a}, \alpha) = \mathrm{qftp}^N(\bar{b}, \beta)$.*

Proof. Let $A = \langle \bar{a} \rangle_M$ and $B = \langle \bar{b} \rangle_M$. There is an isomorphism $f : A \to B$ with $f(\bar{a}) = \bar{b}$. By Theorem 11 we can extend f to an isomorphism $f : \mathrm{Frac}(A) \to \mathrm{Frac}(B)$. Moving N by an isomorphism, we may assume $\mathrm{Frac}(A) = \mathrm{Frac}(B)$ and $f = \mathrm{id}_{\mathrm{Frac}(A)}$. (In particular, $\bar{a} = \bar{b}$.) Let $K = \mathrm{Frac}(A)$.

Claim. There is $\beta \in N$ with $I_{\alpha/K} = I_{\beta/K}$.

Proof. First suppose α is algebraic over K with minimal polynomial $P(x)$. Take $\beta \in N$ with $P(\beta) = 0$. Let $Q(x)$ be the minimal polynomial over β over K. Then $P(x) \in Q(x) \cdot K[x]$. But $P(x)$ is irreducible, so $P(x) = Q(x)$. Then $I_{\alpha/K} = P(x) \cdot K[x] = I_{\beta/K}$.

Next, suppose α is transcendental. By Remark 22, there is transcendental $\beta \in N$. Then $I_{\alpha/K} = \{0\} = I_{\beta/K}$. $\square_{\text{Claim}}$

Take such a β. Let $I = I_{\alpha/K} = I_{\beta/K}$.

- If $P(x) \in K[x]$, then $P(\alpha) = 0 \iff P(x) \in I \iff P(\beta) = 0$.
- If $P(x), Q(x) \in K[x]$, then $P(\alpha) = Q(\alpha) \iff (P - Q)(\alpha) = 0 \iff (P - Q)(\beta) = 0 \iff P(\beta) = Q(\beta)$.
- If $\varphi(x)$ is an atomic $\mathcal{L}(K)$-formula, then $M \models \varphi(\alpha) \iff N \models \varphi(\beta)$.
- If $\varphi(x)$ is a quantifier-free $\mathcal{L}(K)$-formula, then $M \models \varphi(\alpha) \iff N \models \varphi(\beta)$.

In particular, if $\psi(\bar{y}, x)$ is a quantifier-free $\mathcal{L}$-formula, then

$$M \models \psi(\bar{a}, \alpha) \iff N \models \psi(\bar{a}, \beta). \qquad \square$$

Lemma 25. *Lemma 24 holds if we replace "uncountable" with "ω-saturated."*

Proof. Take uncountable $M' \succeq M$ and $N' \succeq N$. (This is possible by upward Löwenheim-Skolem and Lemma 9.) By Lemma 24, there is $\beta_0 \in N'$ such that $\mathrm{qftp}(\bar{a}, \alpha) = \mathrm{qftp}(\bar{b}, \beta_0)$. By ω-saturation, we can find $\beta \in N$ such that $\mathrm{tp}(\beta/\bar{b}) = \mathrm{tp}(\beta_0/\bar{b})$. Then $\mathrm{tp}(\bar{b}, \beta) = \mathrm{tp}(\bar{b}, \beta_0)$, so

$$\mathrm{qftp}(\bar{b}, \beta) = \mathrm{qftp}(\bar{b}, \beta_0) = \mathrm{qftp}(\bar{a}, \alpha). \qquad \square$$

Theorem 26. *ACF has quantifier elimination.*

6 Completions of ACF

If K is a field and $n \in \mathbb{Z}$, let n^K denote the interpretation of n in K, i.e.,

$$n^K = \begin{cases} \underbrace{1 + \cdots + 1}_{n \text{ times}} & \text{if } n > 0 \\ 0 & \text{if } n = 0 \\ \underbrace{-(1 + \cdots + 1)}_{-n \text{ times}} & \text{if } n < 0. \end{cases}$$

where the right-hand side is interpreted in K.

Fact 27. *If $n, m \in \mathbb{Z}$, then*

$$n^K + m^K = (n + m)^K$$
$$n^K \cdot m^K = (n \cdot m)^K$$
$$-(n^K) = (-n)^K.$$

For example, when $n = 2$ and $m = 3$, the first line is saying that

$$K \models (1 + 1) + (1 + 1 + 1) = 1 + 1 + 1 + 1 + 1.$$

Theorem 28. *Let $I = \{n \in \mathbb{Z} : n^K = 0\}$. Then I is a prime ideal in $\mathbb{Z}$, so $I = p\mathbb{Z}$ for some $p \in \{0, 2, 3, 5, 7, 11, \ldots\}$.*

The number p is called the *characteristic* of K, written $\operatorname{char}(K)$.

Example. In $\mathbb{C}$, $n^{\mathbb{C}} = n$, so $n^{\mathbb{C}} = 0 \iff n = 0$, and $I = \{0\} = 0\mathbb{Z}$. Therefore $\operatorname{char}(\mathbb{C}) = 0$.

Theorem 29. *Suppose $M, N \models \mathrm{ACF}$. Then $M \equiv N \iff \operatorname{char}(M) = \operatorname{char}(N)$.*

Proof. The following are equivalent:

- $M \equiv N$.
- For every sentence φ, $M \models \varphi \iff N \models \varphi$.
- For every quantifier-free sentence φ, $M \models \varphi \iff N \models \varphi$.
- For every atomic sentence φ, $M \models \varphi \iff N \models \varphi$.
- For any terms t_1, t_2, $M \models t_1 = t_2 \iff N \models t_1 = t_2$.
- For any term t, $M \models t = 0 \iff N \models t = 0$.
- For any $n \in \mathbb{Z}$, $M \models n = 0 \iff N \models n = 0$.
- $\{n \in \mathbb{Z} : n^M = 0\} = \{n \in \mathbb{Z} : n^N = 0\}$.
- $\operatorname{char}(M) = \operatorname{char}(N)$. □

For $p \in \{0, 2, 3, 5, 7, 11, \ldots\}$, we let ACF_p denote the theory of algebraically closed fields of characteristic p.

Corollary 30. ACF_p *is a complete theory, for each p.*

Corollary 31. *The field $\mathbb{C}$ is completely axiomatized by* ACF_0.

If you know Gödel's completeness theorem and recursion theory, this implies

Corollary 32. *The set $\{\varphi \in L : \mathbb{C} \models \varphi\}$ is computable. There is an algorithm which takes as input a sentence φ in the language of rings, and outputs whether or not φ is true in $\mathbb{C}$.*

Proof. Enumerate all statements provable from ACF_0 until we find a proof of φ or a proof of $\neg\varphi$. By completeness of ACF_0, this algorithm is guaranteed to terminate. □

7 The algebraic closure of a field

Recall if $K \subseteq M \models \text{ACF}$, then K^{alg} is the set of $a \in M$ algebraic over K. If $\varphi(x)$ is a formula, then $\varphi(M)$ denotes the set $\{a \in M : M \models \varphi(a)\}$.

Lemma 33. *Let M be algebraically closed. Let K be a subfield. Let $\varphi(x)$ be an $\mathcal{L}(K)$-formula in one variable. Let $D = \varphi(M)$. Then there is a finite subset $S \subseteq K^{alg}$ such that $D = S$ or $D = M \setminus S$.*

Proof. By quantifier elimination, we may assume φ is quantifier-free. Then φ is a boolean combination of atomic formulas.

Let $\mathcal{F} = \{S : S \subseteq_f K^{alg}\} \cup \{M \setminus S : S \subseteq_f K^{alg}\}$. Note $\mathcal{F}$ is closed under boolean combinations. So we may assume φ is an atomic formula.

Then $\varphi(x)$ is $(P(x) = 0)$ for some $P(x) \in K[x]$. If $P(x) \equiv 0$, then $\varphi(M) = M \in \mathcal{F}$. Otherwise, $\varphi(M) \subseteq_f K^{alg}$, so $\varphi(M) \in \mathcal{F}$. $\square$

Lemma 34. *Suppose $M \preceq N \models$ ACF and K is a subfield of M. Suppose $c \in N$ is algebraic over K. Then $c \in M$.*

Proof. Let $P(x)$ be the minimal polynomial of c over K. Let $b_1, \ldots, b_n$ be the roots of $P(x)$ in M. Then

$$M \models \forall x \left(P(x) = 0 \to \bigvee_{i=1}^{n} x = b_i \right),$$

so the same holds in N. Then $P(c) = 0 \implies c \in \{b_1, \ldots, b_n\} \subseteq M$. $\square$

Theorem 35. *If $M \models$ ACF and K is a subfield, then K^{alg} is a subfield of M and $(K^{alg})^{alg} = K^{alg}$.*

Proof. Suppose $a, b \in K^{alg}$. We claim $a + b \in K^{alg}$. Let $P(x)$ and $Q(y)$ be the minimal polynomials of a, b over K. Let $\varphi(z)$ be the $\mathcal{L}(K)$-formula

$$\exists x, y \ (P(x) = 0 \ \wedge \ Q(y) = 0 \ \wedge \ x + y = z).$$

Then $M \models \varphi(a+b)$, and $\varphi(M) = \{x + y : P(x) = 0 = Q(y)\}$ is finite. Thus $a + b \in \varphi(M) \subseteq K^{alg}$.

A similar argument shows K^{alg} is closed under the field operations, so K^{alg} is a subfield of M.

A similar but more complicated agument shows that if $c_0, \ldots, c_n \in K^{alg}$ with $c_n \neq 0$, and $\sum_{i=0}^{n} c_i a^i = 0$, then $a \in K^{alg}$. So $(K^{alg})^{alg} = K^{alg}$. $\square$

Theorem 36. *Suppose $M \models$ ACF and K is a subfield. The following are equivalent:*

1. *$K = K^{alg}$.*

2. *$K \models$ ACF.*

3. $K \preceq M$*.*

Proof. (1) $\Longrightarrow$ (2): suppose $P(x) \in K[x]$ has degree > 0. Then there is $c \in M$ such that $P(c) = 0$. By definition, $c \in K^{alg} = K$.

(2) $\Longrightarrow$ (3): Let $\varphi(\bar{x})$ be a formula and $\bar{a}$ be a tuple in K. We need

$$K \models \varphi(\bar{a}) \iff M \models \varphi(\bar{a}). \tag{$*$}$$

By quantifier-elimination, we may assume $\varphi(\bar{x})$ is quanifier-free, in which case $(*)$ is automatic.

(3) $\Longrightarrow$ (1): Suppose $c \in K^{alg}$. Then $c \in K$ by Lemma 34. □

Corollary 37. *If* $M \models \mathrm{ACF}$ *and* K *is a subfield, then* $K^{alg} \models \mathrm{ACF}$*.*

K^{alg} is called the *algebraic closure* of K. It's independent of M:

Theorem 38. *Let* M, N *be two algebraically closed fields extending* K*. Let* $(K^{alg})_M$ *and* $(K^{alg})_N$ *be* K^{alg} *in* M *and* N*, respectively. Then* $(K^{alg})_M \cong (K^{alg})_N$*.*

Proof. There are a few cases:

1. $M \preceq N$. Then $(K^{alg})_M = (K^{alg})_N$ by Lemma 34.
2. There is an $\mathcal{L}(K)$-elementary embedding $M \to N$. Moving M by an isomorphism, reduce to case 1.
3. Suppose $M \equiv N$ as $\mathcal{L}(K)$-structures. By elementary amalgamation, there is an $\mathcal{L}(K)$-structure M' and $\mathcal{L}(K)$-elementary embeddings $M \to M'$ and $N \to M'$. Then $(K^{alg})_M \cong (K^{alg})_{M'} \cong (K^{alg})_N$ by case 2.

In fact, case 3 always holds: if φ is an $\mathcal{L}(K)$-sentence, then there is an equivalent quantifier-free $\mathcal{L}(K)$-sentence ψ, and

$$M \models \varphi \iff M \models \psi \iff K \models \psi \iff N \models \psi \iff N \models \varphi.$$

So $M \equiv N$ as $\mathcal{L}(K)$-structures. □

Fact 39. *If* K *is a field, then* K *is a subfield of an algebraically closed field.*

So we can talk about "the" algebraic closure K^{alg} of an abstract field K.

8 Ordered fields and real closed fields

Definition 40. Let K be a field. A *field ordering* is a linear order $\leq$ on K satisfying the following:

- If $x \leq y$, then $x + z \leq y + z$.

- If $x \leq y$ and $0 \leq z$, then $xz \leq yz$.

An *ordered field* is $(K, \leq)$ where K is a field and $\leq$ is a field ordering.

Example. $\mathbb{R}, \mathbb{Q}$ are ordered fields.

Fact 41. *$\mathbb{C}$ does not admit a field ordering. If $\operatorname{char}(K) \neq 0$, then K does not admit a field ordering. Ordered fields have characteristic 0.*

Definition 42. An ordered field K is *real closed* if the intermediate value theorem holds for polynomials: if $P(x) \in K[x]$ and $P(a) < 0 < P(b)$, then $P(c) = 0$ for some c between a and b.

Example. $\mathbb{R}$ is real closed, but $\mathbb{Q}$ is not.

Example. Let $K = \mathbb{Q}^{alg} \cap \mathbb{R}$, the set of real algebraic numbers. Then K is real closed. If $P(x) \in K[x]$ and $P(a) < 0 < P(b)$, then there is some $c \in \mathbb{R}$ such that $P(c) = 0$. But then $c \in K^{alg} = \mathbb{Q}^{alg}$, so $c \in \mathbb{Q}^{alg} \cap \mathbb{R} = K$.

The theory of real closed fields is denoted RCF.

Definition 43. Let K be a field and L be an extension. Then L is an *algebraic extension* of K if every element of L is algebraic over K.

Fact 44. *Let K be an ordered field. Then there is an ordered field extension $L \supseteq K$ such that $L \models \mathrm{RCF}$ and L is algebraic over K. The ordered field L is unique up to isomorphism.*

We call L the *real closure* of K.

Example. The real closure of $\mathbb{Q}$ is $\mathbb{Q}^{alg} \cap \mathbb{R}$.

Fact 45 (Tarski-Seidenberg)**.** *RCF has quantifier elimination.*

See Section 6.6 of the textbook for a proof (which requires some algebra).

Corollary 46. *$\mathbb{R} \cap \mathbb{Q}^{alg}$ is an elementary substructure of $\mathbb{R}$.*

If $M \models \mathrm{RCF}$, then the minimal substructure $\langle \varnothing \rangle_M$ is always isomorphic to $\mathbb{Q}$.

Corollary 47. *RCF is complete. The structure $\mathbb{R}$ is completely axiomatized by RCF. The theory of $\mathbb{R}$ is decidable: there is an algorithm which take a sentence φ as input, and outputs whether or not $\mathbb{R} \models \varphi$.*

Corollary 48. *Let K be a real-closed field. Let $\varphi(x)$ be an $\mathcal{L}(K)$-formula in one variable. Then the set $\varphi(K) = \{a \in K : K \models \varphi(a)\}$ is a finite union of points and intervals.*

The proof is roughly like Lemma 33. This property is called "o-minimality," and turns out to have many very strong consequences. For more about o-minimality, see the book *Tame topology and o-minimal structures*, by Lou van den Dries.