25. Quantifier elimination for ACF

Recall: ACF is the theory of algebraically closed fields in the language of rings $+, -, 0, \cdot, 1$.

Theorem (Tarski)

ACF has quantifier elimination.

For the proof we use basic facts on field theory (see e.g. Dummit & Foote: Abstract Algebra).

- A commutative ring $\mathcal{R} := (R, +, -, 0, \cdot, 1)$ is an **integral domain** if $\mathcal{R} \models \forall x, y \; xy = 0 \rightarrow (x = 0 \vee y = 0)$.
- For an integral domain $\mathcal{R}$, define an equivalence $\sim$ on $R \times (R \setminus \{0\})$ by

$$(a, b) \sim (c, d) \quad \text{if} \quad ad = bc$$

  and write $\frac{a}{b}$ for the equivalence class $(a, b)/\sim$.
- The **field of fractions** of an integral domain $\mathcal{R}$ is the field $\mathcal{F}$ with universe $(R \times (R \setminus \{0\}))/\sim$ where

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}.$$

- If $\mathcal{R}$ is an integral domain, then so is the polynomial ring $\mathcal{R}[x]$.
- Let $\mathcal{F}$ be field. Then field of fractions $\mathcal{F}(x)$ of $\mathcal{F}[x]$ is called a **rational function field**. Elements are of the form $\frac{p(x)}{q(x)}$ for $p(x), q(x) \in F[x], q(x) \neq 0$.

- Let $\mathcal{F}$ be a field with extension $\mathcal{E}$. Then $a \in E$ is **algebraic over** $\mathcal{F}$ if a is the root of some non-zero polynomial over F; else a is **transcendental** over $\mathcal{F}$.
  The extension $\mathcal{F}(a)$ of $\mathcal{F}$ by a is the smallest subfield of $\mathcal{E}$ containing F and a.
- $\mathcal{E}$ is an **algebraic extension** of $\mathcal{F}$ if every $a \in E$ is algebraic over $\mathcal{F}$.
- $\mathcal{F}$ is **algebraically closed** if every non-constant polynomial over F has a root in F.
- (Steinitz) Let $\mathcal{F}$ be a field with algebraic extensions $\mathcal{E}_1$ and $\mathcal{E}_2$ that are algebraically closed. Then there exists an isomorphism between $\mathcal{E}_1$ and $\mathcal{E}_2$ fixing each element of F.
  (Hence the algebraic closure of $\mathcal{F}$ is unique up to isomorphism.)
- If a is transcendental over $\mathcal{F}$, then $\mathcal{F}(x) \to \mathcal{F}(a)$, $\frac{p(x)}{q(x)} \mapsto \frac{p(a)}{q(a)}$, is a field isomorphism fixing F.

Consequences of quantifier elimination

A theory T is **model-complete** if for all models $\mathcal{A}, \mathcal{B}$ of T

$$\mathcal{A} \leq \mathcal{B} \quad \Rightarrow \quad \mathcal{A} \prec \mathcal{B}$$

T is model complete iff all embeddings are elementary.

Theorem

If T has quantifier elimination, then T is model complete.

Proof.

Let $\mathcal{A}, \mathcal{B} \models T$ and $\mathcal{A} \leq \mathcal{B}$.
Let ϕ be an arbitrary formula, equivalent modulo T to some quantifier-free ψ, let $\bar{a} \in A$. Then

$$\mathcal{A} \models \phi(\bar{a}) \quad \text{iff} \quad \mathcal{A} \models \psi(\bar{a}) \quad \text{iff} \quad \mathcal{B} \models \psi(\bar{a}) \quad \text{iff} \quad \mathcal{B} \models \phi(\bar{a})$$

Recall quantifier-free formulas are preserved by substructures and extensions.
Hence $\mathcal{A}$ is an elementary substructure of $\mathcal{B}$. $\square$

We already proved that ACF_p are the completions of ACF by Tarski-Vaught Test (slides 12).

Corollary

ACF is model complete and ACF_p is complete for $p = 0$ or prime.

Proof.

Let $\mathcal{A}, \mathcal{B} \models \mathsf{ACF}_p$, let ϕ be a sentence in the language of rings.
We have a quantifier-free sentence ψ such that $\mathsf{ACF}_p \models \phi \leftrightarrow \psi$.
Since ψ is preserved by substructures and extensions,

$$\mathcal{A} \models \phi \quad \text{iff} \quad \mathcal{A} \models \psi \quad \text{iff} \quad \mathcal{F}_p \models \psi \quad \text{iff} \quad \mathcal{B} \models \psi \quad \text{iff} \quad \mathcal{B} \models \phi,$$

where $\mathcal{F}_p$ is the field of size p if $p > 0$; else $\mathbb{Q}$.
Thus $\mathcal{A} \equiv \mathcal{B}$ and ACF_p is complete. □