A topological approach to undefinability in algebraic extensions of the rationals

Linda Westrick

Penn State University

UW-Madison Logic Seminar

Joint with Kirsten Eisenträger, Russell Miller & Caleb Springer

December 15, 2021
Outline

1. Preliminaries
2. Bird’s eye view
3. Normal form theorem
4. Things happen for a reason
In pursuit of a definition of \( \mathbb{Z} \)

Let \( \overline{\mathbb{Q}} \) be the algebraic closure of \( \mathbb{Q} \).

For fields \( L \subseteq \overline{\mathbb{Q}} \), we are interested in what subsets of \( L \) are first-order definable in the structure \((L; 0, 1, +, \cdot)\).

**Example.** If \( \mathbb{Z} \) were existentially definable in \( \mathbb{Q} \), Hilbert’s Tenth Problem over \( \mathbb{Q} \) would be resolved, but this problem is too hard.

**Question 1:** In which fields \( L \subseteq \overline{\mathbb{Q}} \) is \( \mathbb{Z} \) existentially definable?

**Definition:** The *algebraic integers* \( \mathcal{O}_L \) of \( L \) are exactly those \( z \in L \) which are a root of a *monic* polynomial in \( \mathbb{Z}[X] \).

(But for this talk we only need the fact that \( \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z} \))

**Question 2:** In which fields \( L \subseteq \overline{\mathbb{Q}} \) is \( \mathcal{O}_L \) existentially definable?
A topology on subfields of $\overline{\mathbb{Q}}$

Define $\text{Sub}(\overline{\mathbb{Q}}) = \{ L \subseteq \overline{\mathbb{Q}} : L \text{ is a field} \}$.

Topology: declare that for each $a \in \overline{\mathbb{Q}}$, $\{ L : a \in L \}$ is clopen.

(Equivalently, identifying $L \in \text{Sub}(\overline{\mathbb{Q}})$ with its characteristic function, $\text{Sub}(\overline{\mathbb{Q}}) \subseteq \{0, 1\}^\overline{\mathbb{Q}}$ inherits the product topology.)

A basis: for every pair of finite sets $A, B \subseteq \overline{\mathbb{Q}}$, define

$$U_{A,B} = \{ L \in \text{Sub}(\overline{\mathbb{Q}}) : A \subseteq L \text{ and } L \cap B = \emptyset \}$$

Fact: $\text{Sub}(\overline{\mathbb{Q}})$ is homeomorphic to Cantor space $\{0, 1\}^\mathbb{N}$. 
Baire Category

A subset $S$ of a topological space $X$ is nowhere dense if for every non-empty open $U$, there is a non-empty open $V \subseteq U$ such that $V \cap S = \emptyset$.

A meager set is a countable union of nowhere dense sets.

Meager sets are closed under countable unions.

By the Baire Category Theorem, Cantor space is not meager. Thus, neither is $\text{Sub}(\mathbb{Q})$. 
A simple normal form for existential formulas

Given any existential formula $\alpha(X)$ in the language of rings:

- Express in disjunctive normal form

  $$\alpha(X) \equiv \exists \vec{Y}[\alpha_1(X, \vec{Y}) \lor \cdots \lor \alpha_r(X, \vec{Y})]$$

  where each $\alpha_j$ is a conjunction of equations and inequations,

  $$\alpha_j \equiv (f_1 = 0) \land \cdots \land (f_n = 0) \land (g_1 \neq 0) \land \cdots \land (g_k \neq 0)$$

- Distribute $\exists$ over $\lor$:

  $$\alpha \equiv (\exists \vec{Y} \alpha_1) \lor \cdots \lor (\exists \vec{Y} \alpha_r)$$

- Combine inequations, so that each $\alpha_i$ takes the form

  $$\alpha_i \equiv f_1 = \cdots = f_k = 0 \neq g$$
A simple normal form for existential formulas, cont’d

- Remove unused variables (so different clauses may have different lengths of $\vec{Y}$.)
- Thus $\alpha$ can always be rewritten as a finite disjunction

$$\alpha \equiv \bigvee_{i<r} \beta_i$$

where each $\beta_i$ takes the form

$$\beta_i \equiv \exists \vec{Y}(f_1 = \cdots = f_k = 0 \neq g)$$

(or, with all variables shown,

$$\beta_i(X) = \exists \vec{Y}[f_1(X, \vec{Y}) = \cdots = f_k(X, \vec{Y}) = 0 \neq g(X, \vec{Y})]$$)
1. Preliminaries
2. *Bird’s eye view*
3. Normal form theorem
4. Things happen for a reason
Main theorem

Let \( S = \{ L \in \text{Sub}(\mathbb{Q}) : \text{for some } A \subseteq L, \) 
\[ A \text{ is one-quantifier definable in } L \text{ and } A \cap \mathbb{Q} = \mathbb{Z} \}\}

**Main Theorem:** \( S \) is meager.

This includes any \( L \) for which:
- \( \mathcal{O}_L \) is existentially or universally definable in \( L \)
- \( \mathbb{Z} \) is existentially or universally definable in \( L \)
Normal form for existential definitions

A polynomial $p \in \overline{\mathbb{Q}}[X, \vec{Y}]$ is called *absolutely irreducible* if it is irreducible over $\overline{\mathbb{Q}}$.

**Theorem:** (Normal Form Theorem for existential definitions) Let $L \in \text{Sub}(\overline{\mathbb{Q}})$ and suppose that $A \subseteq L$ is existentially definable in $L$. Then $A$ has an existential definition in $L$ of the form

$$\alpha(X) = \bigvee_{i < r} \beta_i(X)$$

where each $\beta_i(X)$ has one of the following forms:

(i) The quantifier-free formula $X = z_0$ for a fixed $z_0 \in L$.

(ii) $\exists \vec{Y}[f = 0 \neq g]$, where $f, g \in L[X, \vec{Y}]$ and $f$ is absolutely irreducible.
Hilbert’s Irreducibility Theorem

A number field is any field of the form $\mathbb{Q}(A)$ where $A \subseteq \overline{\mathbb{Q}}$ is finite.

If $K$ is a number field, there is a notion of smallness for subsets $T \subseteq K^n$ called thinness which is due to Serre.

**Facts:** For any number field $K$,

- Neither $\mathbb{Z}$ nor $\mathbb{Q} \setminus \mathbb{Z}$ is thin in $K$.
- Neither $\mathbb{Z} \times \mathbb{Q}^{n-1}$ nor $(\mathbb{Q} \setminus \mathbb{Z}) \times \mathbb{Q}^{n-1}$ is thin in $K^n$.

**Theorem.** (Hilbert’s Irreducibility Theorem) Suppose $K$ is a number field and $f \in K[Y_0, \ldots, Y_m]$ is irreducible over $K$. Then there is a thin set $T \subseteq K^m$ such that for all $y_0, \ldots, y_{m-1} \not\in T$, $f(y_0, \ldots, y_{m-1}, Y_m)$ remains irreducible over $K$. 
Proof of a special case of the main theorem

Claim: \( \{ L \in \text{Sub}(\mathbb{Q}) : Z \text{ is existentially definable in } L \} \) is meager.

For each formula \( \alpha(X) \) in normal form, let

\[ S_\alpha = \{ L : \alpha \text{ defines } \mathbb{Z} \text{ in } L \} \]

Suffices to show: Each \( S_\alpha \) is nowhere dense.

Given nonempty \( U_{A,B} \), we seek \( z \in \overline{\mathbb{Q}} \) such that

\[ U_{A \cup \{z\},B} \neq \emptyset \text{ and } U_{A \cup \{z\},B} \cap S_\alpha = \emptyset. \]

(Easy if all disjuncts are \( X = z_0 \), ignore that case)

Fix a disjunct \( \beta(X) = \exists Y_1, \ldots, Y_m[f(X, \vec{Y}) = 0 \neq g(X, \vec{Y})] \).

We will add \( z \) to “mess up” \( \beta \) by making sure \( \beta(x) \) holds for some \( x \in \mathbb{Q} \setminus \mathbb{Z} \).
What could go wrong?

Work in $U_{\emptyset,\{\sqrt{2}\}}$ (fields that do not contain $\sqrt{2}$). Consider

$$\beta(X) = \exists Y [2X^2 - Y^2 = 0]$$

**Task:** Find $x \in \mathbb{Q} \setminus \mathbb{Z}$ and $y \in \overline{\mathbb{Q}}$ which satisfy $\beta$ and with $\sqrt{2} \notin \mathbb{Q}(y)$.

**Impossible,** because $\left(\frac{Y}{X}\right)^2 = 2$. (Things failed for a reason.)

Note: $f = 2X^2 - Y^2$ is irreducible in all fields which avoid $\sqrt{2}$. But $f$ is not absolutely irreducible: $(\sqrt{2}X - Y)(\sqrt{2}X + Y)$. 

Proof of a special case of the main theorem, II

Working inside $U_{A, B}$, given $\beta(X) = \exists Y_1, \ldots, Y_m[f(X, \bar{Y}) = 0]$

(Ignoring $g$ now for simplicity.)

- Let $K = \mathbb{Q}(A \cup B)$. Then $f$ remains irreducible over $K$
  (because $f$ was absolutely irreducible).
- By Hilbert Irreducibility Thm, for all $x, y_1, \ldots, y_{m-1}$ outside a
  thin set, $f(x, y_1, \ldots, y_{m-1}, Y_m)$ remains irreducible over $K$.
- But $\mathbb{Q} \setminus \mathbb{Z} \times \mathbb{Q}^{m-1}$ is not thin, so fix $x, y_1, \ldots, y_{m-1}$ from it.
- Lemma: since $f(x, y_1, \ldots, y_{m-1}, Y_m)$ has coefficients from
  $\mathbb{Q}(A)$ but is irreducible over $\mathbb{Q}(A \cup B)$, for any root $z$ of $f$,
  $\mathbb{Q}(A \cup \{z\})$ is disjoint from $B$.

Thus we have $x \in \mathbb{Q} \setminus \mathbb{Z}$, but $\beta(x)$ holds for all $L$ containing
$A \cup \{z\}$. So $\alpha$ does not define $\mathbb{Z}$ in any $L \in U_{A \cup \{z\}, B}$. 
Computable fields with one-quantifier undefinable integers

**Theorem:** Computable fields in which $\mathbb{Z}$ is not existentially definable are dense in $\text{Sub}(\overline{\mathbb{Q}})$.

The following operations are computable:
- Is a polynomial $f$ absolutely irreducible?
- Is a given $U_{A,B}$ empty?

The first point allows us to list all formulas $\beta$ we need to defeat. Every $\beta$ is defeatable.

The second point allows us to know when we have defeated a given $\beta$: Search $x, y_1, \ldots, y_{m-1}, z$ until finding a root with $x \in \mathbb{Q} \setminus \mathbb{Z}$ and $U_{A \cup \{z\}, B} \neq \emptyset$.

Perhaps some nicer field which has “enough” roots could defeat all $\beta$ naturally, but we do not have a specific example.
Outline

1. Preliminaries
2. Bird’s eye view
3. Normal form theorem
4. Things happen for a reason
Normal form for existential definitions

**Theorem:** (Normal Form Theorem for existential definitions) Let $L \in \text{Sub}(\mathbb{Q})$ and suppose that $A \subseteq L$ is existentially definable in $L$.

Let $\alpha(X) = \bigvee_{i<r} \beta_i(X)$ be “simplest” among all existential $L$-formulas which define $A$ in $L$.

Then each $\beta_i(X)$ has one of the following forms:

(i) The quantifier-free formula $X = z_0$ for a fixed $z_0 \in L$.

(ii) $\exists \vec{Y}[f = 0 \neq g]$, where $f, g \in L[X, \vec{Y}]$ and $f$ is absolutely irreducible.
Well-orderings

A linear order \((L, <)\) is a well-order if it has no infinite descending sequence \(x_1 > x_2 > \ldots\)

**Example:** Define the *multidegree* of a term \(X^{d_0} Y_1^{d_1} \ldots Y_m^{d_m}\) to be the tuple \((d_0, \ldots, d_m)\). Order the multidegrees in reverse lexicographical order. This is a well-order.

**Definition:** The *multidegree* of a polynomial \(f \in \mathbb{Q}[X, \vec{Y}]\) is the maximum of the multidegrees of its terms.
Well-ordering multisets

**Definition:** Given a linear order \((L, <)\), define its *multiset order* \((L^*, <^*)\) as follows.

- \(L^*\) is the set of finite multisets with elements from \(L\).
- If \(C, D \in L^*\), we define \(C <^* D\) if
  - \(C\) is empty and \(D\) is not, or
  - \(\max C < \max D\), or
  - \(\max C = \max D\) and \(C' <^* D'\), where \(C'\) and \(D'\) are obtained by removing one maximum element from each.

**Lemma:** If \((L, <)\) is well-ordered, so is its multiset order.

**Definition:** Define the *multidegree* of a set of polynomials \(\{f_1, \ldots, f_k\}\) to be the multiset of multidegrees of these polynomials, ordered by the multiset order. This is a well-order.
Dimension of a variety

To any system of equations and inequations

\[ f_1(X, Y_1, \ldots, Y_m) = \cdots = f_k(X, \vec{Y}) = 0 \]
\[ g_1(X, \vec{Y})g_2(X, \vec{Y}) \cdots g_r(X, \vec{Y}) \neq 0 \]

we may associate a notion of dimension which is a natural number related to the size of the solution set.

(Take Spec(\(\mathbb{C}[X, \vec{Y}]\)) with the Zariski topology. The Krull dimension of \(W \subseteq Spec(\mathbb{C}[X, \vec{Y}])\) is the supremal length \(r\) of a chain of irreducible closed subsets \(Z_0 \subsetneq Z_1 \subsetneq \cdots \subsetneq Z_r \subseteq W\). Use \(W = V((f_1, \ldots, f_k)) \cap D(g)\).

**Example:** The dimension of the sphere \(X^2 + Y_1^2 + Y_2^2 = 1\) is 2.

**Facts:** Starting from a system as above,

- Additional equations/inequations don’t increase the dimension
- Additional *non-redundant equations* strictly decrease the dimension
Rank of a basic existential formula

**Definition** A *basic rankable formula* $\beta(X)$ is a formula of the form

$$\beta = \exists \vec{Y}[f_1 = \cdots = f_k = 0 \neq g], \text{ where } f_1, \ldots, f_k, g \in \overline{\mathbb{Q}}[X, \vec{Y}].$$

**Definition** The *rank* of a basic rankable formula as above is a triple $(m, d, M)$, where

- $m$ is the number of $Y$-variables
- $d$ is the dimension of $f_1 = \cdots = f_k = 0 \neq g$
- $M$ is the multidegree of $\{f_1, \ldots, f_k\}$

and we order the ranks in lexicographic order. This is a well-order.

Thus $\beta_1$ has smaller rank than $\beta_2$ if either

- $\beta_1$ uses fewer $Y$’s, or
- $m_1 = m_2$ and $\beta_1$ has the smaller dimension, or
- $m_1 = m_2$ and $d_1 = d_2$, but $\beta_1$ uses smaller equations, as measured by the multidegree of the set of equations.
Recall: Every existential formula $\alpha(X)$ can be expressed as a finite disjunction of basic rankable formulas $\alpha(X) = \bigvee_{i < r} \beta_i(X)$.

Definition: The rank of an existential formula $\alpha$ as above is the multiset of ranks of its $\beta_i$, and we order the ranks using the multiset order. This is a well-order.
Normal form for existential definitions

**Theorem:** (Normal Form Theorem for existential definitions) Let \( L \in \text{Sub}(\mathcal{Q}) \) and suppose that \( A \subseteq L \) is existentially definable in \( L \).

Let \( \alpha(X) = \bigvee_{i < r} \beta_i(X) \) have minimal rank among all existential \( L \)-formulas which define \( A \) in \( L \).

Then each \( \beta_i(X) \) has one of the following forms:

(i) The quantifier-free formula \( X = z_0 \) for a fixed \( z_0 \in L \).

(ii) \( \exists \vec{Y}[f = 0 \neq g] \), where \( f, g \in L[X, \vec{Y}] \) and \( f \) is absolutely irreducible.

**Idea:** If some \( \beta_i \) does not take one of these forms, we can find a disjunction of basic rankable formulas which define the same subset of \( L \) as \( \beta_i \), but all have lower rank than \( \beta_i \). Replacing \( \beta_i \) by this disjunction produces a formula of lower rank than \( \alpha \).
Example: Why should $\beta_i$ contain only irreducible $f$?

Let $L \in \text{Sub}(\mathbb{Q})$.

Suppose an existential formula $\alpha$ contains a disjunct $\beta$

$$\beta(X) = \exists \vec{Y}[f = 0 \neq g]$$

and $f$ is reducible in $L$. Say $f = pq$.

Then in $L$, $\beta(X)$ defines the same set as:

$$\exists \vec{Y}[p = 0 \neq g] \lor \exists \vec{Y}[q = 0 \neq g]$$

But both disjuncts above have a lower rank than $\beta$:

- same number of $Y$’s
- dimension did not increase
- multidegree of polynomials reduced

Thus the overall multirank is reduced.
Outline

1. Preliminaries
2. Bird’s eye view
3. Normal form theorem
4. Things happen for a reason
An example which fails

Work in $U_{\emptyset, \{\sqrt{2}\}}$ (fields that do not contain $\sqrt{2}$). Consider

$$\beta(X) = \exists Y [2X^2 - Y^2 = 0]$$

**Task:** Find $x \in \mathbb{Q} \setminus \mathbb{Z}$ and $y \in \overline{\mathbb{Q}}$ which satisfy $\beta$ and with $\sqrt{2} \notin \mathbb{Q}(y)$.

**Impossible**, because $\left( \frac{Y}{X} \right)^2 = 2$. (Things failed for a reason.)

Note: $f = 2X^2 - Y^2$ is irreducible in all fields which avoid $\sqrt{2}$. But $f$ is not absolutely irreducible: $(\sqrt{2}X - Y)(\sqrt{2}X + Y)$. 
Things happen for a reason

**Lemma.** Suppose \( f \in F[X, \tilde{Y}] \) and \( f \) is irreducible over \( F \).

Let \( E = \text{Frac} \left( \frac{F[X, \tilde{Y}]}{(f)} \right) := \left\{ \frac{p + (f)}{q + (f)} : p, q \in F[X, \tilde{Y}] \right\} \).

If \( K \) is a finite Galois extension of \( F \) and \( f \) is reducible over \( K \), then there is \( z \in E \) which is “in” \( K \setminus F \)

- (Experts: there is an \( F \)-linear field embedding \( \phi : F(z) \to K \) with \( \phi(z) \in K \setminus F \))
- There is a rational formula \( \frac{p}{q} \) such that for any \( x, \bar{y} \in \overline{Q} \), if \( f(x, \bar{y}) = 0 \) and \( q(x, \bar{y}) \neq 0 \), then

\[
\frac{p(x, \bar{y})}{q(x, \bar{y})} \in K \setminus F.
\]
Absolute irreducibility in the normal form

Fix $L$. Suppose $\beta(X) = \exists \vec{Y}[f = 0]$ and $f$ is irreducible over $L$ but not absolutely irreducible. We will replace $\beta$ with finitely many lower-ranked formulas.

Let $K$ be a finite normal extension of $\mathbb{Q}$ which contains all coefficients of all absolutely irreducible factors of $f$ over $\mathbb{Q}$.

Let $F = L \cap K$. By Lemma, there is $z = \frac{p+(f)}{q+(f)}$ “in” $K \setminus F$.

For all $x, \bar{y} \in L$, $f(x, \bar{y}) = 0 \implies q(x, \bar{y}) = 0$.

(and we can assume $q$ has smaller $Y_m$-degree than $f$)

Apply the Euclidean algorithm: $cf = dq + r$

Then in $L$, $\beta(X)$ is equivalent to

$$\exists \vec{Y}[q = r = 0 \neq c] \lor \exists \vec{Y}[f = c = 0]$$
References