A topological approach to undefinability in algebraic extensions of the rationals

Joint work with Russell Miller, Caleb Springer and Linda Westrick

$$\begin{array}{ccc} & & \overline{\mathbb{Q}} \\ & & | \\ \mathcal{O}_L & \subseteq & L \\ | & & | \\ \mathbb{Z} & \subseteq & \mathbb{Q} \end{array}$$

Main Question:

When is $\mathcal{O}_L$ $\exists$-definable in L?

$\mathcal{O}_L$ = "ring of integers" = subring of L

"Base Case": $L = \mathbb{Q}$

$\mathcal{O}_L = \mathbb{Z}$

Is $\mathbb{Z}$ $\exists$-definable in $\mathbb{Q}$?

Why the question?

If $\mathbb{Z}$ is $\exists$-definable in $\mathbb{Q}$, then Hilbert's Tenth Problem for $\mathbb{Q}$ is undecidable.

Question is too difficult!

Will show instead:

$$S = \{L \subseteq \overline{\mathbb{Q}} : \mathcal{O}_L \text{ is } \exists\text{-definable in } L\}$$

is "small".

$\hookrightarrow$ Introduce a topology on set of alg. extensions of $\mathbb{Q}$. Show that S is meager.

Hilbert's Tenth Problem (H 10)

$H10/\mathbb{Z}$: Find an algorithm that decides, given a multivariate polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in $\mathbb{Z}$, whether there is a solution with $x_1, \ldots, x_n$ in $\mathbb{Z}$.

1970: Matiyasevich, based on Davis-Putnam-Robinson showed: No such algorithm exists.

H10 (over $\mathbb{Z}$) is undecidable.

How about the same problem over the rationals?

$H10/\mathbb{Q}$: Find an algorithm that decides, given a multivariate polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in $\mathbb{Q}$ whether there is a solution with $x_1, \ldots, x_n$ in $\mathbb{Q}$.

$H10/\mathbb{Q}$ is still open!

One possible way to resolve $H10/\mathbb{Q}$.

Use the following

Lemma: If $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$ then $H10/\mathbb{Q}$ is undecidable.

Proof of lemma is by reduction:

If we had an algorithm for $H10/\mathbb{Q}$, then – using the (pos.) existential definition of $\mathbb{Z}$ in $\mathbb{Q}$ – we would obtain an al orithm for $H10/\mathbb{Z}$ as follows, giving us a contradiction.

So is $\mathbb{Z}$ $\exists$-definable in $\mathbb{Q}$?

If Mazur's Conjecture holds the answer is no.

Setup:

- $\overline{\mathbb{Q}}$ = algebraic closure of $\mathbb{Q}$

Definition: Given a field $L \subseteq \overline{\mathbb{Q}}$,

$\mathcal{O}_L$ = elements of L that are roots of monic polynomials with coefficients in $\mathbb{Z}[X]$.

Example: $L = \mathbb{Q}(\sqrt{3})$

$\mathcal{O}_L = \mathbb{Z}[\sqrt{3}]$

$$\begin{tikzcd} \mathcal{O}_L \arrow[r, phantom, "\subseteq"] \arrow[d, dash] & L \arrow[d, dash] \\ \mathbb{Z} \arrow[r, phantom, "\subseteq"] & \mathbb{Q} \end{tikzcd}$$

Main Fact we need: For any $L \subseteq \overline{\mathbb{Q}}$,

$$\mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}.$$

Question: In which fields $L \subseteq \overline{\mathbb{Q}}$ is $\mathcal{O}_L$ existentially definable?

- Too difficult for specific L. Already the "base case" $L = \mathbb{Z}$ is one of the biggest problem in the area.
- Instead: use topological point of view.

Will show: $\{L \subseteq \overline{\mathbb{Q}} : \mathcal{O}_L \text{ existentially definable in } L\}$ is "small" in topological sense.

What definability results are known?

(1) When K is a finite extension of $\mathbb{Q}$:

(In this $K = \mathbb{Q}(\alpha)$ with α algebraic over $\mathbb{Q}$. We call K a number field.)

- $\mathcal{O}_K$ is first-order definable in K (Julia Robinson, 1959)
- $\mathcal{O}_K$ is $\forall$-definable in K (Koenigsmann, Park)

(2) When K is an infinite extension of $\mathbb{Q}$:

Very little is known.

Only know $\mathcal{O}_K$ is first-order definable in K for very special K

(e.g. $K = \mathbb{Q}(\zeta_{p^n} : n \geq 1)$

p^n-th root of unity

(Fukuzaki, Shlapentokh, Videla)

How about undefinability results?

We know even less.

$\mathbb{Z}^{tr}$ not definable in $\mathbb{Q}^{tr}$.

totally real integers

A topology on the subfields of $\overline{\mathbb{Q}}$

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

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

Basis for this topology:

For any pair A, B of finite subsets of $\overline{\mathbb{Q}}$, consider

$$\mathcal{U}_{A,B} \overset{def}{:=} \{L \in Sub(\overline{\mathbb{Q}}) : A \subseteq L \text{ and } L \cap B = \emptyset\}$$

The $\mathcal{U}_{A,B}$ form a basis of the topology.

Let $S := \{L \subseteq \overline{\mathbb{Q}} : \mathcal{O}_L \text{ is existentially definable in } L\}$

We will show that S is "small" by showing it is a meager set.

Definitions: A subset S of a topological space is nowhere dense if for every non-empty open $\mathcal{U}$, there exists non-empty open $V \subseteq U$ with $V \cap S = \emptyset$

A subset S is called meager if it is a countable union of nowhere dense sets.

Can show: $\mathrm{Sub}(\overline{\mathbb{Q}})$ is homeomorphic to Cantor space $\{0,1\}^{\mathbb{N}}$.

This implies: Every non-empty open set in $\mathrm{Sub}(\overline{\mathbb{Q}})$ is non-meager.

So it makes sense to think of meager subsets of $\mathrm{Sub}(\overline{\mathbb{Q}})$ as small.

MAIN THEOREM (E-Miller-Springer-Westrick)

$\{L \in \mathrm{Sub}(\overline{\mathbb{Q}}) : \mathcal{O}_L$ is existentially or universally definable$\}$ is a meager set.

[Can state a more general version by introducing the notion of a thin set.]

To illustrate the main ideas for the proof: consider special case.

Main Theorem (special case):

$$\{L \subseteq \mathrm{Sub}(\overline{\mathbb{Q}}) : \mathcal{O}_L \text{ is } \exists\text{-definable in } L\}$$

is meager.

PROOF relies on two main ingredients:

① **Proposition:**

Let $f, g \in \mathbb{Q}[X, Y_1, \dots, Y_m]$ be such that f is irreducible over $\overline{\mathbb{Q}}$ and does not divide g. Let

$$\beta(X) = \exists Y_1, \dots, Y_m \left[f(X, Y_1, \dots, Y_m) = 0 \neq g(X, Y_1, \dots, Y_m) \right]$$

Then

$$S_\beta := \left\{ L \subseteq \overline{\mathbb{Q}} : \quad \{x \in \mathbb{Q} : \beta(x) \text{ holds in } L\} \subseteq \mathbb{Z} \right\}$$

is nowhere dense.

② Normal Form Theorem for existential definitions

Let $L \in \mathrm{Sub}(\overline{\mathbb{Q}})$ with $\mathcal{O}_L$ $\exists$-definable in L.

Then $\mathcal{O}_L$ can be defined by a formula of the form

$$\alpha(X) = \bigvee_{i=1}^{r} \beta_i(X) \quad \text{with each } \beta_i$$

having one of two possible forms:

(i) $X = z_0$ for a fixed $z_0 \in L$

(ii) $\exists Y_1, \dots, Y_m$
$f(X, Y_1, \dots, Y_m) = 0 \neq g(X, Y_1, \dots, Y_m)$
with $f, g \in \mathbb{Q}[X, Y_1, \dots, Y_m]$,
f irreducible over $\overline{\mathbb{Q}}$ and not dividing g.

Sketch of proof of Main Theorem using ① and ②:

Let $S := \{L \in \mathrm{Sub}(\overline{\mathbb{Q}}) : \mathcal{O}_L \ \exists\text{-definable in } L\}$.

Consider $\bigcup_{\beta} S_\beta$ where the union is taken over all β as in (1).

That is,

$$S_\beta = \{L \subseteq \overline{\mathbb{Q}} : \{x \in \mathbb{Q} : \beta(x) \text{ holds in } L\} \subseteq \mathbb{Z}\}$$

with

$$\beta(X) = \exists Y_1, \dots, Y_m \left[f(X, Y_1, \dots, Y_m) = 0 \neq g(X, Y_1, \dots, Y_m) \right]$$

<u>Claim</u>: $S \subseteq \bigcup_\beta S_\beta$

If we can prove the claim, then the theorem will follow, because by (1) we will get that S is contained in a countable union of nowhere dense sets, which is meager.

<u>Proof of claim</u>: Assume by contradiction that $L \in \mathrm{Sub}(\overline{\mathbb{Q}})$ with $\mathcal{O}_L$ $\exists$-definable in L, but $L \notin \bigcup_\beta S_\beta$.

By (2), can find $\alpha(X) = \bigvee_{i=1}^{r} \beta_i(X)$ with β_i as in (2). Since $\mathcal{O}_L$ is infinite at least one of the β_i's must be of the form $f(X, \vec{Y}) = 0 \neq g(X, \vec{Y})$.

We had assumed that $L \notin \bigcup_{\beta} S_{\beta}$, so in particular $L \notin S_{\beta_i}$ for this β_i.

Recall:

$$S_{\beta_i} \overset{\text{def}}{=} \left\{ L \in \overline{\mathbb{Q}} : \quad \{ x \in \mathbb{Q} : \beta_i(x) \text{ holds in } L \} \subseteq \mathbb{Z} \right\}$$

So $L \notin S_{\beta_i}$ means there exists $x \in \mathbb{Q} - \mathbb{Z}$ s.t. $\beta_i(x)$ and hence also $\alpha(x)$ holds in L. $\alpha(X)$ defines $\mathcal{O}_L$ in L by assumption, and $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$.

This gives a contradiction. $\square$

We can generalize Main Theorem:

1. Can prove the same theorem for $\mathrm{Sub}(\overline{\mathbb{Q}})/\cong$.

2. Our proof of the main theorem shows something stronger:

   Theorem: Suppose A is any infinite subset of L with A $\exists$-definable in L. If $A \cap \mathbb{Q} \subseteq \mathbb{Z}$, then A lies in

   $$\bigcup_{\beta} S_\beta .$$

   (Have analogous statement for $\forall$-definable sets.)

- After seeing L. Westrick's talk at MSRI: Dittmann–Fehm showed through alternate methods that $\{L \in \mathrm{Sub}(\overline{\mathbb{Q}}) : \mathcal{O}_L \text{ first-order definable in } L\}$ is meager in $\mathrm{Sub}(\overline{\mathbb{Q}})$.