Undecidability and undefinability in algebraic extensions of the rationals

Kirsten Eisenträger

Penn State

Motivating Question

Let L be a field with

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

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

- $\mathcal{O}_L$ = ring of integers of L, which is subring of L
- Ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$

"Base Case": $L = \mathbb{Q}$. Is $\mathbb{Z}$ $\exists$-definable in $\mathbb{Q}$?

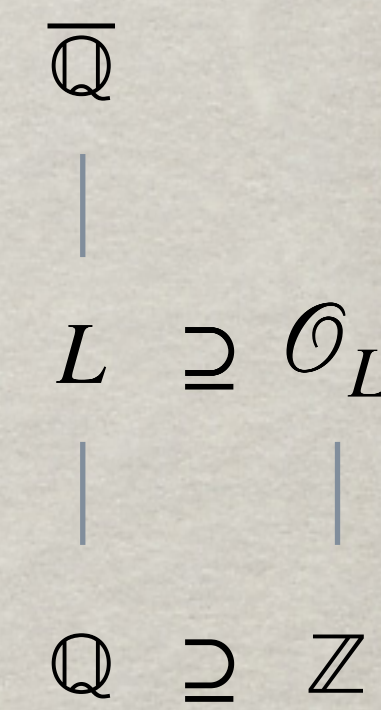
Question is of interest because it is connected to Hilbert's Tenth Problem

This question is already too difficult!

Alternate Question

If the "base case" is already too difficult, what can we show instead?

Theorem (E-Miller-Springer-Westrick):
$S := \{L \subseteq \overline{\mathbb{Q}} : \mathcal{O}_L$ is $\exists$-definable in $L\}$ is "small".



Goal: Introduce topology on set of algebraic extensions of $\mathbb{Q}$ and show that S is meager in that topology.

Hilbert's Tenth Problem

Original Problem: Posed by Hilbert in 1900.

Hilbert's Tenth Problem over $\mathbb{Z}$:

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

- Matiyasevich (1970): No such algorithm exists.
- Matiyasevich's proof was based on work by Davis, Putnam, and Robinson.
- We say that Hilbert's Tenth Problem is undecidable.

Equivalent Problems

- Find an algorithm that decides whether a system of equations as above has integer solutions.

  Equivalent since $f_1 = f_2 = 0 \iff f_1^2 + f_2^2 = 0.$

- Find an algorithm to decide the truth of positive existential sentences.

Hilbert's Tenth Problem (H10) over $\mathbb{Q}$

Can consider analogous problem for $\mathbb{Q}$:

Find an algorithm that decides, given a multivariate polynomial equation with coefficients in $\mathbb{Q}$, whether it has a solution in $\mathbb{Q}$.

This problem is still open!

One possible way to resolve H10 for $\mathbb{Q}$:

Use the following lemma:

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

Existentially defining $\mathbb{Z}$

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

Proof of lemma is by reduction:

Suppose by means of contradiction that $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$ and that there is an algorithm for H10/$\mathbb{Q}$.

Will get contradiction by showing this would give an algorithm for H10/$\mathbb{Z}$:

Given an equation with integer coefficients.

-Algorithm for H10/$\mathbb{Q}$ tells us if there is a rational solution.

-Existential definition of $\mathbb{Z}$ in $\mathbb{Q}$ allows us to force solution to take integer values.

Contradiction since no algorithm for H10/$\mathbb{Z}$ exists!

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

This question is still open.

If Mazur's conjecture holds the answer is no.

Mazur's conjecture: If X is a variety over $\mathbb{Q}$, then the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has only finitely many components.

Defining a topology on algebraic extensions $\mathbb{Q}$

Setup:

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

Definition: Given field $L \subseteq \overline{\mathbb{Q}}$,
ring of integers $\mathcal{O}_L$ = elements in L that are roots of monic polynomial with integer coefficients.

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

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

Main fact we will need: $\mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}$

Want to show:
$S := \{L \subseteq \overline{\mathbb{Q}} : \mathcal{O}_L$ is $\exists$-definable in $L\}$ is small.

FIRST-ORDER DEFINABILITY RESULTS

For K = finite extension of $\mathbb{Q}$ (i.e. K is 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)

For K = infinite extension of $\mathbb{Q}$:

Very little is known.

Know $\mathcal{O}_K$ is first-order definable in K for special fields K (e.g., $K = \mathbb{Q}(\zeta_{p^n})$ with ζ_{p^n}= primitive p^n-th root of unity (Fukuzaki, Shlapentokh, Videla)

Undefinability results

Here we know even less.

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

↑ Totally real integers undecidable (Robinson)

↑ Totally real algebraic numbers decidable (Fried, Haran, Völklein)

$\overline{\mathbb{Z}}$ is not definable in $\overline{\mathbb{Q}}$

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

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

Topology on $\mathrm{Sub}(\overline{\mathbb{Q}})$**:** For each $a \in \overline{\mathbb{Q}}$, $\{L : a \in L\}$ is clopen.

Identify a subset S of $\overline{\mathbb{Q}}$ with its characteristic function.

So can view $\mathrm{Sub}(\overline{\mathbb{Q}})$ as a subset of $2^{\overline{\mathbb{Q}}}$.

Basis for this topology:

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

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

The $U_{A,B}$ form basis for above topology.

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

Will show: S is a meager subset of $\mathrm{Sub}(\overline{\mathbb{Q}})$.

Nowhere dense and meager sets

Definition: A subset S of a topological space is nowhere dense if for every non-empty open U, exists non-empty open $V \subseteq U$ with $V \cap S = \varnothing$.

Definition: A subset S of a topological space is 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 subset of $\mathrm{Sub}(\overline{\mathbb{Q}})$ is non-meager.

Main Theorem

Main Theorem (E-Miller-Springer-Westrick) (Simplified Form)

$\{L \subseteq \overline{\mathbb{Q}} : \mathcal{O}_L$ is $\exists$-definable or $\forall$-definable in $L\}$ is meager.

Can state a more general theorem by introducing the notion of a thin set.

Our proof does not use the ring structure of $\mathcal{O}_L$.

$\exists$-definable ring of integers

Let's specialize further: show that

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

The proof has two main ingredients:

1. **Proposition:** Let $f, g \in \mathbb{Q}[X, Y_1, \ldots, Y_m]$ be such that f is irreducible over $\overline{\mathbb{Q}}$ and does not divide g. Let $\beta(X) = \exists Y_1, \ldots, Y_m[f(X, \overrightarrow{Y} = 0 \neq g(X, \overrightarrow{Y})]$. Then

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

is nowhere dense.

Normal form Theorem for existential definitions

2. **Theorem:** Let $L \subseteq \mathrm{Sub}(\overline{\mathbb{Q}})$ with $\mathcal{O}_L$ $\exists$-definable in L. Then $\mathcal{O}_L$ can be defined by a formula of the form

$$\alpha(X) = \bigvee_{i=1}^{r} \beta_i(x)$$

with each β_i having one of two possible forms:

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

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

Sketch of proof of Main Theorem using 1 and 2

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

Proof: Consider $\bigcup_{\beta} S_\beta$ with β as in 1.

I.e. $\beta(X) = \exists Y_1, \ldots, Y_m\, [f(X, Y_1, \ldots, Y_m) = 0 \neq g(X, Y_1, \ldots, Y_m)]$

Recall $S_\beta = \{L \subseteq \overline{Q} : \{x \in \mathbb{Q} : \beta(x) \text{ holds in } L\} \subseteq \mathbb{Z}\}$ is nowhere dense by 1.

Claim: $S \subseteq \bigcup_{\beta} S_\beta$

Claim implies that S is meager:

By 1. , S_β is nowhere dense. Hence S is contained in a countable union of nowhere dense sets, which is meager.

Last step: prove claim to finish the proof.

Last step: Proof of Claim

Claim: $S \subseteq \bigcup_{\beta} S_{\beta}$

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

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

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

f is irreducible over $\overline{\mathbb{Q}}$ and does not divide g.

Proof by contradiction: assume there exists L with $L \in S$, $L \notin \bigcup_{\beta} S_{\beta}$.

- By 2.: can find $\alpha(X) = \bigvee_{i=1}^{r} \beta_i(X)$ defining $\mathcal{O}_L$ in L

  with each β_i either (i) $X = z_0$ or (ii) $\exists \overrightarrow{Y}\, f(X, \overrightarrow{Y}) = 0 \neq g(X, \overrightarrow{Y})$.

- $\mathcal{O}_L$ is infinite: so at least one β_i must be as in (ii).

-By assumption: $L \notin S_{\beta_i}$.

- This means: $\exists x \in \mathbb{Q} - \mathbb{Z}$ such that $\beta_i(x)$ and hence $\alpha(x)$ holds.

- But $\alpha(x)$ defines $\mathcal{O}_L$ in L, and $\mathbb{Q} \cap \mathcal{O}_L = \mathbb{Z}$, so $\alpha(x)$ does not hold for $x \in \mathbb{Q} - \mathbb{Z}$, contradiction. This finishes proof of main theorem.

Generalizations

1. Can prove Main Theorem with $\mathrm{Sub}(\overline{\mathbb{Q}})$ replaced with $\mathrm{Sub}(\overline{\mathbb{Q}})/\cong$.

2. Proof of Main Theorem shows something stronger:

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

3. Have analogous statement for $\forall$-definable sets.

4. After seeing a talk byWestrick on this topic: Dittmann-Fehm showed, using model theoretic methods, that $\{L \in \mathrm{Sub}(\overline{\mathbb{Q}}) : \mathcal{O}_L$ is first-order definable in $L\}$ is meager in $\mathrm{Sub}(\overline{\mathbb{Q}})$.

Open Question

Can you prove a similar statement in terms of Lebesgue measure?

I.e., can you consider the Lebesgue measure on Cantor space and transfer it to $\mathrm{Sub}(\overline{\mathbb{Q}})/\cong$ via some computable homeomorphism?

Problem: resulting measure is not canonical.

Future Goal: investigate measure theoretic perspective. Want to prove some statement like: set of fields where the ring of integers is existentially definable has measure zero.

Comparison with char $p > 0$

Definability questions for subfields of $\overline{\mathbb{Q}}$: motivated by trying to prove undecidability results.

Theorem (Julia Robinson): Let K be a finite extension of $\mathbb{Q}$. Then $\mathcal{O}_K$ is definable in K and the first-order theory of K is undecidable.

In infinite extensions of $\overline{\mathbb{Q}}$: we know very little

Some people conjecture that there is some "threshold" above which the ring of integer is no longer definable.

Our main theorem shows: non-definability of the ring of integers is the expected outcome.

Analogue in positive characteristic: function fields

Function Fields

k=field of positive characteristic

$k[t]$=polynomial ring in t (t transcendental element)

$k(t)$=fraction field of $k[t]$ = rational function field over k in one variable

Definition: Let K be a finite algebraic extension of $k(t)$. We call K an (algebraic) function field in one variable.

Definition: The constant field of a function field K as above is the algebraic closure of k in K.

Definability Results

Let K = function field of pos. char p, ord_q a discrete valuation on K.

Lemma:

To prove undecidability of existential theory of K:

Suffices to show the following two sets are existentially definable in K:

1. $\text{INT}_q = \{x \in K : \text{ord}_q(x) \geq 0\}$

2. $p(K) = \{(x, y) \in K^2 : \exists s \in \mathbb{Z}_{\geq 0} : y = x^{p^s}\}$.

Can do this when K does not contain the algebraic closure of a finite field (Pheidas, Videla, Shlapentokh, E).

Undecidability for function fields in positive characteristic

Theorem (E-Shlapentokh): The existential theory of a function field of positive char. is undecidable in the language of rings provided that the constant field does not contain the algebraic closure of a finite field.

First-order Theory

For first order theory: to prove undecidability, suffices to show

$$p(K) = \{(x, y) \in K^2 : \exists s \in \mathbb{Z}_{\geq 0} : y = x^{p^s}\} \text{ is definable in } K.$$

This approach was used to prove the following:

Theorem (E-Shlapentokh): The first-order theory of any function field K of characteristic $p > 2$ is undecidable in the language of rings without parameters.

Conclusion

For algebraic extensions of $\mathbb{Q}$, obtaining (un)definability results for individual infinite extensions is very difficult.

Topological approach on $\mathrm{Sub}(\overline{\mathbb{Q}})$ gives a different perspective.

In positive characteristic: situation is much better understood. Only constraint for existential definability is dealing with algebraically closed constant fields.