The World of Definability In Number Theory

according to Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

Montreal Number Theory Seminar,
February 16, 2025

Outline

The Origin, Version 1

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing "yes" or "no" answer to the question "Are there integer solutions?".

This problem became known as Hilbert's Tenth Problem

Origin, Version 2: The first-order theory of $\mathbb{Z}$ in the language of rings is undecidable.

Question

What does it mean?

Origin, Version 2: The first-order theory of $\mathbb{Z}$ in the language of rings is undecidable.

Question

What does it mean?

The language of rings is essentially the language of polynomial equations. A formula in this language can be shown to be equivalent to a conjunction and disjunction of expressions of the form

$$E_1 x_1 \dots E_r x_r P(x_1, \dots, x_r) * 0,$$

where "E_i" is either "$\forall$" or "$\exists$" and "$*$" is either "$=$" or "$\neq$". If all variables are in the range of some quantifier, then the formula is a sentence which is either true or false.

There is no algorithm to decide whether an expression as described above is true with all variables ranging over $\mathbb{Z}$.

Origin, Version 2: The first-order theory of $\mathbb{Z}$ in the language of rings is undecidable, continued.

Question

Who proved it?

Origin, Version 2: The first-order theory of $\mathbb{Z}$ in the language of rings is undecidable, continued.

Question

Who proved it?

- J.B. Rosser, "Extensions of Some Theorems of Gödel and Church", J. Symb Logic, vol. 1, (1936), 87-91.
- Kurt Gödel, "Uber formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I, Monatshefte für Mathematik und Physik 38 (1931), 173-198.
- D. Hilbert and P. Bernays, "Grundlagen der Mathematik", by 1934-39, Springer.
- A. Church, An unsolvable problem of elementary number theory, American Journal of Mathematics 58 (1936), 345-363.

Defining sets in the first order language of rings

Let $\phi(\bar{x}, \bar{y})$ be a formula in the first-order language of rings, where $\bar{x}$ is a vector of length m of free variables and $\bar{y}$ is a vector of variables within the range of some quantifier. Let R be a ring. Then we can define a subset of R in the following manner:

$$A = \{\bar{a} \in R^m | R \models \psi(\bar{a}, \bar{y})\}.$$

Defining sets in the first order language of rings

Let $\phi(\bar{x}, \bar{y})$ be a formula in the first-order language of rings, where $\bar{x}$ is a vector of length m of free variables and $\bar{y}$ is a vector of variables within the range of some quantifier. Let R be a ring. Then we can define a subset of R in the following manner:

$$A = \{\bar{a} \in R^m | R \models \psi(\bar{a}, \bar{y})\}.$$

Proposition

Let $R_1 \subset R_2$ be rings and supposed R_1 is definable over R_2. Then if the first-order theory of R_1 is undecidable, then so is the first-order theory of R_2.

An early inhabitant of the definability world: Julia Robinson

Theorem (1949)

$\mathbb{Z}$ is definable by a first-order formula over $\mathbb{Q}$. Thus the first-order theory of $\mathbb{Q}$ (in the language of rings) is undecidable.

An early inhabitant of the definability world: Julia Robinson

Theorem (1949)

$\mathbb{Z}$ is definable by a first-order formula over $\mathbb{Q}$. Thus the first-order theory of $\mathbb{Q}$ (in the language of rings) is undecidable.

Theorem (1959)

If K is a number field, then $\mathbb{Z}$ is definable over O_K (the ring of integers of K) by a first-order formula (using just one universal quantifier and several existential quantifiers). Thus the first-order theory of O_K (in the language of rings) is undecidable.

An early inhabitant of the definability world: Julia Robinson

Theorem (1949)

$\mathbb{Z}$ is definable by a first-order formula over $\mathbb{Q}$. Thus the first-order theory of $\mathbb{Q}$ (in the language of rings) is undecidable.

Theorem (1959)

If K is a number field, then $\mathbb{Z}$ is definable over O_K (the ring of integers of K) by a first-order formula (using just one universal quantifier and several existential quantifiers). Thus the first-order theory of O_K (in the language of rings) is undecidable.

Remark

That particular definition of the ring of algebraic integers O_K given by Julia Robinson depended on the number field K. It used explicitly the degree of the field and monic irreducible polynomials of the basis elements. Later on she constructed a uniform definition not depending on a particular number field.

Other pioneers and the answer to Hilbert's Question

This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matiyasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine sets. In other words it was shown that $HTP(\mathbb{Z})$, considered as a set of indices of polynomials with roots in $\mathbb{Z}$, is Turing equivalent to the Halting Set.

Diophantine Sets: a Number-Theoretic Definition

For an integral domain R, a subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with coefficients in R such that for any element $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of A over R.

Diophantine Sets: a Number-Theoretic Definition

For an integral domain R, a subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with coefficients in R such that for any element $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of A over R.

Remark

Diophantine sets can also be described as the sets existentially definable in the language of rings or as projections of algebraic sets.

Undecidable and computably (recursively) enumerable sets

Definition

- A subset of $A \subset \mathbb{Z}^m$ is computable (or decidable) if there exists an algorithm to determine its membership.
- A function $f : \mathbb{Z}^m \longrightarrow \mathbb{Z}$ is computable if its graph is computable.
- A subset of $A \subset \mathbb{Z}^m$ is computably enumerable if it can be listed by a computable function given an unlimited amount of time.
- A function defined on a c.e. set is partially computable if there is an algorithm which will compute the value of the function for every element of the domain but might never terminate if given a value outside the domain.
- Given subsets $A \subset \mathbb{Z}^m, B \subset \mathbb{Z}^k$, we say $A \leq_T B$ if using the characteristic function of B as an oracle, we have an algorithm to compute the characteristic function of A.

A classic result from Recursion Theory

Theorem

There are sets which are c.e. but not computable.

Example

Let f_i be an effective listing of all partially computable functions. Then the set

$$H = \{i \in \mathbb{Z}_{>0} | f_i(i) \text{ converges } \}$$

is c.e. but not computable. Every c.e. set is Turing reducible to H.

Undecidable Diophantine Sets

Theorem (MDRP)

Every c.e subset of $\mathbb{Z}_{>0}$ is Diophantine and therefore there are undecidable Diophantine sets over $\mathbb{Z}$.

Undecidable Diophantine Sets

Theorem (MDRP)

Every c.e subset of $\mathbb{Z}_{>0}$ is Diophantine and therefore there are undecidable Diophantine sets over $\mathbb{Z}$.

Corollary

HTP is undecidable or positive exitential theory of $\mathbb{Z}$ is undecidable.

Undecidable Diophantine Sets

Theorem (MDRP)

Every c.e subset of $\mathbb{Z}_{>0}$ is Diophantine and therefore there are undecidable Diophantine sets over $\mathbb{Z}$.

Corollary

HTP is undecidable or positive exitential theory of $\mathbb{Z}$ is undecidable.

Proof.

Let $f(t, \bar{x})$ be a Diophantine definition of an undecidable Diophantine set. If HTP is decidable, then for each $t \in \mathbb{Z}$ we can determine if the polynomial equation $f(t, \bar{x}) = 0$ has solutions in $\mathbb{Z}$. However, this process would also determine whether t is an element of our set, contradicting the fact that the set was undecidable. □

Another Corollary of MDRP

Corollary

Consider an effective listing all polynomials over $\mathbb{Z}$ and let $HTP(\mathbb{Z})$ be the set of indices of polynomials with solutions in $\mathbb{Z}$. Then $HTP(\mathbb{Z}) \equiv_T K$.

Another Corollary of MDRP

Corollary

Consider an effective listing all polynomials over $\mathbb{Z}$ and let HTP($\mathbb{Z}$) be the set of indices of polynomials with solutions in $\mathbb{Z}$. Then HTP($\mathbb{Z}$) $\equiv_T K$.

Proof.

Since HTP($\mathbb{Z}$) is r.e., we have HTP($\mathbb{Z}$) $\leq_T K$, and since K is Diophantine, we have $K \leq_T$ HTP($\mathbb{Z}$). □

Some Properties of Diophantine Sets and Definitions over Subrings (of Algebraic Extensions) of $\mathbb{Q}$

- Intersections and unions of Diophantine sets are Diophantine (unions always, intersection over not algebraically closed fields).

Some Properties of Diophantine Sets and Definitions over Subrings (of Algebraic Extensions) of $\mathbb{Q}$

- Intersections and unions of Diophantine sets are Diophantine (unions always, intersection over not algebraically closed fields).
- One = finitely many (not algebraically closed fields)

Some Properties of Diophantine Sets and Definitions over Subrings (of Algebraic Extensions) of $\mathbb{Q}$

- Intersections and unions of Diophantine sets are Diophantine (unions always, intersection over not algebraically closed fields).
- One = finitely many (not algebraically closed fields)
- The set of non-zero elements is Diophantine (over all integrally closed subrings).

Outline

A General Question

A Question about an Arbitrary Recursive Ring R

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R?

A General Question

A Question about an Arbitrary Recursive Ring R

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R?

The most prominent open question is probably the decidability of HTP for $R = \mathbb{Q}$.

Until recently, there was another prominent open question, where R is equal to the ring of integers of an arbitrary number field. But it is no longer open. :)

Undecidability of HTP over $\mathbb{Q}$ Implies Undecidability of HTP for $\mathbb{Z}$

Indeed, suppose we knew how to determine whether solutions exist over $\mathbb{Z}$. Let $Q(x_1, \ldots, x_k)$ be a polynomial with rational coefficients. Then

$$\exists x_1, \ldots, x_k \in \mathbb{Q} : Q(x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$\exists y_1, \ldots, y_k, z_1, \ldots, z_k \in \mathbb{Z} : Q(\frac{y_1}{z_1}, \ldots, \frac{y_k}{z_k}) = 0 \wedge z_1 \ldots z_k \neq 0.$$

So decidability of HTP over $\mathbb{Z}$ would imply the decidability of HTP over $\mathbb{Q}$.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring containing $\mathbb{Z}$ and such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring containing $\mathbb{Z}$ and such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Proof.

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\begin{cases} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \ldots \\ p(T_l, \bar{X}_l) = 0 \end{cases} \quad [1]$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ iff (1) has solutions in R. Thus if HTP is decidable over R, it is decidable over $\mathbb{Z}$. □

The Plan

So to show that HTP is undecidable over $\mathbb{Q}$ we just need to construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$!!!

Outline

A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

A Nasty Consequence

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

A Conjecture of Barry Mazur

The Conjecture on the Topology of Rational Points

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

A Nasty Consequence

There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Remark

If the conjecture is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$.

Another Plan: Diophantine Models

What is a Diophantine Model of $\mathbb{Z}$?

Let R be a recursive ring whose fraction field is not algebraically closed and let $\phi : \mathbb{Z} \longrightarrow R^k$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of R^k. Then ϕ is called a Diophantine model of $\mathbb{Z}$ over R.

Diophantine Model of $\mathbb{Z}$ Implies Undecidability

If R has a Diophantine model of $\mathbb{Z}$, then R has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of R, we have a contradiction.

Diophantine Model of $\mathbb{Z}$ Implies Undecidability

If R has a Diophantine model of $\mathbb{Z}$, then R has undecidable Diophantine sets. Indeed, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set. Suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of R, we have a contradiction.

$\mathrm{HTP}(R) \equiv_T$ Halting Set

One can also show that if R has a Diophantine model of $\mathbb{Z}$, then $\mathrm{HTP}(R)$ is also Turing equivalent to the Halting Set.

Another Breakthrough Idea

So all we need is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$!!!!

A Theorem of Cornelissen and Zahidi

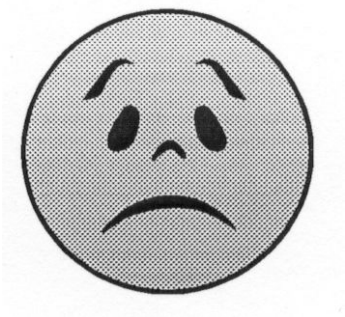
Theorem

If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.

A Theorem of Cornelissen and Zahidi

Theorem

If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.



Outline

The rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

Let $\mathcal{S}$ be a set of prime numbers and let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$:

$$\{x \in \mathbb{Q} | x = \frac{m}{n}, n \neq 0, n \text{ is divisible only by primes in } \mathcal{S}\}$$

The rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

Let $\mathcal{S}$ be a set of prime numbers and let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$:

$$\{x \in \mathbb{Q} | x = \frac{m}{n}, n \neq 0, n \text{ is divisible only by primes in } \mathcal{S}\}$$

Example

$$O_{\mathbb{Q},\{3,5\}} = \left\{ \frac{m}{3^a 5^b}, m \in \mathbb{Z}; a, b \in \mathbb{Z}_{\geq 0} \right\}$$

The rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

Let $\mathcal{S}$ be a set of prime numbers and let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$:

$$\{x \in \mathbb{Q} | x = \frac{m}{n}, n \neq 0, n \text{ is divisible only by primes in } \mathcal{S}\}$$

Example

$$O_{\mathbb{Q},\{3,5\}} = \left\{ \frac{m}{3^a 5^b}, m \in \mathbb{Z}; a, b \in \mathbb{Z}_{\geq 0} \right\}$$

Example

$$O_{\mathbb{Q},\mathcal{P}\setminus\{3,5\}} = \left\{ \frac{m}{n}, m \in \mathbb{Z}; n \not\equiv 0 \mod 3, n \not\equiv 0 \mod 5 \right\},$$

where $\mathcal{P}$ is the set of all prime numbers. If $\mathcal{S}$ contains all the primes, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Q}$. If $\mathcal{S} = \emptyset$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Z}$. If $\mathcal{S}$ is finite, we call the ring small (or the ring of $\mathcal{S}$-integers). If $\mathcal{S}$ is infinite, we call the ring big.

The rings between the ring of algebraic integers and a number field

A Ring in between in a finite algebraic extension of $\mathbb{Q}$

Let $\mathcal{S}$ be a set of primes of a number field K. Let $O_{K,\mathcal{S}}$ be the following subring of K.

$$\{x \in K | \operatorname{ord}_{\mathfrak{p}} x \geq 0, \forall \mathfrak{p} \notin \mathcal{S}\}$$

If $\mathcal{S} = \emptyset$, then $O_{K,\mathcal{S}} = O_K$ – the ring of integers of K.

Definability World: First Glance

$$\mathbb{Q} \overset{\textit{finite}}{\text{———}} O_{\mathbb{Q},\mathcal{V}} \text{———} \ldots \text{———} O_{\mathbb{Q},\mathcal{W}} \text{———} \ldots \text{———} O_{\mathbb{Q},\mathcal{S}} \overset{\textit{finite}}{\text{———}} \mathbb{Z}$$

Defining Integers over Small Subrings of Number Fieds

Theorem (Julia Robinson)

O_K has a Diophantine definition over any small subring of any number field K, including $\mathbb{Q}$.

Defining Integers over Small Subrings of Number Fieds

Theorem (Julia Robinson)

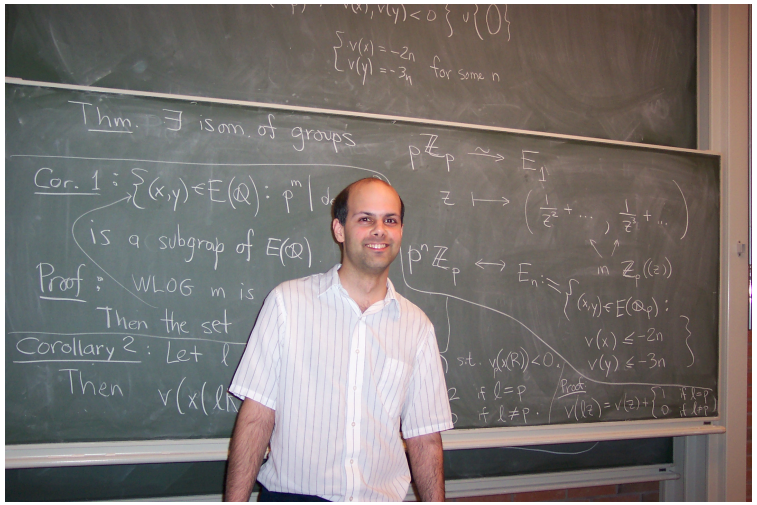
O_K has a Diophantine definition over any small subring of any number field K, including $\mathbb{Q}$.

Corollary

HTP is unsolvable over all small subrings of $\mathbb{Q}$ and is Turing equivalent to the Halting Set.

Outline

Existential Model of $\mathbb{Z}$ over a Very Big Subring



Theorem

There exist recursive sets of primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:

- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

(Poonen, 2003)

Complementary Subrings

Theorem

For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers (i.e. real numbers which can be approximated by a sequence of computable numbers) adding up to 1, the set of primes of $\mathbb{Q}$ may be partitioned into t mutually disjoint recursive subsets $\mathcal{S}_1, \ldots, \mathcal{S}_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that each ring $O_{\mathbb{Q},\mathcal{S}_i}$ has a Diophantine model of $\mathbb{Z}$ and thus has an undecidable HTP Turing equivalent to the Halting Set. (Eisentraeger, Everest 09, Perlega 11, Eisenträger, Everest, S. 11)

Outline

So far

So far, as one can see, all the attempts to resolve the Diophantine status of $\mathbb{Q}$ and the big rings were centered around attempts to prove (sometimes successfully) that these rings (including $\mathbb{Q}$) were like $\mathbb{Z}$ as far as the Turing class of their Diophantine problem is concerned.

So far

So far, as one can see, all the attempts to resolve the Diophantine status of $\mathbb{Q}$ and the big rings were centered around attempts to prove (sometimes successfully) that these rings (including $\mathbb{Q}$) were like $\mathbb{Z}$ as far as the Turing class of their Diophantine problem is concerned. The natural (at least for a computability theorist) question which arises here is whether $\mathrm{HTP}(\mathbb{Q}) \equiv_T \mathrm{HTP}(\mathbb{Z})$ in the case $\mathrm{HTP}(\mathbb{Q})$ is undecidable. In other words, *the Diophantine problem of* $\mathbb{Q}$ *may be undecidable and yet "easier" than the Diophantine problem of* $\mathbb{Z}$, and this would account for the lack of success in attempts to produce the Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ or an algorithm for solving polynomial equations over $\mathbb{Q}$.

What we knew for a long time

Proposition (Julia Robinson)

Let $\mathcal{S}$ contain all but finitely many primes. Then $HTP(O_{\mathbb{Q},\mathcal{S}}) \leq_T HTP(\mathbb{Q})$.

What we knew for a long time

Proposition (Julia Robinson)

Let $\mathcal{S}$ contain all but finitely many primes. Then $HTP(O_{\mathbb{Q},\mathcal{S}}) \leq_T HTP(\mathbb{Q})$.

Proposition

Let R be any big or small ring. Then $HTP(\mathbb{Q}) \leq_T HTP(R)$.

New Results For C. E. Sets

Theorem (Eisenträger, Miller, Park, S.)

There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of c.e. sets of rational primes (with $\mathcal{P}$ denoting the set of all primes) such that

1. $HTP(O_{\mathbb{Q},\mathcal{W}_i}) \equiv_T HTP(\mathbb{Q})$ *for* $i \in \mathbb{Z}_{>0}$,
2. $\mathcal{W}_{i-1} \setminus \mathcal{W}_i$ *has the relative upper density (with respect to* $\mathcal{W}_{i-1}$*) equal to 1 for all* $i \in \mathbb{Z}_{>0}$,
3. *The lower density of* $\mathcal{W}_i$ *is 0, for* $i \in \mathbb{Z}_{>0}$.

New Results For C. E. Sets

Theorem (Eisenträger, Miller, Park, S.)

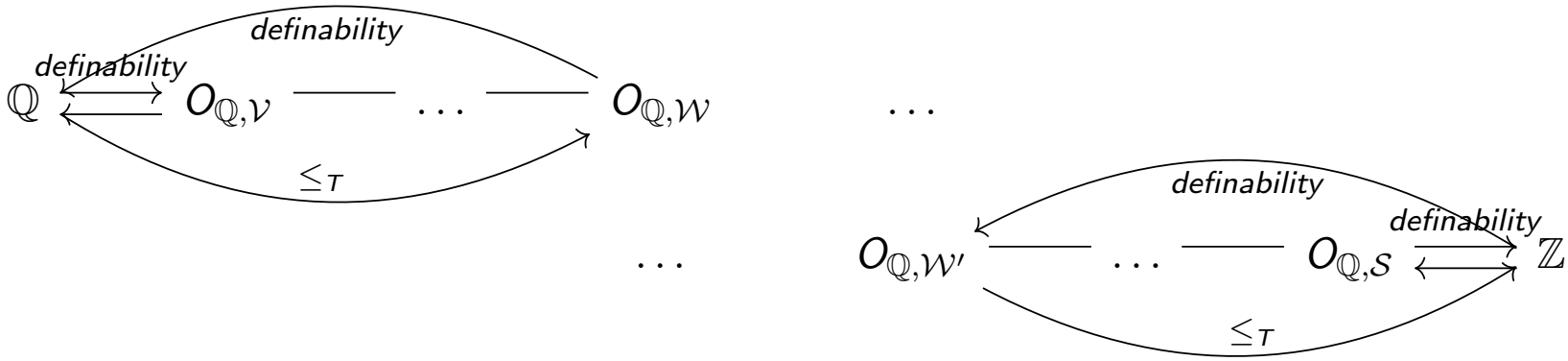
There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of c.e. sets of rational primes (with $\mathcal{P}$ denoting the set of all primes) such that

1. $HTP(O_{\mathbb{Q},\mathcal{W}_i}) \equiv_T HTP(\mathbb{Q})$ *for* $i \in \mathbb{Z}_{>0}$,
2. $\mathcal{W}_{i-1} \setminus \mathcal{W}_i$ *has the relative upper density (with respect to* $\mathcal{W}_{i-1}$*) equal to 1 for all* $i \in \mathbb{Z}_{>0}$,
3. *The lower density of* $\mathcal{W}_i$ *is 0, for* $i \in \mathbb{Z}_{>0}$.

Theorem (Eisenträger, Miller, Park, S.)

For any computable real number r between 0 and 1 there exists a c.e. set $\mathcal{S}$ of primes such that the lower density $\mathcal{S}$ is r and $HTP(O_{\mathbb{Q},\mathcal{S}}) \equiv_T HTP(\mathbb{Q})$.

Definability World: Second Glance



Some Questions Without an Answer and a Remarkable Theorem

Let $\mathcal{W}_1$ be an infinite and co-infinite set of rational primes, let $p \notin \mathcal{W}_1$ and let $\mathcal{W}_2 = \mathcal{W}_1 \cup \{p\}$.

- Is $O_{\mathbb{Q},\mathcal{W}_2} = \mathbb{Z}[\mathcal{W}_2^{-1}]$ existentially definable (as a set of pairs) over $O_{\mathbb{Q},\mathcal{W}_1} = \mathbb{Z}[\mathcal{W}_1^{-1}]$?
- Is $\mathrm{HTP}(\mathbb{Z}[\mathcal{W}_2^{-1}]) \leq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{W}_1^{-1}])$?
- Can we define $\mathbb{Z}$ existentially in any big ring?

Some Questions Without an Answer and a Remarkable Theorem

Let $\mathcal{W}_1$ be an infinite and co-infinite set of rational primes, let $p \notin \mathcal{W}_1$ and let $\mathcal{W}_2 = \mathcal{W}_1 \cup \{p\}$.

- Is $O_{\mathbb{Q},\mathcal{W}_2} = \mathbb{Z}[\mathcal{W}_2^{-1}]$ existentially definable (as a set of pairs) over $O_{\mathbb{Q},\mathcal{W}_1} = \mathbb{Z}[\mathcal{W}_1^{-1}]$?
- Is $\mathrm{HTP}(\mathbb{Z}[\mathcal{W}_2^{-1}]) \leq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{W}_1^{-1}])$?
- Can we define $\mathbb{Z}$ existentially in any big ring?

Theorem (Koenigsmann 16)

There exists a definition of $\mathbb{Z}$ over $\mathbb{Q}$ of the form $\forall\exists\ldots\exists f(\ldots) = 0$, where f is a polynomial, with only one variable in the scope of the universal quantifier.

Outline

The Rings of Integers of Number Fields

Theorem (P. Koymets, C. Pagano, 2025)

The ring $\mathbb{Z}$ has a diophantine definition and Hilbert's Tenth Problem is undecidable over the rings of integers of all number fields.

The Rings of Integers of Number Fields

Theorem (P. Koymets, C. Pagano, 2025)

The ring $\mathbb{Z}$ has a diophantine definition and Hilbert's Tenth Problem is undecidable over the rings of integers of all number fields.

Some history: many examples

Examples of fields with Diophantine definitions of $\mathbb{Z}$ and conditions which would result in definitions of $\mathbb{Z}$ were produced by many people: Denef, Lipshitz, Pheidas, Videla, S., Cornilessen and Pheidas and Zahidi, Murty and Pasten, Garcia-Fritz and Pasten, Mazur and Rubin, Mazur and Rubin and S. .

Theorem (Denef, 1980)

If K is a totally real field, then O_K has a Diophantine definition of $\mathbb{Z}$.

Theorem (Denef, 1980)

If K is a totally real field, then O_K has a Diophantine definition of $\mathbb{Z}$.

Theorem (Poonen 02 and S. 08)

Let L/K be a finite extension of number fields. Suppose there exists an elliptic curve E of positive rank defined over K with $[E(L) : E(K)] < \infty$. Then O_K has a Diophantine definition over O_L.

It would suffice

Proposition (Diophantine Stability for Extensions of Degree 2.)

If for any field K there exists a Galois number field M containing K such that $O_{M\cap\mathbb{R}}$ is diophantine over O_M, then H10 is undecidable over rings of integers of all number fields.

A sequence of simple reductions

Step I

If M/K is an extension of number fields, O_K is Diophantine over O_M and $\mathbb{Z}$ is Diophantine over O_K, then $\mathbb{Z}$ is Diophantine over O_M.
(In our application K will be a totally real field)

A sequence of simple reductions

Step I

If M/K is an extension of number fields, O_K is Diophantine over O_M and $\mathbb{Z}$ is Diophantine over O_K, then $\mathbb{Z}$ is Diophantine over O_M. (In our application K will be a totally real field)

Step II

If M/K is an extension of number fields and $\mathbb{Z}$ has a Diophantine definition over M, then $\mathbb{Z}$ has a Diophantine definition over O_K. Therefore without loss of generality we can assume that all the fields under consideration are Galois over $\mathbb{Q}$ and if necessary we can adjoin elements to our fields. (In our application M will contain i and certain real square roots.)

A sequence of simple reductions

Step I

If M/K is an extension of number fields, O_K is Diophantine over O_M and $\mathbb{Z}$ is Diophantine over O_K, then $\mathbb{Z}$ is Diophantine over O_M. (In our application K will be a totally real field)

Step II

If M/K is an extension of number fields and $\mathbb{Z}$ has a Diophantine definition over M, then $\mathbb{Z}$ has a Diophantine definition over O_K. Therefore without loss of generality we can assume that all the fields under consideration are Galois over $\mathbb{Q}$ and if necessary we can adjoin elements to our fields. (In our application M will contain i and certain real square roots.)

Step III

If K, L are number fields contained in a number field M such that O_K is Diophantine over O_M and O_L is Diophantine over O_M. Then $O_K \cap O_L$ is Diophantine over O_K. (In our application L and K will be conjugate over $\mathbb{Q}$.)

One more reduction and descent to a totally really field

Step IV

Let M/K be an extension of number fields with M being Galois over $\mathbb{Q}$. Suppose O_K has a diophantine definition over O_M and $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$. Then $O_{\sigma(K)}$ has a diophantine definition over O_M.

One more reduction and descent to a totally really field

Step IV

Let M/K be an extension of number fields with M being Galois over $\mathbb{Q}$. Suppose O_K has a diophantine definition over O_M and $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$. Then $O_{\sigma(K)}$ has a diophantine definition over O_M.

The intersection is totally real

Let $M/\mathbb{Q}$ be a finite Galois extension such that M is not totally real field. Let $\sigma \in \mathrm{Gal}(M/\mathbb{Q})$ be complex conjugation. Let $K \subset \mathbb{R}$ be the fixed field of complex conjugation. Then $\bigcap_{\tau \in \mathrm{Gal}(M/\mathbb{Q})} \tau(K)$ is a totally real subfield of M. Further, for all $\tau \in \mathrm{Gal}(M/\mathbb{Q})$ it is the case $[M : \tau(K)] = 2$.

The final step

Theorem (P. Koymets, C. Pagano, 2025)

If M is a number field containing i and $\sqrt{19}, \ldots$ and K is a subfield of M of degree 2, then there exists an elliptic curve over K of positive rank and of the same rank over K and over M.

Big Subrings of Number Fields from the Point of View of $\mathbb{Z}$

Theorem (S. 97, 00, 02, 08)

If K is a totally real number field, an extension of degree 2 of a totally real number field or such that there exists an elliptic curve defined over $\mathbb{Q}$ and of the same positive rank over K and $\mathbb{Q}$, then for any $\varepsilon > 0$, there exists a set $\mathcal{W}$ of primes of K whose natural density is bigger than $1 - [K : \mathbb{Q}]^{-1} - \varepsilon$ and such that $\mathbb{Z}$ has a diophantine definition over $O_{K,\mathcal{W}}$, thus implying that Hilbert's Tenth Problem is undecidable over $O_{K,\mathcal{W}}$.

This can be improved to apply to all number fields using the new results of Koymets and Pagano.

Big Subrings of Number Fields from the Point of View of $\mathbb{Z}$

Theorem (S. 97, 00, 02, 08)

If K is a totally real number field, an extension of degree 2 of a totally real number field or such that there exists an elliptic curve defined over $\mathbb{Q}$ and of the same positive rank over K and $\mathbb{Q}$, then for any $\varepsilon > 0$, there exists a set $\mathcal{W}$ of primes of K whose natural density is bigger than $1 - [K : \mathbb{Q}]^{-1} - \varepsilon$ and such that $\mathbb{Z}$ has a diophantine definition over $O_{K,\mathcal{W}}$, thus implying that Hilbert's Tenth Problem is undecidable over $O_{K,\mathcal{W}}$.

This can be improved to apply to all number fields using the new results of Koymets and Pagano.

Theorem (Poonen, S 05, Eisentraeger, Everest 09, Perlega 11, Eisentraeger, Everest, S. 11)

Assume there is an elliptic curve defined over K with K-rank equal to 1. For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers adding up to 1, the set of primes of K may be partitioned into t mutually disjoint computable subsets $\mathcal{S}_1, \ldots, \mathcal{S}_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that $\mathbb{Z}$ admits a diophantine model in each ring $O_{K,\mathcal{S}_i}$. In particular, Hilbert's Tenth Problem is undecidable for each ring $O_{K,\mathcal{S}_i}$.

Theorem (Eisentraeger, Miller, Park, S. 16)

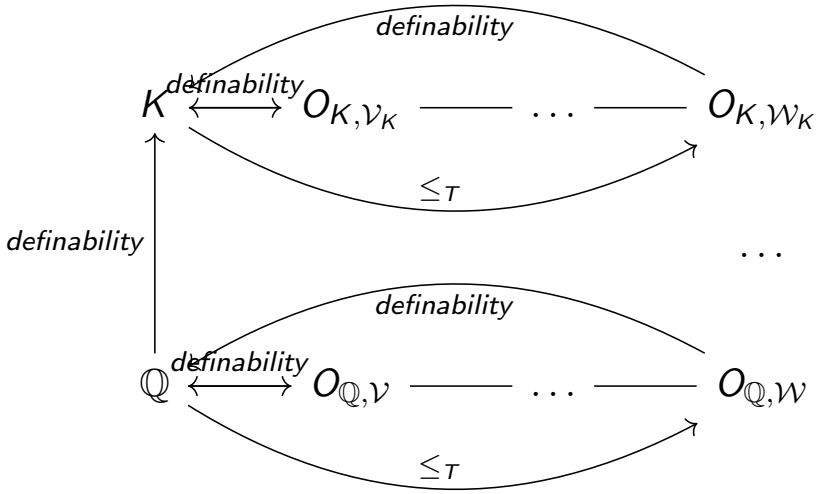
There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of c.e. sets of primes of a number field K (with $\mathcal{P}$ denoting the set of all primes of K) such that

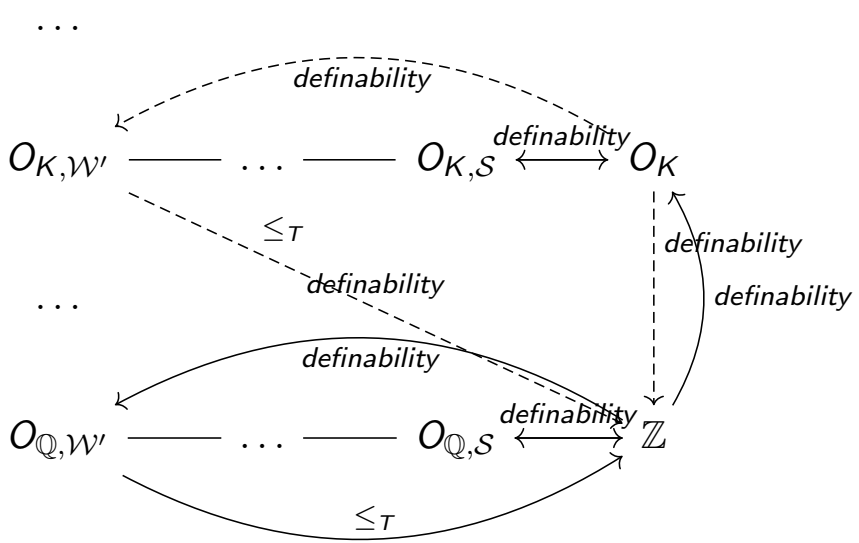
1. $HTP(\mathcal{O}_{K,\mathcal{W}_i}) \equiv_T HTP(K) \leq_T HTP(\mathbb{Q})$ *for* $i \in \mathbb{Z}_{>0}$,
2. $\mathcal{W}_{i-1} - \mathcal{W}_i$ *has the relative upper density (with respect to* $\mathcal{W}_{i-1}$*) equal to 1 for all* $i \in \mathbb{Z}_{>0}$,
3. *The lower density of* $\mathcal{W}_i$ *is 0, for all* $i \in \mathbb{Z}_{>0}$.

Corollary

There exists a computably enumerable subset $\mathcal{W}$ of K-primes, of lower natural density 0, such that
$HTP(\mathbb{Q}) \geq_T HTP(K) \equiv_T HTP(\mathcal{O}_{K,\mathcal{W}})$.

Definability World: Third Glance





Outline

What are we seeking out there?

For the purposes of our discussion we fix an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$ and consider a progression from $\mathbb{Q}$ to its algebraic closure, first through the finite extensions of $\mathbb{Q}$, next through its infinite extensions fairly "far" from the algebraic closure, and finally through the infinite extensions of $\mathbb{Q}$ fairly "close" to $\bar{\mathbb{Q}}$.
As one gets closer to $\bar{\mathbb{Q}}$, there is an expectation that the language of rings would loose more and more of its expressive power. It would be interesting to describe the mile posts signifying various stages of this loss.

Three Questions

Question

If $\mathbf{K}$ *is an infinite algebraic extension of* $\mathbb{Q}$*, then is the ring of integers* $O_{\mathbf{K}}$ *of* $\mathbf{K}$ *first-order definable over* $\mathbf{K}$*?*

Three Questions

Question

If $\mathbf{K}$ *is an infinite algebraic extension of* $\mathbb{Q}$*, then is the ring of integers* $O_{\mathbf{K}}$ *of* $\mathbf{K}$ *first-order definable over* $\mathbf{K}$*?*

Question

Is the first-order theory of $O_{\mathbf{K}}$ *decidable?*

Three Questions

Question

If $\mathbf{K}$ *is an infinite algebraic extension of* $\mathbb{Q}$*, then is the ring of integers* $O_{\mathbf{K}}$ *of* $\mathbf{K}$ *first-order definable over* $\mathbf{K}$*?*

Question

Is the first-order theory of $O_{\mathbf{K}}$ *decidable?*

Question

Is the first-order theory of $\mathbf{K}$ *decidable?*

Results of Rumeley and van den Dries for the Ring of All Algebraic Integers

Theorem (R. Rumely, 1986)

Hilbert's Tenth Problem is decidable over the ring of all algebraic integers.

Results of Rumeley and van den Dries for the Ring of All Algebraic Integers

Theorem (R. Rumely, 1986)

Hilbert's Tenth Problem is decidable over the ring of all algebraic integers.

Theorem (L. van den Dries, 1988)

First-order theory of the ring of all algebraic integers is decidable.

A Result of Fried, Haran and Völklein

Theorem (1994)

The first-order theory of the field of all totally real algebraic numbers is decidable.

Results of Julia Robinson for Totally Real Infinite Extensions of $\mathbb{Q}$

Theorem

The ring of algebraic integers of any totally real field containing an infinite set of the form $\{\cos 2\pi/k, k \in \mathbb{Z}_{>0}\}$ *has an undecidable first-order theory. In particular, the first-order theory of the ring of all totally real integers is undecidable and the first-order theory of the largest totally real abelian extension of* $\mathbb{Q}$ *is undecidable.*

Results of Julia Robinson for Totally Real Infinite Extensions of $\mathbb{Q}$

Theorem

The ring of algebraic integers of any totally real field containing an infinite set of the form $\{\cos 2\pi/k, k \in \mathbb{Z}_{>0}\}$ *has an undecidable first-order theory. In particular, the first-order theory of the ring of all totally real integers is undecidable and the first-order theory of the largest totally real abelian extension of* $\mathbb{Q}$ *is undecidable.*

Corollary

The ring of all totally real algebraic integers is not definable over its fraction field.

Results of Julia Robinson for Totally Real Infinite Extensions of $\mathbb{Q}$

Theorem

The ring of algebraic integers of any totally real field containing an infinite set of the form $\{\cos 2\pi/k, k \in \mathbb{Z}_{>0}\}$ *has an undecidable first-order theory. In particular, the first-order theory of the ring of all totally real integers is undecidable and the first-order theory of the largest totally real abelian extension of* $\mathbb{Q}$ *is undecidable.*

Corollary

The ring of all totally real algebraic integers is not definable over its fraction field.

Theorem

The ring of integers of the field $\mathbb{Q}(\sqrt{p}, p$ *a rational prime*$)$ *has an undecidable first-order theory.*

After J. Robinson

In 2000 Videla constructed a model of $\mathbb{Z}$ over the ring of integers of an infinite cyclotomic extension with finitely many ramified primes showing that the first-order theory of such a ring is undecidable. More results by Videla, Vidaux, Gillibert, Ranier and others followed. Perhaps, the most interesting result was due to C. Springer in 2023 who showed that the ring of integers of a totally complex extension of degree 2 of the field of all totally real integers had an undecidable first-order theory.

Diophantine stability and existential definability

Theorem (Mazur-Rubin-S. 2023)

Let K be a number field, let L be an algebraic (possibly infinite degree) extension of K, and let $O_K \subset O_L$ be their rings of integers. Suppose A is an abelian variety defined over K such that $A(K)$ is infinite and $A(L)/A(K)$ is a torsion group. If at least one of the following conditions is satisfied:

1. *L is a number field,*
2. *L is totally real,*
3. *L is a quadratic extension of a totally real field,*

then O_K has a diophantine definition over O_L.

Diophantine stability and existential definability

Theorem (Mazur-Rubin-S. 2023)

Let K be a number field, let L be an algebraic (possibly infinite degree) extension of K, and let $O_K \subset O_L$ be their rings of integers. Suppose A is an abelian variety defined over K such that $A(K)$ is infinite and $A(L)/A(K)$ is a torsion group. If at least one of the following conditions is satisfied:

1. *L is a number field,*
2. *L is totally real,*
3. *L is a quadratic extension of a totally real field,*

then O_K has a diophantine definition over O_L.

Theorem (Kato 04, Ribet 81, Rohrlich 84, 88, S. 09)

Let $\mathbf{L}$ be an abelian extension with finitely many ramified primes. Then $\mathbb{Z}$ is existentially definable over $O_{\mathbf{L}}$.

Diophantine stability and first-order definability

Theorem (Mazur-Rubin-S. 2023)

Let K be a number field, let L be an algebraic (possibly infinite degree) extension of K, and let $O_K \subset O_L$ be their rings of integers. Suppose A is an abelian variety defined over K such that $A(K)$ is infinite and $A(L)/A(K)$ is a torsion group. Then O_K has a first-order definition over O_L.

Non-big fields

Definition

Let $\mathbf{K}$ be a field of algebraic numbers. We say that $\mathbf{K}$ is *big* if

$$[\mathbf{K} : \mathbb{Q}] = \prod_{p \text{ prime}} p^{\infty}.$$

Equivalently, $\mathbf{K}$ is big if for every positive integer n, $\mathbf{K}$ contains a number field F with $[F : \mathbb{Q}]$ divisible by n.

Non-big fields

Definition

Let $\mathbf{K}$ be a field of algebraic numbers. We say that $\mathbf{K}$ is *big* if

$$[\mathbf{K} : \mathbb{Q}] = \prod_{p \text{ prime}} p^{\infty}.$$

Equivalently, $\mathbf{K}$ is big if for every positive integer n, $\mathbf{K}$ contains a number field F with $[F : \mathbb{Q}]$ divisible by n.

Theorem (Mazur-Rubin-S. 2023)

Let $\mathcal{A}$ be the collection of all non-big fields of algebraic numbers. There exists a first-order formula of the form "$\forall\forall\exists\ldots\exists$" uniformly defining $\mathbb{Z}$ over the rings of integers of all fields in $\mathcal{A}$. In particular the first-order theory of these rings can be uniformly shown to be first-order undecidable.

Defining integers over infinite extensions of $\mathbb{Q}$

Videla in 2000 and then Fukuzaki in 2012 produced the first first-order definitions of rings of integers over infinite extensions of $\mathbb{Q}$. Their results were generalized by S. in 2018. In particular, the following result was proved.

Theorem (S. 2018)

Let $\mathbf{K}$ *be a non-big Galois extension of* $\mathbb{Q}$*. Then* $O_{\mathbf{K}}$ *is first-order definable over* $\mathbf{K}$*.*

Defining integers over infinite extensions of $\mathbb{Q}$

Videla in 2000 and then Fukuzaki in 2012 produced the first first-order definitions of rings of integers over infinite extensions of $\mathbb{Q}$. Their results were generalized by S. in 2018. In particular, the following result was proved.

Theorem (S. 2018)

Let $\mathbf{K}$ *be a non-big Galois extension of* $\mathbb{Q}$*. Then* $O_{\mathbf{K}}$ *is first-order definable over* $\mathbf{K}$*.*

Corollary (Mazur-Rubin-S. 2023)

Let $\mathbf{K}$ *be a non-big Galois extension of* $\mathbb{Q}$*. Then the first-order theory of* $\mathbf{K}$ *is undecidable.*

Outline

Some equivalencies

The goal

Let M/K be a Galois extension of number fields and suppose we need to construct a diophantine definition of O_K over O_M.

Let A be a subset of O_M defined by the following formula:
$x \in A \Leftrightarrow \exists \varepsilon, \delta \in (O_K)^*$ such that

$$\varepsilon - 1 \equiv 0 \bmod (\delta - 1) \wedge$$

$$x \equiv \frac{\varepsilon - 1}{\delta - 1} \bmod (\delta - 1) \wedge$$

$$\forall \sigma \in \mathrm{Gal}(M/K) : |N_{M/\mathbb{Q}}(\delta - 1)| > |N_{M/\mathbb{Q}}(\alpha - \sigma(\alpha))|.$$

Some equivalencies

The goal

Let M/K be a Galois extension of number fields and suppose we need to construct a diophantine definition of O_K over O_M.

Let A be a subset of O_M defined by the following formula:
$x \in A \Leftrightarrow \exists \varepsilon, \delta \in (O_K)^*$ such that

$$\varepsilon - 1 \equiv 0 \bmod (\delta - 1) \wedge$$

$$x \equiv \frac{\varepsilon - 1}{\delta - 1} \bmod (\delta - 1) \wedge$$

$$\forall \sigma \in \mathrm{Gal}(M/K) : |N_{M/\mathbb{Q}}(\delta - 1)| > |N_{M/\mathbb{Q}}(\alpha - \sigma(\alpha))|.$$

Then $\forall \sigma \in \mathrm{Gal}(M/K)$:

$$\sigma(x) \equiv \frac{\varepsilon - 1}{\delta - 1} \bmod (\delta - 1)$$

and $\forall \sigma \in \mathrm{Gal}(M/K)$:

$$\sigma(x) - x \equiv 0 \bmod (\delta - 1).$$

Thus, $\forall \sigma \in \mathrm{Gal}(M/K)$:

$$N_{M/\mathbb{Q}}(\sigma(x) - x) \equiv 0 \bmod N_{M/\mathbb{Q}}(\delta - 1)$$

and

$$|N_{M/\mathbb{Q}}(\sigma(x) - x) \geq N_{M/\mathbb{Q}}(\delta - 1) \vee (\sigma(x) - x) = 0.$$

Therefore, $A \subset O_K$.

Some high school algebra

Proposition

$\mathbb{Z} \subset A$.

Proof.

- For any $x \in \mathbb{Z} \setminus 0$ and any unit $\mu \in O_M$ there exists $n \in \mathbb{Z}$ such that $\mu^n - 1 \equiv 0 \bmod x$.
- Now let $\delta = \mu^n$ and let $\varepsilon = \mu^{nx} = \delta^x$ and observe that

$$\frac{\delta^x - 1}{\delta - 1} \equiv x \bmod (\delta - 1).$$

□

Getting the rest of O_K

Let α be a generator of K over $\mathbb{Q}$ and let $r := [K : \mathbb{Q}]$. Define

$$B = \{x \in O_M | x = \sum_{i=0}^{r-1} \frac{a_i}{b_i} \alpha^i, a_i, b_i \in A, b_i \neq 0\}.$$

Then $B = O_K$.

The bound condition

Translating the bound condition below into the language of rings:

$$\forall \sigma \in \mathrm{Gal}(M/K) : |N_{M/\mathbb{Q}}(\delta - 1)| > |N_{M/\mathbb{Q}}(\alpha - \sigma(\alpha))|.$$

Let $n := [M : \mathbb{Q}]$, $w \in O_M$ and suppose

$$w \equiv 0 \bmod x(1-x)\dots(m-x).$$

Then

$$N_{M/\mathbb{Q}}(w) \equiv 0 \bmod N_{M/\mathbb{Q}}(x(1-x)\dots(m-1-x)).$$

The bound condition

Translating the bound condition below into the language of rings:

$$\forall \sigma \in \mathrm{Gal}(M/K) : |N_{M/\mathbb{Q}}(\delta - 1)| > |N_{M/\mathbb{Q}}(\alpha - \sigma(\alpha))|.$$

Let $n := [M : \mathbb{Q}]$, $w \in O_M$ and suppose

$$w \equiv 0 \bmod x(1-x)\dots(m-x).$$

Then

$$N_{M/\mathbb{Q}}(w) \equiv 0 \bmod N_{M/\mathbb{Q}}(x(1-x)\dots(m-1-x)).$$

Now, for any $\ell \in \mathbb{Z}$ we have that $N_{M/\mathbb{Q}}(\ell - x) = P(\ell)$, where $P(T)$ is the characteristic polynomial with respect to M of x over $\mathbb{Q}$. Assuming $P(T) = \sum_{i=0}^{m-1} a_i T^i$ we have that

$$\sum_{i=0}^{m-1} a_i \ell^i = c_\ell N_{M/\mathbb{Q}}(w), \ell = 0, \dots, m-1,$$

where $c_\ell \in \mathbb{Q}$ and $|c_\ell| \leq 1$. If we solve the linear system above for $a_0, \dots, a_{m-1}$ using Cramer's rule, we will obtain a bound on a_i's in terms of w and m. From the bound on a_i, we can get a bound on all roots of $P(T)$ and thus on the differences of roots.

How do we define a sufficiently large set of O_K-units over O_M?

This is where you need diophantine stability. If K is totally real and M is a totally complex extension of degree 2 of K. Then the ranks of their unit groups are the same. Therefore, there exists $u \in \mathbb{Z}_{>0}$ such that for any unit δ of O_M we have that $\delta^u \in O_K$.