Hilbert's 10th Problem and decidability in number theory

Algebra Colloquium

Nicolas Daans

Charles University, Faculty of Mathematics and Physics, Department of Algebra

29 March 2023

Section 1

Hilbert's 10th Problem

Solving polynomial equations

Recall: for a univariate polynomial $f \in \mathbb{Z}[X]$, it is easy to find all of its integer and rational roots.

Theorem (Rational Root Theorem)

Consider a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ for $n \in \mathbb{N}$ and $a_0, \ldots, a_n \in \mathbb{Z}$ with $a_0, a_n \neq 0$.
All rational roots of $f(X)$ are of the form $\frac{x}{y}$ with $x, y \in \mathbb{Z}$ such that $x \mid a_0$ and $y \mid a_n$.

In particular, there is an *algorithm* which can decide whether a univariate polynomial over $\mathbb{Z}$ has an integer root, and whether it has a rational root.

Solving polynomial equations

Recall: for a univariate polynomial $f \in \mathbb{Z}[X]$, it is easy to find all of its integer and rational roots.

Theorem (Rational Root Theorem)

Consider a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ *for* $n \in \mathbb{N}$ *and* $a_0, \ldots, a_n \in \mathbb{Z}$ *with* $a_0, a_n \neq 0$.
All rational roots of $f(X)$ *are of the form* $\frac{x}{y}$ *with* $x, y \in \mathbb{Z}$ *such that* $x \mid a_0$ *and* $y \mid a_n$.

In particular, there is an *algorithm* which can decide whether a univariate polynomial over $\mathbb{Z}$ has an integer root, and whether it has a rational root.

For multivariate polynomials, it is much harder to decide whether there is an integer (respectively rational) zero.

Hilbert's 10th Problem

At the 1900 International Congress of Mathematicians, David Hilbert posed the following problem, in modern terms:

> *Can one find an algorithm which takes as input a polynomial equation with integer coefficients, and outputs YES if the equation is solvable over the integers, and NO otherwise ?*

This is now known as Hilbert's 10th Problem.

Hilbert's 10th Problem

At the 1900 International Congress of Mathematicians, David Hilbert posed the following problem, in modern terms:

> ~~*Can one*~~ *Find an algorithm which takes as input a polynomial equation with integer coefficients, and outputs YES if the equation is solvable over the integers, and NO otherwise* ~~*?*~~ *!*

This is now known as Hilbert's 10th Problem.

Hilbert's 10th Problem

Note: once we know that a polynomial equation $f(X_1, \ldots, X_n) \doteq g(X_1, \ldots, X_n)$ with $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ has a solution, then there is an algorithm to find a solution:

- Fix a (computable) bijection $B : \mathbb{N} \to \mathbb{Z}^n$.

Hilbert's 10th Problem

Note: once we know that a polynomial equation $f(X_1, \ldots, X_n) \doteq g(X_1, \ldots, X_n)$ with $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ has a solution, then there is an algorithm to find a solution:

- Fix a (computable) bijection $B : \mathbb{N} \to \mathbb{Z}^n$.
- Now initialise the algorithm with an integer $a = 0$ and proceed as follows:

Hilbert's 10th Problem

Note: once we know that a polynomial equation $f(X_1, \ldots, X_n) \doteq g(X_1, \ldots, X_n)$ with $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ has a solution, then there is an algorithm to find a solution:

- Fix a (computable) bijection $B : \mathbb{N} \to \mathbb{Z}^n$.
- Now initialise the algorithm with an integer $a = 0$ and proceed as follows:
  1. Check whether $f(B(a)) = g(B(a))$. If yes, then terminate and output $B(a)$. Otherwise, continue.

Hilbert's 10th Problem

Note: once we know that a polynomial equation $f(X_1, \ldots, X_n) \doteq g(X_1, \ldots, X_n)$ with $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ has a solution, then there is an algorithm to find a solution:

- Fix a (computable) bijection $B : \mathbb{N} \to \mathbb{Z}^n$.
- Now initialise the algorithm with an integer $a = 0$ and proceed as follows:
  1. Check whether $f(B(a)) = g(B(a))$. If yes, then terminate and output $B(a)$. Otherwise, continue.
  2. Replace a by $a + 1$ and go back to step 1.

Hilbert's 10th Problem

Note: once we know that a polynomial equation $f(X_1, \ldots, X_n) \doteq g(X_1, \ldots, X_n)$ with $f, g \in \mathbb{Z}[X_1, \ldots, X_n]$ has a solution, then there is an algorithm to find a solution:

- Fix a (computable) bijection $B : \mathbb{N} \to \mathbb{Z}^n$.
- Now initialise the algorithm with an integer $a = 0$ and proceed as follows:
  1. Check whether $f(B(a)) = g(B(a))$. If yes, then terminate and output $B(a)$. Otherwise, continue.
  2. Replace a by $a + 1$ and go back to step 1.
- Because we know that a solution to $f \doteq g$ exists, this algorithm will eventually output a solution.

Hilbert's 10th Problem

Note: once we know that a polynomial equation $f(X_1, \dots, X_n) \doteq g(X_1, \dots, X_n)$ with $f, g \in \mathbb{Z}[X_1, \dots, X_n]$ has a solution, then there is an algorithm to find a solution:

- Fix a (computable) bijection $B : \mathbb{N} \to \mathbb{Z}^n$.
- Now initialise the algorithm with an integer $a = 0$ and proceed as follows:
  1. Check whether $f(B(a)) = g(B(a))$. If yes, then terminate and output $B(a)$. Otherwise, continue.
  2. Replace a by $a + 1$ and go back to step 1.
- Because we know that a solution to $f \doteq g$ exists, this algorithm will eventually output a solution.

The problem is: without knowing a priori that there is a solution, after how many failed iterations of this procedure can we conclude that the equation does not have a solution?

Hilbert's 10th Problem is unsolvable!

That is, there can never be an algorithm which can decide whether a given polynomial equation with integer coefficients has an integer solution or not.
This was proven by Yuri Matiyasevich in 1970, building on work of Martin Davis, Hilary Putnam, and Julia Robinson.

Tarski's decision procedure

On the other hand: there is an algorithm to determine, given a polynomial in any number of variables, whether it has a zero consisting of real numbers (Alfred Tarski, ca. 1950).

Tarski's decision procedure

On the other hand: there is an algorithm to determine, given a polynomial in any number of variables, whether it has a zero consisting of real numbers (Alfred Tarski, ca. 1950).

Tarski's algorithm is of theoretical interest
→ too unwieldy in practice, compuational requirements grow superexponentially
→ search for efficient algorithms in specific cases topic of ongoing research in real algebra

Hilbert's 10th problem over a ring

Definition

Let R_0 be a computable commutative ring, R a commutative R_0-algebra. We say that Hilbert's 10th Problem over R with coefficients in R_0 is solvable if there exists an algorithm which takes as input a polynomial with coefficients in R_0 and outputs YES if the polynomial has a zero in R, and NO otherwise.
Otherwise, we say that Hilbert's 10th Problem over R with coefficients in R_0 is unsolvable.

Let us abbreviate to "$\mathrm{Hil10}_{R_0}(R)$ is solvable/unsolvable". Examples:

Hilbert's 10th problem over a ring

Definition

Let R_0 be a computable commutative ring, R a commutative R_0-algebra. We say that Hilbert's 10th Problem over R with coefficients in R_0 is solvable if there exists an algorithm which takes as input a polynomial with coefficients in R_0 and outputs YES if the polynomial has a zero in R, and NO otherwise.
Otherwise, we say that Hilbert's 10th Problem over R with coefficients in R_0 is unsolvable.

Let us abbreviate to "$\text{Hil10}_{R_0}(R)$ is solvable/unsolvable". Examples:

- $\text{Hil10}_{\mathbb{Z}}(\mathbb{Z})$ is unsolvable (DPRM, 1970),

Hilbert's 10th problem over a ring

Definition

Let R_0 be a computable commutative ring, R a commutative R_0-algebra. We say that Hilbert's 10th Problem over R with coefficients in R_0 is solvable if there exists an algorithm which takes as input a polynomial with coefficients in R_0 and outputs YES if the polynomial has a zero in R, and NO otherwise.
Otherwise, we say that Hilbert's 10th Problem over R with coefficients in R_0 is unsolvable.

Let us abbreviate to "$\text{Hil10}_{R_0}(R)$ is solvable/unsolvable". Examples:

- $\text{Hil10}_{\mathbb{Z}}(\mathbb{Z})$ is unsolvable (DPRM, 1970),
- $\text{Hil10}_{\mathbb{Z}}(\mathbb{R})$ and $\text{Hil10}_{\mathbb{Z}}(\mathbb{C})$ are solvable. In fact, $\text{Hil10}_{R_0}(\mathbb{R})$ and $\text{Hil10}_{R_0}(\mathbb{C})$ are solvable for many computable subrings R_0 of $\mathbb{R}$ respectively $\mathbb{C}$, e.g. when R_0 is finitely generated (Tarski, 1950),

Hilbert's 10th problem over a ring

Definition

Let R_0 be a computable commutative ring, R a commutative R_0-algebra. We say that Hilbert's 10th Problem over R with coefficients in R_0 is solvable if there exists an algorithm which takes as input a polynomial with coefficients in R_0 and outputs YES if the polynomial has a zero in R, and NO otherwise.
Otherwise, we say that Hilbert's 10th Problem over R with coefficients in R_0 is unsolvable.

Let us abbreviate to "$\mathrm{Hil10}_{R_0}(R)$ is solvable/unsolvable". Examples:

- $\mathrm{Hil10}_{\mathbb{Z}}(\mathbb{Z})$ is unsolvable (DPRM, 1970),
- $\mathrm{Hil10}_{\mathbb{Z}}(\mathbb{R})$ and $\mathrm{Hil10}_{\mathbb{Z}}(\mathbb{C})$ are solvable. In fact, $\mathrm{Hil10}_{R_0}(\mathbb{R})$ and $\mathrm{Hil10}_{R_0}(\mathbb{C})$ are solvable for many computable subrings R_0 of $\mathbb{R}$ respectively $\mathbb{C}$, e.g. when R_0 is finitely generated (Tarski, 1950),
- $\mathrm{Hil10}_{\mathbb{Z}}(\mathbb{R}[X])$ is solvable (a polynomial over $\mathbb{R}$ has a zero over $\mathbb{R}[X]$ if and only if it has a zero over $\mathbb{R}$), but $\mathrm{Hil10}_{\mathbb{Z}[X]}(\mathbb{R}[X])$ is unsolvable (Denef, 1978).

Hilbert's 10th problem over a ring

Definition

Let R_0 be a computable commutative ring, R a commutative R_0-algebra. We say that Hilbert's 10th Problem over R with coefficients in R_0 is solvable if there exists an algorithm which takes as input a polynomial with coefficients in R_0 and outputs YES if the polynomial has a zero in R, and NO otherwise.
Otherwise, we say that Hilbert's 10th Problem over R with coefficients in R_0 is unsolvable.

Let us abbreviate to "$\text{Hil10}_{R_0}(R)$ is solvable/unsolvable". Examples:

- $\text{Hil10}_{\mathbb{Z}}(\mathbb{Z})$ is unsolvable (DPRM, 1970),
- $\text{Hil10}_{\mathbb{Z}}(\mathbb{R})$ and $\text{Hil10}_{\mathbb{Z}}(\mathbb{C})$ are solvable. In fact, $\text{Hil10}_{R_0}(\mathbb{R})$ and $\text{Hil10}_{R_0}(\mathbb{C})$ are solvable for many computable subrings R_0 of $\mathbb{R}$ respectively $\mathbb{C}$, e.g. when R_0 is finitely generated (Tarski, 1950),
- $\text{Hil10}_{\mathbb{Z}}(\mathbb{R}[X])$ is solvable (a polynomial over $\mathbb{R}$ has a zero over $\mathbb{R}[X]$ if and only if it has a zero over $\mathbb{R}$), but $\text{Hil10}_{\mathbb{Z}[X]}(\mathbb{R}[X])$ is unsolvable (Denef, 1978).

We will (informally) just say that Hilbert's 10th Problem over R is solvable ("$\text{Hil10}(R)$ is solvable") if $\text{Hil10}_{R_0}(R)$ is solvable for every *reasonable* choice of computable subring R_0 of R.

Hilbert's 10th problem over other rings and fields

Hil10 is solvable.		Hil10 is unsolvable.

Hilbert's 10th problem over other rings and fields

Hil10 is solvable.		Hil10 is unsolvable.
$\mathbb{R}, \mathbb{C}$		

Hilbert's 10th problem over other rings and fields

Hil10 is solvable.		Hil10 is unsolvable.
$\mathbb{R}, \mathbb{C}$		$\mathbb{Z}$

Hilbert's 10th problem over other rings and fields

Hil10 is solvable.	Hil10 is open.	Hil10 is unsolvable.
$\mathbb{R}, \mathbb{C}$	$\mathbb{Q}$	$\mathbb{Z}$

Hilbert's 10th problem over other rings and fields

Hil10 is solvable.	Hil10 is open.	Hil10 is unsolvable.
$\mathbb{R}, \mathbb{C}$, $\mathbb{F}_q$, $\mathbb{Q}_p$, $\mathbb{Z}_p$, the algebraic integers $\tilde{\mathbb{Z}}$, $\tilde{\mathbb{Z}} \cap \mathbb{R}$, $\tilde{\mathbb{Z}} \cap \mathbb{Q}_p$, ...	$\mathbb{Q}$, all number fields, $\mathbb{C}(X)$, $\mathbb{R}(X)(\sqrt{-(1+X^2)})$, $\mathbb{F}_q((X))$, $\mathbb{Q}^{ab}$, $\mathbb{Z}^{ab}$, Ω, ...	$\mathbb{Z}$, $\mathcal{O}_K$ with K a totally real number field, $A[X]$ for any commutative ring A, rational function fields over $\mathbb{R}, \mathbb{Q}_p, \mathbb{C}(Y), \mathbb{F}_q, \mathbb{C}((Y)), \ldots$

Section 2

Existentially definable subsets

Zero set of a polynomial

Given a polynomial, we can consider its zero set.
E.g. for the polynomial $x^2 + y^2 - 25$.

Zero set of a polynomial

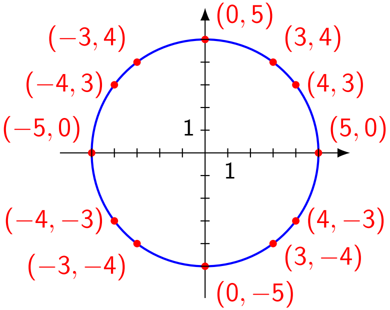
Given a polynomial, we can consider its zero set.
E.g. for the polynomial $x^2 + y^2 - 25$.

- Zero set over $\mathbb{Z}$:

$$\{(a, b) \in \mathbb{Z}^2 \mid a^2 + b^2 = 25\}$$

- Zero set over $\mathbb{R}$:

$$\{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 = 25\}$$

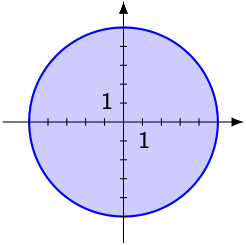


Existentially definable subsets

The ‘filled circle’

$$\{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 \leq 25\}$$

is not the zero set of a bivariate polynomial over $\mathbb{R}$.

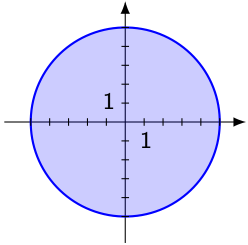


Existentially definable subsets

The 'filled circle'

$$\{(a,b) \in \mathbb{R}^2 \mid a^2 + b^2 \leq 25\}$$

is not the zero set of a bivariate polynomial over $\mathbb{R}$.



But: for $a, b \in \mathbb{R}$ we have

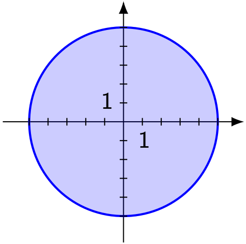
$$a^2 + b^2 \leq 25 \quad \Leftrightarrow \quad \text{there exists } c \in \mathbb{R} : a^2 + b^2 + c^2 = 25.$$

Existentially definable subsets

The 'filled circle'

$$\{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 \leq 25\}$$

is not the zero set of a bivariate polynomial over $\mathbb{R}$.



But: for $a, b \in \mathbb{R}$ we have

$$a^2 + b^2 \leq 25 \quad \Leftrightarrow \quad \text{there exists } c \in \mathbb{R} : a^2 + b^2 + c^2 = 25.$$

Hence

$$\{(a, b) \in \mathbb{R}^2 \mid a^2 + b^2 \leq 25\} = \{(a, b) \in \mathbb{R}^2 \mid \exists c \in \mathbb{R} : a^2 + b^2 + c^2 = 25\}.$$

Existentially definable subsets

The set

$$\{(a,b) \in \mathbb{R}^2 \mid \exists c \in \mathbb{R} : a^2 + b^2 + c^2 = 25\}$$

is an example of an *existentially definable subset of* $\mathbb{R}^2$ *with* 1 *quantifier*.

Existentially definable subsets

The set

$$\{(a, b) \in \mathbb{R}^2 \mid \exists c \in \mathbb{R} : a^2 + b^2 + c^2 = 25\}$$

is an example of an *existentially definable subset of* $\mathbb{R}^2$ *with* 1 *quantifier*.

Definition

Let R be a commutative ring, $n, m \in \mathbb{N}$. As subset A of R^n is called existentially definable over R with m quantifiers ($\exists_m^+$-definable) if there exist $k \in \mathbb{N}$ and polynomials $f_1, \ldots, f_k \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ such that

$$A = \{x \in R^n \mid \exists y \in R^m : f_1(x, y) = \ldots = f_k(x, y) = 0\}.$$

Existentially definable subsets

The set

$$\{(a,b) \in \mathbb{R}^2 \mid \exists c \in \mathbb{R} : a^2 + b^2 + c^2 = 25\}$$

is an example of an *existentially definable subset of* $\mathbb{R}^2$ *with* 1 *quantifier*.

Definition

Let R be a commutative ring, $n, m \in \mathbb{N}$. As subset A of R^n is called existentially definable over R with m quantifiers ($\exists_m^+$-definable) if there exist $k \in \mathbb{N}$ and polynomials $f_1, \ldots, f_k \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ such that

$$A = \{x \in R^n \mid \exists y \in R^m : f_1(x,y) = \ldots = f_k(x,y) = 0\}.$$

We call a subset A of R^n existentially definable over R ($\exists^+$-definable) if it is $\exists_m^+$-definable for some $m \in \mathbb{N}$.

Existentially definable subsets

The set

$$\{(a, b) \in \mathbb{R}^2 \mid \exists c \in \mathbb{R} : a^2 + b^2 + c^2 = 25\}$$

is an example of an *existentially definable subset of* $\mathbb{R}^2$ *with* 1 *quantifier*.

Definition

Let R be a commutative ring, $n, m \in \mathbb{N}$. As subset A of R^n is called existentially definable over R with m quantifiers ($\exists_m^+$-definable) if there exist $k \in \mathbb{N}$ and polynomials $f_1, \ldots, f_k \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ such that

$$A = \{x \in R^n \mid \exists y \in R^m : f_1(x, y) = \ldots = f_k(x, y) = 0\}.$$

We call a subset A of R^n existentially definable over R ($\exists^+$-definable) if it is $\exists_m^+$-definable for some $m \in \mathbb{N}$.

Usually one may assume wlog that $k = 1$ in the above definition (e.g. for $R = \mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$).

Existentially definable subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Which subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are existentially definable?

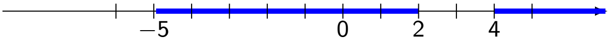
- $\mathbb{C}$ (Tarski, I think): $\exists^+$-definable $=$ $\exists_1^+$-definable $=$ finite or cofinite
  E.g. $\{2, 3, 5\}$, $\mathbb{C} \setminus \{2, 3, 5\}$.

 Existentially definable subsets

Existentially definable subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Which subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are existentially definable?

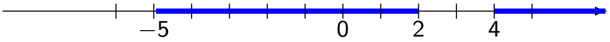
- $\mathbb{C}$ (Tarski, I think): $\exists^+$-definable $=$ $\exists_1^+$-definable $=$ finite or cofinite
  E.g. $\{2, 3, 5\}$, $\mathbb{C} \setminus \{2, 3, 5\}$.
- $\mathbb{R}$ (Tarski): $\exists^+$-definable $=$ $\exists_1^+$-definable $=$ finite union of intervals.
  E.g. $]-5, 2] \cup]4, +\infty[$.



Existentially definable subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Which subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are existentially definable?

- $\mathbb{C}$ (Tarski, I think): $\exists^+$-definable $=$ $\exists^+_1$-definable $=$ finite or cofinite
  E.g. $\{2,3,5\}$, $\mathbb{C} \setminus \{2,3,5\}$.
- $\mathbb{R}$ (Tarski): $\exists^+$-definable $=$ $\exists^+_1$-definable $=$ finite union of intervals.
  E.g. $]-5,2] \cup]4,+\infty[$.

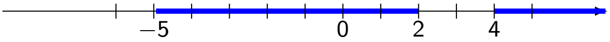


- $\mathbb{Z}$ (DPRM): Every *recursively enumerable* subset of $\mathbb{Z}^n$ is $\exists^+$-definable $=$ $\exists^+_{11}$-definable.
  E.g. the set of prime numbers, the set of 2-powers, the set of factorials, ...

Existentially definable subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

Which subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are existentially definable?

- $\mathbb{C}$ (Tarski, I think): $\exists^+$-definable $=$ $\exists_1^+$-definable $=$ finite or cofinite
  E.g. $\{2,3,5\}$, $\mathbb{C} \setminus \{2,3,5\}$.
- $\mathbb{R}$ (Tarski): $\exists^+$-definable $=$ $\exists_1^+$-definable $=$ finite union of intervals.
  E.g. $]-5,2] \cup]4,+\infty[$.



- $\mathbb{Z}$ (DPRM): Every *recursively enumerable* subset of $\mathbb{Z}^n$ is $\exists^+$-definable $=$ $\exists_{11}^+$-definable.
  E.g. the set of prime numbers, the set of 2-powers, the set of factorials, ...
- $\mathbb{Q}$: Many $\exists^+$-definable subsets.
  E.g. the set of non-negative rational numbers

$$\mathbb{Q}_{\geq 0} = \{x \in \mathbb{Q} \mid \exists y_1, \ldots, y_4 \in \mathbb{Q} : x - (y_1^2 + \ldots + y_4^2) = 0\}.$$

$\exists^+$-definable sets and complexity

Vague, imprecise philosophy: For a commutative ring R, the following seem to correlate:

- more $\exists^+$-definable subsets,
- more and wilder obstructions to polynomials having zeros,
- less likely that Hil10(R) is solvable.

So, showing that Hil10(R) is unsolvable, is related to showing that many subsets of R (or R^n) are $\exists^+$-definable.

DPRM revisited

Theorem (M. Davis, H. Putnam, J. Robinson, Y. Matiyasevich)

Let $n \in \mathbb{N}$. Every recursively enumerable subset of $\mathbb{Z}^n$ is $\exists^+$-definable.

Corollary

$\mathrm{Hil10}(\mathbb{Z})$ *is unsolvable.*

DPRM revisited

Theorem (M. Davis, H. Putnam, J. Robinson, Y. Matiyasevich)

Let $n \in \mathbb{N}$. Every recursively enumerable subset of $\mathbb{Z}^n$ is $\exists^+$-definable.

Corollary

$\text{Hil10}(\mathbb{Z})$ *is unsolvable.*

Proof sketch.

- There exists a recursively enumerable subset $A \subseteq \mathbb{Z}$ such that $\mathbb{Z} \setminus A$ is not recursively enumerable (e.g. by the unsolvability of the Halting Problem).

□

DPRM revisited

Theorem (M. Davis, H. Putnam, J. Robinson, Y. Matiyasevich)

Let $n \in \mathbb{N}$. Every recursively enumerable subset of $\mathbb{Z}^n$ is $\exists^+$-definable.

Corollary

$\mathrm{Hil10}(\mathbb{Z})$ *is unsolvable.*

Proof sketch.

- There exists a recursively enumerable subset $A \subseteq \mathbb{Z}$ such that $\mathbb{Z} \setminus A$ is not recursively enumerable (e.g. by the unsolvability of the Halting Problem).
- By the theorem, A is $\exists^+$-definable, i.e. there exists a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_m]$ such that

$$A = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}^m : f(x, y) = 0\}.$$

$\square$

DPRM revisited

Theorem (M. Davis, H. Putnam, J. Robinson, Y. Matiyasevich)

Let $n \in \mathbb{N}$. Every recursively enumerable subset of $\mathbb{Z}^n$ is $\exists^+$-definable.

Corollary

Hil10($\mathbb{Z}$) *is unsolvable.*

Proof sketch.

- There exists a recursively enumerable subset $A \subseteq \mathbb{Z}$ such that $\mathbb{Z} \setminus A$ is not recursively enumerable (e.g. by the unsolvability of the Halting Problem).
- By the theorem, A is $\exists^+$-definable, i.e. there exists a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_m]$ such that
$$A = \{x \in \mathbb{Z} \mid \exists y \in \mathbb{Z}^m : f(x, y) = 0\}.$$
- Since $\mathbb{Z} \setminus A$ is not recursively enumerable, there cannot be an algorithm which decides, for any input $x \in \mathbb{Z}$, whether $f(x, Y_1, \ldots, Y_m)$ has a zero over $\mathbb{Z}$.

□

$\exists^+$-subsets of $\mathbb{Q}$ and Hil10($\mathbb{Q}$)

Proposition

Suppose $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$. Then Hil10($\mathbb{Q}$) *is unsolvable.*

$\exists^+$-subsets of $\mathbb{Q}$ and Hil10($\mathbb{Q}$)

Proposition

Suppose $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$. Then Hil10($\mathbb{Q}$) *is unsolvable.*

Proof sketch.

- Since $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$, one can effectively find, for every $n \in \mathbb{N}$ and polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, some $m \in \mathbb{N}$ and polynomial $g \in \mathbb{Z}[Y_1, \ldots, Y_m]$ such that

$$f \text{ has a root in } \mathbb{Z}^n \qquad \Leftrightarrow \qquad g \text{ has a root in } \mathbb{Q}^m.$$

□

$\exists^+$-subsets of $\mathbb{Q}$ and Hil10($\mathbb{Q}$)

Proposition

Suppose $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$. Then Hil10($\mathbb{Q}$) *is unsolvable.*

Proof sketch.

- Since $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$, one can effectively find, for every $n \in \mathbb{N}$ and polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, some $m \in \mathbb{N}$ and polynomial $g \in \mathbb{Z}[Y_1, \ldots, Y_m]$ such that

$$f \text{ has a root in } \mathbb{Z}^n \quad \Leftrightarrow \quad g \text{ has a root in } \mathbb{Q}^m.$$

- If Hil10($\mathbb{Q}$) would be decidable, then also Hil10($\mathbb{Z}$) would be decidable, quod non.

□

$\exists^+$-subsets of $\mathbb{Q}$ and Hil10($\mathbb{Q}$)

Proposition

Suppose $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$. Then Hil10($\mathbb{Q}$) *is unsolvable.*

Proof sketch.

- Since $\mathbb{Z}$ is $\exists^+$-definable over $\mathbb{Q}$, one can effectively find, for every $n \in \mathbb{N}$ and polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$, some $m \in \mathbb{N}$ and polynomial $g \in \mathbb{Z}[Y_1, \ldots, Y_m]$ such that

$$f \text{ has a root in } \mathbb{Z}^n \qquad \Leftrightarrow \qquad g \text{ has a root in } \mathbb{Q}^m.$$

- If Hil10($\mathbb{Q}$) would be decidable, then also Hil10($\mathbb{Z}$) would be decidable, quod non.

□

Question

Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

If yes, then every recursively enumerable subset of $\mathbb{Q}$ is $\exists^+$-definable.

Section 3

$\exists^+$-definability and subrings of fields

$\exists^+$-definable subrings of $\mathbb{Q}$

It is possible for subrings (e.g. of $\mathbb{Q}$) to be $\exists^+$-definable subsets.
For a prime number p, consider the local ring

$$\mathbb{Z}_{(p)} = \left\{ \frac{x}{y} \;\middle|\; x \in \mathbb{Z}, y \in \mathbb{Z} \setminus p\mathbb{Z} \right\}.$$

This is always $\exists_3^+$-definable in $\mathbb{Q}$ ("essentially" due to Robinson, 1949).

For example:

Proposition

Let p be a prime number, $p \equiv 3 \bmod 4$. Then

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2\}$$

For example:

Proposition

Let p be a prime number, $p \equiv 3 \bmod 4$. Then

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2\}$$

Proof sketch.

For $x \in \mathbb{Q}$ we have

$$\exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2$$

□

For example:

Proposition

Let p be a prime number, $p \equiv 3 \bmod 4$. Then

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2\}$$

Proof sketch.

For $x \in \mathbb{Q}$ we have

$$\begin{aligned} & \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2 \\ \Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{Q}}(Y_1^2 + Y_2^2 + pY_3^2) \end{aligned}$$

□

For example:

Proposition

Let p be a prime number, $p \equiv 3 \bmod 4$. Then

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2\}$$

Proof sketch.

For $x \in \mathbb{Q}$ we have

$$\begin{aligned} & \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2 \\ \Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{Q}}(Y_1^2 + Y_2^2 + pY_3^2) \\ \Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{R}}(Y_1^2 + Y_2^2 + pY_3^2) \cap \bigcap_{q \text{ prime}} D_{\mathbb{Q}_q}(Y_1^2 + Y_2^2 + pY_3^2) \quad \text{(Minkowski)} \end{aligned}$$

□

For example:

Proposition

Let p be a prime number, $p \equiv 3 \bmod 4$*. Then*

$$\mathbb{Z}_{(p)} = \left\{x \in \mathbb{Q} \;\middle|\; \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2\right\}$$

Proof sketch.

For $x \in \mathbb{Q}$ we have

$$\begin{aligned} & \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2 \\ \Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{Q}}(Y_1^2 + Y_2^2 + pY_3^2) \\ \Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{R}}(Y_1^2 + Y_2^2 + pY_3^2) \cap \bigcap_{q \text{ prime}} D_{\mathbb{Q}_q}(Y_1^2 + Y_2^2 + pY_3^2) \quad \text{(Minkowski)} \\ \Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{Q}_p}(Y_1^2 + Y_2^2 + pY_3^2) \end{aligned}$$

□

For example:

Proposition

Let p be a prime number, $p \equiv 3 \bmod 4$. Then

$$\mathbb{Z}_{(p)} = \left\{x \in \mathbb{Q} \;\middle|\; \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2\right\}$$

Proof sketch.

For $x \in \mathbb{Q}$ we have

$$\begin{aligned}
& \exists y_1, y_2, y_3 \in \mathbb{Q} : 1 + (p-1)px^2 = y_1^2 + y_2^2 + py_3^2 \\
\Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{Q}}(Y_1^2 + Y_2^2 + pY_3^2) \\
\Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{R}}(Y_1^2 + Y_2^2 + pY_3^2) \cap \bigcap_{q \text{ prime}} D_{\mathbb{Q}_q}(Y_1^2 + Y_2^2 + pY_3^2) \quad \text{(Minkowski)} \\
\Leftrightarrow\ & 1 + (p-1)px^2 \in D_{\mathbb{Q}_p}(Y_1^2 + Y_2^2 + pY_3^2) \\
\Leftrightarrow\ & x \in \mathbb{Z}_{(p)}.
\end{aligned}$$

□

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.
- Later generalised to arbitrary number fields by Park, 2013. Heavy machinery from class field theory.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.
- Later generalised to arbitrary number fields by Park, 2013. Heavy machinery from class field theory.
- Analogous result for global fields of odd characteristic (Eisenträger-Morrison, 2018) and characteristic 2 (D., 2021)

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.
- Later generalised to arbitrary number fields by Park, 2013. Heavy machinery from class field theory.
- Analogous result for global fields of odd characteristic (Eisenträger-Morrison, 2018) and characteristic 2 (D., 2021)
- Koenigsmann's original construction: approximately 500 quantifiers.

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.
- Later generalised to arbitrary number fields by Park, 2013. Heavy machinery from class field theory.
- Analogous result for global fields of odd characteristic (Eisenträger-Morrison, 2018) and characteristic 2 (D., 2021)
- Koenigsmann's original construction: approximately 500 quantifiers.
  - D., 2021: 37 quantifiers

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.
- Later generalised to arbitrary number fields by Park, 2013. Heavy machinery from class field theory.
- Analogous result for global fields of odd characteristic (Eisenträger-Morrison, 2018) and characteristic 2 (D., 2021)
- Koenigsmann's original construction: approximately 500 quantifiers.
  - D., 2021: 37 quantifiers
  - Sun-Zhang, 2023: 32 quantifiers

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Question: Is $\mathbb{Z}$ an $\exists^+$-definable subset of $\mathbb{Q}$?

Theorem (Koenigsmann, 2016)

$\mathbb{Q} \setminus \mathbb{Z}$ is an $\exists^+$-definable subset of $\mathbb{Q}$.

- Builds on work of Poonen, 2009.
- Number theoretic/algebraic ingredients include: Minkowski's Theorem, quaternion algebras, Quadratic Reciprocity Law.
- Later generalised to arbitrary number fields by Park, 2013. Heavy machinery from class field theory.
- Analogous result for global fields of odd characteristic (Eisenträger-Morrison, 2018) and characteristic 2 (D., 2021)
- Koenigsmann's original construction: approximately 500 quantifiers.
  - D., 2021: 37 quantifiers
  - Sun-Zhang, 2023: 32 quantifiers
  - D., 2023 (preprint): 10 quantifiers

Rings of integers

For an algebraic extension $K/\mathbb{Q}$, let $\mathcal{O}_K$ denote its ring of integers.

Conjecture

For every finite field extension $K/\mathbb{Q}$, $\text{Hil10}(\mathcal{O}_K)$ is unsolvable.

Rings of integers

For an algebraic extension $K/\mathbb{Q}$, let $\mathcal{O}_K$ denote its ring of integers.

Conjecture

For every finite field extension $K/\mathbb{Q}$, $\mathrm{Hil10}(\mathcal{O}_K)$ is unsolvable.

In each of the following cases, $\mathbb{Z}$ is $\exists^+$-definable in $\mathcal{O}_K$, hence in particular $\mathrm{Hil10}(\mathcal{O}_K)$ is unsolvable.

- K is totally real, or a quadratic extension of a totally real field (Denef-Lipschitz, 1975-1980),
- K has precisely two non-real embeddings into $\mathbb{C}$ (independently by Shlapentokh, Pheidas and Videla, 1988-1989)
- $K/\mathbb{Q}$ abelian (Shapiro-Shlapentokh, 1989).
- For a general number field K, there are results conditional on conjectures from arithmetic geometry (Poonen, 2002, Cornelissen-Pheidas-Zahidi, 2005, Garcia-Fritz-Pasten 2020, ...)

Rings of integers

For an algebraic extension $K/\mathbb{Q}$, let $\mathcal{O}_K$ denote its ring of integers.

Conjecture

For every finite field extension $K/\mathbb{Q}$, $\mathrm{Hil10}(\mathcal{O}_K)$ is unsolvable.

In each of the following cases, $\mathbb{Z}$ is $\exists^+$-definable in $\mathcal{O}_K$, hence in particular $\mathrm{Hil10}(\mathcal{O}_K)$ is unsolvable.

- K is totally real, or a quadratic extension of a totally real field (Denef-Lipschitz, 1975-1980),
- K has precisely two non-real embeddings into $\mathbb{C}$ (independently by Shlapentokh, Pheidas and Videla, 1988-1989)
- $K/\mathbb{Q}$ abelian (Shapiro-Shlapentokh, 1989).
- For a general number field K, there are results conditional on conjectures from arithmetic geometry (Poonen, 2002, Cornelissen-Pheidas-Zahidi, 2005, Garcia-Fritz-Pasten 2020, ...)

Ingredients include: Hasse-Minkowski Theorem, Pell equations, elliptic curves and other abelian varieties, ...

Function fields

Let K be a field. We call a field extension F/K a function field in one variable over K if it is finitely generated of transcendence degree 1. E.g. $F = K(X)$.

Question

Is $\mathrm{Hil10}(\mathbb{C}(X))$ *solvable? More generally, if* F *is a function field in one variable over* $\mathbb{R}$ *in which* -1 *is a sum of squares, is* $\mathrm{Hil10}(F)$ *solvable?*

We have a lot of examples of function fields over which Hilbert's 10th Problem is unsolvable, and no examples where it is solvable.

Valuation rings

A commonly used strategy involves valuation rings. For a field K, a valuation ring of K is a subring $\mathcal{O} \subseteq K$ such that, for all $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

Valuation rings

A commonly used strategy involves valuation rings. For a field K, a valuation ring of K is a subring $\mathcal{O} \subseteq K$ such that, for all $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.
E.g. $\mathbb{Z}_{(p)}$ is a valuation ring of $\mathbb{Q}$.

Valuation rings

A commonly used strategy involves valuation rings. For a field K, a valuation ring of K is a subring $\mathcal{O} \subseteq K$ such that, for all $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.
E.g. $\mathbb{Z}_{(p)}$ is a valuation ring of $\mathbb{Q}$.
E.g. A valuation ring of $K(X)$ containing K is given by

$$K[X]_{(X)} = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[X], X \nmid b \right\}.$$

Valuation rings

A commonly used strategy involves valuation rings. For a field K, a valuation ring of K is a subring $\mathcal{O} \subseteq K$ such that, for all $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.
E.g. $\mathbb{Z}_{(p)}$ is a valuation ring of $\mathbb{Q}$.
E.g. A valuation ring of $K(X)$ containing K is given by

$$K[X]_{(X)} = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[X], X \nmid b \right\}.$$

Theorem

Let F/K be a function field in one variable. If there exists a $\exists^+$-definable valuation ring $\mathcal{O}$ of F with $K \subsetneq \mathcal{O} \subsetneq F$, then Hil10$(F)$ *is unsolvable.*

Valuation rings

A commonly used strategy involves valuation rings. For a field K, a valuation ring of K is a subring $\mathcal{O} \subseteq K$ such that, for all $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.
E.g. $\mathbb{Z}_{(p)}$ is a valuation ring of $\mathbb{Q}$.
E.g. A valuation ring of $K(X)$ containing K is given by

$$K[X]_{(X)} = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[X], X \nmid b \right\}.$$

Theorem

Let F/K be a function field in one variable. If there exists a $\exists^+$-definable valuation ring $\mathcal{O}$ of F with $K \subsetneq \mathcal{O} \subsetneq F$, then Hil10($F$) is unsolvable.

- Technique pioneered by Denef in characteristic 0 (1978) and Pheidas in positive characteristic (1991), then subsequently generalised (char 0 Eisenträger and Moret-Bailly 2005-2007, pos. char Eisenträger-Shlapentokh, Pasten 2017)

Valuation rings

A commonly used strategy involves valuation rings. For a field K, a valuation ring of K is a subring $\mathcal{O} \subseteq K$ such that, for all $x \in K^\times$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.
E.g. $\mathbb{Z}_{(p)}$ is a valuation ring of $\mathbb{Q}$.
E.g. A valuation ring of $K(X)$ containing K is given by

$$K[X]_{(X)} = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[X], X \nmid b \right\}.$$

Theorem

Let F/K be a function field in one variable. If there exists a $\exists^+$-definable valuation ring $\mathcal{O}$ of F with $K \subsetneq \mathcal{O} \subsetneq F$, then Hil10($F$) *is unsolvable.*

- Technique pioneered by Denef in characteristic 0 (1978) and Pheidas in positive characteristic (1991), then subsequently generalised (char 0 Eisenträger and Moret-Bailly 2005-2007, pos. char Eisenträger-Shlapentokh, Pasten 2017)
- Uses: elliptic curves, Frobenius orbits, valuation theory, ...

Function fields

We know that Hilbert's 10th Problem is unsolvable for a function field in one variable F/K when ...

- -1 is not a sum of 4 squares in F (Denef, 1978),

Function fields

We know that Hilbert's 10th Problem is unsolvable for a function field in one variable F/K when ...

- -1 is not a sum of 4 squares in F (Denef, 1978),
- K is a subfield of $\mathbb{Q}_p$ for some odd p (Eisenträger and Moret-Bailly, 2005-2008, going back to Kim-Roush, 1995),

Function fields

We know that Hilbert's 10th Problem is unsolvable for a function field in one variable F/K when ...

- -1 is not a sum of 4 squares in F (Denef, 1978),
- K is a subfield of $\mathbb{Q}_p$ for some odd p (Eisenträger and Moret-Bailly, 2005-2008, going back to Kim-Roush, 1995),
- K is itself a function field in one variable (Eisenträger 2004-2012, going back to Kim-Roush, 1992)

Function fields

We know that Hilbert's 10th Problem is unsolvable for a function field in one variable F/K when ...

- -1 is not a sum of 4 squares in F (Denef, 1978),
- K is a subfield of $\mathbb{Q}_p$ for some odd p (Eisenträger and Moret-Bailly, 2005-2008, going back to Kim-Roush, 1995),
- K is itself a function field in one variable (Eisenträger 2004-2012, going back to Kim-Roush, 1992)
- K contains a finite field but not its algebraic closure (Eisenträger-Shlapentokh 2017, going back to Pheidas, Videla and Kim-Roush, 1991-1994)

Function fields

We know that Hilbert's 10th Problem is unsolvable for a function field in one variable F/K when ...

- -1 is not a sum of 4 squares in F (Denef, 1978),
- K is a subfield of $\mathbb{Q}_p$ for some odd p (Eisenträger and Moret-Bailly, 2005-2008, going back to Kim-Roush, 1995),
- K is itself a function field in one variable (Eisenträger 2004-2012, going back to Kim-Roush, 1992)
- K contains a finite field but not its algebraic closure (Eisenträger-Shlapentokh 2017, going back to Pheidas, Videla and Kim-Roush, 1991-1994)
- K is *large*[1] and has a separable finite field extension of degree divisible by 4, e.g. $\mathbb{C}((T))$ (Becher, D., Dittmann, in progress)

[1] large: Every smooth curve over K has either 0 or infinitely many rational points.

Function fields

We know that Hilbert's 10th Problem is unsolvable for a function field in one variable F/K when ...

- -1 is not a sum of 4 squares in F (Denef, 1978),
- K is a subfield of $\mathbb{Q}_p$ for some odd p (Eisenträger and Moret-Bailly, 2005-2008, going back to Kim-Roush, 1995),
- K is itself a function field in one variable (Eisenträger 2004-2012, going back to Kim-Roush, 1992)
- K contains a finite field but not its algebraic closure (Eisenträger-Shlapentokh 2017, going back to Pheidas, Videla and Kim-Roush, 1991-1994)
- K is *large*[1] and has a separable finite field extension of degree divisible by 4, e.g. $\mathbb{C}((T))$ (Becher, D., Dittmann, in progress)

Conjecture

Let K be a field which has a separable finite extension of degree at least 3. Then for every function field in one variable F/K, $\mathrm{Hil10}(F)$ is unsolvable.

[1] large: Every smooth curve over K has either 0 or infinitely many rational points.

Thanks for your attention!

Nicolas Daans
E-mail: nicolas.daans@matfyz.cuni.cz