Hilbert's 10th Problem and Decidability in Algebra and Number Theory

BMS Young Scholar Day

Nicolas Daans

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

20 December 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 <u>Hilbert's 10th Problem</u>.

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 is unsolvable!

That is, there can <u>never</u> 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
$\rightarrow$ too unwieldy in practice, computational requirements grow superexponentially
$\rightarrow$ search for efficient algorithms in specific cases topic of ongoing research in real algebra

Hilbert's 10th problem over a ring

Definition

Let R be a commutative ring. We say that Hilbert's 10th Problem over R with coefficients is solvable if there exists an algorithm which takes as input a polynomial with integral coefficients 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 is unsolvable.

Let us abbreviate to "Hil10(R) is solvable/unsolvable". Examples:

Hilbert's 10th problem over a ring

Definition

Let R be a commutative ring. We say that Hilbert's 10th Problem over R with coefficients is solvable if there exists an algorithm which takes as input a polynomial with integral coefficients 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 is unsolvable.

Let us abbreviate to "Hil10(R) is solvable/unsolvable". Examples:

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

Hilbert's 10th problem over a ring

Definition

Let R be a commutative ring. We say that Hilbert's 10th Problem over R with coefficients is solvable if there exists an algorithm which takes as input a polynomial with integral coefficients 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 is unsolvable.

Let us abbreviate to "Hil10(R) is solvable/unsolvable". Examples:

- Hil10($\mathbb{Z}$) is unsolvable (DPRM, 1970),
- Hil10($\mathbb{R}$) and Hil10($\mathbb{C}$) are solvable (Tarski, 1950).

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, $\mathbb{F}_q(X)$, $\mathbb{Q}^{\mathrm{ab}}$, $\mathbb{Z}^{\mathrm{ab}}$, Ω, ...	$\mathbb{Z}$, $\mathcal{O}_K$ for many number fields K (e.g. totally real or abelian), ...

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, $\mathbb{F}_q(X)$, $\mathbb{Q}^{\mathrm{ab}}$, $\mathbb{Z}^{\mathrm{ab}}$, Ω, ...	$\mathbb{Z}$, $\mathcal{O}_K$ for many number fields K (e.g. totally real or abelian), ...

Variations of the question consider algorithms which take also other coefficients than integers.

Section 2

Positive-existentially definable subsets

Positive-existentially definable subsets

Let R be a commutative ring, $n \in \mathbb{N}$. A subset A of R^n is called positive-existentially definable ($\exists$-definable) if there exists a positive-existential formula $\varphi(X_1, \ldots, X_n)$ in the language of rings with parameters from R such that

$$A = \{(x_1, \ldots, x_n) \in R^n \mid R \models \varphi(x_1, \ldots, x_n)\}.$$

Positive-existentially definable subsets

Let R be a commutative ring, $n \in \mathbb{N}$. A subset A of R^n is called positive-existentially definable ($\exists$-definable) if there exists a positive-existential formula $\varphi(X_1, \ldots, X_n)$ in the language of rings with parameters from R such that

$$A = \{(x_1, \ldots, x_n) \in R^n \mid R \models \varphi(x_1, \ldots, x_n)\}.$$

Equivalently:

Proposition

Let R be a commutative ring, $n \in \mathbb{N}$. A subset $A \subseteq R^n$ is $\exists$-definable if and only if there exist $k, m \in \mathbb{N}$ and polynomials $f_1, \ldots, f_k \in R[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$ such that

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

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

Positive-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 $=$ finite or cofinite
  E.g. $\{2,3,5\}$, $\mathbb{C} \setminus \{2,3,5\}$.

Positive-existentially definable subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$

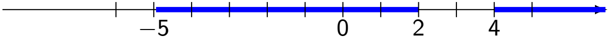
Which subsets of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are existentially definable?

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

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

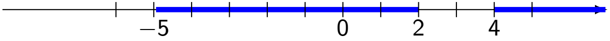


- $\mathbb{Z}$ (DPRM): Every *recursively enumerable* subset of $\mathbb{Z}^n$ is $\exists$-definable.
  E.g. the set of prime numbers, the set of 2-powers, the set of factorials, ...

Positive-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 $=$ finite or cofinite
  E.g. $\{2, 3, 5\}$, $\mathbb{C} \setminus \{2, 3, 5\}$.
- $\mathbb{R}$ (Tarski): $\exists$-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.
  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

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

∃-definable sets and complexity

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

- more ∃-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 ∃-definable.

∃-definable sets and Hilbert 10

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

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

Corollary

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

$\exists$-definable sets and Hilbert 10

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.*

Proposition

Suppose $\mathbb{Z}$ is $\exists$-definable over $\mathbb{Q}$. Then every recursively enumerable subset of $\mathbb{Q}$ is $\exists$-definable and Hil10($\mathbb{Q}$) *is unsolvable.*

$\exists$-definable sets and Hilbert 10

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.*

Proposition

Suppose $\mathbb{Z}$ is $\exists$-definable over $\mathbb{Q}$. Then every recursively enumerable subset of $\mathbb{Q}$ is $\exists$-definable and $\mathrm{Hil10}(\mathbb{Q})$ *is unsolvable.*

Question

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

Section 3

∃-definability and subrings of fields

∃-definable subrings of $\mathbb{Q}$

It is possible for subrings (e.g. of $\mathbb{Q}$) to be ∃-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 ∃-definable in $\mathbb{Q}$ ("essentially" due to Robinson, 1949).

∃-definable subrings of $\mathbb{Q}$

It is possible for subrings (e.g. of $\mathbb{Q}$) to be ∃-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 ∃-definable in $\mathbb{Q}$ ("essentially" due to Robinson, 1949).
For example:

Proposition

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

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

∃-definable subrings of $\mathbb{Q}$

It is possible for subrings (e.g. of $\mathbb{Q}$) to be ∃-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 ∃-definable in $\mathbb{Q}$ ("essentially" due to Robinson, 1949).
For example:

Proposition

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

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

<u>Proof idea:</u>

- By Minkowski's Theorem, the quadratic form $Y_1^2 + Y_2^2 + pY_3^3$ represents an element of $\mathbb{Q}$ over $\mathbb{Q}$ if and only if it does so over $\mathbb{R}$ and $\mathbb{Q}_q$ for each prime q.
- The local cases can be understood entirely via Hensel's Lemma.

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.
- Subsequently generalised to arbitrary global fields (Park 2013, Eisenträger-Morrison 2018, D. 2021).

Subrings of $\mathbb{Q}$

A concrete formula:

Theorem

Let $q \in \mathbb{Q}$. We have that $q \in \mathbb{Q} \setminus \mathbb{Z}$ if and only if

$$\exists a, b, t, x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3 \in \mathbb{Q} :$$

$$7\left(\left(\frac{a^2+1}{a}\right)^2 + \frac{(a^2+1)(b^2+1)}{ab} + \left(\frac{b^2+1}{b}\right)^2\right) + 2 = x_1^2 + x_2^2 + x_3^2,$$

$$(t^2 - (1+4a^2)y_1^2 - 2by_2^2 + (1+4a^2)2by_3^2 - 4)(7 + 4q^2(2 - y_1^2 - y_2^2 - y_3^2)) = 0, \ \textit{and}$$

$$\left(\frac{a^2}{q^2 - q - a^2}\left(\frac{16a^4}{1+4a^2} - \left(\frac{(b-1)^2}{b}\right)^2\right) - t\right)^2 - (1+4a^2)z_1^2 - 2bz_2^2 + (1+4a^2)2bz_3^2 = 4$$

Subrings of $\mathbb{Q}$

A concrete formula:

Theorem

Let $q \in \mathbb{Q}$. We have that $q \in \mathbb{Q} \setminus \mathbb{Z}$ if and only if

$$\exists a, b, t, x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3 \in \mathbb{Q} :$$

$$7\left(\left(\frac{a^2+1}{a}\right)^2 + \frac{(a^2+1)(b^2+1)}{ab} + \left(\frac{b^2+1}{b}\right)^2\right) + 2 = x_1^2 + x_2^2 + x_3^2,$$

$$(t^2 - (1+4a^2)y_1^2 - 2by_2^2 + (1+4a^2)2by_3^2 - 4)(7 + 4q^2(2 - y_1^2 - y_2^2 - y_3^2)) = 0, \text{ and}$$

$$\left(\frac{a^2}{q^2 - q - a^2}\left(\frac{16a^4}{1+4a^2} - \left(\frac{(b-1)^2}{b}\right)^2\right) - t\right)^2 - (1+4a^2)z_1^2 - 2bz_2^2 + (1+4a^2)2bz_3^2 = 4$$

Question

How simple could the description of $\mathbb{Q} \setminus \mathbb{Z}$ in $\mathbb{Q}$ as an $\exists$-definable subset be? E.g. how few quantifiers?

Function fields

For a field K, we can consider the polynomial ring $K[X]$ and field of rational function $K(X)$.

Function fields

For a field K, we can consider the polynomial ring $K[X]$ and field of rational function $K(X)$. We consider a variation of Hilbert's 10th Problem over $K(X)$:

Question ('Geometric' Hilbert's 10th Problem over $K(X)$)

Let K be a field. Is there an algorithm which takes as input a polynomial with coefficients in $\mathbb{Z}[X]$ and outputs YES if the polynomial has a zero in $K(X)$, and NO otherwise?

Function fields

For a field K, we can consider the polynomial ring $K[X]$ and field of rational function $K(X)$.
We consider a variation of Hilbert's 10th Problem over $K(X)$:

Question ('Geometric' Hilbert's 10th Problem over $K(X)$)

Let K be a field. Is there an algorithm which takes as input a polynomial with coefficients in $\mathbb{Z}[X]$ and outputs YES if the polynomial has a zero in $K(X)$, and NO otherwise?

No examples known of fields K for which the answer is positive.
Most mysterious case: $K = \mathbb{C}$.

Valuation rings

Strategy: find existentially definable subrings of $K(X)$.
E.g. Consider in $K(X)$ the subring

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

Like $\mathbb{Z}_{(p)}$, this is a discrete valuation ring (= local principal ideal domain).

Valuation rings

Strategy: find existentially definable subrings of $K(X)$.
E.g. Consider in $K(X)$ the subring

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

Like $\mathbb{Z}_{(p)}$, this is a discrete valuation ring (= local principal ideal domain).

- Existential definability of subrings of $K(X)$ can be used to establish negative solutions to the Geometric Hilbert's 10th Problem over $K(X)$

Valuation rings

Strategy: find existentially definable subrings of $K(X)$.
E.g. Consider in $K(X)$ the subring

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

Like $\mathbb{Z}_{(p)}$, this is a discrete valuation ring ($=$ local principal ideal domain).

- Existential definability of subrings of $K(X)$ can be used to establish negative solutions to the Geometric Hilbert's 10th Problem over $K(X)$
- 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

Strategy: find existentially definable subrings of $K(X)$.
E.g. Consider in $K(X)$ the subring

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

Like $\mathbb{Z}_{(p)}$, this is a discrete valuation ring (= local principal ideal domain).

- Existential definability of subrings of $K(X)$ can be used to establish negative solutions to the Geometric Hilbert's 10th Problem over $K(X)$
- 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, valuation theory, extensions of DPRM Theorem, ...

Function fields

Geometric Hilbert's 10th Problem for $K(X)$ is unsolvable when

- $K \subseteq \mathbb{R}$ (Denef, 1978),

Function fields

Geometric Hilbert's 10th Problem for $K(X)$ is unsolvable when

- $K \subseteq \mathbb{R}$ (Denef, 1978),
- $K \subseteq \mathbb{Q}_p$ for some prime p (Eisenträger and Moret-Bailly, 2005-2008, Degroote and Demeyer 2012, going back to Kim-Roush, 1995),

Function fields

Geometric Hilbert's 10th Problem for $K(X)$ is unsolvable when

- $K \subseteq \mathbb{R}$ (Denef, 1978),
- $K \subseteq \mathbb{Q}_p$ for some prime p (Eisenträger and Moret-Bailly, 2005-2008, Degroote and Demeyer 2012, going back to Kim-Roush, 1995),
- $\mathbb{F}_p \subseteq K$ but $\overline{\mathbb{F}_p} \not\subseteq K$ (Eisenträger-Shlapentokh 2017, going back to Pheidas, Videla and Kim-Roush, 1991-1994),

Function fields

Geometric Hilbert's 10th Problem for $K(X)$ is unsolvable when

- $K \subseteq \mathbb{R}$ (Denef, 1978),
- $K \subseteq \mathbb{Q}_p$ for some prime p (Eisenträger and Moret-Bailly, 2005-2008, Degroote and Demeyer 2012, going back to Kim-Roush, 1995),
- $\mathbb{F}_p \subseteq K$ but $\overline{\mathbb{F}_p} \not\subseteq K$ (Eisenträger-Shlapentokh 2017, going back to Pheidas, Videla and Kim-Roush, 1991-1994),
- $\mathbb{Q} \subseteq K$, $K \cap \overline{\mathbb{Q}} \not\subseteq K^{(2)}$, and K is *large*[1] (Becher, D., and Dittmann 2023), e.g. $K = \mathbb{Q}_p^{\text{unr}}$.

Function fields

Geometric Hilbert's 10th Problem for $K(X)$ is unsolvable when

- $K \subseteq \mathbb{R}$ (Denef, 1978),
- $K \subseteq \mathbb{Q}_p$ for some prime p (Eisenträger and Moret-Bailly, 2005-2008, Degroote and Demeyer 2012, going back to Kim-Roush, 1995),
- $\mathbb{F}_p \subseteq K$ but $\overline{\mathbb{F}_p} \not\subseteq K$ (Eisenträger-Shlapentokh 2017, going back to Pheidas, Videla and Kim-Roush, 1991-1994),
- $\mathbb{Q} \subseteq K$, $K \cap \overline{\mathbb{Q}} \not\subseteq K^{(2)}$, and K is *large*[1] (Becher, D., and Dittmann 2023), e.g. $K = \mathbb{Q}_p^{\mathrm{unr}}$.

Conjecture

Let K be a field with $\mathbb{Q} \subseteq K$, $\overline{\mathbb{Q}} \not\subseteq K$. Then Geometric Hilbert's 10th Problem for $K(X)$ 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