Decidability in local and global fields

Jochen Koenigsmann
Oxford

ICM 2018
Rio de Janeiro

Plan

1 Introduction
Local and global fields
Local-global principles
Decidability and Hilbert's 10th Problem

2 Local fields of characteristic $p > 0$
The existential theory of $\mathbb{F}_q((t))$
Axiomatizing $\mathbb{F}_q((t))$

3 Global fields
Defining $\mathbb{Z}$ in $\mathbb{Q}$
Global function fields

4 Infinite algebraic extensions
... of $\mathbb{Q}$
Two infinite extensions of $\mathbb{Q}_p$

5 Decidability under finite extensions
On a question of Abraham Robinson's
... and on the question he didn't ask

6 Outlook

1 Introduction

1.1 Local and global fields

global fields: finite extensions of

$$\begin{cases} \mathbb{Q} & \text{(number fields)} \\ \mathbb{F}_p(t) & \text{(function fields)} \end{cases}$$

local fields:

- archimedean $\begin{cases} \mathbb{R} \\ \mathbb{C} \end{cases}$

- non-archimedean

$$\begin{cases} \mathbb{Q}_p & \text{and finite extensions} \\ \mathbb{F}_q((t)) \end{cases}$$

= completions of global fields
= fields locally compact
w.r.t. some non-trivial absolute value

1.2 Local-global principles

K	a global field
S_K	the set of all absolute values v on K
K_v	the completion of K w.r.t. v
$\mathcal{P}$	any property of fields

The local-global principle (LGP) for $\mathcal{P}$:

$$K \models \mathcal{P} \iff K_v \models \mathcal{P} \text{ for all } v \in S_K$$

1.2 Local-global principles

K	a global field
S_K	the set of all absolute values v on K
K_v	the completion of K w.r.t. v
$\mathcal{P}$	any property of fields

The local-global principle (LGP) for $\mathcal{P}$:

$$K \models \mathcal{P} \iff K_v \models \mathcal{P} \text{ for all } v \in S_K$$

Examples

- p prime, $a \in \mathbb{Z}$, $\mathcal{P} \sim \exists\, x:\ x^p = a$
- Hasse-Minkowski LGP for quadratic forms

Counterexample (Selmer 1951)
$K = \mathbb{Q}$, $\mathcal{P} \sim \exists\, x, y:\ 3x^3 + 4y^3 = 5$

1.3 Decidability and Hilbert's 10th Problem

R	any integral domain or field
$\mathsf{Th}(R)$	the first-order theory of R in $\mathcal{L}_{ring} = \{+, \cdot; 0, 1\}$
$\mathsf{Th}_\exists(R)$	the existential first-order theory of R

R **decidable** $\iff$ $\mathsf{Th}(R)$ decidable

$\iff$ $\mathsf{Th}(R)$ effectively axiomatizable

1.3 Decidability and Hilbert's 10th Problem

R	any integral domain or field
$\mathrm{Th}(R)$	the first-order theory of R in $\mathcal{L}_{ring} = \{+, \cdot; 0, 1\}$
$\mathrm{Th}_\exists(R)$	the existential first-order theory of R

R **decidable** $\iff$ $\mathrm{Th}(R)$ decidable

$\iff$ $\mathrm{Th}(R)$ effectively axiomatizable

Hilbert's 10th Problem over R

Find an algorithm

which on `INPUT:` $f \in \mathbb{Z}[X_1, \ldots, X_n]$

gives `OUTPUT:` $\begin{cases} \texttt{YES} & \text{if } \exists\, \overline{x} \in R^n \text{ s.t. } f(\overline{x}) = 0 \\ \texttt{NO} & \text{otherwise} \end{cases}$

(Hilbert's original (ICM Paris 1900) for $R = \mathbb{Z}$)

Note: H10/R solvable $\iff$ $\mathrm{Th}_{\exists(+)}(R)$ decidable

R	$\mathsf{Th}(R)$	$\mathsf{Th}_\exists(R)$
$\mathbb{R}$	$+$ $(Tarski)$	$+$
$\mathbb{C}$	$+$ $(Tarski)$	$+$
$\mathbb{Q}_p$	$+$ $(Ax\text{-}Kochen/$	$+$
$\mathbb{Z}_p$	$+$ $Ershov$ '65)	$+$
$\mathbb{F}_p((t))$	? $\rightsquigarrow$	$+$ $(Anscombe\text{-}Fehm$ '16)
$\mathbb{F}_p[[t]]$	?	$+$ $(Anscombe\text{-}K.$ '14)

R	$\mathsf{Th}(R)$	$\mathsf{Th}_\exists(R)$
$\mathbb{R}$	$+$ $(Tarski)$	$+$
$\mathbb{C}$	$+$ $(Tarski)$	$+$
$\mathbb{Q}_p$	$+$ $(Ax\text{-}Kochen/$	$+$
$\mathbb{Z}_p$	$+$ $Ershov$ '65)	$+$
$\mathbb{F}_p((t))$	? $\rightsquigarrow$	$+$ $(Anscombe\text{-}Fehm$ '16)
$\mathbb{F}_p[[t]]$	?	$+$ $(Anscombe\text{-}K.$ '14)
$\mathbb{Q}$	$-$ $(J.Robinson$ '49)	? $\rightsquigarrow$ $(K.$'16)
$\mathbb{Z}$	$-$ $(Gödel)$	$-$ $(Matyiasevich$ '70)
$\mathbb{F}_p(t)$	$-$	$-$ $(Pheidas$ '91)
$\mathbb{F}_p[t]$	$-$	$-$ $(Denef$ '79) $\rightsquigarrow$

2 Local fields of char. $p > 0$

2.1 The existential theory of $\mathbb{F}_q((t))$

Denef-Shoutens (2003)
$\mathrm{Th}_{\exists,\, t}\, \mathbb{F}_q((t))$ *in* $\mathcal{L}_{ring} \cup \{t\}$ *is decidable* **modulo** *resolution of singularities in characteristic* p*.*

Anscombe-Fehm (2016)
$\mathrm{Th}_{\exists}\, \mathbb{F}_q((t))$ *(in* $\mathcal{L}_{ring}$*) is decidable.*
Proof:

$$\bigcup_{i=1}^{\infty} K_i = \overline{\mathbb{F}_q((t))} \cap \mathbb{F}_q((\mathbb{Q})) \preceq \mathbb{F}_q((\mathbb{Q}))$$

where $\mathbb{F}_q((\mathbb{Q}))$ is tame (AKE), hence decidable, and the K_i are finite over, hence $\cong \mathbb{F}_q((t))$.$\square$

Anscombe-K. (2014)
$\mathbb{F}_q[[t]]$ *is* $\exists$*-definable in* $\mathbb{F}_q((t))$ *(no parameters).*

Corollary: $\mathrm{Th}_{\exists}\, \mathbb{F}_q[[t]]$ *is decidable.*

2.2 Axiomatizing $\mathbb{F}_q((t))$

Definition (Ershov, Starchenko, Kuhlmann, ...)
A valued field (K, v) *with valuation ring* $\mathcal{O}_v$
is called **extremal** *if, for every* $f \in K[X_1, \ldots, X_n]$,

$$\{v(f(\overline{a})) \mid \overline{a} \in \mathcal{O}_v^n\} \cup \{\infty\}$$

has a maximal element.

$\Rightarrow$ (K, v) algebr.$^{\text{y}}$ max.: '$e \cdot f = n$' ($\Rightarrow$ henselian)
... & value group divisible or $\equiv \mathbb{Z}$.

2.2 Axiomatizing $\mathbb{F}_q((t))$

Definition (Ershov, Starchenko, Kuhlmann, ...)
A valued field (K, v) with valuation ring $\mathcal{O}_v$ is called **extremal** *if, for every $f \in K[X_1, \ldots, X_n]$,*

$$\{v(f(\overline{a})) \mid \overline{a} \in \mathcal{O}_v^n\} \cup \{\infty\}$$

has a maximal element.

$\Rightarrow$ (K, v) algebr.$^{\text{y}}$ max.: '$e \cdot f = n$' ($\Rightarrow$ henselian)
... & value group divisible or $\equiv \mathbb{Z}$.

Let Σ be the $\mathcal{L}_{ring}$-theory of extremal valued fields of characteristic $p > 0$
with residue field $\mathbb{F}_q$ and value group $\equiv \mathbb{Z}$.
(N.B.: in such fields $\mathcal{O}_v$ is $\mathcal{L}_{ring}$-definable).

Conjecture (Ershov, Kuhlmann, ...)
Σ *axiomatizes* $\mathbb{F}_q((t))$.

`work in progress (Rigler-K.) on QE for` Σ `in` $\mathcal{L}_{Mac}^{+}$

3 Global fields

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

Q: Is $\mathbb{Z}$ **diophantine** (i.e., $\exists$-definable) in $\mathbb{Q}$?

If yes, then

- H10/$\mathbb{Q}$ is not solvable ($\mathrm{Th}_{\exists}(\mathbb{Q})$ undecidable)
- $\mathbb{Z}$ is $\forall$-definable in $\mathbb{Q}$
- irreducibility of polyonomials is dioph. in $\mathbb{Q}$.

3 Global fields

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

Q: Is $\mathbb{Z}$ **diophantine** (i.e., $\exists$-definable) in $\mathbb{Q}$?

If yes, then

- H10/$\mathbb{Q}$ is not solvable ($\mathrm{Th}_\exists(\mathbb{Q})$ undecidable)
- $\mathbb{Z}$ is $\forall$-definable in $\mathbb{Q}$
- irreducibility of polyonomials is dioph. in $\mathbb{Q}$.

Theorem (K. 2016) $\mathbb{Z}$ **is** $\forall$*-definable in* $\mathbb{Q}$:
there is a polynomial $g \in \mathbb{Z}[T; X_1, \ldots, X_{418}]$
such that, for all $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \text{ iff } \forall\, \overline{x} \in \mathbb{Q}^{418}\ g(t; \overline{x}) \neq 0.$$

$\star$ generalised to number fields by Park (2013)

$\star$ reduced to 146 $\forall$'s by Daans (2018)

Theorem (Dittmann 2018)
Irreducibility in global fields **is** *diophantine.*

3.2 Global function fields

Pheidas (1991)
H10/$\mathbb{F}_p(t)$ *is not solvable.*

Demeyer (2007)
The DPRM-Theorem holds for $\mathbb{F}_p[t]$*.*
In particular, H10/$\mathbb{F}_p[t]$ *is not solvable (Denef 1979).*

Open: Is $\mathbb{F}_p[t]$ definable by an $\exists$-$(\mathcal{L}_{ring} \cup \{t\})$-formula in $\mathbb{F}_p(t)$?

Eisentraeger-Morrison (2018), **Tyrrell** (2018)
$\mathbb{F}_p[t]$ *is definable by a* $\forall$-$(\mathcal{L}_{ring} \cup \{t\})$-*formula in* $\mathbb{F}_p(t)$ *using 175* $\forall$*'s.*

4 Infinite algebraic extensions

4.1 ... of $\mathbb{Q}$

R	$\mathsf{Th}(R)$	$\mathsf{Th}_\exists(R)$
$\mathbb{Q}^{tot.r.}$	$+$ ($Moret$-$Bailly$ '89 $Fried$-$Haran$-$Völklein$ '94)	$+$
$\mathbb{Z}^{tot.r.}$	$-$ ($Julia\ \ Robinson$ '62)	?
$\mathbb{Q}^{ab}$	?	?
$\mathbb{Q}^{solv}$	$+$ $modulo\ \ Shafarevich\ \ Conj.$ & $assuming\ \mathbb{Q}^{solv}\ \ is\ \ PAC$ (K.-$Singer$ '14)	$+$ $modulo\ \ldots$

(K is **PAC** if every absolutely irreducible variety over K has a K-rational point)

4.2 Two infinite extensions of $\mathbb{Q}_p$

Ziegler (1972), **Derakhshan-Macintyre** (2016)
$\mathbb{Q}_p^{ur}$ *is decidable and model-complete.*

$\mathbb{Q}_p^{ur}$ is axiomatized as (1) a henselian field with
(2) residue field algebraically closed of char. p
(3) value group $\equiv \mathbb{Z}$
(4) $v(p)$ minimal positive.

4.2 Two infinite extensions of $\mathbb{Q}_p$

Ziegler (1972), **Derakhshan-Macintyre** (2016)
$\mathbb{Q}_p^{ur}$ is decidable and model-complete.

$\mathbb{Q}_p^{ur}$ is axiomatized as (1) a henselian field with
(2) residue field algebraically closed of char. p
(3) value group $\equiv \mathbb{Z}$
(4) $v(p)$ minimal positive.

Conjecture (K. 2017) *$\mathbb{Q}_p^{ab}$ is decidable, axiomatized as (1) a henselian field with*
(2) residue field algebraically closed of char. p
(3) value group $\equiv \frac{1}{p^\infty}\mathbb{Z}$
(4) $q \nmid v(1-\zeta_p)$ for any prime $q \neq p$
(5) $K \cap \overline{\mathbb{Q}} = \mathbb{Q}_p^{ab} \cap \overline{\mathbb{Q}}$
(6) $v = v_K^p$, the canonical *p-hens. val. on K*
(7) Frobenius $x \mapsto x^p$ is surjective on $\mathcal{O}_v/p\,\mathcal{O}_v$.

These axioms are $\mathcal{L}_{ring}$-expressible (Jahnke-K. 2015 for *(6)*) and independent (K. 2017).

5 Decidability under finite extensions

5.1 On a question of Abraham Robinson's

Question (A. Robinson 1973)
Is a finite extension of an undecidable field always undecidable?

Cherlin-vdDries-Macintyre (1980), **K.** (2013)
No: There is an 'outlandish' undecidable field K (of infinite t.d./$\mathbb{Q}$) s.t. all proper finite L/K are isomorphic and decidable (CDM).
There are also counterexamples L/K algebraic over $\mathbb{Q}$ (K.).

Known: $\mathbb{R}(t)$ is undecidable (Denef 1978).

Open: Is $\mathbb{C}(t)$ decidable?

If yes, then $\mathbb{C}(t)/\mathbb{R}(t)$ is the most canonical witness for a negative answer to Abraham Robinson.

5.2 ... and on the qu. he didn't ask

Question (K. 2013) *Is a finite extension of a decidable field always decidable?*

K.-Thanagopal (2017) *No.*

Proof: uses Ershov's **wonderful extension** W of $\mathbb{Q}$:
W is a field with embeddings $\lambda_p : W \to \mathbb{Q}_p$ ($p \in \mathbb{P} \cup \{\infty\}$) inducing a unique p-adic val. (resp. ordering) v_p on W s.t.

(i) if $x \in W^\times$ then $x \in \mathcal{O}_{v_p}^\times$ for almost all p,

(ii) W satisfies LGP w.r.t. $(v_p)_p$ for rational points on varieties over W,

(iii) W is algebraically maximal with (i) and (ii).

Such a W exists, W is decidable and $W \cap \overline{\mathbb{Q}} = \mathbb{Q}$.

Now choose $K \succeq W$ saturated, $\mathcal{S} \subset \mathbb{P}$ non-recursive, $d \in K$ with $v_p(d)$ odd iff $p \in \mathcal{S}$ and let $L = K(\sqrt{d})$.
Then K is decidable and L is undecidable.□

Express outlook

13/12

Express outlook

Agenda for the next 4 years

(1) Show that H10/$\mathbb{Q}$ is not solvable.

(2) Find out whether $\mathbb{Z}$ is diophantine in $\mathbb{Q}$.

(3) Prove decidability of $\mathbb{F}_p((t))$
[and of $\mathrm{Th}_{\exists,t}\,\mathbb{F}_p((t))$].

(4) Is $\mathbb{C}(t)$ decidable?

(5) Is $\mathbb{Q}^{solv}$ PAC?

(6) Verify that $\mathbb{Q}_p^{ab}$ is decidable.