A universal definition of $\mathbb{Z}$ in $\mathbb{Q}$

Nicolas Daans

University of Antwerp

October 15, 2020

Existential and universal definitions in number theory

Let $\mathcal{L}$ always be the first-order language of rings.
Let K be a field. Which subrings of K are (existentially, universally) $\mathcal{L}_K$-definable in K?

Existential and universal definitions in number theory

Let $\mathcal{L}$ always be the first-order language of rings.
Let K be a field. Which subrings of K are (existentially, universally) $\mathcal{L}_K$-definable in K?

Question 1.1

Does $\mathbb{Z}$ have an existential $\mathcal{L}$-definition in $\mathbb{Q}$?

If the answer were yes, it would follow from the undecidability of $\mathrm{Th}_{\exists}(\mathbb{Z})$ that the existential first-order theory of $\mathbb{Q}$ is also undecidable.

Existential and universal definitions in number theory

Let $\mathcal{L}$ always be the first-order language of rings.
Let K be a field. Which subrings of K are (existentially, universally) $\mathcal{L}_K$-definable in K?

Question 1.1

Does $\mathbb{Z}$ have an existential $\mathcal{L}$-definition in $\mathbb{Q}$?

If the answer were yes, it would follow from the undecidability of $\mathrm{Th}_\exists(\mathbb{Z})$ that the existential first-order theory of $\mathbb{Q}$ is also undecidable.

Theorem 1.2 (J. Robinson, 1949)

$\mathbb{Z}$ has a first-order $\mathcal{L}$-definition in $\mathbb{Q}$.

It then follows from the undecidability of $\mathrm{Th}(\mathbb{Z})$ that the first-order theory of $\mathbb{Q}$ is undecidable.

Existential and universal definitions in number theory

Implicitly from Robinson's work, we also get:

Proposition 1.3

For every prime number p the ring

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}$$

has an existential definition in $\mathbb{Q}$.

Existential and universal definitions in number theory

Implicitly from Robinson's work, we also get:

Proposition 1.3

For every prime number p the ring

$$\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid v_p(x) \geq 0\}$$

has an existential definition in $\mathbb{Q}$.

Theorem 1.4 (Poonen, 2009)

$\mathbb{Z}$ has an $\forall\exists\mathcal{L}$-definition in $\mathbb{Q}$.

Theorem 1.5 (Koenigsmann, 2016)

$\mathbb{Z}$ has a universal $\mathcal{L}$-definition in $\mathbb{Q}$.

Theorem 1.5 (Koenigsmann, 2016)

$\mathbb{Z}$ has a universal $\mathcal{L}$-definition in $\mathbb{Q}$.

Theorem 1.6 (Park, 2013)

Let K be a number field. The ring of integers $\mathcal{O}_K$ has a universal $\mathcal{L}$-definition in K.

Existential and universal definitions in number theory

Let K be a global field (number field or function field in one variable over a finite field).
Denote by $\mathcal{V}(K)$ the set of all $\mathbb{Z}$-valuations on K. For a finite subset $S \subseteq \mathcal{V}(K)$, define the *ring of S-integers* of K to be

$$\mathcal{O}_S = \bigcap_{v \in \mathcal{V}(K) \setminus S} \mathcal{O}_v.$$

Existential and universal definitions in number theory

Let K be a global field (number field or function field in one variable over a finite field).
Denote by $\mathcal{V}(K)$ the set of all $\mathbb{Z}$-valuations on K. For a finite subset $S \subseteq \mathcal{V}(K)$, define the *ring of S-integers* of K to be

$$\mathcal{O}_S = \bigcap_{v \in \mathcal{V}(K) \setminus S} \mathcal{O}_v.$$

Theorem 1.7 (Eisenträger-Morrison, 2018)

Let K be a global function field of odd characteristic. For any finite $S \subseteq \mathcal{V}(K)$, $\mathcal{O}_S$ has a universal $\mathcal{L}_K$-definition in K.

E.g. $\mathbb{F}_q[T]$ has a universal definition in $\mathbb{F}_q(T)$.

Outline

Plan for the rest of the talk:

- Give a proof of Koenigsmann's Theorem (universal definability of $\mathbb{Z}$ in $\mathbb{Q}$).

Outline

Plan for the rest of the talk:

- Explain how (properties of) quaternion algebras over global and local fields play a role, building on ideas of Poonen & Koenigsmann.
- Give a proof of Koenigsmann's Theorem (universal definability of $\mathbb{Z}$ in $\mathbb{Q}$).

Outline

Plan for the rest of the talk:

- Explain how (properties of) quaternion algebras over global and local fields play a role, building on ideas of Poonen & Koenigsmann.
- Give a proof of Koenigsmann's Theorem (universal definability of $\mathbb{Z}$ in $\mathbb{Q}$).
- Discuss generalisations to other global fields and function fields

The ramification set

Denote by $\mathbb{P}$ the set of prime numbers and set $\mathbb{P}' = \mathbb{P} \cup \{\infty\}$.
Define $\mathbb{Q}_\infty = \mathbb{R}$.
For $a, b \in \mathbb{Q}^\times$, define the *ramification set* of the quaternion algebra $(a, b)_\mathbb{Q}$:

$$\Delta(a, b) = \{p \in \mathbb{P}' \mid (a, b)_{\mathbb{Q}_p} \text{ is non-split}\}.$$

The ramification set

Denote by $\mathbb{P}$ the set of prime numbers and set $\mathbb{P}' = \mathbb{P} \cup \{\infty\}$.
Define $\mathbb{Q}_\infty = \mathbb{R}$.
For $a, b \in \mathbb{Q}^\times$, define the *ramification set* of the quaternion algebra $(a, b)_\mathbb{Q}$:

$$\Delta(a, b) = \{p \in \mathbb{P}' \mid (a, b)_{\mathbb{Q}_p} \text{ is non-split}\}.$$

Recall: $(a, b)_\mathbb{Q} \cong (ac^2, bd^2)_\mathbb{Q}$ for $a, b, c, d \in \mathbb{Q}^\times$, whence $\Delta(a, b) = \Delta(ac^2, bd^2)$.

The ramification set

The ramification set can be computed precisely as follows:

Proposition 2.1 (Computation of the ramification set)

Let $a, b \in \mathbb{Z} \setminus \{0\}$ be square-free.

1. $\infty \in \Delta(a, b)$ *if and only if* $a < 0$ *and* $b < 0$.
2. *For* $p \in \mathbb{P} \setminus \{2\}$ *we have* $p \in \Delta(a, b)$ *if and only if one of the following holds*
   - $v_p(a) = 1$, $v_p(b) = 0$ *and* b *is not a square mod* p
   - $v_p(a) = 0$, $v_p(b) = 1$ *and* a *is not a square mod* p
   - $v_p(a) = 1 = v_p(b)$ *and* $-ab$ *is not a square mod* p
3. *If* $v_2(b) = 1$ *and* $a \equiv 5 \bmod 8$, *then* $2 \in \Delta(a, b)$.
4. *(Hilbert Reciprocity)* $|\Delta(a, b)|$ *is an even natural number.*

Note: we can scale any $a, b \in \mathbb{Q}^\times$ by a square to obtain square-free elements of $\mathbb{Z} \setminus \{0\}$.

The ramification set

Lemma 2.2

Let p, q be odd prime numbers such that $q \equiv 5 \bmod 8$ and p is not a square modulo q. We have:

$$\Delta(q, 2p) = \{2, p\}.$$

Proof: Follows from computation rules. □

The ramification set

Lemma 2.2

Let p, q be odd prime numbers such that $q \equiv 5 \bmod 8$ and p is not a square modulo q. We have:

$$\Delta(q, 2p) = \{2, p\}.$$

Proof: Follows from computation rules. □

Corollary 2.3

For every odd prime number p we can find $a \in \mathbb{Z}_{(2)}^{\times}$ such that $\Delta(1 + 4a^2, 2p) = \{2, p\}$.

Proof:

Existentially definable semilocal building blocks

For $a, b, c \in \mathbb{Q}^\times$, define

$$\Delta^c(a, b) = \{p \in \Delta(a, b) \cap \mathbb{P} \mid v_p(c) \text{ is odd}\}$$

and for $a, b, c \in \mathbb{Q}^\times$, set

$$J^c(a, b) = \bigcap_{p \in \Delta^c(a,b)} p\mathbb{Z}_{(p)}.$$

Existentially definable semilocal building blocks

For $a, b, c \in \mathbb{Q}^\times$, define

$$\Delta^c(a, b) = \{p \in \Delta(a, b) \cap \mathbb{P} \mid v_p(c) \text{ is odd}\}$$

and for $a, b, c \in \mathbb{Q}^\times$, set

$$J^c(a, b) = \bigcap_{p \in \Delta^c(a,b)} p\mathbb{Z}_{(p)}.$$

Proposition 2.4

There exists an existential $\mathcal{L}$-formula ψ in 4 free variables such that for all $a, b, c \in \mathbb{Q}^\times$ we have

$$J^c(a, b) = \{x \in K \mid K \models \psi(x, a, b, c)\}$$

Relies on work by Poonen, Koenigsmann.

Existential to universal

The following observation (implicit in Koenigsmann's work) links uniform existential definability of prime ideals with universal definability.

Lemma 3.1

If $\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)}$ has an existential $\mathcal{L}$-definition in $\mathbb{Q}$, then $\mathbb{Z}$ has a universal $\mathcal{L}$-definition in $\mathbb{Q}$.

Proof:

Proof of main theorem

Proposition 3.2

Setting

$$\Phi = \{(1 + 4a^2, 2b) \mid a, b \in \mathbb{Z}_{(2)}^{\times}\}$$

we have

$$\bigcup_{p \in \mathbb{P}} p\mathbb{Z}_{(p)} = \left(\bigcup_{(x,y) \in \Phi} J^x(x, y) \cap J^{2y}(x, y) \right) \cup 2\mathbb{Z}_{(2)}.$$

Proof:

Proof of main theorem

Proof of Theorem 1.5:

Generalisation to all global fields

The following ingredients extend verbatim to global fields:

- existential definability of valuation rings and intersections of valuation ideals indexed by ramification sets,

Generalisation to all global fields

The following ingredients extend verbatim to global fields:

- existential definability of valuation rings and intersections of valuation ideals indexed by ramification sets,
  - basis for results by Park and Eisenträger-Morrison

Generalisation to all global fields

The following ingredients extend verbatim to global fields:

- existential definability of valuation rings and intersections of valuation ideals indexed by ramification sets,
  - basis for results by Park and Eisenträger-Morrison
- Hilbert Reciprocity and converse

Generalisation to all global fields

The following ingredients extend verbatim to global fields:

- existential definability of valuation rings and intersections of valuation ideals indexed by ramification sets,
  - basis for results by Park and Eisenträger-Morrison
- Hilbert Reciprocity and converse

Theorem 4.1

Let K be a global field. For any finite $S \subseteq \mathcal{V}(K)$, $\mathcal{O}_S$ has a universal $\mathcal{L}_K$-definition in K.

Generalisation to all global fields

The following ingredients extend verbatim to global fields:

- existential definability of valuation rings and intersections of valuation ideals indexed by ramification sets,
  - basis for results by Park and Eisenträger-Morrison
- Hilbert Reciprocity and converse

Theorem 4.1

Let K be a global field. For any finite $S \subseteq \mathcal{V}(K)$, $\mathcal{O}_S$ has a universal $\mathcal{L}_K$-definition in K.

- Construction yields formulae with 50 universal quantifiers. With a bit more work, one can get down to 38 quantifiers.

Generalisation to all global fields

- Rings of S-integers of a global field K are precisely integrally closed, finitely generated subrings of K with K as fraction field.

Generalisation to all global fields

- Rings of S-integers of a global field K are precisely integrally closed, finitely generated subrings of K with K as fraction field.
- In fact, one can obtain the following (suggested by Dittmann):

Corollary 4.2

Any finitely generated domain with a global field K as fraction field has a universal $\mathcal{L}_K$-definition in K.

Abstraction of the question

We used that $\mathbb{Z} = \bigcap_{p \in \mathbb{P}} \mathbb{Z}_{(p)}$, i.e. $\mathbb{Z}$ is the intersection of all discrete valuations rings of $\mathbb{Q}$.

Question 4.3

Given a field K, which intersections of valuation rings can we define universally?

Abstraction of the question

We used that $\mathbb{Z} = \bigcap_{p\in\mathbb{P}} \mathbb{Z}_{(p)}$, i.e. $\mathbb{Z}$ is the intersection of all discrete valuations rings of $\mathbb{Q}$.

Question 4.3

Given a field K, which intersections of valuation rings can we define universally?

There are two key ingredients in our proof:

- Existential definability of $\bigcap_{v\in\Delta^c(a,b)} \mathfrak{m}_v$ uniformly in a, b, c.
- Good description of ramification sets, in particular a Reciprocity Law

Function fields in one variable over local and global fields

(joint work with Philip Dittmann)

Let F be a function field in one variable over a global or local field K ($\mathrm{char}(K) \neq 2$). Let $\mathcal{V}$ be the set of $\mathbb{Z}$-valuations which are trivial on K. Can we still universally define rings of S-integers?

Function fields in one variable over local and global fields

(joint work with Philip Dittmann)

Let F be a function field in one variable over a global or local field K ($\mathrm{char}(K) \neq 2$). Let $\mathcal{V}$ be the set of $\mathbb{Z}$-valuations which are trivial on K. Can we still universally define rings of S-integers?

- 3-fold Pfister forms (octonion algebras) replace quaternions. For $a, b, c \in F^\times$, define the ramification set

$$\Delta(a, b, c) = \{v \in \mathcal{V} \mid \langle\langle a, b, c\rangle\rangle_{F_v} \text{ is anisotropic}\}.$$

Function fields in one variable over local and global fields

(joint work with Philip Dittmann)

Let F be a function field in one variable over a global or local field K ($\mathrm{char}(K) \neq 2$). Let $\mathcal{V}$ be the set of $\mathbb{Z}$-valuations which are trivial on K. Can we still universally define rings of S-integers?

- 3-fold Pfister forms (octonion algebras) replace quaternions. For $a, b, c \in F^\times$, define the ramification set

$$\Delta(a, b, c) = \{v \in \mathcal{V} \mid \langle\langle a, b, c\rangle\rangle_{F_v} \text{ is anisotropic}\}.$$

- There is an existential formula associating to $(a, b, c, d) \in (F^\times)^3$ the subset $\bigcap_{v \in \Delta^d(a,b,c)} \mathfrak{m}_v$.

Function fields in one variable over local and global fields

Case K local field. The 'description of ramification behaviour' we need is contained in a natural exact sequence

$$k_3 F \longrightarrow \bigoplus_{w \in \mathcal{V}} k_2 F w \longrightarrow \mathbb{Z}/2 \longrightarrow 0$$

Function fields in one variable over local and global fields

Case K local field. The 'description of ramification behaviour' we need is contained in a natural exact sequence

$$k_3 F \longrightarrow \bigoplus_{w \in \mathcal{V}} k_2 Fw \longrightarrow \mathbb{Z}/2 \longrightarrow 0$$

- In particular we have a Reciprocity Law: the ramification sets are precisely the subsets of $\mathcal{V}$ containing an even number of elements. ($\subseteq$: Scharlau, 1972)

Function fields in one variable over local and global fields

Case K local field. The 'description of ramification behaviour' we need is contained in a natural exact sequence

$$k_3F \longrightarrow \bigoplus_{w\in\mathcal{V}} k_2Fw \longrightarrow \mathbb{Z}/2 \longrightarrow 0$$

- In particular we have a Reciprocity Law: the ramification sets are precisely the subsets of $\mathcal{V}$ containing an even number of elements. ($\subseteq$: Scharlau, 1972)
- k_3F in this case consists only of symbols (Parimala, Suresh, 1998)

Function fields in one variable over local and global fields

Case K non-real global field. There is a natural complex

$$0 \longrightarrow k_3F \longrightarrow \bigoplus_{w\in\mathcal{V}} k_2Fw \longrightarrow k_2K \longrightarrow 0$$

which has finite cohomology groups. (building on Kato, 1986)

Function fields in one variable over local and global fields

Case K non-real global field. There is a natural complex

$$0 \longrightarrow k_3 F \longrightarrow \bigoplus_{w \in \mathcal{V}} k_2 Fw \longrightarrow k_2 K \longrightarrow 0$$

which has finite cohomology groups. (building on Kato, 1986)

- All elements of $k_3 F$ are symbols. (Suresh, 2020)

Function fields in one variable over local and global fields

Case K non-real global field. There is a natural complex

$$0 \longrightarrow k_3 F \longrightarrow \bigoplus_{w \in \mathcal{V}} k_2 Fw \longrightarrow k_2 K \longrightarrow 0$$

which has finite cohomology groups. (building on Kato, 1986)

- All elements of $k_3 F$ are symbols. (Suresh, 2020)
- More subtle ramification behaviour ($k_2 K$ is more complicated than $\mathbb{Z}/2$).

References

[Daa20] Nicolas Daans. "Universally defining finitely generated subrings of global fields". https://arxiv.org/abs/1812.04372. Mar. 2020.

[EM18] Kirsten Eisenträger and Travis Morrison. "Universally and existentially definable subsets of global fields". In: *Math. Res. Lett.* 25.4 (2018), pp. 1173–1204.

[Kat86] Kazuya Kato. "A Hasse principle for two dimensional global fields.". In: *Journal für die reine und angewandte Mathematik* 366 (1986), pp. 142–180. URL: http://eudml.org/doc/152817.

[Koe16] Jochen Koenigsmann. "Defining $\mathbb{Z}$ in $\mathbb{Q}$". In: *Annals of Mathematics.* 183 (2016), pp. 73–93.

[Par13] Jennifer Park. "A universal first-order formula defining the ring of integers in a number field". In: *Math. Res. Lett.* 20 nr. 5 (2013), pp. 961–980.

[Poo09] Bjorn Poonen. "Characterizing integers among rational numbers with a universal-existential formula". In: *Amer. J. Math.* 131 (2009), pp. 675–682.

[PS98] Raman Parimala and Venapally Suresh. "Isotropy of quadratic forms over function fields of p-adic curves". In: *Publications Mathématiques de l'IHÉS* 88 (1998), pp. 129–150.

[Rob49] Julia Robinson. "Definability and decision problems in arithmetic". In: *Journal of Symbolic Logic* 14 (Feb. 1949), pp. 98–114. DOI: 10.2307/2266510.

[Sch72] Winfried Scharlau. "Quadratic Reciprocity Laws". In: *Journal of Number Theory* 4 (1972), pp. 78–97.

[Sur20] Venapally Suresh. "Third Galois cohomology group of function fields of curves over number fields". In: *Algebra & Number Theory* 14.3 (2020), pp. 701–729. DOI: 10.2140/ant.2020.14.721.

Nicolas Daans

E-mail: nicolas.daans@uantwerpen.be