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

Nicolas Daans

University of Antwerp

July 7, 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?

Theorem 1.1 (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

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?

Theorem 1.1 (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.

Theorem 1.2 (Poonen, 2009)

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

Existential and universal definitions in number theory

Question 1.3

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

Question 1.3

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 1.4 (Koenigsmann, 2010)

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

Existential and universal definitions in number theory

Question 1.3

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 1.4 (Koenigsmann, 2010)

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

Theorem 1.5 (Park, 2012)

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

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 in obtaining these results.

- 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 in obtaining these results.
- Mention some existentially definable "building blocks" from which we will build our definition.
- Give a proof of Koenigsmann's Theorem (universal definability of $\mathbb{Z}$ in $\mathbb{Q}$).

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 $(a, b)_\mathbb{Q}$ as follows:

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

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 $(a, b)_\mathbb{Q}$ as follows:

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

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

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. *(Hilbert Reciprocity)* $|\Delta(a, b)|$ *is an even natural number.*

Note: this allows us to fully compute the ramification set of a given quaternion algebra over $\mathbb{Q}$ (we can scale any $a, b \in \mathbb{Q}^\times$ be a square to obtain a square-free element of $\mathbb{Z} \setminus \{0\}$).

The ramification set

Lemma 2.2

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

$$\{p, \infty\} = \begin{cases} \Delta(-1,-2) & \text{if } p = 2 \\ \Delta(-1,-2p) & \text{if } p \equiv -1 \bmod 4 \\ \Delta(-p,-2) & \text{if } p \equiv 5 \bmod 8 \\ \Delta(-q,-2p) & \text{if } p \equiv 1 \bmod 8 \end{cases}$$

Proof: Exercise. □

Existentially definable building blocks

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

$$T(a,b) = \bigcap_{p \in \Delta(a,b)} \mathbb{Z}_{(p)}$$

where (for technical reasons) we set $\mathbb{Z}_{(\infty)} =]-4, 4[$.

Existentially definable building blocks

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

$$T(a,b) = \bigcap_{p \in \Delta(a,b)} \mathbb{Z}_{(p)}$$

where (for technical reasons) we set $\mathbb{Z}_{(\infty)} =]-4,4[$.

Proposition 2.3 (Poonen, Koenigsmann)

There exists an existential $\mathcal{L}$-formula ψ in 3 free variables such that for all $a, b \in \mathbb{Q}^\times$ we have

$$T(a,b) = \{x \in \mathbb{Q} \mid \mathbb{Q} \models \psi(x,a,b)\}$$

Proof: tomorrow.

Existentially definable building blocks

Corollary 2.4

For every $p \in \mathbb{P}$ the ring

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

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

Proof: Exercise. □

Already implicit in Robinson's work.

Existentially definable building blocks

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

$$\mathrm{Odd}(c) = \{p \in \mathbb{P} \mid v_p(c) \text{ is odd}\}$$

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

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

Existentially definable building blocks

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

$$\mathrm{Odd}(c) = \{p \in \mathbb{P} \mid v_p(c) \text{ is odd}\}$$

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

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

Lemma 2.5

We have

$$J^c(a,b) = T(a,b) \cdot ((c \cdot (\Box K)) \cap (1 - (\Box K) \cdot T(a,b)^\times)) .$$

Proof: Exercise. $\square$

Corollary 2.6 (Koenigsmann)

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

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

Proof sketch:

First steps

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:

First steps

Lemma 3.2

Let $a, b \in \mathbb{Q}^\times$, $v_2(b) = 0$. *Then*

$$J^{-a}(-a,-2b) \cap J^{-2b}(-a,-2b) = \bigcap_{p \in \Delta(-a,-2b) \cap \mathbb{P}} p\mathbb{Z}_{(p)}.$$

Proof:

Proof of main theorem

Proposition 3.3 (Daans, 2018)

We have

$$\bigcup_{p\in\mathbb{P}} p\mathbb{Z}_{(p)} = \bigcup_{\substack{a,b>0 \\ v_2(b)=0}} J^{-a}(-a,-2b) \cap J^{-2a}(-a,-2b).$$

Proof:

Proof of main theorem

Proof of Theorem 1.4:

Outlook

Tomorrow, I will talk about:

- the proof of Proposition 2.3, i.e. the existential definability of $\bigcap_{p \in \Delta(a,b)} \mathbb{Z}_{(p)}$.

Outlook

Tomorrow, I will talk about:

- the proof of Proposition 2.3, i.e. the existential definability of $\bigcap_{p \in \Delta(a,b)} \mathbb{Z}_{(p)}$.
- What was essentially used in this proof about existential definability and ramification sets? How can we generalise, e.g. to number fields (= finite extensions of $\mathbb{Q}$)?

References

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

[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.

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

Nicolas Daans
E-mail: nicolas.daans@uantwerpen.be