Annals of Mathematics **183** (2016), 73–93
http://dx.doi.org/10.4007/annals.2016.183.1.2

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

By Jochen Koenigsmann

Abstract

We show that $\mathbb{Z}$ is definable in $\mathbb{Q}$ by a universal first-order formula in the language of rings. We also present an $\forall\exists$-formula for $\mathbb{Z}$ in $\mathbb{Q}$ with just one universal quantifier. We exhibit new diophantine subsets of $\mathbb{Q}$ like the complement of the image of the norm map under a quadratic extension, and we give an elementary proof for the fact that the set of nonsquares is diophantine.

1. $\mathbb{Z}$ is universally definable in $\mathbb{Q}$

Hilbert's 10th problem was to find a general algorithm for deciding, given any n and any polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, whether or not f has a zero in $\mathbb{Z}^n$. Building on earlier work by Martin Davis, Hilary Putnam and Julia Robinson, Yuri Matiyasevich proved in 1970 that there can be no such algorithm. In particular, the existential first-order theory $\mathrm{Th}_\exists(\mathbb{Z})$ of $\mathbb{Z}$ (in the language of rings $\mathcal{L}_{\mathrm{ring}} := \{+, \cdot; 0, 1\}$) is undecidable. Hilbert's 10th problem over $\mathbb{Q}$, i.e., the question whether $\mathrm{Th}_\exists(\mathbb{Q})$ is decidable, is still open.

If one had an *existential* (or *diophantine*) definition of $\mathbb{Z}$ in $\mathbb{Q}$ (i.e., a definition by an existential first-order $\mathcal{L}_{\mathrm{ring}}$-formula), then $\mathrm{Th}_\exists(\mathbb{Z})$ would be interpretable in $\mathrm{Th}_\exists(\mathbb{Q})$, and the answer would, by Matiyasevich's Theorem, again be no. But it is still open whether $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$.

The earliest first-order definition of $\mathbb{Z}$ in $\mathbb{Q}$, which is due to Julia Robinson ([Rob49]), can be expressed by an $\forall\exists\forall$-formula of the shape

$$\phi(t) : \forall x_1 \forall x_2 \exists y_1 \cdots \exists y_7 \forall z_1 \cdots \forall z_6 \; f(t; x_1, x_2; y_1, \ldots, y_7; z_1, \ldots, z_6) = 0$$

for some $f \in \mathbb{Z}[t; x_1, x_2; y_1, \ldots, y_7; z_1, \ldots, z_6]$; i.e., for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \text{ if and only if } \phi(t) \text{ holds in } \mathbb{Q}.$$

The research on this paper started while the author enjoyed the hospitality of the Max-Planck-Institut Bonn.

Recently, Bjorn Poonen ([Poo09a]) managed to find an $\forall\exists$-definition with two universal and seven existential quantifiers. In this paper we present a $\forall$-definition of $\mathbb{Z}$ in $\mathbb{Q}$. To search for such a creature is motivated by the following

Observation 0. *If there is an existential definition of $\mathbb{Z}$ in $\mathbb{Q}$, then there is also a universal one.*

Proof. If $\mathbb{Z}$ is diophantine in $\mathbb{Q}$, then so is

$$\mathbb{Q} \setminus \mathbb{Z} = \{x \in \mathbb{Q} \mid \exists m, n, a, b \in \mathbb{Z} \text{ with } n \neq 0, \pm 1,\ am + bn = 1 \text{ and } m = xn\}.$$

□

Theorem 1. [1] *There is, for some positive integer n, a polynomial $g \in \mathbb{Z}[t; x_1, \ldots, x_n]$ such that, for any $t \in \mathbb{Q}$,*

$$t \in \mathbb{Z} \text{ if and only if } \forall x_1 \cdots \forall x_n \in \mathbb{Q} \;\; g(t; x_1, \ldots, x_n) \neq 0.$$

If one measures logical complexity in terms of the number of changes of quantifiers, then this is a definition of $\mathbb{Z}$ in $\mathbb{Q}$ of least possible complexity: there is no quantifier-free definition of $\mathbb{Z}$ in $\mathbb{Q}$.

Corollary 2. *$\mathbb{Q} \setminus \mathbb{Z}$ is diophantine in $\mathbb{Q}$.*

In more geometric terms, this says

Corollary 2′. *There is a (not necessarily irreducible) affine variety V over $\mathbb{Q}$ and a $\mathbb{Q}$-morphism $\pi : V \to \mathbb{A}^1$ such that the image of $V(\mathbb{Q})$ is $\mathbb{Q} \setminus \mathbb{Z}$.*

Together with the undecidability of $\mathrm{Th}_{\exists}(\mathbb{Z})$, Theorem 1 immediately implies

Corollary 3. *$\mathrm{Th}_{\forall\exists}(\mathbb{Q})$ is undecidable.*

Here $\mathrm{Th}_{\forall\exists}(\mathbb{Q})$ is the set of all sentences of the shape

$$\forall x_1 \cdots \forall x_k \exists y_1 \cdots \exists y_l \, \phi(x_1, \ldots, x_k; y_1, \ldots, y_l),$$

where ϕ is a quantifier-free $\mathcal{L}_{\mathrm{ring}}$-formula, that is, a boolean combination of polynomial equations and inequalities between polynomials in

$$\mathbb{Z}[x_1, \ldots, x_k; y_1, \ldots, y_l].$$

Corollary 3 was proved conditionally, using a conjecture on elliptic curves, in [CZ07]. Again, we can phrase this in more geometric terms:

Corollary 3′. *There is no algorithm that decides on input a $\mathbb{Q}$-morphism $\pi : V \to W$ between affine $\mathbb{Q}$-varieties V, W whether or not $\pi : V(\mathbb{Q}) \to W(\mathbb{Q})$ is surjective.*

[1] In the meantime, Theorem 1 has been generalized to arbitrary number fields K: the ring of integers of K is universally definable in K ([Par13]).

Acknowledgements. Among many others, I would, in particular, like to thank Boris Zilber, Jonathan Pila, Marc Hindry and Joseph Silverman for very helpful discussions. I am also most grateful to the anonymous referee whose numerous suggestions have greatly improved the paper. The now much shorter proof of Proposition 16(a) is the referee's.

2. **The proof of Theorem 1**

Like all previous definitions of $\mathbb{Z}$ in $\mathbb{Q}$, we use elementary facts on quadratic forms over $\mathbb{R}$ and $\mathbb{Q}_p$, together with the Hasse-Minkowski local-global principle for quadratic forms. What is new in our approach is the use of the Quadratic Reciprocity Law (e.g., in Propositions 10 or 16) and, inspired by the model theory of local fields, the transformation of some existential formulas into universal formulas (Step 4). A technical key trick is the existential definition of the Jacobson radical of certain rings (Step 3) that makes implicit use of so-called 'rigid elements' as they occur, e.g., in [Koe95].

Step 1: *Diophantine definition of quaternionic semi-local rings à la Poonen.* The first step modifies Poonen's proof ([Poo09a]), thus arriving at a formula for $\mathbb{Z}$ in $\mathbb{Q}$ that, like the formula in his Theorem 4.1, has two $\forall$'s followed by seven $\exists$'s, but we managed to bring down the degree of the polynomial involved from 9244 to 8.

Definition 4. Let $\mathbb{P}$ be the set of rational primes, and let $\mathbb{Q}_\infty := \mathbb{R}$. For $a, b \in \mathbb{Q}^\times$, let

- $H_{a,b} := \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \alpha \oplus \mathbb{Q} \cdot \beta \oplus \mathbb{Q} \cdot \alpha\beta$ be the quaternion algebra over $\mathbb{Q}$ with multiplication defined by $\alpha^2 = a$, $\beta^2 = b$ and $\alpha\beta = -\beta\alpha$.
- $\Delta_{a,b} := \{p \in \mathbb{P} \cup \{\infty\} \mid H_{a,b} \otimes \mathbb{Q}_p \not\cong M_2(\mathbb{Q}_p)\}$ the set of primes (including ∞) where $H_{a,b}$ does not split locally — $\Delta_{a,b}$ is always finite, and $\Delta_{a,b} = \emptyset$ if and only if $a \in N(b)$, i.e., a is in the image of the norm map $\mathbb{Q}(\sqrt{b}) \to \mathbb{Q}$.
- $S_{a,b} := \{2x_1 \in \mathbb{Q} \mid \exists x_2, x_3, x_4 \in \mathbb{Q} : x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$ the set of traces of norm-1 elements of $H_{a,b}$.
- $T_{a,b} := S_{a,b} + S_{a,b}$ — note that $T_{a,b}$ is an existentially defined subset of $\mathbb{Q}$. Here we deviate from Poonen's terminology: his $T_{a,b}$ is $S_{a,b} + S_{a,b} + \{0, 1, \ldots, 2309\}$.

For each $p \in \mathbb{P} \cup \{\infty\}$, we can similarly define $S_{a,b}(\mathbb{Q}_p)$ and $T_{a,b}(\mathbb{Q}_p)$ by replacing $\mathbb{Q}$ by $\mathbb{Q}_p$.

For each $p \in \mathbb{P}$, we will denote the p-adic valuation on $\mathbb{Q}$ or on $\mathbb{Q}_p$ by v_p, and the associated residue map by $\phi_p : \mathbb{Z}_{(p)} \to \mathbb{F}_p$ resp. $\phi_p : \mathbb{Z}_p \to \mathbb{F}_p$.

An explicit criterion for checking whether or not an element $p \in \mathbb{P} \cup \{\infty\}$ belongs to $\Delta_{a,b}$ is given in the following

Observation 5. Assume $a, b \in \mathbb{Q}^\times$ and $p \in \mathbb{P} \cup \{\infty\}$. Then $p \in \Delta_{a,b}$ if and only if

for $p = 2$: After multiplying by suitable rational squares and integers $\equiv 1 \bmod 8$ and, possibly, swapping a and b, the pair (a, b) is one of the following:

$$\begin{array}{lllll} (2,3) & (3,3) & (5,6) & (6,6) & (15,15) \\ (2,5) & (3,10) & (5,10) & (6,15) & (15,30) \\ (2,6) & (3,15) & (5,30) & (10,30) & (30,30) \\ (2,10); & & & & \end{array}$$

for $2 \neq p \in \mathbb{P}$:

$v_p(a)$ is odd, $v_p(b)$ is even, and $\left(\frac{bp^{-v_p(b)}}{p}\right) = -1$, or
$v_p(a)$ is even, $v_p(b)$ is odd, and $\left(\frac{ap^{-v_p(a)}}{p}\right) = -1$ or
$v_p(a)$ is odd, $v_p(b)$ is odd, and $\left(\frac{-abp^{-v_p(ab)}}{p}\right) = -1$;

for $p = \infty$: $a < 0$ and $b < 0$.

Proof. This is an immediate translation of the computation of the Hilbert symbol $(a, b)_p$ (which is 1 or -1 depending on whether or not $p \in \Delta_{a,b}$) as in Theorem 1 of Chapter III in [Ser73]. For finite odd p and $a = p^\alpha u$ and $b = p^\beta v$ (with u, v p-adic units), the formula is

$$(a, b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha,$$

where $\varepsilon(p) := \frac{p-1}{2} \bmod 2$.

For $p = 2$, the formula is

$$(a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)},$$

where $\omega(u) := \frac{u^2-1}{8} \bmod 2$.

For $p = \infty$, the statement is obvious. □

Proposition 6. *For any* $a, b \in \mathbb{Q}^\times$,

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

where $\mathbb{Z}_{(\infty)} := \{x \in \mathbb{Q} \mid -4 \leq x \leq 4\}$.

Here and throughout the rest of the paper, we use the following

Convention. Given an empty collection of subsets of $\mathbb{Q}$, the intersection is $\mathbb{Q}$.

Proof. For each $p \in \mathbb{P}$, let

$$U_p := \{s \in \mathbb{F}_p \mid x^2 - sx + 1 \text{ is irreducible over } \mathbb{F}_p\}.$$

We shall use the following

Facts. For any $a, b \in \mathbb{Q}^\times$ and for any $p \in \mathbb{P}$,

(a) if $p \notin \Delta_{a,b}$, then $S_{a,b}(\mathbb{Q}_p) = \mathbb{Q}_p$;

(b) if $p \in \Delta_{a,b}$, then $\phi_p^{-1}(U_p) \subseteq S_{a,b}(\mathbb{Q}_p) \subseteq \mathbb{Z}_p$;

(c) $S_{a,b}(\mathbb{R}) = \begin{cases} \mathbb{R} & \text{for } a > 0 \text{ or } b > 0, \\ [-2, 2] & \text{for } a, b < 0; \end{cases}$

(d) if $p > 11$, then $\mathbb{F}_p = U_p + U_p$.

(e) $S_{a,b}(\mathbb{Q}) = \mathbb{Q} \cap \bigcap_{p \in \Delta_{a,b}} S_{a,b}(\mathbb{Q}_p)$.

(a) and (b) are [Poo09a, Lemma 2.1], (c) is a straightforward computation, (d) is [Poo09a, Lemma 2.3] and (e) is a special case of the Hasse-Minkowski local-global principle for representing rationals by quadratic forms.

(b) and (c) immediately give the inclusion $T_{a,b} \subseteq \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$.

To prove the converse inclusion $T_{a,b} \supseteq \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$, let us first compute U_p for the primes $p \leq 11$:

$$\begin{aligned} U_2 &= \{1\}, \\ U_3 &= \{0\}, \\ U_5 &= \{1, 4\}, \\ U_7 &= \{0, 3, 4\}, \\ U_{11} &= \{0, 1, 5, 6, 10\}. \end{aligned}$$

For each $p \in \mathbb{P} \cup \{\infty\}$, define $V_p \subseteq \mathbb{Z}_p$ as follows:

$$V_p = \begin{cases} \phi_2^{-1}(U_2) \cup (4 + 8\mathbb{Z}_2) & \text{for } p = 2, \\ \phi_p^{-1}(U_p) \cup [(\pm 2 + p\mathbb{Z}_p) \setminus (\pm 2 + p^2\mathbb{Z}_p)] & \text{for } 3 \leq p \leq 11, \\ \phi_p^{-1}(U_p) & \text{for } 11 < p \in \mathbb{P}, \\ [-2, 2] & \text{for } p = \infty. \end{cases}$$

(We define $\mathbb{Z}_\infty$ to be the real interval $[-4, 4] \subseteq \mathbb{R}$.) By Fact (b), Fact (c), Observation 5 together with an easy direct calculation in the cases $p = 3, 5, 7, 11$, and for $p = 2$, by the table below, one always has

$$V_p \subseteq S_{a,b}(\mathbb{Q}_p) \text{ and, for } p \neq \infty,\ V_p \text{ is open.}$$

The table for $p = 2$ lists those pairs (a, b) with $(a, b)_2 = -1$ as in Observation 5 and gives, in each case,

$$4 + 8\mathbb{Z}_2 \subseteq S_{a,b}(\mathbb{Q}_2)$$

by assuming that we are given $x_1 \in 2 + 8\mathbb{Z}_2$ or $x_1 \in 6 + 8\mathbb{Z}_2$ (which is equivalent to $2x_1 \in 4 + 8\mathbb{Z}_2$) and by specifying elements x_2, x_3 and x_4 that guarantee that

$$-ax_2^2 - bx_3^2 + abx_4^2 \equiv_2 1 - x_1^2 \equiv_2 -3 \mod 8\mathbb{Z}_2.$$

Multiplying x_2^2, x_3^2, x_4^2 by a suitable common element from $1 + 8\mathbb{Z}_2 \subseteq (\mathbb{Q}_2^{\times})^2$ then makes sure that $2x_1 \in S_{a,b}(\mathbb{Q}_2)$.

(a,b)	x_2	x_3	x_4
$(2,3)$	0	1	0
$(2,5)$	2	1	1
$(2,6)$	0	1	$\frac{1}{2}$
$(2,10)$	2	0	$\frac{1}{2}$
$(3,3)$	1	0	0
$(3,10)$	1	0	0
$(3,15)$	1	0	0
$(5,6)$	1	1	0
$(5,10)$	1	0	1
$(5,30)$	1	1	0
$(6,6)$	$\frac{1}{2}$	$\frac{1}{2}$	0
$(6,15)$	1	1	0
$(10,30)$	0	1	$\frac{1}{10}$
$(15,15)$	1	0	$\frac{2}{15}$
$(15,30)$	1	1	$\frac{1}{15}$
$(30,30)$	1	1	$\frac{1}{30}$

Fact (d) and another elementary case-by-case-check for $p \leq 11$ show that for any $p \in \mathbb{P} \cup \{\infty\}$,

$$\mathbb{Z}_p = V_p + V_p.$$

Now pick $t \in \bigcap_{p \in \Delta_{a,b}} \mathbb{Z}_{(p)}$. For each $p \in \Delta_{a,b}$, there is some $s_p \in \mathbb{Z}_p$ such that $s_p, t - s_p \in V_p$.

If $t = \pm 4$ then, clearly, $t = \pm 2 \pm 2 \in S_{a,b} + S_{a,b} = T_{a,b}$.

If $t \neq \pm 4$ and $\infty \in \Delta_{a,b}$, we can choose $s_\infty \in \mathbb{Z}_\infty = [-4, 4] \subseteq \mathbb{R}$ such that $s_\infty, t - s_\infty \in]-2, 2[$. Now approximate the finitely many $s_p \in \mathbb{Z}_p$ $(p \in \Delta_{a,b})$ by a single $s \in \mathbb{Q}$ such that

$$s - s_p \in \begin{cases} 8\mathbb{Z}_2 & \text{if } p = 2, \\ p^2\mathbb{Z}_p & \text{if } 3 \leq p \leq 11, \\ p\mathbb{Z}_p & \text{if } 11 < p \in \mathbb{P}, \\ ]-\varepsilon, \varepsilon[& \text{if } p = \infty, \end{cases}$$

where $\varepsilon = \min\{\mid 2 \pm s_\infty \mid, \mid 2 \pm (t - s_\infty) \mid\}$. This guarantees that for all $p \in \Delta_{a,b}$,

$$s, t - s \in V_p \subseteq S_{a,b}(\mathbb{Q}_p)$$

and hence, by Fact (e), that $s, t - s \in S_{a,b} = S_{a,b}(\mathbb{Q})$. □

One then obtains an $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ from the fact that

$$\mathbb{Z} = \bigcap_{l\in\mathbb{P}} \mathbb{Z}_{(l)} = \bigcap_{a,b>0} T_{a,b}$$

as in [Poo09a, Th. 4.1]. With our simplified $T_{a,b}$, the formula now becomes, for any $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \Longleftrightarrow \begin{array}{l} \forall a, b\, \exists x_1, x_2, x_3, x_4, y_2, y_3, y_4 \\ (a + x_1^2 + x_2^2 + x_3^2 + x_4^2) \cdot (b + x_1^2 + x_2^2 + x_3^2 + x_4^2) \\ \cdot[(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 \\ + ((t - 2x_1)^2 - 4ay_2^2 - 4by_3^2 + 4aby_4^2 - 4)^2] = 0 \end{array}$$

Step 2: *Towards a uniform diophantine definition of all $\mathbb{Z}_{(p)}$'s in $\mathbb{Q}$.* We will present a diophantine definition for the local rings $\mathbb{Z}_{(p)} = \mathbb{Z}_p \cap \mathbb{Q}$ depending on the congruence of the prime p modulo 8 and involving p (and if $p \equiv 1$ mod 8 an auxiliary prime q) as a parameter. However, since in any first-order definition of a subset of $\mathbb{Q}$ we can only quantify over the elements of $\mathbb{Q}$ and not, e.g., over all primes, we will allow arbitrary nonzero rational numbers p and q as parameters in the following definition.

Definition 7. For $p, q \in \mathbb{Q}^\times$, let

- $R_p^{[3]} := T_{-1,-p} + T_{2,-p}$;
- $R_p^{[5]} := T_{-2,-p} + T_{2,-p}$;
- $R_p^{[7]} := T_{-1,-p} + T_{-2,p}$;
- $R_{p,q}^{[1]} := T_{-2p,q} + T_{2p,q}$.

Remark 8.

(a) For any $a, b, c, d \in \mathbb{Q}^\times$ with at least one of them positive,

$$T_{a,b} + T_{c,d} = \bigcap_{l\in\Delta_{a,b}} \mathbb{Z}_{(l)} + \bigcap_{l\in\Delta_{c,d}} \mathbb{Z}_{(l)} = \bigcap_{l\in\Delta_{a,b}\cap\Delta_{c,d}} \mathbb{Z}_{(l)}.$$

(b) The R's are existentially defined, uniformly in p and q, so that for $k = 3, 5$ or 7, the sets

$$\{(p, x) \in \mathbb{Q}^\times \times \mathbb{Q} \mid x \in R_p^{[k]}\}$$

and the set

$$\{(p, q, x) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q} \mid x \in R_{p,q}^{[1]}\}$$

are diophantine.

Proof. (a) The first equation is from Proposition 6. For the second equation, the inclusion '$\subseteq$' is obvious. For '$\supseteq$,' assume $x \in \bigcap_{l\in\Delta_{a,b}\cap\Delta_{c,d}} \mathbb{Z}_{(l)}$. By approximation, there is $y \in \mathbb{Q}$ such that

$$y \in \begin{cases} x + l\mathbb{Z}_{(l)} & \text{for } l \in \Delta_{c,d}, \\ \mathbb{Z}_{(l)} & \text{for } l \in \Delta_{a,b} \setminus \Delta_{c,d}. \end{cases}$$

Then $y \in \bigcap_{l\in\Delta_{a,b}} \mathbb{Z}_{(l)}$ and $x - y \in \bigcap_{l\in\Delta_{c,d}} \mathbb{Z}_{(l)}$, so that $x = y + (x - y) \in \bigcap_{l\in\Delta_{a,b}} \mathbb{Z}_{(l)} + \bigcap_{l\in\Delta_{c,d}} \mathbb{Z}_{(l)}$.

(b) This is immediate from Definitions 4 and 7. □

Definition 9.

(a) For $k = 1, 3, 5$ or 7, define $\mathbb{P}^{[k]} := \{l \in \mathbb{P} \mid l \equiv k \bmod 8\}$.

(b) For $p \in \mathbb{Q}^\times$, define

- $\mathbb{P}(p) := \{l \in \mathbb{P} \mid v_l(p) \text{ is odd}\}$;
- $\mathbb{P}^{[k]}(p) := \mathbb{P}(p) \cap \mathbb{P}^{[k]}$, where $k = 1, 3, 5$ or 7.

(c) For $p, q \in \mathbb{Q}^\times$, define $\mathbb{P}(p, q) := \Delta_{-2p,q} \cap \Delta_{2p,q}$.

Proposition 10.

(a) $\mathbb{Z}_{(2)} = T_{3,3} + T_{2,5}$.

(b) *Suppose that $k = 3, 5$ or 7. Then, for $p \in \mathbb{Q}^\times$,*

$$R_p^{[k]} = \begin{cases} \bigcap_{l\in\mathbb{P}^{[k]}(p)} \mathbb{Z}_{(l)} & \textit{if } p \equiv k \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)}), \\ \bigcap_{l\in\mathbb{P}^{[k]}(p)} \mathbb{Z}_{(l)} \textit{ or } \bigcap_{l\in\mathbb{P}^{[k]}(p)\cup\{2\}} \mathbb{Z}_{(l)} & \textit{otherwise.} \end{cases}$$

(As before, $\bigcap_{l\in\emptyset} \mathbb{Z}_{(l)} = \mathbb{Q}$.) In particular, if p is a prime and $p \equiv k \bmod 8$, then $\mathbb{Z}_{(p)} = R_p^{[k]}$.

(c) *For $p, q \in \mathbb{Q}^\times$ with $p \equiv 1$ (mod $8\mathbb{Z}_{(2)}$) and $q \equiv 3$ (mod $8\mathbb{Z}_{(2)}$),*

$$R_{p,q}^{[1]} = \bigcap_{l\in\mathbb{P}(p,q)} \mathbb{Z}_{(l)}.$$

In particular, if p is a prime $\equiv 1 \bmod 8$ and q is a prime $\equiv 3 \bmod 8$ with $\left(\frac{p}{q}\right) = -1$, then $\mathbb{Z}_{(p)} = R_{p,q}^{[1]}$.

Proof. (a) By Observation 5, $\Delta_{3,3} = \{2, 3\}$ and $\Delta_{2,5} = \{2, 5\}$, hence, by Remark 8(a),

$$T_{3,3} + T_{2,5} = \bigcap_{l\in\Delta_{3,3}\cap\Delta_{2,5}} \mathbb{Z}_{(l)} = \mathbb{Z}_{(2)}.$$

(b) First assume $p \in \mathbb{Q}^\times$ with $p \equiv 3$ (mod $8\mathbb{Z}_{(2)}$). Then, by Observation 5,

$$\Delta_{-1,-p} \cap \mathbb{P} = \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[7]}(p),$$
$$\Delta_{2,-p} = \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[5]}(p) \cup \{2\},$$

so $\Delta_{-1,-p} \cap \Delta_{2,-p} = \mathbb{P}^{[3]}(p)$ and, by Remark 8(a),

$$R_p^{[3]} := T_{-1,-p} + T_{2,-p} = \bigcap_{l\in\Delta_{-1,-p}\cap\Delta_{2,-p}} \mathbb{Z}_{(l)} = \bigcap_{l\in\mathbb{P}^{[3]}(p)} \mathbb{Z}_{(l)}.$$

If $p \not\equiv 3 \pmod{8\mathbb{Z}_{(2)}}$, the only possible additional prime is 2 (e.g., if $p \equiv 5 \pmod{8\mathbb{Z}_{(2)}}$).

If $p \equiv 5 \pmod{8\mathbb{Z}_{(2)}}$ then, again by Observation 5,

$$\begin{aligned}\Delta_{-2,-p} \cap \mathbb{P} &= \mathbb{P}^{[5]}(p) \cup \mathbb{P}^{[7]}(p),\\ \Delta_{2,-p} &= \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[5]}(p) \cup \{2\},\end{aligned}$$

so $\Delta_{-2,-p} \cap \Delta_{2,-p} = \mathbb{P}^{[5]}(p)$, and

$$R_p^{[5]} := T_{-2p,-p} + T_{2p,-p} = \bigcap_{l \in \Delta_{-2,-p} \cap \Delta_{2,-p}} \mathbb{Z}_{(l)} = \bigcap_{l \in \mathbb{P}^{[5]}(p)} \mathbb{Z}_{(l)}.$$

Once more, if $p \not\equiv 5 \pmod{8\mathbb{Z}_{(2)}}$, the prime 2 (and no other prime) may enter.

Finally, if $p \equiv 7 \pmod{8\mathbb{Z}_{(2)}}$ then, again by Observation 5,

$$\begin{aligned}\Delta_{-1,-p} \cap \mathbb{P} &= \mathbb{P}^{[3]}(p) \cup \mathbb{P}^{[7]}(p),\\ \Delta_{-2,p} \cap \mathbb{P} &= \mathbb{P}^{[5]}(p) \cup \mathbb{P}^{[7]}(p) \cup \{2\},\end{aligned}$$

so $\Delta_{-1,-p} \cap \Delta_{-2,p} = \mathbb{P}^{[7]}(p)$, and

$$R_p^{[7]} := T_{-p,-p} + T_{2p,p} = \bigcap_{l \in \Delta_{-1,-p} \cap \Delta_{-2,p}} \mathbb{Z}_{(l)} = \bigcap_{l \in \mathbb{P}^{[7]}(p)} \mathbb{Z}_{(l)}.$$

As before, 2 may enter if $p \not\equiv 7 \pmod{8\mathbb{Z}_{(2)}}$.

(c) The first statement is immediate from Remark 8(a). For the 'in particular,' assume p and q are primes with $p \equiv 1 \bmod 8$, $q \equiv 3 \bmod 8$ and $\left(\frac{p}{q}\right) = -1$. Then, by quadratic reciprocity, $\left(\frac{q}{p}\right) = -1$, and so, from Observation 5, $\Delta_{-2p,q} = \{p, q\}$ and $\Delta_{2p,q} = \{2, p\}$. Hence $R_{p,q}^{[1]} = \mathbb{Z}_{(p)}$. □

Corollary 11.

$$\mathbb{Z} = \mathbb{Z}_{(2)} \cap \bigcap_{p,q \in \mathbb{Q}^\times} (R_p^{[3]} \cap R_p^{[5]} \cap R_p^{[7]} \cap R_{p,q}^{[1]}).$$

Proof. By Remark 8(a), all R's on the right-hand side are semilocal subrings of $\mathbb{Q}$ containing $\mathbb{Z}$. On the other hand, by the 'in particular' parts of the proposition, for each prime p, the right-hand side is contained in $\mathbb{Z}_{(p)}$; note that for $p \equiv 1 \bmod 8$, one always finds a prime $q \equiv 3 \bmod 8$ such that q is congruent to a nonsquare $\bmod\ p$. □

Step 3: *An existential definition for the Jacobson radical.* We will show that, for some rings R occurring in Proposition 10, the Jacobson radical $J(R)$ can be defined by an existential formula. This will also give rise to new diophantine predicates in $\mathbb{Q}$.

Definition 12. For $a, b, c \in \mathbb{Q}^\times$, we define

- $T_{a,b}^\times := \{u \in T_{a,b} \mid \exists v \in T_{a,b} \text{ with } uv = 1\}$;
- $I_{a,b}^c := c \cdot \mathbb{Q}^2 \cdot T_{a,b}^\times \cap (1 - \mathbb{Q}^2 \cdot T_{a,b}^\times)$;

- $J_{a,b} := (I^a_{a,b} + I^a_{a,b}) \cap (I^b_{a,b} + I^b_{a,b})$.

Note that the set $\{(a,b,x) \in \mathbb{Q}^\times \times \mathbb{Q}^\times \times \mathbb{Q} \mid x \in J_{a,b}\}$ is diophantine.

Lemma 13. *Assume $a,b,c \in \mathbb{Q}^\times$. Then*

(a) $T^\times_{a,b} = \begin{cases} \bigcap_{l\in\Delta_{a,b}} \mathbb{Z}^\times_{(l)} & \textit{if } \infty \notin \Delta_{a,b}, \\ ([-4,-\frac{1}{4}] \cup [\frac{1}{4},4]) \cap \bigcap_{l\in\Delta_{a,b}\setminus\{\infty\}} \mathbb{Z}^\times_{(l)} & \textit{if } \infty \in \Delta_{a,b}; \end{cases}$

(b) $I^c_{a,b} = \{0\} \cup \left\{ y \in \mathbb{Q}^\times \,\middle|\, \begin{array}{l} v_l(y) \textit{is odd and positive } \forall l \in \Delta_{a,b} \cap \mathbb{P}(c) \textit{ and} \\ v_l(y), v_l(1-y) \textit{are even } \forall l \in \Delta_{a,b} \setminus (\mathbb{P}(c) \cup \{\infty\}) \end{array} \right\}$;[2]

(c) $I^c_{a,b} + I^c_{a,b} = \bigcap_{l\in\Delta_{a,b}\cap\mathbb{P}(c)} l\,\mathbb{Z}_{(l)}$;

(d) $J_{a,b} = \bigcap_{l\in\Delta} l\mathbb{Z}_{(l)}$, *where*

$$\Delta = \begin{cases} \Delta_{a,b} \setminus \{2,\infty\} & \textit{if } 2 \in \Delta_{a,b} \textit{ and } v_2(a), v_2(b) \textit{ are even,} \\ \Delta_{a,b} \setminus \{\infty\} & \textit{else.} \end{cases}$$

In particular, if $\infty \notin \Delta_{a,b}$, then $T^\times_{a,b}$ is the group of units of the ring $T_{a,b}$ and, if also $2 \notin \Delta_{a,b}$ or at least one of $v_2(a), v_2(b)$ is odd, then $J_{a,b}$ is the Jacobson radical of $T_{a,b}$.

Proof. (a) This is an immediate consequence of Proposition 6.

(b) '$\subseteq$': By weak approximation,

$$\mathbb{Q}^2 \cdot T^\times_{a,b} = \{0\} \cup \bigcap_{l\in\Delta_{a,b}\setminus\{\infty\}} v_l^{-1}(2\mathbb{Z}).$$

So if $y \in I^c_{a,b} \setminus \{0\}$ and $l \in \Delta_{a,b} \cap \mathbb{P}(c)$, then $v_l(y)$ is odd and $v_l(1-y)$ is even (as $1 - y \in \mathbb{Q}^2 \cdot T^\times_{a,b}$) which, by the ultrametric inequality, is only possible when $v_l(y) > 0$. If, on the other hand, $l \in \Delta_{a,b} \setminus (\mathbb{P}(c) \cup \{\infty\})$, then $v_l(y)$ and $v_l(1-y)$ are even.

'$\supseteq$': Clearly, $0 \in I^c_{a,b}$. Now assume $y \in \mathbb{Q}^\times$ such that, for all $l \in \Delta_{a,b} \cap \mathbb{P}(c)$, $v_l(y)$ is positive and odd. Then

$$c^{-1}y \in \bigcap_{l\in\Delta_{a,b}\cap\mathbb{P}(c)} v_l^{-1}(2\mathbb{Z})$$

and

$$1 - y \in \bigcap_{l\in\Delta_{a,b}\cap\mathbb{P}(c)} \mathbb{Z}^\times_{(l)} \subseteq \bigcap_{l\in\Delta_{a,b}\cap\mathbb{P}(c)} v_l^{-1}(2\mathbb{Z}).$$

If we assume that $v_l(y)$ and $v_l(1-y)$ are even for all $l \in \Delta' := \Delta_{a,b} \setminus (\mathbb{P}(c) \cup \{\infty\})$, then both $c^{-1}y$ and $1 - y$ lie in $\bigcap_{l\in\Delta'} v_l^{-1}(2\mathbb{Z})$.

[2] Here we adopt the convention that ∞ is even (to include the case that $y = 1$, which can only happen when $\Delta_{a,b} \cap \mathbb{P}(c) = \emptyset$, a case which will never be used later).

So with both assumptions we see that both $c^{-1}y$ and $1-y$ lie in

$$\bigcap_{l\in\Delta_{a,b}\setminus\{\infty\}} v_l^{-1}(2\mathbb{Z}) \subseteq \mathbb{Q}^2\cdot T_{a,b}^{\times}.$$

(c) For any prime l, any $x\in\mathbb{Q}$ with $v_l(x)>0$ can be written as the sum of two elements of odd positive value. And any $x\in\mathbb{Q}$ can be written as the sum of two elements y_1 and y_2 such that $v_l(y_i)$ and $v_l(1-y_i)$ are both even for both $i=1,2$: choose y_1 of even value $<\min\{0,v_l(x)\}$, and let $y_2=x-y_1$; then $v_l(1-y_1)=v_l(y_1)=v_l(y_2)=v_l(1-y_2)$. Hence the claim follows by approximation.

(d) By definition, $J_{a,b}=(I_{a,b}^a+I_{a,b}^a)\cap(I_{a,b}^b+I_{a,b}^b)$ so, from (c),

$$J_{a,b}=\bigcap_{l\in\Delta_{a,b}\cap\mathbb{P}(a)} l\mathbb{Z}_{(l)}\cap\bigcap_{l\in\Delta_{a,b}\cap\mathbb{P}(b)} l\mathbb{Z}_{(l)}=\bigcap_{l\in\Delta_{a,b}\cap(\mathbb{P}(a)\cup\mathbb{P}(b))} l\mathbb{Z}_{(l)},$$

where the second equality is, again, by weak approximation. But now, from Observation 5,

$$\Delta_{a,b}\cap(\mathbb{P}(a)\cup\mathbb{P}(b))=\begin{cases}\Delta_{a,b}\setminus\{2,\infty\} & \text{if } 2\in\Delta_{a,b} \text{ and } v_2(a),v_2(b) \text{ are even,}\\ \Delta_{a,b}\setminus\{\infty\} & \text{else.}\end{cases}\qquad\square$$

Before we give the existential definition of the Jacobson radical $J(R)$ for some of the rings R in Definition 7 (Corollary 15 and Proposition 16 below) we require another easy lemma.

Lemma 14. *Let $a,b,c,d\in\mathbb{Q}^{\times}$, at least one of which positive, let $\Delta:=\Delta_{a,b}\cap\Delta_{c,d}$, let $R=\bigcap_{l\in\Delta}\mathbb{Z}_{(l)}$ and assume $2\notin\Delta$. Then*

$$J_{a,b}+J_{c,d}=\bigcap_{l\in\Delta} l\mathbb{Z}_{(l)}.$$

In particular, if $\Delta\neq\emptyset$, then $J_{a,b}+J_{c,d}$ is the Jacobson radical $J(R)$ of the semilocal ring R.

Proof. Let

$$\Delta'_{a,b}:=\begin{cases}\Delta_{a,b}\setminus\{2,\infty\} & \text{if } 2\in\Delta_{a,b} \text{ and } v_2(a),v_2(b) \text{ are even,}\\ \Delta_{a,b}\setminus\{\infty\} & \text{else,}\end{cases}$$

and similarly define $\Delta'_{c,d}$. Then, by Lemma 13(d) (for the first equality) and by weak approximation (for the second),

$$J_{a,b}+J_{c,d}=\bigcap_{l\in\Delta'_{a,b}} l\mathbb{Z}_{(l)}+\bigcap_{l\in\Delta'_{c,d}} l\mathbb{Z}_{(l)}=\bigcap_{l\in\Delta'_{a,b}\cap\Delta'_{c,d}} l\mathbb{Z}_{(l)}.$$

By our assumption on a,b,c,d, however, $\Delta_{a,b}\cap\Delta_{c,d}=\Delta'_{a,b}\cap\Delta'_{c,d}$, which proves the first claim. The ‘in particular’ follows immediately. $\square$

Now let us first turn to the rings $R_p^{[k]}$ for $k = 3, 5$ and 7 defined in Definition 7 and recall that

$$R_p^{[k]} = \begin{cases} T_{-1,-p} + T_{2,-p} & \text{if } k = 3, \\ T_{-2,-p} + T_{2,-p} & \text{if } k = 5, \\ T_{-1,-p} + T_{-2,p} & \text{if } k = 7. \end{cases}$$

Corollary 15. *For $k = 1, 3, 5$ and 7, define*

$$\Phi_k := \{p \in \mathbb{Q}^{>0} \mid p \equiv k \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)}) \textit{ and } \mathbb{P}(p) \subseteq \mathbb{P}^{[1]} \cup \mathbb{P}^{[k]}\},$$
$$\Psi := \{(p, q) \in \Phi_1 \times \Phi_3 \mid p \in 2 \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_q^{[3]}))\}.$$

(a) *Then Φ_k is diophantine in $\mathbb{Q}$.*

(b) *If $k = 3, 5$ or 7 and if $p \in \Phi_k$, then $\mathbb{P}^{[k]}(p) \neq \emptyset$ and*

$$\{0\} \neq J(R_p^{[k]}) = \begin{cases} J_{-1,-p} + J_{2,-p} & \textit{if } k = 3, \\ J_{-2,-p} + J_{2,-p} & \textit{if } k = 5, \\ J_{-1,-p} + J_{-2,p} & \textit{if } k = 7. \end{cases}$$

In particular, in each of the cases, the Jacobson radical is diophantine in $\mathbb{Q}$, by a formula that is uniform in p.

(c) *Ψ is diophantine in $\mathbb{Q}$.*

Proof. (a) It is clear that '$p > 0$' is diophantine. It is also clear from Proposition 10(a) that, for $k = 1, 3, 5$ and 7, the property '$p \equiv k \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)})$' is diophantine.

Moreover, if $v_2(p)$ is even and $k' = 3, 5$ or 7 then, by Proposition 10(b),

$$\mathbb{P}^{[k']}(p) = \emptyset \iff p \in (\mathbb{Q}^\times)^2 \cdot (R_p^{[k']})^\times.$$

(Note that we are *not* assuming that $p \equiv k' \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)})$.) So the property on the left is diophantine. But then so are

$$\Phi_1 = \{p \equiv 1 \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)}) \mid p > 0,\ \mathbb{P}_3(p) = \emptyset,\ \mathbb{P}_5(p) = \emptyset \text{ and } \mathbb{P}_7(p) = \emptyset\},$$
$$\Phi_3 = \{p \equiv 3 \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)}) \mid p > 0,\ \mathbb{P}^5(p) = \emptyset \text{ and } \mathbb{P}^7(p) = \emptyset\},$$
$$\Phi_5 = \{p \equiv 5 \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)}) \mid p > 0,\ \mathbb{P}^3(p) = \emptyset \text{ and } \mathbb{P}^7(p) = \emptyset\},$$
$$\Phi_7 = \{p \equiv 7 \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)}) \mid p > 0,\ \mathbb{P}^3(p) = \emptyset \text{ and } \mathbb{P}^5(p) = \emptyset\}.$$

(b) Assume $k = 3, 5$ or 7 and that $p \in \Phi_k$. Then $p \equiv k \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)})$ and so, by Proposition 10(b), $R_p^{[k]} = \bigcap_{l \in \mathbb{P}^{[k]}(p)} \mathbb{Z}_{(l)}$. As $p > 0$ and $p \equiv k \ (\mathrm{mod}\ 8\mathbb{Z}_{(2)})$, $\mathbb{P}^{[k]}(p) \neq \emptyset$ and hence $J(R_p^{[k]}) = \bigcap_{l \in \mathbb{P}^{[k]}(p)} l\mathbb{Z}_{(l)} \neq \{0\}$. The explicit formulas now follow from Lemma 14, as the assumptions of the lemma are satisfied in each case.

Part (c) follows directly from (a) and (b). □

The most difficult case is when $p \in \Phi_1$. Recall from Definition 7 and from Proposition 10(c) that, for $p, q \in \mathbb{Q}^\times$, we have defined $R^{[1]}_{p,q} := T_{-2p,q} + T_{2p,q}$ and $\mathbb{P}(p,q) := \Delta_{-2p,q} \cap \Delta_{2p,q}$.

Proposition 16.

(a) *If* $(p,q) \in \Psi$, *then* $\mathbb{P}(p,q) \neq \emptyset$;

(b) *if* $(p,q) \in \Psi$, *then* $J(R^{[1]}_{p,q}) = J_{-2p,q} + J_{2p,q}$;

(c) *the set* $\{(p,q,x) \in \mathbb{Q}^3 \mid (p,q) \in \Psi$ *and* $x \in J(R^{[1]}_{p,q})\}$ *is diophantine.*

Proof. (a) Assume $(p,q) \in \Psi$. Multiplying p or q by nonzero rational squares does not change $R^{[1]}_{p,q}$ or $J_{-2p,q}$ or $J_{2p,q}$, so we can assume that p and q are squarefree positive integers. Since $p \equiv 1 \pmod{8\mathbb{Z}_{(2)}}$ and $q \equiv 3$ $(\bmod\ 8\mathbb{Z}_{(2)})$, we have, by Observation 5, $(2p,q)_2 = -1$. By Hilbert reciprocity, there must also be an odd prime l such that $(2p,q)_l = -1$. By definition of Ψ and, again, by Observation 5, this implies that $l \in \{1,3\} + 8\mathbb{Z}_{(2)}$ and $l \notin \mathbb{P}^{[3]}(q)$. These two conditions imply $(-1,q)_l = 1$. Multiplying yields $(-2p,q)_l = -1$. Thus $l \in \mathbb{P}(p,q)$.

Part (b) is immediate from (a) and Lemma 14.

Part (c) follows from Corollary 15(c), from (b) and the note preceding Lemma 13. □

Step 4: *From existential to universal.* Let R be a semilocal subring of $\mathbb{Q}$; i.e., $R = \bigcap_{l \in \Delta} \mathbb{Z}_{(l)}$ for some finite $\Delta \subseteq \mathbb{P}$. Define

$$\widetilde{R} := \{x \in \mathbb{Q} \mid \neg\exists y \in J(R) \text{ with } xy = 1\}.$$

Lemma 17.

(a) *If* $J(R)$ *is diophantine in* $\mathbb{Q}$, *then* $\widetilde{R}$ *is defined by a* universal *formula in* $\mathbb{Q}$;

(b) $\widetilde{R} = \bigcup_{l \in \Delta} \mathbb{Z}_{(l)}$, *provided* $\Delta \neq \emptyset$, *i.e., provided* $R \neq \mathbb{Q}$;

(c) *in particular, if* $R = \mathbb{Z}_{(p)}$ *for some* $p \in \mathbb{P}$, *then* $\widetilde{R} = R$.

Proof. (a) is obvious from the definition of $\widetilde{R}$, and (c) is a special case of (b). So we only need to prove (b).

For the inclusion '$\subseteq$,' pick $x \in \widetilde{R}$ and assume that $x \notin \bigcup_{l \in \Delta} \mathbb{Z}_{(l)}$. Then for all $l \in \Delta$, $v_l(x) < 0$, and hence $y := x^{-1} \in \bigcap_{l \in \Delta} l\,\mathbb{Z}_{(l)} = J(R)$, contradicting our assumption that $x \in \widetilde{R}$.

For the converse inclusion '$\supseteq$,' assume $x \in \mathbb{Z}_{(l)}$ for some $l \in \Delta$. Then, for any $y \in J(R)$, $x \cdot y \in l\,\mathbb{Z}_{(l)}$ so, in particular, $x \cdot y \neq 1$. □

Now we can give our universal definition of $\mathbb{Z}$ in $\mathbb{Q}$.

Proposition 18.

(a) $$\mathbb{Z} = \widetilde{\mathbb{Z}_{(2)}} \cap \left(\bigcap_{k=3,5,7} \bigcap_{p \in \Phi_k} \widetilde{R_p^{[k]}} \right) \cap \bigcap_{(p,q)\in\Psi} \widetilde{R_{p,q}^{[1]}},$$

where Φ_k *and* Ψ *are the diophantine sets defined in Corollary* 15;

(b) *for any* $t \in \mathbb{Q}$,

$$\begin{aligned} t \in \mathbb{Z} \Longleftrightarrow t &\in \widetilde{\mathbb{Z}_{(2)}} \\ &\wedge \forall p \bigwedge_{k=3,5,7} (t \in \widetilde{R_p^{[k]}} \vee p \notin \Phi_k) \\ &\wedge \forall p, q (t \in \widetilde{R_{p,q}^{[1]}} \vee (p,q) \notin \Psi); \end{aligned}$$

(c) (*Theorem* 1) *there is*, *for some positive integer* n, *a polynomial* $g \in \mathbb{Z}[t; x_1, \ldots, x_n]$ *such that*, *for any* $t \in \mathbb{Q}$,

$$t \in \mathbb{Z} \textit{ if and only if } \forall x_1 \cdots \forall x_n \in \mathbb{Q}\ g(t; x_1, \ldots, x_n) \neq 0.$$

Proof. (a) The equation is valid by Proposition 10, by Lemma 17(b) (which applies by Corollary 15(b) and Proposition 16(a)) and by Lemma 17(c).

(b) This is a reformulation of (a) revealing that the formula thus obtained for $\mathbb{Z}$ in $\mathbb{Q}$ *is* universal: the $\widetilde{R}$'s are universal by Corollary 15, Proposition 16 and Lemma 17(a); Φ_k and Ψ are existential by Corollary 15(a) and (c), so their negation is universal as well.

(c) This is immediate from (b). □

3. More diophantine predicates in $\mathbb{Q}$

From the results and techniques of Section 2, one obtains new diophantine predicates in $\mathbb{Q}$. They are of interest in their own right, but maybe they can also be used to show that Hilbert's 10th problem over $\mathbb{Q}$ cannot be solved, not by defining or interpreting $\mathbb{Z}$ in $\mathbb{Q}$ but, e.g., by assigning graphs to the various finite sets of primes encoded in these predicates and using graph theoretic undecidability results. We will also use some of these new predicates for our $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ that uses just one universal quantifier (Corollary 22).

Before listing the new diophantine predicates we shall first introduce one last notation and prove another technical lemma.

Definition 19. For $p \in \Phi_1$, define

$$S_p := \{x \in \mathbb{Q} \mid \exists q \text{ with } (p,q) \in \Psi, q \in (R_{p,q}^{[1]})^\times \text{ and } x \in R_{p,q}^{[1]}\}.$$

Note that if $p \in \Phi_1$ is a square, then there is no q with $(p,q) \in \Psi$, and hence $S_p = \emptyset$.

Lemma 20. *Assume* $p \in \Phi_1$. *Then*

(a) S_p *is diophantine in* $\mathbb{Q}$;

(b) $S_p = \bigcup_{l\in\mathbb{P}(p)} \mathbb{Z}_{(l)}$ *(which is* $\emptyset$ *if* $\mathbb{P}(p) = \emptyset$, *i.e., if* $p \in \mathbb{Q}^2$*)*;
(c) *in particular, if* p *is a prime* $\equiv 1 \bmod 8$, *then* $S_p = \mathbb{Z}_{(p)}$.

Proof. (a) That S_p is diophantine in $\mathbb{Q}$ is immediate from Corollary 15.

(b) To show that $S_p \subseteq \bigcup_{l\in\mathbb{P}(p)} \mathbb{Z}_{(l)}$, assume that $x \in S_p$. So we can choose $q \in \mathbb{Q}$ such that $(p,q) \in \Psi$, $q \in (R^{[1]}_{p,q})^\times$ and $x \in R^{[1]}_{p,q}$. By Proposition 10(c),

$$R^{[1]}_{p,q} = \bigcap_{l\in\mathbb{P}(p,q)} \mathbb{Z}_{(l)}, \text{ where } \mathbb{P}(p,q) = \Delta_{-2p,q} \cap \Delta_{2p,q}.$$

By Proposition 16(a), $\mathbb{P}(p,q) \neq \emptyset$, so we may pick some $l \in \mathbb{P}(p,q)$. As $q \in (R^{[1]}_{p,q})^\times$, $v_l(q) = 0$ and so $l \notin \mathbb{P}(q)$. As $(p,q) \in \Phi_1 \times \Phi_3$, by Observation 5, also $2 \notin \mathbb{P}(p,q)$ and so $l \neq 2$. Hence, again by Observation 5, $l \in \mathbb{P}(p)$. As l was a freely chosen element in $\mathbb{P}(p,q)$, this shows that $\mathbb{P}(p,q) \subseteq \mathbb{P}(p)$. Thus

$$x \in R^{[1]}_{p,q} = \bigcap_{l\in\mathbb{P}(p,q)} \mathbb{Z}_{(l)} \subseteq \bigcup_{l\in\mathbb{P}(p)} \mathbb{Z}_{(l)}.$$

Conversely, suppose $l \in \mathbb{P}(p)$ and $x \in \mathbb{Z}_{(l)}$. Choose a prime $q \equiv 3 \bmod 8$ with $\left(\frac{l}{q}\right) = -1$ and with $\left(\frac{l'}{q}\right) = 1$ for each $l' \in \mathbb{P}(p) \setminus \{l\}$.

Then $\left(\frac{pq^{-v_q(p)}}{q}\right) = \prod_{l'\in\mathbb{P}(p)} \left(\frac{l'}{q}\right) = -1$, so $\phi_q(pq^{-v_q(p)})$ is a nonsquare in $\mathbb{F}_q$, i.e., $\in 2\cdot(\mathbb{F}_q^\times)^2$. As $p \in \Phi_1$, $v_q(p)$ is even, and so $p \in 2\cdot(\mathbb{Q}^\times)^2(1+q\mathbb{Z}_{(q)})$. Hence $(p,q) \in \Psi$.

We will now deduce that $\mathbb{P}(p,q) = \{l\}$. As $l \in \mathbb{P}(p)$ and $p \in \Phi_1$, we have that $l \equiv 1 \bmod 8$ and therefore $\left(\frac{q}{l}\right) = \left(\frac{l}{q}\right) = -1$. Hence $l \in \mathbb{P}(p,q)$. On the other hand, for any $l' \in \mathbb{P}(p)\setminus\{l\}$, $\left(\frac{l'}{q}\right) = \left(\frac{q}{l'}\right) = 1$, so $l' \notin \mathbb{P}(p,q)$. Finally, since $(-1,q)_q = \left(\frac{-1}{q}\right) = -1$, either $(2p,q)_q$ or $(-2p,q)$ is 1, so $q \notin \Delta_{2p,q} \cap \Delta_{-2p,q} = \mathbb{P}(p,q)$.

Thus $R^{[1]}_{p,q} = \mathbb{Z}_{(l)}$, so $x \in R^{[1]}_{p,q}$, $q \in (R^{[1]}_{p,q})^\times$ and hence $x \in S_p$.

(c) This is immediate from part (b). □

PROPOSITION 21. *For* $x, y \in \mathbb{Q}^\times$, *the following properties are diophantine*:
(a) *for fixed* $k \in \{3,5,7\}$, *the property that* $x, y \in \Phi_k$ *and* $\mathbb{P}^{[k]}(x) \cap \mathbb{P}^{[k]}(y) = \emptyset$;
(b) $x \notin \mathbb{Q}^2$;
(c) *for fixed* $k \in \{1,3,5,7\}$, *the property that* $x \equiv k \pmod{8\mathbb{Z}_{(2)}}$ *and* $x \notin \Phi_k$;
(d) *for fixed* $k \in \{3,5,7\}$, *the property that* $\mathbb{P}^{[k]}(x) = \emptyset$;
(e) $x \notin N(y)$, *where* $N(y)$ *is the image of the norm* $\mathbb{Q}(\sqrt{y}) \to \mathbb{Q}$.

Proof. (a) By Corollary 15(a), Φ_k is diophantine. By Corollary 15(b), for any $x \in \Phi_k$, $\mathbb{P}^{[k]}(x) \neq \emptyset$ and hence $J(R^{[k]}_x)$ is diophantine. Now let $x, y \in \Phi_k$ and recall that, by Proposition 10(b), $R^{[k]}_x = \bigcap_{l\in\mathbb{P}^{[k]}(x)} \mathbb{Z}_{(l)}$, and likewise for $R^{[k]}_y$. So we have the equivalence

$$\mathbb{P}^{[k]}(x) \cap \mathbb{P}^{[k]}(y) = \emptyset \iff 1 \in J(R^{[k]}_x) + J(R^{[k]}_y).$$

(b) The property that '$v_2(x)$ is odd' is diophantine: $v_2(x)$ is odd if and only if $x = 2yz^2$ for some $y \in \mathbb{Z}_{(2)}^{\times}$ and some $z \in \mathbb{Q}^{\times}$. As the property '$x < 0$' is diophantine as well, by Corollary 15(a) and (b) it suffices to show

$$x \notin \mathbb{Q}^2 \iff \begin{cases} x < 0 \text{ or } v_2(x) \text{ is odd or,} \\ \exists p \in \Phi_3 \text{ with } x \in 2 \cdot (\mathbb{Q}^{\times})^2 \cdot (1 + J(R_p^{[3]})). \end{cases}$$

'$\Rightarrow$': Assume that $x \notin \mathbb{Q}^2$, that $x > 0$ and that $v_2(x)$ is even. Multiplying x by a nonzero rational square does not change the truth of either side of the implication, so we may assume that $x = p_1 \cdots p_r$ for distinct odd primes $p_1, \ldots, p_r$ where $r \geq 1$.

$$\text{Choose } a_1 \in \mathbb{Z} \text{ with } \left(\frac{a_1}{p_1}\right) = \begin{cases} -1 & \text{if } p_1 \equiv 1 \mod 4, \\ 1 & \text{if } p_1 \equiv 3 \mod 4, \end{cases}$$

and for $i > 1$,

$$\text{choose } a_i \in \mathbb{Z} \text{ with } \left(\frac{a_i}{p_i}\right) = \begin{cases} 1 & \text{if } p_i \equiv 1 \mod 4, \\ -1 & \text{if } p_i \equiv 3 \mod 4. \end{cases}$$

Finally, choose a prime $p \equiv 3 \bmod 8$ with $p \equiv a_i \bmod p_i$ $(i = 1, \ldots, r)$. Then, by the Quadratic Reciprocity Law, $\left(\frac{x}{p}\right) = -1$.

By definition, $p \in \Phi_3$. By the last statement in Proposition 10(b), $R_p^{[3]} = \mathbb{Z}_{(p)}$. Hence $x \in 2 \cdot (\mathbb{Q}^{\times})^2 \cdot (1 + J(R_p^{[3]}))$, as $\left(\frac{2}{p}\right) = -1$.

'$\Leftarrow$': If $x < 0$ or $v_2(x)$ is odd, then $x \notin \mathbb{Q}^2$.

Suppose that $p \in \Phi_3$ and $x \in 2 \cdot (\mathbb{Q}^{\times})^2 \cdot (1 + J(R_p^{[3]}))$. By Corollary 15(b), $\mathbb{P}^{[3]}(p)$ contains a prime l, and $J(R_p^{[3]}) \subseteq l\mathbb{Z}_l$. Thus $x \in 2(\mathbb{Q}_l^{\times})^2$. But $l \equiv 3 \bmod 8$, so $\left(\frac{2}{l}\right) = 1$, and hence $2 \notin (\mathbb{Q}_l^{\times})^2$. Thus $x \notin \mathbb{Q}_l^2$, so $x \notin \mathbb{Q}^2$.

(c) By Proposition 10(a), $x \equiv k \pmod{8\mathbb{Z}_{(2)}}$ is diophantine. Let us first consider the case $k = 1$. Assume $x \equiv 1 \pmod{8\mathbb{Z}_{(2)}}$. Then $x \notin \Phi_1$ if and only if $x \leq 0$, or $x > 0$ and for some $k' \in \{3, 5, 7\}$, $\mathbb{P}^{[k']}(x) \neq \emptyset$. This last condition can be expressed diophantinely by distinguishing whether the number of $k' \in \{3, 5, 7\}$ with $\mathbb{P}^{[k']}(x) \neq \emptyset$ is 1, 2 or 3.

If it is 1, say $\mathbb{P}^{[k']}(x) \neq \emptyset$, then $\#\mathbb{P}^{[k']}(x)$ must be even (in order to get $x \equiv 1 \pmod{8\mathbb{Z}_{(2)}}$), so we can choose $p \in \mathbb{P}^{[k']}(x)$ and let

$$y := p^{v_p(x)} \text{ and } y' := \prod_{l \in \mathbb{P}^{[1]}(x)} l^{v_l(x)} \prod_{l \in \mathbb{P}^{[k']}(x) \setminus \{p\}} l^{v_l(x)}.$$

Then $y, y' \in \Phi_{k'}$, $\mathbb{P}^{[k']}(y) \cap \mathbb{P}^{[k']}(y') = \emptyset$ and $x = yy'z^2$ for some $z \in \mathbb{Q}^{\times}$. By (a), the condition that there exist such y, y' and z is diophantine and, when satisfied, it implies $x \notin \Phi_1$.

If $\{k' \in \{3,5,7\} \mid \mathbb{P}^{[k']}(x) \neq \emptyset\} = \{k_1, k_2\}$ for distinct k_1, k_2, then both $\#\mathbb{P}^{[k_1]}(x)$ and $\#\mathbb{P}^{[k_2]}(x)$ must be even, again, and so one constructs similarly $y_1, y_1' \in \Phi_{k_1}$ and $y_2, y_2' \in \Phi_{k_2}$ with $\mathbb{P}^{[k_i]}(y_i) \cap \mathbb{P}^{[k_i]}(y_i') = \emptyset$ for $i = 1, 2$ such that $x = y_1 y_1' y_2 y_2' z^2$ for some $z \in \mathbb{Q}^\times$.

If $\mathbb{P}^{[k']}(x) \neq \emptyset$ for all three $k' \in \{3,5,7\}$, then either all three sets have an even number of elements or all three have an odd number of elements, and in either case it is clear how to proceed along the same lines.

Now consider the case $k = 3$ and assume $x \equiv 3 \pmod{8\mathbb{Z}_{(2)}}$. Then $x \notin \Phi_3$ if and only if $x \leq 0$, or $x > 0$ and $\mathbb{P}^{[5]}(x) \neq \emptyset$ or $\mathbb{P}^{[7]}(x) \neq \emptyset$. Here the last condition can be seen to be diophantine again by distinguishing whether the number of $k' \in \{5,7\}$ with $\mathbb{P}^{[k']}(x) \neq \emptyset$ is 1 or 2 etc.

It is clear how similar existential formulas can be written down for '$x \equiv k \pmod{8\mathbb{Z}_{(2)}}$ and $x \notin \Phi_k$' in case $k = 5$ or in case $k = 7$.

To put it all in one we thus see that, for $x \in \mathbb{Q}^{>0}$ such that $x \equiv k \pmod{8\mathbb{Z}_{(2)}}$, we have $x \notin \Phi_k$ if and only if for some $r \geq 1$ there exist numbers $k_1, \ldots, k_r \in \{3,5,7\}$ not all equal to k, with each number appearing no more than twice, and $y_i \in \Phi_{k_i}$ for each i and $z \in \mathbb{Q}^\times$, such that $x = y_1 \cdots y_r z^2$ and such that, whenever $i \neq j$ and $k_i = k_j$, we have $\mathbb{P}^{[k_i]}(y_i) \cap \mathbb{P}^{[k_j]}(y_j) = \emptyset$.

(d) $\mathbb{P}^{[3]}(x) = \emptyset$ if and only if, modulo a nonzero rational square factor, x or $-x$ or $2x$ or $-2x$ is a product of primes in $\bigcup_{k=1,5,7} \mathbb{P}^{[k]}$. Note that for a fixed $k \in \{1,5,7\}$, each product of primes in $\mathbb{P}^{[k]} \cup \mathbb{P}^{[1]}$ can be expressed as a product of one or two elements in Φ_k. Let $\Phi_k' = \Phi_k \cup \{1\}$, which is diophantine by Corollary 15(a). Let P_k be the set of all finite products of primes in $\mathbb{P}^{[k]} \cup \mathbb{P}^{[1]}$. Then $P_k \cdot (\mathbb{Q}^\times)^2 = \Phi_k' \Phi_k'$, and

$$\{x : \mathbb{P}^{[3]}(x) = \emptyset\} = \{1, -1, 2, -2\} P_1 P_5 P_7 = \bigcup_{k=1,5,7} \Phi_k' \Phi_k'.$$

Thus the condition $\mathbb{P}^{[3]}(x) = \emptyset$ is diophantine. Similarly, the condition $\mathbb{P}^{[k]}(x) = \emptyset$ is diophantine for $k = 5$ and $k = 7$.

(e) $x \notin N(y)$ if and only if

$$\begin{aligned}
&(x < 0 \wedge y < 0)\\
&\quad \vee \bigvee_{k=3,5,7} \exists p \in \Phi_k \text{ with}\\
&\quad \Big(\big(x \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_p^{[k]})^\times\big) \wedge \big(y \text{ or } -xy \in a_k \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[k]}))\big)\\
&\qquad \vee \big(y \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_p^{[k]})^\times\big) \wedge \big(x \text{ or } -xy \in a_k \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_p^{[k]}))\big)\Big)\\
&\quad \vee \exists (p,q) \in \Psi \text{ with } q \in (R_{p,q}^{[1]})^\times \text{ and}\\
&\quad \Big(\big(x \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_{p,q}^{[1]})^\times\big) \wedge \big(y \text{ or } -xy \in q \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_{p,q}^{[1]}))\big)\\
&\qquad \vee \big(y \in p \cdot (\mathbb{Q}^\times)^2 \cdot (R_{p,q}^{[1]})^\times\big) \wedge \big(x \text{ or } -xy \in q \cdot (\mathbb{Q}^\times)^2 \cdot (1 + J(R_{p,q}^{[1]}))\big)\Big),
\end{aligned}$$

where $a_3 = a_5 = 2$ and $a_7 = -1$.

This uses Observation 5(b) and (c), Corollary 15(b) and (c), the previous parts and the local-global principle for norms.

The first line says that $x \notin N(y)$ over $\mathbb{R}$.

Lines 2–4 say that $x \notin N(y)$ over $\mathbb{Q}_l$ for some nonempty set of primes $l \equiv 3, 5$ or $7 \bmod 8$: Fix $k \in \{3, 5, 7\}$. By Corollary 15(b), $p \in \Phi_k$ implies that $\mathbb{P}^{[k]}(p) \neq \emptyset$. We claim that

$$(x, y)_l = -1 \text{ for some } l \in \mathbb{P}^{[k]} \Longleftrightarrow \exists p \in \Phi_k \text{ with } (\cdots)\,,$$

where $(\cdots)$ is the bracket in lines 3 and 4.

'$\Rightarrow$': Assume $l \in \mathbb{P}^{[k]}$ with $(x, y)_l = -1$. Let $p = l$. Then $R_p^{[k]} = \mathbb{Z}_l$ and '$(\cdots)$' says that $v_l(x)$ is odd and $yl^{-v_l(y)}$ or $-xyl^{-v_l(xy)}$ is a quadratic nonresidue $\bmod l$ or the same with x and y swapped. By Observation 5, this is equivalent to $(x, y)_l = -1$, so it holds by our assumption.

'$\Leftarrow$': Suppose $p \in \Phi_k$ satisfies '$(\cdots)$.' Then $\mathbb{P}^{[k]}(p) \neq \emptyset$ and, for any $l \in \mathbb{P}^{[k]}(p)$, $v_l(x)$ is odd and, by the choice of a_k, either $yl^{-v_l(y)}$ or $-xyl^{-v_l(xy)}$ is a quadratic nonresidues $\bmod l$ or the same with x and y swapped, so $(x, y)_l = -1$.

Lines 5–7 say that $x \notin N(y)$ over $\mathbb{Q}_l$ for some nonempty set of primes $l \equiv 1 \bmod 8$. As in the proof of Lemma 20, the condition '$q \in (R_{p,q}^{[1]})^\times$' makes sure that, in the terminology of Proposition 10(c), $\mathbb{P}(p, q) \cap \mathbb{P}(q) = \emptyset$, so $\mathbb{P}(p, q) \subseteq \mathbb{P}(p)$. And, by Proposition 16(a), $\mathbb{P}(p, q) \neq \emptyset$. Line 6 and 7 then say that $x \notin N(y)$ over $\mathbb{Q}_l$ for any $l \in \mathbb{P}(p, q)$. Note that the role of a_k in lines 3 and 4 of being a quadratic nonresidue $\bmod l$ for all $l \in \mathbb{P}^{[k]}$ is here taken by q that is a quadratic nonresidue for all $l \in \mathbb{P}^{[1]}(p)$ with $(p, q) \in \Psi$.

We could disregard the prime $p = 2$, as '$x \notin N(y)$' either happens nowhere locally, or at least at two primes in $\mathbb{P} \cup \{\infty\}$. □

The result in (b) was also obtained in [Poo09b], using a deep result on Châtelet surfaces from [CTCS80]. Our proof is elementary. It has recently been generalized in [CTVG14] to all n-th powers: for any natural number n, the set of non-n-th powers is diophantine in $\mathbb{Q}$.

Let us also mention that (b) follows from (e): $x \notin \mathbb{Q}^2 \Leftrightarrow \exists y\; x \notin N(y)$ (and we did not use (b) in order to prove (e)).

We close this section by showing that there is an $\forall\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$ with just one universal quantifier.

Corollary 22. *For all $t \in \mathbb{Q}$, $t \in \mathbb{Z}$ if and only if*

$$\forall p \left(t \in \mathbb{Z}_{(2)} \wedge \begin{cases} \big(p \in \mathbb{Q}^2 \cdot (2 + 4\mathbb{Z}_{(2)})\big) \\ \vee \bigvee_{k=1,3,5,7} \begin{cases} \big(p \neq 0 \wedge p \in \mathbb{Q}^2 \cdot (k + 8\mathbb{Z}_{(2)})\big) \\ \wedge \Big(\big(p \notin \Phi_k\big) \vee p \in \mathbb{Q}^2 \vee \Big(p \in \Phi_k \setminus \mathbb{Q}^2 \wedge t \in R_p^{[k]}\Big)\Big) \end{cases} \end{cases} \right).$$

Proof. This follows from Proposition 10(a) and (b) and by Lemma 20. That the resulting formula is of the shape $\forall\exists$ with just one universal quantifier '$\forall p$' follows from Proposition 10, Corollary 15, Lemma 20 and Proposition 21. Note that, under the assumption '$p \in \mathbb{Q}^2 \cdot (k + 8\mathbb{Z}_{(2)})$,' the property '$p \notin \Phi_k$' is equivalent to '$p \notin \mathbb{Z}_{(2)}^{\times}$ or ($p \in k + \mathbb{Z}_{(2)}$ and $p \notin \Phi_k$),' which is diophantine by Proposition 21(c). And '$p \notin \mathbb{Q}^2$' is diophantine by 21(b). □

4. **A model theoretic outlook**

If $\mathbb{Q}^\star$ is a field elementarily equivalent to $\mathbb{Q}$ (in the first-order language of rings, $\mathcal{L}_{\text{ring}} := \{+, \cdot; 0, 1\}$) or, equivalently, if $\mathbb{Q}^\star$ is a model of $\mathrm{Th}(\mathbb{Q})$, the first-order theory of $\mathbb{Q}$, then it makes sense to speak of the *ring of integers* $\mathbb{Z}^\star$ of $\mathbb{Q}^\star$: $\mathbb{Z}^\star = \phi(\mathbb{Q}^\star)$, where $\phi(x)$ is any $\mathcal{L}_{\text{ring}}$-formula in one free variable defining $\mathbb{Z}$ in $\mathbb{Q}$. It is part of $\mathrm{Th}(\mathbb{Q})$ that any two such formulas define the same set. So it does not make a difference whether ϕ is Julia Robinson's formula or Bjorn Poonen's or ours.

There is a well-known general model theoretic criterion for definable subsets of first-order structures to be *existentially* definable. (It follows immediately from, e.g., Lemma 3.1.6 in [PD11].) For $\mathbb{Z}$ in $\mathbb{Q}$, this criterion reads as follows:

> *$\mathbb{Z}$ is diophantine in $\mathbb{Q}$ if and only if, for any two models $\mathbb{Q}^\star$, $\mathbb{Q}^{\star\star}$ of* $\mathrm{Th}(\mathbb{Q})$ *with $\mathbb{Q}^\star \subseteq \mathbb{Q}^{\star\star}$ and with rings of integers $\mathbb{Z}^\star$, $\mathbb{Z}^{\star\star}$ respectively, the inclusion $\mathbb{Z}^\star \subseteq \mathbb{Z}^{\star\star}$ also holds.*

Let us conclude with a collection of closure properties for pairs of models of $\mathrm{Th}(\mathbb{Q})$, one a substructure of the other, which might have a bearing on the question whether or not $\mathbb{Z}$ is diophantine in $\mathbb{Q}$.

Proposition 23. *Let $\mathbb{Q}^\star, \mathbb{Q}^{\star\star}$ be models of* $\mathrm{Th}(\mathbb{Q})$ *(i.e., elementary extensions of $\mathbb{Q}$) with $\mathbb{Q}^\star \subseteq \mathbb{Q}^{\star\star}$ (as $\mathcal{L}_{\text{ring}}$-substructure, so $\mathbb{Q}^\star$ is a subfield of $\mathbb{Q}^{\star\star}$), and let $\mathbb{Z}^\star$ and $\mathbb{Z}^{\star\star}$ be their rings of integers. Then*

(a) $\mathbb{Z}^{\star\star} \cap \mathbb{Q}^\star \subseteq \mathbb{Z}^\star$;
(b) $\mathbb{Z}^{\star\star} \cap \mathbb{Q}^\star$ *is integrally closed in* $\mathbb{Q}^\star$;
(c) *for each $n \in \mathbb{N}$, $(\mathbb{Q}^{\star\star})^n \cap \mathbb{Q}^\star = (\mathbb{Q}^\star)^n$ — i.e., $\mathbb{Q}^\star$ is radically closed in $\mathbb{Q}^{\star\star}$*;
(d) *if $\mathbb{Z}$ is diophantine in $\mathbb{Q}$, then $\mathbb{Z}^{\star\star} \cap \mathbb{Q}^\star = \mathbb{Z}^\star$ and $\mathbb{Q}^\star$ is algebraically closed in $\mathbb{Q}^{\star\star}$.*

Proof. (a) is an immediate consequence of our universal definition of $\mathbb{Z}$ in $\mathbb{Q}$. The very same definition holds for $\mathbb{Z}^\star$ in $\mathbb{Q}^\star$ and for $\mathbb{Z}^{\star\star}$ in $\mathbb{Q}^{\star\star}$. So if this universal formula holds for $x \in \mathbb{Z}^{\star\star} \cap \mathbb{Q}^\star$ in $\mathbb{Q}^{\star\star}$, it also holds in $\mathbb{Q}^\star$, i.e. $x \in \mathbb{Z}^\star$.

(b) is true because $\mathbb{Z}^{\star\star}$ is integrally closed in $\mathbb{Q}^{\star\star}$.

(c) The nontrivial inclusion follows since the property of not being an n-th power is, by the main result in [CTVG14], diophantine in $\mathbb{Q}$. (For $n = 2$, this was shown in [Poo09b], an elementary proof being given in our Proposition 21(b).)

(d) If $\mathbb{Z}$ is diophantine in $\mathbb{Q}$, then $\mathbb{Z}^{\star\star} \cap \mathbb{Q}^\star \supseteq \mathbb{Z}^\star$ and hence by (a), equality holds.

To show that $\mathbb{Q}^\star$ is then also algebraically closed in $\mathbb{Q}^{\star\star}$, let us observe that, for each $n \in \mathbb{N}$,

$$A_n := \{(a_0, \dots, a_{n-1}) \in \mathbb{Z}^n \mid \exists x \in \mathbb{Z} \text{ with } x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0\}$$

is decidable: zeros of polynomials in one variable are bounded in terms of their coefficients, so one only has to check finitely many $x \in \mathbb{Z}$. In particular, by (for short) Matiyasevich's Theorem, there is an $\exists$-formula $\phi(t_0, \dots, t_{n-1})$ such that

$$\mathbb{Z} \models \forall t_0 \cdots t_{n-1} \left(\{\forall x [x^n + t_{n-1}x^{n-1} + \cdots + t_0 \neq 0]\} \leftrightarrow \phi(t_0, \dots, t_{n-1}) \right).$$

Since both A_n and its complement in $\mathbb{Z}^n$ are diophantine in $\mathbb{Z}$, the same holds in $\mathbb{Q}$, by our assumption of $\mathbb{Z}$ being diophantine in $\mathbb{Q}$: both A_n and its complement in $\mathbb{Q}^n$ are diophantine in $\mathbb{Q}$, and so $A_n^{\star\star} \cap (\mathbb{Q}^\star)^n = A_n^\star$. As any finite extension of $\mathbb{Q}^\star$ is generated by an element integral over $\mathbb{Z}^\star$, this implies that $\mathbb{Q}^\star$ is relatively algebraically closed in $\mathbb{Q}^{\star\star}$. □

The strongest closure property a complete first-order theory (whose models are infinite) might have is that it is model complete, that is, that if one model of the theory is a substructure of another model, it is an *elementary* substructure or, equivalently, that the smaller model is existentially closed in the larger model. Let us show that $\mathrm{Th}(\mathbb{Q})$ does not have this strong closure property.

Remark 24. $\mathbb{Q}$ is not model complete; i.e., there are models $\mathbb{Q}^\star$ and $\mathbb{Q}^{\star\star}$ of $\mathrm{Th}(\mathbb{Q})$ with $\mathbb{Q}^\star \subseteq \mathbb{Q}^{\star\star}$ such that $\mathbb{Q}^\star$ is not existentially closed in $\mathbb{Q}^{\star\star}$.

Proof. Choose a recursively enumerable subset $A \subseteq \mathbb{Z}$ that is not decidable. Then $B := \mathbb{Z} \setminus A$ is definable in $\mathbb{Z}$ and hence in $\mathbb{Q}$. If B were diophantine in $\mathbb{Q}$, it would be recursively enumerable. But then A would be decidable: contradiction.

So not every definable subset of $\mathbb{Q}$ is diophantine in $\mathbb{Q}$, and hence $\mathbb{Q}$ is not model complete. Or, in other words, there are models $\mathbb{Q}^\star, \mathbb{Q}^{\star\star}$ of $\mathrm{Th}(\mathbb{Q})$ with $\mathbb{Q}^\star \subseteq \mathbb{Q}^{\star\star}$ where $\mathbb{Q}^\star$ is not existentially closed in $\mathbb{Q}^{\star\star}$. □

Replacing the condition that a model of $\mathrm{Th}(\mathbb{Q})$ that is a substructure of another model should be existentially closed with respect to *arbitrary* existential formulas by the weaker condition where only existential formulas with *one* existential quantifier are considered amounts to asking the smaller model to be relatively algebraically closed in the larger model. While we know, by Proposition 23(c), that the smaller model is radically closed in the larger model, we have no answer to the following:

Question 25. For $\mathbb{Q}^\star \equiv \mathbb{Q}^{\star\star} \equiv \mathbb{Q}$ with $\mathbb{Q}^\star \subseteq \mathbb{Q}^{\star\star}$, is $\mathbb{Q}^\star$ always algebraically closed in $\mathbb{Q}^{\star\star}$?

By Proposition 23(d), a negative answer would imply that $\mathbb{Z}$ is not diophantine in $\mathbb{Q}$.

References

[CTCS80] J.-L. Colliot-Thélène, D. Coray, and J.-J. Sansuc, Descente et principe de Hasse pour certaines variétés rationnelles, *J. reine angew. Math.* **320** (1980), 150–191. MR 0592151. Zbl 0434.14019. http://dx.doi.org/10.1515/crll.1980.320.150.

[CTVG14] J.-L. Colliot-Thélène and J. Van Geel, Le complémentaire des puissances n-ièmes dans un corps de nombres est un ensemble diophantien, 2014. arXiv 1401.0915v1.

[CZ07] G. Cornelissen and K. Zahidi, Elliptic divisibility sequences and undecidable problems about rational points, *J. reine angew. Math.* **613** (2007), 1–33. MR 2377127. Zbl 1178.11076. http://dx.doi.org/10.1515/CRELLE.2007.089.

[Koe95] J. Koenigsmann, From p-rigid elements to valuations (with a Galois-characterization of p-adic fields), *J. reine angew. Math.* **465** (1995), 165–182, With an appendix by Florian Pop. MR 1344135. Zbl 0824.12006. http://dx.doi.org/10.1515/crll.1995.465.165.

[Par13] J. Park, A universal first-order formula defining the ring of integers in a number field, *Math. Res. Lett.* **20** (2013), 961–980. MR 3207365. Zbl 1298.11113. http://dx.doi.org/10.4310/MRL.2013.v20.n5.a12.

[Poo09a] B. Poonen, Characterizing integers among rational numbers with a universal-existential formula, *Amer. J. Math.* **131** (2009), 675–682. MR 2530851. Zbl 1179.11047. http://dx.doi.org/10.1353/ajm.0.0057.

[Poo09b] B. Poonen, The set of nonsquares in a number field is Diophantine, *Math. Res. Lett.* **16** (2009), 165–170. MR 2480570. Zbl 1183.14031. http://dx.doi.org/10.4310/MRL.2009.v16.n1.a16.

[PD11] A. Prestel and C. N. Delzell, *Mathematical Logic and Model Theory: A Brief Introduction*, *Universitext*, Springer-Verlag, New York, 2011. MR 3025452. Zbl 1241.03001. http://dx.doi.org/10.1007/978-1-4471-2176-3.

[Rob49] J. Robinson, Definability and decision problems in arithmetic, *J. Symbolic Logic* **14** (1949), 98–114. MR 0031446. Zbl 1241.03001. http://dx.doi.org/10.2307/2266510.

[Ser73] J-P. Serre, *A Course in Arithmetic*, *Grad. Texts in Math.* **7**, Springer-Verlag, New York, 1973. MR 0344216. Zbl 0256.12001.

(Received: November 22, 2010)
(Revised: August 2, 2015)

Mathematical Institute, University of Oxford, Oxford, UK
E-mail: koenigsmann@maths.ox.ac.uk