DEFINING $\mathbb{Z}$ USING UNIT GROUPS

BARRY MAZUR, KARL RUBIN, AND ALEXANDRA SHLAPENTOKH

To Henryk Iwaniec on his 75th birthday, with admiration

ABSTRACT. We consider first-order definability and decidability questions over rings of integers of algebraic extensions of $\mathbb{Q}$, paying attention to the uniformity of definitions. The uniformity follows from the simplicity of our first-order definition of $\mathbb{Z}$. Namely, we prove that for a large collection of algebraic extensions $K/\mathbb{Q}$,

$$\{x \in \mathscr{O}_K : \forall \varepsilon \in \mathscr{O}_K^\times \, \exists \delta \in \mathscr{O}_K^\times \text{ such that } \delta - 1 \equiv (\varepsilon - 1)x \pmod{(\varepsilon - 1)^2}\} = \mathbb{Z}$$

where $\mathscr{O}_K$ denotes the ring of integers of K. One of the corollaries of our results is undecidability of the field of constructible numbers, a question posed by Tarski in 1948.

CONTENTS

1. INTRODUCTION

We consider first-order definability and decidability questions over rings and fields of integers of algebraic extensions of $\mathbb{Q}$, paying attention to the uniformity of the manner in which definability is established.

Let K be an algebraic, possibly infinite, extension of $\mathbb{Q}$ and let $\mathscr{O}_K$ be the ring of integers of K.

2020 *Mathematics Subject Classification.* Primary 11U05.

Key words and phrases. Hilbert's Tenth Problem, Diophantine definition, First-order definition.

The authors would like to thank Caleb Springer for his careful reading of their paper and the anonymous Referee for very helpful comments and for pointing out the implication of our results for a question of Tarski.

The research for this paper was partially supported by DMS grants 2152098 (AS), 2152149 (BM), 2152262 (KR). AS was also partially supported by an ECU Creative Activity and Research Grant during the summer of 2022.

Question 1.1. Is there a first-order definition of $\mathbb{Z}$ over $\mathscr{O}_K$ in the language of rings?

Question 1.2. Is the first-order theory of $\mathscr{O}_K$ in the language of rings undecidable?

Question 1.3. Is the first-order theory of K in the language of rings undecidable?

It is well-known that if $\mathscr{O}_K$ is definable over K and the first-order theory of $\mathscr{O}_K$ is undecidable, then the first-order theory of K is undecidable. In this paper we concentrate on the first-order theory of rings of integers of infinite algebraic extensions of $\mathbb{Q}$ and then use some existing results on definability of the rings of integers of these fields over the fields to obtain undecidability results for fields.

In particular, we answer a question of A. Tarski concerning (un)decidability of the first-order theory of the field of constructible numbers (see [Tar48], Notes #10 and see Corollary 1.11 below) and a question posed by C. Martinez-Ranero, J. Utreras and C. Videla concerning undecidability of $K^{(d)}$, the compositum of all extensions of degree less or equal to a fixed integer d of a number field K (see [MRUV20]).

1.1. **The language of rings.** The first-order language $(0, 1, +, \times)$ of rings is essentially the language of polynomial equations. For a fixed ring R, a sentence in this language can be shown to be equivalent to one that has the form:

$$E_1 x_1 \dots E_r x_r \bigwedge_{i=1}^{\ell} P_i(x_1, \dots, x_r) = 0, \tag{1.4}$$

where each E_i is either the universal or the existential quantifier ranging over R and each P_i is a polynomial with coefficients in $\mathbb{Z}$.

The first-order theory of a countable ring R is the set of all sentences of the form (1.4) that are true over R.

Using this language we can define subsets of our ring:

$$A = \{a \in R | E_1 x_1 \dots E_r x_r \bigwedge_{i=1}^{\ell} P_i(a, x_1, \dots, x_r) = 0\}, \tag{1.5}$$

where as above each E_i is either the universal or the existential quantifier ranging over R and P_i are polynomials over $\mathbb{Z}$. That is, an element $a \in R$ is in A if and only if the sentence $E_1 x_1 \dots E_r x_r \bigwedge_{i=1}^{\ell} P_i(a, x_1, \dots, x_r) = 0$ is true over R. If (1.5) holds for a set A we say that the set A is *(first-order) definable over* R.

If the sentence 1.4 has existential quantifiers only, then it is in what is called *the existential language of rings* and we say that the set A satisfying 1.5 is *existentially definable over* R. The problem of deciding whether a sentence is true in this language over a ring R is essentially Hilbert's Tenth Problem for the ring.

Sometimes we expand the language of rings by adding countably many constant symbols to allow the coefficients of the polynomials to be in R.

Given two rings $R_1 \subset R_2$ such that R_1 has an undecidable first-order theory and has a first-order definition over R_2 as in (1.5), we can conclude that the first-order theory of R_2 is undecidable. For, if R_2 were decidable, combining the algorithm giving first-order decidability in R_2 with the first-order definition of R_1 over R_2 would then give us an algorithm for decidability of R_1, a contradiction.

Applying this reasoning wiith $R_1 = \mathbb{Z}$ shows that if the answer to Question 1.1 above is "yes", then the answer to Question 1.2 is "yes" as well.

1.2. **Uniform definitions.**

Definition 1.6 (Uniform definitions over rings of algebraic integers)**.** Let K be a field of algebraic numbers, $\mathscr{L}$ a collection of extensions of K in the algebraic closure $\bar{K}$, and A a subset of $\mathscr{O}_{\bar{K}}$. We say that A *has a uniform first-order definition over rings of integers of all fields in* $\mathscr{L}$ if there is a single polynomial $P(t, \bar{x}) \in \mathscr{O}_K[t, \bar{x}]$ in $1 + r$ variables (t and $\bar{x} = (x_1, x_2, \dots x_r)$, for some $r \in \mathbb{Z}_{\geq 1}$) and a first-order formula

$$Q(t) := E_1 x_1 \dots E_r x_r P(t, \bar{x}),$$

where E_i is either a universal or an existential quantifier and t is the only free variable, such that $Q(t)$ is a first-order definition of $A \cap \mathscr{O}_L$ over $\mathscr{O}_L$ for every $L \in \mathscr{L}$.

Remark 1.7. Since $\mathbb{Z}$ is existentially undecidable, if $\mathbb{Z}$ has a uniform first-order definition over rings of integers of all fields in $\mathscr{L}$, then we have a single formula giving us a "uniform" way of showing that these rings of integers are first-order undecidable.

1.3. **Brief history.** The first result showing that a first-order theory of a ring is undecidable was due to J.B. Rosser [Ros36] building on results of A. Church [Chu36] and K. Gödel [Göd31]. The ring in question was $\mathbb{Z}$. J. Robinson [Rob49] produced a definition of $\mathbb{Z}$ for the rings of integers of every number field, thus showing that the first-order theory of these rings is undecidable. Her definition was of a simple form $\forall\exists \dots \exists$ but depended explicitly on the degree of the extension. Later in [Rob62] she produced a uniform definition of $\mathbb{Z}$ across all rings of integers of number fields, but the uniform formula was much more complicated. (See Definition 1.6 for our interpretation of the notion of uniformity.) In this paper we construct a definition of $\mathbb{Z}$, without parameters, over the rings of integers of all number fields and some classes of infinite algebraic extensions of $\mathbb{Q}$. This definition has the form $\forall\forall\exists \dots \exists$.

There are of course existential definitions of $\mathbb{Z}$ over rings of integers of some number fields and some infinite algebraic extensions of $\mathbb{Q}$ (see, for example, [Den75], [DL78], [Den80], [Phe88], [SS89], [Shl89], [Vid89], [CPZ05], [Shl07], [Shl08], [Shl09], [GFP20], [MRS22]) and some well-known conjectures imply that $\mathbb{Z}$ has an existential definition over rings of integers of every number field (see [MR10], [MP18], [Pas23]). However, these definitions are not uniform across all number fields, and by Corollary 5.4 they cannot be.

While we now have a pretty good understanding of the first-order theory of rings of integers of number fields, the situation is quite different when it comes

to infinite algebraic extensions of $\mathbb{Q}$. For example there are infinite extensions whose ring of integers has decidable first-order theory ([Rum86] and [vdD88]), and other infinite extensions whose ring of integers has undecidable first-order theory.

J. Robinson was the first person to produce examples of infinite algebraic extensions of $\mathbb{Q}$ where the first-order theory of the ring of integers is undecidable. She developed a method for constructing a first-order definition of $\mathbb{Z}$ for rings of totally real integers and a method for constructing a first-order model of $\mathbb{Z}$ and thus proving undecidability for some rings of integers that are not totally real. See for example [Vid00b], [VV15], [VV16], [GR19], [CVV20], [MRUV20], [Spr20], [CF21], [Spr23] for results using J. Robinson's method applied to rings of totally real integers and rings of integers of extensions of degree 2 of totally real fields.

The first important results showing that rings of integers of some infinite algebraic extensions of $\mathbb{Q}$ are first-order definable over their fields of fractions are due to C. Videla (see [Vid00a], [Vid00b]). These results were generalized by the third author in [Shl18].

1.4. **Totally real algebraic numbers versus totally real algebraic integers.** The rings of integers and their fields of fractions do not always behave in the same fashion with respect to decidability/undecidability of their first-order theories. A remarkable result due to M. Fried, D. Haran and H. Völklein in [FHV94] shows that the first-order theory of the field of all totally real algebraic numbers is decidable. This field constitutes a boundary of sorts between the "decidable" and "undecidable", since J. Robinson showed in [Rob62] that $\mathbb{Z}$ is first-order definable over the ring of all totally real integers and therefore the first-order theory of the ring of all totally real integers is undecidable.

1.5. **Non-big fields of algebraic numbers.** Our formula for defining $\mathbb{Z}$ is not dependent on whether the ring in question is real or not. Rather it depends on whether the field in question is "big" or not (see [MR20]).

Definition 1.8. Let K be a field of algebraic numbers. We say that K is *big* if

$$[K : \mathbb{Q}] = \prod_{p \text{ prime}} p^{\infty}.$$

Equivalently, K is big if for every positive integer n, K contains a number field F with $[F : \mathbb{Q}]$ divisible by n.

Our main theorem, which will be proved in §4, is the following.

Theorem 4.8. *Let $\mathscr{A}$ be the collection of all non-big fields of algebraic numbers. There exists a first-order formula of the form "$\forall\forall\exists\ldots\exists$" uniformly defining $\mathbb{Z}$ over the rings of integers of all fields in $\mathscr{A}$. In particular the first-order theory of these rings can be uniformly shown to be first-order undecidable.*

Definition 1.9. Let $\{F_i\}, i \in \mathbb{Z}_{>0}$ be a sequence of fields such that $F_i \subset F_{i+1}$ and F_{i+1}/F_i is Galois. Then we will call the sequence $\{F_i\}$ a *tower of Galois extensions*.

Corollary 1.10. *The following fields have an undecidable first-order theory.*

(1) *A non-big union of a tower of Galois extensions of a number field.*
(2) *A non-big Galois extension of a number field.*
(3) *A union of a tower of extensions of degree less or equal to $d \in \mathbb{Z}_{>1}$.*
(4) *A compositum of all extensions of degree less or equal to $d \in \mathbb{Z}_{>1}$ of a number field.*
(5) *The closure of a number field under taking of n-th roots or under taking $2n$-th roots of positive elements.*

Proof. If M is a tower of Galois extensions (or a Galois extension) of a number field K and is not big, then for some prime p the field M is uniformly p-bounded in the sense of [Shl18], so $\mathcal{O}_M$ has a first-order definition over M. (See [Shl18] for the proof and note that in that paper the term "q-bounded" is used in place of "p-bounded".) By Theorem 4.8, we have that $\mathbb{Z}$ is first-order definable over $\mathcal{O}_M$. So $\mathbb{Z}$ is first-order definable over M and therefore the first-order theory of M is undecidable.

In the case of the last three assertions of the corollary, the field in question is clearly non-big and uniformly p-bounded for any $p > d$ in the case of the compositum or a tower of extensions of degree less or equal to d and for any $p > 2n$ in the case of the closure under taking n-th roots or $2n$-th roots. The rest of the argument is the same as for the first two assertions of the corollary.

□

The last item in the corollary implies the following corollary answering a question of Tarski.

Corollary 1.11. *The first-order theory of the field of constructible numbers is undecidable.*

Proof. The field of constructible numbers is the smallest subfield of the field of algebraic numbers that is closed under the operation of taking a square root of positive elements of the field.

□

Our methods also provide a potential approach to proving undecidability of the ring of integers of the maximal abelian extension of $\mathbb{Q}$ (see Corollary 2.14).

1.6. **Using units.** One of the main ideas behind our use of units is a simple algebraic identity $\frac{x^n-1}{x-1} \equiv n \bmod (x-1)$ in $\mathbb{Z}[x]$ for $x \neq 1$. If x is a unit of a ring of integers, then so is x^n leading to our Definition 2.1.

The first use of units exploiting this algebraic identity for the purposes of (existential) definability in the form of Pell equation belongs to J. Robinson (see [Rob69]) and M. Davis (see [Dav73]). The Pell equation over $\mathbb{Z}$ is after all just a norm equation of the units of a quadratic extension. Later, J. Denef and L. Lipshitz adapted this idea for algebraic extensions (see [Den75], [Den80],[DL78]). Following their lead T. Pheidas ([Phe88]), C. Videla ([Vid89]) and the third author ([Shl89]) used this particular unit method for another collection of number fields.

The third author used units, S-units and more generic norm equations of units to define $\mathbb{Z}$ over big subrings of number fields and infinite algebraic extensions of $\mathbb{Q}$ (see for example [Shl94], [Shl02], [Shl04]).

C. Martinez-Ranero, J. Utreras and C. Videla in [MRUV20] and C. Springer in [Spr20] and [Spr23] also make use of units of the field under consideration but their methods are entirely different from ours.

2. First-order passage from submonoids to subrings

For any algebraic extension K of $\mathbb{Q}$ let $\mathscr{O}_K$ denote the ring of integers of K and $U_K := \mathscr{O}_K^\times$ the group of units of $\mathscr{O}_K$.

Definition 2.1. Let K be a field of algebraic numbers, and $M \subset \mathscr{O}_K$ a multiplicative monoid. Define

$$\begin{aligned} R_{K,M} :=& \{x \in \mathscr{O}_K : \forall \varepsilon \in M\ \exists \delta \in M\ \exists w \in \mathscr{O}_K \text{ such that } \delta - 1 = (\varepsilon-1)x + (\varepsilon-1)^2 w\} \\ =& \{x \in \mathscr{O}_K : \forall \varepsilon \in M\ \exists \delta \in M \text{ such that } \delta - 1 \equiv (\varepsilon-1)x \pmod{(\varepsilon-1)^2}\}. \end{aligned}$$

When $M = U_K$ we will denote R_{K,U_K} simply by R_K.

Lemma 2.2. *Suppose $\varepsilon, x_1, x_2, \dots, x_n, \delta_1, \dots, \delta_n \in \mathscr{O}_K$ for some $n \geq 1$, and for every i*

$$\delta_i - 1 \equiv (\varepsilon-1)x_i \pmod{(\varepsilon-1)^2}.$$

Then

$$\prod_i \delta_i - 1 \equiv (\varepsilon-1)\sum_i x_i \pmod{(\varepsilon-1)^2}.$$

Proof. By induction it is enough to prove the lemma for $n = 2$. Since $\delta_i - 1 \equiv 0 \pmod{(\varepsilon-1)}$, when $n = 2$ the lemma follows from the congruence

$$\begin{aligned} \delta_1\delta_2 - 1 &= (\delta_1 - 1) + (\delta_2 - 1) + (\delta_1 - 1)(\delta_2 - 1) \\ &\equiv (\delta_1 - 1) + (\delta_2 - 1) \equiv (\varepsilon-1)x_1 + (\varepsilon-1)x_2 \pmod{(\varepsilon-1)^2}. \end{aligned}$$

□

Proposition 2.3. *Let M be a monoid in $\mathscr{O}_K$, and let $\mathbb{Q}(M)$ be the field generated over $\mathbb{Q}$ by M. Then:*

(1) $R_{K,M}$ is closed under addition and multiplication (i.e., is a 'semi-ring').
(2) If M is a subgroup of U_K then $R_{K,M}$ is a subring of $\mathscr{O}_K$.
(3) If M contains a unit of infinite order, then $R_{K,M} \subset \mathscr{O}_{\mathbb{Q}(M)}$.

Proof. That $R_{K,M}$ is closed under addition follows directly from Lemma 2.2.

Suppose $x, y \in R_{K,M}$ and $\varepsilon \in M$. Since $x \in R_{K,M}$, there is a $\delta \in M$ such that

$$\delta - 1 \equiv (\varepsilon-1)x \pmod{(\varepsilon-1)^2}.$$

Since $y \in R_{K,M}$, there is a $\delta' \in M$ such that

$$\delta' - 1 \equiv (\delta-1)y \equiv ((\varepsilon-1)x)y \pmod{(\varepsilon-1)^2}.$$

It follows that $xy \in R_{K,M}$, which completes the proof of (1).

Now suppose M is a subgroup of U_K. That $R_{K,M}$ is a ring will follow from (1) once we show that $-1 \in R_{K,M}$. Suppose $\varepsilon \in M \subset U_K$. Since M is a group, $\varepsilon^{-1} \in M$, and

$$\varepsilon^{-1} - 1 = -(\varepsilon - 1) + \varepsilon^{-1}(\varepsilon - 1)^2 \equiv -(\varepsilon - 1) \pmod{(\varepsilon - 1)^2}.$$

It follows that $-1 \in R_{K,M}$, which completes the proof of (2).

Finally, suppose that M contains a unit ε of infinite order. If $\mathfrak{a}$ is a nonzero ideal of $\mathscr{O}_{\mathbb{Q}(\varepsilon)}$, then the reduction of ε has finite order in $(\mathscr{O}_{\mathbb{Q}(\varepsilon)}/\mathfrak{a})^\times$, i.e., $\varepsilon^n - 1 \in \mathfrak{a}$ for some $n \geq 1$. Therefore

$$\bigcap_{n \geq 1} (\varepsilon^n - 1)\mathscr{O}_K \subset \bigcap_{\text{nonzero ideals } \mathfrak{a} \text{ of } \mathscr{O}_{\mathbb{Q}(\varepsilon)}} \mathfrak{a}\mathscr{O}_K = 0. \tag{2.4}$$

Suppose $x \in R_{K,M}$, and $n \in \mathbb{Z}_{>0}$. Since $\varepsilon^n \in M$, there is a $\delta \in M$ such that

$$\delta - 1 \equiv x(\varepsilon^n - 1) \pmod{(\varepsilon^n - 1)^2}.$$

If y is any conjugate of x over $\mathbb{Q}(M)$, then the same congruence holds with x replaced by y, and since $\varepsilon^n \neq 1$ we get

$$x - y \in (\varepsilon^n - 1)\mathscr{O}_K.$$

Thus $x - y \in \cap_{n>0}(\varepsilon^n - 1)\mathscr{O}_K$, which is zero by (2.4). Hence $y = x$, and it follows that $x \in \mathscr{O}_{\mathbb{Q}(M)}$. □

Remark 2.5. Suppose M is a subgroup of U_K. A priori, the ring $R_{K,M}$ is not necessarily the full ring of integers $\tilde{R}_{K,M}$ in its field of fractions. But $\tilde{R}_{K,M}$ admits an existential definition in terms of $R_{K,M}$:

Proposition 2.6. *If M is a subgroup of U_K, then*

$$\tilde{R}_{K,M} = \{x \in \mathscr{O}_K \mid \exists y, z \in R_{K,M}, y \neq 0, xy = z\}.$$

Proof. Note that the set $\{y \in \mathscr{O}_K : y \neq 0\}$ has an existential definition by a result of Denef ([Den80, Lemma 9]; see also [MRS22, Lemma 4.6]).

Let R denote the right hand side of the equation in the statement of the proposition. Then $R \subset \tilde{R}_{K,M}$.

For every number field F contained in the field of fractions of $R_{K,M}$, there is an element $\alpha \in R_{K,M}$ such that $\mathbb{Q}(\alpha) = F$. For every $\beta \in \mathscr{O}_F$ there exists $m \in \mathbb{Z}$ such that $m\beta \in \mathbb{Z}[\alpha] \subset R_{K,M}$, and taking $x = \beta$, $y = m$, and $z = m\beta$ in the definition of R we see that $\beta \in R$. Thus R contains every algebraic integer of F. Since this is true for every number field F in the field of fractions of $\tilde{R}_{K,M}$, it follows that R is integrally closed in its field of fractions, i.e., $R = \tilde{R}_{K,M}$. □

Corollary 2.7. *If M is a subgroup of U_K, and M admits a first-order definition in $\mathscr{O}_K$, then the rings $R_{K,M}$ and $\tilde{R}_{K,M}$ admit first-order definitions in $\mathscr{O}_K$ as well.*

Lemma 2.8. *Let L/K be a finite extension. Suppose $\varepsilon \in U_K$, $x \in \mathscr{O}_K$, and $\delta \in U_L$ satisfy*

$$(\varepsilon - 1)x \equiv \delta - 1 \pmod{(\varepsilon - 1)^2\mathscr{O}_L}.$$

Then

$$(\varepsilon - 1)[L : K]x \equiv N_{L/K}(\delta) - 1 \pmod{(\varepsilon - 1)^2\mathscr{O}_K}.$$

Proof. Let Σ be the set of embeddings of L/K into the Galois closure $\tilde{L}$ of L/K. Since x and ε lie in K, for every $\sigma \in \Sigma$ we have that

$$(\varepsilon - 1)x \equiv \sigma(\delta) - 1 \pmod{(\varepsilon-1)^2 \mathscr{O}_{\tilde{L}}}.$$

We have $\prod_{\sigma\in\Sigma} \sigma(\delta) = N_{L/K}(\delta)$ and $|\Sigma| = [L : K]$. Therefore Lemma 2.2 applied with $n = [L : K]$, the given ε, all x_i equal to the given x, and the δ_i equal to $\sigma(\delta)$ for $\sigma \in \Sigma$ shows that

$$N_{L/K}(\delta) - 1 \equiv (\varepsilon - 1)[L : K]x \pmod{(\varepsilon-1)^2 \mathscr{O}_{\tilde{L}}}.$$

Both sides of this congruence belong to $\mathscr{O}_K$, so the congruence holds modulo $(\varepsilon - 1)^2 \mathscr{O}_K$. □

Recall that we denote R_{K,U_K} simply by R_K.

Lemma 2.9. *Let W be a subgroup of U_K, let $n \in \mathbb{Z}_{>0}$ and let $\mathfrak{a}$ be an ideal of $\mathscr{O}_K$. Let*

$$M := \{u^n : u \in W, u \equiv 1 \pmod{\mathfrak{a}}\}.$$

Then $nR_{K,W} \subset R_{K,M}$.

Proof. Let $x \in R_{K,W}$. We will show $nx \in R_{K,M}$. Let $\varepsilon \in W$. Since $x \in R_{K,W}$ there exists $\delta \in W$ such that

$$(\varepsilon - 1)x \equiv \delta - 1 \pmod{(\varepsilon-1)^2}$$

and it follows that $\delta \equiv 1 \pmod{\mathfrak{a}}$ and $\delta^n \in M$. Therefore by Lemma 2.2 applied with this n and ε, all $x_i := x$, and all $\delta_i := \delta$,

$$(\varepsilon - 1)nx \equiv \delta^n - 1 \pmod{(\varepsilon-1)^2}.$$

Thus $nx \in R_{K,M}$. □

Definition 2.10. We call a field K of algebraic numbers a *CM-field* if K is a totally imaginary quadratic extension of a totally real field. We include the case $[K : \mathbb{Q}] = \infty$.

Proposition 2.11. *Let K be a CM-field that is not an imaginary quadratic field, and let F be the maximal real subfield of K. Then $R_K \subset \mathscr{O}_F$.*

Proof. Fix $d \in \mathbb{Z}_{>2}$ and let $M := \{u^2 : u \in U_K, u \equiv 1 \pmod{d\mathscr{O}_K}\}$. We first claim that $M \subset U_F$. Let $\alpha \mapsto \bar{\alpha}$ denote complex conjugation on K. If $\varepsilon \in M$, we can write $\varepsilon = u^2$ with $u \in U_K$, $u \equiv 1 \pmod{d}$. Thus

$$\varepsilon = u^2 = (u\bar{u})(u/\bar{u}).$$

Since $u/\bar{u} \in U_K$ and all of its archimedean absolute values are 1, $u/\bar{u}$ is a root of unity. Since $u \equiv 1 \pmod{d}$ we must have $u/\bar{u} = 1$. Thus $\varepsilon = u\bar{u} \in U_F$.

Since K is not an imaginary quadratic field, M contains units of infinite order. Thus, by Lemma 2.9 for the first containment and Proposition 2.3(3) for the second, we have

$$2R_K \subset R_{K,M} \subset \mathscr{O}_{\mathbb{Q}(M)} \subset \mathscr{O}_F.$$

It follows that $R_K \subset \mathscr{O}_F$. □

Remark 2.12. We can apply Proposition 2.11 to $\mathbb{Q}^{\mathrm{ab}}$, the maximal abelian extension of $\mathbb{Q}$, to conclude that there is a totally real ring (namely, $R_{\mathbb{Q}^{\mathrm{ab}}}$) that is first-order definable over $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$. Unfortunately, at the moment we cannot identify the ring $R_{\mathbb{Q}^{\mathrm{ab}}}$.

Remark 2.13. Let $\mathbb{Q}^{\mathrm{ab},+}$ be the the maximal totally real subfield of $\mathbb{Q}^{\mathrm{ab}}$. It is easy to see that the proof of J. Robinson from [Rob62] showing undecidability of the ring of integers of the field of totally real numbers applies to the ring of integers of $\mathbb{Q}^{\mathrm{ab},+}$. So, the first-order theory of $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab},+}}$ is undecidable. Moreover, she conjectured that the ring of integers of any totally real field is undecidable. J. Koenigsmann [Koe14] conjectured that $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab},+}}$ has a first-order definition over $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$ implying via the above mentioned result that $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$ also has an undecidable first-order theory. As a corollary of Proposition 2.11 we can add the following conditions that would imply undecidability of the first-order theory of $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$.

Corollary 2.14. *The ring $\mathscr{O}_{\mathbb{Q}^{ab}}$ is first-order undecidable if at least one of the following conditions is satisfied:*

(1) the ring $R_{\mathbb{Q}^{ab}}$ is undecidable, or
(2) the ring of integers of every real abelian extension of $\mathbb{Q}$ is undecidable, or
(3) there exists a non-big subfield of $\mathbb{Q}^{\mathrm{ab}}$ whose ring of integers is first-order definable over $\mathscr{O}_{\mathbb{Q}^{\mathrm{ab}}}$.

3. Computing R_K in special cases

Proposition 3.1. *Let K be an imaginary quadratic field. Then $R_K = \mathbb{Z} + 2\mathscr{O}_K$.*

Proof. For $\varepsilon, \delta \in U_K$ let

$$S_{\varepsilon,\delta} := \{x \in \mathscr{O}_K : \delta - 1 \equiv (\varepsilon - 1)x \pmod{(\varepsilon - 1)^2}\}.$$

Then by definition,

$$R_K := \bigcap_{\varepsilon \in U_K} \Big(\bigcup_{\delta \in U_K} S_{\varepsilon,\delta} \Big). \tag{3.2}$$

One checks easily that $S_{1,1} = \mathscr{O}_K$, $S_{-1,1} = 2\mathscr{O}_K$, and $S_{-1,-1} = 1 + 2\mathscr{O}_K$. When $U_K = \{-1, 1\}$, the proposition now follows from (3.2).

Now suppose $K = \mathbb{Q}(i)$. In this case

$$\begin{gathered} S_{i,1} = S_{i,-1} = (1+i)\mathscr{O}_K, \quad S_{i,i} = S_{i,-i} = 1 + (1+i)\mathscr{O}_K, \\ S_{-i,1} = S_{-i,-1} = (1+i)\mathscr{O}_K, \quad S_{-i,i} = S_{-i,-i} = 1 + (1+i)\mathscr{O}_K, \\ S_{-1,i} = S_{-1,-i} = \emptyset. \end{gathered}$$

Again it follows from (3.2) that $R_{\mathbb{Q}(i)} = \mathbb{Z} + 2\mathbb{Z}[i]$. The proof when $K = \mathbb{Q}(\sqrt{-3})$ is similar. □

The following theorem will be used to study the case of unit groups of rank 1. Its proof can be found in [EG15].

Theorem 3.3 (Corollary 6.1.2 of [EG15]). *Suppose K is a number field. Then the equation $x_1 + x_2 + x_3 = 1$ has only finitely many solutions with all $x_i \in U_K - \{1\}$.*

Lemma 3.4. *Suppose K is a number field, $\varepsilon \in U_K$ is a unit of infinite order, and $a, b \in \mathbb{Z}$. Let $g := \gcd(a, b)$.*

(1) If $b \mid a$ then $(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$ and $(\varepsilon^a - 1)/(\varepsilon^b - 1) \equiv a/b \pmod{(\varepsilon^b - 1)}$.
(2) The ideal of $\mathscr{O}_K$ generated by $\varepsilon^a - 1$ and $\varepsilon^b - 1$ is $(\varepsilon^g - 1)\mathscr{O}_K$.
(3) If $(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$ then $(\varepsilon^b - 1)/(\varepsilon^g - 1) \in U_K$.

Proof. Assertion (1) follows from the polynomial identity $X^n - 1 = (X - 1)\sum_{i=0}^{n-1} X^i$ applied with $X := \varepsilon^b$, $n := a/b$.

Let $\mathfrak{d}$ be the ideal of $\mathscr{O}_K$ generated by $\varepsilon^a - 1$ and $\varepsilon^b - 1$. By (1) we have that $\mathfrak{d} \subset (\varepsilon^g - 1)\mathscr{O}_K$. Fix $x, y \in \mathbb{Z}$ such that $ax - by = g$. Using (1) again we see that $\mathfrak{d}$ contains

$$(\varepsilon^{ax} - 1) - (\varepsilon^{by} - 1) = \varepsilon^{ax} - \varepsilon^{by} = \varepsilon^{by}(\varepsilon^{ax-by} - 1) = \varepsilon^{by}(\varepsilon^g - 1).$$

Since ε is a unit, we have $\varepsilon^g - 1 \in \mathfrak{d}$, which completes the proof of (2).

By (1) and (2) we have that $(\varepsilon^b - 1)/(\varepsilon^g - 1)$ and $(\varepsilon^a - 1)/(\varepsilon^g - 1)$ are relatively prime integers of K. If in addition $(\varepsilon^b - 1)/(\varepsilon^g - 1)$ divides $(\varepsilon^a - 1)/(\varepsilon^g - 1)$, then $(\varepsilon^b - 1)/(\varepsilon^g - 1)$ must be a unit. This proves (3). □

Proposition 3.5. *Suppose K is a number field, and $u \in U_K$ is a unit of infinite order. There is an $N \in \mathbb{Z}_{>0}$ such that for every $a, b \in \mathbb{Z}_{>0}$, and every $n > N$, the unit $\varepsilon := u^n$ satisfies*

$$(\varepsilon^b - 1) \mid (\varepsilon^a - 1) \iff b \mid a.$$

Proof. The "$\Longleftarrow$" implication holds for every n by Lemma 3.4(1).

Consider the set

$$S := \{d \in \mathbb{Z}_{\neq 0} : \exists x_2, x_3 \in U_K - \{1\} \text{ such that } u^d + x_2 + x_3 = 1\}.$$

By Theorem 3.3, S is finite, and we set $N := \sup(S)$. Fix $n > N$ and let $\varepsilon = u^n$.

Suppose $(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$. By Lemma 3.4(3), it follows that $\delta := (\varepsilon^b - 1)/(\varepsilon^g - 1) \in U_K$, where $g := \gcd(a, b)$. Thus we have a solution of the unit equation

$$\varepsilon^b - \delta\varepsilon^g + \delta = 1.$$

We have $\varepsilon^b = u^{nb}$ with $nb \geq n > N$, so by definition of S we must have either $-\delta\varepsilon^g = 1$ or $\delta = 1$. Suppose $-\delta\varepsilon^g = 1$. Since u has infinite order, $\varepsilon^{b+g} \neq 1$. At the same time from the definition of δ we get that

$$\varepsilon^g - 1 = -\delta\varepsilon^g(\varepsilon^g - 1) = \varepsilon^g(1 - \varepsilon^b) = \varepsilon^g - \varepsilon^{b+g}$$

and $\varepsilon^{b+g} = 1$. This contradiction implies that $-\delta\varepsilon^g \neq 1$. Therefore $\delta = 1$, i.e., $\varepsilon^b - 1 = \varepsilon^g - 1$. Again using that u has infinite order we conclude that $g = b$, so $b \mid a$. □

Proposition 3.6. *Let K be a number field and let W be a subgroup of U_K such that $\operatorname{rank} W = 1$. Then $R_{K,W} = \mathbb{Z}$.*

Proof. Let $M := \{u^n : u \in W\}$, where n is chosen large enough so that M is torsion-free, and n is larger than the N of Proposition 3.5. Applying Lemma 2.9 with this M (and $\mathfrak{a} = \mathscr{O}_K$) shows that $nR_{K,W} \subset R_{K,M}$, so to prove the proposition it is enough to show that $R_{K,M} = \mathbb{Z}$.

Fix a generator ε of M, and suppose $x \in R_{K,M}$. Choose $m \in \mathbb{Z}_{>0}$, and choose $b \in \mathbb{Z}_{>0}$ such that $\varepsilon^b \equiv 1 \pmod{m}$. By definition of $R_{K,M}$, for some $a \in \mathbb{Z}$ we have

$$\varepsilon^a - 1 \equiv (\varepsilon^b - 1)x \pmod{(\varepsilon^b - 1)^2}.$$

In particular $(\varepsilon^b - 1) \mid (\varepsilon^a - 1)$, so by Proposition 3.5 we conclude that $b \mid a$. Then

$$x \equiv (\varepsilon^a - 1)/(\varepsilon^b - 1) \equiv a/b \pmod{(\varepsilon^b - 1)}$$

by Lemma 3.4(1), so $x - a/b \in m\mathscr{O}_K$. In particular, x is divisible by m in the free $\mathbb{Z}$-module $\mathscr{O}_K/\mathbb{Z}$. Since m is arbitrary, we conclude that $x = 0$ in $\mathscr{O}_K/\mathbb{Z}$, i.e., $x \in \mathbb{Z}$. □

Lemma 3.7. *Let p be a rational prime, and K a number field. Suppose $j \in \mathbb{Z}_{>0}$, and $\varepsilon \in U_K - \{1\}$ satisfies $\varepsilon \equiv 1 \pmod{p^{j+1}}$. Then there exists $x \in \mathscr{O}_K$ such that for every integer n prime to p, the congruence*

$$\delta - 1 \equiv (\varepsilon - 1)p^j nx \pmod{p^{j+1}(\varepsilon - 1)\mathscr{O}_K}$$

has no *solutions $\delta \in U_K$.*

Proof. Let $\mathfrak{a} = \prod_{\mathfrak{p}|p} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(\varepsilon-1)}$, where $\mathfrak{p}$ runs through the primes of K above p. Note that p^{j+1} divides $\mathfrak{a}$ by our choice of ε. Define groups

$$W_{\mathfrak{a}} := \{u \in U_K : u \equiv 1 \pmod{p^j\mathfrak{a}}\}, \quad V_{\mathfrak{a}} := p^j\mathfrak{a}/p^{j+1}\mathfrak{a}.$$

Then $W_{\mathfrak{a}} \subset U_K$ is a free abelian group of rank strictly less than $[K : \mathbb{Q}]$ (there are no nontrivial roots of unity congruent to 1 modulo $p\mathfrak{a}$), and $V_{\mathfrak{a}}$ is an $\mathbb{F}_p$-vector space of dimension $[K : \mathbb{Q}]$. There is a natural homomorphism

$$\lambda_{\mathfrak{a}} : W_{\mathfrak{a}} \longrightarrow V_{\mathfrak{a}}$$

defined by

$$\lambda_{\mathfrak{a}}(u) = u - 1 \pmod{p^{j+1}\mathfrak{a}},$$

and it follows that the cokernel of $\lambda_{\mathfrak{a}}$ has dimension at least one.

The map

$$\mathscr{O}_K/p\mathscr{O}_K \longrightarrow p^j\mathfrak{a}/p^{j+1}\mathfrak{a} = V_{\mathfrak{a}} \quad \text{defined by} \quad x \mapsto (\varepsilon - 1)p^j x$$

is an isomorphism, so we can choose $x \in \mathscr{O}_K$ such that for every integer n prime to p the product $(\varepsilon - 1)p^j nx$ is not in the image of $\lambda_{\mathfrak{a}}$. But not being in the image of $\lambda_{\mathfrak{a}}$ means precisely that there is no $\delta \in U_K$ such that

$$\delta - 1 \equiv (\varepsilon - 1)p^j nx \pmod{p^{j+1}(\varepsilon - 1)\mathscr{O}_K}.$$

□

Definition 3.8. Let p be a prime. Let $K/\mathbb{Q}$ be a possibly infinite degree algebraic extension. Then we will say that K is *p-finite* if $\mathrm{ord}_p[K:\mathbb{Q}] < \infty$, or equivalently if for some number field $L \subset K$ no finite extension of L in K has degree divisible by p.

Remark 3.9. An algebraic extension of $\mathbb{Q}$ is not big (cf. Definition 1.8) if and only if there exists a prime p for which it is p-finite.

Lemma 3.10. *Suppose K is a number field such that U_K is infinite. Let L be an algebraic extension of K that is not big. Then for every $m \in \mathbb{Z}_{>0}$ we have that $m\mathscr{O}_K \not\subset R_L$.*

Proof. Since L is not big, we can choose a rational prime p such that L is p-finite. Fix $m \geq 1$, and define

$$j := 1 + \mathrm{ord}_p(m) + \sup\{\mathrm{ord}_p[K':K] : K' \text{ is a finite extension of } K \text{ in } L\}$$

which is finite by assumption. Since U_K is infinite, we can fix $\varepsilon \in U_K - \{1\}$ such that $\varepsilon \equiv 1 \pmod{p^{j+1}}$. Let $x \in \mathscr{O}_K$ be as in Lemma 3.7 with this choice of p, K, ε, and this j.

Suppose $mx \in R_L$. Then there exists $\delta \in U_L$ such that

$$\delta - 1 \equiv (\varepsilon - 1)mx \pmod{(\varepsilon-1)^2\mathscr{O}_L}.$$

By Lemma 2.8,

$$N_{K(\delta)/K}\delta - 1 \equiv (\varepsilon - 1)[K(\delta):K]mx \pmod{(\varepsilon-1)^2\mathscr{O}_K}.$$

Write $[K(\delta):K]m = np^s$, with n prime to p. Then $s < j$, and by Lemma 2.2

$$(N_{K(\delta)/K}\delta)^{p^{j-s}} - 1 \equiv (\varepsilon-1)[K(\delta):K]p^{j-s}mx \equiv (\varepsilon-1)p^j nx \pmod{(\varepsilon-1)^2\mathscr{O}_K}.$$

This contradicts our choice of x (Lemma 3.7), so we must have $mx \notin R_L$. □

Theorem 3.11. *Let K be an algebraic extension of $\mathbb{Q}$ that is not big. Then either $R_K = \mathbb{Z}$ or R_K is an order in some imaginary quadratic field F contained in K.*

Proof. Let $x \in R_K$, and assume that that $\mathbb{Q}(x)$ is neither $\mathbb{Q}$ nor an imaginary quadratic field. In particular $U_{\mathbb{Q}(x)}$ is infinite. Since R_K is a ring we have $\mathbb{Z}[x] \subset R_K$, so there exists $m \in \mathbb{Z}_{>0}$ such that $m\mathscr{O}_{\mathbb{Q}(x)} \subset R_K$. Thus contradicts Lemma 3.10.

Hence for any $x \in R_K$ we have that $\mathbb{Q}(x) = \mathbb{Q}$ or $\mathbb{Q}(x)$ is an imaginary quadratic field. If $x_1, x_2 \in R_K$ generate two different imaginary quadratic fields $\mathbb{Q}(x_1), \mathbb{Q}(x_2)$, then R_K contains an element x such that $\mathbb{Q}(x) = \mathbb{Q}(x_1, x_2)$ leading to a contradiction again. Thus either $R_K = \mathbb{Z}$ or K is an imaginary quadratic field. □

Corollary 3.12. *Suppose K is not big. If K does not contain an imaginary quadratic field, or K is a CM-field, then $R_K = \mathbb{Z}$.*

Proof. The case of a field K without an imaginary quadratic subfield follows directly from Theorem 3.11. The CM-field case follows from Theorem 3.11 and Proposition 2.11. □

Corollary 3.13. *Let K be a degree 4 extension of $\mathbb{Q}$. Then $R_K = \mathbb{Z}$.*

Proof. If K does not contain an imaginary quadratic field, then the corollary follows from Corollary 3.12. If K does contain an imaginary quadratic field, then K has no real embeddings, so $\operatorname{rank} U_K = 1$ and the corollary follows from Proposition 3.6. □

Given a non-big field K that contains more than one imaginary quadratic field, at most one of these fields can be the fraction field of R_K. This lack of symmetry, together with Corollaries 3.12 and 3.13, leads us to the following conjecture.

Conjecture 3.14. *Let K be a non-big field that is not imaginary quadratic. Then $R_K = \mathbb{Z}$.*

We conclude this section by describing a class of (necessarily big) fields K such that $R_K = \mathscr{O}_K$.

Lemma 3.15. *Suppose K is a number field, $I \subset \mathscr{O}_K$ is a nonzero ideal, and $\beta \in \mathscr{O}_K$ is relatively prime to I. Then there is a finite extension L/K and a unit $\delta \in U_L$ such that $\delta \equiv \beta \pmod{I\mathscr{O}_L}$. Further, the field L can be taken to be generated by a root of a polynomial of the form $X^d + aX^{d-1} + b$, where $d \in \mathbb{Z}_{>0}$ and $a, b \in \mathscr{O}_K$.*

Proof. Without loss of generality (replacing I by a multiple if necessary) we can assume that I is principal. Fix a generator μ of I.

Let d be the order of $-\beta$ in $(\mathscr{O}_K/I)^\times/\{\text{image of } U_K\}$. Then we can fix a unit $u \in U_K$ such that $(-\beta)^d \equiv u \pmod{I}$.

Consider the polynomial

$$f(X) := X^d + aX^{d-1} + b \in \mathscr{O}_K[X]$$

where $a, b \in \mathscr{O}_K$ will be chosen later. Let ρ be a root of f, let $L = K(\rho)$, and define another monic polynomial

$$g(X) := \mu^d f((X - \beta)/\mu) \in \mathscr{O}_K[X].$$

Then $\delta := \mu\rho + \beta \in \mathscr{O}_L$ is a root of g, and $\delta \equiv \beta \pmod{I\mathscr{O}_L}$.

We claim that there are elements $a, b \in \mathscr{O}_K$ such that $g(0) = u$ is a unit. In that case we will have that δ is a unit, so δ will have all the desired properties, concluding the proof of Lemma 3.15.

To prove the claim we have

$$g(0) = \mu^d f(-\beta/\mu) = (-\beta)^d + a\mu(-\beta)^{d-1} + \mu^d b \\ = u + ((-\beta)^d - u) + a\mu(-\beta)^{d-1} + b\mu^d. \tag{3.16}$$

Since β is relatively prime to μ, we have

$$\{a\mu(-\beta)^{d-1} + b\mu^d : a, b \in \mathscr{O}_K\} = \mu\mathscr{O}_K.$$

In particular since $(-\beta)^d \equiv u \pmod{\mu}$, we can find $a, b \in \mathscr{O}_K$ such that

$$a\mu(-\beta)^{d-1} + b\mu^d = u - (-\beta)^d.$$

By (3.16) we have $g(0) = u$. This completes the proof of the claim, and the lemma. □

Proposition 3.17. *Let F be a field of algebraic numbers such that for every $d \in \mathbb{Z}_{>0}$ and every $a, b \in \mathscr{O}_F$, the polynomial $X^d + aX^{d-1} + b$ has a root in F. Then $R_F = \mathscr{O}_F$.*

Proof. Suppose $x \in \mathscr{O}_F$ and $\varepsilon \in U_F, \varepsilon \neq 1$. Applying Lemma 3.15 with

$$K := \mathbb{Q}(x, \varepsilon), \quad \beta := 1 + x(\varepsilon - 1), \quad I := (\varepsilon - 1)^2$$

we get a unit $\delta \in U_F$ satisfying

$$\delta - 1 \equiv x(\varepsilon - 1) \pmod{(\varepsilon - 1)^2}$$

(note that $\delta \in U_F$ thanks to our assumption on F). It follows that $x \in R_F$. □

Remark 3.18. The field $\overline{\mathbb{Q}}$ satisfies the hypothesis of Proposition 3.17; we don't know of any other field that does.

Among big fields of algebraic numbers K, which of them have the property that the field of fractions of R_K is K?

For a big field K denote by $K_{\{1\}}$ the field of fractions of R_K. We have $K_{\{1\}} \subset K$ by Proposition 2.3(2), and we can iterate this operation, denoting by $K_{\{i+1\}}$ the field of fractions of the ring $R_{K_{\{i\}}}$. This tower

$$\mathbb{Q} \subset \cdots K_{\{i\}} \subset K_{\{i-1\}} \cdots \subset K_{\{1\}} \subset K$$

gives us a first order definition (involving $i+1$ universal quantifiers) of the ring of integers of $K_{\{i\}}$ in $\mathscr{O}_K$.

Are there examples of big fields K where this descending sequence of fields doesn't stabilize? That is, such that $K_{\{i+1\}}$ is a proper subfield of $K_{\{i\}}$ for all i?

4. Proof of the main theorem

Before proving our main result, Theorem 4.8, we need a lemma to handle the case where our formula possibly defines an order in an imaginary quadratic field. In what follows we suppress—i.e., we understand implicitly—equations and/or variables needed to say that an element of a ring is a unit or that a congruence holds over a ring.

Let

$$D(w) := 3^{12} w^4 (w-1)^4 (w-2)^4 \in \mathbb{Z}[w]$$

be the quantity denoted $D(2, w)$ in [MRS22, §11].

Lemma 4.1 (Cf. §3 of [Den75])**.** *Fix a non-square positive integer $d \equiv 3 \bmod 4$. For F an imaginary quadratic field let $\mathscr{S}_F = \mathscr{S}_{F,d}(w, s_1, s_2, t_1, t_2, u_1, u_2, v_1, v_2)$ denote the system of equations and congruences (4.2) through (4.5):*

$$\delta_i := s_i + t_i\sqrt{d} \in U_{F(\sqrt{d})}, \quad s_i, t_i \in \mathscr{O}_F, \quad i = 1, 2, \tag{4.2}$$

$$\varepsilon_i := \delta_i^2 = u_i + v_i\sqrt{d}, \quad u_i, v_i \in \mathscr{O}_F, \quad i = 1, 2, \tag{4.3}$$

$$\varepsilon_1 \equiv 1 \pmod{dD(w)\mathscr{O}_F}, \tag{4.4}$$

$$\varepsilon_2 - 1 \equiv w(\varepsilon_1 - 1) \pmod{(\varepsilon_1 - 1)^2}. \tag{4.5}$$

Then $\mathscr{S}_{F,d}$ constitutes a uniform existential definition of $\mathbb{Z}$ over the ring of integers $\mathscr{O}_F$ of any imaginary quadratic field F.

Proof. Suppose $(w, s_1, s_2, t_1, t_2, u_1, u_2, v_1, v_2) \in \mathscr{O}_F^9$ is a zero of $\mathscr{S}$. Then ε_1 and ε_2 are squares of units by (4.2), (4.3), and congruent to $1 \pmod{d}$ by (4.4), (4.5), so by the same argument as in the proof of Proposition 2.11 we conclude that $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}[\sqrt{d}] = \mathscr{O}_{\mathbb{Q}(\sqrt{d})}$. Now by Corollary 11.12 of [MRS22] applied to the extension $F(\sqrt{d})/\mathbb{Q}(\sqrt{d})$ and the ideal $I = (\varepsilon - 1)$ we have that $w \in \mathscr{O}_F \cap \mathbb{Z}[\sqrt{d}] = \mathbb{Z}$.

Conversely, suppose $w \in \mathbb{Z}$. Let $s_1, t_1 \in \mathbb{Z}$ be such that $\delta_1 \in U_{\mathbb{Q}(\sqrt{d})} \subset U_{F(\sqrt{d})}$ and

$$s_1 \equiv 1, \quad t_1 \equiv 0 \pmod{dD(w)}.$$

Let $u_1, v_1 \in \mathbb{Z}$ be such that $\varepsilon_1 = \delta_1^2$. Then (4.2)- (4.4) hold for $i = 1$.

Let $s_2, t_2 \in \mathbb{Z}$ be such that $\delta_2 = \delta_1^w$. Let $u_2, v_2 \in \mathbb{Z}$ be such that $\varepsilon_2 = \delta_2^2$. Then (4.2)-(4.4) hold for $i = 2$. □

Remark 4.6. If we replace $\mathscr{O}_F$ by $\mathbb{Z}$ then for any integer w we can still satisfy all equations $\mathscr{S}_F$ in the proof of Lemma 4.1.

Remark 4.7. Denef's proof in [Den75], while not formally asserting *uniformity* across imaginary quadratic fields, can be easily converted into a uniform proof.

Theorem 4.8. *Let $\mathscr{A}$ be the collection of all non-big fields of algebraic numbers. There exists a first-order formula of the form "$\forall\forall\exists\ldots\exists$" uniformly defining $\mathbb{Z}$ over the rings of integers of all fields in $\mathscr{A}$. Thus, the first-order theory of these rings is undecidable.*

Before beginning the proof, let K be any field of algebraic numbers and consider the following first-order formula of the form "$\forall\forall\exists\ldots\exists$" and the set $Z_K \subset \mathscr{O}_K$ it defines:

Definition 4.9. Define $Z_K \subset \mathscr{O}_K$ to be the set of all $w \in \mathscr{O}_K$ satisfying

$$\forall \varepsilon \in U_K \setminus \{1\}, \exists \mu, \mu_1, \mu_2, \nu_1, \nu_2, \gamma_1, \gamma_2, \tau_1, \tau_2 \in U_K, s_1, s_2, t_1, t_2, u_1, u_2, v_1, v_2 \in \mathscr{O}_K$$

such that

$$w(\varepsilon-1)\equiv\mu-1 \pmod{(\varepsilon-1)^2}, \tag{4.10}$$

$$u_i(\varepsilon-1)\equiv\mu_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.11}$$

$$v_i(\varepsilon-1)\equiv\nu_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.12}$$

$$s_i(\varepsilon-1)\equiv\sigma_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.13}$$

$$t_i(\varepsilon-1)\equiv\tau_i-1 \pmod{(\varepsilon-1)^2}, \quad i=1,2, \tag{4.14}$$

$$\mathscr{S}_F(w,s_1,s_2,t_1,t_2,u_1,u_2,v_1,v_2), \tag{4.15}$$

with $\mathscr{S}$ as in the proof of Lemma 4.1.

Remark 4.16. Unfortunately, we cannot quantify over the group of units. Therefore, instead of using "$\forall\varepsilon\in U_K\setminus\{1\}$" in Definition 4.9 we will quantify over all $\varepsilon,\beta\in\mathscr{O}_K$ by requiring nothing if $\varepsilon\beta$ is not equal to 1 or if $\varepsilon=1$ and requiring (4.10)–(4.15) if $\varepsilon\beta=1$. More formally, we have the following definition of $\mathbb{Z}$:

$$\forall\varepsilon\forall\beta\in\mathscr{O}_K:(\varepsilon\beta=1\wedge[(\varepsilon=1)\vee((\varepsilon\neq1)\wedge\ldots))])\vee(\varepsilon\beta\neq1),$$

where we insert equations (4.10)–(4.15) in place of "$\ldots$". Essentially we need a second universal quantifier if ε is not a unit. Having a uniform existential definition of non-units would eliminate the need for the second universal quantifier, but we do not know how to construct such a definition or even if it exists.

Proof of Theorem 4.8. Let K be non-big, and Z_K as in Definition 4.9. We will show that $Z_K=\mathbb{Z}$.

Suppose $w\in Z_K$. Then by Theorem 3.11 we have that either

$$w,u_1,u_2,v_1,v_2,s_1,s_2,t_1,t_2\in\mathbb{Z} \quad \text{or} \quad w,u_1,u_2,v_1,v_2,s_1,s_2,t_1,t_2\in\mathscr{O}_F$$

for some imaginary quadratic field F. In either case equations (4.15) imply $w\in\mathbb{Z}$.

Conversely, if $w\in\mathbb{Z}$, then the proof of Lemma 4.1 shows that the equations of (4.15) can be satisfied with all variables ranging over $\mathbb{Z}$. Therefore equations (4.10)–(4.15) can be satisfied over $\mathscr{O}_K$, so $w\in Z_K$. □

Remark 4.17. Let $\mathscr{A}$ denote the set of all algebraic extensions K of $\mathbb{Q}$ such that the set Z_K of Definition 4.9 is equal to $\mathbb{Z}$. Theorem 4.8 implies that $\mathscr{A}$ contains all non-big fields, including in particular all number fields. This leads us to the following questions.

Question 4.18. Does $\mathscr{A}$ contain any big fields?

Question 4.19. Does $\mathscr{A}$ contain all abelian fields?

Remark 4.20. The construction we used above can be adapted in the case of number fields to produce a definition of $\mathbb{Z}$ of the form $\forall\exists\ldots\exists$. Unfortunately this definition, as in the case of the definition in this form constructed by J. Robinson, is uniform only across classes of number fields of bounded degree.

5. Non-existence of uniform existential or purely universal definitions of $\mathbb{Z}$

Recall the definition of "uniform" (Definition 1.6) and consider the following definition.

Definition 5.1. Let R be a ring. Let $A \subset R$ and assume there exists a polynomial $p(t, x_1, \ldots, x_k) \in R[t, x_1, \ldots, x_k]$ such that

$$A = \{t \in R | \exists x_1, \ldots, x_k \in R^k : p(t, x_1, \ldots, x_k) = 0\}.$$

Then $p(t, \bar{x})$ is called a diophantine definition of A over R.

Proposition 5.2. *Let K be a number field, L an algebraic extension of K, and A a subset of $\mathcal{O}_L$. If there is a diophantine definition of $A \cap \mathcal{O}'_L$ over $\mathcal{O}_{L'}$ uniform across the rings of algebraic integers $\mathcal{O}_{L'}$ for all finite extensions L' of K in L, then there exists a diophantine definition of A over $\mathcal{O}_L$.*

Proof. Let $p(t, \bar{x}) \in \mathcal{O}_K[t, \bar{x}]$ be a diophantine definition of $\mathcal{O}_{L'} \cap A$ for all finite extensions L' of K in L. Let $t \in A \subset \mathcal{O}_L$. Let $L' = K(t)$. Then there exists an m-tuple $\bar{x} \in \mathcal{O}_{L'}^m \subset \mathcal{O}_L^m$ such that $p(t, \bar{x}) = 0$.

Now suppose there exists $t \in \mathcal{O}_L \setminus A$ such that for some $\bar{y} \in \mathcal{O}_L$ we have that $p(t, \bar{y}) = 0$. Let $L' = K(t, \bar{y})$. Then $p(t, \bar{x})$ is not a diophantine definition of $A \cap \mathcal{O}_{L'}$ over $\mathcal{O}_{L'}$, contradicting our assumption on $p(t, \bar{x})$. Thus, for any $t \in \mathcal{O}_L$ we have that there exists $\bar{x} \in \mathcal{O}_L$ such that $p(t, \bar{x}) = 0$ if and only if $t \in A$. □

Corollary 5.3. *Let K be a number field and $\mathscr{L}$ the collection of all finite extensions of K. Then there is no uniform purely existential or purely universal definition of $\mathcal{O}_K$ across rings of integers of elements of $\mathscr{L}$.*

Proof. We apply Proposition 5.2 to $A := A_1 = \mathcal{O}_K$ and $A := A_2 = \mathcal{O}_{\bar{K}} \setminus \mathcal{O}_K$, with $F = \bar{K}$, the algebraic closure of K. If A_1 has a uniform diophantine definition across fields in $\mathscr{L}$, then $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_{\bar{K}}$. If A_2 has a uniform diophantine definition across rings of integers of fields in $\mathscr{L}$, then $\mathcal{O}_{\bar{K}} \setminus \mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_{\bar{K}}$ or, equivalently, $\mathcal{O}_K$ has a purely universal definition over $\mathcal{O}_{\bar{K}}$. In either case $\mathcal{O}_K$ has a first-order definition over $\mathcal{O}_{\bar{K}}$. But by the result of J. Robinson ([Rob49]) we know that the first-order theory of any number field is undecidable and by a result of van den Dries ([vdD88]) we know that the first-order theory of $\mathcal{O}_{\mathbb{Q}}$ is decidable. Hence neither A_1, nor A_2 can have a uniform existential definition across elements of $\mathscr{L}$. Therefore, there is no uniform purely universal definition of $\mathcal{O}_K$ across rings of integers of elements of $\mathscr{L}$. □

Applying the discussion above to $K = \mathbb{Q}$. we get:

Corollary 5.4. *There is no existential or purely universal definition of $\mathbb{Z}$ uniform across all rings of integers of number fields.*

Finally we note that in view of the results above, the uniform definition of $\mathbb{Z}$ across all number fields we give in Theorem 4.8 is the best possible as far as the

arithmetic hierarchy is concerned: the statement of that theorem would be false if we replaced "$\forall\exists\ldots\exists$" by "$\exists\ldots\exists$".

REFERENCES

[CVV20] Marianela Castillo, Xavier Vidaux, and Carlos R. Videla, *Julia Robinson numbers and arithmetical dynamic of quadratic polynomials*, Indiana Univ. Math. J. **69** (2020), no. 3, 873–885. ↑4

[CF21] Sara Checcoli and Arno Fehm, *On the Northcott property and local degrees*, Proc. Amer. Math. Soc. **149** (2021), no. 6, 2403–2414. ↑4

[Chu36] Alonzo Church, *An unsolvable problem of elementary number theory*, American Journal of Mathematics **58** (1936), 345 –363. ↑3

[CPZ05] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and diophantine problem for rings of integers*, Journal de Théorie des Nombres Bordeaux **17** (2005), 727–735. ↑3

[Dav73] Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80(3)** (1973), 233-269. ↑5

[Den75] Jan Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220. ↑3, 5, 14, 15

[Den80] Jan Denef, *Diophantine sets of algebraic integers, II*, Transactions of American Mathematical Society **257** (1980), no. 1, 227–236. ↑3, 5, 7

[DL78] Jan Denef and Leonard Lipshitz, *Diophantine sets over some rings of algebraic integers*, Journal of London Mathematical Society **18** (1978), no. 2, 385–391. ↑3, 5

[EG15] Jan-Hendrik Evertse and Kálmán Győry, *Unit equations in Diophantine number theory*, Cambridge Studies in Advanced Mathematics, vol. 146, Cambridge University Press, Cambridge, 2015. ↑9, 10

[FHV94] Michael D. Fried, Dan Haran, and Helmut Völklein, *Real Hilbertianity and the field of totally real numbers*, Arithmetic geometry (Tempe, AZ, 1993), 1994, pp. 1–34. ↑4

[GFP20] Natalia Garcia-Fritz and Hector Pasten, *Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points*, Math. Ann. **377** (2020), no. 3-4, 989–1013. ↑3

[GR19] Pierre Gillibert and Gabriele Ranieri, *Julia Robinson numbers*, Int. J. Number Theory **15** (2019), no. 8, 1565–1599. ↑4

[Göd31] Kurt Gödel, *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik **38** (1931), 173 –198. ↑3

[Koe14] Jochen Koenigsmann, *Undecidability in number theory*, Model theory in algebra, analysis and arithmetic, Lecture Notes in Math., vol. 2111, Springer, Heidelberg, 2014. ↑9

[MRUV20] Carlos Martínez-Ranero, Javier Utreras, and Carlos R. Videla, *Undecidability of* $\mathbb{Q}^{(2)}$, Proc. Amer. Math. Soc. **148** (2020), no. 3, 961–964. ↑2, 4, 6

[MR10] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's Tenth Problem*, Inventiones Mathematicae **181** (2010), 541–575. ↑3

[MR20] Barry Mazur and Karl Rubin, *Big fields that are not large*, Proc. Amer. Math. Soc. Ser. B **7** (2020), 159–169. ↑4

[MRS22] B Mazur, K Rubin, and A Shlapentokh, *Existential definability and diophantine stability*, 2022. ↑3, 7, 14, 15

[MP18] M. Ram Murty and Hector Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem*, J. Number Theory **182** (2018), 1–18. ↑3

[Pas23] Hector Pasten, *Superficies elípticas y el décimo problema de Hilbert/Elliptic surfaces and Hilbert's tenth problem*, Rev. Mat. Teor. Apl. **30** (2023), no. 1, 113 –120. ↑3

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proceedings of American Mathematical Society **104** (1988), no. 2, 611–620. ↑3, 5

[Rob49] Julia Robinson, *Definability and decision problems in arithmetic*, Journal of Symbolic Logic **14** (1949), 98–114. ↑3, 17

[Rob62] Julia Robinson, *On the decision problem for algebraic rings*, Studies in mathematical analysis and related topics, 1962, pp. 297–304. ↑3, 4, 9

[Rob69] Julia Robinson, *Unsolvable diophantine problems*, Proc. Amer. Math. Soc. **22** (1969), 534–538, DOI 10.2307/2037095. ↑5

[Ros36] Barkley Rosser, *Extensions of some theorems of Gödel and Church*, Journal of Symbolic Logic **1** (1936), no. 3, 87–91, DOI 10.2307/2269028. ↑3

[Rum86] Robert S. Rumely, *Arithmetic over the ring of all algebraic integers*, J. Reine Angew. Math. **368** (1986), 127–133. ↑4

[SS89] Harold Shapiro and Alexandra Shlapentokh, *Diophantine relations between algebraic number fields*, Communications on Pure and Applied Mathematics **XLII** (1989), 1113–1122. ↑3

[Shl07] Alexandra Shlapentokh, *Diophantine definability and decidability in the extensions of degree 2 of totally real fields*, Journal of Algebra **313** (2007), no. 2, 846–896. ↑3

[Shl08] Alexandra Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555. ↑3

[Shl09] Alexandra Shlapentokh, *Rings of algebraic numbers in infinite extensions of $\mathbb{Q}$ and elliptic curves retaining their rank*, Arch. Math. Logic **48** (2009), no. 1, 77–114. ↑3

[Shl18] Alexandra Shlapentokh, *First-order decidability and definability of integers in infinite algebraic extensions of the rational numbers*, Israel J. Math. **226** (2018), no. 2, 579–633. ↑4, 5

[Shl89] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Communications on Pure and Applied Mathematics **XLII** (1989), 939–962. ↑3, 5

[Shl02] Alexandra Shlapentokh, *Diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2*, J. Number Theory **95** (2002), no. 2, 227–252. ↑6

[Shl04] Alexandra Shlapentokh, *On Diophantine definability and decidability in some infinite totally real extensions of $\mathbb{Q}$*, Trans. Amer. Math. Soc. **356** (2004), no. 8, 3189–3207. ↑6

[Shl94] Alexandra Shlapentokh, *Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of* **Q**, Ann. Pure Appl. Logic **68** (1994), no. 3, 299–325. ↑6

[Spr20] Caleb Springer, *Undecidability, unit groups, and some totally imaginary infinite extensions of $\mathbb{Q}$*, Proc. Amer. Math. Soc. **148** (2020), no. 11, 4705–4715. ↑4, 6

[Spr23] Caleb Springer, *Definability and decidability for rings of integers in totally imaginary fields*, Bulletin of LMS (2023). ↑4, 6

[Tar48] Alfred Tarski, *A decision method for elementary Algebra and Geometry*, Rand Corporation report (1948). ↑2

[vdD88] Lou van den Dries, *Elimination theory for the ring of algebraic integers*, J. Reine Angew. Math. **388** (1988), 189–205. ↑4, 17

[VV15] Xavier Vidaux and Carlos R. Videla, *Definability of the natural numbers in totally real towers of nested square roots*, Proc. Amer. Math. Soc. **143** (2015), no. 10, 4463–4477. ↑4

[VV16] Xavier Vidaux and Carlos R. Videla, *A note on the Northcott property and undecidability*, Bull. Lond. Math. Soc. **48** (2016), no. 1, 58–62. ↑4

[Vid00a] Carlos Videla, *Definability of the ring of integers in pro-p extensions of number fields*, Israel Journal of Mathematics **118** (2000), 1–14. ↑4

[Vid00b] Carlos R. Videla, *The undecidability of cyclotomic towers*, Proc. Amer. Math. Soc. **128** (2000), no. 12, 3671–3674. ↑4

[Vid99] Carlos Videla, *On the constructible numbers*, Proceedings of American Mathematical Society **127** (1999), no. 3, 851–860. ↑

[Vid89] Carlos Videla, *Sobre el décimo problema de Hilbert*, Atas da Xa Escola de Algebra (Vitoria, ES, Brasil), Coleção Atas 16 da Sociedade Brasileira de Matemática 1989, 1989, pp. 95 – 108. ↑3, 5

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138-2901
Email address: mazur@g.harvard.edu
URL: http://www.math.harvard.edu/~mazur

DEPARTMENT OF MATHEMATICS, UC IRVINE, IRVINE, CA 92697, USA
Email address: krubin@uci.edu
URL: https://math.uci.edu/~krubin

DEPARTMENT OF MATHEMATICS, EAST CAROLINA UNIVERSITY, GREENVILLE, NC 27858
Email address: shlapentokha@ecu.edu
URL: myweb.ecu.edu/shlapentokha