Definability and decidability for rings of integers in totally imaginary fields

Caleb Springer\textsuperscript{1,2} \begin{figure}
\begin{itemize}
\item \textsuperscript{1}Department of Mathematics, University College London, London, UK
\item \textsuperscript{2}The Heilbronn Institute for Mathematical Research, Bristol, UK
\end{itemize}
\end{figure}

Correspondence
Caleb Springer, Department of Mathematics, University College London, Gower St, London, UK.
Email: c.springer@ucl.ac.uk

Funding information
Additional Funding Programme for Mathematical Sciences; EPSRC, Grant/Award Number: EP/V521917/1; Heilbronn Institute for Mathematical Research

Abstract
We show that the ring of integers of $\mathbb{Q}^{\text{tr}}$ is existentially definable in the ring of integers of $\mathbb{Q}^{\text{tr}}(\iota)$, where $\mathbb{Q}^{\text{tr}}$ denotes the field of all totally real numbers. This implies that the ring of integers of $\mathbb{Q}^{\text{tr}}(\iota)$ is undecidable and first-order nondefinable in $\mathbb{Q}^{\text{tr}}(\iota)$. More generally, when $L$ is a totally imaginary quadratic extension of a totally real field $K$, we use the unit groups $R^X$ of orders $R \subseteq \mathcal{O}_L$ to produce existentially definable totally real subsets $X \subseteq \mathcal{O}_L$. Under certain conditions on $K$, including the so-called JR-number of $\mathcal{O}_K$ being the minimal value $\text{JR}(\mathcal{O}_K) = 4$, we deduce the undecidability of $\mathcal{O}_L$.

This extends previous work that proved an analogous result in the opposite case $\text{JR}(\mathcal{O}_K) = \infty$. In particular, unlike prior work, we do not require that $L$ contains only finitely many roots of unity.

MSC 2020
11R04, 11R80, 11U05 (primary), 12L05 (secondary)

1 \quad INTRODUCTION

1.1 \quad A motivating example

This paper is motivated by the desire to prove the following theorem concerning definability and decidability. For background and an overview of decidability and definability for infinite algebraic extensions of $\mathbb{Q}$, we refer readers to the introduction of [28]; see also the prequel to our...
work here [30]. Recall that $\alpha \in \overline{\mathbb{Q}}$ is totally real if the roots of its minimal polynomial are all real numbers. We write $\mathbb{Q}^{tr}$ for the field of all totally real algebraic numbers and $\mathbb{Z}^{tr}$ for its ring of integers, and we set $i = \sqrt{-1}$.

**Theorem 1.1.** The ring of integers $\mathbb{Z}^{tr}$ of $\mathbb{Q}^{tr}$ is existentially definable in the ring of integers of $\mathbb{Q}^{tr}(i)$. In particular, the first-order theory of the ring of integers of $\mathbb{Q}^{tr}(i)$ is undecidable.

**Remark 1.2.** The paragraph below [16, Corollary 3.19] mistakenly declared the ring of integers of $\mathbb{Q}^{tr}(i)$ to be decidable.† The reference given for this claim is [6, Theorem 10.7], which actually proves the decidability of the overring $\mathcal{O}_{\mathbb{Q}^{tr}(i)}\left[\frac{1}{p}\right]$ where $p$ is any prime number. As seen above, the ring of integers $\mathcal{O}_{\mathbb{Q}^{tr}(i)}$ itself is undecidable.

Theorem 1.1 is proven by extending and generalizing the methods that were first used to prove the first-order undecidability of rings of integers in fields such as $\mathbb{Q}(2)$ [19] and $\mathbb{Q}(d)$ for $d \geq 2$ [30]. Here, $F^{(d)}$ denotes the compositum of all extensions of degree at most $d$ of a field $F$, and $F^{(d)}_{ab} \subseteq F^{(d)}$ is the maximal abelian subfield. However, notice that the papers [19, 30] additionally proved that the fields $\mathbb{Q}^{(d)}_{ab}$ themselves are undecidable by appealing to results of Videla [34] and Shlapentokh [28] which imply that each $\mathbb{Q}^{(d)}_{ab}$ has a first-order definable ring of integers.

The situation is entirely the opposite in the setting of Theorem 1.1. Indeed, Fried, Haran, and Völklein proved that $\mathbb{Q}^{tr}$ is decidable [11], which implies that $\mathbb{Q}^{tr}(i)$ is also decidable. It has been previously observed that, because Robinson proved that $\mathbb{Z}^{tr}$ is undecidable [25], the field $\mathbb{Q}^{tr}$ is thus an example of a subfield of $\mathbb{Q}$ whose ring of integers $\mathbb{Z}^{tr}$ does not admit any first-order definition in $\mathbb{Q}^{tr}$. In the framework of Shlapentokh [28, Section 2.1], this is intuitively understood as a result of the fact that the field $\mathbb{Q}^{tr}$ is too “close” to $\mathbb{Q}$, so it does not have enough “expressive power” to have a definable ring of integers. By Theorem 1.1, we immediately see that $\mathbb{Q}^{tr}(i)$ also has a first-order nondefinable ring of integers, as expected.

We pause to note that $\mathbb{Q}^{tr}(i)$ is known to be an $\omega$-free PAC field; see [13, Example 5.10.7]. Therefore, the nondefinability of the ring of integers of $\mathbb{Q}^{tr}(i)$ can also be deduced from the following result of Dittman and Fehm: If $R$ is a first-order definable subring of an $\omega$-free PAC field $L$, then $R$ is a field [8, Proposition 3]. Their method, which builds upon work of Chatzidakis [5], is entirely different from the techniques that we use below.

### 1.2 Main results

In general, this paper considers totally imaginary quadratic extensions of totally real fields. We begin with a definability result. Say that a totally real field $K \subseteq \overline{\mathbb{Q}}$ is closed under square roots if $\alpha \in K$ whenever $\alpha$ is a totally real number such that $\alpha^2 \in K$.

**Theorem 1.3** (Theorem 3.5). If $K$ is a totally real field that is closed under square roots and $L$ is any quadratic totally imaginary extension of $K$, then $\mathcal{O}_K$ is existentially definable in $\mathcal{O}_L$.

This theorem implies Theorem 1.1 immediately, given Robinson’s proof that $\mathbb{Z}^{tr}$ is undecidable [25]. However, we can actually prove first-order undecidability for rings of integers $\mathcal{O}_L$ in a more

---

† We thank Aharon Razon for pointing this out after reading an earlier draft of this paper.
general context where $\mathcal{O}_K$ is not known to be existentially definable in $\mathcal{O}_L$. For any $n \geq 1$, let $\zeta_n$ denote a primitive $n$th root of unity.

**Theorem 1.4** (Theorem 4.5). Let $S \subseteq \mathbb{N}$ be infinite. Define $K_0 = \mathbb{Q}(\{\zeta_n + \bar{\zeta}_n : n \in S\})$ and let $K_1$ be the maximal totally real subfield of $K_0^{(2)}$. If $K \supseteq K_1$ is a totally real field and $L$ is any totally imaginary quadratic extension of $K$, then $\mathcal{O}_L$ is undecidable.

In this theorem, the so-called JR-number is $JR(\mathcal{O}_K) = 4$, that is, the minimal possible value, while the totally real fields $K$ considered in [19, 30] have the maximal possible value $JR(\mathcal{O}_K) = \infty$; see Subsection 4.1 for definitions and notation. We also provide a version of our undecidability result, namely Theorem 4.4, which does not place a restriction on the value of $JR(\mathcal{O}_K)$.

### 1.3 Proof method: Leveraging unit groups

Within the body of literature concerning undecidability results for rings of integers of algebraic extensions of $\mathbb{Q}$, the totally real subfields of $\mathbb{Q}$ and their totally imaginary quadratic extensions have received special attention. There are multiple methods that can be used in this context, but we focus on the work stemming from Robinson for now, and delay the discussion of elliptic curves until the following section.

Robinson [25] provided a general sufficient condition for proving the undecidability of a ring of algebraic integers $\mathcal{O}$, and we follow Videla [35] by using an improved version credited to Henson [31]: If there is a parameterized family $F$ of definable subsets of $\mathcal{O}$ that contains finite sets of arbitrarily large cardinality, then the first-order theory of $\mathcal{O}$ is undecidable. This sufficient condition, along with a theorem of Siegel [29], leads to a strategy that can be applied to $\mathcal{O}_K$ when $K$ is a totally real field. Indeed, we use the parameterized family of subsets $\{X_t\}_{t \in \mathbb{Q}}$, where $X_t$ contains the elements $\alpha \in \mathcal{O}_K$ whose conjugates all lie in the real interval $(0, t)$. Determining whether $\{X_t\}_{t \in \mathbb{Q}}$ contains finite sets of arbitrarily large size is related to the JR-number of $\mathcal{O}_K$; see Subsection 4.1 for more details. This strategy enabled Robinson to prove the undecidability of the rings of integers of both $\mathbb{Q}_{tr}$ and $\mathbb{Q}_{tr}^{(2)} = \mathbb{Q}(\sqrt{n} : n \in \mathbb{N})$.

After using this method to prove $\mathcal{O}_K$ is undecidable for a totally real field $K$, we wish to do the same for the rings of integers $\mathcal{O}_L$ for all totally imaginary quadratic extensions $L$ of $K$. To extend the JR-number argument to such a field, a key ingredient is the fact that $[\mathcal{O}_L^\times : \mu(L)\mathcal{O}_K^\times] \leq 2$ where $\mu(L)$ is the set of roots of unity in $L$. Therefore, if $N = \#\mu(L) < \infty$ is finite, then $\mathcal{O}_L^\times 2N \subseteq K$ is an existentially definable totally real subset of $\mathcal{O}_L$. By using sums and difference of powers of units, we can produce a useful parameterized family of subsets of $\mathcal{O}_L$ analogous to the sets $X_t$ defined above. Undecidability is thereby proved for $\mathcal{O}_L$ in many cases, including $L = \mathbb{Q}^{(2)}$ or more generally $L = \mathbb{Q}_d^{(d)}$ for $d \geq 2$; see [19, 30].

However, the assumption $\#\mu(L) < \infty$ above implies that this method cannot yet apply when $L = \mathbb{Q}^{(i)}$. To remedy this, we choose to instead work with the unit group $\mathbb{R}^\times$ of an existentially definable nonmaximal order $R \subseteq \mathcal{O}_L$ with $\mu(R) = \{\pm1\}$ trivial. In this case, we can show that $(\mathbb{R}^\times)^2$ is totally real set. By choosing a suitable ring $R \subseteq \mathcal{O}_L$, we obtain the foundation for developing a unit group-based argument similar to the ones appearing in [19, 30] that allows $L$ to contain infinitely many roots of unity.
1.4 | A comparison with abelian varieties

We conclude this section by comparing our main theorems to similar results that leverage elliptic curves instead of unit groups. There are many papers that use elliptic curves, or abelian varieties in general, to prove various undecidability results, including [7, 21, 23, 35]. We refer to [27] for additional background. As an example that is relevant to the consideration of totally imaginary extensions of totally real fields, consider the following theorem of Shlapentokh.

**Theorem 1.5** [27, Main Theorem B]. Let $K$ be a totally real algebraic extension of $\mathbb{Q}$ that has a totally real extension of degree 2, and let $K'$ be a finite extension of $K$ such that there exists an elliptic curve $E$ defined over $K'$ with $E(K')$ finitely generated and of positive rank. If $L$ is a quadratic totally imaginary extension of $K$, then $\mathbb{Z}$ is existentially definable in the ring of integers $\mathcal{O}_K$ and Hilbert’s Tenth Problem is unsolvable over $\mathcal{O}_K$.

Although Theorems 1.4 and 1.5 are similar insofar as they both apply in the context of totally imaginary quadratic extensions of totally real subfields of $\mathbb{Q}$, it is instructive to also note the differences and complementary strengths. Heuristically, it is easiest to apply the elliptic curve-based methods to relatively “small” algebraic extensions of $\mathbb{Q}$ over which it is easy to find elliptic curves with a finitely generated group of rational points. In contrast, the unit group-based methods work best for “bigger” fields in which there is an abundance of units available for manipulation. We can make this more precise with a couple of examples.

The prototypical example of an infinite algebraic extension $K \supseteq \mathbb{Q}$ that satisfies the hypotheses of Theorem 1.5 is a $\mathbb{Z}_p$-extension of $\mathbb{Q}$; see [27, Section 10]. These $\mathbb{Z}_p$-extensions are difficult to handle with the unit group-based methods because there is at most one subextension of $K$ of any given degree, hence a paucity of units. We also note that Theorem 1.5 proves that Hilbert’s Tenth Problem is unsolvable, rather than only showing that the first-order theory is undecidable, and it also applies when $[K: \mathbb{Q}] < \infty$.

On the other hand, when deploying elliptic curves, we emphasize that it is necessary for the group of rational points to be a finitely generated group. This is a core requirement of the proof method, and the restriction would remain for any straightforward variant or generalization that uses abelian varieties instead of elliptic curves, such as [21, Theorem 1.1]. Therefore, the following theorem of Fehm and Petersen shows that this general method is not useable when the field $K$ is large, in the sense of Pop [24].

**Theorem 1.6** [9, Theorem 1.2]. If $L \subseteq \overline{\mathbb{Q}}$ is a large field and $A/L$ is an abelian variety, then $A(L)$ has infinite rank.

The first proof of this theorem in the case of elliptic curves is credited to Tamagawa; see Kobayashi [15, Proposition 1]. We refer to [10, 18, 20, 22] for some additional results on finitely and nonfinitely generated groups of rational points.

Because any algebraic extension of a large field is itself large, Theorem 1.6 shows that if $K \subseteq \overline{\mathbb{Q}}$ is a large totally real field, then abelian variety-based methods such as Theorem 1.5 cannot handle $K$ or its quadratic totally imaginary extensions. However, it is clear that the unit group-based methods presented in this paper can work for large fields because the field $\mathbb{Q}^{ur}$ is large. It is also conjectured that $\mathbb{Q}^{ab}$ is a large field (see [1, Section 3] for background and an overview), and it is easy to construct extensions $L \supseteq \mathbb{Q}^{ab}$ that are covered by Theorem 1.4. It would be interesting to
determine whether or not the methods of this paper can be refined to prove the undecidability of the ring of integers of \( \mathbb{Q}^{ab} \) itself.

# 2 Nonmaximal Orders and Units

As indicated in Subsection 1.3, given a totally real field \( K \) and a totally imaginary quadratic extension \( L \), we want a subring \( R \subseteq \mathcal{O}_L \) that does not contain any nontrivial roots of unity. We start by defining the desired ring, then proceed to analyze its group of units.

## 2.1 A useful nonmaximal subring

**Definition 2.1.** Given an integer \( m \geq 1 \) and a field \( L \subseteq \overline{\mathbb{Q}} \), let \( R_{m,L} \) be the subset of \( \mathcal{O}_L \) defined by the positive existential formula \( \varphi_m(x) \), given as follows:

\[
\exists a \ (x - ma)(x - 1 - ma) \cdots (x - (m - 1) - ma) = 0
\]

The following properties of \( R_{m,L} \) are immediate from the definition.

**Lemma 2.2.** Let \( L \subseteq \overline{\mathbb{Q}} \) be a field and let \( m \geq 1 \) be an integer.

(a) If \( K \subseteq L \) is a subfield, then \( R_{m,L} \cap K = R_{m,K} \).

(b) \( R_{m,L} \) is an existentially definable subring of \( \mathcal{O}_L \) that contains \( m\mathcal{O}_L \).

(c) \( R_{m,L} \subseteq \mathcal{O}_L \) is nonmaximal if and only if \( m \geq 2 \) and \( L \neq \mathbb{Q} \).

**Proof.** By the definition of \( R_{m,L} \) and the formula \( \varphi_m(x) \) above, the first claim is obvious. Moreover, \( R_{m,L} \) is the preimage of \( \mathbb{Z}/m\mathbb{Z} \) under the natural surjective map \( \mathcal{O}_L \to \mathcal{O}_L/m\mathcal{O}_L \). Therefore, \( R_{m,L} \) is a subring of \( \mathcal{O}_L \) and nonmaximal precisely when \( \mathbb{Z}/m\mathbb{Z} \neq \mathcal{O}_L/m\mathcal{O}_L \), that is, when \( m \geq 2 \) and \( L \neq \mathbb{Q} \).

Before we analyze the unit group \( R_{m,L}^\times \), we recall some general elementary facts. In essence, this theorem clarifies that any ring containing an algebraic unit \( u \) also contains \( u^{-1} \), and computes the rank of the unit groups of any ring of algebraic integers. Given a set \( S \subseteq \overline{\mathbb{Q}} \), let \( \mu(S) \) denote the set of roots of unity contained in \( S \).

**Theorem 2.3.** Let \( L \subseteq \overline{\mathbb{Q}} \) be a number field with \( r \) real and \( 2s \) imaginary embeddings.

(a) If \( u \in \mathcal{O}_L^\times \), then \( u^{-1} \in \mathbb{Z}[u] \).

(b) If \( R \subseteq \mathcal{O}_L \) is any subring, then \( R^\times = \mathcal{O}_L^\times \cap R \).

(c) If \( \mathcal{O} \subseteq \mathcal{O}_L \) is any suborder, then \( \mathcal{O}^\times = \mu(\mathcal{O}) \times \mathbb{Z}^{r+s-1} \).

**Proof.** An algebraic unit \( u \) has minimal polynomial \( m(x) = x^n + c_{n-1}x^{n-1} \cdots + c_1x + 1 \) with integer coefficients. Evaluating this polynomial at \( u \), along with rearranging terms, shows that \( u(u^{n-1} + c_{n-1}u^{n-2} + \cdots + c_1) = \pm 1 \), which proves the first claim. The second claim follows immediately from the first.
By Dirichlet’s unit theorem, $\mathcal{O}_L^\times \cong \mu(L) \times \mathbb{Z}^{r+s-1}$. Thus, we only need to check the rank of $\mathcal{O}_L^\times$. Because $\mathcal{O} \subseteq \mathcal{O}_L$ is a suborder, the index $N = [\mathcal{O}_L : \mathcal{O}]$ is finite and $N \mathcal{O}_L \subseteq \mathcal{O}$. If $u \in \mathcal{O}_L^\times$ then $u$ reduces modulo $N$ to an element of $(\mathcal{O}_L/N \mathcal{O}_L)^\times$, and $u^t \equiv 1 \mod N \mathcal{O}_L$ for some $1 \leq t \leq \#(\mathcal{O}_L/N \mathcal{O}_L)^\times < N[L:Q]$. We conclude $u^t \in \mathcal{O}_L^\times$. Therefore, $\mathcal{O}_L^\times$ has the same rank as $\mathcal{O}_L^\times$ and we are done. □

As an application, this shows the structure of the unit group of the ring $R_{m,L}$.

**Proposition 2.4.** Let $m \geq 2$ be an integer. If $L$ is a number field with $r$ real embeddings and $2s$ imaginary embeddings, then

$$R_{m,L}^\times \cong \{\pm 1\} \times \mathbb{Z}^{r+s-1}.$$  

In particular, the only roots of unity contained in $R_{m,L}$ are trivial.

**Proof.** By Theorem 2.3, we need to show that $R_{m,L}$ has no roots of unity other than $\pm 1$. If $\zeta \in R_{m,L}^\times$ is a nontrivial root of unity, then $L$ contains the nontrivial cyclotomic subfield $L_0 = \mathcal{O}(\zeta) \supseteq \mathbb{Q}$, and thus $R_{m,L_0} = R_{m,L} \cap L_0 \supseteq \mathbb{Z}[\zeta]$ by Lemma 2.2. But $\mathbb{Z}[\zeta]$ is the maximal order of $L_0$, while $R_{m,L_0}$ is a nonmaximal order, which is a contradiction. □

### 2.2 Totally imaginary extensions of totally real fields

We now restrict our attention to the main focus of this paper: totally imaginary quadratic extensions of totally real fields. The following is a generalization of [36, Theorem 4.12] to the case of nonmaximal orders. Given a field $L$ and a subring $\mathcal{O} \subseteq L$, we write $\mu(\mathcal{O})$ for the set of roots of unity in $\mathcal{O}$.

**Theorem 2.5.** Let $K$ be a totally real field, let $L$ be a totally imaginary quadratic extension, and let $\mathcal{O} \subseteq L$ be an order that is stable under complex conjugation. If $u \in \mathcal{O}_L^\times$, then its complex conjugate is $\overline{u} = \zeta u$ where $\zeta \in \mu(\mathcal{O})$. In particular, writing $\mathcal{O}_u^\times = \mathcal{O} \cap K$,

$$[\mathcal{O}_L : \mu(\mathcal{O}) \cdot \mathcal{O}_u^\times] \leq 2.$$  

**Proof.** Notice that every conjugate of $u/\overline{u}$ has absolute value 1 because $\sigma(\overline{u}) = \overline{\sigma(u)}$ for every embedding $\sigma : L \hookrightarrow \mathbb{C}$; see [36, p. 39]. Therefore, $\overline{u}/u$ is a root of unity [36, Lemma 1.6]. In other words, $\overline{u}/u \in \mu(L) \cap \mathcal{O} = \mu(\mathcal{O})$.

Thus, we define a group homomorphism $\varphi : \mathcal{O}_L^\times \to \mu(\mathcal{O})/\mu(\mathcal{O})^2$ induced by $u \mapsto u/\overline{u}$ and compute its kernel. First, we check that if $u = \zeta u_1$ for $\zeta \in \mu(\mathcal{O})$ and $u_1 \in \mathcal{O}_L^\times \cap K$, then $\varphi(u) = u/\overline{u} = \zeta u_1/\overline{\zeta u_1} = \zeta^2$. Conversely, if $u \in \mathcal{O}_L^\times$ and $\varphi(u) = u/\overline{u} = \zeta^2$, then we rearrange to see $\overline{\zeta} u = \overline{\zeta} \overline{u} \in \mathcal{O}_u^\times$ is totally real. Thus, $\ker \varphi = \mu(\mathcal{O}) \cdot \mathcal{O}_u^\times$. Since we know the index $[\mu(\mathcal{O}) : \mu(\mathcal{O})^2] \leq 2$, the proof is done. □

We now wish to apply this theorem to the nonmaximal subrings defined in the previous section. In our context, this theorem is helpful because we define subrings with no nontrivial roots of unity. Before we move on, we note that the application of Theorem 2.5 in the case when $\mathcal{O} = \mathcal{O}_L$
is a central ingredient in [19, 30]. The following corollary was also inspired by an analogous fact for maximal orders [36, Proof of Proposition 1.5].

Remark 2.6. It is easy to show, for example, using Magma [2], that it is possible to have $R \not\subseteq K$ in Corollary 2.7. Indeed, this occurs for the cyclotomic field $L = \mathbb{Q}(\zeta_{15})$. Thus, squaring the group of units is necessary in the statement of the corollary when $m = 2$.

Corollary 2.7. Let $K$ be a totally real field with totally imaginary quadratic extension $L$.

\begin{enumerate}[(a)]
  \item $(R_{2,L}^\times)^2 \subseteq R_{2,K}^\times$.
  \item If $m \geq 3$, then $R_{m,L}^\times = R_{m,K}^\times$.
\end{enumerate}

Proof. Let $u \in R_{m,L}^\times$. Clearly, $R_{m,L}$ is stable under complex conjugation by definition. Combining Proposition 2.4 and Theorem 2.5, either $\bar{u} = u$ or $\bar{u} = -u$. To finish the proof, assume $m \geq 3$ and suppose that $\bar{u} = -u$. Writing $u = mb + j$ for $b \in \mathcal{O}_L$ and $j \in \mathbb{Z}$ we have $\bar{u} = m\bar{b} + j$. Therefore,

$$2u = u - \bar{u} = mb - m\bar{b} \in m\mathcal{O}_L.$$ 

However, this implies that $m$ divides 2 because $u$ is a unit, and this is impossible because $m \geq 3$. We conclude that $\bar{u} = u$ is totally real. \hfill \Box

3 | DEFINING THE TOTALLY REAL SUBRING

We now show how to deploy the unit groups described in the previous section. To do this, we explicitly write certain totally real algebraic integers as the sum of units.

Lemma 3.1. Let $K_0 \subseteq K_1$ be totally real fields. If $a = 2(2d + 1)$ for some $d \in \mathcal{O}_{K_0}$ such that $\sqrt{d^2 + d} \in K_1$, then there is a unit $u \in R_{2,K_1}^\times$ such that $a = u + 1/u$. In particular,

$$a^2 = u^2 + 1/u^2 + 2.$$ 

Proof. Define $u_j = 2b_j + 1 \in R_{2,K_1}$ where $b_1 = d + \sqrt{d^2 + d}$ and $b_2 = d - \sqrt{d^2 + d}$. It is easy to compute directly that $u_1$ and $u_2$ are inverses of each other, and hence units from $R_{2,K_1}$:

$$u_1u_2 = (2b_1 + 1)(2b_2 + 1) = (2d + 1 + 2\sqrt{d^2 + d})(2d + 1 - 2\sqrt{d^2 + d})$$

$$= (2d + 1)^2 - 4(d^2 + d) = 1.$$ 

Moreover, $u_1 + u_2 = 2(b_1 + b_2 + 1) = 2(2d + 1) = a$. We take $u = u_1$, in which case $1/u = u_2$. It follows immediately that $a^2 = (u + 1/u)^2 = u^2 + 1/u^2 + 2$. \hfill \Box

Lemma 3.2. Let $K_0$ be a totally real field. If $d \in \mathcal{O}_{K_0}$ and all conjugates of $d$ are outside the open interval $(-1, 1) \subseteq \mathbb{R}$, then

$$32d = u^2 + 1/u^2 - v^2 - 1/v^2$$

for units $u, v \in R_{2,K_1}^\times$ where $K_1 = K_0(\sqrt{d^2 + d}, \sqrt{(d - 1)^2 + (d - 1)})$ is totally real.
Proof. It is easy to see that the values of the function \( f(x) = x^2 + x \) are negative precisely when \( x \in (-1, 0) \), so the element \( d^2 + d \) is totally nonnegative if and only if all conjugates of \( d \) lie outside of \((-1, 0)\). Similarly, \((d - 1)^2 + (d - 1)\) is totally nonnegative if and only if all conjugates of \( d \) lie outside of \((0,1)\). Therefore, if the conjugates of \( d \) lie outside of \((-1,1)\), then elements \( d^2 + d \) and \((d - 1)^2 + (d - 1)\) are both totally nonnegative, so their square roots \( \sqrt{d^2 + d} \) and \( \sqrt{(d - 1)^2 + (d - 1)} \) are totally real. Thus, applying Lemma 3.1 twice,

\[
32d = 4(2d + 1)^2 - 4(2(d - 1) + 1)^2 = u^2 + 1/u^2 - v^2 - 1/v^2
\]

for some \( u, v \in \mathbb{R}_{2, K_1} \). \( \square \)

Now we are ready to define the desired totally real subsets \( X \) within the totally imaginary fields. This can be seen as a generalization of [19, Lemma 7] and [30, Lemma 2.7].

**Theorem 3.3.** Let \( K_0 \) be a totally real field and let \( K_1 \) be the maximal totally real subfield of \( K_0^{(2)} \). If \( K \supseteq K_1 \) is a totally real field, then for every totally imaginary quadratic extension \( L \) of \( K \), there is an existentially definable subset \( X \subseteq \mathcal{O}_L \) satisfying

\[
\mathcal{O}_{K_0} \subseteq X \subseteq \mathcal{O}_K.
\]

**Proof.** We write

\[
X_0 = \{u_1^2 + u_2^2 - u_3^2 - u_4^2 : u_1, \ldots, u_4 \in \mathbb{R}_{2,L}^x \}.
\]

We have \( X_0 \subseteq \mathcal{O}_K \) by Corollary 2.7, and the set

\[
X_1 = \{d \in \mathcal{O}_L : 32d \in X_0 \}
\]

contains all elements \( d \in \mathcal{O}_{K_0} \) whose conjugates are all outside \((-1, 1)\) by Lemma 3.2. We repeat the same trick from before to finish the proof: If \( d \in \mathcal{O}_{K_0} \), then \((d - 1)^2 \) and \((d + 1)^2 \) are totally nonnegative. In particular, the elements \((d - 1)^2 + 1\) and \((d + 1)^2 + 1\) are contained in \( X_1 \) because their conjugates lie inside \([1, \infty)\), and outside \((-1, 1)\). Thus, we may write \( 4d \) as the difference of these two elements of \( X_1 \), namely, \( 4d = (d + 1)^2 + 1 - ((d - 1)^2 + 1) \).

In summary, \( \mathcal{O}_{K_0} \subseteq X \subseteq \mathcal{O}_K \), where

\[
X = \{\alpha \in \mathcal{O}_L : \exists x_1, x_2 \in X_1, 4\alpha = x_1 - x_2 \}.
\]

Because the ring \( R_{2,L} \) is existentially definable in \( \mathcal{O}_L \), this completes the proof. \( \square \)

**Remark 3.4.** The definition of the subset \( X \) in Theorem 3.3 is uniform in the sense that the formula defining \( X \) does not depend on the choices of \( K_0, K_1, K, \) or \( L \).

By applying the previous theorem in the case where \( K_0 = K \), we find that the ring of integers \( \mathcal{O}_K \) itself is existentially definable in \( \mathcal{O}_L \), as written in the following theorem. Recall that \( K \) is closed under square roots if \( \alpha \in K \) whenever \( \bar{\alpha} \in \overline{\mathbb{Q}} \) is totally real and \( \alpha^2 \in K \).
Theorem 3.5. If $K$ is a totally real field that is closed under square roots and $L$ is any quadratic totally imaginary extension of $K$, then $\mathcal{O}_K$ is existentially definable in $\mathcal{O}_L$.

As $\mathbb{Q}^{\text{tr}}$ is closed under square roots, we obtain the definability portion of Theorem 1.1.

Corollary 3.6. $\mathbb{Z}^{\text{tr}}$ is existentially definable in the ring of integers of $\mathbb{Q}^{\text{tr}}(i)$.

Throughout this section, we have exploited the fact that, within the fields $K$ that we consider, many algebraic integers can be written as the sum of a bounded number of units. For contrast, note that Frey and Jarden showed the following when $F$ is a number field: There is no integer $n \geq 1$ such that every element of $\mathcal{O}_F$ is the sum of at most $n$ units in $\mathcal{O}_F^\times$ [14, Theorem 1]. In the same paper, they construct many infinite algebraic extensions of $\mathbb{Q}$ in which every element of the ring of integers is the sum of at most two units; see [14, Theorem 8]. Although the fields they consider are not used in this paper, their complementary results illustrate how we are exploiting a phenomenon that exists only for (some) infinite algebraic extensions of $\mathbb{Q}$, and not for number fields.

4 | UNDECIDABILITY

The definability results in the preceding section have immediate consequences for decidability. Namely, in the context of Theorem 3.5, if the existential or first-order theory of $\mathcal{O}_K$ is undecidable then the same is true for $\mathcal{O}_L$. However, this is not the end of the story because the implications for decidability go beyond the hypotheses of the theorem. Indeed, we can deduce a much more general undecidability result with a further development of the ideas used in previous unit group-based methods [19, 30]. Specifically, we only need to define “enough” of the maximal totally real subring to realize the JR-number.

To start, we recall the following lemma, which is Henson’s extension [31, Section 3.3] of a result of Robinson [25, Theorem 2]; see also the presentation in [19, Lemma 2.2]. This will be the basis for all of our undecidability results.

Lemma 4.1. Let $\mathcal{O}$ be a ring of algebraic integers. If there is a family $F$ of subsets of $\mathcal{O}$, parameterized by an $L_{\text{ring}}$-formula, which contains finite sets of arbitrarily large cardinality, then $\mathcal{O}$ has undecidable first-order theory.

4.1 | Undecidability for totally real $\mathcal{O}_K$

Before considering totally imaginary fields, we briefly sketch the JR-number method for proving the undecidability of the ring of integers of a totally real field; see [25, 32, 33] for more details.

Definition 4.2. Given a totally real number $\alpha \in \overline{\mathbb{Q}}$ and $t \in \mathbb{R}$, we write $0 \ll \alpha \ll t$ if every conjugate of $\alpha$ lies in the interval $(0, t)$. For a totally real subset $X \subseteq \overline{\mathbb{Q}}$, write $X_t = \{\alpha \in X : 0 \ll \alpha \ll t\}$. The JR-number of $X$ is

$$\text{JR}(X) = \inf\{t \in \mathbb{R} : \#X_t = \infty\}.$$
In particular, when $K$ is totally real, Robinson [25] observed that if $JR(O_K)$ is either $\infty$ or a minimum, then Lemma 4.1 implies that $O_K$ is undecidable. Indeed, $\{X_t\}_{t \in \mathbb{Q}}$ can be realized as a parameterized family of existentially definable sets when $X = O_K$ and $t \in \mathbb{Q}$, as written below. This follows from Siegel’s proof that the totally nonnegative elements of $K$ are precisely the elements that are sums of four squares [29]. Consequently, Robinson deduced that the ring of totally real algebraic integers $\mathbb{Z}^{tr}$ is undecidable.

**Theorem 4.3.** Let $K$ be a totally real field. If $X = O_K$ and $t = \frac{a}{b} \in \mathbb{Q}$, then $X_t$ is defined in $O_K$ by the formula:

$$\exists y_0, \ldots, y_8 \in O_K [bxy_0^2 \neq 0 \land bxy_0^2 \neq a \land xy_0^2 = y_1^2 + \cdots + y_4^2 \land (a - bxy_0^2) = y_5^2 + \cdots + y_8^2].$$

Note that, in general, algebraic integers might be written as the sum of squares of algebraic nonintegers, so $y_0$ plays the role of a common denominator.

### 4.2 Undecidability for totally imaginary $O_L$

We are now ready to deploy a modified version of the JR-method for totally imaginary fields; compare with [19, 30].

**Theorem 4.4.** Let $K_0$ be a totally real field for which $JR(O_{K_0})$ is either an attained minimum or $\infty$, and let $K_1$ be the maximal totally real subfield of $K_0^{(2)}$. If $K \supseteq K_1$ is any totally real field with $JR(O_K) = JR(O_{K_0})$, and $L$ is any totally imaginary quadratic extension of $K$, then the first order theory of $O_L$ is undecidable.

**Proof.** By Theorem 3.3, there is an existentially definable subset $X \subseteq O_L$ satisfying

$$O_{K_0} \subseteq X \subseteq O_K.$$  

Therefore, the parameterized formula $\phi_X(x; a, b)$ defined by

$$\exists y_0, \ldots, y_8 \in X [bxy_0^2 \neq 0 \land bxy_0^2 \neq a \land xy_0^2 = y_1^2 + \cdots + y_4^2 \land (a - bxy_0^2) = y_5^2 + \cdots + y_8^2]$$

defines sets that satisfy the containments

$$\left\{ x \in O_{K_0} : 0 \ll x \ll \frac{a}{b} \right\} \subseteq \{ x \in O_L : \phi_X(x; a, b) \} \subseteq \left\{ x \in O_K : 0 \ll x \ll \frac{a}{b} \right\}.$$  

The containments follow from Theorem 4.3. Because $JR(O_K) = JR(O_{K_0})$ is either infinite or an attained minimum, the sets on the left-hand and right-hand sides above are finite sets of arbitrarily large size as $\frac{a}{b}$ ranges over positive rational numbers approaching $JR(O_K)$ from the left. Therefore, by Lemma 4.1, we have proved first-order undecidability.  

There are two extremes for the JR-number of a ring of totally real algebraic integers, namely $4$ and $\infty$. For example, the fields $K_0 = \mathbb{Q}$ and $K_1 = \mathbb{Q}(\sqrt{n} : n \geq 1)$ have $JR(O_{K_0}) = JR(O_{K_1}) = \infty$. 
Applying Theorem 4.4 in this case leads to a recovery of some of the results that appeared in [19, 30]. At the other extreme, we write the following.

**Theorem 4.5.** Let $S$ be any infinite set of positive integers, let $K_0 = \mathbb{Q}(\{\zeta_n + \overline{\zeta}_n : n \in S\})$, and let $K_1$ be the maximal totally real subfield of $K_0^{(2)}$. If $K$ is any totally real extension of $K_1$ and $L$ is any totally imaginary quadratic extension of $K$, then the first order theory of $\mathcal{O}_L$ is undecidable.

**Proof.** Under the given hypotheses, $JR(\mathcal{O}_{K_0}) = 4$ is the smallest possible $JR$-number and is realized as a minimum. Indeed, we have $0 \ll \zeta_n + \overline{\zeta}_n + 2 \ll 4$ for all $n \in S$, and these are the only totally real elements of $\overline{\mathbb{Q}}$ with this property; see Kronecker [17] and also [26]. Therefore, $JR(\mathcal{O}_{K_0}) = JR(\mathcal{O}_K)$ is clear and Theorem 4.4 applies. □

In recent years, examples of totally real fields $K$ have been discovered for which $JR(\mathcal{O}_K)$ is neither 4 nor $\infty$, that is, $JR(\mathcal{O}_K)$ is nonextremal; see [3, 4, 12, 32]. A better understanding of the behavior of $JR$-numbers under field extension would be required before applying Theorem 4.4 to fields $K_0$ for which $JR(\mathcal{O}_{K_0}) \in (4, \infty)$ is nonextremal.

**ACKNOWLEDGMENTS**

The author thanks Arno Fehm for assistance with references, and Aharon Razon for sharing Remark 1.2. Additional thanks to Kirsten Eisenträger, Jochen Koenigsmann, Alexandra Shlapentokh, and Carlos Videla for their helpful comments. This work was supported by the Additional Funding Programme for Mathematical Sciences, delivered by EPSRC (EP/V521917/1) and the Heilbronn Institute for Mathematical Research.

**JOURNAL INFORMATION**

The *Bulletin of the London Mathematical Society* is wholly owned and managed by the London Mathematical Society, a not-for-profit Charity registered with the UK Charity Commission. All surplus income from its publishing programme is used to support mathematicians and mathematics research in the form of research grants, conference grants, prizes, initiatives for early career researchers and the promotion of mathematics.

**ORCID**

*Caleb Springer* © https://orcid.org/0000-0003-1514-4755

**REFERENCES**

1. L. Bary-Soroker and A. Fehm, *Open problems in the theory of ample fields*, Geometric and differential Galois theories, Sémin. Congr., vol. 27, Soc. Math. France, Paris, 2013, pp. 1–11.
2. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3–4, 235–265. Computational algebra and number theory (London, 1993).
3. M. Castillo Fernández, *On the julia robinson number of rings of totally real algebraic integers in some towers of nested square roots*, Ph.D. thesis, Universidad de Concepción, 2018. http://repositorio.udec.cl/handle/11594/3003.
4. M. Castillo Fernández, X. Vidaux, and C. R. Videla, *Julia Robinson numbers and arithmetical dynamic of quadratic polynomials*, Indiana Univ. Math. J. 69 (2020), no. 3, 873–885.
5. Z. Chatzidakis, *Amalgamation of types in pseudo-algebraically closed fields and applications*, J. Math. Log. 19 (2019), no. 2, 1950006, 28.
6. L. Darnière, Decidability and local-global principles, Hilbert’s tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 145–167.

7. J. Denef, Diophantine sets over algebraic integer rings. II, Trans. Amer. Math. Soc. 257 (1980), no. 1, 227–236.

8. P. Dittmann and A. Fehm, Nondefinability of rings of integers in most algebraic fields, Notre Dame J. Form. Log. 62 (2021), no. 3, 589–592.

9. A. Fehm and S. Petersen, On the rank of abelian varieties over ample fields, Int. J. Number Theory 6 (2010), no. 3, 579–586.

10. G. Frey and M. Jarden, Approximation theory and the rank of abelian varieties over large algebraic fields, Proc. Lond. Math. Soc. (3) 28 (1974), 112–128.

11. M. D. Fried, D. Haran, and H. Völklein, Real Hilbertianity and the field of totally real numbers, Arithmetic geometry (Tempe, AZ, 1993), Contemp. Math., vol. 174, Amer. Math. Soc., Providence, RI, 1994, pp. 1–34.

12. P. Gillibert and G. Ranieri, Julia robinson’s numbers, arxiv:1710:11382, 2017.

13. M. Jarden, Algebraic patching, Springer Monographs in Mathematics, Springer, Heidelberg, 2011.

14. M. Jarden and W. aw Narkiewicz, On sums of units, Monatsh. Math. 150 (2007), no. 4, 327–332.

15. E. Kobayashi, A remark on the Mordell–Weil rank of elliptic curves over the maximal abelian extension of the rational number field, Tokyo J. Math. 29 (2006), no. 2, 295–300.

16. J. Koenigsmann, Undecidability in number theory, Model theory in algebra, analysis and arithmetic, Lecture Notes in Mathematics, vol. 2111, Springer, Heidelberg, 2014, pp. 159–195.

17. L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, J. Reine Angew. Math. 53 (1857), 173–175.

18. A. Lozano-Robledo, Ranks of abelian varieties over infinite extensions of the rationals, Manuscripta Math. 126 (2008), no. 3, 393–407.

19. C. Martínez-Ranero, J. Utreras, and C. R. Videla, Undecidability of $\mathbb{Q}(2)$, Proc. Amer. Math. Soc. 148 (2020), no. 3, 961–964.

20. B. Mazur and K. Rubin, Diophantine stability, Amer. J. Math. 140 (2018), no. 3, 571–616. (With an appendix by Michael Larsen.)

21. B. Mazur, K. Rubin, and A. Shlapentokh, Existential definability and diophantine stability, arXiv:2208.09963, 2022.

22. S. Petersen, On a question of Frey and Jarden about the rank of abelian varieties, J. Number Theory 120 (2006), no. 2, 287–302.

23. B. Poonen, Using elliptic curves of rank one towards the undecidability of Hilbert’s tenth problem over rings of algebraic integers, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42.

24. F. Pop, Embedding problems over large fields, Ann. of Math. (2) 144 (1996), no. 1, 1–34.

25. J. Robinson, On the decision problem for algebraic rings, Studies in mathematical analysis and related topics, Stanford Univ. Press, Stanford, CA, 1962, pp. 297–304.

26. R. M. Robinson, Intervals containing infinitely many sets of conjugate algebraic units, Ann. of Math. (2) 80 (1964), 411–428.

27. A. 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.

28. A. 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.

29. C. Siegel, Darstellung total positiver Zahlen durch Quadrate, Math. Z. 11 (1921), no. 3–4, 246–275.

30. C. Springer, Undecidability, unit groups, and some totally imaginary infinite extensions of $\mathbb{Q}$, Proc. Amer. Math. Soc. 148 (2020), no. 11, 4705–4715.

31. L. Van Den Dries, Elimination theory for the ring of algebraic integers, J. fur die Reine und Angewandte Mathematik 1988 (1988), no. 388, 189–205.

32. X. Vidaux and C. 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.

33. X. Vidaux and C. R. Videla, A note on the Northcott property and undecidability, Bull. Lond. Math. Soc. 48 (2015), no. 1, 58–62.
34. C. R. Videla, *Definability of the ring of integers in pro-p galois extensions of number fields*, Israel J. Math. **118** (2000), no. 1, 1–14.

35. C. R. Videla, *The undecidability of cyclotomic towers*, Proc. Amer. Math. Soc. **128** (2000), no. 12, 3671–3674.

36. L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., vol. 83, Springer, New York, 1997.