UNDECIDABILITY OF FAMILIES OF RINGS OF TOTALLY REAL INTEGERS[*]

by

Moshe Jarden[**]

School of Mathematics, Tel Aviv University
Ramat Aviv, Tel Aviv 69978, Israel
e-mail: jarden@post.tau.ac.il

and

Carlos R. Videla

Department of Mathematics, Mount Royal College
Calgary, AB, T3E-6K6, Canada
e-mail: cvidela@mtroyal.ca

Abstract

Let $\mathbb{Z}_{\rm tr}$ be the ring of totally real integers, $\mathrm{Gal}(\mathbb{Q})$ the absolute Galois group of $\mathbb{Q}$, and e a positive integer. For each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\mathbb{Q})^e$ let $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ be the fixed ring in $\mathbb{Z}_{\rm tr}$ of $\sigma_1, \ldots, \sigma_e$. Then the theory of all first order sentences θ that are true in $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ (in the sense of the Haar measure) is undecidable.

Key words: Totally real integers, Absolute Galois group, Haar measure, Undecidability

MR Classification: 12E30
3 July, 2007

[*] Research initiated in a working team during a conference on Hilbert's Ten's Problem, in the American Institute for Mathematics, Palo Alto, California, March 2005. The research team included, in addition to the authors, also Charles Poo and Aharon Razon.

[**] Research suppoerted by the Minkowski Center for Geometry at Tel Aviv University, established by the Minerva Foundation.

Introduction

Julia Robinson proves in [Rob] that the semiring $N = \{0, 1, 2, \ldots\}$ is definable in the ring $\mathbb{Z}_{\rm tr}$ of all totally real algebraic integers. This implies that the first order theory of $\mathbb{Z}_{\rm tr}$ is undecidable. Her proof is based on four principles:

(1a) The map $z \mapsto 2 + z + z^{-1}$ maps the set of all roots of unity onto the set of all totally real integers in the interval $[0, 4]$ (Kronecker).

(1b) The set of totally real integers in the interval $[0, 4 - \frac{1}{n}]$ is finite and becomes arbitrarily large as $n \to \infty$.

(1c) Each totally positive integer x is the sum of four squares in $\mathbb{Q}(x)$ (Siegel).

(1d) Uniqueness in a division with a remainder: If a, b, m are totally real algebraic integers, $a, b, m - 1 - a, m - 1 - b$ are totally positive integers, and $a \equiv b \mod m$, then $a = b$ (Lemma 3.2).

These principles are fairly general to allow interpretation of arithmetic in the first order theory of some families of rings of totally real integers. Specifically, we consider the absolute Galois group $\mathrm{Gal}(\mathbb{Q})$ of $\mathbb{Q}$ and equip it with its unique normalized Haar measure $\mu_{\mathbb{Q}}$. Let $\tilde{\mathbb{Q}}$ be the field of all algebraic numbers and $\mathbb{Q}_{\rm tr}$ the field of totally real algebraic numbers. For each positive integer e and each $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_e) \in \mathrm{Gal}(\mathbb{Q})^e$, let $\tilde{\mathbb{Q}}(\boldsymbol{\sigma}) = \{x \in \tilde{\mathbb{Q}} \mid \sigma_1 x = \cdots \sigma_e x = x\}$, $\mathbb{Q}_{\rm tr}(\boldsymbol{\sigma}) = \mathbb{Q}_{\rm tr} \cap \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$, and $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) = \mathbb{Z}_{\rm tr} \cap \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. The presence of roots of unity in the fields $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ depends on whether $e = 1$ or $e \geq 2$. If $e = 1$, then for almost all $\sigma \in \mathrm{Gal}(\mathbb{Q})$, the field $\mathbb{Q}(\sigma)$ contains infinitely many roots of unity, while if $e \geq 2$, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$, the field $\mathbb{Q}(\boldsymbol{\sigma})$ contains only finitely many roots of unity [FrJ, Thm. 18.11.7]. Nevertheless, in the latter case, the number of roots of unity in the fields $\mathbb{Q}(\boldsymbol{\sigma})$ is unbounded.

Now let $\mathcal{L}(\mathrm{ring})$ be the first order language of the theory of rings. For each $e \geq 1$ let $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$ be the set of all sentences in $\mathcal{L}(\mathrm{ring})$ which hold in $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$. Using the principles (1a)–(1d) we prove:

THEOREM A: *Arithmetic is interpretable in* $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q}))$, *hence that theory is undecidable.*

While the interpretability of arithmetic in $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$ for $e \geq 2$ has yet to be settled, we prove the undecidability of $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$ using the theory of finite graphs which is also known to be undecidable [FrJ, Cor. 28.5.3]:

THEOREM B: *For each* $e \geq 2$ *the theory of finite graphs in interpretable in* $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$ *which is therefore undecidable.*

The proof of Theorem B follows the pattern of the proof of the undecidability of the theory of PAC fields [FrJ, Chapter 28]. The main point of that proof is the definition of each subset of a given finite subset of a PAC field F. The defining property of PAC fields to have rational points of each absolutely irreducible variety defined over F plays an essential role in the definition [FrJ, Proof of Lemma 29.2.1]. Unfortunately, the rings $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ do not have that property. However, we manage to solve a special kind of system of equations (equations (1) of Section 4) in almost all $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ which serve the same goal as for PAC fields. The equations involve an absolutely positive unit of $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ which is not a square in $\mathbb{Q}_{\rm tr}(\boldsymbol{\sigma})$. A theorem of Hasse supplies an absolutely positive unit ε in $\mathbb{Q}(\sqrt{p})$ for each $p \equiv 3 \mod 4$. The condition that ε is not a square in $\mathbb{Q}_{\rm tr}(\boldsymbol{\sigma})$ forces us to consider only $\boldsymbol{\sigma} \in \Sigma = {\rm Gal}(\mathbb{Q})^e \smallsetminus {\rm Gal}(\mathbb{Q}(\sqrt{2})^e$. Thus, we first interpret the theory of finite graphs only in the theory of sentences true in almost all rings $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ with $\boldsymbol{\sigma} \in \Sigma$. Fortunately, the latter theory is interpretable in ${\rm Almost}({\rm Gal}(\mathbb{Q})^e)$, so the latter theory is undecidable.

Finally recall that the theory of all sentences of $\mathcal{L}(\text{ring})$ which hold in $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in {\rm Gal}(\mathbb{Q})^e$ is decidable [FrJ, Thm. 20.6.7 or Thm. 30.7.2]. We do not know yet if the theory of all sentences of $\mathcal{L}(\text{ring})$ which hold in $\mathbb{Q}_{\rm tr}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in {\rm Gal}(\mathbb{Q})^e$ is decidable.

1. Kronecker map

Consider the field $\mathbb{C}$ of complex numbers and the field $\mathbb{R}$ of real numbers. As usual, let $\bar{z}$ be the complex conjugate of a complex number z and $|z|$ its absolute value. Let $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ be the unit circle in $\mathbb{C}$ and $[0,r] = \{x \in \mathbb{R} \mid 0 \le x \le r\}$ the closed interval defined by a nonnegative $r \in \mathbb{R}$. We study the continuous map $f\colon \mathbb{T} \to [0,4]$ defined by

$$f(z) = 2 + z + z^{-1} \tag{1}$$

We denote the algebraic closure of a field K by $\tilde{K}$ and by ${\rm Gal}(K) = {\rm Gal}(\tilde{K}/K)$ its absolute Galois group (if ${\rm char}(K) = 0$). In particular, $\tilde{\mathbb{Q}}$ is the field of all algebraic numbers in $\mathbb{C}$ and ${\rm Gal}(\mathbb{Q})$ is the absolute Galois group of $\mathbb{Q}$.

LEMMA 1.1: *The function f satisfies the following conditions:*
(a) *f maps $\mathbb{T}$ onto $[0,4]$.*

(b) *If $z \in \mathbb{T} \smallsetminus \{\pm 1\}$ and $s = f(z)$, then $f^{-1}(s) = \{z, z^{-1}\}$ and $\mathbb{Q}(z)$ is a quadratic extension of $\mathbb{Q}(s)$. If $z = \pm 1$, then $\mathbb{Q}(z) = \mathbb{Q}(s) = \mathbb{Q}$.*

(c) *Let $z \in \mathbb{T} \cap \tilde{\mathbb{Q}}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q})$ such that $\sigma f(z) \in [0,4]$. Then $\sigma z \in \mathbb{T}$ and $f(\sigma z) = \sigma f(z)$.*

(d) *Let w be a root of unity. Then all of the conjugates of w are in $\mathbb{T}$, $f(\sigma w) = \sigma f(w)$ for each $\sigma \in \mathrm{Gal}(\mathbb{Q})$, and all of the conjugates of $f(w)$ belong to the interval $[0,4]$.*

Proof of (a): We may write $z = \cos\theta + i \sin\theta$, with θ ranges on the interval $[-\pi, \pi]$ and $i = \sqrt{-1}$. Then $z^{-1} = \bar{z} = \cos\theta - i\sin\theta$ and $f(z) = 2(1 + \cos\theta)$ ranges on the interval $[0,4]$.

Proof of (b): First note that $f(z) = f(z^{-1})$, so $\{z, z^{-1}\} \subseteq f^{-1}(s)$. By (1), both z and z^{-1} satisfy $z + z^{-1} = s - 2$ and $zz^{-1} = 1$. If $z \neq \pm 1$, then $z \in \mathbb{C} \smallsetminus \mathbb{R}$ and $z \neq z^{-1}$. Hence, z and z^{-1} are the distinct roots of the quadratic equation $X^2 - (s-2)X + 1 = 0$. This implies that $f^{-1}(s) = \{z, z^{-1}\}$.

It follows also that $\mathbb{Q}(s) \subseteq \mathbb{Q}(z, z^{-1}) = \mathbb{Q}(z)$ and that $[\mathbb{Q}(z) : \mathbb{Q}(s)] = 2$.

Proof of (c): Let $s = f(z)$. We may assume that $z \neq \pm 1$. By (a), there is a $w \in \mathbb{T}$ with $\sigma s = f(w)$. Then $w^{-1} \in \mathbb{T}$ and by the proof of (b), w, w^{-1} are the distinct roots of the equation $X^2 - (\sigma s - 2)X + 1 = 0$. Also, $\sigma z, \sigma z^{-1}$ are the distinct roots of the that equation. Hence, by (b), $\{\sigma z, \sigma z^{-1}\} = \{w, w^{-1}\} = f^{-1}(\sigma s)$. Consequently, $\sigma z \in \mathbb{T}$ and $f(\sigma z) = \sigma s = \sigma f(z)$.

Proof of (d): Each root of unity has the form $e^{2\pi i \frac{k}{n}}$, where e is the basis of the natural logarithms and $k \in \mathbb{Z}$. Thus $|w| = 1$, so $w \in \mathbb{T}$. Each conjugate of w is again a root of unity, hence belongs to $\mathbb{T}$. Therefore $\sigma f(w) = 2 + \sigma w + \sigma w^{-1} = f(\sigma w)$. Consequently, all of the conjugates of $f(w)$ are in $[0,4]$. ∎

LEMMA 1.2 ([Kro, I.]): *Suppose all of the conjugates of an algebraic integer z are in $\mathbb{T}$. Then z is a root of unity.*

Each $z \in T$ can be uniquely be presented as $z = e^{i\zeta}$ with $\zeta \in \mathbb{R}$ and $-\pi < \zeta \leq \pi$. Then, $\zeta = \arg(z)$. For each positive real number θ let $\mathbb{T}_\theta = \{z \in \mathbb{T} \mid |\arg(z)| < \theta\}$. Let $\tilde{\mathbb{Z}}$ be the set of all algebraic integers. For $a, b \in \mathbb{R}$ with $a < b$ we denote the set of all $s \in \tilde{\mathbb{Z}} \cap \mathbb{R}$ such that all of the conjugates of s lie in $[a,b]$ by $\mathbb{P}[a,b]$. Let $\mathbb{W}$ be the set of all roots of unity in $\tilde{\mathbb{Q}}$.

LEMMA 1.3: *The function f maps $\mathbb{W}$ onto $\mathbb{P}[0,4]$.*

Proof: By Lemma 1.1(d), $f(\mathbb{W}) \subseteq \mathbb{P}[0,4]$. Conversely, for each $s \in \mathbb{P}[0,4]$, Lemma 1.1(a) gives $w \in \mathbb{T}$ with $f(w) = s$. For each $\sigma \in \mathrm{Gal}(\mathbb{Q})$ we have $\sigma f(w) = \sigma s \in [0,4]$. By Lemma 1.1(c), $\sigma w \in \mathbb{T}$. It follows from Lemma 1.2 that $w \in \mathbb{W}$. ∎

We denote the ring of integers of an algebraic extensions M of $\mathbb{Q}$ by O_M.

LEMMA 1.4: *Let M be an algebraic extension of $\mathbb{Q}$ and denote the compositum of all quadratic extensions of M by $M^{(2)}$.*

(a) *For each $\theta > 0$ there are only finitely many $w \in \mathbb{W}$ such that all of the conjugates of w belong to $\mathbb{T} \smallsetminus \mathbb{T}_\theta$.*

(b) *For each $\varepsilon > 0$ the set $\mathbb{P}[0, 4-\varepsilon]$ is finite.*

(c) *Let M be an algebraic extension of $\mathbb{Q}$ such that $M \cap \mathbb{W}$ is infinite. Then, for each $c > 0$ there exists a positive integer n such that $|O_M \cap \mathbb{P}[0, 4-\frac{1}{n}]| > c$.*

(d) *If $M^{(2)} \cap \mathbb{W}$ is finite, then so is $M \cap \mathbb{P}[0,4]$.*

Proof of (a): Choose a positive integer n with $\frac{2\pi}{n} < \theta$. Then $e^{\frac{2\pi i}{n}} \in \mathbb{T}_\theta$, so there is no root of unity of order n all of whose conjugates belong to $\mathbb{T} \smallsetminus \mathbb{T}_\theta$. Since only finitely many n's satisfy $\frac{2\pi}{n} \geq \theta$ and for each n there are only finitely many roots of unity of order n, there are only finitely many $w \in \mathbb{W}$ all of whose conjugates belong to $\mathbb{T} \smallsetminus \mathbb{T}_\theta$.

Proof of (b): Since $f(1) = 4$ and f is continuous, there is $\theta > 0$ with $f(\mathbb{T}_\theta) \subseteq (4-\varepsilon, 4]$. Let W be the set of all $w \in \mathbb{W}$ all of their conjugates belong to $\mathbb{T} \smallsetminus \mathbb{T}_\theta$. Consider $s \in \mathbb{P}[0, 4-\varepsilon]$ and $w \in \mathbb{T}$ with $f(w) = s$. For each $\sigma \in \mathrm{Gal}(\mathbb{Q})$ we have, by Lemma 1.1, that $\sigma w \in \mathbb{T}$ and $f(\sigma w) = \sigma s \in [0, 4-\varepsilon]$, so $\sigma w \in \mathbb{T} \smallsetminus \mathbb{T}_\theta$. By Lemma 1.2, $w \in \mathbb{W}$. Thus, $f^{-1}(\mathbb{P}[0, 4-\varepsilon]) \subseteq W$. By (a), W is finite, hence $\mathbb{P}[0, 4-\varepsilon]$ is finite.

Proof of (c): If $w \in M \cap \mathbb{W}$, then $\mathbb{Q}(w)/\mathbb{Q}$ is an Abelian extension and $\mathbb{Q}(f(w)) \subseteq \mathbb{Q}(w)$ (Lemma 1.1(b)). Hence, all of the conjugates of $f(w)$ belongs to $\mathbb{Q}(f(w))$ and therefore to $M \cap [0,4]$. Moreover, since both w and w^{-1} are algebraic integers, $f(w) \in M \cap \mathbb{P}[0,4]$. Since each fiber of f contains at most two elements (Lemma 1.1(b)), $O_M \cap \mathbb{P}[0,4]$ is infinite.

By (b), $M \cap \mathbb{P}[0, 4-\frac{1}{n}]$ is finite. Since $|M \cap \mathbb{P}[0, 4-\frac{1}{n}]|$ increases with n, there exists n such that $|M \cap \mathbb{P}[0, 4-\frac{1}{n}]| > c$.

Proof of (d): For each $s \in M \cap \mathbb{P}[0,4]$ lemma 1.3 gives $w \in \mathbb{W}$ with $f(w) = s$. By Lemma 1.1(b), $[M(w) : M] \leq 2$, so $w \in M^{(2)}$. Thus, $M \cap \mathbb{P}[0,4] \subseteq f(M^{(2)} \cap W)$, so $M \cap \mathbb{P}[0,4]$ is finite. ∎

An algebraic number $x \in \tilde{\mathbb{Q}}$ is said to be **totally real** if all of the conjugates of x belong to $\mathbb{R}$. We denote the field of all totally real algebraic numbers by $\mathbb{Q}_{\mathrm{tr}}$. An element $x \in \mathbb{Q}_{\mathrm{tr}}$ is said to be **totally positive** if each conjugate of x is positive. By a theorem of Siegel, x is totally positive if and only if x is a sum of four squares in $\mathbb{Q}(x)$ [Sie]. This result follows also from the Hasse-Minkowski local-global principle for quadratic forms and the fact that each quadratic form with at least 5 variables over a finite extension of $\mathbb{Q}_p$ represents 0 [CaF, p. 359, Ex. 4.9].

We abbreviate $O_{\mathbb{Q}_{\mathrm{tr}}}$ by $\mathbb{Z}_{\mathrm{tr}}$. Given $a, b \in \mathbb{Q}_{\mathrm{tr}}$, we write $a \ll b$ if $b - a$ is totally positive. By Siegel, this is a definable relation. Indeed, denote the elementary language of rings by $\mathcal{L}(\mathrm{ring})$ and let K be a subfield of $\mathbb{Q}_{\mathrm{tr}}$ containing a, b. Then $a \ll b$ if and only if

$$O_K \models (\exists x_0)(\exists x_1)(\exists x_2)(\exists x_3)(\exists x_4)[x_0 \neq 0 \wedge x_0^2(b-a) = x_1^2 + x_2^2 + x_3^2 + x_4^2].$$

In particular, the sets $\mathbb{P}[a, b]$ are definable in each subring of $\mathbb{Z}_{\mathrm{tr}}$.

2. Coding in Rings with Monadic Quantifiers

This section adjusts material on monadic theories of PAC fields developed in [ChJ] and represented in [FrJ, Chapter 29] to rings of totally real numbers.

Every first order language $\mathcal{L}$ naturally extends to a language $\mathcal{L}_n$, the **language of n-adic quantifiers**. It is the simplest extension of $\mathcal{L}$ which allows for each $m \leq n$ quantification over certain m-ary relations on the underlying sets of structures of $\mathcal{L}$. To obtain $\mathcal{L}_n$ from $\mathcal{L}$ adjoin for each $m \leq n$ a sequence of **m-ary variable symbols** $X_{m1}, X_{m2}, X_{m3}, \ldots$. The variable symbols of $\mathcal{L}$ are taken here as $x_1, x_2, x_3, \ldots$. An **atomic formula** of $\mathcal{L}_n$ is either an atomic formula of $\mathcal{L}$ or a formula $(x_{i_1}, \ldots, x_{i_m}) \in X_{mj}$, where $m \leq n$ and $i_1, \ldots, i_m, j$ are positive integers. As usual we close the set of formulas of $\mathcal{L}_n$ under negation, disjunction, conjunction, and quantification on variables. A **structure** for $\mathcal{L}_n$ (or an **n-adic structure** for $\mathcal{L}$) is a system $\langle A, \mathcal{Q}_1, \ldots, \mathcal{Q}_n \rangle$, where A is a structure for $\mathcal{L}$ and, for each $m \leq n$, $\mathcal{Q}_m$ is a nonempty collection of m-ary relations on the underlying set of A (which we also denote by A). The structure is **weak** if for each m, all relations in $\mathcal{Q}_m$ are finite. We interpret the variables x_i as elements of A and the variables X_{mj} as elements of $\mathcal{Q}_j$. Thus, "$(x_1, \ldots, x_m) \in X_{mj}$" means "$(x_1, \ldots, x_m)$ belongs to X_{mj}", "$\exists x_i$" means "there exists an element x_i in A", and "$\exists X_{mj}$" means "there exists an element X_{mj} in $\mathcal{Q}_m$".

Theories of $\mathcal{L}_n$, also called **n-adic theories**, are often undecidable. Thus, whenever we “interpret” such a theory in another theory the latter also turns out to be undecidable.

We are mainly interested in the case where $\mathcal{L} = \mathcal{L}(\mathrm{ring})$. For an integer $q \geq 2$ and for an integral domain R with quotient field F we say that **hypothesis $G(q)$ holds in R** if the following condition holds:

(1) There exists $c \in R \smallsetminus F^q$ such that for all distinct $a_1, \ldots, a_m, b_1, \ldots, b_n \in R$ there exist $x, y_1, \ldots, y_m, z_1, \ldots, z_n \in R$ such that

$$\begin{aligned} a_i + x &= y_i^q, \qquad i = 1, \ldots, m \\ b_j + x &= cz_j^q, \qquad j = 1, \ldots, n. \end{aligned}$$

Note that this condition forces c to be a unit of R. Indeed, take no a_i's, let $b_1 = 0$ and $b_2 = 1$. Then there exist $x, z_1, z_2 \in R$ with $x = cz_1^q$ and $1 + x = cz_2^q$. Hence, $1 = c(z_2^q - z_1^q)$, so $c \in R^\times$.

We say that a class $\mathcal{R}$ of n-adic structures over integral domains satisfy **Hypothesis $G(q)$** if for each structure $\langle R, \mathcal{Q}_1, \ldots, \mathcal{Q}_n \rangle$ in $\mathcal{R}$, R is an integral domain that satisfies Hypothesis $G(q)$.

For the rest of this section we fix a class $\mathcal{R}$ of weak monadic structures (i.e. weak 1-adic structures) over integral domains. To each $\langle R, \mathcal{Q} \rangle$ in $\mathcal{R}$ we associate another monadic structure $\langle R, \mathcal{Q}' \rangle$ where $\mathcal{Q}'$ is the collection of all subsets

$$D(A, x) = \{a \in A \mid (\exists y \in R)[y \neq 0 \wedge a + x = y^q]\}$$

of R with $A \in \mathcal{Q}$ and $x \in R$. Let $\mathcal{R}'$ be the class of all $\langle R, \mathcal{Q}' \rangle$ with $\langle R, \mathcal{Q} \rangle \in \mathcal{R}$.

Note that our framework slightly generalize that of [FrJ, Sec. 29.2], where we considered a class $\mathcal{F}$ of n-adic structures over fields. The proofs of the results about $\mathcal{R}$ are verbatim repetitions of those for $\mathcal{F}$, so we cite the former from [FrJ], replacing $\mathcal{F}$ by $\mathcal{R}$.

LEMMA 2.1 ([FrJ, Lemma 29.2.1, Case A]): *Suppose $\mathcal{R}$ satisfies Hypothesis $G(q)$.*

(a) *For each structure $\langle R, \mathcal{Q} \rangle$ in $\mathcal{R}$ the collection $\mathcal{Q}'$ consists of all subsets of the sets $A \in \mathcal{Q}$.*

(b) *The monadic theory* $\mathrm{Th}(\mathcal{R}')$ *is interpretable in* $\mathrm{Th}(\mathcal{R})$.

Our next construction allows us to replace monadic structures by certain n-adic structures. For each structure $\langle R, \mathcal{Q} \rangle \in \mathcal{R}$ and every $m \leq n$ let $\mathcal{Q}_m$ be the collection of all subsets of $A_1 \times \cdots \times A_m$, where $A_1, \ldots, A_m \in \mathcal{Q}$. Denote the class of n-adic structures $\langle R, \mathcal{Q}_1, \ldots, \mathcal{Q}_n \rangle$ obtained in this way by $\mathcal{R}_n$.

LEMMA 2.2 ([FrJ, Lemma 29.2.2, Parts A and B]): *Suppose for each structure $\langle R, \mathcal{Q} \rangle$ in $\mathcal{R}$ the integral domain R is infinite. Then* $\mathrm{Th}(\mathcal{R}_n)$ *is interpretable in* $\mathrm{Th}(\mathcal{R}')$.

A **graph** in this work is a structure $\langle A, E \rangle$ where A is a set and E is a binary symmetric nonreflexive relation on A. Denote the language of graphs without equality by $\mathcal{L}(\mathrm{graph})$.

LEMMA 2.3 ([FrJ, Prop. 29.2.3]): *Let $\mathcal{R}$ be a class of weak monadic structures over integral domains. Suppose*

(4) *for each positive integer n there exists $\langle R, \mathcal{Q} \rangle \in \mathcal{R}$ and an $A \in \mathcal{Q}$ of cardinality at least n.*

Then the theory of finite graphs is interpretable in $\mathrm{Th}(\mathcal{R}_2)$.

PROPOSITION 2.4: *Let $\mathcal{R}$ be a class of weak monadic structures over integral domains. Suppose:*

(5a) *$\mathcal{R}$ satisfy Hypothesis $G(q)$ for some positive integer q.*

(5b) *For each $\langle R, \mathcal{Q} \rangle \in \mathcal{R}$ the integral domain R is infinite.*

(5c) *For each positive integer n there exist $\langle R, \mathcal{Q} \rangle \in \mathcal{R}$ and $A \in \mathcal{Q}$ of cardinality at least n.*

Then the theory of finite graphs is interpretable in $\mathrm{Th}(\mathcal{R})$.

Proof: By Lemma 2.3 and Condition (5c), the theory of finite graphs is interpretable in $\mathrm{Th}(\mathcal{R}_2)$. By Lemma 2.2 and Condition (5b), $\mathrm{Th}(\mathcal{R}_2)$ is interpretable in $\mathrm{Th}(\mathcal{R}')$. By Lemma 2.1 and Condition (5a), $\mathrm{Th}(\mathcal{R}')$ is interpretable in $\mathrm{Th}(\mathcal{R})$. Consequently, the theory of finite graphs is interpretable in $\mathrm{Th}(\mathcal{R})$. ∎

3. Interpretation of Arithmetic

For each $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ let $\tilde{\mathbb{Q}}(\boldsymbol{\sigma}) = \{x \in \tilde{\mathbb{Q}} \mid \sigma_i x = x \text{ for } i = 1, \ldots, e\}$,

$$\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}) = \{x \in \mathbb{Q}_{\mathrm{tr}} \mid \sigma_i x = x \text{ for } i = 1, \ldots, e\} \text{ and } \mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}) = \mathbb{Z}_{\mathrm{tr}} \cap \mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}) = O_{\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma})}.$$

In this section we consider the case $e = 1$ and prove that the theory of all sentences of $\mathcal{L}(\mathrm{ring})$ which hold in $\mathbb{Z}_{\mathrm{tr}}(\sigma)$ for almost all $\sigma \in \mathrm{Gal}(\mathbb{Q})$ is undecidable. As usual, we use the expression "for almost all" in the sense of the Haar measure μ_Q of $\mathrm{Gal}(\mathbb{Q})$. Our proof follows ideas of Julia Robinson [Rob]. It that article Robinson proves that if a subring R of $\mathbb{Z}_{\rm tr}$ contains infinitely many absolutely positive algebraic integers between 0 and 4, then arithmetic can be interpreted in $\mathrm{Th}(R)$, thus proving that $\mathrm{Th}(R)$ is undecidable. The proof of our result relies on the observation that Robinson's interpretation of arithmetic is actually independent of R.

Lemma 3.1 ([Rob, Lemma 1]): *Let A be a finite set of non-zero algebraic integers and t, g_0 positive integers. Then there exists a positive integer $g > g_0$ such that*
(a) *t and all numbers $1 + ag$ with $a \in A$ are relatively prime in pairs and*
(b) *the numbers $1 + ag$ are neither units nor zero.*

As usual we write $x \equiv y \mod m$ for elements x, y, m of a ring R if $(\exists a)[x-y = am]$ holds in R. The following result is a uniqueness statement for division with a remainder in rings of totally real algebraic integers.

Lemma 3.2 ([Rob, Lemma 3]): *Given two totally real algebraic integers m and t, there is at most one totally real integer a such that $a \equiv t \mod m$ and $0 \ll a \ll m - 1$.*

Let R be the ring of integers of a subfield of $\mathbb{Q}_{\rm tr}$ and let $m, t, g \in R$. Let $\beta(m, t, g, x)$ be the following formula of $\mathcal{L}(\mathrm{ring})$:

$$(\exists b)[0 \ll bm \ll 4m - 1 \wedge 0 \ll x \ll bg \wedge t \equiv x \mod 1 + bg].$$

Using β we define a formula $\gamma(x)$ of $\mathcal{L}(\mathrm{ring})$:

$$(\exists m)(\exists t)(\exists g)\big[\beta(m, t, g, x) \wedge (\forall y)[\beta(m, t, g, y) \rightarrow y = 0 \vee \beta(m, t, g, y - 1)]\big].$$

Let

$$B_m(R) = R \cap \mathbb{P}\Big[0, 4 - \frac{1}{m}\Big] = \{b \in R \mid 0 \ll bm \ll 4m - 1\}.$$

By Lemma 1.4(b), $B_m(R)$ is a finite set.

Let N be the set of nonnegative integers. We view N as a sub-semi-ring of R.

Lemma 3.3 (An extract from [Rob, Thm. 2]): *Let R be the ring of integers of a subfield of $\mathbb{Q}_{\rm tr}$, let $m \in R$, and let $n \in N$. Suppose the set $B_m(R)$ has more than n elements. Then there exist $t, g \in R$ such that $R \models \beta(m, t, g, a)$ if and only if $a \in \{0, 1, \ldots, n\}$.*

Proof: Use Lemma 3.1 to choose a positive integer g such that the numbers $1 + bg$ with $b \in B_m(R)$ are relatively prime in pairs and they are nonunits nonzero elements of R. Moreover, since all $b \in B_m(R)$ are totally nonnegative, g can be chosen to be so large such that $n \ll bg$ for all $b \in B_m(R)$, $b \neq 0$.

Now choose distinct nonzero elements $b_1, \ldots, b_n$ of $B_m(R)$. By the Chinese remainder theorem, there exists $t \in R$ such that

$$\begin{aligned} t &\equiv j \mod 1 + b_j g \quad \text{for } j = 1, \ldots, n, \\ t &\equiv 0 \mod 1 + bg \quad \text{for all other } b \in B_m(R) \end{aligned}$$

For this choice of m, t, g, the statement $\beta(m, t, g, a)$ holds in R for $a = 0, 1, \ldots, n$. By Lemma 3.2, these are the only values of a such that $\beta(m, t, g, a)$ holds. ∎

Let $\mathcal{B}(R) = \{B_m(R) \mid m \in R,\ 1 \ll m\}$.

Lemma 3.4: *Let R be the ring of integers of a subfield of $\mathbb{Q}_{\mathrm{tr}}$ and let $n \in R$. Suppose $\mathcal{B}(R)$ contains sets of arbitrarily large finite cardinalities. Then $n \in N$ if and only if $R \models \gamma(n)$.*

Proof: Suppose $R \models \gamma(n)$. Then there exist $m, t, g \in R$ such that

$$R \models \beta(m, t, g, n) \wedge (\forall y)[\beta(m, t, g, y) \rightarrow y = 0 \vee \beta(m, t, g, y - 1)].$$

If $n \notin N$, then $R \models \beta(m, t, g, n - k)$, so $k \ll n$ for each $k \in N$. Since $n \in \mathbb{R}$, this is a contradiction. Consequently, $n \in N$.

Conversely, consider $n \in N$. Choose $m \in R$ such that $|B_m(R)| \geq n$. By Lemma 3.3, there exist $t, g \in R$ such that $\{a \in R \mid R \models \beta(m, t, g, a)\} = \{0, 1, \ldots, n\}$. Hence,

$$R \models (\forall y)[\beta(m, t, g, y) \rightarrow y = 0 \vee \beta(m, t, g, y - 1)].$$

Consequently, $R \models \gamma(n)$, as claimed. ∎

We set $\mathcal{N} = \langle N, +, \cdot, 0, 1 \rangle$ and refer to $\mathrm{Th}(N)$ as **arithmetic**. By Gödel, Church, and Rosser, arithmetic is undecidable [ELT, Thm. 3.2.4]. Thus, if arithmetic is interpretable in a theory T, then T is undecidable.

Corollary 3.5 (Main theorem of [Rob]): *Let M be a subfield of $\mathbb{Q}_{\mathrm{tr}}$. Suppose $O_M \cap \mathbb{P}[0, 4]$ is infinite. Then $\mathrm{Th}(O_M)$ is undecidable. In particular, $\mathrm{Th}(\mathbb{Z}_{\mathrm{tr}})$ is undecidable.*

Proof: By Lemma 1.4(b), the subsets $B_m(O_M)$ have an arbitrarily large cardinality. Hence, by Lemma 3.4, N is definable in O_M and arithmetic is interpretable in $\mathrm{Th}(O_M)$. Therefore, $\mathrm{Th}(O_M)$ is undecidable. ∎

Denote the set of all sentences of $\mathcal{L}(\text{ring})$ which hold in $\mathbb{Z}_{\text{tr}}(\sigma)$ for almost all $\sigma \in \text{Gal}(\mathbb{Q})$ by $\text{Almost}(\text{Gal}(\mathbb{Q}))$. The undecidability of $\text{Almost}(\text{Gal}(\mathbb{Q}))$ we are now going to prove depends on the following result:

PROPOSITION 3.6: *The following statements hold for almost all $\boldsymbol{\sigma} \in \text{Gal}(\mathbb{Q})^e$:*

(a) *If $e = 1$, then the set $\tilde{\mathbb{Q}}(\boldsymbol{\sigma}) \cap \mathbb{W}$ is infinite. If $e \geq 2$, then $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})^{(2)} \cap \mathbb{W}$ is finite.*

(b) *If $e = 1$, then each of the sets $B_m(\mathbb{Z}_{\text{tr}}(\boldsymbol{\sigma}))$ is finite and becomes arbitrarily large as m tends to infinity.*

(c) *If $e \geq 2$, then $\mathbb{Z}_{\text{tr}}(\boldsymbol{\sigma}) \cap \mathbb{P}[0,4]$ is finite.*

Proof: The first statement (a) can be found in [FrJ, Thm. 18.1.7]. For the second one note that for almost all $\boldsymbol{\sigma} \in \text{Gal}(\mathbb{Q})^e$ we have $\lim_{n\to\infty}[\tilde{\mathbb{Q}}(\boldsymbol{\sigma})(\zeta_n) : \tilde{\mathbb{Q}}(\boldsymbol{\sigma})] = \infty$ [Jar, Lemma 5.3]. Since $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ has only finitely many quadratic extensions, $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})^{(2)}$ is a finite extension of $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})$. Therefore, $\tilde{\mathbb{Q}}(\boldsymbol{\sigma})^{(2)}$ contains only finitely many roots of unity.

Statement (b) follows from (a) by Lemma 1.4 (c). Statement (c) follows from (a) by Lemma 1.4(d). ∎

LEMMA 3.7: *Arithmetic is interpretable in* $\text{Almost}(\text{Gal}(\mathbb{Q}))$.

Proof: To each formula $\varphi(x_1,\ldots,x_n)$ of $\mathcal{L}(\text{ring})$ we recursively associate a formula $\varphi^*(x_1,\ldots,x_n)$ of $\mathcal{L}(\text{ring})$. The map $\varphi \mapsto \varphi^*$ is defined by induction on the structure of φ. If $\varphi(x_1,\ldots,x_n)$ is an atomic formula of $\mathcal{L}(\text{ring})$, then $\varphi^*(x_1,\ldots,x_n)$ is the formula $\bigwedge_{i=1}^n \gamma(x_i) \wedge \varphi(x_1,\ldots,x_n)$. Next we let the star operation commute with negation and disjunction. Finally, if $\varphi^*(x_1,\ldots,x_n,y)$ has been defined for a formula $\varphi(x_1,\ldots,x_n,y)$, then $(\exists y)[\gamma(y) \wedge \varphi^*(x_1,\ldots,x_n,y)]$ is the formula we associate with $(\exists y)\varphi(x_1,\ldots,x_n,y)$.

By Proposition 3.6(c), for almost all $\sigma \in \text{Gal}(\mathbb{Q})$ the family $\mathcal{B}(\mathbb{Z}_{\text{tr}}(\sigma))$ consists of arbitrarily large finite sets. Induction on the structure of formulas in $\mathcal{L}(\text{ring})$ and Lemma 3.4 imply that each formula $\varphi(x_1,\ldots,x_n)$ of $\mathcal{L}(\text{ring})$, for almost all $\sigma \in \text{Gal}(\mathbb{Q})$, and all $a_1,\ldots,a_n \in \mathbb{Z}_{\text{tr}}(\sigma)$

$$a_1,\ldots,a_n \in N \mathbin{\&} \mathcal{N} \models \varphi(a_1,\ldots,a_n) \Longleftrightarrow \mathbb{Z}_{\text{tr}}(\sigma) \models \varphi^*(a_1,\ldots,a_n).$$

In particular, a sentence θ of $\mathcal{L}(\text{ring})$ holds in $\mathcal{N}$ if and only if $\mathbb{Z}_{\text{tr}}(\sigma) \models \theta^*$ for almost all $\sigma \in \text{Gal}(\mathbb{Q})$. Consequently, the map $\theta \mapsto \theta^*$ is an interpretation of arithmetic in $\text{Almost}(\text{Gal}(\mathbb{Q}))$. ∎

THEOREM 3.8: *The theory of all sentences in* $\mathcal{L}(\text{ring})$ *which hold in* $\mathbb{Z}_{\text{tr}}(\sigma)$ *for almost all* $\sigma \in \text{Gal}(\mathbb{Q})$ *is undecidable.*

Remark 3.9: The combination of Corollary 3.5 and Proposition 3.6 shows that for almost all $\sigma \in \mathrm{Gal}(\mathbb{Q})$ the theory of $\mathbb{Z}_{\mathrm{tr}}(\sigma)$ is undecidable. As much as this result sounds attractive, it follows from a quite general principle which has nothing to do with the fine analysis that led to the proof of Corollary 3.5. Indeed, that principle applies to arbitrary $e \geq 1$.

To this end choose for each set A of prime numbers an e-tuple $\boldsymbol{\sigma} = \boldsymbol{\sigma}_A \in \mathrm{Gal}(\mathbb{Q})^e$ such that $\sigma_i(\sqrt{p}) = \sqrt{p}$, $i = 1, \ldots, e$, for each $p \in A$ and $\sigma_1(\sqrt{p}) = -\sqrt{p}$ for each $p \notin A$. If $A \neq A'$, then $\mathbb{Z}_{\mathrm{tr}}(\sigma_A)$ is not elementarily equivalent to $\mathbb{Z}_{\mathrm{tr}}(\sigma_{A'})$. Thus, there are $2^{\aleph_0}$ unequivalent classes of rings of the form $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})$. On the other hand, each decision procedure for a ring is determined by finitely many instructions taken from a countable vocabulary. Thus, there are only countably many decision procedures (Equivalently, there are only countably many recursive subsets of N.) If two rings with decidable theories have the same decision procedure, then they are elementarily equivalent.

If $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}) \equiv \mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}')$ for $\boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \mathrm{Gal}(\mathbb{Q})^e$, then $\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}) \equiv \mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}')$. Hence, $\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma})$ is conjugate over $\mathbb{Q}$ to $\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}')$ [FrJ, Lemma 20.6.3(b)]. Therefore, $\mathbb{Q}_{\mathrm{ab}} \cap \mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}) = \mathbb{Q}_{\mathrm{ab}} \cap \mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma}')$ (here $\mathbb{Q}_{\mathrm{ab}}$ is the maximal Abelian extension of $\mathbb{Q}$.) It follows that $\mathrm{res}(\boldsymbol{\sigma}')$ lies in the closed subgroup $\langle \mathrm{res}(\boldsymbol{\sigma}) \rangle$ of $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}} \cap \mathbb{Q}_{\mathrm{tr}}/\mathbb{Q})$ generated by $\mathrm{res}(\boldsymbol{\sigma})$, where res is the restriction map from $\mathrm{Gal}(\mathbb{Q})^e$ to $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}} \cap \mathbb{Q}_{\mathrm{tr}}/\mathbb{Q})^e$. But $\langle \mathrm{res}(\boldsymbol{\sigma}) \rangle$ has an infinite index in $\mathrm{Gal}(\mathbb{Q}_{\mathrm{ab}} \cap \mathbb{Q}_{\mathrm{tr}}/\mathbb{Q})$, so its Haar measure is zero. Consequently, for each $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ the set $\{\boldsymbol{\sigma}' \in \mathrm{Gal}(\mathbb{Q})^e \mid \mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}) \equiv \mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}')\}$ has Haar measure 0.

To sum up, $\mathrm{Th}(\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}))$ is decidable only for $\boldsymbol{\sigma}$'s that belong to at most countably many sets of measure 0. Consequently, the set of all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ such that $\mathrm{Th}(\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}))$ is decidable has Haar measure 0. ▮

Remark 3.10: Julia Numbers. The Corollary on page 301 of [Rob] says that if R is a ring of totally real algebraic integers and there exists a minimal s between 0 and ∞ such that $R \cap \mathbb{P}[0, s]$ is infinite, then the semiring $\mathbb{N}$ is definable in R. Julia Robinson adds that s may exist for R. If it does, we call it the **Julia number** of R. In that case it must be at least 4 (Lemma 1.4(b)). By Lemma 3.6, for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$, the Julia number of $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})$ is 4 if $e = 1$ and greater than 4 if $e \geq 2$ and if it exists. We conjecture that in the latter case the Julia number is ∞. In other words, $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma}) \cap \mathbb{P}[0, s]$ is finite for each positive real number s. ▮

4. Undecidability

If R is a PAC field, then Hypothesis $G(q)$ holds for R for each positive integer q. If R is a subring of $\mathbb{Z}_{\rm tr}$, this need not be the case. Nevertheless, we prove that for each positive integer and almost all $\boldsymbol{\sigma} \in {\rm Gal}(\mathbb{Q})^e \smallsetminus {\rm Gal}(\mathbb{Q}(\sqrt{2}))^e$ the ring $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ satisfies Hypothesis $G(2)$. For $e \geq 2$ this allows us to apply Proposition 2.4 to prove that the theory of finite graphs is interpretable in the theory of all sentences of $\mathcal{L}({\rm ring})$ which hold in $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in {\rm Gal}(\mathbb{Q})^e$, proving that the latter theory is undecidable.

For the rest of this section we assume $e \geq 2$ and denote the normalized Haar measure of ${\rm Gal}(\mathbb{Q})^e$ by $\mu_{\mathbb{Q}}$.

Lemma 4.1: *Let K be a finite extension of $\mathbb{Q}$ in $\mathbb{Q}_{\rm tr}$, let e be a positive integer, let $a_1, \ldots, a_m, b_1, \ldots, b_n$ be distinct elements of O_K, and let c be an absolutely positive unit of O_K. Then, for almost all $\boldsymbol{\sigma} \in {\rm Gal}(K)^e$ there are $x \in \mathbb{Z}$ and $y_1, \ldots, y_m, z_1, \ldots, z_n \in \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ such that*

$$\begin{aligned} a_i + x &= y_i^2, \qquad i = 1, \ldots, m \\ b_j + x &= cz_j^2, \qquad j = 1, \ldots, n. \end{aligned} \tag{1}$$

Proof: Denote the distinct archimedean absolute values of K by $|\ |_1, \ldots, |\ |_r$. Choose a positive integer d which is greater than $|a_i|_k, |b_j|_k$ for all i, j, k. Suppose by induction we have already constructed linearly disjoint Galois extensions $K_1, \ldots, K_s$ of K of degree 2^{m+n} in $\mathbb{Q}_{\rm tr}$ such that for each l between 1 and s there exist $x \in \mathbb{Z}$ and $y_1, \ldots, y_m, z_1, \ldots, z_n \in \mathbb{Z}_{\rm tr}$ which satisfy (1). Then $L = K_1 K_2 \cdots K_s$ is a finite Galois extension of $\mathbb{Q}$. By Duret, the system of equations

$$\begin{aligned} a_i + X &= Y_i^2, \qquad i = 1, \ldots, m \\ b_j + X &= cZ_j^2, \qquad j = 1, \ldots, n \end{aligned} \tag{2}$$

defines an absolutely irreducible variety V over K [FrJ, Lemma 29.1.2]. Let $\hat{x}$ be a transcendental element over K and choose $\hat{y}_1, \ldots, \hat{y}_m, \hat{z}_1, \ldots, \hat{z}_n \in \widetilde{K(\hat{x})}$ which satisfy (1). Then $(\hat{x}, \hat{\mathbf{y}}, \hat{\mathbf{z}})$ is a generic point of V over K. Moreover, by Kummer theory, $K(\hat{\mathbf{y}}, \hat{\mathbf{z}})$ is a Galois extension of $K(\hat{x})$ with Galois group $(\mathbb{Z}/2\mathbb{Z})^{m+n}$ (see also the proof of [FrJ, Lemma 29.1.2(a)]). By [FrJ, Lemma 13.1.1], L has a Hilbert subset H such that for each $x \in K \cap H$, there are $(\mathbf{y}, \mathbf{z}) \in \tilde{\mathbb{Q}}$ such that

(3a) $(x, \mathbf{y}, \mathbf{z})$ is a specialization of $(\hat{x}, \hat{\mathbf{y}}, \hat{\mathbf{z}})$ over L.

(3b) $K(\mathbf{y}, \mathbf{z})$ is a Galois extension of K with $(\mathbb{Z}/2\mathbb{Z})^{m+n}$ as its Galois group, (3c) and $K(\mathbf{y},\mathbf{z})$ is linearly disjoint from L over K

By [FrJ, Cor. 12.2.3], H contains a Hilbert subset H_0 of $\mathbb{Q}$. The latter set contains infinitely many positive integers ([FrJ, Lemma 13.5.3(c)] or [Lan, p. 231, Cor. 2.4]). In particular, there exists $x \in H_0$ such that $x > d$. Thus, $a_i + x$, $i = 1, \ldots, m$, and $b_j + x$, $j = 1, \ldots, n$, are absolutely positive elements of $\mathbb{Z}_{\rm tr}$. Let $(\mathbf{y},\mathbf{z}) \in \tilde{\mathbb{Q}}^{m+n}$ be elements which satisfy (3). Since $(\hat{x}, \hat{\mathbf{y}}, \hat{\mathbf{z}})$ is a zero of (2), (3a) implies that $(x,\mathbf{y},\mathbf{z})$ satisfy (1). For each i and j, $a_i + x$ and $c^{-1}(b_j + x)$ are absolutely positive elements of $\mathbb{Z}_{\rm tr}$. Therefore, $y_i, z_j \in \mathbb{Z}_{\rm tr}$. Finally set $K_{s+1} = K(\mathbf{y},\mathbf{z})$ to conclude the induction.

Now use Borel-Cantelli to find for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(K)^e$ a positive integer s such that $K_s \subseteq \tilde{\mathbb{Q}}(\boldsymbol{\sigma})$ [FrJ, Lemma 18.5.3]. The construction gives $(x,\mathbf{y},\mathbf{z}) \in K^{1+m+n}$ satisfying (1). Then $(x,\mathbf{y},\mathbf{z}) \in \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})^{1+m+n}$, as desired. ∎

For a positive number e we consider the set

$$\begin{aligned}\Sigma &= \{\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e \mid \tilde{\mathbb{Q}}(\boldsymbol{\sigma}) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}\} \\ &= \mathrm{Gal}(\mathbb{Q})^e \smallsetminus \mathrm{Gal}(\mathbb{Q}(\sqrt{2}))^e \\ &= \bigcup_{i=1}^{e} \{\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e \mid \sigma_i\sqrt{2} = -\sqrt{2}\}.\end{aligned}$$

Then $\mu_{\mathbb{Q}}(\Sigma) = 1 - \frac{1}{2^e}$. We make Σ into a probability space by defining $\mu_\Sigma(A) = \frac{\mu_{\mathbb{Q}}(A)}{\mu_{\mathbb{Q}}(\Sigma)}$ for each measurable subset A of $\mathrm{Gal}(\mathbb{Q})^e$ which is contained in Σ.

Lemma 4.2: *For almost all $\boldsymbol{\sigma} \in \Sigma$ the ring $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ has an absolutely positive unit c which is not a square in $\mathbb{Q}_{\rm tr}(\boldsymbol{\sigma})$.*

Proof: Let $p \equiv -1 \mod 4$ be a prime number. By [Has, p. 554], $O_{\mathbb{Q}(\sqrt{p})}$ has a fundamental unit $\varepsilon = \varepsilon_p$ such that $N\varepsilon = 1$. In other words, if $\bar{\epsilon}$ is the conjugate of ε over $\mathbb{Q}$, then $\varepsilon\bar{\epsilon} = 1$, i.e. $\bar{\epsilon} = \varepsilon^{-1}$. Replacing ε with $-\varepsilon$, if necessary, we may assume that $\varepsilon > 1$. Then ε is unique with these properties and ε is absolutely positive. Saying that ε is a fundamental unit means that ε is a generator of the group of units of $O_{Q(\sqrt{p})}$ (which is in our case isomorphic to $\mathbb{Z}$). In particular, $\mathbb{Q}(\varepsilon_p) = \mathbb{Q}(\sqrt{p})$ and ε is not a square of $\mathbb{Q}(\sqrt{p})$. It follows that $\delta = \delta_p = \sqrt{\varepsilon_p}$ generates a quadratic extension $\mathbb{Q}(\delta)$ of $\mathbb{Q}(\sqrt{p})$ in $\mathbb{Q}_{\rm tr}$.

Let $a = \varepsilon + \bar{\epsilon} \in \mathbb{Z}$. Then ε is a root of the polynomial $X^2 - aX + 1$, so δ is a root of the polynomial $X^4 - aX^2 + 1$ and $X^4 - aX^2 + 1 = (X - \delta)(X + \delta)(X - \delta^{-1})(X + \delta^{-1})$. Thus, $\mathbb{Q}(\delta)$ is a Galois extension of $\mathbb{Q}$ of degree 4. Consider $\sigma \in \mathrm{Gal}(\mathbb{Q}(\delta)/\mathbb{Q})$. If

$\sigma\delta = -\delta$, then $\sigma^2\delta = \delta$. If $\sigma\delta = \delta^{-1}$, then $\sigma\delta^{-1} = \delta$, so $\sigma^2\delta = \delta$. If $\sigma\delta = -\delta^{-1}$, then $\sigma\delta^{-1} = -\delta$, so $\sigma^2\delta = -(\sigma\delta)^{-1} = -(-\delta^{-1})^{-1} = \delta$. In each case $\sigma^2 = 1$. It follows that $\mathrm{Gal}(\mathbb{Q}(\delta)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. This gives a square free integer d with $\mathbb{Q}(\delta) = \mathbb{Q}(\sqrt{p}, \sqrt{d})$. In particular, $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}_{\mathrm{tr}}$, so $d > 1$.

Since ε_p is a unit, the extension $\mathbb{Q}(\delta)/\mathbb{Q}(\sqrt{p})$ is ramified at most in primes that lie over 2 [FrJ, Example 2.3.8, Case C]. Hence, $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is ramified at most in $2, p$. This forces d to be 2 or $2p$. In both cases $\mathbb{Q}(\delta_p) = \mathbb{Q}(\sqrt{p}, \sqrt{2})$. It follows that

$$\begin{aligned} S_p &= \{\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e \mid\ \tilde{\mathbb{Q}}(\boldsymbol{\sigma}) \cap \mathbb{Q}(\delta_p) = \mathbb{Q}(\sqrt{p})\} \\ &= \mathrm{Gal}(\mathbb{Q}(\sqrt{p}))^e \smallsetminus \mathrm{Gal}(\mathbb{Q}(\delta_p))^e \\ &= \mathrm{Gal}(\mathbb{Q}(\sqrt{p}))^e \smallsetminus \mathrm{Gal}(\mathbb{Q}(\sqrt{2}))^e \\ &= \mathrm{Gal}(\mathbb{Q}(\sqrt{p}))^e \cap \Sigma \end{aligned} \tag{2}$$

Hence, $\mu_{\mathbb{Q}}(S_p) = \frac{1}{2^e} - \frac{1}{4^e} = \frac{1}{2^e}\big(1 - \frac{1}{2^e}\big)$, so $\mu_\Sigma(S_p) = \frac{1}{2^e}$.

List the prime numbers congruent to -1 modulo 4 as $p_1, p_2, p_3, \ldots$. Then the fields $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{p_1}), \mathbb{Q}(\sqrt{p_2}), \ldots$ are linearly disjoint over $\mathbb{Q}$ (because each p_i is ramified in $\mathbb{Q}(\sqrt{p_i})$ and in no other field of that sequence). In addition,

$$S_{p_1} \cap \cdots \cap S_{p_n} = \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}))^e \smallsetminus \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{2}))^e.$$

Hence, $\mu_{\mathbb{Q}}(S_{p_1} \cap \cdots \cap S_{p_n}) = \frac{1}{2^{ne}} - \frac{1}{2^{(n+1)e}} = \frac{1}{2^{ne}}\big(1 - \frac{1}{2^e}\big)$. Therefore,

$$\mu_\Sigma(S_{p_1} \cap \cdots \cap S_{p_n}) = \frac{1}{2^{ne}} = \mu_\Sigma(S_{p_1}) \cap \cdots \cap S_{p_n}) = \mu_\Sigma(S_{p_1}) \cdots \mu_\Sigma(S_{p_n}).$$

Consequently, $S_{p_1}, S_{p_2}, S_{p_e}, \ldots$ are independent in Σ.

By Borel-Cantelli, almost all $\boldsymbol{\sigma} \in \Sigma$ belong to at least one S_{p_n} [FrJ, Lemma 18.3.4]. Then ε_{p_n} is an absolutely positive unit of $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})$ which is not a square in $\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma})$, as desired. ∎

LEMMA 4.3: *For almost all $\boldsymbol{\sigma} \in \Sigma$ the ring $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})$ satisfies Hypothesis G(2).*

Proof: Let Σ' be the set of all $\boldsymbol{\sigma} \in \Sigma$ such that $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})$ has an absolutely positive unit which is not a square in $\mathbb{Q}_{\mathrm{tr}}(\boldsymbol{\sigma})$. For each totally real number field K, each absolutely positive unit c of O_K, and all distinct elements $a_1, \ldots, a_m, b_1, \ldots, b_n$ in O_K let $S(K, \mathbf{a}, \mathbf{b}, c)$ be the set of all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{K})^e$ for which there exists $(x, \mathbf{y}, \mathbf{z}) \in \mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})^{1+m+n}$ that satisfies (1). There are only countably many quadruple $(K, \mathbf{a}, \mathbf{b}, c)$ of that form. Hence, by Lemmas 4.2 and 4.1, the measure of $S = \Sigma' \cap \bigcap_{K,\mathbf{a},\mathbf{b},c} S(K, \mathbf{a}, \mathbf{b}, c)$ in Σ is 1.

We prove that $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ satisfies Hypothesis G(2) for each $\boldsymbol{\sigma} \in S$. Indeed, $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ has an absolutely positive unit c. Let $a_1, \ldots, a_m, b_1, \ldots, b_n \in \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ and set $K = \mathbb{Q}(\mathbf{a}, \mathbf{b}, c)$. Then K is an absolutely real number field, c is an absolutely positive unit of O_K, $a_1, \ldots, a_m, b_1, \ldots, b_n \in O_K$, and $\boldsymbol{\sigma} \in S(K, \mathbf{a}, \mathbf{b}, c)$. By definition, there exists $(x, \mathbf{y}, \mathbf{z}) \in \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})^{1+m+n}$ that satisfies (1). Consequently, $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ satisfies Hypothesis G(2). ∎

Lemma 4.4: *For each positive integer n there exists $\boldsymbol{\sigma} \in \Sigma$ such that $|\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \cap \mathbb{P}[0,4]| \geq n$.*

Proof: Choose an odd prime $p > 2n$. Then $\mathbb{Q}(\zeta_p) \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$, because 2 ramifies in $\mathbb{Q}(\sqrt{2})$ but not in $\mathbb{Q}(\zeta_p)$. Let $K_p = \mathbb{Q}(f(\zeta_p))$. By Lemma 1.1, all of the conjugates of $f(\zeta_p)$ are in $O_{K_p} \cap \mathbb{P}[0,4]$ and there are at least n of them. Moreover, $\mathbb{Q}(\zeta_p)$ is a quadratic extension of K_p, so $[K_p : \mathbb{Q}] = \frac{p-1}{2}$ and $K_p \cap \mathbb{Q}(\sqrt{2}) = \mathbb{Q}$. The latter relation implies that $\mathrm{Gal}(K_p)^e \cap \Sigma = \mathrm{Gal}(K_p)^e \smallsetminus \mathrm{Gal}(K_p(\sqrt{2}))^e$ and

$$\mu(\mathrm{Gal}(K_p)^e \cap \Sigma) = \frac{1}{\left(\frac{p-1}{2}\right)^e} - \frac{1}{(p-1)^e} = \frac{2^e - 1}{(p-1)^e} > 0.$$

Each $\sigma \in \mathrm{Gal}(K_p)^e \cap \Sigma$ will satisfy the conclusion of the lemma. ∎

Denote the set of all sentences of $\mathcal{L}(\mathrm{ring})$ which hold in $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in \Sigma$ by Almost(Σ). For each $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ let $U(\boldsymbol{\sigma}) = \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \cap \mathbb{P}[0,4]$. The proof of the following result is modeled after the proof of [FrJ, Thm. 23.3.1].

Proposition 4.5: *The theory of finite graphs is interpretable in* Almost(Σ), *so* Almost(Σ) *is undecidable.*

Proof: The theory of finite graphs is undecidable [FrJ, Cor. 28.5.3], so it suffices to interpret the theory of finite graphs in Almost(Σ).

For each sentence η of $\mathcal{L}(\mathrm{ring})$ let $\mathrm{Truth}(\eta) = \{\sigma \in \Sigma \mid \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \models \eta\}$. Let

$$(3) \qquad S = \bigcap_{\eta \in \mathrm{Almost}(\Sigma)} \mathrm{Truth}(\eta) \cap \{\boldsymbol{\sigma} \in \Sigma \mid U(\boldsymbol{\sigma}) \text{ is finite }\} \cap \{\boldsymbol{\sigma} \in \Sigma \mid \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \text{ satisfies hypothesis } G(2)\}.$$

By definition, $\mu_\Sigma(\mathrm{Truth}(\eta)) = 1$ for each $\eta \in \mathrm{Almost}(\Sigma)$. Since there are only countable many sentences η, the measure (in Σ) of the first term on the right hand side of (3) is 1. By Proposition 3.6(c), $\mu_\Sigma\{\sigma \in \Sigma \mid U(\boldsymbol{\sigma}) \text{ is finite }\} = 1$. By Lemma 4.3,

$$\mu_\Sigma\{\boldsymbol{\sigma} \in \Sigma \mid \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \text{ satisfies hypothesis } G(2)\} = 1.$$

Therefore, $\mu_\Sigma(S) = 1$.

Let $\mathcal{Q}_{\boldsymbol{\sigma}} = \{U(\boldsymbol{\sigma})\}$ and $\mathcal{R} = \{\langle \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}), \mathcal{Q}_\sigma\rangle \mid \boldsymbol{\sigma} \in S\}$. Then $\mathcal{R}$ is a set of weak monadic structures over the rings $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ which satisfies Hypothesis $G(2)$ (by (3)) with $|U(\boldsymbol{\sigma})|$ unbounded (Lemma 4.4). By Proposition 2.4, the theory of finite graphs is interpretable in $\mathrm{Th}(\mathcal{R})$. Thus, it suffices to interpret $\mathrm{Th}(\mathcal{R})$ in $\mathrm{Almost}(\Sigma)$.

By definition, for all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ and $s \in \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$,

$$s \in U(\boldsymbol{\sigma}) \Longleftrightarrow \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \models 0 \ll s \ll 4 \tag{4}$$

We define a map $\varphi \mapsto \varphi^*$ from formulas of $\mathcal{L}_1$ to formulas of $\mathcal{L}(\mathrm{ring})$ in the following way. If φ is the atomic formula $z \in X$, then φ^* is $0 \ll z \ll 4$. If φ is an atomic formula of $\mathcal{L}(\mathrm{ring})$, set φ^* to be φ. Next let the star operation commute with negation and disjunction. Finally, if φ^* is an interpretation of a formula φ of $\mathcal{L}_1$, then φ^* is also the interpretation of $(\exists X)\varphi$. Starting from (4), an induction on the structure of formulas in $\mathcal{L}_1$ proves the following statement: Let $\varphi(z_1, \ldots, z_m, X_1, \ldots, X_n)$ be a formula of $\mathcal{L}_1$, $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$, and $s_1, \ldots, s_m \in \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$. Then $\varphi^*(z_1, \ldots, z_m)$ has its free variables among the $z_1, \ldots, z_m$'s and

$$\langle \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}), \mathcal{Q}_\sigma\rangle \models \varphi(\mathbf{s}, U(\boldsymbol{\sigma}), \ldots, U(\boldsymbol{\sigma})) \Longleftrightarrow \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \models \varphi^*(\mathbf{s}). \tag{5}$$

The induction step from φ to $(\exists X_n)\varphi$ is justified by the observation, that $U(\boldsymbol{\sigma})$ is the only element of $\mathcal{Q}_{\boldsymbol{\sigma}}$.

It follows from (5) that a sentence θ of $\mathcal{L}_1$ belongs to $\mathrm{Th}(\mathcal{R})$ if and only if θ^* is in $\mathrm{Almost}(\Sigma)$. Indeed, if $\theta \in \mathrm{Th}(\mathcal{R})$, then $\langle \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}), \mathcal{Q}_{\boldsymbol{\sigma}}\rangle \models \theta$, so $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \models \theta^*$ for all $\boldsymbol{\sigma} \in S$. Since $\mu_\Sigma(S) = 1$, we conclude that $\theta^* \in \mathrm{Almost}(\Sigma)$. Conversely, suppose $\theta^* \in \mathrm{Almost}(\Sigma)$. Then $S \subseteq \mathrm{Truth}(\theta^*)$. Hence, $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}) \models \theta^*$, so $\langle \mathbb{Z}_{\rm tr}(\boldsymbol{\sigma}), \mathcal{Q}_{\boldsymbol{\sigma}}\rangle \models \theta$ for all $\boldsymbol{\sigma} \in S$, that is $\theta \in \mathrm{Th}(\mathcal{R})$.

This conclude the interpretation of $\mathrm{Th}(\mathcal{R})$ in $\mathrm{Almost}(\Sigma)$. ∎

Denote the set of all sentences of $\mathcal{L}(\mathrm{ring})$ which hold in $\mathbb{Z}_{\rm tr}(\boldsymbol{\sigma})$ for almost all $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q})^e$ by $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$.

THEOREM 4.6: *Let $e \geq 2$. Then the theory of finite graphs is interpretable in* $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$, *hence that theory is undecidable.*

Proof: By Proposition 4.5, it suffices to interpret $\mathrm{Almost}(\Sigma)$ in $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$. To each sentence θ of $\mathcal{L}(\mathrm{ring})$ let θ' be the sentence

$$\theta \vee (\exists x)[x^2 = 2].$$

The second disjunct of θ' holds in $\mathbb{Z}_{\mathrm{tr}}(\boldsymbol{\sigma})$ for each $\boldsymbol{\sigma} \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}))$. By definition, $\Sigma = \mathrm{Gal}(\mathbb{Q})^e \smallsetminus \mathrm{Gal}(\mathbb{Q}(\sqrt{2}))^e$. Hence, $\theta \in \mathrm{Almost}(\Sigma)$ if and only if $\theta' \in \mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$. Thus, $\theta \mapsto \theta'$ is the desired interpretation of $\mathrm{Almost}(\Sigma)$ in $\mathrm{Almost}(\mathrm{Gal}(\mathbb{Q})^e)$. ∎

References

[ChJ] G. Cherlin and M. Jarden, *Undecidability of some elementary theories over PAC fields,* Annals of pure and applied logic **30** (1986), 137–163.

[ELT] Yu. L. Ershov, I. A. Lavrov, A. D. Taimanov, and M. A. Taitslin, *Elementary theories,* Russian Mathematical Surveys **20** (1965), 35–105.

[FrJ] M. D. Fried and M. Jarden, *Field Arithmetic, Second Edition, revised and enlarged by Moshe Jarden,* Ergebnisse der Mathematik (3) **11**, Springer, Heidelberg, 2005.

[Has] H. Hasse, *Number Theory,* Grundlehren der mathematischen Wissenschaften **229**, Springer-Verlag, Berlin, 1980.

[Jar] M. Jarden, *Roots of unity over large algebraic fields,* Mathematische Annalen **213** (1975), 109–127.

[Kro] L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten,* Journal für die reine und angewandte Mathematik **53** (1985), 173–175.

[Lan] S. Lang, *Fundamentals of Diophantine Geometry,* Springer-Verlag, New York, 1983.

[Rob] J. Robinson, *On the decision problem for algebraic rings,* Collected Papers, in Studies in Mathematical Analysis and Related Topics: Essays in Honor of G. Polya, Stanford University Press, Standford, California, 1962, pp. 297–304. See also The Collected Works of Julia Robinson (Solomon Fefferman ed.), pp. 91–98, American Mathematical Society, Collected Works Volume 6, 1997.

[Sie] C. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Mathematische Zeitschrift **11** (1921), 246-275.