UNDECIDABILITY OF $\mathbb{Q}^{(2)}$.

CARLOS MARTINEZ-RANERO, JAVIER UTRERAS, AND CARLOS R. VIDELA

Abstract. It is shown that the compositum $\mathbb{Q}^{(2)}$ of all degree 2 extensions of $\mathbb{Q}$ has undecidable theory.

MSC: 11U05, 03B25, 11R11.

1. Introduction

In this note we are interested in the following question.

Problem 1. For which infinite algebraic extensions $K$ of $\mathbb{Q}$ is the theory Th($K$) undecidable?

This question was first raised by A. Tarski and J. Robinson. In the 1930’s A. Tarski showed that $\mathbb{Q}^{alg}$ and $\mathbb{R} \cap \mathbb{Q}^{alg}$ have decidable theories, and in 1959 J. Robinson showed that all number fields (that is, finite extensions of $\mathbb{Q}$) have undecidable theory. Since there are uncountably many, non-elementarily equivalent, infinite algebraic extensions of $\mathbb{Q}$ and only countably many decision algorithms, it follows that most of them are undecidable. Such examples were pointed out by J. Robinson [4]: for any non-recursive set $S$ of prime numbers the field $\mathbb{Q}_S = \mathbb{Q}(\{\sqrt{p} : p \in S\})$ has undecidable theory. Later the third named author [7] showed that the field $\mathbb{Q}_S$ has undecidable theory for any infinite set of primes $S$.

An interesting class of fields in which to study the above question, and to test current methods is the class of fields $K^{(d)}$, which are the compositum of all extensions fields $F/K$ of degree at most $d$ over $K$, where $K$ is a number field.

These fields are Galois over $K$ of infinite degree over $K$, and every element of $\text{Gal}(K^{(d)}/K)$ has order dividing $d!$. Thus $\text{Gal}(K^{(d)}/K)$ is a pro-$S$ Galois extension, where $S$ is the set of prime numbers that divide $d!$.

E. Bombieri and U. Zannier [1] conjecture that these fields have the Northcott property making them, in this respect, similar to number fields. They proved that $K^{(2)}$ has the Northcott property.

The first named author was partially supported by Proyecto VRID-Enlace No. 218.015.022-1.0.

The second named author was supported by FONDECYT-Postdoctorado No. 3160301.

Part of this work was done while the third author was visiting X. Vidaux in Concepción during May 2018 under Conicyt Project: Fondecyt 1170315.
In this note, we show the following result:

**Main Theorem.** The theory $Q$ of R. Robinson is first-order interpretable in $Q^{(2)}$, hence $Th(Q^{(2)})$ is undecidable.

X. Vidaux and C. Videla [8] establish a relation between the Northcott property and undecidability. Based on this connection and our present result we conjecture that all $K^{(d)}$ have undecidable theory.

We refer the reader to A. Shlapentokh ([5]) for an update on the subject, and to J. Koenigsmann [2] for a general survey.

2. Undecidability

Before proceeding any further let us fix some notation. Let $Q_{al}^{alg}$ denote a fixed algebraic closure of $Q$. Recall that for any field $T \subset Q_{al}^{alg}$, the ring $O_T$ denotes the integral closure of $Z$ in $T$, $O_T^\times$ denotes the multiplicative group of units of $O_T$ and $\mu_T$ denotes the group of roots of unity of the field $T$. Let $\{p_n: n \in \mathbb{N}_{\geq 1}\}$ be the increasing enumeration of the rational prime numbers, $K = Q(\{\sqrt{p}: p \text{ is prime}\})$, $L = K(i)$, $K_n = Q(\{\sqrt{p}: \ell \leq n\})$ and $L_n = K_n(i)$. Note that $L = Q^{(2)}$. Recall that for $f(x) \in Z[x]$ given by $a_nx^n + \cdots + a_0$ and any $k \in \mathbb{N}$, the forward difference operator is given by $\Delta^k f(x) = f(x + k) - f(x)$ and that the $n$-th iteration satisfies $\Delta^k f(x) = n!a_nk^n$.

Let $L_{ring} = \{0, 1; +, \cdot\}$ denote the language of rings, and for any $L_{ring}$-structure $F$ we denote by $Th(F)$ its first-order $L_{ring}$-theory.

In order to show that $Th(L)$ is undecidable, we first use the following Theorem of the third named author (see [7]).

**Theorem 2.** Let $F$ be a number field and $T \subset \hat{Q}$ a pro-$p$ Galois extension of $F$, then $O_T$ is first-order definable in $T$.

In particular since $L$ is a pro-2 Galois extension it follows that $O_L$ is first-order definable in $L$. This reduces the problem to showing that the theory $Th(O_L)$ is undecidable. In order to do so, we use an improvement, due to C. W. Henson (see [6]), of a result of J. Robinson (see [3]).

**Lemma 3.** Let $R$ be a ring of algebraic integers and let $F \subset P(R)$ be a family of subsets of $R$ parametrised by an $L_{ring}$-formula $\varphi(x; y_1, \ldots, y_n)$, i.e.,

$$F \in F \iff \exists b_1, \ldots, b_n \in R \forall x [x \in F \leftrightarrow \varphi(x; b_1, \ldots, b_n)]$$

If the family $F$ contains sets of arbitrary large finite cardinality, then the theory of the ring $Th(R)$ interprets the theory $Q$ of R. Robinson, hence is undecidable.

Moreover, in the same paper, J. Robinson proves the following result:
Lemma 4. For each \( t \in \mathbb{R} \) the set \( \{ x \in \mathcal{O}_K : 0 \ll x \ll t \} \) is finite where \( 0 \ll x \ll t \) means that \( x \) and all its conjugates lie strictly between 0 and \( t \).

We are left to show that there is a family as in Lemma 3. This will be done below.

Lemma 5. The group \( \mu_L \) of roots of unity of \( L \) is finite.

Proof. Suppose otherwise. Fix \( \{ w_k : k \in \mathbb{N} \} \) an enumeration of \( \mu_L \), and consider the sequence \( t_k = 2 + w_k + w_k^{-1} \), note that each \( t_k \in K \) and \( 0 \ll t_k \ll 4 \), which contradicts Lemma 4. \( \square \)

Let \( N \) denote the order of the finite group \( \mu_L \).

Lemma 6. If \( u \) is an element of \( \mathcal{O}_K^\times \), then \( u^{2N} \in \mathcal{O}_K^\times \).

Proof. Fix \( n \) such that \( u \in \mathcal{O}_L^n \). By a theorem of H. Hasse (see [9], Theorem 4.12), we have that \( \mathcal{O}_L^n : \mu_L \mathcal{O}_K^\times \in \{ 1, 2, \ldots \} \). Thus, \( u^2 \in \mu_L \mathcal{O}_K^\times \), so we can write \( u^2 = \zeta w \) for some \( \zeta \in \mu_L \) and \( w \in \mathcal{O}_K^\times \). It follows from the choice of \( N \) that \( u^{2N} = w^N \in \mathcal{O}_K^\times \). \( \square \)

Lemma 7. There is a first-order definable subset \( W \) of \( \mathcal{O}_L \) such that \( \mathbb{N} \subset W \subset \mathcal{O}_K \).

Proof. We define, recursively, a sequence of definable sets as follows: Let \( X^{(0)} = \{ x_1^2 + x_2^2 : x_1, x_2 \in \mathcal{O}_L^\times \} \), and let \( X^{(n+1)} = \{ x \in \mathcal{O}_L : \exists x_1, x_2 \in X^{(n)} \, (x = x_1 - x_2) \} \). Observe that for each \( n \), the set \( X^{(n)} \) is first-order definable and \( X^{(n)} \subseteq \mathcal{O}_K \). Consider the following polynomial with integer coefficients

\[
\phi(x) = (x + \sqrt{x^2 + 1})^{2N} + (x - \sqrt{x^2 + 1})^{2N}.
\]

Note that for each \( n \in \mathbb{N}, f(n) \in X^{(0)} \). Thus, it follows that for each \( k \in \mathbb{N} \), the \( 2N \)-th iteration of the discrete derivative \( \Delta^{2N}_k f = 2(2N)!k^{2N} \in X^{(2N)} \). By Hilbert’s solution to Waring’s problem, there is a natural number, usually denoted by \( g(2N) \), so that every natural number is a sum of at most \( g(2N) \) \( 2N \)-powers of natural numbers. Thus,

\[
W = \bigcup_{\ell=0}^{2(2N)!} \{ x \in \mathcal{O}_L : \exists x_1, \ldots, x_{2^{(2N)}} \in X^{(2N)} \, (x = \sum_{k=1}^{g(2N)} x_k + \ell) \}
\]

is as required. \( \square \)

We are now in position to prove the main theorem of this note.

Main Theorem. The theory \( Th(\mathbb{Q}^{(2)}) \) is undecidable.

Proof. Consider the family \( \mathcal{F} \) parametrised by the formula \( \varphi(x, p, q) \)

\[
px \neq 0 \land px \neq q \land \exists x_1, \ldots, x_8 \in W \, [px = x_1^2 + \cdots + x_4^2 \land (q - px) = x_5^2 + \cdots + x_8^2]
\]
In particular, for $p, q \in \mathbb{N}$ this means that $\varphi(x; p, q)$ implies that $0 \ll px \ll q$. Hence, it follows from Lemma 4 and Lagrange’s four square theorem that $F$ contains sets of arbitrary large finite cardinality.

We are unable to treat the case of $K^{(2)}$, where $K$ is an arbitrary totally real number field.

References

[1] Bombieri, Enrico; Zannier, Umberto A note on heights in certain infinite extensions of $\mathbb{Q}$. Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei (9) Mat. Appl. 12 (2001), 5-14 (2002).

[2] Koenigsmann, Jochen Undecidability in number theory. Model theory in algebra, analysis and arithmetic, 159-195, Lecture Notes in Math., 2111, Fond. CIME/CIME Found. Subser., Springer, Heidelberg, 2014.

[3] Robinson, Julia On the decision problem for algebraic rings. 1962 Studies in mathematical analysis and related topics pp. 297-304 Stanford Univ. Press, Stanford, Calif.

[4] Robinson, Julia The decision problem for fields. 1965 Theory of Models (Proc. 1963 Internat. Sympos. Berkeley) pp. 299-311 North-Holland, Amsterdam.

[5] Shlapentokh, Alexandra First order definability and decidability in infinite algebraic extensions of rational numbers. Israel Journal Math. 226 (2018), 579-633.

[6] van den Dries, Lou Elimination theory for the ring of algebraic integers. J. Reine Angew. Math. 388 (1988), 189-205.

[7] Videla, Carlos R. Definability of the ring of integers in pro-p Galois extensions of number fields. Israel J. Math. 118 (2000), 1-14.

[8] Vidaux, Xavier; Videla, Carlos R. A note on the Northcott property and undecidability. Bull. Lond. Math. Soc. 48 (2016), no. 1, 58-62.

[9] Washington, Lawrence C. Introduction to cyclotomic fields. Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997. xiv+487 pp. ISBN: 0-387-94762-0

Universidad de Concepción, Concepción, Chile, Facultad de Ciencias Físicas y Matemáticas, Departamento de Matemática, Casilla 160 C

E-mail address: cmartinezr@udec.cl

Universidad de Concepción, Concepción, Chile, Facultad de Ciencias Físicas y Matemáticas, Departamento de Matemática, Casilla 160 C

E-mail address: javierutreras@udec.cl

Mount Royal University, Calgary, Canada, Department of Mathematics and Computing

E-mail address: cvidela@mtroyal.ca