TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 356, Number 8, Pages 3189–3207
S 0002-9947(03)03343-9
Article electronically published on November 4, 2003

ON DIOPHANTINE DEFINABILITY AND DECIDABILITY IN SOME INFINITE TOTALLY REAL EXTENSIONS OF $\mathbb{Q}$

ALEXANDRA SHLAPENTOKH

Abstract. Let M be a number field, and W_M a set of its non-Archimedean primes. Then let $O_{M,W_M} = \{x \in M | \operatorname{ord}_{\mathfrak{t}} x \geq 0, \forall \mathfrak{t} \notin W_M\}$. Let $\{p_1, \ldots, p_r\}$ be a finite set of prime numbers. Let F_{inf} be the field generated by all the p_i^j-th roots of unity as $j \to \infty$ and $i = 1, \ldots, r$. Let K_{inf} be the largest totally real subfield of F_{inf}. Then for any $\varepsilon > 0$, there exist a number field $M \subset K_{inf}$, and a set W_M of non-Archimedean primes of M such that W_M has density greater than $1 - \varepsilon$, and $\mathbb{Z}$ has a Diophantine definition over the integral closure of O_{M,W_M} in K_{inf}.

1. Introduction

The interest in the questions of Diophantine definability and decidability goes back to a question which was posed by Hilbert: given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, is there a uniform algorithm to determine whether such an equation has solutions in $\mathbb{Z}$? This question, otherwise known as Hilbert's 10th problem, has been answered negatively in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich. (See [3] and [4].) Since the time when this result was obtained, similar questions have been raised for other fields and rings. In other words, let R be a recursive ring. Then, given an arbitrary polynomial equation in several variables over R, is there a uniform algorithm to determine whether such an equation has solutions in R?

Arguably the two most interesting and difficult problems in the area concern $R = \mathbb{Q}$ and R equal to the ring of algebraic integers of an arbitrary number field.

One way to resolve the question of Diophantine decidability negatively over a ring of characteristic 0 is to construct a Diophantine definition of $\mathbb{Z}$ over such a ring. This notion is defined below.

1.1. **Definition.** Let R be a ring and let $A \subset R$. Then we say that A has a Diophantine definition over R if there exists a polynomial $f(t, x_1, \ldots, x_n) \in R[t, x_1, \ldots, x_n]$ such that for any $t \in R$,

$$\exists x_1, \ldots, x_n \in R, f(t, x_1, ..., x_n) = 0 \Longleftrightarrow t \in A.$$

Received by the editors June 5, 2000 and, in revised form, March 10, 2003.

2000 *Mathematics Subject Classification.* Primary 11U05, 11U09; Secondary 03C07.

Key words and phrases. Hilbert's tenth problem, Diophantine definability.

The research for this paper has been partially supported by NSA grant MDA904-98-1-0510 and NSF grant DMS-9988620.

If the quotient field of R is not algebraically closed, we can allow a Diophantine definition to consist of several polynomials without changing the nature of the relationship. (See [4] for more details.)

The usefulness of Diophantine definitions stems from the following easy lemma.

1.2. **Lemma.** *Let $R_1 \subset R_2$ be two recursive rings such that the quotient field of R_2 is not algebraically closed. Assume that Hilbert's tenth problem (abbreviated as "HTP"in the future) is undecidable over R_1, and R_1 has a Diophantine definition over R_2. Then HTP is undecidable over R_2.*

One can also combine Diophantine definitions to obtain the following observation.

1.3. **Combining Diophantine definitions.** Suppose $R_3 \subset R_2 \subset R_1$ are integral domains whose fraction fields are not algebraically closed. Assume further that R_2 has a Diophantine definition $f_1(t, x_1, \ldots, x_{m_1})$ over R_1 and R_3 has a Diophantine definition $f_2(t, y_1, \ldots, y_{m_2})$ over R_2. Then the following system of equations would correspond to a Diophantine definition of R_3 over R_1:

$$\begin{cases} f_2(t, y_1, \ldots, y_{m_2}) = 0, \\ f_1(t, x_1, \ldots, x_{m_1}) = 0, \\ f_1(y_i, x_{i,1}, \ldots, x_{i,m_1}) = 0, i = 1, \ldots, m_2. \end{cases}$$

Diophantine definitions have been obtained for $\mathbb{Z}$ over the rings of algebraic integers of some number fields. Jan Denef has constructed a Diophantine definition of $\mathbb{Z}$ for the finite degree totally real extensions of $\mathbb{Q}$. Jan Denef and Leonard Lipshitz extended Denef's results to the totally complex extensions of degree 2 of the finite degree totally real fields. Thanases Pheidas and the author have independently constructed Diophantine definitions of $\mathbb{Z}$ for number fields with exactly one pair of complex conjugate embeddings. Finally, Harold N. Shapiro and the author of this paper showed that the subfields of all the fields mentioned above "inherited" the Diophantine definitions of $\mathbb{Z}$. (These subfields include all the abelian extensions.) The proofs of the results listed above can be found in [5], [7], [6], [15], [22], and [23]. The problem is still open for a general number field, but there are also some recent results of Bjorn Poonen which depend on the existence of rank one elliptic curves over $\mathbb{Q}$ keeping their rank in number field extensions. See [18] for more details.

A similar approach can in theory be applied to $\mathbb{Q}$. In other words, one could show that HTP is undecidable over $\mathbb{Q}$ by showing that $\mathbb{Z}$ has a Diophantine definition over $\mathbb{Q}$. Unfortunately, one of the consequences of a series of conjectures by Barry Mazur and Colliot-Thélène, Swinnerton-Dyer and Skorobogatov is that $\mathbb{Z}$ does not have a Diophantine definition over $\mathbb{Q}$, and thus one would have to look to some other method for resolving HTP over $\mathbb{Q}$. (Mazur's conjectures can be found in [10], [11], [12] and [13]. However, Colliot-Thélène, Swinnerton-Dyer and Skorobogatov have found a counterexample to the strongest of the conjectures in the papers cited above. Their modification of Mazur's conjecture in view of the counterexample can be found in [1].) Thanases Pheidas has recently proposed another approach to the question of Diophantine decidability of $\mathbb{Q}$. If this method proves to be successful, it would imply that another conjecture of Mazur is false. (See [16].) For more connections between Mazur's conjectures and the questions of Diophantine definability and decidability over global fields, see [2] and [29].

Given the difficulty of the Diophantine problem for $\mathbb{Q}$ (and number fields in general), one might adopt a gradual approach, i.e., consider the following problem.

1.4. **An intermediate problem for $\mathbb{Q}$ and number fields.** Let W be a recursive set of rational primes. Let

$$O_{\mathbb{Q},W} = \{x \in \mathbb{Q} \mid x = \frac{a}{b}, a, b \in \mathbb{N}, \forall p \not\in W, p \nmid b\}.$$

Then we can ask whether HTP is decidable for $O_{\mathbb{Q},W}$ or whether $\mathbb{Z}$ has a Diophantine definition over $O_{\mathbb{Q},W}$. We can answer these questions for *finite* W. More precisely, we know that for finite W, $\mathbb{Z}$ does have a Diophantine definition over $O_{\mathbb{Q},W}$ and therefore HTP is undecidable over $O_{\mathbb{Q},W}$. (More generally, using some ideas dating back to Julia Robinson, one can show that the set of algebraic numbers integral at a *finite* set of primes of a number field is Diophantine over this number field. See [19], [20] and [24] for more details.) Unfortunately, we have been unsuccessful in obtaining the analogous definability results for infinite W. However, Bjorn Poonen has recently constructed a Diophantine model of $\mathbb{Z}$ in a subring of $\mathbb{Q}$ where the natural density of primes allowed in the denominator is 1. This construction showed that the analog of Hilbert's tenth problem is undecidable over such rings. For more details, see [17].

We have been more successful in solving the definability problem in some extensions of $\mathbb{Q}$. Before we state these results, we need a definition.

1.5. **Definition.** Let M be a number field and let W be a set of its primes. Then a ring

$$O_{M,W} = \{x \in M \mid \text{ord}_{\mathfrak{p}} x \geq 0 \, \forall \mathfrak{p} \not\in W\}$$

is called a ring of W*-integers* . (The term W-integers usually presupposes that W is finite, but we will use this term for infinite W also.) If $W = \emptyset$, then $O_{M,W} = O_M$ – the ring of algebraic integers of M. If W contains all the primes of M, then $O_{M,W} = M$.

Below we state our best definability results as far as the Dirichlet density of the prime sets allowed in the denominator is concerned.

1.6. **Theorem.** *Let K be a totally real number field or a totally complex extension of degree 2 of a totally real number field. Then for any $\varepsilon > 0$, there exists a set W of primes of K whose Dirichlet density is bigger than $1 - [K : \mathbb{Q}]^{-1} - \varepsilon$ and such that $\mathbb{Z}$ has a Diophantine definition over $O_{K,W}$. (Thus, Hilbert's tenth problem is undecidable over $O_{K,W}$.)*

1.7. **Theorem.** *Let K be as above and let $\varepsilon > 0$ be given. Let $S_{\mathbb{Q}}$ be the set of all the rational primes splitting in K. (If the extension is Galois but not cyclic, $S_{\mathbb{Q}}$ contains all the rational primes.) Then there exists a set of K-primes W such that the set of rational primes $W_{\mathbb{Q}}$ below W differs from $S_{\mathbb{Q}}$ by a set contained in a set of Dirichlet density less than ε and such that $\mathbb{Z}$ has a Diophantine definition over $O_{K,W}$. (Again this will imply that Hilbert's tenth problem is undecidable in $O_{K,W}$.)*

The proofs of these theorems can be found in [25], [28] and [26].

In this paper we consider the integral closures of the rings of W-integers in some totally real infinite extensions of rational numbers. In general, much less is known about the existential definability and decidability in the infinite extensions of $\mathbb{Q}$ than in the finite extensions. Due to results of Rumely and others, we know that HTP is *decidable* in the ring of all algebraic integers and some other "sufficiently large" rings. (See [21], [8], [9] for more details.) On the other hand, in [27], the author proved the following theorem.

1.8. **Theorem.** *Let K_{inf} be a totally real infinite extension of $\mathbb{Q}$ with a finite degree subextension K containing primes $p_1, \ldots, p_s$ with the following property. If M is a number field such that $K \subset M \subset K_{inf}$, then $p_1, \ldots, p_s$ remain prime in the extension M/K. Let $S = \{p_1, \ldots, p_s\}$. Then $\mathbb{Z}$ has a Diophantine definition in the integral closure of $O_{K,S}$ in K_{inf}. (See Theorem 4.3 of* [27]*.)*

In this paper we extend Theorem 1.6 and Theorem 1.8 in the following fashion.

1.9. **Theorem.** *Let K_{inf} be a totally real field of algebraic numbers, possibly of infinite degree over $\mathbb{Q}$. Assume that for some finite degree subfield K of K_{inf} the following conditions are satisfied.*

(1) *K_{inf}/K is a normal extension.*
(2) *There exists a prime $\mathfrak{p}$ such that $\mathfrak{p}$ remains prime in the extension M/K, where M is any number field with $K \subset M \subset K_{inf}$.*
(3) *Only finitely many primes of K ramify in the extension K_{inf}/K.*
(4) *There exists a natural number A such that for every number field M with $K \subset M \subset K_{inf}$ there exists a non-trivial subfield $\bar{M}$ of M containing K and satisfying the following conditions.*
   (a) *$[M : \bar{M}] \le A$.*
   (b) *For some basis $\Omega_{M/\bar{M}}$ of M over $\bar{M}$, with $\{1\} \subset \Omega_{M/\bar{M}} \subset O_M$, for all $\omega \in \Omega_{M/\bar{M}}$ and every σ-embedding of M into $\mathbb{C}$, we have $|\sigma(\omega)| \le A$.*
(5) *There exists a number field E, a totally real cyclic extension of $\mathbb{Q}$ of degree p such that, for any subfield M of K_{inf}, p is prime to $[M : \mathbb{Q}]$, $\mathfrak{p}$ splits completely in the extension KE/K, and for some $\gamma_E \in O_E$ generating E over $\mathbb{Q}$, $\mathfrak{p}$ does not divide the coefficients of the monic irreducible polynomial of γ_E over $\mathbb{Q}$.*

Let W_K be a union of a set of primes of K not splitting in the extension KE/K and not dividing the discriminant or the coefficients of the monic irreducible polynomial of γ_E over $\mathbb{Q}$, and $\{\mathfrak{p}\}$. Then O_{K,W_K} has a Diophantine definition in its integral closure in K_{inf}.

1.10. **Corollary.** *Let K_{inf} be a field satisfying conditions 1 – 4 of Theorem 1.9 with respect to any number field $K \subset K_{inf}$, and also the following conditions.*

(1) *There are infinitely many rational primes p such that for any number field $M \subset K_{inf}$ we have $[M : \mathbb{Q}] \not\cong 0 \mod p$.*
(2) *Any rational prime has only finitely many distinct factors in K_{inf}.*

Then for any $\varepsilon > 0$, there exist a number field $M \subset K_{inf}$ and a set W_M of non-Archimedean primes of M such that W_M has density greater than $1 - \varepsilon$, and $\mathbb{Z}$ has a Diophantine definition over the integral closure of O_{M,W_M} in K_{inf}.

Finally, we will show that for totally real subfields of some infinite cyclotomic extensions of $\mathbb{Q}$, the conditions of Corollary 1.10 are satisfied.

2. Notation and assumptions

In this section we describe notation and assumptions to be used in the rest of the paper.

- K will denote a totally real number field of degree n_K over $\mathbb{Q}$.
- K_{inf} will denote an infinite totally real extension of $\mathbb{Q}$ with $K \subset K_{inf}$ and K_{inf}/K normal.
- M will range over number fields such that $K \subseteq M \subset K_{inf}$.
- W_K will denote a set of non-Archimedean primes or valuations of K containing a prime $\mathfrak{p}$ of K.
- W_M will denote the set of all the primes of M above the primes of W_K.
- There exists a natural number A such that for every number field $M \neq K$ there exists a non-trivial subfield $\bar{M}$ containing K and satisfying the following conditions.
  1. $[M : \bar{M}] \leq A$
  2. For some basis $\Omega_{\bar{M}/M}$ of M over $\bar{M}$ such that $\{1\} \subset \Omega_{M/\bar{M}} \subset O_M$, for all $\omega \in \Omega_{M/\bar{M}}$ and every σ-embedding of M into $\mathbb{C}$, we have
  $$|\sigma(\omega)| \leq A.$$
- D will denote a natural number not divisible by any prime from W_K and such that for any pair of fields $(M, \bar{M})$ as described above, D is greater than the absolute value of any conjugate of the discriminant $\mathcal{D}_{M/\bar{M}}$ of $\Omega_{M/\bar{M}}$ over $\mathbb{Q}$.
- For any field M, $\mathfrak{p}$ has only one factor in M. $P > 2$ will denote the rational prime below $\mathfrak{p}$ and $e = e(\mathfrak{p}/P)$ will denote the ramification degree of $\mathfrak{p}$ over P.
- Let
$$W_{K_{inf}} = \bigcup_{K \subseteq M \subset K_{inf}} W_M.$$
- $O_{K_{inf}, W_{K_{inf}}}$ will denote the integral closure of O_{K,W_K} in K_{inf}.
- L will denote a totally complex extension of degree 2 of $\mathbb{Q}$ such that LK_{inf} contains no complex roots of unity.
- E will denote a totally real cyclic extension of $\mathbb{Q}$ of degree p such that for all fields M we have $([M : \mathbb{Q}], p) = 1$, and the field LEK_{inf} does not contain any complex roots of unity.
- Let $\gamma_E \in O_E, \gamma_L \in O_L$ be generators of E and L over $\mathbb{Q}$, respectively.
- Let $F_E(T)$ be the monic irreducible polynomial of γ_E over $\mathbb{Q}$.
- Let h_{KEL} denote the class number of KEL.
- Let $l_0 = 0$ and $l_1, \ldots, l_{2eph_{KEL}} \in \mathbb{N}$ be such that the set of polynomials $\{F_E(PT^{2e} + Pl_i)^{h_{LEK}}, i = 0, \ldots, 2eh_{KEL}p\}$ is linearly independent over $\mathbb{R}$.
- Let $\gamma_L \in O_L$ be a generator of L over $\mathbb{Q}$, and assume that $\operatorname{ord}_{\mathfrak{p}} \gamma_L = 0$.
- W_{ELM} and $W_{EL\bar{M}}$ will denote the set of all the primes of ELM and $EL\bar{M}$ respectively above the primes of W_K.
- No prime of $W_K \setminus \{\mathfrak{p}\}$ will split in the extension KE/K.
- No prime of W_K will divide any coefficient or the discriminant of $F_E(T)$.
- $\mathfrak{p}$ will split completely in the extension KEL/K.
- Let $c_F \in \mathbb{N}$ be such that for any $t \in \mathbb{N}, t > c_F$, we have $F_E(t) > 0$.

3. Some properties of algebraic numbers of norm 1

Algebraic numbers of norm 1 play an important role in the construction of Diophantine definitions below. The following lemma explains why.

3.1. **Lemma.** *Let $x \in O_{MLE,W_{MLE}}$, $x \neq \pm 1$, be a solution to the following system of equations:*

$$\left\{\begin{array}{l}\mathbf{N}_{MLE/ML}(x) = 1,\\ \mathbf{N}_{MLE/EM}(x) = 1.\end{array}\right. \tag{3.1}$$

Then $x^{2h_{KLE}} \in ELK$. Furthermore, such a solution exists.

Proof. This lemma is similar to lemmas which can be found in [27] or [26] and deal with finite extensions. To prove the lemma in our case, we had to change a few details.

First we observe that without loss of generality we can assume that M is Galois over K. (If not, we can replace M by its Galois closure over K and look for solutions in the bigger field, since x will have the same conjugates in the bigger field.) Next note that no prime of $W_M \setminus \{\mathfrak{p}_M\}$, where $\mathfrak{p}_M$ is the M-prime above $\mathfrak{p}$, splits in the extension ME/M. Indeed, suppose $\mathfrak{t}_M \in W_M$ splits in the extension ME/M. Since ME/M is cyclic of prime degree, $\mathfrak{t}_M$ splits completely. Let $\mathfrak{t}_K \in W_K$ be the K-prime below $\mathfrak{t}_M$. Then in ME the number of factors of $\mathfrak{t}_K$ is divisible by p. On the other hand, by assumption, $\mathfrak{t}_K$ does not split in the extension KE/K and $[ME : KE] = [M : K]$ is prime to p, while the extension ME/KE is Galois. Hence, the number of factors of $\mathfrak{t}_K$ in ME cannot be divisible by p, and our claim is true.

Further, we note that given our assumptions on $\mathfrak{p}$, by Lemma 8.2, $\mathfrak{p}_M$ splits completely in the extension MLE/M.

Suppose now that $x \in LEM$ is a solution to the system of norm equations. Then the divisor of x must be composed of the primes lying above primes of EM and LM splitting in the extensions LEM/EM and LEM/LM respectively. Given the fact that both extensions are cyclic of distinct prime degrees, we can conclude that LEM-primes occurring in the divisor of x lie above M-primes splitting completely in the extension LEM/M. Thus, if $x \in O_{MLE,W_{MLE}}$ is a solution to the norm system, its divisor consists of factors of $\mathfrak{p}$ in MLE only.

Further, since LEM/EM is a totally complex extension of degree 2 of a totally real field, all the integral solutions to the second equation have to be roots of unity. Since MEL does not have any complex roots of unity, we can conclude the following. Let x_1, x_2 be two solutions to the second norm equation above such that x_1 and x_2 have the same divisor; then $x_1 = \pm x_2$. On the other hand, since $\mathfrak{p}$ does not split in the extension M/K and $\mathfrak{p}$ splits completely in the extension LKE/K, factors of $\mathfrak{p}$ do not split in the extension MLE/KLE. Thus, there exists $y \in O_{LKE,W_{KLE}}$ such that y has the same divisor as $x^{h_{LKE}}$. Therefore, $y = \nu x^{h_{LEK}}$, where ν is an integral unit of MLE, and $\mathbf{N}_{MEL/EM}(y) = \mu$ is an integral unit of EM. On the other hand, since γ_L is of the same degree over EK as over EM, $\mathbf{N}_{MEL/EM}(y) = \mathbf{N}_{KEL/EK}(y)$ and therefore μ is an integral unit of EK. Let $\bar{y} = \mu^{-1}y^2$. Then $\mathbf{N}_{MEL/EM}(\bar{y}) = \mathbf{N}_{KEL/EK}(\bar{y}) = 1$. The divisors of $\bar{y}$ and $x^{2h_{KEL}}$ are the same, and therefore $x^{2h_{KEL}} \in ELK$.

Next we note that we always have solutions to the norm system in $O_{KLE,W_{KLE}}$. Indeed, let

$$G(LEK/K), G(LEK/LK), G(LEK/EK), G(LK/K), G(EK/K)$$

be the Galois groups of the extensions LEK/K, LEK/LK, LEK/EK, LK/K, EK/K respectively. Given our assumptions on the fields L, E, K,

$$G(LEK/LK) \cong G(EK/K) \cong G(E/\mathbb{Q}), G(LEK/EK) \cong G(LK/K) \cong G(L/\mathbb{Q}),$$
$$G(LEK/K) \cong G(LEK/EK) \times G(LEK/LK).$$

Let σ_L be a generator of $G(LEK/EK)$ and let σ_E be a generator of $G(LEK/LK)$. Then $\sigma_L\sigma_E = \sigma_E\sigma_L$ will generate $G(LEK/K)$. Since $\mathfrak{p}$ splits completely in the extension LEK/K, if $\tau_1, \tau_2 \in G(LEK/K)$ are such that $\tau_1(\mathfrak{p}_{LEK}) = \tau_2(\mathfrak{p}_{LEK})$, where $\mathfrak{p}_{LEK}$ is a factor of $\mathfrak{p}$ in LEK, then $\tau_1 = \tau_2$. Let $y \in LEK$ be such that its divisor is $\mathfrak{p}^a_{LEK}$, where $a \in \mathbb{N}$. (Such a y certainly exists if $a \cong 0 \mod h_{LEK}$.) Next consider

$$x = \frac{y\sigma_E\sigma_L(y)}{\sigma_L(y)\sigma_E(y)} = \frac{y/\sigma_L(y)}{\sigma_E(y)/\sigma_L\sigma_E(y)} = \frac{y/\sigma_E(y)}{\sigma_L(y)/\sigma_E\sigma_L(y)}.$$

We claim that x is not a root of unity and satisfies the norm system above. First of all, note that since $y = u/\sigma_L(u) = v/\sigma_E(v)$, the EK-norm and the LK-norm of y are equal to 1 and

$$\mathbf{N}_{LEK/EK}(y) = \mathbf{N}_{LEM/EM}(y), \qquad \mathbf{N}_{LEK/LK}(y) = \mathbf{N}_{LEM/LM}(y).$$

Secondly, note that the divisor of x is of the form

$$\left(\frac{\mathfrak{p}_{LEK}\sigma_E\sigma_L(\mathfrak{p}_{LEK})}{\sigma_L(\mathfrak{p}_{LEK})\sigma_E(\mathfrak{p}_{LEK})}\right)^a.$$

But by the argument above, the primes $\mathfrak{p}_{LEK}, \sigma_L(\mathfrak{p}_{LEK}), \sigma_E(\mathfrak{p}_{LEK}), \sigma_E\sigma_L(\mathfrak{p}_{LEK})$ are all distinct. Thus the divisor of x is not trivial, and x is not a root of unity. It is not hard to see that x's of this form will generate all the solutions to the norm system above.

4. Bounds

In this section we introduce the second ingredient necessary for the construction of Diophantine equations below.

4.1. **Lemma.** *Denote $[MLE : \bar{M}LE]$ by q. Let $y \in O_{MLE,W_{MLE}} \setminus \{0\}$ satisfy the following conditions.*

(1) $y = \frac{u}{\delta}, u \in O_{KLE}, \delta \in O_{MLE}$.
(2) *For every σ-embedding of MLE into $\mathbb{C}$, $|\sigma(y)| > 1$.*

Then

$$\mathbf{N}_{MLE/\bar{M}LE}(\delta)y = a_0 + a_1\omega_1 + \ldots + a_{q-1}\omega_{q-1},$$

where $\{1, \omega_1, \ldots, \omega_{q-1}\} = \Omega_{M/\bar{M}}$, $a_0, \ldots, a_1 \in \bar{M}LE$, and, for all $i = 0, \ldots, q-1$,

$$|\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(a_i)| < C^{[\bar{M}LE:\mathbb{Q}]}|N_{MLE/\mathbb{Q}}(u^2)| \leq |N_{\bar{M}LE/\mathbb{Q}}(Cu^{2A})|,$$

where C is a natural number not divisible by any prime of W_K, and C depends on A and W_K only.

Proof. First of all we observe that, for every σ-embedding of MLE into $\mathbb{C}$, $|\sigma(u)| \geq |\sigma(\delta)|$. Therefore,

$$|\mathbf{N}_{MLE/\mathbb{Q}}(\delta)| \leq |\mathbf{N}_{MLE/\mathbb{Q}}(u)|.$$

Further, let $y = b_0 + b_1\omega_1 + \ldots + b_{q-1}\omega_{q-1}, b_i \in \bar{M}LE$, and consider the following linear system:

$$b_0 + b_1\sigma_j(\omega_1) + \ldots + b_{q-1}\sigma_j(\omega_{q-1}) = \sigma_j(y),$$

where $j = 1, \ldots, q$ and σ_j is an embedding of MLE into $\mathbb{C}$ leaving $\bar{M}LE$ fixed. By Cramer's rule we deduce that for $i = 0, \ldots, q-1$,

$$b_i = \frac{D_i}{\det(\sigma_j(\omega_i))},$$

where $D_i = \sum A_{i,j}\sigma_j(y)$ and $A_{i,j}$ is the (i,j)-th cofactor of the matrix $(\sigma_j(\omega_i))$. Since $|\sigma_j(\omega_i)| \leq A, q \leq A, 1 \leq |\sigma_j(y)|$, we deduce that for $i = 0, \ldots, q-1$,

$$|b_i|^2 \leq \frac{C|\mathbf{N}_{MLE/\bar{M}LE}(y)^2|}{\det^2(\sigma_j(\omega_i))},$$

where $C \in \mathbb{N}$ depends on A only, C is not divisible by any prime in W_K and $\det^2(\sigma_j(\omega_i)) \in \bar{M}$. Next let τ be an embedding of MLE into $\mathbb{C}$ which does not necessarily fix $\bar{M}LE$. By an argument similar to the one above, we then can conclude that for $i = 0, \ldots, q-1$,

$$\tau(b_i)^2 \leq \left|\frac{C\mathbf{N}_{\tau(MLE)/\tau(\bar{M}LE)}(\tau(y))^2}{\det^2(\tau(\sigma_j(\omega_i)))}\right| = \left|\frac{C\tau(\mathbf{N}_{MLE/\bar{M}LE}(y)^2)}{\tau(\det^2(\sigma_j(\omega_i)))}\right|.$$

Since $a_i = \mathbf{N}_{MLE/\bar{M}LE}(\delta)b_i$, we obtain the following:

$$|\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(a_i^2)| = |\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(\mathbf{N}_{MLE/\bar{M}LE}(\delta^2))\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(b_i^2)|$$

$$= |\mathbf{N}_{MLE/\mathbb{Q}}(\delta^2)\prod_{\tau}\tau(b_i^2)| \leq |\mathbf{N}_{MLE/\mathbb{Q}}(u^2)|\prod_{\tau}\left|\frac{C\tau(\mathbf{N}_{MLE/\bar{M}LE}(y)^2)}{\tau(\det^2(\sigma_j(\omega_i)))}\right|$$

and

$$|\mathbf{N}_{MLE/\mathbb{Q}}(u^2)|\left|\frac{C^{[\bar{M}LE:\mathbb{Q}]}\mathbf{N}_{MLE/\mathbb{Q}}(y)^2}{\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(\det^2(\sigma_j(\omega_i)))}\right| \leq C^{[\bar{M}LE:\mathbb{Q}]}|\mathbf{N}_{MLE/\mathbb{Q}}(u^2)\mathbf{N}_{MLE/\mathbb{Q}}(u^2)|$$

$$\leq C^{[\bar{M}LE:\mathbb{Q}]}|\mathbf{N}_{MLE/\mathbb{Q}}(u^4)| \leq |\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(Cu^{4A})|,$$

where products are taken over all embeddings τ of $\bar{M}LE$ into $\mathbb{C}$, and we have used the fact that

$$|\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(\det^2(\sigma_j(\omega_i)))| \geq 1$$

and $|\mathbf{N}_{MLE/\mathbb{Q}}(\delta) \geq 1$.

5. Some useful congruences

The final input into our construction consists of a series of congruences.

5.1. **Lemma.** *Let $x, \xi, \alpha \in O_{MEL,W_{MEL}}$, let $z, w \in O_{KEL,W_{KEL}}$, assume that $\operatorname{ord}_{\mathfrak{t}} x \leq 0$ for all $\mathfrak{t} \in W_{MEL}$, and let the following equalities hold:*

$$w = x^2\xi, \tag{5.1}$$

$$x - z = w\alpha. \tag{5.2}$$

Then $x^{h_{KLE}} = u\delta^{-1}$, where $u \in O_{KLE}$, $\delta \in O_{MLE}$, and all the primes in the divisor of δ are in W_{MLE}.

Proof. Without loss of generality we can assume that $w \neq 0$. Let $\mathfrak{t}$ be a prime of MLE such that $\operatorname{ord}_{\mathfrak{t}} x > 0$. Then $\mathfrak{t} \not\in W_{MLE}$, $\operatorname{ord}_{\mathfrak{t}} \alpha \geq 0$, $\operatorname{ord}_{\mathfrak{t}} \xi \geq 0$, and $\operatorname{ord}_{\mathfrak{t}} z = \operatorname{ord}_{\mathfrak{t}} x$. Indeed, suppose that the last claim is not true. Then either $\operatorname{ord}_{\mathfrak{t}} z < \operatorname{ord}_{\mathfrak{t}} x$ and

$$\operatorname{ord}_{\mathfrak{t}} x < \operatorname{ord}_{\mathfrak{t}} w \leq \operatorname{ord}_{\mathfrak{t}} w\alpha = \operatorname{ord}_{\mathfrak{t}}(x - z) = \operatorname{ord}_{\mathfrak{t}} z < \operatorname{ord}_{\mathfrak{t}} x,$$

or $\operatorname{ord}_{\mathfrak{t}} x < \operatorname{ord}_{\mathfrak{t}} z$ and

$$\operatorname{ord}_{\mathfrak{t}} x < \operatorname{ord}_{\mathfrak{t}} w \leq \operatorname{ord}_{\mathfrak{t}} w\alpha = \operatorname{ord}_{\mathfrak{t}}(z - x) = \operatorname{ord}_{\mathfrak{t}} x < \operatorname{ord}_{\mathfrak{t}} z.$$

In either case we obtain a contradiction. Thus for any $\mathfrak{t}$ such that $\operatorname{ord}_{\mathfrak{t}} x > 0$ we have $\operatorname{ord}_{\mathfrak{t}} x \cong 0 \mod e(\mathfrak{t})$, where $e(\mathfrak{t})$ is the ramification degree of $\mathfrak{t}$ over KLE. Further, let $\mathfrak{q}$ be a conjugate of $\mathfrak{t}$ over KLE. Then by assumption on W_{MLE} we have that $\mathfrak{q} \not\in W_{MLE}$. Thus $\operatorname{ord}_{\mathfrak{q}} \alpha \geq 0$. Further, $\operatorname{ord}_{\mathfrak{q}} w > 0, \operatorname{ord}_{\mathfrak{q}} w\alpha > 0, \operatorname{ord}_{\mathfrak{q}} z > 0$. Thus, $\operatorname{ord}_{\mathfrak{q}} x > 0$. Therefore, by the argument above $\operatorname{ord}_{\mathfrak{q}} x = \operatorname{ord}_{\mathfrak{q}} z = \operatorname{ord}_{\mathfrak{t}} z = \operatorname{ord}_{\mathfrak{t}} x$.

5.2. **Lemma.** *Let $y \in O_{M,W_M}$ be such that the following conditions are satisfied.*

1. *For all $\mathfrak{t} \in W_M$ we have* $\operatorname{ord}_{\mathfrak{t}} y \leq 0$, *$y = \frac{u}{\delta}, u \in O_{KLE}, \delta \in O_{MLE}$.*
2. *For all σ-embeddings of M into $\mathbb{C}$, $1 < |\sigma(y)|$.*
3. *For some $t \in O_{K,W_K}$ and $\mu \in O_{M,W_M}$ we have $y - t = CDy^{2A}\mu$, where C is the constant defined in Lemma 4.1.*

Then $y \in \bar{M}$.

Proof. By Lemma 4.1, $\mathbf{N}_{MLE/\bar{M}LE}(\delta)y = a_0 + a_1\omega_1 + \ldots + a_{q-1}\omega_{q-1}$, where $a_0, \ldots, a_{q-1} \in \bar{M}LE$ and

$$|\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(a_i)| < |N_{\bar{M}LE/\mathbb{Q}}(Cu^{2A})|.$$

On the other hand,

$$N_{MLE/\bar{M}LE}(\delta)y - N_{MLE/\bar{M}LE}(\delta)t = N_{MLE/\bar{M}LE}(\delta)CDu^{2A}\delta^{-2A}\mu.$$

Let $z \in O_{\bar{M}LE}$ be such that $z - N_{MLE/\bar{M}LE}(\delta)t = CDu^{2A}w, w \in O_{\bar{M}LE,W_{\bar{M}LE}}$. (Such a z exists by the strong approximation theorem.) Then

$$N_{MLE/\bar{M}LE}(\delta)y - z = CDu^{2A}v,$$

where $v \in O_{MLE,W_{MLE}}$. However, since $N_{MLE/\bar{M}LE}(\delta)y - z \in O_{MLE}, CDu^{2A} \in O_{MLE}$ and $\operatorname{ord}_{\mathfrak{t}} CDu^{2A} = 0$ for all $\mathfrak{t} \in W_{MLE}$, we conclude that $v \in O_{MLE}$. Thus,

$$\frac{a_0 - z + a_1\omega_1 + \ldots + a_{q-1}\omega_{q-1}}{CDu^{2A}} \in O_{MLE}.$$

Consequently, for $i = 1, \ldots, q-1$,

$$\frac{\mathcal{D}_{M/\bar{M}}a_i}{CDu^{2A}} \in O_{\bar{M}LE}$$

and

$$|\mathbf{N}_{\bar{M}LE/\mathbb{Q}}(\frac{a_i}{Cu^{2A}})| \geq 1$$

or $a_i = 0$. Clearly the first alternative is not true. Thus, $a_1, \ldots, a_{q-1}$ are all zero and $y \in \bar{M}LE \cap M = \bar{M}$.

5.3. **Lemma.** *Let $t \in M$. Then for any $l \in \mathbb{N}$ and $\mathfrak{t} \in W_M$,*

$$\operatorname{ord}_{\mathfrak{t}} F_E(Pt^{2e} + Pl) \leq 0.$$

Proof. First let $\mathfrak{t} \neq \mathfrak{p}$ be any other prime of W_M. Then powers of γ_E constitute a local integral basis of EM over M with respect to $\mathfrak{t}$, and $\mathfrak{t}$ does not split in the extension EM/M. Thus, if y is integral at $\mathfrak{t}$, $\operatorname{ord}_{\mathfrak{t}} F_E(y) = 0$. On the other hand, given our assumptions on $F_E(T)$, $\operatorname{ord}_{\mathfrak{t}} y < 0$ implies $\operatorname{ord}_{\mathfrak{t}} F_E(y) < 0$. Thus, for any $y \in M$, including $y = Pt^{2e} + Pl$ we have $\operatorname{ord}_{\mathfrak{t}} F_E(y) \leq 0$.

Next we consider the case of $\mathfrak{p}$. If t is integral at $\mathfrak{p}$, then $F_E(Pt^{2e} + Pl)$ is congruent to the free term of the polynomial mod $\mathfrak{p}$. Since $\mathfrak{p}$ does not divide any of the coefficients, in this case

$$F_E(Pt^{2e} + Pl) \not\cong 0 \mod \mathfrak{p}.$$

Suppose now that $\operatorname{ord}_{\mathfrak{p}} t < 0$. Then $\operatorname{ord}_{\mathfrak{p}} Pt^{2e} < 0$ and, since P does not divide any coefficients of $F_E(T)$, $\operatorname{ord}_{\mathfrak{p}} F_E(Pt^{2e} + Pl) < 0$.

6. Diophantine decidability and definability over $O_{K_{inf}, W_{K_{inf}}}$

6.1. **Proposition.** *The following sets are Diophantine over $O_{K_{inf}, W_{K_{inf}}}$.*

(1) $\{x \in O_{K_{inf}, W_{K_{inf}}} | x \neq 0\}$.
(2) $\{x \in O_{K_{inf}, W_{K_{inf}}} | \sigma(x) \geq 0$ *for all embeddings* $\sigma : K_{inf} \longrightarrow \mathbb{C}\}$.

Proof. The first statement follows by a slight adjustment of arguments in [7] and in [24]. Since by assumption $W_K \setminus \{\mathfrak{p}\}$ will contain only the primes not splitting in the extension EK/K, the complement of W_K contains at least two primes, $\mathfrak{p}_1$ and $\mathfrak{p}_2$. Let $a_i \cong 0 \mod \mathfrak{p}_i, a_i \in O_K$ for $i = 1, 2$, and $(a_1, a_2) = 1$. (Such $a_1, a_2 \in O_K$ exist by the strong approximation theorem. See [14], page 71.) Let $x \in O_{K_{inf}, W_{inf}}$. Then $x \neq 0$ if and only if the following equation has solutions in $O_{K_{inf}, W_{K_{inf}}}$:

$$xw = (u_1 a_1 - 1)(u_2 a_2 - 1).$$

Indeed, suppose that $x = 0$; then either a_1 or a_2 is invertible in $O_{K_{inf}, W_{K_{inf}}}$. This is not true by the choice of $\mathfrak{p}_1$ or $\mathfrak{p}_2$. Suppose now $x \neq 0$. Then let $M = K(x)$, and we can let $\frac{\mathfrak{A}_1 \mathfrak{A}_2}{\mathfrak{B}}$ be the divisor of x in M, where $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{B}$ are integral divisors, with $\mathfrak{A}_i$ and the divisor of a_i relatively prime. By the strong approximation theorem, there exists $u_i \in O_M$ such that $u_i \cong a_i^{-1} \mod \mathfrak{A}_i$. Thus, the divisor of $(u_1 a_1 - 1)(u_2 a_2 - 1)$ is of the form $\mathfrak{A}_1 \mathfrak{A}_2 \mathfrak{C}$, where $\mathfrak{C}$ is an integral divisor. Hence, the divisor of w is of the form $\mathfrak{B}\mathfrak{C}$, and consequently, $w \in O_M \subset O_{K_{inf}, W_{K_{inf}}}$.

The second claim of the lemma follows from an argument in [6].

6.2. **Proposition.** *Let K, K_{inf} be as in Section 2. Consider the following set of equations and inequalities, with all the variables ranging over $O_{K_{inf}, W_{K_{inf}}}$:*

$$\prod_{\phi} \sum_{k=0,1, s=0,\ldots,p-1} \bar{a}_{k,s} \gamma_L^k \phi(\gamma_E)^s = 1, \tag{6.1}$$

$$\prod_{\tau} \sum_{k=0,1, s=0,\ldots,p-1} \bar{a}_{k,s} \tau(\gamma_L)^k \gamma_E^s = 1, \tag{6.2}$$

$$\sum_{k=0,1,s=0,\dots,p-1} \bar{a}_{k,s}\gamma_L^k\gamma_E^s \neq \pm 1, \tag{6.3}$$

$$\prod_{\phi}\sum_{k=0,1,s=0,\dots,p-1} \bar{b}^{(i)}_{k,s}\gamma_L^k\phi(\gamma_E)^s = 1, i=0,\dots,2h_{KLE}ep, \tag{6.4}$$

$$\prod_{\tau}\sum_{k=0,1,s=0,\dots,p-1} \bar{b}^{(i)}_{k,s}\tau(\gamma_L)^k\gamma_E^s = 1, i=0,\dots,2h_{KLE}ep, \tag{6.5}$$

$$\sum_{k=0,1,s=0,\dots,p-1} \bar{b}^{(i)}_{k,s}\gamma_L^k\gamma_E^s \neq \pm 1, i=0,\dots,2h_{KLE}ep, \tag{6.6}$$

$$\prod_{\phi}\sum_{k=0,1,s=0,\dots,p-1} \bar{d}^{(i)}_{k,s}\gamma_L^k\phi(\gamma_E)^s = 1, i=0,\dots,2h_{KLE}ep, \tag{6.7}$$

$$\prod_{\tau}\sum_{k=0,1,s=0,\dots,p-1} \bar{d}^{(i)}_{k,s}\tau(\gamma_L)^k\gamma_E^s = 1, i=0,\dots,2h_{KLE}ep \tag{6.8}$$

$$\sum_{k=0,1,s=0,\dots,p-1} \bar{d}^{(i)}_{k,s}\gamma_L^k\gamma_E^s \neq \pm 1, i=0,\dots,2h_{KLE}ep, \tag{6.9}$$

where τ ranges over all the embeddings of L into $\mathbb{C}$, and ϕ ranges over all the embeddings of E into $\mathbb{C}$,

$$\sum_{k=0,1,s=0,\dots,p-1} a_{k,s}\gamma_L^k\gamma_E^s = \left(\sum_{k=0,1,s=0,\dots,p-1} \bar{a}_{k,s}\gamma_L^k\gamma_E^s\right)^{2h_{KLE}}, \tag{6.10}$$

$$\sum_{k=0,1,s=0,\dots,p-1} b^{(i)}_{k,s}\gamma_L^k\gamma_E^s = \left(\sum_{k=0,1,s=0,\dots,p-1} \bar{b}^{(i)}_{k,s}\gamma_L^k\gamma_E^s\right)^{2h_{KLE}}, i=0,\dots,2h_{KLE}ep, \tag{6.11}$$

$$\sum_{k=0,1,s=0,\dots,p-1} d^{(i)}_{k,s}\gamma_L^k\gamma_E^s = \left(\sum_{k=0,1,s=0,\dots,p-1} \bar{d}^{(i)}_{k,s}\gamma_L^k\gamma_E^s\right)^{2h_{KLE}}, \quad i=0,\dots,2h_{KLE}ep, \tag{6.12}$$

$$\begin{aligned}\sum_{k=0,1,s=0,\dots,p-1} & b^{(i)}_{k,s}\gamma_L^k\gamma_E^s - 1\\ &= \left(\sum_{k=0,1,s=0,\dots,p-1} a_{k,s}\gamma_L^k\gamma_E^s - 1\right)\left(\sum_{k=0,1,s=0,\dots,p-1} c^{(i)}_{k,s}\gamma_L^k\gamma_E^s\right),\\ & i=0,\dots,2h_{KLE}ep,\end{aligned} \tag{6.13}$$

$$\begin{aligned}\sum_{k=0,1,s=0,\dots,p-1} & d^{(i)}_{k,s}\gamma_L^k\gamma_E^s - 1\\ &= \left(\sum_{k=0,1,s=0,\dots,p-1} a_{k,s}\gamma_L^k\gamma_E^s - 1\right)\left(\sum_{k=0,1,s=0,\dots,p-1} f^{(i)}_{k,s}\gamma_L^k\gamma_E^s\right),\\ & i=0,\dots,2h_{KLE}ep,\end{aligned} \tag{6.14}$$

$$x_i - \left(\sum_{k=0,1,s=0,\ldots,p-1} c^{(i)}_{k,s}\gamma_L^k\gamma_E^s\right) = \left(\sum_{k=0,1,s=0,\ldots,p-1} a_{k,s}\gamma_L^k\gamma_E^s - 1\right)\left(\sum_{k=0,1,s=0,\ldots,p-1} w^{(i)}_{k,s}\gamma_L^k\gamma_E^s\right), \quad i = 0,\ldots,2h_{KLE}ep, \tag{6.15}$$

$$a_{0,0} - 1 = x_i^2\tilde{a}_{0,0}, a_{k,s} = x_i^2\tilde{a}_{k,s}, s = 0,\ldots,p-1, k = 0,1,(s,k) \neq (0,0), \tag{6.16}$$

$$x_i = F_E(Py + Pl_i), y_i = x_i^{h_{KLE}}, i = 0,\ldots,2h_{KLE}ep \tag{6.17}$$

$$|\sigma(y_i)| > 1, i = 0,\ldots,2h_{KLE}ep, \tag{6.18}$$

where σ is any embedding of K_{inf} into $\mathbb{C}$,

$$y_i - \sum_{k=0,1,s=0,\ldots,p-1} f^{(i)}_{k,s}\gamma_L^k\gamma_E^s = y_i^{2A}CD\sum_{k=0,1,s=0,\ldots,p-1} u^{(i)}_{k,s}\gamma_L^k\gamma_E^s. \tag{6.19}$$

If all of these equations are satisfied in $O_{K_{inf},W_{K_{inf}}}$, then $y \in O_{K,W_K}$. Conversely, if $y - c_F \in \mathbb{N}$, then these equations can be satisfied with all the other variables taking values in O_{K,W_K}.

Proof. Suppose all the equations are satisfied over $O_{K_{inf},W_{K_{inf}}}$. Let $\hat{M} \subset K_{inf}$ be the smallest overfield of K containing the values of the variables $\bar{a}_{k,s}, a_{k,s}, \bar{b}^{(i)}_{k,s}, b^{(i)}_{k,s}, \bar{d}^{(i)}_{k,s}, d^{(i)}_{k,s}, c^{(i)}_{k,s}, f^{(i)}_{k,s}, w^{(i)}_{k,s}$ for $k = 0,1, i = 0,\ldots,2eh_{KEL}p, s = 0.\ldots,p-1$. If $M = K(y) \neq K$, then let $\bar{M}$ be a subfield of M satisfying the conditions in Section 2. Since $([\hat{M} : \mathbb{Q}], p) = 1$, and L is a totally complex extension of $\mathbb{Q}$, the following equalities hold:

$$[KE : K] = [\hat{M}E : M] = [\hat{M}EL : \hat{M}L] = p,$$
$$[LK : K] = [\hat{M}L : \hat{M}] = [\hat{M}EL : E\hat{M}] = 2.$$

Thus, the conjugates of γ_E over $\mathbb{Q}$ and over $\hat{M}L$ are the same, and the conjugates of γ_L over $\mathbb{Q}$ and $\hat{M}E$ are the same. Next let

$$\bar{\nu} = \sum_{k=0,1,s=0,\ldots,p-1} \bar{a}_{k,s}\gamma_L^k\gamma_E^s, \tag{6.20}$$

$$\bar{\lambda}_i = \sum_{k=0,1,s=0,\ldots,p-1} \bar{b}^{(i)}_{k,s}\gamma_L^k\gamma_E^s = 1, i = 0,\ldots,2h_{KLE}ep, \tag{6.21}$$

$$\bar{\varepsilon}_i = \sum_{k=0,1,s=0,\ldots,p-1} \bar{d}^{(i)}_{k,s}\gamma_L^k\gamma_E^s = 1, i = 0,\ldots,2h_{KLE}ep. \tag{6.22}$$

Then $\bar{\nu}, \bar{\lambda}_i, \bar{\varepsilon}_i \in O_{\hat{M}LE, W_{\hat{M}LE}}$ for $i = 0, \ldots, 2h_{KLE}ep$, and we can rewrite (6.1)–(6.9) as the following equations:

$$\begin{gathered}
\mathbf{N}_{\hat{M}EL/L\hat{M}}(\bar{\nu}) = 1,\\
\mathbf{N}_{\hat{M}EL/E\hat{M}}(\bar{\nu}) = 1,\\
\bar{\nu} \neq \pm 1,\\
\mathbf{N}_{\hat{M}EL/L\hat{M}}(\bar{\lambda}_i) = 1, i = 0, \ldots, 2h_{KLE}ep,\\
\mathbf{N}_{\hat{M}EL/E\hat{M}}(\bar{\lambda}_i) = 1, i = 0, \ldots, 2h_{KLE}ep,\\
\bar{\lambda}_i \neq \pm 1, i = 0, \ldots, 2h_{KLE}ep,\\
\mathbf{N}_{\hat{M}EL/L\hat{M}}(\bar{\varepsilon}_i) = 1, i = 0, \ldots, 2h_{KLE}ep,\\
\mathbf{N}_{\hat{M}EL/E\hat{M}}(\bar{\varepsilon}_i) = 1, i = 0, \ldots, 2h_{KLE}ep,\\
\bar{\varepsilon}_i \neq \pm 1, i = 0, \ldots, 2h_{KLE}ep.
\end{gathered}$$

Next let

$$\begin{aligned}
\nu &= \sum_{k=0,1,s=0,\ldots,p-1} a_{k,s}\gamma_L^k\gamma_E^s,\\
\lambda_i &= \sum_{k=0,1,s=0,\ldots,p-1} b_{k,s}^{(i)}\gamma_L^k\gamma_E^s,\\
\varepsilon_i &= \sum_{k=0,1,s=0,\ldots,p-1} d_{k,s}^{(i)}\gamma_L^k\gamma_E^s.
\end{aligned}$$

Then, by (6.10) – (6.12), $\nu = \bar{\nu}^{2h_{KLE}}, \lambda_i = \bar{\lambda}_i^{2h_{KLE}}, \varepsilon_i = \bar{\varepsilon}_i^{2h_{KLE}}$ for $i = 0, \ldots, 2h_{KLE}ep$. By Lemma 3.1,

$$\nu, \lambda_i, \varepsilon_i \in KEL, i = 0, \ldots, 2h_{KLE}ep. \tag{6.23}$$

Since $\{\gamma_E^s\gamma_L^k, s = 0, \ldots, p-1, k = 0, 1\}$ is a basis of KEL over K, we can conclude that

$$\begin{aligned}
&\{a_{k,s}, b_{k,s}^{(i)}, d_{k,s}^{(i)}, s = 0, \ldots p-1, k = 0, 1, i = 0, \ldots, 2h_{KLE}ep\}\\
&\qquad \subset K \cap O_{\hat{M}, W_{\hat{M}}} = O_{K, W_K}.
\end{aligned}$$

From (6.13) and (6.14) it follows that

$$\sum_{k=0,1,s=0,\ldots,p-1} c_{k,s}^{(i)}\gamma_L^k\gamma_E^s = \frac{\lambda_i - 1}{\nu - 1}, i = 0, \ldots, 2h_{KLE}ep,$$

and

$$\sum_{k=0,1,s=0,\ldots,p-1} f_{k,s}^{(i)}\gamma_L^k\gamma_E^s = \frac{\varepsilon_i - 1}{\nu - 1}, i = 0, \ldots, 2h_{KLE}ep.$$

Using (6.23) again, we deduce that $\{c_{k,s}^{(i)}, f_{k,s}^{(i)}, s = 0, \ldots, p-1, k = 0, 1, i = 0, \ldots, 2h_{KLE}ep\} \subset O_{K,W_K}$. From (6.15) we conclude that

$$x_i - \sum_{k=0,1,s=0,\ldots,p-1} c_{k,s}^{(i)}\gamma_L^k\gamma_E^s = (\nu - 1)\left(\sum_{k=0,1,s=0,\ldots,p-1} w_{k,s}^{(i)}\gamma_L^k\gamma_E^s\right),$$
$$i = 0, \ldots, 2h_{KLE}ep,$$

while by (6.16), $x_i^2|(\nu-1)$ in $O_{MLE,W_{MLE}}$. Further, by Lemma 5.3, for all $\mathfrak{t} \in W_M$,

$$\operatorname{ord}_{\mathfrak{t}} F_E(Py^{2e} + Pl_i) = \operatorname{ord}_{\mathfrak{t}} x_i \leq 0.$$

Therefore by Lemma 5.1, $y_i = x_i^{h_{LKE}} = u_i\delta_i^{-1}$, where $u_i \in O_{KLE}$, $\delta_i \in O_{MLE}$ and all the primes in the divisor of δ_i are in W_{MLE}. From (6.19) we conclude that

$$y_i - f_{0,0}^{(i)} = CDy_i^{2A}u_{0,0}^{(i)}.$$

Thus, by Lemma 5.2, $y_i \in \bar{M}, i = 0, \ldots, 2eh_{LKE}p$. By Lemma 5.1 of [25] and the assumptions on $l_0, \ldots, l_{2eph_{KLE}}$, we can now deduce that $y \in O_{\bar{M},W_{\bar{M}}}$. Since $M = K(y)$ and $M/\bar{M}$ is a non-trivial extension unless $M = K$, we conclude that $y \in K$.

Conversely, suppose $y - c_F \in \mathbb{N}$. Then for all $i = 0, \ldots, 2eph_{EKL}$ we have $x_i = F_E(Py^{2e} + Pl_i), y_i = x_i^{h_{EKL}} \in \mathbb{N}$. Further, neither x_i nor y_i is divisible by any prime from W_K. Let $\xi \in O_{KEL,W_{KEL}}$ be a non-root of unity solution to the system (3.1). We know that such a solution exists by Lemma 3.1. Further, from Lemma 3.1, we know that the divisor of ξ consists of factors of $\mathfrak{p}$ only. By Lemma 2.6 in [25], we know that, for some $r \in \mathbb{N}$,

$$\xi^r - 1 \in O_{K,W_K}[x_i^{4h_{KLE}A}CD\gamma_L, x_i^{4h_{KLE}A}CD\gamma_E].$$

So let $\bar{\nu} = \xi^r$ and $\nu = \xi^{2rh_{KLE}}$. Assign O_{K,W_K}-values to $a_{k,s}, \bar{a}_{k,s}, \tilde{a}_{k,s}$ so that (6.20), (6.10), and (6.16) are satisfied. Then (6.1), (6.2) and (6.3) will also be satisfied.

Next set $\bar{\lambda}_i = \bar{\nu}^{x_i}$. Note that

$$\frac{\lambda_i - 1}{\nu - 1} \cong x_i \mod (\nu - 1) \text{ in } \mathbb{Z}[\nu] \subset O_{K,W_K}[\gamma_E, \gamma_L].$$

Assign the O_{K,W_K} values to $\bar{b}_{k,s}^{(i)}, b_{k,s}^{(i)}, c_{k,s}^{(i)}$ so that (6.21), (6.11) and (6.13) are satisfied. These assignments will imply that (6.4), (6.5) and (6.6) will also be satisfied. One can also find the O_{K,W_K} values for $w_{k,s}^{(i)}$ so that (6.15) is satisfied.

Finally, set $\bar{\varepsilon}_i = \bar{\nu}^{y_i}$. Assign the O_{K,W_K}-values to $\bar{d}_{k,s}^{(i)}, d_{k,s}^{(i)}, f_{k,s}^{(i)}$ so that (6.22), (6.12), and (6.14) are satisfied. Then (6.7), (6.8), and (6.9) are also satisfied. Note further that

$$\frac{\varepsilon_i - 1}{\nu - 1} \cong y_i \mod (\nu - 1) \text{ in } \mathbb{Z}[\nu] \subset O_{K,W_K}[\gamma_E, \gamma_K],$$

and

$$\nu - 1 \cong 0 \mod y_i^{2A}CD.$$

Thus,

$$\frac{\varepsilon_i - 1}{\nu - 1} \cong y_i \mod y_i^{2A}CD \text{ in } O_{K,W_K}[\gamma_E, \gamma_K].$$

Therefore, for some values in O_{K,W_K} for $u_{k,s}^{(i)}$, (6.19) is satisfied.

6.3. **Corollary.** *O_{K,W_K} has a Diophantine definition over $O_{K_{inf},W_{K_{inf}}}$.*

Proof. Consider (6.1)–(6.19). Observe that by Lemma 6.1, all these equations and inequalities can be rewritten as polynomial equations and inequalities over $O_{K_{inf},W_{inf}}$. Now, it is not hard to see that, using a basis of K over $\mathbb{Q}$, one can use these equations and inequalities to construct a Diophantine definition of O_{K,W_K} over $O_{K_{inf},W_{K_{inf}}}$.

Finally, the existence of $l_0, \ldots, l_{2eph_{KLE}}$ follows from Lemma 8.1 of the Appendix.

To complete the proof of Theorem 1.9, we need to show that all the assumptions in Section 2 follow from the assumptions of Theorem 1.9. This is done in the propositions below.

6.4. **Lemma.** *Let G be any totally real field, algebraic over $\mathbb{Q}$. Let $K \subset \mathbb{Q}$ be a number field such that there exists a natural number A with the following property. For every number field M with $G \supset M \supset K$ there exists a non-trivial subfield $\bar{M}$ satisfying the following conditions.*

(1) *$[M : \bar{M}] \leq A$.*
(2) *For some basis $\Omega_{M/\bar{M}}$ of M over $\bar{M}$ with $\{1\} \subset \Omega_{M/\bar{M}} \subset O_M$, for all $\omega \in \Omega_{M/\bar{M}}$ and every σ – embedding of M into $\mathbb{C}$ we have $|\sigma(\omega)| \leq A$.*

Then there exists a natural number D_G such that for any choice of M, for some $\bar{M}$, D_G is greater than any conjugate of the discriminant $\mathcal{D}_{M/\bar{M}}$ of $\Omega_{M/\bar{M}}$ over $\mathbb{Q}$.

Proof. Note that for any embedding σ of M into $\mathbb{C}$,

$$|\sigma(\mathcal{D}_{M/\bar{M}})| = \left| \prod_{1 \leq i < j \leq [M:\bar{M}]} (\sigma(\omega_i) - \sigma(\omega_j))^2 \right| < (2A)^{A(A-1)}.$$

Thus the constant D described in Section 2 exists.

Next we address the issue of the existence of L.

6.5. **Lemma.** *Let G be any totally real field, algebraic and normal over $\mathbb{Q}$, such that there exists a rational prime P having only finitely many factors in G. Let $T > 2$ be a rational prime. Let B_T be a set of primes equivalent to 1 modulo T. Then for all but finitely many primes q in B_T we have $[G \cap \mathbb{Q}(\xi_q) : \mathbb{Q}] < \frac{q-1}{2}$, where ξ_q is a q-th primitive root of unity.*

Proof. Assume the opposite. Then for infinitely many $q \cong 1 \mod T$ we have $[G \cap \mathbb{Q}(\xi_q) : \mathbb{Q}] = \frac{q-1}{2}$. Therefore, G contains infinitely many linearly disjoint over $\mathbb{Q}$ finite cyclic subextensions of degree T. Hence G contains subfields whose Galois group over $\mathbb{Q}$ is congruent to $(\mathbb{Z}/T)^r$, where r is arbitrarily large. But in a number field with such a Galois group every prime has at least T^{r-1} factors. Thus the number of factors for any rational prime is not bounded in G.

6.6. **Corollary.** *Let G be as above. Then there exists a totally complex field L of degree 2 over $\mathbb{Q}$ such that LG contains no complex roots of unity, L is generated by $\gamma_L \in O_L$ over $\mathbb{Q}$ with $\operatorname{ord}_{P_i} \gamma_L = 0$ for all factors P_i of P in LG, and P splits completely in $L/\mathbb{Q}$.*

Proof. Let q be a rational prime such that $G \cap \mathbb{Q}(\xi_q)$ is of degree less than $\frac{q-1}{2}$ over $\mathbb{Q}$, q is not ramified in the extension $K_{inf}/\mathbb{Q}$, and $-q \neq \pm P$ is a square modulo P. (Such a q exists by Lemma 6.5. Indeed, let T be any prime greater than P. Let B_T contain all the primes equivalent to 1 modulo T and congruent to minus a square modulo P. Since any arithmetic progression contains infinitely many primes, B_T will be an infinite set.) Then let $L = \mathbb{Q}(\sqrt{-q})$. Note that P will split in the extension $L/\mathbb{Q}$. Further, suppose GL contains ξ_t, for some prime number $t > 2$. Then $G(\xi_t) \subseteq GL$. But since ξ_t is of degree at least 2 over G, $G(\xi_t) = LG$. Thus in the extension GL/G, only some factor of t can be ramified. But q is ramified in the extension LG/G. Therefore $t = q$. Further we note that G is the largest subfield of $LG = G(\xi_q)$ fixed under complex conjugation. Therefore, $\mathbb{Q}(\cos(2\pi/q)) \subset G$. But the last inclusion implies that $G \cap \mathbb{Q}(\xi_q)$ is of degree greater than or equal to $\frac{q-1}{2}$ over $\mathbb{Q}$. Hence, $\xi_t \notin GL$ for any prime $t > 2$.

The last corollary completes the proof Theorem 1.9. Next we complete the proof of Corollary 1.10.

6.7. **Lemma.** *Let G be an algebraic extension of $\mathbb{Q}$. Assume further that every rational prime has a finite number of factors in G. Then for every rational prime p there exist a number field U and a U-prime P_U such that P_U has only one factor in G and P, the rational prime below P_U, splits completely in the extension $E/\mathbb{Q}$ for some totally real cyclic number field E of degree p over $\mathbb{Q}$. Further, E is generated over $\mathbb{Q}$ by $\gamma_E \in O_E$ such that P does not divide the discriminant or the coefficients of the monic irreducible polynomial of γ_E over $\mathbb{Q}$.*

Proof. Let p be fixed. Let P be a rational prime splitting completely in the extension $E/\mathbb{Q}$, where E is a totally real cyclic extension of degree p. Assume further that E is generated by γ_E with properties described in the statement of the lemma. (Since there are infinitely many rational primes P splitting in the extension $E/\mathbb{Q}$, we can always find a P not dividing the coefficients or the discriminant of a monic irreducible polynomial of a generator of E over $\mathbb{Q}$.) Since P has only finitely many factors in G, there exists a number field $U \subset G$ where the number of factors of P is the same as the number of factors of P in G. Let P_U be one of the factors of P in U. Then P_U and U satisfy the requirements of the lemma.

Note that if G does not contain a number field whose degree over $\mathbb{Q}$ is divisible by p, then by Lemma 8.2, the factor of P_U in any overfield M of U in G will split completely in the extension ME/M.

To complete the proof of Corollary 1.10, we observe the following. Let $\varepsilon > 0$ be given. Then we can choose $p > 2\varepsilon^{-1}$ such that for any number field $M \subset K_{inf}$ we have $[M : \mathbb{Q}] \not\equiv 0 \mod p$. Further, we can choose a number field $U \subset K_{inf}$ to be of degree greater than $2\varepsilon^{-1}$ over $\mathbb{Q}$, to contain a prime P_U with only one K_{inf}-factor, and splitting completely in the extension EU/U, where E is a totally real cyclic extension of degree p over $\mathbb{Q}$. Let W_U be any set of primes containing P_U and such that all the primes in $W_U \setminus P_U$ do not split in the extension EU/U and are not zeros of the discriminant or coefficients of $F_E(T)$. Then by Theorem 1.9, O_{U,W_U} has a Diophantine definition in its integral closure in K_{inf}. Using Theorem 2.4 of [28] and an argument similar to the one used to prove Theorem 2.7 and Corollary 2.8 of [28], one can show that we can select W_U as above to be of Dirichlet density greater than $1-[U:\mathbb{Q}]^{-1}-1/p > 1-\varepsilon$ and such that $\mathbb{Z}$ has a Diophantine definition over O_{U,W_U}. Thus, the integral closure of O_{U,W_U} in K_{inf} will have a Diophantine definition of $\mathbb{Z}$, and the density condition on W_U will be satisfied.

7. Examples of K_{inf}: Totally real subfields of cyclotomics

Let $C = \{q_1, \ldots, q_r\}$ be a finite set of distinct rational prime numbers greater than 2. Let G be the largest totally real subfield of the cyclotomic extension generated by q_i^j-th roots of unity as $j \to \infty, i = 1, \ldots, r$. We claim that G satisfies the condition of Corollary 1.10.

First of all we note that by Lemma 5.3 of [27], every rational prime will have only finitely many factors in K_{inf}. Secondly, the only rational primes ramified in K_{inf} are $q_1, \ldots, q_r$. Thirdly, G is a normal extension of $\mathbb{Q}$ and for every pair of number fields K, M with $K \subset M \subset G$ and K containing $\mathbb{Q}(\cos(2\pi/q_i)), i = 1, \ldots, r$, the extension M/K is cyclic of degree $\prod q_i^{a_i}, a_i \in \mathbb{N}$, and will have a subextension $\bar{M} \supset K$ of prime degree less than or equal to $\max_i\{q_i\}$. Further, M will be generated over $\bar{M}$ by a basis of the form $\{1, \cos(2\pi/q_i^{b_i}), \ldots, \cos(2\pi/q_i^{b_i})^{[M:\bar{M}]-1}\}$. Finally, for any number field $M \subset G$, $[M : \mathbb{Q}]$ can be divisible by $q_1, \ldots, q_r$ and primes dividing $q_1 - 1, \ldots, q_r - 1$ only.

8. Appendix

8.1. **Lemma.** *Let K be a real number field. Let $F(T) \in K[T]$ be a polynomial of degree $n > 0$. Then there exist $l_0 = 0, \ldots, l_n \in \mathbb{N}$ such that the polynomials $F(T + l_i), i = 0, \ldots, l_n$, are linearly independent over $\mathbb{R}$.*

Proof. Let $F(T) = a_0 + a_1T + \ldots a_nT^n$. Then for $l \in \mathbb{N}$,

$$F(T + l) = a_0 + a_1(T + l) + \ldots + a_n(T + l)^n$$

$$= a_0 + a_1(T + l) + \ldots + a_i\left(\sum_{j=0}^{i}\left(\begin{array}{c} i \\ j \end{array}\right)T^jl^{i-j}\right) + \ldots + a_n\left(\sum_{j=0}^{n}\left(\begin{array}{c} n \\ j \end{array}\right)T^jl^{n-j}\right)$$

$$= \sum_{j=0}^{n} a_jl^j + \ldots + \left(\sum_{j=k}^{n}\left(\begin{array}{c} j \\ k \end{array}\right)a_jl^{j-k}\right)T^k + \ldots + a_nT^n$$

$$= P_n(l) + P_{n-1}(l)T + \ldots P_0(l)T^n, \tag{8.1}$$

where $P_i(l) \in K[l]$ is a polynomial of degree i in l. Let $F_k(T+l) = \sum_{j=0}^{k} P_j(l)T^{n-j}$. Suppose now that we found $l_0, \ldots, l_k, k < n$, such that

$$F_k(T), F_k(T + l_1), \ldots, F_k(T + l_k)$$

are linearly independent over $\mathbb{R}$ but, for any $l \in \mathbb{N}$,

$$F_{k+1}(T + l) = \sum_{i=0}^{k} A_iF_{k+1}(T + l_i), \quad A_i(l) = A_i \in \mathbb{R}.$$

Thus, we have a linear system

$$P_j(l) = \sum_{i=0}^{k} A_iP_j(l_i), j = 0, \ldots, k + 1. \tag{8.2}$$

We can solve the first $k + 1$ equations simultaneously for A_i using Cramer's rule. Thus,

$$A_i = \frac{\sum_{j=0}^{k} b_jP_j(l)}{\det(P_j(l_i))},$$

where $\det(P_j(l_i)), j = 0, \ldots, k, i = 0, \ldots, k$, is not zero by the induction hypothesis, and $b_j \in \mathbb{R}$. Therefore, for each $i = 0, \ldots, k, A_i = A_i(l)$ is a fixed polynomial in l of degree at most k. Next consider equation number $k + 2$ of system (8.2):

$$P_{k+1}(l) = \sum_{i=0}^{k} A_i(l)P_{k+1}(l_i).$$

Note that on the left we have a polynomial in l of degree $k + 1$ and on the right a polynomial of degree at most k. Thus, the equality will not hold for sufficiently large l.

8.2. **Lemma.** *Let $M/K, F/K$ be number field extensions. Let $\mathfrak{p}$ be a prime splitting completely in the extension F/K. Assume further that F/K is generated by $\gamma_F \in O_K$ such that $\mathfrak{p}$ is not a zero of the discriminant of γ_F. Suppose that $[FM : M] = [F : K]$. Then any factor of $\mathfrak{p}$ will split completely in the extension FM/M.*

Proof. Let $H_F(T)$ be the monic irreducible polynomial of γ_F over K. Since

$$[FM : M] = [F : K],$$

$H_F(T)$ is also the monic irreducible polynomial of γ_F over M. By assumption, the power basis of γ_F is an integral basis with respect to $\mathfrak{p}$. Thus $\mathfrak{p}$ splitting completely in the extension F/K is equivalent to $H_F(T)$ factoring completely modulo $\mathfrak{p}$. If $\mathfrak{p}_M$ is a factor of $\mathfrak{p}$ in M, then the power basis of γ_F is an integral basis with respect to $\mathfrak{p}_M$ for the extension MF/M. Since the residue field of $\mathfrak{p}_M$ is an extension of the residue field of $\mathfrak{p}$, $H_F(T)$ will factor completely modulo $\mathfrak{p}_M$. Thus, $\mathfrak{p}_M$ will split completely in the extension MF/M.

References

[1] Jean-Louis Colliot-Thélène, Alexei Skorobogatov, and Peter Swinnerton-Dyer. Double fibres and double covers: Paucity of rational points. *Acta Arithmetica*, 79:113–135, 1997. MR **98a:**11081

[2] Gunther Cornelissen and Karim Zahidi. Topology of diophantine sets: Remarks on Mazur's conjectures. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 253–260. American Mathematical Society, 2000. MR **2001m:**11217

[3] Martin Davis. Hilbert's tenth problem is unsolvable. *American Mathematical Monthly*, 80:233–269, 1973. MR **47:**6465

[4] Martin Davis, Yurii Matijasevich, and Julia Robinson. Hilbert's tenth problem: Diophantine approximation. Positive aspects of a negative solution. In *Proc. Sympos. Pure Math.*, volume 28, pages 323– 378. Amer. Math. Soc., 1976. MR **55:**5522

[5] Jan Denef. Hilbert's tenth problem for quadratic rings. *Proc. Amer. Math. Soc.*, 48:214–220, 1975. MR **50:**12961

[6] Jan Denef. Diophantine sets of algebraic integers, II. *Transactions of American Mathematical Society*, 257(1):227–236, 1980. MR **81b:**12031

[7] Jan Denef and Leonard Lipshitz. Diophantine sets over some rings of algebraic integers. *Journal of London Mathematical Society*, 18(2):385–391, 1978. MR **80a:**12030

[8] Barry Green, Florian Pop, and Peter Roquette. On Rumely's local-global principle. *Jahresber. Deutsch. Math.-Verein.*, 97(2):43–74, 1996. MR **96g:**11065

[9] Moshe Jarden and Aharon Razon. Rumely's local-global principle for algebraic P$\mathcal{S}$C fields over rings. *Transactions of American Mathematical Society*, 350(1):55–85, 1998. MR **98d:**11142

[10] Barry Mazur. The topology of rational points. *Experimental Mathematics*, 1(1):35–45, 1992. MR **93j:**14020

[11] Barry Mazur. Questions of decidability and undecidability in number theory. *Journal of Symbolic Logic*, 59(2):353–371, 1994. MR **96c:**03091

[12] Barry Mazur. Speculation about the topology of rational points: An update. *Asterisque*, 228:165–181, 1995. MR **96c:**11068

[13] Barry Mazur. Open problems regarding rational points on curves and varieties. In A. J. Scholl and R. L. Taylor, editors, *Galois Representations in Arithmetic Algebraic Geometry.* Cambridge University Press, 1998, pp. 239–265. MR **2001g:**14031

[14] O. T. O'Meara. *Introduction to Quadratic Forms*. Springer Verlag, Berlin, 1973. MR **2000m:**11032 (reprint)

[15] Thanases Pheidas. Hilbert's tenth problem for a class of rings of algebraic integers. *Proceedings of American Mathematical Society*, 104(2):611–620, 1988. MR **90b:**12002

[16] Thanases Pheidas. An effort to prove that the existential theory of $\mathbb{Q}$ is undecidable. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 237–252. American Mathematical Society, 2000. MR **2001m:**03085

[17] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. To appear.

[18] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers. In C. Fieker and D. Kohel, editors, *Algorithmic Number Theory*, volume 2369 of *Lecture Notes in Computer Science*, pages 33–42. Springer Verlag, 2002.

[19] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949. MR **11:**151f

[20] Julia Robinson. The undecidability of algebraic fields and rings. *Proceedings of the American Mathematical Society*, 10:950–957, 1959. MR **22:**3691

[21] Robert S. Rumely. Arithmetic over the ring of all algebraic integers. *J. Reine Angew. Math.*, 368:127–133, 1986. MR **87i:**11041

[22] Harold Shapiro and Alexandra Shlapentokh. Diophantine relations between algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:1113–1122, 1989. MR **92b:**11018

[23] Alexandra Shlapentokh. Extension of Hilbert's tenth problem to some algebraic number fields. *Communications on Pure and Applied Mathematics*, XLII:939–962, 1989. MR **91g:**11155

[24] Alexandra Shlapentokh. Diophantine classes of holomorphy rings of global fields. *Journal of Algebra*, 169(1):139–175, 1994. MR **95h:**12007

[25] Alexandra Shlapentokh. Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator. *Inventiones Mathematicae*, 129:489–507, 1997. MR **98h:**11163

[26] Alexandra Shlapentokh. Defining integrality at prime sets of high density in number fields. *Duke Mathematical Journal*, 101(1):117–134, 2000. MR **2001a:**11200

[27] Alexandra Shlapentokh. Hilbert's tenth problem over number fields, a survey. In Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 107–137. American Mathematical Society, 2000. MR **2001m:**03023

[28] Alexandra Shlapentokh. On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2. *Journal of Number Theory*, 95:227–252, 2002. MR **2003h:**03068

[29] Alexandra Shlapentokh. A ring version of Mazur's conjecture on topology of rational points. *International Mathematics Research Notices*, 2003:7:411–423, 2003.

Department of Mathematics, East Carolina University, Greenville, North Carolina 27858

E-mail address: `shlapentokha@mail.ecu.edu`