Elliptic Curves Retaining Their Rank in Finite Extensions and Hilbert's Tenth Problem for Rings of Algebraic Numbers.

Alexandra Shlapentokh*
Department of Mathematics
East Carolina University
Greenville, NC 27858
shlapentokha@ecu.edu

April 17, 2006

Abstract

Using Poonen's version of "weak vertical method" we produce new examples of "large" and "small" rings of algebraic numbers (including rings of integers) where $\mathbb{Z}$ and/or the ring of integers of a subfield are existentially definable and/or where the ring version of Mazur's conjecture on topology of rational points does not hold.

1 Introduction

The interest in the questions of existential definability and decidability over rings goes back to a question that 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 [5] and [6].) 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? 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 $t \in R$,

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

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 relation. (See [6] for more details.)

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

*The research for this paper has been partially supported by NSF grants DMS-9988620 and DMS-0354907.

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.

Using norm equations, 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 degree 2 extensions of the finite degree totally real fields. Thanases Pheidas and the author of this paper 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 [7], [9], [8], [15], [23], and [24].

Using elliptic curves Bjorn Poonen has shown the following in [17].

1.3 Theorem.

Let M/K be a number field extension with an elliptic curve E defined over K, of rank one over K, such that the rank of E over M is also one. Then O_K (the ring of integers of K) is Diophantine over O_M.

In a recent paper (see [3]), Cornelissen, Pheidas and Zahidi weakened somewhat assumptions of Poonen's theorem. Instead of requiring a rank 1 curve retaining its rank in the extension, they require existence of a rank 1 elliptic curve over the bigger field and an abelian variety over the smaller field retaining its rank in the extension.

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, Mazur's conjectures tell us that this might not be the way to proceed. These conjectures state the following.

1.4 Conjecture.

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components. ([13][Conjecture 2, page 256.])

Conjecture 1.4 implies the following conjecture.

1.5 Conjecture.

$\mathbb{Z}$ does not have a Diophantine definition over $\mathbb{Q}$.

These conjectures are a part of a series of conjectures that can be found in [10], [11], [12] and [13]. 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 [2]. At the moment the resolution of either Conjecture 1.4 or Conjecture 1.5 seems to be out of reach.

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

Let $\mathcal{W}$ be a recursive set of rational primes. Let

$$O_{\mathbb{Q},\mathcal{W}} = \{x \in \mathbb{Q} \mid x = \frac{a}{b}, a, b \in \mathbb{N}, \forall p \notin \mathcal{W}, p \nmid b\}.$$

Then we can ask whether HTP is decidable for $O_{\mathbb{Q},\mathcal{W}}$ or whether $\mathbb{Z}$ has a Diophantine definition over $O_{\mathbb{Q},\mathcal{W}}$. We can answer these questions for *finite* $\mathcal{W}$ (see Proposition 2.1). More precisely, we know that for finite $\mathcal{W}$, rational integers do have a Diophantine definition over $O_{\mathbb{Q},\mathcal{W}}$ and therefore HTP is undecidable over $O_{\mathbb{Q},\mathcal{W}}$. (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 [20], [21] and [25] for more details.) Unfortunately, we have been unsuccessful in obtaining such definability results for infinite $\mathcal{W}$. On the other hand, we have been more successful in solving the analogous problem in some extensions of $\mathbb{Q}$. Before we state these results, we need a definition.

1.6 Definition.

Let M be a number field and let $\mathcal{W}$ be a set of its primes. Then a ring

$$O_{M,\mathcal{W}} = \{x \in M \mid \mathrm{ord}_{\mathfrak{p}} x \geq 0 \, \forall \mathfrak{p} \notin \mathcal{W}\}$$

is called a ring of $\mathcal{W}$-*integers* . (The term $\mathcal{W}$-integers usually presupposes that $\mathcal{W}$ is finite, but we will use this term for infinite $\mathcal{W}$ also.)

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

1.7 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 $\mathcal{W}$ 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 $O_{K,\mathcal{W}}$. (Thus, Hilbert's Tenth Problem is undecidable over $O_{K,\mathcal{W}}$.)

The proof of this theorem can be found in [26], [29] and [27].

As an alternative to a Diophantine definition of $\mathbb{Z}$ over a ring whose Diophantine status is unknown, one might consider a more general approach: a construction of a Diophantine models of $\mathbb{Z}$. (See [4] or [30] for a definition of a Diophantine model). We should note however, that Conjecture 1.4 also implies that $\mathbb{Q}$ has no Diophantine model of $\mathbb{Z}$. (See [4] for the proof of this assertion.) On the other hand, since the consideration of (generalized) rings of S-integers has produced some definability results, it is reasonable to hope for similar outcomes for Conjecture 1.4 and Diophantine models over some such rings. (Of course, Conjecture 1.4 has to be restated for rings. This is done in [30].) Indeed, following through on some ideas from [4] and [30], in [18], Poonen proved the following.

1.8 Theorem

There exists a set $\mathcal{W}$ of primes of $\mathbb{Q}$ of natural density 1 such that the following statements are true for the ring $R = O_{\mathbb{Q},\mathcal{W}}$.

1. R is a recursive ring.
2. R has a Diophantine model of $\mathbb{Q}$.
3. HTP is not decidable over R.
4. The ring version of Conjecture 1.4 does not hold over R.

Thus for the first time we have gained some insight into what the Diophantine status of $\mathbb{Q}$ might be. Using similar methodology one is able to obtain similar results for all number fields having a rank one elliptic curve. (This construction was carried out by Poonen and the author in [19].)

In this paper we combine the methods of [17] and [29] to obtain the following results.

1.9 Theorem

Let K/F be a number field extension of degree $s > 1$. Let E be an elliptic curve defined over F such that the rank of $E(K)$ is positive and the same as the rank of $E(F)$. Then the following statements are true.

1. *For any $\varepsilon > 0$ there exists set of K-primes of natural density greater than $1 - \varepsilon$ such that $O_{K,\mathcal{W}_K} \cap F$ has a Diophantine definition over $O_{K,\mathcal{W}_K}$. (See Theorem 6.2.)*
2. *Let $\mathcal{S}_K$ be a finite set of primes of K. Then $O_{K,\mathcal{S}_K} \cap F$ has a Diophantine definition over $O_{K,\mathcal{S}_K}$. If F is a totally real field (including $\mathbb{Q}$), an extension of degree 2 of a totally real field or a field with exactly one pair of complex conjugate embeddings, then HTP is undecidable over $O_{K,\mathcal{S}_K}$. (See Corollary 6.3.)*
3. *The ring of integers O_F of F has a Diophantine definition over O_K – the ring of integers of K. If F is a totally real field (including $\mathbb{Q}$), an extension of degree 2 of a totally real field or a field with exactly one pair of complex conjugate embeddings, then HTP is undecidable over O_K. (See Corollary 6.4.)*
4. *For any $\varepsilon > 0$ there exists a set $\mathcal{V}_K$ of K-primes of natural density greater than $1 - \frac{1}{s} - \varepsilon$ such that O_F and O_K have Diophantine definitions over $O_{K,\mathcal{V}_K}$. If F is a totally real field (including $\mathbb{Q}$), a totally complex extension of degree 2 of a totally real field or a field with exactly one pair of complex conjugate embeddings, then HTP is undecidable over $O_{K,\mathcal{V}_K}$.(See Theorem 6.5.)*
5. *Assume that F is either a totally real field (including $\mathbb{Q}$) or a totally complex extension of degree 2 of a totally real field. Then for any $\varepsilon > 0$ there exists a set $\mathcal{W}_K$ of K-primes of natural density greater than $1 - \varepsilon$ such that for some variety V defined over K, we have that $\overline{V(O_{K,\mathcal{W}_K})}$ (the closure of $V(O_{K,\mathcal{W}_K})$ in the usual archimedean topology in $\mathbb{R}$ if K is real, and $\mathbb{C}$, if K is not real) has infinitely many components.(See Theorem 6.6.)*

We should note here that Part 3 of the theorem was proved independently by Bjorn Poonen and he has generously provided his unpublished notes to the author (see [16]). Also a special case of Part 3, namely the case when $E(F)$ and $E(K)$ are both of rank one over $\mathrm{End}_F(E)$, was solved by a group of students at the 2003 Arizona Winter School. (See [1] for more details.)

2 Preliminary Results and Notation.

In this section we state two technical propositions which will be used in the proofs and describe notation and assumptions to be used in Sections 3 – 5. We start with the proposition which has been mentioned already in the discussion of definability of integrality at finitely many primes.

2.1 Proposition.

Let K be a number field. Let $\mathcal{W}_K$ be any set of primes of K. Let $\mathcal{S}_K \subseteq \mathcal{W}_K$ be a finite set. Let $\mathcal{V}_K = \mathcal{W}_K \backslash \mathcal{S}_K$. Then $O_{K,\mathcal{V}_K}$ has a Diophantine definition over $O_{K,\mathcal{W}_K}$. (See, for example, [25].)

Next we state another proposition which is also quite important for the proofs in this paper.

2.2 Proposition.

Let K be a number field. Let $\mathcal{W}_K$ be any set of primes of K. Then the set of non-zero elements of $O_{K,\mathcal{W}_K}$ has a Diophantine definition over $O_{K,\mathcal{W}_K}$. (See, for example, [25].)

This proposition allows us to use variables which take values in K while we are "officially" working with variables taking values in $O_{K,\mathcal{W}_K}$. We write these K-variables as ratios of variables in $O_{K,\mathcal{W}_K}$ with the proviso that the denominator is not zero.

2.3 Notation.

- Let K/F be a finite extension of number fields of degree $s > 1$.
- Let $n = [K : \mathbb{Q}]$.
- Let h be the least common multiple of the class numbers of K and F.
- Let $\{1, \phi, \ldots, \phi^{s-1}\} \in O_K$ be a basis of K over F.
- Let $D \in F$ be the discriminant of the basis.
- Let E denote an elliptic curve over F – i.e. a non-singular curve whose affine part is given by a fixed equation of the form $y^2 + cx + d = x^3 + ax + b$, where $a, b, c, d \in O_F$. We will also assume that rank of E is positive, and over F it is the same as over K.
- Let $i = [E(K) : E(F)]$.
- For an infinite order point $Q \in E(K)$ let $(x(Q), y(Q))$ be the affine coordinates of Q given by the Weierstrass equation above.
- Let $M_1, \ldots, M_{n+1}$ be pairwise linearly disjoint over K extensions of K of distinct degrees $m_1, \ldots, m_{n+1}$. Let $H_1(T), \ldots, H_{n+1}(T) \in O_K[T]$ be the monic irreducible polynomials of some integral generators $\gamma_1, \ldots, \gamma_{n+1}$ of $M_1, \ldots, M_{n+1}$ over K respectively.
- Let $m = \prod_{i=1}^{n+1} m_i!$.
- Let $\mathcal{W}_K$ be a set of primes of K. Let $\bar{\mathcal{W}}_K$ be the closure of $\mathcal{W}_K$ under conjugation over F, augmented by all the primes ramifying in the extension K/F and their conjugates.
- Let $\bar{H}_i(x) = H_i(x^b + \frac{1}{a})$, where a, b are positive integers defined in Lemma 4.3.
- Let $t \in K$. Then let $\mathfrak{d}(t) = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, where the product is taken over all the primes $\mathfrak{p}$ of K not in $\mathcal{W}_K$ such that $-a(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}} t < 0$. Let $\bar{\mathfrak{d}}(t) = \prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, where the product is taken over all the primes $\mathfrak{p}$ of K not in $\bar{\mathcal{W}}_K$ such that $-a(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}} t < 0$. Further, let $\mathfrak{n}(t) = \mathfrak{d}(t^{-1})$, $\bar{\mathfrak{n}}(t) = \bar{\mathfrak{d}}(t^{-1})$.
- Let r be a positive integer defined in Lemma 3.3.
- Let $c > 0$ be the constant defined in Lemma 4.4. Let $n_c > c$ be a natural number.
- Let $c' > 0$ be the constant defined in Lemma 3.3. Let $n_{c'} > \frac{1}{c'}$ be a natural number not divisible by any prime of $\bar{\mathcal{W}}_K$.

The set $\mathcal{W}_K$ will satisfy the following assumption.

2.4 Assumption.

All but finitely many primes of $\bar{\mathcal{W}}_K$ have no factor of relative degree 1 in any of the the extensions $M_1/K, \ldots, M_{n+1}/K$.

3 Properties of Elliptic Curves

In this section we go over some properties of elliptic curves necessary for our construction.

3.1 Lemma.

Let $P \in E(K)$ (or $P \in E(F)$) and let $\mathfrak{p}$ be a K-prime (resp. F-prime) such that $\mathrm{ord}_{\mathfrak{p}} x(P) < 0$. Then $2 \Big| \mathrm{ord}_{\mathfrak{p}} x(P)$.

Proof.

This follows from considering the Weierstrass equation.

3.2 Lemma.

If $I \subset O_K$ is a nonzero ideal not divisible by any primes of $\mathcal{W}_K$, then there exists a non-zero multiple $[l]P$ of P such that $I \Big| \mathfrak{d}(x([l]P))$.

Proof.

This lemma follows immediately from Lemma 10 of [17] even though we no longer assume that the curve is of rank 1. The proof is unaffected by this change.

3.3 Lemma.

There exists a positive integer r such that for any positive integers l, k,

$$\mathfrak{d}(x([lr]P) \Big| \mathfrak{n}(\frac{x[lr](P)}{x([klr]P)} - k^2)^2.$$

Proof.

Let r be a positive integer defined in Lemma 8 of [17]. Then the statement above follows immediately from Lemma 11 of [17]. The proof is again unaffected by the fact that we no longer assume E to be of rank 1.

3.4 Lemma.

Let r be as in Lemma 3.3. Let $Q', Q \in [r]E(K) \setminus \{O\}, Q' = [k]Q$. Then $\mathfrak{d}(x(Q)) \big| \mathfrak{d}(x(Q'))$.

Proof.

See Lemma 9 of [17].

3.5 Lemma.

Let Q, Q' be as in Lemma 3.4. Then

$$x(Q)^h = \frac{a}{b}, a, b \in O_K, (a, b) = 1 \tag{3.1}$$

$$\left(\frac{x(Q)}{x(Q')}\right)^h = \frac{c}{d}, c, d \in O_K, (c, d) = 1 \tag{3.2}$$

and $\mathfrak{n}(b)$ and $\mathfrak{n}(d)$ do not have any common factors.

Proof.

Existence of a, b, c, d satisfying Equations (3.1) and (3.2) follows from the definition of the class number. Similarly, we can let $x(Q')^h = \frac{a'}{b'}, a', b' \in O_K, (a', b') = 1$. Next we observe

$$\mathfrak{n}(b) = \mathfrak{d}(x(Q))^h, \mathfrak{n}(b') = \mathfrak{d}(x(Q'))^h,$$

and by Lemma 3.4 we have that $\mathfrak{n}(b)|\mathfrak{n}(b')$. Therefore, $\mathfrak{d}(\frac{b'}{b})$ is a trivial divisor. Next we note that

$$\mathfrak{n}(d) = \mathfrak{d}(\frac{x(Q)}{x(Q')})^h = \mathfrak{d}(\frac{ab'}{a'b}) = \mathfrak{d}(\frac{a}{a'})\mathfrak{d}(\frac{b'}{b}) = \mathfrak{d}(\frac{a}{a'})$$

so that $\mathfrak{n}(d)|\mathfrak{n}(a')$. Now $\mathfrak{n}(a')$ has no common factors with $\mathfrak{n}(b')$. Since by Lemma 3.4, all the factors of $\mathfrak{n}(b)$ are factors of $\mathfrak{n}(b')$, we must conclude that $\mathfrak{n}(b)$ and $\mathfrak{n}(d)$ have no common factors.

4 Bounds and Divisors

This section is devoted to equations which impose bounds on the height of elements of the ring and the related issues of divisibility in $O_{K,\mathcal{W}_K}$. We start with a lemma which follows immediately from the Strong Approximation Theorem.

4.1 Lemma.

Let $t, w \in O_{K,\mathcal{W}_K}$. Then there exist $X, Y \in O_{K,\mathcal{W}_K}$ with $Xt + Yw = 1$ if and only if for every $\mathfrak{p} \notin \mathcal{W}_K$,

$$(\mathrm{ord}_{\mathfrak{p}} w > 0 \Rightarrow \mathrm{ord}_{\mathfrak{p}} t = 0).$$

The next lemma describes circumstances when a divisor from K is a divisor from F.

4.2 Lemma.

Let $t, w \in O_{K,\mathcal{W}_K}$. Assume further that the following statements are true.

1. There exists $X, Y \in O_{K,\mathcal{W}_K}$, such that $Xt + Yw = 1$.
2. $\frac{t}{w} = z^h$, where $z \in F$.

Then $\bar{\mathfrak{n}}(w)$ is a divisor of F in the following sense. Let $\mathfrak{P}$ be a prime of F and let $\prod_i \mathfrak{p}_i^{e_i}$ be its factorization in K. Suppose further that for some i we have that $\mathrm{ord}_{\mathfrak{p}_i}\bar{\mathfrak{n}}(w) > 0$. Then for some positive integer l, for all i it is the case that $\mathrm{ord}_{\mathfrak{p}_i}\bar{\mathfrak{n}}(w) = le_i$, and $e_i\mathrm{ord}_{\mathfrak{p}_i} w = -e_i\mathrm{ord}_{\mathfrak{p}_i}\frac{t}{w} = -\mathrm{ord}_{\mathfrak{P}}\frac{t}{w}$.

Further, $w = yW$, where $y \in O_F$ and y is not divisible by any K-prime outside $\bar{\mathcal{W}}_K$, while all the K-primes occurring in the divisor of W are in $\bar{\mathcal{W}}_K$.

Proof.

First of all, we observe that by Lemma 4.1, the first condition assures us that if $\mathfrak{q} \notin \bar{\mathcal{W}}_K$ and $\mathrm{ord}_{\mathfrak{q}} w > 0$, then $\mathrm{ord}_{\mathfrak{q}} t = 0$. Thus, if $\mathrm{ord}_{\mathfrak{q}} w > 0$, then $\mathrm{ord}_{\mathfrak{q}} w = -\mathrm{ord}_{\mathfrak{q}} \frac{t}{w}$. Conversely, suppose $\mathfrak{q} \notin \bar{\mathcal{W}}_K$ and $\mathrm{ord}_{\mathfrak{q}} \frac{t}{w} < 0$. Then, since $\mathrm{ord}_{\mathfrak{q}} t \geq 0$ and $\mathrm{ord}_{\mathfrak{q}} w \geq 0$ we have that

$$\mathrm{ord}_{\mathfrak{q}} \frac{t}{w} < 0 \Rightarrow (\mathrm{ord}_{\mathfrak{q}} t = 0 \wedge \mathrm{ord}_{\mathfrak{q}} w = -\mathrm{ord}_{\mathfrak{q}} \frac{t}{w}).$$

Now the first assertion of the lemma follows from the fact that $t/w \in F$ and $\bar{\mathcal{W}}_K$ is closed under conjugation over F.

Next let $\bar{\mathfrak{n}}_F(w) = \bar{\mathfrak{n}}(w)$ considered as a divisor of F. Then $\bar{\mathfrak{n}}_F(w)$ is an h power of an integral divisor of F, and by assumption on h there exists $y \in F$ such that $\bar{\mathfrak{n}}_F(w) = \bar{\mathfrak{n}}(y)$. Let $W = \frac{w}{y}$. Then $W \in O_{K,\mathcal{W}_K}$ and all the K-primes occurring in the divisor of W are in $\bar{\mathcal{W}}_K$.

4.3 Lemma.

There exist $\bar{H}_1(X), \ldots, \bar{H}_{n+1}(X) \in K[X]$ such that for all $i = 1, \ldots, n+1$, all $x \in K$, for all primes $\mathfrak{q} \in \bar{\mathcal{W}}_K$, $\mathrm{ord}_{\mathfrak{q}} \bar{H}_i(x) \leq 0$ and no two $\bar{H}_i$, $\bar{H}_j$ have a common root for $i \neq j$.

Proof.

First suppose $\mathfrak{p} \in \bar{\mathcal{W}}_K$ is such that $\mathfrak{p}$ does not divide the discriminant of any H_i and does not have a relative degree 1 factor in any extension M_i/K. In this case we can use the proof of Lemma A.8 of [29], to assert that for any $i = 1, \ldots, n+1$, for any $x \in K$ we have that $\mathrm{ord}_{\mathfrak{p}} H_i(x) \leq 0$. (Since we assumed H_i's to be monic with integral coefficients, we do not need to assume that $\mathfrak{p}$ does not divide the coefficients of $H_i(X)$.) Next let $\mathcal{Q}$ be the finite (possibly empty) subset of $\bar{\mathcal{W}}_K$ consisting of primes not satisfying the conditions above. If $\mathcal{Q} \neq \emptyset$ let a be a rational integer divisible by every prime of $\mathcal{Q}$ and let $\bar{H}_i(x) = H_i(x^b + \frac{1}{a})$, where a positive integer b is such that

$$b > m\mathrm{ord}_{\mathfrak{q}} a \text{ and } (b, m\mathrm{ord}_{\mathfrak{q}} a) = 1 \tag{4.3}$$

for all $\mathfrak{q} \in \mathcal{Q}$. (Here we remind the reader that m is a constant defined in Notation 2.3.) If $\mathcal{Q} = \emptyset$ then let $b = 1, a = 1$. Now let $x \in K, \mathfrak{p} \in \bar{\mathcal{W}}_K$ and consider $\mathrm{ord}_{\mathfrak{p}} \bar{H}_i(x)$. If $\mathfrak{p} \notin \mathcal{Q}$, then as indicated above, $\mathrm{ord}_{\mathfrak{p}} \bar{H}_i(x) = \mathrm{ord}_{\mathfrak{p}} H_i(x^b + \frac{1}{a}) \leq 0$. If $\mathfrak{p} \in \mathcal{Q}$, then $\mathrm{ord}_{\mathfrak{p}}(x^b + \frac{1}{a}) < 0$, and since $H_i(x)$ is monic and has integral coefficients, $\mathrm{ord}_{\mathfrak{p}} H_i(x^b + \frac{1}{a}) < 0$.

To show that the last assertion of the lemma holds, it is enough to show that any root of $H_i(X^b + \frac{1}{a})$ is of degree $b[M_i : K]$ over K. Indeed, let β_i be a root of $H_i(X^b + \frac{1}{a})$. Then for some root γ_i of $H_i(X)$, $\gamma_i \in K(\beta_i)$. Further, $\beta_i^b + \frac{1}{a} = \gamma_i \in O_{K(\gamma_i)}$. From Equation (4.3) and the fact that γ_i is an algebraic integer it follows that all elements of $\mathcal{Q}$ will be ramified in extension $K(\beta_i)/K(\gamma_i)$ with ramification degree b. Thus, $[K(\beta_i) : K(\gamma_i)] = b$ and for all $i = 1, \ldots, n+1$ the polynomial $\bar{H}_i(X)$ is irreducible of degree $b[M_i : K]$ over K. Hence, $\bar{H}_i(X)$ and $\bar{H}_j(X)$ have no roots in common for $i \neq j$.

4.4 Lemma.

Let $\frac{\alpha}{\beta} \in K$ with $\alpha, \beta \in O_K$ and relatively prime to each other. Let $y \in O_K$ be such that $y \neq 0$ is not an integral unit,

$$\frac{y}{\bar{H}_u(\alpha/\beta - l_j)} \in O_K, j = 0, \ldots, z, u = 1, \ldots, n+1 \tag{4.4}$$

where $l_0 = 0, \ldots, l_z$, $z = \max_u(b[M_u : \mathbb{Q}])$ are distinct natural numbers. Let

$$\mathbf{N}_{K/\mathbb{Q}}(\beta)\alpha/\beta = e_0 + e_1\phi + \ldots + e_{s-1}\phi^{s-1}, e_0, e_1, \ldots, e_{s-1} \in F. \tag{4.5}$$

Then there exists a constant $c > 0$ depending on $l_0, \ldots, l_z, K, \bar{H}_u(T), M_u, D, \phi$ only such that

$$|\mathbf{N}_{K/\mathbb{Q}}(De_j)| < |\mathbf{N}_{K/\mathbb{Q}}(y)|^c, j = 0, \ldots, s-1. \tag{4.6}$$

Proof.

The proof is essentially the same as for Lemma 1.3.3 of [28].

4.5 Lemma.

There exists a constant $c' > 0$ depending only on F and K such that the following holds: Let I be a non-zero ideal of O_F. Suppose $\mu \in O_K$ and $\omega \in O_F$. Write $\mu = \sum_{i=0}^{s-1} e_j \phi^j$, with $e_j \in F$. Suppose $N_{K/\mathbb{Q}}(De_j) < c' N_{K/\mathbb{Q}}(I)$ for all j, and $\mu \cong \omega(\mod IO_K)$. Then $\mu \in O_F$.

Proof.

This is Lemma 5 of [17].

5 Diophantine Definitions.

This section is devoted to the proof of the vertical definability result in Proposition 5.3. This proposition will serve as foundation for the results of Section 6.

5.1 Proposition.

Consider the following equations.

$$\lambda = \nu^{2h}, \tag{5.7}$$

$$P_1, P_2, P_3 \in [ir]E(K) \setminus \{O\}, \tag{5.8}$$

$$(x(P_j))^{h_k} = \frac{u_j}{v_j}, u_j, v_j \in O_{K,\mathcal{W}_K} \setminus \{0\}, j = 1, 2, \tag{5.9}$$

$$X_j u_j + Y_j v_j = 1, j = 1, 2, \tag{5.10}$$

$$\frac{u}{v} = \left(\frac{x(P_2)}{x(P_3)}\right)^h, u, v \in O_{K,\mathcal{W}_K} \setminus \{0\}, \tag{5.11}$$

$$V_{u,j} = \frac{v_1}{\bar{H}_u(\lambda - l_j)}, u = 1, \ldots, n+1, j = 1, \ldots, z = \max_u(b[M_u : \mathbb{Q}]), \tag{5.12}$$

$$V = \frac{v_2}{(n_{c'} v_1)^{2hn_c}}, \tag{5.13}$$

$$Av + Bv_2 = 1, \tag{5.14}$$

$$(v\lambda - u)^{2h} = v^{2h} w v_2. \tag{5.15}$$

We claim that if these equations hold with all the variables except for $P_j, x(P_j), j = 1, 2, 3$, ranging over elements of $O_{K,\mathcal{W}_K}$, then $\lambda \in F$.

Proof.

First we observe that $\lambda = \frac{\alpha}{\beta}, \alpha, \beta \in O_K$ and are relatively prime integers. Further, by definition of i (see Notation 2.3), we conclude that $u/v \in F$. Next note that by Lemma 3.1, Lemma 4.2 and our assumptions, $\bar{\mathfrak{n}}(v_2)$ is a $2h$-th power of an integral divisor of F. So let $\mathfrak{v}_2^{2h} = \bar{\mathfrak{n}}(v_2)$, where $\mathfrak{v}_2$ is an integral divisor of F. By Equation (5.14) and Lemma 4.1 we know that $\frac{u}{v}$ is integral at all the primes occurring in $\mathfrak{v}_2$. Thus, by the Strong Approximation Theorem, there exists $t \in O_F$ such that the numerator of the divisor of $t - \frac{u}{v}$ is divisible by $\mathfrak{v}_2$. Then for any K-prime $\mathfrak{q}$ occurring in $\mathfrak{v}_2$, the following statements are true.

1. $\mathrm{ord}_{\mathfrak{q}}(\lambda - \frac{u}{v}) \geq \mathrm{ord}_{\mathfrak{q}} \mathfrak{v}_2$.

2. $\mathrm{ord}_{\mathfrak{q}}(\lambda - t) \geq \min(\mathrm{ord}_{\mathfrak{q}}(\lambda - \frac{u}{v}), \mathrm{ord}_{\mathfrak{q}}(\frac{u}{v} - t)) \geq \mathrm{ord}_{\mathfrak{q}}\mathfrak{v}_2$.

3. $\mathrm{ord}_{\mathfrak{q}}(\mathbf{N}_{K/\mathbb{Q}}(\beta)\lambda - N_{K/\mathbb{Q}}(\beta)t) \geq \mathrm{ord}_{\mathfrak{q}}\mathfrak{v}_2$.

Let $t' = N_{K/\mathbb{Q}}(\beta)t \in O_F$ and note $\mathbf{N}_{K/\mathbb{Q}}(\beta)\lambda - t' \in I_{\mathfrak{v}_2}O_K$, where $I_{\mathfrak{v}_2} \subset O_F$ is the O_F ideal with the divisor $\mathfrak{v}_2$.

On the other hand, by Lemma 4.2 we can write $v_1 = yW$, where the divisor of $y \in O_K$ consists of K-primes outside $\bar{\mathcal{W}}_K$ and the divisor of W consists of primes in $\bar{\mathcal{W}}_K$ only. As in the case of $\mathfrak{v}_2$ we can also conclude that the divisor $\mathfrak{y}$ of y is equal to $\bar{\mathfrak{n}}(v_1)$ and is a divisor of F. Note further that $\bar{H}_u(\lambda - l_i)$ does not have a positive order at primes of $\bar{\mathcal{W}}_K$, and therefore

$$V_{u,i} = \frac{v_1}{\bar{H}_u(\lambda - l_i)} \in O_{K,\mathcal{W}_K} \Rightarrow \frac{y}{\bar{H}_u(\lambda - l_i)} \in O_{K,\bar{\mathcal{W}}_K} \Leftrightarrow \frac{y}{\bar{H}_u(\lambda - l_i)} \in O_K.$$

Thus we can apply Lemma 4.4 and conclude that Equation (4.6) holds. Further, from Equation (5.13) we must conclude that $\mathfrak{n}(n_{c'}v_1^{n_c})\Big|\mathfrak{v}_2$, or $(n_{c'})\mathfrak{y}^{n_c}\Big|\mathfrak{v}_2$. Thus,

$$\left|\mathbf{N}_{K/\mathbb{Q}}(y^c)\right| < \left|\mathbf{N}_{K/\mathbb{Q}}(y^{n_c})\right| < \left|\frac{1}{n_{c'}}\mathbf{N}_{K/\mathbb{Q}}(I_{\mathfrak{v}_2})\right| < \left|c'\mathbf{N}_{K/\mathbb{Q}}(I_{\mathfrak{v}_2})\right|$$

Therefore by Lemma 4.5 we have that $\mathbf{N}_{K/\mathbb{Q}}(\beta)\lambda \in F \Leftrightarrow \lambda \in F$.

5.2 Proposition.

Suppose $\nu = k$, with $k \in \mathbb{Z}, k \neq 0$. Then Equations (5.7)–(5.15) can be satisfied over $O_{K,\mathcal{W}_K}$.

Proof.

If $\nu = k^2$, then $\lambda = k^{2h}$. By Lemma 3.2, there exists a positive integer l such that for some $P \in E(K)$, $x^h([lir]P) = \frac{u_1}{v_1}, u_1, v_1 \in O_K \setminus \{0\}$ are relatively prime integers and (5.12) holds for all u, i for some $V_{u,i} \in O_{K,\mathcal{W}_K}$. Next by Lemma 3.2 again, there exists a positive integer l' such that $x([l'ir])^h = \frac{u_2}{v_2}, u_2, v_2 \in O_K$ are relatively prime integers and (5.13) holds for some $V \in O_{K,\mathcal{W}_K}$. Finally, let $P_3 = [k]P_2$. By definition of the class number, there exist $u, v \in O_K$ so that Equation (5.11) holds and $u, v \in O_K$ and are relatively prime. Then by Lemma 3.5 we have that $\mathfrak{n}(v_2)$ and $\mathfrak{n}(v)$ have no common factors and therefore $\mathfrak{d}_2$ and $\mathfrak{n}(v)$ have no common factors. Hence by Lemma 4.1, Equation (5.14) can be satisfied. Further, by Lemma 3.3 we have that

$$\mathfrak{d}(x(P_2))\Big|\mathfrak{n}(x(P_2)/x(P_3) - k^2)^2$$

as integral divisors, and therefore

$$\mathfrak{d}(x(P_2))\Big|\mathfrak{n}(\frac{u}{v} - k^{2h})^2,$$

since

$$\left(\frac{x(P_2)}{x(P_1)}\right)^h - k^{2h} = \left(\frac{x(P_2)}{x(P_1)} - k^2\right)U,$$

where for any K-prime $\mathfrak{q} \notin \mathcal{W}_K$ we have that $\mathrm{ord}_{\mathfrak{q}}U < 0 \Rightarrow \mathrm{ord}_{\mathfrak{q}}v > 0 \Rightarrow \mathrm{ord}_{\mathfrak{q}}v_2 = 0 \Rightarrow \mathrm{ord}_{\mathfrak{q}}\mathfrak{d}(x(P_2)) = 0$ by the discussion above. Therefore, (5.15) can also be satisfied.

5.3 Proposition.

$O_{K,\mathcal{W}_K} \cap F$ has a Diophantine definition over $O_{K,\mathcal{W}_K}$.

Proof.

Let $\mu \in O_{K,\mathcal{W}_K}$ and suppose Equations (5.7)–(5.15) can be satisfied in $O_{K,\mathcal{W}_K}$ with $\nu = \mu, \mu+1, \ldots, \mu+2h$. Then by Proposition 5.1 we have that $\mu^{2h}, (\mu+1)^{2h}, \ldots, (\mu+2h)^{2h} \in F$. Consequently, by Lemma 5.2 of [26] we have that $\mu \in F$. On the other hand if $\mu \in \mathbb{Z}, \mu \neq 0$, then by Proposition 5.2, Equations (5.7)–(5.15) can be satisfied in $O_{K,\mathcal{W}_K}$. Next let

$$A = \{\mu \in O_{K,\mathcal{W}_K} | \text{Equations (5.7)–(5.15) can be satisfied in } O_{K,\mathcal{W}_K} \text{ with } \nu = \mu, \mu+1, \ldots, \mu+2h\} \cup \{0\}$$

Then by the argument above, $\mathbb{Z} \subset A \subset F$, and A has a Diophantine definition over $O_{K,\mathcal{W}_K}$. Next let δ be an integral generator of F over $\mathbb{Q}$. Then $u \in O_{K,\mathcal{W}_K} \cap F$ if and only if $u \in O_{K,\mathcal{W}_K}$ and $u = \sum_j \frac{a_i}{b_i}\delta^i$, where $a_i, b_i \in A, b_i \neq 0$. Thus, $O_{K,\mathcal{W}_K} \cap F$ has a Diophantine definition over $O_{K,\mathcal{W}_K}$.

5.4 Corollary.

Let $\hat{\mathcal{W}}_K$ be a set of primes of K such that $\mathcal{W}_K \subseteq \hat{\mathcal{W}}_K$ and $\hat{\mathcal{W}}_K \setminus \mathcal{W}_K$ is finite. Then $O_{K,\hat{\mathcal{W}}_K} \cap F$ has a Diophantine definition over $O_{K,\hat{\mathcal{W}}_K}$.

Proof.

This corollary follows from Proposition 5.3, since $\hat{\mathcal{W}}$ still satisfies Assumption 2.4.

6 Main Results.

In this section we prove the main results of this paper. In all the propositions below we will use the following assumptions.

6.1 Assumptions.

- K/F is a finite extension of number fields of degree $s > 1$.
- There exists an elliptic curve defined over F such that its rank over K is the same as over F and is positive.

6.2 Theorem.

For any $\varepsilon > 0$ there exists set of K-primes of natural density greater than $1-\varepsilon$ such that $O_{K,\mathcal{W}_K} \cap F$ has a Diophantine definition over $O_{K,\mathcal{W}_K}$.

Proof.

Let ε be given. Let K_G be the Galois closure of K over F and let $N_1, \ldots, N_{n+1}$ be cyclic extensions of $\mathbb{Q}$ of degrees $q_1, \ldots, q_{n+1}$, where $q_1 < \ldots < q_{n+1}$ are distinct prime numbers such that for all j we have that $(q_j, [K_G : \mathbb{Q}]) = 1$ and

$$1 - \frac{(q_1 - 1)\ldots(q_{n+1}-1)}{q_1 \cdots q_{n+1}} < \varepsilon.$$

Next let $M_j = N_j K$. Let $\gamma_j \in O_{N_j}$ be a generator of N_j over $\mathbb{Q}$. Let $\mathcal{W}_K$ be the set of all primes of K not splitting in any of the extensions M_j/K. Given our assumptions on the degrees of field extensions, every prime of $\mathcal{W}_K$ has all of its F-conjugates in $\mathcal{W}_K$, and therefore Proposition 5.3 applies to $\mathcal{W}_K$. It remains to establish the density of $\mathcal{W}_K$. Consider the extension $M_1 \ldots M_{n+1}/K$. Since q_i's are pairwise relatively prime and also prime to $[K_G : \mathbb{Q}]$, this is a Galois extension whose group is isomorphic to $\prod_{j=1}^{n+1} \mathrm{Gal}(N_j/\mathbb{Q})$.

Let $\mathfrak{q}_K$ be a prime of K splitting in one of the extensions M_j/K. Then it must have a factor in $M_1 \dots M_{n+1}$ with Frobenius automorphism of the form

$$(\tau_1, \dots, \mathrm{id}_j, \dots, \tau_{n+1}), \tag{6.16}$$

where $\tau_j \in \mathrm{Gal}(N_j/\mathbb{Q})$ is not necessarily an identity and id_j is the identity element of $\mathrm{Gal}(N_j/\mathbb{Q})$. Further, if $\mathfrak{p}_K$ has a factor with Frobenius of the form (6.16), it splits in M_j/K. Therefore, by the natural density version of Chebotarev Density Theorem ((see Theorem 1 of [22]), $\mathcal{W}_K$ has natural density and this density is equal to

$$\frac{(q_1 - 1) \dots (q_{n+1} - 1)}{q_1 \dots q_{n+1}}.$$

Next we specialize Theorem 6.2 to the cases whether $\mathcal{W}_K$ is either finite or empty to obtain the following corollaries.

6.3 Corollary.

Let $\mathcal{S}_K$ be a finite set of primes of K. Then $O_{K,\mathcal{S}_K} \cap F$ has a Diophantine definition over $O_{K,\mathcal{S}_K}$. If F is a totally real field (including $\mathbb{Q}$), an extension of degree 2 of a totally real field or a field with exactly one pair of non-real conjugate embeddings, then HTP is undecidable over $O_{K,\mathcal{S}_K}$.

6.4 Corollary.

O_F has a Diophantine definition over O_K. If F is a totally real field (including $\mathbb{Q}$), an extension of degree 2 of a totally real field or a field with exactly one pair of complex conjugate embeddings, then HTP is undecidable over O_K.

Once we established these vertical definability results, we can proceed as in [29] and [30] to obtain results pertaining to definability of integers over large subrings of fields and Mazur's Conjectures over such rings.

6.5 Theorem.

For any $\varepsilon > 0$ there exists a set $\mathcal{V}_K$ of K-primes of natural density greater than $1 - \frac{1}{s} - \varepsilon$ such that O_F and O_K have Diophantine definitions over $O_{K,\mathcal{V}_K}$. If F is a totally real field (including $\mathbb{Q}$), a totally complex extension of degree 2 of a totally real field or a field with exactly one pair of non-real conjugate embeddings, then HTP is undecidable over $O_{K,\mathcal{V}_K}$.

Proof.

Let $\mathcal{W}_K$ be defined as in Theorem 6.2. We will form $\mathcal{V}_K$ out of $\mathcal{W}_K$ in the following manner. For each complete set of F-conjugates in $\mathcal{W}_K$ remove a prime of the highest norm. From Chebotarev Density Theorem it follows that only primes of relative degree 1 will contribute to the density (if it exists) of the removed set of primes. Furthermore, the density of the set of removed primes of relative degree 1 is equal to the density of the set of F-primes below them. Thus, it is enough to compute the density of the set of primes $\mathfrak{q}_F$ of F satisfying the following conditions:

1. $\mathfrak{q}_F$ splits completely in the extension K/F.
2. For all $j = 1, \dots, n+1$ it is the case that $\mathfrak{q}_F$ does not split in the extension N_jF/F.

Note that $\mathfrak{q}_F$ splits completely in the extension K/F if and only if it splits completely in the extension K_G/F. Further, given the assumptions on the degree of the extensions, for any j, we have that $\mathfrak{q}_F$ splits completely in the extension N_jF/F if and only if every factor $\mathfrak{q}_{K_G}$ of $\mathfrak{q}_F$ in K_G splits completely in the

extension $K_G N_j/K_G$ and every factor $\mathfrak{q}_K$ of $\mathfrak{q}_F$ in K splits completely in the extension M_j/K. Thus, $\mathfrak{q}_F$ satisfies Conditions 1 and 2 above if and only if in the extension $K_G M_1 \dots M_{n+1}/F$, $\mathfrak{q}_F$ has a factor whose Frobenius is of the form $(\mathrm{id}_{K_G}, \sigma_1, \dots, \sigma_{n+1})$, where id_{K_G} is the identity element of $\mathrm{Gal}(K_G/F)$ and σ_i is not the identity element of $\mathrm{Gal}(N_j/\mathbb{Q})$. Therefore, by Chebotarev Density Theorem (the natural version), this set of primes has natural density and it is equal to

$$\frac{(q_1-1)\dots(q_{n+1}-1)}{[K_G:F]q_1\dots q_{n+1}}.$$

Thus the natural density of $\mathcal{V}_K$ is equal to

$$\frac{(q_1-1)\dots(q_{n+1}-1)}{q_1\dots q_{n+1}} - \frac{(q_1-1)\dots(q_{n+1}-1)}{[K_G:F]q_1\dots q_{n+1}} \geq \frac{s-1}{s}\frac{(q_1-1)\dots(q_{n+1}-1)}{q_1\dots q_{n+1}} \longrightarrow 1-\frac{1}{s}.$$

as $q_1, \dots, q_{n+1} \longrightarrow \infty$. Observe now that $O_{K,\mathcal{V}_K} \cap F = O_F$ and the assertion of the theorem follows.

Finally we state a result concerning Mazur's Conjecture.

6.6 Theorem.

Suppose F is either a totally real field or a totally complex extension of degree 2 of a totally real field. Then for any $\varepsilon > 0$ there exists a set $\mathcal{W}_K$ of K-primes of natural density greater than $1-\varepsilon$ such that for some variety V defined over K we have that $\overline{V(O_{K,\mathcal{W}_K})}$ has infinitely many components.

Proof.

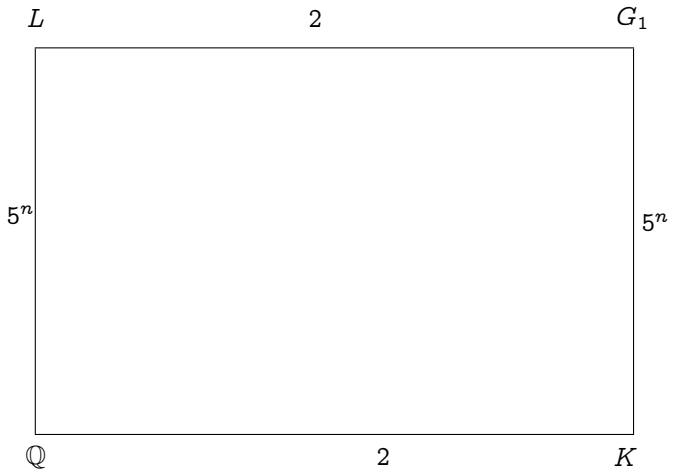
The proof of this theorem is completely analogous to the proof of Theorem 3.6 of [30].

7 Examples.

In this section we will present some examples drawn from [14] and [3] where we can make use of results from Section 6 to obtain new definability and undecidability results and new counterexamples to the ring version of Mazur's Conjecture. We will start with an example from [14].

7.1 Example.

Let $K = \mathbb{Q}(\sqrt{-7})$. Let K_∞ be a $\mathbb{Z}_5^2$-extension of K. Let $K_\infty^{anti} \subset K_\infty$ be the anticyclotomic extension of K contained in K_∞, i.e. the unique subfield of K_∞ containing K such that it is a $\mathbb{Z}_5$-extension of K which is a non-abelian (dihedral) Galois extension of $\mathbb{Q}$. Let K_∞^{cycle} be the compositum of K with a unique cyclotomic $\mathbb{Z}_5$ extension of $\mathbb{Q}$. Let E be the elliptic curve corresponding to the equation $y^2+y = x^3-x$. Then, for any number field F with $K \subseteq F \subset K_\infty$ we have that rank $(E(F)) = [F \cap K_\infty^{anti} : K]$. Note that from definition of K_∞^{anti} and K_∞^{cycle}, the intersection of these fields is K. Now let F^{anti} be a number field, Galois over $\mathbb{Q}$, such that $K \subset F^{anti} \subset K_\infty^{anti}$ and let $F_1^{cycle} \subseteq F_2^{cycle}$ be number fields such that $K \subseteq F_1^{cycle} \subset F_2^{cycle} \subset K_\infty^{cycle}$. Next consider fields $G_1 = F_1^{cycle}F^{anti} \subset F_2^{cycle}F^{anti} = G_2$ and observe that $G_1 \cap K_\infty^{anti} = G_2 \cap K_\infty^{anti} = F^{anti}$. Therefore, E would have the same rank over G_1 and G_2. Observer further that $G_1/\mathbb{Q}$ is not abelian and is totally complex since it contains $\sqrt{-7}$. Further, it is of degree at least 10 over $\mathbb{Q}$, so it has more than one pair of non-real embeddings. Finally, G_1 is not an extension of degree 2 of a totally real field. Indeed, suppose that it is not the case and consider the following diagram, where L is this totally real subfield of G_1 of degree 2.



First of all, $L/\mathbb{Q}$ is not Galois, otherwise K and L are two linearly disjoint abelian extensions of $\mathbb{Q}$ and G_1 is also abelian. Let α generate L over $\mathbb{Q}$. Then at least one conjugate of α over $\mathbb{Q}$ is not in L. On the other hand, all the conjugates of α over $\mathbb{Q}$ must be in G_1. Let β be this conjugate. Then $\beta \in \mathbb{R}$ and $G_1 = \mathbb{Q}(\alpha, \beta) \subset \mathbb{R}$ in contradiction of the fact that G_1 is a non-real field. Thus, when we apply Diophantine definability results from Section 6, to the pair G_2/G_1, we will indeed obtain new diophantine definitions.

Finally, the reader might wonder why we do not consider simply the subfields of K_∞^{cycle}. For these subfields our method will indeed produce undecidability results and counterexamples to the ring version of Mazur's Conjecture. However, the subfields of K_∞^{cycle} are cyclic extensions of $\mathbb{Q}$ and Theorems 6.2, 6.5 and 6.6 are known for these fields (see [26], [29], [27] and [30]).

We will next consider examples computed in [3].

7.2 Example.

In [3], Cornelissen, Pheidas, and Zahidi computed the rank of $y^2 = x^3 + 8x$ over $\mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[4]{2})$, and determined that it is 1 over all three fields. First of all, we note that $\mathbb{Q}(\sqrt[3]{2})$ is a field with one pair of non-real embeddings and therefore the case of integers and $\mathcal{S}$-integers (with $\mathcal{S}$ of finite size) of this field is covered by the results obtained independently by the author and Pheidas in [24] and [15] respectively. The case of integers and $\mathcal{S}$-integers (with $\mathcal{S}$ of finite size) for $\mathbb{Q}(\sqrt[4]{2})$ is covered by results in Poonen's paper (see [17]). On the other hand, the statements from Theorems 6.2, 6.5, 6.6 are new results for these fields. We should note here that, as mentioned above, since $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[4]{2})$ both have a rank one elliptic curves, the method Poonen used in [18] will apply to these fields so that for each of these fields one can construct a sets of primes $\mathcal{W}_{\mathbb{Q}(\sqrt[3]{2})}$ and $\mathcal{W}_{\mathbb{Q}(\sqrt[4]{2})}$ of natural density equal to one and the rings $O_{\mathbb{Q}(\sqrt[3]{2}),\mathcal{W}_{\mathbb{Q}(\sqrt[3]{2})}}$ and $O_{\mathbb{Q}(\sqrt[4]{2}),\mathcal{W}_{\mathbb{Q}(\sqrt[4]{2})}}$ will posses a Diophantine model of $\mathbb{Z}$ and will falsify the ring version of Mazur's Conjecture. (Also as we have mentioned above, this kinds of results are discussed in [19].) However, the rings obtained by this method are different from the rings constructed for the proofs of Theorems 6.5 and 6.6.

References

[1] Zubeir Cinkir, Andrei Glubkov, Matilde Lalin, Amador Martin-Pizarro, Javier Moreno, Haidi Williams, Soroosh Yazdani, and Eunjeong Yi. Elliptic curves of rank 1 over their endomorphism rings and Hilbert's Tenth Problem. Presentation at the 2003 Arizona Winter School on "Logic and Number Theory", March 2003.

[2] 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.

[3] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi. Division-ample sets and diophantine problem for rings of integers. to appear in Journal de Théorie des Nombres Bordeaux.

[4] 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.

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

[6] Martin Davis, Yuri Matiyasevich, and Julia Robinson. Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution. In *Proc. Sympos. Pure Math.*, volume 28, pages 323– 378. Amer. Math. Soc., 1976.

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

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

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

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

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

[12] Barry Mazur. Speculation about the topology of rational points: An up-date. *Asterisque*, 228:165–181, 1995.

[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.

[14] Barry Mazur and Karl Rubin. Elliptic curves and class field theory. In *Proceedings of the International Congress of Mathematicians, Vol. II (Beijing, 2002)*, pages 185–195, Beijing, 2002. Higher Ed. Press.

[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.

[16] Bjorn Poonen. Elliptic curves whose rank does not grow and Hilbert's Tenth Problem over the rings of integers. Private Communication.

[17] 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.

[18] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of AMS*, 16(4):981–990, 2003.

[19] Bjorn Poonen and Alexandra Shlapentokh. Diophantine definability of infinite discrete non-archimedean sets and diophantine models for large subrings of number fields. *Journal für die Reine und Angewandte Mathematik*, 2005:27–48, 2005.

[20] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949.

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

[22] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

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

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

[25] Alexandra Shlapentokh. Diophantine classes of holomorphy rings of global fields. *Journal of Algebra*, 169(1):139–175, October 1994.

[26] 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.

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

[28] 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.

[29] 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.

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