Journal of Number Theory 254 (2024) 1–64

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

JNT Prime

Existential definability and diophantine stability ☆

Barry Mazur [a], Karl Rubin [b], Alexandra Shlapentokh [c,*]

[a] *Department of Mathematics, Harvard University, Cambridge, MA 02138-2901, USA*
[b] *Department of Mathematics, UC Irvine, Irvine, CA 92697, USA*
[c] *Department of Mathematics, East Carolina University, Greenville, NC 27858, USA*

ARTICLE INFO

Article history:
Received 18 September 2022
Received in revised form 25 April 2023
Accepted 26 April 2023
Available online 2 August 2023
Communicated by A. Pal

In memory of Martin Davis

MSC:
primary 11U05
secondary 11G05

Keywords:
Hilbert's Tenth Problem
Diophantine definition

ABSTRACT

Let K be a number field, let L be an algebraic (possibly infinite degree) extension of K, and let $\mathcal{O}_K \subset \mathcal{O}_L$ be their rings of integers. Suppose A is an abelian variety defined over K such that $A(K)$ is infinite and $A(L)/A(K)$ is a torsion group. If at least one of the following conditions is satisfied:

1. L is a number field,
2. L is totally real,
3. L is a quadratic extension of a totally real field,

then $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_L$.

☆ The authors thank Hector Pasten for his comments and suggestions for the paper. The research for this paper was partially supported by DMS grants 2152098 (AS), 2152149 (BM), 2152262 (KR). AS was also partially supported by an ECU Creative Activity and Research Grant 2121-02 during the summer of 2022.

* Corresponding author.
E-mail addresses: mazur@g.harvard.edu (B. Mazur), krubin@uci.edu (K. Rubin), shlapentokha@ecu.edu (A. Shlapentokh).
URLs: http://www.math.harvard.edu/~mazur (B. Mazur), https://math.uci.edu/~krubin (K. Rubin), https://myweb.ecu.edu/shlapentokha (A. Shlapentokh).

https://doi.org/10.1016/j.jnt.2023.04.011
0022-314X/

Contents

1. Introduction

For the definition of "diophantine definition", "diophantine undecidable", "existentially definable", and similar terms used in this introduction, see §2 and §4.

Here is a corollary of one of our main results (see Theorems 3.1 and 3.9 below). By "number field" we mean a finite extension of $\mathbb{Q}$.

Theorem 1.1. *Let K be a number field, let L be an algebraic (possibly infinite degree) extension of K, and let $\mathcal{O}_K \subset \mathcal{O}_L$ be their rings of integers. Suppose A is an abelian variety defined over K such that $A(K)$ is infinite and $A(L)/A(K)$ is a torsion group. If at least one of the following conditions is satisfied:*

(1) L is a number field,
(2) L is totally real,
(3) L is a quadratic extension of a totally real field,

then $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_L$.

Theorem 1.1 answers a question raised by B. Poonen in [Poo02, Question 2.6(3)]. For a discussion of previous results in the direction of Theorem 1.1, see §2.

Theorem 1.1 is a special case of a more general result (see Propositions 14.3, 14.4, and 14.5) where the abelian variety is replaced by a smooth group scheme over $\mathcal{O}_K$ satisfying some mild additional hypotheses (Assumption 7.4). In this paper the group schemes we mainly use are Néron models of abelian varieties and twists of multiplicative groups.

One way of describing the main structural element in the proof of Theorem 1.1 is the following. We pass, via an 'existential definition'—from an appropriate subgroup of the group of rational points on the group scheme we work with—to the (additive group of the) ring $\mathcal{O}_K$, by constructing a scheme-theoretic (existentially defined) analogue to some approximation of the standard logarithm mapping that sends an appropriate open subset of the identity in an algebraic group to its Lie algebra.

The following concept, implicit in the statement of Theorem 1.1, is fundamental to our results in this paper.

Definition 1.2. Let L/K be an extension of fields, and V an algebraic variety defined over K. We denote by $V(K)$ the set of K-rational points of V.

- Say that V is **diophantine stable** for L/K, or L/K is **diophantine stable** for V, if the inclusion $V(K) \hookrightarrow V(L)$ is an isomorphism, i.e., if V acquires no new rational points after passing from K to L.
- If $V = A$ is an abelian variety over a field K, say that A is **rank stable** for L/K if $A(L)/A(K)$ is a torsion group. If L is a number field, this is equivalent to saying that $\operatorname{rank} A(K) = \operatorname{rank} A(L)$.

A study of diophantine stability for elliptic curves can be found in [MR10], and for higher dimension abelian varieties in [MR18].

Definition 1.3. We say that number fields L/K are **connected by a diophantine chain** if there is an $n \geq 0$ and a tower of number fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_n \supset L$$

such that for every i, $1 \leq i \leq n$, there is an abelian variety A_i defined over K_{i-1} that is rank stable for K_i/K_{i-1} and such that $\operatorname{rank} A_i(K_{i-1}) > 0$.

The condition of being 'connected by a diophantine chain *descends* in the following sense.

Theorem 1.4. *Let L/K and K'/K be linearly disjoint number field extensions of K, and consider $L' := K'L$, the compositum of K' and L. If the number fields L'/K' are connected by a diophantine chain then so are the number fields L/K.*

(See Theorem 3.3 below.)

Remark 1.5. The abelian varieties involved in the descended chain connecting L to K in the conclusion of Theorem 1.4 are 'Weil traces' of those involved in the chain connecting L' to K' and, in particular, each are of dimension $[K' : K]$ times the dimension of the corresponding abelian varieties in that initial chain.

Moreover, by the nature of Weil trace, the Mordell-Weil ranks of the relevant abelian varieties are equal to the Mordell-Weil ranks of the corresponding descended abelian varieties.

The following corollary follows directly from Theorem 1.1 and Lemma 4.3 below.

Corollary 1.6. *If L/K is an extension of number fields connected by a diophantine chain, then the ring of integers of K has a diophantine definition over the ring of integers of L.*

Conjecture 1.7. *Every number field L is connected to $\mathbb{Q}$ by a diophantine chain.*

A consequence of Conjecture 1.7 is the following conjecture, first formulated by Denef and Lipshitz in [DL78], which is also known to follow from other standard conjectures about elliptic curves ([MR10,MP18]):

Conjecture 1.8. *The ring $\mathbb{Z}$ of rational integers has a diophantine definition over the ring of integers of any number field. Hence Hilbert's Tenth Problem has a negative answer for the ring of integers of every number field.*

For a discussion of Hilbert's Tenth Problem see §2.

Inspired by conjectures of C. David, J. Fearnley, and H. Kisilevsky [DFK07,FK12], the first two authors of this article developed in [MR22] a "heuristic" (based on the statistics of modular symbols) for groups of rational points on elliptic curves over infinite abelian extensions of $\mathbb{Q}$. Using specially constructed abelian varieties, this heuristic and the main results of this article led us to make the following diophantine undecidability conjecture. See §16, §17, and §18, especially Consequences 16.15, 17.3, and 18.4 for details. Let $\mathbb{Q}^{\mathrm{ab}}$ denote the maximal abelian extension of $\mathbb{Q}$, the field generated over $\mathbb{Q}$ by all roots of unity.

Conjecture 1.9. *For the primes $p = 7$, 11, or 13 there are subfields $\mathbf{L} \subset \mathbb{Q}^{\mathrm{ab}}$ for which the field extension $\mathbb{Q}^{\mathrm{ab}}/\mathbf{L}$ is cyclic of degree p and such that $\mathcal{O}_{\mathbf{L}}$, the ring of integers in $\mathbf{L}$, is diophantine undecidable.*

In fact, we conjecture (the stronger statement) that $\mathbb{Z}$ is existentially definable over $\mathcal{O}_{\mathbf{L}}$ for the fields $\mathbf{L}$ in Conjecture 1.9. We do not make the same conjecture for $\mathcal{O}_{\mathbb{Q}^{\mathrm{ab}}}$.

The following result—related to Conjecture 1.9—is due to the third author [Shl09], K. Kato [Kat04], K. Ribet [Rib81] and D. Rohrlich [Roh84,Roh88] (see [LR08, Theorem 1.2]).

Theorem 1.10. *Let* $\mathbf{L}$ *be an abelian extension with finitely many ramified primes. Then* $\mathbb{Z}$ *is existentially definable over* $\mathcal{O}_{\mathbf{L}}$.

Part 1. Existential definability and Hilbert's Tenth Problem

2. Hilbert's Tenth Problem over rings of algebraic integers

The original "Hilbert's Tenth Problem" was one of 23 problems posed over a century ago by David Hilbert in the International Congress of Mathematicians, at the Sorbonne, in Paris:

Problem. Find an algorithm that, when given an arbitrary polynomial equation in several variables over $\mathbb{Z}$, answers the question of whether that equation has solutions in $\mathbb{Z}$.

Work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich shows that there is no such algorithm. (See [Dav73] and [DMR76].)

Since the time when this result was obtained, similar questions have been raised for other fields and rings. E.g.,

Question 2.1. Let R be a computable ring, i.e., a countable ring computable as a set and with ring operations represented by computable functions. Is there an algorithm (equivalently: computer program) taking the coefficients of an arbitrary polynomial over R as its input and outputting a "Yes" or "No" answer to the question whether the polynomial in question has solutions in R?

This question in the special case of $R = \mathbb{Q}$ remains an open basic diophantine issue; we wonder (a) why Hilbert didn't formulate this question as an addendum to his initial "tenth problem," and (b) whether there is currently a strong consensus guess by the experts about its answer.

One way to resolve the question of diophantine decidability negatively over a ring of characteristic zero is to construct a diophantine definition of $\mathbb{Z}$ over such a ring. The usefulness of such a diophantine definition stems from the fact that if a ring has a diophantine definition of $\mathbb{Z}$, then its analog of Hilbert's Tenth Problem is undecidable. We explain how diophantine definitions are used in the following section.

Deriving undecidability of Hilbert's Tenth Problem over a ring R *using a diophantine definition of* $\mathbb{Z}$ *over* R.

Definition 2.2. Let R be a ring and let E be a subset of R. Then we say that E **has a diophantine definition over** R if there exists finite collection of polynomials with coefficients in R,

$$\mathcal{F}: \ f_i(t, x_1, x_2, x_3, \dots x_n) \ \in \ R[t, x_1, \dots, x_n] \text{ for } i = 1, 2, \dots, m$$

such that for any $\tau \in R$,

$$\tau \in E \Longleftrightarrow \exists a_1, \ldots, a_n \in R \text{ satisfying } f_i(\tau, a_1, ..., a_n) = 0 \text{ for } i = 1, 2, \ldots, m.$$

We will use interchangeably the terminology *E has a diophantine definition over R*, or *E is diophantine over R*, or *E is existentially definable over R*—noting that this last is a slight abuse of language: properly speaking, we should say *E is positively existentially definable over R.*

We now prove an easy proposition that explains the importance of diophantine definition discussed above.

Proposition 2.3.

(1) Suppose R is a ring containing $\mathbb{Z}$, and $\mathbb{Z}$ has a diophantine definition over R. Then there is no algorithm to determine whether an arbitrary finite system of polynomial equations with coefficients in R has solutions in R.

(2) More generally, suppose I is an arbitrary index set, and $\{R_\alpha : \alpha \in I\}$ is a collection of subrings of some ring $\hat{R}$ containing $\mathbb{Z}$. Let $R_0 := \cap_{\alpha \in I} R_\alpha$, and suppose there exists a finite collection of polynomials

$$f_i(t, x_1, \ldots, x_n) \in R_0[t, x_1, \ldots x_n], \quad 1 \leq i \leq m$$

that constitutes a diophantine definition of $\mathbb{Z}$ over R_α for every *$\alpha \in I$. Then there is no algorithm to determine whether an arbitrary finite system of polynomial equations with coefficients in R_0 has solutions in R_α for* some *$\alpha \in I$.*

Proof. Assertion (1) is a special case of (2), where we take I to have only one element. As for (2), let $p(t_1, \ldots, t_r) \in \mathbb{Z}[t_1, \ldots, t_r]$. Then for $\alpha \in I$, the system equations

$$p(t_1, \ldots, t_r) = 0, \quad f_i(t_j, x_{j,1}, \ldots, x_{j,n}) = 0, \quad 1 \leq i \leq m, 1 \leq j \leq r \tag{2.4}$$

have solutions in R_α if and only if the equation $p(t_1, \ldots, t_r) = 0$ has solutions in $\mathbb{Z}$. So if there is an algorithm to determine whether (2.4) has solutions in R_α for some α, then there is an algorithm to determine whether $p(t_1, \ldots, t_r)$ has solutions in $\mathbb{Z}$. □

Here is a brief account of some of the history of diophantine definitions. Using norm equations, diophantine definitions have been obtained for $\mathbb{Z}$ over the rings of algebraic integers of some number fields. J. Denef has constructed a diophantine definition of $\mathbb{Z}$ for the finite degree totally real extensions of $\mathbb{Q}$. J. Denef and L. Lipshitz extended Denef's results to all quadratic extensions of finite degree totally real fields. (These fields include all finite abelian extensions of $\mathbb{Q}$.) T. Pheidas, C. Videla and the third author of this paper have independently constructed diophantine definitions of $\mathbb{Z}$ for number

fields with exactly one pair of non-real conjugate embeddings. Lemma 4.3 below shows that the subfields of all the fields mentioned above "inherit" the diophantine definitions of $\mathbb{Z}$. The proofs of the results listed above can be found in [Den75], [DL78], [Den80], [Phe88], [Vid89], [SS89], and [Shl89].

The first abelian varieties put to use for the purpose of definability were elliptic curves. Perhaps the first mention of elliptic curves in the context of the first-order definability belongs to R. Robinson in [Rob64] and in the context of existential definability and diophantine stability relative to $\mathbb{Q}$ to J. Denef in [Den80]. Using elliptic curves B. Poonen has shown in [Poo02] that if for a number field extension M/K we have an elliptic curve E defined over K, of rank one over K, such that the rank of E over M is also one, then $\mathcal{O}_K$ (the ring of integers of K) is diophantine over $\mathcal{O}_M$. G. Cornelissen, T. Pheidas and K. Zahidi weakened somewhat the assumptions of B. Poonen's theorem. Instead of requiring a rank one curve retaining its rank in the extension, they require existence of a rank one elliptic curve over the number field and an abelian variety or a commutative group-scheme of positive rank defined over $\mathbb{Q}$ and diophantine stable relative to $\mathbb{Q}$ (see [CPZ05]). This paper was the first to use a higher dimensional abelian variety or a group-scheme to show that Hilbert's Tenth Problem is undecidable over a ring of integers of a number field.

Somewhat later B. Poonen and the third author have independently shown that the conditions of B. Poonen's theorem can be weakened to remove the assumption that the rank is one and require only that the rank in the extension is positive and the same as the rank over the ground field, i.e. the elliptic curve is rank stable and with a positive rank (see [Shl08] and [Poo]). Additional use of diophantine stable elliptic curves can be found in [CS08], where G. Cornelissen and the third author of this paper used elliptic curves to define a subfield of a number field using one universal and existential quantifiers. Recent papers by N. Garcia-Fritz and H. Pasten ([GFP20]) and by D. Kundu, A. Lei and F. Sprung ([KLS22]) also use diophantine stability of elliptic curves to construct diophantine definitions of $\mathbb{Z}$ over new families of rings of integers of number fields.

The first two authors showed in [MR10] that if the Shafarevich–Tate conjecture holds over a number field K, then for any prime degree cyclic extension M of K, there exists an elliptic curve of rank one over K, keeping its rank over M. Combined with B. Poonen's theorem, this result shows that the Shafarevich–Tate conjecture implies that Hilbert's Tenth Problem is undecidable over the rings of integers of any number field. While in [MR10], the case of a general extension was reduced to a cyclic extension of prime degree, in fact, it would be enough to show that result holds for any quadratic extension of number fields. The proof of this fact relies on well-known properties of diophantine definitions; see Theorem 4.8 below. R. Murty and H. Pasten produced another conjectural instance where one could use diophantine stability of elliptic curves in finite extensions of number fields to show that $\mathbb{Z}$ has a diophantine definition in the rings of integers ([MP18]). The authors relied on a different set of conjectures for elliptic curves (automorphic, parity and the analytic rank 0 part of the twisted Birch and Swinnerton-Dyer conjecture) and the results from [Shl08] and [Poo] for their proof. An accessible exposition of the proof

can be found in [MF19]. H. Pasten also showed in [Pas22b] that existential definability of $\mathbb{Z}$ over rings of integers of number fields follows from a well-known conjecture on elliptic surfaces.

3. Main theorems: diophantine definitions from diophantine stability

Number field results.

Theorem 3.1. *Let L/K be a number field extension with $\mathcal{O}_L/\mathcal{O}_K$ the corresponding extension of their rings of integers. Let A be an abelian variety defined over K such that* $\operatorname{rank} A(L) = \operatorname{rank} A(K) \geq 1$. *Then $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_L$.*

Remark 3.2. Regarding the diophantine definitions provided by Theorem 3.1, fix the number field K and choose an abelian variety A over K with $\operatorname{rank} A(K) \geq 1$.

(1) For any positive number d there is a single set of equations $\mathcal{F}(K, A, d)$ (i.e., equations of the form described in Definition 2.2), with coefficients in $\mathcal{O}_K$, such that for any field extension L/K of degree $\leq d$ such that $\operatorname{rank} A(L) = \operatorname{rank} A(K)$ that set of equations provides a diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_L$.
(2) By Theorem 16.5 below ([MR18, Theorem 1.2]), if A is a non-CM elliptic curve there are (infinitely) many integers d for which there exist infinitely many pairwise linearly disjoint extensions L/K with $[L : K] = d$ and $\operatorname{rank} A(L) = \operatorname{rank} A(K)$.
(3) Without any restriction on the degree of L, if L is a totally real field or a quadratic extension of a totally real field there is a single set of equations $\mathcal{F}(K, A)$ with coefficients in $\mathcal{O}_K$ that provides a diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_L$ for any field extension L/K such that $\operatorname{rank} A(L) = \operatorname{rank} A(K)$.
(4) If we set $K = \mathbb{Q}$ or let K be any number field with a diophantine definition of $\mathbb{Z}$ over $\mathcal{O}_K$ then Proposition 2.3 applies to each collection of fields described above.

For the proof of Theorem 3.1, see Proposition 14.3 and Lemma 13.8 below. Theorem 3.1 can be sharpened to:

Theorem 3.3. *Let L/K be a number field extension with $\mathcal{O}_L/\mathcal{O}_K$ the corresponding extension of their rings of integers. Let K'/K be a number field extension with K' linearly disjoint from L over K. Put $L' := K'L$. Suppose that the number fields L'/K' are connected by a diophantine chain (cf. Definition 1.3). Then*

(1) the number fields L/K are connected by a diophantine chain,
(2) $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_L$.
(3) If L is a totally real field or a quadratic extension of a totally real field, the diophantine definition in (2) depends only on K and A, and not on L.

Proof. Since the number fields L'/K' are connected by a diophantine chain, there is an $n \geq 0$ and a tower of number fields

$$K' = K'_0 \subset K'_1 \subset \cdots \subset K'_n \supset L'$$

such that for every $i = 1, \ldots, n$ there is an abelian variety A'_i defined over K'_{i-1} satisfying

$$\operatorname{rank} A'_i(K'_{i-1}) = \operatorname{rank} A'_i(K'_i) > 0. \tag{3.4}$$

For $i = 0, 1, \ldots, n$ define

$$K_i := L \cap K'_i. \tag{3.5}$$

Then

$$K_0 = L \cap K'_0 = L \cap K' = K \subset K_1 \subset \cdots \subset K_n = L \cap K'_n \supset L. \tag{3.6}$$

Set A_i to be the "Weil trace" of A'_i with respect to the field extension K'_{i-1}/K_{i-1} (see [Wei82, §1.3]). Then A_i is an abelian variety of dimension $[K'_{i-1} : K_{i-1}] \dim A'_i$ defined over K_{i-1}, and if F is a field containing K_{i-1} and $F \cap K'_{i-1} = K_{i-1}$, then

$$A_i(F) = A'(K'_{i-1}F). \tag{3.7}$$

Using (3.5) and (3.7) with $F = K_{i-1}$ and with $F = K_i$, we have

$$A_i(K_{i-1}) = A'_i(K'_{i-1}), \quad A_i(K_i) = A'_i(K'_{i-1}K_i) \subset A'_i(K'_i).$$

Thus (3.4) and the inclusion $A'_i(K'_{i-1}) \subset A'_i(K'_i)$ show that

$$\operatorname{rank} A_i(K_{i-1}) = \operatorname{rank} A_i(K_i) > 0.$$

This proves (1), with the diophantine chain given by (3.6) and the abelian varieties A_i.

Applying Theorem 3.1 to A_{i-1} for $i = 1, 2, \ldots, n$ shows that each $\mathcal{O}_{K_{i-1}}$ has a diophantine definition over $\mathcal{O}_{K_i}$, and (2) follows from the "transitivity lemma" (Lemma 4.3). Assertion (3) follows from Remark 3.2. □

Combined with Theorem 16.5 below ([MR18, Theorem 1.2]), we get the following corollary.

Corollary 3.8. *For any number field K, there is an integer N_K such that for every prime $\ell > N_K$, and every positive integer n, there exist infinitely many cyclic extensions L/K of degree ℓ^n such that $\mathcal{O}_K$ is diophantine over $\mathcal{O}_L$.*

Proof. Let E be a non-CM elliptic curve defined over K such that $\mathrm{rank}(E(K)) > 0$. (Such a curve always exists.) Then by Theorem 16.5, for all sufficiently large primes ℓ and all n, there are infinitely many cyclic extensions L/K of degree ℓ^n such that $E(L) = E(K)$. Now the corollary follows from Theorem 3.1. □

Results for infinite algebraic extensions of $\mathbb{Q}$. We will generally use boldface letters (e.g., $\mathbf{L}, \mathbf{K}$) to denote fields of algebraic numbers that are allowed to have infinite degree over $\mathbb{Q}$, and normal type (e.g., L, K) for number fields, i.e., fields of finite degree over $\mathbb{Q}$.

Theorem 3.9. *Let* $\mathbf{L}$ *be an algebraic extension of* $\mathbb{Q}$. *Assume that* $\mathbf{L}$ *is totally real or a quadratic extension of a totally real field. Let* $\mathbf{K}$ *be a subfield of* $\mathbf{L}$. *Let* $\mathcal{O}_{\mathbf{L}}/\mathcal{O}_{\mathbf{K}}$ *be the corresponding extension of their rings of integers. Let* A *be an abelian variety defined over* $\mathbf{K}$ *such that* $A(\mathbf{K})$ *contains an element of infinite order and* $A(\mathbf{L})/A(\mathbf{K})$ *is a torsion group. If* $\mathbf{K}$ *is a number field, then* $\mathcal{O}_{\mathbf{K}}$ *has a diophantine definition over* $\mathcal{O}_{\mathbf{L}}$. *If* $\mathbf{K}$ *is an infinite extension of* $\mathbb{Q}$, *then* $\mathcal{O}_{\mathbf{L}}$ *contains a subset* D *such that* D *is diophantine over* $\mathcal{O}_{\mathbf{L}}$ *and* $\mathbb{Z} \subset D \subset \mathcal{O}_{\mathbf{K}}$.

The proof of Theorem 3.9 is similar to that of Theorem 3.1, using Propositions 14.4 and 14.5 below.

Remark 3.10. If K is a number field, then the diophantine definition $f(t, x_1, \ldots, x_\ell)$ of $\mathcal{O}_K$ over $\mathcal{O}_L$ or $\mathcal{O}_{\mathbf{L}}$ constructed in the proofs of Theorems 3.1, 3.3 and 3.9 has the property that for all $t \in \mathcal{O}_K$ there exist $x_1, \ldots, x_\ell \in \mathcal{O}_K$ such that $f(t, x_1, \ldots, x_\ell) = 0$. This follows from the fact that we use points of $A(K)$ to generate rational integers and then a basis of $K/\mathbb{Q}$ to generate all elements of $\mathcal{O}_K$.

Corollary 3.11. *Suppose* $\mathbf{K} \subset \mathbf{L}$ *and* A *are as in Theorem 3.9. If* $\mathbf{K}$ *is a number field then the existential theory of* $\mathcal{O}_{\mathbf{L}}$ *is undecidable. Alternatively, Hilbert's Tenth Problem is undecidable over* $\mathcal{O}_{\mathbf{L}}$.

Proof. By the result of Denef and Lipshitz [DL78] mentioned in §2, $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{K}}$. Combining this with Theorem 3.9 and Lemma 4.3 proves the corollary. □

4. Existential definitions

The basics of existential definability. Recall Definition 2.2 above.

Lemma 4.1. *Let* $\mathcal{O}$ *be an integral domain whose fraction field* K *is not algebraically closed, and suppose* $p(t) \in \mathcal{O}[t]$ *is a (non-constant) polynomial with no root in* K. *Let*

$$\{f_i(x_1, x_2, \ldots, x_m) = 0 : 1 \leq i \leq r\}$$

be a system of polynomial equations over $\mathcal{O}$. Then there exists a single effectively computable polynomial $F(x_1, x_2, \ldots, x_m) \in \mathcal{O}[x_1, x_2, \ldots, x_m]$ such that the solutions to $F = 0$ in $\mathcal{O}^m$ are the same as the common solutions in $\mathcal{O}^m$ of the system $\mathcal{F}$.

Proof. The proof is taken from [Shl06]. Write $p(t) = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_0$ with $a_i \in \mathcal{O}$. If $f, g \in \mathcal{O}[x_1, x_2, \ldots, x_m]$ and $\mathbf{x} \in \mathcal{O}^m$, then

$$(a_n f^n + a_{n-1} f^{n-1} g + \cdots + a_1 f g^{n-1} + a_0 g^n)(\mathbf{x}) = 0 \iff f(\mathbf{x}) = g(\mathbf{x}) = 0.$$

Now we proceed by induction to combine any finite number of polynomials $\{f_1, \ldots, f_r\}$ into one. □

Note that although the degree of $F(x_1, x_2, \ldots, x_m)$ in Lemma 4.1 may be significantly higher than the degree of the polynomials $f_i(x_1, x_2, \ldots, x_m)$ that comprise the system, the number of variables m remains the same.

Here are some easy (and well-known) properties of *existential definability* we use in this paper. The proofs of many of the statements below can be found (among other places) in Chapter 2 of [Shl06].

Lemma 4.2. *The set $\mathcal{O}^\times$ of units in any commutative ring $\mathcal{O}$ (with unit) is existentially definable over the ring $\mathcal{O}$.*

Proof. The polynomial $f(t, s) := ts - 1 \in \mathcal{O}[t, s]$ has a zero for $t = \alpha \in \mathcal{O}$ if and only if $\alpha \in \mathcal{O}^\times$. □

Below, if $\mathbf{K}$ is a subfield of $\bar{\mathbb{Q}}$, then $\mathcal{O}_\mathbf{K}$ will be its ring of integers. The following lemma is proved in [SS89].

Lemma 4.3 *(Transitivity descent for diophantine definitions). Let $\mathbf{K} \subset \mathbf{L} \subset \mathbf{H}$ be algebraic possibly infinite extensions of $\mathbb{Q}$.*

- *If $\mathcal{O}_\mathbf{K}$ has a diophantine definition over $\mathcal{O}_\mathbf{L}$, and $\mathcal{O}_\mathbf{L}$ has a diophantine definition over $\mathcal{O}_\mathbf{H}$, then $\mathcal{O}_\mathbf{K}$ has a diophantine definition over $\mathcal{O}_\mathbf{H}$.*
- *If $\mathbf{H}/\mathbf{L}$ is a finite extension and $\mathcal{O}_\mathbf{K}$ has a diophantine definition over $\mathcal{O}_\mathbf{H}$, then $\mathcal{O}_\mathbf{K}$ has a diophantine definition over $\mathcal{O}_\mathbf{L}$.*

Remark 4.4. In particular, if $\mathbf{H}/\mathbf{K}$ is a finite extension and $\mathcal{O}_\mathbf{K}$ has a diophantine definition over $\mathcal{O}_\mathbf{H}$, then $\mathcal{O}_\mathbf{K}$ has a diophantine definition over $\mathcal{O}_\mathbf{L}$ for every intermediate field $\mathbf{L}$ such that $\mathbf{K} \subset \mathbf{L} \subset \mathbf{H}$.

The following lemma is clear.

Lemma 4.5 *(Intersection). Let $E_1, E_2 \subset \mathcal{O}_K$ be subsets each existentially definable in $\mathcal{O}_K$. Then $E_1 \cap E_2 \subset \mathcal{O}_K$ is existentially definable.*

The following is due to J. Denef ([Den80]).

Lemma 4.6. *Let* $\mathbf{K}$ *be any field of algebraic numbers. The set* $\mathcal{O}_{\mathbf{K}} \setminus \{0\}$ *of non-zero elements of* $\mathcal{O}_{\mathbf{K}}$ *is existentially definable over* $\mathcal{O}_{\mathbf{K}}$.

Proof. Let $x \in \mathcal{O}_{\mathbf{K}}$. We claim that $x \neq 0$ is equivalent to the existential statement

$$\exists y, z, w \in \mathcal{O}_K : (2y-1)(3z-1) = xw.$$

For if $x = 0$, then either $y = 1/2$ or $z = 1/3$, so either y or z is not in $\mathcal{O}_K$. Suppose now $x \neq 0$. Working in the number field $K_0 := \mathbb{Q}(x)$, we can factor the principal ideal $(x) = \mathfrak{a}\mathfrak{b}$, where $(\mathfrak{a}, (2)) = 1$, and $(\mathfrak{b}, (3)) = 1$. (It is possible that either $\mathfrak{a}$ or $\mathfrak{b}$ is the unit ideal.) Choose $y, z \in \mathcal{O}_{K_0}$ such that $2y \equiv 1 \pmod{\mathfrak{a}}$ and $3z \equiv 1 \pmod{\mathfrak{b}}$. Then $(2y-1)(3z-1) \equiv 0 \pmod{\mathfrak{a}\mathfrak{b}}$, and so x divides $(2y-1)(3z-1)$ in $\mathcal{O}_{K_0}$, and therefore in $\mathcal{O}_{\mathbf{K}}$ as well. □

Lemma 4.7. *Let* $\mathbf{L}/K$ *be an algebraic extension possibly of infinite degree, where* K *is a number field. Suppose that there exists a subset* S *of* $\mathcal{O}_K$ *containing* $\mathbb{N}$ *such that* S *has a diophantine definition over* $\mathcal{O}_{\mathbf{L}}$. *Then* $\mathcal{O}_K$ *has a diophantine definition over* $\mathcal{O}_{\mathbf{L}}$.

Proof. Let $\alpha \in \mathcal{O}_{\mathbf{L}}$ be any element such that $K = \mathbb{Q}(\alpha)$ and consider the following subset E of $\mathcal{O}_{\mathbf{L}}$:

$$E = \{x \in \mathcal{O}_{\mathbf{L}} : bx = \sum_{i=0}^{[\mathbb{Q}(\alpha):\mathbb{Q}]} a_i \alpha^i, \text{ with } b \neq 0, \pm a_i, b \in S\}$$

Now if $y \in E$, then $y \in K \cap \mathcal{O}_{\mathbf{L}} = \mathcal{O}_K$ because $b \in \mathcal{O}_K$ and all $a_i \in \mathcal{O}_K$. Conversely, if $y \in \mathcal{O}_K$, then $y \in E$, since every element of $\mathcal{O}_K$ can be represented as the sum in the definition of E with $b \neq 0, a_i \in \mathbb{Z}$. Finally the condition $b \neq 0$ is diophantine over $\mathcal{O}_L$ by Lemma 4.6. □

The following theorem due to the third author was mentioned in the discussion at the end of Section 2.

Theorem 4.8. *Suppose that for every quadratic extension of number fields* L/K *we have that* $\mathcal{O}_K$ *has a diophantine definition over* $\mathcal{O}_L$. *Then* $\mathbb{Z}$ *has a diophantine definition over the ring of integers of any number field.*

Proof. Let M be a number field. By Remark 4.4, without loss of generality we can assume that M is Galois over $\mathbb{Q}$. For any complex embedding $\mathrm{M} \hookrightarrow \mathbb{C}$ consider the corresponding complex conjugation which gives an involution $\sigma : M \to M$ of the field M. Let $M^\sigma \subset M$ be the fixed field of this involution. Since M/M^σ is a quadratic extension, we obtain—from the assumption in the statement of the theorem—that its ring of integers has a

diophantine definition in $\mathcal{O}_M$. By Corollary 4.5 the same is true for the ring of integers in the intersection

$$M^+ := \cap_\sigma M^\sigma.$$

That is, $\mathcal{O}_{M^+}$ has a diophantine definition in $\mathcal{O}_M$. Since M^+ is totally real, the result of Denef [Den80] discussed above gives us that $\mathbb{Z}$ has a diophantine definition in $\mathcal{O}_{M^+}$. By "transitivity" of diophantine definitions (Lemma 4.3) we have that $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_M$. □

Total positivity; replacing inequalities by equations.

Proposition 4.9. *Let* $\mathbf{F}$ *be an algebraic (possibly infinite) extension of* $\mathbb{Q}$. *Let* $x, z \in \mathcal{O}_\mathbf{F}$ *with* $x \neq z$. *Then there exists* $y_1, \dots, y_5 \in \mathcal{O}_\mathbf{F}$ *with* $y_5 \neq 0$ *such that*

$$y_5^2(x - z) = y_1^2 + y_2^2 + y_3^2 + y_4^2 \tag{4.10}$$

if and only if for every embedding $\sigma : \mathbf{F} \hookrightarrow \mathbb{R}$ *we have that* $\sigma(x) > \sigma(z)$.

Proof. The existence of $y_1, \dots, y_5 \in \mathcal{O}_\mathbf{F}$ with $y_5 \neq 0$ implies the inequality $\sigma(x) > \sigma(z)$ for all real embeddings $\sigma : \mathbf{F} \hookrightarrow \mathbb{R}$.

To go the other way, assume the inequality $\sigma(x) > \sigma(z)$ for all real embeddings. It follows that (4.10) has a solution in all real completions of $\mathbf{F}$, and hence in all archimedean completions. In any non-archimedean completion a quadratic form of dimension four represents every element; so (4.10) has a solution in every completion of $\mathbf{F}$. By the Hasse-Minkowski Theorem ([Shi12] Corollary 27.5) it has a solution in $\mathbf{F}$. □

Part 2. On the geometry of group schemes over rings of integers in number fields

5. The conormal bundle to a section of a smooth scheme

Let $S = \mathrm{Spec}(\mathcal{O})$ where $\mathcal{O}$ is a Dedekind domain, and let $X \to S$ be a morphism of finite type and smooth of dimension d. Let $e : S \hookrightarrow X$ be a section. We'll refer to the pair (X, e) as an S**-pointed scheme**. Let $I = I_e$ be the sheaf of ideals on X that cut out the section e. For a general reference to this, see [Gro61, §I.4], especially Proposition 4.1.2.

Denote by $X_{e,[2]} = X_{[2]} \subset X$ the subscheme cut out by I^2. In the language of [Gro61], $X_{e,[2]}$ is a "formal scheme" with support equal to the closed subscheme $e : S \hookrightarrow X_{e,[2]}$ and has I, restricted to $\mathcal{O}_{X_{e,[2]}}$, as its ideal of definition (which is an ideal of square zero in $\mathcal{O}_{X_{[2]}}$).

The pullback $e^*(I/I^2)$ to S is a locally free coherent sheaf of rank d over S (the **conormal bundle** to the section e; for another general reference, cf. [Har77]).

Let

$$\mathcal{N} = \mathcal{N}_{X,e} := H^0(S, e^*(I/I^2)) \quad \subset \quad \mathcal{R}_X = \mathcal{R}_{X,e} := H^0(S, e^*(\mathcal{O}_X/I^2)).$$

So $\mathcal{N}_{X,e}$ is the (locally free, rank d) $\mathcal{O}$-module of sections of the coherent sheaf $e^*(I/I^2)$ over S, viewed as an ideal in $\mathcal{R}_{X,e}$, the $\mathcal{O}$-algebra of global sections (over S) of $e^*(\mathcal{O}_X/I^2)$.

We can write

$$\mathcal{R}_{X,e} = \mathcal{O} \oplus \mathcal{N}_{X,e} = \mathcal{O}[\mathcal{N}_{X,e}],$$

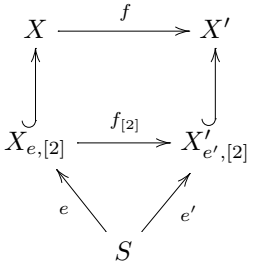
where the object on the right is the $\mathcal{O}$-algebra generated by the $\mathcal{O}$-module $\mathcal{N}_{X,e}$ where the square of $\mathcal{N}_{X,e} \subset \mathcal{R}_{X,e}$ is zero. (Compare: [Gro61, Proposition 10.8.11].)

Proposition 5.1 *(Functoriality).*

(1) There is a canonical isomorphism

$$X_{e,[2]} \simeq \mathrm{Spec}(\mathcal{R}_{X,e}).$$

(2) Let $f : (X, e) \to (X', e')$ be a morphism of smooth (S-pointed) schemes over S. Then f induces (via the canonical mapping $I_X \to f^* I_{X'}$) functorial morphisms



and (correspondingly) contravariant functorial $\mathcal{O}$-homomorphisms

$$\begin{array}{ccc} \mathcal{N}_{X'} & \longrightarrow & \mathcal{N}_X \\ \downarrow & & \downarrow \\ \mathcal{R}_{X'} & \longrightarrow & \mathcal{R}_X. \end{array} \tag{5.2}$$

(3) If $f : X \to X'$ is a closed immersion, so is

$$f_{[2]} : X_{[2]} \to X'_{[2]},$$

and the horizontal morphisms in (5.2) are surjections.

(4) If (X, e) and (X', e') are smooth (S-pointed) schemes over S, letting $(Y, y) := (X, e) \times_S (X', e')$ we have an isomorphism of $\mathcal{O}$-modules

$$\mathcal{N}_{(Y,y)} \simeq \mathcal{N}_{(X,e)} \oplus \mathcal{N}_{(X',e')}.$$

Proof. The statements follow directly from the functoriality of the construction $X \mapsto X_{[2]}$ and the fact that $e' = f \circ e$ so $(e')^* = e^* \circ f^*$. □

6. The conormal bundle to the identity section of a smooth group scheme

We will be dealing with smooth group schemes G of finite type over our base S, which we now suppose to be $\mathrm{Spec}(\mathcal{O}_K)$ for some number field K. Our main applications will use group schemes G that are either

- the Néron model over the base S of an abelian variety $A_{/K}$, or
- the multiplicative group $\mathbf{G}_m$ over S, or more generally a torus over S, or
- (possibly in the future) extensions of these groups.

As the reader will see, we will only be "using" the connected component of the identity of G, so we could restrict to connected group schemes over S. Moreover, there are few properties of G (besides smoothness along the identity section) that are required, in the constructions to follow. Specifically, G needn't be commutative; it needn't even have inverses: it could just be a monoid; more curious is that—although it would take some discussion which we won't enter to explain this: it needn't even be associative. The main requirement is that there be a binary law $\gamma : G \times G \to G$ of schemes over S with a two-sided identity section $e : S \to G$; i.e., such that this diagram is commutative:

$$\begin{array}{ccccc} G = S \times_S G & \xrightarrow{e \times Id} & G \times_S G & \xleftarrow{Id \times e} & G \times_S S = G \\ & \searrow & \downarrow \gamma & \swarrow & \\ & & G & & \end{array}$$

But let $(X, e) = (G, e)$ just be a smooth group scheme of finite type over S pointed by its "identity section." Below we'll begin to drop the e from (G, e) and just call it G.

Lemma 6.1. *Let h denote the class number of the number field K. For G a smooth group scheme of finite type over S, let*

$$G' := \{G\}^h := G \times_S G \times_S \cdots \times_S G$$

denote the h-fold power of G, and $\mathcal{N}_G$ and $\mathcal{N}_{G'}$ their corresponding conormal bundle $\mathcal{O}_K$-modules. Then

$$\mathcal{N}_{G'} = \oplus^h \mathcal{N}_G,$$

and $\mathcal{N}_{G'}$ is a free *(finite rank) $\mathcal{O}_K$-module.*

Proof. The first part of that sentence follows from Proposition 5.1(4). The second follows from the fact that $\mathcal{N}_G$ is locally free over $\mathcal{O}_K$, and if h is the class number of K the h-fold direct sum of any locally free $\mathcal{O}_K$-module is free ([FT93, Theorem II.4.13]). □

Remark 6.2. This lemma will be useful later. Whenever we have a group scheme that is diophantine stable for a field extension L/K, Lemma 6.1 allows us to choose one with the further property that its conormal bundle module $\mathcal{N}_G$ is free over $\mathcal{O}_K$.

Proposition 6.3.

(1) The functor $(G, e) \mapsto G_{e,[2]}$ preserves closed immersions.
(2) The functor $G \mapsto \mathcal{N}_G$ sends closed immersions $G_1 \hookrightarrow G_2$ to surjections

$$\mathcal{N}_{G_2} \longrightarrow \mathcal{N}_{G_1}.$$

(3) If G, H are S-group schemes we have canonical closed immersions of S-schemes

$$\begin{array}{ccccc} (G \times_S H)_{[2]} & \hookrightarrow & G_{[2]} \times_S H_{[2]} & \hookrightarrow & G \times_S H \\ \downarrow = & & \downarrow = & & \\ \mathrm{Spec}(\mathcal{R}_{G\times_S H}) & \hookrightarrow & \mathrm{Spec}(\mathcal{R}_G) \times_S \mathrm{Spec}(\mathcal{R}_H) & & \end{array}$$

(4) Letting $1_G \in \mathcal{R}_G = \mathcal{R}_{G,e}$ denote the unit, and ditto for H, we have a canonical isomorphism of $\mathcal{O}_K$-modules

$$\mathcal{N}_{G\times_S H} \xrightarrow{\simeq} \mathcal{N}_G \otimes_{\mathcal{O}_K} 1_H \oplus 1_G \otimes_{\mathcal{O}_K} \mathcal{N}_H.$$

(5) Let $\gamma : G \times_S G \to G$ denote the group law $(g_1, g_2) \mapsto g_1 g_2$. We have a commutative diagram

$$\begin{array}{ccccccc} \mathrm{Spec}(\mathcal{R}_{G\times_S G}) & \xrightarrow{=} & \{G \times_S G\}_{[2]} & \hookrightarrow & G_{[2]} \times_S G_{[2]} & \hookrightarrow & G \times_S G \\ \downarrow \gamma_{[2]} & & \downarrow \gamma_{[2]} & & \downarrow \gamma & & \downarrow \gamma \\ \mathrm{Spec}(\mathcal{R}_G) & \xrightarrow{=} & G_{[2]} & \hookrightarrow & G & \xrightarrow{=} & G. \end{array}$$

Proof. Items (1) and (2) follow from item (3) of Proposition 5.1. The remaining items follow straight from the definitions or the functoriality of the objects named, except for (4) which is a direct computation.

Note that the natural $\mathcal{O}_K$-homomorphism

$$\mathcal{R}_G \otimes_{\mathcal{O}_K} \mathcal{R}_H \longrightarrow \mathcal{R}_{G\times_S H}$$

is a surjection, but not (necessarily) an isomorphism. □

Proposition 6.4. *Recall that $\gamma : G \times G \to G$ denotes the group operation. The mapping*

$$\gamma_{[2]} : \mathcal{N}_G \longrightarrow \mathcal{N}_{G\times_S G} = (\mathcal{N}_G \otimes_{\mathcal{O}} 1_G) \oplus (1_G \otimes_{\mathcal{O}} \mathcal{N}_G)$$

is given by the formula

$$x \quad \mapsto \quad x \otimes 1_G + 1_G \otimes x. \tag{6.5}$$

Proof. Since e is the identity section we have the commutative diagram

$$\begin{array}{ccccc} e\times G & \hookrightarrow & G\times G & \hookleftarrow & G\times e \\ & \searrow^{=} & \downarrow{\scriptstyle \gamma} & \swarrow_{=} & \\ & & G & & \end{array}$$

which gives us that the composition of

$$\mathcal{N}_G \xrightarrow{\gamma_{[2]}} \mathcal{N}_{G\times_S G} = \mathcal{N}_G \otimes_{\mathcal{O}} 1_G \oplus 1_G \otimes_{\mathcal{O}} \mathcal{N}_G$$

with projection to $\mathcal{N}_G \otimes_{\mathcal{O}} 1_G$ or to $1_G \otimes_{\mathcal{O}} \mathcal{N}_G$ induces the 'identity mapping' (i.e., $x \mapsto x \otimes 1_G$ or $x \mapsto 1_G \otimes x$ respectively). □

Corollary 6.6. *Let G and G' be two smooth group schemes over S. Let $G_0 \subset G$ be an open subscheme containing e, the identity section, and let $G'_0 \subset G'$ be, similarly, an open subscheme containing e', the identity section. We view (G_0, e) and (G'_0, e') as (smooth) S-pointed schemes. Let $\iota : (G_0, e) \to (G'_0, e')$ be a morphism of S-pointed schemes that is a closed immersion of schemes (but ι is not required to extend to a homomorphism, or even a morphism, of the ambient groups). We have a commutative diagram*

$$\begin{array}{ccccccccccc} G\times G & \leftarrow & (G\times G)_{[2]} & \xrightarrow{=} & (G_0\times G_0)_{[2]} & \xrightarrow{\iota\times\iota} & (G'_0\times G'_0)_{[2]} & \xrightarrow{=} & (G'\times G')_{[2]} & \hookrightarrow & G'\times G' \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \gamma_{[2]}} & & \downarrow{\scriptstyle \gamma_{[2]}} & & \downarrow{\scriptstyle \gamma'_{[2]}} & & \downarrow{\scriptstyle \gamma'_{[2]}} & & \downarrow{\scriptstyle \gamma'} \\ G & \leftarrow & G_{[2]} & \xrightarrow{=} & G_{0\,[2]} & \xrightarrow{\iota} & G'_{0\,[2]} & \xrightarrow{=} & G'_{[2]} & \hookrightarrow & G'. \end{array} \tag{6.7}$$

Remark 6.8. We will make use of this discussion in the case where $G = \mathcal{A}$ is the Néron model of an abelian variety, and $G' = \mathrm{Aff}^n$ is n-dimensional affine space. The key fact we use is Proposition 6.4 and the commutativity of the inner square in diagram (6.7) (and this follows directly from the formula (6.5)).

7. A prepared group scheme

Fix a number field K.

Projective space over $\mathcal{O}_K$. For n a positive integer, consider n-dimensional projective space $\mathbb{P}^n$ viewed as a scheme (over $\mathbb{Z}$, or more relevant to our context, over $\mathcal{O}_K$). A point in $\mathbb{P}^n$ rational over K (which is the same as being rational over $\mathcal{O}_K$) can be represented in $n+1$ homogeneous coordinates (not all of them 0),

$$(x_1 : x_2 : \cdots : x_{n+1})$$

for $x_i \in K$ noting that such a representation is unique up to scalar multiplication by a nonzero element in K. Two such vectors $(x'_1 : x'_2 : \cdots : x'_{n+1}), (x_1 : x_2 : \cdots : x_{n+1})$ are *equivalent* if and only if there is a nonzero element $c \in K$ such that $x'_i = cx_i$ for $i = 1, 2, \ldots n+1$. Any such point can therefore be represented by such a vector with $x_i \in \mathcal{O}_K$. (Below, we keep to the convention that the colons signify that we are considering "homogeneous coordinates.")

Definition 7.1. In the special case that the entries $a_1, a_2, \ldots, a_{n+1}$ of an $n+1$-vector

$$\alpha = (a_1 : a_2 : \cdots : a_{n+1})$$

generates a principal ideal "$\gcd(\alpha)$" $= (a) \subset \mathcal{O}_K$, define

- the **denominator** of α to be

$$\delta(\alpha) := a_{n+1}/a \subset \mathcal{O}_K,$$

  noting that $\delta(\alpha)$ is only well-defined up to a unit in K—i.e., it is only the principal ideal generated by $\delta(\alpha)$ that is well-defined,
- the **numerator** of α to be

$$\nu(\alpha) := \text{the ideal } (a_1/a, a_2/a, \ldots, a_n/a) \subset \mathcal{O}_K,$$

noting that $\nu(\alpha)$ and $\delta(\alpha)$ are relatively prime—i.e., the ideal generated by $\nu(\alpha)$ and $\delta(\alpha)$ is the unit ideal.

Affine space over $\mathcal{O}_K$. We view affine n-dimensional space

$$\mathrm{Spec}(\mathcal{O}_K[y_1, y_2, \dots, y_n]) =: \mathrm{Aff}^n \simeq \mathbf{G}_a^n$$

as an additive group scheme over $\mathcal{O}_K$; with

$$e := (0, 0, \dots, 0) \in \mathrm{Aff}^n$$

its zero-section (cut out by the ideal $I := (y_1, y_2, \dots, y_n) \subset \mathcal{O}_K[y_1, y_2, \dots, y_n]$).

Letting $\mathbb{P}^{n-1} \simeq H \subset \mathbb{P}^n$ denote the hyperplane defined by $x_{n+1} = 0$, we have an isomorphism

$$\mathrm{Aff}^n \simeq \mathbb{P}^n \setminus H \subset \mathbb{P}^n,$$

defined by

$$(a_1, a_2, \dots, a_n) \mapsto (a_1 : a_2 : \cdots : a_n : 1).$$

"Going the other way:" if $(a_1 : a_2 : \cdots : a_n : a_{n+1})$ is a homogeneous representative of a point $\mathbf{a} \in \mathbb{P}^n(\mathcal{O}_K)$, where $a_{n+1} \neq 0$, denote by

$$\mathbf{a}^! := (\frac{a_1}{a_{n+1}}, \frac{a_2}{a_{n+1}}, \dots, \frac{a_n}{a_{n+1}}) \in \mathrm{Aff}^n\big(\mathcal{O}_K[\frac{1}{a_{n+1}}]\big). \tag{7.2}$$

Remark 7.3. If the ideal $(a_1, a_2, \dots, a_n) \in \mathcal{O}_K$ is relatively prime to the ideal (a_{n+1}) then $\mathbf{a}^!$ reduces to a well-defined element—call it $\mathbf{a}^!_{[2]}$—in the quotient

$$\mathcal{O}_K^n/(a_1, a_2, \dots, a_n)^2\mathcal{O}_K^n.$$

Visibly, $\mathbf{a}^!_{[2]}$ is dependent only on the equivalence class of $(a_1 : a_2 : \cdots : a_n : a_{n+1})$ as long as the hypothesis in Remark 7.3 holds. This will be relevant in the discussion below.

We will be working with the quotient: $\mathcal{O}_K \to \mathcal{O}_K[y_1, y_2, \dots, y_n]/I^2$. Form the corresponding closed subscheme

$$\mathrm{Aff}^n_{[2]} := \mathrm{Spec}(\mathcal{O}_K[y_1, y_2, \dots, y_n]/I^2) \subset \mathrm{Aff}^n = \mathrm{Spec}(\mathcal{O}_K[y_1, y_2, \dots, y_n]).$$

An embedded group scheme

Assumption 7.4. Let G be a smooth connected quasi-projective group scheme over $S = \mathrm{Spec}(\mathcal{O}_K)$. Assume further that the conormal bundle module, $\mathcal{N}_G$ is free over $\mathcal{O}_K$ (see Lemma 6.1 and Remark 6.2).

There is a positive integer n and an $\mathcal{O}_K$-morphism of schemes

$$G \overset{\iota}{\hookrightarrow} \mathbb{P}^n$$

that is a local immersion, identifying G with a locally closed $\mathcal{O}_K$-subscheme of $\mathbb{P}^n$.

Denote by e the zero-section of G over $\mathcal{O}_K$, and let $\mathfrak{I}$ be the sheaf of ideals in G that cuts out e.

Recall the construction $G_{[2]} \subset G$ of §6; i.e., the subscheme of G cut out by $\mathfrak{I}^2$.

Proposition 7.5. *If $\bar{G} \subset \mathbb{P}^n$ is the Zariski-closure of the $\mathcal{O}_K$-subscheme $G \subset \mathbb{P}^n$, then setting*

$$\mathcal{X} := \bar{G} \setminus G \subset \mathbb{P}^n,$$

the support of $\mathcal{X}$ is disjoint from the zero-section e.

Proof. Since the group scheme G is smooth along the zero-section, the injection $G \hookrightarrow \bar{G}$ induces an isomorphism on normal bundles along the zero-section, establishing the proposition. □

Remark 7.6. If, for example, $G = \mathcal{A}$, the Néron model of an abelian variety A over K, then the support of $\mathcal{X}$ in Proposition 7.5 is concentrated in fibers of $\mathcal{A} \to \mathrm{Spec}(\mathcal{O}_K)$ over the finite punctual subscheme $\Sigma_{\mathrm{bad}}(A) \subset \mathrm{Spec}(\mathcal{O}_K)$ where $\Sigma_{\mathrm{bad}}(A)$ is the set of bad primes of A, i.e.:

$$\Sigma_{\mathrm{bad}}(A) := \sqcup_{\mathfrak{p}|\mathrm{cond}(A)}\, \mathrm{Spec}(k_{\mathfrak{p}}).$$

(Here $k_{\mathfrak{p}}$ is the residue field of the prime $\mathfrak{p}$ of K, and $\mathrm{cond}(A)$ is the conductor of $A_{/K}$.)

Definition 7.7. An injective (local immersion) $\mathcal{O}_K$-morphism $\iota : G \hookrightarrow \mathbb{P}^n$ will be called **well-arranged** if both of the following properties hold:

- ι takes any point $P \in G(\mathcal{O}_K)$ to a point $\iota(P) \in \mathbb{P}^n$ that can be written in homogeneous coordinates $(a_1 : a_2 : \cdots : a_{n+1})$ with $a_i \in \mathcal{O}_K$, and such that the ideal generated by the entries, $(a_1, a_2, \ldots, a_{n+1}) \subset \mathcal{O}_K$, is the unit ideal,
- ι takes the zero-section, $e \in G$ to the point $(0 : 0 : \cdots : 0 : 1)$—this being written in homogeneous coordinates; i.e., $x_{n+1} = 1$:

$$\begin{array}{ccccc} e & \xrightarrow{\iota} & e & \xleftarrow{=} & e \\ \downarrow & & \downarrow & & \downarrow \\ G & \xrightarrow{\iota} & \mathbb{P}^n & \hookleftarrow & \mathrm{Aff}^n \end{array}$$

Proposition 7.8. *Let*

$$\begin{array}{ccc} S & \xrightarrow{s} & \mathbb{P}^n \\ & \searrow^{=} & \downarrow \\ & & S \end{array}$$

be an S-section. Then there is an injective S-morphism $\mathfrak{v} : \mathbb{P}^n \hookrightarrow \mathbb{P}^N$ for some N such that

(1) the image of any S-section of $\mathbb{P}^n$ in $\mathbb{P}^N$, when written in homogeneous coordinates $(a_1 : a_2 : \cdots : a_{N+1})$ has the property that the ideal generated by the entries, $(a_1, a_2, \ldots, a_{N+1}) \subset \mathcal{O}_K$, is a principal ideal in $\mathcal{O}_K$, and hence after scaling can be taken to be the unit ideal, and
(2) $\mathfrak{v}(s) = (0 : 0 : \cdots : 0 : 1)$.

Proof. Let $h = h_K$ denote the class number of K. Let

$$\mathfrak{v}_{n,h} : \mathbb{P}^n \to \mathbb{P}^N$$

(with $N := \binom{n+h}{n} - 1$) be the h-fold Veronese embedding of $\mathbb{P}^n_{/\mathcal{O}_K}$ in $\mathbb{P}^N_{/\mathcal{O}_K}$ (see for example [Sha74, §1.4.4.2]), i.e., the embedding defined by the rule

$$(x_1, x_2, \ldots x_{n+1}) \overset{\mathfrak{v}_{n,h}}{\longmapsto} (\mu_1(x_1, \ldots, x_{n+1}) \ldots, \mu_N(x_1, \ldots, x_{n+1})),$$

where the entries of the vector on the right, $\mu_k(x_1, \ldots, x_{n+1})$, run through the $N+1$ monomials of degree h in the variables $x_1, x_2, \ldots, x_{n+1}$.

For any K-valued point $\alpha \in \mathbb{P}^n(K)$ represented by the $n+1$-vector $(a_1, a_2, \ldots a_{n+1})$ the $\mathcal{O}_K$-fractional ideal generated by the entries $\mu_k(a_1, \ldots, a_{n+1})$ of the vector $\mathfrak{v}_{n,h}(\alpha)$ is the h-th power of the fractional ideal generated by the entries of α. So this (fractional) ideal is principal. By scaling our homogeneous coordinates by dividing each entry by the inverse of a generator of that principal ideal we get assertion (1) of the proposition.

For part (2) of the proposition, let the image of the section s (i.e., $\mathfrak{v}_{n,h}(s) \in \mathbb{P}^N(\mathcal{O}_K)$) be represented by the point $\tau := (\tau_1, \tau_2, \ldots, \tau_{N+1}) \in \mathrm{Aff}^{N+1}(\mathcal{O}_K)$ where the entries generate the unit ideal. Let $W := \mathrm{Aff}^{N+1}(\mathcal{O}_K)$ and let $T := \tau\mathcal{O}_K \subset W$ be the cyclic $\mathcal{O}_K$-module generated by τ. Then $W_0 := W/T$ is a torsion-free $\mathcal{O}_K$-module, and hence projective, so the exact sequence

$$0 \longrightarrow T \longrightarrow W \longrightarrow W_0 \longrightarrow 0$$

splits. Therefore $W \cong W_0 \oplus T$, and by the classification theorem for projective modules (of finite rank) over Dedekind domains (see for example [FT93, Theorem II.4.13]), since

W and T are free over $\mathcal{O}_K$, so is W_0. It follows that we can find an $\mathcal{O}_K$-basis of W where the first N elements of that basis generate W_0. That is, there is an $\mathcal{O}_K$-linear change of coordinates of Aff^{N+1} so that after that change Aff^{N+1} is given by coordinates $(z_1, z_2, \ldots, z_N, z_{N+1})$ where Aff^N is cut out by $z_{N+1} = 0$ and the element τ has coordinates $(0, 0, \ldots, 0, 1)$. □

Corollary 7.9. *Let G be a group scheme over $S = \mathrm{Spec}(\mathcal{O}_K)$ satisfying Assumption 7.4. There is a well-arranged injective S-morphism $G \overset{\iota}{\hookrightarrow} \mathbb{P}^n$ (for some positive number n). For any rational point, $P : S \to G$, its image, $\lambda(P) := \iota P(S) \in \mathbb{P}^n$, when written in homogeneous coordinates $\lambda(P) = (\lambda_1(P), \ldots, \lambda_{n+1}(P))$ has the property that the entries $\lambda_i(P)$ for $i = 1, 2, \ldots, n$ generate a principal ideal in $\mathcal{O}_K$—equivalently: one can arrange the homogeneous coordinates of $\lambda(P)$ by appropriate scalar multiplication so that the entries generate the unit ideal.*

8. The open piece in $\bar{G}$

From now on, we will fix a quasi-projective group scheme G over $S = \mathrm{Spec}(\mathcal{O}_K)$ as in Assumption 7.4 such that its conformal bundle module $\mathcal{N}_G$ is free over $\mathcal{O}_K$ (using Lemma 6.1) and with a fixed well-arranged injective S-morphism $G \overset{\iota}{\hookrightarrow} \mathbb{P}^n$ (this being guaranteed to exist by Corollary 7.9).

Recall its Zariski-closure $G \subset \bar{G} \overset{\iota}{\hookrightarrow} \mathbb{P}^n$ as defined in 7.5. Letting $H \subset \mathbb{P}^n$ be the hyperplane described in §7 above, i.e., cut out by $x_{n+1} = 0$. Let $B := \bar{G} \cap H \subset G$ denote the divisor in $\bar{G}$ at infinity.

Definition 8.1. Let $\bar{G}_0 \subset \bar{G}$ be the Zariski-dense open ($\mathcal{O}_K$-scheme) defined by the cartesian diagram:

$$\begin{array}{ccccccc}
e & \longrightarrow & \bar{G}_0 := \bar{G} \cap \mathrm{Aff}^n & \longrightarrow & \bar{G} \setminus B & \longrightarrow & G \\
\downarrow{\scriptstyle =} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} & & \downarrow{\scriptstyle \iota} \\
e & \longrightarrow & \mathrm{Aff}^n & \xrightarrow{=} & \mathbb{P}^n \setminus H & \longrightarrow & \mathbb{P}^n
\end{array}$$

The $\mathcal{O}_K$-scheme $\bar{G}_0$ is an affine scheme, immersed as a closed subscheme of Aff^n, and contains an open subscheme of the zero-section e in G.

The injection

$$\bar{G}_0 \overset{\iota}{\hookrightarrow} \mathrm{Aff}^n$$

is induced by the (surjective) ring homomorphism

$$\iota : \mathcal{O}_K[x_1, x_2, \ldots, x_n] \longrightarrow \mathcal{O}_K[x_1, x_2, \ldots, x_n]/(t_1, t_2, \ldots, t_m)$$

where

$$t_j(x_1, x_2, \ldots, x_n) \in I \subset \mathcal{O}_K[x_1, x_2, \ldots, x_n]; \text{ for } j = 1, 2, \ldots, m$$

are the polynomials (all with 'no constant term') that cut out the affine subscheme $\bar{G}_0$ in Aff^n. (Recall that I is the ideal generated by the x_i.)

Passing to quotients by I^2 we have:

$$\begin{array}{ccc} \iota : \mathcal{O}_K[x_1, x_2, \ldots, x_n] & \longrightarrow & \mathcal{O}_K[x_1, x_2, \ldots, x_n]/(t_1, t_2, \ldots, t_m) \\ \downarrow & & \downarrow \\ \iota_{[2]} : \mathcal{O}_K[x_1, x_2, \ldots, x_n]/I^2 & \longrightarrow & \mathcal{O}_K[x_1, x_2, \ldots, x_n]/(t_1, t_2, \ldots, t_m, I^2) \end{array} \tag{8.2}$$

these being the ring homomorphisms inducing the morphisms of affine schemes:

$$\begin{array}{ccc} \mathrm{Aff}^n & \hookleftarrow & \bar{G}_0 \\ \uparrow & & \uparrow \\ \mathrm{Aff}^n_{[2]} & \leftarrow & \bar{G}_{0,[2]} = G_{[2]}. \end{array}$$

Lemma 8.3. *After an appropriate $\mathcal{O}_K$-linear automorphism of the group scheme Aff^n we may rewrite the surjective ring homomorphism of* (8.2)

$$\iota_{[2]} : \mathcal{O}_K[x_1, x_2, \ldots, x_n]/I^2 \to \mathcal{O}_K[x_1, x_2, \ldots, x_n]/(t_1, t_2, \ldots, t_m, I^2) \tag{8.4}$$

that induces the group scheme morphism $G_{[2]} \overset{\iota}{\hookrightarrow} \mathrm{Aff}^n_{[2]}$ as the projection

$$\iota_{[2]} : \mathcal{O}_K[x_1, x_2, \ldots, x_n]/(x_1, x_2, \ldots, x_n)^2 \to \mathcal{O}_K[x_1, x_2, \ldots, x_d]/(x_1, x_2, \ldots, x_d)^2$$

where d is the dimension of the group scheme $G_{/K}$, and the mapping $\iota_{[2]}$ is given by:

- $x_i \mapsto x_i$ *if* $i \leq d$, *and*
- $x_i \mapsto 0$ *if* $d < i \leq n$.

Proof. This uses the fact that the group scheme G is smooth, its conormal bundle module $\mathcal{N}_G$ is free over $\mathcal{O}_K$, and the injection $G \hookrightarrow \mathbb{P}^n$ is well-arranged. To be explicit, consider the ideal $J := (t_1, t_2, \ldots, t_m, I^2)$, so we may rewrite (8.4) above as

$$\iota_{[2]} : \mathcal{O}_K[x_1, x_2, \ldots, x_n]/I^2 \to \mathcal{O}_K[x_1, x_2, \ldots, x_n]/J,$$

and we can find $n - d$ generators for the free $\mathcal{O}_K$-module J/I^2. Letting $\{t_j;\ j = 1, 2, \ldots, n-d\} \subset J$ be lifts of those generators, the ideal $J := (t_1, t_2, \ldots, t_{n-d}, I^2)$ as positioned in the sequence of ideals

$$I^2 = (x_1, x_2, \ldots, x_n)^2 \subset J = (t_1, t_2, \ldots, t_{n-d}, I^2) \subset I = (x_1, x_2, \ldots, x_n) \subset \mathcal{O}_K$$

has the property that J/I^2 is a free $\mathcal{O}_K$-module with $n-d$ generators

$$\{t_j;\ j=1,2,\dots,n-d\}$$

and is—as (free) $\mathcal{O}_K$-submodule of the free $\mathcal{O}_K$-module I/I^2—a direct summand. That is, there is a free $\mathcal{O}_K$-submodule $\mathcal{U}\subset I/I^2$ such that:

$$I'^2 = J/J^2 \oplus \mathcal{U}.$$

It follows that after a linear change of variables (over $\mathcal{O}_K$) we can arrange it so that $t_i \equiv x_{d+i} \mod I^2$ for $i=1,2,\dots,n-d$. □

Corollary 8.5. *Keeping to the above notation, and the terminology of §6 we have:*

(1) $\mathcal{R}_G = \mathcal{O}_K[x_1,x_2,\dots,x_d]/(x_1,x_2,\dots,x_d)^2$,

(2) $\mathcal{N}_G = \bigoplus_{i=1}^{d} \bar{x}_i\mathcal{O}_K$ *where* $\bar{x}_i$ *is the image of* x_i *in* $\mathcal{O}_K[x_1,x_2,\dots,x_d]/(x_1,x_2,\dots,x_d)^2$,

(3) $\mathcal{N}_G^* = \bigoplus_{i=1}^{d} \bar{x}_i^*\mathcal{O}_K$ *where* $\bar{x}_i^* : \mathcal{N}_G \to \mathcal{O}_K$ *is the ring homomorphism sending* $\bar{x}_i$ *to* $1\in\mathcal{O}_K$ *and* $\bar{x}_j$ *to* 0 *if* $j\neq i$.

9. Vanishing and congruence ideals

Recall that we have fixed a group scheme G satisfying Assumption 7.4 above. Denote by $e: S\to G$ its identity-section. To say that G is quasi-projective means the structure morphism $G\to S$ is a quasi-projective morphism (see [Gro61, Definition 5.3.1]) hence is of finite type, and since S is an affine noetherian scheme, $G\to S$ is a morphism of finite presentation. Let P be an $\mathcal{O}_K$-point of G.

Definition 9.1. By the **vanishing ideal of** P we mean the ideal $z_P\subset\mathcal{O}_K$ defining the intersection of the S-section P with the identity section.

By the **congruence ideal of** P we mean the ideal $c_P\subset\mathcal{O}_K$ defining the intersection of the S-section P with the subscheme $G_{[2]}\subset G$.

That is, the ideals z_P and c_P are the ideals that fit into diagram (9.2) below where the rectangles are cartesian.

$$\begin{array}{ccccc}
\mathrm{Spec}(\mathcal{O}_K/z_P) & \hookrightarrow & \mathrm{Spec}(\mathcal{O}_K/c_P) & \hookrightarrow & S \\
\downarrow & & \downarrow{\scriptstyle P_{[2]}} & & \downarrow{\scriptstyle P} \\
S & \xrightarrow{\ e\ } & G_{[2]} & \hookrightarrow & G \\
\downarrow{\scriptstyle \simeq} & & \downarrow{\scriptstyle \simeq} & & \\
\mathrm{Spec}(\mathcal{O}_K) & \hookrightarrow & \mathrm{Spec}(\mathcal{R}_G) & &
\end{array} \tag{9.2}$$

Lemma 9.3.

(1) The ideal c_P is the square of the ideal z_P.
(2) For $P = e$, the identity section, we have that z_e and c_e are equal to (0). If $P \neq e$ then z_P and c_P are nonzero ideals.
(3) Let Q, P be $\mathcal{O}_K$-valued points of G. Then (writing the group law of G multiplicatively) $z_{Q\cdot P}$ is contained in the ideal (z_Q, z_P) generated by z_Q and z_P.

Proof. (1) Recalling that the identity section $S \overset{e}{\hookrightarrow} G$ is the subscheme cut out by the sheaf of ideals $\mathcal{I} \subset \mathcal{O}_G$, and $G_{[2]} \overset{e}{\hookrightarrow} G$ is the subscheme cut out by the square of that sheaf of ideals $\mathcal{I}^2 \subset \mathcal{O}_G$, cartesian-ness of (9.2) then implies that ideal c_P is the square of the ideal z_P.
(2) The cartesian square

$$\begin{array}{ccc} \mathrm{Spec}(\mathcal{O}_K/z_e) & \hookrightarrow & S \\ \downarrow & & \downarrow{\scriptstyle P=e} \\ S & \xrightarrow{e} & G \end{array}$$

gives us that $\mathrm{Spec}(\mathcal{O}_K/z_e) = S$; so $z_e = (0)$, and hence $c_e = z_e^2 = (0)$ as well.
(3) Briefly: note that P and Q restricted to the base $\mathrm{Spec}(\mathcal{O}_K/(z_P, z_Q))$ are both equal to the identity section (over that base), so their product is as well. □

Lemma 9.4. *For $\nu \in \mathbb{N}$, let $Q = P^\nu$. Then $z_Q \subset z_P$.*

Proof. Induction on ν, using Lemma 9.3(3). □

10. Coordinates of rational points

Assume now that we have arranged coordinates as in Lemma 8.3 and Corollaries 8.5 and 7.9. The $\mathcal{O}_K$-rational point P of G and its image $\iota(P) \in \mathbb{P}^n$ fit into a diagram

$$\begin{array}{ccccc} S = \mathrm{Spec}(\mathcal{O}_K) & \xrightarrow{P} & G & \xrightarrow{\iota} & \mathbb{P}^n \\ \downarrow & & \downarrow & & \uparrow \\ \mathrm{Spec}(\mathcal{O}_K/c_P) & \longrightarrow & G_{[2]} & \xrightarrow{\iota_{[2]}} & \mathrm{Aff}^n_{[2]} \\ \downarrow & & \downarrow & & \uparrow \\ \mathrm{Spec}(\mathcal{O}_K/z_P) & \longrightarrow & e & \xrightarrow{\simeq} & e \end{array}$$

and the image $\iota(P) := \iota P(S) \in \mathbb{P}^n$ has homogeneous coordinates

$$\lambda(P) = \big(\lambda_1(P) : \lambda_2(P) : \cdots : \lambda_n(P) : \lambda_{n+1}(P)\big) \in \mathrm{Aff}^{n+1}(\mathcal{O}_K)$$

where the elements

$$\{\lambda_1(P), \lambda_2(P), \ldots, \lambda_n(P), \lambda_{n+1}(P)\} \subset \mathcal{O}_K$$

generate the unit ideal. In particular, the ideal generated by $\{\lambda_1(P), \ldots, \lambda_n(P)\}$ and the principal ideal generated by $\lambda_{n+1}(P)$ are relatively prime ideals in $\mathcal{O}_K$. Also, using Lemma 8.3 and Corollary 8.5 we may assume that $\lambda_j(P) = 0$ for $d < j \leq n$.

Proposition 10.1. *The vanishing ideal z_P is the ideal generated by*

$$\{\lambda_1(P), \ldots, \lambda_n(P)\}.$$

Proof. This follows directly from the definitions. □

If

$$\mathbf{a} := (\lambda_1 : \lambda_2 : \cdots : \lambda_n : \lambda_{n+1}) \ \in \ \mathcal{O}_K^{n+1}$$

are homogeneous coordinates for the point P with properties described above, then letting $\delta(P) := \lambda_{n+1}$ (i.e., the denominator), with notation defined in (7.2) above we may write:

$$\mathbf{a}^! = (\frac{\lambda_1(P)}{\delta(P)}, \frac{\lambda_2(P)}{\delta(P)}, \ldots, \frac{\lambda_n(P)}{\delta(P)}) \in \big(\mathcal{O}_K[\frac{1}{\delta(P)}]\big)^n$$

Write the morphism $P_{[2]} : \mathrm{Spec}(\mathcal{O}_K/c_P) \to G_{[2]}$ as a homomorphism of the underlying affine rings,

$$P_{[2]} : \mathcal{O}_K \oplus \mathcal{N}_G \ = \ \mathcal{R}_G \to \mathcal{O}_K/c_P. \tag{10.2}$$

Consider the $\mathcal{O}_K$-dual of the locally free $\mathcal{O}_K$-module $\mathcal{N}_G$

$$\mathcal{N}^* = \mathcal{N}_G^* = \mathrm{Hom}_{\mathcal{O}_K}(\mathcal{N}_G, \mathcal{O}_K) \tag{10.3}$$

Definition 10.4. If P is an S-section of $G_{/S}$ let $\partial P \in \mathcal{N}^* \otimes_{\mathcal{O}_K} (\mathcal{O}_K/c_P)$ denote the element (in $\mathcal{N}^* \otimes_{\mathcal{O}_K} (\mathcal{O}_K/c_P) \ = \ \mathcal{N}^* \otimes_{\mathcal{O}_K} (\mathcal{O}_K/z_P^2)$) determined by the $\mathcal{O}_K$-homomorphism $P_{[2]}$ restricted to $\mathcal{N}_G$ in (10.2).

Using the quotation marks below to indicate passing to the quotient

$$\mathcal{O}_K[\frac{1}{\delta(P)}] \to \mathcal{O}_K/z_P^2$$

we get

$$\mathbf{a}^!_{[2]} = \text{“}\left(\frac{\lambda_1(P)}{\delta(P)}, \frac{\lambda_2(P)}{\delta(P)}, \dots, \frac{\lambda_d(P)}{\delta(P)}, 0, 0, \dots 0\right)\text{”} \in (\mathcal{O}_K/z_P^2)^n,$$

and using Lemma 8.3 and (8.4), we get that coordinates for ∂P are given by:

$$\partial P = \text{“}\left(\frac{\lambda_1(P)}{\delta(P)}, \frac{\lambda_2(P)}{\delta(P)}, \dots, \frac{\lambda_d(P)}{\delta(P)}\right)\text{”} \in z_P(\mathcal{N}_G^* \otimes_{\mathcal{O}_K} \mathcal{O}_K/z_P^2) \subset (\mathcal{N}_G^* \otimes_{\mathcal{O}_K} \mathcal{O}_K/z_P^2). \tag{10.5}$$

Definition 10.6. If R is a commutative ring, and W is a free R-module of finite rank, an element $w \in W$ is called a **basis element** if any of the following equivalent properties hold:

- $W/(Rw)$ is a free R-module;
- w is a member of a basis of the free R-module W;
- if I is any nonunit ideal of R then $w \notin IW$.

Lemma 10.7. *Let P be a section of G that is* not *the identity section, so $z_P \neq 0$. Suppose, as well, that z_P is not the unit ideal. Let*

$$\mathcal{W}_P := \mathcal{N}^* \otimes_{\mathcal{O}_K} (z_P/z_P^2) \subset \mathcal{N}^* \otimes_{\mathcal{O}_K} (\mathcal{O}_K/z_P^2).$$

Then

(1) $\partial P \equiv 0 \pmod{\mathcal{N}^* \otimes_{\mathcal{O}_K} z_P}$, so $\partial P \in \mathcal{W}_P$,
(2) the $\mathcal{O}_K/z_P$ module $\mathcal{W}_P$ is free over $\mathcal{O}_K/z_P$,
(3) ∂P is a basis element of $\mathcal{W}_P$.

Proof. Assertions (1) and (3) follow directly from the definition of vanishing ideal, while assertion (2) follows from the fact that $\mathcal{N}^*$ is locally free over $\mathcal{O}_K$. □

Remark 10.8. With notation as in Lemma 10.7, if P, Q are S-sections with property that $z_Q \subset z_P$ we have the natural $\mathcal{O}_K$-module homomorphism

$$\mathcal{W}_Q \xrightarrow{\iota(P,Q)} \mathcal{W}_P.$$

Proposition 10.9. $\partial(P \cdot Q) \equiv \partial(P) + \partial(Q) \pmod{(c_Q, c_P)}$.

Proof. The mapping $(P \cdot Q)_{[2]} : \mathcal{R}_G \to \mathcal{O}_K$ is given by the composition of the maps

$$\mathcal{R}_G \xrightarrow{\gamma_{[2]}} \mathcal{R}_{G \times_{\mathcal{O}_K} G} \xrightarrow{\phi} \mathcal{O}_K$$

where ϕ restricted to $\mathcal{N}_G \otimes_{\mathcal{O}_K} 1$ is $P_{[2]} \otimes_{\mathcal{O}_K} 1$, and ϕ restricted to $1 \otimes_{\mathcal{O}_K} \mathcal{N}_G$ is $1 \otimes_{\mathcal{O}_K} Q_{[2]}$. The result follows from Proposition 6.4. □

Corollary 10.10. *Let $Q = P^\nu$. Then*

$$\partial Q = \nu \cdot \partial P \in \mathcal{W}_P.$$

Proof. This follows from Lemmas 9.3(1) and 9.4 and Proposition 10.9. □

Part 3. Proof of the main theorems

We will keep to the convention that a field of algebraic numbers that is allowed to have infinite degree over $\mathbb{Q}$ will be put in boldface, e.g., $\mathbf{L}, \mathbf{K}$, but if it is assumed to be a number field, i.e., a field of finite degree over $\mathbb{Q}$, it will be in normal type, e.g., L, K.

11. Capturing subrings by congruences

Lemma 11.1. *Let L/K be an extension of number fields, $\mathcal{O}_L/\mathcal{O}_K$ their corresponding rings of integers, and let M/K be the Galois closure of L/K. Let $\alpha \in \mathcal{O}_L$ and $b \in \mathcal{O}_K$. Suppose there exists an ideal $I \subset \mathcal{O}_K$ with the following properties:*

$$|\mathbf{N}_{M/\mathbb{Q}}(I\mathcal{O}_M)| > |\mathbf{N}_{M/\mathbb{Q}}(\alpha - \beta)| \text{ for every conjugate } \beta \text{ of } \alpha \text{ over } K, \tag{11.2}$$

$$\alpha \equiv b \pmod{I\mathcal{O}_L}. \tag{11.3}$$

Then $\alpha \in \mathcal{O}_K$.

Proof. Since $I \subset \mathcal{O}_K$, it follows from (11.3) that every conjugate β of α satisfies $\beta \equiv b \pmod{I\mathcal{O}_M}$. Therefore $\alpha - \beta \equiv 0 \pmod{I\mathcal{O}_M}$. Consequently,

$$\mathbf{N}_{M/\mathbb{Q}}(\alpha - \beta) \equiv 0 \pmod{\mathbf{N}_{M/\mathbb{Q}}(I\mathcal{O}_M)}$$

in $\mathbb{Z}$. Thus, either $\alpha = \beta$ or

$$|\mathbf{N}_{M/\mathbb{Q}}(\alpha - \beta)| \geq |\mathbf{N}_{M/\mathbb{Q}}(I\mathcal{O}_M)|$$

which contradicts (11.2). □

Norm inequalities. While it is clear that a congruence like (11.3) can be rewritten as a divisibility condition in the ring of integers assuming we are given generators of the ideal I, it is not a priori clear how to convert (11.2) into a polynomial equation with variables ranging over that ring. The propositions below explain how it can be done.

Definition 11.4. For m a positive integer let $C(m)$ denote $(m+1)^2$ times the smallest positive integer greater than the maximum absolute value of any minor of the matrix

$$\begin{pmatrix} 0 & 0 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & & & \\ m^m & m^{m-1} & \dots & 1 \end{pmatrix}. \tag{11.5}$$

Proposition 11.6. *Let $M/\mathbb{Q}$ be a Galois number field extension of degree m. Suppose $\alpha \in \mathcal{O}_M$ and define*

$$u = u(m, \alpha) := C(m) \cdot \alpha(1-\alpha)\cdots(m-\alpha). \tag{11.7}$$

Then for every conjugate β of α over $\mathbb{Q}$ and every ideal I of $\mathcal{O}_M$ contained in $u^{m^2}\mathcal{O}_L$, we have

$$|\mathbf{N}_{M/\mathbb{Q}}(\alpha-\beta)| < |\mathbf{N}_{M/\mathbb{Q}}(I\mathcal{O}_M)|.$$

Proof. Let $g(T)$ be the characteristic polynomial of α over $\mathbb{Q}$ as an element of M. Let $g(T) = T^m + a_{m-1}T^{m-1} + \ldots + a_0$ with $a_i \in \mathbb{Z}$. For every $r \in \mathbb{Z}$ we have

$$\mathbf{N}_{M/\mathbb{Q}}(r-\alpha) = g(r). \tag{11.8}$$

Put $C := C(m)$. By definition of u, if $1 \le r \le m$, then

$$r - \alpha = \frac{u}{C\prod_{i=1, i\neq r}^{m}(i-\alpha)}. \tag{11.9}$$

Put

$$w_r := \prod_{i=1, i\neq r}^{m}(i-\alpha).$$

Then from (11.8) and (11.9) it follows that

$$r^m + a_{m-1}r^{m-1} + \ldots + a_0 = \frac{1}{C^m \mathbf{N}_{M/\mathbb{Q}}(w_r)}\mathbf{N}_{M/\mathbb{Q}}(u) = c_r \mathbf{N}_{M/\mathbb{Q}}(u),$$

where $|c_r| \le \frac{1}{C^m}$. Now consider the following linear system

$$\begin{pmatrix} 0 & 0 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \dots & & & \\ m^m & m^{m-1} & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 \\ a_{m-1} \\ \dots \\ a_0 \end{pmatrix} = \begin{pmatrix} c_0\mathbf{N}_{M/\mathbb{Q}}(u) \\ c_1\mathbf{N}_{M/\mathbb{Q}}(u) \\ \dots \\ c_m\mathbf{N}_{M/\mathbb{Q}}(u) \end{pmatrix}.$$

Using Cramer's rule we obtain that $a_i = \frac{D_i}{D}$, where

$$D_i = \begin{vmatrix} 0 & 0 & \dots & c_0\mathbf{N}_{M/\mathbb{Q}}(u) & \dots & 1 \\ 1 & 1 & \dots & c_1\mathbf{N}_{M/\mathbb{Q}}(u) & \dots & 1 \\ \dots & & & & & \\ (m)^m & (m)^{m-1} & \dots & c_m\mathbf{N}_{M/\mathbb{Q}}(u) & \dots & 1 \end{vmatrix},$$

with the column $(c_r\mathbf{N}_{M/\mathbb{Q}}(u)), r = 0, \dots, m$ replacing the i-th column of the matrix (11.5) and D is the discriminant of (11.5). Factoring out $\mathbf{N}_{M/\mathbb{Q}}(u)$ and expanding along the i-th column we obtain the following:

$$\left|\frac{D_i}{\mathbf{N}_{M/\mathbb{Q}}(u)}\right| = \begin{vmatrix} 0 & 0 & \dots & c_0 & \dots & 1 \\ 1 & 1 & \dots & c_1 & \dots & 1 \\ \dots & & & & & \\ m^m & m^{m-1} & \dots & c_m & \dots & 1 \end{vmatrix} = \left|\sum_{r=0}^{m} \pm c_r M_{r,i}\right| \leq \sum_{r=0}^{m} |c_r||M_{r,i}|,$$

where $M_{r,i}$ is the minor of (11.5) corresponding to the elimination of the r-th row and the i-th column. By assumption

$$|M_{r,i}| < \frac{C}{(m+1)^2},$$

and by construction $|c_r| \leq \frac{1}{C^m}$. Thus, for all $i = 0, \dots, m$, we have that

$$|D_i| < \frac{1}{(m+1)C^{m-1}}|\mathbf{N}_{M/\mathbb{Q}}(u)|.$$

Finally, taking into account that $|D| > 1$, we conclude that

$$|a_i| < |D_i| < \frac{1}{(m+1)C^{m-1}}|\mathbf{N}_{M/\mathbb{Q}}(u)|.$$

Suppose now that some root γ of g is greater in absolute value than $|ma_r|$ for all $r = 0, \dots, m-1$. Let $|a_{\max}| = \max_{0 \leq i \leq m-1} |a_i|$. In this case we have that

$$|\gamma^m| = |-a_{m-1}\gamma^{m-1} - \dots - a_0| \leq \sum_{r=0}^{m-1} |a_r\gamma^r| \leq |ma_{\max}\gamma^{m-1}| < |\gamma^m|,$$

and we have a contradiction. Thus, every root γ of g satisfies

$$|\gamma| < \frac{1}{C^{m-1}}|\mathbf{N}_{M/\mathbb{Q}}(u)| \leq \frac{1}{2}|\mathbf{N}_{M/\mathbb{Q}}(u)|,$$

and for any two roots γ and δ of g we have that

$$|\gamma - \delta| < |\mathbf{N}_{M/\mathbb{Q}}(u)|$$

(we may assume $m > 1$ or there is nothing to prove). Now

$$|\mathbf{N}_{M/\mathbb{Q}}(\alpha-\beta)| < |\mathbf{N}_{M/\mathbb{Q}}(u)^{m(m-1)}| < |\mathbf{N}_{M/\mathbb{Q}}(I\mathcal{O}_M)|. \quad \square$$

Lemma 11.10. *Let M be a finite Galois totally real extension of $\mathbb{Q}$, and put $m := [M:\mathbb{Q}]$. Further, let $x \in \mathcal{O}_M$ be such that $|\sigma(x)| > 1$ for every embedding $\sigma : M \hookrightarrow \mathbb{R}$. Then for every $\gamma \in \mathrm{Gal}(M/\mathbb{Q})$ we have*

$$|\mathbf{N}_{M/\mathbb{Q}}(x-\gamma(x))| \leq 2^m \mathbf{N}_{M/\mathbb{Q}}(x^2).$$

Proof. Let $\sigma, \tau : M \hookrightarrow \mathbb{R}$ be embeddings. Since $|\sigma(x)|, |\tau(x)| > 1$ we have that

$$|\sigma(x) - \tau(x)| < 2|\sigma(x)\tau(x)|,$$

so

$$\begin{aligned} |\mathbf{N}_{M/\mathbb{Q}}(x-\gamma(x))| &= \prod_\sigma |\sigma(x) - (\sigma\circ\gamma)(x)| \\ &< \prod_\sigma 2|\sigma(x)(\sigma\circ\gamma)(x)| = 2^m \prod_\sigma |\sigma(x)|^2 = 2^m \mathbf{N}_{M/\mathbb{Q}}(x^2). \quad \square \end{aligned}$$

Corollary 11.11. *Let α be an algebraic integer contained in some totally real Galois extension $M/\mathbb{Q}$ and such that $\sigma(\alpha) > 1$ for every embedding $\sigma : M \hookrightarrow \mathbb{R}$. Let I be an ideal of M such that $I \subset (2\alpha+1)^2\mathcal{O}_M$.*

Then for any conjugate β of α over $\mathbb{Q}$ we have that $|\mathbf{N}_{M/\mathbb{Q}}(\alpha-\beta)| \leq |\mathbf{N}_{M/\mathbb{Q}}(I\mathcal{O}_M)|$.

Proof. Let $v := 2\alpha+1$ and $m := [M:\mathbb{Q}]$. For every embedding $\sigma : M \hookrightarrow \mathbb{R}$ we have

$$2 \leq 2\sigma(\alpha) \leq \sigma(v),$$

and therefore

$$2^m \leq 2^m \mathbf{N}_{M/\mathbb{Q}}(\alpha) \leq \mathbf{N}_{M/\mathbb{Q}}(v).$$

By Lemma 11.10, we now have

$$|\mathbf{N}_{M/\mathbb{Q}}(\alpha-\beta)| \leq 2^m \mathbf{N}_{M/\mathbb{Q}}(\alpha^2) < \mathbf{N}_{M/\mathbb{Q}}(v^2) \leq \mathbf{N}_{M/\mathbb{Q}}(I). \quad \square$$

The basic congruence relation for extensions of finite degree and totally real fields. Fix L/K an extension of number fields and let m denote the degree of M, the Galois closure of $L/\mathbb{Q}$.

For a positive integer m and an algebraic integer $\alpha \in \mathcal{O}_L$ define

$$D(m,\alpha) := u(m,\alpha)^{m^2} = (C\alpha(1-\alpha)\cdots(m-\alpha))^{m^2} \in \mathcal{O}_L,$$

where $C = C(m)$ is as in Definition 11.4 and $u(m,\alpha)$ is as in Definition 11.7.

Putting together Lemma 11.1, Proposition 11.6 and Corollary 11.11 we immediately obtain these corollaries.

Corollary 11.12. *Let $E \subset \mathcal{O}_L$ be the set of all elements $\alpha \in \mathcal{O}_L$ such that there exists $b \in \mathcal{O}_K$ and an ideal $I \subset \mathcal{O}_K$ satisfying*

$$I\mathcal{O}_L \subset D(m,\alpha)\mathcal{O}_L, \quad \alpha \equiv b \pmod{I\mathcal{O}_L}.$$

Then $E \subset \mathcal{O}_K$.

Corollary 11.13. *Let $\mathbf{L}$ be a totally real extension of $\mathbb{Q}$, possibly infinite. Let $K \subset \mathbf{L}$ be a number field. Let $E \subset \mathcal{O}_{\mathbf{L}}$ be the set of all elements $\alpha \in \mathcal{O}_L$ such that there exists $b \in \mathcal{O}_K$, an ideal $I \subset \mathcal{O}_K$, and $u_1, u_2, u_3, u_4 \in \mathcal{O}_{\mathbf{L}}$ satisfying*

$$I\mathcal{O}_{\mathbf{L}} \subset (2\alpha+1)^2\mathcal{O}_{\mathbf{L}}, \quad \alpha = 1 + u_1^2 + \ldots + u_4^2, \quad \alpha \equiv b \pmod{I\mathcal{O}_{\mathbf{L}}}.$$

Then $E \subset \mathcal{O}_K$.

Remark 11.14. The equations for the totally real case are the same across all pairs of totally real fields K and $\mathbf{L}$, including the case where one or both extensions are infinite. We will show that the same is true in the case of a quadratic extension of a totally real field.

12. Quadratic extensions of totally real fields

We treat separately quadratic extensions of totally real fields because if the totally real field is of infinite degree over $\mathbb{Q}$, this case is technically much more complicated than the case of finite extensions or the case of totally real fields. The main reason for the complications is the difficulty with bounds on norms.

Norm inequalities for quadratic extensions of totally real fields. The construction of diophantine bounds on norms of elements of a non-totally real quadratic extension of a totally real field of infinite degree over $\mathbb{Q}$ is not as simple as the analogous constructions in the case of extensions of finite degree over $\mathbb{Q}$ or totally real fields of arbitrary degree. We construct a diophantine definition of these bounds in several steps starting with Lemma 12.1 below and continuing with Lemma 12.5, Corollaries 12.6, 12.13, 12.15 and 12.16. Unlike diophantine definitions of bounds in the other two cases, in the case of non-totally real quadratic extensions of totally real fields of infinite degree over $\mathbb{Q}$, we will need to use diophantine stability of a commutative group scheme in the extension $\mathbf{F}/\mathbf{L}$, where $\mathbf{L}$ is a totally real field possibly of infinite degree over $\mathbb{Q}$ and $\mathbf{F}$ is a non-totally real quadratic extension of $\mathbf{L}$. The group scheme, a twist of $\mathbf{G}_m$, is constructed in §12.

Proposition 12.1. *Let* $\mathbf{L}$ *be a possibly infinite totally real extension of* $\mathbb{Q}$ *and let* $\mathbf{F}$ *be a quadratic extension of* $\mathbf{L}$*. Let* $\delta \in \mathcal{O}_{\mathbf{F}}$*,* $\delta^2 = d \in \mathcal{O}_{\mathbf{L}}$*,* $\mathbf{F} = \mathbf{L}(\delta)$*. Let* $x = y_0 + y_1\delta \in \mathcal{O}_{\mathbf{F}}$ *with* $y_0, y_1 \in \mathbf{L}$*, and let* $w \in \mathbf{L}$ *be such that*

$$\text{for all embeddings } \sigma : \mathbf{F} \hookrightarrow \mathbb{R} \text{ we have that } 1 < \sigma(x) < \sigma(w), \tag{12.2}$$

$$\text{for all embeddings } \tau : \mathbf{F} \hookrightarrow \mathbb{C} \text{ with } \tau(\mathbf{F}) \not\subset \mathbb{R} \text{ we have that } |\tau(w)| \geq 1. \tag{12.3}$$

Let $L \subset \mathbf{L}$ *be a number field containing* d, y_0, y_1 *and* w*. Let* $F = L(\delta)$*. Then* $|\mathbf{N}_{F/\mathbb{Q}}(\delta y_1)| \leq |\mathbf{N}_{F/\mathbb{Q}}(xw)|$.

Remark 12.4. Recall that the inequality involving σ can be converted to an equation by Proposition 4.9.

Proof. If τ is a non-real embedding of F, then $|\tau(y_1\delta)| \leq |\tau(x)|$. If σ is a real embedding of F, then let $\hat{\sigma}$ be an embedding of F such that $\sigma_{|L} = \hat{\sigma}_{|L}$ but $\hat{\sigma} \neq \sigma$. In other words, if $\sigma(x) = \sigma(y_0) + \sigma(\delta)\sigma(y_1)$, then $\hat{\sigma}(x) = \sigma(y_0) - \sigma(\delta)\sigma(y_1)$. Then either

$$|\sigma(x)| = |\sigma(y_0)| + |\sigma(\delta y_1)|,$$

or

$$|\hat{\sigma}(x)| = |\sigma(y_0)| + |\sigma(\delta y_1)|.$$

So, either $|\hat{\sigma}(x)| \geq |\hat{\sigma}(\delta y_1)|$ or $|\sigma(x)| \geq |\sigma(\delta y_1)|$. Since $\sigma(w) = \hat{\sigma}(w)$, for all real embeddings σ of F we have that $|\sigma(w)| > |\sigma(\delta y_1)|$. Let Σ be the collection of all real embeddings of F, and let T be the collection of all embeddings of F that are not real. Now we have the following inequalities:

$$\begin{aligned}
|\mathbf{N}_{F/\mathbb{Q}}(y_1\delta)| &= \prod_{\tau\in T} |\tau(\delta y_1)| \prod_{\sigma\in\Sigma} |\sigma(\delta y_1)| \\
&\leq \prod_{\tau\in T} |\tau(x)| \prod_{\sigma\in\Sigma} |\sigma(wx)| \\
&\leq \prod_{\tau\in T} |\tau(x)| \prod_{\sigma\in\Sigma} |\sigma(x)| \prod_{\tau\in T} |\tau(w)| \prod_{\sigma\in\Sigma} |\sigma(W)| = |\mathbf{N}_{F/\mathbb{Q}}(xw)|. \quad \square
\end{aligned}$$

For Proposition 12.1 to be useful we need to be provided with an existentially defined bound "w" that satisfies (12.2) and (12.3). This is Corollary 12.6 below. In preparation, we have:

Lemma 12.5. *Let* K *be a totally real number field. Let* $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ *be the collection of all embeddings of* K *into* $\mathbb{R}$*. Let* $\Omega \subset K$ *be an infinite set. Then for any integer* $N > 0$ *there exists* $u \neq v \in \Omega$ *such that for all* $\sigma \in \Sigma$ *we have that*

$$\left|\sigma\left(\left[\left(\frac{1}{u-v}\right)^2+1\right](u^2+1)\right)\right| > N.$$

Proof. As an infinite subset of $\mathbb{R}$, for each embedding σ of K into $\mathbb{R}$, the set $\sigma(\Omega)$ is either unbounded or it has a limit point and therefore contains a non-constant Cauchy sequence. Assume without loss of generality that $\sigma_1(\Omega)$ contains a Cauchy sequence $\{\sigma_1(u_i)\}$ such that all elements of the sequence are distinct. If $\{|\sigma_2(u_i)|\}$ is unbounded, then select a subsequence $\{u_{i,2}\}$ such that $\{|\sigma_2(u_{i,2})|\} \to \infty$. If $\{\sigma_3(u_{i,2})\}$ is bounded, then let $\{u_{i,3}\}$ be a subsequence of $\{u_{i,2}\}$ such that $\{\sigma_3(u_{i,2})\}$ is a Cauchy sequence. Continuing by induction we construct a sequence $\{u_{i,n}\}$ such that for all $\sigma \in \Sigma$ we have that $\{\sigma(u_{i,n})\}$ is either a Cauchy sequence or is going to infinity. Now let $N > 0$ be given. Choose $j \in \mathbb{Z}_{>0}$ such that for all $\sigma \in \Sigma$ and all $\ell \geq j$ either $|\sigma(u_{\ell,n})| > N$ or $|\sigma(u_{j,n} - u_{\ell,n})| < \frac{1}{N}$. We claim that for all $\sigma \in \Sigma, \ell > j$ it is the case that

$$\left|\sigma\left(\left[\left(\frac{1}{u_{j,n}-u_{\ell,n}}\right)^2+1\right](u_{j,n}^2+1)\right)\right| > N.$$

Indeed, for each $\sigma \in \Sigma$ we have that either $|\sigma(u_{j,n})| > N$ or

$$\left|\sigma\left(\frac{1}{u_{j,n}-u_{\ell,n}}\right)\right| > N$$

while the σ-images of both factors are always bigger than 1. □

Corollary 12.6. *Let* $\mathbf{L} \subset \mathbf{F}$ *be as in Proposition 12.1. Let* $\Omega \subset \mathbf{L}$ *contain infinitely many elements of some number field* $K \subset \mathbf{L}$*. Then for any* $x \in \mathcal{O}_{\mathbf{F}}$ *there exist* $u, v \in \Omega$ *such that*

$$w := \left[\left(\frac{1}{u-v}\right)^2+1\right](u^2+1)$$

satisfies (12.2) *and* (12.3)*.*

A special case of stability for quadratic extensions of totally real fields. As we have mentioned above, to construct diophantine bounds on norms of elements of non-totally real extensions of degree 2 of totally real fields, we will need to use a particular case of diophantine stability. We discuss this case in this section. More specifically, we consider diophantine stability of multiplicative groups over rings of integers in quadratic extensions $\mathbf{F}/\mathbf{L}$, where $\mathbf{L}$ is a totally real possibly infinite algebraic extension of $\mathbb{Q}$.

J. Denef and L. Lipshitz were the first to use this phenomenon for the purposes of existential definability over finite extensions (see [DL78]). The third author used it over infinite extensions in conjunction with diophantine stability of elliptic curves (see [Shl09]).

Here we present a different proof of these results using the vocabulary of diophantine stability. Our goal is to show that this case is of the same nature as other instances of diophantine stability already discussed in this paper. We begin by considering number fields and then move to infinite extensions.

The case of finite extensions. Suppose M/L is a quadratic extension of fields. We denote by $\mathbf{G}_m^{M/L}$ the twist of the multiplicative group $\mathbf{G}_m$ over L by the quadratic character corresponding to M/L, as defined for example in [MRS07]. If F/L is a field extension and $F \cap M = L$, then

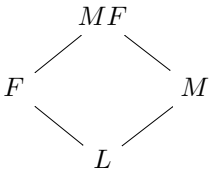
$$\mathbf{G}_m^{M/L}(\mathcal{O}_F) = \{x \in \mathcal{O}_{MF}^\times : \mathbf{N}_{MF/F} x = 1\}, \tag{12.7}$$

$$\mathbf{G}_m^{M/L}(\mathcal{O}_L) = \{x \in \mathcal{O}_M^\times : \mathbf{N}_{M/L} x = 1\}. \tag{12.8}$$

Lemma 12.9. *Suppose L is a totally real number field, and F is a quadratic extension of L. Suppose M/L is a quadratic extension such that for every infinite place v of L, v ramifies in M/L if and only if v does* not *ramify in F/L. Then*

(1) $[\mathbf{G}_m^{M/L}(\mathcal{O}_F) : \mathbf{G}_m^{M/L}(\mathcal{O}_L)]$ is finite,
(2) if F is not totally real, then $\mathbf{G}_m^{M/L}(\mathcal{O}_L)$ has elements of infinite order,
(3) if n is an integer, $n \geq 3$, then $\ker\{\mathbf{G}_m^{M/L}(\mathcal{O}_F) \to \mathbf{G}_m^{M/L}(\mathcal{O}_F/n\mathcal{O}_F)\} \subset \mathbf{G}_m^{M/L}(\mathcal{O}_L)$.

Proof. Consider the diagram of fields in the hypothesis of the lemma.



Let V be the set of archimedean places of L (all real, by hypothesis). Write $V = V_F \sqcup V_M$ where $V_F \subset V$ is the subset consisting of the places that do not ramify in F/L and V_M is the subset consisting of the places that do not ramify in M/K. So

$$[L : \mathbb{Q}] = |V| = |V_F| + |V_M|.$$

We have that $r_F := 2 \cdot |V_F|$ is the number of real places of F and $r_M := 2 \cdot |V_M|$ is the number of real places of M. Letting s_F, s_M denote the number of complex places of F and M respectively, we have: $s_F = |V_M|$ and $s_M = |V_F|$. As for MF/L we have that MF is totally complex and every archimedean place of L lifts to two complex places of MF. Letting u_K denote the rank of the group of units of a field K, we have, by Dirichlet's Unit Theorem:

$$u_L = |V| - 1, \qquad u_M = 2|V_M| + |V_F| - 1,$$
$$u_F = 2|V_F| + |V_M| - 1, \qquad u_{MF} = 2|V| - 1$$

so that

$$u_{MF} - u_F = |V_M| = u_M - u_L.$$

Let G denote the group $\mathbf{G}_m^{M/L}$. The above combined with (12.7), shows that

$$\begin{aligned} \mathrm{rank}_{\mathbb{Z}} G(\mathcal{O}_F) &= u_{MF} - u_F = |V_M|, \\ \mathrm{rank}_{\mathbb{Z}} G(\mathcal{O}_L) &= u_M - u_L = |V_M|, \end{aligned} \tag{12.10}$$

so that $\mathrm{rank}_{\mathbb{Z}} G(\mathcal{O}_F) = \mathrm{rank}_{\mathbb{Z}} G(\mathcal{O}_L)$. This proves (1).

Equation (12.10) shows that $\mathrm{rank}_{\mathbb{Z}} G(\mathcal{O}_L) > 0$ unless $|V_M| = 0$, i.e., unless F is totally real. This proves (2).

Suppose now that $x \in \ker\{G(\mathcal{O}_F) \to G(\mathcal{O}_F/n\mathcal{O}_F)\}$. Using (12.7) we can view $x \in \mathcal{O}_{FM}^{\times}$ such that $x \equiv 1 \pmod{n}$. By (1), there is a positive integer k such that $x^k \in \mathcal{O}_M^{\times}$. If σ is the nontrivial automorphism of MF/M, then $(x/x^\sigma)^k = 1$, so x/x^σ is a root of unity. But $x/x^\sigma \equiv 1 \pmod{n}$, so we have $x/x^\sigma = 1$, i.e., $x \in M$. Since $\mathbf{N}_{M/L} x = \mathbf{N}_{MF/F} x = 1$, we have $x \in G(\mathcal{O}_L)$ by (12.7). This proves (3). □

Lemma 12.11. *Suppose L is a totally real number field, and F is a quadratic extension of L. Then there is a quadratic extension M/L such that for every infinite place v of L, v ramifies in M/L if and only if v does* not *ramify in F/L.*

Proof. Choose $d \in L$ such that $F = L(\sqrt{d})$ and let $M = L(\sqrt{-d})$. Then for every infinite place v of L, $-\alpha$ is negative at v if and only if α is positive at v, so v ramifies in M/L if and only if v doesn't ramify in F/L. □

The case of quadratic extensions of totally real fields $\mathbf{L}$ *of infinite degree.* Let $\mathbf{L}$ be a totally real algebraic extension of $\mathbb{Q}$. Let $\mathbf{F}$ and $\mathbf{M}$ be quadratic extensions of $\mathbf{L}$ such that for every embedding σ of $\mathbf{MF}$ into $\bar{\mathbb{Q}}$ we have that $\sigma(F) \subset \mathbb{R}$ if and only if $\sigma(M) \not\subset \mathbb{R}$. Let $\mathbf{F} = \mathbf{L}(\delta)$ where $\delta^2 = d \in \mathcal{O}_{\mathbf{L}}$ and let $\mathbf{M} = \mathbf{L}(\beta)$ where $\beta^2 = -d \in \mathcal{O}_{\mathbf{L}}$. We let $G := \mathbf{G}_m^{\mathbf{M/L}}$ as above.

Lemma 12.12. *if n is an integer, $n \geq 3$, then* $\ker\{G(\mathcal{O}_{\mathbf{F}}) \to G(\mathcal{O}_{\mathbf{F}}/n\mathcal{O}_{\mathbf{F}})\} \subset G(\mathcal{O}_{\mathbf{L}})$.

Proof. Suppose $x \in \ker\{G(\mathcal{O}_{\mathbf{F}}) \to G(\mathcal{O}_{\mathbf{F}}/n\mathcal{O}_{\mathbf{F}})\}$. Let L be a number field contained in $\mathbf{L}$ such that $d \in L$ and $x \in G(\mathcal{O}_{L(\delta)})$. Let $F = L(\delta)$ and $M = L(\beta)$. Then $x \in \ker\{G(\mathcal{O}_F) \to G(\mathcal{O}_F/n\mathcal{O}_F)\} \subset \mathbf{G}_m^{M/L}(\mathcal{O}_L)$ by Lemma 12.9(3). By (12.8) we have $\mathbf{G}_m^{M/L}(\mathcal{O}_L) \subset \mathbf{G}_m^{\mathbf{M/L}}(\mathcal{O}_{\mathbf{L}})$, so $x \in G(\mathcal{O}_{\mathbf{L}})$. □

Corollary 12.13. *Let* $\mathbf{L}$ *be a totally real algebraic extension of* $\mathbb{Q}$*. Let* $\mathbf{F}$ *be a quadratic extension of* $\mathbf{L}$ *and assume that* $\mathbf{F}$ *is not totally real. Then there exists a commutative group scheme* G *defined over* $\mathcal{O}_{\mathbf{L}}$ *such that*

(1) $G(\mathcal{O}_{\mathbf{L}})$ *contains an element of infinite order,*
(2) for every integer $n \geq 3$*,* $\ker\{G(\mathcal{O}_{\mathbf{F}}) \to G(\mathcal{O}_{\mathbf{F}}/n\mathcal{O}_{\mathbf{F}})\} \subset G(\mathcal{O}_{\mathbf{L}})$*.*

Proof. By Lemmas 12.9(2) and 12.12, the commutative group scheme $G := \mathbf{G}_m^{\mathbf{M}/\mathbf{L}}$ has these properties. □

Remark 12.14. In the language of Definition 13.5 below, Corollary 12.13(2) says that if $n \geq 3$ then $(1, n\mathcal{O}_{\mathbf{L}})$ is an exponent of diophantine stability for G relative to $\mathbf{F}/\mathbf{L}$.

There is another consequence of diophantine stability we will use later to produce bounds for elements of $\mathbf{F}$.

Corollary 12.15. *Let* $\mathbf{F}/\mathbf{L}$ *be as in Corollary 12.13. Then there exists a set* $B \subset \mathcal{O}_{\mathbf{F}} \times (\mathcal{O}_{\mathbf{F}} \setminus \{0\})$ *satisfying the following conditions.*

(1) B *is diophantine over* $\mathcal{O}_{\mathbf{F}}$*.*
(2) If $(a, b) \in B$*, then* $a/b \in \mathbf{L}$*.*
(3) For some number field $L \subset \mathbf{L}$*, the set* $\{a/b : (a, b) \in B \text{ and } a/b \in L\}$ *is infinite.*

Proof. Let G be a group scheme satisfying the conclusions of Corollary 12.13. Let $G \hookrightarrow \mathbb{P}^n$ be a well-arranged embedding (see Definition 7.7)

$$P \mapsto \big(x_1(P) : x_2(P) : \cdots : x_{n+1}(P)\big).$$

Let A be the set of all $(n+1)$-tuples in $\mathcal{O}_{\mathbf{F}} \times \cdots \times \mathcal{O}_{\mathbf{F}}$ that are homogeneous coordinates of some point $P \in \ker\{G(\mathcal{O}_{\mathbf{F}}) \to G(\mathcal{O}_{\mathbf{F}}/n\mathcal{O}_{\mathbf{F}})\}$. Then A is diophantine over $\mathcal{O}_{\mathbf{F}}$. It follows that the set

$$B := \{(y_i, y_j) : 0 \leq i, j \leq n+1, y_j \neq 0, (y_1, \ldots y_{n+1}) \in A\}$$

is diophantine over $\mathcal{O}_{\mathbf{F}}$ as well. By Corollary 12.13(2), if $(a, b) \in B$ then $a/b \in \mathbf{L}$.

By Corollary 12.13 we can fix a point P of infinite order in $G(\mathcal{O}_{\mathbf{L}})$. For some positive k we have $P^k \in \ker\{G(\mathcal{O}_{\mathbf{F}}) \to G(\mathcal{O}_{\mathbf{F}}/n\mathcal{O}_{\mathbf{F}})\}$. Then $P^k \in G(\mathcal{O}_L)$ for some number field $L \subset \mathbf{L}$, and for every integer m we have

$$P^{km} \in \ker\{G(\mathcal{O}_{\mathbf{F}}) \to G(\mathcal{O}_{\mathbf{F}}/n\mathcal{O}_{\mathbf{F}})\} \cap G(\mathcal{O}_L),$$

and it follows that the set in assertion (3) of the corollary is infinite. □

Combining bound equations and basic congruence equations in the case of non-totally real quadratic extensions of totally real fields. In the following corollary we combine Proposition 12.1, Lemma 12.5, Corollaries 12.6 and 12.15 to finish our construction of norm bounds. We remind the reader that inequalities for real embeddings are implemented using sums of squares, pairs in B come from a totally real field, and the role of u and v is explained in Corollary 12.6.

Corollary 12.16. *Let $\mathbf{F}$ be a quadratic extension of a totally real field $\mathbf{L}$. Let B be as in Corollary 12.15. Let $\alpha \in \mathcal{O}_{\mathbf{F}}$. Let $\delta \in \mathcal{O}_{\mathbf{F}}$ be such that $\mathbf{F} = \mathbf{L}(\delta)$ and $\delta^2 := d \in \mathcal{O}_{\mathbf{L}}$. Let $H \subset \mathbf{L}$ be a number field such that $d \in H$, $\alpha \in H(\delta)$ and let $\hat{\alpha}$ be the conjugate of α over H. Let Σ be the set of all real embeddings of the field $\mathbf{F}$. Consider now the following equations and conditions:*

$$(a,b),(c,d) \in B,$$
$$u = a/b, v = c/d, bd \neq 0$$
$$X_2 \neq 0$$
$$X_1 = X_2 \left[\left(\frac{1}{u-v} \right)^2 + 1 \right] (u^2+1)$$
$$\forall \sigma \in \Sigma : |\sigma(X_2)| < |\sigma(X_2\alpha)| < |\sigma(X_1)|.$$

If this system of equations and conditions is satisfied over $\mathcal{O}_{\mathbf{F}}$, then

$$|\mathbf{N}_{H(\delta,u,v)/\mathbb{Q}}(\alpha - \hat{\alpha})| \leq |\mathbf{N}_{H(\delta,u,v)/\mathbb{Q}}(2X_1\alpha)|.$$

Conversely, for any $\alpha \in \mathcal{O}_{\mathbf{F}}$, this system can be satisfied.

Proof. First, assume the equations and the conditions in the statement of the corollary are satisfied. Then by construction of B we have that $u, v \in \mathbf{L}$. Let $W = \frac{X_1}{X_2} \in L$ and observe that for any embedding $\mu : \mathbf{F} \hookrightarrow \mathbb{C}$ we have that $\mu(W) > 1$. Further, for every $\sigma \in \Sigma$ we have that $1 < |\sigma(\alpha)| < \sigma(W)$. If we let $\alpha = y_0 + \delta y_1$ and $\hat{\alpha} = y_0 - y_1\delta$, then

$$\begin{aligned} |\mathbf{N}_{H(\delta,u,v)/\mathbb{Q}}(\hat{\alpha} - \alpha)| = |\mathbf{N}_{H(\delta,u,v)/\mathbb{Q}}(2\delta y_1)| &\leq |\mathbf{N}_{H(\delta,u,v)/\mathbb{Q}}(2\alpha W)| \\ &\leq |\mathbf{N}_{H(\delta,u,v)/\mathbb{Q}}(2\alpha X_1)|, \end{aligned}$$

where the penultimate inequality is true by Proposition 12.1.

Suppose now that $\alpha \in \mathcal{O}_F$, then by construction of B, Corollary 12.15 and Corollary 12.6 we can find (a,b) and (c,d) in B to satisfy the equations and conditions of the corollary. □

Finally, we combine the bounds in Corollary 12.16 with the basic congruence condition (Lemma 11.1) for the case of a non-totally real quadratic extension.

Corollary 12.17. *Let* $\mathbf{L}$ *be a totally real field. Let* $\mathbf{F}$ *be a quadratic extension of* $\mathbf{L}$*. Let* K *be a number field contained in* $\mathbf{F}$*. Let* Σ *be the set of all embeddings of* $\mathbf{F}$ *into* $\mathbb{R}$*. Let* T *be the set of all non-real embeddings of* $\mathbf{F}$ *into* $\mathbb{C}$*.*

Let $E \subset \mathcal{O}_{\mathbf{F}}$ *be the set of elements* $\alpha \in \mathcal{O}_{\mathbf{F}}$ *such that there exist elements* $X_1 \in \mathcal{O}_{\mathbf{F}}, 0 \neq X_2 \in \mathcal{O}_{\mathbf{F}}$ *with* $\frac{X_1}{X_2} \in \mathbf{L}$*,* $b \in \mathcal{O}_K$*, and* I *an ideal of* $\mathcal{O}_K$ *satisfying the following conditions:*

$$\forall \sigma \in \Sigma : \ 1 < \sigma(\alpha) < \sigma\left(\frac{X_1}{X_2}\right),$$

$$\forall \tau \in T : \ \tau\left(\frac{X_1}{X_2}\right) \geq 1,$$

$$I\mathcal{O}_{\mathbf{F}} \subset 2X_1\alpha\mathcal{O}_{\mathbf{F}}$$

$$\alpha \equiv b \pmod{I\mathcal{O}_{\mathbf{F}}}.$$

Then $E \subset \mathcal{O}_K$*. (Here we again remind the reader that for real embeddings we can convert inequalities to equations via Proposition 4.9.)*

13. Rational points

Let G be a group scheme satisfying Assumption 7.4 above.

Definition 13.1. Let

$$\begin{array}{ccc} S & \xrightarrow{P} & G \\ & \searrow & \downarrow \\ & & S \end{array}$$

be an S-section of G. We allow ourselves a number of synonyms for this notion. If the ring $\mathcal{O}_K$ rather than the corresponding scheme S is more prominent in the surrounding discussion, we may also call an S-section an "$\mathcal{O}_K$-section," or an "$\mathcal{O}_K$-rational point." In the case, for example, when the group scheme $G := \mathcal{A}$ is the Néron model over $S = \mathrm{Spec}(\mathcal{O}_K)$ of an abelian variety $A_{/K}$, the S-sections of G—alias $\mathcal{O}_K$-sections of $\mathcal{A}$—are in one-one correspondence with the K-rational points of the abelian variety A over K to which these sections restrict.

Definition 13.2. Set $M := G(S)$. The letter "M" is for *Mordell-Weil group*, a label we use even if G is any of the group schemes that we work with—i.e., as in Assumption 7.4; we may also denote M as $G(\mathcal{O}_K)$.

Definition 13.3. For any algebraic extension L of $\mathbb{Q}$ and any nonempty subset $I \subset \mathcal{O}_L$ different from $\{0\}$ let

$$M_{I,L}(G) := \ker\{G(\mathcal{O}_L) \longrightarrow G(\mathcal{O}_L/I\mathcal{O}_L)\}$$

where $I\mathcal{O}_L$ denotes the (nonzero) ideal of $\mathcal{O}_L$ generated by I. If $r \in \mathbb{Z}_{>0}$ define

$$M_{I,L}^r \ := \ \{x^r : x \in M_{I,L}\}.$$

That is, we have a surjection

$$M_{I,L} \xrightarrow{r\text{-th power}} M_{I,L}^r \subset M_{I,L}.$$

Lemma 13.4. *The group $M_{I,L} = M_{I,L}(G)$ is a subgroup of $M = G(\mathcal{O}_L)$ of finite index.*

Proof. Since $I\mathcal{O}_L$ is a nonzero ideal, $\mathcal{O}_L/I\mathcal{O}_L$ is a finite ring, so $G(\mathrm{Spec}(\mathcal{O}_L/I\mathcal{O}_L))$ is a finite group. □

Definition 13.5. Say that a pair (r, I) consisting of a positive integer r together with a nonzero ideal $I \subset \mathcal{O}_K$ is an **exponent of diophantine stability for G relative to a field extension** L/K if the subgroup $M_{I,L}^r(G) \subset G(\mathcal{O}_L)$ is contained in $G(\mathcal{O}_K)$:

$$\{x^r : x \in M_{I,L}\} \ \subset \ G(\mathcal{O}_K).$$

Example 13.6. Property (3) of Lemma 12.9 says that, in the notation of that lemma, if $n \geq 3$ then the pair $(1, n\mathcal{O}_K)$ is an exponent of diophantine stability for $\mathbf{G}_m^{M/L}$ relative to F/L.

Remark 13.7. If the subgroup $G(\mathcal{O}_K)$ is of finite index m in $G(\mathcal{O}_L)$ then $(m, \mathcal{O}_L)$ is an exponent of diophantine stability for G relative to L/K. If $G_{/K} = A$ is an abelian variety, then there exists an exponent of diophantine stability for G relative to L/K if and only if A is *rank stable* for the field extension L/K.

Lemma 13.8. *Suppose A is an abelian variety over K, rank stable for the extension $\mathbf{L}/K$. Then there is a positive integer n such that $(1, n\mathcal{O}_K)$ is an exponent of diophantine stability for A relative to $\mathbf{L}/K$.*

Proof. Let $\mathbf{L}'$ denote the Galois closure of $\mathbf{L}$ over K. Let $\mathfrak{p}, \mathfrak{q}$ be primes of $\mathbf{L}'$ where A has good reduction, and with distinct residue characteristics p, q, respectively. By [ST68, Lemma 2], reduction modulo $\mathfrak{p}$ is injective on prime-to-p torsion, and reduction modulo $\mathfrak{q}$ is injective on prime-to-q torsion. Hence the only torsion in $M_{\mathfrak{p},\mathbf{L}'}$ is p-power torsion, and the only torsion in $M_{\mathfrak{q},\mathbf{L}'}$ is q-power torsion. Thus, setting $n = pq$, the torsion subgroup of $M_{n,\mathbf{L}'}$ is zero.

Now suppose $P \in M_{n,\mathbf{L}}$. Since A is rank stable for $\mathbf{L}/K$, there is a positive integer t such that $tP \in A(K)$. If $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, then $t(\sigma P - P) = \sigma(tP) - tP = 0$. Therefore $\sigma P - P$ is a torsion point in $M_{n,\mathbf{L}'}$, so $\sigma P - P = 0$ and we conclude that $\sigma P = P$. Since this holds for every $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, we have $P \in A(K)$. This proves the lemma. □

Remark 13.9. If (r, I) is an exponent of diophantine stability for G relative to L/K, we have the diagram

$$\begin{array}{ccccc} M_{I,L}^r & \hookrightarrow & M_{I,L} & \hookrightarrow & G(\mathcal{O}_L)\ . \\ & \searrow & & \nearrow & \\ & & G(\mathcal{O}_K) & & \end{array}$$

Lemma 13.10. *If G_1 and G_2 are two smooth group schemes over $\mathcal{O}_K$ and (r, I) is an exponent of diophantine stability for both G_1 and G_2 relative to a field extension L/K, then (r, I) is an exponent of diophantine stability for $G_1 \times_{\mathcal{O}_K} G_2$ relative to L/K.*

Lemma 13.11. *Suppose that $G(\mathcal{O}_{\mathbf{K}})$ contains a point of infinite order. Then for every nonzero ideal $I \subset \mathcal{O}_{\mathbf{K}}$, every $r \in \mathbb{Z}_{>0}$, and every $\mathbf{L}/\mathbf{K}$, the group $M_{I,\mathbf{L}}^r(G)$ contains a point of infinite order.*

Proof. Let L be a number field contained in $\mathbf{L}$, let $P \in G(\mathcal{O}_L) \subset G(\mathcal{O}_{\mathbf{L}})$ be a point of infinite order. Let $N := |G(\mathcal{O}_L/(I \cap \mathcal{O}_L)\mathcal{O}_L)|$. Then $N < \infty$, P^N is contained in $M_{I\cap\mathcal{O}_L,L} \subset M_{I,\mathbf{L}}$ and P^{rN} is contained in $M_{I,\mathbf{L}}^r$. Since P^{rN} has infinite order, this proves the lemma. □

Lemma 13.12. *Let $I \subset \mathcal{O}_K$ be any nonzero ideal, and let P be an S-section of G in $M_{I,K}$. Then $z_P \subset I$.*

Proof. This follows directly from Definition 13.3: if $P \in M_{I,K}(G)$ then the image of P in $G(\mathcal{O}_K/I)$ is trivial. □

Proposition 13.13. *Let L/K be a finite extension, with $\mathcal{O}_L/\mathcal{O}_K$ their corresponding rings of integers. Let $m :=$ the degree of the Galois closure $M/\mathbb{Q}$ of L over $\mathbb{Q}$. Let $C := C(m)$ be as in Proposition 11.6.*

Fix $\alpha \in \mathcal{O}_L$, and let $D(m, \alpha) := (C\alpha(1-\alpha)\dots(m-\alpha))^{m^2} \in \mathcal{O}_L$. Suppose

- *$z \subset \mathcal{O}_K$ is an ideal such that $z\mathcal{O}_L \subset D(\alpha)\mathcal{O}_L$,*
- *W is a free $\mathcal{O}_K/z$-module of finite rank.*

If either $D(m, \alpha) = 0$ or if there are elements $v, w \in W$ such that $w \in W$ is a basis element and

$$v \otimes 1 = w \otimes \alpha = \alpha(w \otimes 1) \in W \otimes_{\mathcal{O}_K} \mathcal{O}_L \tag{13.14}$$

then $\alpha \in \mathcal{O}_K$.

Proof. Suppose that α, v, w satisfy (13.14). Let $z_L := z\mathcal{O}_L$. Since w is a basis element of the free $\mathcal{O}_K/z$-module W, we see that $w \otimes 1$ is a basis element of the free $\mathcal{O}_L/z_L$-module $W \otimes_{\mathcal{O}_K} \mathcal{O}_L$.

All of (13.14) 'takes place' in the free $\mathcal{O}_L/z_L$-submodule of $W \otimes_{\mathcal{O}_K} \mathcal{O}_L$ (of rank one) generated by $w \otimes 1$. In particular $v \in (\mathcal{O}_K/z)w$ so we can choose $b \in \mathcal{O}_K$ such that $v = bw$. Then, using (13.14),

$$w \otimes \alpha = v \otimes 1 = bw \otimes 1 = w \otimes b.$$

Since $w \otimes 1$ is a basis vector, it follows that $b \equiv \alpha \pmod{z_L}$. The proposition then follows from Corollary 11.12. □

In the same manner, using Corollaries 11.13 and 12.17, one can prove a totally real version and a quadratic extension of a totally real field version of Proposition 13.13.

Proposition 13.15. *Let* $\mathbf{L}/\mathbf{K}$ *be an extension of totally real fields, with* $\mathcal{O}_\mathbf{L}/\mathcal{O}_\mathbf{K}$ *their corresponding rings of integers. Fix* $\alpha \in \mathcal{O}_\mathbf{L}$ *such that* $\alpha = 1 + v_1^2 + \ldots + v_4^2$ *with* $v_i \in \mathcal{O}_\mathbf{L}$. *Suppose*

- $z \subset \mathcal{O}_\mathbf{K}$ *is an ideal such that* $z\mathcal{O}_\mathbf{L} \subset (2\alpha + 1)^2\mathcal{O}_\mathbf{L}$,
- W *is a free* $\mathcal{O}_\mathbf{K}/z$*-module of finite rank.*

If there are elements $v, w \in W$ *such that* $w \in W$ *is a basis element and*

$$v \otimes 1 = w \otimes \alpha = \alpha(w \otimes 1) \in W \otimes_{\mathcal{O}_\mathbf{K}} \mathcal{O}_\mathbf{L}$$

then $\alpha \in \mathcal{O}_\mathbf{K}$.

Proposition 13.16. *Let*

$$\begin{array}{ccc} \mathbf{L} & \hookrightarrow & \mathbf{F} \\ & & \uparrow \\ & & \mathbf{K} \end{array}$$

be a diagram of fields of algebraic numbers where $\mathbf{K}$ *is an algebraic possibly infinite extension of* $\mathbb{Q}$, $\mathbf{L}$ *is totally real, and* $[\mathbf{F} : \mathbf{L}] = 2$. *For elements* $\alpha \in \mathcal{O}_\mathbf{F}$ *and* $X_1, X_2 \in \mathcal{O}_\mathbf{F}$ *with* X_2 *nonzero, putting* $X := \frac{X_1}{X_2}$ *suppose that:*

(1) $X \in \mathbf{L}$,
(2) for every embedding $\tau : \mathbf{F} \hookrightarrow \mathbb{C}$, *we have* $\tau(X) \in \mathbb{R}$ *and* $\tau(X) > 1$,
(3) for every real embedding $\tau : \mathbf{F} \hookrightarrow \mathbb{R}$, *we have* $1 < \tau(\alpha) < \tau(X)$ *(this inequality can be rewritten as an equation by Proposition 4.9).*

Suppose further that $z \subset \mathcal{O}_{\mathbf{K}}$ is an ideal such that $z\mathcal{O}_{\mathbf{F}} \subset X_1\alpha\mathcal{O}_{\mathbf{F}}$ and there is a free $\mathcal{O}_K/z$-module of finite rank W for which there are elements $v, w \in W$ such that $w \in W$ is a basis element and

$$v \otimes 1 = w \otimes \alpha = \alpha(w \otimes 1) \in W \otimes_{\mathcal{O}_{\mathbf{K}}} \mathcal{O}_{\mathbf{F}}.$$

Then $\alpha \in \mathcal{O}_{\mathbf{K}}$.

Before stating the corollary below we recall the definition of $\mathcal{W}_P$ from Lemma 10.7:

$$\mathcal{W}_P := \mathcal{N}^* \otimes_{\mathcal{O}_K} (z_P/z_P^2) \subset \mathcal{N}^* \otimes_{\mathcal{O}_K} (\mathcal{O}_K/z_P^2).$$

Corollary 13.17. *Let (r, I) be an exponent of diophantine stability for G relative to L/K (resp. $\mathbf{L}/\mathbf{K}$, $\mathbf{F}/\mathbf{K}$). Let Y denote the set of $\alpha \in \mathcal{O}_L$ for which there are points $P, Q \in M^r_{ID(\alpha),L}$ (resp. $M^r_{(2\alpha+1)^2I,\mathbf{L}}$, $M^r_{IX_1\alpha,\mathbf{F}}$) with $P \neq e$ such that*

$$\partial Q = \alpha \cdot \partial P \ \in \ \mathcal{W}_P \otimes_{\mathcal{O}_K} \mathcal{O}_L(\ \text{resp. } \mathcal{W}_P \otimes_{\mathcal{O}_{\mathbf{K}}} \mathcal{O}_{\mathbf{L}}, \mathcal{W}_P \otimes_{\mathcal{O}_{\mathbf{K}}} \mathcal{O}_{\mathbf{F}}). \tag{13.18}$$

In the totally real case assume $\alpha = 1 + u_1^2 + \cdots + u_4^2$. In the case of a quadratic extension let X_1 be defined as in Proposition 13.16. Then:

(1) $Y \subset \mathcal{O}_K$ (resp. $Y \subset \mathcal{O}_{\mathbf{K}}$).
(2) If $G(\mathcal{O}_K)$ (resp. $G(\mathcal{O}_{\mathbf{K}})$) contains a point of infinite order, then $\mathbb{N} \subset Y \subset \mathcal{O}_K$ (resp. $\mathbb{N} \subset Y \subset \mathcal{O}_{\mathbf{K}}$).

Proof. We consider the case of a number field extension L/K first. If $D(m, \alpha) = 0$ then $\alpha \in \{0, 1, 2, \ldots, m\}$, so we may suppose that $D(m, \alpha) \neq 0$. By the diophantine stability hypothesis of this corollary we have $P, Q \in G(\mathcal{O}_K)$—in particular these are K-rational points.

To connect with the notation of Proposition 13.13 above, let $W := \mathcal{W}_P$ and $z := z_P$, noting that $\mathcal{W}_P$ is a free $\mathcal{O}_K/z_P$-module by Lemma 10.7(2). Take the v and w of Proposition 13.13 to be, respectively, the images of ∂P and ∂Q in $\mathcal{W}_P$. Since $P \in M^r_{D(m,\alpha)I,L} \subset M_{D(\alpha)I,L}$ we have that $z_P \subset D(m, \alpha)I\mathcal{O}_L$. Proposition 13.13 then gives us that Y is contained in $\mathcal{O}_K$, which is (1).

Now suppose $\alpha \in \mathbb{N}$. Find a nontrivial point $P \in M^r_{D(m,\alpha)I,L}$. Note that such a P exists by Lemma 13.11 since $G(\mathcal{O}_K)$ contains a point of infinite order. Let $Q := P^\alpha$. By Corollary 10.10 we have

$$\partial Q = \alpha \cdot \partial P \in \mathcal{W}_P$$

so $\alpha \in Y$. This proves (2).

In the case of a totally real extension or quadratic extension of a totally real field, we note that $(2\alpha+1)^2$ and X_1 cannot be 0. Next we proceed exactly as above replacing $D(m,\alpha)$ by $(2\alpha+1)^2$ in the totally real case and replacing $D(m,\alpha)$ by $X_1\alpha I$, with n being an integer greater or equal to 3, in the case of a quadratic extension of a totally real field. □

The case $\mathbf{K}=\mathbf{L}$ is of particular interest to us, so we add the following corollary.

Corollary 13.19. *Let $\mathbf{F},\mathbf{L}$ be as above with $\mathbf{F}$ not totally real and let G be the twist of G_m defined at the beginning of Section 12. Let $(r,I)=(1,3\mathcal{O}_F)$. Let Y denote the set of $\alpha\in\mathcal{O}_{\mathbf{F}}$ for which there are points $P,Q\in M^1_{3X_1\alpha\mathcal{O}_{\mathbf{F}},\mathbf{F}}$ with $P\neq e$ such that*

$$\partial Q=\alpha\cdot\partial P\ \in\ \mathcal{W}_P\otimes_{\mathcal{O}_{\mathbf{L}}}\mathcal{O}_{\mathbf{F}}.$$

Here X_1 is again defined as in Proposition 13.16. Then $\mathbb{N}\subset Y\subset\mathcal{O}_{\mathbf{L}}$.

Proof. The corollary follows from Proposition 13.16, Lemmas 12.9 and 12.12. □

Remark 13.20. While $D(\alpha)$ and $(2\alpha+1)^2$ are obviously polynomial in nature, we remind the reader that one can see that X_1,X_2 can be described in a diophantine fashion from Corollaries 12.15 and 12.16.

Remark 13.21. Whether or not there are any points of infinite order in $G(\mathcal{O}_K)$, our proof will show that a given natural number ν is in E as long as $M^r_{D(\nu),L}$ (resp. $M^r_{D(\nu),\mathbf{L}}$) is not trivial.

14. An existential formulation of Corollaries 13.17 and 13.19

Our aim is to give a formulation of Corollaries 13.17 and 13.19 entirely in the language of $\mathcal{O}_{\mathbf{L}}$. Assume that G is a group scheme over $\mathcal{O}_K$ satisfying Assumption 7.4. Then:

(1) There exists a system of homogeneous equations over $\mathcal{O}_K$ that defines $\bar{G}$ the Zariski closure of G in $\mathbb{P}^n$ as described in Proposition 7.5 above, so using Lemma 4.6 above, there is an existential definition of the set of homogeneous coordinates $(\lambda_1:\lambda_2:\cdots:\lambda_{n+1})\in\mathrm{Aff}^{n+1}(\mathcal{O}_L)$ that are representatives of points $P\in\bar{G}(\mathcal{O}_L)$.
(2) Hence if, for example, $G=\mathcal{A}$ is an abelian scheme, G is an open $\mathcal{O}_L$-subscheme in $\bar{G}$ defined by a finite set of local congruences (see Remark 7.6) so there is an existential definition of the set of homogeneous coordinates

$$(\lambda_1:\lambda_2:\cdots:\lambda_{n+1})\in\mathrm{Aff}^{n+1}(\mathcal{O}_L)$$

that are representatives of points $P\in G(\mathcal{O}_L)$.

(3) Given two points $P, Q \in G(\mathcal{O}_L)$ add a further set of variables

$$\{r_1, r_2, \ldots, r_{n+1}; s_1, s_2, \ldots, s_{n+1}\}$$

and the equations (in the rings $\mathcal{O}_L[r_1, r_2, \ldots, r_{n+1}]$ and $\mathcal{O}_L[s_1, s_2, \ldots, s_{n+1}]$ respectively):

$$\mathcal{E}_P: \quad \sum_{i=1}^{n+1} r_i \lambda_i(P) = 1, \qquad \mathcal{E}_Q: \quad \sum_{i=1}^{n+1} s_i \lambda_i(Q) = 1. \tag{14.1}$$

This augmented system of equations gives us an existential definition of the sets of homogeneous coordinates that generate the unit ideal for P and for Q, a pair of points in $G(\mathcal{O}_L)$.

(4) Given an ideal $J \subset \mathcal{O}_L$ defined by an explicit finite set of generators $J := (j_1, j_2, \ldots, j_t) \subset \mathcal{O}_L$, we have an existential definition of the sets of homogeneous coordinates that generate the unit ideal for P and for Q, a pair of points in $M_{J,L}$ since the subgroup $M_{J,L} \subset G(\mathcal{O}_L)$ is defined by explicit congruence conditions.

(5) Since the r-th power mapping

$$G \xrightarrow{r\text{-th power}} G^r \subset G$$

is defined by a system of equations over $\mathcal{O}_L$ it then follows that $M_{J,L}^r$ has an existential definition in terms of $M_{J,L}$.

(6) Note that if (r, I) is an exponent of diophantine stability for L/K then if $P \in M_{J,L}^r \subset G(\mathcal{O}_K)$ is such that set of homogeneous coordinates

$$\{\lambda_i(P) : 1 \leq i \leq n+1\} \subset \mathcal{O}_L$$

generates the unit ideal in $\mathcal{O}_L$ then there exists a unit $u \in \mathcal{O}_L^\times$ such that

$$\{u\lambda_i(P) : 1 \leq i \leq n+1\} \subset \mathcal{O}_K \subset \mathcal{O}_L.$$

A consequence of this discussion is:

Corollary 14.2. *Assume given:*

- *a group scheme G satisfying Assumption 7.4,*
- *a well-arranged embedding $\iota : G \hookrightarrow \mathbb{P}^n$,*
- *a finite extension L/K,*
- *an exponent (r, I) of diophantine stability for L/K, and*
- *a set of generators $j_1, j_2, \ldots, j_t \in \mathcal{O}_K$ of I.*

Then there is a finite system of polynomials

$$\psi_i \in \mathcal{O}_K[X_1, X_2, \dots, X_{n+1}; Y_1, Y_2, \dots, Y_m; Z_1, Z_2, \dots, Z_t], \quad 1 \leq i \leq k,$$

where we call

- $X_1, X_2, \dots, X_{n+1}$ *the* **fundamental** *variables,*
- $Y_1, Y_2, \dots, Y_m$ *the* **auxiliary** *variables (to take care of items (1)–(6) above),*
- $Z_1, Z_2, \dots, Z_t$ *the* **congruence** *variables,*

with the following property. Set the congruence variables $Z_1, Z_2, \dots, Z_t$ to the given elements $j_1, j_2, \dots, j_t \in \mathcal{O}_K$ to obtain a system $\Psi_I := \{\psi_{I,1}, \dots, \psi_{I,k}\}$ defined by

$$\begin{aligned}&\psi_{I,i}(X_1, X_2, \dots, X_{n+1}; Y_1, Y_2, \dots, Y_m)\\ &\quad := \psi_i(X_1, X_2, \dots, X_{n+1}; Y_1, Y_2, \dots, Y_m; j_1, j_2, \dots, j_t)\\ &\quad \in \mathcal{O}_K[X_1, X_2, \dots, X_{n+1}; Y_1, Y_2, \dots, Y_m].\end{aligned}$$

If

$$(X_1, X_2, \dots, X_{n+1}; Y_1, Y_2, \dots, Y_m) \mapsto (\lambda_1, \lambda_2, \dots, \lambda_{n+1}; \mu_1, \mu_2, \dots, \mu_m) \in \mathrm{Aff}^{n+1+m}(\mathcal{O}_L)$$

is a common zero (in $\mathcal{O}_L$) of the system of equations Ψ_I, then there exists a rational point $P \in M^r_{I,L}$ such that the first $n+1$ entries of that common zero, i.e., the values of the fundamental variables:

$$(X_1, X_2, \dots, X_{n+1}) \;\mapsto\; (\lambda_1, \lambda_2, \dots, \lambda_{n+1}) \in \mathrm{Aff}^{n+1}(\mathcal{O}_L)$$

represent homogeneous coordinates for $\iota(P) \in \mathrm{Aff}^{n+1}(\mathcal{O}_L)$ that generate the unit ideal in $\mathcal{O}_L$:

$$(\lambda_1, \lambda_2, \dots, \lambda_{n+1}) = (\lambda_1(P), \lambda_2(P), \dots, \lambda_{n+1}(P)).$$

Moreover, every $P \in M^r_{I,L}$ is so represented.

Now recall Corollary 13.17: Let (r, I) be an exponent of diophantine stability for G relative to L/K. Let Y denote the set of $\alpha \in \mathcal{O}_L$ for which there are points $P, Q \in M^r_{ID(\alpha),L}$ with $P \neq e$ such that

$$\partial Q = \alpha \cdot \partial P \;\in\; \mathcal{W}_P \otimes_{\mathcal{O}_K} \mathcal{O}_L.$$

Assuming that we have chosen representative homogeneous coefficients for P and Q for which there are solutions in equations (14.1), consider an equation in the form of (13.18):

$$\partial Q = \alpha \cdot \partial P \ \in \ \mathcal{W}_P \otimes_{\mathcal{O}_K} \mathcal{O}_L$$

which can be written (appealing to (10.5) above):

$$\delta(P) \cdot \big(\lambda_1(Q), \dots, \lambda_d(Q)\big) \equiv \alpha \cdot \delta(Q) \cdot (\lambda_1(P), \dots, \lambda_d(P)) \pmod{z_P^2 \cdot (\mathcal{O}_L)^d}.$$

In order to rewrite the equivalence above as a polynomial equation we note that for any $x \in \mathcal{O}_L$, we have that $x \in z_P^2 \mathcal{O}_L$ if and only if $x = \sum_{i,j} a_{i,j} \lambda_i(P) \lambda_j(P), a_{i,j} \in \mathcal{O}_L$. As observed earlier, any two sets of coordinates corresponding to P will differ by a unit and therefore will generate the same ideal.

We now summarize the discussion above in the following three propositions.

Proposition 14.3. *Let L/K be a number field extension. Suppose G is a group scheme over $\mathcal{O}_K$ satisfying Assumption 7.4 and $G(\mathcal{O}_L)$ has a point of infinite order. If there is an exponent of diophantine stability for L/K, then there exists an* existential definition *$f(t, \bar{x}) \in \mathcal{O}_K[t, \bar{x}]$ of $\mathcal{O}_K$ in $\mathcal{O}_L$ such that for every $t \in \mathcal{O}_K$ we have that the equation $f(t, \bar{x}) = 0$ has solutions in $\mathcal{O}_K$.*

Proof. The assertion follows from Corollaries 13.17 and 14.2 combined with Lemma 4.7. □

In the same fashion we can prove the following proposition.

Proposition 14.4. *Let $\mathbf{L}$ be a totally real algebraic extension of $\mathbb{Q}$, possibly of infinite degree. Let $\mathbf{K}$ be a subfield of $\mathbf{L}$. Suppose G is a group scheme over $\mathcal{O}_\mathbf{K}$ satisfying Assumption 7.4 and $G(\mathcal{O}_\mathbf{L})$ has a point of infinite order. If there is an exponent of diophantine stability for $\mathbf{L}/\mathbf{K}$, then*

- *if $\mathbf{K}$ is a number field we have an* existential definition *$f(t, \bar{x})$ of $\mathcal{O}_\mathbf{K}$ over $\mathcal{O}_\mathbf{L}$ such that for every $t \in \mathcal{O}_\mathbf{K}$ the equation $f(t, \bar{x}) = 0$ has solutions in $\mathcal{O}_\mathbf{K}$.*
- *if $\mathbf{K}$ is an infinite extension of $\mathbb{Q}$ there exists $D \subset \mathcal{O}_\mathbf{L}$ such that D has an existential definition $f(t, \bar{x})$ over $\mathcal{O}_\mathbf{L}$, $\mathbb{N} \subset D \subset \mathcal{O}_\mathbf{K}$ and for any $t \in D$ the equation $f(t, \bar{x}) = 0$ has solutions in $\mathcal{O}_\mathbf{K}$.*

We now consider the case of quadratic extensions of totally real fields.

Proposition 14.5. *Let $\mathbf{F}$ be a quadratic extension of a totally real algebraic extension $\mathbf{L}$ of $\mathbb{Q}$, possibly of infinite degree over $\mathbb{Q}$. Let $\mathbf{K} \subset \mathbf{F}$ be a field. Suppose G is a group scheme over $\mathcal{O}_\mathbf{K}$ satisfying Assumption 7.4 and $G(\mathcal{O}_\mathbf{F})$ has a point of infinite order. If there is an exponent of diophantine stability for $\mathbf{F}/\mathbf{K}$, then*

- *if $\mathbf{K}$ is a number field we have an* existential definition *of $\mathcal{O}_\mathbf{K}$ over $\mathcal{O}_\mathbf{F}$.*
- *if $\mathbf{K}$ is an infinite extension of $\mathbb{Q}$ there exists $D \subset \mathcal{O}_\mathbf{L}$ such that D has an existential definition over $\mathcal{O}_\mathbf{F}$ and $\mathbb{N} \subset D \subset \mathcal{O}_\mathbf{K}$.*

Proof. The proof of the proposition follows from Corollaries 12.17, 13.17, 14.2 combined with Lemma 4.7. □

Proposition 14.5 does not require an assumption on existence of a group scheme, because we know such a group scheme exists.

Proposition 14.6. *Let* $\mathbf{F}$ *be a quadratic extension of a totally real algebraic extension* $\mathbf{L}$ *of* $\mathbb{Q}$*, possibly of infinite degree over* $\mathbb{Q}$*. There exists a set* $D \subset \mathcal{O}_{\mathbf{F}}$ *such that* D *has an existential definition over* $\mathcal{O}_{\mathbf{F}}$ *and* $\mathbb{N} \subset D \subset \mathcal{O}_{\mathbf{L}}$*.*

Proof. The proof of the proposition follows from Corollaries 12.13, 12.16, 12.17, 13.19 and 14.2. □

Below we state another corollary emphasizing the fact that in the case of totally real number fields and quadratic extensions of totally real number fields, our diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_M$ does not depend on the degree $[M : \mathbb{Q}]$.

Corollary 14.7. *Let* $\mathbf{M}$ *be a totally real algebraic extension of* $\mathbb{Q}$ *or a quadratic extension of a totally real algebraic extension of* $\mathbb{Q}$*. Let* $K \subset \mathbf{M}$ *be a number field. Suppose* G *is a group scheme over* $\mathcal{O}_K$ *satisfying Assumption 7.4 and* $G(\mathcal{O}_{\mathbf{M}})$ *has a point of infinite order. Suppose also there is an exponent of diophantine stability for* G *relative to* $\mathbf{M}/K$*. Let* $\mathcal{M}$ *be the collection of all number fields* M *such that* $K \subset M \subset \mathbf{M}$*. Then there exists a single diophantine definition of* $\mathcal{O}_K$ *over* $\mathcal{O}_M$ *across all fields* $\mathcal{O}_M \in \mathcal{M}$*.*

Theorem 3.1 follows directly from Proposition 14.3, and Theorem 3.9 follows directly from Propositions 14.4 and 14.6.

15. A simple example

Definition 15.1. A **CM-field** $\mathbf{F}$ is a totally complex field of algebraic numbers (possibly of infinite degree over $\mathbb{Q}$) possessing an involution σ with fixed field $\mathbf{F}^+ := \mathbf{F}^\sigma$ totally real.

Remarks 15.2.

(1) This terminology is usually only used for number fields $F/\mathbb{Q}$ (i.e., of finite degree over $\mathbb{Q}$) such fields being related to complex multiplication on abelian varieties—hence the "CM."
(2) The involution σ referred to in the definition above is unique: there is at most one involution of a totally complex field whose fixed field is totally real. Equivalently, the field $\mathbf{F}^+$ is the only totally real subfield $\mathbf{L}$ of $\mathbf{F}$ such that $\mathbf{F}/\mathbf{L}$ is quadratic. We will refer to $\mathbf{F}^+$ as *the* maximal totally real subfield of $\mathbf{F}$.

Let $\mathbf{F}$ be a CM-field and let $\mathbf{L} = \mathbf{F}^+$. Take our group scheme $G = \mathbf{G}_m := \mathrm{Spec}(\mathcal{O}_{\mathbf{L}}[s, s^{-1}])$ to be the multiplicative group. We view this as a quasi-projective smooth group scheme over $\mathcal{O}_{\mathbf{L}}$. We have that $G(\mathcal{O}_{\mathbf{L}}) = \mathcal{O}_{\mathbf{L}}^\times \subset G(\mathcal{O}_{\mathbf{F}}) = \mathcal{O}_{\mathbf{F}}^\times$.

Lemma 15.3. *Suppose I is an ideal of $\mathcal{O}_{\mathbf{F}}$ divisible by a rational integer $n \geq 3$. Then $M_{I,\mathbf{F}}^2 \subset \mathcal{O}_{\mathbf{L}}^\times$. That is, the pair $(2, I)$ is an exponent of diophantine stability for G relative to the field extension $\mathbf{F}/\mathbf{L}$ (see Definition 13.5(2)).*

Proof. Let σ denote complex conjugation, the nontrivial automorphism of $\mathbf{F}/\mathbf{L}$. Suppose $x \in M_{I,\mathbf{F}}$, i.e., $x \in \mathcal{O}_{\mathbf{F}}^\times$ and $x \equiv 1 \pmod{I}$. We have

$$x^2 = (xx^\sigma)(x/x^\sigma). \tag{15.4}$$

By Dirichlet's unit theorem (or the fact that all absolute values of x/x^σ are 1), we have that x/x^σ is a root of unity. Since $x/x^\sigma \equiv 1 \pmod{n}$, we have $x/x^\sigma = 1$. Since xx^σ is fixed by σ, it follows from (15.4) that $x^2 \in \mathcal{O}_{\mathbf{L}}$. □

This $(r = 2, I)$ exponent of diophantine stability for G relative to the extension $\mathcal{O}_{\mathbf{F}}/\mathcal{O}_{\mathbf{L}}$ allows one to prove the following proposition due to Denef for the case when $\mathbf{F}$ is a number field.

Proposition 15.5. *Let $\mathbf{F}$ be a CM field, and let K be any number field contained in $\mathbf{F}^+$. There exists a set $\mathcal{E}_K \subset \mathcal{O}_{\mathbf{F}^+}$ such that the following conditions are satisfied.*

(1) $\mathcal{E}_K$ is diophantine over $\mathcal{O}_{\mathbf{F}}$,
(2) $\mathcal{O}_K \subset \mathcal{E}_K$.

If $\mathbf{F}^+$ is a number field then we can take $\mathcal{E}_K = \mathcal{O}_K$.

Proof. Put $\mathbf{L} := \mathbf{F}^+$. We have the well-arranged embedding

$$\iota : \mathbf{G}_m \hookrightarrow \mathrm{Aff}^1 = \mathbf{G}_a = \mathrm{Spec}(\mathcal{O}_{\mathbf{L}}[t])$$

given by $t \mapsto s - 1$. The ideal cutting out the identity section of $\mathbf{G}_a$ is (t); the ideal cutting out the identity section of $\mathbf{G}_m$ is $(s-1)$. So the mapping $G_{[2]} \to \mathrm{Aff}^1_{[2]}$ is given by the homomorphism (isomorphism, in fact)

$$\mathcal{O}_{\mathbf{L}}[t]/(t^2) \xrightarrow{\simeq} \mathcal{O}_{\mathbf{L}}[s, s^{-1}]/((s-1)^2) = \mathcal{O}_{\mathbf{L}}[s]/((s-1)^2)$$

that sends $t \mapsto s - 1$.

Let us connect with the notation of Section 9 and more specifically equations (10.2) and (10.3) of that section.

- As above, $G = \mathbf{G}_m = \mathrm{Spec}(\mathcal{O}_{\mathbf{L}})[s, s^{-1}]$ and $G_{[2]} = \mathrm{Spec}(\mathcal{O}_{\mathbf{L}}[s]/((s-1)^2))$.

- An $\mathcal{O}_{\mathbf{L}}$-rational point $P \in G(\mathcal{O}_{\mathbf{L}})$ is given by a homomorphism

$$P : \mathcal{O}_{\mathbf{L}}[s, s^{-1}] \longrightarrow \mathcal{O}_{\mathbf{L}}$$

  sending s to a unit $u \in \mathcal{O}_{\mathbf{L}}^{\times} \subset \mathcal{O}_{\mathbf{L}}$.
- The vanishing ideal z_P is the ideal generated by $u - 1$ in $\mathcal{O}_{\mathbf{L}}$.
- The congruence ideal $c_P = z_P^2$ is the ideal generated by $(u-1)^2$.
- $\mathcal{N}_G = (s-1) \cdot \mathcal{O}_{\mathbf{L}}[s]/((s-1)^2)$; it is a free $\mathcal{O}_{\mathbf{L}}$-module of rank 1.
- $\partial P : \mathcal{N}_G \to \mathcal{O}_{\mathbf{L}}/(c_P) = \mathcal{O}_{\mathbf{L}}/((u-1)^2)$ is the $\mathcal{O}_{\mathbf{L}}$-homomorphism sending $s-1$ to $u-1$. We view ∂P as an element in

$$\mathcal{W}_P := \mathcal{N}^* \otimes_{\mathcal{O}} (z_P/z_P^2) \subset \mathcal{N}^* \otimes_{\mathcal{O}} (\mathcal{O}/z_P^2)$$

  as in Lemma 10.7 above.

Now the "Y" in Corollary 13.17 (combined with Lemma 4.7) gives the desired subset:

$$\mathcal{E}_K := Y = \{\alpha \in \mathcal{O}_L : \alpha \text{ satisfies (15.6) and (15.7) below}\}$$

$$\exists u_1, u_2, u_3, u_4 \in \mathcal{O}_L \text{ such that } \alpha = 1 + u_1^2 + \ldots u_4^2 \tag{15.6}$$

$$\exists P, Q \in M^2_{(2\alpha+1)^2, \mathbf{L}} \text{ with } P \neq e \text{ and } \partial Q = \alpha \cdot \partial P \ \in \ \mathcal{W}_P \otimes_{\mathcal{O}_K} \mathcal{O}_{\mathbf{L}}. \quad \square \tag{15.7}$$

Part 4. Diophantine stability in infinite algebraic extensions of $\mathbb{Q}$—results and conjectures

To date existential undecidability is known for very few rings with fraction fields equal to infinite algebraic extensions of $\mathbb{Q}$. The third author has shown that in any abelian extension of $\mathbb{Q}$ with finitely many ramified primes $\mathbb{Z}$ is existentially definable in infinitely many rings of $\mathcal{S}$-integers strictly larger than the ring of integers of the field in question. ([Shl94] and [Shl07]).

All the known results about existential definability of $\mathbb{Z}$ over the ring of integers in infinite extensions require some form of diophantine stability of elliptic curves. The first such results appear in [Shl18] and require diophantine stability of an elliptic curve in a totally real infinite extension of $\mathbb{Q}$. The definability of $\mathbb{Z}$ can then be extended to any quadratic extension of the totally real field under consideration.

From results of K. Kato [Kat04], K. Ribet [Rib81] and D. Rohrlich [Roh84,Roh88] we know that in cyclotomic extensions with finitely many ramified primes there exist elliptic curves with groups of points over these fields of positive rank and finitely generated (see [LR08], Theorem 1.2). Thus—as discussed in the introduction (Theorem 1.10)—$\mathbb{Z}$ is existentially definable in any abelian extension of $\mathbb{Q}$ having only finitely many ramified primes.

Below we show that diophantine stability of general abelian varieties, not just elliptic curves, can be used to establish existential definability of $\mathbb{Z}$ over the rings of integers of

totally real infinite extensions of $\mathbb{Q}$ and their totally complex quadratic extensions. We also make use of diophantine stability of multiplicative groups as described in Section 15. Additionally, we state some conjectures and questions based on conjectures and questions from Section 16.

16. Diophantine stability in abelian extensions

Our expectation, based on conjectures about elliptic curves over $\mathbb{Q}$ (some of which we describe below), is that diophantine *instability* is rare for abelian varieties in abelian extensions unless there is a good reason (analytic or geometric) for it. In this section we discuss this expectation and some open questions.

Notation 16.1. If A/K is an abelian variety and F/K is a finite Galois extension, we denote by $\mathbf{N}_{F/K} : A(F) \to A(K)$ the map $x \mapsto \sum_{\gamma \in \mathrm{Gal}(F/K)} \gamma x$.

If F/K is an abelian extension (finite or infinite) and $\chi : \mathrm{Gal}(F/K) \to \mathbb{C}^\times$ is a character of finite order, we will say that χ *occurs in* $A(F)$ if χ occurs in the representation of $\mathrm{Gal}(F/K)$ acting on $A(F) \otimes \mathbb{C}$.

From now on, a *character* of a Galois group G means a continuous character, i.e., a homomorphism $G \to \mathbb{C}^\times$ of finite order.

The following lemma shows that to understand diophantine stability in abelian extensions it suffices to understand diophantine stability in cyclic extensions.

Lemma 16.2. *Suppose* $\mathbf{L}$ *is an abelian extension of a number field* K*, and* A *is an abelian variety defined over* K*. Then the following are equivalent:*

(1) $\operatorname{rank} A(F) > \operatorname{rank} A(K)$ *for some finite extension* F/K *contained in* $\mathbf{L}$*,*
(2) $\operatorname{rank} A(F) > \operatorname{rank} A(K)$ *for some finite cyclic extension* F/K *contained in* $\mathbf{L}$*,*
(3) $\{x \in A(F) : \mathbf{N}_{F/K} x = 0\}$ *is infinite for some finite cyclic* F/K *contained in* $\mathbf{L}$*,*
(4) there is a nontrivial character χ *of* $\mathrm{Gal}(\mathbf{L}/K)$ *that occurs in* $A(\mathbf{L})$*.*

Proof. The implication (2) $\Rightarrow$ (1) is trivial.

Suppose F is a finite cyclic extension of K. Let $Z_F := \ker \mathbf{N}_{F/K} \subset A(F)$. Then $A(K) \cap Z_F \subset A(K)_{\mathrm{tors}}$ is finite, and if $x \in A(F)$ then

$$[F : K]x = \mathbf{N}_{F/K} x + ([F : K] - \mathbf{N}_{F/K})x \ \in A(K) + Z_F.$$

Thus there is a homomorphism with finite kernel and cokernel

$$A(K) \oplus Z_F \longrightarrow A(F), \tag{16.3}$$

so in particular (3) $\Leftrightarrow$ (2).

Now suppose (4) holds, and let F be the cyclic extension of K cut out by χ. Then χ occurs in $A(F)$ but not in $A(K)$, so (16.3) shows that χ must occur in Z_F. In particular Z_F is infinite, so (4) $\Rightarrow$ (3).

Finally, if (1) holds, then $A(F)/A(K)$ is infinite, so some character χ of $\mathrm{Gal}(\mathbf{L}/K)$ occurs in $A(F)/A(K)$, and such a χ is necessarily nontrivial. Thus (1) $\Rightarrow$ (4). □

Lemma 16.4. *Suppose* $\mathbf{L}$ *is an abelian extension of* $\mathbb{Q}$*, and* A *is an abelian variety defined over* $\mathbb{Q}$*. Then the following are equivalent:*

(1) $A(\mathbf{L})$ *is finitely generated,*
(2) the set $\{$*characters* χ *of* $\mathrm{Gal}(\mathbf{L}/\mathbb{Q}) : \chi$ *occurs in* $A(\mathbf{L})\}$ *is finite.*

Proof. The implication (1) $\Rightarrow$ (2) is clear.

Suppose (2) holds. A theorem of Ribet [Rib81] shows that $A(\mathbf{L})_{\mathrm{tors}}$ is finite. Let w be the exponent of $A(\mathbf{L})_{\mathrm{tors}}$. Fix a finite abelian extension K of $\mathbb{Q}$, contained in $\mathbf{L}$, such that $A(\mathbf{L})_{\mathrm{tors}} \subset A(K)$ and all characters χ of $\mathrm{Gal}(\mathbf{L}/\mathbb{Q})$ that occur in $A(\mathbf{L})$ factor through $\mathrm{Gal}(K/\mathbb{Q})$. Then for every finite extension F of K contained in $\mathbf{L}$ we have that $[A(F) : A(K)]$ is finite.

For every such F, define a homomorphism

$$\kappa_F : A(F) \longrightarrow H^1(F/K, A(F)_{\mathrm{tors}}) = \mathrm{Hom}(\mathrm{Gal}(F/K), A(F)_{\mathrm{tors}})$$

by sending $x \in A(F)$ to the $\mathrm{Gal}(F/K)$-cocycle $g \mapsto gx - x$. Note that $gx - x \in A(F)_{\mathrm{tors}}$ since $[A(F) : A(K)]$ is finite. It is easy to see that the kernel of κ_F is $A(K)$, and hence $A(F)/A(K)$ is killed by w. This holds for every field extension F of K in $\mathbf{L}$, so w annihilates $A(\mathbf{L})/A(K)$ as well, i.e.,

$$A(\mathbf{L}) \subset \{x \in A(\bar{\mathbb{Q}}) : wx \in A(K)\}.$$

Since the right-hand side is finitely generated, so is $A(\mathbf{L})$. Thus (2) $\Rightarrow$ (1). □

A lower bound for diophantine stability is given by the following theorem from [MR18].

Theorem 16.5 *(Theorem 1.2 of [MR18]). Suppose* A *is a simple abelian variety over* K *and all* $\bar{K}$*-endomorphisms of* A *are defined over* K*. Then there is a set* $\mathcal{S}$ *of rational primes with positive density such that for every* $\ell \in \mathcal{S}$ *and every* $n \geq 1$*, there are infinitely many cyclic extensions* L/K *of degree* ℓ^n *such that* $A(L) = A(K)$*.*

If A *is an elliptic curve without complex multiplication, then* $\mathcal{S}$ *can be taken to contain all but finitely many rational primes.*

Proof. All but the last sentence is proved in [MR18]. In the case that A is a non-CM elliptic curve, the proof in [MR18] shows that we can take $\mathcal{S}$ to contain all primes ℓ such

that the ℓ-adic representation $G_K \to \mathrm{Aut}(A[\ell^\infty]) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ is surjective. By Serre's theorem [Ser72] this holds for all but finitely many ℓ. □

The next two conjectures are formulated in [MR22], where they are motivated by the statistical properties of modular symbols. They were inspired by earlier conjectures (based on random matrix theory) given by others; notably David, Fearnley, and Kisilevsky [DFK07,FK12].

Conjecture 16.6 *(Conjecture 10.2 of [MR22]). Suppose E is an elliptic curve over $\mathbb{Q}$, and $\mathbf{L} \subset \mathbb{Q}^{\mathrm{ab}}$ is a real abelian field that contains only finitely many extensions of $\mathbb{Q}$ of degree 2, 3, or 5. Then $E(\mathbf{L})$ is finitely generated.*

Conjecture 16.7 *(Conjecture 10.1 of [MR22], combined with the Birch and Swinnerton-Dyer conjecture). Suppose E is an elliptic curve over $\mathbb{Q}$. Let X denote the set of even characters of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$. Then*

$$\{\chi \in X : \mathrm{order}(\chi) \geq 7,\ \mathrm{order}(\chi) \neq 8, 10 \text{ or } 12, \text{ and } \chi \text{ occurs in } E(\mathbb{Q}^{\mathrm{ab}})\}$$

is finite.

We now give some consequences of these conjectures for diophantine stability of abelian varieties over $\mathbb{Q}$.

Consequence 16.8. *Suppose Conjecture 16.6 holds, E is an elliptic curve over $\mathbb{Q}$, and $\mathbf{L} \subset \mathbb{Q}^{\mathrm{ab}}$ is a real abelian field that contains only finitely many extensions of $\mathbb{Q}$ of degree 2, 3, or 5. Then there is a finite extension $M/\mathbb{Q}$ such that for every number field F satisfying $F \subset \mathbf{L}$ and $F \cap M = \mathbb{Q}$, we have that $F/\mathbb{Q}$ is diophantine stable for E.*

Proof. Take M to be the field generated by the coordinates of points in $E(\mathbf{L})$, so $E(M) = E(\mathbf{L})$. Conjecture 16.6 says that $E(\mathbf{L})$ is finitely generated, so $M/\mathbb{Q}$ is finite. If $F \subset \mathbf{L}$ and $F \cap M = \mathbb{Q}$, then

$$E(F) = E(F) \cap E(\mathbf{L}) = E(F) \cap E(M) = E(F \cap M) = E(\mathbb{Q}). \quad \square$$

Definition/Proposition 16.9. *Suppose A is an abelian variety defined over a number field K, and F/K is a finite cyclic extension. Let $G := \mathrm{Gal}(F/K)$, let $\mathbb{Q}[G]_F$ be the unique irreducible $\mathbb{Q}[G]$-submodule of $\mathbb{Q}[G]$ on which G acts faithfully, and let*

$$\mathbb{Z}[G]_F := \mathbb{Q}[G]_F \cap \mathbb{Z}[G].$$

Following [MRS07, §5] we construct an abelian variety A_F over K (the twist of A by F/K) that has these properties:

(1) $\dim(A_F) = \varphi([F : K]) \dim(A)$, *where φ denotes the Euler φ-function.*

(2) The base change of A_F to F is canonically (and G-equivariantly) isomorphic to $A \otimes \mathbb{Z}[G]_F$ (over F).
(3) Suppose $\mathbf{L}$ is a field containing K and $\mathbf{L} \cap F = K$. Then:
(a) There is a natural inclusion $A_F(\mathbf{L}) \subset A(F\mathbf{L})$ that identifies

$$A_F(\mathbf{L}) \cong \{x \in A(F\mathbf{L}) : \mathbf{N}_{F\mathbf{L}/M\mathbf{L}} x = 0 \text{ for every } M \text{ with } K \subseteq M \subsetneq F\}.$$

(b) Suppose χ is a character of $\mathrm{Gal}(\mathbf{L}/K)$. Then χ occurs in $A_F(\mathbf{L})$ if and only if $\chi\rho$ occurs in $A(F\mathbf{L})$ for some faithful character ρ of $\mathrm{Gal}(F/K)$.

Proof. Assertion (1) is [MRS07, Theorem 2.1(i)], (3.a) is [MRS07, Theorem 5.8(ii)], and (3.b) follows from (3.a). □

Corollary 16.10. *Let F/K, A, and A_F be as in Proposition 16.9. If $[F : K]$ is prime, then* $\mathrm{rank}\, A_F(K) > 0$ *if and only if* $\mathrm{rank}\, A(F) > \mathrm{rank}\, A(K)$.

Proof. Taking $\mathbf{L} = K$ in Proposition 16.9(3) shows that $\mathrm{rank}\, A_F(K) > 0$ if and only if some faithful character ρ of $\mathrm{Gal}(F/K)$ occurs in $A(F)$. If $[F : K]$ is prime, then ρ is faithful if and only if it is nontrivial. By Lemma 16.2(1,4) a nontrivial ρ occurs in $A(F)$ if and only if $\mathrm{rank}\, A(F) > \mathrm{rank}\, A(K)$. This proves the corollary. □

Consequence 16.11. *Suppose $F/\mathbb{Q}$ is a cyclic extension of prime degree $p \geq 7$, and E is an elliptic curve over $\mathbb{Q}$. Let $A := E_F$ be the twist of E as in Definition 16.9. Suppose Conjecture 16.7 holds and $\mathbf{L}$ is a real abelian extension of $\mathbb{Q}$ not containing F. Then:*

(1) $A(\mathbf{L})$ is finitely generated.
(2) If $\mathrm{rank}\, E(F) > \mathrm{rank}\, E(\mathbb{Q})$ *then* $\mathrm{rank}\, A(\mathbb{Q}) > 0$.

Proof. Proposition 16.9(3b) shows that a character χ of $\mathrm{Gal}(\mathbf{L}/\mathbb{Q})$ occurs in $A(\mathbf{L})$ if and only if $\chi\rho$ occurs in $E(F\mathbf{L})$ for some nontrivial character ρ of $\mathrm{Gal}(F/\mathbb{Q})$. Since $\mathbf{L} \cap F = \mathbb{Q}$, we have $\mathrm{Gal}(\mathbf{L}F/\mathbb{Q}) = \mathrm{Gal}(\mathbf{L}/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q})$, so such a character $\chi\rho$ has order divisible by $p \geq 7$. Thus Conjecture 16.7 predicts that only finitely many characters occur in $A(\mathbf{L})$. Now (1) follows by Lemma 16.4, and (2) follows from (1) by Corollary 16.10. □

The following construction shows that there is a large collection of abelian fields $\mathbf{L}$ "close" to $\mathbb{Q}^{\mathrm{ab}}$ to which we can try to apply Consequence 16.11.

Example 16.12. Fix a prime $p \geq 7$, and another prime $\ell \equiv 1 \pmod{p}$ but $\ell \not\equiv 1 \pmod{p^2}$. Let F denote the unique cyclic extension of $\mathbb{Q}$ of degree p and conductor ℓ. It follows from class field theory that there are infinitely many real abelian extensions $\mathbf{L}/\mathbb{Q}$ such that

- $[\mathbb{Q}^{\mathrm{ab},+} : \mathbf{L}] = p$,

- $\mathbf{L} \cap F = \mathbb{Q}$

(where $\mathbb{Q}^{\mathrm{ab},+}$ denotes the real subfield of $\mathbb{Q}^{\mathrm{ab}}$).

In order to apply Consequence 16.11 to the arithmetic of the "big" fields of Example 16.12 (see Consequences 17.3 and 18.4), we need to have that $\operatorname{rank} E(F) > \operatorname{rank} E(\mathbb{Q})$. This leads to the following question:

Question 16.13. Suppose $F/\mathbb{Q}$ is a cyclic extension of prime degree p. Is there an elliptic curve E defined over $\mathbb{Q}$ such that $\operatorname{rank} E(F) > \operatorname{rank} E(\mathbb{Q})$?

Remark 16.14. Computer calculations and heuristics similar to [MR22] suggest that when $p = 7$, the answer to Question 16.13 is "yes". When $p > 7$ the answer is less clear, but Fearnley and Kisilevsky [FK12] produce some examples with $p = 7$ and 11. Our own calculations, assuming the Birch and Swinnerton-Dyer conjecture, found four examples with $p = 13$. For instance, if E is the curve labeled 4025.c1 in [Col], and F is the extension of degree 13 in $\mathbb{Q}(\zeta_{53})$, then $L(E/F, s)/L(E/\mathbb{Q}, s)$ vanishes at $s = 1$. Thus the Birch and Swinnerton-Dyer conjecture predicts that $\operatorname{rank} E(F) > \operatorname{rank} E(\mathbb{Q})$.

Consequence 16.15. *Suppose Conjecture 16.7 holds, and $p = 7$ or 11. Then there is an abelian variety A over $\mathbb{Q}$ and infinitely many real abelian fields $\mathbf{L}$ such that $[\mathbb{Q}^{\mathrm{ab},+} : \mathbf{L}] = p$, and $A(\mathbf{L})$ is infinite and finitely generated.*

If the Birch and Swinnerton-Dyer conjecture holds for elliptic curves, then the same statement holds for $p = 13$.

Proof. If $p = 7$, let E be the elliptic curve $y^2 + xy + y = x^3 - x^2 - 6x + 5$ and F the abelian field of degree 7 and conductor 29. If $p = 11$, let E be the elliptic curve $y^2 + xy = x^3 + x^2 - 32x + 58$ and F the abelian field of degree 11 and conductor 23. Let $\mathbf{L}$ be a real abelian field as in Example 16.12, and let $A := E_F$ be the twist of E as in Definition 16.9. Fearnley and Kisilevsky [FK12] show that $\operatorname{rank} E(F) > \operatorname{rank} E(\mathbb{Q})$. Thus for $p = 7$ or 11 the desired conclusion follows from Consequence 16.11.

For $p = 13$ the proof is the same, except that for the elliptic curve E labeled 4025.c1 in [Col], and the cyclic extension F of degree 13 and conductor 53, we need the Birch and Swinnerton-Dyer conjecture in order to conclude that $\operatorname{rank} E(F) > \operatorname{rank} E(\mathbb{Q})$. □

The following consequence of Conjecture 16.7 gives rise to a collection of "big" abelian fields $\mathbf{L}$ over whose ring of integers Hilbert's Tenth Problem has a negative answer. Although these fields are not as close to $\mathbb{Q}^{\mathrm{ab}}$ as those of Example 16.12, we can produce them without needing to know the answer to Question 16.13.

Consequence 16.16. *Suppose Conjecture 16.7 holds. There is a positive integer n and an abelian variety $A/\mathbb{Q}$ such that*

(1) $\operatorname{rank} A(\mathbb{Q}) > 0$,
(2) *if L is a finite real abelian extension of $\mathbb{Q}$ and $[L:\mathbb{Q}]$ is relatively prime to n, then* $\operatorname{rank} A(L) = \operatorname{rank} A(\mathbb{Q})$,

Proof. Fix an elliptic curve E defined over $\mathbb{Q}$. By Conjecture 16.7 there is a finite cyclic extension F of $\mathbb{Q}$ that is maximal in the sense that

(a) there is a faithful character ψ of $\mathrm{Gal}(F/\mathbb{Q})$ that occurs in $E(F)$,
(b) there is no cyclic extension F' of $\mathbb{Q}$ with property (a) that properly contains F.

Fix such an F, and let $n := [F:\mathbb{Q}]$ and $A := E_F$. By property (a) and 16.9(3b), the trivial character occurs in $A(\mathbb{Q})$, so $A(\mathbb{Q})$ is infinite.

Now fix an abelian extension $L/\mathbb{Q}$ of degree prime to n. In particular $L \cap F = \mathbb{Q}$. Suppose χ is a nontrivial character of $\mathrm{Gal}(L/\mathbb{Q})$, and let L' be the cyclic extension of $\mathbb{Q}$ cut out by χ. Since $[L:\mathbb{Q}]$ is prime to $[F:\mathbb{Q}]$, the compositum FL' is also cyclic over $\mathbb{Q}$. By the maximality of F (property (b)) and 16.9(3.b), we conclude that χ does not occur in $A(L)$. Lemma 16.4 now shows that $\operatorname{rank} A(L) = \operatorname{rank} A(\mathbb{Q})$. □

It is natural to try to generalize Conjectures 16.6 and 16.7 by asking whether they still hold for abelian varieties over number fields instead of elliptic curves over $\mathbb{Q}$.

Question 16.17. How much diophantine instability can there be? For example, suppose K is a totally real number field, and A is an abelian variety over K. Is there a constant $C(A,K)$ such that for every finite abelian extension L/K, and every character $\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$ of order greater than $C(A,K)$, χ does *not* occur in the representation of $\mathrm{Gal}(L/K)$ on $A(L)\otimes\mathbb{C}$? If there is such a constant $C(A,K)$, how does it depend on A, and on K?

Remark 16.18. The reason to restrict to totally real fields in Question 16.17 is that otherwise the Birch and Swinnerton-Dyer conjecture can be used to force diophantine instability. For example, suppose K is an imaginary quadratic field, and E is an elliptic curve over $\mathbb{Q}$ with the property that every prime where E has bad reduction splits into 2 distinct primes in K. Then the theory of Heegner points gives rise to arbitrarily large cyclic extensions L/K such that

$$\operatorname{rank} E(L) > \operatorname{rank} \sum_{K \subseteq F \subsetneq L} E(F).$$

The fields in question are anticylotomic extensions of K, i.e., Galois extensions of $\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q})$ acting as -1 on $\mathrm{Gal}(L/K)$. These extensions are "sparse" in the set of all abelian extensions of K.

17. Totally real fields

The biggest difference between definability problems over finite and infinite extensions of $\mathbb{Q}$ lies in the difficulty of bounding heights of elements in infinite extensions. Recall that for finite extensions, the bound in Section 11 was generated by using explicitly the degree of the extension over $\mathbb{Q}$. For obvious reasons such a method of producing bounds on the height of elements will not work over a ring of integers of an infinite extension. However, over a totally real field there is a substitute method relying on sums of squares that we used in Section 11 and other sections of Part 3. So in order to prove existential undecidability over the ring of integers of an infinite totally real extension $\mathbf{L}$ of $\mathbb{Q}$, all we need is an abelian variety A over $\mathbf{L}$ with $A(\mathbf{L})$ finitely generated and of positive rank.

Corollary 17.1. *Let $\mathbf{L}$ be a totally real infinite extension of $\mathbb{Q}$ and let A be an abelian variety such that $A(\mathbf{L})$ is infinite and finitely generated. Then $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{L}}$.*

Proof. Let K be the field generated over $\mathbb{Q}$ by points in $A(\mathbf{L})$. Then K is a totally real number field and $A(K) = A(\mathbf{L})$. By Proposition 14.4, we have that $\mathcal{O}_K$ is diophantine over $\mathcal{O}_{\mathbf{L}}$. As was described in the introduction, J. Denef showed that the ring of integers of any totally real number field has a diophantine definition of $\mathbb{Z}$. Therefore from Lemma 4.3 we can deduce that $\mathbb{Z}$ is diophantine over $\mathcal{O}_{\mathbf{L}}$. □

Consequence 17.2. *Suppose Conjecture 16.6 holds, and $\mathbf{L} \subset \mathbb{Q}^{\mathrm{ab},+}$ is a real abelian field that contains only finitely many extensions of $\mathbb{Q}$ of degree 2, 3, or 5. Then $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{L}}$ and Hilbert's Tenth Problem for $\mathcal{O}_{\mathbf{L}}$ has a negative solution.*

Proof. By Conjecture 16.6, we can find an elliptic curve E such that $E(\mathbf{L})$ is infinite and finitely generated. Thus the assertion of the consequence holds by Corollary 17.1. □

From Consequence 16.15 combined with Corollary 17.1, we also obtain the following consequence.

Consequence 17.3. *Suppose Conjecture 16.7 holds. If $p = 7$ or 11, then there exists a totally real abelian extension $\mathbf{L}$ such that $[\mathbb{Q}^{\mathrm{ab},+} : \mathbf{L}] = p$ and $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{L}}$.*

If the Birch and Swinnerton-Dyer conjecture holds for elliptic curves, then the same is true with $p = 13$.

18. Quadratic extensions of totally real fields again

A reduction to the maximal totally real subfield. As has been noted above, totally real fields are special in the sense that sums of squares allow us to impose bounds on heights

of variables using existential language of the rings only. Much of this definability "advantage" is inherited by quadratic extensions of totally real fields; in other words one can reduce a definability problem over a quadratic extension of a totally real field to a definability problem over this totally real field. From Proposition 14.5 we have the following corollary.

Corollary 18.1. *Let* $\mathbf{F}$ *be a quadratic extension of a totally real field. If there exists an abelian variety* A *over* $\mathbf{F}$ *such that* $A(\mathbf{F})$ *is infinite and finitely generated, then* $\mathbb{Z}$ *is existentially definable over* $\mathcal{O}_{\mathbf{F}}$*, and Hilbert's Tenth Problem is undecidable over* $\mathcal{O}_{\mathbf{F}}$*.*

Proof. Let $\mathbf{F} = \mathbf{L}(\gamma)$ where $\mathbf{L}$ is totally real and $\gamma^2 \in \mathbf{L}$. Let F be the subfield of $\mathbf{F}$ generated over $\mathbb{Q}$ by the points in $A(\mathbf{F})$. Since $A(\mathbf{F})$ is finitely generated, F is a number field, so we have $F = \mathbb{Q}(\delta)$ where $\delta \in \mathbf{F}$, i.e., $\delta = a + b\gamma$ with $a, b \in \mathbf{L}$. Let $L := F(a, b, \gamma^2) \cap \mathbf{L}$ and $K := L(\delta)$. Then L is totally real, and $a, b, \gamma^2 \in L$, so $[K : L] = 2$. Thus K is a quadratic extension of a totally real number field, and $F \subset K$ so $A(K) = A(\mathbf{F})$.

By a result of Denef ([Den75]) and a result Denef and Lipshitz ([DL78]) we have that $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_K$. By Proposition 14.5 we have that $\mathcal{O}_K$ has a diophantine definition over $\mathcal{O}_{\mathbf{F}}$. Finally by Lemma 4.3 (Transitivity of diophantine definitions), we can now conclude that $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{F}}$ and the assertion of the corollary follows. □

Then following corollary provides a slightly different way of establishing diophantine undecidability of quadratic extensions of totally real fields.

Corollary 18.2. *Let* $\mathbf{F}$ *be a quadratic extension of a totally real field* $\mathbf{L}$*. If there exists an abelian variety* A *over* $\mathbf{L}$ *such that* $A(\mathbf{L})$ *is infinite and finitely generated, then* $\mathbb{Z}$ *is existentially definable over* $\mathcal{O}_{\mathbf{F}}$*, and Hilbert's Tenth Problem is undecidable over* $\mathcal{O}_{\mathbf{F}}$*.*

Proof. Let K be the number field generated by the points in $A(\mathbf{L})$, so $A(K) = A(\mathbf{L})$. By Proposition 14.4, there exists a diophantine definition $f(t, \bar{x})$ of $\mathcal{O}_K$ over $\mathcal{O}_{\mathbf{L}}$ such that for all $t \in \mathcal{O}_K$ the equation $f(t, x_1, \ldots, x_r) = 0$ has solutions in $\mathcal{O}_K$. By Proposition 14.6, we have that there exists $D \subset \mathcal{O}_{\mathbf{F}}$ such that D is diophantine over $\mathcal{O}_{\mathbf{F}}$ and $\mathbb{N} \subset D \subset \mathcal{O}_{\mathbf{L}}$.

Let $\gamma \in \mathcal{O}_K$ generate K over $\mathbb{Q}$ and define $\hat{D} \subset \mathcal{O}_{\mathbf{F}}$ in the following manner.

$$\hat{D} = \{ \sum_{i=0}^{[K:\mathbb{Q}]-1} a_i \gamma^i | \pm a_i \in D \}.$$

Observe that since D is diophantine of over $\mathcal{O}_{\mathbf{F}}$, we have that $\hat{D}$ is diophantine over $\mathcal{O}_{\mathbf{F}}$. Further, $\mathcal{O}_K \subset \hat{D} \subset \mathcal{O}_{\mathbf{F}}$. Let $g(x, \bar{y})$ be a diophantine definition of $\hat{D}$ over $\mathcal{O}_{\mathbf{F}}$. Now consider the following system of equations:

$$\begin{cases} g(x_1, \bar{y}_1) = 0, \\ \cdots \\ g(x_r, \bar{y}_r) = 0, \\ g(t, z_1, \ldots, z_r), \\ f(t, x_1, \ldots, x_r) = 0 \end{cases} \tag{18.3}$$

Suppose (18.3) has solutions in $\mathcal{O}_{\mathbf{F}}$. Then by assumption on g being the diophantine definition of $\hat{D}$, we have that $t, x_1, \ldots, x_r \in \hat{D} \subset \mathcal{O}_{\mathbf{L}}$. Since f is a diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_{\mathbf{L}}$, we conclude that $t \in \mathcal{O}_K$. Conversely, suppose $t \in \mathcal{O}_K$, then there exist $x_1, \ldots, x_r \in \mathcal{O}_K \subset \hat{D}$ such that $f(t, x_1, \ldots, x_r) = 0$. Since $t, x_1, \ldots, x_r \in \mathcal{O}_K \subset \hat{D}$, there exist $\bar{y}_1, \ldots, \bar{y}_r, \bar{z}$ with all components in $\mathcal{O}_{\mathbf{F}}$ such that all g-equations are satisfied. Thus (18.3) is a diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_{\mathbf{F}}$.

From [Den75] we have that $\mathcal{O}_K$ has a diophantine definition of $\mathbb{Z}$. Thus applying Lemma 4.3 to the tower $\mathbb{Z} \subset \mathcal{O}_K \subset \mathcal{O}_{\mathbf{F}}$, we have that $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{F}}$. □

Combining Corollary 18.2 with Consequence 16.15 we get another consequence of Conjecture 16.7.

Consequence 18.4. *Suppose Conjecture 16.7 holds. If $p = 7$ or 11, then there exists an abelian extension $\mathbf{L}$ such that $[\mathbb{Q}^{\mathrm{ab}} : \mathbf{L}] = p$ and $\mathbb{Z}$ has a diophantine definition over $\mathcal{O}_{\mathbf{L}}$.*

If the Birch and Swinnerton-Dyer conjecture holds for elliptic curves, then the same is true with $p = 13$.

Data availability

No data was used for the research described in the article.

Appendix A. A geometric formulation of diophantine stability

19. The same structures described in a different vocabulary

If K is a number field let $\mathcal{O}_K$ denote its ring of integers.

Definition 19.1 *(Compare with Definition 1.2).* Let L/K be an extension of number fields. Let

$$\boxed{\mathcal{F}: \ f_i(\mathsf{t}; x_1, x_2, x_3, \ldots x_n)}$$

be a system of m polynomials ($i = 1, 2, \ldots, m$) with coefficients in $\mathcal{O}_K$. We've singled out the first variable t, which will play a special role. Say that $\mathcal{F}$ is **diophantine stable at t** for L/K if all the simultaneous solutions

$$f_i(\mathsf{a}; a_1, a_2, \dots, a_n) = 0$$

for $\mathsf{a}, a_1, a_2, \dots, a_n \in \mathcal{O}_L$ and $i = 1, 2, \dots, m$ have the property that *the "singled out"* entry $\mathsf{t} = \mathsf{a}$ lies in $\mathcal{O}_K$.

Example 19.2. Let $\mathcal{F}$ be the equation over $\mathcal{O}_K$ that says that t is a unit:

$$\boxed{f(\mathsf{t}; x_1) := 1 - \mathsf{t} \cdot x_1 = 0.}$$

So $\mathcal{F}$ is diophantine stable at t for any L/K where $\mathcal{O}_L$ and $\mathcal{O}_K$ have the same unit group.

Any system of equations $\mathcal{F}$ over $\mathcal{O}_K$ (as in Definition 19.1 above) determines a finitely presented affine $\mathcal{O}_K$-scheme

$$V = V_{\mathcal{F}} := \mathrm{Spec}(\mathcal{O}_K[\mathsf{t}; x_1, x_2, \dots, x_n]/(f_1, f_2, \dots, f_m))$$

Let $\mathrm{Aff}^1 = \mathrm{Spec}(\mathcal{O}_K[t])$ be 1-dimensional affine space, viewed as (an affine) scheme over $\mathcal{O}_K$. The homomorphism $\mathcal{O}_K[\mathsf{t}] \to \{\mathcal{O}_K[\mathsf{t}; x_1, x_2, \dots, x_n]/(f_1, f_2, \dots, f_m)\}$ induced by sending $\mathsf{t} \mapsto \mathsf{t}$ can be viewed as an $\mathcal{O}_K$-morphism:

$$V \xrightarrow{\mathsf{t}} \mathrm{Aff}^1$$

which in turn induces a map on $\mathcal{O}_L$-valued points

$$V(\mathcal{O}_L) \xrightarrow{\mathsf{t}} \mathcal{O}_L. \tag{19.3}$$

The *diophantine stable at* t property of $\mathcal{F}$ relative to L/K is equivalent to the property that the image of $V(\mathcal{O}_L)$ under (19.3) is contained in the subset $\mathcal{O}_K$ of $\mathcal{O}_L$.

If we denote the image of (19.3) in $\mathcal{O}_L$ by E, then

$$V(\mathcal{O}_L) \xrightarrow{\text{onto}} E \subset \mathcal{O}_L = \mathrm{Aff}^1(\mathcal{O}_L)$$

shows that $\mathcal{F}$ (or equivalently, the pair (V, t)) is a **diophantine definition of** E **over** $\mathcal{O}_L$ (see Definition 2.2). We are especially interested in the case where $E = \mathcal{O}_K \subset \mathcal{O}_L$.

Proposition 19.4. *If L/K is an extension of number fields, $\mathcal{F}$ is a system of polynomials as in Definition 19.1, and the image E of the map (19.3) on $\mathcal{O}_L$-valued points of $V_{\mathcal{F}}$ satisfies $\mathbb{N} \subset E \subset \mathcal{O}_K$, then there is a system $\mathcal{F}'$ such that the corresponding pair $(V_{\mathcal{F}'}, \mathsf{t})$ is a diophantine definition of $\mathcal{O}_K$ over $\mathcal{O}_L$.*

Proof. This is Lemma 4.7 above. □

A diophantine definition $(V, \mathtt{t})$ of $\mathcal{O}_K$ over $\mathcal{O}_L$ can be used to transport any algorithm that determines whether a system of polynomials with coefficients in $\mathcal{O}_L$ has a solution over $\mathcal{O}_L$ to a similar algorithm for systems of polynomials with coefficients in $\mathcal{O}_K$, as follows.

Construction 19.5. *Suppose we are given a diophantine definition $(V, \mathtt{t})$ of $\mathcal{O}_K$ over $\mathcal{O}_L$. For every finitely presented affine scheme $\mathcal{B}$ over $S = \mathrm{Spec}(\mathcal{O}_K)$ we can construct an S-scheme $\mathcal{V} = \mathcal{V}_{\mathcal{B}}$ with a surjective S-morphism $\tau : \mathcal{V} \twoheadrightarrow \mathcal{B}$:*

$$\begin{array}{ccc} \mathcal{V} & \xrightarrow{\tau} & \mathcal{B} \\ & \searrow & \downarrow \\ & & S \end{array}$$

with the property that the image of the set of $\mathcal{O}_L$-valued points of $\mathcal{V}$ under τ is equal to the set of $\mathcal{O}_K$-valued points of $\mathcal{B}$:

$$\begin{array}{ccc} & & \mathcal{V}(\mathcal{O}_L) \\ & \overset{\text{onto}}{\swarrow} & \downarrow \tau \\ \mathcal{B}(\mathcal{O}_K) & \longrightarrow & \mathcal{B}(\mathcal{O}_L) \end{array}$$

Proof. Let $(V, \mathtt{t})$ be the diophantine definition, and

$$\mathcal{G}: \ g_i(z_1, z_2, \ldots, z_\nu) \in \mathcal{O}_K[z_1, z_2, \ldots, z_\nu] \quad \text{for } i = 1, 2, \ldots, \mu$$

the presentation of the affine scheme $\mathcal{B}$. We can view this presentation as giving us a closed embedding

$$\mathrm{Spec}(\mathcal{O}_K[z_1, z_2, \ldots, z_\nu]/(g_1, g_2 \ldots, g_\mu)) = \mathcal{B} \overset{j}{\hookrightarrow} \mathrm{Aff}^\nu = \mathrm{Spec}(\mathcal{O}_K[z_1, z_2, \ldots, z_\nu]).$$

Let $V^{\{\nu\}} := V \times_{\mathcal{O}_K} V \times_{\mathcal{O}_K} \ldots V$ be the ν-fold power of V (fiber-product over $S = \mathrm{Spec}(\mathcal{O}_K)$) and form the cartesian diagram:

$$\begin{array}{ccc} \mathcal{V}_{\mathcal{B}} = \mathcal{V} & \hookrightarrow & V^{\{\nu\}} \\ \downarrow \tau & & \phi \downarrow (\mathtt{t},\mathtt{t},\ldots,\mathtt{t}) \\ \mathcal{B} & \hookrightarrow & \mathrm{Aff}^\nu. \end{array} \tag{19.6}$$

Since the map ϕ of (19.6) is a surjective morphism of schemes, so is the projection $\tau : \mathcal{V} \to \mathcal{B}$. Since $(V, \mathtt{t})$ is a diophantine definition, the mapping ϕ is a surjection of $V^{\{\nu\}}(\mathcal{O}_L)$, the set of $\mathcal{O}_L$-valued points of $V^{\{\nu\}}$, onto $\mathrm{Aff}^\nu(\mathcal{O}_K)$. If v is an $\mathcal{O}_L$-valued point of $\mathcal{V}$ then, by commutativity of (19.6), $\tau(v)$ is an $\mathcal{O}_K$-valued point of $\mathcal{B}$; and,

by cartesian-ness of (19.6), any $\mathcal{O}_K$-valued point of $\mathcal{B}$, viewed in $\mathrm{Aff}^\nu(\mathcal{O}_K)$ lifts to an $\mathcal{O}_L$-valued point of $V^{\{\nu\}}$. □

Therefore

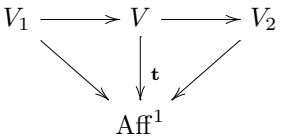
Corollary 19.7. *Suppose* $(V, \mathtt{t})$ *is a diophantine definition of* $\mathcal{O}_K$ *over* $\mathcal{O}_L$*. Then the following are equivalent:*

(1) The $\mathcal{O}_K$*-scheme* $\mathcal{B}$ *has an* $\mathcal{O}_K$*-rational 'point' (meaning: a* $\mathrm{Spec}(\mathcal{O}_K)$*-section).*
(2) The system of equations $\mathcal{G} : g_i(z_1, z_2, \ldots, z_\nu) \in \mathcal{O}_K[z_1, z_2, \ldots, z_\nu]$ *for* $i = 1, 2, \ldots, \mu$ *has a simultaneous solution in* $\mathcal{O}_K$*.*
(3) The finitely presented $\mathcal{O}_L$*-scheme* $\mathcal{V}_\mathcal{B}$ *has an* $\mathcal{O}_L$*-rational 'point' (meaning: a* $\mathrm{Spec}(\mathcal{O}_L)$*-section).*
(4) The system of equations over $\mathcal{O}_L$ *finitely presenting the* $\mathcal{O}_L$*-scheme* $\mathcal{V}_\mathcal{B}$ *has a simultaneous solution in* $\mathcal{O}_L$*.*

Remark 19.8. Suppose $\mathcal{G}$ is a finite system of polynomial equations over $\mathcal{O}_K$ defining a scheme $\mathcal{B}$ as in Construction 19.5, and we are given a diophantine definition $(V, \mathtt{t})$ of $\mathcal{O}_K$ over $\mathcal{O}_L$. If we have a finite algorithm to determine whether or not a finite system of polynomial equations over $\mathcal{O}_L$ has a simultaneous solution over $\mathcal{O}_L$, then—by Corollary 19.7—applying this algorithm to the system of equations over $\mathcal{O}_L$ that finitely present the $\mathcal{O}_L$-scheme $\mathcal{V}_\mathcal{B}$ will tell us whether or not $\mathcal{G}$ has a simultaneous solution over $\mathcal{O}_K$. In particular, a negative answer for $\mathcal{O}_K$ to the question posed by Hilbert's Tenth Problem implies a similar negative answer for $\mathcal{O}_L$.

Remark 19.9. What can be said about the category comprising the various diophantine definitions of rings of integers related to a given L/K? E.g., beyond the fact that:

- The diophantine definitions, $(V, \mathtt{t})$, of $\mathcal{O}_K$ over $\mathcal{O}_L$ are closed under fiber product over Aff^1.
- Any $(V, \mathtt{t})$ sandwiched between two diophantine definitions of $\mathcal{O}_K$ in $\mathcal{O}_L$ is again one:



Question 19.10. Given L/K what is the smallest Krull dimension of a diophantine definition $(V, \mathtt{t})$ of $\mathcal{O}_K$ over $\mathcal{O}_L$? For example, what is the smallest Krull dimension of a diophantine definition of $\mathbb{Z}$ over $\mathbb{Z}[i]$?

A related question concerns the smallest number of variables one needs to define $\mathcal{O}_K$ over $\mathcal{O}_L$. The smallest number of variables question has a long history. In its first

version, the question concerned the smallest number of variables necessary to define a non-recursive c.e. subset of natural numbers or integers. Yu. Matiyasevich, J. Robinson and J. Jones were the first people considering this problem. Later on they were joined by Zhi-Wei Sun, among others. His recent paper [Sun21] contains the most recent survey of the results in the area. H. Pasten in [Pas22a] and independently A. Fehm, P. Dittman and N. Daans in [DDF21] considered the smallest number of variables question in the context of diophantine definitions over rings and fields. They called this number the *diophantine rank* of a set.

References

[Col] LMFDB Collaboration, The L-functions and modular forms database, www.lmfdb.org.

[CS08] Gunther Cornelissen, Alexandra Shlapentokh, Defining the integers in large rings of number fields using one universal quantifier, Zap. Nauč. Semin. POMI 358 (2008) 199–223.

[CPZ05] Gunther Cornelissen, Thanases Pheidas, Karim Zahidi, Division-ample sets and diophantine problem for rings of integers, J. Théor. Nr. Bordx. 17 (2005) 727–735.

[DDF21] Nicolas Daans, Philip Dittmann, Arno Fehm, Existential rank and essential dimension of diophantine sets, arXiv:2102.06941v2 [math.NT], 2021.

[DFK07] Chantal David, Jack Fearnley, Hershy Kisilevsky, Vanishing of L-Functions of Elliptic Curves over Number Fields, London Math. Soc. Lecture Note Ser., vol. 341, Cambridge Univ. Press, Cambridge, 2007, MR2322350.

[Dav73] Martin Davis, Hilbert's tenth problem is unsolvable, Am. Math. Mon. 80 (1973) 233–269.

[DMR76] Martin Davis, Yuri Matiyasevich, Julia Robinson, Hilbert's tenth problem. Diophantine equations: positive aspects of a negative solution, in: Proc. Sympos. Pure Math., in: Amer. Math. Soc., vol. 28, 1976, pp. 323–378.

[Den75] Jan Denef, Hilbert's tenth problem for quadratic rings, Proc. Am. Math. Soc. 48 (1975) 214–220.

[Den80] Jan Denef, Diophantine sets of algebraic integers, II, Trans. Am. Math. Soc. 257 (1) (1980) 227–236.

[DL78] Jan Denef, Leonard Lipshitz, Diophantine sets over some rings of algebraic integers, J. Lond. Math. Soc. 18 (2) (1978) 385–391.

[FK12] Jack Fearnley, Hershy Kisilevsky, Critical values of higher derivatives of twisted elliptic L-functions, Exp. Math. 21 (3) (2012) 213–222, MR2988574.

[FT93] A. Fröhlich, M.J. Taylor, Algebraic Number Theory, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993, MR1215934.

[GFP20] Natalia Garcia-Fritz, Hector Pasten, Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points, Math. Ann. 377 (3–4) (2020) 989–1013, MR4126887.

[Gro61] Alexander Grothendieck, Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes, IHÉS Publ. Math. 8 (1961).

[Har77] Robin Hartshorne, Algebraic Geometry, Springer Verlag, 1977.

[Kat04] Kazuya Kato, p-Adic Hodge theory and values of zeta functions of modular forms, Astérisque (295) (2004) ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III, MR2104361.

[KLS22] Debanjana Kundu, Antonio Lei, Florian Sprung, arXiv:2207.07021, 2022.

[LR08] Álvaro Lozano-Robledo, Ranks of abelian varieties over infinite extensions of the rationals, Manuscr. Math. 126 (3) (2008) 393–407, MR2411235.

[MR10] Barry Mazur, Karl Rubin, Ranks of twists of elliptic curves and Hilbert's Tenth Problem, Invent. Math. 181 (2010) 541–575.

[MR18] Barry Mazur, Karl Rubin, Diophantine stability, Am. J. Math. 140 (3) (2018) 571–616, With an appendix by Michael Larsen, MR3805014.

[MR22] Barry Mazur, Karl Rubin, Arithmetic conjectures suggested by the statistical behavior of modular symbols, Exp. Math. (2022), https://doi.org/10.1080/10586458.2021.1982424, in press.

[MRS07] B. Mazur, K. Rubin, A. Silverberg, Twisting commutative algebraic groups, J. Algebra 314 (1) (2007) 419–438, MR2331769.

[MF19] M. Ram Murty, Brandon Fodden, Hilbert's Tenth Problem: An Introduction to Logic, Number Theory, and Computability, Student Mathematical Library, vol. 88, American Mathematical Society, Providence, RI, 2019, MR3931317.
[MP18] M. Ram Murty, Hector Pasten, Elliptic curves, L-functions, and Hilbert's tenth problem, J. Number Theory 182 (2018) 1–18, MR3703929.
[Pas22a] Hector Pasten, Notes on the DPRM property for listable structures, J. Symb. Log. 87 (1) (2022) 273–312, https://doi.org/10.1017/jsl.2021.97, MR4404628.
[Pas22b] Hector Pasten, Superficies elípticas y el décimo problema de Hilbert, arXiv:2207.10005 [math.NT], 2022.
[Phe88] Thanases Pheidas, Hilbert's tenth problem for a class of rings of algebraic integers, Proc. Am. Math. Soc. 104 (2) (1988) 611–620.
[Poo02] Bjorn Poonen, Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers, in: C. Fieker, D. Kohel (Eds.), Algorithmic Number Theory, Sidney, 2002, in: Lecture Notes in Computer Science, vol. 2369, Springer Verlag, 2002, pp. 33–42.
[Poo] Bjorn Poonen, Elliptic curves whose rank does not grow and Hilbert's Tenth Problem over the rings of integers, Private Communication.
[Rib81] Kenneth Ribet, Torsion points of abelian varieties in cyclotomic extensions, Enseign. Math. 27 (1981) 315–319.
[Rob64] Raphael M. Robinson, The undecidability of pure transcendental extensions of real fields, Z. Math. Log. Grundl. Math. 10 (1964) 275–282, MR0172803 (30 #3021).
[Roh84] David E. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, Invent. Math. 75 (3) (1984) 409–423, MR735333.
[Roh88] David E. Rohrlich, L-functions and division towers, Math. Ann. 281 (4) (1988) 611–632, MR958262.
[Ser72] Jean-Pierre Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331, MR52#8126.
[ST68] Jean-Pierre Serre, John Tate, Good reduction of abelian varieties, Ann. Math. 88 (3) (1968) 492–517, MR0236190.
[Sha74] I.R. Shafarevich, Basic Algebraic Geometry, Die Grundlehren der Math. Wissenschaften, vol. 213, Springer-Verlag, 1974.
[SS89] Harold Shapiro, Alexandra Shlapentokh, Diophantine relations between algebraic number fields, Commun. Pure Appl. Math. XLII (1989) 1113–1122.
[Shi12] Goro Shimura, Modular Forms: Basics and Beyond, Springer Monographs in Mathematics, Springer, New York, 2012, MR3025356.
[Shl06] Alexandra Shlapentokh, Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields, Cambridge University Press, 2006.
[Shl07] Alexandra Shlapentokh, Diophantine definability and decidability in the extensions of degree 2 of totally real fields, J. Algebra 313 (2) (2007) 846–896.
[Shl08] Alexandra Shlapentokh, Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers, Trans. Am. Math. Soc. 360 (7) (2008) 3541–3555, MR2386235.
[Shl09] Alexandra Shlapentokh, Rings of algebraic numbers in infinite extensions of $\mathbb{Q}$ and elliptic curves retaining their rank, Arch. Math. Log. 48 (1) (2009) 77–114, MR2480937.
[Shl18] Alexandra Shlapentokh, First-order decidability and definability of integers in infinite algebraic extensions of the rational numbers, Isr. J. Math. 226 (2) (2018) 579–633, MR3819703.
[Shl89] Alexandra Shlapentokh, Extension of Hilbert's tenth problem to some algebraic number fields, Commun. Pure Appl. Math. XLII (1989) 939–962.
[Shl94] Alexandra Shlapentokh, Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of $\mathbb{Q}$, Ann. Pure Appl. Log. 68 (1994) 299–325.
[Sun21] Zhi-Wei Sun, Further results on Hilbert's Tenth Problem, Sci. China Math. 64 (2) (2021) 281–306, MR4211129.
[Vid89] Carlos Videla, Sobre el décimo problema de Hilbert, in: Atas da Xa Escola de Algebra, Vitoria, ES, Brasil, in: Coleção Atas 16 da Sociedade Brasileira de Matemática 1989, 1989, pp. 95–108.
[Wei82] André Weil, Adeles and Algebraic Groups, Progress in Math., vol. 23, Springer Verlag, 1982.