Diophantine sets of polynomials over algebraic extensions of the rationals

Claudia Degroote* Jeroen Demeyer†

June 20, 2013

Abstract

Let L be a recursive algebraic extension of $\mathbb{Q}$. Assume that, given $\alpha \in L$, we can compute the roots in L of its minimal polynomial over $\mathbb{Q}$ and we can determine which roots are $\mathrm{Aut}(L)$-conjugate to α. We prove there exists a pair of polynomials that characterizes the $\mathrm{Aut}(L)$-conjugates of α, and that these polynomials can be effectively computed. Assume furthermore that L can be embedded in $\mathbb{R}$, or in a finite extension of $\mathbb{Q}_p$ (with p an odd prime). Then we show that subsets of $L[X]^k$ that are recursively enumerable for every recursive presentation of $L[X]$, are diophantine over $L[X]$.

1 Introduction

Let L be a recursive, algebraic extension of $\mathbb{Q}$ that can be embedded in $\mathbb{R}$ or in a finite extension of $\mathbb{Q}_p$ (p an odd prime) and satisfying the extra condition of being "automorphism-recursive", which is defined in section 3. We prove that subsets of $L[X]^k$ that are recursively enumerable for every recursive presentation of the polynomial ring $L[X]$ are diophantine over $L[X]$.

That recursively enumerable sets are diophantine has originally been proved for $\mathbb{Z}$ by Matiyasevich, Davis, Putnam and Robinson in the context of Hilbert's tenth problem (see [2] for an overview of the complete proof). It had as consequence the negative answer to Hilbert's tenth problem: there exists no algorithm that, given a polynomial over $\mathbb{Z}$ in any number of variables, decides whether this polynomial has a solution over $\mathbb{Z}$.

Hilbert's tenth problem can be formulated for other rings than $\mathbb{Z}$, an overview of known results and open problems can be found in [15] and [14]. The stronger result that recursively enumerable sets are diophantine has also been studied for other rings than the integers. First, there is the result of Denef that recursively enumerable sets are diophantine for the polynomial ring $\mathbb{Z}[X]$ (see [8]). The equivalence has also been proved by Zahidi in [18] for $O_K[X_1, \ldots, X_n]$ with O_K the ring of integers in a totally real number field K, and by the second author in [7] for $R[X]$ with R a recursive subring of a number field. In characteristic p, the second author proved in [6] the equivalence for $\mathbb{F}_q[X]$. He also proved for $K[X]$, with K a recursive algebraic extension

*Ph. D. fellow of the Research Foundation — Flanders (FWO). **Address:** Ghent University, Department of Mathematics, Krijgslaan 281, 9000 Gent, Belgium. **E-mail:** cdegroote@cage.ugent.be.

†Postdoctoral Fellow of the Research Foundation — Flanders (FWO). **Address:** Ghent University, Department of Mathematics, Krijgslaan 281, 9000 Gent, Belgium. **E-mail:** jdemeyer@cage.ugent.be.

of a finite field, that sets that are recursively enumerable for every recursive presentation are diophantine. We must consider all recursive presentations because $K[X]$ is not a recursively stable ring: whether a set is r.e. or not depends on the chosen recursive presentation. We have to make the same consideration for the ring $L[X]$, with $L/\mathbb{Q}$ a recursive, algebraic extension.

1.1 Overview

In section 2, we find some kind of refinement of the notion of minimal polynomial for elements of a separable algebraic (finite or infinite) extension L/F. For Galois extensions L/F, the roots of the minimal polynomial of $\alpha \in L$ are precisely the images of α under $\mathrm{Gal}(L/F)$. For separable algebraic extensions which are not necessarily Galois, we use instead a system of two polynomials that allows us to characterize the $\mathrm{Aut}(L/F)$-conjugates of α.

In section 3, we give the definition of an automorphism-recursive field. It is a recursive algebraic extension of $\mathbb{Q}$ such that, given $\alpha \in L$, we can compute the roots in L of the minimal polynomial p_α of α over $\mathbb{Q}$ and such that we can determine which roots are $\mathrm{Aut}(L)$-conjugates.

In section 4, we give an algebraic characterization of the recursively enumerable sets that are recursively enumerable for every recursive presentation. The main statement in that section corresponds to Proposition 6.2 in [5]. In the proof however, we had to make amends for the case that $L/\mathbb{Q}$ is not Galois.

With the preparatory work in sections 3 and 4, we can almost finish the proof (this is done in section 6). However, we will still need a diophantine definition of $\mathbb{Z}[X]$ over $L[X]$. From [7, Theorem 3.1], this follows if we can give a diophantine definition of the predicate "$\deg a \leq \deg b$", with $a, b \in L[X] \setminus \{0\}$. In section 5, we give a diophantine definition of the degree for the case that L is a real field. For fields that can be embedded in a finite extension of $\mathbb{Q}_p$, p odd, this has been done implicitly by Kim and Roush in [10]. We also refer to the reformulation of their statements in section 4 of [7].

In section 6, we finish the proof that recursively enumerable sets in $L[X]$ are diophantine. This is also based on section 6.3, Lemma 6.10 and section 6.6 in [5].

In the rest of this section, we briefly recall the definitions concerning recursively enumerable and diophantine sets.

1.2 Recursively enumerable sets

Definition 1.1. Let k be a natural number. A set $A \subseteq \mathbb{N}^k$ is *recursive* if there exists an algorithm that, on input $a \in \mathbb{N}^k$, decides whether $a \in A$.

Definition 1.2. A set $A \subseteq \mathbb{N}^k$ is *recursively enumerable* (or short r.e.) if there exists an algorithm that prints the elements of A. This algorithm can run infinitely long and can use an unbounded amount of memory. Each element of A is hereby printed at least once, and no elements that are not in A are printed.

To prove that r.e. sets are diophantine for other rings than $\mathbb{Z}$, we have to transfer the notion of recursively enumerable sets to an arbitrary ring R. This will only work if it is possible to effectively compute in R, i.e. if R is a recursive ring. The idea of a recursive ring is that each element $a \in R$ has a code $\sigma(a) \in \mathbb{N}$. Given the codes $\sigma(a)$ and $\sigma(b)$ of $a, b \in R$, a computer has to be able to compute the codes $\sigma(a + b)$ and $\sigma(ab)$.

Definition 1.3. We call R a *recursive ring* if R is a ring with a bijection $\sigma : R \xrightarrow{\sim} \mathbb{N}$ such that the sets

$$R^\sigma_+ = \{(\sigma(a), \sigma(b), \sigma(a+b)) \mid a, b \in R\} \subseteq \mathbb{N}^3$$
$$R^\sigma_\times = \{(\sigma(a), \sigma(b), \sigma(ab)) \mid a, b \in R\} \subseteq \mathbb{N}^3$$

are recursive subsets of $\mathbb{N}^3$. Then σ is called a *recursive presentation* of R.

Examples 1.4.

1. The field $\mathbb{Q}$ of rationals is recursive, as well as any finite extension of $\mathbb{Q}$.
2. The real closure and algebraic closure of $\mathbb{Q}$ are recursive.
3. Let $\mathcal{S} \subseteq \mathbb{N}$ be a subset of the prime numbers and let $L = \mathbb{Q}(\{\sqrt{p} \mid p \in \mathcal{S}\})$. Then L is a recursive field if and only if $\mathcal{S}$ is recursively enumerable.
4. If R is a recursive ring, then the polynomial ring $R[X]$ is recursive ([9, Theorem 3.1]). Moreover, let ι be the natural embedding $R \hookrightarrow R[X]$. Given a recursive presentation $\sigma : R \xrightarrow{\sim} \mathbb{N}$, there exists a recursive presentation $\tau : R[X] \xrightarrow{\sim} \mathbb{N}$ such that $\tau \circ \iota \circ \sigma^{-1}$ is recursive and such that $\iota(R) \subset R[X]$ is a recursive set w.r.t. τ. Intuitively, this means that we can freely mix computations in R and $R[X]$.

Definition 1.5. A recursive ring R is called *recursively stable* if for any two recursive presentations $\sigma : R \xrightarrow{\sim} \mathbb{N}$ and $\tau : R \xrightarrow{\sim} \mathbb{N}$, the set $\{(\sigma(r), \tau(r)) \in \mathbb{N}^2 \mid r \in R\}$ is recursive.

Equivalently, "recursively stable" means that, given any two recursive presentations σ and τ, there exists a recursive permutation $\pi : \mathbb{N} \xrightarrow{\sim} \mathbb{N}$ such that $\tau = \pi \circ \sigma$.

Examples 1.6.

1. The field $\mathbb{Q}$ of rationals is recursively stable, as well as any finite extension of $\mathbb{Q}$.
2. Let $\sigma : R \xrightarrow{\sim} \mathbb{N}$ be a recursive presentation of a ring R and $\varphi \in \mathrm{Aut}(R)$. Then $\sigma \circ \varphi$ is again a recursive presentation (with the same sets R^σ_+ and $R^\sigma_\times$). If R is recursively stable, then $\sigma \circ \varphi \circ \sigma^{-1} : \mathbb{N} \xrightarrow{\sim} \mathbb{N}$ must be recursive. Since there exist only countably many recursive functions, any ring with uncountably many automorphisms (such as $\bar{\mathbb{Q}}$) cannot be recursively stable.
3. If R is recursively stable, then the polynomial ring $R[X]$ is also recursively stable.

Using a recursive presentation, we can now define recursively enumerable subsets of a ring R.

Definition 1.7. Let R be a recursive ring with recursive presentation $\sigma : R \xrightarrow{\sim} \mathbb{N}$. A set $A \subseteq R^k$ is defined to be *recursively enumerable* if the set

$$\{(\sigma(a_1), \ldots, \sigma(a_k)) \in \mathbb{N}^k \mid (a_1, \ldots, a_k) \in A\}$$

is an r.e. subset of $\mathbb{N}^k$.

A priori, this definition may depend on the chosen recursive presentation. However, if R is recursively stable, it does not depend on the recursive presentation. For rings which are not recursively stable, it still makes sense to consider the sets which are r.e. *for every recursive presentation*.

1.3 Diophantine sets

Definition 1.8. Let R be an integral domain. A subset $A \subseteq R^k$ is *diophantine* over R if and only if there exists an $n \in \mathbb{N}$ and a polynomial $f(a_1, \ldots, a_k, x_1, \ldots, x_n)$ with coefficients in R such that

$$A = \{(a_1, \ldots, a_k) \mid \exists x_1, \ldots, x_n \in R \text{ such that } f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0\}.$$

We can write this also as

$$(a_1, \ldots, a_k) \in A \Leftrightarrow (\exists x_1, \ldots, x_n)\ f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0$$

and we call this a diophantine definition of A over R.

A relation δ on R^k is called diophantine over R if the set $\{a \in R^k \mid \delta(a)\}$ is diophantine over R.

2 Refining minimal polynomials

Let F be a field and L a separable algebraic extension of F. In this short section, we first prove a proposition concerning the extension of field embeddings. Next, we show how $\mathrm{Aut}(L/F)$-conjugate elements can be characterized using a couple (f, g) of polynomials just as $\mathrm{Aut}(\bar{F}/F)$-conjugates can be characterized by the minimal polynomial. The authors do not know a reference for these results, although the techniques used are standard in the theory of field extensions.

Definition 2.1. Let K be a field, $\mathrm{Aut}(K)$ its automorphism group. If F is a subfield of K, then $\mathrm{Aut}(K/F)$ denotes those automorphisms of K which fix all elements of F.

We say that two elements $\alpha, \beta \in K$ are $\mathrm{Aut}(K)$-*conjugate*, if there exists a $\varphi \in \mathrm{Aut}(K)$, such that $\varphi(\alpha) = \beta$. We also denote this with $\beta \in \mathrm{Aut}(K)(\alpha)$, meaning that β is in the orbit of α under the action of $\mathrm{Aut}(K)$ on K.

Proposition 2.2. *Let F be a field, L a separable algebraic extension of F. Let M be a field and let $\psi : F \hookrightarrow M$ be an embedding of F in M. Suppose that for each finite extension K of F in L, there exists an embedding $\chi : K \hookrightarrow M$, such that $\chi|_F = \psi$. Then there exists an embedding $\varphi : L \hookrightarrow M$ such that $\varphi|_F = \psi$.*

Proof. This is a variation of [11, Ch. VII, Theorem 2.8]. One needs to apply Zorn's Lemma to the partially ordered set

$$\mathcal{F} = \{(K, \chi) \mid F \subseteq K \subseteq L, \chi : K \hookrightarrow M, \chi|_F = \psi, \chi \text{ extends to all finite extensions of } K \text{ in } L\},$$

with the partial ordering $(K_1, \chi_1) \leq (K_2, \chi_2)$ if $K_1 \subseteq K_2$ and $\chi_2|_{K_1} = \chi_1$.

Theorem 2.3. *Let F be a field, L a separable algebraic extension of F and $\alpha \in L$. There exist polynomials $f(X), g(X) \in F[X]$ with g irreducible such that the system*

$$\begin{cases} f(X) = \beta \\ g(X) = 0 \end{cases} \tag{1}$$

(with a parameter $\beta \in L$) has a solution $X \in L$ if and only if $\beta = \varphi(\alpha)$ for some $\varphi \in \mathrm{Aut}(L/F)$.

Proof. In this proof, we consider F as base field. All fields we mention are extensions of F and all morphisms are the identity on F.

Let $K = F(\alpha)$. This is a finite extension, so K has finitely many F-embeddings $\varphi_1, \ldots, \varphi_n$ into L. For each of these embeddings, we define a finite extension $N_i \subseteq L$ of K: if φ_i extends to an automorphism of L, then $N_i := K$. If it does not extend, it follows from Proposition 2.2 that there exists a finite extension N_i/K such that φ_i does not extend to an embedding of N_i into L. Let N be a finite extension of F inside L containing all N_i.

Now choose any $\gamma \in N$ such that $N = F(\gamma)$. Let $g(X)$ be the minimal polynomial (over F) of γ and let $f(X)$ be such that $\alpha = f(\gamma)$. By construction, (1) has a solution $X = \gamma$ for $\beta = \alpha$. Since the system is $\mathrm{Aut}(L/F)$-invariant, it will have a solution for all $\beta \in \mathrm{Aut}(L/F)(\alpha)$.

Conversely, assume $\xi \in L$ satisfies (1) for a parameter $\beta \in L$. Since γ and ξ have the same minimal polynomial (namely $g(X)$) over F, there is an embedding $\psi : N \hookrightarrow L$ mapping γ to ξ. Let φ be the restriction of ψ to $K = F(\alpha)$. Then

$$\varphi(\alpha) = \varphi(f(\gamma)) = f(\psi(\gamma)) = f(\xi) = \beta.$$

The embedding $\varphi : K \hookrightarrow L$ obviously extends to an embedding ψ of N into L. Because of the construction of N, this implies that φ extends to an automorphism $\tilde{\varphi}$ of L (remark that $\tilde{\varphi}$ does not need to be equal to ψ on N). We conclude that $\tilde{\varphi}(\alpha) = \beta$, where $\tilde{\varphi} \in \mathrm{Aut}(L/F)$.

Remark 2.4. If L/F is a Galois extension, then we can take $f(X) = X$ and g the minimal polynomial of α in Theorem 2.3. In this sense, one can say that the couple (f, g) refines the minimal polynomial because it can be used to characterize the $\mathrm{Aut}(L/F)$-conjugates of elements of L. However, there is no notion of uniqueness or minimality.

3 Automorphism-recursive fields

Let L be a recursive algebraic extension of $\mathbb{Q}$. In this section, we give the definition of an automorphism-recursive field. Such fields have the property that, given $\alpha \in L$, we can compute the set $\mathrm{Aut}(L/F)(\alpha)$, with F a number field. To do this, we will use the polynomials f and g appearing in Theorem 2.3.

Suppose we have a given $\alpha \in L$. For every β in the algebraic closure $\bar{L}$ with the same minimal polynomial as α over $\mathbb{Q}$ (this means α and β are $\mathrm{Aut}(\bar{L})$-conjugates), there are three possible cases:

1. $\beta \in L$ and $\beta = \varphi(\alpha)$ for some $\varphi \in \mathrm{Aut}(L)$;
2. $\beta \in L$ but $\beta \neq \varphi(\alpha)$ for all $\varphi \in \mathrm{Aut}(L)$;
3. $\beta \notin L$.

Let L be an algebraic extension of $\mathbb{Q}$, with recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$.

For $\alpha \in L$, let $p_\alpha \in \mathbb{Q}[X]$ denote the minimal polynomial of α. Given $\sigma(\alpha) \in \mathbb{N}$, we can compute p_α. More precisely, we can compute the codes (under σ) of the coefficients of p_α. To do this, we try all monic irreducible polynomials in $\mathbb{Q}[X]$, until we find an $f(X)$ for which $f(\alpha) = 0$. Checking whether a polynomial over $\mathbb{Q}$ is irreducible can be done algorithmically, see for instance [1, Section 3.5].

Definition 3.1. We call L *automorphism-recursive* if there exists an algorithm with input $\sigma(\alpha) \in \mathbb{N}$, and with output the natural numbers n_1 and n_2, with n_1 the number of roots in L of the minimal polynomial p_α, and n_2 the number of different $\mathrm{Aut}(L)$-conjugates of α.

Saying that L is automorphism-recursive is equivalent to saying that we can count the number of elements β in the three cases mentioned above.

Examples 3.2.

1. Let L be the real closure of $\mathbb{Q}$, then L is automorphism-recursive. Since $\mathrm{Aut}(L/\mathbb{Q}) = 1$, we have $n_2 = 1$. To compute n_1, there exist real-root counting algorithms, for example using Sturm sequences (see [1, Algorithm 4.1.11]).

2. Let L be the p-adic closure of $\mathbb{Q}$ for some prime p, that is the field of elements of $\mathbb{Q}_p$ that are algebraic over $\mathbb{Q}$. Since $\mathrm{Aut}(L/\mathbb{Q}) = 1$ (see [11, Chapter XII, Exercise 3]), we have that $n_2 = 1$. To compute n_1, we can use repeatedly Nerode's algorithm in [12] that decides whether a given polynomial has a zero in $\mathbb{Q}_p$.

3. Let $L/\mathbb{Q}$ be Galois and suppose that L is a recursive field. Then L is automorphism-recursive, because then $n_1 = n_2 = \deg p_\alpha$.

4. If $L/\mathbb{Q}$ is a finite extension, then L is automorphism-recursive because we can simply compute the finitely many automorphisms of L as linear maps of the finite dimensional $\mathbb{Q}$-vector space L.

Recall that Theorem 2.3 with $F = \mathbb{Q}$ stated that there exist polynomials $f(X), g(X) \in \mathbb{Q}[X]$ such that the system $f(X) = \beta, g(X) = 0$ has a solution if and only if $\beta \in \mathrm{Aut}(L)(\alpha)$. These polynomials can be effectively computed.

Proposition 3.3. *Let L be an automorphism-recursive algebraic extension of $\mathbb{Q}$ and fix a recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$. Then we can compute, given $\sigma(\alpha)$ for some $\alpha \in L$, polynomials $f(X), g(X) \in \mathbb{Q}[X]$ satisfying Theorem 2.3 with $F = \mathbb{Q}$.*

Proof. We loop over all triples $(f(X), g(X), \gamma) \in \mathbb{Q}[X] \times \mathbb{Q}[X] \times L$ and look for those such that $f(\gamma) = \alpha$, $g(\gamma) = 0$ and g is irreducible. If we find such a triple, we compute all roots $\xi_1, \ldots, \xi_n$ in L of g. These can be enumerated since we know the number of roots of $g = p_\gamma$ by our hypothesis that L is automorphism-recursive. Let $\beta_i := f(\xi_i)$ and count the number of different β_i's (it is possible that $\beta_i = \beta_j$ even if $\xi_i \neq \xi_j$). Clearly, the $\mathrm{Aut}(L)$-conjugates of α appear amongst the β_i's. If the number of different β_i's equals this number of conjugates (which we know again by hypothesis), we are done and output $(f(X), g(X))$.

This algorithm always finishes because Theorem 2.3 guarantees the existence of such polynomials.

This has as a corollary that we can compute all $\mathrm{Aut}(L/F)$-conjugates of $\alpha \in L$, even using different recursive presentations.

Theorem 3.4. *Let L be an automorphism-recursive algebraic extension of $\mathbb{Q}$. Consider two recursive presentations $\sigma, \tau : L \tilde{\to} \mathbb{N}$. There exists an algorithm which takes as input $\sigma(\alpha)$, $\sigma(\zeta)$ and $\tau(\zeta)$ for some $\alpha, \zeta \in L$ and outputs the set*

$$\{\tau(\beta) \in \mathbb{N} \mid \beta \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))(\alpha)\}.$$

Proof. Let $F := \mathbb{Q}(\zeta)$ and $N := \mathbb{Q}(\zeta, \alpha) \subseteq L$. We first find an $\varepsilon \in N$ such that $N = \mathbb{Q}(\varepsilon)$. This can be done for example by enumerating the triples $(k, z(X), a(X)) \in \mathbb{Q} \times \mathbb{Q}[X] \times \mathbb{Q}[X]$ until $\zeta = z(\zeta + k\alpha)$ and $\alpha = a(\zeta + k\alpha)$ and then letting $\varepsilon = \zeta + k\alpha$. Since $\mathbb{Q}(\zeta, \alpha)$ has only finitely many subfields, [11, Ch. VII, Theorem 6.1] guarantees that this will work. We use the recursive presentation σ for this computation.

Using Proposition 3.3, we compute $f(X), g(X) \in \mathbb{Q}[X]$ for ε. Now, we loop over all $\xi \in L$ (using the recursive presentation τ) to find all zeros of $g(X)$. For each ξ such that $g(\xi) = 0$, compute $\eta = f(\xi)$. Then $\eta = \varphi(\varepsilon)$ for some $\varphi \in \mathrm{Aut}(L)$ and we will find all elements of $\mathrm{Aut}(L)(\varepsilon)$ this way. Since $z(\varepsilon) = \zeta$, it follows that φ is the identity on F if and only $z(\eta) = \zeta$. If indeed $z(\eta) = \zeta$, then $a(\eta) = \varphi(\alpha)$ with $\varphi \in \mathrm{Aut}(L/F)$ and we output $\tau(a(\eta))$.

We can now generalize Proposition 3.3 to the relative situation, over a base number field F.

Theorem 3.5. *Let L be an automorphism-recursive algebraic extension of $\mathbb{Q}$ and fix a recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$. Then we can compute, given $\sigma(\alpha)$ and $\sigma(\zeta)$ for some $\alpha, \zeta \in L$, polynomials $f(X), g(X) \in F[X]$ satisfying Theorem 2.3 with $F = \mathbb{Q}(\zeta)$.*

Proof. Start by applying Theorem 3.4 to compute the set $\mathrm{Aut}(L/F)(\alpha)$. Now loop over all 4-tuples $(f(X), g(X), g_0(X), \gamma) \in F[X] \times F[X] \times \mathbb{Q}[X] \times L$ and look for those such that $f(\gamma) = \alpha$, $g(\gamma) = 0$, $g \mid g_0$ and g is irreducible. If we find such a tuple, we compute all roots $\xi_1, \ldots, \xi_n$ in L of g_0. Consider only those roots ξ_i which are also roots of g. If $f(\xi_i) \in \mathrm{Aut}(L/F)(\alpha)$ for all those roots, then we output $(f(X), g(X))$ and we are done.

The next proposition is a generalization of Theorem 3.4 to the polynomial ring $L[X]$. As mentioned in Examples 1.4, the polynomial ring $L[X]$ is recursive (given that L is recursive). And the recursive presentation of $L[X]$ can be chosen such that we can go back and forth between L and $L[X]$ in a recursive way. We extend the action of $\mathrm{Aut}(L)$ to the elements of $L[X]$ by acting only on the coefficients: we define $\varphi(X) = X$ for $\varphi \in \mathrm{Aut}(L)$.

Theorem 3.6. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$. Suppose $\sigma : L[X] \tilde{\to} \mathbb{N}$ and $\tau : L[X] \tilde{\to} \mathbb{N}$ are recursive presentations of the polynomial ring $L[X]$. There exists an algorithm which takes as input $\sigma(a)$, $\sigma(\zeta)$ and $\tau(\zeta)$ for some $a(X) \in L[X]$ and $\zeta \in L$ and outputs the set*

$$\{\tau(b) \in \mathbb{N} \mid b(X) = \varphi(a(X)) \text{ for some } \varphi \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))\}.$$

Proof. Suppose $a(X) = \alpha_n X^n + \cdots + \alpha_1 X + \alpha_0$ and let $K = \mathbb{Q}(\alpha_0, \ldots, \alpha_n)$ be the number field generated by the coefficients of a. Let $\varepsilon \in L$ such that $K = \mathbb{Q}(\varepsilon)$. This implies that $a(X) \in \mathbb{Q}(\varepsilon)[X]$, so there exists a polynomial $h(X, Y) \in \mathbb{Q}[X, Y]$ such that $a(X) = h(X, \varepsilon)$. We can find such an h and ε simply by enumerating the elements of $\mathbb{Q}[X, Y] \times L$. We use the recursive presentation σ for this, so we actually get $\sigma(\varepsilon)$.

Now $\varphi(a(X)) = h(X, \varphi(\varepsilon))$ for $\varphi \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))$. By Theorem 3.4, given $\sigma(\varepsilon)$, $\sigma(\zeta)$ and $\tau(\zeta)$, we can enumerate all $\tau(\varphi(\varepsilon))$ for $\varphi \in \mathrm{Aut}(L/\mathbb{Q}(\zeta))$. We then output the set of all $\tau(h(X, \varphi(\varepsilon)))$.

4 Recursively enumerable sets

In this section, L is an automorphism-recursive, algebraic extension of $\mathbb{Q}$. We will give an algebraic characterization of the sets $\mathcal{S} \subseteq L$ that are r.e. for every recursive presentation of L. Namely, we will prove in Theorem 4.2 that they are the r.e. sets $\mathcal{S} \subseteq L$ for which there

exists a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant as a set under $\mathrm{Aut}(L/F)$. This theorem is formulated for r.e. subsets of L, but also holds for the polynomial ring $L[X]$. After that, we give an example of a recursive algebraic extension of $\mathbb{Q}$ that is *not* automorphism-recursive. By way of a counterexample, we show that the algebraic characterization in Theorem 4.2 does not need to hold if assumption of the field being automorphism-recursive is not satisfied.

4.1 Algebraic characterization

Lemma 4.1. *Let $L/\mathbb{Q}$ be an algebraic extension. Then there exists a chain $\mathbb{Q} = E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$ of finite extensions $E_i/\mathbb{Q}$, such that $L = \cup_{i\geq 0} E_i$ and such that for every i, $\psi(E_i) = E_i$ for each $\psi \in \mathrm{Aut}(L)$.*

Proof. There exists a bijection $\sigma : L \tilde{\to} \mathbb{N}$. Let $L_0 = \mathbb{Q}$ and $L_i = \mathbb{Q}(\sigma^{-1}(1), \ldots, \sigma^{-1}(i))$ for $i \geq 1$. Then clearly $L_0 \subseteq L_1 \subseteq \ldots$ is an ascending chain of finite extensions $L_i/\mathbb{Q}$ such that $L = \cup_{i\geq 0} L_i$. Now let $\alpha_i \in L$ such that $L_i = \mathbb{Q}(\alpha_i)$, and let $E_i = \mathbb{Q}(\{\varphi(\alpha_i) \mid \varphi \in \mathrm{Aut}(L)\})$. Then $E_0 \subseteq E_1 \subseteq \ldots$ satisfies the thesis of the lemma.

Theorem 4.2. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$. Let $\mathcal{S} \subseteq L$, such that $\mathcal{S}$ is r.e. for some recursive presentation $\sigma : L \tilde{\to} \mathbb{N}$. Then $\mathcal{S}$ is r.e. for every recursive presentation $\tau : L \tilde{\to} \mathbb{N}$ if and only if there exists a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant (as a set) under* $\mathrm{Aut}(L/F)$.

Proof. Suppose there is a finite extension $F/\mathbb{Q}$ such that $\mathcal{S}$ is invariant under $\mathrm{Aut}(L/F)$. After enlarging F with its $\mathrm{Aut}(L)$-conjugates, we may assume without loss of generality that $\psi(F) = F$ for all $\psi \in \mathrm{Aut}(L)$. Let $F = \mathbb{Q}(\zeta)$.

Let σ and τ be given recursive presentations of L. We consider σ, τ and F as part of the input data, so the algorithm will depend on these. This implies we know $\sigma(\zeta)$ and $\tau(\zeta)$.

We give an algorithm which runs over all elements of $\sigma(\mathcal{S})$ and outputs all elements of $\tau(\mathcal{S})$. This goes as follows: for every $a \in \sigma(\mathcal{S})$, let $\alpha = \sigma^{-1}(a) \in L$ and use Theorem 3.4 to output the set $\tau(\mathrm{Aut}(L/F)(\alpha))$. Since $\mathrm{Aut}(L/F)(\alpha) \subseteq \mathcal{S}$, we will eventually output the set $\tau(\mathcal{S})$ this way.

Now suppose that $\mathcal{S}$ is r.e. for every recursive presentation but that for every finite extension $F/\mathbb{Q}$, $\mathcal{S}$ is not invariant under $\mathrm{Aut}(L/F)$. Take such a recursive presentation τ. For every automorphism φ of L, $\tau \circ \varphi$ is also a recursive presentation of L. The idea is that we will construct a set $A \subseteq \mathrm{Aut}(L)$ of cardinality $2^{\aleph_0}$, such that $\varphi(\mathcal{S}) \neq \psi(\mathcal{S})$ for different elements $\varphi \neq \psi$ of A. When τ runs over the $\varphi(S)$ with $\varphi \in A$, we will find uncountably many r.e. sets in $\mathbb{N}$, a contradiction.

From Lemma 4.1, it follows that there exist $E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$, finite extensions $E_i/\mathbb{Q}$, such that $L = \cup_{i\geq 0} E_i$ and such that for every i, $\psi(E_i) = E_i$ for each $\psi \in \mathrm{Aut}(L)$. By assumption, for every i, $\mathrm{Aut}(L/E_i)(\mathcal{S}) \neq \mathcal{S}$. So let $\varphi_i \in \mathrm{Aut}(L/E_i)$, such that $\varphi_i(\mathcal{S}) \neq \mathcal{S}$. From this follows that there exists a finite extension K/E_i, such that $\varphi_i(\mathcal{S} \cap K) \neq \mathcal{S} \cap K$. Since there exists a $j > i$, such that $K \subseteq E_j$, we have that $\varphi_i(\mathcal{S} \cap E_j) \neq \mathcal{S} \cap E_j$. We now delete the intermediate fields $E_{i+1}, \ldots, E_{j-1}$ from our chain. In the resulting chain, E_j from the old chain becomes the new E_{i+1}. Summarizing, we have a chain $E_0 \subseteq E_1 \subseteq E_2 \subseteq \ldots$ of finite extensions $E_i/\mathbb{Q}$, such that $L = \cup_{i\geq 0} E_i$ such that for every i, $\psi(E_i) = E_i$ for each $\psi \in \mathrm{Aut}(L)$, and we have a $\varphi_i \in \mathrm{Aut}(L/E_i)$ such that $\varphi_i(\mathcal{S} \cap E_{i+1}) \neq \mathcal{S} \cap E_{i+1}$.

Now we are ready to define the set $A \subseteq \mathrm{Aut}(L/\mathbb{Q})$. Let I be a subset of $\mathbb{N}$, then we define $\varphi_I \in \mathrm{Aut}(L)$ as the composition of all φ_i with $i \in I$, and the order is such that $\varphi_{\mathbb{N}} = \cdots \circ \varphi_2 \circ \varphi_1 \circ \varphi_0$. So φ_I is an infinite composition, but this is well defined since at each finite level $E_k/\mathbb{Q}$, there are

only finitely many φ_i that act nontrivially, namely those with $i < k$ (by construction of the E_i). We set $A = \{\varphi_I \in \mathrm{Aut}(L) \mid I \subseteq \mathbb{N}\}$.

Now take different subsets I, J of $\mathbb{N}$, we have to prove that $\varphi_I(\mathcal{S}) \neq \varphi_J(\mathcal{S})$. Let i be the minimal natural number in which I and J differ, without loss of generality, we can assume that $i \in I \setminus J$. Consider $\varphi_I \circ \varphi_J^{-1}$, on $\mathcal{S} \cap E_{i+1}$ this works as φ_i. From this follows that $\varphi_I(\mathcal{S} \cap E_{i+1}) \neq \varphi_J(\mathcal{S} \cap E_{i+1})$, so $\varphi_I(\mathcal{S}) \neq \varphi_J(\mathcal{S})$.

This last theorem was stated for the field L, but the same statement also holds for $L[X]$ (recall that $\varphi(X) = X$ for $\varphi \in \mathrm{Aut}(L)$). The proof is essentially the same, instead of Theorem 3.4, we would use Theorem 3.6.

4.2 An example of a non automorphism-recursive field

We construct an algebraic extension $M/\mathbb{Q}$ with recursive presentation $\sigma : M \tilde{\to} \mathbb{N}$, such that M is not automorphism-recursive. We also give a counterexample to Theorem 4.2: we give a subset $C \subset M$ such that $\sigma(C)$ is r.e. and such that C is invariant (as a set) under $\mathrm{Aut}(M/\mathbb{Q})$, but we will give a recursive presentation $\tau : M \tilde{\to} \mathbb{N}$ such that $\tau(C)$ is not r.e.

Let $n \in \mathbb{N} \setminus \{0, 2, 5, 8, 27\}$ and $p_n(X) = X^3 + 3X^2 - nX - 4$. Then p_n is irreducible and the discriminant of p_n is $\Delta(p_n) = n(4n^2 + 9n + 216)$. So if $n > 0$, then $p_n(X)$ has three different real roots $x_n, y_n, z_n \in \mathbb{R}$. Without loss of generality, we may suppose that $x_n < y_n < z_n$. The only rational point on the elliptic curve $y^2 = n(4n^2 + 9n + 216)$ is the point $(0, 0)$, so for all $n \in \mathbb{Q}^*$, $\Delta(p_n)$ is not a square. Therefore $\mathbb{Q}(z_n)/\mathbb{Q}$ is not Galois.

Let $E_n := \mathbb{Q}(x_n, y_n, z_n)$ for $n \in \mathbb{N} \setminus \{0, 2, 5, 8, 27\}$. One can prove that there exist $q_n, r_n \in \mathbb{Q}$ satisfying $x_n < q_n < y_n < r_n < z_n$ such that $z_n - r_n$ is not a square in $E_n = \mathbb{Q}(x_n, y_n, z_n)$ and $y_n - q_n$ is not a square in $E_n(\sqrt{z_n - r_n})$. Let

$$L_n := \mathbb{Q}(x_n, y_n, z_n, \sqrt{z_n - r_n}, \sqrt{y_n - q_n}).$$

One can also show that there exists a recursive set $A \subset \mathbb{N}$ and a recursive bijection $\mathbb{N} \to A : k \mapsto a_k$ such that $L_{a_1} \dots L_{a_{k-1}}$ and L_{a_k} are linearly disjoint over $\mathbb{Q}$ for all $k > 1$. For more details of the proofs, we refer to Section 6.4 in the Ph.D. thesis of the first author [3].

Now let $S \subseteq A$ be a subset that is recursively enumerable but not recursive.

We construct the field extension $M/\mathbb{Q}$ as the compositum of $\mathbb{Q}(z_n)$ if $n \in A \setminus S$, and L_n if $n \in S$.

Proposition 4.3. *The field M is recursive.*

Proof. We give an algorithm that constructs M as a chain of fields $M_1 := \mathbb{Q} \subset M_2 \subset M_3 \subset \dots$ such that $M = \cup_i M_i$. Let a background algorithm $\mathcal{A}$ run, that prints the elements of S. Now we describe our algorithm step by step. In step 1, we let $M_1 = \mathbb{Q}$. In step $2n$, we let $M_{2n} := M_{2n-1}\mathbb{Q}(z_n)$ for $n \in A$, and $M_{2n} := M_{2n-1}$ if $n \in \mathbb{N} \setminus A$. We keep a list of the $\mathbb{Q}(z_n)$ that we add. In step $2n + 1$ of our algorithm, if $k \in S$ is printed in step n of algorithm $\mathcal{A}$, we let $M_{2n+1} := M_{2n}L_k$. Otherwise, set $M_{2n+1} := M_{2n}$. From [9, Theorem 6.12] follows that this gives a recursive presentation $\sigma : M \tilde{\to} \mathbb{N}$. □

Proposition 4.4. *For all $\varphi \in \mathrm{Aut}(M)$ and $n \in A$, we have $\varphi(z_n) = z_n$.*

Proof. Let $\varphi \in \mathrm{Aut}(M)$ and $n \in A$. If $n \notin S$, then z_n is the only root in M of its minimal polynomial, so the assertion is true.

Now assume that $n \in S$ such that $\{x_n, y_n, z_n\} \subseteq M$. Suppose that $\varphi(z_n) = y_n$. Then $\varphi(\sqrt{z_n - r_n}) \in M$ is a root of $X^2 - (y_n - r_n)$. Since M is a subfield of $\mathbb{R}$ and $y_n - r_n < 0$, this is a contradiction. Analogously, $\varphi(z_n) \neq x_n$ and $\varphi(y_n) \neq x_n$. It follows that $\varphi(x_n) = x_n$, $\varphi(y_n) = y_n$ and $\varphi(z_n) = z_n$. □

From this Proposition 4.4 follows that if $n \in S$, the two $\mathrm{Aut}(\bar{\mathbb{Q}})$-conjugates of z_n are in M, but they are not $\mathrm{Aut}(M)$-conjugate to z_n. So for z_n, the number of $\mathrm{Aut}(M)$-conjugates is always 1, but the number of roots of its minimal polynomial p_n in M is 3 if and only if $n \in S$. So if M would be automorphism-recursive, then we would have an algorithm that gives the number of roots of p_n in M for every $n \in A$, so that decides whether $n \in S$. Therefore, M is not automorphism-recursive.

In the same way, we construct the field extension $M'/\mathbb{Q}$ as the compositum of $\mathbb{Q}(y_n)$ if $n \in A \setminus S$, and L_n if $n \in S$. Similarly as in Proposition 4.3, one can prove that this is also a recursive field, let $\tau : M' \tilde{\to} \mathbb{N}$ be a recursive presentation. We define an isomorphism $\psi : M \to M'$, by letting $\psi(z_n) = y_n$ if $n \in A \setminus S$, and $\psi(z_n) = z_n$ if $n \in S$. If $L_n \subset M$, then we let $\psi|_{L_n} = id|_{L_n}$.

Now consider the subset $C = \{z_n \mid n \in A\}$ in M. It is clear that $\sigma(C)$ is r.e. Furthermore, by Proposition 4.4, C is invariant under $\mathrm{Aut}(M)$. We have that $\psi(C) = \{y_n \mid n \in A \setminus S\} \cup \{z_n \mid n \in S\}$. Now suppose that $\tau(\psi(C))$ is also r.e. Since we also have that the subset $\mathcal{D} = \{y_n \mid n \in A\}$ is r.e. for the recursive presentation τ, $\mathcal{D} \cap \psi(C) = \{y_n \mid n \in A \setminus S\}$ is r.e. for τ. This is a contradiction since S is not recursive. So C is invariant under $\mathrm{Aut}(M)$ and r.e. for σ, but not r.e. for the presentation $\tau \circ \psi : M \tilde{\to} \mathbb{N}$.

5 Diophantine definition of degree

As before, L is an algebraic extension of $\mathbb{Q}$, and $L[X]$ the polynomial ring in one variable over L. In this section, we give a diophantine definition of the predicate "$\deg a(X) \leq \deg b(X)$" with $a(X), b(X) \in L[X]$, $a \neq 0$ and $b \neq 0$, for two classes of fields L. We handle the case that L is a real field and the case that L can be embedded in a finite extension of $\mathbb{Q}_p$, with p an odd prime.

5.1 For real fields

We repeat some definitions concerning real fields.

Definition 5.1. A field K is called a *(formally) real field* if -1 is not a sum of squares in K.

A field K is real if and only if K is an ordered field, this means there exists a subset P (the positive elements) of K such that if $\alpha, \beta \in P$ then $\alpha + \beta \in P$ and $\alpha\beta \in P$, $P \cap (-P) = \{0\}$ and $P \cup (-P) = K$. A real field can have more than one ordering P.

In this section, L is a real, algebraic extension of $\mathbb{Q}$. The orderings P on L correspond exactly to the embeddings $\varphi : L \hookrightarrow \mathbb{R}$.

Definition 5.2. A rational function $a(X) \in L(X)$ is called *positive-definite* on L if $\varphi(a(\xi)) \geq 0$ for all $\xi \in L$ on which a is defined, and for all embeddings $\varphi : L \hookrightarrow \mathbb{R}$. We denote this with $a \geq 0$, the notation $a \geq b$ is equivalent with $a - b \geq 0$.

Proposition 5.3. *The set of positive-definite polynomials in $L[X]$ is diophantine.*

Proof. Let $a(X) \in L[X]$ be a positive-definite polynomial. We claim that $a(X)$ is a sum of squares in the function field $L(X)$. Suppose this is not the case. By the Artin-Schreier theorem (see for instance [13, Ch. 6, Corollary 1.8]), there exists at least one ordering $\leq$ on $L(X)$ for which $a(X) < 0$. Let $\tilde{R}$ be the real closure of $L(X), \leq$ and let R be the relative algebraic closure of L inside $\tilde{R}$. The property of being real closed can be defined by certain polynomials having roots, therefore R is also real closed.

It follows that $\tilde{R}$ is an elementary extension (as models of real closed fields) of R. This means that the formula $(\exists x)(a(x) < 0)$, which is true in $\tilde{R}$ since $X \in L(X)$ satisfies, is also true in R.

Now L is an algebraic extension of $\mathbb{Q}$, which is dense in all its real closures (these are algebraic extensions of L which can be embedded in $\mathbb{R}$). Because of this, there must also exist a $y \in L$ such that $a(y) < 0$. This contradicts the fact that $a(X)$ is positive definite.

So we know that $a(X)$ is a sum of squares in $L(X)$. Let F be the number field generated by the coefficients of $a(X)$. From a theorem of Pourchet (see [16]) follows that $a(X)$ is a sum of at most 5 squares in $F(X)$. So we have

$$a(X) \in L[X] \text{ is positive-definite} \Leftrightarrow (\exists a_1, \ldots, a_5, b \in L[X])(b \neq 0 \wedge b^2 a = a_1^2 + \cdots + a_5^2),$$

where b is used to cancel the common denominator.

Theorem 5.4. *Let $a(X), b(X) \in L[X]$, $a \neq 0$ and $b \neq 0$. Then*

$$\deg a(X) \leq \deg b(X) \Leftrightarrow (\exists \rho, \pi \in L)\ a^2 \leq \rho + \pi b^2.$$

Proof. Let $\deg a(X) = n, \deg b(X) = m$, $a(X) = \alpha_n X^n + \cdots + \alpha_0$ and $b(X) = \beta_m X^m + \cdots + \beta_0$. Let F be a number field containing all the coefficients α_i and β_i.

Suppose first that $n \leq m$. Then we need to prove that $\varphi(a(\xi)^2) \leq \varphi(\rho + \pi b(\xi)^2)$ for every $\xi \in L$ and every embedding $\varphi : L \hookrightarrow \mathbb{R}$. If $n = m$, we choose $\pi \in \mathbb{Q}$ such that $\varphi(\alpha_n^2) < \pi\varphi(\beta_n^2)$ for every real embedding φ. This is possible, since there are only finitely many embeddings of F in $\mathbb{R}$. If $n < m$, we set $\pi = 1$. In both cases, the polynomial $\varphi(a^2 - \pi b^2)$ has even degree with a negative leading term. Therefore, $\varphi(a^2 - \pi b^2)$ reaches a maximum $m_\varphi \in \mathbb{R}$. We now take $\rho \in \mathbb{Q}$ such that $\rho \geq m_\varphi$ for every embedding $\varphi : F \hookrightarrow \mathbb{R}$. As before, this is possible since there are only finitely many such embeddings. It follows that $\varphi(a^2 - \pi b^2) \leq \rho$.

For the converse, we choose one particular real embedding of L. Suppose that there exist $\rho, \pi \in L$ such that $\varphi(a^2) \leq \varphi(\rho + \pi b^2)$. Since the left hand side is a positive definite polynomial of degree $2n$, dominated by a polynomial of degree at most $2m$, it follows that $n \leq m$.

5.2 For subfields of p-adic fields

Now let L be an algebraic extension of $\mathbb{Q}$ that can be embedded in a finite extension of $\mathbb{Q}_p$, with p an odd prime. Let $a(X), b(X) \in L[X]$, $a \neq 0$ and $b \neq 0$. Then $\deg a \leq \deg b$ is equivalent with $v_\infty(a/b) \geq 0$ (with v_∞ the degree valuation on $L(X)$). We refer to section 4 of [7], where the second author proves that "$v_\infty \geq 0$" is diophantine for polynomials over a number field. The proof follows the method of Kim and Roush, namely by giving a diophantine definition of the valuation ring of v_∞ in $L(X)$, with L a field that can be embedded in a finite extension of $\mathbb{Q}_p$, with p an odd prime. Theorem 4.8 in section 4 of [7] is proved only for a subring of a number field. One can easily see that the proof of this theorem still holds for $L/\mathbb{Q}$ an algebraic, not necessarily finite, extension.

In [4], we gave a diophantine definition of the valuation ring in $K(X)$, K a finite extension of $\mathbb{Q}_p$, with p an odd prime or $p = 2$. This followed some of the ideas in Kim and Roush's article [10], but we gave a unified proof for both $p = 2$ and p odd. In the Ph.D. thesis of the first author [3], we also extended the diophantine definition of the valuation ring to rational function fields over an algebraic subfield of a possibly dyadic p-adic field. So the predicate "$\deg a \leq \deg b$" for $a, b \in L[X] \setminus \{0\}$ is also diophantine for L an algebraic extension of $\mathbb{Q}$ that can be embedded in a finite extension of $\mathbb{Q}_2$. Since this is at the moment not published, from here on we exclude the case $p = 2$.

6 Recursively enumerable sets are diophantine

As before, L is an algebraic extension of $\mathbb{Q}$, and $L[X]$ the polynomial ring in one variable over L.

Lemma 6.1. *Let F be a number field and L an algebraic field extension of F. Suppose that $\mathbb{Z}[X]$ is diophantine over $L[X]$. Then $F[X]$ is diophantine over $L[X]$.*

Proof. Let $\alpha \in L$ such that $F = \mathbb{Q}[\alpha]$, and suppose $d = [F : \mathbb{Q}]$. Then $a(X) \in F[X]$ if and only if there exist $b \in \mathbb{Z} \setminus \{0\}$ and $a_0(X), \ldots, a_{d-1}(X) \in \mathbb{Z}[X]$ such that

$$ba(X) = a_0(X) + a_1(X)\alpha + \cdots + a_{d-1}(X)\alpha^{d-1}.$$

Since $\mathbb{Z} \setminus \{0\}$ is diophantine in $\mathbb{Z}[X]$ (it is r.e.), and $\mathbb{Z}[X]$ is by assumption diophantine over $L[X]$, it follows that $F[X]$ is diophantine over $L[X]$.

Definition 6.2. A *bounding predicate* for $L[X]$ is a relation $\delta(a, n)$ with $a(X) \in L[X]$ and $n \in \mathbb{N}$ such that:

1. For a fixed $n \in \mathbb{N}$, there are only finitely many $a \in L[X]$ that satisfy $\delta(a, n)$.
2. If $\mathcal{B}$ is a finite subset of $L[X]$, then there exists an $n \in \mathbb{N}$ such that $\delta(b, n)$ holds for every $b \in \mathcal{B}$.

We call a bounding predicate *effective* if the following also holds:

3. There exists an algorithm, with input $n \in \mathbb{N}$, that produces a finite set $\mathcal{B}_n \subset \bar{L}[X]$, such that $\mathcal{B}_n \cap L[X]$ is exactly the set of the $b \in L[X]$ that satisfy $\delta(b, n)$.

To make sense of this last condition, we use the known fact that $\bar{L}$ is a recursive field with a recursive embedding of L into $\bar{L}$, see [17, Theorem 7]. More precisely, if ι denotes the embedding $L \hookrightarrow \bar{L}$ and σ is a recursive presentation of L, then there exists a recursive presentation $\tau : \bar{L} \tilde{\to} \mathbb{N}$ such that $\tau \circ \iota \circ \sigma^{-1} : \mathbb{N} \to \mathbb{N}$ is a recursive function. However, in general, the image $\iota(L)$ (as a subset of $\bar{L}$) is not recursive. In other words, given an element of $\bar{L}$, we cannot decide whether it belongs to L.

We now give a diophantine effective bounding predicate for $L[X]$.

Lemma 6.3. *Let L be an algebraic extension of $\mathbb{Q}$, and suppose that $\mathbb{Z}[X]$ is diophantine over $L[X]$. Let $\sigma : \mathbb{Z}[X] \tilde{\to} \mathbb{N}$ be a recursive presentation, and let $p_n(X) = \sigma^{-1}(n)$ if $\sigma^{-1}(n)$ is non-zero and $p_{\sigma(0)}(X) = 1$. Then "$a(X)X + 1 \mid p_n(X)$" is an effective bounding predicate for $L[X]$, which is diophantine over $L[X]$.*

Proof. Fix $n \in \mathbb{N}$ and consider $p_n(X)$, which is a non-zero polynomial. As a polynomial in $L[X]$, this has only finitely many divisors, up to units. If we force the constant coefficient of such a divisor to be 1, there are only finitely many possibilities, so only finitely many values for $a(X)$.

Given finitely many polynomials $a_1(X), \ldots, a_m(X) \in L[X]$, we define $q(X) = \prod_i (a_i(X)X + 1)$. If K denotes the field over which q is defined, we let $r(X) = \mathrm{N}_{K/\mathbb{Q}}(q(X))$, which is an element of $\mathbb{Q}[X]$. Finally, we multiply $r(X)$ with a non-zero integer to clear all denominators to get a non-zero polynomial $s(X) = d \cdot r(X) \in \mathbb{Z}[X]$. Let $n = \sigma(s)$. We conclude that $a_i(X)X + 1 \mid q(X) \mid r(X) \mid s(X) = p_n(X)$ for all i.

The bounding predicate is effective because we can easily factor $p_n(X)$ in $\bar{L}[X]$ (search for all the zeros by trying every element of $\bar{L}$). Then we can compute all divisors of $p_n(X)$ and normalize them such that the constant coefficient becomes 1, skipping those divisors with constant coefficient 0. For each divisor $a(X)X + 1$, we output $a(X)$.

Finally, we show that it is diophantine. Consider the set $\mathcal{S} = \{(p_n(X), n) \in \mathbb{Z}[X] \times \mathbb{N}\}$ as subset of $\mathbb{Z}[X] \times \mathbb{Z}[X]$. By definition, this set is r.e. if and only if $\{(\sigma(p_n(X)), \sigma(n)) \in \mathbb{N} \times \mathbb{N}\}$ is r.e. If we ignore $n = \sigma(0)$ and $n = \sigma(1)$ for simplicity, this set is equal to $\{(n, \sigma(n)) \in \mathbb{N} \times \mathbb{N}\}$. Since we can easily compute $\sigma(n)$ for any n (it suffices to know $\sigma(1)$), it follows that $\mathcal{S}$ is a recursively enumerable (even recursive) subset of $\mathbb{Z}[X] \times \mathbb{Z}[X]$. By [8], this is also a diophantine subset of $\mathbb{Z}[X] \times \mathbb{Z}[X]$. Using the assumption that $\mathbb{Z}[X]$ is diophantine over $L[X]$ gives us that $\mathcal{S}$ is diophantine over $L[X]$. Since divisibility is obviously diophantine, this shows that the predicate $\delta(a, n)$: $a(X)X + 1 \mid p_n(X)$ is diophantine.

We will now finish the proof of the main theorem.

Theorem 6.4. *Let L be an automorphism-recursive, algebraic extension of $\mathbb{Q}$ and assume either that L is real, or that L can be embedded in a finite extension of $\mathbb{Q}_p$ with p odd. Let $\mathcal{S} \subseteq L[X]$ be r.e. for every recursive presentation of $L[X]$. Then $\mathcal{S}$ is diophantine over $L[X]$.*

Proof. Using the hypotheses on the field L, we proved in Section 5 that "$\deg a(X) \leq \deg b(X)$" is diophantine, so from [7, Theorem 3.1] follows that $\mathbb{Z}[X]$ is diophantine over $L[X]$. Since $\mathcal{S}$ is r.e. for every recursive presentation of $L[X]$, Theorem 4.2 shows that $\mathrm{Aut}(L/F)(\mathcal{S}) = \mathcal{S}$ for some finite extension F of $\mathbb{Q}$ in L.

We give an algorithm that codes the elements of $\mathcal{S}$ into a triple $(n, \omega, \alpha) \in \mathbb{N} \times F \times L$. We call the set of these triples $\mathcal{R}_1$. Given $a(X) \in \mathcal{S}$, we let n be the smallest natural number for which $\delta(a, n)$ holds, with δ the bounding predicate from Lemma 6.3. Since δ is effective, we can find n algorithmically by computing $\mathcal{B}_n \subseteq \bar{L}[X]$ for increasing values of n until $a(X) \in \mathcal{B}_n$.

Next, let $d(X) = \prod_{b \in \mathcal{B}_n \setminus \{a\}} (a(X) - b(X))$, which is an element of $\bar{L}[X]$. Since d is not the zero polynomial, there exists an $\omega \in \mathbb{Q}$ such that $a(\omega) \neq b(\omega)$ for all $b \in \mathcal{B}_n \setminus \{a\}$. We know that ω exists, so we can try every $\omega \in \mathbb{Q}$ until we find one that works, and we let $\alpha = a(\omega)$.

Now we do a second encoding of the elements of $\mathcal{R}_1$ into a quadruple $(n, \omega, f(X), g(X)) \in \mathbb{N} \times F \times F[X] \times F[X]$. Given $(n, \omega, \alpha) \in \mathcal{R}_1$, we find $f(X), g(X) \in F[X]$ (see Theorem 3.5) such that the system

$$\begin{cases} f(X) = \alpha \\ g(X) = 0 \end{cases}$$

has a zero in L, but for every $\beta \in L$ with $\beta \notin \mathrm{Aut}(L/F)(\alpha)$ the system

$$\begin{cases} f(X) = \beta \\ g(X) = 0 \end{cases}$$

does not have a zero in L. The set of these quadruples $(n, \omega, f(X), g(X))$ will be called $\mathcal{R}$.

Since both these encodings are recursive procedures, the sets $\mathcal{R}_1$ and $\mathcal{R}$ are r.e. For the ring $F[X]$, we know that r.e. sets are diophantine (see [7, Theorem 5.1]). So $\mathcal{R}$ is diophantine over $F[X]$. Since $F[X]$ is diophantine in $L[X]$ (Lemma 6.1), $\mathcal{R}$ is diophantine over $L[X]$.

Now the final step is to give a diophantine definition of $\mathcal{S}$, given that $\mathcal{R}$ is diophantine. For this, we need to undo the two encodings using diophantine formulas.

We claim that:

$$a \in \mathcal{S} \tag{2}$$

$$\Updownarrow$$

$$(\exists\, n \in \mathbb{N})(\exists\, \omega \in F)(\exists\, f(X), g(X) \in F[X])(\exists\, \alpha, \gamma \in L)$$

$$(n, \omega, f(X), g(X)) \in \mathcal{R} \tag{3}$$

$$\wedge\ f(\gamma) = \alpha\ \wedge\ g(\gamma) = 0 \tag{4}$$

$$\wedge\ \delta(a, n) \wedge a(\omega) = \alpha. \tag{5}$$

First we prove that the definition is indeed diophantine. We have that L is diophantine in $L[X]$, since the constants in $L[X]$ are the invertible elements and 0. As shown above, the set $\mathcal{R}$ is diophantine over $L[X]$. From Lemma 6.1, it follows that $F[X]$ is diophantine over $L[X]$, and therefore F is also diophantine over $L[X]$.

If $a \in \mathcal{S}$, we take the corresponding $(n, \omega, \alpha) \in \mathcal{R}_1$ and $(n, \omega, f(X), g(X)) \in \mathcal{R}$. Then (3) is true and (4) and (5) follow from the construction of $\mathcal{R}_1$ and $\mathcal{R}$.

Conversely, assume (3), (4) and (5). Consider $(n, \omega, f(X), g(X)) \in \mathcal{R}$, this must come from some $(n, \omega, \beta) \in \mathcal{R}_1$, which in turn comes from some $b \in \mathcal{S}$. Since the system $f(X) = \alpha$ and $g(X) = 0$ has a solution $\gamma \in L$, we must have $\alpha = \varphi(\beta)$ for some $\varphi \in \mathrm{Aut}(L/F)$.

The construction of $\mathcal{R}_1$ implies that $\delta(b, n)$ holds, that $b(\omega) = \beta$ and that $b(\omega) \neq q(\omega)$ for all $q \neq b$ for which $\delta(q, n)$ holds. Applying φ^{-1} on (5) and considering $\omega \in F$, we get $\varphi^{-1}(a)(\omega) = \beta$. Since $\delta(a, n)$ holds and δ is invariant under $\mathrm{Aut}(L/\mathbb{Q})$, also $\delta(\varphi^{-1}(a), n)$ holds.

All this implies that $b = \varphi^{-1}(a)$. Since $\mathrm{Aut}(L/F)(\mathcal{S}) = \mathcal{S}$ and $b \in \mathcal{S}$, we conclude that $a \in \mathcal{S}$.

References

[1] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, 1993.

[2] Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly **80** (1973), no. 3, 233–269.

[3] Claudia Degroote, *Undecidability problems and diophantine sets over polynomial rings and function fields*, Ph.D. thesis, Ghent University, 2013.

[4] Claudia Degroote and Jeroen Demeyer, *Hilbert's tenth problem for rational function fields over p-adic fields*, J. Algebra **361** (2012), 172–187.

[5] Jeroen Demeyer, *Diophantine sets over polynomial rings and Hilbert's tenth problem for function fields*, Ph.D. thesis, Ghent University, 2007.

[6] ———, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Invent. Math. **170** (2007), no. 3, 655–670.

[7] ———, *Diophantine sets of polynomials over number fields*, Proc. Amer. Math. Soc. **138** (2010), no. 8, 2715–2728.

[8] Jan Denef, *Diophantine sets over* $\mathbb{Z}[T]$, Proc. Amer. Math. Soc. **69** (1978), no. 1, 148–150.

[9] Albrecht Fröhlich and John C. Shepherdson, *Effective procedures in field theory*, Phil. Trans. Roy. Soc. London **248** (1956), 407–432.

[10] Ki Hang Kim and Fred Roush, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), no. 1, 83–110.

[11] Serge Lang, *Algebra*, Advanced Book Program (Second ed.), Addison-Wesley Publishing Company, Reading, Massachusetts, 1984.

[12] Anil Nerode, *A decision method for p-adic integral zeros of diophantine equations*, Bull. Amer. Math. Soc. **69** (1963), 513–517.

[13] Albrecht Pfister, *Quadratic forms with applications to Algebraic Geometry and Topology*, London Mathematical Society Lecture Note Series, vol. 127, Cambridge University Press, 1995.

[14] Thanases Pheidas and Karim Zahidi, *Undecidability of existential theories of rings and fields: a survey*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (Denef et al., eds.), Contemp. Math., vol. 270, 2000, pp. 49–105.

[15] Bjorn Poonen, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350.

[16] Yves Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.

[17] Michael Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

[18] Karim Zahidi, *Existential undecidability for rings of algebraic functions*, Ph.D. thesis, Ghent University, 1999.