Faculteit Wetenschappen
Vakgroep Zuivere Wiskunde en Computeralgebra
28 Maart 2007

Diophantine Sets over Polynomial Rings and Hilbert's Tenth Problem for Function Fields

Jeroen Demeyer

Promotoren: Jan Van Geel
Karim Zahidi

Proefschrift voorgelegd aan de Faculteit Wetenschappen tot het behalen van de graad van Doctor in de Wetenschappen richting Wiskunde.

2

Contents

Thanks

The person who deserves the most thanks is Jan Van Geel. During these four years, he has always been there to help me. I was sometimes surprised how he always managed to make time for me just when I needed it the most. He also made sure I made some international contacts, such as Thanases Pheidas and Bjorn Poonen.

Also thanks to Karim Zahidi. As he was traveling all around, I saw him less, but he gave me some good suggestions, particularly on the logic side of my thesis.

I certainly have to thank Thanases Pheidas, one of the specialists in Hilbert's Tenth Problem. Besides discussing mathematics, Thanases also showed me Crete and the Greek way of living. During my first of three stays with him, he suggested me to have a look at Davis' survey article [Dav73] about the equivalence of recursively enumerable and diophantine sets for the integers. While reading that, I started thinking about $\mathbb{F}_q[Z]$. Thanases actually discouraged me to work on that (too many people had tried before, without results), but luckily I did not listen to him.

Thanks to Kirsten Eisenträger for her comments on this thesis, especially some important points concerning Chapter 4.

I would also like to thank my parents for giving me the opportunity to study and do research in mathematics. They always encouraged me, even though they probably do not understand much of what I'm doing.

Almost one year ago at a summer school on abelian varieties in Utrecht I had the pleasure to get to know Antonella Perucca, who showed me that life is more than mathematics and computers. Thanks a lot for checking my thesis, for making sure I kept my deadlines and for comforting me when necessary. And happy birthday!

Finally, all of this thesis was written using free/open-source software. Thanks to all volunteers who developed the GNU tools, Linux, Gentoo, LaTeX, GIMP, PARI/GP, Perl and Vim. All these programs were used for this thesis or the invitation.

Jeroen Demeyer 28 March 2007

Part I

Preliminaries

Chapter 1

Introduction

1.1 Hilbert's Tenth Problem and related problems

In 1900, David Hilbert gave a list of 23 mathematical problems. He presented some of these problems at the International Congress of Mathematicians, which was held in Paris in August 1900. These problems were meant to influence the mathematics of the twentieth century, and Hilbert certainly achieved this goal. In his paper [Hil01], Hilbert defines the 10th problem as follows:

> "*Eine diophantische Gleichung mit irgend welchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen Zahlen lösbar ist.*"

> Let a diophantine equation with any number of variables and with rational integer coefficients be given: one should present a procedure after which, by means of a finite number of operations, it can be decided whether the equation is solvable in whole numbers.

Hilbert talks about a finite procedure, but today we would call that an algorithm. However, a formal definition of the term "algorithm" was only given in the 1930s (see Section 3.1). Of course, Hilbert's "Verfahren" captures the intuition of an algorithm.

So, Hilbert's Tenth Problem is the problem to find an algorithm to decide whether or not a diophantine equation has a solution in integers. By a "diophantine equation" he means a polynomial equation with coefficients in $\mathbb{Z}$. "Deciding" means that the algorithm should have one input for the equation (in some suitable encoding), and one output, which is `YES` if the equation has a solution, or `NO` if it does not. For every input, the algorithm must give the correct answer in a finite amount of time, but that time can be arbitrarily long.

Hilbert's Tenth Problem has a negative answer, in the sense that there does not exist an algorithm to decide whether or not a diophantine equation has a solution in $\mathbb{Z}$. This was proven in 1970 by Yuri Matiyasevich (see [Mat70]), building on earlier work by Martin Davis, Hilary Putnam and Julia Robinson.

Actually, the undecidability of diophantine equations was a consequence of the following positive result, which is much stronger:

Theorem (DPRM, 1970)**.** *For all $k \geq 1$, a subset of $\mathbb{Z}^k$ is recursively enumerable if and only if it is diophantine over $\mathbb{Z}$.*

We refer to this theorem as "DPRM" after Davis, Putnam, Robinson and Matiyasevich. The proof was developed in several different papers. We refer to [Dav73], where Davis gives a full proof of DPRM without requiring prior knowledge. In a historical appendix, he gives references to the original papers.

One can pose the same questions, not just for $\mathbb{Z}$, but for any ring or field. Then Hilbert's Tenth Problem (HTP) for a ring $\mathcal{R}$ is the problem to find an algorithm which can decide whether polynomial equations with coefficients in $\mathcal{R}$ have solutions in $\mathcal{R}$. Actually, we will often take coefficients not in $\mathcal{R}$, but in a smaller ring. This is certainly necessary if the ring $\mathcal{R}$ is uncountable, because we cannot input elements of an uncountable ring in a Turing machine. Usually, we will take the coefficients from a finitely generated $\mathbb{Z}$-algebra. For example, for HTP over $\mathbb{R}$ one usually considers diophantine equations with coefficients in $\mathbb{Q}$ (equivalently, in $\mathbb{Z}$). In this case, the problem is decidable (see [Tar51]). In Part II of this thesis, we will prove the negative answer to HTP for certain function fields of curves over valued field with residue characteristic zero.

If the ring $\mathcal{R}$ is countable, one can also try to generalize the second result, the equivalence of recursively enumerable and diophantine sets. This is a much harder problem, and there are only a few rings where the answer is known to be positive. If we can prove this equivalence for a ring $\mathcal{R}$, we automatically have a negative answer to HTP for $\mathcal{R}$. In Part III, we will generalize DPRM to polynomial

rings over algebraic extensions of a finite field and rings of integers in totally real algebraic extensions of $\mathbb{Q}$.

We give two references to introductory texts: the first one, *Undecidability of Existential Theories of Rings and Fields: a Survey* by Pheidas and Zahidi ([PhZ00]) gives some history about the problem and also a very good idea of the rings and fields for which HTP is decidable, undecidable or still an open question. It also indicates some connections with logic and has a very extensive bibliography. The second text, *Hilbert's Tenth Problem over Rings of Number-Theoretic Interest* by Poonen ([Poo03]) is shorter and perhaps better suited as a first introduction to HTP. It goes into much less detail but concentrates more on the number theory.

1.2 Thesis overview

1.2.1 Part I: Preliminaries

The first part of the thesis establishes the definitions and basic properties of diophantine sets and of recursively enumerable sets. All the propositions are either well known, or easy exercises. However, for completeness, we will often give proofs anyway.

In Chapter 2, we discuss diophantine sets, together with some important examples. We briefly discuss languages. Then we define diophantine interpretations, with diophantine models as a special case.

The first section of Chapter 3 is about algorithms. In Section 3.2, this is used to define recursively enumerable (r.e.) and recursive sets over the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$. In Section 3.3, we introduce recursive presentations which allow us to transfer the definitions of r.e. and recursive sets to other rings. A ring can have many recursive presentations, so which sets are r.e. and recursive may depend on the recursive presentation. However, for a certain class of rings, called recursively stable rings, all recursive presentations yield the same r.e. and recursive sets. In Section 3.4, we discuss generalizations of DPRM (r.e. sets are diophantine) to other rings $\mathcal{R}$. A recursive presentation $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$ gives an enumeration of $\mathcal{R}$, so we can talk about the n-th element $\theta^{-1}(n)$. In Section 3.4.1, we explain how a diophantine definition of the relation "X is the n-th element" with $X \in \mathcal{R}$ and $n \in \mathbb{N}$ implies that r.e. sets are diophantine.

1.2.2 Part II: Hilbert's Tenth Problem for function fields

We prove the negative answer to HTP for certain function fields of curves over valued fields with residue characteristic zero. This generalizes a result by Kim and Roush (see [KR92]), who proved the negative answer to HTP for $\mathbb{C}(Z_1, Z_2)$. Eisenträger extended this to function fields of varietes of dimension ≥ 2 over $\mathbb{C}$ (see [Eis04]). In many cases, our method also works for such function fields, but there are some extra conditions. There exist many more results regarding HTP for function fields, see the introduction to Chapter 4.

In our Main Theorem 4.31, we consider fields $K(C)$, the function field of a curve C over K. Here, K is a valued field with residue field k, both of characteristic zero. In Section 4.11, we list many fields where our result can be applied. An important example is function fields of curves over $\mathbb{C}((T))$.

In Main Theorem 4.31, there are three conditions on the field $K(C)$: the first is that the value group must not be 2-divisible, i.e. there must be an element $T \in K$ such that $v(T)$ is not equal to $2v(U)$ for any $U \in K$. The second condition has to do with Galois cohomology. Write F for a maximal subfield of K on which the valuation is trivial (F exists by Zorn's Lemma). For example, if $K = \mathbb{C}((T))$, then F would be $\mathbb{C}$. Then we require that the 2-cohomological dimensions of F and the residue field k are equal, and finite. Finally, the third condition states that the curve C must have a non-singular point in the reduction (over $\bar{k}$). Note that we can change the curve C up to birational equivalence, since we are only interested in the function field $K(C)$. Under these conditions, we can prove that HTP for $K(C)$ has a negative answer.

1.2.3 Part III: Diophantine sets over polynomial rings

This part is about generalizations of DPRM, i.e. the equivalence of recursively enumerable (r.e.) and diophantine sets.

In Chapter 5, we look at the ring $\mathbb{F}_q[Z]$ of polynomials over a finite field. It is well known that the arithmetic of $\mathbb{F}_q[Z]$ is very analogous to that of $\mathbb{Z}$. Therefore, it is a very natural question whether we can prove something like DPRM for $\mathbb{F}_q[Z]$. HTP for this ring has a negative answer, as proven by Denef in 1979 (see [Den79]). We will prove that r.e. sets are diophantine for $\mathbb{F}_q[Z]$. This will be done in two stages: first, we show that r.e. sets over $\mathbb{F}_q[Z]$ are diophantine over $\mathbb{F}_q[W, Z]$. In other words, if we take a set $\mathcal{S} \subseteq \mathbb{F}_q[W, Z]^k$ such that no element of $\mathcal{S}$ involves W, then $\mathcal{S}$ is diophantine over $\mathbb{F}_q[W, Z]$. This result will be published

in [Dem07a], and is the content of Section 5.2–5.7. In Section 5.8, we give a diophantine interpretation of $\mathbb{F}_q[W, Z]$ inside $\mathbb{F}_q[Z]$. This has been written down in a paper [Dem07b]. These two results can be put together to prove that r.e. sets are diophantine over $\mathbb{F}_q[Z]$.

In Chapter 6 we start from two cases where we know that r.e. sets are diophantine, and generalize them to infinite extensions. The first known case is $\mathcal{O}_K[Z_1, \ldots, Z_n]$, the n-variable polynomial ring over the ring of integers in a totally real number field K (see [Zah99, Chapter III] or [Zah00]). We will generalize this to the case where K is algebraic over $\mathbb{Q}$ (not necessarily of finite dimension), but still totally real. Similarly, we will generalize the result of Chapter 5 to rings $\mathbb{F}[Z]$, where $\mathbb{F}$ is an infinite algebraic extension of a finite field. This last result appears also in [Dem07b].

For the rings $\mathcal{O}_K[Z_1, \ldots, Z_n]$ and $\mathbb{F}[Z]$, we can no longer prove that all r.e. sets are diophantine. There are several reasons for this. First of all, the ring we consider might not be recursive, in that case it is impossible to define r.e. sets, so the problem is not even well-defined.

These infinite algebraic extensions are not recursively stable, i.e. there is no absolute definition of "r.e. set". Whether a set is r.e. might depend on the chosen recursive presentation. Since diophantine sets are always r.e., regardless of the recursive presentation, we will only consider sets which are r.e. for *every* recursive presentation. Diophantine sets are always defined by an equation over some finite extension. For example, in the $\mathbb{F}[Z]$ case, any diophantine equation must have its coefficients in some finite field $\mathbb{F}_q$. Then the set defined by that equation will be invariant under $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. But a general r.e. set is not invariant under any $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. So, it looks like we have two necessary conditions on our r.e. sets: first, they must be r.e. for every recursive presentation; second, they must be invariant under $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ for some finite field $\mathbb{F}_q$. However, in Section 6.1 we will prove that these two conditions are actually equivalent. In the case of $\mathcal{O}_K[Z_1, \ldots, Z_n]$, the analogous result holds.

Then, starting from Section 6.2, we prove that the sets, which are r.e. for every recursive presentation, are exactly the diophantine sets. We prove this for $\mathcal{O}_K[Z_1, \ldots, Z_n]$ and $\mathbb{F}[Z]$. In both cases, the structure of the proof is the same, but the proofs themselves are very different. Eventually, we will reduce the problem to finite extensions, where we know the answer.

1.3 Notation

Throughout this thesis, we will use a uniform notation for variables inside formulas: unless specified otherwise, variables with lowercase Latin letters (a, b, c, ..., z) stand for natural numbers, where $\mathbb{N} = \{0, 1, 2, \dots\}$. Uppercase Latin letters (A, B, C, ..., Z) stand for elements of the structure we are considering, i.e. elements of $K(C)$ in Chapter 4, elements of $\mathbb{F}_q[Z]$ in Chapter 5, or elements of $\mathcal{R}$ in Chapter 6. Finally, lowercase Greek letters (α, β, γ, ..., ω) stand for elements of the base field or ring, i.e. K if we are working in $K(C)$ or $\mathbb{F}_q$ if we are working in $\mathbb{F}_q[Z]$.

Chapter 2

Diophantine sets

The most important definition in this thesis is that of a *diophantine set*. In this chapter we give the definition and we explain why it is so important.

2.1 Diophantine sets

Definition 2.1. Let $\mathcal{R}$ be a ring (all rings we consider are commutative with 1) and k a positive integer. We call a subset $\mathcal{S}$ of $\mathcal{R}^k$ *diophantine* over $\mathcal{R}$ if and only if there exists a number n and a polynomial $f(A_1, \ldots, A_k, X_1, \ldots, X_n)$ with coefficients in $\mathcal{R}$ such that:

$$\mathcal{S} = \{(A_1, \ldots, A_k) \in \mathcal{R}^k \mid f(A_1, \ldots, A_k, X_1, \ldots, X_n) = 0 \text{ has a solution in } \mathcal{R}\}. \tag{2.1}$$

Usually, we will write this as

$$(A_1, \ldots, A_k) \in \mathcal{S} \iff (\exists X_1, \ldots, X_n \in \mathcal{R})(f(A_1, \ldots, A_k, X_1, \ldots, X_n) = 0). \tag{2.2}$$

(2.1) and (2.2) are called *diophantine definitions* of the set $\mathcal{S}$.

In this definition, the ring $\mathcal{R}$ plays an important role, since certain sets are diophantine over one ring, but not over another. If we have rings $\mathcal{R}_1 \subset \mathcal{R}_2$, then a set $\mathcal{S} \subseteq \mathcal{R}_1^k$ could be diophantine over $\mathcal{R}_1$ but not over $\mathcal{R}_2$, or diophantine over $\mathcal{R}_2$ but not over $\mathcal{R}_1$.

A function $f : \mathcal{R}^k \to \mathcal{R}^n$ is called diophantine over $\mathcal{R}$ if its graph

$$\mathcal{G} := \{(X, f(X)) \in \mathcal{R}^{k+n} \mid X \in \mathcal{R}^k\}$$

is diophantine over $\mathcal{R}$. Similarly, a relation R on $\mathcal{R}^k$ is called diophantine over $\mathcal{R}$ if the set $\{X \in \mathcal{R}^k \mid R(X)\}$ is diophantine over $\mathcal{R}$.

2.2 Some diophantine sets

We start with a well-known proposition about unions and intersections of diophantine sets.

Proposition 2.2. *Let $\mathcal{R}$ be an integral domain (i.e. a commutative ring without zero divisors). Then the union of two diophantine sets is diophantine and if the fraction field of $\mathcal{R}$ is not algebraically closed then the intersection of two diophantine sets is also diophantine.*

Proof. Let $\mathcal{S}_1 \subseteq \mathcal{R}^k$ be defined by the equation $f(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0$, and $\mathcal{S}_2 \subseteq \mathcal{R}^k$ by the equation $g(a_1, \ldots, a_k, y_1, \ldots, y_n) = 0$.

Then it is easy to see that the union $\mathcal{S}_1 \cup \mathcal{S}_2$ is defined by the product

$$f(a_1, \ldots, a_k, x_1, \ldots, x_m)g(a_1, \ldots, a_k, y_1, \ldots, y_n) = 0. \tag{2.3}$$

For the intersection, we use a polynomial $h(x) = \sum_{i=0}^{d} c_i x^i \in \mathcal{R}[x]$ of degree $d > 0$, which has no roots in the fraction field of $\mathcal{R}$. Such a polynomial exists because we assumed that this field is not algebraically closed. We claim that $\mathcal{S}_1 \cap \mathcal{S}_2$ is defined by

$$\sum_{i=0}^{d} c_i f(a_1, \ldots, a_k, x_1, \ldots, x_m)^{d-i} g(a_1, \ldots, a_k, y_1, \ldots, y_n)^i = 0. \tag{2.4}$$

It is clear that a solution to $f = 0$ and $g = 0$ gives a solution to (2.4).

Conversely, suppose (2.4) has a solution $x_1, \ldots, x_m, y_1, \ldots, y_n$. Then

$$0 = f(\overrightarrow{a}, \overrightarrow{x})^d \sum_{i=0}^{d} c_i \frac{g(\overrightarrow{a}, \overrightarrow{y})^i}{f(\overrightarrow{a}, \overrightarrow{x})^i} = f(\overrightarrow{a}, \overrightarrow{x})^d h\left(\frac{g(\overrightarrow{a}, \overrightarrow{y})}{f(\overrightarrow{a}, \overrightarrow{x})}\right).$$

Since h has no zeros in the fraction field of $\mathcal{R}$, $f(\overrightarrow{a}, \overrightarrow{x})$ must be zero, and the only term remaining in (2.4) is $a_d g(\overrightarrow{a}, \overrightarrow{y})^d = 0$, which implies $g(\overrightarrow{a}, \overrightarrow{y}) = 0$. So we see that $f(\overrightarrow{a}, \overrightarrow{x}) = g(\overrightarrow{a}, \overrightarrow{y}) = 0$, which means that we have defined the intersection of $\mathcal{S}_1$ and $\mathcal{S}_2$. □

In what follows, we will write down diophantine definitions with existential quantifiers ("there exists", $\exists$), as in equation (2.2). In this notation, intersections correspond to logical conjunctions ("and", $\wedge$), and unions to logical disjunctions ("or", $\vee$). All the rings we encounter will satisfy the conditions of the preceding proposition, so we can use $\wedge$ and $\vee$ as many times as we like in our diophantine definitions.

A very important subset of an integral domain $\mathcal{R}$ is the set of its non-zero elements. If this set is diophantine, then "$x \neq y$" is a diophantine relation. In the following proposition, which is based on [Shl94, Theorem 4.2], we see that this works for a large class of rings.

Proposition 2.3. *Let $\mathcal{R}$ be a Noetherian integral domain. Assume that, for all prime non-maximal ideals $\mathfrak{p} \subset \mathcal{R}$, the quotient $\mathcal{R}/\mathfrak{p}$ is a non-local ring with non-algebraically closed fraction field. Then the set $\mathcal{R} \setminus \{0\}$ is diophantine.*

Proof. We will prove this by induction on the Krull dimension d of the ring $\mathcal{R}$. The Noetherian property ensures us that d is finite (see [AM69, Corollary 11.11]). If $d = 0$, then $\mathcal{R}$ is a field and we can simply say

$$a \neq 0 \iff (\exists b \in \mathcal{R})(ab = 1).$$

Now take $d > 0$ and assume that the proposition holds for dimensions less than d. In this case, (0) is a prime non-maximal ideal, so by assumption $\mathcal{R} = \mathcal{R}/(0)$ is not local and its fraction field is not algebraically closed. Let $\mathfrak{p}$ be any prime ideal of height 1 in $\mathcal{R}$ (i.e. a prime ideal such that there is no prime ideal $\mathfrak{q}$ with $(0) \subset \mathfrak{q} \subset \mathfrak{p}$). Since $\mathcal{R}$ is not a local ring, there exists a non-unit $q \in \mathcal{R} \setminus \mathfrak{p}$. By Krull's Hauptidealsatz (see [AM69, Corollary 11.17]), all principal ideals apart from (0) and (1) have height 1, therefore (q) is contained in a prime ideal $\mathfrak{q} \supseteq (q)$ of height 1. Since $q \notin \mathfrak{p}$, it follows that $\mathfrak{p} \neq \mathfrak{q}$.

We claim that the following is a diophantine definition of $\mathcal{R} \setminus \{0\}$:

$$a \neq 0 \tag{2.5}$$

$$\Updownarrow$$

$$(\exists b, x, y \in \mathcal{R})(ab = xy \ \wedge \ x \not\equiv 0 \bmod \mathfrak{p} \ \wedge \ y \not\equiv 0 \bmod \mathfrak{q}). \tag{2.6}$$

Before we prove the equivalence, let us try to see that (2.6) is diophantine. For the subformula "$ab = xy$", this is obvious. The ideals $\mathfrak{p}$ and $\mathfrak{q}$ are diophantine because they are finitely generated $\mathcal{R}$-modules. This gives a diophantine interpretation

of the ring $\mathcal{R}/\mathfrak{p}$ in $\mathcal{R}$. Define $x \sim y$ as $x - y \in \mathfrak{p}$, and use the addition and multiplication from $\mathcal{R}$. This way, "$x \not\equiv 0 \bmod \mathfrak{p}$" becomes "$x \neq 0$" in $\mathcal{R}/\mathfrak{p}$. Since the ring $\mathcal{R}/\mathfrak{p}$ is a Noetherian integral domain of Krull dimension $< d$, we can use the induction hypothesis to see that "$x \neq 0$" is diophantine in $\mathcal{R}/\mathfrak{p}$. Analogously, "$y \not\equiv 0 \bmod \mathfrak{q}$" is also diophantine. Finally, using Proposition 2.2, we see that (2.6) is diophantine.

It is easy to see that (2.6) implies $a \neq 0$. Indeed, if $a = 0$, then either $x = 0$ or $y = 0$, since $\mathcal{R}$ is an integral domain. This contradicts $x \not\equiv 0 \bmod \mathfrak{p}$ or $y \not\equiv 0 \bmod \mathfrak{q}$.

Conversely, assume that $a \neq 0$. If a is a unit, then we simply set $b = a^{-1}$ and $x = y = 1$. So we may assume that $(a) \neq (1)$. Since $\mathcal{R}$ is Noetherian, every ideal different from (1) has a primary decomposition, hence we can write

$$(a) = \bigcap_{i=1}^{n} \mathfrak{a}_i \qquad (\mathfrak{a}_i \text{ primary}).$$

Take such a primary $\mathfrak{a}_i$. We claim that either $\mathfrak{a}_i \not\subseteq \mathfrak{p}$ or $\mathfrak{a}_i \not\subseteq \mathfrak{q}$. Assume that $\mathfrak{a}_i \subseteq \mathfrak{p} \cap \mathfrak{q}$. Since $\mathfrak{a}_i$ is primary, its radical $\mathfrak{r}_i = \operatorname{rad}(\mathfrak{a}_i)$ is prime. Because $\mathfrak{p}$ is prime, $\mathfrak{a}_i \subseteq \mathfrak{p}$ implies $\mathfrak{r}_i \subseteq \mathfrak{p}$. If $\mathfrak{r}_i = (0)$, then $\mathfrak{a}_i = 0$ and $(a) = 0$, contradicting $a \neq 0$. But $\mathfrak{p}$ has height 1, therefore $\mathfrak{r}_i$ must be equal to $\mathfrak{p}$. By the same argument one can prove that $\mathfrak{r}_i = \mathfrak{q}$, contradicting $\mathfrak{p} \neq \mathfrak{q}$.

We are now ready to construct the x and y appearing in (2.6). Let $I \subseteq \{1, \ldots, n\}$ be the indices for which $\mathfrak{a}_i \not\subseteq \mathfrak{p}$. Now choose $x_i \in \mathfrak{a}_i \setminus \mathfrak{p}$ for $i \in I$, and let $x = \prod_{i \in I} x_i$. Since $\mathfrak{p}$ is prime, this product will also lie outside of $\mathfrak{p}$, in other words $x \not\equiv 0 \bmod \mathfrak{p}$. Similarly, we choose $y_i \in \mathfrak{a}_i \setminus \mathfrak{q}$ for $i \notin I$, and let $y = \prod_{i \notin I} y_i$. Then

$$xy \in \prod_{i=1}^{n} \mathfrak{a}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{a}_i = (a).$$

Hence, we can write xy as ab for some $b \in \mathcal{R}$. □

We finish this section with two more examples of diophantine definitions:

Example 2.4. The gcd function in $\mathbb{Z}$ is diophantine. Indeed, it is easy to see that

$$\gcd(a, b) = c \iff (\exists w)(cw = a) \ \wedge \ (\exists x)(cx = b) \ \wedge (\exists y, z)(ax + by = c).$$

Example 2.5. Consider a polynomial ring $\mathcal{R}[Z]$. Then the ternary relation $F(\alpha) = \beta$, between $F \in \mathcal{R}[Z]$ and $\alpha, \beta \in \mathcal{R}$ is diophantine over $\mathcal{R}[Z]$. Indeed,

$$F(\alpha) = \beta \iff (\exists M \in \mathcal{R}[Z])\big(F - \beta = M(Z - \alpha)\big).$$

Note that the right hand side is equivalent to $F \equiv \beta \bmod Z - \alpha$. We required a priori that α and β are elements of $\mathcal{R}$. As part of a bigger formula, this definition is therefore only useful if $\mathcal{R}$ is a diophantine subset of $\mathcal{R}[Z]$.

2.3 Languages

In Chapter 1, we briefly mentioned the fact that for Hilbert's Tenth Problem over a ring $\mathcal{R}$, we often consider diophantine equations with coefficients in a subring of $\mathcal{R}$. This happens for example if the ring $\mathcal{R}$ is uncountable.

The ring where we will take our coefficients will be formalized with the use of a *language*, which is simply a set of symbols. We define a *diophantine equation in the language* $\mathcal{L}$ (or shorter, an $\mathcal{L}$*-diophantine equation*) as any equation which can be written using variable symbols, equality and symbols from $\mathcal{L}$. We illustrate this with the equation $y^2 - 2x = 3$. This is a diophantine equation in the language $\{+, \cdot, 0, 1\}$, because $y^2 - 2x = 3$ can be written as $y \cdot y = 1 + 1 + 1 + x + x$. The language $\{+, \cdot, 0, 1\}$ allows us to write any diophantine equation with coefficients in $\mathbb{Z}$. However, for diophantine equations over the polynomial ring $\mathbb{Z}[Z]$ for instance, it makes sense to take $\{+, \cdot, 0, 1, Z\}$ as a language. This way, we can express all diophantine equations with coefficients in $\mathbb{Z}[Z]$.

The languages $\{+, \cdot, 0, 1\}$ and $\{+, \cdot, 0, 1, Z\}$ are two examples of ring languages. A *ring language* is a language consisting of $\{+, \cdot, 0, 1\}$ and some symbols standing for elements of the ring we are working with. Sometimes, we can work with a derivative of a ring language, for example the language $\{+, |, 0, 1\}$, where $|$ denotes the divisibility relation. Therefore, one could consider "$(x + 2y)|(x + z + 1)$" as a diophantine equation in the language $\{+, |, 0, 1\}$. We did not write "=" in that formula, because "|" is already a relation.

Let $\mathcal{L}$ be a language. We say that a set $\mathcal{S} \subseteq \mathcal{R}^k$ is $\mathcal{L}$*-diophantine* over $\mathcal{R}$ if $\mathcal{S}$ is diophantine over $\mathcal{R}$ as in Definition 2.1, with the additional condition that f can be written in the language $\mathcal{L}$. Similarly, we can consider *Hilbert's Tenth Problem* for a ring $\mathcal{R}$ and a language $\mathcal{L}$. Then we only want to decide diophantine equations which can be written in the language $\mathcal{L}$.

In model theory, one makes a very clear distinction between symbols (or names) and the actual functions, relations or elements. For example, the symbol "0" is just a symbol, it is not tied to a specific ring. However, we will consider every ring with its own language, so we will abuse terminology and not make this distinction.

In this thesis, we will always consider finite languages. As a consequence, there can only be countably many diophantine equations.

2.4 Diophantine interpretations and models

In this section, we will define *diophantine interpretations* (with a *diophantine model* as special case) of a ring $\mathcal{Z}$ within another ring $\mathcal{R}$. The idea is to encode elements of $\mathcal{Z}$ inside $\mathcal{R}$. For example, if $\mathcal{R} = \mathbb{F}_q[Z]$, a polynomial ring over a finite field, then there exists a diophantine interpretation of the natural numbers $\mathbb{N}$ inside $\mathcal{R}$ (note that $\mathbb{N}$ is not a ring, but that does not matter since $\mathbb{Z}$ can be interpreted over $\mathbb{N}$). This is done by encoding a natural number n as the monomial $Z^n \in \mathbb{F}_q[Z]$. Of course, we want to transfer the diophantine structure from $\mathbb{N}$ to this encoding: we have to diophantinely define Z^{a+b} and Z^{ab} as a function of Z^a and Z^b. For the addition, one can see immediately how to do this, since $Z^{a+b} = Z^a Z^b$. The multiplication is harder, but it can also be done (see Chapter 5).

We can now give the formal definition, where elements of $\mathcal{Z}$ are encoded as equivalence classes in $\mathcal{R}^r$.

Definition 2.6. Let $\mathcal{R}$ and $\mathcal{Z}$ be rings, let $\mathcal{L}$ be a language for the ring $\mathcal{R}$. Then an *$\mathcal{L}$-diophantine interpretation* of $\mathcal{Z}$ over $\mathcal{R}$ consists of a set $\mathcal{S} \subseteq \mathcal{R}^r$ for some $r \geq 1$, an equivalence relation $\sim$ on $\mathcal{S}$ and a bijection $\tau : \mathcal{Z} \xrightarrow{\sim} \mathcal{S}/\sim$ such that

1. The set $\mathcal{S}$ is $\mathcal{L}$-diophantine.
2. The relation $\sim$ is $\mathcal{L}$-diophantine, i.e. the set $\{(X, Y) \in \mathcal{S} \times \mathcal{S} \mid X \sim Y\} \subseteq \mathcal{R}^{2r}$ is $\mathcal{L}$-diophantine.
3. $\mathcal{G}_+ := \{(X, Y, Z) \in \mathcal{S}^3 \mid \tau^{-1}(X) + \tau^{-1}(Y) = \tau^{-1}(Z)\}$ is $\mathcal{L}$-diophantine.
4. $\mathcal{G}_\times := \{(X, Y, Z) \in \mathcal{S}^3 \mid \tau^{-1}(X)\tau^{-1}(Y) = \tau^{-1}(Z)\}$ is $\mathcal{L}$-diophantine.

Definition 2.7. As a special case of this, a *diophantine model* of $\mathcal{Z}$ over $\mathcal{R}$ is a diophantine interpretation where the equivalence relation is equality (i.e. where $X \sim Y \iff X = Y$).

Example 2.8. The most basic diophantine model is when $\mathcal{Z}$ is a diophantine subring of $\mathcal{R}$ (i.e. $\mathcal{Z}$ is a subring of $\mathcal{R}$ and is diophantine over $\mathcal{R}$). Indeed, we take $\mathcal{S}$ to be equal to $\mathcal{Z}$ (then $\mathcal{S} \subseteq \mathcal{R}$), $\sim$ is equality and τ is the identity. This trivially satisfies all conditions in order to have a diophantine interpretation.

Diophantine interpretations are very important because of the following proposition, which will usually be applied with $\mathcal{Z} = \mathbb{Z}$.

Proposition 2.9. *Let $\mathcal{R}$ be a ring admitting a diophantine interpretation of a ring $\mathcal{Z}$. If diophantine equations over $\mathcal{Z}$ in the language $\{+, \cdot, 0, 1\}$ are undecidable, then diophantine equations are undecidable over $\mathcal{R}$.*

The idea is that every diophantine equation over $\mathcal{Z}$ can be transferred to a diophantine equation over $\mathcal{R}$. So, if diophantine equations over $\mathcal{R}$ were decidable, then diophantine equations over $\mathcal{Z}$ would also be decidable.

We have an interpretation of $\mathcal{Z}$ over $\mathcal{R}$, let $\mathcal{G}_+$ and $\mathcal{G}_\times$ be as in Definition 2.6. Instead of explaining the transfer of diophantine equations formally, we illustrate it with an example. Consider the diophantine equation $(\exists a, b, c, d \in \mathcal{Z})(ab + c = d)$. This can be transferred to $\mathcal{R}$ as follows:

$$(\exists A, B, C, D \in \mathcal{S})(\exists X, Y \in \mathcal{S})\big((A, B, X) \in \mathcal{G}_\times \ \wedge \ (X, C, Y) \in \mathcal{G}_+ \ \wedge \ Y \sim D\big).$$

Here, A, B, C and D are the images of a, b, c and d under the bijection $\mathcal{Z} \xrightarrow{\sim} \mathcal{S}/\!\sim$. Then X is the image of ab, and Y is the image of $ab + c$.

We can extend Definition 2.6 and Proposition 2.9 to the case where we consider a richer language $\mathcal{L}_\mathcal{Z}$ for $\mathcal{Z}$. If the language $\mathcal{L}_\mathcal{Z}$ contains constants c_i, then the images $\tau(c_i) \subseteq \mathcal{S}$ must be $\mathcal{L}$-diophantine. Because of the third and fourth items in Definition 2.6, $\tau(0)$ and $\tau(1)$ are always $\mathcal{L}$-diophantine, so we do not get extra conditions in the case $\mathcal{L}_\mathcal{Z} = \{+, \cdot, 0, 1\}$. For functions or relations on $\mathcal{L}_\mathcal{Z}$, the sets analogous to $\mathcal{G}_+$ and $\mathcal{G}_\times$ must be $\mathcal{L}$-diophantine. If we have such an $\mathcal{L}$-diophantine interpretation, then Proposition 2.9 still holds, with $\mathcal{L}_\mathcal{Z}$ instead of $\{+, \cdot, 0, 1\}$.

Finally, we give a diophantine interpretation of the fraction field in a given integral domain, provided that the non-zero elements are diophantine (see also Proposition 2.3).

Proposition 2.10. *Let $\mathcal{R}$ be an integral domain such that $\mathcal{R} \setminus \{0\}$ is $\mathcal{L}$-diophantine for some ring language $\mathcal{L}$. Then the fraction field of $\mathcal{R}$ is $\mathcal{L}$-diophantinely interpretable over $\mathcal{R}$ and the natural injection of $\mathcal{R}$ into this interpretation is also $\mathcal{L}$-diophantine.*

Proof. Write K for the fraction field of $\mathcal{R}$. Then every element of K can be written as P/Q, where $P, Q \in \mathcal{R}$ and $Q \neq 0$. Conversely, P/Q represents an element of K whenever $Q \neq 0$. This gives an interpretation $K \to \mathcal{R} \times (\mathcal{R} \setminus \{0\})/\sim : P/Q \mapsto (P, Q)$. Here the equivalence relation $\sim$ is defined as $(P, Q) \sim (R, S) \leftrightarrow PS = QR$. An element $P \in \mathcal{R}$ becomes $(P, 1)$ in the interpretation.

The equivalence, the addition and multiplication of such fractions are given by easy formulas, which are clearly diophantine. □

2.5 Product Rings

In this section we study diophantine equations over a finite product of rings $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_f$ (recall that all rings we consider are commutative with 1). Such rings arise naturally by the Chinese Remainder Theorem if we take the quotient of a ring by an ideal. This will be used in Chapter 5.

The following proposition more or less says that a diophantine equation has a solution in a product ring if and only if it has a solution in each of the rings separately.

Proposition 2.11. *Let $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_f$ be rings and set $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_f$ with the natural projection maps $\pi_j : \mathcal{R} \to \mathcal{R}_j$ $(1 \leq j \leq f)$. Let $F_1, \ldots, F_n$ be elements of $\mathcal{R}$ and Δ a polynomial over $\mathbb{Z}$ in $n + m$ variables. Consider the diophantine equation*

$$\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m) = 0. \tag{2.7}$$

This equation has a solution $(X_1, \ldots, X_m) \in \mathcal{R}^m$ if and only if the system

$$\begin{cases} \Delta(\pi_1(F_1), \ldots, \pi_1(F_n), X_1^{(1)}, \ldots, X_m^{(1)}) = 0 & (\text{in } \mathcal{R}_1) \\ \vdots & \\ \Delta(\pi_f(F_1), \ldots, \pi_f(F_n), X_1^{(f)}, \ldots, X_m^{(f)}) = 0 & (\text{in } \mathcal{R}_f) \end{cases} \tag{2.8}$$

has a solution $(X_i^{(j)})_{1 \leq i \leq m, 1 \leq j \leq f}$ where $X_i^{(j)} \in \mathcal{R}_j$.

Proof. If (2.7) holds for some $X_1, \ldots, X_m \in \mathcal{R}$, then we simply take $X_i^{(j)} = \pi_j(X_i)$. Equation (2.7) implies $\pi_j\big(\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m)\big) = 0$ for all $j =$

$1, \ldots, f$. The projections π_j are ring morphisms, so all equations in the system (2.8) will be satisfied.

Conversely, assume we have a solution for (2.8). Set

$$X_i = (X_i^{(1)}, X_i^{(2)}, \ldots, X_i^{(f)}) \in \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_f = \mathcal{R}.$$

Formula (2.7) is equivalent to

$$\pi_j\big(\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m)\big) = 0 \qquad \text{for all } j = 1, \ldots, f.$$

The projections are ring morphisms, so this is equivalent to

$$\Delta(\pi_j(F_1), \ldots, \pi_j(F_n), \pi_j(X_1), \ldots, \pi_j(X_m)) = 0 \qquad \text{for all } j = 1, \ldots, f.$$

But we know the latter is true because $\pi_j(X_i) = X_i^{(j)}$. □

The proposition still holds if we allow conjunctions ($\wedge$) in the equation. But adding disjunctions ($\vee$) or inequations ($\neq$) breaks it, as in the following examples:

- "$(2X = 1) \vee (3X = 1)$" has solutions in $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, but not in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- "$(2X \neq 0)$" has a solution in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, but not in $\mathbb{Z}/2\mathbb{Z}$.

Combining Proposition 2.11 with the Chinese Remainder Theorem, we get:

Corollary 2.12. *Let $\mathcal{R}$ be a ring, let $\mathcal{I}_1, \ldots, \mathcal{I}_f$ be pairwise coprime ideals (i.e. $\mathcal{I}_i + \mathcal{I}_j = \mathcal{R}$ whenever $i \neq j$), and set $\mathcal{I} = \prod_{j=1}^{f} \mathcal{I}_j$. Let $F_1, \ldots, F_n$ be elements of $\mathcal{R}$ (or $\mathcal{R}/\mathcal{I}$), and Δ a polynomial over $\mathbb{Z}$ in $n + m$ variables. Consider the equation*

$$\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m) \equiv 0 \mod \mathcal{I} \tag{2.9}$$

This has a solution if and only if the following system has a solution:

$$\begin{cases} \Delta(F_1, \ldots, F_n, X_1^{(1)}, \ldots, X_m^{(1)}) \equiv 0 \mod \mathcal{I}_1 \\ \vdots \\ \Delta(F_1, \ldots, F_n, X_1^{(f)}, \ldots, X_m^{(f)}) \equiv 0 \mod \mathcal{I}_f \end{cases} \tag{2.10}$$

2.6 Short-circuiting operators and partially diophantine functions

To write down certain logical formulas, we will use so-called *short-circuiting* or *left-to-right* boolean operators. These are the short-circuiting conjunction $\mathbin{\&\!\!\rightarrow}$ and disjunction $\mathbin{\vee\!\!\rightarrow}$. The idea is the following: take an ordinary conjunction $\phi \wedge \psi$. If ϕ is false, then $\phi \wedge \psi$ is always false, no matter what ψ is. So we do not even need to look at ψ if ϕ is already false, we might as well allow ψ to be undefined (e.g. some formula involving $1/x$ when x is 0).

To make this more explicit, we define the operator $\phi \mathbin{\&\!\!\rightarrow} \psi$: if ϕ is false, then $\phi \mathbin{\&\!\!\rightarrow} \psi$ is always false, so ψ can be undefined. If ϕ is true, then ψ must be defined and the truth value of $\phi \mathbin{\&\!\!\rightarrow} \psi$ is equal to the truth value of ψ. Analogously, we can define $\phi \mathbin{\vee\!\!\rightarrow} \psi$, which is automatically true if ϕ is true. Only if ϕ is false does ψ have to be defined, and then $\phi \mathbin{\vee\!\!\rightarrow} \psi$ is true if and only if ψ is true.

An example might be the following formula, which is true in $\mathbb{R}$:

$$x \geq 0 \mathbin{\vee\!\!\rightarrow} 1/x < 0.$$

These operators are familiar to computer programmers, consider the two examples "`if (str != NULL && str[0] != 0)`" in C or "`open(FILE, $filename) || die "Cannot open file $filename"`" in Perl. Here, the `&&` (and) and `||` (or) must be interpreted as short-circuiting to get the desired result. In the second example, the statement `die "Cannot open file $filename"` aborts the program with the error message "`Cannot open file` *filename*". But this will only be executed if `open(FILE, $filename)` is false, in other words, when the file failed to be opened.

These short-circuiting operators can be used to deal with partial functions, but we will also use them for partially diophantine functions. A function (or relation) is called *partially diophantine* if it is diophantine on a subset of the domain. For example, the Euler totient function φ is easily seen to be diophantine on the set of prime numbers, where $\varphi(p) = p - 1$. The function φ is also globally diophantine, this follows from the deep DPRM result (see Section 1.1).

Suppose ϕ is some unary predicate in $\mathbb{Z}$, which is only diophantine for even arguments. Then the whole formula "$a \in 2\mathbb{Z} \ \wedge \ \phi(a)$" is diophantine. Indeed, let $(\exists x_1, \ldots, x_n)(f(a, x_1, \ldots, x_n) = 0)$ be the diophantine definition of $\phi(a)$ for a even. Then

$$a \in 2\mathbb{Z} \ \wedge \ \phi(a) \iff (\exists b, x_1, \ldots, x_n)(a = 2b \ \wedge \ f(a, x_1, \ldots, x_n) = 0).$$

If a is odd, then this formula is always false; the value of $f(a, x_1, \ldots, x_n)$ does not matter at all. Note that the part "$\phi(a)$" is not diophantine by itself. To emphasize this, we will write that "$a \in 2\mathbb{Z} \mathrel{\not\Rightarrow} \phi(a)$" is diophantine.

Chapter 3

Recursively enumerable and recursive sets

In this chapter, we will define recursively enumerable (r.e.) and recursive sets. These concepts come from logic, and define the sets which can be constructed by algorithms. Originally, these kinds of sets were defined for subsets of $\mathbb{N}$, but it is possible to extend the definitions to general rings. However, this only works if the ring is a so-called recursive ring.

All the definitions in this chapter will play an important role in Part III of this thesis. There we will study the question whether r.e. sets are diophantine for certain polynomial rings.

Some words about terminology: in the contemporary literature in logic, the word "computable" is often used instead of "recursive". However, we will use the older terminology of recursive sets, since that has been used in the standard references about Hilbert's Tenth Problem.

3.1 Algorithms

Before we can define recursively enumerable or recursive sets, we have to say something about algorithms. The theory of algorithms was developed in the 1930s by Church, Gödel, Kleene, Post and Turing.

Intuitively, one can think about an ordinary desktop computer running some program (written in some programming language), but with unbounded memory. Since we are dealing with logic and not computer science, we do not care how long our algorithms take. For example, factoring an integer $n > 1$ is very easy: just try all $2 \leq d < n$ and check whether d divides n. In practice, there are much faster algorithms, but for our purposes this is irrelevant.

The most well known formal definition of algorithm is given by *Turing machines*. Algorithms can also be defined using λ-calculus, recursive functions, register machines, random access stored program machines (a formalization of ordinary computers), and many others. It turns out that all these definitions are equivalent, they can all compute exactly the same things.

The *Church–Turing thesis* states that everything which is intuitively considered to be computable, is actually computable by a Turing machine (or any of the other equivalent machines mentioned before). In other words, there is only one natural definition of "algorithm". Therefore, we will just talk about algorithms from now on, instead of Turing machines or computer programs.

3.1.1 Universal algorithms and the halting problem

Algorithms have as input and output a sequence of natural numbers. Any given algorithm has a fixed program: for example, there is an algorithm to add two numbers, an algorithm to compute the k-th prime number, and so on.

Every program can be encoded as a natural number, the so-called *Gödel number*. This encoding can be made into an algorithmic bijection between algorithms and the natural numbers. With algorithmic, we mean that, given a natural number, we can write down the corresponding program for an algorithm, and vice versa. Write T_n for the n-th algorithm (the T stands for Turing machine).

With this, it is possible to make a universal algorithm (universal Turing machine). This is an algorithm, which takes its first input $n \in \mathbb{N}$ and then runs as if it were algorithm T_n with the remaining inputs. In other words, a universal algorithm is one which can run every other algorithm.

If we run an algorithm with a certain input, there are two possible outcomes: either the algorithm halts after a finite number of operations, or it keeps running forever. The *halting problem* is the question to determine this outcome, given the program and the input. We use a diagonal argument to show that this is an undecidable problem. If it were decidable, then we could make an algorithm

which halts on input n if and only if T_n does *not* halt on input n. But this is itself an algorithm T_h. Then T_h would halt on input h if and only if T_h does not halt on input h, clearly a contradiction.

3.2 In the natural numbers

We will write $\mathbb{N}$ for the set of non-negative integers $\{0, 1, 2, \dots\}$.

We start with two equivalent definitions of recursively enumerable sets:

Definition 3.1. A set $\mathcal{S} \subseteq \mathbb{N}^k$ is called *recursively enumerable* (r.e.) if there exists an algorithm which on input $x \in \mathbb{N}^k$, halts if and only if $x \in \mathcal{S}$.

Definition 3.2. A set $\mathcal{S} \subseteq \mathbb{N}^k$ is called *recursively enumerable* if there exists an algorithm which runs forever and prints elements of $\mathbb{N}^k$, such that the set of k-tuples printed is exactly $\mathcal{S}$. In other words, the program must not print elements outside $\mathcal{S}$, and must print every $x \in \mathcal{S}$ at least once.

Proposition 3.3. *The two definitions of r.e. sets are equivalent.*

Proof. Assume that $\mathcal{S}$ is r.e. according to Definition 3.2. We have to construct an algorithm which, given $x \in \mathcal{S}$, halts if and only if $x \in \mathcal{S}$. We let the algorithm printing $\mathcal{S}$ run, and look at the output. If we see the given x, then we halt, otherwise we keep running.

The converse is more difficult. To print $\mathcal{S}$, we do the following: we loop through $\mathbb{N}^{k+1}$ (this can be done since $\mathbb{N}^{k+1}$ is countable), and for every $(\overrightarrow{x}, t) \in \mathbb{N}^k \times \mathbb{N}$, we run an algorithm like in Definition 3.1 with input $\overrightarrow{x}$. If it has halted before t seconds passed, then we print $\overrightarrow{x}$. Otherwise, we abort after t seconds, and try the next $(\overrightarrow{x}, t)$. Since every $\overrightarrow{x}$ will eventually be tried for arbitrarily long time, we will find every $\overrightarrow{x} \in \mathcal{S}$. □

Next we define recursive sets, even though these will not play such an important role for our purposes.

Definition 3.4. A subset $\mathcal{S} \subseteq \mathbb{N}^k$ is called *recursive* if there exists an algorithm which on input $x \in \mathbb{N}^k$, decides in finite time whether or not $x \in \mathcal{S}$.

Proposition 3.5. *A set $\mathcal{S}$ is recursive if and only if both $\mathcal{S}$ and its complement $\overline{\mathcal{S}}$ are recursively enumerable.*

Proof. If $\mathcal{S}$ is recursive, it is also r.e. (Definition 3.1). Indeed, if the answer to the question "is x in $\mathcal{S}$?" is `YES`, then we halt. If the answer is `NO`, we run forever. Analogously, $\overline{\mathcal{S}}$ is also r.e..

Conversely, assume both $\mathcal{S}$ and $\overline{\mathcal{S}}$ are r.e. as in Definition 3.1, and we are asked to decide whether a given x lies in $\mathcal{S}$. On even days, we run the algorithm which halts if $x \in \mathcal{S}$; on odd days, the algorithm which halts if $x \notin \mathcal{S}$. Eventually, one of these must halt, and then we will know whether $x \in \mathcal{S}$ or not. □

We saw that recursive sets are always r.e., but the converse does not hold:

Proposition 3.6. *There exists a set $\mathcal{S} \subseteq \mathbb{N}$ such that $\mathcal{S}$ is r.e., but not recursive.*

Proof. Let $\mathcal{S}$ be the so-called halting set, which is the set of all $n \in \mathbb{N}$ such that the n-th algorithm T_n halts on input n (see Section 3.1.1). Since the halting problem is undecidable, $\mathcal{S}$ is not recursive.

To show that $\mathcal{S}$ is r.e. according to Definition 3.1, we consider the following algorithm, which is a slightly modified universal algorithm. When given input n, it runs as T_n with input n. It is clear that this algorithm halts on input n if and only if $n \in \mathcal{S}$. □

Definition 3.7. If $f : \mathbb{N}^k \to \mathbb{N}^n$ is a function (defined everywhere), then f is called a *recursive function* if its graph $\mathcal{G} := \{(x, f(x)) \in \mathbb{N}^{k+n} \mid x \in \mathbb{N}^k\}$ is recursive.

If this graph is r.e., it is automatically recursive. Indeed, if we are asked whether (x, y) is on $\mathcal{G}$, then we let the algorithm run which prints $\mathcal{G}$ (see Definition 3.2). Since f is everywhere defined, we must eventually find the point $(x, f(x))$. Then we simply check whether y is equal to $f(x)$.

The image of a recursive function is always r.e., but not necessarily recursive.

3.3 In recursive rings

If we want to extend the notions of recursively enumerable and recursive sets to other rings, we require the ring to be recursive. This means that we want to represent that ring in a computer. The problem is that computers work with natural numbers, not with elements of arbitrary rings. Take for example the

ring $\mathbb{F}_p[Z]$, with p prime. We have to represent the elements of $\mathbb{F}_p[Z]$ as natural numbers, such that a computer can work with them. One way to do this is to map $\sum_{i=0}^{n} a_i Z^i$ (with $0 \leq a_i < p$) to $2^{a_0} 3^{a_1} 5^{a_2} \dots p_{n+1}{}^{a_n}$, where p_k is the k-th prime number. We also want a computer to be able to compute with these representations: given a representation for polynomials A and B, it should be possible to compute the representation for $A+B$ and AB. Such a representation is formalized as a *recursive presentation*, which we will now define.

Definition 3.8. Let $\mathcal{R}$ be a ring. A *recursive presentation* for $\mathcal{R}$ is a bijection $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$ such that the following sets are recursive (as subsets of $\mathbb{N}^3$):

$$\mathcal{R}_\theta^+ = \{(\theta(A), \theta(B), \theta(A+B)) \in \mathbb{N}^3 \mid A, B \in \mathcal{R}\},$$
$$\mathcal{R}_\theta^\times = \{(\theta(A), \theta(B), \theta(AB)) \in \mathbb{N}^3 \mid A, B \in \mathcal{R}\}.$$

We call $\mathcal{R}_\theta^+$ the *addition table*, and $\mathcal{R}_\theta^\times$ the *multiplication table* of θ. These subsets of $\mathbb{N}^3$ are what a computer uses to compute in $\mathcal{R}$. A ring admitting a recursive presentation is called a *recursive ring* (or *computable ring* or *explicit ring*). Note that such a ring must be countable.

However, we also define all finite rings to be recursive. It is obvious that we can compute in a finite ring, since the ring structure is given by finitely much information. In this case, a recursive presentation cannot be a bijection between $\mathcal{R}$ and $\mathbb{N}$, but it can be an embedding.

More background on recursive rings can be found in [FS56] or [Rab60].

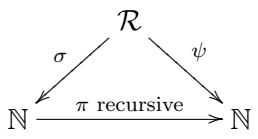
Definition 3.9. Let $\mathcal{R}$ be a recursive ring with recursive presentation $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$. A subset $\mathcal{S}$ of $\mathcal{R}^k$ is said to be r.e. (resp. recursive) if

$$\{\big(\theta(X_1), \dots, \theta(X_k)\big) \in \mathbb{N}^k \mid (X_1, \dots, X_k) \in \mathcal{S}\}$$

is an r.e. (resp. recursive) subset of $\mathbb{N}^k$.

The problem with these definitions is that the recursive presentation θ is far from unique, so a certain set $\mathcal{S} \subseteq \mathcal{R}^k$ could be r.e. for one presentation θ_1, but not for another θ_2. Therefore, we introduce the following definition:

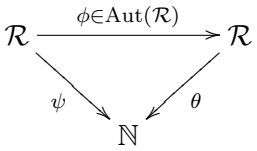
Definition 3.10. A recursive ring $\mathcal{R}$ is called *recursively stable* if for any two recursive presentations $\sigma, \psi : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$, the composition $\pi := \psi \circ \sigma^{-1}$ is recursive as a function $\mathbb{N} \to \mathbb{N}$.



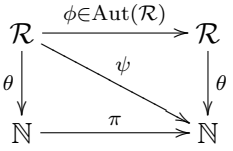
Proposition 3.11. *If a ring $\mathcal{R}$ is recursively stable, then the r.e. sets are the same for every recursive presentation.*

Proof. Let σ, ψ be two recursive presentations and let $\pi := \psi \circ \sigma^{-1}$, which is recursive by Definition 3.10. Consider a set $\mathcal{S} \subseteq \mathcal{R}$, r.e. for σ. This means that $\sigma(\mathcal{S})$ is r.e., but then $\pi(\sigma(\mathcal{S}))$ is also r.e., because π is recursive. Hence, we see that $\mathcal{S}$ is also r.e. for $\psi = \pi \circ \sigma$. □

It is easy to see that the fields $\mathbb{F}_q$ and $\mathbb{Q}$ are recursively stable. Whenever $\mathcal{R}$ is recursively stable, the polynomial ring $\mathcal{R}[Z]$ is also recursively stable (see [FS56, Theorem 3.1]). The algebraic closure of a finite field is an example of a field which is not recursively stable. In Chapter 6, we will solve this by considering only the sets which are r.e. for every recursive presentation.



Let us now investigate what a ring automorphism does to a recursive presentation. Let $\mathcal{R}$ be a recursive ring with presentation $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$, and let ϕ be an automorphism of $\mathcal{R}$. Then $\psi := \theta \circ \phi$ is again a recursive presentation with exactly the same addition and multiplication tables. Consider for example an element $\big(\psi(A), \psi(B), \psi(A+B)\big)$ of the addition table $\mathcal{R}^+_\psi$. This is equal to $\big(\theta(\phi(A)), \theta(\phi(B)), \theta(\phi(A)+\phi(B))\big)$, which is an element of $\mathcal{R}^+_\theta$.



This implies that recursively stable rings can have at most $\aleph_0$ automorphisms. Indeed, let $\mathcal{R}$ be recursively stable with a recursive presentation θ. If $\phi \in \mathrm{Aut}(\mathcal{R})$, then $\psi := \theta \circ \phi$ is also a recursive presentation, hence $\pi := \theta \circ \phi \circ \theta^{-1}$ must be recursive. But there are only $\aleph_0$ different recursive functions π, so there can only be $\aleph_0$ different automorphisms ϕ.

3.4 And diophantine sets

As mentioned in Section 1.1, we have the famous DPRM theorem:

Theorem (DPRM)**.** *For all $k \geq 1$, a subset of $\mathbb{Z}^k$ is recursively enumerable if and only if it is diophantine over $\mathbb{Z}$.*

It is easy to see that every diophantine subset of $\mathbb{Z}^k$ is recursively enumerable. Take a diophantine set

$$\mathcal{S} = \{(a_1, \ldots, a_k) \in \mathbb{Z}^k \mid f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0 \text{ has a solution over } \mathbb{Z}\}.$$

Construct an algorithm which tries all possible values for $(a_1, \ldots, a_k, x_1, \ldots, x_n) \in \mathbb{Z}^{k+n}$, and prints $(a_1, \ldots, a_k)$ whenever a zero of f is found. This algorithm will list exactly the set $\mathcal{S}$, hence $\mathcal{S}$ is r.e. according to Definition 3.2. The converse, i.e. that recursively enumerable sets are diophantine, is the hard part.

Together with the existence of a set which is r.e. but not recursive (see Proposition 3.6), DPRM implies the negative answer to HTP for $\mathbb{Z}$. Indeed, let $\mathcal{S} \subseteq \mathbb{Z}$ be r.e., but not recursive. By DPRM, there exists some f such that

$$\mathcal{S} = \{a \in \mathbb{Z} \mid f(a, x_1, \ldots, x_n) = 0 \text{ has a solution over } \mathbb{Z}\}.$$

If HTP would have a positive answer, then we would be able to decide whether the equation $f(a, x_1, \ldots, x_n) = 0$ has a solution for a given $a \in \mathbb{Z}$. This way, we could decide whether a is in $\mathcal{S}$, hence $\mathcal{S}$ would be recursive and we have a contradiction.

HTP has been settled for a large number of rings, either by proving undecidability, or by giving a decision algorithm (see [PhZ00] for a list of results). On the contrary, very little is known about the analogue of DPRM: are diophantine sets over $\mathcal{R}$ the same as recursively enumerable sets over $\mathcal{R}$? Obviously, this question only makes sense if the ring $\mathcal{R}$ is recursive; in particular it has to be countable.

Let $\mathcal{O}_K$ be a number ring. In the case where $\mathbb{Z}$ is diophantine in $\mathcal{O}_K$, one can easily prove the analogue of DPRM for $\mathcal{O}_K$, using the fact that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. For polynomial rings, Denef proved the analogue of DPRM for $\mathbb{Z}[Z]$ (see [Den78b]) and Zahidi extended this result to $\mathcal{O}_K[Z_1, Z_2, \ldots, Z_m]$ with $\mathcal{O}_K$ the ring of integers in a totally real number field (see [Zah99]). Apart from the results in this thesis, this is a complete list.

3.4.1 Defining the n-th element

After the proof of DPRM in 1970, the strategy to prove that recursively enumerable sets are diophantine has always been the same. Let $\mathcal{R}$ be an integral domain, which admits a diophantine interpretation of $\mathbb{Z}$ (by Proposition 2.9 this already implies undecidability). The idea is to transfer the fact that r.e. sets are diophantine from $\mathbb{Z}$ to $\mathcal{R}$. To do this, we have to give a diophantine definition of

the relation "X is the n-th element of $\mathcal{R}$". With the n-th element, we mean the element of $\mathcal{R}$ which gets mapped to n for a certain recursive presentation. This strategy has been successfully applied in [Den78b] and [Zah99]. A less general version of the following theorem appeared in [Zah99, III (2.1)].

Theorem 3.12. *Let $\mathcal{R}$ be an integral domain admitting a recursive presentation $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$. Assume that there is a diophantine interpretation $\tau : \mathbb{Z} \xrightarrow{\sim} \mathcal{Z}/\!\sim$ with $\mathcal{Z} \subseteq \mathcal{R}^r$. Then the following are equivalent:*

1. *For all $k \geq 1$, every r.e. subset of $\mathcal{R}^k$ is diophantine over $\mathcal{R}$.*
2. *The function $\tau \circ \theta : \mathcal{R} \to \mathcal{Z}/\!\sim$ is diophantine (this means that "$\overrightarrow{A} \sim \tau(\theta(X))$" is a diophantine relation between $\overrightarrow{A} \in \mathcal{Z} \subseteq \mathcal{R}^r$ and $X \in \mathcal{R}$).*

Proof. $1 \Rightarrow 2$: Combine the facts that θ is a recursive presentation of $\mathcal{R}$, that τ is a diophantine (hence r.e.) interpretation, and that $\sim$ is diophantine (hence r.e.). Then we get that the relation "$\tau(\theta(X)) \sim \overrightarrow{A}$" is an r.e. relation on $\mathcal{R}$. Using our hypothesis, this means that the relation between $\overrightarrow{A}$ and X is diophantine.

$2 \Rightarrow 1$: Take an r.e. subset $\mathcal{S}$ of $\mathcal{R}^k$. By definition, this means that

$$\mathcal{S}^\theta := \{\big(\theta(X_1), \ldots, \theta(X_k)\big) \in \mathbb{N}^k \mid (X_1, \ldots, X_k) \in \mathcal{S}\}$$

is an r.e. subset of $\mathbb{N}^k \subset \mathbb{Z}^k$. By DPRM, $\mathcal{S}^\theta$ is diophantine over $\mathbb{Z}$. Hence, we can use the diophantine interpretation of $\mathbb{Z}$ in $\mathcal{R}$ to establish that

$$\begin{aligned}\mathcal{S}' &= \big\{(\overrightarrow{A_1}, \ldots, \overrightarrow{A_k}) \in \mathcal{Z}^k \mid \big(\exists (x_1, \ldots, x_k) \in \mathcal{S}^\theta\big) \\ &\qquad\qquad \big(\overrightarrow{A_1} \sim \tau(x_1) \ \wedge \ \ldots \ \wedge \ \overrightarrow{A_k} \sim \tau(x_k)\big)\big\} \\ &= \big\{(\overrightarrow{A_1}, \ldots, \overrightarrow{A_k}) \in \mathcal{Z}^k \mid \big(\exists (X_1, \ldots, X_k) \in \mathcal{S}\big) \\ &\qquad\qquad \big(\overrightarrow{A_1} \sim \tau(\theta(X_1)) \ \wedge \ \ldots \ \wedge \ \overrightarrow{A_k} \sim \tau(\theta(X_k))\big)\big\}\end{aligned}$$

is diophantine over $\mathcal{R}$. For $(X_1, \ldots, X_k) \in \mathcal{R}^k$ we have

$$\begin{aligned}(X_1, \ldots, X_k) \in \mathcal{S} \iff &\big(\exists \overrightarrow{A_1}, \ldots, \overrightarrow{A_k} \in \mathcal{Z}\big) \\ &\big((\overrightarrow{A_1}, \ldots, \overrightarrow{A_k}) \in \mathcal{S}' \ \wedge \ \overrightarrow{A_1} \sim \tau(\theta(X_1)) \ \wedge \ \ldots \ \wedge \ \overrightarrow{A_k} \sim \tau(\theta(X_k))\big).\end{aligned}$$

We saw that $\mathcal{S}'$ is diophantine, and we know by assumption that the set $\mathcal{Z}$ and the relation "$\overrightarrow{A} \sim \tau(\theta(X))$" are diophantine, so $\mathcal{S}$ is also diophantine. □

In the preceding theorem, the formula "$\overline{A} \sim \tau(\theta(X))$" essentially states that X is the n-th element, where n is being represented by $\overline{A}$ in the interpretation.

Part II

Hilbert's Tenth Problem for function fields

Chapter 4

Function fields over valued fields in characteristic zero

4.1 Introduction

This chapter deals with Hilbert's Tenth Problem (HTP) for function fields over valued fields, where both the valued field and the residue field have characteristic zero. Under some conditions on the valuation, the residue field and the variety whose function field we are considering, we will prove the negative answer to HTP (see Main Theorem 4.31).

Our Main Theorem generalizes a result by Kim and Roush (see [KR92]), who proved the negative answer to HTP for $\mathbb{C}(Z_1, Z_2)$. Eisenträger extended this to function fields of varietes of dimension ≥ 2 over $\mathbb{C}$ (see [Eis04]). In many cases, our method also works for such function fields, but there are some extra conditions (see condition (iii) in Main Theorem 4.31).

There are already a lot of results on HTP for function fields: Denef proved undecidability for rational function fields over real fields (see [Den78a]), Moret-Bailly generalized this to function fields of varieties over real fields (see [MB05]). Kim and Roush proved the negative answer to HTP for rational function fields over p-adic fields (subfields of $\mathbb{Q}_p$, including all number fields). This was generalized to function fields of varieties independently by Moret-Bailly (see [MB05]) and Eisenträger (see [Eis07]). In positive characteristic, Pheidas proved undecidability for $\mathbb{F}_q(Z)$ (see [Phe91]) with q odd, Videla did the same for q even (see

[Vid94]). This was generalized to function fields over finite fields by Shlapentokh (see [Shl96]) and Eisenträger (see [Eis03]).

One of the biggest open questions is HTP for $\mathbb{C}(Z)$. Generally, this is believed to have a negative answer. If we do not take the whole field $\mathbb{C}(Z)$, but certain (semi-)local subrings, then it is known to have a negative answer (see [Zah02]).

For our result, we consider function fields of curves over valued fields with residue characteristic zero. So we cannot apply our result to $\mathbb{Q}_p(Z)$ for example. One important application of our result where HTP was not known before is the field $\mathbb{C}((T))(Z)$.

Before we can state the Main Theorem (see Section 4.6 and Section 4.9), we need some definitions, regarding valuations, quadratic forms and elliptic curves.

4.2 Valuations

In this section we give definitions and properties of valuations. Readers with a background in commutative algebra will probably have heard of discrete valuations, but we will describe general valuations. As a reference, we will use [EP05].

Definition 4.1. A *totally ordered* $\mathbb{Z}$*-module* Γ is a $\mathbb{Z}$-module (equivalently, an abelian group) with a total order $\leq$ such that $a \leq b \ \rightarrow \ a + c \leq b + c$ for all $a, b, c \in \Gamma$.

In what follows, we will consider only total orders, so we will omit the word "total". The easiest way to define an order on an abelian group Γ is to give the set Γ^+ of non-negative elements. Indeed, let $\Gamma^+ \subset \Gamma$ such that

1. $\Gamma^+ \cap -\Gamma^+ = \{0\}$.
2. $\Gamma^+ \cup -\Gamma^+ = \Gamma$.
3. $\Gamma^+ + \Gamma^+ \subseteq \Gamma^+$.

Then we can put a total order on Γ by defining $a \leq b \iff b - a \in \Gamma^+$.

Ordered $\mathbb{Z}$-modules are always torsion-free. Indeed, assume that $ng = 0$ for some $n \in \mathbb{Z} \setminus \{0\}$ and $g \in \Gamma \setminus \{0\}$. We may assume that $g > 0$ and $n > 0$, otherwise change g to $-g$ and/or n to $-n$. Since $g \geq 0$, we have $g + g \geq g$, $g + g + g \geq g$, $\ldots$, $ng \geq g$. This means that $0 \geq g$, contradicting $g > 0$.

Definition 4.2. With a *valuation* v on a field K, we mean a map $v : K^* \twoheadrightarrow \Gamma$, where Γ is a totally ordered $\mathbb{Z}$-module, satisfying the following conditions:

1. For all $x, y \in K^*$, $v(xy) = v(x) + v(y)$.
2. For all $x, y \in K^*$, $v(x + y) \geq \min(v(x), v(y))$.

Γ is called the *value group* of the valuation. Usually one defines $v(0) = \infty$, which is consistent with the above axioms.

Every field has a *trivial valuation* with value group $\{0\}$. Then $v(x) = 0$ for $x \in K^*$ and $v(0) = \infty$.

If $v : K^* \twoheadrightarrow \Gamma$ is a valuation, the *valuation ring* $\mathcal{O}$ is the ring consisting of all elements of K having non-negative valuation:

$$\mathcal{O} = \{x \in K \mid v(x) \geq 0\}.$$

In $\mathcal{O}$, the elements with strictly positive valuation form a *maximal ideal* $\mathfrak{m}$. The field $k := \mathcal{O}/\mathfrak{m}$ is called the *residue field* of K with respect to v. We have a natural surjection $\pi : \mathcal{O} \twoheadrightarrow k$. Note that for all $x \in K$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. The elements for which both hold form the *unit group* $\mathcal{O}^*$, the set of elements with valuation equal to zero. Also, note that $\mathcal{O}^* = \pi^{-1}(k^*)$.

Proposition 4.3. *The following sequences of abelian groups are exact:*

$$0 \longrightarrow \mathfrak{m} \longrightarrow \mathcal{O} \xrightarrow{\pi} k \longrightarrow 0, \tag{4.1}$$

$$1 \longrightarrow \mathcal{O}^* \longrightarrow K^* \xrightarrow{v} \Gamma \longrightarrow 0, \tag{4.2}$$

$$1 \longrightarrow 1 + \mathfrak{m} \longrightarrow \mathcal{O}^* \xrightarrow{\pi} k^* \longrightarrow 1, \tag{4.3}$$

$$1 \longrightarrow k^* \xrightarrow{\pi^{-1}} K^*/(1 + \mathfrak{m}) \xrightarrow{v} \Gamma \longrightarrow 0. \tag{4.4}$$

Proof. All this follows immediately from the definitions (note that $\pi^{-1}(1) = 1+\mathfrak{m}$ is indeed a subgroup of $\mathcal{O}^*$). □

It turns out that the ring $\mathcal{O}$ completely determines the valuation: let K be a field and $\mathcal{O}$ a *valuation ring* in K, that is a ring such that for all $x \in K$, either $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$. Given such a ring, the quotient map $K^* \to K^*/\mathcal{O}^*$ defines a valuation with value group $\Gamma := K^*/\mathcal{O}^*$, where an element $x\mathcal{O}^*$ is non-negative if $x \in \mathcal{O}$. The exact sequence (4.2) shows that this is, up to isomorphism, the only valuation on K with valuation ring $\mathcal{O}$.

Proposition 4.4. *Let K be a valued field with notations as above. Let k' be a finite extension of the residue field k. Then there exists a K' with $[K' : K] = [k' : k]$, with the property that v can be extended to K' in such a way that the new residue field becomes k' and the value group remains the same (i.e. the extension is unramified).*

Proof. See [End72, Theorem (27.1)]. □

Definition 4.5. With notations as above, a valued field K is called *henselian* if and only if the following property (called *Hensel's Lemma*) holds:

For every $P \in \mathcal{O}[Z]$ and $\alpha \in k$ such that α is a simple root of $P \bmod \mathfrak{m}$, there exists a $\beta \in \pi^{-1}(\alpha) \subseteq \mathcal{O}$ such that $P(\beta) = 0$ (the simple root α in the reduction can be lifted to a global root β).

As shown in [EP05, Theorem 4.1.3], there exist many equivalent formulations of Hensel's Lemma. The one given above is probably the most well known (but also rather weak).

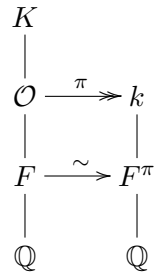
Definition 4.6. If K is a field with valuation v, the *henselisation* K^{H} is the smallest extension of K which is henselian.

Given an algebraic closure $\bar{K}$, the henselisation K^{H} is a uniquely defined subfield of $\bar{K}$. The henselisation is an immediate extension, i.e. the value group Γ and the residue field k remain the same. It is actually the maximal extension of K with this property. All this follows from [EP05, Section 5.2].

Proposition 4.7. *Let K be a valued field with notations as above. If K is henselian and $\operatorname{char} K = \operatorname{char} k = 0$, then $\mathcal{O}$ contains a maximal subfield F. The projection π maps F isomorphically onto k.*

Proof. We give a sketch of the proof, see [CK77, Lemma 5.4.13 (ii)] for more details.

Since $\operatorname{char} k = 0$, the valuation will be trivial on $\mathbb{Q}$, so $\mathcal{O}$ contains $\mathbb{Q}$. By Zorn's Lemma, $\mathcal{O}$ contains a maximal subfield F.



Since F is a field, all non-zero elements are invertible. Therefore, F^* is contained in $\mathcal{O}^*$. It follows that v is trivial on F and that π embeds F as a subfield of k. Denote this field by F^π, we must prove that $F^\pi = k$. Assume this is not the case and let $\alpha \in k \setminus F^\pi$.

If α is transcendental over F^π, choose $\beta \in \mathcal{O}$ such that $\pi(\beta) = \alpha$. Then π gives an isomorphism between $F(\beta)$ and $F^\pi(\alpha)$. Since $F[\beta]$ is mapped isomorphically to $F^\pi[\alpha]$, the valuation v is trivial on $F[\beta]$. Therefore, it is also trivial on $F(\beta)$, hence $F(\beta) \subseteq \mathcal{O}$, contradicting the maximality of F.

If α is algebraic over F^π, let $\overline{f}(X) \in F^\pi[X]$ be the minimal polynomial of α. Write $f(X)$ for the corresponding polynomial in $F[X]$, under the isomorphism π. $\overline{f}(X)$ has a simple zero α in k, so we can use Hensel's Lemma to construct a $\beta \in \mathcal{O}$ for which $f(\beta) = 0$. Again, one can prove that $F(\beta) \cong F^\pi(\alpha)$ under π, contradicting the maximality of F. □

In what follows, we will forget the isomorphism and identify a maximal subfield $F \subseteq \mathcal{O}$ with k. In other words, we simply see k as a subfield of K.

In the proof of Proposition 4.7, we only used the hypothesis that K is henselian to exclude that k is an algebraic extension of F^π. So, for non-henselian fields, we can still say the following:

Proposition 4.8. *Let K be a valued field with notations as above. If $\operatorname{char} K = \operatorname{char} k = 0$, then $\mathcal{O}$ contains a maximal subfield F. The projection π embeds F as a subfield of k, such that k is algebraic over $\pi(F)$.*

Note that "F is contained in $\mathcal{O}$" is equivalent to "v is the trivial valuation on F", so F is maximal with respect to the property that v is trivial on F. It is this definition of F that we will use later on.

Counterexample 4.9. Because Zorn's Lemma does not imply uniqueness, the maximal field $F \subseteq \mathcal{O}$ is not unique. Consider for example the rational function field $K = \mathbb{C}(S, T)$, and let v be the discrete valuation associated to the ideal (T) in $\mathbb{C}[S, T]$, i.e. v is trivial on $\mathbb{C}(S)$ and $v(T) = 1$. Then $\mathbb{C}(S)$ is a maximal subfield of $\mathcal{O}$, but also $\mathbb{C}(S + T)$ is a maximal subfield.

Proof. The valuation v is trivial on $\mathbb{C}(S)$, so clearly $\mathbb{C}(S)$ is a subfield of $\mathcal{O}$. To prove the second statement, let $f \in \mathbb{C}[S+T]$. Then we can write $f = \sum_i a_i(S+T)^i$ with $a_i \in \mathbb{C}$. Applying π, we get $\pi(f) = \sum_i a_i S^i$. Since S is transcendental, $\pi(f)$ can only be zero whenever f is zero. But $\pi(f) \neq 0$ means that $v(f) = 0$. Every element of $\mathbb{C}(S+T)^*$ can be written as f/g, with $f, g \in \mathbb{C}[S+T] \setminus \{0\}$. Since $v(f) = v(g) = 0$, we get $v(f/g) = 0$, hence v is trivial on $\mathbb{C}(S+T)$. If $\mathbb{C}(S+T)$ were not maximal, it would be contained in a field $F \subseteq \mathcal{O}$ of transcendence degree 2 over $\mathbb{C}$. Since v is trivial on F, it would also be trivial on the algebraic extension $\mathbb{C}(S,T)$ of F, which is not the case. □

We end this section by introducing the *composition* of valuations (see also [EP05, Section 2.3, p. 45]). We will only use this in the examples (see Section 4.11).

Proposition 4.10. *Let K be a field with a valuation v and residue field k_v. Assume u is a valuation on k_v, with residue field k_u. Then there exists a valuation w on K, called the composition of v with u, with residue field $k_w \cong k_u$ and such that the value groups form an exact sequence*

$$0 \longrightarrow \Gamma_u \longrightarrow \Gamma_w \longrightarrow \Gamma_v \longrightarrow 0. \tag{4.5}$$

Proof. In this proof we will encounter several valuations so, for example, we will write $\mathcal{O}_v$ for the valuation ring of v.

In K, we define a set $\mathcal{O}_w$ as follows:

$$\mathcal{O}_w = \mathfrak{m}_v + \pi_v^{-1}(\mathcal{O}_u).$$

Equivalently, we can also define $\mathcal{O}_w$ as:

$$x \in \mathcal{O}_w \iff (v(x) > 0) \ \vee \ (v(x) = 0 \nrightarrow u(\pi_v(x)) \geq 0).$$

From these definitions, one can easily check that $\mathcal{O}_w$ is indeed a valuation ring. We let w be the corresponding valuation.

For the maximal ideal and unit group we get

$$\mathfrak{m}_w = \mathfrak{m}_v + \pi_v^{-1}(\mathfrak{m}_u) \qquad \text{and} \qquad \mathcal{O}_w^* = \pi_v^{-1}(\mathcal{O}_u^*).$$

To prove that the sequence (4.5) is exact, we start from (4.4) applied to v:

$$1 \longrightarrow k_v^* \xrightarrow{\pi_v^{-1}} K^*/(1+\mathfrak{m}_v) \xrightarrow{v} \Gamma_v \longrightarrow 0. \tag{4.6}$$

We use the following general statement: if $1 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 1$ is a short exact sequence of abelian groups and G is a subgroup of A, then $1 \longrightarrow A/G \xrightarrow{\alpha} B/\alpha(G) \xrightarrow{\beta} C \longrightarrow 1$ is well-defined and exact (in the non-abelian case, the statement still holds if $\alpha(G)$ is a normal subgroup of B). We apply this to (4.6) and the subgroup $\mathcal{O}_u^*$ of k_v^*, noting that $1+\mathfrak{m}_v$ is contained in $\pi_v^{-1}(\mathcal{O}_u^*)$ since $\pi_v(\mathfrak{m}_v) = \{0\}$. Therefore, the following sequence is also exact:

$$1 \longrightarrow k_v^*/\mathcal{O}_u^* \xrightarrow{\pi_v^{-1}} K^*/\pi_v^{-1}(\mathcal{O}_u^*) \xrightarrow{v} \Gamma_v \longrightarrow 0.$$

Now (4.2) says that $k_v^*/\mathcal{O}_u^* \cong \Gamma_u$, and similarly $K^*/\pi_v^{-1}(\mathcal{O}_u^*) = K^*/\mathcal{O}_w^* \cong \Gamma_w$, so the above sequence is isomophic to (4.5).

We now compute the residue field of w from the definition:

$$k_w = \mathcal{O}_w \Big/ \mathfrak{m}_w = \big(\mathfrak{m}_v + \pi_v^{-1}(\mathcal{O}_u)\big) \Big/ \big(\mathfrak{m}_v + \pi_v^{-1}(\mathfrak{m}_u)\big).$$

The $\mathfrak{m}_v$ in the numerator becomes trivial, therefore

$$k_w = \pi_v^{-1}(\mathcal{O}_u) \Big/ \big(\mathfrak{m}_v + \pi_v^{-1}(\mathfrak{m}_u)\big) \cap \pi_v^{-1}(\mathcal{O}_u) = \pi_v^{-1}(\mathcal{O}_u) \Big/ \pi_v^{-1}(\mathfrak{m}_u).$$

Since π_v is surjective, $\pi_v^{-1}(\mathcal{O}_u)/\pi_v^{-1}(\mathfrak{m}_u)$ is canonically isomorphic to $\mathcal{O}_u/\mathfrak{m}_u$, the residue field of u. This proves that $k_w \cong k_u$. □

Definition 4.11. Let Γ be a $\mathbb{Z}$-module. For a prime $p \in \mathbb{N}$, we say that Γ is *p-divisible* if every $x \in \Gamma$ can be written as py, with $y \in \Gamma$. In other words, if $p\Gamma = \Gamma$. We call a $\mathbb{Z}$-module *divisible* if it is p-divisible for every prime p.

For composite valuations, with the notations of Proposition 4.10, one can prove that Γ_w is p-divisible if and only if both Γ_u and Γ_v are p-divisible. This follows from the exact sequence (4.5), combined with the fact that the groups are torsion-free.

Definition 4.12. Let Γ be a $\mathbb{Z}$-module. An element $g \in \Gamma$ is called *even* if $g \in 2\Gamma$, otherwise g is called *odd*.

Note that odd elements exist if and only if Γ is not 2-divisible. Unlike in $\mathbb{Z}$, it is no longer true that the sum of two odd elements is even.

4.3 Quadratic forms

In this section, we give some very basic definitions about quadratic forms.

Definition 4.13. A *quadratic form* Q over a field K is a polynomial over K in any number of variables, which is homogeneous of degree two.

In the case that $\operatorname{char} K \neq 2$ (for us this will always be the case), we can do a linear variable transformation such that Q becomes of the form

$$Q(x_1, x_2, \ldots, x_n) = a_1 x_1^2 + \cdots + a_n x_n^2 \qquad (a_i \in K).$$

We abbreviate this as $Q = \langle a_1, \ldots, a_n \rangle$. In what follows, we will always work with quadratic forms in the latter notation.

We define two operators on quadratic forms: the *orthogonal sum* ($\perp$) and *tensor product* ($\otimes$). Let $Q_1 = \langle a_1, a_2, \ldots, a_n \rangle$ and $Q_2 = \langle b_1, b_2, \ldots, b_m \rangle$. Then

$$Q_1 \perp Q_2 = \langle a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m \rangle,$$
$$Q_1 \otimes Q_2 = \langle a_1 b_1, a_1 b_2, \ldots, a_1 b_m, a_2 b_1, a_2 b_2, \ldots, a_2 b_m, \ldots, a_n b_1, a_n b_2, \ldots, a_n b_m \rangle.$$

With these operators, the space of quadratic forms over K becomes a semiring. In the special case of multiplying by a one-dimensional quadratic form, we get $\langle c \rangle \otimes \langle a_1, \ldots, a_n \rangle = \langle ca_1, \ldots, ca_n \rangle$ for $c \in K^*$.

A quadratic form $\langle a_1, \ldots, a_n \rangle$ is called *isotropic* over K if and only if there exist $z_1, \ldots, z_n \in K$, not all zero, such that $a_1 z_1^2 + \cdots + a_n z_n^2 = 0$. Otherwise, the quadratic form is called *anisotropic*.

An important special class of quadratic forms are the *Pfister forms*. These are the quadratic forms which can be written as

$$\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle \otimes \cdots \otimes \langle 1, a_n \rangle.$$

The following propoposition will be crucial to prove Main Theorem 4.19. It gives a way to reduce isotropicity of quadratic forms from a valued field K to the residue field k, provided that the value group is not 2-divisible. For discrete valuations this is well known, see [Lam05, VI.1.9].

Proposition 4.14. *Let K be a field with a valuation $v : K^* \twoheadrightarrow \Gamma$, and let k be its residue field. Assume* $\operatorname{char} k \neq 2$. *Let $T \in K$ have odd valuation (i.e. $v(T) \notin 2\Gamma$). Consider two quadratic forms $Q_1 = \langle a_1, \ldots, a_n \rangle$ and $Q_2 = \langle b_1, \ldots, b_m \rangle$ over K, such that all a_i's and b_j's have valuation 0. If $Q_1 \perp (\langle T \rangle \otimes Q_2)$ is isotropic over K, then either Q_1 or Q_2 is isotropic over the residue field k.*

Proof. If $Q_1 \perp (\langle T\rangle \otimes Q_2)$ is isotropic over K, we can find $x_1, \dots, x_n, y_1, \dots, y_m \in K$, not all zero, such that

$$a_1x_1^2 + \cdots + a_nx_n^2 + T(b_1y_1^2 + \cdots + b_my_m^2) = 0. \tag{4.7}$$

Consider the element from $\{x_1^2, \dots, x_n^2, Ty_1^2, \dots, Ty_m^2\}$ with minimal valuation. This element is not necessarily unique, but an element from $\{x_1^2, \dots, x_n^2\}$ cannot have the same valuation as an element from $\{Ty_1^2, \dots, Ty_m^2\}$, since $v(T)$ is odd.

This gives us two cases. In the first case, an element from $\{x_1^2, \dots, x_n^2\}$ has minimal valuation, and without loss of generality we may assume that it is x_1^2. Then we know that $v(x_i) \geq v(x_1)$ and $v(Ty_i^2) > v(x_1^2)$. We divide (4.7) by x_1^2:

$$a_1 + a_2\left(\frac{x_2}{x_1}\right)^2 \cdots + a_n\left(\frac{x_n}{x_1}\right)^2 + T\left(b_1\left(\frac{y_1}{x_1}\right)^2 + \cdots + b_n\left(\frac{y_m}{x_1}\right)^2\right) = 0.$$

Since we have $v(T(y_i/x_1)^2) > 0$, all the terms with T disappear if we go to the residue field. Then we get

$$a_1 + a_2\left(\frac{x_2}{x_1}\right)^2 \cdots + a_m\left(\frac{x_n}{x_1}\right)^2 = 0 \qquad (\text{over } k)$$

and this proves that Q_1 is isotropic over k.

In the second case, the valuation of Ty_i^2 is minimal. But if we divide (4.7) by T we get

$$b_1y_1^2 + b_2y_2^2 + \cdots + b_my_m^2 + \frac{1}{T}(a_1x_1^2 + a_2x_2^2 \cdots + a_nx_n^2) = 0.$$

With a reasoning analogous to the first case, we will find that Q_2 is isotropic over k. □

If $Q_1 = Q_2$, we can formulate the proposition as follows:

Corollary 4.15. *Let K be a field with a valuation $v : K^* \twoheadrightarrow \Gamma$, and let k be its residue field. Assume* $\operatorname{char} k \neq 2$. *Let $T \in K$ have odd valuation. Consider a quadratic form $Q = \langle a_1, \dots, a_n\rangle$ over K, such that all a_i's have valuation* 0. *If $\langle 1, T\rangle \otimes Q$ is isotropic over K, then Q is isotropic over the residue field k.*

It is easy to see that the converse of this proposition and corollary holds for henselian fields: if K is henselian, and either Q_1 or Q_2 is isotropic over the residue field, then $Q_1 \perp (\langle T\rangle \otimes Q_2)$ is isotropic over K.

4.4 Denef's method

Consider an elliptic curve E defined over a field K of characteristic zero. Such a curve can be defined by an affine equation of the form $Y^2 = f(X) = X^3 + aX^2 + bX + c$, where $f(X)$ has only simple zeros. There is exactly one point at infinity, which will be denoted by $\mathbf{0}$. It would lead us too far to explain the theory of elliptic curves here, the necessary background is in [Sil86].

Consider the rational function field $K(Z)$. Over $K(Z)$ we can define the following quadratic twist of E (sometimes called the *Manin–Denef curve*):

$$\mathcal{E} : f(Z)Y^2 = f(X).$$

Consider a point $(X, Y) \in \mathcal{E}(K(Z))$. We claim that such a point can be seen as a morphism from E to itself (morphism as a curve, $\mathbf{0}$ does not have to be mapped to $\mathbf{0}$). Define the action of $(X, Y) \in \mathcal{E}(K(Z))$ as follows:

$$\begin{aligned} (X, Y) : E(K) &\to E(K) \\ (x, y) &\mapsto (X(x), Y(x)y). \end{aligned} \tag{4.8}$$

One can easily check that this is a well-defined morphism on $E(K)$. The identity is given by $(Z, 1)$, and we denote its multiples $n \cdot (Z, 1)$ with $(\mathrm{X}_n, \mathrm{Y}_n) \in \mathcal{E}(K(Z))$. This determines the rational functions $\mathrm{X}_n, \mathrm{Y}_n \in K(Z)$, which obviously depend on the elliptic curve E.

The curve $\mathcal{E}$ was first used by Denef to prove existential undecidability for the field $\mathbb{R}(Z)$ (see [Den78a]). The proof is based on the following theorem, where $\mathrm{End}_K(E)$ stands for the group of endomorphisms of E defined over K and $E[2](K)$ stands for the group of K-rational points on E having order dividing 2.

Theorem 4.16 (Denef)**.** *Let K be a field of characteristic zero and let $E : Y^2 = f(X)$ be an elliptic curve over K. Consider the curve $\mathcal{E}$ with equation $f(Z)Y^2 = f(X)$, defined over the rational function field $K(Z)$. Then $\mathcal{E}(K(Z))$ is isomorphic to $\mathrm{End}_K(E) \oplus E[2](K)$. Under this isomorphism, the action* (4.8) *translates to an action of $(\phi, T) \in \mathrm{End}_K(E) \oplus E[2](K)$ on E by mapping $P \in E(K)$ to $\phi(P) + T$.*

Proof. This follows from the proof of [Den78a, Lemma 3.1]. □

In our applications, we will take a curve without complex multiplication (i.e. $\mathrm{End}(E) \cong \mathbb{Z}$). Then $\mathcal{E}(K(Z)) \cong \mathbb{Z} \oplus E[2](K)$, hence $2 \cdot \mathcal{E}(K(Z)) \cong \mathbb{Z}$. This is how we will make our model of $\mathbb{Z}$ over $K(Z)$.

4.5 Elliptic curve 40a3

In this chapter, we will work exclusively with one particular elliptic curve, namely

$$E : Y^2 = f(X) := X^3 - 2X + 1. \tag{4.9}$$

This is curve "40a3" according to Cremona's classification [Crem], it has no complex multiplication. It will be important that $(0, \pm 1)$ are 4-torsion points with $2 \cdot (0, \pm 1) = (1, 0)$. The curve was specifically chosen for this reason.

Proposition 4.17. *For the elliptic curve E, the rational functions $\mathrm{X}_n, \mathrm{Y}_n \in \mathbb{Q}(Z)$ introduced in Section 4.4 satisfy*

$$\mathrm{X}_{4n} = \frac{1}{4n^2} Z^{-2} + O(Z^{-1}), \tag{4.10}$$

$$\mathrm{Y}_{4n} = \frac{-1}{8n^3} Z^{-3} + O(Z^{-2}). \tag{4.11}$$

Proof. This is a matter of simple computation by induction on n, using the formulas for adding points on an elliptic curve in Weierstrass form. These computations are straightforward, the details are in Appendix A. □

One thing which is easy to see is that X_{4n} and Y_{4n} must have negative valuations. Indeed, the point $(0, 1) \in E(\mathbb{Q})$ is 4-torsion, hence $(\mathrm{X}_4(0), \mathrm{Y}_4(0)) = (\infty, \infty)$. This means that X_4 and Y_4 (and also X_{4n} and Y_{4n}) have poles at 0.

Corollary 4.18. *Let K be a valued field with valuation v and residue field k, with $\operatorname{char} K = \operatorname{char} k = 0$. Let (X, Y) be a point of $E(K)$ with $v(X) > 0$. Then, for all $n \in \mathbb{Z} \setminus \{0\}$, the x-coordinate of the point $4n \cdot (X, Y)$ has valuation $-2v(X)$ and the y-coordinate has valuation $-3v(X)$.*

Proof. Write (U, V) for the point $4n(X, Y)$, we have to prove that $v(U) = -2v(X)$ and that $v(V) = -3v(X)$. However, the theory from Section 4.4 implies that $(U, V) = (\mathrm{X}_{4n}(X), \mathrm{Y}_{4n}(X)Y)$. Applying (4.10), we get

$$U = \mathrm{X}_{4n}(X) = \frac{1}{4n^2} X^{-2} + O(X^{-1}).$$

Now the valuation of the $O(X^{-1})$-term is at least $-v(X)$. Because $v(X) > 0$, we have that $v(1/(4n^2) \cdot X^{-2}) = -2v(X) < -v(X)$. Therefore, $v(U) = -2v(X)$. Then it follows from the elliptic curve equation $V^2 = U^3 - 2U + 1$ that V must have valuation $\frac{1}{2} v(U^3 - 2U + 1) = -3v(X)$. □

4.6 First version of the Main Theorem

Main Theorem 4.19. *Let K be a field of characteristic zero with a valuation $v : K^* \twoheadrightarrow \Gamma$. Let $\mathcal{O}$ denote the valuation ring, $\mathfrak{m}$ the maximal ideal and k the residue field. Assume that* $\operatorname{char} k = 0$*, and let F be a maximal subfield of $\mathcal{O}$ (see Propositions 4.7 and 4.8).*

Let C be an affine plane curve (possibly singular) defined over K, and let $K(C)$ be its function field. Write coordinates (Z, U) for $\mathbb{A}^2$ and let $c \in \mathcal{O}[Z, U]$ be a polynomial defining C. Write $\tilde{c} \in k[Z, U]$ for the reduction of c modulo $\mathfrak{m}$ and call $\tilde{C}$ the curve defined over k by $\tilde{c}$.

Assume the following conditions are satisfied:

(i) The value group Γ is not 2-divisible.

(ii) There is a number $q \geq 0$ such that there exists a 2^q-dimensional Pfister form with coefficients in F which is anisotropic over k and such that every 2^{q+2}-dimensional Pfister form over a finite extension of $F(Z)$ is isotropic.

(iii) The curve C has only nodes as singularities and there exists a non-singular point in $\tilde{C}(k)$, i.e. a $(\zeta, \eta) \in k \times k$ such that $\tilde{c}(\zeta, \eta) = 0$, but $\frac{\partial \tilde{c}}{\partial Z}(\zeta, \eta) \neq 0$ or $\frac{\partial \tilde{c}}{\partial U}(\zeta, \eta) \neq 0$.

Then there exists a diophantine model of $\mathbb{Z}$ over $K(C)$ in some finite ring language $\mathcal{L}$.

Remark. By Proposition 2.9, this implies the negative answer to HTP for $K(C)$ in the language $\mathcal{L}$. However, as Eisenträger notes in the introduction of [Eis07], this undecidability can be "trivial" in some cases, simply because of certain constants appearing in the language. To explain this better, consider Tarski's proof that the theory of $\mathbb{R}$ in the language $\{0, 1, +, \cdot, \leq\}$ admits quantifier elimination (see [Tar51]). This immediately implies decidability for first-order sentences (in particular, diophantine equations). However, if we add some non-computable real α to the language, we still have quantifier elimination, but then atomic formulas (such as $2\alpha^3 - \alpha + 4 \geq 0$) are no longer decidable. This shows that undecidability can sometimes be a simple consequence of the chosen language. However, for a general field K, it is not at all clear what the 'natural' language should be. In Section 4.10, we will discuss which constants will appear in $\mathcal{L}$. In the concrete examples in Section 4.11, we will see that this language is quite natural.

To prove the Main Theorem, we would like to use the method with two elliptic curves, as applied on $\mathbb{C}(Z_1, Z_2)$ by Kim and Roush ([KR92]) and on function fields of curves over $\mathbb{C}(Z_1)$ by Eisenträger ([Eis04]). The big obstacle however is that K might be much bigger than $F(Z_1)$; it could be that there is no rank one (or even finite rank) elliptic curve over K.

Note that the Main Theorem is about the field $K(C)$ and not about the curve C. So we are allowed to alter C as long as we preserve the function field. Geometrically, we are considering the curve C up to birational morphisms.

The rest of this section will be the proof of Main Theorem 4.19. We start with some lemmas. In the first lemma, we will change the equation of the curve C to get a new curve with the same function field and some extra properties.

By condition (iii), we know that $\tilde{C}$ (the reduction of C) has a non-singular k-rational point. We write $\tilde{D}$ for the k-irreducible component of $\tilde{C}$ containing this point. Since the non-singular points on $\tilde{C}(\bar{k})$ form a Zariski-open subset, there will only be finitely many singular points in $\tilde{C}(\bar{k})$. In what follows, we will not use that $\tilde{D}$ is irreducible (in any sense), just that almost every point is non-singular.

We write $\tilde{d} \in k[Z,U]$ for the equation of $\tilde{D}$, and $\tilde{e} \in k[Z,U]$ for the equation of the other components. Then $\tilde{c} = \tilde{d}\tilde{e}$ with $\gcd(\tilde{d}, \tilde{e}) = 1$. The fact that almost every point of $\tilde{D}$ is non-singular on $\tilde{C}$ implies that $\tilde{d}$ has no factors occuring with multiplicity more than one.

Lemma 4.20. *Let $\mathbb{Q}^+ := \{\zeta \in \mathbb{Q} \mid \zeta > 0\}$. We can find a new curve C in $\mathbb{A}^2(K)$ with the same function field, such that the following holds for all lines $\tilde{L}$ of the form $Z = \zeta$ with $\zeta \in \mathbb{Q}^+$ (writing coordinates (Z,U) for $\mathbb{A}^2$, these lines are parallel to the U-axis):*

1. *$\tilde{L}(\bar{k})$ and $\tilde{D}(\bar{k})$ have an odd number of intersection points in the affine plane.*
2. *All these intersections have intersection multiplicity equal to 1.*
3. *All these intersection points are non-singular points of $\tilde{C}$.*

Algebraically, these conditions mean "$\deg_U \tilde{d}(\zeta, U)$ is odd" and "$\frac{\partial \tilde{c}}{\partial U}(\zeta, \eta) \neq 0$ whenever $\tilde{d}(\zeta, \eta) = 0$". These have to be satisfied for all $\zeta \in \mathbb{Q}^+$.

Remark. If $K(C) \cong K(Z)$ is a rational function field, we can simply take the line $U = 0$ as the curve C. This immediately satisfies the lemma.

Proof. Take the projective closure of $\tilde{D}$, in projective coordinates $(Z : U : \Omega)$. If $\tilde{D}$ has even degree, then take a non-singular point on $\tilde{D}(k)$ and change coordinates such that this point becomes $(0 : 1 : 0)$, i.e. the point at infinity in the direction of the U-axis. If $\tilde{D}$ has odd degree, then change coordinates such that $(0 : 1 : 0)$ does not lie in $\tilde{D}(k)$. Now go back to the affine plane by setting $\Omega = 1$. The transformations we described were over the residue field k. This means of course that we actually apply a coordinate change over K, such that we have the desired transformation in the reduction. Since affine curves have the same function field as their projective closures, these operations did not change the field $K(C)$.

Write $\tilde{d}$ as a polynomial in U: $\tilde{d} = \sum_{i=0}^{n} d_i U^i$, with $d_i \in k[Z]$. Because of the coordinate change, n will be odd.

To prove the lemma, we will show that there are only finitely many lines $Z = \zeta$ with $\zeta \in \bar{k}$ which do not satisfy the three conditions in the statement. Then we consider the finitely many bad ζ's in $\mathbb{Q}$. We can always find a translation $Z \mapsto Z + z$ for some $z \in \mathbb{Q}$ such that all these bad ζ's become negative.

So we consider a line $Z = \zeta$ with $\zeta \in \bar{k}$. If ζ is not a zero of d_n, then $\deg_U \tilde{d}(\zeta, U) = n$ is odd. This excludes finitely many lines.

To prove the other conditions, note that

$$\frac{\partial \tilde{c}}{\partial U} = \frac{\partial(\tilde{d}\tilde{e})}{\partial U} = \frac{\partial \tilde{d}}{\partial U}\tilde{e} + \tilde{d}\frac{\partial \tilde{e}}{\partial U}.$$

But $\tilde{d}(\zeta, \eta) = 0$ for every intersection point (ζ, η), so $\frac{\partial \tilde{c}}{\partial U} = \frac{\partial \tilde{d}}{\partial U}\tilde{e}$.

Common zeros of $\tilde{d}(Z, U)$ and $\tilde{e}(Z, U)$ correspond to the intersections of $\tilde{D}$ with another component of $\tilde{C}$. There can only be finitely many such intersections, the lines $Z = \zeta$ through those points must be excluded.

Next, we look at common zeros of $\tilde{d}(Z, U)$ and $\frac{\partial \tilde{d}}{\partial U}(Z, U)$. For a fixed $Z = \zeta$, such a zero exists if and only if $\Delta_U \tilde{d}(\zeta, U) = 0$, where Δ_U denotes the discriminant w.r.t. the variable U. Now $\Delta_U \tilde{d}(Z, U) \in k[Z]$. If we exclude the roots of this discriminant, then $\tilde{d}(\zeta, U)$ and $\frac{\partial \tilde{d}}{\partial U}(\zeta, U)$ have no common zero. Since $\tilde{D}(\bar{k})$ has only finitely many singular points, it cannot have any components occuring with multiplicity > 1, in other words $\tilde{d}$ has no factors with multiplicity > 1. So, $\Delta_U \tilde{d}(Z, U)$ cannot be the zero polynomial. Therefore, we again only excluded finitely many lines.

In the end, we find that $\tilde{d}(Z, U)$ and $\frac{\partial \tilde{c}}{\partial U}(Z, U)$ have no common zero. □

Example 4.21. We illustrate this lemma with an example over $k = \mathbb{R}$. Let $\tilde{C}$ be the curve given by

$$\tilde{c}(Z,U) = 45Z^6 - 60Z^5U - 9Z^5 + 20Z^4U^2 + 12Z^4U - 36Z^4 \\ - 4Z^3U^2 + 48Z^3U - 7Z^2U^2 - 12ZU^3 + 4U^4 = 0. \quad (4.12)$$

We have a non-singular $\mathbb{R}$-point $(1,0)$. The equation (4.12) factors as follows:

$$(5Z^4 - Z^3 - 4Z^2 + U^2)(3Z - 2U)^2 = 0. \quad (4.13)$$

We see that $(1,0)$ lies on the degee 4 component, so that component is $\tilde{D}$, defined by $\tilde{d}(Z,U) = 5Z^4 - Z^3 - 4Z^2 + U^2$. We see that $\tilde{e} = \tilde{c}/\tilde{d} = (3Z-2U)^2$. The curve $\tilde{D}$ has even degree, but $(0:1:0)$ is not a point of $\tilde{D}$, so we have to transform $\tilde{D}$ such that $(1:0:1)$ becomes $(0:1:0)$. We do this with the following linear transformation of $\mathbb{P}^2$:

$$\begin{pmatrix} Z \\ U \\ \Omega \end{pmatrix} = \begin{pmatrix} 0 & 1 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} Z' \\ U' \\ \Omega' \end{pmatrix}.$$

The equation (4.13) transforms to

$$(Z'^2U'^2 - 9U'^3 + 23U'^2 - 19U' + 5)(-2Z' + 3U' - 3)^2 = 0.$$

Writing $\tilde{d}'$ for the first factor, we see that the U'-degree of $\tilde{d}'$ is 3, which is odd.

We now check which lines parallel to the U'-axis we have to exclude: First of all, there are singular points: the point $(0,1)$ is a singular point of $\tilde{D}'$, and the points $(-1/2, 2/3)$ and $(7/2, 10/3)$ are on the intersection of $\tilde{D}'$ with the other component, hence they are singular points of $\tilde{C}'$. This excludes the lines $Z' = 0$, $Z' = -1/2$ and $Z' = 7/2$.

Next, we have to compute when $Z' = \zeta$ is a tangent line of $\tilde{D}'$. This happens when $\Delta_U \tilde{d}'(\zeta, U) = 0$. One can compute that

$$\Delta_U \tilde{d}'(\zeta, U) = -\zeta^2(2\zeta - 1)(2\zeta + 1)(5\zeta^2 + 256).$$

Therefore, we have to exclude the five lines $Z' = 0$, $Z' = \pm 1/2$ and $Z' = \pm 16/\sqrt{-5}$. Now all lines which were not excluded, will have exactly three intersections with $\tilde{D}'$, all of them transversal. The largest Z'-coordinate for an exceptional line in $\mathbb{A}^2(\mathbb{Q})$ is $7/2$. If we do the translation $Z' = Z'' + 4$, then no exceptional line $Z'' = \zeta$ will have $\zeta \in \mathbb{Q}^+$.

After this lemma, we continue with the proof of the Main Theorem. Take an element $T \in K$ such that $v(T)$ is positive and odd (this is possible because of (i)). We will identify $\mathbb{Z}$ with a subgroup of Γ by sending 1 to $v(T)$. An ordered $\mathbb{Z}$-module is always torsion-free, so the map $\mathbb{Z} \hookrightarrow \Gamma : n \mapsto nv(T)$ is an embedding of ordered $\mathbb{Z}$-modules. In what follows, we will write for example "$v(X) = -3$", instead of "$v(X) = -3v(T)$".

Recall that we defined the elliptic curve E with equation $Y^2 = f(X) = X^3 - 2X + 1$. Let

$$A_\lambda := \lambda(T + T^2 Z) \quad \text{and} \quad B_\mu := \mu T^{-2} Z.$$

Here λ and μ are parameters in $\mathbb{Q}^+$, which will be fixed later. In Lemma 4.23 below, we will apply Moret-Bailly's result from [MB05]. In order to do this, the functions $A_1 = T + T^2 Z$ and $B_1 = T^{-2} Z$ must be admissible, as in [MB05, Definition 1.5.2]. A function $G : C \to \mathbb{P}^1$ is called *admissible* if

1. G has no ramification index ≥ 3 (the ramification is simple).
2. G is étale above ∞ and the branch points of $\pi : E \to \mathbb{P}^1$.
3. There is some finite set Q of points of C such that every point of Q is a zero of G.

Lemma 4.22. *We can apply a projective transformation $t \in \mathrm{PGL}(3, \mathbb{Q}[T]_{(T)})$ on C such that $t \equiv \mathrm{id} \bmod T$ and such that A_1 and B_1 are admissible for this transformed C.*

Remark. This t will not change anything in the reduction, so Lemma 4.20 remains true.

Proof. In this proof, we consider C as a projective plane curve, with coordinates (Z, U, Ω) for $\mathbb{P}^2$.

First of all, we want that the first condition of admissible is satisfied for the function Z. This function simply projects $\mathbb{P}^2$ onto $\mathbb{P}^1$ from the point $(0 : 1 : 0)$, so the choice of Z is given by the choice of the point with coordinates $(0 : 1 : 0)$. Since A_1 and B_1 can be seen as elements of $\mathrm{PGL}(2, K)$ composed with Z, the first condition of admissible will also be satisfied for A_1 and B_1 if it is satisfied for Z.

Consider all lines which intersect C in some point where the intersection multiplicity is greater than 2. These are the lines tangent to a flex of C and also

the tangent lines in the nodes of C. Since we are working in characteristic zero, there are a finite number of these lines. Therefore, there must be a point of the form $(\alpha T : 1 : \beta T)$ with $\alpha, \beta \in \mathbb{Q}$ which is not on any of these lines. Then the transformation

$$Z = Z' + \alpha TU, \qquad U = U', \qquad \Omega = \Omega' + \beta TU$$

puts the point $(\alpha T : 1 : \beta T)$ in $(0 : 1 : 0)$. Now the function Z will not have any ramification with index greater than 2.

Now we fixed the point $(0 : 1 : 0)$, but we can still apply $\mathrm{PGL}(2, \mathbb{Q}[T]_{(T)})$ on the $\mathbb{P}^1$ where our functions map to. The conditions that A_1 and B_1 are étale above ∞ and the branch points of π are equivalent to saying that Z is étale above some finite set of points of $\mathbb{P}^1$. Since there are only finitely many points of $\mathbb{P}^1$ where Z is not étale, we have enough freedom to find a projective transformation of $\mathbb{P}^1$ which maps the bad points outside of some finite set, and which is the identity modulo T.

Finally, for A_1 resp. B_1 we simply take a singleton Q, one point of C with Z/Ω equal to $-T^{-1}$ resp. 0. □

Define $L := K(C)(\sqrt{f(A_\lambda)}, \sqrt{f(B_\mu)})$, which will turn out to be a degree 4 extension of $K(C)$. In what follows, we assume that we have T and Z in our ring language. A_λ and B_μ are elements of $\mathbb{Q}(T, Z)$ and f has coefficients in $\mathbb{Q}$, therefore $f(A_\lambda)$ and $f(B_\mu)$ are diophantine and we can make a diophantine model of L in $K(C)^4$.

Lemma 4.23. *There exist λ and μ in $\mathbb{Q}^+$ such that*

$$P_1 := (A_\lambda, \sqrt{f(A_\lambda)}) \quad \textit{and} \quad P_2 := (B_\mu, \sqrt{f(B_\mu)})$$

are points on $E(L)$ satisfying the following conditions:

1. *Let $\mathbb{Z}_0 = \mathbb{Z} \setminus \{0\}$. The sets of multiples $\mathbb{Z}_0 \cdot P_1$ and $\mathbb{Z}_0 \cdot P_2$ are diophantine over L.*
2. *P_1 and P_2 are independent points on $E(L)$.*
3. *Let $\bar{K}$ be an algebraic closure of K. Then the field $\bar{K}(C)(\sqrt{f(A_\lambda)}, \sqrt{f(B_\mu)})$ is a degree 4 extension of $\bar{K}(C)$.*

Proof. Define the following quadratic twist of E, over the rational function field $\bar{K}(\xi)$:

$$\mathcal{E}_\xi : f(\xi)Y^2 = f(X). \tag{4.14}$$

Because $\operatorname{char} \bar{K} = 0$ and E does not have complex multiplication, Theorem 4.16 says that the group $\mathcal{E}_\xi(\bar{K}(\xi))$ is equal to $\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$, where the $\mathbb{Z}$-component is generated by the point $(\xi, 1)$.

Unfortunately, we want to work over $\bar{K}(C)$ instead of $\bar{K}(\xi)$. However, consider the quadratic twist

$$\mathcal{E}_{A_\lambda} : f(\lambda(T + T^2Z))Y^2 = f(X)$$

depending on the parameter λ, which a priori can be chosen in $\bar{K}^*$. Because of Lemma 4.22, the function $T + T^2Z$ is admissible. Therefore, we can use Moret-Bailly's result (see [MB05, Theorem 1.8 and Section 10]), stating that $\mathcal{E}_\xi(\bar{K}(\xi)) \cong \mathcal{E}_{A_\lambda}(\bar{K}(C))$ for all λ in a Hilbert subset $\mathcal{S}$ of $\mathbb{Q}$ (see [FJ86, Section 11.1] for the definition of Hilbert sets, intuitively $\mathcal{S}$ contains 'most' elements of $\mathbb{Q}$). The isomorphism is given by mapping ξ to $A_\lambda = \lambda(T + T^2Z)$. Note that we always have an embedding $\mathcal{E}_\xi(\bar{K}(\xi)) \hookrightarrow \mathcal{E}_{A_\lambda}(\bar{K}(C))$, but in general this is not surjective.

From the definition of Hilbert sets, it follows that $-\mathcal{S} = \{-x \mid x \in \mathcal{S}\}$ and $\mathcal{S} \cap (-\mathcal{S})$ are also Hilbert sets. But $\mathbb{Q}$ is a Hilbertian field, which means that all Hilbert subsets are infinite. Therefore, it is impossible that $\mathcal{S}$ contains only nonpositive numbers. So, there exists a $\lambda \in \mathcal{S} \cap \mathbb{Q}^+$. We choose one such λ which will remain fixed for the rest of the proof. For simplicity in notation, we will omit the index and write "A" instead of "A_λ".

By combining these results of Denef and Moret-Bailly, we know that $\mathcal{E}_A(\bar{K}(C))$ is generated by the point $(A, 1)$ and 2-torsion. But the point $(A, 1)$ is defined over $K(C)$, so $\mathcal{E}_A(K(C))$ is also generated by $(A, 1)$ and 2-torsion (it does not matter at all how much 2-torsion is $K(C)$-rational).

The set of multiples of $(A, 1)$ on $\mathcal{E}_A(K(C))$ is diophantine because it can be written as

$$\big\{2 \cdot \mathcal{E}_A(K(C))\big\} \cup \big\{(A, 1) + 2 \cdot \mathcal{E}_A(K(C))\big\}.$$

Since the $K(C)$-rational points of $\mathcal{E}_A$ are simply given by the elliptic curve equation, the above set is diophantine. We will use the affine equation, so we cannot get the point at infinity, we only get $\mathbb{Z}_0 \cdot (A, 1)$. The coefficients of the equation for $\mathcal{E}_A$ lie in $\mathbb{Q}(T, Z)$, so we just need T and Z in the language to make the diophantine definition.

Over $L = K(C)(\sqrt{f(A)}, \sqrt{f(B)})$, the curves $\mathcal{E}_A$ and E become isomorphic:

$$\begin{aligned} \theta : \mathcal{E}_A(L) &\xrightarrow{\sim} E(L) \\ (x, y) &\mapsto (x, y\sqrt{f(A)}). \end{aligned} \tag{4.15}$$

Now we can diophantinely define the set of non-zero multiples of $P_1 = (A, \sqrt{f(A)})$ on $E(L)$ by taking the multiples of $(A, 1)$ on $\mathcal{E}_A(L)$ and simply multiplying the y-coordinate by $\sqrt{f(A)}$.

The proof that $\mathbb{Z}_0 \cdot P_2$ is diophantine is completely analogous (fixing $\mu \in \mathbb{Q}^+$), which finishes the first point of the lemma.

To prove 2, assume we would have a relation $mP_1 = nP_2$, then also $4mP_1 = 4nP_2$. Since the x-coordinate of P_1 is A, it follows from Section 4.4 that the x-coordinate of $4mP_1$ equals $\mathrm{X}_{4m}(A)$. Similarly, the x-coordinate of $4nP_2$ is $\mathrm{X}_{4n}(B)$. So, we have $\mathrm{X}_{4m}(A) = \mathrm{X}_{4n}(B)$. If we specialize the variable Z to T^4, we get $\mathrm{X}_{4m}(\lambda T + \lambda T^6) = \mathrm{X}_{4n}(\mu T^2)$. But Corollary 4.18 says that $v(\mathrm{X}_{4m}(\lambda T + \lambda T^6)) = -2v(\lambda T + \lambda T^6) = -2$ and $v(\mathrm{X}_{4n}(\mu T^2)) = -2v(\mu T^2) = -4$. This is the contradiction we were looking for.

Finally, let us prove point 3. Assume that $\sqrt{f(A)}$ is in $\bar{K}(C)$. Since $(0, 1)$ is a 4-torsion point on $E(K)$, it follows that $(0, 1/\sqrt{f(A)})$ would be a 4-torsion point on $\mathcal{E}_A(\bar{K}(C))$. But by our construction, $\mathcal{E}_A(\bar{K}(C))$ has only 2-torsion points and points of infinite order. Therefore, the point $(0, 1/\sqrt{f(A)})$ cannot be $\bar{K}(C)$-rational, hence $[\bar{K}(C)(\sqrt{f(A)}) : \bar{K}(C)] = 2$.

Now assume that $\sqrt{f(B)} \in \bar{K}(C)(\sqrt{f(A)})$. Then we can write $\sqrt{f(B)} = R + S\sqrt{f(A)}$ with R and S in $\bar{K}(C)$. Squared, we get

$$f(B) = R^2 + S^2 f(A) + 2RS\sqrt{f(A)} \in \bar{K}(C).$$

But $\sqrt{f(A)}$ does not lie in $\bar{K}(C)$, so we have two possibilities: either $R = 0$ or $S = 0$. If $S = 0$, then $\sqrt{f(B)} \in \bar{K}(C)$, which we can exclude as in the previous paragraph.

If $R = 0$, then $\sqrt{f(B)}$ is a $\bar{K}(C)$-multiple of $\sqrt{f(A)}$. Then $(B, \sqrt{f(B)}/\sqrt{f(A)})$ would be a point on $\mathcal{E}_A(\bar{K}(C))$. This means that 2 times this point is a multiple of $(A, 1)$. Applying the isomorphism θ from (4.15), we find that $2 \cdot P_2$ is a multiple of P_1, in contradiction with the independence of P_1 and P_2. □

We have to make a technical remark about affine versus projective points. We just defined $\mathbb{Z}_0 \cdot P_i$, the affine multiples of P_i. However, we would also like to work

with the point at infinity. So we work with projective coordinates in $\mathbb{P}^2(L) = (L^3\backslash\{0\})/L^*$. The equivalence relation between different coordinates for the same point is clearly diophantine. Now $\mathbb{Z}\cdot P_i = (0:1:0)\cup\{(x:y:1) \mid (x,y)\in\mathbb{Z}_0\cdot P_i\}$.

On $\mathbb{P}^2(L)$, there is a partial function $y : \mathbb{P}^2(L) \dashrightarrow L : (X:Y:W) \mapsto Y/W$. For points at infinity, y is not defined, so we have to be careful not to allow such points as arguments of y (see Section 2.6 on how we can do this). The function y is clearly diophantine where it is defined.

We define a model of $\mathbb{Z}\times\mathbb{Z}$ inside $E(L)\subset\mathbb{P}^2(L)$ by mapping $(n,r)\in\mathbb{Z}\times\mathbb{Z}$ to $4nP_1 + rP_2$ (the 4 is there for technical reasons).

In $\mathbb{Z}\times\mathbb{Z}$ we define the unary predicates $\mathcal{Z}_1$, $\mathcal{Z}_2$ and the binary relation $\|$:

$$\begin{aligned} \mathcal{Z}_1(n,r) &\iff n=0,\\ \mathcal{Z}_2(n,r) &\iff r=0,\\ (m,t)\parallel(n,r) &\leftrightarrow (\exists k\in\mathbb{Z})(mk=n \ \wedge\ tk=r). \end{aligned} \tag{4.16}$$

Let $|$ be the restriction of $\|$ to the case $t=1$, in other words

$$(m,t)\mid(n,r) \iff t=1 \ \wedge\ (\exists k\in\mathbb{Z})(mk=n \ \wedge\ k=r) \iff t=1 \ \wedge\ n=mr.$$

Eisenträger proves (see [Eis04, Propositions 2.1 and 2.2]) that there exists a diophantine model of $\mathbb{Z}$ with addition and multiplication inside the structure $\langle\mathbb{Z}\times\mathbb{Z},+,\mathcal{Z}_1,\mathcal{Z}_2,|\rangle$. Hence, it suffices to construct a diophantine model of this structure over $K(C)$.

We can diophantinely define $\mathcal{Z}_1$ in our model, it is just $\mathbb{Z}\cdot P_2$. Similarly, $\mathcal{Z}_2$ is given by $4\mathbb{Z}\cdot P_1$. The addition in $\mathbb{Z}\times\mathbb{Z}$ is the addition on the elliptic curve E. This is given by rational functions, hence is diophantine. To finish the proof of Main Theorem 4.19, we need a diophantine definition of the weak divisibility relation $|$.

Theorem 4.24. *Let Q be a 2^q-dimensional anisotropic Pfister form over k with coefficients in F, which exists by assumption. Then $n = mr$ if and only if $4nP_1 + rP_2 = 0$ or*

$$\langle 1, y(4mP_1+P_2)\rangle\otimes\langle 1, y(4nP_1+rP_2)\rangle\otimes Q \tag{4.17}$$

is isotropic over L.

Remark. Because P_1 and P_2 are independent, $4nP_1+rP_2=0$ is the only possible occurance of a point at infinity in formula (4.17). So, if we interpret the "or" in the Lemma as short-circuiting (see Section 2.6), everything is well-defined.

A quadratic form being isotropic is a diophantine condition, if all the coefficients are diophantine. Therefore, the coefficients of Q must be expressible in the language.

Proof. The statement clearly holds if $n = r = 0$. For the rest of the proof, we assume this is not the case.

Assume $n = mr$ and set $P_3 := 4mP_1 + P_2$. Now (4.17) becomes

$$\langle 1, y(P_3)\rangle \otimes \langle 1, y(rP_3)\rangle \otimes Q. \tag{4.18}$$

The coefficients of this quadratic form live in $F(y(P_3), y(rP_3))$, which is a subfield of $L_0 := F(x(P_3), y(P_3))$. This latter field is isomorphic to the function field of E over F, so we can use condition (ii) from the Theorem. The Pfister form (4.18) is 2^{q+2}-dimensional, therefore it is isotropic over $L_0 \subseteq L$.

Conversely, assume that (4.17) is isotropic over L. Let $s := n - mr$ and suppose that $s \neq 0$ in order to find a contradiction. Putting $P_3 := 4mP_1 + P_2$, we rewrite (4.17) as

$$\langle 1, y(P_3)\rangle \otimes \langle 1, y(4sP_1 + rP_3)\rangle \otimes Q. \tag{4.19}$$

For the rest of this proof, we will take the henselisation K^{H} as a base field, instead of K. Take any extension of the valuation v to K^{H}. This extension is immediate, this means that the value group Γ and the residue field k remain the same. The henselisation is an algebraic extension, and K is relatively algebraically closed in L (because $K(C)$ is a function field over C and because of Lemma 4.23, item 3). Define

$$M := L \otimes_K K^{\mathrm{H}} = K^{\mathrm{H}}(C)(\sqrt{f(A)}, \sqrt{f(B)}).$$

Since (4.19) is isotropic over L, it is certainly isotropic over M. We just need the field M in this proof, we certainly do not need a diophantine interpretation of M.

The points $4mP_1$ and P_2 have the following coordinates:

$$4mP_1 = \big(\mathrm{X}_{4m}(A), \mathrm{Y}_{4m}(A)\sqrt{f(A)}\big), \tag{4.20}$$

$$P_2 = (B, \sqrt{f(B)}). \tag{4.21}$$

Consider $H(Z) := \mathrm{X}_{4m}(A) - B \in K^{\mathrm{H}}(Z)$, we want to find a simple zero of this rational function. Here, we see K^{H} as the constant field, and Z as the variable. Write the rational function $\mathrm{X}_{4m}(\xi)$ as $R_{4m}(\xi)/S_{4m}(\xi)$ with $R_{4m}(\xi), S_{4m}(\xi) \in \mathbb{Q}[\xi]$

and $\gcd(R_{4m}(\xi), S_{4m}(\xi)) = 1$. We choose $R_{4m}(\xi)$ to have constant term 1, then it follows from Proposition 4.17 that the lowest degree term of $S_{4m}(\xi)$ is $4m^2\xi^2$. Keeping in mind that $A = \lambda T(1 + TZ)$ and that $\lambda, \mu \in \mathbb{Q}$, the following is a polynomial with coefficients in $\mathbb{Q}[T] \subseteq \mathcal{O}$:

$$G(Z) := S_{4m}(A)H(Z) = R_{4m}(A) - \frac{S_{4m}(A)}{T^2}\mu Z. \tag{4.22}$$

We would like to apply Hensel's Lemma to find a root of $G(Z)$ in K^{H}. Modulo T, we have the following:

$$R_{4m}(A) \equiv R_{4m}(0) = 1 \mod T \qquad \text{and} \qquad S_{4m}(A)/T^2 \equiv 4m^2\lambda^2 \mod T.$$

Note that none of these depend on Z. Therefore $G(Z) \equiv 1 - 4m^2\lambda^2\mu Z \mod T$, which is linear, so it has a simple zero modulo T. Hensel's Lemma proves that $G(Z)$ has a simple root $\gamma \in K^{\mathrm{H}}$ with

$$\gamma \equiv \frac{1}{4m^2\lambda^2\mu} \mod T. \tag{4.23}$$

In order for γ to be a zero of the rational function $H(Z) = G(Z)/S_{4m}(A)$, it must not be a zero of $S_{4m}(A)$. But $S_{4m}(A) \equiv 4m^2\lambda^2T^2 \bmod T^3$, which does not depend on Z, so $S_{4m}(A)$ cannot have any roots of valuation zero (all roots must have negative valuation).

Define w as the discrete valuation on $K^{\mathrm{H}}(Z)$ at the point $Z = \gamma$. This means that $w(Z - \gamma) = 1$ and that w is trivial on K^{H}. Clearly, the residue field is K^{H}. We found γ as a simple zero of $H(Z) = \mathrm{X}_{4m}(A) - B$, therefore

$$w(\mathrm{X}_{4m}(A) - B) = 1. \tag{4.24}$$

We defined w as a valuation on $K^{\mathrm{H}}(Z)$, but we would like to extend w to the finite extension $M = K^{\mathrm{H}}(C)(\sqrt{f(A)}, \sqrt{f(B)})$. The residue field of $K^{\mathrm{H}}(Z)$ for w is equal to K^{H}. This field has itself a valuation v. While we are extending w to M, we will keep track of how v extends to a valuation on the new residue field of M for w.

We use the notation $\overline{x}$ for the reduction of x with respect to w, this gives a map $K^{\mathrm{H}}(Z) \dashrightarrow K^{\mathrm{H}}$. Similarly, we write $\tilde{x}$ for the reduction of x with respect to v, this gives a map $K^{\mathrm{H}} \dashrightarrow k$. As we extend v and w to finite extensions, we keep the same notation.

First, we extend w to $K^{\mathrm{H}}(C)$. This means we have to adjoin U, where U is a root of $c(Z,U)=0$. To find an extension of w to $K^{\mathrm{H}}(C)$, we must find a root of $c(\gamma,U)$ in K^{H}.

Let $\tilde{D}$ be as in Lemma 4.20 and let $\tilde{d}(Z,U)\in k[Z,U]$ be the polynomial defining $\tilde{D}$. From equation (4.23), we see that $\tilde{\gamma}\in\mathbb{Q}^+$. Applying Lemma 4.20, we know that the polynomial $\tilde{d}(\tilde{\gamma},U)\in k[U]$ has odd degree. Let $\tilde{\delta}\in\bar{k}$ be a zero of $\tilde{d}(\tilde{\gamma},U)$ of odd degree. Let e denote this degree, i.e. $e=[k(\tilde{\delta}):k]$. Now apply Proposition 4.4. This means we get an extension $K^{\mathrm{H}'}/K^{\mathrm{H}}$ with $[K^{\mathrm{H}'}:K^{\mathrm{H}}]=e$ and that we can extend v to $K^{\mathrm{H}'}$ such that $k(\tilde{\delta})$ is the new residue field. Since algebraic extensions of henselian fields are again henselian (see [EP05, Section 4.1]), $K^{\mathrm{H}'}$ is also henselian.

Recall that $\tilde{c}(\tilde{\gamma},\tilde{\delta})=0$. The second and third condition of Lemma 4.20 ensure that $\frac{\partial\tilde{c}(\tilde{\gamma},U)}{\partial U}(\tilde{\delta})\neq 0$. Therefore, we can apply Hensel's Lemma to lift $\tilde{\delta}$ to a $\delta\in K^{\mathrm{H}'}$ with $c(\gamma,\delta)=0$. Because δ reduces to $\tilde{\delta}$, it follows that $[K^{\mathrm{H}}(\delta):K^{\mathrm{H}}]\geq[k(\tilde{\delta}):k]=e$. But $K^{\mathrm{H}}(\delta)$ is a subextension of $K^{\mathrm{H}'}$, with $[K^{\mathrm{H}'}:K^{\mathrm{H}}]=e$. We conclude that $K^{\mathrm{H}'}=K^{\mathrm{H}}(\delta)$ and that $[K^{\mathrm{H}}(\delta):K^{\mathrm{H}}]=e$ is odd.

All this means that w can be extended to $K^{\mathrm{H}}(C)=K^{\mathrm{H}}(Z)[U]/c(Z,U)$ in such a way that the residue field becomes $K^{\mathrm{H}}(\delta)$, and such that v extended to $K^{\mathrm{H}}(\delta)$ has residue field $k(\tilde{\delta})$.

Now we just have to adjoin $\sqrt{f(A)}$ and $\sqrt{f(B)}$ to $K^{\mathrm{H}}(C)$. From (4.23) it follows that $v(\gamma)=0$, hence $v(\overline{A})=v(\lambda(T+\gamma T^2))=1$ and $v(\overline{B})=v(\mu\gamma T^{-2})=-2$. It follows that

$$\begin{aligned} v(f(\overline{A})) &= v(\overline{A}^3-2\overline{A}+1)=0,\\ v(f(\overline{B})) &= v(\overline{B}^3-2\overline{B}+1)=-6. \end{aligned}$$

These valuations are even, so $f(\overline{A})$ and $f(\overline{B})$ are squares in $K^{\mathrm{H}}(\delta)$. After extending w to $M=K^{\mathrm{H}}(C)(\sqrt{f(A)},\sqrt{f(B)})$, the residue field remains $K^{\mathrm{H}}(\delta)$ and we do not need to change v.

Equation (4.24) implies that $\overline{4mP_1}$ and $\overline{P_2}$ have the same x-coordinate (an element of K^{H}). This means that there are 2 possibilities: either they are the same point (equal y-coordinates), or they are opposite points (opposite y-coordinates). But M has an involution σ mapping $\sqrt{f(B)}$ to $-\sqrt{f(B)}$, while fixing $K^{\mathrm{H}}(C)(\sqrt{f(A)})$ (this follows from Lemma 4.23). On the curve, $\sigma(P_1)=P_1$ but $\sigma(P_2)=-P_2$. We want that $\overline{4mP_1}$ and $\overline{P_2}$ are opposite points. If this is not the case, replace w by the valuation $w\circ\sigma$. Then the points become opposite and

$$w\left(\mathrm{Y}_{4m}(A)\sqrt{f(A)}-\sqrt{f(B)}\right)=0. \tag{4.25}$$

We will now determine $w(y(P_3))$ using the fact that $P_3 = 4mP_1 + P_2$. We can do this with (4.24) and (4.25). The elliptic curve addition formula says that

$$\begin{aligned} x(P_3) &= -x(4mP_1) - x(P_2) + \left(\frac{y(4mP_1) - y(P_2)}{x(4mP_1) - x(P_2)}\right)^2 \\ &= -\underbrace{\mathrm{X}_{4m}(A)}_{w=0} - \underbrace{B}_{w=0} + \underbrace{\left(\frac{\mathrm{Y}_{4m}(A)\sqrt{f(A)} - \sqrt{f(B)}}{\mathrm{X}_{4m}(A) - B}\right)^2}_{w=2(0-1)=-2}. \end{aligned}$$

We see that $w(x(P_3)) = -2$. Now $y(P_3)^2 = x(P_3)^3 - 2x(P_3) + 1$ has valuation -6, therefore $w(y(P_3)) = -3$. This means that $\overline{P_3}$ is the point at infinity.

So far we determined the w-valuation of the coefficient $y(P_3)$ in the quadratic form (4.19). We claim that $w(y(4sP_1 + rP_3)) = 0$. If $w(y(4sP_1 + rP_3)) < 0$, then $\overline{4sP_1 + rP_3} = 4s\overline{P_1} = 0$; if $w(y(4sP_1 + rP_3)) > 0$, then the y-coordinate of $\overline{4sP_1 + rP_3} = 4s\overline{P_1}$ is zero, hence $4s\overline{P_1}$ is 2-torsion. In any case, if $w(y(4sP_1 + rP_3)) \neq 0$, then $\overline{P_1}$ is a torsion point on E (here we need $s \neq 0$). But E has coefficients in $\mathbb{Q}$, hence all torsion is algebraic over $\mathbb{Q}$. The x-coordinate of $\overline{P_1}$ is $\overline{A} = \lambda(T + \gamma T^2)$ with $v(\overline{A}) = 1$, therefore $\overline{A}$ cannot be algebraic over $\mathbb{Q}$ and $\overline{P_1}$ cannot be torsion.

We conclude $w(y(P_3)) = -3$ and $w(y(4sP_1 + rP_3)) = 0$, therefore we can apply Corollary 4.15 on (4.19) to find that

$$\langle 1, y(4s\overline{P_1})\rangle \otimes Q. \tag{4.26}$$

is isotropic over $K^{\mathrm{H}}(\delta)$.

The point $\overline{P_1}$ has x-coordinate $\overline{A} = \lambda(T + \gamma T^2)$ with $v(\overline{A}) = 1$. Corollary 4.18 implies that $v(y(4s\overline{P_1})) = -3$, which is odd. We can apply Corollary 4.15 on (4.26) to conclude that Q is isotropic over the residue field $k(\tilde{\delta})$ of v. Since $[k(\tilde{\delta}) : k]$ is odd, it follows from Springer's Theorem (see [Lam05, VII.2.7]) that Q is also isotropic over k. But Q was chosen to be anisotropic over k, so we have found a contradiction. □

4.7 Galois Cohomology

Thanks to Voevodsky's work on the Milnor Conjectures (see [Pfi00] for a survey), we can replace condition (ii) in Main Theorem 4.19 by a simple condition on the 2-cohomological dimensions of F and K.

We will recall some definitions and propositions from Galois cohomology, we refer to [Ser02] for background and proofs.

Throughout this section, K will be a characteristic zero field. Let $H^q(K, \mu_p)$ denote the q-th cohomology group of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ with coefficients in the group $\mu_p \subset \bar{K}$ of p-th roots of unity.

Definition 4.25. Let p be a prime number. The *p-cohomological dimension* of $\mathrm{Gal}(\bar{K}/K)$, denoted by $\mathrm{cd}_p(K)$, is the smallest integer q such that

$$H^{q+1}(L, \mu_p) = 0 \qquad \text{for all finite extensions } L \text{ of } K.$$

If there is no such q, then we define $\mathrm{cd}_p(K) = \infty$.

Serre gives a different definition of p-cohomological dimension, but ours is equivalent, see the proof of [Ser02, II.§ 2.3 Prop. 4].

It turns out that we can describe how these cohomological dimensions behave with respect to field extensions:

Proposition 4.26. *Let K be a characteristic zero field with $\mathrm{cd}_p(K) < \infty$, and let L be any extension of K. Then*

$$\mathrm{cd}_p(L) \leq \mathrm{cd}_p(K) + \mathrm{tr.\,deg}(L/K). \tag{4.27}$$

If L is finitely generated over K, the equality holds. In particular, cohomological dimensions remain the same under finite extensions, provided that $\mathrm{cd}_p(K) < \infty$.

Proof. See [Ser02, II.§ 4.2 Prop. 11]. □

The Milnor Conjectures, now proven by Voevodsky and others, provide a connection between Pfister forms over K and the Galois cohomology groups $H^q(K, \mu_2)$. We need the following formulation of the Milnor Conjectures:

Theorem 4.27. *Let I denote the fundamental ideal in the Witt ring $W(K)$ (for definitions, see for example [Lam05, Chapter II]). Then $I^q/I^{q+1} \cong H^q(K, \mu_2)$.*

Using this, we know the possible dimensions of anisotropic Pfister forms over K:

Corollary 4.28. *There exists an anisotropic 2^q-dimensional Pfister form over K if and only if $H^q(K, \mu_2) \neq 0$.*

Proof. If $H^q(K, \mu_2) = 0$, then $I^q/I^{q+1} = 0$. This implies that $I^q = I^{q+1}$, hence also $I^{q+1} = I^{q+2}$ and so on. The Arason–Pfister Hauptsatz (see [Lam05, X.5.1]) implies that $\bigcap_{n\geq 0} I^n = 0$, therefore $I^q = 0$. But I^q is generated by the 2^q-dimensional Pfister forms, therefore all 2^q-dimensional Pfister forms are hyperbolic (hence isotropic).

Conversely, if $H^q(K, \mu_2) \neq 0$, then $I^q \neq 0$. Therefore, there exists a non-hyperbolic Pfister form Q of dimension 2^q. But for Pfister forms, non-hyperbolic is the same as anisotropic. □

We can now change condition (ii) from Main Theorem 4.19:

Proposition 4.29. *Main Theorem 4.19 is still true if we replace condition* (ii) *by: the* 2*-cohomological dimensions of F and k are equal and finite. We can do this without loss of generality.*

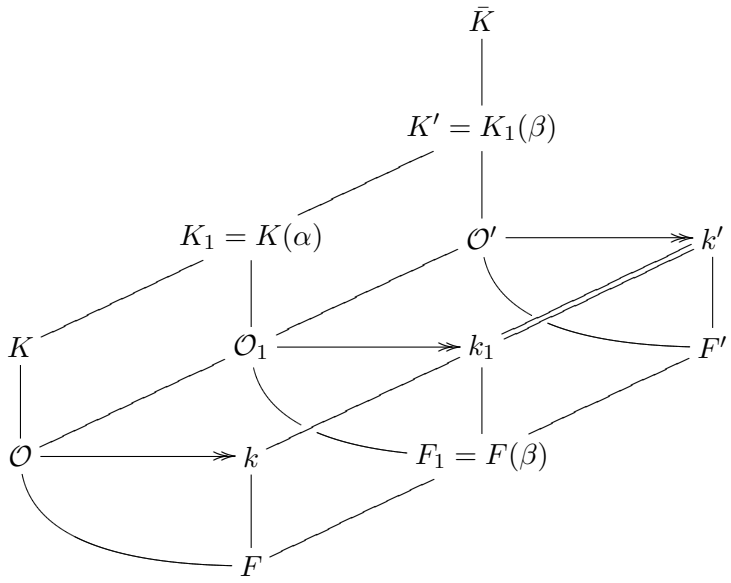
Before giving the proof, we explain better what this means. This does *not* mean that condition (ii) from the Main Theorem is equivalent to "$\mathrm{cd}_2(F) = \mathrm{cd}_2(k) < \infty$", it just means that we can also prove the Main Theorem with the new condition instead of (ii). When we say "without loss of generality", it means that "$\mathrm{cd}_2(F) = \mathrm{cd}_2(k) < \infty$" always holds if (ii) is satisfied.

Proof. Assume $q := \mathrm{cd}_2(F) = \mathrm{cd}_2(k)$ is finite. By definition of cohomological dimension, there is a finite extension k_1/k for which $H^q(k_1, \mu_2) \neq 0$.

By Proposition 4.4, we can find an extension K_1/K such that v extended to K_1 has residue field k_1 and value group Γ. Fix an algebraic closure $\bar{K}$ of K, and choose $\alpha \in \bar{K}$ such that $K_1 = K(\alpha)$.

Since $H^q(k_1, \mu_2) \neq 0$, Corollary 4.28 implies that there exists an anisotropic 2^q-dimensional Pfister form Q over k_1. The coefficients of Q are algebraic over F, since k_1/k and k/F are algebraic extensions.

By Proposition 4.7, we can identify k_1 with a subfield of the henselisation K_1^{H}, containing F. Let $F_1 \subseteq k_1$ be the field obtained by adjoining the coefficients of Q to F. This is a finite extension of F, so we can choose $\beta \in F_1$ such that $F_1 = F(\beta)$. Then we define $K' := K_1(\beta)$. Since K' is a subfield of K_1^{H}, the residue field $k' := k_1$ and value group Γ will remain the same if we take an extension of v to K'. Let $F' \supseteq F_1$ be a maximal subfield of K' on which v is trivial.



We claim that the conditions of Main Theorem 4.19 are satisfied for K', with maximal subfield F' and residue field k'. The value group stayed the same, so condition (i) is satisfied.

We have the quadratic form Q which is anisotropic over k'. We made sure that the coefficients of Q lie in $F_1 \subseteq F'$, by adjoining them.

By construction, k' is a finite extension of k, so we have $\mathrm{cd}_2(F) = \mathrm{cd}_2(k') = q$. Since k'/F' and F'/F are algebraic, we must also have $\mathrm{cd}_2(F') = q$.

On the other hand, from $\mathrm{cd}_2(F') = q$ it follows that $\mathrm{cd}_2(F'(Z)) = q + 1$. By definition of cohomological dimension, we have $H^{q+2}(L, \mu_2) = 0$ for all finite extensions L of $F'(Z)$, which implies that all Pfister forms over L of dimension 2^{q+2} will be isotropic.

Using Main Theorem 4.19, this would prove undecidability for $K'(C)$. However, $[K' : K]$ is finite, therefore one can make a model of $K'(C)$ in $K(C)^{[K':K]}$. So undecidability for a finite extension $K'(C)$ implies undecidability for $K(C)$.

Conversely, suppose that condition (ii) holds. The second part of this condition says that $H^{q+2}(L, \mu_2) = 0$ for all finite extentions L of $F(Z)$. This implies $\mathrm{cd}_2(F(Z)) \leq q + 1$, and Proposition 4.26 gives $\mathrm{cd}_2(F) = \mathrm{cd}_2(F(Z)) - 1 \leq q$.

The existence of an anisotropic 2^q-dimensional Pfister form over k implies that $H^q(k, \mu_2) \neq 0$ and $\mathrm{cd}_2(k) \geq q$. But k is algebraic over F, so by Proposition 4.26 we have the inequalities

$$q \leq \mathrm{cd}_2(k) \leq \mathrm{cd}_2(F) \leq q$$

which imply $\mathrm{cd}_2(F) = \mathrm{cd}_2(k) = q$, hence finite. □

Note that the inequality "$\mathrm{cd}_2(F) \geq \mathrm{cd}_2(k)$" is always satisfied, because k is an algebraic extension of F (see Proposition 4.8). So, it suffices to check that $\mathrm{cd}_2(F) \leq \mathrm{cd}_2(k)$.

4.8 The curve C

We can also generalize condition (iii) of Main Theorem 4.19.

Proposition 4.30. *In condition* (iii) *from Main Theorem 4.19, it suffices if there is a non-singular point of $\tilde{C}$ over $\bar{k}$ (so it does not have to be k-rational).*

Proof. We use the formulation of condition (ii) as in Proposition 4.29, so we assume that $\mathrm{cd}_2(F) = \mathrm{cd}_2(k) < \infty$.

Assume we have a point $P \in \tilde{C}(\bar{k})$. Then P is actually defined over a finite extension k' of k. Using Proposition 4.4, we can extend v to K'/K with residue field k'. Let $\mathcal{O}$ be the valuation ring of K', and F' its maximal subfield.

We will now apply Main Theorem 4.19 for K'. Condition (i) is still satisfied, Γ did not change. Since all extensions are finite, $\mathrm{cd}_2(F') = \mathrm{cd}_2(F)$ and $\mathrm{cd}_2(k') = \mathrm{cd}_2(k)$, therefore $\mathrm{cd}_2(F') = \mathrm{cd}_2(k') < \infty$, proving the new condition (ii). Condition (iii) is satisfied because now P is k'-rational. Main Theorem 4.19 gives undecidability for $K'(C)$, hence also for $K(C)$. □

4.9 Second version of the Main Theorem

Applying the previous two sections, we can reformulate Main Theorem 4.19 as follows:

Main Theorem 4.31. *Let K be a field of characteristic zero with a valuation $v : K^* \twoheadrightarrow \Gamma$. Let $\mathcal{O}$ denote the valuation ring, $\mathfrak{m}$ the maximal ideal and k the residue field. Assume that* $\operatorname{char} k = 0$*, and let F be a maximal subfield of $\mathcal{O}$ (see Propositions 4.7 and 4.8).*

Let C be an affine plane curve (possibly singular or reducible) defined over K, and let $K(C)$ be its function field. Write coordinates (Z, U) for $\mathbb{A}^2$ and let $c \in \mathcal{O}[Z, U]$ be a polynomial defining C. Write $\tilde{c} \in k[Z, U]$ for the reduction of c modulo $\mathfrak{m}$ and call $\tilde{C}$ the curve defined over k by $\tilde{c}$.

Assume the following conditions are satisfied:

(i) The value group Γ is not 2-divisible.

(ii) The 2-cohomological dimensions of F and k are equal and finite.

(iii) The curve C has only nodes as singularities and there exists a non-singular point in $\tilde{C}(\bar{k})$.

Then there exists a diophantine model of $\mathbb{Z}$ over $K(C)$ in some finite ring language $\mathcal{L}$.

4.10 Language

So far, we have not discussed the language for which we have undecidability. We start from the ring language $\mathcal{L}_R = \{+, \cdot, 0, 1\}$ and add some constant symbols to make our diophantine model of $\mathbb{Z} \times \mathbb{Z}$. There are four places in the proof where we need extra constants:

1. To define the extension L and the points P_1 and P_2 on $E(L)$, the language must at least contain T and Z. For T any element from K having positive odd valuation will do, Z is simply a transcendental element over K generating $K(Z)$.

2. To apply Proposition 4.29, we might need to extend our field K to a finite extension $K' = K(\alpha, \beta)$. So we need constants in our language for the minimal polynomial of α and β. From the proof of Proposition 4.29, it can be seen that these are algebraic over F, so it suffices to have constants for elements of F. However, in many cases the finite extension in Proposition 4.29 is not necessary, then we do not need extra constants.

3. Similarly, we might need a finite extension to apply Proposition 4.30.
4. Finally, we have to express the coefficients of the quadratic form Q. These will be algebraic over F.

In general it is not always clear which are the constants that have to be added to the language. In concrete examples, one can usually specify the language, see some of the examples below.

As Eisenträger notes in the introduction of [Eis07], the undecidability of diophantine equations over $K(C)$ follows trivially if the language contains uncomputable numbers.

4.11 Examples

In this section we give some examples for which our theorem can be applied. We recover many known results.

Example 4.32. If F is a characteristic zero field with $\mathrm{cd}_2(F)$ finite, then HTP for the 2-variable rational function field $F(T, Z)$ has a negative answer, for some finite ring language.

Proof. Apply the theorem with $K = F(T)$ and v the valuation associated to T, which has residue field F. □

Example 4.33. If F is a number field, then HTP for $F(T, Z)$ has a negative answer for the language $\{+, \cdot, 0, 1, T, Z\}$ (this was already in [KR95]).

Proof. From the Theorem of Hasse–Minkowski it follows that all 4-dimensional quadratic forms over a non-real (i.e. -1 is a sum of squares) number field are isotropic. On the other hand, over a real field there are anisotropic Pfister forms of arbitrarily high dimension: take $\langle 1, 1\rangle \otimes \langle 1, 1\rangle \otimes \ldots$. Using the results mentioned in Section 4.7, this implies that $\mathrm{cd}_2(F) = \infty$ if F is a real number field, and $\mathrm{cd}_2(F) = 2$ otherwise. So in the non-real case we just have to apply Example 4.32.

If F is real, this does not work. However, we can always take a finite extension F'/F such that F' is no longer real. For instance, $F' = F(\sqrt{-1})$ always works. Then Main Theorem 4.31 gives undecidability for $F'(T, Z)$, which implies undecidability for $F(T, Z)$. □

Example 4.34. HTP for $\mathbb{R}(T, Z)$ and $\mathbb{C}(T, Z)$ has a negative answer for the language $\{+, \cdot, 0, 1, T, Z\}$ (for $\mathbb{R}$, this was already in [Den78a], for $\mathbb{C}$ this was already in [KR92]).

Example 4.35. Let $K(C)$ be a field for which the conditions of the Theorem are satisfied, and let K' be a finite extension of K. Then HTP for $K'(C)$ has a negative answer.

Proof. Let v be an extension of the given valuation to K'. The new value group Γ' might be larger than the original Γ, but in any case $[\Gamma' : \Gamma]$ is finite, so Γ' will still be non-2-divisible.

The maximal subfield F' of $\mathcal{O}' \subseteq K'$ will be a finite extension of F, so $\mathrm{cd}_2(F') = \mathrm{cd}_2(F)$. The same is true for the new residue field k', so $\mathrm{cd}_2(F') = \mathrm{cd}_2(k') < \infty$.

The conditions on the curve are independent of the base field, so they remain satisfied. □

Example 4.36. Let F be a field with $\mathrm{cd}_2(F)$ finite. Then HTP for $F((T))(Z)$ has a negative answer, for some finite ring language.

Proof. Let $K = F((T))$ and let v be the discrete valuation at T. The valuation ring $\mathcal{O} = F[[T]]$ has F as maximal subfield. This way, the conditions for Main Theorem 4.31 are satisfied. □

This example can be generalized somewhat:

Example 4.37. Let K be a field for which the conditions of Main Theorem 4.31 are satisfied, with $\mathcal{L}$ the needed language (see Section 4.10). Let K' be any extension of K, contained in the completion $\hat{K}$. Then HTP for $K'(Z)$ has a negative answer for the language $\mathcal{L}$.

Proof. Extend the given valuation v to a valuation on K'. The residue field will remain the same. In general, the maximal subfield F' of $\mathcal{O}'$ could be an extension of F, but still contained in k. Since $F \subseteq F' \subseteq k$ and k/F is algebraic, the extensions k/F' and F'/F are also algebraic. Hence

$$q = \mathrm{cd}_2(k) \leq \mathrm{cd}_2(F') \leq \mathrm{cd}_2(F) = q$$

from which $\mathrm{cd}_2(F') = \mathrm{cd}_2(k) = q$.

We do not have to extend the language, because F does not change at all, and because we can take the same T and Z. □

Example 4.38. Let F be a characteristic zero field for which $\mathrm{cd}_2(F)$ is finite. Let $\{X_i\}_{i\in I}$ be a set of algebraically independent variables, with $\#I \geq 2$. Then HTP for $F(\{X_i\}_{i\in I})$ has a negative answer for some finite ring language.

Proof. Choose a well-ordering $\preccurlyeq$ on I, this is a total order on I such that every non-empty subset of I has a minimal element (the existence of well-orderings is equivalent to the axiom of choice). I itself also has a smallest element i_0, let $Z := X_{i_0}$. We also define $I_0 := I \setminus \{i_0\}$ and $K := F(\{X_i\}_{i\in I_0})$. We have to prove undecidability for $F(\{X_i\}_{i\in I}) = K(Z)$.

Let

$$\Gamma := \bigoplus_{i\in I_0} \mathbb{Z}. \qquad \text{(direct sum of abelian groups)}$$

Clearly, Γ is not 2-divisible (here we use $\#I_0 \geq 1$).

We make this into an ordered abelian group $\Gamma, \leq$ by using the lexicographic ordering coming from $I, \preccurlyeq$. In detail: let $\gamma = \oplus_{i\in I_0}\gamma_i \in \Gamma$. Assume $\gamma \neq 0$ and look at the set $J \subseteq I_0$ of all i such that $\gamma_i \neq 0$. Let j_0 be the minimal element from J, and define $0 < \gamma$ if and only if $0 < \gamma_{j_0}$.

To define a valuation $v : K^* \twoheadrightarrow \Gamma$, we let v be trivial on F and define v for monomials:

$$v\left(\prod_{i\in I_0} X_i^{m_i}\right) = \bigoplus_{i\in I_0} m_i \in \Gamma.$$

Then the valuation of a polynomial is defined to be the minimal valuation of its terms. Finally, for rational functions we take $v(x/y) = v(x) - v(y)$ as usual. One can check that this does indeed satisfy the axioms of a valuation, and that the residue field is F (hence $\mathrm{cd}_2(k) = \mathrm{cd}_2(F) < \infty$). □

Example 4.39. If K admits a valuation with non-2-divisible value group Γ, and K contains an algebraically closed field, then HTP for $K(Z)$ has a negative answer for $\mathcal{L} = \{+, \cdot, 0, 1, T, Z\}$. Here T stands for an element with odd valuation.

Proof. Remark that K cannot be algebraically closed itself, because all valuations on algebraically closed fields have divisible value groups.

Write v for the given valuation. Since we will encounter other valuations, we write an index with the residue field, value group, ... For example, we write F_v for the maximal subfield of $\mathcal{O}_v$, the valuation ring corresponding to v. Let C be

an algebraically closed subfield of F_v (one can always take $C = \bar{\mathbb{Q}}$, since $\bar{\mathbb{Q}}$ has no non-trivial valuations with residue characteristic zero).

C is contained in F_v, so it is also contained in k_v. We would like to define a valuation u on k_v with C as residue field, we do this as follows: Choose a transcendence basis $\{X_i\}_{i\in I}$ for k_v over C. As in Example 4.38, we can construct a valuation u on $C(\{X_i\}_{i\in I})$ with residue field C. Extend this valuation to k_v. This extension is algebraic, so the new residue field is an algebraic extension of C, hence C itself.

Let w be the composite valuation of v and u, as defined in Proposition 4.10. We would like the apply the Main Theorem on K with valuation w. Since Γ_v is not 2-divisible, the exact sequence (4.5) ensures that Γ_w is not 2-divisible either.

We claim that C is a subfield of $\mathcal{O}_w$. We know that $C^* \subseteq \mathcal{O}_u^*$, and since π_v is an isomorphism on C, we also have $C^* \subseteq \pi_v^{-1}(\mathcal{O}_u^*) = \mathcal{O}_w^*$.

The residue field of w is C, so C must be a maximal subfield of $\mathcal{O}_w$. We have $\mathrm{cd}_2(C) = \mathrm{cd}_2(C) = 0$, so we can apply Main Theorem 4.31 with the valuation w. □

Part III

Diophantine sets over polynomial rings

Chapter 5

Polynomials over a finite field

5.1 Introduction and outline

In this chapter, we will prove

Main Theorem 5.1. *Let p be a prime, and $\mathbb{F}_q$ a finite field of characteristic p. For all $k \geq 1$, a subset of $\mathbb{F}_q[Z]^k$ is recursively enumerable if and only if it is diophantine over $\mathbb{F}_q[Z]$ in the language $\mathcal{L} = \{0, 1, +, \cdot, \alpha, Z\}$, where $\mathbb{F}_p[\alpha] = \mathbb{F}_q$.*

As far as the author knows, everything in this chapter is new, except for Denef's diophantine model of $\mathbb{F}_q[Z]$ in Section 5.2, and the well-known theory of cyclotomic polynomials in Section 5.5.

To prove this, the first thing we need is a diophantine model of $\mathbb{N}$ over $\mathbb{F}_q[Z]$ (see Section 5.2), by mapping a natural number $n \geq 0$ to the polynomial Z^n. This model is strongly based on Denef's model for $\mathbb{Z}$ over $\mathbb{F}_q[Z]$ (see [Den79]). We will do the construction of our model more generally, namely for rings $\mathcal{R}[Z]$ with $\mathcal{R}$ having characteristic $p > 0$. This is the only place in this chapter where we must distinguish between odd and even characteristic.

Given this model of $\mathbb{N}$ over $\mathbb{F}_q[Z]$, the proof will proceed in three steps:

1. Enumerate $\mathbb{F}_q[Z]$ as $\{P^{(0)}, P^{(1)}, P^{(2)}, \dots\}$, where $P^{(n)}$ is seen as the n-th polynomial in $\mathbb{F}_q[Z]$. Because of DPRM, it suffices to prove that the relation "$X = P^{(n)}$", with X in $\mathbb{F}_q[Z]$ and n in $\mathbb{N}$, is diophantine (see Section 3.4.1). In Section 5.6, we will give a defintion of "$X = P^{(n)}$", but it will not be diophantine.

Indeed, in the formula defining that relation, there will be a bounded universal quantifier. Such a quantifier, written $(\forall k)_{\leq d}$, means "for $k = 0, 1, \ldots, d$". Here, k and d are natural numbers, represented by Z^k and Z^d in the model. In our case, the bound will be the degree of the polynomial $P^{(n)}$ to be defined. A quantifier $(\forall k)_{\leq d}$ gives $d+1$ values for k. A polynomial of degree d has $d+1$ coefficients, so we just need to express that the degree of X is (at most) d, and that the k-th coefficient of X equals the k-th coefficient of $P^{(n)}$ for all $k \leq d$. Then X must be equal to $P^{(n)}$.

2. Elimination of the bounded universal quantifier. Given a formula with a bounded universal quantifier (and any number of existential quantifiers), we have to show that it is equivalent to a formula with only existential quantifiers. In Section 5.7, we will show how to do this, but only if we introduce a new variable W. That is, we have to work over $\mathbb{F}_q[W, Z]$, where we can prove that everything is diophantine. This extra variable gives us more freedom in our diophantine definitions.

The elimination of bounded univeral quantifiers was also one of the key ingredients in the proof of DPRM (see [Dav73, p. 252–256]). There, each of the $d+1$ formulas arising from the bounded universal quantifier $(\forall k)_{\leq d}$ is considered modulo a different large number in an arithmetic progression. Then the Chinese Remainder Theorem is used to encode these $d+1$ formulas into just one formula. Our method is also based on the Chinese Remainder Theorem, but modulo a product of certain cyclotomic polynomials, instead of numbers in an arithmetic progression. Apart from this idea of using the Chinese Remainder Theorem, there is very little in the DPRM proof which works for $\mathbb{F}_q[Z]$.

3. This already yields a proof of the fact that r.e. sets over $\mathbb{F}_q[Z]$ are diophantine over $\mathbb{F}_q[W, Z]$. However, we want them to be diophantine over $\mathbb{F}_q[Z]$. In Section 5.8, we will construct a diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$. Essential for this will be stride polynomials. A (w, s)-stride polynomial (with $0 \leq w \leq s$) is a polynomial in the $\mathbb{F}_q[Z^s]$-module spanned by $\{1, Z, Z^2, \ldots, Z^{w-1}\}$. We will prove that stride polynomials are diophantine, and use them to encode elements of $\mathbb{F}_q[W, Z]$ in $\mathbb{F}_q[Z]$. If we have this interpretation, it will follow that r.e. sets over $\mathbb{F}_q[Z]$ are actually diophantine over $\mathbb{F}_q[Z]$.

5.2 A model of $\mathbb{N}$

Let $\mathcal{R}$ be any integral domain of characteristic $p > 0$, later we will set $\mathcal{R} = \mathbb{F}_q$. In this section, we will construct a model of $\mathbb{N} = \{0, 1, 2, \ldots\}$ over $\mathcal{R}[Z]$. In this

model, $n \in \mathbb{N}$ will correspond to Z^n in $\mathcal{R}[Z]$. In [Den79], Denef constructs a model of $\mathbb{Z}$ in $\mathcal{R}[Z]$, by interpreting the integers as Chebyshev polynomials in $\mathcal{R}[Z]$. We write X_n for the n-th Chebyshev polynomial of the first kind, and Y_n for the $(n-1)$-th Chebyshev polynomial of the second kind. They satisfy $\mathrm{X}_n^2 - (Z^2-1)\mathrm{Y}_n^2 = 1$, and (up to sign), these are the only solutions to the Pell equation $X^2 - (Z^2-1)Y^2 = 1$. This is true in any polynomial ring $\mathcal{R}[Z]$, with $\mathcal{R}$ an integral domain of characteristic different from 2. In characteristic 2, we can use different polynomials, defined by a similar quadratic equation.

Even though it is possible to do the whole proof with Chebyshev polynomials, we will not use Denef's model. One reason is that Chebyshev polynomials do not work in characteristic 2, so Denef has to give a slightly different proof in that case. A second reason is that our model will be easier to work with. Number theoretically, the Chebyshev polynomials are related to the real number fields $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\cos(2\pi/n))$, while the polynomials Z^n are related to $\mathbb{Q}(\zeta_n)$. The Galois groups are $(\mathbb{Z}/n\mathbb{Z})^*/\langle -1\rangle$ resp. $(\mathbb{Z}/n\mathbb{Z})^*$, which already motivates that the latter are easier. Cyclotomic polynomials will play a very important role in this chapter (see Section 5.5).

We will construct the model for $\mathcal{R}[Z]$ where $\mathcal{R}$ is an integral domain of positive characteristic. In this chapter we will only apply it with $\mathcal{R} = \mathbb{F}_q$ a finite field. However, in Chapter 6 we will also apply it for infinite algebraic extensions of $\mathbb{F}_p$. Just like in Denef's paper, we have to make a distinction between odd and even characteristic.

5.2.1 Odd characteristic

In the case p is odd, we will use the Chebyshev polynomials $\mathrm{X}_n, \mathrm{Y}_n \in \mathbb{Z}[Z]$. These are defined by

$$(Z + \sqrt{Z^2-1})^n = \mathrm{X}_n(Z) + \sqrt{Z^2-1}\mathrm{Y}_n(Z) \qquad (n \in \mathbb{Z}).$$

Note that $(Z + \sqrt{Z^2-1})^{-1} = (Z - \sqrt{Z^2-1})$, so this definition also makes sense for negative n.

The couples $(\mathrm{X}_n, \mathrm{Y}_n)$ are solutions of the Pell equation

$$X^2 - (Z^2-1)Y^2 = 1. \tag{5.1}$$

We can see them as elements of $\mathbb{F}_p[Z] \subseteq \mathcal{R}[Z]$ by reducing the coefficients modulo p.

Facts 5.2. We list some easy facts about the Chebyshev polynomials (see for instance [Den79]). They are true in all polynomial rings of characteristic different from 2.

$$\begin{aligned} \mathrm{X}_0 &= 1, & \mathrm{Y}_0 &= 0, \\ \mathrm{X}_1 &= Z, & \mathrm{Y}_1 &= 1, \\ \mathrm{X}_{n+k} &= \mathrm{X}_n\mathrm{X}_k + (Z^2-1)\mathrm{Y}_n\mathrm{Y}_k, & \mathrm{Y}_{n+k} &= \mathrm{X}_n\mathrm{Y}_k + \mathrm{Y}_n\mathrm{X}_k, \\ \mathrm{X}_{-n} &= \mathrm{X}_n, & \mathrm{Y}_{-n} &= -\mathrm{Y}_n, \\ \deg \mathrm{X}_n &= n \quad (n \geq 0), & \deg \mathrm{Y}_n &= n-1 \quad (n \geq 1). \end{aligned}$$

Proposition 5.3 (Pell equation)**.** *Let T, X and Y be elements of $\mathcal{R}[Z]$, with T non-constant ($T \notin \mathcal{R}$). Then*

$$(\exists n \in \mathbb{Z})\big(X = \mathrm{X}_n(T) \wedge Y = \mathrm{Y}_n(T)\big) \iff (X^2 - (T^2-1)Y^2 = 1 \wedge T-1 | X-1).$$

Proof. This follows from [Den79, p. 137, (4)–(5)]. □

Proposition 5.4. *Let A and B be elements of $\mathcal{R}[Z]$ with B non-constant. Then*

$$(\exists k \in \mathbb{N})(A = B^{p^k}) \iff (\exists m \in \mathbb{Z})\big(A = \mathrm{X}_m(B)\big) \wedge (\exists n \in \mathbb{Z})\big(A+1 = \mathrm{X}_n(B+1)\big).$$

Proof. The direction "$\Longrightarrow$" follows from the fact that $\mathrm{X}_{p^k} = Z^{p^k}$, hence $\mathrm{X}_{p^k}(T) = T^{p^k}$.

Conversely, from the right hand side of the equivalence follows that

$$\mathrm{X}_m(B) + 1 = \mathrm{X}_n(B+1).$$

Considering degrees, we see that m and n have to be equal. Now the statement follows from [Den79, Lemma 2.1 6]. □

Proposition 5.5. *Let $T \in \mathcal{R}(Z)^*$ and $n \in \mathbb{Z}$. Then the following equality holds:*

$$T^n = \mathrm{X}_n\left(\frac{T+T^{-1}}{2}\right) + \frac{T-T^{-1}}{2}\mathrm{Y}_n\left(\frac{T+T^{-1}}{2}\right). \tag{5.2}$$

Proof. We prove this by induction on n, using Facts 5.2. The statement clearly holds for $n = 0$, because $\mathrm{X}_0 = 1$ and $\mathrm{Y}_0 = 0$. For n positive, we will expand the right hand side of (5.2). For ease of notation, we omit the arguments of the Chebyshev polynomials, which are always $\frac{T+T^{-1}}{2}$.

$$\begin{aligned}
&\mathrm{X}_n + \frac{T - T^{-1}}{2}\mathrm{Y}_n \\
&\quad = \mathrm{X}_1\mathrm{X}_{n-1} + \left(\left(\tfrac{T+T^{-1}}{2}\right)^2 - 1\right)\mathrm{Y}_1\mathrm{Y}_{n-1} + \tfrac{T-T^{-1}}{2}\mathrm{X}_1\mathrm{Y}_{n-1} + \tfrac{T-T^{-1}}{2}\mathrm{Y}_1\mathrm{X}_{n-1} \\
&\quad = \tfrac{T+T^{-1}}{2}\mathrm{X}_{n-1} + \tfrac{T^2-2+T^{-2}}{4}\mathrm{Y}_{n-1} + \tfrac{T^2-T^{-2}}{4}\mathrm{Y}_{n-1} + \tfrac{T-T^{-1}}{2}\mathrm{X}_{n-1} \\
&\quad = T\mathrm{X}_{n-1} + \tfrac{T^2-1}{2}\mathrm{Y}_{n-1} = T\left(\mathrm{X}_{n-1} + \tfrac{T-T^{-1}}{2}\mathrm{Y}_{n-1}\right).
\end{aligned}$$

The proposition for negative n follows by exchanging the roles of T and T^{-1}, and by the fact that $\mathrm{X}_{-n} = \mathrm{X}_n$ and $\mathrm{Y}_{-n} = -\mathrm{Y}_n$. □

This proposition also has an interpretation in complex numbers. The polynomials X_n and Y_n are exactly the polynomials appearing in the formulas for $\cos(n\theta)$ and $\sin(n\theta)$ (this can also be used as a definition of X_n and Y_n):

$$\cos(n\theta) = \mathrm{X}_n(\cos\theta) \quad \text{and} \quad \sin(n\theta) = \sin(\theta)\mathrm{Y}_n(\cos\theta).$$

If we set $T = \cos\theta + \mathrm{i}\sin\theta$, then $T^{-1} = \cos\theta - \mathrm{i}\sin\theta$, hence $(T + T^{-1})/2 = \cos\theta$ and $(T - T^{-1})/2 = \mathrm{i}\sin\theta$. Then (5.2) says that

$$\begin{aligned}
(\cos\theta + \mathrm{i}\sin\theta)^n &= \mathrm{X}_n(\cos\theta) + \mathrm{i}\sin(\theta)\mathrm{Y}_n(\cos\theta) \\
&= \cos(n\theta) + \mathrm{i}\sin(n\theta).
\end{aligned}$$

Using Proposition 5.5, we will define the set $\{T^n \mid n \in \mathbb{N}\}$. Because T^{-1} is not a polynomial, we cannot apply (5.2) directly to define T^n. Instead, we will define powers modulo a particular polynomial.

Proposition 5.6. *Let T be a non-constant polynomial in $\mathcal{R}[Z]$. Then the powers*

of T form a diophantine set:

$$(\exists n \in \mathbb{N})(A = T^n) \tag{5.3}$$
$$\Updownarrow$$
$$(\exists S, X, Y \in \mathcal{R}[Z])$$
$$(\exists k \in \mathbb{N})(S = T^{p^k}) \tag{5.4}$$
$$\wedge\ (\exists n \in \mathbb{Z})\left(X = \mathrm{X}_n\left(\tfrac{T+S}{2}\right)\ \wedge\ Y = \mathrm{Y}_n\left(\tfrac{T+S}{2}\right)\right) \tag{5.5}$$
$$\wedge\ A \equiv X + \tfrac{T-S}{2}Y \mod TS - 1 \tag{5.6}$$
$$\wedge\ A|S. \tag{5.7}$$

Proof. Suppose that $A = T^n$. Take k such that $n \leq p^k$, and let S be T^{p^k}. Set $X := \mathrm{X}_n\left(\frac{T+S}{2}\right)$ and $Y := \mathrm{Y}_n\left(\frac{T+S}{2}\right)$. This already gives (5.4), (5.5) and (5.7). Now S is the inverse of T modulo $TS-1$, so Proposition 5.5 implies (5.6).

Conversely, assume that (5.4)–(5.7) hold. From (5.5) and (5.6) it follows that $A \equiv T^m \bmod TS-1$ for a certain $m \in \mathbb{Z}$. Since $S = T^{p^k}$, we have $T^{p^k+1} \equiv 1 \bmod TS-1$. Let n be the unique integer such that $0 \leq n \leq p^k$ and $n \equiv m \bmod p^k+1$. This implies that

$$A \equiv T^n \mod TS - 1. \tag{5.8}$$

We know that $\deg A \leq \deg S = p^k \deg T$ because A divides S. But also $\deg T^n = n \deg T \leq p^k \deg T$. We see that the degrees of A and of T^n are both less than $\deg(TS-1) = (p^k+1)\deg T$. Now it follows from (5.8) that A is equal to T^n. □

5.2.2 Even characteristic

This case is analogous to the case p odd, we just need to change the equations a little. We cannot expect the usual Pell equation $X^2 - (T^2-1)Y^2 = 1$ to work in characteristic 2, so we must use a different equation.

Let α satisfy $\alpha^2 + Z\alpha + 1 = 0$. Then we define the polynomials $\mathrm{X}_n, \mathrm{Y}_n \in \mathbb{F}_2[Z] \subseteq \mathcal{R}[Z]$ as

$$\alpha^n = \mathrm{X}_n(Z) + \alpha \mathrm{Y}_n(Z).$$

These are solutions of

$$X^2 + ZXY + Y^2 = 1.$$

These polynomials X_n and Y_n have properties very analogous to the Chebyshev polynomials. We will not give any proofs since they are practically the same as in the case p odd. Again, we refer to [Den79].

Facts 5.7.

$$\begin{aligned} \mathrm{X}_0 &= 1, & \mathrm{Y}_0 &= 0, \\ \mathrm{X}_1 &= 0, & \mathrm{Y}_1 &= 1, \\ \mathrm{X}_{n+k} &= \mathrm{X}_n\mathrm{X}_k + \mathrm{Y}_n\mathrm{Y}_k, & \mathrm{Y}_{n+k} &= \mathrm{X}_n\mathrm{Y}_k + \mathrm{Y}_n\mathrm{X}_k + Z\mathrm{Y}_n\mathrm{Y}_k, \\ \mathrm{X}_{-n} &= \mathrm{X}_n + Z\mathrm{Y}_n, & \mathrm{Y}_{-n} &= \mathrm{Y}_n, \\ \deg \mathrm{X}_n &= n-2 \quad (n \geq 2), & \deg \mathrm{Y}_n &= n-1 \quad (n \geq 1). \end{aligned}$$

Proposition 5.8. *Let T, X and Y be elements of $\mathcal{R}[Z]$, with T non-constant. Then*

$$(\exists n \in \mathbb{Z})\big(X = \mathrm{X}_n(T) \ \wedge \ Y = \mathrm{Y}_n(T)\big) \iff (X^2 + ZXY + Y^2 = 1).$$

Proposition 5.9. *Let A and B be elements of $\mathcal{R}[Z]$ with B non-constant. Then*

$$\begin{aligned} &(\exists k \in \mathbb{N})(A = B^{2^k}) \iff \\ &\quad (\exists m \in \mathbb{Z})\big(A = B \cdot \mathrm{Y}_m(B)\big) \ \wedge \ (\exists n \in \mathbb{Z})\big(A + 1 = (B+1) \cdot \mathrm{Y}_n(B+1)\big). \end{aligned}$$

Proposition 5.10. *Let $T \in \mathcal{R}(Z)^*$ and $n \in \mathbb{Z}$. Then the following equality holds:*

$$T^n = \mathrm{X}_n\left(T + T^{-1}\right) + T\mathrm{Y}_n\left(T + T^{-1}\right). \tag{5.9}$$

Proposition 5.11. *Let T be a non-constant polynomial in $\mathcal{R}[Z]$. Then the powers of T form a diophantine set:*

$$\begin{aligned} &(\exists n \in \mathbb{N})(A = T^n) && (5.10) \\ &\qquad \Updownarrow \\ &(\exists S, X, Y \in \mathcal{R}[Z]) \\ &\qquad (\exists k \in \mathbb{N})(S = T^{2^k}) && (5.11) \\ &\qquad \wedge \ (\exists n \in \mathbb{Z})\,(X = \mathrm{X}_n(T+S) \ \wedge \ Y = \mathrm{Y}_n(T+S)) && (5.12) \\ &\qquad \wedge \ A \equiv X + TY \mod TS - 1 && (5.13) \\ &\qquad \wedge \ A | S. && (5.14) \end{aligned}$$

5.2.3 Addition and multiplication

We are now ready to define a diophantine model of $\mathbb{N}$ in $\mathcal{R}[Z]$. In this model, the natural number n corresponds to the polynomial Z^n. Using Proposition 5.6 (if $p > 2$) or Proposition 5.11 (if $p = 2$) with $T = Z$, we can define the *set* of

powers of Z. It is convenient that we have the same result for odd and even characteristic, because everything which follows can be done uniformly. We will not have to distinguish between characteristics anymore.

In order to have a *diophantine* model, we must also give diophantine definitions of addition and multiplication. Addition is trivial, because $Z^{a+b} = Z^a Z^b$.

Instead of defining multiplication directly, we use a trick by Denef. Let the symbol $|$ denote the usual divisibity in $\mathbb{N}$ and define the relation $|^p \subseteq \mathbb{N}^2$ as

$$a|^p b \iff (\exists k \in \mathbb{N})(b = p^k a).$$

Then multiplication can be defined in $\langle \mathbb{N}, +, |, |^p \rangle$ (see [Den79]). So, in order to have a model of $\langle \mathbb{N}, +, \cdot \rangle$ in $\langle \mathcal{R}[Z], +, \cdot \rangle$, we just need to define the relations $|$ and $|^p$ in this model. This can be done in a diophantine way as follows:

$$\begin{aligned} a|b &\iff Z^a - 1 | Z^b - 1, \\ a|^p b &\iff (\exists k) \left((Z^a)^{p^k} = Z^b \right). \end{aligned}$$

This model leads to two types of variables: the first type will be written with Latin uppercase letters (A, B, C, $\ldots$, Z), and run in $\mathcal{R}[Z]$; the second type, written with Latin lowercase letters (a, b, c, $\ldots$, z), run in $\mathbb{N}$ and are represented by powers of Z.

If we write down a formula mixing these two types, the variables of the second type can only occur as powers of Z. Consider, as an example, the formula

$$(\exists n \in \mathbb{N})((Z-1)A = Z^n - 1).$$

This really means

$$(\exists X \in \mathcal{R}[Z])\big((\exists n \in \mathbb{N})(X = Z^n) \ \wedge \ ((Z-1)A = X - 1)\big).$$

The part $(\exists n \in \mathbb{N})(X = Z^n)$ is diophantine as shown above, so the whole formula is diophantine.

Sometimes we will write down formulas containing only variables of the second type (natural numbers). An example of this could be

$$(\exists a \in \mathbb{N})(a \text{ is prime } \wedge \ n = m^a - 1).$$

When we see all variables in this formula as natural numbers, it is diophantine over $\mathbb{N}$, by DPRM (see Section 3.4). As we encode these variables as powers of Z, the resulting relation between Z^n and Z^m is diophantine over $\mathcal{R}[Z]$ because our model of $\mathbb{N}$ is diophantine.

5.3 Degree and order at zero

Now we turn our attention to the ring of polynomials over finite fields. On the fraction field $\mathbb{F}_q(Z)$, we will use two discrete valuations v_∞ and v_0. For $P \in \mathbb{F}_q[Z]$, we define $v_\infty(P)$ as $-\deg(P)$ and $v_0(P)$ as the maximal n such that Z^n divides P. For rational functions, $v(P/Q) = v(P) - v(Q)$ for $P, Q \in \mathbb{F}_q[Z]$.

To give diophantine definitions of these valuations, we will have to work in the field of rational functions. This is allowed because of Propositions 2.3 and 2.10.

Now it is well known (see [Rum80] or [Shl94]) that all discrete valuation rings in $\mathbb{F}_q(Z)$ are diophantine. This also follows from the Existential Divisibility Lemma (see [Phe00] and [DVG06]). In other words, "$v_\infty(P/Q) \geq 0$" and "$v_0(P/Q) \geq 0$" are diophantine.

From this it follows that "degree" and "order at zero" are diophantine functions $\mathbb{F}_q[Z] \setminus \{0\} \to \mathbb{N}$:

$$\begin{aligned} \deg(P) = n &\iff v_\infty(P/Z^n) \geq 0 \ \wedge \ v_\infty(Z^n/P) \geq 0, \\ v_0(P) = n &\iff v_0(P/Z^n) \geq 0 \ \wedge \ v_0(Z^n/P) \geq 0. \end{aligned}$$

5.4 Defining arbitrary powers

In the following proposition, we prove that B^n is a diophantine function of $B \in \mathbb{F}_q[Z]$ and $n \in \mathbb{N}$. Remember that n is being represented by Z^n, so we should say a function of B and Z^n.

Proposition 5.12. *We can diophantinely define powering in $\mathbb{F}_q[Z]$ as follows:*

$$A = B^n \tag{5.15}$$

$$\Updownarrow$$

$$(A = 0 \ \wedge \ B = 0 \ \wedge \ n > 0) \ \vee \ (A = 1 \ \wedge \ B = 0 \ \wedge \ n = 0) \tag{5.16}$$

$$\vee \ (AB \neq 0 \ \nrightarrow \ (\exists k)(Z^n A = (ZB)^k \ \wedge \ v_0(A) = n v_0(B))). \tag{5.17}$$

Diophantineness. Formula (5.16) is clearly diophantine. The formula "$AB \neq 0$" is diophantine because of Proposition 2.3 and "$(\exists k)(Z^n A = (ZB)^k)$" is diophantine because of Proposition 5.6 or 5.11. Finally, Section 5.3 explains why "$v_0(A) = n v_0(B)$" is diophantine.

Proof. For $A = 0$ or $B = 0$, the equivalence is clear because of (5.16). So, we may assume that $AB \neq 0$.

If $A = B^n$, then clearly (5.17) is true with $k = n$. Conversely, assume (5.17). Comparing the order at zero of $Z^n A = (ZB)^k$, we find $n + v_0(A) = k(1 + v_0(B))$. Using $v_0(A) = nv_0(B)$, this implies $n(1+v_0(B)) = k(1+v_0(B))$. Since $v_0(B) \geq 0$, it follows that $n = k$, therefore $A = B^n$. □

5.5 Cyclotomic polynomials

In the rest of this chapter, we will often work with cyclotomic polynomials (a good reference is [Was82]). To define the n-th cyclotomic polynomial $\Phi_n \in \mathbb{Q}[Z]$, consider ζ_n, a primitive n-th root of unity in some number field. Then Φ_n is defined as

$$\Phi_n(Z) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} \left(Z - \zeta_n^k\right),$$

which is the minimal polynomial of ζ_n. We see that Φ_n is monic of degree $\varphi(n)$, where φ denotes the Euler totient function. Since ζ_n is an algebraic integer, $\Phi_n(Z)$ has integer coefficients. Therefore, it makes sense to view the cyclotomic polynomials in $\mathbb{F}_q[Z]$. From the definition it is easy to see that

$$Z^n - 1 = \prod_{d|n} \Phi_d(Z).$$

When n is prime, we can use this to diophantinely define the n-th cyclotomic polynomial in $\mathbb{F}_q[Z]$ as

$$X = \Phi_n \iff (Z-1)X = Z^n - 1. \tag{5.18}$$

In the previous section, we constructed a diophantine model of $\mathbb{N}$, with n being represented by Z^n. This means that (5.18) gives a diophantine function $\mathbb{N} \to \mathbb{F}_q[Z]$, mapping n to Φ_n whenever n is prime.

We need the following easy facts about cyclotomic polynomials:

Proposition 5.13. *If n is prime to the characteristic p, then $Z^n - 1$ is a squarefree polynomial in $\mathbb{F}_q[Z]$.*

Proof. The derivative of $Z^n - 1$ is nZ^{n-1} with n non-zero in $\mathbb{F}_q$. So $\gcd(Z^n - 1, nZ^{n-1}) = 1$, which implies that $Z^n - 1$ is squarefree. □

Proposition 5.14. *Let a and b be two distinct integers, both prime to p. Then* $\gcd(\Phi_a, \Phi_b) = 1$ *in* $\mathbb{F}_q[Z]$.

Proof. If Φ_a and Φ_b had a common factor, then the polynomial $Z^{ab} - 1$, which is a multiple of $\Phi_a\Phi_b$, would not be squarefree. □

Definition 5.15. Let g and a be coprime integers. In what follows, the notation $\mathrm{ord}(g \bmod a)$ means the order of g seen as an element of the group $(\mathbb{Z}/a\mathbb{Z})^*$. In other words, this is the smallest positive integer k such that $g^k \equiv 1 \bmod a$.

Proposition 5.16. *Let a and b be prime, with b not dividing $q - 1$. Then*

$$a | \Phi_b(q) \iff \mathrm{ord}(q \bmod a) = b.$$

Proof. ($\Longrightarrow$): Since b is prime, we know that $\Phi_b(q) = (q^b - 1)/(q - 1)$, so

$$\frac{q^b - 1}{q - 1} \equiv 0 \mod a. \tag{5.19}$$

We claim that q cannot be congruent to 1 modulo a. Otherwise, we would have

$$0 \equiv \Phi_b(q) = 1 + q + q^2 + \cdots + q^{b-1} \equiv b \mod a.$$

In other words, b would have to be a multiple of a, hence equal to a. By Fermat's Little Theorem and the fact that $q \not\equiv 1 \bmod b$, we have

$$\frac{q^b - 1}{q - 1} \equiv 1 \mod b,$$

a contradiction with (5.19).

Given $q \not\equiv 1 \bmod a$, (5.19) implies that $q^b \equiv 1 \bmod a$.

($\Longleftarrow$): Since b is prime, $\mathrm{ord}(q \bmod a) = b$ means $q^b \equiv 1 \mod a$ and $q \not\equiv 1 \mod a$. Therefore

$$\frac{q^b - 1}{q - 1} \equiv 0 \mod a.$$

□

Proposition 5.17. *Let a be prime to the characteristic p. Then the irreducible factors of the cyclotomic polynomial Φ_a (seen as an element of $\mathbb{F}_q[Z]$) all have degree equal to* $\mathrm{ord}(q \bmod a)$.

Proof. See [LN88, Theorem 2.47]. □

Combining the last two propositions, we get:

Corollary 5.18. *Let q be a power of a prime p. Let a and b be primes with $b \nmid q-1$. Then the following are equivalent:*

1. $a|\Phi_b(q)$.
2. $a \neq p$ *and* $\operatorname{ord}(q \bmod a) = b$.
3. $a \neq p$ *and all the irreducible factors of* Φ_a *over* $\mathbb{F}_q$ *have degree equal to* b.

Proof. The only thing we still have to prove is that $a \neq p$ whenever $a|\Phi_b(q)$. We know that $a|\Phi_b(q)|q^b - 1$, which implies that $\gcd(a,p) = 1$. □

This can be used to find cyclotomic polynomials with factors of prescribed degree, if that degree is prime and does not divide $q-1$. This will be one of the main tools in Section 5.7.

5.6 Reducing to a bounded universal quantifier

Let $\theta : \mathbb{F}_q[Z] \xrightarrow{\sim} \mathbb{N}$ be a recursive presentation (see Section 3.3). Define $P^{(n)}$ as the polynomial in $\mathbb{F}_q[Z]$ such that $\theta(P^{(n)}) = n$. In other words, $P^{(n)}$ is the "n-th polynomial".

Set $P^{(n)} = \alpha_0^{(n)} Z^d + \alpha_1^{(n)} Z^{d-1} + \cdots + \alpha_d^{(n)}$, where d is the degree of $P^{(n)}$. We also define:

$$\begin{aligned} Q_{-1}^{(n)} &= 0, \\ Q_0^{(n)} &= \alpha_0^{(n)}, \\ Q_1^{(n)} &= \alpha_0^{(n)} Z + \alpha_1^{(n)}, \\ &\vdots \\ Q_d^{(n)} &= \alpha_0^{(n)} Z^d + \alpha_1^{(n)} Z^{d-1} + \cdots + \alpha_d^{(n)} = P^{(n)}. \end{aligned}$$

We claim that all these polynomials (and hence also the degree of $P^{(n)}$) are recursive, i.e. given k and n it must be possible to compute $Q_d^{(n)}$. Because all recursive presentations of $\mathbb{F}_q[Z]$ are equivalent (see Section 3.3), it suffices that this is true for just one recursive presentation. But now it is not difficult to construct a recursive presentation where $Q_k^{(n)}$ is recursive as a function of k and n.

As shown in Section 3.4.1, we need to give a diophantine definition of "$X = P^{(n)}$" to prove the Main Theorem. The following theorem almost gives such a definition. Apart from the allowed existential quantifiers, there is a *bounded universal quantifier* $(\forall k)_{\leq d}$. This quantifier means "for all $k \in \mathbb{N}$ with $k \leq d$". In Section 5.7, we will show how to get rid of this quantifier.

Theorem 5.19. *Let p_k denote the k-th prime number in $\mathbb{N}$ and enumerate $\mathbb{F}_q$ as $\mathbb{F}_q = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_q\}$. Then, for $X \in \mathbb{F}_q[Z]$ and $n \in \mathbb{N}$, we have:*

$$X = P^{(n)} \tag{5.20}$$

$$\Updownarrow$$

$$(\exists d, e, t)$$

$$d = \deg P^{(n)} \tag{5.21}$$

$$\wedge\ \deg(Q_0^{(n)}) \leq e\ \wedge\ \deg(Q_1^{(n)}) \leq e\ \wedge\ \ldots\ \wedge\ \deg(Q_d^{(n)}) \leq e \tag{5.22}$$

$$\wedge\ e < p_{t-1} - 1 \tag{5.23}$$

$$\wedge\ (\exists C)$$

$$0 \equiv C \mod \Phi_{p_{t-1}} \tag{5.24}$$

$$\wedge\ X \equiv C \mod \Phi_{p_{t+d}}\ \wedge\ \deg(X) \leq e \tag{5.25}$$

$$\wedge\ (\forall k)_{\leq d}(\exists A, Y)$$

$$(\alpha_k^{(n)} = \varepsilon_1\ \wedge\ A = \varepsilon_1)\ \vee\ \ldots\ \vee\ (\alpha_k^{(n)} = \varepsilon_q\ \wedge\ A = \varepsilon_q) \tag{5.26}$$

$$\wedge\ Y \equiv C \mod \Phi_{p_{t+k-1}}\ \wedge\ \deg(Y) \leq e \tag{5.27}$$

$$\wedge\ YZ + A \equiv C \mod \Phi_{p_{t+k}}. \tag{5.28}$$

Diophantineness. Formulas (5.21), (5.22) and (5.23) depend only on the variables d, n, e and t (q is a constant). All these are natural numbers, represented by powers of Z. By DPRM, these formulas are diophantine because they are recursively enumerable (see the argument at the end of Section 5.2.3).

Formulas (5.24), (5.25), (5.27) and (5.28) are diophantine because the cyclotomic polynomials with prime indices are diophantinely definable using (5.18).

Formula (5.26) simply means "$\alpha_k^{(n)} = A$", but we have to write it like (5.26) to see that it is diophantine. For each $1 \leq i \leq q$, the formula "$\alpha_k^{(n)} = \varepsilon_i$" depends only

on the variables $k, n \in \mathbb{N}$ (every ε_i is just a constant), therefore it is diophantine by DPRM. The language stated in our Main Theorem allows us to define every element of $\mathbb{F}_q$, therefore "$A = \varepsilon_i$" is also diophantine.

Proof. Suppose first that $X = P^{(n)}$. Set $d = \deg P^{(n)}$ and take e and t such that (5.22) and (5.23) are satisfied. Then use the Chinese Remainder Theorem to find a $C \in \mathbb{F}_q[Z]$ for which

$$\begin{aligned} 0 &\equiv C \mod \Phi_{p_{t-1}}, \\ Q_0^{(n)} &\equiv C \mod \Phi_{p_t}, \\ Q_1^{(n)} &\equiv C \mod \Phi_{p_{t+1}}, \\ &\vdots \\ X = P^{(n)} = Q_d^{(n)} &\equiv C \mod \Phi_{p_{t+d}}. \end{aligned}$$

This gives formulas (5.24) and (5.25). Take a k in $\{0, 1, \ldots, d\}$, set $A = \alpha_k^{(n)}$ and $Y = Q_{k-1}^{(n)}$. The choice of C and e gives (5.27). Finally, (5.28) is true because $Q_{k-1}^{(n)} Z + \alpha_k^{(n)} = Q_k^{(n)}$.

For the other direction ($\Uparrow$), we claim that $Q_k^{(n)} \equiv C \bmod \Phi_{p_{t+k}}$ for $-1 \le k \le d$. We prove it by induction on k. For $k = -1$, the claim is true by (5.24). Suppose it is true for $k-1$ and let us prove it for k ($0 \le k \le d$). The induction hypothesis, together with (5.27) and (5.22) gives

$$Y \equiv Q_{k-1}^{(n)} \bmod \Phi_{p_{t+k-1}} \ \wedge\ \deg(Y) \le e \ \wedge\ \deg(Q_{k-1}^{(n)}) \le e. \tag{5.29}$$

Using (5.23), we have $\deg(Y) \le e < p_{t-1} - 1 \le p_{t+k-1} - 1 = \deg \Phi_{p_{t+k-1}}$ and the same bound holds for $\deg(Q_{k-1}^{(n)})$. It follows that $Y = Q_{k-1}^{(n)}$. To finish the proof the claim, we use (5.26) and (5.28) to get

$$Q_k^{(n)} = Q_{k-1}^{(n)} Z + \alpha_k^{(n)} \equiv YZ + A \equiv C \mod \Phi_{p_{t+k}}.$$

A similar argument, but applied to (5.25) instead of (5.27), shows that $X = Q_d^{(n)} = P^{(n)}$. □

5.7 Eliminating the bounded universal quantifier

Combining Theorems 3.12 and 5.19, we see that we can prove our Main Theorem if we can eliminate the bounded universal quantifier (b.u.q.) coming from Theorem 5.19.

Consider the formula

$$(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0. \tag{5.30}$$

where $F_1, \ldots, F_n$ are free (unbounded) variables and Δ is a polynomial with coefficients in $\mathbb{F}_q[Z]$. This is the general form of a formula where a b.u.q. is followed by something diophantine.

Set $d := \deg_{\text{total}}(\Delta)$. Now we have constants d, n, m as a function of Δ. First we need a small lemma to write formula (5.30) in a special form (but still with a b.u.q.). It is in this form that we will eliminate the b.u.q. to get an equivalent formula with only existential quantifiers.

Lemma 5.20.

$$\begin{aligned}
&(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0 && (5.30)\\
&\qquad\qquad \Updownarrow \\
&(\exists u, e, t) \\
&\qquad \deg(F_1) \leq e \ \wedge \ \ldots \ \wedge \ \deg(F_n) \leq e && (5.31)\\
&\quad \wedge\ d \cdot \max\{y, e, u\} \leq t && (5.32)\\
&\quad \wedge\ (\forall k)_{\leq y}(\exists X_1, \ldots, X_m) \\
&\qquad\quad \deg(X_1) \leq u \ \wedge \ \ldots \ \wedge \ \deg(X_m) \leq u && (5.33)\\
&\qquad\quad \wedge\ \Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0. && (5.34)
\end{aligned}$$

Proof. Assuming (5.30), there exist $X_1^{(0)}, \ldots, X_m^{(0)}, \ldots, X_1^{(y)}, \ldots, X_m^{(y)}$ such that

$$\Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots X_m^{(k)}) = 0 \qquad (0 \leq k \leq y).$$

Take e and u large enough such that (5.31) and (5.33) are satisfied, and then take t large enough to satisfy the inequality (5.32).

The other implication is trivial, since it only removes conditions. □

In the next theorem, we will eliminate the b.u.q. appearing in the last 3 lines of the preceding lemma. Instead of trying to prove that (5.33)∧(5.34) is diophantine by itself, we will prove that (5.33) ∧ (5.34) is diophantine provided that formulas (5.31) and (5.32) are true. So, (5.33) ∧ (5.34) will be partially diophantine (see Section 2.6) on the set defined by (5.31) and (5.32). As explained in Section 2.6, this suffices to conclude that the conjunction (5.31) ∧ (5.32) ∧ (5.33) ∧ (5.34) appearing in Lemma 5.20 is diophantine.

Theorem 5.21. *Let $F_1, \dots, F_n \in \mathbb{F}_q[Z]$ and $y, u, e, t \in \mathbb{N}$. Assume that* (5.31) *and* (5.32) *are satisfied. Let $b_0, b_1, \dots, b_y$ be distinct primes, all greater than t, and none of them a divisor of $q-1$. Let a_k $(0 \le k \le y)$ be a prime factor of $\Phi_{b_k}(q)$. Then*

$$
\begin{aligned}
&(\forall k)_{\le y}(\exists X_1, \dots, X_m) \\
&\qquad \deg(X_1) \le u \ \wedge \ \dots \ \wedge \ \deg(X_m) \le u && (5.33)\\
&\quad \wedge\ \Delta(Z^y, Z^k, F_1, \dots, F_n, X_1, \dots, X_m) = 0 && (5.34)\\
&\qquad \Updownarrow \\
&(\exists c)(\exists A_1, \dots, A_m)(\exists P) \\
&\qquad c \equiv k \mod a_k \qquad (0 \le k \le y) && (5.37)\\
&\quad \wedge\ \Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y} | P | \frac{Z^{a_0 a_1 \dots a_y} - 1}{Z - 1} && (5.38)\\
&\quad \wedge\ P | \prod_{\deg J \le u} (A_i - J) \qquad (1 \le i \le m) && (5.39)\\
&\quad \wedge\ \Delta(Z^y, Z^c, F_1, \dots, F_n, A_1, \dots, A_m) \equiv 0 \mod P. && (5.40)
\end{aligned}
$$

Proof. First of all, the primes a_k are all distinct (this follows from Proposition 5.14 or Corollary 5.18).

Suppose we have

$$\Delta(Z^y, Z^k, F_1, \dots, F_n, X_1^{(k)}, \dots, X_m^{(k)}) = 0 \quad \text{with } \deg(X_i^{(k)}) \le u \qquad (0 \le k \le y). \tag{5.41}$$

Use the Chinese Remainder Theorem to get a c satisfying (5.37). This implies that $Z^c \equiv Z^k \bmod Z^{a_k} - 1$, in particular $Z^c \equiv Z^k \bmod \Phi_{a_k}$.

Now we apply the Chinese Remainder Theorem again to choose $A_1, \dots, A_m \in \mathbb{F}_q[Z]$ such that

$$A_i \equiv X_i^{(k)} \mod \Phi_{a_k} \qquad (1 \le i \le m, 0 \le k \le y). \tag{5.42}$$

We can do this because the moduli Φ_{a_k} are coprime by Proposition 5.14.

Using (5.41), we have

$$\Delta(Z^y, Z^c, F_1, \ldots, F_n, A_1, \ldots, A_m) \\ \equiv \Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}) \equiv 0 \mod \Phi_{a_k}. \quad (5.43)$$

Let $P := \Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}$, this satisfies (5.38). Since (5.43) holds for all k, we have (5.40).

Using the fact that $\deg(X_i^{(k)}) \leq u$, it follows from (5.42) that

$$\prod_{\deg J \leq u} (A_i - J) \equiv 0 \mod \Phi_{a_k} \qquad (1 \leq i \leq m, 0 \leq k \leq y).$$

This immediately implies (5.39).

For the other direction, we assume the bottom part of the theorem holds. Taking a k less than or equal to y, we need to find $X_1^{(k)}, \ldots, X_m^{(k)}$ with degrees at most u and such that $\Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}) = 0$. Formulas (5.38) and (5.39) give us

$$\Phi_{a_k} | P | \prod_{\deg J \leq u} (A_i - J) \qquad (1 \leq i \leq m, 0 \leq k \leq y).$$

Let Ψ_{a_k} be any irreducible factor of Φ_{a_k}. Corollary 5.18 tells us that $\deg \Psi_{a_k} = \operatorname{ord}(q \bmod a_k) = b_k$.

Ψ_{a_k} is irreducible, so if it divides a product, it divides one of the factors, say $\Psi_{a_k} | A_i - X_i^{(k)}$, with $\deg X_i^{(k)} \leq u$. Written otherwise, this becomes

$$A_i \equiv X_i^{(k)} \mod \Psi_{a_k} \qquad (1 \leq i \leq m, 0 \leq k \leq y).$$

From (5.37) it follows that $Z^c \equiv Z^k \bmod \Psi_{a_k}$. All this gives

$$\Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}) \\ \equiv \Delta(Z^y, Z^c, F_1, \ldots, F_n, A_1, \ldots, A_m) \equiv 0 \mod \Psi_{a_k}.$$

If we can prove that the degree of the left hand side is less than the degree of Ψ_{a_k}, we are done. For this we will use the assumptions of the theorem (recall

that d is the total degree of Δ).

$$\begin{aligned}
&\deg \Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}) \\
&\qquad \leq d \cdot \max\left\{\deg Z^y, \deg Z^k, \deg F_1, \ldots, \deg F_n, \deg X_1^{(k)}, \ldots, \deg X_m^{(k)}\right\} \\
&\qquad \leq d \cdot \max\{y, e, u\} \leq t \\
&\qquad < b_k = \deg \Psi_{a_k}.
\end{aligned}$$

□

This theorem does indeed reduce the original formula with a b.u.q. to one with only existential quantifiers. However, it is far from clear that all the formulas used are diophantine, in particular (5.38) and (5.39) seem problematic. For the other formulas, it is easy to see that they are diophantine, we will discuss this in more detail in Section 5.7.3. In the next section we will prove that (5.38) is also diophantine.

For (5.39) however, we have to do more work. It is not clear how to diophantinely define (5.39) directly. Instead, we will give a diophantine definition of (5.39), not over $\mathbb{F}_q[Z]$, but over $\mathbb{F}_q[W, Z]$. So, we will pretend that we are working in the two-variable ring $\mathbb{F}_q[W, Z]$. Then the variables P and A_i occuring in (5.39) will be seen as elements of $\mathbb{F}_q[W, Z]$. Of course, these variables do not depend on W, so they are in the subring $\mathbb{F}_q[Z]$ of $\mathbb{F}_q[W, Z]$. But eventually we would like (5.39) to be diophantine over $\mathbb{F}_q[Z]$. This will follow from Section 5.8, where we will construct a diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$.

5.7.1 Defining (5.38)

We can now look at formula (5.38) from Theorem 5.21. As in that theorem, let $b_0, b_1, \ldots, b_y$ be distinct primes and a_k $(0 \leq k \leq y)$ a prime factor of $\Phi_{b_k}(q)$. Set

$$r := (q-1)\Phi_{b_0}(q)\Phi_{b_1}(q)\ldots\Phi_{b_y}(q). \tag{5.44}$$

Lemma 5.22. *Let $b_0, b_1, \ldots, b_y$ be distinct primes and r as in (5.44). For all $0 \leq i < j \leq y$, $q^{b_i b_j} - 1$ is not a divisor of r.*

Proof. We will prove this by contradiction, so we assume that

$$q^{b_i b_j} - 1 \Big| (q-1) \prod_{k=0}^{y} \Phi_{b_k}(q).$$

Dividing both sides by $(q-1)\Phi_{b_i}(q)\Phi_{b_j}(q)$ gives

$$\Phi_{b_ib_j}(q)\Big|\prod_{k\neq i,k\neq j}\Phi_{b_k}(q).$$

Let a be any prime dividing $\Phi_{b_ib_j}(q)$. Then a has to divide $\Phi_{b_k}(q)$ for a certain k different from i and j. Since b_k is prime, this implies that $\operatorname{ord}(q \bmod a) = b_k$ by Proposition 5.16. But $a|\Phi_{b_ib_j}(q)$ implies that $q^{b_ib_j} \equiv 1 \mod a$. This is a contradiction because b_ib_j would have to be a multiple of b_k. □

Theorem 5.23. *Let a_k, b_k $(0 \le k \le y)$ and r be chosen as above. Then*

$$\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}|P|\frac{Z^{a_0a_1\ldots a_y}-1}{Z-1} \tag{5.45}$$

$$\Updownarrow$$

$$(\exists Q,G,H,M)$$

$$(Z-1)PQ = (Z^{a_0a_1\ldots a_y}-1) \tag{5.46}$$

$$\wedge\ GH \equiv 1 \mod Q \tag{5.47}$$

$$\wedge\ (G^r-1)M \equiv 1 \mod Q. \tag{5.48}$$

Proof. Assume (5.45). To get (5.46), set

$$Q = \frac{Z^{a_0a_1\ldots a_y}-1}{(Z-1)P}.$$

which is a polynomial by assumption. It follows from the theory of cyclotomic polynomials (see Section 5.5) that

$$Z^{a_0a_1\ldots a_y}-1 = \prod_{d|a_0a_1\ldots a_y}\Phi_d = \underbrace{(Z-1)}_{\Phi_1}\ \underbrace{\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}}_{\substack{\Phi_d \text{ with } d|a_0a_1\ldots a_y,\\ d \text{ prime}}}\ \underbrace{\Phi_{a_0a_1}\Phi_{a_0a_2}\cdots\Phi_{a_0a_1\ldots a_y}}_{\substack{\Phi_d \text{ with } d|a_0a_1\ldots a_y,\\ d \text{ having at least 2 factors}}}.$$

Since $\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}|P$, this implies that

$$Q|\prod_{\substack{d|a_0a_1\ldots a_y,\\ d \text{ has} \ge 2 \text{ factors}}}\Phi_d. \tag{5.49}$$

We will apply Corollary 2.12 on the irreducible factors of Q to prove (5.47) and (5.48). So, for each irreducible factor Ψ of Q, we need to find G, H and M

such that (5.47) and (5.48) are satisfied modulo Ψ. Note that G, H and M may depend on Ψ.

By (5.49), an irreducible factor of Q will be a divisor of a particular Φ_d. We denote this factor by Ψ_d. We know that d has at least 2 prime factors, say a_i and a_j $(i \neq j)$. By Proposition 5.17, the degree of Ψ_d is equal to $\mathrm{ord}(q \bmod d)$, so working modulo Ψ_d is the same as working in the finite field $\mathbb{F}_{q^{\mathrm{ord}(q \bmod d)}}$. From the definition of ord it is clear that

$$a_i | d \implies \mathrm{ord}(q \bmod a_i) | \, \mathrm{ord}(q \bmod d) \implies b_i | \, \mathrm{ord}(q \bmod d).$$

Analogously, we have $b_j | \, \mathrm{ord}(q \bmod d)$. Both b_i and b_j are prime, so $b_i b_j$ divides $\mathrm{ord}(q \bmod d)$. Let G be a generator of the multiplicative group of the subfield $\mathbb{F}_{q^{b_i b_j}} \subseteq \mathbb{F}_{q^{\mathrm{ord}(q \bmod d)}}$. Then G has an inverse H. By Lemma 5.22, r is not a multiple of the order of this group, so $G^r \neq 1$, hence $G^r - 1$ has an inverse M. This proves (5.47) and (5.48) modulo Ψ_d.

For the converse, it follows from (5.46) that

$$\Phi_{a_0} \Phi_{a_1} \cdots \Phi_{a_y} | \frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} = PQ.$$

We are done if we can prove that $\gcd(\Phi_{a_k}, Q) = 1$ for all k. Suppose this is not the case, and let Ψ_{a_k} be a common irreducible factor of Φ_{a_k} and Q. Then (5.47) implies that $G \not\equiv 0 \mod \Psi_{a_k}$. But the order of $(\mathbb{F}_q[Z]/\Psi_{a_k})^*$ is equal to $q^{\deg \Psi_{a_k}} - 1 = q^{b_k} - 1 = (q-1)\Phi_{b_k}(q)$, which divides r. Therefore, $G^r \equiv 1 \mod \Psi_{a_k}$, in contradiction to (5.48). □

5.7.2 Defining (5.39)

In this section we will prove that formula (5.39) from Theorem 5.21 is diophantine. We only need to define it in the case that (5.38) holds. As mentioned before, we will do this in the ring $\mathbb{F}_q[W, Z]$.

Theorem 5.24. *Let P be a polynomial in $\mathbb{F}_q[Z]$ dividing $Z^{a_0 a_1 \ldots a_y} - 1$, and let $A \in \mathbb{F}_q[Z]$. Here, $\mathbb{F}_q[Z]$ must be viewed as a subring of $\mathbb{F}_q[W, Z]$. Then the*

following equivalence holds:

$$P \mid \prod_{\deg J \le u} \big(A - J\big) \tag{5.50}$$

$$\Updownarrow$$

$$(\exists h)$$

$$q^h > u \ \wedge \ \gcd(h, \varphi(a_0 a_1 \dots a_y)) = 1 \tag{5.51}$$

$$\wedge \ (\exists B \in \mathbb{F}_q[W, Z])$$

$$\deg_W(B) \le u \tag{5.52}$$

$$\wedge \ B \equiv B^{q^h} \mod (P(Z), W^{q^h} - W) \tag{5.53}$$

$$\wedge \ B \equiv A \mod (P(Z), W - Z). \tag{5.54}$$

Proof. To begin, we consider the factorization of P:

$$P = \prod_{j=1}^{f} P_j \qquad (P_j \text{ irreducible}).$$

We know that P divides $Z^{a_0 a_1 \dots a_y} - 1$, therefore every P_j is some irreducible factor of Φ_s with $s | a_0 a_1 \dots a_y$.

If (5.50) holds, then there exist $J_j \in \mathbb{F}_q[Z]$ for which

$$J_j(Z) \equiv A(Z) \mod P_j(Z) \quad \text{and} \quad \deg(J_j) \le u \qquad (1 \le j \le f).$$

By the Chinese Remainder Theorem, we know there exists a $B \in \mathbb{F}_q[W, Z]$ for which

$$B \equiv J_j(W) \mod P_j(Z) \qquad (1 \le j \le f).$$

Since all J_j's have degree at most u, we can assure that the degree in W of B is also at most u.

To prove (5.53), we see that

$$B^{q^h} \equiv J_j(W)^{q^h} \equiv J_j(W) \equiv B \mod (P_j(Z), W^{q^h} - W).$$

Since this holds for all j, the Chinese Remainder Theorem gives (5.53).

Finally, (5.54) holds because

$$B \equiv J_j(W) \equiv J_j(Z) \equiv A \mod (P_j(Z), W - Z).$$

Again, we use the Chinese Remainder Theorem to go from P_j to P.

Conversely, assume that (5.51)–(5.54) hold. To prove that P divides the product in (5.50), we will show that every P_j divides the product.

So, take an irreducible factor P_j of P. We have to show that there exists a $J \in \mathbb{F}_q[Z]$ with $\deg(J) \leq u$ such that $A \equiv J \mod P_j$.

Write $\overline{B}$ for the reduction of B modulo $P_j(Z)$. If we write $d := \deg(P_j)$, then $\overline{B}$ can be seen as an element of $\mathbb{F}_{q^d}[W]$.

Since $\deg(\overline{B}) \leq u$, we may write $\overline{B}$ as

$$\overline{B} = \sum_{i=0}^{u} \alpha_i W^i \qquad (\alpha_i \in \mathbb{F}_{q^d}).$$

Using (5.53), we find that

$$\overline{B} \equiv \overline{B}^{q^h} = \sum_{i=0}^{u} \alpha_i^{q^h} W^{iq^h} \equiv \sum_{i=0}^{u} \alpha_i^{q^h} W^i \mod W^{q^h} - W.$$

Now $\overline{B}$ and $\sum \alpha_i^{q^h} W^i$ are two polynomials in W with degree at most $u < q^h$, congruent modulo $W^{q^h} - W$. Therefore, they are equal. It follows that $\alpha_i = \alpha_i^{q^h}$, so $\alpha_i \in \mathbb{F}_{q^h}$.

By construction, α_i is an element of $\mathbb{F}_{q^d} = \mathbb{F}_q[Z]/P_j(Z)$. This extension of $\mathbb{F}_q$ has degree $d = \deg(P_j) = \operatorname{ord}(q \bmod s) | \phi(s) | \phi(a_0 a_1 \dots a_y)$. So, from (5.51) it follows that $\gcd(h, d) = 1$, hence $\alpha_i \in \mathbb{F}_{q^h} \cap \mathbb{F}_{q^d} = \mathbb{F}_q$. All this implies that $\overline{B}$ is actually in $\mathbb{F}_q[W]$.

Let $J := \sum_{i=0}^{u} \alpha_i Z^i \in \mathbb{F}_q[Z]$, then $\deg(J) \leq u$ and it follows from (5.54) that

$$A \equiv \overline{B} = \sum_{i=0}^{u} \alpha_i W^i \equiv \sum_{i=0}^{u} \alpha_i Z^i = J \mod (P_j(Z), W - Z).$$

Since neither A nor J depend on W, we get $A \equiv J \mod P_j$, which completes the proof of Theorem 5.24. □

5.7.3 Putting everything together

Putting Lemma 5.20 and Theorems 5.21, 5.23 and 5.24 together, we get the following equivalence:

$$(\forall k)_{\le y}(\exists X_1,\dots,X_m)\Delta(Z^y,Z^k,F_1,\dots,F_n,X_1,\dots,X_m)=0 \tag{5.30}$$

$$\Updownarrow$$

$$(\exists u,e,t)$$

$$\deg(F_1)\le e \ \wedge\ \dots\ \wedge\ \deg(F_n)\le e \tag{5.31}$$

$$\wedge\ d\cdot\max\{y,e,u\}\le t \tag{5.32}$$

$$\wedge\ (\exists \bar b\in\mathbb{N})(\exists \bar a\in\mathbb{N})$$

$$\bar b \text{ is a product of } y+1 \text{ primes } b_0,b_1,\dots,b_y \text{ with } t<b_0<b_1<\ldots<b_y \text{ and } b_k\nmid q-1 \text{ for all } k. \tag{5.35}$$

$$\wedge\ \bar a \text{ is a product of } y+1 \text{ primes } a_0<a_1<\ldots<a_y, \text{ with } a_k \text{ a divisor of } \Phi_{b_k}(q). \tag{5.36}$$

$$\wedge\ (\exists c)(\exists A_1,\dots,A_m)(\exists P)$$

$$c\equiv k \mod a_k \qquad (0\le k\le y) \tag{5.37}$$

$$\wedge\ \Delta(Z^y,Z^c,F_1,\dots,F_n,A_1,\dots,A_m)\equiv 0 \mod P \tag{5.40}$$

$$\wedge\ (\exists r)(\exists Q,G,H,M)$$

$$r=(q-1)\Phi_{b_0}(q)\Phi_{b_1}(q)\dots\Phi_{b_y}(q) \tag{5.44}$$

$$\wedge\ (Z-1)PQ=\left(Z^{\bar a}-1\right) \tag{5.46}$$

$$\wedge\ GH\equiv 1 \mod Q \tag{5.47}$$

$$\wedge\ (G^r-1)M\equiv 1 \mod Q \tag{5.48}$$

$$\wedge\ (\exists h)$$

$$q^h>u\ \wedge\ \gcd(h,\varphi(\bar a))=1 \tag{5.51}$$

$$\left.\begin{array}{l} \wedge\ \displaystyle\bigwedge_{i=1}^{m}(\exists B_i\in\mathbb{F}_q[W,Z]) \\ \qquad \deg_W(B_i)\le u \\ \qquad \wedge\ B_i\equiv B_i^{q^h} \mod (P(Z),W^{q^h}-W) \\ \qquad \wedge\ B_i\equiv A \mod (P(Z),W-Z) \end{array}\right\} \text{ in } \mathbb{F}_q[W,Z]. \tag{5.52--5.54}$$

We examine this formula more closely, in particular we want to see that it is diophantine. We have constant numbers d, m and n depending on the given Δ. Then we have constants p and q coming from the ring we work in. The variables $F_1,\dots,F_n$ and y (represented by Z^y) occur free (unbounded).

Since y is not constant, b_0 through b_y cannot be variables; b_i is just a notation for a recursive function applied on the variable $\bar{b}$, returning the i-th smallest prime factor of $\bar{b}$. Formula (5.35) is a relation between the variables $\bar{b}$, y and t. Similarly, $a_0, \ldots, a_y$ are not variables, but $\bar{a}$ is. All the other letters occuring in the equivalence are variables, quantified by an existential quantifier.

There are several formulas whose variables run only in the natural numbers. These variables are represented by powers of Z and have to be interpreted as explained in Section 5.2.3. Therefore, these formulas are diophantine. Special attention has to be paid to the formula (5.37). This must be seen as one formula, in the variables c, y and $\bar{a}$. We cannot write this down as a system of y formulas, because y is not constant.

Formulas (5.52)–(5.54) are diophantine over $\mathbb{F}_q[W, Z]$. But in Section 5.8 we will construct a diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$. Apart from the usual operators addition and multiplication, this interpretation will also allow us to define powering (as in W^{q^h}) and the degree function $\deg_W$. Then it will follow that the formulas (5.52)–(5.54) are diophantine over $\mathbb{F}_q[Z]$.

All the other formulas are easily seen to be diophantine. Also note that the only quantifiers appearing are existential. Therefore, the whole formula, which is equivalent to $(\forall k)_{\leq y}(\exists X_1, \ldots, X_m)\Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0$, is diophantine.

5.8 The interpretation of $\mathbb{F}_q[V, W]$ over $\mathbb{F}_q[Z]$

Inside $\mathbb{F}_q[Z]$, we will now construct a diophantine interpretation of a two-variable polynomial ring over $\mathbb{F}_q$. Before, we wrote $\mathbb{F}_q[W, Z]$ for this ring, but to avoid confusion between the Z from $\mathbb{F}_q[W, Z]$ and the Z from $\mathbb{F}_q[Z]$, we change notation and write $\mathbb{F}_q[V, W]$ instead for the two-variable polynomial ring.

5.8.1 Stride polynomials

To give this interpretation of $\mathbb{F}_q[V, W]$, we have to introduce *stride polynomials*:

Definition 5.25. For integers $0 \leq w \leq s$, a (w, s)-stride polynomial (over $\mathbb{F}_q$) is a polynomial where a term $\alpha_n Z^n$ can only occur if $n \in \{0, 1, \ldots, w-1\} \bmod s$.

Such a polynomial has the following form:

$$\sum_{i=0}^{d-1}\sum_{j=0}^{w-1}\alpha_{ij}Z^{si+j} \qquad \text{(for a certain } d\text{, all } \alpha_{ij} \text{ in } \mathbb{F}_q\text{)}.$$

For example, a $(3,8)$-stride polynomial is of the form

$$\alpha_{00}+\alpha_{01}Z+\alpha_{02}Z^2+\alpha_{10}Z^8+\alpha_{11}Z^9+\alpha_{12}Z^{10}+\alpha_{20}Z^{16}+\alpha_{21}Z^{17}+\alpha_{22}Z^{18}+\dots.$$

Write $\mathcal{S}_{w,s}$ for the set of all (w,s)-stride polynomials. If $w=0$, then $\mathcal{S}_{0,s}=\{0\}$. We call w the *width* and s the *stride* of these polynomials.

In general $\mathcal{S}_{w,s}$ is not a ring, but it is always a free $\mathbb{F}_q[Z^s]$-module with basis $\{1,Z,Z^2,\dots,Z^{w-1}\}$. In particular, $\mathcal{S}_{w,s}$ is $\mathbb{F}_q$-linear.

Next, we define the set containing all stride polynomials where s is a power of q:

$$\mathcal{M}=\{(F,w,s)\in\mathbb{F}_q[Z]\times\mathbb{N}\times\mathbb{N}\mid w\le s=q^k \text{ for some } k \text{ and } F\in\mathcal{S}_{w,s}\}. \quad (5.55)$$

If we encode a natural number n as Z^n, then $\mathcal{M}$ becomes a subset of $\mathbb{F}_q[Z]^3$.

Proposition 5.26. *The following is a diophantine definition of the set $\mathcal{M}$:*

$$\begin{aligned}
&(F,w,s)\in\mathcal{M} && (5.56)\\
&\qquad\Updownarrow\\
&(\exists G)(\exists d)(\exists k)\\
&\qquad 0\le w\le s=q^k && (5.57)\\
&\qquad\wedge\ \deg F<sd\ \wedge\ \deg G<wd && (5.58)\\
&\qquad\wedge\ F\equiv G^s \pmod{Z^{sd}-Z}. && (5.59)
\end{aligned}$$

Proof. Let $(F,w,s)\in\mathcal{M}$. By definition, (5.57) is satisfied and there exists a d such that

$$F=\sum_{i=0}^{d-1}\sum_{j=0}^{w-1}\alpha_{ij}Z^{si+j}.$$

Set

$$G=\sum_{i=0}^{d-1}\sum_{j=0}^{w-1}\alpha_{ij}Z^{i+dj}.$$

Then (5.58) is true because

$$\deg F \le s(d-1) + (w-1) \le s(d-1) + (s-1) = sd - 1 < sd,$$
$$\deg G \le (d-1) + d(w-1) = wd - 1 < wd.$$

Using the fact that s is a power of q, we find

$$G^s = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+sdj} \equiv \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j} = F \mod Z^{sd} - Z.$$

Conversely, assume (5.57)–(5.59) are satisfied. We have to prove that $F \in \mathcal{S}_{w,s}$. Because the degree of G is less than wd, we can write G as

$$G = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{i+dj}.$$

Note that $i + dj$ indeed runs over all of $\{0, 1, 2, \ldots, wd - 1\}$ in the preceding formula. Let

$$F_1 = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j}.$$

Then $\deg F_1 < sd$ and $F_1 \in \mathcal{S}_{w,s}$. If we can show that $F = F_1$, then we are done. Using (5.59), we find

$$F \equiv G^s = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+sdj} \equiv \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j} = F_1 \mod Z^{sd} - Z.$$

Now we use a standard argument: F and F_1 both have degree less than sd (for F, we use (5.58)). But F and F_1 are congruent modulo something of degree sd, hence $F = F_1$. □

5.8.2 Construction

We will encode elements of $\mathbb{F}_q[V, W]$ as certain equivalence classes of triples (F, w, s) in $\mathcal{M}$. To explain this, we will construct a map $\theta : \mathcal{M} \to \mathbb{F}_q[V, W]$ giving the correspondence. Then the equivalence relation $\sim$ on $\mathcal{M}$ is simply given by the fibers of θ (2 elements are equivalent if they have the same image under θ).

Take a triple $(F,w,s) \in \mathcal{M}$. Then F is a (w,s)-stride polynomial, so it can be written as

$$F = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j}.$$

We let this represent the following element of $\mathbb{F}_q[V,W]$:

$$\theta(F,w,s) = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} V^i W^j.$$

As an example, we look again at the case $w=3$ and $s=8$. Then F is of the form

$$\alpha_{00} + \alpha_{01}Z + \alpha_{02}Z^2 + \alpha_{10}Z^8 + \alpha_{11}Z^9 + \alpha_{12}Z^{10} + \alpha_{20}Z^{16} + \alpha_{21}Z^{17} + \alpha_{22}Z^{18} + \dots.$$

This represents

$$\alpha_{00} + \alpha_{01}W + \alpha_{02}W^2 + \alpha_{10}V + \alpha_{11}VW + \alpha_{12}VW^2 + \alpha_{20}V^2 + \alpha_{21}V^2W + \alpha_{22}V^2W^2 + \dots$$

Conversely, suppose we are given an $\widetilde{F} \in \mathbb{F}_q[V,W]$. We want to figure out which triples (F,w,s) represent $\widetilde{F}$, in other words, what is $\theta^{-1}(\widetilde{F})$? Clearly, a necessary condition for $\theta(F,w,s) = \widetilde{F}$ is that $w > \deg_W(\widetilde{F})$ ($\deg_W$ is the highest power of W occuring). If we take any w satisfying this condition and any $s \geq w$ which is a power of q, then there is a unique F for which $\theta(F,w,s) = \widetilde{F}$. Indeed, for $d > \deg_V(\widetilde{F})$, it is possible to write $\widetilde{F}$ as

$$\widetilde{F} = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} V^i W^j.$$

Then $\widetilde{F}$ is represented by

$$\sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j}.$$

This proves that θ is surjective. What we just observed, can be written as follows:

Lemma 5.27. *Given a triple $(F,w,s) \in \mathcal{M}$, and any $1 \leq w' \leq s' = q^{k'}$ such that $w \leq w'$ and $s \leq s'$, there is a unique F' such that $(F,w,s) \sim (F',w',s')$.*

In this case, F' will actually be an element of $\mathcal{S}_{w,s'}$ and $(F',w',s') \sim (F',w,s')$.

5.8.3 Diophantine definition of the equivalence relation

So far, we have an interpretation of $\mathbb{F}_q[V,W]$ over $\mathbb{F}_q[Z]$, but is it diophantine? We already showed that the set $\mathcal{M}$ is diophantine. The key ingredient to making the interpretation diophantine, is a diophantine definition of the equivalence relation (the fibers of θ). Once we have this, it is very easy to give a diophantine definition of addition and multiplication in this interpretation.

We start by defining the equivalence relation in a special case:

Lemma 5.28. *Let $(F,w,s),(G,w,ms) \in \mathcal{M}$ (this implies that m is a power of q), with $m \geq w$. Then*

$$(F,w,s) \sim (G,w,ms) \tag{5.60}$$

$$\Updownarrow$$

$$\big(\exists X \in \mathcal{S}_{m(s-1),ms}\big)\big(F^m - G = (Z^m - Z)\cdot X\big). \tag{5.61}$$

Proof. If $m = 1$, then (5.60) and (5.61) are both equivalent to $F = G$, which proves the statement. So, for the rest of the proof we may assume $m > 1$.

Assume (5.60). We know from the definition of stride polynomials that F can be written as

$$F = \sum_{i=0}^{d-1}\sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j}.$$

The equivalence between (F,w,s) and (G,w,ms) means that

$$G = \sum_{i=0}^{d-1}\sum_{j=0}^{w-1} \alpha_{ij} Z^{msi+j}.$$

Now $F^m - G = (Z^m - Z)X$ where

$$X = \sum_{i=0}^{d-1}\sum_{j=0}^{w-1} \alpha_{ij} Z^{msi}(Z^{m(j-1)} + Z^{m(j-2)+1} + \cdots + Z^{m+j-2} + Z^{j-1}).$$

The expression between parentheses, $Z^{m(j-1)} + \cdots + Z^{j-1}$, has degree at most $m(w-2) \leq m(s-2) < m(s-1)$, so $X \in \mathcal{S}_{m(s-1),ms}$.

Conversely, assume (5.61). For a large enough d, we can write F and G as

$$F = \sum_{i=0}^{d-1}\sum_{j=0}^{w-1} \alpha_{ij} Z^{si+j} \qquad \text{and} \qquad G = \sum_{i=0}^{d-1}\sum_{j=0}^{w-1} \beta_{ij} Z^{msi+j}.$$

We have to prove that the coefficients α_{ij} and β_{ij} are equal. Let

$$G_1 = \sum_{i=0}^{d-1} \sum_{j=0}^{w-1} \alpha_{ij} Z^{msi+j}.$$

Then $(F, w, s) \sim (G_1, w, ms)$ and from the first part of the proof it follows that there exists an $X_1 \in \mathcal{S}_{m(s-1),ms}$ such that $F^m - G_1 = (Z^m - Z)X_1$.

If we set $G_2 = G - G_1$ and $X_2 = X_1 - X$, then we get, using (5.61),

$$G_2 = (Z^m - Z)X_2. \tag{5.62}$$

If $G = G_1$, we are done. Otherwise, $G_2 \neq 0$, so $X_2 \neq 0$ too. We would like to find a contradiction.

The linearity of stride polynomials implies that $G_2 \in \mathcal{S}_{w,ms}$ and $X_2 \in \mathcal{S}_{m(s-1),ms}$. We look at the degree of both sides of (5.62). The degree of G_2 is in $\{0, 1, \ldots, w-1\}+\mathbb{Z}ms$ and the degree of $(Z^m-Z)X$ in $\{m, m+1, \ldots, ms-1\}+\mathbb{Z}ms$. But (5.62) says that the degrees are equal, which is impossible because of the inequality $w \leq m$. □

This would be a definition of the equivalence $\sim$, if it were not for the hypothesis that $m \geq w$ and that the w's are equal. The following Proposition reduces the general case to this special case.

Proposition 5.29. *Let* $(F_1, w_1, s_1), (F_2, w_2, s_2) \in \mathcal{M}$. *Then*

$$(F_1, w_1, s_1) \sim (F_2, w_2, s_2) \tag{5.63}$$

$$\Updownarrow$$

$$(\exists F_3)(\exists s_3)$$

$$(s_3 \geq w_1 s_1 \ \wedge \ s_3 \geq w_2 s_2) \tag{5.64}$$

$$\nrightarrow (F_3, w_1, s_3) \in \mathcal{M} \ \wedge \ (F_1, w_1, s_1) \sim (F_3, w_1, s_3) \tag{5.65}$$

$$\nrightarrow (F_3, w_2, s_3) \in \mathcal{M} \ \wedge \ (F_2, w_2, s_2) \sim (F_3, w_2, s_3). \tag{5.66}$$

Diophantineness. Because of the conditions (5.64), the equivalences in (5.65) and (5.66) are of the special type of the preceding Lemma (with $m = s_3/s_1$, resp. $m = s_3/s_2$). We will not use (5.64) in the proof; it is there to make the whole formula diophantine. Indeed, we only know that $(F_i, w_i, s_i) \sim (F_3, w_i, s_3)$ is diophantine if $s_3 \geq w_i s_i$ (see Lemma 5.28).

Proof. Assume that $(F_1, w_1, s_1) \sim (F_2, w_2, s_2)$. Take an $s_3 = q^{k_3}$ large enough such that (5.64) is satisfied. Let w_3 be the maximum of w_1 and w_2. Using Lemma 5.27, we can find an F_3 such that $(F_1, w_1, s_1) \sim (F_3, w_3, s_3)$. By transitivity of $\sim$, we also have $(F_2, w_2, s_2) \sim (F_3, w_3, s_3)$. Using the second part of Lemma 5.27, we find the relations (5.65) and (5.66).

Conversely, assume (5.65) and (5.66). Let $w_3 = \max\{w_1, w_2\}$. Applying Lemma 5.27 gives $(F_3, w_1, s_3) \sim (F_3, w_3, s_3)$ and $(F_3, w_2, s_3) \sim (F_3, w_3, s_3)$. Now

$$(F_1, w_1, s_1) \sim (F_3, w_1, s_3) \sim (F_3, w_3, s_3) \sim (F_3, w_2, s_3) \sim (F_2, w_2, s_2).$$

□

5.8.4 Addition, multiplication and powering

Now that we have a diophantine definition of the equivalence relation, the hard work is done. To define addition and multiplication for our interpretation of $\mathbb{F}_q[V, W]$, we may assume that both operands have the same w and s. This follows from the following:

Observation 5.30. *Let (F_1, w_1, s_1), (F_2, w_2, s_2) and (F_3, w_3, s_3) be elements of $\mathcal{M}$. Then*

$$\begin{aligned}
\theta(F_1, w_1, s_1) + \theta(F_2, w_2, s_2) = \theta(F_3, w_3, s_3) \\
\Updownarrow \\
(\exists G_1, G_2)(\exists w, s) \\
\quad (G_1, w, s) \in \mathcal{M} \ \wedge \ (F_1, w_1, s_1) \sim (G_1, w, s) \\
\wedge\ (G_2, w, s) \in \mathcal{M} \ \wedge \ (F_2, w_2, s_2) \sim (G_2, w, s) \\
\wedge\ \theta(G_1, w, s) + \theta(G_2, w, s) \sim \theta(F_3, w_3, s_3).
\end{aligned}$$

For ($\Downarrow$), pick $w \geq \max(w_1, w_2, w_3)$ and $s \geq \max(s_1, s_2, s_3, w)$. Then use Lemma 5.27 to choose G_1, G_2 and G_3. Exactly the same Observation holds for multiplication instead of addition. This shows that it suffices to define "$\theta(F_1, w, s) + \theta(F_2, w, s)$" (with equal w and s) as opposed to "$\theta(F_1, w_1, s_1) + \theta(F_2, w_2, s_2)$".

Lemma 5.31. *Let $(F, w, s), (G, w, s) \in \mathcal{M}$.*

1. *Then*

$$\theta(F, w, s) + \theta(G, w, s) = \theta(F + G, w, s). \tag{5.67}$$

2. *If $2w \leq s$ (this can be ensured by choosing $s \geq 2w$ in Observation 5.30), then*

$$\theta(F, w, s) \cdot \theta(G, w, s) = \theta(FG, 2w, s). \tag{5.68}$$

3. *If $nw \leq s$ (this can be ensured analogously), then*

$$\theta(F, w, s)^n = \theta(F^n, nw, s). \tag{5.69}$$

Proof. (5.67) is immediate because the sets $\mathcal{S}_{w,s}$ are $\mathbb{F}_q$-linear, and the map θ is also $\mathbb{F}_q$-linear in the first argument.

For the multiplication, we rely on the fact that if $\deg_W(F_1)$ and $\deg_W(F_2)$ are both less than w, then $\deg_W(F_1F_2)$ is less than $2w$. If we fix w and s, then θ acts as an 'isomorphism' between $\mathbb{F}_q[Z]$ and $\mathbb{F}_q[V, W]$, if we restrict ourselves to polynomials with W-degree small enough. An analogous reasoning works for powering. □

5.8.5 Embedding $\mathbb{F}_q[Z]$ into $\mathbb{F}_q[V, W]$

We have defined a diophantine interpretation of $\mathbb{F}_q[V, W]$ inside $\mathbb{F}_q[Z]$, but to be useful, we also need a way of mixing statements concerning $\mathbb{F}_q[V, W]$ and $\mathbb{F}_q[Z]$. Consider for example, formula (5.53), which states

$$\text{“}B \equiv B^{q^h} \mod (P(Z), W^{q^h} - W)\text{”}.$$

Here, P is an element of $\mathbb{F}_q[Z]$, but B lives in the interpretation. So, given a polynomial $F(Z) \in \mathbb{F}_q[Z]$, we would like to be able to construct $F(V)$ and $F(W)$ in the interpretation of $\mathbb{F}_q[V, W]$.

Let $F(Z) \in \mathbb{F}_q[Z]$, and let $k \in \mathbb{N}$ be such that $\deg(F) < q^k$. Then it is easy to see that $\theta(F(Z), 1, 1) = F(V)$ and $\theta(F(Z), q^k, q^k) = F(W)$. Since the degree function is diophantine, these mappings are diophantine.

5.8.6 Definition of degree

Finally, we need to give a diophantine definition of the degree function $\deg_V$ in the interpretation. This is necessary for (5.52) to be diophantine (recall that we renamed our variables, such that the W from (5.52) corresponds to V in $\mathbb{F}_q[V, W]$). In general, it is not clear how to define $\deg_V$ in $\mathbb{F}_q[V, W]$, but in this

interpretation it is possible because we can use the degree from $\mathbb{F}_q[Z]$ (which is diophantine, see Section 5.3). From the construction of $\theta : \mathcal{M} \to \mathbb{F}_q[V, W]$ it is easy to see that $\deg_V(\theta(F, w, s)) = \lfloor \deg(F)/s \rfloor$. This immediately leads to a diophantine definition of $\deg_V$.

Chapter 6

Infinite extensions

In the previous chapter, we have proven that r.e. sets are diophantine in rings $\mathbb{F}_q[Z]$, where $\mathbb{F}_q$ is a finite field. In this chapter, we will look at *infinite* subfields $L \subseteq \bar{\mathbb{F}}_p$. Then we can also generalize DPRM for polynomial rings $L[Z]$.

Similarly, we will generalize the results of Denef and Zahidi to infinite extensions. Denef (see [Den78b]) proved that r.e. sets are diophantine for $\mathbb{Z}[Z]$. In his PhD thesis, Zahidi extended this (see [Zah99, Chapter III]) to rings $\mathcal{O}_K[Z_1, \ldots, Z_n]$, where $\mathcal{O}_K$ is the ring of integers in a totally real number field. We will consider polynomial rings over $\mathcal{O}_L$, where L is a totally real algebraic extension of $\mathbb{Q}$, possibly of infinite degree.

For these polynomial rings, we ask ourselves the question whether r.e. sets are diophantine. It turns out that this is no longer true. First of all, the ring we consider might not be recursive (for definitions, see Section 3.3), then there are no r.e. sets. Even if L is recursive, it is still not clear what we mean with "recursively enumerable set", because whether a set is r.e., might depend on the chosen recursive presentation. This is a more interesting problem and will be solved by considering sets which are r.e. for *every* recursive presentation. We will address these issues in more detail in Section 6.1, then we will state the Main Theorem and give an outline of the proof in Section 6.2.

6.1 Recursive structure

Let K be a prime field. There are two cases: either $K = \mathbb{Q}$ or K is a finite field $\mathbb{F}_p$ with $p > 0$ prime. Let L be an algebraic extension of K having an infinite

number of elements. In this section, we will consider what r.e. subsets of L look like. The author does not know a reference for the results in this section, even though these issues have probably been studied in recursion theory.

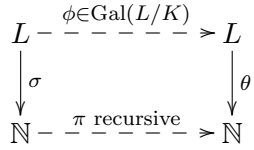
First of all, not every algebraic extension of $\mathbb{F}_p$ or $\mathbb{Q}$ is recursive. This can simply be seen by considering cardinalities: $\bar{\mathbb{F}}_p$ and $\bar{\mathbb{Q}}$ have $2^{\aleph_0}$ subfields, but at most $\aleph_0$ of them can be recursive. So, we have to require that L is a recursive field, otherwise we cannot possibly give any meaning to r.e. sets in L.

As an example of a non-recursive field, we construct a non-recursive subfield of $\bar{\mathbb{F}}_p$. Take a set $\mathcal{S} \subseteq \mathbb{N}$, containing only prime numbers, which is not recursively enumerable. Now let L be the union of the $\mathbb{F}_{p^h}$, for all h whose prime factors all lie in $\mathcal{S}$. We claim that this field L is not recursive. If it were, imagine an algorithm which loops over all $\xi \in L$ and computes the smallest n such that $\xi^{p^n} = \xi$. The set $\{n \in \mathbb{N} \mid n \text{ is prime } \wedge\ (\exists \xi \in L)(\xi^{p^n} = \xi)\}$ would be r.e., but this is a contradiction because that set is exactly $\mathcal{S}$.

We can factor polynomials over a finite extension of the base field: given an element $\gamma \in L$ and its minimal polynomial $t(Z) \in K[Z]$, we can algorithmically factor polynomials over the field $K(\gamma)$. This means the following: suppose we are given an $f(Z) \in K[\gamma][Z]$, where the coefficients of f are given as polynomials in γ over K. Then we can algorithmically write $f(Z)$ as a product of irreducible polynomials in $K[\gamma][Z]$. For finite fields, this is trivial, since we just have to try finitely many polynomials to find the factors of a given polynomial. Of course, we can also use more fancy algorithms, see [Coh93, Section 3.4]. For factoring over number fields, there is an algorithm explained in [Coh93, Section 3.6.2]. The idea is that factoring $f(Z) \in K[\gamma][Z]$ can be done by factoring the norm of the polynomial $f(Z + k\gamma)$, for a suitable $k \in \mathbb{Z}$. This norm is an element of $\mathbb{Q}[Z]$, for which there are well-known factoring algorithms (see [Coh93, Section 3.5] or [LLL82]). It is important to understand that this factoring only works over *finite* extensions of the base field. It is not clear whether we can factor polynomials over $L[Z]$, if L is an infinite algebraic extension of the prime field K.

We write $\mathrm{Gal}(L/K)$ for the group of field-automorphisms of L fixing the elements of K, even if L/K is not a Galois extension. For example, if L would be the real closure of $\mathbb{Q}$, then $\mathrm{Gal}(L/K) = \{1\}$, and the field L is recursively stable. However, if $\mathrm{Gal}(L/K)$ is infinite it has to be uncountable because it is a profinite group (see [RZ00, Proposition 2.3.1]). Then the field L cannot be recursively stable, because it has too many automorphisms, as explained at the end of Section 3.3. So, in general we do not have a canonical definition of r.e. sets in L. Obviously, we need a way to avoid this problem. First we have a look at how different recursive presentations relate to one another.

Lemma 6.1. *Let K be $\mathbb{F}_p$ or $\mathbb{Q}$, and L be a recursive algebraic extension of K with infinitely many elements. Assume we have two recursive presentations $\sigma : L \xrightarrow{\sim} \mathbb{N}$ and $\theta : L \xrightarrow{\sim} \mathbb{N}$. Then there exists a recursive permutation π of $\mathbb{N}$ and an automorphism $\phi \in \mathrm{Gal}(L/K)$ such that $\pi \circ \sigma = \theta \circ \phi$.*



Remark. In recursion theory, structures satisfying this property are called *recursively categorical*. For many applications, this is as useful as recursively stable. But in our context it does make a difference whether we need an automorphim ϕ.

Proof. This proof will go as follows: we explain an algorithm to compute π. Then, while we construct the recursive function π, we will prove that $\phi := \theta^{-1} \circ \pi \circ \sigma$ is an automorphism. Note that the algorithm to compute π does not know at all about ϕ.

We will use some kind of induction to do this: we start by considering the base field K. We start π as a bijection between $\sigma(K)$ and $\theta(K)$, and ϕ as the identity on K. Then we continue to enlarge the set on which π and ϕ are defined. After every induction step, there will be a finite extension F/K such that $\phi \in \mathrm{Gal}(F/K)$ and π is a bijection between $\sigma(F)$ and $\theta(F)$, satisfying $\pi \circ \sigma_{|F} = \theta \circ \phi_{|F}$. In every step of the induction, F will be enlarged.

To start the proof, let ϕ be the identity on K and define π as the function which maps $a \in \sigma(K)$ to $\theta(\sigma^{-1}(a)) \in \theta(K)$. Since K is recursively stable, π is recursive.

Now we do the induction: Assume that we have a finite extension F/K, with F given as $K(\gamma)$ with $\gamma \in L$. To be more precise, the algorithm is given $\sigma(\gamma)$ and the minimal polynomial of γ, which is an element of $K[Z]$. We have a bijection π between $\sigma(F) \subset \mathbb{N}$ and $\theta(F) \subset \mathbb{N}$, and a $\phi \in \mathrm{Gal}(F/K)$ such that $\pi \circ \sigma = \theta \circ \phi$ on F. Then the algorithm knows π on $\sigma(F)$. Summarizing, the induction hypothesis consists of three things: the element $\sigma(\gamma)$, the minimal polynomial of γ and the function π on the set $\sigma(K(\gamma))$. For the latter, we will see later that it suffices to know $\theta(\phi(\gamma)) = \pi(\sigma(\gamma))$. A priori, we do not require that we can decide whether or not a given $x \in \mathbb{N}$ is in $\sigma(F)$ (but if it is, we must be able to compute $\pi(x)$).

Find the first element $a \in \mathbb{N}$ whose image under π is not yet known, in other words the first $a \in \mathbb{N}$ such that $\sigma^{-1}(a) \notin F$. If we write $\alpha := \sigma^{-1}(a)$, then a is the code for the element $\alpha \in L$. To check algorithmically whether $\alpha \in F = K(\gamma)$, we compute the minimal polynomial of α over F. To do this, we simply try all possible non-constant monic polynomials in $K[Z]$ until we find a $g(Z) \in K[Z]$

for which $g(\alpha) = 0$. Such a polynomial always exists, so eventually we will find one. As explained before, we can factor $g(Z)$ over F, so we can check for which irreducible factor $f(Z)|g(Z)$ we have $f(\alpha) = 0$. This is the minimal polynomial. If $f(Z)$ is linear, it must be equal to $Z - \alpha$, therefore $\alpha \in F$, and we try the next $a \in \mathbb{N}$. Assume now that we have found an $a \in \mathbb{N}$ such that $d := \deg(f)$ is greater than 1, then $\sigma^{-1}(a) = \alpha \notin F$.

We explain in more detail what it means to compute the minimal polynomial, because an algorithm can only work with natural numbers (representing elements of L via a recursive presentation). So, our algorithm cannot really compute the polynomial, but only the codes of the coefficients. The minimal polynomial of α over F will be represented as some numbers $a_i \in \sigma(F)$ such that $f(Z) = \sum_{i=0}^{n} \sigma^{-1}(a_i)Z^i$ is the actual minimal polynomial.

Then we would like to find a $b \in \mathbb{N}$ such that $\beta := \theta^{-1}(b)$ has the 'same' minimal polynomial. This means that the codes of the coefficients of the minimal polynomial are $b_i = \pi(a_i)$. Hence, the actual minimal polynomial of β will be $\sum \theta^{-1}(b_i)Z^i = (\phi f)(Z)$. In the algorithm, we try every $b \in \mathbb{N}$ and compute (in the sense as explained above) the minimal polynomial of $\theta^{-1}(b)$. If the codes of the coefficients are equal to $b_i = \pi(a_i)$, then we found the right b and we set $\pi(a) = b$. Together, $f(\alpha) = 0$ and $(\phi f)(\beta) = 0$ imply that ϕ can be extended to an element of $\mathrm{Gal}(F(\alpha)/K)$, mapping α to β.

In our induction step, we still have to show how we can compute π on $\sigma(F(\alpha))$. We already know how to do it on $\sigma(F)$ (the induction hypothesis), and we know that $\pi(a) = b$. Say we are given a $c \in \sigma(F(\alpha))$. Then c must be of the form

$$c = \sigma\left(\sum_{i=0}^{d-1} \varepsilon_i \alpha^i\right) \qquad \text{(for some } \varepsilon_i \in F\text{)}.$$

We just try all possible values for the $\sigma(\varepsilon_i) \in \sigma(F)$, then we can compute $\sigma(\sum \varepsilon_i \alpha^i)$, given $\sigma(\varepsilon_i)$ and $\sigma(\alpha) = a$. Eventually, we will find $\sigma(\varepsilon_i)$ for which $c = \sigma(\sum \varepsilon_i \alpha^i)$. Then

$$\pi(c) = \theta\left(\sum_{i=0}^{d-1} \phi(\varepsilon_i)\beta^i\right).$$

This can be computed, because we know $\theta(\beta) = b$ and $\theta(\phi(\varepsilon_i)) = \pi(\sigma(\varepsilon_i))$. Since $\varepsilon_i \in F$, we know $\pi(\sigma(\varepsilon_i))$ by the induction hypothesis.

To only thing which remains to do in the induction step is to write the field $F(\alpha) = K(\gamma, \alpha)$ as $K(\delta)$ for some $\delta \in L$. Since we do not care about efficiency, we can just try every $\delta \in L$, compute its minimal polynomial, check that the

degree is equal to $[F(\alpha) : F][K(\gamma) : K]$, and check that $K(\delta)$ contains γ and α. In order to know π on $\sigma(K(\delta))$, it suffices to know the image of $\sigma(\delta)$. So we keep track of 3 things: the element $\sigma(\delta) \in \mathbb{N}$, its image $\pi(\sigma(\delta))$ and the minimal polynomial (over K) of δ.

We would like to remark that there is also an efficient algorithm to find a δ for which $K(\gamma, \alpha) = K(\delta)$. This is explained in much detail in [Coh00, Section 2.1.5]. This algorithm is based on the fact that $K(\gamma, \alpha) = K(\gamma + k\alpha)$ for all but finitely many $k \in K$. Then the minimal polynomial of $\delta := \gamma + k\alpha$ can be computed using resultants. □

Since the definition of recursively enumerable sets depends on the recursive presentation chosen, we will restrict ourselves to a special class of r.e. sets in L, namely the sets $\mathcal{S} \subseteq L$ which are r.e. for every recursive presentation of L. In the following proposition, we will see that these sets can also be characterized algebraically: they are exactly the r.e. sets $\mathcal{S}$ for which there exists a finite extension F/K such that $\mathcal{S}$ is invariant (as a set, not pointwise) under $\mathrm{Gal}(L/F)$. In other words, the stabilizer of the set $\mathcal{S}$ has finite index in $\mathrm{Gal}(L/K)$. In the finite field case, this criterion simplifies to saying that there exists a $q = p^h$ such that $\mathcal{S}$ is invariant under the Frobenius $\xi \mapsto \xi^q$.

Proposition 6.2. *Let $\mathcal{S}$ be a subset of L, r.e. for some recursive presentation of L. Then $\mathcal{S}$ is r.e. for every recursive presentation $\theta : L \xrightarrow{\sim} \mathbb{N}$ if and only if $\mathcal{S}$ is invariant under* $\mathrm{Gal}(L/F)$ *for some finite extension F/K.*

Proof. If L/K is a finite extension, then the statement is trivially true. Indeed, since L is a finite extension of a prime field, it is recursively stable. If we take $F = L$, then we want the set $\mathcal{S}$ to be invariant under $\mathrm{Gal}(L/L) = \{\mathrm{id}_L\}$, which is obviously always true.

First, we do the "if" direction, so we assume that we have a finite extension F/K such that $\mathrm{Gal}(L/F)(\mathcal{S}) = \mathcal{S}$. Take two recursive presentations σ and θ of L and let π and ϕ be as in Lemma 6.1. Let $\mathcal{S}$ be r.e. for σ, this means by definition that $\sigma(\mathcal{S})$ is r.e. as a subset of $\mathbb{N}$. We have to prove that $\theta(\mathcal{S})$ is also r.e.. It is clear that $\theta(\phi(\mathcal{S}))$ is r.e., because $\theta(\phi(\mathcal{S})) = \pi(\sigma(\mathcal{S}))$ and π is recursive. Since $\mathrm{Gal}(L/F)(\mathcal{S}) = \mathcal{S}$, we can say that ϕ acts on $\mathcal{S}$ as an element of $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/F) \cong \mathrm{Gal}(F/K)$.

To show that $\theta(\mathcal{S})$ is r.e., we loop over all $a \in \theta(\phi(\mathcal{S}))$, these a's encode elements of $\phi(\mathcal{S})$. As explained in the proof of Lemma 6.1, we can compute the minimal polynomial $f(Z)$ over F of $\theta^{-1}(a)$. Since $\phi(\mathcal{S})$ is invariant under $\mathrm{Gal}(L/F)$, every

zero of f (and not just $\theta^{-1}(a)$) is an element of $\phi(\mathcal{S})$. Then every zero of $\phi^{-1}f$ is an element of $\mathcal{S}$. We use this to compute $\theta(\mathcal{S})$: the action of ϕ on the finite extension F is computable (indeed, writing $F = K(\gamma)$, we just need to know the image of γ), so we can compute $\phi^{-1}f$. Then, we try all elements of $b \in \mathbb{N}$ and check whether $\theta^{-1}(b)$ is a zero of $\phi^{-1}f$, until we have found all zeros of $\phi^{-1}f$. This way, we will eventually find exactly all elements of $\theta(\mathcal{S})$.

Conversely, assume that there is no $\mathrm{Gal}(L/F)$ with $[F : K]$ finite which stabilizes $\mathcal{S}$, but that $\theta(\mathcal{S})$ is r.e. for every θ. We have to find a contradiction. Fix one particular recursive presentation θ. If ϕ is any automorphism of L, then $\theta\circ\phi$ is also a recursive presentation. We will construct a subset $A \subseteq \mathrm{Gal}(L/K)$ of cardinality $2^{\aleph_0}$ such that $\phi_1(\mathcal{S}) \neq \phi_2(\mathcal{S})$ for any two elements $\phi_1 \neq \phi_2$ of A. Since θ is a bijection, we get $2^{\aleph_0}$ different sets $\theta(\phi(\mathcal{S}))$ if ϕ runs through A. These should all be r.e., which is a contradition, since there exist only $\aleph_0$ different r.e. sets.

We start by constructing an infinite chain of finite extensions $K = F_0 \subset F_1 \subset F_2 \subset \ldots$ and elements $\phi_k \in \mathrm{Gal}(L/F_k)$ as follows: Given F_k, we know that $\mathcal{S}$ is not invariant under $\mathrm{Gal}(L/F_k)$, let $\phi_k \in \mathrm{Gal}(L/F_k)$ be outside of the stabilizer of $\mathcal{S}$. Since $\phi_k(\mathcal{S}) \neq \mathcal{S}$, there exists a finite extension F_{k+1}/F_k such that $\mathcal{S} \cap F_{k+1}$ is not invariant under ϕ_k. We write F_∞ for the inductive limit of this infinite chain.

Now we are ready to define the set $A \subseteq \mathrm{Gal}(L/K)$: For any subset $I \subseteq \mathbb{N}$, we define $\phi_I \in \mathrm{Gal}(F_\infty/K)$ as the composition of all ϕ_i for which $i \in I$. The order of composition should be such that $\phi_{\mathbb{N}} = \ldots \circ \phi_2 \circ \phi_1 \circ \phi_0$. Clearly, ϕ_I can be an infinite composition, but this still defines an element of $\mathrm{Gal}(F_\infty/K)$ because at every finite level F_k/K only finitely many ϕ_i act non-trivially (those with $i < k$). Since $F_\infty \subseteq L$, every ϕ_I can be extended (non-canonically) to an element of $\mathrm{Gal}(L/K)$. Let A be the set of all these extended ϕ_I, then A has $2^{\aleph_0}$ elements.

It remains to prove that $\phi_I(\mathcal{S}) \neq \phi_J(\mathcal{S})$ for $I \neq J$. Take sets $I, J \subseteq \mathbb{N}$ with $I \neq J$, and take the minimal $i \in \mathbb{N}$ where I and J differ. We may assume without loss of generality that $i \in I \setminus J$ (otherwise, exchange I and J). Consider $\mathcal{S} \cap F_{i+1}$. On this set, the automorphism $\phi_I \circ \phi_J^{-1}$ acts like ϕ_i. But by our construction, $\mathcal{S} \cap F_{i+1}$ in not invariant under ϕ_i. Therefore, $\phi_I(\mathcal{S} \cap F_{i+1}) \neq \phi_J(\mathcal{S} \cap F_{i+1})$, hence $\phi_I(\mathcal{S}) \neq \phi_J(\mathcal{S})$. □

This whole discussion was for the field L, but it also applies to the polynomial ring $L[Z]$. In [FS56, Theorem 3.1], it is proven that $L[Z]$ is recursive, whenever L is. We can extend all automorphisms $\phi \in \mathrm{Gal}(L/K)$ to automorphisms on $L[Z]$ by setting $\phi(Z) = Z$. In other words, we let automorphisms just work on the coefficients of polynomials. In $L[Z]$, we will work with sets $\mathcal{S}$ which are r.e.

for every recursive presentation $L[Z] \xrightarrow{\sim} \mathbb{N}$. As in Proposition 6.2 above, one can prove that such a set $\mathcal{S}$ will be invariant under $\mathrm{Gal}(L/F)$ for a finite extension F/K.

In the number field case, we will actually work with the ring of integers $\mathcal{O}_L$ instead of the field L, but again this does not really make a difference. The set $\mathcal{O}_L$ is a recursive subset of L, because we can check whether the monic minimal polynomial of an element $\alpha \in L$ has coefficients in $\mathbb{Z}$ (as opposed to $\mathbb{Q}$).

6.2 Outline

We will now state the Main Theorem, but first we specify some notation. As before, K is either $\mathbb{Q}$ or $\mathbb{F}_p$, with p prime. In the case $K = \mathbb{Q}$ (we will call this the "number field case"), L is a totally real recursive algebraic extension of $\mathbb{Q}$. "Totally real" means that every embedding $L \hookrightarrow \mathbb{C}$ has its image in $\mathbb{R}$. Then $\mathcal{O}_L$ is the integral closure of $\mathbb{Z}$ in L, and $\mathcal{R} := \mathcal{O}_L[Z_1, \ldots, Z_n]$ for some $n \geq 1$. In the finite field case, L is an infinite recursive algebraic extension of $K = \mathbb{F}_p$, and $\mathcal{R} := L[Z]$. To make statements more uniform though, we define $\mathcal{O}_L := L$ and $Z_1 := Z$ with $n = 1$ in the finite field case. This way, $\mathcal{R} = \mathcal{O}_L[Z_1, \ldots, Z_n]$ in both cases.

The plan is to prove that the diophantine sets $\mathcal{S} \subseteq \mathcal{R}$ are exactly the sets which are r.e. for every recursive presentation of $\mathcal{R}$. We write F for the finite extension of K such that $\mathcal{S}$ is invariant under $\mathrm{Gal}(L/F)$, as in Proposition 6.2. Then $\mathcal{O}_F$ is the integral closure of $\mathbb{Z}$ in F (number field case) or $\mathcal{O}_F = F$ (finite field case).

There is another, algebraic, reason why we need the assumption that $\mathcal{S}$ is invariant under some $\mathrm{Gal}(L/F)$: take any diophantine subset $\mathcal{D}$ of $\mathcal{R}$. In the polynomial used to define $\mathcal{D}$, only finitely many elements from L can appear. This is true even if we allow an infinite language. Let F be the field generated by these elements of L, this is a finite extension of K. Then the polynomial to define $\mathcal{D}$ is invariant under $\mathrm{Gal}(L/F)$, so $\mathcal{D}$ also has to be invariant.

Eventually, we will prove:

Main Theorem 6.3. *With notations as above, a set $\mathcal{S} \subseteq \mathcal{R}^k$ is diophantine if and only if $\mathcal{S}$ is recursively enumerable and $\mathrm{Gal}(L/F)(\mathcal{S}) = \mathcal{S}$ for some finite extension F of K. Moreover, an r.e. set invariant under $\mathrm{Gal}(L/F)$ can be diophantinely defined using only constants from $\mathcal{O}_F[Z_1, \ldots, Z_n]$.*

The prove this Main Theorem, we have to do the following five steps:

1. **Defining constants**. Diophantinely define the ring of constants $\mathcal{O}_L$ in $\mathcal{R}$.
2. **Bounding predicate**. Give an extension-effective diophantine bounding predicate for the ring $\mathcal{R}$. This defines a sequence of sets $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2, \ldots$ such that every $\mathcal{A}_e$ is a finite subset of $\mathcal{R}$ and such that every finite subset of $\mathcal{R}$ is contained in at least one $\mathcal{A}_e$. We will give a more precise definition in Section 6.3 below, and explain what it means for such a predicate to be extension-effective.
3. **Defining $\mathcal{O}_F[Z]$**. Give a diophantine definition of $\mathcal{O}_F[Z]$ in $\mathcal{R}$ (where Z means Z_1 if we have more than 1 variable).
4. **Distinguishing lemma**. For $P \in \mathcal{R}$ and $\{Q_1, \ldots, Q_m\} \subset \mathcal{R}$ such that P is not $\mathrm{Gal}(L/F)$-conjugate to any Q_i, we can find an $\overrightarrow{\alpha} \in \mathcal{O}_L^n$ such that $P(\overrightarrow{\alpha}^{\overrightarrow{\sigma}}) \neq Q_i(\alpha)^\tau$ for any $\overrightarrow{\sigma} \in \mathrm{Gal}(L/F)^n$, $\tau \in \mathrm{Gal}(L/F)$ and $i \in \{1, \ldots, m\}$. (If $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\overrightarrow{\sigma} = (\sigma_1, \ldots, \sigma_n)$, then the notation $\overrightarrow{\alpha}^{\overrightarrow{\sigma}}$ means $(\alpha_1^{\sigma_1}, \ldots, \alpha_n^{\sigma_n})$.)

   This generalizes the well known fact that for two polynomials $P \neq Q$ over an infinite field, there is a value α such that $P(\alpha) \neq Q(\alpha)$.

   We call it the *distinguishing lemma* because it is a way to distinguish between finitely many polynomials. The bounding predicate is used to select finitely many polynomials in $\mathcal{R}$, and then the distinguishing lemma can be used to select one polynomial (actually, one conjugacy class).
5. **Finishing the proof**. By considering minimal polynomials of elements of $\mathcal{O}_L$, reduce the problem to diophantine definitions inside $\mathcal{O}_F[Z]$, where we know that r.e. sets are diophantine.

Except for the last step, the proofs will be very different in the number field and finite field case. In Section 6.4, we prove the first 4 steps in the number field case, and in Section 6.5 we do the same in the finite field case. Then we will do the last step uniformly in Section 6.6.

6.3 Bounding predicates

First, we explain the second step of the outline.

Definition 6.4. Let $\mathcal{R}$ be a ring. A *bounding predicate* for $\mathcal{R}$ is a relation $\delta(X, e)$ with $X \in \mathcal{R}$ and $e \in \mathbb{N}$, such that:

1. If e is fixed, then there are only finitely many X's in $\mathcal{R}$ satisfying $\delta(X, e)$.
2. Let $\mathcal{B}$ be a finite subset of $\mathcal{R}$. Then there exists an $e \in \mathbb{N}$ such that $\delta(X, e)$ for all $X \in \mathcal{B}$.

We call a bounding predicate *effective* if it satisfies the additional property

3. There exists an algorithm, which, given $e \in \mathbb{N}$, produces a list of all X's in $\mathcal{R}$ satisfying $\delta(X, e)$. This algorithm must eventually halt when the list is finished. Remark that this is stronger than requiring that δ is a recursive relation.

Obviously, we are only interested in *diophantine* bounding predicates. In order for a bounding predicate to be diophantine, the ring $\mathcal{R}$ needs to have a diophantine interpretation of $\mathbb{N}$. Then δ is called diophantine if the following set is diophantine:

$$\{(X, \overrightarrow{E}) \in \mathcal{R} \times \mathcal{R}^r \mid (\exists e)(\overrightarrow{E} \text{ represents } e \text{ in the interpretation } \wedge\ \delta(X, e)\}.$$

Example 6.5. We already saw an effective diophantine bounding predicate for $\mathbb{F}_q[Z]$. Indeed, the predicate "$\deg(X) \leq e$" is diophantine (see Section 5.3), and clearly satisfies the three conditions above.

It turns out that our notion of effectiveness is too strong. The problem is that the algorithm has to know the ring $\mathcal{R}$ very well. For starters, it only works when $\mathcal{R}$ is a recursive ring. Bounding predicates for a polynomial ring will often be of the form "X divides some polynomial P_e". To find all X's satisfying this, we just have to factor P_e and then combine the factors, and multiply with units. However, if $P_e = Z^2 - 5$ for example, then the algorithm might not know whether $\sqrt{5}$ is in $\mathcal{R}$. This is what we mean when we said that the algorithm has to "know" the ring $\mathcal{R}$. So, we give a weaker notion of effectiveness:

Definition 6.6. A bounding predicate $\delta(X, e)$ for a ring $\mathcal{R}$ is called *extension-effective* if there exists a recursive ring $\mathcal{S} \supseteq \mathcal{R}$ and an algorithm which does the following: on input $e \in \mathbb{N}$, it produces a finite set $\mathcal{B}_e \subseteq \mathcal{S}$ such that $\mathcal{B}_e \cap \mathcal{R}$ is exactly the set of X's in $\mathcal{R}$ satisfying $\delta(X, e)$.

So, in the example given above, if $\mathcal{S}$ contains $\sqrt{5}$, then $\mathcal{B}_e$ would be $\{1, Z + \sqrt{5}, Z - \sqrt{5}, Z^2 - 5\}$, multiplied with units. Then it does not matter whether $\sqrt{5}$ is in $\mathcal{R}$ or not.

6.4 Number field case

We recall some notation from Section 6.2: L is a totally real algebraic extension of $K = \mathbb{Q}$, and F is a finite extension of $\mathbb{Q}$ (a number field) contained in L. We write $\mathcal{O}_L$ resp. $\mathcal{O}_F$ for the integral closure of $\mathbb{Z}$ inside L resp. F. Then $\mathcal{R} = \mathcal{O}_L[Z_1, \ldots, Z_n]$ for some $n \geq 1$.

First, we have to give a diophantine definition of the ring of constants $\mathcal{O}_L$. In characteristic zero, this has traditionally (see for example [DP63, Lemma 3.1] for $\mathbb{Z}[Z]$) been done using a Pell equation $A^2 - dB^2 = 1$ with $d > 0$. But this method only works whenever d is not a square, then $A^2 - dB^2$ is the norm form from $\mathbb{Q}(\sqrt{d})$. In our setting, L could be the totally real closure of $\mathbb{Q}$, and then every $d \in \mathbb{N}$ becomes a square. However, the degree 3 number field $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\xi]/(\xi^3 - 2)$ is not totally real, so we work with that instead.

Lemma 6.7 (Defining constants)**.** *We can define the constants in $\mathcal{R}$ as follows:*

$$
\begin{aligned}
& X \in \mathcal{O}_L && (6.1)\\
& \quad \Updownarrow \\
& (\exists A, B, C, U, V, W) \\
& \qquad A^3 + 2B^3 + 4C^3 - 6ABC = 1 && (6.2)\\
& \wedge\ A = 1 + UX \ \wedge\ B = VX \ \wedge\ C = WX && (6.3)\\
& \wedge\ (U \neq 0 \ \vee\ V \neq 0 \ \vee\ W \neq 0). && (6.4)
\end{aligned}
$$

Proof. The form in (6.2) is a norm form from the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Since L is a totally real field, it cannot contain $\sqrt[3]{2}$. Therefore, the field $L(\sqrt[3]{2})$ is a degree 3 extension of L. One can check that $\mathbb{Z}[\sqrt[3]{2}]$ is the integral closure of $\mathbb{Z}$ inside $\mathbb{Q}(\sqrt[3]{2})$ and that the unit group of $\mathbb{Z}[\sqrt[3]{2}]$ is generated by -1 and $\sqrt[3]{2} - 1$, with norm $\mathrm{N}(\sqrt[3]{2} - 1) = 1$.

Assume $X \in \mathcal{O}_L$. If $X = 0$, then set $A = 1$, $B = 0$, $C = 0$ and $U = V = W = 1$. We continue with the case $X \neq 0$. Let E be a number field containing X and $\sqrt[3]{2}$, then $X \in \mathcal{O}_E$. Let $u := \sqrt[3]{2} - 1$, which is the fundamental unit of $\mathbb{Z}[\sqrt[3]{2}]$. Consider the finite ring $\mathcal{O}_E/(X)$. Since u is a unit, the reduction $\bar{u}$ in $\mathcal{O}_E/(X)$ is still a unit. The multiplicative group $(\mathcal{O}_E/(X))^*$ is finite, therefore there exists a $k > 0$ such that $u^k \equiv 1 \mod (X)$. Write $u^k = A + B\sqrt[3]{2} + C\sqrt[3]{4}$ with $A, B, C \in \mathbb{Z}$. From $\mathrm{N}(u) = 1$ it follows that $\mathrm{N}(u^k) = A^3 + 2B^3 + 4C^3 - 6ABC = 1$, proving (6.2). The congruence $u^k \equiv 1 \mod (X)$ means that there exists a $U + V\sqrt[3]{2} + W\sqrt[3]{4}$ (with $U, V, W \in \mathcal{O}_E \subseteq L$) for which

$$(A - 1) + B\sqrt[3]{2} + C\sqrt[3]{4} = (U + V\sqrt[3]{2} + W\sqrt[3]{4})X.$$

Since $X \in L$, we can consider it as a scalar in the 3-dimensional L-vector space $L(\sqrt[3]{2})$. The formulas (6.3) follow. Now if (6.4) were not satisfied, then $u^k = 1$, which is excluded since $k > 0$ and u is a fundamental (non-torsion) unit.

Conversely, assume (6.2)–(6.4), but that X is non-constant. Assume that $U \neq 0$ (the other cases are analogous), then $A - 1$ (and hence A) is non-constant. If A depends on more than one variable, we specialize all but one variable to some value, such that $A \in \mathcal{O}_L[Z] \setminus \mathcal{O}_L$. Let $d := \max(\deg(A), \deg(B), \deg(C))$, then $d \geq 1$ because A is non-constant. Write a resp. b resp. c for the coefficient of Z^d in A resp. B resp. C. Then it follows from (6.2) that $a^3 + 2b^3 + 4c^3 - 6abc = 0$. But this is the $L(\sqrt[3]{2})/L$-norm of $a + b\sqrt[3]{2} + c\sqrt[3]{4}$. The only way that this norm can be zero is that $a = b = c = 0$, which contradicts the definition of d. □

Next, we will diophantinely define $\mathbb{Z}[Z_1, \ldots, Z_n]$ inside $\mathcal{R} = \mathcal{O}_L[Z_1, \ldots, Z_n]$. This will be the basis for the bounding predicate, as well as the diophantine definition of $\mathcal{O}_F[Z_1]$.

This is based on [Zah99] and [Den78b]. In this part of the proof we have to use that L is totally real. If P is a function with values in L, then P is called *positive definite* if $\sigma(P(\overrightarrow{X})) \geq 0$ for all $\overrightarrow{X}$ and all embeddings $\sigma : L \hookrightarrow \mathbb{R}$. We denote this with $P \gg\gg 0$, then the notation $P \lll Q$ means that $Q - P$ is positive definite.

Proposition 6.8. *The set of all positive definite polynomials in $\mathcal{R}$ is diophantine.*

Proof. Zahidi proves (see [Zah99, II (5.5)]) that the positive definite rational functions over a totally real field are exactly those which are a sum of squares in $L(Z_1, \ldots, Z_n)$.

We can use this to make a diophantine definition, provided that we have a bound on the number of squares needed. The minimal s such that any sum of squares can be written as the sum of s squares, is called the *Pythagoras number* of the field. For $L(Z_1, \ldots, Z_n)$, it follows from the Milnor Conjectures that $s \leq 2^{n+2}$ (see [Pfi00, Section 6, application 4] where there are also references to sharper bounds).

If s is the Pythagoras number of $L(Z_1, \ldots, Z_n)$, it follows that an element $P \in \mathcal{R}$ is positive definite if and only if

$$(\exists A_1, \ldots, A_s)(\exists B_1, \ldots, B_s)$$
$$(B_1 \neq 0 \ \wedge \ \ldots \ \wedge \ B_s \neq 0) \ \twoheadrightarrow \ P = \left(\frac{A_1}{B_1}\right)^2 + \cdots + \left(\frac{A_s}{B_s}\right)^2.$$

□

To prove that $\mathbb{Z}[Z_1, \dots, Z_n]$ is diophantine in $\mathcal{R}$, we first want $\mathbb{Z}$ to be diophantine. Using Lemma 6.7, we can already define $\mathcal{O}_L$. Then Zahidi proves ([Zah99, III (3.5)]) that we can define $\mathbb{Z}$ once we can define constants. This is based on the fact that $\mathrm{Y}_k(1) = k$, with Y_k the $(k-1)$-th Chebyshev polynomial of the second kind. The Chebyshev polynomials are (up to sign) exactly the solutions of the Pell equation $X^2 - (Z^2 - 1)Y^2 = 1$.

Lemma 6.9. *Consider a recursive presentation $\theta : \mathbb{Z}[Z_1, \dots, Z_n] \xrightarrow{\sim} \mathbb{N}$, and write $P^{(e)}$ for the e-th polynomial of $\mathbb{Z}[Z_1, \dots, Z_n]$, i.e. $P^{(e)} := \theta^{-1}(e)$. Let X_k and Y_k stand for the k-th Chebyshev polynomial of the first and second kind, respectively. The following is a diophantine definition of the polynomials with coefficients in $\mathbb{Z}$:*

$$
\begin{aligned}
& Q \in \mathbb{Z}[Z_1, \dots, Z_n] && (6.5)\\
& \quad \Updownarrow \\
& (\exists c, d, e \in \mathbb{N}) \\
& \qquad d \geq \deg_{\text{total}} \left(P^{(e)} \right) && (6.6)\\
& \qquad \wedge\ {P^{(e)}}^2 \lll cY_{d+1}(2 + Z_1^2 + \cdots + Z_n^2) && (6.7)\\
& \wedge\ (\exists u_1, \dots, u_n \geq d)(\forall a \in \{2, 3, 4, \dots, nd^2, nd^2 + 1, nd^2 + 2\}) \\
& \qquad \left.\begin{aligned}
& 4cY_{d+1}(a) < (u_1 - d)^2 \\
& \wedge\ 4cY_{d+1}(u_1^2 + a) < (u_2 - d)^2 \\
& \wedge\ \cdots\cdots\cdots \\
& \wedge\ 4cY_{d+1}(u_1^2 + \cdots + u_{n-1}^2 + a) < (u_n - d)^2
\end{aligned}\right\} && (6.8)\\
& \wedge\ (\exists v \in \mathbb{Z}) \\
& \qquad \wedge\ P^{(e)}(\overrightarrow{u}) = v && (6.9)\\
& \wedge\ (\exists X, Y) \\
& \qquad X^2 + \big((2 + Z_1^2 + \cdots + Z_n^2)^2 - 1\big)Y^2 = 1 && (6.10)\\
& \qquad \wedge\ Y(0, \dots, 0) = d + 1 && (6.11)\\
& \qquad \wedge\ Q^2 \lll cY && (6.12)\\
& \qquad \wedge\ Q(\overrightarrow{u}) = v. && (6.13)
\end{aligned}
$$

Diophantineness. Formulas (6.6)–(6.9) depend only on natural numbers, hence they are diophantine by DPRM. Formula (6.10) is clearly diophantine, and (6.12) is diophantine because of Proposition 6.8. Formula (6.13) is equivalent to

$$(\exists M_1, \dots, M_n)(Q - v = M_1(Z_1 - u_1) + \cdots + M_n(Z_n - u_n)),$$

which is clearly diophantine (this generalizes Example 2.5). Analogously, (6.11) is diophantine.

Proof. First, we will prove that, given $Q = P^{(e)}$, we can find c, d, $\overrightarrow{u}$ and v such that (6.6)–(6.9) are satisfied. Second, given c, d, $\overrightarrow{u}$ and v, there is at most one polynomial Q satisfying (6.10)–(6.13). Since $P^{(e)}$ satisfies these four formulas, it follows that $Q = P^{(e)}$, proving that $Q \in \mathbb{Z}[Z_1, \ldots, Z_n]$.

Assume (6.5). Then Q must be equal to some $P^{(e)}$. Let d be the total degree of $P^{(e)}$, as in (6.6) (set $d = 0$ for $Q = 0$).

We claim that we can always find a $c \in \mathbb{N}$ large enough such that (6.7) is satisfied. Because both $P^{(e)}$ and cY_{d+1} have coefficients in $\mathbb{Z}$, the embedding $\sigma : L \hookrightarrow \mathbb{R}$ in the definition of "positive definite" only applies to the variables Z_i. But then, $\sigma(Z_i)$ is simply a real number, so it suffices to prove that

$$P^{(e)}(Z_1, \ldots, Z_n) \leq cY_{d+1}(2 + Z_1^2 + \cdots + Z_n^2) \qquad \text{for all } \overrightarrow{Z} \in \mathbb{R}^n \tag{6.14}$$

We know that Y_{d+1} has degree d, so we can write

$$\mathrm{Y}_{d+1} = \sum_{i=0}^{d} a_i Z^i \qquad (a_i \in \mathbb{Z}).$$

Moreover, one can prove that the leading coefficient a_d equals 2^d. Let $a \in \mathbb{R}$ such that $|a_i| < a$ for every coefficient a_i. If $\overrightarrow{Z} = (Z_1, \ldots, Z_n)$, then the notation $||\overrightarrow{Z}||$ stands for $\sqrt{Z_1^2 + \cdots + Z_n^2}$. Writing $T := 2 + Z_1^2 + \cdots + Z_n^2 = 2 + ||\overrightarrow{Z}||^2$ (hence $T \geq 2$), we get

$$\begin{aligned}
\mathrm{Y}_{d+1}(T) &= a_d T^d - \sum_{i=0}^{d-1} (-a_i) T^i \geq T^d - \sum_{i=0}^{d-1} |a_i| T^i \\
&\geq T^d - a \sum_{i=0}^{d-1} T^i = T^d - a \frac{T^d - 1}{T - 1} \\
&\geq T^d \left(1 - \frac{a}{T-1}\right) \geq ||\overrightarrow{Z}||^{2d} \left(1 - \frac{a}{1 + ||\overrightarrow{Z}||^2}\right).
\end{aligned}$$

Since $P^{(e)}$ has degree at most d, there exists a $b \in \mathbb{R}$ such that $|P^{(e)}(\overrightarrow{Z})| \leq b||\overrightarrow{Z}||^d$ for all $\overrightarrow{Z} \in \mathbb{R}^n$.

If $\overrightarrow{Z}$ is such that $||\overrightarrow{Z}|| \geq \sqrt{2a-1}$, then $a/(1+||\overrightarrow{Z}||^2)$ is at most $1/2$. So, if we choose $c \geq 2b^2$, then (6.14) holds for all $\overrightarrow{Z}$ with $||\overrightarrow{Z}|| \geq \sqrt{2a-1}$, because

$$P^{(e)^2}(\overrightarrow{Z}) \leq b^2||\overrightarrow{Z}||^{2d} = c||\overrightarrow{Z}||^{2d}\frac{1}{2} \leq c||\overrightarrow{Z}||^{2d}\left(1 - \frac{a}{1+||\overrightarrow{Z}||^2}\right) \leq c\mathrm{Y}_{d+1}(T).$$

Another property of the Chebyshev polynomials X_k and Y_k is that all their zeros are in the real interval $[-1,1]$. In particular, $\mathrm{Y}_{d+1}(T)$ cannot be zero, because $T \geq 2$. Then $P^{(e)^2}(\overrightarrow{Z})/\mathrm{Y}_{d+1}(T)$ is a continuous function, hence bounded on the closed ball $\{\overrightarrow{Z} \in \mathbb{R}^n \mid ||\overrightarrow{Z}|| \leq \sqrt{2a-1}\}$. Therefore, we can choose a c large enough such that (6.14) also holds inside that ball.

Now choose the u_i's large enough to satisfy (6.8). The order of constructing the u_i's is important, because every u_k depends on the previous $u_1, \ldots, u_{k-1}$. Then set v equal to $P^{(e)}(u_1, \ldots, u_n)$, as in (6.9). Let $X := \mathrm{X}_{d+1}(2 + Z_1^2 + \cdots + Z_n^2)$ and $Y := \mathrm{Y}_{d+1}(2 + Z_1^2 + \cdots + Z_n^2)$, formula (6.10) follows. Then (6.11) is also true because $Y(0, \ldots, 0) = \mathrm{Y}_{d+1}(1) = d+1$. Finally (6.12) and (6.13) are equivalent to (6.7) and (6.9).

Conversely, assume (6.6)–(6.13). From (6.10) it follows that $X = \mathrm{X}_k(2 + Z_1^2 + \cdots + Z_n^2)$ and $Y = \mathrm{Y}_k(2 + Z_1^2 + \cdots + Z_n^2)$ for some $k \in \mathbb{Z}$. Then formula (6.11) says that $k = d+1$.

We claim that (6.12) implies that Q has total degree at most d. Indeed, assume that $k := \deg_{\text{total}}(Q) > d$ and let Q_0 be the sum of all terms of Q having degree k. Choose $(a_1, \ldots, a_n) \in L^n$ such that $Q_0(a_1, \ldots, a_n) \neq 0$. Using this, we write all variables in function of just one: Let $Z_1 := a_1 Z$, $\ldots$, $Z_n := a_n Z$. Then $Q(a_1 Z, \ldots, a_n Z)$ is a polynomial in $L[Z]$ of degree at least $d+1$, and Q^2 is positive definite of degree at least $2d+2$. However, $cY(a_1 Z, \ldots, a_n Z) = cY_{d+1}(2 + (a_1^2 + \cdots + a_n^2)Z^n)$ has degree $2d$. Formula (6.12) says that Q^2 is dominated by cY, but by comparing degrees we see that this is impossible.

If we can prove that $Q = P^{(e)}$, then it follows immediately that $Q \in \mathbb{Z}[Z_1, \ldots, Z_n]$. Assume, in order to get a contradiction, that $Q \neq P^{(e)}$. Let $S := Q - P^{(e)}$, then $S(\overrightarrow{u}) = 0$ because of (6.9) and (6.13). We can write S in the following form:

$$\begin{aligned} S(\overrightarrow{Z}) = {} & S_1(Z_1, \ldots, Z_n)(Z_1 - u_1) + S_2(Z_2, \ldots, Z_n)(Z_2 - u_2) \\ & + \cdots + S_{n-1}(Z_{n-1}, Z_n)(Z_{n-1} - u_{n-1}) + S_n(Z_n)(Z_n - u_n). \end{aligned} \quad (6.15)$$

Here S_1 is the quotient of the Euclidean division $S/(Z_1 - u_1)$. Then the remainder R_1 has degree less than 1 in Z_1, hence R_1 does not depend on Z_1. Next, we divide

R_1 by $(Z_2 - u_2)$, we let S_2 be this quotient, and we get a new remainder R_2 not depending on Z_1 nor Z_2. We continue like this, then every S_i depends only on the variables $\{Z_i, Z_{i+1}, \ldots, Z_n\}$. In the end, we have a remainder R_n which is a constant. But both sides of (6.15) are 0 in the point $\overrightarrow{u}$, therefore this remainder must be zero.

Since the degree of S is at most d, there must be a vector $\overrightarrow{z} \in \{0, 1, \ldots, d\}^n$ for which $S(\overrightarrow{z}) \neq 0$. Take the largest k for which $S_k(\overrightarrow{z}) \neq 0$. We now evaluate (6.15) in the point $\overrightarrow{w} := (u_1, \ldots, u_{k-1}, z_k, \ldots, z_n)$. Then the first $k-1$ terms vanish and we get

$$S(\overrightarrow{w}) = \sum_{i=k}^{n} S_i(u_1, \ldots, u_{k-1}, z_k, \ldots, z_n)(z_i - u_i).$$

But S_i with $i \geq k$ does not depend on the first $k-1$ variables, so we also have

$$S(\overrightarrow{w}) = \sum_{i=k}^{n} S_i(\overrightarrow{z})(z_i - u_i) = S_k(\overrightarrow{z})(z_k - u_k).$$

In the last equality we used that $S_i(\overrightarrow{z}) = 0$ for $i > k$ (this is how we chose k).

Because $S_k(\overrightarrow{z})$ is an algebraic integer, it follows that $|S_k(\overrightarrow{z})|_{\mathfrak{p}} \leq 1$ for every non-archimedean ('finite') absolute value $|\ |_{\mathfrak{p}}$. Now the product formula for absolute values implies that there exists at least one achimedean ('infinite') absolute value for which $|S_k(\overrightarrow{z})| \geq 1$. Since L is totally real, there is an embedding $\sigma : L \hookrightarrow \mathbb{R}$ such that $|x| = +\sqrt{\sigma(x^2)}$ for all $x \in L$. For this absolute value, it follows that

$$|S(\overrightarrow{w})| = |S_k(\overrightarrow{z})| \cdot |z_k - u_k| \geq |z_k - u_k| \geq u_k - d.$$

Taking squares, this becomes

$$\sigma(S(\overrightarrow{w})) \geq (u_k - d)^2. \tag{6.16}$$

On the other hand, using (6.7) and (6.12) we also have

$$\begin{aligned} |S(\overrightarrow{w})| &\leq |P^{(e)}(\overrightarrow{w})| + |Q(\overrightarrow{w})| \\ &\leq +\sqrt{\sigma\big(cY_{d+1}(2 + ||\overrightarrow{w}||^2)\big)} + \sqrt{\sigma\big(cY(\overrightarrow{w})\big)}. \end{aligned} \tag{6.17}$$

Since $Y(\overrightarrow{Z}) = \mathrm{Y}_{d+1}(2 + ||\overrightarrow{Z}||^2)$, both these square roots are equal. We may omit the σ because $\overrightarrow{w}$ has coordinates in $\mathbb{Z}$ and Y_{d+1} is defined over $\mathbb{Z}$. Squaring (6.17), we get

$$\sigma(S(\overrightarrow{w})) \leq 4cY_{d+1}(2 + u_1^2 + \cdots + u_{k-1}^2 + z_k^2 + \cdots + z_n^2).$$

Keeping in mind that every z_i satisfies $0 \leq z_i \leq d$, we can use one of the inequalities from (6.8) to find $\sigma(S(\overrightarrow{w})) < (u_k - d)^2$, contradicting (6.16) □

Once we have this, it is easy to make the bounding predicate:

Lemma 6.10 (Bounding predicate)**.** *As in the previous lemma, consider a recursive presentation $\theta : \mathbb{Z}[Z_1, \dots, Z_n] \xrightarrow{\sim} \mathbb{N}$, and write $P^{(e)}$ for $\theta^{-1}(e)$. Then "$(XZ_1+1)|P^{(e)}$" is an extension-effective diophantine bounding predicate for $\mathcal{R}$.*

Proof. Let us start by proving that this is a bounding predicate. For the first property, we fix an $e \in \mathbb{N}$. Then $P^{(e)}$ has only finitely many divisors, up to units. But for every divisor $D|P^{(e)}$, there can be at most one unit u such that $uD \equiv 1 \bmod Z_1$. It follows that $P^{(e)}$ has only finitely many divisors of the form $XZ_1 + 1$.

For the second property, consider a finite set $\mathcal{B} \subset \mathcal{R}$ and let $e \in \mathbb{N}$ be such that

$$P^{(e)} = \mathrm{N}\left(\prod_{X \in \mathcal{B}} XZ_1 + 1\right).$$

Here N stands for the absolute norm of the number field generated by the coefficients of the X's in $\mathcal{B}$. This implies that the right hand side is indeed an element of $\mathbb{Z}[Z_1, \dots, Z_n]$, so it is equal to some $P^{(e)}$.

To prove that "$(XZ_1+1)|P^{(e)}$" is diophantine, we have to use Zahidi's result (see [Zah99, Chapter III]) that r.e. relations in $\mathbb{Z}[Z_1, \dots, Z_n]$ are diophantine. Then Theorem 3.12 proves that $P^{(e)}$ is a diophantine function of e, inside $\mathbb{Z}[Z_1, \dots, Z_n]$. Since $\mathbb{Z}[Z_1, \dots, Z_n]$ is a diophantine subset of $\mathcal{R}$, it follows that "$(XZ_1+1)|P^{(e)}$" is diophantine.

To prove that the bounding predicate is extension-effective, we consider the extension $\bar{\mathbb{Q}}[Z_1, \dots, Z_n]$ of $\mathcal{R}$. This ring is recursive, because $\bar{\mathbb{Q}}$ is recursive (see [Rab60]). Given $e \in \mathbb{N}$, we consider $P^{(e)}$ and factor it over $\bar{\mathbb{Q}}[Z_1, \dots, Z_n]$. Then we can compute all divisors of $P^{(e)}$ of the form $XZ_1 + 1$.

Multivariate factoring is a difficult problem, but can be done algorithmically. It is described briefly in [vzGG03, Section 16.6]. The idea is to reduce to factoring in 2 variables by substituting $Z_3, \dots, Z_n$ by some suitable linear combination of Z_1 and Z_2. There exists an algorithm based on lattice basis reduction to factor bivariate polynomials. Originally, this method was developed for factoring in $\mathbb{Z}[Z]$ (see [LLL82]), but it can be adapted to factor in $\bar{\mathbb{Q}}[Z_1, Z_2]$. □

Using Lemma 6.9, we can also easily give a diophantine definition of $\mathcal{O}_F[Z_1]$.

Lemma 6.11 (Defining $\mathcal{O}_F[Z]$)**.** *Let F be a number field contained in L. Then $\mathcal{O}_F[Z_1]$ is a diophantine subset of $\mathcal{R}$.*

Proof. Let $\{\omega_1, \omega_2, \ldots, \omega_d\}$ be a $\mathbb{Z}$-module basis for $\mathcal{O}_F$. Then

$$\mathcal{O}_F[Z_1] = \omega_1\mathbb{Z}[Z_1] + \cdots + \omega_d\mathbb{Z}[Z_1].$$

But $\mathbb{Z}[Z_1]$ is an r.e. subset of $\mathbb{Z}[Z_1, \ldots, Z_n]$, hence it is also a diophantine subset. Using Lemma 6.9, $\mathbb{Z}[Z_1]$ is also diophantine in $\mathcal{R}$. □

We finish this section with a proof of the distinguishing lemma, which is not so difficult, since $\mathbb{Z}$ is an infinite set.

Lemma 6.12 (Distinguishing lemma)**.** *Let $P \in \mathcal{R}$ be a polynomial. Consider a finite set $\{Q_1, \ldots, Q_m\} \subset \mathcal{R}$, such that P is not* $\mathrm{Gal}(L/F)$*-conjugate to any Q_i. Then there exists an $\overrightarrow{\alpha} \in \mathcal{O}_L^n$ such that*

$$P(\overrightarrow{\alpha}^{\overrightarrow{\sigma}}) \neq Q_i(\overrightarrow{\alpha})^{\tau} \tag{6.18}$$

for all $\overrightarrow{\sigma} \in \mathrm{Gal}(L/F)^n$, $\tau \in \mathrm{Gal}(L/F)$ and $i \in \{1, \ldots, m\}$.

Proof. We will actually take $\overrightarrow{\alpha}$ in $\mathbb{Z}^n$, then $\overrightarrow{\alpha}$ will be invariant under $\mathrm{Gal}(L/F)$. This way, (6.18) becomes "$P(\overrightarrow{\alpha}) \neq Q_i^{\tau}(\overrightarrow{\alpha})$".

Without loss of generality, we may assume that if a polynomial Q is amongst $\{Q_1, \ldots, Q_m\}$, all its $\mathrm{Gal}(L/F)$-conjugates Q^{τ} also are. We can assure this by adding a finite number of polynomials to the given set. Since P was not $\mathrm{Gal}(L/F)$-conjugate to any Q_i, we will not add P to the set of Q's. Now (6.18) becomes "$P(\overrightarrow{\alpha}) \neq Q_j(\overrightarrow{\alpha})$", because Q_i^{τ} is simply another Q_j.

Let $S := \prod_{j=1}^{m}(P - Q_j)$. We know that P is not equal to any Q_j, therefore S is not the zero polynomial. Since $\mathbb{Z}$ is infinite, there exists an $\overrightarrow{\alpha} \in \mathbb{Z}^n$ such that $S(\overrightarrow{\alpha}) \neq 0$. This is the $\overrightarrow{\alpha}$ we are looking for, because $S(\overrightarrow{\alpha}) \neq 0$ implies $P(\overrightarrow{\alpha}) \neq Q_j(\overrightarrow{\alpha})$ for all j. □

6.5 Finite field case

In this case, $K = \mathbb{F}_p$ is a finite field with p prime, and L is an infinite algebraic extension of $\mathbb{F}_p$. The field F is a finite field contained in L, sometimes we write

$\mathbb{F}_q$ for F. Then $\mathcal{R} = \mathcal{O}_L[Z] = L[Z]$ (for analogy with the number field case, we write $\mathcal{O}_L = L$).

Defining constants is trivial, since $\mathcal{R}^* = (L[Z])^* = L^* = \mathcal{O}_L^*$:

Lemma 6.13 (Defining constants)**.**

$$X \in \mathcal{O}_L \iff (X = 0) \vee (\exists Y)(XY = 1).$$

Next, we give a bounding predicate:

Lemma 6.14 (Bounding predicate)**.** *For $X \in \mathcal{R}$ and $e \in \mathbb{N}$, we define*

$$\delta(X, e) \leftrightarrow (XZ + 1)|(Z^e - 1).$$

This defines an extension-effective diophantine bounding predicate for $\mathcal{R}$.

Proof. Exactly as in the proof of Lemma 6.10, $(Z^e - 1)$ has only finitely many divisors of the form $XZ + 1$.

Now let $\mathcal{B}$ be a finite subset of $L[Z]$, and let $P := \prod_{X \in \mathcal{B}}(XZ + 1)$. We have to find an $e \in \mathbb{N}$ such that $P|(Z^e - 1)$. Let $\mathbb{F}_q$ be a finite field containing all coefficients of P, and consider the ring $\mathbb{F}_q[Z]/P$. The constant term of P equals 1, hence $\gcd(P, Z) = 1$ and $Z \in (\mathbb{F}_q[Z]/P)^*$. Since $\mathbb{F}_q$ is a finite field, $(\mathbb{F}_q[Z]/P)^*$ is a finite group, so we must have $Z^e \equiv 1 \bmod P$ for some e.

To prove that the predicate is diophantine, we use the model of $\mathbb{N}$ in $L[Z]$ from Section 5.2. In this model, a natural number e is represented by Z^e. This suffices to conclude that "$(XZ + 1)|(Z^e - 1)$" is diophantine.

If we consider the extension $\bar{\mathbb{F}}_p[Z]$ of $\mathcal{R}$, then we easily see that the predicate is extension-effective. Over $\bar{\mathbb{F}}_p[Z]$, factoring means finding zeros, and we can do that by trying all possibilities. Then we combine the factors of $Z^e - 1$, and multiply them with a suitable unit such that we get something of the form $XZ + 1$. □

We will now give a diophantine definition of the ring $\mathcal{O}_F[Z]$ inside $\mathcal{R}$. Since we are in the finite field case, $\mathcal{O}_F = F$ is some finite field $\mathbb{F}_q$ of characteristic p.

Lemma 6.15 (Defining $\mathcal{O}_F[Z]$)**.** *For $X \in L[Z]$, the following holds:*

$$X \in \mathbb{F}_q[Z] \tag{6.19}$$
$$\Updownarrow$$
$$(\exists a, b, e \in \mathbb{N})$$
$$(XZ+1) | (Z^e - 1) \tag{6.20}$$
$$\wedge\ q^a > e \ \wedge\ q^b > e \ \wedge\ \gcd(a,b) = 1 \tag{6.21}$$
$$\wedge\ X^{q^a} \equiv X \mod Z^{q^a} - Z \tag{6.22}$$
$$\wedge\ X^{q^b} \equiv X \mod Z^{q^b} - Z. \tag{6.23}$$

Proof. Assume $X \in \mathbb{F}_q[Z]$ and write $X = \sum_{i=0}^{d} \alpha_i Z^i$ with $\alpha_i \in \mathbb{F}_q$. From Lemma 6.14 it follows that we can choose e such that (6.20) holds. Then we take any a and b satisfying (6.21). Since $\alpha_i \in \mathbb{F}_q$, we find

$$X^{q^a} = \sum_{i=0}^{d} \alpha_i Z^{iq^a} \equiv \sum_{i=0}^{d} \alpha_i Z^i = X \mod Z^{q^a} - Z.$$

Analogously, $X^{q^b} \equiv X \bmod Z^{q^b} - Z$.

Conversely, assume (6.20)–(6.23). From (6.20) it follows that $\deg X \leq e$, so we can write X as $\sum_{i=0}^{e} \alpha_i Z^i$, with $\alpha_i \in L$. We want to prove that every α_i is actually in $\mathbb{F}_q$. (6.22) implies that

$$\sum_{i=0}^{e} \alpha_i Z^i = X \equiv X^{q^a} = \sum_{i=0}^{e} \alpha_i^{q^a} Z^{iq^a} \equiv \sum_{i=0}^{e} \alpha_i^{q^a} Z^i \mod Z^{q^a} - Z.$$

The left and right hand sides of this congruence are polynomials of degree at most e, however they are congruent modulo a polynomial of degree $q^a > e$, hence they are equal. This means that $\alpha_i = \alpha_i^{q^a}$, in other words $\alpha_i \in \mathbb{F}_{q^a}$. In the same way, it follows from (6.23) that $\alpha_i \in \mathbb{F}_{q^b}$. Since $\gcd(a,b) = 1$, we have $\mathbb{F}_{q^a} \cap \mathbb{F}_{q^b} = \mathbb{F}_q$, therefore $\alpha_i \in \mathbb{F}_q$. □

We remark that we can use this lemma to define $\mathbb{F}_q[Z]$ in $\mathcal{S}[Z]$, where $\mathcal{S}$ is any integral domain of characteristic p. This is because we just need the model of $\mathbb{N}$ as in Section 5.2, but that model works for any such $\mathcal{S}$.

Next, we prove the distinguishing lemma for the finite field case. We have to add a technical condition that we must not consider polynomials which are p-th

powers, where p is the characteristic. This is because Z^p and Z^σ with σ the Frobenius $\xi \mapsto \xi^p$ have exactly the same values, we cannot distinguish them.

In the number field case, we could take every component of $\overrightarrow{\alpha}$ in the base ring $\mathbb{Z}$. However, here we cannot do that anymore since $\mathbb{F}_p$ is finite. This means we have to take α in an extension, which makes the proof more difficult because we no longer have that $\alpha^\sigma = \alpha$.

Lemma 6.16 (Distinguishing lemma)**.** *Let $P \in \mathcal{R}$ be a polynomial. Consider a finite set $\{Q_1, \dots, Q_m\} \subset \mathcal{R}$, such that P is not $\mathrm{Gal}(L/F)$-conjugate to any Q_i. Assume that none of $\{P, Q_1, \dots, Q_m\}$ is a p-th power. Then there exists an $\alpha \in \mathcal{O}_L$ such that*

$$P(\alpha^\sigma) \neq Q_i(\alpha)^\tau. \tag{6.24}$$

for all $\sigma, \tau \in \mathrm{Gal}(L/F)$ and $i \in \{1, \dots, m\}$.

Proof. Writing $\beta := \alpha^\sigma$, we have to find a $\beta \in \mathcal{O}_L$ such that $P(\beta) \neq Q_i(\beta^{\sigma^{-1}})^\tau$ for all σ, τ, i as in the statement of the lemma. Applying $\rho := \tau^{-1}\sigma$ on this condition, we rewrite it as "$P(\beta)^\rho \neq Q_i^\sigma(\beta)$". As in the proof of Lemma 6.12, we can add all $\mathrm{Gal}(L/F)$-conjugates of the Q_i, to replace the condition by "$P(\beta)^\rho \neq Q_j(\beta)$". This has to be satisfied by all $\rho \in \mathrm{Gal}(L/F)$ and $j \in \{1, \dots, m\}$.

Let q be such that $F \cong \mathbb{F}_q$. Fix a finite subfield $\mathbb{F}_r \subset L$ containing $\mathbb{F}_q$ and all the coefficients of the Q_j. Note that there is a minimal r, but we can take r arbitrarily large (since L is infinite).

In symbols, we have to prove that

$$(\exists \beta \in \mathcal{O}_L)(\forall j \leq m)\big(\forall \rho \in \mathrm{Gal}(L/\mathbb{F}_q)\big)\big(P(\beta)^\rho \neq Q_j(\beta)\big). \tag{6.25}$$

We will take β in $\mathbb{F}_r$, so everything is well-defined if we see ρ as an element of $\mathrm{Gal}(\mathbb{F}_r/\mathbb{F}_q)$. We want to prove (6.25) by contradiction, so we assume that

$$(\forall \beta \in \mathbb{F}_r)(\exists j \leq m)\big(\exists \rho \in \mathrm{Gal}(\mathbb{F}_r/\mathbb{F}_q)\big)\big(P(\beta)^\rho = Q_j(\beta)\big). \tag{6.26}$$

We will use a counting argument to show that (6.26) is not possible if r is large enough. If (6.26) holds, then to every $\beta \in \mathbb{F}_r$, there corresponds a couple (j, ρ) such that $P(\beta)^\rho = Q_j(\beta)$. There are at most $m \log_q(r)$ such couples, by the pigeonhole principle at least $N = \left\lceil \frac{r}{m \log_q(r)} \right\rceil$ different β's have the same (j, ρ). In other words, there exist certain fixed $j \in \mathbb{N}$ and $\rho \in \mathrm{Gal}(\mathbb{F}_r/\mathbb{F}_q)$ such that $P(\beta)^\rho = Q_j(\beta)$ for at least N different values of $\beta \in \mathbb{F}_r$.

But on $\mathbb{F}_r$, the automorphism ρ is simply raising to a certain power q^h, with $0 \leq h < \log_q(r)$. Assume that $h \leq \log_q(r)/2$, otherwise we do the following reasoning with P and Q_j exchanged (then h changes to $\log_q(r) - h$). So, for N different values of $\beta \in \mathbb{F}_r$, the following holds:

$$P(\beta)^{q^h} = Q_j(\beta).$$

If $P(Z)^{q^h} - Q_j(Z)$ is the zero polynomial, then either $h = 0$ and $P = Q_j$, or $h > 0$ and Q_j is a p-th power. Both these cases are excluded, so $P(Z)^{q^h} - Q_j(Z)$ has only finitely many zeros. If d denotes the maximum degree of all given polynomials $\{P, Q_1, \ldots, Q_m\}$, then $P(Z)^{q^h} - Q_j(Z)$ has degree at most $dq^h \leq d\sqrt{r}$. But this polynomial has N different zeros, therefore

$$d\sqrt{r} \geq N \geq \frac{r}{m \log_q(r)}.$$

Since d, m and q do not depend on r, it is possible to take r large enough such that this inequality is not satisfied, giving a contradiction. □

6.6 Finishing the proof

Given the lemmas from the previous two sections, we can now finish Main Theorem 6.3. We will continue using the notations from Section 6.2.

Let $\mathcal{S}$ be an r.e. subset of $\mathcal{R}$, and let F be the finite extension of K such that $\mathrm{Gal}(L/F)(\mathcal{S}) = \mathcal{S}$. We want to find a diophantine definition of the set $\mathcal{S}$, using only constants from $\mathcal{O}_F[Z_1, \ldots, Z_n]$. Recall that $\mathcal{O}_F[Z_1, \ldots, Z_n] = F[Z]$ in the finite field case.

Given $\mathcal{S}$, we construct a set $\mathcal{P}_1 \subseteq \mathbb{N} \times \mathcal{O}_L^n \times \mathcal{O}_L$ which will encode the elements of $\mathcal{S}$. In the finite field case, $n = 1$, and all vector arrows may be ignored. For an $X \in \mathcal{S}$, the following algorithm gives a triple $(e, \overrightarrow{\alpha}, \beta) \in \mathbb{N} \times \mathcal{O}_L^n \times \mathcal{O}_L$ corresponding to X:

- e is the smallest number for which $\delta(X, e)$ holds, where δ is an extension-effective diophantine bounding predicate for the ring $\mathcal{R}$ (see Lemmas 6.10 and 6.14). Since δ is extension-effective, we can find this e algorithmically.

- $\overrightarrow{\alpha}$ comes from the distinguishing lemma (Lemma 6.12 or 6.16) applied with $P = X$ and the Q's all elements satisfying $\delta(Q, e)$, except for those which are $\mathrm{Gal}(L/F)$-conjugate to P. Note that, in the finite field case, there is the condition that these polynomials must not be p-th powers, but we will deal with that later.

  To find such an $\overrightarrow{\alpha}$ algorithmically, we do the following: We take the finite set $\mathcal{B}_e \subset \bar{K}[Z_1, \ldots, Z_n]$ such that $\mathcal{B}_e \cap \mathcal{R} = \{X \in \mathcal{R} \mid \delta(X, e)\}$ (see Definition 6.6). Then remove all $\mathrm{Gal}(L/F)$-conjugates of P (including P itself) from the set $\mathcal{B}_e$. We now apply the distinguishing lemma with this $\mathcal{B}_e$ as the set of Q's. Since we can compute the set $\mathcal{B}_e$, we can try every $\overrightarrow{\alpha} \in \mathcal{O}_L^n$ until we find one which works.

- $\beta = X(\overrightarrow{\alpha})$.

Now we will do a further encoding of $\mathcal{P}_1$ in $\mathbb{N} \times \mathcal{O}_F[Z]^n \times \mathcal{O}_F[Z]$. We encode a triple $(e, \overrightarrow{\alpha}, \beta) \in \mathcal{P}_1$ as $(e, \overrightarrow{A}, B)$, where e remains the same, B is the minimal polynomial (over F) of β, and every component A_i of $\overrightarrow{A}$ is the minimal polynomial (over F) of the corresponding component α_i of $\overrightarrow{\alpha}$. The set of all these $(e, \overrightarrow{A}, B)$ will be called $\mathcal{P}$.

Both these encodings are recursive procedures, therefore $\mathcal{P}_1$ and $\mathcal{P}$ are r.e. sets. But for the ring $\mathcal{O}_F[Z]$, we know that r.e. sets are diophantine. For the finite field case, this was proved in Chapter 5, and for the number field case, this is in [Zah99, Chapter III]. So, we know that $\mathcal{P}$ is diophantine over $\mathcal{O}_F[Z]$. In Lemma 6.11 or 6.15, we proved that $\mathcal{O}_F[Z]$ is diophantine in $\mathcal{R}$. Therefore, $\mathcal{P}$ is diophantine in $\mathcal{R}$.

Looking back at the definitions of $\mathcal{P}$ and $\mathcal{P}_1$, we can now find a diophantine definition of the set $\mathcal{S}$:

Theorem 6.17.

$$
\begin{aligned}
& X \in \mathcal{S} && (6.27)\\
& \quad \Updownarrow \\
& (\exists e \in \mathbb{N})(\exists \overrightarrow{A} \in \mathcal{O}_F[Z]^n)(\exists B \in \mathcal{O}_F[Z]) \\
& \qquad (e, \overrightarrow{A}, B) \in \mathcal{P} && (6.28)\\
& \wedge\ (\exists \overrightarrow{\alpha} \in \mathcal{O}_L^n)(\exists \beta \in \mathcal{O}_L) \\
& \qquad A_1(\alpha_1) = 0 \ \wedge\ \ldots \ \wedge\ A_n(\alpha_n) = 0 && (6.29)\\
& \quad \wedge\ B(\beta) = 0 && (6.30)\\
& \quad \wedge\ \delta(X, e) \ \wedge\ X(\overrightarrow{\alpha}) = \beta. && (6.31)
\end{aligned}
$$

Diophantineness. In order for this to be diophantine, $\mathcal{O}_L$ and $\mathcal{O}_F[Z]$ must be diophantine subsets of $\mathcal{R}$. But this was the content of steps 1 and 3 in the outline. By construction $\mathcal{P}$ is diophantine. Finally, polynomial evaluations are diophantine because of Example 2.5.

Proof. If $X \in \mathcal{S}$, we take the corresponding $(e, \overrightarrow{\alpha}, \beta) \in \mathcal{P}_1$ and $(e, \overrightarrow{A}, B) \in \mathcal{P}$. (6.28) is obviously satisfied, and (6.29), (6.30) and (6.31) are true because of the construction of $\mathcal{P}_1$ and $\mathcal{P}$.

Conversely, assume (6.28)–(6.31). By definition of $\mathcal{P}$, it follows from $(e, \overrightarrow{A}, B) \in \mathcal{P}$ that there exist $\overrightarrow{\alpha}'$ and β' with $(e, \overrightarrow{\alpha}', \beta') \in \mathcal{P}_1$ with α_i' a zero of A_i (for $i = 1, \ldots, n$) and β' a zero of B. This triple $(e, \overrightarrow{\alpha}', \beta')$ has to come from some $X' \in \mathcal{S}$, which means that $X'(\overrightarrow{\alpha}') = \beta'$ and $\delta(X', e)$. But α_i and α_i' are zeros of the same irreducible polynomial A_i, so they are $\mathrm{Gal}(L/F)$-conjugates, the same holds for β and β'.

Now the distinguishing lemma comes in. Recall that the construction of $\mathcal{P}_1$ in the beginning of Section 6.6 was only correct in the number field case, because the distinguishing lemma in characteristic p requires that the polynomials are not p-th powers. Therefore this last part of the proof is only correct in the number field case, for the finite field case we refer to the remark after this proof.

Assume that X and X' are not $\mathrm{Gal}(L/F)$-conjugates. Since $\delta(X, e)$ holds, X must be one of the Q's in the distinguishing lemma applied with $P = X'$ (look back at the construction of $\mathcal{P}_1$). Therefore, $X'(\overrightarrow{\alpha}^{\overrightarrow{\sigma}}) \neq X(\overrightarrow{\alpha})^\tau$ for any $\overrightarrow{\sigma}$ and τ. If we substitute $X(\overrightarrow{\alpha}) = \beta$ and choose $\overrightarrow{\sigma}$ and τ such that $\overrightarrow{\alpha}^{\overrightarrow{\sigma}} = \overrightarrow{\alpha}'$ and $\beta^\tau = \beta'$, we find $X'(\overrightarrow{\alpha}') \neq \beta'$, which is a contradiction.

So, the only possibility is that the polynomial X' is $\mathrm{Gal}(L/F)$-conjugate to X. Knowing that $X' \in \mathcal{S}$ and that $\mathcal{S}$ is invariant under $\mathrm{Gal}(L/F)$, we get $X \in \mathcal{S}$. □

Remark. This finishes the proof of Main Theorem 6.3 in the number field case. For finite fields, we just have the problem that our elements of $\mathcal{S}$ should not be p-th powers, in order to apply Lemma 6.16 (see the construction of the set $\mathcal{P}_1$ in the beginning of this section). To ensure this, we apply some kind of transformation on $\mathcal{S}$. We define $\mathcal{S}' := \{A^p + Z \in \mathcal{R} \mid A \in \mathcal{S}\}$. If we do this, then $\mathcal{S}'$ does not contain any p-th powers. Now we do the whole reasoning with $\mathcal{S}'$ instead of $\mathcal{S}$. In the construction of $\mathcal{P}_1$, we still have to exclude the Q's which are a power of p to apply the distinguishing lemma. In the proof of Theorem 6.17, we cannot conclude that X and X' are $\mathrm{Gal}(L/F)$-conjugate, if X is a power of p. But this problem can be avoided by adding the diophantine condition "X is of

the form $A^p + Z$" to the formula (6.31). Then X cannot be a power of p, so the distinguishing lemma works again. At the end of the proof, we have a diophantine definition of $\mathcal{S}'$, from which we can easily recover $\mathcal{S}$ with the diophantine definition $A \in \mathcal{S} \iff A^p + Z \in \mathcal{S}'$.

Part IV

Appendices

Appendix A

Explicit computation

A.1 Proof of Proposition 4.17

We will prove the approximations of X_{4n} and Y_{4n} by induction on n. For $n = 1$, one can compute that

$$\mathrm{X}_4 = \frac{1}{4}Z^{-2} - \frac{1}{4}Z^{-1} - \frac{1}{16}Z^0 + O(Z^2),$$
$$\mathrm{Y}_4 = -\frac{1}{8}Z^{-3} + \frac{1}{16}Z^{-2} + O(Z).$$

Similarly, for $n = 2$ we get

$$\mathrm{X}_8 = \frac{1}{16}Z^{-2} - \frac{1}{16}Z^{-1} - \frac{1}{64}Z^0 + O(Z^2),$$
$$\mathrm{Y}_8 = -\frac{1}{64}Z^{-3} + \frac{1}{128}Z^{-2} + O(Z).$$

Truncating these power series gives the desired result for $n = 1$ and $n = 2$.

Now assume Proposition 4.17 holds for a certain $n \geq 2$, let us prove it for $n+1$. We will use the elliptic curve addition formula (see for example [Sil86, Algorithm 2.3]), in the following form: if $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ are points on $E : y^2 = x^3 + ax + b$, then their sum $R = (x_R, y_R)$ is given by

$$x_R = -x_P - x_Q + c^2 \qquad y_R = -y_P + c(x_P - x_R) \qquad \text{with } c = \frac{y_P - y_Q}{x_P - x_Q}.$$

We apply these for $P = (x_4, y_4 Y)$ and $Q = (x_{4n}, y_{4n} Y)$:

$$\begin{aligned}
c &= \frac{y_4 Y - y_{4n} Y}{x_4 - x_{4n}} \\
&= \left(\frac{-\frac{1}{8Z^3} + \frac{1}{8n^3 Z^3} + O(Z^{-2})}{\frac{1}{4Z^2} - \frac{1}{4n^2 Z^2} + O(Z^{-1})} \right) Y \\
&= \left(\frac{\frac{1-n^3}{8n^3} + O(Z)}{\frac{n^2-1}{4n^2} + O(Z)} \right) \frac{Y}{Z} \\
&= \left(-\frac{n^2+n+1}{2n(n+1)} + O(Z) \right) \frac{Y}{Z} \\
x_{4n+4} &= -x_4 - x_{4n} + c^2 \\
&= -\frac{1}{4Z^2} - \frac{1}{4n^2 Z^2} + O(Z^{-1}) + \left(-\frac{n^2+n+1}{2n(n+1)} + O(Z) \right)^2 \frac{Y^2}{Z^2} \\
&= -\frac{1+n^2}{4n^2 Z^2} + O(Z^{-1}) + \left(-\frac{n^2+n+1}{2n(n+1)} + O(Z) \right)^2 \left(\frac{1+O(Z)}{Z^2} \right) \\
&= \left[-\frac{1+n^2}{4n^2} + \left(-\frac{n^2+n+1}{2n(n+1)} \right)^2 \right] \frac{1}{Z^2} + O(Z^{-1}) \\
&= \frac{1}{4(n+1)^2 Z^2} + O(Z^{-1}) \\
y_{4n+4} &= -y_4 + \frac{c}{Y}(x_4 - x_{4n+4}) \\
&= \frac{1}{8Z^3} + O(Z^{-2}) \\
&\qquad + \left(-\frac{n^2+n+1}{2n(n+1)} + O(Z) \right) \frac{1}{Z} \left(\frac{1}{4Z^2} - \frac{1}{4(n+1)^2 Z^2} + O(Z^{-1}) \right) \\
&= \frac{1}{8Z^3} + O(Z^{-2}) + \left(-\frac{n^2+n+1}{2n(n+1)} + O(Z) \right) \left(\frac{n^2+2n}{4(n+1)^2} + O(Z) \right) \frac{1}{Z^3} \\
&= \left[\frac{1}{8} + \left(-\frac{n^2+n+1}{2n(n+1)} \right) \left(\frac{n^2+2n}{4(n+1)^2} \right) \right] \frac{1}{Z^3} + O(Z^{-2}) \\
&= -\frac{1}{8(n+1)^3 Z^3} + O(Z^{-2}).
\end{aligned}$$

Bijlage B

Samenvatting

B.1 Het Tiende Probleem van Hilbert en aanverwante problemen

In 1900 stelde David Hilbert een lijst op met 23 wiskundige problemen. Sommige van deze werden voorgesteld op het International Congress of Mathematicians, in Parijs in augustus 1900. De problemen waren bedoeld om de wiskunde van de twintigste eeuw te beïnvloeden, en dat is zeker gelukt. In zijn artikel definieert Hilbert zijn 10e probleem als volgt:

> *"Eine Diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlenkoeffizienten sei vorgelegt: Man soll ein Verfahren angeben, nach welchem sich mittels einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen Zahlen lösbar ist."*

> Zij een diophantische vergelijking met eender hoeveel variabelen en met rationaal gehele coëfficiënten gegeven: Men zal een procedure geven, zodat, na een eindig aantal operaties, het beslist kan worden of de vergelijking in gehele getallen oplosbaar is.

Hilbert spreekt over een eindige procedure, maar vandaag zouden we dat een algoritme noemen. Een formele definitie van algoritmes werd echter maar in de

jaren 1930 gegeven. Het is duidelijk dat Hilbert zijn "Verfahren" wel de intuïtie van een algoritme beschrijft.

Het Tiende Probleem van Hilbert is dus de vraag of er een algoritme bestaat dat kan beslissen of een diophantische vergelijking al dan niet een oplossing heeft in gehele getallen. Met een "diophantische vergelijking" bedoelt hij een veeltermvergelijking met coëfficiënten in $\mathbb{Z}$.

Het Tiende Probleem van Hilbert heeft een negatief antwoord, in de zin dat er geen algoritme bestaat dat kan beslissen of een diophantische vergelijking een oplossing heeft in $\mathbb{Z}$. Dit werd in 1970 bewezen door Yuri Matiyasevich (zie [Mat70]), voortbouwend op eerder werk van Martin Davis, Hilary Putnam en Julia Robinson.

De onbeslisbaarheid van diophantische vergelijkingen was eigenlijk maar een gevolg van het volgende positieve resultaat, dat veel sterker is:

Stelling (DPRM, 1970)**.** *Voor alle $k \geq 1$ is een deelverzameling van $\mathbb{Z}^k$ recursief opsombaar als en slechts als ze diophantisch is over $\mathbb{Z}$.*

We verwijzen naar deze stelling als "DPRM", voor Davis, Putnam, Robinson en Matiyasevich. Het bewijs werd ontwikkeld in meerdere artikels. We verwijzen naar [Dav73], waar Davis het volledige bewijs van DPRM geeft, zonder voorkennis te eisen. In een historische appendix geeft hij referenties naar de originele artikels.

Men kan dezelfde vragen stellen, niet enkel voor $\mathbb{Z}$, maar voor elke ring of veld. Het Tiende Probleem van Hilbert (TPH) voor een ring $\mathcal{R}$ is dan het probleem om een algoritme te vinden dat kan beslissen of veeltermvergelijkingen met coëfficiënten in $\mathcal{R}$ oplossingen hebben in $\mathcal{R}$. Meestal gaan we echter de coëfficiënten niet in $\mathcal{R}$ nemen, maar in een kleinere ring. Dit is zeker nodig als de ring $\mathcal{R}$ overaftelbaar is, want we kunnen de elementen van een overaftelbare ring niet eens invoeren in een algoritme. Gewoonlijk nemen we de coëfficiënten in een eindig voortgebrachte ring. Voor TPH over $\mathbb{R}$ beschouwt men bijvoorbeeld diophantische vergelijkingen met coëfficiënten in $\mathbb{Q}$ (equivalent, in $\mathbb{Z}$). In dit geval is het probleem beslisbaar (zie [Tar51]). In Deel II van deze thesis hebben we het negatieve antwoord op TPH bewezen voor bepaalde functievelden van krommen, over valuatievelden met residu-karakteristiek nul.

Als de ring $\mathcal{R}$ aftelbaar is, kunnen we ook het tweede resultaat veralgemenen, zijnde de equivalentie van recursief opsombare en diophantische verzamelingen. Dit is een veel moeilijker probleem, en er zijn slechts enkele ringen gekend waarvoor het antwoord positief is. Als we deze equivalentie kunnen bewijzen voor

een ring $\mathcal{R}$, dan hebben we onmiddellijk het negatieve antwoord op TPH voor $\mathcal{R}$. In Deel III, hebben we DPRM veralgemeend naar veeltermringen over algebraïsche uitbreidingen van een eindig veld en ringen van gehelen in totaal reële algebraïsche uitbreidingen van $\mathbb{Q}$.

We geven twee referenties naar inleidende teksten (in het Engels): de eerste, *Undecidability of Existential Theories of Rings and Fields: a Survey* van Pheidas en Zahidi ([PhZ00]) geeft wat geschiedenis over het probleem en ook een goed overzicht van de ringen en velden waarvoor TPH beslisbaar, onbeslisbaar of nog een open probleem is. Het geeft ook enkele verbanden met logica aan en heeft een zeer uitgebreide bibliografie. De tweede tekst, *Hilbert's Tenth Problem over Rings of Number-Theoretic Interest* van Poonen ([Poo03]) is korter en misschien beter geschikt als eerste introductie tot TPH. Het gaat veel minder in detail maar is meer geconcentreerd op de getaltheorie.

B.2 Overzicht van de thesis

B.2.1 Deel I: Inleiding

In Hoofdstuk 2 geven we de definitie van een diophantische verzameling, en ook enkele belangrijke voorbeelden. We spreken ook kort over talen. Dan definiëren we diophantische interpretaties, met diophantische modellen als speciaal geval.

De eerste sectie van Hoofdstuk 3 gaat over algoritmen. In Section 3.2 worden deze gebruikt om recursief opsombare (r.o.) en recursieve verzamelingen te definiëren over de natuurlijke getallen $\mathbb{N} = \{0, 1, 2, \dots\}$. In Section 3.3 leiden we recursieve presentaties in, die ons toelaten om de definities van r.o. en recursieve verzamelingen naar andere ringen over te dragen. Een ring kan meerdere recursieve presentaties hebben, het kan dus van de recursieve presentatie afhangen welke verzamelingen r.o. of recursief zijn. Maar voor een bepaalde klasse van ringen, de recursief stabiele ringen, geven alle recursieve presentaties dezelfde r.o. en recursieve verzamelingen. Section 3.4 gaat over veralgemeningen van DPRM (r.o. verzamelingen zijn diophantisch) naar andere ringen $\mathcal{R}$. Een recursieve presentatie $\theta : \mathcal{R} \xrightarrow{\sim} \mathbb{N}$ geeft een opsomming van $\mathcal{R}$, we kunnen dus spreken over het n-de element $\theta^{-1}(n)$. In Section 3.4.1 leggen we uit hoe een diophantische definitie van de relatie "X is het n-de element" met $X \in \mathcal{R}$ en $n \in \mathbb{N}$ impliceert dat r.o. verzamelingen diophantisch zijn.

B.2.2 Deel II: Het Tiende Probleem van Hilbert voor functievelden

We bewijzen het negatieve antwoord op TPH voor bepaalde functievelden van krommen over valuatievelden met residu-karakteristiek nul. Dit veralgemeent een resultaat van Kim en Roush (zie [KR92]), die het negatieve antwoord op TPH bewezen voor $\mathbb{C}(Z_1, Z_2)$. Eisenträger heeft dit uitgebreid naar functievelden van variëteiten van dimensie ≥ 2 over $\mathbb{C}$ (zie [Eis04]). In veel gevallen werkt onze methode ook voor zulke functievelden, maar er zijn enkele extra voorwaarden.

In onze Hoofdstelling 4.31 beschouwen we velden $K(C)$, het functieveld van een kromme C over K. Hier is K een valuatieveld met residu-veld k, waar beide karakteristiek nul hebben. In Section 4.11 geven we een lange lijst met velden waar ons resultaat toegepast kan worden. Functievelden van krommen over $\mathbb{C}((T))$ zijn een belangrijk voorbeeld.

In Hoofdstelling 4.31 zijn er drie voorwaarden op het veld $K(C)$: de eerste is dat de valuatiegroep niet 2-deelbaar mag zijn, er moet met andere woorden een element $T \in K$ bestaan zodat $v(T)$ niet gelijk is aan $2v(U)$ voor eender welke $U \in K$. De tweede voorwaarde heeft te maken met Galois cohomologie. Schrijf F voor een maximaal deelveld van K waarop de valuatie triviaal is (F bestaat dankzij het Lemma van Zorn). Neem bijvoorbeeld $K = \mathbb{C}((T))$, dan is F gelijk aan $\mathbb{C}$. We eisen dat de 2-cohomologische dimensies van F en het residu-veld k gelijk zijn, en eindig. Tenslotte zegt de derde voorwaarde dat de kromme C een niet-singulier punt moet hebben in de reductie (over $\bar{k}$). Merk op dat we de kromme C mogen vervangen door een birationaal equivalente kromme, aangezien we enkel geïnteresseerd zijn in het functieveld $K(C)$. Onder deze voorwaarden kunnen we bewijzen dat TPH voor $K(C)$ een negatief antwoord heeft.

B.2.3 Deel III: Diophantische verzamelingen over veeltermringen

Dit deel gaat over veralgemeningen van DPRM, zijnde de equivalentie van recursief opsombare (r.o.) en diophantische verzamelingen.

In Hoofdstuk 5 kijken we naar de ring $\mathbb{F}_q[Z]$ van veeltermen over een eindig veld. Het is algemeen bekend dat de aritmetiek van $\mathbb{F}_q[Z]$ zeer analoog is aan die van $\mathbb{Z}$. Daarom is het een heel natuurlijke vraag of we iets gelijkaardig als DPRM kunnen bewijzen voor $\mathbb{F}_q[Z]$. TPH heeft voor deze ring een negatief antwoord, dit was bewezen door Denef in 1979 (zie [Den79]). Wij bewijzen dat r.o. verzamelingen

diophantisch zijn voor $\mathbb{F}_q[Z]$. Dit gebeurt in twee stappen: ten eerste tonen we aan dat r.o. deelverzamelingen over $\mathbb{F}_q[Z]$ diophantisch zijn over $\mathbb{F}_q[W, Z]$. Met andere woorden, als we een verzameling $\mathcal{S} \subseteq \mathbb{F}_q[W, Z]^k$ nemen waarbij W in geen enkel element van $\mathcal{S}$ voorkomt, dan is $\mathcal{S}$ diophantisch over $\mathbb{F}_q[W, Z]$. Dit resultaat zal verschijnen in [Dem07a], en is de inhoud van Section 5.2–5.7. In Section 5.8 geven we een diophantische interpretatie van $\mathbb{F}_q[W, Z]$ in $\mathbb{F}_q[Z]$. Dit werd neergeschreven in een artikel [Dem07b]. Deze twee resultaten kunnen samen genomen worden om te bewijzen dat r.o. verzamelingen diophantisch zijn over $\mathbb{F}_q[Z]$.

In Hoofdstuk 6 vertrekken we van twee gevallen waar we weten dat r.o. verzamelingen diophantisch zijn, en we veralgemenen deze naar oneindige uitbreidingen. Het eerste gekende geval is $\mathcal{O}_K[Z_1, \ldots, Z_n]$, de veeltermring in n variabelen over de ring van gehelen in aan totaal reëel getallenveld K (zie [Zah99, Chapter III] of [Zah00]). We veralgemenen dit naar het geval waar K algebraïsch is over $\mathbb{Q}$ (niet noodzakelijk van eindige dimensie), maar nog altijd totaal reëel. Op een gelijkaardige manier veralgemenen we ook het resultaat uit Hoofdstuk 5 naar ringen $\mathbb{F}[Z]$, waar $\mathbb{F}$ een oneindige algebraïsche uitbreiding van een eindig veld is. Dit laatste resultaat staat ook in [Dem07b].

Voor de ringen $\mathcal{O}_K[Z_1, \ldots, Z_n]$ en $\mathbb{F}[Z]$ kunnen we niet langer bewijzen dat r.o. verzamelingen diophantisch zijn. Er zijn hiervoor verschillende reden. Ten eerste zou het kunnen dat de ring die we beschouwen niet recursief is, in dat geval is het onmogelijk om r.o. verzamelingen te definiëren, het probleem is dus niet eens goed gedefinieerd.

Deze oneindige algebraïsche uitbreidingen zijn niet recursief stabiel, er is dus geen absolute definitie van "r.o. verzameling". Het al dan niet r.o. zijn van een verzameling kan afhangen van de gekozen recursieve presentatie. Aangezien diophantische verzamelingen altijd r.o. zijn, onafhankelijk van de recursieve presentatie, beschouwen we enkel verzamelingen die r.o. zijn voor *elke* recursieve presentatie. Diophantische verzamelingen worden altijd gedefinieerd door een vergelijking over een zekere eindige uitbreiding. Neem bijvoorbeeld $\mathbb{F}[Z]$, daar heeft elke diophantische vergelijking zijn coëfficiënten in een eindig veld $\mathbb{F}_q$. Een verzameling gedefinieerd door zo'n vergelijking zal dan invariant zijn onder $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. Maar een algemene r.o. verzameling is invariant onder geen enkele $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. Het lijkt dus alsof we twee voorwaarden moeten opleggen op onze r.o. verzamelingen: ten eerste moeten ze r.o. zijn voor elke recursieve presentatie; ten tweede moeten ze invariant zijn onder $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$ voor een zeker eindig veld $\mathbb{F}_q$. In Section 6.1 kunnen we echter bewijzen dat deze twee voorwaarden equivalent zijn. In het geval van $\mathcal{O}_K[Z_1, \ldots, Z_n]$ geldt de analoge stelling.

Beginnend in Section 6.2 bewijzen we dat de verzamelingen, die r.o. zijn voor elke

recursieve presentatie, precies de diophantische verzamelingen zijn. We bewijzen dit voor $\mathcal{O}_K[Z_1, \ldots, Z_n]$ en voor $\mathbb{F}[Z]$. In beide gevallen is de strucuur van het bewijs dezelfde, maar de bewijzen zelf zijn heel verschillend. Uiteindelijk brengen we het probleem terug naar eindige uitbreidingen, waar het antwoord gekend is.

Bibliography

[AM69] Michael Atiyah and Ian Macdonald, *Introduction to commutative algebra*, Addison–Wesley, 1969.

[CK77] Chen Chung Chang and Jerome Keisler, *Model theory*, North-Holland, 1977.

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, 1993.

[Coh00] Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, no. 193, Springer, 2000.

[Crem] John Cremona, *Elliptic curve data*, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

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

[DP63] Martin Davis and Hilary Putnam, *Diophantine sets over polynomial rings*, Illinois J. Math. **7** (1963), 251–256.

[Dem07a] Jeroen Demeyer, *Recursively enumerable sets of polynomials over a finite field*, J. Algebra **310** (2007), 801–828.

[Dem07b] Jeroen Demeyer, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Submitted to Invent. Math., 2007.

[DVG06] Jeroen Demeyer and Jan Van Geel, *An existential divisibility lemma for global fields*, Monatsh. Math. **147** (2006), 293–308.

[Den78a] Jan Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc. **242** (1978), 391–399.

[Den78b] Jan Denef, *Diophantine sets over* $\mathbb{Z}[T]$, Proc. Amer. Math. Soc. **69** (1978), 148–150.

[Den79] Jan Denef, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium 78, North-Holland, 1979, 131–145.

[Eis03] Kirsten Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210** (2003), 261–281.

[Eis04] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over* $\mathbb{C}$, Int. Math. Res. Not. **59** (2004), 3191–3205.

[Eis07] Kirsten Eisenträger, *Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields*, J. Algebra **310** (2007), 775–792.

[End72] Otto Endler, *Valuation theory*, Springer, 1972.

[EP05] Antonio Engler and Alexander Prestel, *Valued fields*, Springer Monographs in Mathematics, Springer, 2005.

[FJ86] Michael Fried and Moshe Jarden, *Field arithmetic*, Springer, 1986.

[FS56] A. Fröhlich and C. Shepherdson, *Effective procedures in field theory*, Phil. Trans. Roy. Soc. London **248** (1956), 407–432.

[Hil01] David Hilbert, *Mathematische Probleme*, Archiv der Mathematik und Physik, 3d ser. **1** (1901), 44–63 and 213–237.

[KR92] Ki Hang Kim and Fred Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$, J. Algebra **150** (1992), 35–44.

[KR95] Ki Hang Kim and Fred Roush, *Diophantine unsolvability over p-adic function fields*, J. Algebra **176** (1995), 83–110.

[Lam05] Tsit-Yuen Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, no. 67, American Mathematical Society, 2005.

[LLL82] Arjen Lenstra, Hendrik Lenstra and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[LN88] Rudolf Lidl and Harald Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1988.

[Mat70] Yuri Matiyasevich, *Enumerable sets are Diophantine*, Soviet Math. Dokl. **11** (1970), 354–358.

[MB05] Laurent Moret-Bailly, *Elliptic curves and Hilbert's tenth problem for algebraic function fields over real and p-adic fields*, J. für die reine und angew. Math. **587** (2005), 77–143.

[Pfi00] Albrecht Pfister, *On the Milnor conjectures: History, influence, applications*, Jber. d. Dt. Math.-Verein **102** (2000), 15–39.

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for rational function fields over finite fields*, Invent. Math. **103** (1991), 1–8.

[Phe00] Thanases Pheidas, *An effort to prove that the existential theory of $\mathbb{Q}$ is undecidable*, Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry (Ghent, 1999) (Denef et al., eds.), Contemp. Math., vol. 270, 2000, 237–252.

[PhZ00] 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, 49–105.

[Poo03] Bjorn Poonen, *Hilbert's tenth problem over rings of number-theoretic interest*, Arizona Winter School 2003 notes, `http://math.berkeley.edu/~poonen/papers/aws2003.pdf`.

[Rab60] Michael Rabin, *Computable algebra, general theory and theory of computable fields*, Trans. Amer. Math. Soc. **95** (1960), 341–360.

[RZ00] Luis Ribes and Pavel Zalesskii, *Profinite groups*, Springer, 2000.

[Rum80] Robert Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262** (1980), 195–217.

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Springer, 2002.

[Shl94] Alexandra Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), 139–175.

[Shl96] Alexandra Shlapentokh, *Diophantine undecidability over algebraic function fields over finite fields of constants*, J. Number Theory **58** (1996), 317–342.

[Sil86] Joseph Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, no. 106, Springer, 1986.

[Tar51] Alfred Tarski, *A decision method for elementary algebra and geometry*, University of California Press, 1951.

[Vid94] Carlos Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), 249–253.

[vzGG03] Joachim von zur Gathen and Jürgen Gerhard, *Modern computer algebra*, Cambridge University Press, 2003.

[Was82] Lawrence Washington, *Introduction to cylotomic fields*, Graduate Texts in Mathematics, no. 83, Springer, 1982.

[Zah99] Karim Zahidi, *Existential undecidability for rings of algebraic functions*, Ph.D. thesis, Ghent University, 1999.

[Zah00] Karim Zahidi, *On diophantine sets over polynomial rings*, Proc. Amer. Math. Soc. **128** (2000), no. 3, 877–884.

[Zah02] Karim Zahidi, *Hilbert's tenth problem for rings of rational functions*, Notre Dame J. Formal Logic **43** (2002), no. 3, 181–192.

Index