Universidad de Concepción

Dirección de Postgrado

Facultad de Ciencias Físicas y Matemáticas - Programa de Doctorado en Matemática

Problemas de Decidibilidad en Torno a Estructuras con Adición y la Relación de Divisibilidad.

Tesis para optar al grado de *Doctor en Matemática*

LEONIDAS ANTONIO CERDA ROMERO

CONCEPCIÓN-CHILE

2017

Profesor Guía: Carlos Martinéz

Codirector: Xavier Vidaux

Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas

Universidad de Concepción

Universidad de Concepción

Dirección de Postgrado

Facultad de Ciencias Físicas y Matemáticas - Programa de Doctorado en Matemática

Problemas de Decidibilidad en Torno a Estructuras con Adición y la Relación de Divisibilidad.

LEONIDAS ANTONIO CERDA ROMERO

CONCEPCIÓN-CHILE

2017

Profesor Guía: Carlos Martinéz

Codirector: Xavier Vidaux

Dpto. de Matemática, Facultad de Ciencias Físicas y Matemáticas

Universidad de Concepción

Comisión Evaluadora:

Paola D'Aquino (Universita Degli Studi Della Campania)

Natalia García Fritz (Pontificia Universidad Católica de Chile)

Ricardo Menares (Pontificia Universidad Católica de Valparaiso)

Andrea Tironi (Universidad de Concepción)

Problemas de Decidibilidad en Torno a Estructuras con Adición y la Relación de Divisibilidad.

LEONIDAS ANTONIO CERDA ROMERO
UNIVERSIDAD DE CONCEPCIÓN

Concepción 2017

Contents

Agradecimientos

En primer lugar me gustaría dar las gracias a mis asesores, el Doctor Carlos Martínez y el Doctor Xavier Vidaux por todas las horas que dedicaron para mejorar la redacción de esta tesis. Estoy muy agradecido por todas las sugerencias, consejos y sobre todo por su enorme paciencia en la realización de este trabajo.

Finalmente, quisiera agradecer a todos aquellos que hicieron posible la realización de esta tesis.

Introduction

The object of this thesis is to extend (first-order) Diophantine undecidability results on addition and divisibility to rings that are localized at finite sets of primes. Our main results are resumed in the following theorem (the logical terms will be explained in Chapter 1).

Theorem 1. *1. Let S be a finite and non-empty set of prime numbers. Multiplication is positive-existentially definable in $\mathcal{Z}_S = (\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$, where the symbol $|$ stands for the usual divisibility (binary) relation.*

2. Let S be a non-empty finite set of irreducible polynomials over a finite field $\mathbb{F}$ of odd characteristic. Multiplication is positive-existentially definable in the structure $\mathcal{F}_S = (S^{-1}\mathbb{F}[t]; =, \mathbb{F}, 0, 1, +, |, f \mapsto tf)$, where $f \mapsto tf$ is the multiplication by t map. If $\mathbb{F}$ has a prime number of elements, then one can remove the constants $\mathbb{F}$ from the language.

In particular, the positive existential theory of both $\mathcal{Z}_S$ and $\mathcal{F}_S$ are undecidable.

This implies that there is no algorithm to decide whether or not an arbitrary system of linear equations over $\mathbb{Z}$ (resp. $\mathbb{F}[t]$), together with conditions of the form $x \mid y$ on the variables, has a solution over $\mathbb{Z}[S^{-1}]$ (resp. $S^{-1}\mathbb{F}[t]$).

We now introduce the historical context of our result.

Hilbert's Tenth Problem (referred to as "H10" in the sequel) asks for the following:

Given a polynomial equation (in an arbitrary number of variables) and with coefficients in $\mathbb{Z}$, find a process according to which it can be determined in a finite number of steps whether the equation is solvable in $\mathbb{Z}$.

Nowadays, one would ask whether the positive existential theory of the structure $(\mathbb{Z}; =, 0, 1, +, \cdot)$ is or not decidable — see Chapter 1 for the meaning of the logical concepts. Building on works by M. Davis, H. Putnam and J. Robinson, Y. Matiyasevich gave in 1970 a negative answer to H10 (see [Mat70], or [Da73]). Using J. Robinson's work [Ro49] and Matiyasevich's result for H10 over $\mathbb{Z}$, one can show that, if S is a finite set of primes, then Hilbert's Tenth problem over $\mathbb{Z}[S^{-1}]$ has a negative answer (see [Sh11, p. 240] or [Po03, p. 982]). It is not known whether the analogue of H10 for the field $\mathbb{Q}$ of rational numbers is decidable or not.

Before going specifically to addition and divisibility, we should mention that there has been a lot of results extending the negative solution to H10 in (at least) two directions.

On the one hand, undecidability results have been obtained for many classical structures over the ring language or extensions of it. We first list a few results regarding rings of functions in one or more variables (the language usually contains constant symbols for the variables), as they are relevant for possible extensions of our result about polynomial rings over finite fields — for general surveys on H10, or more generally on decidability problems in number theory, see for instance [Ph94, PhZ00, PhZ08, Ko14], and the book [Sh07], and the references therein. For polynomial rings (in any characteristic), this was solved by J. Denef [De78, De79]. T. Pheidas [Ph91] solved the problem for rational function fields over finite fields — see [Vide94] for the characteristic 2 case, and [Z03] for partial results towards the still open case where the base field is an algebraically closed field of characteristic zero. As far as algebraic extensions are concerned, see [Sh92, Ei03, Sh00], and with respect to completions see [Ph87a, Ph87b, LiPh95, Vida03, GaPas15]. Famously open problems are: $\mathbb{C}(t)$ (unless one adds a valuation in the language — note that even the full theory is not known to be undecidable) and the ring of entire functions over $\mathbb{C}$.

Concerning number fields, we should mention the following results. In [De75, De80, Ph88, Sh89, Vide89], it is shown that H10 for the ring of integers of a number field is unsolvable, as long as there are at most one pair of complex conjugate embeddings (the general case is solved modulo conjectures).

On the other hand, a lot of work has been done recently on trying to recover the ring structure from "looking-weaker" structures over the same base ring. See for instance [Wo81, Wo93, U11, Ga13, Ri16, PasVida16, U16]. More specifically for the case of defining positive-existentially multiplication from addition and k-th powers (for some fixed $k \geq 2$), we refer to the general survey [PasPhVida10] and the references therein.

In the late seventies, L. Lipshitz [Li77], and in parallel A. P. Bel'tyukov [B80], showed that the positive existential theory of the structure $(\mathbb{Z}; =, 0, 1, +, |)$ is decidable. Namely, there is an algorithm for deciding whether or not an arbitrary sentence of the form

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) \mid g_i(x_1, \ldots, x_n),$$

where the f_i and g_i are linear polynomials with integer coefficients, is true over $\mathbb{Z}$. Note that the full theory is undecidable (see [Wo81] — this is because the coprimality relation is defined from divisibility using Bézout's identity).

The full theory of the structure $(\mathbb{Q}; 0, 1, +, |)$ is decidable (see [Mar02, Th. 3.1.9]). Indeed, the structure $(\mathbb{Q}; 0, 1, +, |)$ is bi-interpretable with $(\mathbb{Q}; 0, 1, +, \neq)$.

In view of the results above, the following question arises naturally.

Question 1. *For which subrings $A \subseteq \mathbb{Q}$ is the positive existential theory of the structure $(A; =, 0, 1, +, |)$ decidable?*

Our main theorem answers this question for $A = \mathbb{Z}[S^{-1}]$, where S is any fixed finite set of primes.

At first sight, it is slightly surprising that inverting a single prime makes a difference about the decidability of the structure. Nevertheless, inverting just one prime makes the group of units infinite. Moreover, our result can be contrasted with the following result of J. Denef — see [De75]: the positive existential theory of the structure $(\mathbb{Z}; 0, 1, +, |_p)$ is undecidable, where the symbol $|_p$ has the following meaning for a fixed integer $p > 1$:

$$x \mid_p y \text{ if and only if there exist } z, i \in \mathbb{Z} \text{ such that } y = xzp^i.$$

Observe that the predicate $|_p$ is, in disguise, the divisibility in $\mathbb{Z}[\frac{1}{p}]$ restricted to $\mathbb{Z}$.

The main difficulties in adapting the arguments of J. Denef to our case come from the fact that our structure is not discrete. Nevertheless, we follow the classical strategy which consists of gradually defining the multiplication: first we square units, then we multiply a unit by an arbitrary element of the ring, and finally we define the squaring function. Multiplication is definable from the squaring function thanks to the identity $(x+y)^2 = x^2 + 2xy + y^2$.

Note that analogues of Lipshitz's result on addition and divisibility have been obtained for several rings of functions (for example for polynomial rings over a decidable field — see [Ph85], and for some richer structures — see [Si09]), so one may ask the analogue of Question 1 for all those rings. Our main theorem also essentially solves the problem for finite S over $\mathbb{F}_p[t]$, though we needed to extend the language with a symbol for multiplication $f \mapsto tf$ (the multiplication by t map). The technique uses more or less the strategy that we use for the integers, though one has to put a special attention to the dominant coefficients of the polynomials, and the final formula is different and requires new arguments.

We finish the introduction with a few questions that naturally arise from our main theorem.

B. Poonen showed [Po03] that there exist infinite sets S of primes of natural density 1 such that $\mathbb{Z}$ has a diophantine model in $\mathbb{Z}[S^{-1}]$ over the language of rings. This leads to the following question.

Question 2. *Is there a set S consisting of infinitely many primes such that multiplication is positive-existentially definable in the structure $\mathcal{Z}_S$? What about $\mathcal{F}_S$?*

In [Li78b], L. Lipshitz shows that if $\mathcal{O}$ is the ring of integers of a number field K, then multiplication can be recovered in a positive existential way from addition and divisibility if and only if K is not an imaginary quadratic extension of $\mathbb{Q}$. So more generally, we may ask:

Question 3. *For which rings of algebraic S-integers is multiplication positive-existentially definable from addition and divisibility?*

Introducción

El objetivo de esta tesis es extender algunos resultados de indecidibilidad (en lógica de primer orden) sobre problemas diofantinos en adición y divisibilidad, a anillos localizados por conjuntos finitos de primos. Nuestros principales resultados se resumen en el siguiente teorema (los términos lógicos serán explicados en el Capítulo 1).

Teorema 1. *1. Sea S un conjunto finito y no vacío de números primos. La multiplicación es definible de manera positivo existencial en $\mathcal{Z}_S = (\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$, donde el símbolo $|$ representa la relación (binaria) usual de divisibilidad.*

2. Sea S un conjunto no vacío y finito de polinomios irreducibles sobre un campo finito $\mathbb{F}$ de característica impar. La multiplicación es definible de manera positivo existencial en la estructura $\mathcal{F}_S = (S^{-1}\mathbb{F}[t]; =, \mathbb{F}, 0, 1, +, |, f \mapsto tf)$, donde $f \mapsto tf$ es la multiplicación por t. Más aún, si $\mathbb{F}$ tiene un número primo de elementos, entonces podemos remover el conjunto de constantes $\mathbb{F}$ de nuestro lenguaje.

En particular, la teoría positivo existencial de $\mathcal{Z}_S$ y $\mathcal{F}_S$ es indecidible.

Esto implica que no existe un algoritmo para decidir si o no un sistema de ecuaciones lineales arbitrario sobre $\mathbb{Z}$ (resp. $\mathbb{F}[t]$), junto con condiciones de la forma $x \mid y$ en las variables, tiene solución sobre $\mathbb{Z}[S^{-1}]$ (resp. $S^{-1}\mathbb{F}[t]$).

Ahora introducimos el contexto histórico de nuestro resultado.

El Décimo Problema de Hilbert (referido como "H10" en lo sucesivo) es el siguiente:

Dada una ecuación polinomial (en un número arbitrario de variables) con coeficientes en $\mathbb{Z}$, hallar un proceso según el cual se pueda determinar en un número finito de pasos si la ecuación tiene soluciones en $\mathbb{Z}$.

Utilizando el lenguaje moderno de lógica matemática, la pregunta se traduce a si la teoría positivo existencial de la estructura $(\mathbb{Z}; =, 0, 1, +, \cdot)$ es o no decidible — ver Capítulo 1. Basándose en trabajos de M. Davis, H. Putnam y J. Robinson, Y. Matiyasevich dio en 1970 una respuesta negativa a H10 (ver [Mat70], o [Da73]). Usando el trabajo de J. Robinson [Ro49] y el resultado de Matiyasevich para H10 sobre $\mathbb{Z}$, uno puede mostrar que, si S es un conjunto finito de primos, entonces el Décimo Problema de Hilbert sobre $\mathbb{Z}[S^{-1}]$ tiene una respuesta negativa (ver [Sh11, p. 240] o [Po03, p. 982]). No se conoce si el análogo de H10 para el campo $\mathbb{Q}$ de los números racionales es decidible o no.

Antes de tratar específicamente a la adición y divisibilidad, debemos mencionar que ha habido muchos resultados que extienden la solución negativa de H10 en (al menos) dos direcciones.

Por un lado, se han obtenido resultados de indecidibilidad para muchas estructuras clásicas sobre el lenguaje de anillos o extensiones del mismo. Primero enunciaremos algunos resultados con respecto a anillos de funciones en una o más variables (el lenguaje normalmente contiene símbolos de constantes para las variables), ya que son relevantes para posibles extensiones de nuestro resultado sobre anillos de polinomios sobre campos finitos — para estudios generales sobre H10 o, más generalmente, sobre problemas de decidibilidad en teoría de números, ver, por ejemplo, [Ph94, PhZ00, PhZ08, Ko14] y el libro [Sh07], y las referencias citadas en el. Para anillos de polinomios (en cualquier característica), este fue resuelto por J. Denef [De78, De79]. T. Pheidas [Ph91] resolvió el problema para los campos de funciones racionales sobre campos finitos — see [Vide94] para el caso de característica 2, y [Z03] para resultados parciales para el caso aún abierto de característica cero sobre un campo algebraicamente cerrado. Para extensiones algebraicas, ver [Sh92, Ei03, Sh00], y con respecto a completaciones ver [Ph87a, Ph87b, LiPh95, Vida03, GaPas15]. Los famosos problemas abiertos son: $\mathbb{C}(t)$ (a menos que se añada la valuación al lenguaje — observamos que incluso la

teoría completa no se sabe si es indecidible) y el anillo de funciones enteras sobre $\mathbb{C}$.

Con respecto a los campos de números, deberíamos mencionar los siguientes resultados. En [De75, De80, Ph88, Sh89, Vide89], se demuestra que H10 para el anillo de enteros de un campo de números es insoluble, siempre que haya a lo más un par de incrustaciones complejas (para el caso general sólo se conocen soluciones módulo conjeturas).

Por otro lado, recientemente ha habido mucho trabajo en intentar recuperar la estructura de anillo desde estructuras que son, a primera vista, más débiles sobre el mismo conjunto base. Ver por ejemplo [Wo81, Wo93, U11, Ga13, Ri16, PasVida16, U16]. Más específicamente, para el caso de definir de manera positivo existencial la multiplicación utilizando la adición y k-ésima potencias (para algún $k \geq 2$ fijo), ver el artículo [PasPhVida10] y las referencias contenidas en el.

A finales de los setenta, L. Lipshitz [Li77], y en paralelo A. P. Bel'tyukov [B80], demostraron que la teoría positivo existencial de la estructura $(\mathbb{Z}; =, 0, 1, +, |)$ es decidible. En otras palabras, existe un algoritmo para decidir si o no un enunciado arbitrario de la forma

$$\exists x_1 \ldots \exists x_n \bigwedge_{i=1}^{k} f_i(x_1, \ldots, x_n) \mid g_i(x_1, \ldots, x_n),$$

donde los f_i y g_i son polinomios lineales con coeficientes enteros, es verdadero sobre $\mathbb{Z}$. Observamos que la teoría completa es indecidible (ver [Wo81] — ya que ser coprimo se puede definir utilizando divisibilidad y la identidad de Bézout).

La teoría completa de la estructura $(\mathbb{Q}; 0, 1, +, |)$ es decidible (ver [Mar02, Th. 3.1.9]). Vale la pena mencionar que la estructura $(\mathbb{Q}; 0, 1, +, |)$ es bi-interpretable con la estructura $(\mathbb{Q}; 0, 1, +, \neq)$.

En vista de los resultados anteriores, la siguiente pregunta surge de manera natural.

Pregunta 1. *¿Para qué subanillos $A \subseteq \mathbb{Q}$ es la teoría positivo existencial de la estructura $(A; =, 0, 1, +, |)$ decidible?*

Nuestro teorema principal responde esta pregunta para $A = \mathbb{Z}[S^{=1}]$, donde S es un conjunto finito fijo de primos.

A primera vista, es un poco sorprendente que invertir un solo primo haga diferencia acerca de la indecidibilidad de la estructura. Sin embargo, invertir un solo primo hace el grupo de unidades infinito. Además, nuestro resultado puede ser contrastado con el siguiente resultado de J. Denef (ver [De75]) donde demuestra que la teoría positivo existencial de la estructura $(\mathbb{Z}; 0, 1, +, |_p)$ es indecidible, donde el símbolo "$|_p$" tiene el siguiente significado para un entero $p > 1$ fijo:

$$x \mid_p y \text{ si y sólo si existe } z, i \in \mathbb{Z} \text{ such that } y = xzp^i.$$

Observamos que el predicado $|_p$ corresponde a la divisibilidad en $\mathbb{Z}[\frac{1}{p}]$ restringida a $\mathbb{Z}$.

La principales dificultades para adaptar el argumento de J. Denef a nuestro caso viene del hecho que nuestra estructura no es discreta. Sin embargo, seguimos la estrategia clásica que consiste en ir definiendo gradualmente la multiplicación: primero para el cuadrado de unidades, luego la multiplicación de una unidad por un elemento arbitrario del anillo, y finalmente definimos la función cuadrádo. La multiplicación es definible utilizando el cuadrado gracias a la identidad $(x + y)^2 = x^2 + 2xy + y^2$.

Observamos que análogos al resultado de Lipshitz en adición y divisibilidad se han obtenido para varios anillos de funciones (por ejemplo para anillos de polinomios sobre un campo decidible —ver [Ph85], y para algunas estructuras enriquecidas — ver [Si09]), así uno puede preguntar sobre el análogo de la Pregunta 1 para todos estos anillos. Nuestro principal teorema también resuelve el problema para S finito sobre $\mathbb{F}[t]$, aunque, en este caso, necesitamos extender el lenguaje con un símbolo para la multiplicación $f \mapsto tf$ (la multiplicación por t). La demostración utiliza más o menos la misma estrategia que utilizamos para los enteros, aunque hay que prestar especial atención a los coeficientes principales de los polinomios, y la fórmula final es diferente y requiere nuevos argumentos.

Terminamos esta introducción con algunas preguntas que surgen naturalmente de nuestro teorema principal.

B. Poonen mostró [Po03] que existe un conjunto infinito S de números primos de densidad natural 1 tal que $\mathbb{Z}$ tiene un modelo diofantino en $\mathbb{Z}[S^{-1}]$ sobre el lenguaje

de anillos. Esto conduce a la siguiente pregunta:

Pregunta 2. *¿Existe un conjunto de infinitos números primos S tal que la multiplicación es positiva existencialmente definible en la estructura $\mathcal{Z}_S$? Qué se puede decir con respecto a $\mathcal{F}_S$.*

En [Li78b], L. Lipshitz muestra que si $\mathcal{O}$ es el anillo de enteros de un campo de números K, entonces la multiplicación puede recuperarse en forma positivo existencial utilizando la adición y divisibilidad si y sólo si K no es una extención cuadrática imaginaria de $\mathbb{Q}$. De manera más general, podemos preguntar:

Pregunta 3. *¿Para qué anillos de S-enteros algebraicos es la multiplicación positiva existencialmente definible utilizando adición y divisibilidad?*

Chapter 1

Logical background

In this chapter we recall the basic facts about Mathematical Logic that we need. For more details, see for instance [CL00] or [Mar02].

Given an algebraic structure, we are concerned with its *underlying language*, which consists of symbols for the distinguished constants, the operations and the relations of the structure. For instance, the underlying language $\mathcal{L}_0$ for the structure

$$\mathcal{Z}_S = (\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$$

is the set

$$\mathcal{L}_0 = \{=, 0, 1, +, |\},$$

and the underlying language $\mathcal{L}_1$ for the structure

$$\mathcal{F}_S = (S^{-1}\mathbb{F}[t]; =, \mathbb{F}, 0, 1, +, |, f \mapsto tf)$$

is the set

$$\mathcal{L}_1 = \{=, \mathbb{F}, 0, 1, +, |, f \mapsto tf\}.$$

A set of *variables* has been previously fixed. Here we will use the letters x, y and so on for variables. For our purposes, we shall assume that the set of variables is numerable.

Terms of the language are finite words that are made of variables, constants of the language and operations of the language, following the usual building rules of mathematics (using parenthesis as delimiters). For example, the word

$$x + 1 + 1 + y$$

is a term of $\mathcal{L}_0$, and the word

$$(t \times t + 1)x + (1 + 1)ty + t \times t \times t + 1$$

is a term of $\mathcal{L}_1$. We use the usual priority reading conventions and abbreviations, so for instance we may write 2 in the formulas instead of $1 + 1$, and t^2 instead of $t \times t$. So the second term that we wrote above takes the usual form

$$(t^2 + 1)x + 2ty + t^3 + 1.$$

Hence, for the language $\mathcal{L}_0$, the terms are the degree one polynomial functions over $\mathbb{N}$, while for $\mathcal{L}_1$ they are the degree one polynomial functions over $\mathbb{F}$. Note that we cannot write xy in a term because we do not have multiplication in our languages (in $\mathcal{L}_1$ the multiplication is only "multiplication by t").

An *atomic formula* is a relation of terms, where the relation is taken from the language. So for instance the words

$$(t^2 + 1)x + 2ty + t^3 + 1 = t^4x + 2z + 1$$

and

$$(t^2 + 1)x + 2ty + t^3 + 1 \mid t^4x + 2z + 1$$

are atomic formulas of $\mathcal{L}_1$. The atomic formulas with equality can have a "minus symbol", with its obvious meaning, so for instance we may write

$$(t^2 + 1)x + 2ty + t^3 + 1 - t^4x - 2z - 1 = 0$$

for the above atomic formula.

A *quantifier-free formula* is built from atomic formulas and logical connectives in the usual way, and following the usual conventions. In our context they are always finite words. So for instance, the word

$$(t^2x + y + 3 \mid ty + z \wedge tz = x + 1) \Longrightarrow x = z$$

is a quantifier-free formula in $\mathcal{L}_1$.

We obtain *formulas* from quantifier-free formulas by adding existential or universal quantifiers on the variables (in our context, quantification on sets is not

allowed — this is the difference between first-oder and higher-order predicate logic). So for instance

$$\exists y(t^2x + y + 3 \mid ty + z \wedge tz = x + 1) \Longrightarrow \forall z(x = z)$$

is a formula in $\mathcal{L}_1$.

A *sentence* is a formula in which every variable is quantified. A sentence may be true or false depending on the structure in which we *interpret* it. For instance, the sentence

$$\forall x \exists y(x = y + 1)$$

is true in the structure $(\mathbb{Z}; 1, +)$, but is false in $(\mathbb{N}; 1, +)$.

The universal closure of a formula φ is obtained from φ by adding in front of it a universal quantifier for each free variable in φ ("free" means "not quantified"). Two formulas φ and ψ are said to be *logically equivalent* if the universal closure of $\varphi \Longleftrightarrow \psi$ is true in every structure. A basic theorem of first-order predicate logic says that every formula is logically equivalent to a formula in *prenex form*, namely, in which all the quantifiers appear at the beginning (what come after the quantifiers is then called the *free part* of the prenex form).

An *existential formula* is a formula whose prenex form has only existential quantifiers. A *positive existential formula* is an existential formula whose prenex form has no negation in its free part.

A *theory* is a set of sentences. An *existential theory* is a set of existential sentences (namely, existential formulas which are sentences). A *positive existential theory* is a set of positive existential sentences.

The *(full) theory of a structure* is the set of all the sentences that are true in the structure. The *existential theory of a structure* is the set of all the existential sentences that are true in the structure. The *positive existential theory of a structure* is the set of all the positive existential sentences that are true in the structure.

Let T denote the (resp. existential, resp. positive existential) theory of a structure. We say that T is decidable if there is an algorithm (i.e. Turing machine, for instance), that takes as input an arbitrary (resp. existential, resp. positive existential) sentence, and outputs after finitely many steps an answer YES or NO,

depending on whether the sentence is true or not in the structure. It is obvious that if the theory of a structure is decidable, then also the existential theory and the positive existential theory of that structure are decidable. In the three cases, we say that T is *undecidable* if it is not decidable. So if the positive existential theory of a structure is undecidable, then also the existential theory and the theory of that structure are undecidable. A famous theorem by Presburger (see [St84]) says that the full theory of $(\mathbb{N}; 0, 1, +)$ is decidable. On the other hand, a consequence of Matiyasevich's theorem, mentioned in the introduction, is that the positive existential theory of $(\mathbb{Z}; 0, 1, +, \cdot)$ is undecidable.

We need another concept from mathematical logic which is the key ingredient for our work. Given an algebraic structure $\mathcal{M}$ with underlying set M, a natural number $n \geq 1$, and $A \subseteq M^n$, we say that A is *definable* if there is a formula $\varphi(x_1, ..., x_n)$ so that the following happens: $(a_1, ..., a_n) \in A$ if and only if the formula $\varphi(a_1, ..., a_n)$, obtained from $\varphi(x_1, ..., x_n)$ by substituting x_i by a_i, is true in the structure. We also say that a function $f\colon M^n \to M$ is *definable* if its graph is definable. For example, it follows from Lagrange's four square theorem, that $\mathbb{N}$ is definable in $(\mathbb{Z}, 0, 1, +, \cdot)$ by the formula

$$\exists x_1, x_2, x_3, x_4 (x = x_1^2 + x_2^2 + x_3^2 + x_4^2).$$

We say that $A \subseteq M^n$ is *existentially* (resp. *positive-existentially*) *definable* if it is definable by an existential (resp. positive existential) formula.

Definability is of utmost importance because it allows to transfer undecidability results from a structure to another. To be more precise, if we have two structures $\mathcal{M}_1$ and $\mathcal{M}_2$ with the same underlying set M such that, the theory of $\mathcal{M}_1$ is undecidable, and the constants, operations and relations of $\mathcal{M}_1$ are definable in $\mathcal{M}_2$, then the theory of $\mathcal{M}_2$ is also undecidable, as definability allows to translate formulas from one language to the other. We will finish these preliminaries with a more formal explanation of how this works in our situation.

Let $\varphi(x, y, z)$ be a formula that positive-existentially defines multiplication in the structure $\mathcal{Z}_S$. This means that for any triple $(a, b, c) \in \mathbb{Z}[S^{-1}]^3$, we have $c = ab$ if and only if $\varphi(a, b, c)$ is true in $\mathcal{Z}_S$. Assume that there exists an algorithm $\mathcal{A}$ to decide whether a positive existential sentence is true or false in $\mathcal{Z}_S$. Here is

an algorithm that would decide the truth of any positive existential sentence in $(\mathbb{Z}[S^{-1}]; 0, 1, +, \cdot)$, contradicting a result by Julia Robinson. Given a sentence ψ in the language $(0, 1, +, \cdot)$, we can transform it into a positive existential sentence $\overline{\psi}$ in the language $\mathcal{L}_0$ using our formula φ to get rid of each occurrence of multiplication, in such a way that $\overline{\psi}$ is true in $\mathcal{Z}_S$ if and only if ψ is true in $(\mathbb{Z}[S^{-1}]; 0, 1, +, \cdot)$. Using the algorithm $\mathcal{A}$, we could decide whether $\overline{\psi}$ is true in $\mathcal{Z}_S$, hence we could decide whether ψ is true in $(\mathbb{Z}[S^{-1}]; 0, 1, +, \cdot)$.

It is important to realize that the transformation of ψ into $\overline{\psi}$ can be done by an algorithm (the algorithm should not depend on the specific ψ that we want to transform, but only on the languages involved). To illustrate the idea, we just give one example of transformation, and let the reader convince himself that one can write a general algorithm. So, for instance, the sentence

$$\exists u, v(uv + 2 = 3)$$

is true in $(\mathbb{Z}[S^{-1}]; 0, 1, +, \cdot)$ if and only if the sentence

$$\exists z, u, v(\varphi(u, v, z) \wedge z + 2 = 3)$$

is true in $\mathcal{Z}_S$.

Chapter 2

The Diophantine problem for addition and divisibility over subrings of the rationals.

This chapter is dedicated to prove the first part of Theorem 1.

2.1 Preliminaries

We need to introduce some notations and definitions which will be used throughout this chapter.

Notation 2.1. *1. The notation*

$$\mathrm{as}(x, y)$$

stands for the formula

$$x|y \wedge y|x$$

(namely, x and y are associate).

2. The notation

$$x \pm y \mid w \pm z$$

stands for

$$x + y \mid w + z \wedge x - y \mid w - z.$$

3. *If* $\gamma = (\gamma_1, \ldots, \gamma_M)$ *is a vector of natural numbers, then* p^γ *will denote the product*
$$\prod_{i=1}^{M} p_i^{\gamma_i}.$$
4. *We may write* $v \equiv w \pmod{l}$ *instead of* $l \mid v - w$ *in some formulas.*
5. *If* p *is a prime number and* x *is a rational number, we will denote by* $\mathrm{ord}_p(x)$ *the usual order at* p *of* x.

We now introduce a concept of *norm* for elements of $\mathbb{Z}[S^{-1}]$, which will play a central role in our proof.

Definition 2.2. *We will call* norm function *the map* $N\colon \mathbb{Z}[S^{-1}] \longrightarrow \mathbb{Z}$ *defined by*
$$N(x) = x \prod_{p_i \in S} p_i^{-\mathrm{ord}_{p_i} x}$$
if $x \neq 0$, *and* $N(0) = 0$.

It is immediate to see that the function N satisfies the following properties. For every $x, y \in \mathbb{Z}[S^{-1}]$, we have:

1. $N(xy) = N(x)N(y)$.
2. $N(x) = 0$ if only if $x = 0$.
3. x divides y (in $\mathbb{Z}[S^{-1}]$) if only if $N(x)$ divides $N(y)$ (in $\mathbb{Z}$).
4. The norm of a unit is ± 1.

2.2 Undecidability of the structure $\mathcal{Z}$

We recall that $\mathcal{Z}_S$ is by definition the structure $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$. We first show that the relation "different from 0" is positive-existentially definable in $\mathcal{Z}_S$. In order to do this we need the following result of F. Pappalardi (see Theorem 3.1 [Pap97]).

Let $p_1, \ldots, p_M$ be prime numbers. Let Γ denote the subgroup of $\mathbb{Q}^*$ generated by $p_1, \ldots, p_M$. For each prime q different from any of $p_1, \ldots, p_M$, we consider the reduction Γ_q of Γ modulo q. The group Γ_q can be viewed as a subgroup of $\mathbb{F}_q^*$. We denote by $N_\Gamma(x)$ the number of primes $q \leq x$ such that

- q is not equal to any of $p_1, \ldots, p_M$, and
- $\mathbb{F}_q^* = \Gamma_q$.

Theorem 2.3 (Pappalardi, '97)**.** *There exist constants c_Γ and δ_Γ, depending only on Γ, such that*

$$N_\Gamma(x) \leq \delta_\Gamma \frac{x}{\log x} + c_\Gamma \frac{x}{(\log\log x)^M \log x}.$$

Moreover, $\delta_\Gamma < 1$ and it can be explicitly computed.

Lemma 2.4. *Let S be a finite non-empty set of prime numbers. There exists a prime q not in S, and an integer $b \in \{1, \ldots, q-1\}$, such that $qx + b$ is never a unit of $\mathbb{Z}[S^{-1}]$ as x varies in $\mathbb{Z}[S^{-1}]$.*

Proof. From Theorem 2.3 and the Prime Number Theorem, we can find a prime number $q \notin S$ so that $\Gamma_q \neq \mathbb{F}_q^*$, because since $\delta_\Gamma < 1$, we have that there is an N and $0 < \delta < 1$ such that

$$\forall x \geq N \quad N_\Gamma(x) \leq \left(\delta_\Gamma + \frac{c_\Gamma}{(\log\log x)^M}\right) \frac{x}{\log x} < \delta \frac{x}{\log x}$$

Thus, $N_\Gamma(x) \neq \pi(x)$ for some x, as otherwise this would contradict $\pi(x) \sim \frac{x}{\log x}$. Choose $b \in \{1, \ldots, q-1\}$ whose class modulo q is an element of $\mathbb{F}_q^* \setminus \Gamma_q$. It is straightforward to check that q and b are as required. □

Lemma 2.5. *The relation "$\neq$" is positive-existentially definable in the structure $\mathcal{Z}_S$.*

Proof. Let q and b be the integers given by Lemma 2.4. We will show that the formula

$$\psi_{\neq}(y) : \exists A, B, x (y \mid A \wedge qx + b \mid B \wedge A + B = 1)$$

defines the relation "$y \neq 0$" in $\mathcal{Z}_S$.

First note that the formula $\psi_{\neq}(y)$ translates to "There exist $r, s, x \in \mathbb{Z}[S^{-1}]$ such that $ry + s(qx + b) = 1$" in $\mathcal{Z}_S$.

If $y = 0$, then the formula is false, since by Lemma 2.4, $qx + b$ is never a unit in $\mathbb{Z}[S^{-1}]$.

Assume $y \neq 0$. Since q and b are relatively prime, by Dirichlet's theorem on primes in arithmetic progression, there exists x such that $qx + b$ is a prime number,

and furthermore coprime with $N(y)$. By Bézout's identity, there are integers r' and s such that

$$r'N(y) + s(qx + b) = 1.$$

Since $y = N(y)u$, where u is a unit in $\mathbb{Z}[S^{-1}]$, we have

$$\frac{r'}{u}y + s(qx + b) = 1.$$

□

Remark 2.6. *Lemma 2.5 allows us to write in our formulas expressions of the form* $x \neq y$.

Lemma 2.7. *Let* x, y, z *and* v *be arbitrary elements of* $\mathbb{Z}[S^{-1}]$. *If for all* i *such that* $1 \leq i \leq M$, *we have* $\operatorname{ord}_{p_i} x \neq \operatorname{ord}_{p_i} y$, $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} v$ *and, furthermore* $\operatorname{as}(x \pm y, z \pm v)$ *holds in* $\mathcal{Z}_S$, *then either* $xv = yz$ *or* $xz = yv$.

Proof. From $\operatorname{as}(x \pm y, z \pm v)$ there are units u_1 and u_2 such that

$$x + y = u_1(z + v) \quad \text{and} \quad x - y = u_2(z - v). \tag{2.1}$$

Observe that since $\operatorname{ord}_{p_i} x \neq \operatorname{ord}_{p_i} y$, we have

$$\operatorname{ord}_{p_i}(x + y) = \min\{\operatorname{ord}_{p_i} x, \operatorname{ord}_{p_i} y\} = \operatorname{ord}_{p_i}(x - y)$$

and since $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} v$, we have

$$\operatorname{ord}_{p_i}(z + v) = \min\{\operatorname{ord}_{p_i} z, \operatorname{ord}_{p_i} v\} = \operatorname{ord}_{p_i}(z - v)$$

for all $1 \leq i \leq M$. Thus, for each $1 \leq i \leq M$, we have

$$\begin{cases} \operatorname{ord}_{p_i} u_1 + \min\{\operatorname{ord}_{p_i} z, \operatorname{ord}_{p_i} v\} = \min\{\operatorname{ord}_{p_i} x, \operatorname{ord}_{p_i} y\} \\ \operatorname{ord}_{p_i} u_2 + \min\{\operatorname{ord}_{p_i} z, \operatorname{ord}_{p_i} v\} = \min\{\operatorname{ord}_{p_i} x, \operatorname{ord}_{p_i} y\} \end{cases}$$

so that $\operatorname{ord}_{p_i} u_1 = \operatorname{ord}_{p_i} u_2$ (note that the hypothesis of the Lemma implies that all the terms in these equalities are actual integers). This implies that either $u_1 = u_2$ or $u_1 = -u_2$. We proceed by cases.

If $u_1 = u_2$, then from Equations (2.1), we have

$$x + y = u_1 z + u_1 v$$

and

$$x - y = u_1 z - u_1 v.$$

By adding and subtracting these equations, we obtain $x = u_1 z$ and $y = u_1 v$, hence $xv = yz$.

If $u_1 = -u_2$, then from Equations (2.1), we have $x + y = u_1 z + u_1 v$ and $x - y = -u_1 z + u_1 v$. By adding and subtracting these equations again, we obtain $x = u_1 v$ and $y = u_1 z$, hence $xz = yv$. □

The next Lemma is a fundamental step to show that the squaring function among units of $\mathbb{Z}[S^{-1}]$ is positive-existentially definable in $\mathcal{Z}_S$(see Proposition 2.9).

Lemma 2.8. *Let x, y be units in $\mathbb{Z}[S^{-1}]$ with $x \neq \pm 1$ and $y \neq 1$. If for all i such that $1 \leq i \leq M$, we have $\operatorname{ord}_{p_i} x \neq \operatorname{ord}_{p_i} y$, then $y = x^2$ if and only if $\operatorname{as}(x \pm 1, y \pm x)$ holds in $\mathcal{Z}_S$.*

Proof. If $y = x^2$ then trivially $\operatorname{as}(x \pm 1, y \pm x)$ holds in $\mathcal{Z}_S$ (since x is a unit). Suppose that $\operatorname{as}(x \pm 1, y \pm x)$ is true in $\mathbb{Z}[S^{-1}]$. By Lemma 2.7, either $y = x^2$ or $xy = x$. Since x is a unit and $y \neq 1$, we conclude that $y = x^2$. □

Proposition 2.9. *The set*

$$\mathrm{SQ_u} = \{(x, y) \colon x, y \text{ are units in } \mathbb{Z}[S^{-1}] \text{ and } y = x^2\}$$

is positive-existentially definable in the structure $\mathcal{Z}_S$.

Proof. Write $I = \{0, 1, 2, 3\}^M$. The formula

$$\mathrm{Sq_u}(x, y) \colon x \mid 1 \wedge y \mid 1 \wedge \bigwedge_{\gamma \in I} \operatorname{as}(p^\gamma x \pm 1, p^{2\gamma} y \pm p^\gamma x)$$

where $\gamma = (\gamma_1, \ldots, \gamma_M)$, defines the set $\mathrm{SQ_u}$.

Assume that $\mathrm{Sq_u}(x, y)$ holds. In particular, the formula

$$\operatorname{as}(p^\gamma x \pm 1, p^{2\gamma} y \pm p^\gamma x)$$

holds for γ being such that

$$\gamma_i \in \{0, 1, 2, 3\} \setminus \left\{ -\operatorname{ord}_{p_i} x, -\frac{1}{2} \operatorname{ord}_{p_i} y, \operatorname{ord}_{p_i} x - \operatorname{ord}_{p_i} y \right\}$$

for each i. We have

- $\operatorname{ord}_{p_i} p^\gamma x = \gamma_i + \operatorname{ord}_{p_i} x \neq 0$,
- $\operatorname{ord}_{p_i} p^{2\gamma} y = 2\gamma_i + \operatorname{ord}_{p_i} y \neq 0$ and
- $\operatorname{ord}_{p_i} p^\gamma x - \operatorname{ord}_{p_i} p^{2\gamma} y = \gamma_i + \operatorname{ord}_{p_i} x - 2\gamma_i - \operatorname{ord}_{p_i} y \neq 0$,

so that $p^\gamma x$ and $p^{2\gamma} y$ satisfy the hypothesis of Lemma 2.8. We conclude that $y = x^2$. □

Remark 2.10. *Proposition 2.9 allows us to write in our formulas expressions of the form $x^2, x^4, \ldots$ whenever x is a unit.*

The next Lemma is the first step to show that multiplication between units and arbitrary elements is definable. Write $\nu(x, y, z)$ for the formula

$$\operatorname{as}(y \pm 1, z \pm x) \wedge \operatorname{as}(y \pm x, z \pm x^2).$$

Lemma 2.11. *Let x be a unit in $\mathbb{Z}[S^{-1}]$ with $x \neq \pm 1$. If for all i such that $1 \leq i \leq M$, we have $\operatorname{ord}_{p_i} y \neq 0$, $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} x$, $\operatorname{ord}_{p_i} y \neq \operatorname{ord}_{p_i} x$ and $\operatorname{ord}_{p_i} z \neq \operatorname{ord}_{p_i} x^2$, then $z = xy$ if and only if $\mathcal{Z}_S$ satisfies $\nu(x, y, z)$.*

Proof. Assume that the formula $\nu(x, y, z)$ holds in $\mathcal{Z}_S$. By Lemma 2.7, since $\operatorname{as}(y \pm 1, z \pm x)$ holds, we have that either $z = xy$ or $x = yz$. Again by Lemma 2.7, since $\operatorname{as}(y \pm x, z \pm x^2)$ holds, we have that either $z = xy$ or $x^3 = yz$. So the only case in which we may have $z \neq xy$ is when $x = yz$ and $x^3 = yz$, which would imply that $x = \pm 1$. □

Proposition 2.12. *The set*

$$P = \{(x, y, z) : x \text{ is a unit and } z = xy\}$$

is positive-existentially definable in the structure $\mathcal{Z}_S$.

Proof. Write $I = \{0, 1, 2, 3\}^M$. The formula

$$\operatorname{Pro}(x, y, z) \colon x \mid 1 \wedge \bigwedge_{(\delta,\gamma) \in I \times I} \nu(p^\gamma x, p^\delta y, p^{\delta+\gamma} z)$$

defines the set P. Note that if $z = xy$, then $\mathrm{Pro}(x, y, x)$ is trivially satisfied for $(x, y, z) \in P$, since $p^\gamma x$ is a unit. We now prove the converse. We choose δ_i such that

$$\delta_i \in \{0, 1, 2, 3\} \setminus \{-\operatorname{ord}_{p_i} y, \operatorname{ord}_{p_i} x - \operatorname{ord}_{p_i} z\}.$$

Once δ_i has been chosen, we choose γ_i such that

$$\gamma_i \in \{0, 1, 2, 3\} \setminus \{-\operatorname{ord}_{p_i} x, \delta_i + \operatorname{ord}_{p_i} y - \operatorname{ord}_{p_i} x, \delta_i + \operatorname{ord}_{p_i} z - 2\operatorname{ord}_{p_i} x\}.$$

From $\gamma_i \neq -\operatorname{ord}_{p_i} x$ we have $p^\gamma x \neq \pm 1$. In addition for each i, we have

- $\operatorname{ord}_{p_i} p^\delta y = \delta_i + \operatorname{ord}_{p_i} y \neq 0$,
- $\operatorname{ord}_{p_i} p^{\delta+\gamma} z - \operatorname{ord}_{p_i} p^\gamma x = \delta_i + \operatorname{ord}_{p_i} z - \operatorname{ord}_{p_i} x \neq 0$,
- $\operatorname{ord}_{p_i} p^\delta y - \operatorname{ord}_{p_i} p^\gamma x = \delta_i + \operatorname{ord}_{p_i} y - \gamma_i - \operatorname{ord}_{p_i} x \neq 0$ and
- $\operatorname{ord}_{p_i} p^{\delta+\gamma} z - \operatorname{ord}_{p_i} p^{2\gamma} x^2 = \delta_i + \operatorname{ord}_{p_i} z - \gamma_i - 2\operatorname{ord}_{p_i} x \neq 0$,

so that $p^\gamma x$, $p^\delta y$ and $p^{\delta+\gamma} z$ satisfy the hypothesis of Lemma 2.11. Since we assumed that $\mathrm{Pro}(x, y, z)$ holds, in particular $\nu(p^\gamma x, p^\delta y, p^{\delta+\gamma} z)$ holds, so we can conclude that $z = xy$. □

Remark 2.13. *Proposition 2.12 allows us to write in our formulas polynomial expressions with coefficients in $\mathbb{Z}$ whenever the variable is a unit. For example, we can write the term $a_0 + a_1 x + a_2 x^2 + a_3 x^3$ as follows:*

$$\mathrm{Pro}(x, x, y) \wedge \mathrm{Pro}(x, y, z) \wedge w = a_0 + a_1 x + a_2 y + a_3 z.$$

In particular, we can write expressions of the form $(x \pm 1)^n$ whenever x is a unit.

Lemma 2.14. *Given $x_1, \ldots, x_n \neq 0$ in $\mathbb{Z}[S^{-1}]$, there exists a unit $u \neq 1$ such that each x_i divides $u - 1$.*

Proof. Choose any prime q in S and consider

$$u = q^{\operatorname{lcm}\{\varphi(|N(x_i)|)\colon i=1,\ldots,n\}}$$

where "lcm" stands for "least common multiple". Since $N(x_i)$ divides

$$q^{\varphi(|N(x_i)|)} - 1$$

in $\mathbb{Z}$ (by Euler's theorem - note that $N(x_i)$ is prime with q by definition of the norm), also it divides $u-1$, hence

$$x_i = N(x_i)\prod p_j^{\mathrm{ord}_{p_j} x_i}$$

divides $u-1$ in $\mathbb{Z}[S^{-1}]$. □

The following formulas are inspired by the ones in Lemma 3 of [Ph87b]. The adjustment that is needed is due to the fact that we are dealing with a non discrete structure.

Let $I := \{0,1\}^M$. We will write u instead of (u_1,u_2,u_3,u_4). The following formula will allow us to define the quadratic function in the structure $\mathbb{Z}_S$.

$$\varphi(x,y)\colon \exists u(\bigwedge_{i=1}^{4} u_i \mid 1 \wedge \bigwedge_{i=1}^{3} u_i \neq 1 \wedge \varphi_0(x,y,u)),$$

where $\varphi_0(x,y,u)$ is the conjunction of the following formulas:

$$\varphi_1(x,u_1)\colon \bigwedge_{\delta\in I} p^{\delta}x \pm 1 \mid u_1 - 1,$$

$$\varphi_2(y,u_1)\colon \bigwedge_{\gamma\in I} p^{\gamma}y \pm 1 \mid u_1 - 1,$$

$$\varphi_3(u_1)\colon p_1\dots p_M + 1 \mid u_1 - 1$$

$$\varphi_4(u_1,u_2)\colon (u_1-1)^{8M} \mid u_2 - 1,$$

$$\varphi_5(u_2,u_3)\colon u_2 - 1 \mid u_3 - 1,$$

$$\varphi_6(x,u_2,u_3,u_4)\colon \frac{u_3-1}{u_2-1}u_4 \equiv x \pmod{u_2-1},$$

$$\varphi_7(y,u_2,u_3,u_4)\colon \left(\frac{u_3-1}{u_2-1}u_4\right)^2 \equiv y \pmod{u_2-1}.$$

Remark 2.15. *It is worth mentioning that in the formulas φ_6 and φ_7 we are using (abusing of) the congruence notation in order to make the forthcoming arguments more transparent.*

However, for sake of completeness we spell out, in gory details, the formula φ_6. First note that $\dfrac{u_3-1}{u_2-1} = z$ is equivalent to

$$\exists z'(u_3 - 1 = z' - z \wedge \mathrm{Pro}(u_2,z,z')).$$

Hence, $\varphi_6(x, u_2, u_3, u_4)$ can be written as:

$$\exists z', z''(u_2 - 1|z'' - x \wedge \mathrm{Pro}(u_4, z, z'') \wedge \ u_3 - 1 = z' - z \wedge \mathrm{Pro}(u_2, z, z')).$$

Lemma 2.16. *Let x and y in $\mathbb{Z}[S^{-1}]$. If $\varphi(x, y)$ holds in $\mathcal{Z}_S$, then $y = x^2$.*

Proof. Let $\delta, \gamma \in I$ be such that, for each $1 \leq j \leq M$, we have

$$\mathrm{ord}_{p_j} p^{\delta} x \neq 0 \quad \text{and} \quad \mathrm{ord}_{p_j} p^{\gamma} y \neq 0.$$

Write $a = N(x)$ and $b = N(y)$, and for each i, $\alpha_i = \mathrm{ord}_{p_i} x$ and $\beta_i = \mathrm{ord}_{p_i} y$, so that

$$x = a \prod p_i^{\alpha_i} \quad \text{and} \quad y = b \prod p_i^{\beta_i}.$$

Since $\varphi_1(x, u_1)$ holds, we have that $N(\prod p_i^{\delta_i} x \pm 1)$ divides $N(u_1 - 1)$, hence if $x \neq 0$, then each α_i is non zero and

$$\begin{aligned} |N(u_1 - 1)| &\geq \left| N\left(1 \pm x \prod p_i^{\delta_i}\right)\right| \\ &= \left| N\left(1 \pm a \prod p_i^{\alpha_i + \delta_i}\right)\right| \\ &= \left| a \prod_{\alpha_i + \delta_i \geq 0} p_i^{\alpha_i + \delta_i} \pm \prod_{\alpha_i + \delta_i < 0} p_i^{-\alpha_i - \delta_i} \right|. \end{aligned}$$

Analogously, since $\varphi_2(y, u_1)$ holds, if $y \neq 0$, then each β_i is non zero and we have

$$\left| b \prod_{\beta_i + \gamma_i \geq 0} p_i^{\beta_i + \gamma_i} \pm \prod_{\beta_i + \gamma_i < 0} p_i^{-\beta_i - \gamma_i} \right| \leq |N(u_1 - 1)|.$$

Therefore, for each i such that $1 \leq i \leq M$, we have

$$|N(u_1 - 1)| \geq \begin{cases} \max\{|a|, |b|, p_i^{|\alpha_i| + \delta_i}, p_i^{|\beta_i| + \gamma_i}\} & \text{if } x \neq 0 \text{ and } y \neq 0, \\ \max\{|b|, p^{|\beta_i| + \gamma_i}\} & \text{if } x = 0 \text{ and } y \neq 0, \\ \max\{|a|, p^{|\alpha_i| + \delta_i}\} & \text{if } x \neq 0 \text{ and } y = 0, \end{cases} \tag{2.2}$$

We prove that in all cases, we have

$$|N(y - x^2)| < |N(u_2 - 1)|. \tag{2.3}$$

Indeed, if x and y are non zero, then we have

$$\begin{aligned}
|N(y-x^2)| &= \left|N\left(b\prod p_i^{\beta_i} - a^2\prod p_i^{2\alpha_i}\right)\right| \\
&= \left|N\left(b\prod p_i^{\beta_i-2\alpha_i} - a^2\right)\right| \\
&= \left|N\left(b\prod_{\beta_i-2\alpha_i\geq 0} p_i^{\beta_i-2\alpha_i} - a^2\prod_{\beta_i-2\alpha_i<0} p_i^{2\alpha_i-\beta_i}\right)\right| \\
&\leq \left|b\prod_{\beta_i-2\alpha_i\geq 0} p_i^{\beta_i-2\alpha_i} - a^2\prod_{\beta_i-2\alpha_i<0} p_i^{2\alpha_i-\beta_i}\right| \\
&\leq 2a^2|b|\prod_{i=1}^{M} p_i^{2|\alpha_i|+|\beta_i|} \\
&< |N(u_1-1)|^{8M} \\
&\leq |N(u_2-1)|,
\end{aligned}$$

where the strict inequality is justified by Equation (2.2) and the fact that

$$|N(u_1-1)| \geq 3$$

(since $\varphi_3(u_1)$ holds), and the last inequality by the fact that $\varphi_4(u_1,u_2)$ holds. Similarly, if $x=0$ and $y\neq 0$, we have

$$|N(y)| = |b| < |N(u_1-1)|^{8M} \leq |N(u_2-1)|,$$

and if $x\neq 0$ and $y=0$, then

$$|N(x^2)| = a^2 < |N(u_1-1)|^{8M} \leq |N(u_2-1)|.$$

On the other hand, since $\varphi_6(x,u_2,u_3,u_4)$ and $\varphi_7(y,u_2,u_3,u_4)$ hold, u_2-1 divides $y-x^2$. Hence, if $y-x^2\neq 0$, then

$$|N(y-x^2)| \geq |N(u_2-1)|,$$

which contradicts the strict inequality (2.3). □

Lemma 2.17. *The set*

$$SQ = \{(x,y)\colon x,y \text{ are in } \mathbb{Z}[S^{-1}] \text{ and } y=x^2\}$$

is positive existentially definable in the structure $\mathcal{Z}_S$.

Proof. We claim that the formula

$$\mathrm{Sq}(x,y)\colon (x=0\wedge y=0)\vee\bigvee_{\delta\in I}(x=\pm p^{-\delta}\wedge y=p^{-2\delta})\vee\varphi(x,y),$$

defines the set SQ. Indeed, if the formula holds, then it is immediate from Lemma 2.16 that $y=x^2$.

Suppose that $(x,y)\in SQ$. If $x=0$ or $x=\pm p^{-\delta}$ for some $\delta\in I$, then $Sq(x,y)$ is trivially satisfied. Hence we can suppose $x\neq 0$ and $x\neq\pm p^{-\delta}$ for every $\delta\in I$.

For each $\delta\in I$, since $x\neq\pm p^{-\delta}$, we have $p^{\delta}x\pm 1\neq 0$. We prove that $p^{\delta}y\pm 1\neq 0$ for every δ. If $p^{\delta}y=\pm 1$, then $p^{\delta}x^2=\pm 1$, hence $\delta_i+2\,\mathrm{ord}_{p_i}x=0$, so that δ_i is even, namely $\delta_i=0$ (since $\delta_i\in\{0,1\}$). So we have $x=\pm 1$, which contradicts our hypothesis on x.

From Lemma 2.14, there is a unit u_1 distinct from 1 such that the formulas $\varphi_1(x,u_1)$, $\varphi_2(y,u_1)$ and $\varphi_3(u_1)$ are satisfied. Because u_1-1 is not zero we deduce, from Lemma 2.14 again, that there is a unit u_2 different from 1 such that the formula $\varphi_4(u_1,u_2)$ is satisfied. If we put

$$u_3=u_2^{|N(x)|},$$

then u_3 is different from 1 (recall that $x\neq 0$), so that the formula $\varphi_5(u_2,u_3)$ is also satisfied.

Since

$$\frac{u_3-1}{u_2-1}=u_2^{|N(x)|-1}+\cdots+1$$

and the right-hand side of this equality has $|N(x)|$ summands, we deduce that

$$\frac{u_3-1}{u_2-1}\equiv|N(x)|\pmod{u_2-1}.$$

If we choose

$$u_4=\frac{x}{N(x)},$$

then the formulas $\varphi_6(x,u_2,u_3,u_4)$ and $\varphi_7(y,u_2,u_3,u_4)$ are satisfied. Thus, the formula $\varphi(x,y)$ is satisfied. □

Remark 2.18. *From Lemma 2.17 is possible to define multiplication in the structure $\mathcal{Z}_S$. Indeed, is sufficient to use the following equivalence:*

$$z=xy \text{ if and only if } (x+y)^2=x^2+2z+y^2.$$

Chapter 3

Definability in rings of polynomials over finite fields of positive characteristic.

In this chapter we will prove the second part of Theorem 1. So from now on we fix an arbitrary finite field $\mathbb{F}$ of odd characteristic, and a non-empty finite set

$$S = \{Q_1, \dots, Q_M\}$$

of M irreducible polynomials. We want to define multiplication in the structure

$$\mathcal{F}_S = (S^{-1}\mathbb{F}[t]; =, \mathbb{F}, 0, 1, +, |, f \mapsto tf).$$

3.1 Definability of "to be distinct"

We start by proving that the relation "different from 0" is positive-existentially definable in $\mathcal{F}_S$. In order to do this, we need the following results. The first one is an analogue of Dirichlet theorem for primes in arithmetic progressions — see [KorLan19].

Theorem 3.1 (Kornblum, '19)**.** *Let $a, m \in \mathbb{F}[t]$ be two relatively prime polynomials. If m has positive degree, then the set*

$$\Gamma = \{p \in \mathbb{F}[t] \colon p \equiv a \ (mod\ m),\ p \text{ is irreducible}\}$$

has positive Dirichlet density. In particular, Γ *is infinite.*

Before stating the next result, we need to introduce some notation:

- K is a function field in one variable over a finite field.
- F is a finite Galois extension of K.
- $C \subseteq \mathrm{Gal}(F/K)$ is a union of conjugacy classes.
- W is a finitely generated subgroup of K^*, of rank $r \geq 1$ modulo its torsion subgroup.
- k is an integer relatively prime with the characteristic p of K.
- If $\mathfrak{p}$ is a prime of K, $(\mathfrak{p}, F/K)$ will denote the *Frobenius symbol*.

Let $\mathcal{M} = \mathcal{M}(K, F, C, W, k)$ denote the set of primes $\mathfrak{p}$ so that:

1. $(\mathfrak{p}, F/K) \subseteq C$,
2. $\mathrm{ord}_{\mathfrak{p}}(w) = 0$ for all $w \in W$, and
3. if $\psi\colon W \to \overline{K}_{\mathfrak{p}}^*$ denote the quotient map to the unit subgroup of the residue class field, then the index of $\psi(W)$ in $\overline{K}_{\mathfrak{p}}^*$ divides k.

Lenstra [Le77] found a formula for the Dirichlet density of $\mathcal{M}$. In order to state this formula, we need to introduce some further notation. Consider K, F, C, W and k as above. For a prime number $\ell \neq p$, let $q(\ell)$ be the smallest power of ℓ not dividing k and let

$$L_\ell = K\left(\zeta_{q(\ell)}, W^{\frac{1}{q(\ell)}}\right)$$

be the field obtained by adjoining all $q(\ell)$-roots of the elements of W to K. If n is a positive square-free integer, relatively prime to p, then define L_n to be the composite of the fields L_ℓ so that $\ell | n$ and ℓ is a prime number. Define

$$C_n = \{\sigma \in \mathrm{Gal}(F \cdot L_n/K)\colon \sigma_{\restriction F} \in C, \text{ and } \sigma_{\restriction L_\ell} \neq id_{L_\ell} \text{ for all } \ell | n\}$$

and

$$a_n = \frac{|C_n|}{[F \cdot L_n\colon K]}.$$

Note that if n divides m, then $a_n \geq a_m \geq 0$. It follows that the sequence (a_n) has a limit as n ranges over all square free integers relatively prime to p, ordered by divisibility. Let $a = \lim a_n$.

Theorem 3.2 (Lenstra, '77)**.** *If K is a function field in one variable over a finite field then the set $\mathcal{M}$ has Dirichlet density a.*

Now, we are ready to prove the analogue of Lemma 2.4.

Lemma 3.3. *There exists an irreducible polynomial q not in S, and a polynomial $b \in \mathbb{F}[t]$ of degree less than q, such that $qx + b$ is never a unit of $S^{-1}\mathbb{F}[t]$ as x varies over $S^{-1}\mathbb{F}[t]$.*

Proof. Let $K = F = \mathbb{F}(t)$, $C = \{\mathrm{Id}_K\}, k = 2$ and let W be the multiplicative subgroup of K^* generated by $\mathbb{F}^* \cup S$. Observe that if $\mathfrak{p} \notin \mathcal{M}(K, F, C, W, k)$, then the index of $\psi(W)$ in $\overline{K}_{\mathfrak{p}}^*$ does not divide 2. In particular, $\psi(W) \neq \overline{K}_{\mathfrak{p}}^*$. Since S is non-empty, the identity is not in C_n, hence $a_n < 1$ for each possible $n > 1$, so by Lenstra's theorem, the Dirichlet density of $\mathcal{M}$ is less than 1.

Choose $\mathfrak{q} = (q) \notin \mathcal{M}$ such that $q \in K$ is irreducible and different from all Q_i, and b a polynomial of degree less than the degree of q whose class modulo q lies in $\overline{K}_{\mathfrak{q}}^* \setminus \psi(W)$. The polynomials q and b trivially satisfy the desired condition. □

In order to conclude this section, observe that Bézout's identity holds in any Euclidean domain, and that our concept of norm (see Definition 2.2) extends naturally to our situation (we will use it also in the next section). So the proof of the following lemma works exactly like the proof of Lemma 2.5, using Lemma 3.3 instead of Lemma 2.4, and Kornblum's theorem instead of Dirichlet's theorem on primes in arithmetic progression.

Lemma 3.4. *The relation $\neq$ is positive-existentially definable in the structure $\mathcal{F}_S$.*

3.2 Definability of multiplication

Given $R \in \mathbb{F}(t)^*$, define $\mathrm{Cp}(R)$ to be the unique $a \in \mathbb{F}$ such that

$$R = \frac{aP_0}{P_1},$$

and P_0 and P_1 are monic polynomials in $\mathbb{F}[t]$. By $\operatorname{ord}_\infty R$ we mean the difference of degrees $\deg P_1 - \deg P_0$. In order to have simpler statements along this Chapter, we may write $\operatorname{ord}_{Q_\infty}$ instead of $\operatorname{ord}_\infty$. It is easy to see that

$$\operatorname{Cp}(P_0 \cdot P_1) = \operatorname{Cp}(P_0) \cdot \operatorname{Cp}(P_1),$$

and if $\operatorname{ord}_\infty P_0 \neq \operatorname{ord}_\infty P_1$, then

$$\operatorname{Cp}(P_0 + P_1) \in \{\operatorname{Cp}(P_0), \operatorname{Cp}(P_1)\}.$$

The next lemma is the analogue of Lemma 2.7 for the structure $\mathcal{F}_S$. The proof goes along the same lines, but we need some extra care for the leading coefficient of the polynomials.

Lemma 3.5. *Let x, y, z and v be arbitrary elements of $S^{-1}\mathbb{F}[t]$. Assume that for all $i \in \{\infty, 1, \ldots, M\}$ we have $\operatorname{ord}_{Q_i} x \neq \operatorname{ord}_{Q_i} y$ and $\operatorname{ord}_{Q_i} z \neq \operatorname{ord}_{Q_i} v$. If the formula $\operatorname{as}(x \pm y, z \pm v)$ holds in $\mathcal{F}_S$, then either we have $xv = yz$ or $xz = yv$.*

Proof. Let u_1, u_2 be units such that

$$x + y = u_1(z + v) \qquad \text{and} \qquad x - y = u_2(z - v) \tag{3.1}$$

Proceeding as in the proof of Lemma 2.7, we get $u_1 = au_2$ for some $a \in \mathbb{F}^*$. In order to be able to finish the proof as in Lemma 2.7, it is sufficient to show that we have $a = \pm 1$.

Since $\operatorname{ord}_\infty x \neq \operatorname{ord}_\infty y$ and $\operatorname{ord}_\infty z \neq \operatorname{ord}_\infty v$ we have

$$\operatorname{Cp}(x + y) = \pm \operatorname{Cp}(x - y) \quad \text{and} \quad \operatorname{Cp}(z + v) = \pm \operatorname{Cp}(z - v).$$

On the other hand, since we have

$$\operatorname{Cp}(u_1) = \frac{\operatorname{Cp}(x + y)}{\operatorname{Cp}(z + v)} \quad \text{and} \quad \operatorname{Cp}(u_2) = \frac{\operatorname{Cp}(x - y)}{\operatorname{Cp}(z - v)},$$

we get $a = \pm 1$. □

Lemma 3.6. *Let x and y be units in $S^{-1}\mathbb{F}[t]$ such that $x \neq \pm 1$ and $y \neq 1$. Assume that for all $i \in \{\infty, 1, \ldots, M\}$ we have $\operatorname{ord}_{Q_i} x \neq \operatorname{ord}_{Q_i} y$. We have:*

$$y = x^2 \text{ if and only if } \mathcal{F} \text{ satisfies } \operatorname{as}(x \pm 1, y \pm x).$$

Proof. It follows from Lemma 3.5, the same way that Lemma 2.8 follows from Lemma 2.7. □

From Lemma 3.6, we can show that the squaring function between units is positive-existentially definable.

Proposition 3.7. *The set*

$$\mathrm{SQ_u} = \{(x, y) \colon x, y \text{ are units in } S^{-1}\mathbb{F}[X] \text{ and } y = x^2\}$$

is positive-existentially definable in the structure $\mathcal{F}_S$.

Proof. The proof follows the proof of Proposition 2.9, except that we need more elements in I on order to deal with the order at infinity. So, write $I = \{0, 1, 2, 3, 4\}^M$ and consider the formula

$$\mathrm{Sq_u}(x, y) \colon x \mid 1 \wedge y \mid 1 \wedge \bigwedge_{\gamma \in I} \mathrm{as}(Q^\gamma x \pm 1, Q^{2\gamma} y \pm Q^\gamma x)$$

where γ reads as $(\gamma_1, \ldots, \gamma_M)$ (see Notation 2.1).

Assume that $\mathrm{Sq_u}(x, y)$ holds. In particular, as in the proof of Proposition 2.9, for each γ_i in

$$\gamma_i \in \{0, 1, 2, 3, 4\} \setminus \left\{ -\operatorname{ord}_{Q_i} x, -\frac{1}{2}\operatorname{ord}_{Q_i} y, \operatorname{ord}_{Q_i} x - \operatorname{ord}_{Q_i} y \right\},$$

$Q^\gamma x$ and $Q^{2\gamma} y$ satisfy the hypothesis of Lemma 3.6 except maybe for the order at infinity. So we have to make sure that

$$\operatorname{ord}_\infty Q^{2\gamma} y - \operatorname{ord}_\infty Q^\gamma x \neq 0,$$

hence that

$$\operatorname{ord}_\infty y - \operatorname{ord}_\infty x + \sum_{i=1}^{M} \operatorname{ord}_\infty Q_i^{\gamma_i} \neq 0,$$

which clearly can be done since we still have two degrees of liberty for choosing γ_1 (say). □

The analogues of Lemma 2.11 and Proposition 2.12 are proved in exactly the same way, so we can now multiply a unit by an arbitrary element in a positive

existential way, and therefore we can write in our formulas polynomial expressions with coefficients in $\mathbb{F}[t]$ whenever the variable is a unit.

Also, the analogue of Lemma 2.14 for $\mathbb{F}[t]$ is proven in an analogous way, using the well-known version of Euler's Theorem for polynomial rings over finite fields. We state it for further reference.

Lemma 3.8. *Given $x_1, \ldots, x_n \in S^{-1}[\mathbb{F}] \setminus \{0\}$, there exists a unit $u \neq 1$ so that each of x_1, …, and x_n divides $u - 1$.*

At this step of the proof, the analogy between $\mathbb{Z}$ and $\mathbb{F}[t]$ breaks down and the proof goes in a different direction.

Write $I = \{0,1\}^M$. Consider the formula $\varphi(x, y)$

$$\exists u_1 \exists u (u_1 \mid 1 \wedge u_1 \neq 1 \wedge u \neq 1 \wedge x+1 \mid u_1 - 1 \wedge y+1 \mid u_1 - 1 \wedge (u_1-1)^{16} \mid u - 1 \wedge \varphi_0(x,y))$$

where $\varphi_0(x, y)$ is defined as:

$$\bigwedge_{\gamma \in I} x \pm Q^{\gamma} u \mid y - Q^{2\gamma} u^2.$$

Lemma 3.9. *Let $x, y \in S^{-1}\mathbb{F}[t]$. Assume that for all $i \in \{\infty, 1, \ldots, M\}$ we have $\operatorname{ord}_{Q_i} x \neq 0$, $\operatorname{ord}_{Q_i} y \neq 0$. If $\varphi(x, y)$ holds in $\mathcal{F}_S$, then $y = x^2$.*

Proof. Write

$$x = f \prod_{i=1}^{M} Q_i^{\alpha_i}, \quad y = g \prod_{i=1}^{M} Q_i^{\beta_i} \quad \text{and} \quad u = \kappa \prod_{i=1}^{M} Q_i^{\delta_i}$$

where f (and g) is a polynomial relatively prime with each Q_i, and $\kappa \in \mathbb{F}^*$. From $\operatorname{ord}_{Q_i} x \neq 0$ and $\operatorname{ord}_{Q_i} y \neq 0$ we have

$$N(x+1) = f \prod_{\alpha_i > 0} Q_i^{\alpha_i} + \prod_{\alpha_i < 0} Q_i^{-\alpha_i}$$

and

$$N(y+1) = g \prod_{\beta_i > 0} Q_i^{\beta_i} + \prod_{\beta_i < 0} Q_i^{-\beta_i}.$$

Since $x + 1$ divides $u_1 - 1$, also $N(x + 1)$ divides $N(u_1 - 1)$ in $\mathbb{F}[t]$, hence in particular, since u_1 is not 1, we have

$$\deg(N(x+1)) \leq \deg(N(u_1 - 1)).$$

On the other hand, since x has non-zero order at infinity, the degree of $N(x+1)$ is equal to either

$$\deg(f) + \sum_{\alpha_i > 0} \alpha_i$$

or

$$\sum_{\alpha_i < 0} (-\alpha_i),$$

so that we have

$$\deg(f) + \sum_{i=1}^{M} |\alpha_i| \leq 2\deg(N(u_1 - 1)) \tag{3.2}$$

Analogously, we have

$$\deg(g) + \sum_{i=1}^{M} |\beta_i| \leq 2\deg(N(u_1 - 1)) \tag{3.3}$$

From Equations (3.2) and (3.3) and because u is not 1 by hypothesis, we have

$$\begin{aligned} 2\left(2\deg(f) + 2\sum_{i=1}^{M} |\alpha_i| + \deg(g) + \sum_{i=1}^{M} |\beta_i|\right) &\leq 12\deg(N(u_1 - 1)) \\ &< 16\deg(N(u_1 - 1)) \\ &< \deg(N(u - 1)), \end{aligned}$$

hence

$$\begin{aligned} 2\deg(f) + 2\sum_{i=1}^{M} |\alpha_i| + \deg(g) + \sum_{i=1}^{M} |\beta_i| \\ < \deg(N(u-1)) - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right). \end{aligned} \tag{3.4}$$

On other hand, we have

$$y - x^2 = P\left(g \prod_{\beta_i - 2\alpha_i \geq 0} Q_i^{\beta_i - 2\alpha_i} - f^2 \prod_{\beta_i - 2\alpha_i < 0} Q_i^{2\alpha_i - \beta_i}\right)$$

where P is a product of powers of the polynomials Q_i, hence

$$\begin{aligned} \deg(N(y - x^2)) &\leq \deg\left(g \prod_{\beta_i - 2\alpha_i \geq 0} Q_i^{\beta_i - 2\alpha_i} - f^2 \prod_{\beta_i - 2\alpha_i < 0} Q_i^{2\alpha_i - \beta_i}\right) \\ &\leq 2\deg(f) + 2\sum_{i=1}^{M} |\alpha_i| + \deg(g) + \sum_{i=1}^{M} |\beta_i|, \end{aligned}$$

so from the relation (3.4), we get

$$\deg(N(y-x^2)) < \deg(N(u-1)) - \left(\sum_{i=1}^{M}|\alpha_i| + \sum_{\alpha_i>\delta_i}(\alpha_i-\delta_i)\right). \tag{3.5}$$

For the sake of contradiction, assume that y is not equal to x^2. Since we assume that $\varphi(x,y)$ holds, in particular by choosing $\gamma_i \in \{0,1\} \setminus \{\alpha_i - \delta_i\}$ for each i, we have

$$x \pm \prod Q_i^{\gamma_i} u \mid y - \prod Q_i^{2\gamma_i} u^2.$$

Since also

$$x \pm \prod Q_i^{\gamma_i} u \mid x^2 - \prod Q_i^{2\gamma_i} u^2,$$

by taking the difference, we obtain

$$x \pm \prod Q_i^{\gamma_i} u \mid y - x^2,$$

therefore

$$\deg\left(N(x \pm \prod Q_i^{\gamma_i} u)\right) \leq \deg(N(y-x^2)). \tag{3.6}$$

We claim that either

$$\deg(N(u-1)) - \sum_{i=1}^{M}|\alpha_i| \leq \deg(N(x + \prod Q_i^{\gamma_i} u)),$$

or

$$\deg(N(u-1)) - \sum_{i=1}^{M}|\alpha_i| \leq \deg(N(x - \prod Q_i^{\gamma_i} u)),$$

hence by (3.5), either

$$\deg(N(y-x^2)) < \deg(N(x + \prod Q_i^{\gamma_i} u))$$

or

$$\deg(N(y-x^2)) < \deg(N(x - \prod Q_i^{\gamma_i} u))$$

which contradicts (3.6).

In order to prove the claim, note that

$$\deg(N(u-1)) \leq \sum_{i=1}^{M}|\delta_i|,$$

hence

$$\deg(N(u-1)) - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right)$$

is less than or equal to

$$\sum_{i=1}^{M} |\delta_i| - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right).$$

On other hand, for some choice of the sign (and from our choice of the γ_i) we have that $\deg(N(x \pm \prod Q_i^{\gamma_i} u))$ is equal to the maximum value between

$$\deg(f) + \sum_{\alpha_i \geq \gamma_i + \delta_i} (\alpha_i - (\gamma_i + \delta_i))$$

and

$$\sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i)$$

(indeed, only choice of sign may produce cancelation in $x \pm \prod Q_i^{\gamma_i} u$). Hence it suffices to show that

$$\sum_{i=1}^{M} |\delta_i| - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right) \leq \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i).$$

We have

$$\begin{aligned}
&\sum_{i=1}^{M} |\delta_i| - \left(\sum_{i=1}^{M} |\alpha_i| + \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i)\right) - \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i) \\
&\leq \sum |\delta_i - \alpha_i| - \sum_{\alpha_i > \delta_i} (\alpha_i - \delta_i) - \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i) \\
&= \sum_{\alpha_i < \delta_i} (\delta_i - \alpha_i) - \sum_{\alpha_i < \gamma_i + \delta_i} (\gamma_i + \delta_i - \alpha_i) \\
&\leq \sum_{\alpha_i < \delta_i} (\delta_i - \alpha_i) - \sum_{\alpha_i < \delta_i} (\gamma_i + \delta_i - \alpha_i) \leq 0.
\end{aligned}$$

□

Write $J = \{0, 1, 2\}^M$ and consider the following formula $\psi(x, y)$:

$$\bigwedge_{\delta \in J} \varphi\left(Q^{\delta} x, Q^{2\delta} y\right).$$

Proposition 3.10. *If $\psi(x, y)$ holds in $\mathcal{F}_S$, then $y = x^2$.*

Proof. This is an immediate consequence of Lemma 3.9, noting that there exists a choice of δ for which we have $\operatorname{ord}_{Q_i} Q^{\delta} x \neq 0$ and $\operatorname{ord}_{Q_i} Q^{2\delta} y \neq 0$ for each i (from the definition of J). □

We can now conclude.

Lemma 3.11. *The set*

$$\mathrm{SQ} = \{(x, y) \colon x, y \text{ are in } S^{-1}\mathbb{F}[t] \text{ and } y = x^2\}$$

is existentially definable in the structure $\mathcal{F}_S$.

Proof. We claim that the formula

$$\mathrm{Sq}(x, y) : (x = 0 \wedge y = 0) \vee \bigvee_{\delta \in J} (x = \pm Q^{-\delta} \wedge y = Q^{-2\delta}) \vee \psi(x, y),$$

defines the set SQ. Indeed, if the formula holds, then it is immediate from Proposition 3.10 that $y = x^2$.

Assume $(x, y) \in \mathrm{SQ}$. Without loss of generality, we can assume $x \neq 0$ and, $x \neq Q^{-\delta}$ and $x \neq -Q^{-\delta}$ for all $\delta \in J$. For each $\delta \in J$, since $|x| \neq Q^{-\delta}$, we have $Q^{\delta}|x| - 1 \neq 0$, hence also $Q^{2\delta}|y| + 1 \neq 0$.

From Lemma 3.8, there is a unit u_1 distinct from 1 such that $Q^{\delta} x \pm 1$ divides $u_1 - 1$ and $Q^{2\delta} y \pm 1$ divides $u_1 - 1$. Because $u_1 - 1$ is not zero we deduce, from Lemma 3.8 again, that there is a unit u different from 1 such that $(u_1 - 1)^{16} \mid u - 1$. In addition, we have $\bigwedge_{(\delta,\gamma) \in J \times I} Q^{\delta} x \pm Q^{\gamma} u \mid Q^{2\delta} y - Q^{2\gamma} u^2$. Thus, the formula $\psi(x, y)$ is satisfied. □

Bibliography

[B80] Bel'tyukov, A. *Decidability of the universal theory of natural numbers with addition and divisibility.* Journal of Soviet Mathematics 14 (1980), no. 5, 1436–1444.

[CL00] Cori, René; Lascar, Daniel. *Mathematical Logic: A Course with Exercises.* Oxford University Press (2000).

[Da73] Davis, Martin. *Hilbert's Tenth Problem is Unsolvable.* The American Mathematical Monthly 80 (1973), no. 3, 233–269.

[De75] Denef, Jan. *Hilbert's Tenth Problem for Quadratic Rings.* Proceedings of the American Mathematical Society 48 (1975), no. 1, 214–220.

[De78] Denef, Jan. *The Diophantine problem for polynomial rings and fields of rational functions.* Transactions of the American Mathematical Society 242 (1978), 391–399.

[De79] Denef, Jan. *The diophantine problem for polynomial rings of positive characteristic.* In Logic Colloquium 78 (1979), 131–154. Boffa, M., van Dalen, D., McAloon, K. (eds.). North-Holland Publishing Company.

[De80] Denef, Jan. *Diophantine sets over algebraic integers rings II.* Transactions of the American Mathematical Society 257(1) (1980), 227–236.

[DeLi78] Denef, Jan; Lipshitz, Leonard. *Diophantine sets over some rings of algebraic integers.* Journal London Mathematical Society 18(3) (1978), 385–391.

[Ei03] Eisenträger, Kirsten. *Hilbert's tenth problem for algebraic function fields of characteristic* 2. Pacific Journal of Mathematics 203 (2003), no. 2, 261–281.

[En01] Enderton, Herbert. *A Mathematical Introduction to Logic.* Academic Press. Second Edition (2001).

[Ga13] Garcia-Fritz, Natalia. *Representation of powers by polynomials and the language of powers.* J. Lond. Math. Soc. (2) 87 (2013), no. 2, 347–364.

[GaPas15] Garcia-Fritz, Natalia; Pasten, Hector. *Uniform positive existential interpretation of the integers in rings of entire functions of positive characteristic.* J. Number Theory 156 (2015), 368–393.

[He04] Hedman, Shawn. *A First Course in Logic: An Introduction to Model Theory, Proof Theory, Computability, and Complexity.* Oxford University Press (2004).

[Ho93] Hodges, Wilfrid. *Model Theory.* 1st ed. Cambridge: Cambridge University Press (1993).

[KR92a] Kim, K.; Roush, F. *Diophantine undecidability of $C(t_1, t_2)$.* Journal of Algebra 150(1) (1992), 35–44.

[KR92b] Kim, K.; Roush, F. *Diophantine undecidability for functions fields over certain infinitie fields of characteristic p.* Journal of Algebra 152(1) (1992), 230–239.

[Ko14] Koenigsmann, Jochen. *Undecidability in number theory.* Model theory in algebra, analysis and arithmetic, 159–195, Lecture Notes in Math., 2111, Fond. CIME/CIME Found. Subser., Springer, Heidelberg, 2014.

[KorLan19] Kornblum, Heinrich; Landau, E.; *Über die Primfunktionen in einer arithmetischen Progression.* (German) Math. Z. 5 (1919), no. 1-2, 100–111.

[Le77] Lenstra, H. W., Jr. *On Artin's conjecture and Euclid's algorithm in global fields.* Invent. Math. 42 (1977), 201–224.

[Li77] Lipshitz, Leonard. *Undecidable existential problem for addition and divisibility in algebraic number rings II.* Proceedings of the American Mathematical Society 64 (1977), no. 1, 122–128.

[Li78a] Lipshitz, Leonard. *The Diophantine Problem for Addition and Divisibility.* Transactions of the American Mathematical Society 235 (1978), 271–283.

[Li78b] Lipshitz, Leonard. *Undecidable existential problem for addition and divisibility in algebraic number rings.* Transactions of the American Mathematical Society 241 (1978), 121–128.

[LiPh95] Lipshitz, Leonard; Pheidas, Thanases. *An analogue of Hilbert's tenth problem for p-adic entire functions.* J. Symbolic Logic 60 (1995), no. 4, 1301–1309.

[Mar02] Marker, David. *Model Theory: An Introduction.* Graduate Text in Mathematics Volume 127 (2002).

[Mat70] Matijasevic, Juri. *The Diophantineness of enumerable sets.* (Russian) Dokl. Akad. Nauk SSSR 191 (1970), 279–282.

[Pap97] Pappalardi, Francesco. *On the r-rank Artin conjecture.* Mathematics of Computation 66 (1997), no. 218, 853–868.

[Pas17] Pasten, Hector. *Definability of Frobenius orbits and a result on rational distance sets.* Monatsh. Math. 182 (2017), no. 1, 99–126.

[PasPhVida10] Pasten, Hector; Pheidas, Thanases; Vidaux, Xavier. *A survey on Büchi's problem: new presentations and open problems.* Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) 377 (2010), Issledovaniya po Teorii Chisel. 10, 111–140, 243; translation in J. Math. Sci. (N.Y.) 171 (2010), no. 6, 765–781.

[PasPhVida14] Pasten, Hector; Pheidas, Thanases; Vidaux, Xavier. *Uniform existential interpretation of arithmetic in rings of functions of positive characteristic.* Inventiones Mathematicae 196 (2014), no. 2, 453–484.

[PasVida16] Pasten, Hector; Vidaux, Xavier. *Positive existential definability of multiplication from addition and the range of a polynomial.* Israel J. Math. 216 (2016), no. 1, 273–306.

[Ph85] Pheidas, Thanases. *The diophantine problem for addition and divisibility in polynomial rings*, Thesis, Purdue Univ (1985).

[Ph87a] Pheidas, Thanases *An undecidability result for power series rings of positive characteristic*. Proceedings of the American Mathematical Society 99 (2) (1987), 364–366.

[Ph87b] Pheidas, Thanases. *An undecidability result for power series rings of positive characteristic, II*. Proceedings of the American Mathematical Society 100 (3) (1987), 526–530.

[Ph88] Pheidas, Thanases. *Hilbert's tenth problem for a class of rings of algebraic integers.* Proc. Amer. Math. Soc. 104 (1988), no. 2, 611–620.

[Ph91] Pheidas, Thanases. *Hilbert's tenth problem for fields of rational functions over finite fields*. Inventions Mathematicae 103 (1991), 1–8.

[Ph94] Pheidas, Thanases. *Extensions of Hilbert's tenth problem.* J. Symbolic Logic 59 (1994), no. 2, 372–397.

[Ph04] Pheidas, Thanases. *Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic.* J. Algebra 273 (2004), no. 1, 395–411.

[PhZ00] Pheidas, Thanases; Zahidi, Karim. *Undecidability of existential theories of rings and fields: a survey. Hilbert's tenth problem: relations with arithmetic and algebraic geometry* (Ghent, 1999), 49–105, Contemp. Math., 270, Amer. Math. Soc., Providence, RI, 2000.

[PhZ08] Pheidas, Thanases; Zahidi, Karim. *Decision problems in algebra and analogues of Hilbert's tenth problem.* Model theory with applications to algebra and analysis. Vol. 2, 207–235, London Math. Soc. Lecture Note Ser., 350, Cambridge Univ. Press, Cambridge, 2008.

[Po03] Poonen, Bjorn. *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$. Journal of the American Mathematical Society 16 (2003), no. 4, 981–990.

[Ra93] Rabin, Michael. *Decidable Theories.* In Studies in Logic and The Foundations of Mathematics volume 90 (1993), 596–627. Keiser, H., Mostowki, A., Robinson, A., Suppes, P., Troelstra, A. (eds.). ELSEVIER SCIENCE PUBLISHERS B. V.

[Ri16] Riquelme, José Luis. *The Erdös-Woods conjecture for entire functions*, preprint.

[Ro49] Robinson, Julia. *Definability and Decision Problems in Arithmetic.* The Journal of Symbolic Logic 14 (1949), 98–114.

[Sh89] Shlapentokh, Alexandra. *Extension of Hilbert's tenth problem to some algebraic number fields.* Comm. Pure Appl. Math. 42 (1989), no. 7, 939–962.

[Sh92] Shlapentokh, Alexandra. *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic.* Transactions of the American Mathematical Society 333 (1992), no. 1, 275–298.

[Sh94] Shlapentokh, Alexandra. *Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of* $\mathbb{Q}$. Annals of Pure and Applied Logic 68 (1994), no. 3, 299–325.

[Sh96] Shlapentokh, Alexandra. *Diophantine undecidability over algebraic function fields over finite fields of constants.* Journal of Number Theory 58(2) (1996), 317–342.

[Sh00] Shlapentokh, Alexandra. *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic.* Pacific Journal of Mathematic 193(2) (2000), 463–500.

[Sh07] Shlapentokh, Alexandra. *Hilbert's tenth problem. Diophantine classes and extensions to global fields.* New Mathematical Monographs, 7. Cambridge University Press, Cambridge, 2007. xiv+320 pp.

[Sh11] A. Shlapentokh, *Defining integers.* Bulletin of Symbolic Logic 17 (2011), no. 2, 230–251.

[Sh12] Shlapentokh, Alexandra. *Elliptic curve points and Diophantine models of $\mathbb{Z}$ in large subrings of number fields.* International Journal of Number Theory 8 (2012), no. 6, 1335–1365.

[Si09] Sirokofskich, Alla. *Decidability of sub-theories of polynomials over a finite field.* Mathematical theory and computational practice (2009), 437–446, Lecture Notes in Comput. Sci., 5635, Springer, Berlin.

[St84] Stansifer, Ryan. *Presburger's Article on Integer Airthmetic: Remarks and Translation.* Cornell University, Computer Science Department, number: TR84-639 (1984).

[U11] Utreras, Javier. *A logical approach to the problem of representation of integers by systems of diagonal forms.* Bull. Lond. Math. Soc. 43 (2011), no. 2, 299–310.

[U16] Utreras, Javier. *Interpreting arithmetic in the first-order theory of addition and coprimality of rings of polynomials.* Preprint.

[Vida03] Vidaux, Xavier. *An analogue of Hilbert's 10th problem for fields of meromorphic functions over non-Archimedean valued fields.* J. Number Theory 101 (2003), no. 1, 48–73.

[Vide89] Videla, Carlos. *On Hilbert's Tenth Problem.* (in Spanish), Atas da a Escola de Algebra, Vitoria, E.S., Brasil, in Atas 16, Sociedade Brasileira de Matematica (1989), 95–108.

[Vide94] Videla, Carlos. *Hilbert's tenth problem for rational function fields in characteristic 2.* Proceedings of the American Mathematical Society 120(1) (1994), 249–253.

[Wo81] Woods, Alan R. *Some problems in logic and number theory, and their connections.* Ph.D. Thesis, University of Manchester, 1981.

[Wo93] Woods, Alan R. *Decidability and Undecidability of Theories with a Predicate for the Primes.* J. Symbolic Logic 58 (1993), 672–687.

[Z03] Zahidi, Karim. *Hilbert's tenth problem for rings of rational functions.* Notre Dame J. Formal Logic 43 (2002), no. 3, 181–192 (2003).