Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas - Programa Magíster en Matemática

# Problema Diofantino para adición y divisibilidad en extensiones cuadráticas imaginarias

Tesis presentada para optar al grado académico de
Magíster en Matemática

NATALIA HORMAZÁBAL MERINO
FEBRERO 2025
CONCEPCIÓN - CHILE

Profesor Guía: Carlos Martínez Ranero
Departamento de Matemática
Universidad de Concepción, Chile

*Dedicado a mi familia, y*
*a todos aquellos que me apoyaron*

# Contents

**Introducción** **1**

**Introduction** **4**

**1 Preliminaries** **7**

**2 Undecibility of $\mathcal{Z}_S$** **11**
2.1 Definitions and notations . . . . . 11
2.2 Square of units . . . . . 12
2.3 Defining the square function . . . . . 15

**Bibliography** **23**

# Introducción

En la lista de 23 problemas propuestos por el matemático alemán David Hilbert en 1900, el décimo pide lo siguiente:

> Encontrar un algoritmo que determine si una ecuación diofantina (ecuación polinomial con finitas variables y coeficientes enteros) dada tiene solución en los enteros.

Este problema fue resuelto recién en el año 1970 por Yuri Matiyasevich [7], quien demostró que tal algoritmo no existe, utilizando en la demostración resultados anteriores de Martin Davis, Hilary Putnam, y Julia Robinson [3]. En el lenguaje moderno de lógica, la pregunta se traduce a si la teoría positiva existencial de la estructura $(\mathbb{Z}; =, 0, 1, +, \cdot)$ es indecidible.

Naturalmente, a partir de este problema, uno se puede hacer la misma pregunta de manera general para ecuaciones polinomiales con coeficientes en $\mathbb{Z}$, pero con soluciones en un anillo conmutativo $R$. A este problema lo llamaremos el décimo problema de Hilbert para $R$. La mayor parte de la investigación en esta área se ha centrado en el campo de números racionales $\mathbb{Q}$, pero también se ha enfocado en el caso de anillos de números enteros de campos de números algebraicos, o de campos de números en general.

Con respecto al caso de los números racionales, desafortunadamente aún no se conoce una respuesta al décimo problema de Hilbert. Por otro lado, en en el caso de campos de números se han hecho avances

significativos. Entre estos, destacamos que la teoría positivo existencial de la estructura $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, \cdot)$, con $S$ un conjunto finito de números primos no vacío, es indecidible, lo que fue demostrado gracias al trabajo de Julia Robinson [11] y el resultado de Matiyasevich. En 2003, Bjorn Poonen [9] demostró que existe un conjunto recursivo de primos $T$ de densidad 1 tal que el anillo $(\mathbb{Z}[T^{-1}]; =, 0, 1, +, \cdot)$ es indecidible. Por otro lado, Harold N. Shapiro y Alexandra Shlapentokh [12], demostraron que el problema no tiene solución en anillos de enteros de cualquier campos de números algebraicos cuyo grupo de Galois sobre los racionales sea abeliano. También se mostró, por Shlapentokh [13] y, de manera independiente, por Thanases Pheidas [8] y C. Videla que el problema no tiene solución sobre anillos de enteros de campos de números algebraicos que admitan exactamente un par de encajes conjugados complejos. Más recientemente, Natalia García-Fritz y Héctor Pastén [4] mostraron que existen conjuntos de primos $\mathcal{P}$ y $\mathcal{Q}$ tales que para $K = \mathbb{Q}(\sqrt[3]{p}, \sqrt{q})$ con $p \in \mathcal{P}$ y $q \in \mathcal{Q}$, el décimo problema de Hilbert para $\mathcal{O}_K$ no tiene solución.

Una vez sabiendo que el décimo problema de Hilbert en $R$ es indecidible, podemos considerar sistemas de ecuaciones especiales (es decir, trabajar con otras estructuras) y ver si todavía tenemos indecibilidad. En el caso de la división, en la década de los 70's Lipshitz [5] y, en paralelo, Bel'tyukov [1], mostraron que la teoría positivo existencial de la estructura $(R; =, 0, 1, +, |)$, con $R$ anillo de enteros de una extensión cuadrática imaginaria de $\mathbb{Q}$, es decidible. Posteriormente, Lipshitz [6] probó que si $K$ no es una extensión cuadratica imaginaria, entonces la multiplicación es positivo-existencialmente definible en $(O_K; =, 0, 1, +, |)$, lo que quiere decir que el problema con la división se transforma en el décimo problema original con la multiplicación.

Sabiendo que la teoría de $(\mathbb{Z}; =, 0, 1, +, |)$ es decidible, surge la duda de si la teoría de $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$, con $S$ conjunto finito de primos no vacío, también los es. En este caso, Leonidas Cerda y Carlos Martínez-Ranero [2] mostraron que no, por lo que el hecho de tan solo

invertir un primo cambia la decidibilidad de la estructura, principalmente debido al cambio del rango a nuestro grupo de unidades.

Tomando en cuenta este último resultado y el hecho de que, por lo demostrado por Lipshitz y Bel'tyukov, el problema de la división en anillos de enteros de extensiones cuadráticas imaginarias de $\mathbb{Q}$ es indecidible, surge naturalmente la duda sobre la decibilidad de la teoría positivo existencial de $(O_{K,S}; =, 0, 1, +, |)$, con $K$ una extensión cuadrática imaginaria de $\mathbb{Q}$, $S$, un conjunto finito, no vacío de ideales primos de $K$ y donde $O_{K,S} = \{x \in K : \forall \mathfrak{p} \notin S \; v_{\mathfrak{p}}(x) \geq 0\}$. Vale notar que el conjunto $S$ se conforma de ideales debido a que típicamente no contamos con factorización única en $K$. En esta tesis demostraremos que esta teoría es decidible, siguiendo la idea de la demostración en $\mathbb{Z}[S^{-1}]$. Denominaremos, por simplicidad, $\mathcal{Z}_S$ a la estructura con la que vamos a trabajar, y en nuestro caso agregaremos la relacion "ser distinto de 0" ($\neq 0$) al lenguaje, al que llamaremos $\mathcal{L}_{div}$, debido a que en $\mathbb{Z}[S^{-1}]$ necesitarímos herramientas de teoría analítica de número que no tenemos disponible para la demostración. Dicho esto, lo que queremos mostrar es lo siguiente:

**Theorem 1.** *La multiplicación es positivo existencialmente definible en la estructura $\mathcal{Z}$. Por ende, la estructura $\mathcal{Z}$ es indecidible.*

# Introduction

On the list of 23 problems proposed by the German mathematician David Hilbert in 1900, the tenth asks for the following:

> Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined in a finite number of operations whether the equation is solvable in rational integers.

This problem was finally solved in the year 1970 by Yuri Matiyasevich [7], who proved that such an algorithm does not exist, his proof is based on previous results by Martin Davis, Hilary Putnam, and Julia Robinson [3]. In the language of mathematical logic, one would ask if the positive existential theory of the structure $(\mathbb{Z}; =, 0, 1, +, \cdot)$ is undecidable.

Naturally, from this problem, one could more generally ask the same question for polynomial equations with coefficients in $\mathbb{Z}$, but solutions in a commutative ring $R$. We call this problem the tenth Hilbert's problem for $R$. A large part of the investigation in this area has been focused on the field of rational numbers $\mathbb{Q}$, but also in the cases of rings of integers of algebraic numbers fields, or number fields in general.

Regarding the case of rational numbers, unfortunately there is still not a solution for Hilbert's tenth problem. On the other hand, in the case of number fields there are a lot of significant advancements. Among these, we highlight that the positive existential theory of the structure $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, \cdot)$, with $S$ a non-empty finite set of prime numbers,

is undecidable. This was proved thanks to the work of Julia Robinson [11] and the result of Matiyasevich. In 2003, Bjorn Poonen [9] proved that there is a recursive set of primes $T$ of density 1 such that the ring $(\mathbb{Z}[T^{-1}]; =, 0, 1, +, \cdot)$ is undecidable. On the other side, Harold N. Shapiro and Alexandra Shlapentok [12] proved that the problem does not have a solution for ring of integers of any algebraic number field whose Galois group over the rationals is abelian. It was also shown, by Shlapenthok [13] and, independently, by Thanases Pheidas [8] and Carlos Videla that the problem does not have a solution over rings of integers of algebraic number fields that admit exactly one pair complex conjugate embedding. More recently, Natalia García-Fritz and Héctor Pastén [4] showed that there exist sets of primes $\mathcal{P}$ and $\mathcal{Q}$ such that for $K = \mathbb{Q}(\sqrt[3]{p}, \sqrt{q})$ with $p \in \mathcal{P}$ and $q \in \mathcal{Q}$, Hilbert's tenth problem for $\mathcal{O}_K$ does not have a solution.

Once we know that Hilbert's tenth problem for $R$ is undecidable, we can consider special equation systems (that is, work with different structures) and see if we still have undecidability. In the case of division, in the 70's Lipshitz [5] and, in parallel, Bel'tyukov [1] proved that the positive existential theory of the structure $(R; =, 0, 1, +, |)$, with $R$ ring of integers of a quadratic imaginary extension of $\mathbb{Q}$, is decidable. Later, also Lipshitz [6] proved that if $K$ is not a quadratic imaginary extension, then multiplication is positive existentially definable in $(O_K; =, 0, 1, +, |)$, which means that the problem for division is equivalent to the original problem with multiplication.

Once we know that the existential theory of $(\mathbb{Z}; =, 0, 1, +, |)$ is decidable, a question that arises is if the theory of $(\mathbb{Z}[S^{-1}]; =, 0, 1, +, |)$, with $S$ a non-empty finite set of primes, is decidable as well. In this case, Leonidas Cerda and Carlos Martínez-Ranero [2] proved that it is not, which means that only inverting one primer causes the decidability of the structure to change, mainly because it changes the rank of the group of units.

Taking into account this last result and the fact that, as was shown by Lipshitz and Bel'tyukov, the division problem in rings of integers of quadratic imaginary extensions of $\mathbb{Q}$ is undecidable, naturally one could ask about the decidability of the positive existential theory of the structure $(O_{K,S}; =, 0, 1, +, |)$, with $K$ a quadratic imaginary extension of $\mathbb{Q}$, $S$ a non-empty finite set of prime ideals of $K$ and $\mathcal{O}_{K,S} = \{x \in K : \forall \mathfrak{p} \notin S \ v_{\mathfrak{p}}(x) \geq 0\}$. It is worth noting that we work with prime ideals because there is not unique factorization in $K$. In this thesis, we will prove that this theory is decidable, following the idea of the proof in the the case of $\mathbb{Z}[S^{-1}]$. We will call the structure that we are going to work with, for simplicity, $\mathcal{Z}_S$, and in our case we will add the relation "different from 0" ($\neq 0$) to the language, which we will call $\mathcal{L}_{div}$, because for this proof in $\mathbb{Z}[S^{-1}]$ we would need tools from analytical number theory that we do not have available. That said, what we shall prove is the following:

**Theorem 2.** *Multiplication is positive existentially definable in the structure $\mathcal{Z}$. Therefore, the structure $\mathcal{Z}$ is undecidable.*

# Chapter 1

# Preliminaries

This chapter is going to be dedicated to introduce the necessary concepts for the demonstration. In order to do so, we are going to recall some basic Mathematical Logic definitions. For more depth, refer to books like [10] for instance.

A *first order language* $\mathcal{L}$ is a set of symbols consisting of the union of the following:

- a set $\mathcal{C}$ of constant symbols;
- a set of function symbols $\mathcal{F}$, and positive integers $n_f$ for every $f \in \mathcal{F}$, and;
- a set of relation symbols $\mathcal{R}$, and positive integers $n_R$ for evert $R \in \mathcal{R}$.

The integers $n_f$ and $n_R$ indicate that $f$ is a function on $n_f$ variables and $R$ is a $n_R-$ary relation, respectively.

Languages are what give shape to our structure, so given a language $\mathcal{L}$, a $\mathcal{L}-$*structure* is going to be a non-empty set $M$ with:

- an element $c^M$ of $M$ for every constant symbol $c$ of $\mathcal{C}$;
- a $n_f - ary$ function for every $n_f - ary$ function symbol $f$ of $\mathcal{F}$, and;

- a $n_R - ary$ relation for every $n_R - ary$ relation symbol $R$ of $\mathcal{R}$.

For instance, the structure we are working with is

$$\mathcal{Z}_S = (O_{K,S}; =, \neq, 0, 1, +, |)$$

and its language is

$$\mathcal{L}_{div} = (=, \neq, 0, 1, +, |).$$

We want to use the language to create formulas. A $\mathcal{L}-formula$ will be a string of symbols consisting of:

- the symbols of $\mathcal{L}$,
- the equality symbol $=$,
- variable symbols $x_i$, with $i \in \mathbb{N}$,
- Boolean connectives $\wedge, \vee, \neg, \rightarrow$ and $\leftrightarrow$,
- quantifiers $\exists$ and $\forall$, and
- parentheses.

Formulas are going to be made up of terms. We define the set of $\mathcal{L}-terms$ as the smallest set containing the constant symbols of $\mathcal{L}$, variables and operations of the language using the previous variables and constants.

We say that a formula is an *atomic formula* if it is a relation of terms, where the relation is either taken from the language or an equality.

A formula is *positive existential* if the the only connectives are $\wedge$ and $\vee$ and the only quantifiers are $\exists$, which have to appear at the beginning of the formula before any of the connectives.

Lastly, a formula is a *sentence* if every variable is quantified.

Given a language $\mathcal{L}$ and a $\mathcal{L}-$structure $\mathcal{M}$, we say that a $\mathcal{L}-$formula $F$ is *satisfied* in $\mathcal{M}$ if it is true in $\mathcal{M}$. In this case, we write $\mathcal{M} \models F$.

The *theory* of a structure is the set of all the sentences that are true for that structure. It follows, that the *positive existential theory* of a structure is the set of all the positive existential sentences that are true in the structure.

Given a theory of an structure, let's say $T$, we say that $T$ is *decidable* if there is an algorithm (a Turing machine) that determines, in a finite amount of steps, whether an arbitrary sentence is true or false on the structure. If it is not decidable, we say that $T$ is undecidable. Analogously, a theory is positive existentially decidable if there exists an algorithm as before but for an arbitrary positive existential sentence. As mentioned previously, the negative answer to Hilbert's tenth problem means that the positive existential theory of $(\mathbb{Z}; =, 0, 1, +, \cdot)$ is undecidable, while the existential theory of $(\mathbb{Z}; =, 0, 1, +, |)$ is decidable.

We are going to finish the logical background with the concept of definability. Let $\mathcal{M}$ be a $\mathcal{L}-$structure with and underlying set $M$. For any integer $n \geq 1$ and $A \subseteq M^n$, we say that $A$ is *definable* in $\mathcal{M}$ if there exists a formula $\varphi(x_1, ..., x_n)$, with $n$ free variables, such that $(a_1, ..., a_n) \in A$ if and only if $\mathcal{M} \models \varphi(a_1, ..., a_n)$. In this case, we call the formula $\varphi$ a definition of $A$.

Throughout this thesis, we will be working with the aforementioned structure $(O_{K,S}; =, 0, 1, +, |)$, where $\mathcal{O}_{K,S} = \{x \in K : \forall \mathfrak{p} \notin S \ v_{\mathfrak{p}}(x) \geq 0\}$ and $K$ quadratic imaginary extension of $\mathbb{Q}$. What makes this case different to the result by Lipshitz is that in here or group of units is finite.

As we said before, because our structure doesn't count with unique prime factorization, we are going to work with prime ideals. For any prime ideal $\mathfrak{p}$, there is a unique natural prime $p$ such that $(p)|\mathfrak{p}$. This fact

is going to be important for the following results, and we will call $p$ the natural prime *under* $\mathfrak{p}$. On the other hand, given a natural prime $p$, then $(p)$ is either the product of two prime ideals or it is itself a prime ideal.

# Chapter 2

# Undecibility of $\mathcal{Z}_S$

## 2.1 Definitions and notations

Before beginning with the proof of our theorem, we are going to introduce some notations that are going to be used through this chapter.

- $K = \mathbb{Q}[\sqrt{D}]$, with $D \leq -1$ square free, is the field we will be working with.
- $S = \{\mathfrak{p}_1, ..., \mathfrak{p}_s\}$ a finite non-empty set of prime ideals of $K$.
- $\mathcal{O}_{K,S} = \{x \in K : v_{\mathfrak{p}}(x) \geq 0 \text{ for every } \mathfrak{p} \notin S\}$.
- $\mathfrak{as}(x, y)$ stands for the formula $x|y \wedge y|x$. We say that $x$ and $y$ are associate.
- The notation $x \pm y|z \pm t$ stands for

$$x + y|z + t \wedge x - y|z - t$$

- $p_1, ..., p_M$ will denote the rational primes of $\mathbb{Z}$ lying below the primes of $S$.
- If $\gamma = (\gamma_1, ..., \gamma_M)$ is a vector of natural numbers, then $p^\gamma$ stands for

$$\prod_{i=1}^{M} p_i^{\gamma_i}$$

- Let $q_1, ..., q_{N+1}$ pairwise different primes of $\mathbb{Z}$ that are not below any prime of $S$, where $N = \#\mathcal{O}_K^\times$.

## 2.2 Square of units

In this section, we will show that the square function restricted to units is positive existentially definable in $\mathcal{Z}$. We will also define, later on, the multiplication between units and arbitrary elements of $\mathcal{O}_{K,S}$.

**Lemma 2.2.1.** *Let $x, y, z$ and $t$ be elements of $\mathcal{O}_{K,S}$. If for every $1 \leq i \leq s$ we have $v_{\mathfrak{p}_i}(x) \neq v_{\mathfrak{p}_i}(y)$, $v_{\mathfrak{p}_i}(z) \neq v_{\mathfrak{p}_i}(t)$ and $\mathfrak{as}(q_j x + y, q_j z + t)$ holds in $\mathcal{Z}$ for every $1 \leq j \leq N+1$, then $xt = yz$.*

*Proof.* For each $1 \leq j \leq N+1$, let $u_j$ be units in $\mathcal{O}_{K,S}$ such that

$$q_j x + y = u_j(q_j z + t).$$

As we have that $v_{\mathfrak{p}_i}(x) \neq v_{\mathfrak{p}_i}(y)$ for each $i$, then

$$\begin{aligned} v_{\mathfrak{p}_i}((q_j x) + (y)) &= \min\{v_{\mathfrak{p}_i}(q_j x), v_{\mathfrak{p}_i}(y)\} \\ &= \min\{v_{\mathfrak{p}_i}(x), v_{\mathfrak{p}_i}(y)\}, \end{aligned}$$

and analogously, as $v_{\mathfrak{p}_i}(z) \neq v_{\mathfrak{p}_i}(t)$, we have that

$$v_{\mathfrak{p}_i}((q_j z) + (t)) = \min\{v_{\mathfrak{p}_i}(z), v_{\mathfrak{p}_i}(t)\}$$

for every $1 \leq i \leq s$. Therefore, we have for each $i, j$ that

$$\begin{aligned} v_{\mathfrak{p}_i}(u_j) &= v_{\mathfrak{p}_i}(q_j z + t) - v_{\mathfrak{p}_i}(q_j x + y) \\ &= \min\{v_{\mathfrak{p}_i}(z), v_{\mathfrak{p}_i}(t)\} - \min\{v_{\mathfrak{p}_i}(x), v_{\mathfrak{p}_i}(y)\}, \end{aligned}$$

which does not depend on $j$. Therefore, for every $j, k$, we have $v_{\mathfrak{p}_i}(u_j) = v_{\mathfrak{p}_i}(u_k)$ for all $i$, and this tells us that $u_j\mathcal{O}_K = u_k\mathcal{O}_K$. This means that $u_j$ and $u_k$ differ only by a unit on $\mathcal{O}_K$, but since there are more equations than units on $\mathcal{O}_K$, then by the pigeonhole principle it follows that there

exist $j \neq k$ so that $u_j = u_k$. Thus, we get

$$q_j x + y = u_j(q_j z + t)$$
$$q_k x + y = u_j(q_k z + t).$$

Subtracting both equations we obtain $x = u_j z$. Replacing on the first equation, we also get $y = u_j t$, hence we have

$$\frac{x}{z} = \frac{y}{t} \implies xt = yz.$$

□

**Lemma 2.2.2.** *Let $x$ and $y$ be units of $\mathcal{O}_{K,S}$. If for every $i$ such that $1 \leq i \leq M$ we have $v_{\mathfrak{p}_i}(x) \neq v_{\mathfrak{p}_i}(y)$, then $y = x^2$ if, and only if, $\mathfrak{as}(q_j x + 1, q_j y + x)$ holds in $\mathcal{Z}$ for every $j$.*

*Proof.* If $y = x^2$ then, as $x$ is a unit, we see that $\mathfrak{as}(q_j x + 1, q_j y + x)$ holds in $\mathcal{Z}$ obviously for every $j$. On the other hand, if $\mathfrak{as}(q_j x + 1, q_j y + x)$, then Lemma 2.2.1 tells us that $y = x^2$.

□

**Proposition 2.2.3.** *The set*

$$SQ_u = \{(x, y) : x \text{ and } y \text{ are units in } \mathcal{O}_{K,S} \text{ and } y = x^2\}$$

*is positive existentially definable in $\mathcal{Z}$.*

*Proof.* Let $I = \{0, 1, 2\}^s$ and $J = \{1, ..., N + 1\}$ The set $SQ_u$ is defined by the formula

$$Sq_u(x, y) : x|1 \wedge y|1 \wedge \bigwedge_{\substack{\delta \in I \\ j \in J}} \mathfrak{as}(q_j p^{\gamma} x + 1, q_j p^{2\gamma} y + p^{\gamma} x)$$

Suppose $Sq_u(x, y)$ holds: in this case, in particular, the formula

$$\mathfrak{as}(q_j p^{\gamma} x + 1, q_j p^{2\gamma} y + p^{\gamma} x)$$

holds for every $\gamma$ such that

$$\gamma_i \in \{0,1,2\} \setminus \left\{ \frac{v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(y)}{e(\mathfrak{p} : p_i))} : \mathfrak{p}|p_i \right\}$$

for each $1 \leq i \leq s$. Therefore, we have

$$v_{\mathfrak{p}_i}(p^{\gamma}x) - v_{\mathfrak{p}_i}(p^{2\gamma}y) = \gamma_i v_{\mathfrak{p}_i}(p_i) + v_{\mathfrak{p}_i}(x) - 2\gamma_i v_{\mathfrak{p}_i}(p_i) - v_{\mathfrak{p}_i}(y) \neq 0,$$

and this tells us that $p^{\gamma}x$ and $p^{2\gamma}y$ satisfy the hypothesis of Lemma 2.2.2. Thus, we conclude $y = x^2$. □

This proves that we can define the square of units in our structure. Next, we want to define the multiplication by units as well. The next result is going to be the first step on doing so.

**Corollary 3.** *Let $x$ unit of $\mathcal{O}_{K,S}$. If for every $i$ such that $1 \leq i \leq M$ we have $v_{\mathfrak{p}_i}(y) \neq 0$ and $v_{\mathfrak{p}_i}(z) \neq v_{\mathfrak{p}_i}(x)$, then $z = xy$ if, and only if, $\mathfrak{as}(q_j y + 1, q_j z + x)$ holds in $\mathcal{Z}$ for every $j$.*

*Proof.* Immediate from Lemma 2.2.1. □

**Proposition 2.2.4.** *The set*

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

*is positive existentially definable in $\mathcal{Z}$.*

*Proof.* Let $I = \{0,1,2,3\}^s$. The formula

$$\mathrm{Pro}(x, y, z) : x|1 \wedge \bigwedge_{\delta \in I} \mathfrak{as}(q_j p^{\delta} y + 1, q_j p^{\delta} z + x)$$

defines $P$. Note that if $z = xy$, then $\mathrm{Pro}(x, y, z)$ holds trivially for$(x, y, z) \in P$, as $x$ is a unit.

To demonstrate the converse, choose $\delta$ such that

$$\delta_i \in \{0,1,2,3\} \setminus \left( \left\{ -\frac{v_{\mathfrak{p}}(y)}{e(\mathfrak{p} : p_i))} : \mathfrak{p}|p_i \right\} \cup \left\{ \frac{v_{\mathfrak{p}}(x) - v_{\mathfrak{p}}(z)}{e(\mathfrak{p} : p_i)} : \mathfrak{p}|p_i \right\} \right).$$

For every $i$, we have:

- $v_{\mathfrak{p}_i}(p^\delta y) = \delta_i v_{\mathfrak{p}_i}(p_i) + v_{\mathfrak{p}_i}(y) \neq 0$,
- $v_{\mathfrak{p}_i}(p^\delta z) - v_{\mathfrak{p}_i}(x) = \delta_i v_{\mathfrak{p}_i}(p_i) + v_{\mathfrak{p}_i} z - v_{\mathfrak{p}_i} x \neq 0$.

Therefore $p^\gamma x, p^\delta y$ and $p^{\delta+\gamma} z$ satisfy the hypothesis of Lemma 3. As we assumed that $\mathrm{Pro}(x, y, z)$ holds, in particular $\mathfrak{as}(q_j p^\delta y + 1, q_j p^\delta z + x)$, hold, thus we can conclude that $z = xy$. □

## 2.3 Defining the square function

The final part of the manuscript will be dedicated to prove that the square function is positive existentially definable.

**Lemma 2.3.1.** *Let $x \neq 0$ in $\mathcal{O}_{K,S}$. There is a unit $u \neq 1$ of infinite order such that $x$ divides $u - 1$.*

*Proof.* Let $x \in \mathcal{O}_{K,S}$ given. Without loss of generality, we may assume that $x$ is not a unit and $x \in \mathcal{O}_K$. Let $x\mathcal{O}_K = \Pi_{i=1}^s \mathfrak{p}_i^{\alpha_i}$, and let $h_K$ be the ideal class number of $K$. We have that for each $i$, the ideal $\mathfrak{p}_i^{\alpha_i h_K}$ is principal, therefore we can write $x^{h_K} = x_1 \cdots x_l$, with each $x_i$ being a generator of $\mathfrak{p}_i^{\alpha_i h_K}$. Fix $\mathfrak{p} \in S$, and let $u_0$ be a generator of $\mathfrak{p}^{h_K}$.

We may assume, without loss of generality, that none of the $\mathfrak{p}_i$ is in $S$. As $\mathcal{O}_K/(x^{h_K})$ is of finite order and $u_0$ is not a zero-divisor, there exist $m < n$ such that

$$u_0^n \equiv u_0^m \mod (x),$$

thus, as $u_0^m$ is a unit we can see that

$$u_0^{n-m} \equiv 1 \mod (x).$$

Therefore, $u = u_0^{n-m}$ is as required. □

**Remark 2.3.2.** Note that, since the torsion part of $O_{K,S}^\times$ is finite, there is a positive existential $\mathcal{L}_{div}-$formula $\varphi_\infty$ so that $\varphi_\infty$ holds in $O_{K,S}$ if and only if $u$ is a unit of infinite order.

The idea of this is, roughly speaking, that there are large enough units. Now, we want to prove how much larger than $x$ this unit is. Next, we want to make this precise and, in order to do so, first we will find a way to control the elements of $\mathcal{O}_{K,S}$.

For each nonzero prime $\mathfrak{p}$ in $\mathcal{O}_K$, we define $k(\mathfrak{p}) = \mathcal{O}_K/\mathfrak{p}$, that is, the residue field at $\mathfrak{p}$. We recall the product formula

$$|a|^2 = \prod_{\mathfrak{p} \in Specm(\mathcal{O}_K)} \#k(\mathfrak{p})^{v_\mathfrak{p}(a)}$$

for each $a$ in $K$.

**Lemma 2.3.3.** *There is a constant $0 < C < 1$ so that for every $x \in \mathcal{O}_{K,S}^*$, there exists $a \in \mathcal{O}_{K,S}^*$ and $b \in \mathcal{O}_K^*$ such that $x = \frac{a}{b}, v_\mathfrak{p}(a) \geq -h_K$ for every $\mathfrak{p} \in S$ and $|a| > C$. Moreover, if $v_\mathfrak{p}(a) > 0$, then $v_\mathfrak{p}(b) = 0$.*

*Proof.* Let $C^2 = \prod_{\mathfrak{p} \in S} \#k(\mathfrak{p})^{-h_K}$. If $v_\mathfrak{p}(x) \geq 0$ for every $\mathfrak{p} \in S$, then we set $a = x$ and $b = 1$. If not, let $N(x) = \{\mathfrak{p} \in S : v_\mathfrak{p}(x) < 0\}$. For every $\mathfrak{p} \in N(x)$, we define $0 < \beta_\mathfrak{p} \leq -v_\mathfrak{p}(x)$ as the greatest integer such that $\mathfrak{p}^{\beta_\mathfrak{p}}$ is a principal ideal. If such $\beta_\mathfrak{p}$ for some $\mathfrak{p} \in S$ does not exist, then we say $\beta_\mathfrak{p} = 0$. Let $b_\mathfrak{p} \in \mathcal{O}_K^*$ such that $(b_\mathfrak{p}) = \mathfrak{p}^{\beta_\mathfrak{p}}$, and let $b = \prod_{\mathfrak{p} \in N(x)} b_\mathfrak{p}$. Finally, let $a = bx$. Then:

$$v_\mathfrak{p}(a) = v_\mathfrak{p}(b) + v_\mathfrak{p}(x) = \beta_\mathfrak{p} + v_\mathfrak{p}(x).$$

If $v_\mathfrak{p}(a) < -h_K$, then $\beta_\mathfrak{p} + h_K < -v_\mathfrak{p}(x)$, which contradicts our choice of $\beta_\mathfrak{p}$. This proves that $v_\mathfrak{p}(a) \geq -h_K$.

If $v_\mathfrak{p}(a) > 0$, then $\beta_\mathfrak{p} > -v_\mathfrak{p}(x)$. This means by construction that $v_\mathfrak{p}(b) = 0$.
Finally, we have to prove that $|a| > C$, which is given by the product

formula:

$$\begin{aligned}|a|^2 &= \prod_{\mathfrak{p}\in Specm(\mathcal{O}_K)} \#k(\mathfrak{p})^{v_{\mathfrak{p}}(a)} \\ &= \prod_{\mathfrak{p}\in Specm(\mathcal{O}_K)\setminus S} \#k(\mathfrak{p})^{v_{\mathfrak{p}}(a)} \prod_{\mathfrak{p}\in S} \#k(\mathfrak{p})^{v_{\mathfrak{p}}(a)} \\ &> \prod_{\mathfrak{p}\in S} \#k(\mathfrak{p})^{-h_K} = C^2.\end{aligned}$$

This means that $|a| > C$, which completes the proof. □

Let $q$ be a rational prime not below any of the primes of $S$ and such that $q > 4C^{-2}$.

**Lemma 2.3.4.** *Let $x \in \mathcal{O}_{K,S}$ be such that $v_{\mathfrak{p}}(x) \neq 0$ for every $\mathfrak{p} \in S$ and let $u \in \mathcal{O}_{K,S}^{\times}$ be a unit such that $x \pm 1 | u - 1$ and $q | u - 1$. Then,*

$$\max\left\{\frac{2}{C}, |a|, |b|\right\} \leq \max\{|v|^2, |w|^2\},$$

*with $x = \frac{a}{b}$ and $u = \frac{v}{w}$ as in Lemma 2.3.3.*

*Proof.* First, we will prove that if $q|u-1$, then $\frac{2}{C} \leq \max\{|v|, |w|\}$. Notice that, since $w$ is a unit, then $q|u-1$ if and only if $q|v-w$. Let $r = \frac{v-w}{q}$. For every $\mathfrak{p} \in S$, we have:

$$v_{\mathfrak{p}}(r) = v_{\mathfrak{p}}(q) + v_{\mathfrak{p}}(r) = v_{\mathfrak{p}}(v-w) > -h_K.$$

Therefore, by the product formula, $|r| > C$. It follows, from our hypothesis on $q$ and the triangle inequality, that

$$\max\{|v|, |w|\} \geq \frac{1}{2}|v-w| = \frac{1}{2}|q||r| \geq \frac{1}{2}qC > \frac{2}{C}.$$

Now, we prove that if $x \pm 1 | u - 1$, then $C|a \pm b| \leq |v - w|$. Without loss of generality, we will focus on the $+$ case, as the other is analogous.

As $x+1|u-1$ and $b$ is a unit, we can see that $a+b|v-w$. Let $c$ be such that $c(a+b)=v-w$. We will now show that $v_{\mathfrak{p}}(c)>-h_K$. Notice that:

- If $v_{\mathfrak{p}}(x)\geq 0$, then $v_{\mathfrak{p}}(b)=0$ and $v_{\mathfrak{p}}(a)\geq 0$, therefore $v_{\mathfrak{p}}(a+b)=0$.
- If $v_{\mathfrak{p}}(x)<0$, then either $v_{\mathfrak{p}}(b)>0$ and $v_{\mathfrak{p}}(a)\leq 0$ or $v_{\mathfrak{p}}(b)=0$ and $v_{\mathfrak{p}}(a)<0$. In any case, $v_{\mathfrak{p}}(a+b)\leq 0$.

Next, observe that $v_{\mathfrak{p}}(v-w)\geq \min\{v_{\mathfrak{p}}(v),v_{\mathfrak{p}}(w)\}\geq -h_K$. It follows that

$$v_{\mathfrak{p}}(c)=v_{\mathfrak{p}}(v-w)-v_{\mathfrak{p}}(a+b)\geq -h_K.$$

Again thanks to the product formula, it follows that $|c|>C$, which tells us that $|v-w|>C|a+b|$. Thus,

$$2|a|\leq |a+b|+|a-b|<\frac{2}{C}|v-w|\leq \frac{4}{C}\max\{|v|,|w|\}.$$

Hence, $|a|<\frac{2}{C}\max\{|v|,|w|\}$, and proceeding in a analogous way we get $|b|<\frac{2}{C}\max\{|v|,|w|\}$. Combining this with our previous inequality $\frac{2}{C}<\max\{|v|,|w|\}$, we infer that $\max\{\frac{2}{C},|a|,|b|\}\leq\max\{|v|^2,|w|^2\}$.

□

Now, we can prove the final part of our theorem. For this, we need the formula that will define the quadratic function in $\mathcal{Z}_S$, which is going to be:

$$\varphi(x,y):(x=0\wedge y=0)\vee\bigvee_{\alpha\in I}(x=\pm p^{-\alpha}\wedge y=p^{-2\alpha})$$

$$\vee\exists u_0(u_0|1\wedge\varphi_\infty(u_0))\wedge\psi(x,y),$$

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

$$\psi_1(x,u_0):\bigwedge_{\alpha\in I}p^\alpha x\pm 1|u_0-1$$

$$\psi_2(y,u_0):\bigwedge_{\alpha\in I}p^{2\alpha}y\pm 1|u_0-1$$

$$\psi_3(u_0) : q|u_0 - 1$$

$$\psi_4(u_0) : \exists u(u_0^{17} = u)$$

$$\psi_5(x, y, u) : \bigwedge_{\alpha \in I} p^\alpha x \pm u | p^{2\alpha} y - u^2,$$

with $I = \{0, ..., 6\}^s$.

**Lemma 2.3.5.** *Let $x$ and $y$ be elements of $\mathcal{O}_{K,S}$. If $\varphi(x, y)$ holds in $\mathcal{Z}$, then $y = x^2$.*

*Proof.* Assume $\varphi(x, y)$ holds. If $x = 0$ or $x = \pm p^{-\alpha}$ the result is obvious, so we may assume $x \neq 0$ and $x \neq \pm p^{-\alpha}$ for every $\alpha \in I$, and we fix $u_0$ so $\psi(x, y)$ holds.
For every $1 \leq i \leq s$, let:

$$\alpha_i \in \{0, ..., 6\} \backslash \left( \left\{ \frac{-v_\mathfrak{p}(x)}{e(\mathfrak{p} : p_i)} : \mathfrak{p} | p_i \right\}, \left\{ \frac{-v_\mathfrak{p}(y)}{2e(\mathfrak{p} : p_i)} : \mathfrak{p} | p_i \right\}, \left\{ \frac{v_\mathfrak{p}(u) - v_\mathfrak{p}(x)}{e(\mathfrak{p} : p_i)} : \mathfrak{p} | p_i \right\} \right),$$

arbitrarily. It is possible because there are at most two $\mathfrak{p} \in S$ above any of the $p_i$. This gives us an $\alpha \in I$ such that $v_\mathfrak{p}(p^\alpha x) \neq 0, v_\mathfrak{p}(p^{2\alpha} y \neq 0)$ and $v_\mathfrak{p}(p^\alpha x) \neq v_\mathfrak{p}(u)$ for every $\mathfrak{p} \in S$.

From now on, in order to simplify notation, we will write $X = p^\alpha x$ and $Y = p^{2\alpha} y$. Let $X = \frac{a}{b}, Y = \frac{c}{d}$ and $u = \frac{v}{w}$ as in Lemma 2.3.3. Since $\psi_1(x, u_0), \psi_2(y, u_0)$ and $\psi_3(u_0)$ hold, from Lemma 2.3.4 we get:

$$\max \left\{ \frac{2}{C}, |a|, |b|, |c|, |d| \right\} \leq \max\{|v|^2, |w|^2\}.$$

From $\psi_4(u_0)$ and $\psi_5(x, y, u)$, we have

$$X \pm u_0^{17} | Y - u_0^{34},$$

and trivially

$$X \pm u_0^{17} | X^2 - u_0^{34},$$

hence $X \pm u_0^{17} | X^2 - Y$. In order to get a contradiction, suppose $Y \neq X^2$.

It follows, form the previous equation, that

$$aw^{17} \pm u^{17}b | a^2d - cb^2.$$

We will show that this last equation does not hold.

Let $e^{\pm}$ be such that $(aw^{17} \pm v^{17}b)e^{\pm} = a^2d - cb^2$. First, notice that $|a^2d - cb^2| \leq |a^2d| + |cb^2| \leq 2\max\{|a|^2, |b|^3, |c|^3, |d|^3\}$, and also $v_{\mathfrak{p}}(a^2d - cb^2) \geq \min\{v_{\mathfrak{p}}(a^2d), v_{\mathfrak{p}}(cb^2)\} > -2h_K$, for every $\mathfrak{p} \in S$.

Next, we shall obtain lower bounds for $|e^{\pm}|$. In order to do so, first we will show that for every $\mathfrak{p} \in S, v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) \leq h_K + v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b)$. By assumption on $\alpha$, we have $v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) = \min\{v_{\mathfrak{p}}(aw^{17}, v_{\mathfrak{p}}(v^{17}b))\}$. We proceed by cases:

- If $v_{\mathfrak{p}}(a) > 0$ and $v_{\mathfrak{p}}(w) > 0$, then $v_{\mathfrak{p}}(b) = 0$ and $v_{\mathfrak{p}}(v) \leq 0$, thus $v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) \leq 0$.
- If $v_{\mathfrak{p}}(a) > 0$ and $v_{\mathfrak{p}}(w) = 0$, then $v_{\mathfrak{p}}(b) = 0$ and $v_{\mathfrak{p}}(v) \geq -h_K$, thus $v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) = \min\{v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(v^{17})\} \leq v_{\mathfrak{p}}(a)$.
- If $v_{\mathfrak{p}}(a) \leq 0$ and $v_{\mathfrak{p}}(w) > 0$, then $v_{\mathfrak{p}}(b) \geq 0$ and $v_{\mathfrak{p}}(v) \leq 0$, thus $v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) = \min\{v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(w^{17}, v_{\mathfrak{p}}(b) + v_{\mathfrak{p}}(v^{17}))\} \leq v_{\mathfrak{p}}(b)$.
- If $v_{\mathfrak{p}}(a) \leq 0$ and $v_{\mathfrak{p}}(w) = 0$, then $v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) \leq 0$.

Therefore,

$$\begin{aligned} v_{\mathfrak{p}}(aw^{17} \pm v^{17}b) &\leq \max\{0, v_{\mathfrak{p}}(a), v_p p(b)\} \\ &\leq h_K + v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b). \end{aligned}$$

This tells us that $v_{\mathfrak{p}}(e^{\pm}) = v_{\mathfrak{p}}(a^2d - cb^2) - v_{\mathfrak{p}}(aw^{16} \pm v^{16}b) \geq -3h_K -$

$v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b)$, and by the product rule once more

$$|e^{\pm}|^2 \geq \prod_{\mathfrak{p}\in Specm(\mathcal{O}_K)} \#k(\mathfrak{p})^{-3h_K - v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b)}$$
$$\geq \prod_{\mathfrak{p}\in Specm(\mathcal{O}_K)} \#k(\mathfrak{p})^{-v_{\mathfrak{p}}(a) - v_{\mathfrak{p}}(b)} \prod_{\mathfrak{p}\in S} \#k(\mathfrak{p})^{-3h_K} \geq \frac{C^6}{|ab|^2}.$$

Notice that, by the triangle inequality,

$$2|a^2d - cb^2| = |aw^{17} + v^{17}b||e^+| + |aw^{17} - v^{17}b||e^-| \geq \frac{2C^3|aw^{17}|}{|ab|}$$

and analogously

$$2|a^2d - cb^2| = |aw^{17} + v^{17}b||e^+| + |aw^{17} - v^{17}b||e^-| \geq \frac{2C^3|bv^{17}|}{|ab|}.$$

Thus, we obtain $|a^2d - cb^2| \geq \max\left\{\frac{C^3|w^{17}|}{|b|}, \frac{C^3|v^{17}|}{|a|}\right\}$. Considering that $\max\left\{\frac{2}{C}, |a|, |b|, |c|, |d|\right\} \leq \max\{|v|^2, |w|^2\}$, it follows that

$$\max\left\{\frac{C^3|w^{17}|}{|b|}, \frac{C^3|v^{17}|}{|a|}\right\} \geq \max\{|v|^9, |w|^9\}.$$

On the other hand,

$$|a^2d - cb^2| \leq 2\max\{|a|^2, |b|^3, |c|^3, |d|^3\} \leq \max\{|v|^8, |w|^8\},$$

and combining these we get

$$\max\{|v|^8, |w|^8\} \geq \max\{|v|^9, |w|^9\},$$

which is a contradiction.

□

**Theorem 4.** *The set*

$$SQ = \{(x, y) : x, y \text{ are in } O_{K,S} \text{ and } y = x^2\}$$

*is positive existentially definable in* $\mathcal{Z}$.

*Proof.* Because of the previous result, the only part left to prove is that if $y = x^2$, then $\varphi(x, y)$ holds. If $x = 0$ or $x = p^{-\alpha}$ for $\alpha \in I$, the result is trivial. We may then assume $x \neq 0$ and $x \neq p^{-\alpha}$ for any $\alpha \in I$, but in this case the result follows immediately from Lemma 2.3.1. □

This finishes the proof of our Theorem. As a corollary, we obtain the undecidability of $\mathrm{Th}^{+\exists}(\mathcal{O}_{K,S})$.

**Corollary 5.** *The positive existential theory of the* $\mathcal{L}_{div}-$*structure* $\mathcal{O}_{K,S}$ *is undecidable.*

*Proof.* Follows immediately from the undecidability of $\mathcal{O}_{K,S}$ in the language of rings (see [14]). □

# Bibliography


[1] A. P. Bel tjukov. Decidability of the universal theory of natural numbers with addition and divisibility. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 60:15–28, 221, 1976. Studies in constructive mathematics and mathematical logic, VII.

[2] Leonidas Cerda-Romero and Carlos Martinez-Ranero. The Diophantine problem for addition and divisibility over subrings of the rationals. *J. Symb. Log.*, 82(3):1140–1149, 2017.

[3] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Ann. of Math. (2)*, 74:425–436, 1961.

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

[5] L. Lipshitz. The Diophantine problem for addition and divisibility. *Trans. Amer. Math. Soc.*, 235:271–283, 1978.

[6] L. Lipshitz. Undecidable existential problems for addition and divisibility in algebraic number rings. *Trans. Amer. Math. Soc.*, 241:121–128, 1978.

[7] Ju. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[8] Thanases Pheidas. Hilbert's tenth problem for a class of rings of algebraic integers. *Proc. Amer. Math. Soc.*, 104(2):611–620, 1988.

[9] Bjorn Poonen. Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *J. Amer. Math. Soc.*, 16(4):981–990, 2003.

[10] Donald H. Pelletier Rene Cori, Daniel Lascar. *Mathematical Logic: A Course with Exercises Part I: Propositional Calculus, Boolean Algebras, Predicate Calculus, Completeness Theorems.* Oxford University Press, USA, 2002.

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

[12] Harold N. Shapiro and Alexandra Shlapentokh. Diophantine relationships between algebraic number fields. *Comm. Pure Appl. Math.*, 42(8):1113–1122, 1989.

[13] Alexandra Shlapentokh. Extension of Hilbert's tenth problem to some algebraic number fields. *Comm. Pure Appl. Math.*, 42(7):939–962, 1989.

[14] Alexandra Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. New Mathematical Monographs. Cambridge University Press, 2007.