Universidad de Concepción
Dirección de Postgrado
Facultad de Ciencias Físicas y Matemáticas–Programa de Doctorado en Matemática

On the Julia Robinson Number of Rings of Totally Real Algebraic Integers in Some Towers of Nested Square Roots (Sobre el Número de Julia Robinson de Anillos de Enteros Algebraicos Totalmente Reales en Algunas Torres de Raíces Cuadráticas Iteradas)

Tesis para optar al grado de Doctor en Matemática

MARIANELA ISABEL CASTILLO FERNÁNDEZ
CONCEPCIÓN-CHILE
2018

Profesor Guía: Xavier Vidaux Negre
Departamento 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

On the Julia Robinson Number of Rings of Totally Real Algebraic Integers in Some Towers of Nested Square Roots (Sobre el Número de Julia Robinson de Anillos de Enteros Algebraicos Totalmente Reales en Algunas Torres de Raíces Cuadráticas Iteradas)

Tesis para optar al grado de Doctor en Matemática

MARIANELA ISABEL CASTILLO FERNÁNDEZ
CONCEPCIÓN-CHILE
2018

Profesor Guía: Xavier Vidaux Negre
Departamento de Matemática, Facultad de Ciencias Físicas y Matemáticas
Universidad de Concepción

Profesor Co-Guía: Carlos R. Videla
Department of Mathematics and Computing
Mount Royal University

Agradecimientos

A las siguientes personas:

A Xavier Vidaux, por guiar mi formación de posgrado desde el inicio.

A Carlos Videla, por su apoyo durante la realización de este trabajo y por su hospitalidad.

A mis padres, Hector y Miriam, por su incondicional apoyo.

A mis hermanas Fabiola y María Jośe.

A Luis, por acompañarme en todo momento.

Dedicatoria

Dedico este trabajo a mis hijos
Francisca y Diego.

Contents

List of Tables

Abstract

After Julia Robinson, following a technique by Vidaux and Videla, in order to show that a ring R of totally real algebraic integers has undecidable first-order theory, one needs to characterize the set of elements of R that belong, together with all its conjugates, to a certain fixed interval. In the first part of this thesis, we obtain such characterizations for new families of such rings. The second part is concerned with showing that some of the rings studied are monogeneous. Finally, the third part is dedicated to the study of the ring of integers of the fields of fractions of these rings.

Resumen

Después de Julia Robinson, siguiendo una técnica de Vidaux y Videla, para demostrar que un anillo R de enteros algebraicos totalmente reales tiene su teoría de primer orden indecidible, se requiere caracterizar el conjunto de los elementos de R que están, junto con todos sus conjugados, dentro de un cierto intervalo fijo. En la primera parte de esta tesis, obtenemos tales caracterizaciones para nuevas familias de este tipo de anillo. En la segunda parte, se estudia la monogeneidad de dichos anillos. Finalmente, la tercera parte está dedicada al estudio del anillo de enteros de sus campos de fracciones.

Introduction

This thesis deals with the general problem, going back to Tarski, of classifying subfields of an algebraic closure $\mathbb{Q}^{\text{alg}}$ of $\mathbb{Q}$ by the decidability of their first order theory, seen as field structures (i.e. over the language $\mathcal{L} = \{0, 1, +, \cdot\}$) — we invite the reader who is not familiar with the language of mathematical logic to read Chapter 1 first. Alfred Tarski [Tarski31] proved that the theory of $\mathbb{Q}^{\text{alg}}$ and $\mathbb{Q}^{\text{alg}} \cap \mathbb{R}$ are decidable. The next important steps were done by Julia Robinson. In order to show undecidability of a given subfield K of $\mathbb{Q}^{\text{alg}}$, her strategy consists first of dividing the problem into the two following:

1. Define in K its ring of integers $\mathcal{O}_K$.

2. Define the semi-ring $\mathbb{N}$ of natural numbers in $\mathcal{O}_K$.

If one manages this, then one gets immediately a definition of $\mathbb{N}$ in K, which implies that the (full first-order) theory of K is undecidable, simply because the theory of the semi-ring $\mathbb{N}$ is known to be undecidable (this is essentially a consequence of Gödel's incompleteness theorem — see for instance [Church36]). Following this strategy, she showed [Rob59] that the theory of any number field is undecidable (so in particular the theory of the field $\mathbb{Q}$ of rational numbers is undecidable — this was proven before in [Rob49]).

Building on a result by Rumely [Rum80], Lou van den Dries showed [Dries88] that the theory of the ring of all algebraic integers is decidable. C. R. Videla [Videla99] solved Problem 1 for the field of constructible numbers, and extended his method to pro-p Galois extensions of number fields — see [Videla00b]. Using the latter, he could show [Videla00a] that the theory of any cyclotomic tower $\mathbb{Q}(p^\infty)$ is undecidable (this field is obtained by adjoining to $\mathbb{Q}$ all p-th power roots of unity, where p is a fixed prime). More recently, A. Shlapentokh proved [Sh14] that the first-order theory of any abelian extension of $\mathbb{Q}$ with finitely many ramified rational primes is undecidable. See also [Sh04, Sh09], and [Koe14] for a general survey.

We now turn our attention to the special case of subfields of the field $\mathbb{Q}^{\text{tr}}$ of all totally real algebraic numbers, that is, algebraic numbers whose conjugates are all real numbers. We will write $\mathbb{Z}^{\text{tr}}$ for the ring of integers of $\mathbb{Q}^{\text{tr}}$, and if K is any subfield of $\mathbb{Q}^{\text{tr}}$, we will write $\mathcal{O}_K$ for its ring of integers.

In [Rob62, p. 91-98], J. Robinson found a necessary and sufficient condition for $\mathbb{N}$ to have a definition in any ring of totally real algebraic integers — indeed, she did it for rings $\mathcal{O}_K$, but we will see in Chapter 1 that her proof extends easily to the general situation. If r is a totally real algebraic integer and t is either a real number or $+\infty$,

$$r \ll t$$

means that r and all its conjugates are strictly less than t. Vidaux and Videla [VV15] define the JR *number* ("Julia Robinson number") of a ring $\mathcal{O}$ of totally real algebraic integers as the infimum of the set of $t \in \mathbb{R} \cup \{+\infty\}$ such that the set

$$\mathcal{O}_{\ll t} = \{r \in \mathcal{O} \colon 0 \ll r \ll t\}$$

is infinite. Julia Robinson proved that whenever this infimum is a minimum (if it is $+\infty$, we consider that it is a minimum), the semi-ring of natural numbers is definable in $\mathcal{O}$ — this will be discussed in Chapter 1. For example:

- Every order of a totally real number field (i. e. of a totally real finite extension of $\mathbb{Q}$) has JR number equal to $+\infty$.
- In [Rob62, p. 91-98], J. Robinson proved that the JR number of the ring of integers of any subfield of $\mathbb{Q}(\sqrt{p}; p \text{ is prime})$ is $+\infty$.
- The JR number of $\mathbb{Z}^{\mathrm{tr}}$ is 4, and it is a minimum (it is a consequence of a theorem of Kronecker, see [Rob62], or [JV08] for a more detailed account).

Hence all these rings have undecidable theory. The JR number of a ring is relevant for decision problems in Logic, as discovered by Julia Robinson, and it is also connected to the Northcott property of sets of algebraic numbers — see [VV16] and [Widmer16].

In view of the undecidability of $\mathbb{Z}^{\mathrm{tr}}$, one may expect that the theory of $\mathbb{Q}^{\mathrm{tr}}$ is also undecidable, but it is indeed decidable, as was shown by Fried, Haran and Völklein [FHV94]. More recently, Vidaux and Videla proved [VV16] the following: If K denotes the compositum of all totally real algebraic extensions of $\mathbb{Q}$ of a given degree, then the maximal abelian subextension of K has undecidable first order theory. They achieve this by showing in particular that the ring of integers of such fields has infinite JR number.

The following questions arise naturally from all these results:

Q1. Does there exist rings of totally real algebraic integers with JR number strictly between 4 and $+\infty$?

Q2. Is the JR number always a minimum?

In [VV15], Vidaux and Videla construct infinitely many rings of totally real algebraic integers with JR number strictly between 4 and $+\infty$, and for infinitely many of them, the JR number is not a minimum. Nevertheless, it is not clear that any of the rings they consider is the ring of integers of its fraction field, so both questions are still unanswered for rings $\mathcal{O}_K$. Question 2 for rings $\mathcal{O}_K$ was asked by J. Robinson [Rob62].

They consider the following rings of algebraic integers

$$\mathbb{Z}^{(\nu,x_0)} = \bigcup_{n\geq 0} R_n,$$

where $R_0 = \mathbb{Z}$ and $R_n = R_{n-1}[x_n]$, for some fixed non-negative rational integers ν and x_0 such that $x_n = \sqrt{\nu + x_{n-1}}$ and $x_1 \neq x_0$. These rings are proven to be totally real exactly when,

- either $\nu > x_0^2 - x_0$ and $\nu \geq 2$ — in which case the sequence (x_n) is increasing —, or
- $\nu < x_0^2 - x_0$ and $x_{n_0} \leq \nu^2 - \nu$, where n_0 is the largest integer n such that x_n is a rational integer for every $n \leq n_0$ — in which case the sequence (x_n) is decreasing.

They say that $\mathcal{O}$ has the *isolation property* if its JR number is not a minimum and there exists a positive real number M such that for every $\varepsilon > 0$, if $\varepsilon < M$, then the set

$$\mathcal{O}_{\ll \mathrm{JR}(\mathcal{O})+M} \backslash \mathcal{O}_{\ll \mathrm{JR}(\mathcal{O})+\varepsilon}$$

is finite. They also adapt J. Robinson's argument to show that the isolation property implies the definability of $\mathbb{N}$. Assuming that the tower $\mathbb{Z}^{(\nu,x_0)}$ increases at each step (which happens infinitely often in both the increasing and the decreasing cases — see below), they prove:

- In the increasing case, except for $\nu = 3$, the JR number is a minimum.
- In the decreasing case, for infinitely many pairs (ν, x_0), the JR number satisfies the isolation property.

In order for their proof to work, they need that the tower increases at each step, meaning that for every n, the fraction field of R_n has degree 2 over the fraction field of R_{n-1}. They show that this happens whenever $\nu + x_0$ is congruent to 2 or 3 modulo 4. We observe that if $x_0 = 0$ and ν is not a square, also the tower increases at each step — apply [Stoll92, Cor. 1.3] to the iterated of $f(t) = t^2 - \nu$.

This thesis addresses the following problems:

1. Get rid of as many hypothesis as possible on ν and x_0 in the theorem of Vidaux and Videla.
2. Find out whether any of the rings $\mathbb{Z}^{(\nu,x_0)}$ is the ring of integers of its fraction field.
3. Find out whether the integral closure of any of the rings $\mathbb{Z}^{(\nu,x_0)}$ has JR number strictly between 4 and $+\infty$.
4. Find out whether the JR number of the integral closure of any of the rings $\mathbb{Z}^{(\nu,x_0)}$ is not a minimum.

Chapter 2 is dedicated to Problem 1. We get rid of all the conditions on the pairs (ν, x_0) in the decreasing case (as long as ν is not 3), which were [VV15, Thm. 1.4]: $x_1 < \lfloor \alpha \rfloor + 1$ and $\nu \geq x_1 + 1$, where α is the limit of the sequence (x_n). In particular, we show that, as long as the tower increases at each step, the ring has the isolation property, hence undecidable theory — see Theorem 2.1.1. For that we follow the general strategy from [VV15], which consists of characterizing the complete sets of conjugates that are included in a certain *ad-hoc* interval — see Theorem 2.1.3. Putting all together, we obtain:

Theorem 1. *Assume that $\mathbb{Z}^{(\nu,x_0)}$ is totally real and that $\nu + x_0$ is congruent to 2 or 3 modulo 4 and is square-free, or $x_0 = 0$ and ν is not a square. Assume $\nu > 3$. The* JR *number of $\mathbb{Z}^{(\nu,x_0)}$ is either a minimum or has the isolation property, and it lies strictly between 4 and $+\infty$.*

The objective of Chapter 3 is to solve Problem 2. If we can do this, then we can calculate the JR number precisely, answering Problem 3, and if $\mathcal{O}$ has the isolation property, then Problem 4 is solved as well, answering J. Robinson's question in the negative.

For example, the ring $\mathbb{Z}^{(2,0)}$ is the ring of integers of its fraction field — this is a special case of a theorem by Liang [Li76]. Nevertheless, this example does not answer any of the problems 3 or 4, since the JR number of this ring is 4 and it is a minimum.

For each n, let P_n denote the minimal polynomial of x_n. We prove the following result in Chapter 3.

Theorem 2. *Assume that $\mathbb{Z}^{(\nu,x_0)}$ is totally real and that $\nu + x_0$ is congruent to 2 or 3 modulo 4 and is square-free. For each $n \geq 1$, $\mathbb{Z}[x_n]$ is the ring of integers of $\mathbb{Q}(x_n)$ if and only if $P_n(0)$ is square-free.*

We are unable to determine any pair other than (2,0) for which the above result applies. It appears to be a very difficult problem. However, numerically we have established that for many pairs (ν, x_0) and values of n, the hypothesis holds, and therefore we are able to produce new examples of monogenic number fields. It should be noted that the problem of determining whether or not a number field is monogenic goes back to Dedekind, who showed that cyclotomic number fields are monogenic. In Section 3.4.1, under the ABC-Conjecture, and assuming that $x_0 = 0$, we prove that for each n, there exist infinitely many values of ν for which $P_n(0)$ is square-free.

Chapter 4 is dedicated to Problems 3 and 4. For a ring of totally real integers $\mathcal{O}$, let us define

$$A(\mathcal{O}) = \{t \in \mathbb{R} \cup \{+\infty\} \colon \mathcal{O}_{\ll t} \text{ is infinite}\}.$$

Notice that $A(\mathcal{O})$ is $\{+\infty\}$ or an interval. We will find infinitely many fields K whose ring of integers $\mathcal{O}_K$ is such that $A(\mathcal{O}_K)$ is an interval different from $[4, \infty)$ and from $\{+\infty\}$ — see Theorem 4.1.1.

Introducción

Esta tesis aborda el problema general, volviendo al trabajo de Tarski, de clasificar subcampos de una clausura algebraica $\mathbb{Q}^{\mathrm{alg}}$ de $\mathbb{Q}$ mediante la decidibilidad de su teoría de primer orden, vistos con estructura de campos (es decir, sobre el lenguaje $\mathcal{L} = \{0, 1, +, \cdot\}$) — se invita al lector que no está familiarizado con el lenguaje de la lógica matemática a leer primero el Capítulo 1. Alfred Tarski [Tarski31] demostró que la teoría de $\mathbb{Q}^{\mathrm{alg}}$ y $\mathbb{Q}^{\mathrm{alg}} \cap \mathbb{R}$ son decidibles. Los siguientes pasos importantes fueron dados por Julia Robinson. Con el fin de mostrar la indecidibilidad de un subcampo K de $\mathbb{Q}^{\mathrm{alg}}$, su estrategia consiste en primero dividir el problema en los dos problemas siguientes:

1. Definir en K su anillo de enteros $\mathcal{O}_K$.
2. Definir el semianillo $\mathbb{N}$ de los números naturales en $\mathcal{O}_K$.

Con esto tenemos inmediatamente una definición de $\mathbb{N}$ en K, lo cual implica que la teoría (completa de primer orden) de K es indecidible, simplemente porque sabemos que la teoría del semi-anillo $\mathbb{N}$ es indecidible (esta es esencialmente una consequencia de los teoremas de incompletitud de Gödel — ver por ejemplo [Church36]). Siguiendo esta estrategia, ella muestra [Rob59] que la teoría de cualquier campo de números es indecidible (luego, en particular, la teoría del campo $\mathbb{Q}$ de los números racionales es indecidible — esto lo demostró antes en [Rob49]).

Trabajando sobre un resultado de Rumely [Rum80], Lou van den Dries mostró [Dries88] que la toería del anillo de todos los enteros algebraicos es decidible. C. R. Videla [Videla99] resuelve el Problema 1 para el campo de números constructibles, y extiende su método a extensiones de Galois pro-p de campos de números — ver [Videla00b]. Usando esto último, pudo mostrar [Videla00a] que la teoría de cualquier torre ciclotómica $\mathbb{Q}(p^\infty)$ es indecidible (este campo se obtiene adjuntando a $\mathbb{Q}$ todas las raíces p-ésimas de la unidad, donde p es un primo fijo). Más recientemente, A. Shlapentokh probó [Sh14] que la teoría de primer orden de cualquier extensión abeliana de $\mathbb{Q}$ con un número finito de primos racionales ramificados es indecidible. Ver también [Sh04, Sh09], y [Koe14] para un estudio general.

Pondremos nuestra atención en el caso especial de subcampos del campo $\mathbb{Q}^{\mathrm{tr}}$ de todos los números enteros algebraicos totalmente reales, esto es, números algebraicos cuyos conjugados son todos números reales. Escribiremos $\mathbb{Z}^{\mathrm{tr}}$ para el anillo de enteros de $\mathbb{Q}^{\mathrm{tr}}$, y si K es cualquier subcampo de $\mathbb{Q}^{\mathrm{tr}}$, escribiremos $\mathcal{O}_K$ para su anillo de enteros.

En [Rob62, p. 91-98], J. Robinson encuentra una condición necesaria y suficiente para que $\mathbb{N}$ sea definible en cualquier anillo de enteros algebraicos totalmente real — en realidad, ella lo hizo para anillos $\mathcal{O}_K$, pero se puede ver en el Capítulo 1 que su demostración se extiende facilmente al caso general. Si r es un entero algebraico totalmente real y t es o bien un número real o $+\infty$,

$$r \ll t$$

significa que r y todos sus conjugados son estrictamente menor que t. Vidaux y Videla [VV15] definen el *número* JR ("Número de Julia Robinson") de un anillo $\mathcal{O}$ de enteros algebraicos totalmente reales como el ínfimo del conjunto de $t \in \mathbb{R} \cup \{+\infty\}$ tal que el conjunto

$$\mathcal{O}_{\ll t} = \{r \in \mathcal{O} \colon 0 \ll r \ll t\}$$

es infinito. Julia Robinson demostró que cuando este ínfimo es un mínimo (si éste es $+\infty$, consideramos que es un mínimo), el semi-anillo de los números naturales es definible en $\mathcal{O}$ — esto será discutido en el Capítulo 1. Por ejemplo:

- Todo orden de un campo de números totalmente real (es decir, de una extensión finita totalmente real de $\mathbb{Q}$) tiene numero JR igual a $+\infty$.
- En [Rob62, p. 91-98], J. Robinson demostró que el número JR del anillo de enteros de cualquier subcampo de $\mathbb{Q}(\sqrt{p}; p$ es primo) es $+\infty$.
- El número JR de $\mathbb{Z}^{\mathrm{tr}}$ es 4, y es un mínimo (esto es concecuencia de un teorema de Kronecker, ver [Rob62], o [JV08] para más detalles).

Luego, todos estos anillos tienen teoría indecidible. El número JR de un anillo es relevante para los problemas de decisión en Lógica, como lo descubrió Julia Robinson, y está también conectado con la propiedad de Northcott de conjuntos de números algebraicos — ver [VV16] y [Widmer16].

Viendo la indecidibilidad de $\mathbb{Z}^{\mathrm{tr}}$, se podría esperar que la teoría de $\mathbb{Q}^{\mathrm{tr}}$ sea también indecidible, pero es, de hecho, decidible, como fue demostrado por Fried, Haran y Völklein [FHV94]. Más recientemente, Vidaux y Videla demuestran [VV16] lo siguiente: Si K denota la composición de todas las extensiones algebraicas totalmente reales de $\mathbb{Q}$ de un grado fijo, entonces la subextensión abeliana maximal de K tiene teoría de primer orden indecidible. Lo que ellos muestran en particular es que el anillo de enteros de estos campos tienen número JR infinito.

Las siguientes preguntas surgen naturalmente de estos resultados:

Q1. ¿Existen anillos de enteros algebraicos totalmente reales con número JR estrictamente entre 4 y $+\infty$?

Q2. ¿Es el número JR siempre un mínimo?

En [VV15], Vidaux y Videla construyen un número infinito de anillos de enteros algebraicos totalmente reales con número JR estrictamente entre 4 y $+\infty$, y muestran que para un número infinito de ellos, el número JR no es un mínimo. Sin embargo, no queda claro si alguno de los anillos que consideran es el anillo de enteros de su campo de fracciones, por lo que ambas preguntas quedan sin respuesta para anillos $\mathcal{O}_K$. La Pregunta 2 para anillos $\mathcal{O}_K$ fue hecha por J. Robinson [Rob62].

Vidaux y Videla consideran los siguientes anillos de enteros algebraicos

$$\mathbb{Z}^{(\nu,x_0)} = \bigcup_{n\geq 0} R_n,$$

donde $R_0 = \mathbb{Z}$ y $R_n = R_{n-1}[x_n]$, para enteros racionales no negativos ν y x_0 tales que $x_n = \sqrt{\nu + x_{n-1}}$ y $x_1 \neq x_0$. Estos anillos son totalemente reales exactamente cuando,

- o bien $\nu > x_0^2 - x_0$ y $\nu \geq 2$ — en cuyo caso la sucesión (x_n) es creciente —, o bien
- $\nu < x_0^2 - x_0$ y $x_{n_0} \leq \nu^2 - \nu$, donde n_0 es el mayor entero n tal que x_n es un entero racional para todo $n \leq n_0$ — en cuyo caso la sucesión (x_n) es decreciente.

Dicen que $\mathcal{O}$ tiene la *propiedad de aislación (isolation property)* si su número JR no es un mínimo y existe un número real positivo M tal que para todo $\varepsilon > 0$, si $\varepsilon < M$, entonces el conjunto

$$\mathcal{O}_{\ll \mathrm{JR}(\mathcal{O})+M} \backslash \mathcal{O}_{\ll \mathrm{JR}(\mathcal{O})+\varepsilon}$$

es finito. Ellos adaptan el argumento de J. Robinson para mostrar que la propiedad de aislación implica la definibilidad de $\mathbb{N}$. Asumiendo que la torre $\mathbb{Z}^{(\nu,x_0)}$ crece en cada paso (lo cual sucede en infinitos casos, tanto cuando la sucesión (x_n) es creciente como cuando es decreciente — véase más adelante), prueban lo siguiente:

- En el caso creciente, excepto para $\nu = 3$, el número JR es un mínimo.
- En el caso decreciente, para infinitos pares (ν, x_0), el número JR satisface la propiedad de aislación.

Para que su técnica de demostración funcione, necesitan que la torre crezca a cada paso, es decir, que para cada n, el campo de fracciones de R_n tenga grado 2 sobre el campo de fracciones de R_{n-1}. Muestran que esto sucede cuando $\nu + x_0$ es congruente con 2 o 3 módulo 4. Observamos que si $x_0 = 0$ y ν no es un cuadrado, también la torre crece a cada paso — aplicamos [Stoll92, Cor. 1.3] a la iteración de $f(t) = t^2 - \nu$.

Esta tesis aborda los siguientes problemas:

1. Deshacerse de todas las hipótesis que sea posible sobre ν y x_0 en el teorema de Vidaux y Videla.
2. Averiguar si alguno de los anillos $\mathbb{Z}^{(\nu,x_0)}$ es el anillo de enteros de su campo de fracciones.
3. Averiguar si la clausura entera de alguno de los anillos $\mathbb{Z}^{(\nu,x_0)}$ tiene número JR extrictamente entre 4 y $+\infty$.
4. Averiguar si el número JR de la clausura entera de alguno de los anillos $\mathbb{Z}^{(\nu,x_0)}$ no es un mínimo.

El Capítulo 2 está dedicado al Problema 1. Se eliminan todas las condiciones sobre los pares (ν, x_0) en el caso decreciente (siempre que ν no sea 3), las cuales eran [VV15, Thm. 1.4]: $x_1 < \lfloor\alpha\rfloor + 1$ y $\nu \geq x_1 + 1$, donde α es el límite de la sucesión (x_n). En particular, se muestra que, siempre que la torre crezca en cada paso, el anillo tiene la propiedad de aislación, luego tiene teoría indecidible — ver Teorema 2.1.1. Para esto se siguió la estrategia general de [VV15], que consiste en caracterizar el conjunto completo de conjugados que están dentro de cierto intervalo *conveniente* — ver Teorema 2.1.3. Juntando todo esto se obtiene:

Teorema 1. *Asumamos que $\mathbb{Z}^{(\nu,x_0)}$ es totalmente real y que $\nu + x_0$ es congruente con 2 o 3 módulo 4 y es libre de cuadrados, o $x_0 = 0$ y ν no es un cuadrado. Asumamos $\nu > 3$. El número* JR *de $\mathbb{Z}^{(\nu,x_0)}$ o bien es un mínimo o bien tiene la propiedad de aislación , y está estrictamente entre 4 y $+\infty$.*

El objetivo del Capítulo 3 es resolver el Problema 2. Si podemos hacer esto, entonces podemos calcular el número JR preciso, respondiendo al Problema 3, y si $\mathcal{O}$ tiene la propiedad de aislación, entonces el Problema 4 queda resuelto también, respondiendo la pregunta de J. Robinson en forma negativa.

Por ejemplo, el anillo $\mathbb{Z}^{(2,0)}$ es el anillo de enteros de su campo de fracciones — este es un caso especial de un teorema de Liang [Li76]. Sin embargo, este ejemplo no resuelve ninguno de los problemas 3 o 4, porque el número JR de este anillo es 4 y es un mínimo.

Para cada n, denotamos por P_n al polinomio mínimo de x_n. En el Capítulo 3 se pueban los siguientees resultados.

Teorema 2. *Asumamos que $\mathbb{Z}^{(\nu,x_0)}$ es totalmente real y que $\nu + x_0$ es congruente con 2 o 3 modulo 4 y es libre de cuadrados. Para cada $n \geq 1$, $\mathbb{Z}[x_n]$ es el anillo de enteros de $\mathbb{Q}(x_n)$ si y sólo si $P_n(0)$ es libre de cuadrados.*

No se ha podido determinar un par diferente de $(2, 0)$ para el cual se aplique el resultado anterior. Este parece ser un problema muy dificil. Sin embargo, numéricamente se ha establecido que para muchos pares (ν, x_0) y valores de n, la hipótesis se cumple, y por lo tanto, podemos producir nuevos ejemplos de campos de números monógenos. Cabe señalar que el problema de determinar si un campo de números es monógeno o no se remonta a Dedekind, quien mostró que los campos de números ciclotómicos son monógenos. En la Sección 3.4.1, bajo la Congetura ABC, y asumiendo que $x_0 = 0$, se prueba que para cada n, existen infinitos valores de ν para los cuales $P_n(0)$ es libre de cuadrados.

El Capítulo 4 está dedicado a los Problemas 3 y 4. Para un anillo de enteros algebraicos totalmente reales $\mathcal{O}$, se define

$$A(\mathcal{O}) = \{t \in \mathbb{R} \cup \{+\infty\} \colon \mathcal{O}_{\ll t} \text{ es infinito}\}.$$

Notamos que $A(\mathcal{O})$ es $\{+\infty\}$ o un intervalo. Se encuentra una cantidad infinita de campos K con anillo de enteros $\mathcal{O}_K$ es tal que $A(\mathcal{O}_K)$ es un intervalo diferente de $[4, \infty)$ y de $\{+\infty\}$ — ver Teorema 4.1.1.

Chapter 1

Preliminaries

1.1 Logic

In our context, a *sentence* is a first-order closed formula in the ring language, which can be thought of simply as a statement made of a disjunction of systems of polynomial equations and inequations over $\mathbb{Z}$, where all the variables (i. e. unknowns) are quantified by either an existential quantifier or a universal quantifier. A formula is such a statement, but without the requirement that all the variables are quantified. The variables which are not quantified are called *free variables.* So for example,

$$\forall x \exists y \forall z (x^2 - 2y^3 = y^2 + z^3 \wedge x \neq y)$$

is a sentence, whereas

$$\exists y \forall z (x^2 - 2y^3 = y^2 + z^3 \wedge x \neq y)$$

is a formula which is not a sentence. Note that a sentence may be true or false, depending in which structure we consider it, while a formula will be true or false in a certain structure for certain realizations of the free variables. So for instance, the sentence

$$\forall x \exists y (x = 2y)$$

is true in $\mathbb{Q}$ but not in $\mathbb{Z}$, and the formula

$$\exists y (x = 2y)$$

is true in $\mathbb{Z}$ precisely when x is even.

The *theory* of a ring R is the set of all sentences that are true in R. We say that the theory of a ring R is *decidable* (or simply that *R is decidable*) if there exists an algorithm which, given an arbitrary sentence, decides in finite time (i. e. in a finite number of steps) whether the sentence belongs or not to the theory of R.

We say that a subset S of a ring R is *definable* if there exists a formula ϕ with just one free variable such that the following is true:

$$r \in S \text{ if and only if } \phi(r) \text{ is true in } R.$$

So for instance the set of even integers is definable in $\mathbb{Z}$ by the formula $\exists y (x = 2y)$.

The definability is extremely useful to transfer undecidability results. Suppose for instance that $\mathbb{N}$ can be defined in a ring R. If there were an algorithm to decide membership for the theory of R, using the formula which defines $\mathbb{N}$, we could test membership for the theory of $\mathbb{N}$ by imposing that each variable appearing in a given sentence lies in $\mathbb{N}$. Since we know that the theory of $\mathbb{N}$

is undecidable, this would be a contradiction. Hence, any ring in which $\mathbb{N}$ can be defined has undecidable theory. For example, it is known that any natural number can be written as a sum of four squares of integers (Lagrange's Theorem), so the formula

$$\phi(n) = \exists x \exists y \exists z \exists w (n = x^2 + y^2 + z^2 + w^2)$$

defines the natural numbers in $\mathbb{Z}$. Therefore, the theory of $\mathbb{Z}$ is undecidable.

1.2 Julia Robinson's definability criterium

In [Rob62], Julia Robinson shows that $\mathbb{N}$ is definable in any ring $R = \mathcal{O}_K$ of totally real integers which satisfies some hypothesis. In this section, we give a precise statement and a sketch of proof for the more general case where R is an arbitrary ring of totally real integers.

For an $\mathcal{L}$-formula $\phi(x; \bar{y})$ where $\bar{y} = (y_1, \ldots, y_k)$ and for $\bar{r} = (r_1, \ldots, r_k) \in R^k$, we put

$$\varphi_{\bar{r}} = \{s \in R : R \models \phi(s, \bar{r})\}.$$

Definition 1.2.1. *A family $\mathcal{F}$ of sets of elements of R is said to be* definable *if there exists a formula $\varphi(x; \bar{y})$ such that for each set $A \in \mathcal{F}$, there exists $\bar{r} \in R^k$ such that $A = \varphi_{\bar{r}}$, and for every $\bar{r} \in R^k$, $\varphi_{\bar{r}} \in \mathcal{F}$.*

We can now state the theorem:

Theorem 1.2.2 ([Rob62] Theorem 2)**.** *If there exists a definable family of subsets of R which contains arbitrarily large finite sets, then $\mathbb{N}$ is definable in R.*

The proof of this theorem goes through with no change for arbitrary R, except for [Rob62, Lemma 1], for which we provide a proof.

Lemma 1.2.3. *Let $A = \{a_1, \ldots, a_n\} \subset R$ a set with $n \geq 1$ non-zero elements. There exists $g \in R$ totally positive that can be taken arbitrarily large, so that the ideals $I_i = (1 + a_i g)$ are pairwise coprime, and for each i, $1 + a_i g$ is not zero and is not invertible.*

Proof. Let M be a natural number. Put

$$g = M \prod_{a_i \neq a_j} (a_i - a_j)^2.$$

Clearly g is totally positive and becomes arbitrarily large as M increases. Since the set A is finite and each a_i is non-zero, we can take g large enough so that each $1 + a_i g$ and all its conjugates do not belong to the closed real interval $[-1, 1]$. Hence, the norm of $1 + a_i g$ is in $\mathbb{Z} - \{0, \pm 1\}$, so that the numbers $1 + a_i g$ are neither units nor zero.

We need to show that for each $i \neq j$, the ideal $I_i + I_j$ is equal to R. We have

$$(a_i - a_j)g = (1 + a_i g) - (1 + a_j g) \in I_i + I_j$$

for each $i \neq j$. By definition of g, there exists $s \in R$ such that $s(a_i - a_j) = g$, hence $s(a_i - a_j)g = g^2$ belongs to $I_i + I_j$. This implies that

$$1 + 2a_i g = (1 + a_i g)^2 - a_i^2 g^2$$

belongs to $I_i + I_j$, hence

$$a_i g = -(1 + a_i g) + (1 + 2a_i g)$$

belongs to $I_i + I_j$. So finally $1 = (1 + a_i g) - a_i g$ belongs to $I_i + I_j$. $\square$

J. Robinson proved the following corollary of Theorem 1.2.2 when the JR number is a minimum, and this was adapted in [VV15] to the case of the isolation property. We give a proof for sake of completeness.

Corollary 1.2.4. *The semi-ring of natural numbers is definable in any ring of totally real algebraic integers whose* JR *number is either a minimun or has the isolation property.*

Proof. By a theorem of C. Siegel (1921), the relation $x \ll y$ is definable in any ring of totally real algebraic integers by the formula

$$(\exists t \exists u \exists v \exists w \exists z)(t^2(y-x) = u^2+v^2+w^2+z^2 \wedge t \neq 0).$$

If the JR number is a minimum, then the family of sets defined by the following formula $\varphi(x; y_1, y_2)$

$$0 \ll y_1 x \ll y_2$$

contains arbitrarily large finite subsets of R. If the JR number has the isolation property, then the following formula works:

$$\varphi(x; y_1, y_2) \wedge \neg\varphi(x; y_3, y_4).$$

□

Chapter 2

Characterizing intervals containing complete sets of conjugates in a family of totally real towers of nested square roots

2.1 Introduction

The objective of this Chapter is to prove the following theorem, which together with [VV15, Thm. 1.4] gives Theorem 1.

Theorem 2.1.1. *Let ν and x_0 be non-negative rational integers with $\nu \neq 3$ such that the fraction field of R_{n+1} has degree 2 over the fraction field of R_n for each $n \geq 0$ and the sequence (x_n) is decreasing. Let α be the limit of the sequence (x_n) as n tends to infinity. The ring $\mathbb{Z}^{(\nu,x_0)}$ has* JR *number $\lfloor\alpha\rfloor+\alpha+1$, where $\lfloor\alpha\rfloor$ denotes the largest integer smaller than or equal to α, and it satisfies the isolation property. In particular, its first order theory is undecidable.*

Following the strategy in [VV15], in order to prove the theorem one needs to completely determine a set of the form

$$\mathcal{O}_{\ll t} = \{r \in \mathcal{O} \colon 0 \ll r \ll t\}\,.$$

The first difficulty is to guess for which t this can be achieved (in our case, it turns out that one can always take $t = 2\lfloor\alpha\rfloor + 2$), the main difficulty being then to guess which r should be in the set, so that one can proceed by induction.

Before we can state our main technical result, we need to introduce some notation.

Notation 2.1.2. *Let $m = m(\nu, x_0)$ be the smallest index n such that $x_n < \lfloor\alpha\rfloor + 1$ (such an m exists because (x_n) is decreasing and tends to α).*

We will have to consider four exceptional cases, namely when

$$(\nu, x_0) \in E = \{(4, 11), (6, 29), (8, 55), (12, 131)\}.$$

In the generic situation, we put $X = X^{(\nu,x_0)} = \bigcup_{n\geq 0} X_n$, where

$$X_0 = \cdots = X_{m-1} = \{1, 2, \ldots, 2\lfloor\alpha\rfloor + 1\}$$

and

$$X_n = X_{n-1} \cup \{\lfloor\alpha\rfloor + 1 \pm x_k \colon m \leq k \leq n\},$$

for any $n \geq m$. When $(\nu, x_0) \in E$, one can easily verify that $m = 2$. In that case, X_2 is changed into

$$X_1 \cup \{\lfloor\alpha\rfloor + 1 \pm x_2\} \cup \{\lfloor\alpha\rfloor + 1 \pm (y - x_1)x_2 \colon y \in \{\nu - 1, \nu\}\}$$

when $(\nu, x_0) \notin \{(6, 29)\}$, and into

$$X_1 \cup \{\lfloor\alpha\rfloor + 1 \pm x_2\} \cup \{\lfloor\alpha\rfloor + 1 \pm (y - x_1)x_2 \colon y \in \{\nu - 1, \nu, \nu + 1\}\}$$

in the remaining case.

It is easy to verify that for any $x \in X$ we have $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$. We prove:

Theorem 2.1.3. *Let ν and x_0 be non-negative rational integers with $\nu \neq 3$ such that the fraction field of R_{n+1} has degree 2 over the fraction field of R_n for each $n \geq 0$ and the sequence (x_n) is decreasing. We have*

$$\mathbb{Z}^{(\nu, x_0)}_{\ll 2\lfloor\alpha\rfloor + 2} = X.$$

The Main Theorem follows in the same manner as in [VV15]. The proof of theorem 2.1.3 comes from the fact that $\nu - x_n > 1$ for some $n \geq 1$. In case $\nu = 3$ we have $\nu - \alpha < 1$, hence when x_n is decreasing we have $\nu - x_n < 1$ for all $n \geq 1$ (for this reason we do not consider the case $\nu = 3$ in the Main Theorem).

2.2 Technical lemmas

From now on, σ will denote any of the embeddings of $\mathbb{Q}(x_n)$ into $\mathbb{R}$ which fixes $\mathbb{Q}$. We assume that ν and x_0 are non-negative rational integers with $\nu \neq 3$ and that the sequence (x_n) is decreasing — hence in particular we have $\nu < x_0^2 - x_0$. Without loss of generality, we assume moreover that $n_0 = 0$, namely, x_n is a rational integer only for $n = 0$ (this corresponds to Assumption 2.8 in [VV15] — see also the paragraph just before it). Note that since (x_n) is decreasing and the tower is totally real, we have $x_0 \leq \nu^2 - \nu$, and $x_n < \nu^2 - \nu$ for every $n \geq 1$. Finally, we will write $\mathcal{O}$ instead of $\mathbb{Z}^{(\nu, x_0)}$.

Remark 2.2.1. *The conditions $x_0 \leq \nu^2 - \nu$ and $\nu < x_0^2 - x_0$ together imply $\nu \geq 3$. Hence, we will assume $\nu \geq 4$ for the rest of this work.*

We start by stating a general lemma — see [VV15, Lemmas 2.3, 2.10 and 2.19].

Lemma 2.2.2. 1. *The sequence (x_n) is convergent with limit $\alpha = \frac{1+\sqrt{1+4\nu}}{2}$.*

2. *We have $x_0 \geq 3$ and $\alpha > 2$.*

3. *Let r be a real number, $n \geq 1$, and $a, b \in R_{n-1}$. For $n = 1$, if $0 \ll a + bx_1 \ll 2r$, then $a, b \in \mathbb{Z}$ satisfy $0 < a < 2r$ and $|b| < \frac{r}{x_1}$. For $n \geq 2$, if $0 \ll a + bx_n \ll 2r$, then $0 \ll a \ll 2r$ and*

$$|b^\sigma| < \frac{r}{\sqrt{\nu - x_{n-1}}},$$

for all σ.

We start by proving some lemmas that give a lower bound for the sequence $(\nu - x_n)_n$.

Lemma 2.2.3. *For all $n \geq 0$, we have $\nu - x_{n+2} > 1$.*

Proof. Since $\nu \geq 4$, we have $\nu > 2 + \sqrt{3}$, hence $\nu^2 - 4\nu + 1 > 0$, hence $\nu^2 - 2\nu + 1 > 2\nu$, and finally $\nu - 1 > \sqrt{2\nu}$. Therefore, we have

$$\nu - x_{n+2} = \nu - \sqrt{\nu + \sqrt{\nu + x_n}} \geq \nu - \sqrt{\nu + \sqrt{\nu + \nu^2 - \nu}} = \nu - \sqrt{2\nu} > 1.$$

where the first inequality comes from the fact that $x_n \leq \nu^2 - \nu$ (by general hypothesis). □

Lemma 2.2.4. *For all $n \geq 1$, if $x_n < \lfloor \alpha \rfloor + 1$, then $\nu - x_n > 1$.*

Proof. Since $x_n < \lfloor \alpha \rfloor + 1$, we have $\nu - x_n > \nu - \lfloor \alpha \rfloor - 1$. When $\nu = 4$, $\nu - \lfloor \alpha \rfloor - 1$ is equal to 1, so we may assume $\nu \geq 5$. Recalling that $\alpha = \frac{1+\sqrt{1+4\nu}}{2}$, we have $\nu - \alpha - 1 > 1$ if and only if $\nu - \alpha > 2$, if and only if $2\nu - (1 + \sqrt{1+4\nu}) > 4$, if and only if $2\nu - 5 > \sqrt{1+4\nu}$, if and only if $4\nu^2 - 20\nu + 25 > 1 + 4\nu$, if and only if $4\nu^2 - 24\nu + 24 > 0$, which is true since $\nu \geq 5$. So we have $\nu - \alpha - 1 > 1$, hence also $\nu - \lfloor \alpha \rfloor - 1 > 1$. □

In particular, the conclusion of Lemma 2.2.4 is precisely Assumption 3.1 in [VV15].

We now turn to a sequence of technical lemmas that will lead us eventually towards a characterization of the sets X_n (in the next Section).

Lemma 2.2.5. *Suppose that $x_1 > \lfloor \alpha \rfloor + 1$. Let $a, b \in \mathbb{Z}$ be such that $a + bx_1 \in R_1$ satisfies $0 \ll a + bx_1 \ll 2\lfloor \alpha \rfloor + 2$. We have $a \in \{1, \dots, 2\lfloor \alpha \rfloor + 1\}$ and $b = 0$.*

Proof. If $0 \ll a + bx_1 \ll 2\lfloor \alpha \rfloor + 2$, then by Lemma 2.2.2 we have $0 < a < 2\lfloor \alpha \rfloor + 2$ and

$$|b| < \frac{\lfloor \alpha \rfloor + 1}{x_1}.$$

Since $x_1 > \lfloor \alpha \rfloor + 1$ and b is an integer, we deduce that b is zero. □

Lemma 2.2.6. *Let $n \geq 1$ and let $a + bx_n \in R_n$, where $a, b \in R_{n-1}$. Suppose that $0 \ll a + bx_n \ll 2\lfloor \alpha \rfloor + 2$ and $x_n \geq \lfloor \alpha \rfloor + 1$. If $a \in \{1, \dots, 2\lfloor \alpha \rfloor + 1\}$ then $|b| < 1$.*

Proof. For the sake of contradiction, we assume $|b| \geq 1$.

Assume first $a \in \{1, \dots, \lfloor \alpha \rfloor\}$. We can choose σ such that $(a + bx_n)^\sigma = a - |b|x_n$. We have

$$(a + bx_n)^\sigma = a - |b|x_n \leq \lfloor \alpha \rfloor - x_n \leq \lfloor \alpha \rfloor - \lfloor \alpha \rfloor - 1 = -1,$$

which contradicts the hypothesis $0 \ll a + bx_n$.

If $a \in \{\lfloor \alpha \rfloor + 1, \dots, 2\lfloor \alpha \rfloor + 1\}$, we can choose σ such that $(a + bx_n)^\sigma = a + |b|x_n$. We have

$$(a + bx_n)^\sigma = a + |b|x_n \geq \lfloor \alpha \rfloor + 1 + x_n \geq \lfloor \alpha \rfloor + 1 + \lfloor \alpha \rfloor + 1 = 2\lfloor \alpha \rfloor + 2,$$

which contradicts the hypothesis $a + bx_n \ll 2\lfloor \alpha \rfloor + 2$. □

When we will characterize the elements of X, we will have to show that certain families of algebraic numbers do not belong to it. The following lemma will be used often for this purpose in Lemma 2.3.10.

Lemma 2.2.7. *Let $b_1, b_2 \in \mathbb{Z}$ and $a \in \{1, \dots, 2\lfloor \alpha \rfloor + 1\}$. Let*

$$x = a + (b_1 + b_2 x_1)x_2 \in R_2$$

be such that $0 \ll x \ll 2\lfloor \alpha \rfloor + 2$. Suppose that $m = 2$ (see Not. 2.1.2).

1. *If $b_1 = 0$, then $b_2 = 0$.*

2. *If $b_2 = 0$, then either $b_1 = 0$, or $a = \lfloor\alpha\rfloor + 1$ and $b_1 \in \{0, \pm 1\}$.*

Proof. Assume $b_1 = 0$ and $|b_2| \geq 1$. For any $a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$, there exists σ which fixes R_1 such that $x^\sigma = a + |b_2|x_1x_2$. Therefore, we have

$$x^\sigma > 1 + (\lfloor\alpha\rfloor + 1)x_2 \geq 1 + \lfloor\alpha\rfloor + \lfloor\alpha\rfloor^2 > 2\lfloor\alpha\rfloor + 2,$$

because $\lfloor\alpha\rfloor \geq 2$ by Lemma 2.2.2. This contradicts our hypothesis on x, so we have $b_2 = 0$.

Assume $b_2 = 0$ and $|b_1| \geq 1$. For $a \in \{1, \ldots, \lfloor\alpha\rfloor\}$, choose σ such that $x^\sigma = a - |b_1|x_2$, so that

$$x^\sigma = a - |b_1|x_2 \leq \lfloor\alpha\rfloor - x_2 < \lfloor\alpha\rfloor - \alpha \leq 0.$$

If $a \in \{\lfloor\alpha\rfloor + 2, \ldots, 2\lfloor\alpha\rfloor + 1\}$, choose σ such that $x^\sigma = a + |b_1|x_2$, so that

$$x^\sigma = a + |b_1|x_2 \geq \lfloor\alpha\rfloor + 2 + x_2 > \lfloor\alpha\rfloor + 2 + \alpha \geq 2\lfloor\alpha\rfloor + 2.$$

Hence, we have $b_1 = 0$ unless $a = \lfloor\alpha\rfloor + 1$.

Assume $a = \lfloor\alpha\rfloor + 1$ and $|b_1| \geq 2$. There exists σ such that

$$x^\sigma = a + |b_1|x_2 \geq \lfloor\alpha\rfloor + 1 + 2x_2 > \lfloor\alpha\rfloor + 1 + 2\alpha > 2\lfloor\alpha\rfloor + 2,$$

so that $|b_1| < 2$. □

Lemma 2.2.8. *Let $a, b_1, b_2 \in \mathbb{Z}$ and $x = a + (b_1 + b_2x_1)x_2$ be such that $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$. Suppose that $x_1 > \lfloor\alpha\rfloor + 1$. If $a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$ and $b_1b_2 \neq 0$, then $b_1b_2 < 0$.*

Proof. Since $b_1b_2 \neq 0$, we have $|b_1| \geq 1$ and $|b_2| \geq 1$. For the sake of contradiction, assume that b_1 and b_2 have the same sign, so that there exists σ fixing R_1 such that

$$x^\sigma = a + |b_1|x_2 + |b_2|x_1x_2.$$

Hence we have

$$\begin{aligned} x^\sigma &\geq 1 + x_2 + x_1x_2 \\ &> 1 + \lfloor\alpha\rfloor + (\lfloor\alpha\rfloor + 1)\lfloor\alpha\rfloor \\ &= (1 + \lfloor\alpha\rfloor)^2 \\ &> 2\lfloor\alpha\rfloor + 2, \end{aligned}$$

because $\lfloor\alpha\rfloor \geq 2$. □

Lemma 2.2.9. *Assume that $x_n < \lfloor\alpha\rfloor + 1$ for all $n \geq 3$. Suppose that for all $x \in R_2$ such that $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$ we have*

$$x \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 \pm x_2\}.$$

For all $n \geq 2$, if $x \in R_n$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then

$$x \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 \pm x_k \colon k = 2, \ldots, n\}.$$

Proof. The proof is part of the proof of Lemma 3.2 of [VV15] (Facts 2.1 up to 2.5). We include it here for the convenience of the reader, as we will use some of our lemmas instead of assumptions that were made in [VV15].

We prove the Lemma by induction on n. For $n = 2$ there is nothing to prove. Assume that this is true up to $n - 1 \geq 2$. Let $a, b \in R_{n-1}$ and $x = a + bx_n \in R_n$. By Lemma 2.2.2, if $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$ then

$$0 \ll a \ll 2\lfloor\alpha\rfloor + 2$$

and for all σ

$$|b^\sigma| < \frac{\lfloor\alpha\rfloor + 1}{\sqrt{\nu - x_{n-1}}}.$$

Since $n \geq 3$, by Lemma 2.2.3 we have $\sqrt{\nu - x_{n-1}} > 1$, hence $|b^\sigma| < \lfloor\alpha\rfloor + 1$, that is, $0 \ll b + \lfloor\alpha\rfloor + 1 \ll 2\lfloor\alpha\rfloor + 2$. By induction hypothesis

$$a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 \pm x_k : k = 2, \ldots, n-1\}$$

and

$$b \in \{-\lfloor\alpha\rfloor, \ldots, \lfloor\alpha\rfloor\} \cup \{\pm x_k : k = 2, \ldots, n-1\}.$$

Fact 1. If $a \in \{1, \ldots, \lfloor\alpha\rfloor\}$, then $b = 0$.

Assume $a \in \{1, \ldots, \lfloor\alpha\rfloor\}$ and $b \neq 0$. Either $b \in \mathbb{Z}$ and $|b| \geq 1$, or $|b| = x_j > \alpha$ for some $2 \leq j \leq n-1$. In both cases we have $|b| \geq 1$. We can consider an embedding σ that fixes R_{n-1} and such that $x^\sigma = a - |b|x_n$, we obtain

$$x^\sigma \leq \lfloor\alpha\rfloor - x_n \leq \alpha - x_n < 0.$$

Fact 2. If $a \in \{\lfloor\alpha\rfloor + 2, \ldots, 2\lfloor\alpha\rfloor + 1\}$, then $b = 0$.

As in Fact 1, suppose that $|b| \geq 1$. By choosing σ such that $x^\sigma = a + |b|x_n$, we obtain

$$x^\sigma \geq \lfloor\alpha\rfloor + 2 + x_n > \lfloor\alpha\rfloor + 2 + \alpha \geq 2\lfloor\alpha\rfloor + 2.$$

Fact 3. If $a = \lfloor\alpha\rfloor + 1$ then b is a rational integer and $|b| \leq 1$.

Suppose that $|b| \geq 2$. Choose σ fixing R_{n-1} such that $x^\sigma = a + |b|x_n$. We have

$$x^\sigma > \lfloor\alpha\rfloor + 1 + 2x_n > \lfloor\alpha\rfloor + 1 + 2\alpha > 2\lfloor\alpha\rfloor + 2.$$

This contradiction implies $|b| \leq 1$, and in particular it is a rational integer (because we already know that either $b \in \mathbb{Z}$ or $|b| = x_k > \alpha \geq 2$ by Lemma 2.2.2).

Fact 4. If $a = \lfloor\alpha\rfloor + 1 + x_k$ for some $2 \leq k \leq n-1$, then $b = 0$.

Otherwise $|b| \geq 1$, and by choosing σ such that $x^\sigma = \lfloor\alpha\rfloor + 1 + x_k + |b|x_n$, we would obtain

$$x^\sigma = \lfloor\alpha\rfloor + 1 + x_k + |b|x_n > \lfloor\alpha\rfloor + 1 + 2\alpha \geq 2\lfloor\alpha\rfloor + 2.$$

Fact 5. If $a = \lfloor\alpha\rfloor + 1 - x_k$ for some $2 \leq k \leq n-1$, then $b = 0$.

As in Fact 4, by choosing σ such that $x^\sigma = \lfloor\alpha\rfloor + 1 - x_k - |b|x_n$, we would obtain

$$x^\sigma < \lfloor\alpha\rfloor + 1 - 2\alpha < 0.$$

□

2.3 Proof of Theorem 2.1.3

Recall that m is the smallest index n such that $x_n < \lfloor\alpha\rfloor + 1$. When (ν, x_0) is not in the exceptional set E, we will consider four cases separately:

- $m \neq 2$,
- $m = 2$ and $\nu - x_1 > 1$, and
- $m = 2$ and $\nu - x_1 < 1$.

Note that when $(\nu, x_0) \in E$, we have $m = 2$ and $\nu - x_1 < 1$.

2.3.1 Case $m \neq 2$.

The following Lemma proves Theorem 2.1.3 when $m \leq 1$.

Lemma 2.3.1. *Assume that $m \leq 1$. If $x \in \mathcal{O}$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X$.*

Proof. By definition of m, since $m \leq 1$, we have $x_1 < \lfloor\alpha\rfloor + 1$, so Assumption 2.17 of [VV15] is satisfied. We have $\sqrt{\nu - x_1} > 1$ by Lemma 2.2.4, so Assumption 3.1 in [VV15] is also satisfied. Hence Lemma 3.2 from [VV15] is now true with no extra hypothesis. □

Lemmas 2.3.2 and 2.3.3 below deal with the case $m \geq 3$.

Lemma 2.3.2. *Assume $m \geq 3$. For all $n = 1, \ldots, m-1$, if $x \in R_n$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$.*

Proof. We prove it by induction on n. For $n = 1$, this is Lemma 2.2.5, since we have $x_1 > \lfloor\alpha\rfloor + 1$ by definition of m. Let $x = a + bx_n \in R_n$ for some $2 \leq n \leq m-1$, where $a, b \in R_{n-1}$, and assume that the lemma is true for $n-1$. If $0 \ll a + bx_n \ll 2\lfloor\alpha\rfloor + 2$, then by Lemma 2.2.2 we have

$$0 \ll a \ll 2\lfloor\alpha\rfloor + 2$$

and

$$|b^\sigma| < \frac{\lfloor\alpha\rfloor + 1}{\sqrt{\nu - x_{n-1}}}.$$

By induction hypothesis, we have $a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$. Since $x_{n-1} > \lfloor\alpha\rfloor + 1$, by Lemma 2.2.4 we have $\sqrt{\nu - x_{n-1}} > 1$, hence $|b^\sigma| < \lfloor\alpha\rfloor + 1$. This implies $0 \ll b + \lfloor\alpha\rfloor + 1 \ll 2\lfloor\alpha\rfloor + 2$, and by induction hypothesis we have $b \in \{-\lfloor\alpha\rfloor, \ldots, \lfloor\alpha\rfloor\}$. Finally, by Lemma 2.2.6 we have $b = 0$.

□

Lemma 2.3.3. *Assume $m \geq 3$. For all $n \geq m$, if $x \in R_n$ is such that $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 \pm x_k : k = m, \ldots, n\}$.*

Proof. In the proof of Lemma 3.2 in [VV15], replace x_1 by x_m, $\mathcal{O}_1$ by R_m and so on. The assumption there that x_1 is less than $\lfloor\alpha\rfloor + 1$ is now replaced by the *fact* that $x_m < \lfloor\alpha\rfloor + 1$ (by definition of m). They use $x_1 > 1$ (in the first step of the induction) and $\sqrt{\nu - x_1} \geq 1$ (their Assumption 3.1), which are now replaced by the only fact that $\sqrt{\nu - x_{m-1}} > 1$ (which comes from Lemma 2.2.3, because $m \geq 3$). □

From Lemmas 2.3.2 and 2.3.3 we deduce the following corollary.

Corollary 2.3.4. *Assume $m \geq 3$. Let $x \in \mathcal{O}$. If $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X$.*

2.3.2 Case $m = 2$ and $\nu - x_1 > 1$.

In this subsection, we assume $\nu - x_1 > 1$ and $m = 2$, so in particular we have $x_1 > \lfloor\alpha\rfloor + 1$ and $x_2 < \lfloor\alpha\rfloor + 1$.

Lemma 2.3.5. *Let $x = a + bx_2 \in R_2$, with $a, b \in R_1$, satisfying $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$. We have $a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$ and $b \in \{0, \pm 1\}$. Moreover, if $a \neq \lfloor\alpha\rfloor + 1$, then $b = 0$.*

Proof. By Lemma 2.2.2, we have

$$0 \ll a \ll 2\lfloor\alpha\rfloor + 2$$

and

$$|b^\sigma| < \frac{\lfloor\alpha\rfloor + 1}{\sqrt{\nu - x_1}} < \lfloor\alpha\rfloor + 1.$$

Note that by Lemma 2.2.5 we have $a \in \{1, \dots, 2\lfloor\alpha\rfloor + 1\}$. Write $b = b_1 + b_2 x_1$, with $b_1, b_2 \in \mathbb{Z}$. Since $|b^\sigma| < \lfloor\alpha\rfloor + 1$, we have

$$0 \ll b_1 + b_2 x_1 + \lfloor\alpha\rfloor + 1 \ll 2\lfloor\alpha\rfloor + 2.$$

From Lemma 2.2.5 again, we deduce $b_1 \in \{-\lfloor\alpha\rfloor, \dots, \lfloor\alpha\rfloor\}$ and $b_2 = 0$, that is $b \in \{-\lfloor\alpha\rfloor, \dots, \lfloor\alpha\rfloor\}$.

- *Fact 1. If $a \in \{1, \dots, \lfloor\alpha\rfloor\}$, then $b = 0$.*
  Suppose that $|b| \geq 1$. We can choose the embedding σ such that $x^\sigma = a - |b| x_2$. We have

  $$x^\sigma \leq \lfloor\alpha\rfloor - x_2 < \lfloor\alpha\rfloor - \alpha \leq 0,$$

  which contradicts the hypothesis on x.

- *Fact 2. If $a \in \{\lfloor\alpha\rfloor + 2, \dots, 2\lfloor\alpha\rfloor + 1\}$, then $b = 0$.*
  Suppose that $|b| \geq 1$. By choosing σ such that $x^\sigma = a + |b| x_2$ we have

  $$x^\sigma \geq \lfloor\alpha\rfloor + 2 + x_2 > \lfloor\alpha\rfloor + 2 + \alpha \geq 2\lfloor\alpha\rfloor + 2.$$

  which contradicts the hypothesis on x.

- *Fact 3. If $a = \lfloor\alpha\rfloor + 1$, then $b \in \{-1, 0, 1\}$.*
  Assume $|b| \geq 2$. By choosing σ such that $x^\sigma = a + |b| x_2$ we have

  $$x^\sigma \geq \lfloor\alpha\rfloor + 1 + 2x_2 > \lfloor\alpha\rfloor + 1 + 2\alpha > 2\lfloor\alpha\rfloor + 2$$

  since $\alpha > 1$ by Lemma 2.2.2.

□

We finally obtain:

Corollary 2.3.6. *Assume $m = 2$ and $\nu - x_1 > 1$. Let $x \in \mathcal{O}$. If $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X$.*

Proof. It is clear that if $x \in R_0 = \mathbb{Z}$, then $x \in X_0$. By Lemma 2.2.5, if $x \in R_1$, then $x \in X_0 = X_1$. By Lemma 2.3.5, if $x \in R_2$, then $x \in X_2$. By Lemma 2.2.9, for all $n \geq 3$, if $x \in R_n$, then $x \in X_n$. □

2.3.3 Case $m = 2$ and $\nu - x_1 < 1$

For all this section, we assume $m = 2$ and $\nu - x_1 < 1$. First we will characterize which pairs (ν, x_0) are involved. Then, in order to prove Theorem 2.1.3, we will have to consider separately a small set of exceptional pairs.

Characterization of the pairs (ν, x_0) involved.

Remark 2.3.7. *In case $x_0 = \nu^2 - \nu$ we have $x_1 = \nu$, hence the tower $\mathbb{Z}^{(\nu, \nu^2 - \nu)}$ is equivalent, in general, to the tower $\mathbb{Z}^{(\nu, \nu)}$.*

By above remark, in the following lemma we will not consider the case $x_0 = \nu^2 - \nu$.

Lemma 2.3.8. *The pairs (ν, x_0) that satisfy $\nu < x_0^2 - x_0$, $x_0 < \nu^2 - \nu$, $m = 2$ and $\nu - x_1 < 1$ are such that $\nu \in \{4, 6, 7, 8, 12\}$ and, given any such ν, x_0 ranges in $\{\nu^2 - 3\nu + 2, \dots, \nu^2 - \nu - 1\}$.*

Proof. The conditions $x_2 < \lfloor \alpha \rfloor + 1$ (coming from the hypothesis $m = 2$) and $\nu - x_1 < 1$ imply that

$$\nu - 1 < x_1 < (\lfloor \alpha \rfloor + 1)^2 - \nu \leq (\alpha + 1)^2 - \nu.$$

Consider the functions $f(\nu) = \nu - 1$ and $g(\nu) = (\alpha + 1)^2 - \nu$. We first characterize the values of ν for which $g(\nu) > f(\nu)$. We have

$$\begin{aligned}
g(\nu) > f(\nu) &\Leftrightarrow (\alpha + 1)^2 - \nu > \nu - 1 \\
&\Leftrightarrow \left(\frac{1 + \sqrt{1 + 4\nu}}{2} + 1 \right)^2 - \nu > \nu - 1 \\
&\Leftrightarrow \frac{1}{4} \left(3 + \sqrt{1 + 4\nu} \right)^2 - \nu > \nu - 1 \\
&\Leftrightarrow \frac{5}{2} + \frac{3}{2} \sqrt{1 + 4\nu} > \nu - 1 \\
&\Leftrightarrow \frac{3}{2} \sqrt{1 + 4\nu} > \nu - \frac{7}{2} \\
&\Leftrightarrow 3\sqrt{1 + 4\nu} > 2\nu - 7 \\
&\Leftrightarrow 9(1 + 4\nu) > 4\nu^2 - 28\nu + 49 \\
&\Leftrightarrow 0 > \nu^2 - 16\nu + 10 \\
&\Leftrightarrow 0 > \left(\nu - \left(8 - 3\sqrt{6} \right) \right) \left(\nu - \left(8 + 3\sqrt{6} \right) \right) \\
&\Leftrightarrow 8 - 3\sqrt{6} < \nu < 8 + 3\sqrt{6} \approx 13.34.
\end{aligned}$$

So we have $g(\nu) > f(\nu)$ if and only if $4 \leq \nu \leq 13$. In particular, recalling that $x_0 \leq \nu^2 - \nu$, we have $x_0 \leq 13^2 - 13 = 156$. So we are left with finitely many pairs to check. In the following table we put the pairs (ν, x_0) and why it does not satisfy the hypothesis.

ν	x_0	Satisfy	ν	x_0	Satisfy
4	$0, \ldots, 5$ $12, \ldots$	$\nu - x_1 \geq 1$ $x_0 \geq \nu^2 - \nu$	9	$0, \ldots, 55$ $56, \ldots, 71$ $72, \ldots$	$\nu - x_1 \geq 1$ $m \geq 3$ $x_0 \geq \nu^2 - \nu$
5	$0, \ldots, 11$ $12, \ldots, 19$ $20, \ldots$	$\nu - x_1 \geq 1$ $m \geq 3$ $x_0 \geq \nu^2 - \nu$	10	$0, \ldots, 70$ $71, \ldots, 90$ $91, \ldots$	$\nu - x_1 \geq 1$ $m \geq 3$ $x_0 \geq \nu^2 - \nu$
6	$0, \ldots, 19$ $30, \ldots$	$\nu - x_1 \geq 1$ $x_0 \geq \nu^2 - \nu$	11	$0, \ldots, 88$ $89, \ldots, 110$ $111, \ldots$	$\nu - x_1 \geq 1$ $m \geq 3$ $x_0 \geq \nu^2 - \nu$
7	$0, \ldots, 29$ $42, \ldots$	$\nu - x_1 \geq 1$ $x_0 \geq \nu^2 - \nu$	12	$0, \ldots, 109$ $132, \ldots$	$\nu - x_1 \geq 1$ $x_0 \geq \nu^2 - \nu$
8	$0, \ldots, 41$ $56, \ldots$	$\nu - x_1 \geq 1$ $x_0 \geq \nu^2 - \nu$	13	$0, \ldots, 130$ $131, \ldots, 156$ $157, \ldots$	$\nu - x_1 \geq 1$ $m \geq 3$ $x_0 \geq \nu^2 - \nu$

Table 2.1: Why the pairs (ν, x_0) do not satisfy the hypothesis of Lemma 2.3.8. Source: Own elaboration.

One easily verifies that the remaining pairs (ν, x_0) satisfy the hypothesis. They correspond to pairs such that $\nu \in \{4, 6, 7, 8, 12\}$ and, given any such ν, x_0 ranges in $\{\nu^2 - 3\nu + 2, \ldots, \nu^2 - \nu - 1\}$. In particular, there is no pair left with $\nu \in \{5, 9, 10, 11, 13\}$.

□

We will need to consider two cases:

- Generic Case: either $\nu \in \{4, 6, 7, 8, 12\}$ and, for each given ν,
$$x_0 \in \{\nu^2 - 3\nu + 2, \ldots, \nu^2 - \nu - 2\};$$
- Exceptional Case: $\nu \in \{4, 6, 8, 12\}$ and, for each given ν, $x_0 = \nu^2 - \nu - 1$ (we do not consider the pair $(7, 41)$ because the tower does not increase — we have indeed $R_1 = R_2$ in that case).

Generic case.

Assume that (ν, x_0) satisfy the condition of the Generic Case.

Remark 2.3.9. *Note that for any A and B positive real numbers, we have*

$$A \le x_0 \le B \Leftrightarrow \sqrt{\nu - \sqrt{\nu + B}} \le \sqrt{\nu - x_1} \le \sqrt{\nu - \sqrt{\nu + A}}.$$

Lemma 2.3.10. *If $x \in R_2$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then*

$$x \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 \pm x_2\}.$$

Proof. Let $x = a + bx_2 \in R_2$, where $a, b \in R_1$. If $0 \ll a + bx_2 \ll 2\lfloor\alpha\rfloor + 2$, then by Lemma 2.2.2 we have

$$0 \ll a \ll 2\lfloor\alpha\rfloor + 2$$

and

$$|b^\sigma| < \frac{\lfloor\alpha\rfloor + 1}{\sqrt{\nu - x_1}}.$$

By Lemma 2.2.5, we have $a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$. Write $b = b_1 + b_2 x_1$, with $b_1, b_2 \in \mathbb{Z}$. By Lemma 2.2.8, b_1 and b_2 have opposite sign.

Case 1: Assume $x_0 \in \{\nu^2 - 3\nu + 2, \ldots, \nu^2 - \nu - 3\}$, or $\nu = 4$ and $x_0 = \nu^2 - \nu - 2 = 10$. Suppose that $|b_1| \ge 1$ and $|b_2| \ge 1$. In both cases, we will use Lemma 2.2.7 in order to conclude that $b_1 = b_2 = 0$ if $a \ne \lfloor\alpha\rfloor + 1$, and that $b_2 = 0$ and $b_1 \in \{0, \pm 1\}$ if not.

Case 1a: Assume $a \in \{1, \ldots, \lfloor\alpha\rfloor\}$. If $b_1 < 0$, choose σ such that $x_1 \mapsto -x_1$, so that we have

$$x^\sigma = a + (b_1 + b_2 x_1^\sigma)\sqrt{\nu + x_1}^{\sigma} = a + (b_1 - b_2 x_1)\sqrt{\nu - x_1}.$$

If $b_1 > 0$, choose σ so that $\sigma(x_1) = -x_1$, and $\sigma(x_2) = -\sqrt{\nu - x_1}$. In that case, we have

$$x^\sigma = a + (b_1 + b_2 x_1^\sigma)\sqrt{\nu + x_1}^{\sigma} = a - (b_1 - b_2 x_1)\sqrt{\nu - x_1}.$$

Therefore, in both cases, there exists σ such that:

$$x^\sigma = a - (|b_1| + |b_2| x_1)\sqrt{\nu - x_1}.$$

If $(\nu, x_0) = (4, 10)$, then we have

$$x^\sigma = a - (|b_1| + |b_2| x_1)\sqrt{\nu - x_1} \le \lfloor\alpha\rfloor - (1 + x_1)\sqrt{\nu - x_1},$$

and the latter can be checked to be negative, and otherwise, using Remark 2.3.9, we have

$$\begin{aligned} x^\sigma &= a - (|b_1| + |b_2| x_1)\sqrt{\nu - x_1} \\ &\le \lfloor\alpha\rfloor - (1 + x_1)\sqrt{\nu - x_1} \\ &\le \lfloor\alpha\rfloor - (1 + \sqrt{\nu^2 - 2\nu + 2})\sqrt{\nu - \sqrt{\nu^2 - 3}}, \end{aligned}$$

and again one can check that the latter is negative. So in both cases we have $b_1 = b_2 = 0$ by Lemma 2.2.7.

Case 1b: Assume $a \in \{\lfloor\alpha\rfloor + 2, \dots, 2\lfloor\alpha\rfloor + 1\}$. We proceed in a way similar to Case 1a, choosing σ such that

$$x^\sigma = a + (|b_1| + |b_2|x_1)\sqrt{\nu - x_1}.$$

If $(\nu, x_0) = (4, 10)$, then

$$x^\sigma \geq \lfloor\alpha\rfloor + 2 + (1 + x_1)\sqrt{\nu - x_1},$$

which can be checked to be greater than $2\lfloor\alpha\rfloor + 2$. Otherwise, using Remark 2.3.9, we obtain

$$\begin{aligned} x^\sigma &= a + (|b_1| + |b_2|x_1)\sqrt{\nu - x_1} \\ &\geq \lfloor\alpha\rfloor + 2 + (1 + x_1)\sqrt{\nu - x_1} \\ &\geq \lfloor\alpha\rfloor + 2 + (1 + \sqrt{\nu^2 - 2\nu + 2})\sqrt{\nu - \sqrt{\nu^2 - 3}}, \end{aligned}$$

which is again greater than $2\lfloor\alpha\rfloor + 2$. Hence $b_1 = b_2 = 0$ by Lemma 2.2.7.

Case 1c: Assume $a = \lfloor\alpha\rfloor + 1$. As before, choose σ such that $x^\sigma = \lfloor\alpha\rfloor + 1 - (|b_1| + |b_2|x_1)\sqrt{\nu - x_1}$. So we have

$$x^\sigma = a - (|b_1| + |b_2|x_1)\sqrt{\nu - x_1} \leq \lfloor\alpha\rfloor + 1 - (1 + x_1)\sqrt{\nu - x_1}.$$

This is negative in the following cases:

- $\nu = 4$ and $x_0 \in \{6, 7, 8\}$,
- $\nu = 6$ and $x_0 \in \{20, \dots, 26\}$,
- $\nu = 7$ and $x_0 \in \{30, \dots, 38\}$,
- $\nu = 8$ and $x_0 \in \{42, \dots, 52\}$ or
- $\nu = 12$ and $x_0 \in \{110, \dots, 128\}$,

so in these cases, we have $b_1 = b_2 = 0$. For the remaining cases, some conjugates are outside the interval.

- When $\nu = 4$ and $x_0 = 9$ we have $a = \lfloor\alpha\rfloor + 1 = 3$. By Lemma 2.2.2 we have

  $$|b^\sigma| \leq \frac{\lfloor\alpha\rfloor + 1}{\sqrt{\nu - x_1}} \approx 4.78 < 5,$$

  hence $0 \ll b + 5 \ll 10$. Write $b = b_1 + b_2x_1$, with $b_1, b_2 \in \mathbb{Z}$. By Lemma 2.2.2 we have

  $$b_1 \in \{-4, \dots, 4\}$$

  and

  $$|b_2| \leq \frac{5}{x_1} \approx 1.38,$$

  and since $b_2 \in \mathbb{Z}$ we deduce $b_2 \in \{-1, 0, 1\}$.

Using Lemma 2.2.2 in the same way, we obtain the following for some of the other pairs (ν, x_0).

Next, we need to do a case by case analysis. We consider $x = \lfloor\alpha\rfloor + 1 + (b_1 + b_2x_1)x_2$, where $b_1, b_2 \in \mathbb{Z}$ and the following embeddings:

$$\begin{aligned} \sigma_1(x) &= \lfloor\alpha\rfloor + 1 + (b_1 + b_2x_1)x_2 \\ \sigma_2(x) &= \lfloor\alpha\rfloor + 1 + (b_1 - b_2x_1)\sqrt{\nu - x_1} \\ \sigma_3(x) &= \lfloor\alpha\rfloor + 1 - (b_1 + b_2x_1)x_2 \\ \sigma_4(x) &= \lfloor\alpha\rfloor + 1 - (b_1 - b_2x_1)\sqrt{\nu - x_1} \end{aligned}$$

(ν, x_0)	$a = \lfloor\alpha\rfloor + 1$	b_1	b_2
$(4, 10)$	3	$-5, \dots, 5$	$-1, 0, 1$
$(6, 27)$	4	$-7, \dots, 7$	$-1, 0, 1$
$(7, 39)$	4	$-8, \dots, 8$	$-1, 0, 1$
$(8, 53)$	4	$-9, \dots, 9$	$-1, 0, 1$
$(12, 129)$	5	$-14, \dots, 14$	$-1, 0, 1$

Table 2.2: Possible values of b_1 and b_2 in Case 1c, proof of Lemma 2.3.10. Source: Own elaboration.

b_2	b_1	$\sigma_i < 0$	b_2	b_1	$\sigma_i < 0$	b_2	b_1	$\sigma_i < 0$
$\nu = 4, x_0 = 9$			$\nu = 4, x_0 = 10$			$\nu = 6, x_0 = 27$		
-1	≤ 2	σ_1	-1	≤ 2	σ_1	-1	≤ 4	σ_1
-1	≥ 3	σ_4	-1	≥ 3	σ_4	-1	≥ 5	σ_4
0	≤ -2	σ_1	0	≤ -2	σ_1	0	≤ -2	σ_1
0	≥ 2	σ_3	0	≥ 2	σ_3	0	≥ 2	σ_3
1	≤ -2	σ_2	1	≤ -3	σ_2	1	≤ -3	σ_2
1	≥ -1	σ_3	1	≥ -2	σ_3	1	≥ -2	σ_3
$\nu = 7, x_0 = 39$			$\nu = 8, x_0 = 53$			$\nu = 12, x_0 = 129$		
-1	≤ 5	σ_1	-1	≤ 6	σ_1	-1	≤ 10	σ_1
-1	≥ 6	σ_4	-1	≥ 7	σ_4	-1	≥ 11	σ_4
0	≤ -2	σ_1	0	≤ -2	σ_1	0	≤ -2	σ_1
0	≥ 2	σ_3	0	≥ 2	σ_3	0	≥ 2	σ_3
1	≤ -2	σ_2	1	≤ -2	σ_2	1	≤ -3	σ_2
1	≥ -1	σ_3	1	≥ -1	σ_3	1	≥ -2	σ_3

Table 2.3: An embedding σ such that $\sigma(x) \leq 0$ in Case 1c, proof of Lemma 2.3.10. Source: Own elaboration.

In all cases there exists an embedding σ such that $\sigma(x) \leq 0$ or $\sigma(x) \geq 2\lfloor\alpha\rfloor + 2$. For example, the following table shows, for each pair (ν, x_0), an embedding σ such that $\sigma(x) \leq 0$.

Case 2: Assume $x_0 = \nu^2 - \nu - 2$ and $\nu \in \{6, 7, 8, 12\}$. Proceeding as before, by Lemma 2.2.2 we have:

(ν, x_0)	a	b_1	b_2
$(6, 28)$	$1, \dots, 7$	$-9, \dots, 9$	$-1, 0, 1$
$(7, 40)$	$1, \dots, 7$	$-10, \dots, 10$	$-1, 0, 1$
$(8, 54)$	$1, \dots, 7$	$-11, \dots, 11$	$-1, 0, 1$
$(12, 130)$	$1, \dots, 9$	$-17, \dots, 17$	$-1, 0, 1$

Table 2.4: Possible values of b_1 and b_2 in Case 2, proof of Lemma 2.3.10. Source: Own elaboration.

In all cases there exists an embedding σ such that $\sigma(x) \leq 0$ or $\sigma(x) \geq 2\lfloor\alpha\rfloor + 2$. For example, when $\nu = 6$ and $x_0 = 28$, the following table shows the embeddings σ_i such that $\sigma(x) \leq 0$ for the values of a, b_1 and b_2 that are indicated.

Similarly, for $a \geq 5$, the following table shows the embedding σ such that $\sigma(x) \geq 2\lfloor\alpha\rfloor + 2$.

We leave to the reader checking what happens with the other values of ν and x_0: the verifications are tedious, but easily done using any computer algebra system (more or less the same program may be used to various situations below). □

a	b_2	b_1	σ_i	a	b_2	b_1	σ_i
1	-1	≤ 5	σ_1	2	-1	≤ 5	σ_1
1	-1	≥ 6	σ_4	2	-1	≥ 6	σ_4
1	0	≤ -1	σ_1	2	0	≤ -1	σ_1
1	0	≥ 1	σ_3	2	0	≥ 1	σ_3
1	1	≤ 3	σ_2	2	1	≤ 0	σ_2
1	1	≥ 4	σ_3	2	1	≥ 1	σ_3
3	-1	≤ 4	σ_1	4	-1	≤ 4	σ_1
3	-1	≥ 5	σ_4	4	-1	≥ 5	σ_4
3	0	≤ -1	σ_1	4	0	≤ -2	σ_1
3	0	≥ 1	σ_3	4	0	≥ 2	σ_3
3	1	≤ -2	σ_2	4	1	≤ -4	σ_2
3	1	≥ -1	σ_3	4	1	≥ -3	σ_3

Table 2.5: Embeddings σ_i such that $\sigma_i(x) \leq 0$ in Case 2, proof of Lemma 2.3.10. Source: Own elaboration.

a	b_2	b_1	σ_i	a	b_2	b_1	σ_i	a	b_2	b_1	σ_i
5	-1	≤ 4	σ_3	6	-1	≤ 5	σ_3	7	-1	≤ 5	σ_3
5	-1	≥ 5	σ_2	6	-1	≥ 6	σ_2	7	-1	≥ 6	σ_2
5	0	≤ -1	σ_3	6	0	≤ -1	σ_3	7	0	≤ -1	σ_3
5	0	≥ 1	σ_1	6	0	≥ 1	σ_1	7	0	≥ 1	σ_1
5	1	≤ -2	σ_4	6	1	≤ 0	σ_4	7	1	≤ 3	σ_4
5	1	≥ -1	σ_1	6	1	≥ 1	σ_1	7	1	≥ 4	σ_1

Table 2.6: Embeddings σ such that $\sigma(x) \geq 2\lfloor\alpha\rfloor + 2$ in Case 2, proof of Lemma 2.3.10. Source: Own elaboration.

Lemma 2.3.11. *If $x \in \mathcal{O}$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X$.*

Proof. Let $x \in \mathcal{O}$ be such that $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$. If $x \in R_0 = \mathbb{Z}$, then it is clear that $x \in X_0$. By Lemma 2.2.5, if $x \in R_1$, then $x \in X_1$. By Lemma 2.3.10, if $x \in R_2$, then $x \in X_2$. By Lemma 2.2.9, for all $n \geq 3$, if $x \in R_n$, then $x \in X_n$. □

Exceptional cases.

Assume $(\nu, x_0) \in C = \{(\nu, \nu^2 - \nu - 1) \colon \nu = 4, 6, 8, 12\}$. In this case, we have $m = 2$ and $\nu - x_1 < 1$.

Lemma 2.3.12. *If $x \in R_2$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X_2$.*

Proof. Let $x = a + bx_2 \in R_2$, where $a, b \in R_1$. As before, if $0 \ll a + bx_2 \ll 2\lfloor\alpha\rfloor + 2$, then by Lemma 2.2.2 we have

$$0 \ll a \ll 2\lfloor\alpha\rfloor + 2$$

and

$$|b^\sigma| < \frac{\lfloor\alpha\rfloor + 1}{\sqrt{\nu - x_1}}.$$

By Lemma 2.2.5, we have $a \in \{1, \ldots, 2\lfloor\alpha\rfloor + 1\}$. Write $b = b_1 + b_2 x_1$, with $b_1, b_2 \in \mathbb{Z}$. As in the previous section, the following table summarizes the possible values of b_1 and b_2.

(ν, x_0)	a	b_1	b_2
$(4, 11)$	$1, \dots, 5$	$-8, \dots, 8$	$-2, \dots, 2$
$(6, 29)$	$1, \dots, 7$	$-13, \dots, 13$	$-2, \dots, 2$
$(8, 55)$	$1, \dots, 7$	$-15, \dots, 15$	$-2, \dots, 2$
$(12, 131)$	$1, \dots, 9$	$-24, \dots, 24$	$-2, \dots, 2$

Table 2.7: Possible values of b_1 and b_2 in the proof of Lemma 2.3.12. Source: Own elaboration.

We leave to the reader to finish the proof of the lemma, as again it is an easy but lengthy case by case analysis. □

For proving Lemmas 2.3.13 and 2.3.14, we need the approximate values of

1. $|\nu - 1 - x_1| x_2 \alpha$,
2. $|\nu + 1 - x_1| x_2 \alpha$,
3. $|\nu + x_1| \sqrt{\nu - x_1} \sqrt{\nu + \sqrt{\nu - x_1}}$,
4. $\lfloor\alpha\rfloor + 1 + (\nu + x_1)\sqrt{\nu - x_1} + \sqrt{\nu - \sqrt{\nu - x_1}}$,
5. $\lfloor\alpha\rfloor + 1 + (\nu + x_1)\sqrt{\nu - x_1} + \sqrt{\nu + \sqrt{\nu - x_1}}$ and
6. $\lfloor\alpha\rfloor + 1 - (\nu - x_1)x_2 + \alpha^2$.
7. $\lfloor\alpha\rfloor + 1 + (\nu - x_1)x_2 + \alpha^2$

These aproximate values are in the following table:

(ν, x_0)	$2\lfloor\alpha\rfloor + 2$	(1)	(2)	(3)	(4)	(5)	(6)	(7)
$(4, 11)$	6	6.27	8.10	5.86	7.71	7.89	9.21	9.91
$(6, 29)$	8	9.49	11.22	8.66	9.84	9.96	12.71	13.29
$(8, 55)$	8	12.62	14.30	11.47	10.78	10.86	15.12	15.62
$(12, 131)$	10	18.76	20.39	17.10	13.33	13.39	20.80	21.20

Table 2.8: Approximate values of certain expressions used in the proof of Lemma 2.3.13. Source: Own elaboration.

Lemma 2.3.13. *If $x \in R_3$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X_2 \cup \{\lfloor\alpha\rfloor + 1 \pm x_3\}$.*

Proof. Let $x = a + bx_3$ where $a, b \in R_2$. By Lemma 2.2.2, since $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, we have $0 \ll a \ll 2\lfloor\alpha\rfloor + 2$ and $|b^\sigma| < \frac{\lfloor\alpha\rfloor+1}{\sqrt{\nu-x_2}} < \lfloor\alpha\rfloor + 1$ (because $\sqrt{\nu - x_2} > 1$), that is $0 \ll b + \lfloor\alpha\rfloor + 1 \ll 2\lfloor\alpha\rfloor + 2$. By Lemma 2.3.12 we have

$$a \in \{1, \dots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 \pm x_2\} \cup \{\lfloor\alpha\rfloor + 1 \pm (\beta - x_1)x_2 \colon \beta \in B\}$$

and

$$b \in \{-\lfloor\alpha\rfloor, \dots, \lfloor\alpha\rfloor\} \cup \{\pm x_2\} \cup \{\pm(\beta - x_1)x_2 \colon \beta \in B\},$$

where

$$B = \begin{cases} \{\nu - 1, \nu\}, & \text{if } \nu \in \{4, 8, 12\} \\ \{5, 6, 7\}, & \text{if } \nu = 6. \end{cases}$$

Fact 1. We have $b \notin \{\pm(\beta - x_1)x_2 \colon \beta \in B\}$.

Suppose that $b \in A = \{(\nu \pm 1 - x_1)x_2, -(\nu \pm 1 - x_1)x_2\}$. There exists σ such that $x_1^\sigma = x_1$, $x_2^\sigma = x_2$ and

$$x_3^\sigma = \begin{cases} x_3 & \text{if } b > 0 \\ -x_3 & \text{if } b < 0. \end{cases}$$

Hence

$$x^\sigma = a + |\nu \pm 1 - x_1| x_2 x_3.$$

Since $x_3 > \alpha$, by Table 2.8 we have $|\nu \pm 1 - x_1|x_2x_3 > 2\lfloor\alpha\rfloor + 2$. Since $a > 0$, we have $x^\sigma > 2\lfloor\alpha\rfloor + 2$, so that $b \notin A$.

Suppose that $b = \pm(\nu - x_1)x_2$ and consider σ such that $x_1^\sigma = -x_1$, $x_2^\sigma = \sqrt{\nu - x_1}$ and

$$x_3^\sigma = \begin{cases} \sqrt{\nu + \sqrt{\nu - x_1}} & \text{if } b = (\nu - x_1)x_2 \\ -\sqrt{\nu + \sqrt{\nu - x_1}} & \text{if } b = -(\nu - x_1)x_2. \end{cases}$$

So

$$(bx_3)^\sigma = (\nu + x_1)\sqrt{\nu - x_1}\sqrt{\nu + \sqrt{\nu - x_1}}.$$

When $\nu = 4$ and $x_0 = 11$ we have that $(bx_3)^\sigma$ is > 5.8. Moreover, if $a \in \{1, 2, 3, 4, 5\} \cup \{3 \pm x_2, 3 \pm (3 - x_1)x_2, 3 \pm (4 - x_1)x_2\}$, then $a^\sigma \geq 1$, hence

$$(a + bx_3)^\sigma > 1 + 5.8 > 2\lfloor\alpha\rfloor + 2.$$

For $\nu \in \{6, 8, 12\}$ we have $(bx_3)^\sigma > 2\lfloor\alpha\rfloor + 2$ (see Table 2.8), so that $b \neq \pm(\nu - x_1)x_2$.

Fact 2. If $a \in \{1, \ldots, \lfloor\alpha\rfloor\} \cup \{\lfloor\alpha\rfloor + 1 - x_2\} \cup \{\lfloor\alpha\rfloor + 1 \pm (\nu \mp 1 - x_1)x_2\}$, then $b = 0$.

In this case we have $a \leq \lfloor\alpha\rfloor$. When $b \in \{-\lfloor\alpha\rfloor, \ldots, \lfloor\alpha\rfloor\} \cup \{\pm x_2\}$ we have $|b| \geq 1$. We can choose σ such that $(a + bx_3)^\sigma = a - |b|x_3$. Since $x_3 > \alpha$, we have

$$(a + bx_3)^\sigma = a - |b|x_3 \leq \lfloor\alpha\rfloor - \alpha < 0.$$

This is a contradiction, so that $b = 0$.

Fact 3. If $a \in \{\lfloor\alpha\rfloor + 2, \ldots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 + x_2\} \cup \{\lfloor\alpha\rfloor + 1 \pm (\nu \pm 1 - x_1)x_2\}$, then $b = 0$.

In this case $a \geq \lfloor\alpha\rfloor + 2$. When $b \in \{-\lfloor\alpha\rfloor, \ldots, \lfloor\alpha\rfloor\} \cup \{\pm x_2\}$ we have $|b| \geq 1$. We can choose σ such that $(a + bx_3)^\sigma = a + |b|x_3$. Since $x_3 > \alpha$, we have

$$(a + bx_3)^\sigma = a + |b|x_3 \geq \lfloor\alpha\rfloor + 2 + x_3 > 2\lfloor\alpha\rfloor + 2.$$

This is a contradiction, so that $b = 0$.

Fact 4. If $a = \lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2$, then $b = 0$.

If $b \in \{-\lfloor\alpha\rfloor, \ldots, \lfloor\alpha\rfloor\}$, then assuming $b \neq 0$, we have $b \geq 1$. We can choose σ such that

$$(\lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + bx_3)^\sigma = \lfloor\alpha\rfloor + 1 + (\nu + x_1)\sqrt{\nu - x_1} + |b|\sqrt{\nu \pm \sqrt{\nu - x_1}},$$

that is greater than $2\lfloor\alpha\rfloor + 2$ by Table 2.8. So that $b = 0$.

If $b \in \{\pm x_2\}$, then we can choose σ such that

$$(\lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + bx_3)^\sigma = \lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + x_2x_3 > \lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + \alpha^2$$

and the latter is greater than $2\lfloor\alpha\rfloor + 2$ in all cases (see Table 2.8), so that $b = 0$.

Fact 5. If $a = \lfloor\alpha\rfloor + 1$, then $b \in \{-1, 0, 1\}$.
Suppose that $|b| \geq 2$ (note that $x_2 > 2$), there exists σ such that

$$(\lfloor\alpha\rfloor + 1 + bx_3)^\sigma = \lfloor\alpha\rfloor + 1 + |b|x_3 > \lfloor\alpha\rfloor + 1 + 2\alpha \geq 2\lfloor\alpha\rfloor + 2,$$

so that $b \in \{-1, 0, 1\}$

□

Lemma 2.3.14. *For $n \geq 3$, if $x \in R_n$ satisfies $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then $x \in X$.*

Proof. The proof is by induction on n. The case $n = 3$ holds by Lemma 2.3.13. Assume $n \geq 4$ and suppose that for all $x \in R_n$, if $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$, then

$$x \in X_2 \cup \{\lfloor\alpha\rfloor + 1 \pm x_k \colon k = 3, \dots, n\}.$$

Let $x \in R_{n+1}$ be such that $0 \ll x \ll 2\lfloor\alpha\rfloor + 2$. Write $x = a + bx_{n+1}$, with $a, b \in R_n$. By Lemma 2.2.2 and by induction hypothesis we have: $a \in X_n$ and $b + \lfloor\alpha\rfloor + 1 \in X_n$, that is

$$a \in \{1, \dots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor \pm x_k \colon k = 2, \dots, n\} \cup \{\lfloor\alpha\rfloor + 1 \pm (\beta - x_1)x_2 \colon \beta \in B\}$$

and

$$b \in \{-\lfloor\alpha\rfloor, \dots, \lfloor\alpha\rfloor\} \cup \{\pm x_k \colon k = 2, \dots, n\} \cup \{\pm(\beta - x_1)x_2 \colon \beta \in B\},$$

where

$$B = \begin{cases} \{\nu - 1, \nu\} & \text{, if } \nu \in \{4, 8, 12\} \\ \{5, 6, 7\} & \text{, if } \nu = 6. \end{cases}$$

Fact 1. We have $b \notin \{\pm(\beta - x_1)x_2 : \beta \in B\}$. Suppose that $b \in A = \{(\nu \pm 1 - x_1)x_2, -(\nu \pm 1 - x_1)x_2\}$. There exists σ such that $x_j^\sigma = x_j$ for $j = 1, \dots, n$ and

$$x_{n+1}^\sigma = \begin{cases} x_{n+1} & \text{if } b > 0 \\ -x_{n+1} & \text{if } b < 0. \end{cases}$$

Hence

$$x^\sigma = a^\sigma + |\nu \pm 1 - x_1|x_2x_{n+1} > a^\sigma + |\nu \pm 1 - x_1|x_2\alpha.$$

By Table 2.8 we have $|\nu \pm 1 - x_1|x_2\alpha > 2\lfloor\alpha\rfloor + 2$. Since $a^\sigma > 0$, we have $x^\sigma > 2\lfloor\alpha\rfloor + 2$, so that $b \notin A$.

Suppose that $b = \pm(\nu - x_1)x_2$ and consider σ such that $x_1^\sigma = -x_1$, $x_2^\sigma = \sqrt{\nu - x_1}$ and

$$x_{n+1}^\sigma = \begin{cases} \sqrt{\nu + \sqrt{\nu + \dots \sqrt{\nu - x_1}}} & \text{if } b = (\nu - x_1)x_2 \\ -\sqrt{\nu + \sqrt{\nu + \dots \sqrt{\nu - x_1}}} & \text{if } b = -(\nu - x_1)x_2 \end{cases}$$

(the choice for x_j^σ, for $j = 3, \dots, n$, is not relevant). So

$$\begin{aligned} x^\sigma &= a^\sigma + (\nu + x_1)\sqrt{\nu - x_1}\sqrt{\nu + \sqrt{\nu + \dots + \sqrt{\nu - x_1}}} \\ &> a^\sigma + (\nu + x_1)\sqrt{\nu - x_1}\sqrt{\nu + \sqrt{\nu - x_1}}, \end{aligned}$$

that is greater than $2\lfloor\alpha\rfloor + 2$ by the proof of Fact 1 of Lemma 2.3.13, so that $b \neq \pm(\nu - x_1)x_2$.

Fact 2. If $a \in \{1, \dots, \lfloor\alpha\rfloor\} \cup \{\lfloor\alpha\rfloor + 1 - x_k \colon k = 2, \dots, n\} \cup \{\lfloor\alpha\rfloor + 1 \pm (\nu \mp 1 - x_1)x_2\}$, *then* $b = 0$.

In this case we have $a \leq \lfloor\alpha\rfloor$. When $b \in \{-\lfloor\alpha\rfloor, \dots, \lfloor\alpha\rfloor\} \cup \{\pm x_k \colon 2, \dots, n\}$ we have $|b| \geq 1$. We can choose σ such that $(a + bx_{n+1})^\sigma = a - |b|x_{n+1}$. Since $x_{n+1} > \alpha$, we have

$$(a + bx_{n+1})^\sigma = a - |b|x_{n+1} \leq \lfloor\alpha\rfloor - \alpha < 0.$$

This is a contradiction, so that $b = 0$.

Fact 3. If $a \in \{\lfloor\alpha\rfloor + 2, \dots, 2\lfloor\alpha\rfloor + 1\} \cup \{\lfloor\alpha\rfloor + 1 + x_k \colon k = 2, \dots, n\} \cup \{\lfloor\alpha\rfloor + 1 \pm (\nu \pm 1 - x_1)x_2\}$, *then* $b = 0$.

In this case $a \geq \lfloor\alpha\rfloor + 2$. When $b \in \{-2\lfloor\alpha\rfloor - 1, \dots, 2\lfloor\alpha\rfloor + 1\} \cup \{\pm x_k \colon k = 2, \dots, n\}$ we have $|b| \geq 1$. We can choose σ such that $(a + bx_{n+1})^\sigma = a + |b|x_{n+1}$. Since $x_{n+1} > \alpha$, we have

$$(a + bx_{n+1})^\sigma = a + |b|x_{n+1} \geq \lfloor\alpha\rfloor + 2 + x_{n+1} > 2\lfloor\alpha\rfloor + 2.$$

This is a contradiction, so that $b = 0$.

Fact 4. If $a = \lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2$, *then* $b = 0$.

If $b \in \{-\lfloor\alpha\rfloor, \dots, \lfloor\alpha\rfloor\}$, then $b^\sigma \geq 1$. We can choose σ such that

$$\begin{aligned} &(\lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + bx_{n+1})^\sigma = \\ &\qquad \lfloor\alpha\rfloor + 1 + (\nu + x_1)\sqrt{\nu - x_1} + |b|\sqrt{\nu + \dots \sqrt{\nu + \sqrt{\nu \pm \sqrt{\nu - x_1}}}} \\ &\qquad\qquad \geq \lfloor\alpha\rfloor + 1 + (\nu + x_1)\sqrt{\nu - x_1} + \sqrt{\nu \pm \sqrt{\nu - x_1}}, \end{aligned}$$

that is greater than $2\lfloor\alpha\rfloor + 2$ by Table 2.8, so that $b = 0$.

If $b \in \{\pm x_k \colon k = 2, \dots, n\}$, then we can choose σ such that

$$\begin{aligned} (\lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + bx_{n+1})^\sigma &= \lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + x_k x_{n+1} \\ &> \lfloor\alpha\rfloor + 1 \pm (\nu - x_1)x_2 + \alpha^2 \end{aligned}$$

and the latter is greater than $2\lfloor\alpha\rfloor + 2$ in all cases (see Table 2.8), so that $b = 0$.

Fact 5. If $a = \lfloor\alpha\rfloor + 1$, *then* $b \in \{-1, 0, 1\}$.

Suppose that $|b| \geq 2$ (note that $x_2 > 2$), there exists σ such that

$$(\lfloor\alpha\rfloor + 1 + bx_{n+1})^\sigma = \lfloor\alpha\rfloor + 1 + |b|x_{n+1} > \lfloor\alpha\rfloor + 1 + 2\alpha \geq 2\lfloor\alpha\rfloor + 2,$$

so that $b \in \{-1, 0, 1\}$

□

Let us conclude with a question that we were not able to answer:

Question 2.3.15. *Given* $x_0 \in \{0, 2, 3, 4\}$, *what is the* JR-*number of* $\mathbb{Z}^{(3, x_0)}$*?*

Chapter 3

Monogenity

3.1 Introduction

In this chapter, for each $n \geq 0$, P_n will denote the minimal polynomial of x_n over $\mathbb{Q}$.

We will prove in Section 3.3 the following theorem.

Theorem 3.1.1 (Main Theorem 2)**.** *Assume that $\nu + x_0$ is congruent to 2 or 3 modulo 4 and is square-free. The ring $\mathbb{Z}^{(\nu,x_0)}$ is the ring of integers of its fraction field if and only if $P_n(0)$ is square-free for all $n \geq 1$.*

As we will see, the condition on $\nu + x_0$ cannot be dropped, because it is well known that for square-free $\nu + x_0$, $\mathbb{Z}[x_1] = \mathcal{O}_{\mathbb{Q}(x_1)}$ if and only if $\nu + x_0$ is congruent to 2 or 3 modulo 4, and because of the following proposition, which will be proven at the end of Section 3.3.

Proposition 3.1.2. *If $\mathbb{Z}[x_n] = \mathcal{O}_{\mathbb{Q}(x_n)}$ for some $n \geq 2$, then also $\mathbb{Z}[x_{n-1}] = \mathcal{O}_{\mathbb{Q}(x_{n-1})}$.*

Hence for all this chapter we assume the following:

Assumption 3.1.3. *The integer $\nu + x_0$ is square-free and congruent to 2 or 3 modulo 4.*

For example, when $(\nu, x_0) = (2, 0)$, we have $P_n(0) = 2$ for all $n \geq 1$ (hence, $P_n(0)$ is square-free for all $n \geq 1$). By Theorem 3.1.1, the infinite tower

$$\mathbb{Z} \subset \mathbb{Z}\left[\sqrt{2}\right] \subset \mathbb{Z}\left[\sqrt{2+\sqrt{2}}\right] \subset \dots$$

is the ring of integers of its fraction field — this is a special case of a theorem by Liang [Li76].

Assuming $x_0 = 0$, we computed $P_n(0)$ for n from 1 to 6 and for ν up to 100. Considering only the values of ν which are square-free and congruent to 2 or 3 modulo 4, in the following table, an X in the cell (ν, n) means that $P_k(0)$ is square-free for k up to n.

Assuming $x_0 = 0$, we show in Section 3.4.1 that under the ABC-Conjecture, there are infinitely many ν for which $P_n(0)$ is square-free for every $n \geq 1$.

3.2 Discriminant of x_n.

In this section, we will prove the following result.

Proposition 3.2.1. *Assume that $\mathbb{Q}(x_n)$ has degree 2^n over $\mathbb{Q}$. We have*

$$\text{disc}\,(x_0) = 1 \textit{ and } \text{disc}\,(x_1) = 2^2(\nu + x_0),$$

ν	$n=1$	$n=2$	$n=6$	ν	$n=1$	$n=2$	$n=6$
3			X	47			X
6			X	51	X		
7			X	55	X		
10	X			58			X
11			X	59		X	
14			X	62			X
15			X	66			X
19	X			67			X
21	X			70			X
22			X	71			X
23			X	74			X
26	X			78			X
30			X	79			X
31			X	82	X		
34		X		83			X
35			X	86			X
38			X	87			X
39			X	91	X		
42			X	94			X
43			X	95		X	
46	X						

Table 3.1: Values of n such that $P_k(0)$ is square-free for k up to n. Source: Own elaboration.

and for $n \geq 2$ we have

$$\operatorname{disc}(x_n) = (\operatorname{disc}(x_{n-1}))^2 \cdot 2^{2^n} P_n(0).$$

In our situation, the assumption that $\mathbb{Q}(x_n)$ has degree 2^n over $\mathbb{Q}$ will be fulfilled for instance when $\nu + x_0$ is congruent to 2 or 3 modulo 4 — see [VV15, Prop. 2.15]. Under this assumption, $\mathbb{Q}(x_n)$ has basis

$$B_n := \{1, x_n, x_n^2, \ldots, x_n^{2^n-1}\}$$

over $\mathbb{Q}$. Note that the field extension $\mathbb{Q}(x_n)/\mathbb{Q}(x_m)$ has degree 2^{n-m}. We will denote by $\operatorname{disc}{}^{\,n}_{\,n-1}(x_n)$ the discriminant of x_n from $\mathbb{Q}(x_n)$ to $\mathbb{Q}(x_{n-1})$. Hence, for $n \geq 1$, we have

$$\operatorname{disc}{}^{\,n}_{\,n-1}(x_n) = \begin{vmatrix} 1 & x_n \\ 1 & -x_n \end{vmatrix}^2 = 4(x_n)^2 = 4(\nu + x_{n-1}).$$

Notation 3.2.2. *For $n \geq 1$, we denote by N_n the norm from $\mathbb{Q}(x_n)$ to $\mathbb{Q}$ of $\operatorname{disc}{}^{\,n+1}_{\,n}(x_{n+1})$, and by N_0 the discriminant of x_1 from $\mathbb{Q}(x_1)$ to $\mathbb{Q}$.*

Proposition 3.2.3. *We have*

1. *$N_0 = 2^2(\nu + x_0)$, and*

2. *$N_n = 2^{2^{n+1}} P_{n+1}(0)$ for any $n \geq 1$.*

Proof. Item 1 is immediate from our above computation, so we prove item 2. Let $\ell_1 = \nu^2$ and

$\ell_n = ((\ell_{n-1}) - \nu)^2$ for $n \geq 2$. Let $n \geq 1$. We have

$$\begin{aligned} N_n &= \operatorname{Norm}_{\mathbb{Q}}^{\mathbb{Q}(x_n)}\left(\operatorname{disc}{}_n^{n+1}(x_{n+1})\right) \\ &= \operatorname{Norm}_{\mathbb{Q}}^{\mathbb{Q}(x_n)}(4(\nu + x_n)) \\ &= (2^2)^{2^n}\operatorname{Norm}_{\mathbb{Q}}^{\mathbb{Q}(x_n)}(\nu + x_n) \\ &= 2^{2^{n+1}}\prod_{i=1}^{2^n}(\nu + x_n^{\sigma_i^n}), \end{aligned}$$

where the σ_i^n are the 2^n embeddings from $\mathbb{Q}(x_n)$ to $\mathbb{C}$.

Fact. *For all $t \in \{0, \ldots, n\}$ we have*

$$\prod_{i=1}^{2^n}\left(\nu + x_n^{\sigma_i^{n-1}}\right) = \prod_{i=1}^{2^{n-t}}\left(\ell_t - (\nu + x_{n-t})^{\sigma_i^{n-t}}\right).$$

We prove the fact by induction on t. Assume it is true for $t-1$, namely,

$$\prod_{i=1}^{2^n}\left(\nu + x_n^{\sigma_i^{n-1}}\right) = \prod_{i=1}^{2^{n-(t-1)}}\left(\ell_{t-1} - (\nu - x_{n-(t-1)})^{\sigma_i^{n-(t-1)}}\right),$$

we have

$$\begin{aligned} \prod_{i=1}^{2^n}\left(\nu + x_n^{\sigma_i^{n-1}}\right) &= \prod_{i=1}^{2^{n-t+1}}\left(\ell_{t-1} - (\nu - x_{n-t+1})^{\sigma_i^{n-t+1}}\right) \\ &= \prod_{i=1}^{2^{n-t+1}}\left((\ell_{t-1} - \nu) + x_{n-t+1}^{\sigma_i^{n-t+1}}\right) \\ &= \prod_{i=1}^{2^{n-t}}\left((\ell_{t-1} - \nu) - x_{n-t+1}^{\sigma_i^{n-t}}\right)\left((\ell_{t-1} - \nu) + x_{n-t+1}^{\sigma_i^{n-t}}\right) \\ &= \prod_{i=1}^{2^{n-t}}\left((\ell_{t-1} - \nu)^2 - (x_{n-t+1}^2)^{\sigma_i^{n-t}}\right) \\ &= \prod_{i=1}^{2^{n-t}}\left(\ell_t - (\nu + x_{n-t})^{\sigma_i^{n-t}}\right). \end{aligned}$$

This proves the fact.

Hence, taking $t = n$ in the Fact above, we obtain

$$\prod_{i=1}^{2^n}\left(\nu + x_n^{\sigma_i^{n-1}}\right) = (\ell_n - (\nu + x_0)) = P_{n+1}(0).$$

□

We need the following proposition — see [Marcus77, Chap. 2, Exercise 23, p. 43].

Proposition 3.2.4. *Let $K \subset L \subset M$ be number fields, $[L\colon K] = n$, $[M\colon L] = m$, and let $\{\alpha_1, \ldots, \alpha_n\}$ and $\{\beta_1, \ldots, \beta_m\}$ be bases for L over K and M over L, respectively. We have*

$$\operatorname{disc}{}_K^M(\alpha_1\beta_1, \ldots, \alpha_n\beta_m) = \left(\operatorname{disc}{}_K^L(\alpha_1 \ldots, \alpha_n)\right)^m \cdot \operatorname{Norm}_K^L\left(\operatorname{disc}{}_L^M(\beta_1 \ldots, \beta_m)\right).$$

Proposition 3.2.1 follows from Propositions 3.2.3 and 3.2.4 in the following way. Take

$$K = \mathbb{Q}, \quad L = \mathbb{Q}(x_{n-1}) \quad \text{and} \quad M = \mathbb{Q}(x_n).$$

The degree of L over K is 2^{n-1} and L has basis

$$\left\{1, x_{n-1}, x_{n-1}^2, \ldots, x_{n-1}^{2^{n-1}-1}\right\}$$

over K, while the degree of M over L is 2 and M has basis $\{1, x_n\}$ over L. The set $\{\alpha_1\beta_1, \ldots, \alpha_n\beta_m\}$ in Proposition 3.2.4 corresponds to the set

$$B' = \left\{1, x_{n-1}, x_{n-1}^2, \ldots, x_{n-1}^{2^{n-1}-1}, x_n, x_{n-1}x_n, x_{n-1}^2 x_n, \ldots, x_{n-1}^{2^{n-1}-1} x_n\right\}.$$

This set B' is a basis for M over K. Indeed, we have

$$|B'| = 2\left(2^{n-1} - 1\right) + 2 = 2^n = |B_n|,$$

and since $x_n^2 = \nu + x_{n-1}$, each element of B_n can be written as a $\mathbb{Z}$-linear combination of elements of B'. Similarly, each element of B' is a $\mathbb{Z}$-linear combination of elements of B_n. Since the base change matrices from B_n to B' and from B' to B_n have an integral determinant and because the discriminants are also integers, we deduce

$$\operatorname{disc}{}_K^M(B') = \operatorname{disc}{}_K^M(B_n) = \operatorname{disc}{}_K^M(x_n).$$

One obtains the formula in Proposition 3.2.1 by using in Proposition 3.2.4 the formulas from Proposition 3.2.3.

3.3 Proof of Theorem 3.1.1 and Proposition 3.1.2

We need the following result from K. Uchida (we will apply for $R = \mathbb{Z}$ and $\theta = x_n$).

Theorem 3.3.1 ([U77]). *Let R be a Dedeking ring. Let θ be an element of some integral domain which contains R and assume that θ is integral over R. Then $R[\theta]$ is a Dedekind ring if and only if the defining polynomial $f(t)$ of θ is not contained in $\mathfrak{m}^2$ for any maximal ideal $\mathfrak{m}$ of the polynomial ring $R[t]$.*

Before we go to the proof of the theorem, we need to recall a few facts.

Proposition 3.3.2 (Prop. 2.13, [Nark04]). *Let θ be an algebraic integer. We have*

$$\operatorname{disc}(\theta) = m^2 \operatorname{disc}(\mathbb{Q}(\theta)),$$

where m is the index in $\mathcal{O}_{\mathbb{Q}(\theta)}$ of the $\mathbb{Z}$-module $\mathbb{Z}[\theta]$.

Definition 3.3.3. *We say that a monic polynomial*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

with coefficients in $\mathbb{Z}$ is p-Eisenstein *with respect to the prime number p, if $a_0, a_1, \ldots, a_{n-1}$ are divisible by p, and p^2 does not divide a_0.*

Lemma 3.3.4 (Lemma 2.17, [Nark04]). *Let θ be an algebraic integer and p be a prime number. If the minimal polynomial of θ over $\mathbb{Q}$ is p-Eisenstein, then the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_{\mathbb{Q}(\theta)}$ is not divisible by p.*

In the proof of Proposition 2.15 in [VV15], Vidaux and Videla proved the following result.

Proposition 3.3.5 ([VV15])**.** *For each $n \geq 1$, let P_n be the minimal polynomial of x_n. Suppose that $\nu + x_0$ is congruent to 2 or 3 modulo 4. We have:*

1. *if n is odd, then $P_n(t+a)$ is 2-Eisenstein, where $a = \begin{cases} 0 \text{ if } \nu + x_0 \equiv 2 \mod 4 \\ 1 \text{ if } \nu + x_0 \equiv 3 \mod 4 \end{cases}$, and*

2. *if n is even, then $P_n(t + x_0)$ is 2-Eisenstein.*

Moreover, writing $f(t) = t^2 - \nu$, we have $P_n(t) = f^{\circ n}(t) - x_0$, hence in particular P_n has no monomial of odd degree.

Proposition 3.3.6. *For all $n \geq 1$, if $\nu + x_0$ is congruent to 2 or 3 modulo 4, then the index in $\mathcal{O}_{\mathbb{Q}(x_n)}$ of the $\mathbb{Z}$ module $\mathbb{Z}[x_n]$ is not divisible by 2.*

Proof. It is an immediate consequence of Proposition 3.3.5 and Lemma 3.3.4, since for any rational integer c, $P_n(t+c)$ is the minimal polynomial of $x_n - c$, $\mathbb{Z}[x_n - c] = \mathbb{Z}[x_n]$, and $\mathbb{Q}(x_n - c) = \mathbb{Q}(x_n)$. □

Proof of Theorem 3.1.1. Assume first that there exists $n \geq 1$ such that $P_n(0)$ is not square-free. Let p be a prime such that p^2 divides $P_n(0)$ and write $P_n(0) = p^2 s$, where $s \in \mathbb{Z} - \{0\}$. Since P_n has only monomials of even degree, we have

$$P_n(t) = p^2 s + pt \cdot 0 + t^2 g(t),$$

for some $g(t) \in \mathbb{Z}[t]$. Hence $P_n(t) \in (p,t)^2 \subseteq \mathbb{Z}[t]$. The ideal (p,t) is maximal, hence $\mathbb{Z}[x_n] \neq \mathcal{O}_{\mathbb{Q}(x_n)}$ by Theorem 3.3.1.

We show the other direction by induction on n. Let m_n be the index in $\mathcal{O}_{\mathbb{Q}(x_n)}$ of the $\mathbb{Z}$-module $\mathbb{Z}[x_n]$, so we have

$$\text{disc}\,(x_n) = m_n^2 \text{disc}\,\mathbb{Q}(x_n)$$

by Proposition 3.3.2.

On the one hand, we have

$$\text{disc}\,(x_1) = \text{disc}\,(\sqrt{\nu + x_0}) = \begin{vmatrix} 1 & \sqrt{\nu + x_0} \\ 1 & -\sqrt{\nu + x_0} \end{vmatrix}^2 = 4(\nu + x_0),$$

and on the other hand, it is well known that for $\nu + x_0 \equiv 2, 3 \pmod 4$, we have $\text{disc}\,\mathbb{Q}(x_1) = \text{disc}\,(\mathbb{Q}(\sqrt{\nu + x_0})) = 4(\nu + x_0)$, so in particular we have $m_1 = 1$.

For $n \geq 2$, suppose that $m_{n-1} = 1$, that is $\text{disc}\,(x_{n-1}) = \text{disc}\,\mathbb{Q}(x_{n-1})$. By Proposition 3.2.1 we have

$$\text{disc}\,(x_n) = (\text{disc}\,(x_{n-1}))^2 \cdot 2^{2^n} P_n(0),$$

and by induction hypothesis we have

$$\text{disc}\,(x_n) = (\text{disc}\,\mathbb{Q}(x_{n-1}))^2 \cdot 2^{2^n} P_n(0),$$

so

$$(\text{disc}\,\mathbb{Q}(x_{n-1}))^2 \cdot 2^{2^n} P_n(0) = m_n^2 \text{disc}\,\mathbb{Q}(x_n).$$

On the one hand, by Proposition 3.3.6 we have that 2 does not divide m_n, and on the other hand, by [Nark04, Cor. 1 of Prop. 4.15], the discriminant of $\mathbb{Q}(x_n)$ is divisible by

$$(\text{disc}\,\mathbb{Q}(x_{n-1}))^{[\mathbb{Q}(x_n):\mathbb{Q}(x_{n-1})]} = (\text{disc}\,\mathbb{Q}(x_{n-1}))^2.$$

Hence, $P_n(0) = m_n^2 \ell$ for some $\ell \in \mathbb{Z}$. We deduce that $m_n = 1$ because $P_n(0)$ is assumed to be square-free. □

Proof of Proposition 3.1.2. Let $n \geq 2$ be such that $\mathbb{Z}[x_n] = \mathcal{O}_{\mathbb{Q}(x_n)}$. Let $\alpha \in \mathcal{O}_{\mathbb{Q}(x_{n-1})}$. By hypothesis, we have

$$\alpha = a_0 + a_1 x_n + a_2 x_n^2 + \cdots + a_{2^n-1} x_n^{2^n-1}$$

for some $a_i \in \mathbb{Z}$. Separating even and odd powers of x_n, since $x_n^2 = \nu + x_{n-1}$, we have

$$\alpha = a + b x_n,$$

for some $a, b \in \mathbb{Z}[x_{n-1}]$. Since $x_n \notin \mathbb{Q}(x_{n-1})$ by assumption, we deduce that b is 0. □

3.4 Computational evidence (under ABC)

Given an integer $r \geq 2$ and a polynomial $h \in \mathbb{Z}[X]$ of degree r, we consider

$$N_h(x) = \#\left\{n \leq x \colon h(n) \text{ is square-free}\right\},$$

and

$$G_h = \gcd\{h(n) \colon n \geq 1\}.$$

Theorem 3.4.1 ([G98], Th 1)**.** *Assume the ABC-Conjecture. Let $h \in \mathbb{Z}[t]$ be a polynomial with integer coefficients, of degree at least 2, without repeated factors. If G_h is square-free, then*

$$N_h(x) \sim c_h x,$$

for some $c_h > 0$.

Assume $x_0 = 0$. Recall that in this case, we have $P_n(t) = f^{\circ n}(t)$, where $f(t) = t^2 - \nu$. We define the polynomials $g_n(t) \in \mathbb{Z}[t]$ by induction on n:

- $g_1(t) = -t$, and
- $g_{n+1}(t) = (g_n(t))^2 - t$, for each $n \geq 2$.

So in particular we have $P_1(0) = -\nu = g_1(\nu)$, and if $P_n(0) = g_n(\nu)$, then

$$P_{n+1}(0) = (f \circ f^{\circ n})(0) = (f^{\circ n}(0))^2 - \nu = P_n(0)^2 - \nu = g_n(\nu)^2 - \nu = g_{n+1}(\nu).$$

Therefore, for each $n \geq 1$, we have

$$P_n(0) = g_n(\nu).$$

Given $\ell \geq 1$, we consider

$$h_\ell(t) = \operatorname{lcm}\{g_n(t) \colon 1 \leq n \leq \ell\}.$$

Lemma 3.4.2. *For every $\ell \geq 1$, G_{h_ℓ} is square-free.*

Proof. Since $2^2 - 2 = 2$, for all $n \geq 1$ we have $g_n(2) = \pm 2$. Also, it is immediate from the definition of g that there exists a polynomial $q_n(t)$ in $\mathbb{Z}[t]$ such that $g_n(t) = t q_n(t)$. Hence for each $n \geq 1$ we have $q_n(2) = \pm 1$, and for each polynomial $p(t)$ in $\mathbb{Z}[t]$ which divides $q_n(t)$, we have $p(2) = \pm 1$. Hence for each $\ell \geq 1$, we have $h_\ell(2) = \pm 2$. Since $g_2(t) = t(t-1)$, the product $t(t-1)$ divides $h_\ell(t)$ for each $\ell \geq 2$, so 2 divides $h_\ell(j)$ for any $j \geq 2$ and for each $\ell \geq 2$, hence for each $\ell \geq 1$. We have $h_\ell(1) = -1$ for odd ℓ, in which case $G_{h_\ell} = 1$, and $h_\ell(1) = 0$ for even ℓ, in which case $G_{h_\ell} = \pm 2$. □

Lemma 3.4.3. *For every $\ell \geq 1$, the polynomial $h_\ell \in \mathbb{Z}[t]$ has degree ≥ 2 and no repeated factors.*

Proof. The fact that h_ℓ has degree ≥ 2 is immediate from its definition. It is enough to show that each g_n has no repeated factor. The derivative of $g_n(t)$ is

$$g_n'(t) = 2(g_{n-1}(t)) \cdot ((g_{n-1})'(t)) - 1.$$

Hence the reduction modulo 2 of $g_n'(t)$ is equal to 1. If there were a root α in common between $g_n(t)$ and $g_n'(t)$, then $g_n'(t)$ would have the form $A(t)B(t)$, with $A(t)$ the minimal polynomial of α. Since $g_n(t)$ is monic with integral coefficients, α would be an algebraic integer, hence $A(t)$ also would be a monic polynomial with integral coefficients. By Gauss' Lemma, $B(t)$ also has integer coefficients. Reducing modulo 2, we get $A(t)B(t) \equiv 1$, hence in particular $A(t) \equiv 1$, which contradicts the fact that it is monic and non-constant. □

Corollary 3.4.4. *Assume $x_0 = 0$ and fix an integer $\ell \geq 2$. Under the ABC Conjecture, there exist infinitely many values of ν such that, for all $1 \leq n \leq \ell$, $P_n(0)$ is square-free. Moreover, all these ν are congruent to 2 or 3 modulo 4.*

Proof. By Theorem 3.4.1 and Lemmas 3.4.2 and 3.4.3, we know that $h_\ell(\nu)$ is square-free for infinitely many ν. For each of those ν, given $1 \leq n \leq \ell$, since g_n divides h_ℓ in $\mathbb{Z}[t]$, also $g_n(\nu) = P_n(0)$ is square-free. Let ν be such that $P_n(0)$ is square-free for each $1 \leq n \leq \ell$. In particular, $P_1(0) = -\nu$ and $P_2(0) = \nu^2 - \nu$ are square-free, so ν cannot be congruent to 0 or 1 modulo 4. □

Chapter 4

Fields K with $A(\mathcal{O}_K)$ distinct from $[4, \infty)$

4.1 Introduction

The objective of this chapter is to find some pairs (ν, x_0) such that the JR number of the ring of integers of the fraction field of $\mathbb{Z}^{(\nu,x_0)}$ is strictly between 4 and $+\infty$, or is 4 and it is not a minimum.

Let $\mathcal{O}_{\mathbb{Q}(x_n)}$ be the ring of integers of $\mathbb{Q}(x_n)$ and let

$$\mathcal{O}^{(\nu,x_0)} = \cup \mathcal{O}_{\mathbb{Q}(x_n)},$$

so that $\mathcal{O}^{(\nu,x_0)}$ is the ring of integers of the fraction field of $\mathbb{Z}^{(\nu,x_0)}$. If m is an integer, we write ζ_m for a primitive m-th root of unity.

The JR number of $\mathcal{O}^{(\nu,x_0)}$ is 4 and is a minimum if and only if, in $\mathcal{O}^{(\nu,x_0)}$ there exist infinitely many numbers of the form

$$\zeta_m^j + \zeta_m^{-j} = 2\cos\left(\frac{2\pi j}{m}\right),$$

with $j = 1, \ldots, m-1$, if and only if in $\mathcal{O}^{(\nu,x_0)}$ there exist infinitely many numbers of the form

$$\zeta_m + \zeta_m^{-1} = 2\cos\left(\frac{2\pi}{m}\right).$$

The first equivalence is a consequence of theorem of Kronecker, see [Nark04, Thm. 2.5].

Since the fraction field of $\mathcal{O}^{(\nu,x_0)}$ is a 2-tower, for each m, $\zeta_m + \zeta_m^{-1}$ is constructible with ruler and compass, and we have the following equivalence: $\zeta_m + \zeta_m^{-1}$ is constructible with ruler and compass, if and only if $m = 2^d p_1 \ldots p_k$, where $d \geq 0$ and p_i are distinct Fermat Primes (by Gauss-Wantzel Theorem). Thus, the strategy consists in finding a pair (ν, x_0) such that $\mathcal{O}^{(\nu,x_0)}$ has only finitely many numbers $\zeta_m + \zeta_m^{-1}$ with m of the form $2^d p_1 \ldots p_k$.

We prove the following.

Theorem 4.1.1. *The* JR *number of* $\mathcal{O}^{(2^{2m}\mu,0)}$*, with* $m \geq 1$*,* $\mu \geq 3$ *odd and not a quadratic residue modulo any Fermat prime greater than* 3*, is either strictly between 4 and* $+\infty$*, or it is* 4 *and it is not a minimum.*

The fact that the JR number is not $\{+\infty\}$ is an immediate consequence of the fact that $\mathcal{O}^{(\nu,0)}$ has a subring with JR number not $\{+\infty\}$ — the subring in question is $\mathbb{Z}^{(\nu,0)}$ and its JR number is $\lceil\alpha\rceil + \alpha$, where $\alpha = (1 + \sqrt{1+4\nu})/2$. This is proven in [VV15, Thm. 1.4]. The hypothesis of this theorem that $\nu + x_0$ must be congruent to 2 or 3 modulo 4 is not satisfied for our choice of (ν, x_0), but this hypothesis was only there to ensure that the tower increases at each step. In our case, the tower is ensured to increase by a theorem by Stoll — see Theorem 4.4.1 below.

In Section 4.3 we prove that 3 and 7 are non-squares modulo any Fermat prime greater than 3. So for example, when $x_0 = 0$, for any odd integer k and for any $m \geq 1$, $\nu = 2^{2m}k^2 \cdot 3$ and $\nu = 2^{2m}k^2 \cdot 7$ satisfy the hypothesis of Theorem 4.1.1.

The proof is done in two steps. In Section 4.2, we will prove the following proposition.

Proposition 4.1.2. *Assume that $\mathbb{Q}(x_n)$ has degree 2^n over $\mathbb{Q}$. Suppose that*

1. *for every Fermat prime $p > 3$, $\nu + x_0$ is not a square modulo p, and*
2. *$\sqrt{2}$ is not in $\mathcal{O}^{(\nu, x_0)}$.*

The JR *number of $\mathcal{O}^{(\nu, x_0)}$ is either strictly between 4 and $+\infty$, or it is* 4 *and it is not a minimum.*

In Section 4.4 we prove that if $x_0 = 0$ and $\nu = 2^{2m}\mu$, with $m \geq 1$ and $\mu \geq 3$ odd and square-free, then $\sqrt{2}$ is not in $\mathcal{O}^{(\nu, x_0)}$.

Putting everything together, this proves Theorem 4.1.1. Note that if there are only finitely many Fermat primes, then item 1 of Proposition 4.1.2 is not relevant for our purposes, because they would contribute only to finitely many elements of the form $\zeta_m + \zeta_m^{-1}$.

4.2 Proof of Proposition 4.1.2

The following remark shows that it is sufficient to consider $\zeta_m + \zeta_m^{-1}$ where $m \in \{2^d : d \geq 2\} \cup \{p : p \text{ is a Fermat prime}\}$.

Remark 4.2.1. *Let m_1 and m_2 be positive coprime integers, and write $m = m_1 m_2$. The field $\mathbb{Q}(\zeta_{m_1 m_2})$ is the compositum of $\mathbb{Q}(\zeta_{m_1})$ and $\mathbb{Q}(\zeta_{m_2})$.*

We need the following result.

Proposition 4.2.2.

1. *([Wash82], p. 15) The field $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is the maximal totally real subfield of $\mathbb{Q}(\zeta_m)$. The extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is of degree* 2*.*
2. *([Wash82], Ex. 2.1, p. 17) Let p be a prime number. The field $\mathbb{Q}(\zeta_p)$ contains the field $\mathbb{Q}(\sqrt{p})$ if $p \equiv 1 \pmod 4$ and contains $\mathbb{Q}(\sqrt{-p})$ if $p \equiv 3 \pmod 4$.*
3. *Let K be a number field. The number p is ramified in K if and only if p divides* disc *K.*

We prove the following proposition.

Proposition 4.2.3. *Let $p > 3$ be a Fermat prime. If $\zeta_p + \zeta_p^{-1} \in \mathcal{O}^{(\nu, x_0)}$, then there exists $n \geq 1$ such that p divides* disc *$\mathbb{Q}(x_n)$.*

Proof. Let $p = 2^{2^m} + 1 > 3$ be a Fermat prime. Note that, since $m \geq 1$, p is congruent to 1 modulo 4. Hence, by Proposition 4.2.2, we have

$$\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1}),$$

hence $\sqrt{p} \in \mathcal{O}^{(\nu, x_0)}$ by hypothesis, so in particular $\sqrt{p}$ lies in $\mathbb{Q}(x_n)$ for some $n \geq 1$. Therefore, $p = (\sqrt{p})^2$ is ramified in $\mathbb{Q}(x_n)$, so p divides disc $\mathbb{Q}(x_n)$ by Proposition 4.2.2. □

Lemma 4.2.4. *Let p be an odd prime. If p divides* disc *(x_n), then p divides the product $P_1(0) \ldots P_n(0)$.*

Proof. By induction on n. For $n = 1$ we have $\operatorname{disc}(x_1) = 4(\nu + x_0) = -4P_1(0)$.

If it is true for n, then it is true for $n + 1$ by Proposition 3.2.1, since we have

$$\operatorname{disc}(x_{n+1}) = (\operatorname{disc}(x_n))^2 \cdot 2^{2^{n+1}} P_{n+1}(0).$$

□

Corollary 4.2.5. *Let p be an odd prime. If p divides $\operatorname{disc}(\mathbb{Q}(x_n))$ for some $n \geq 1$, then p divides the product $P_1(0) \dots P_n(0)$.*

Proof. This is an immediate consequence of Lemma 4.2.4, because we know by Proposition 3.3.2 that the discriminant of $\mathbb{Q}(x_n)$ divides the discriminant of x_n. □

Proposition 4.2.6. *Let $p > 3$ be a Fermat prime. If $\nu + x_0$ is not a square modulo p (so in particular p does not divide $\nu + x_0$), then for each $n \geq 1$, p does not divide $\operatorname{disc}\mathbb{Q}(x_n)$.*

Proof. We prove by induction on n. For $n = 1$ we have that

$$\operatorname{disc}\mathbb{Q}(x_1) = \begin{cases} \nu + x_0, & \text{if } \nu + x_0 \equiv 1 \mod 4 \\ 4(\nu + x_0), & \text{if } \nu + x_0 \equiv 2, 3 \mod 4 \end{cases}$$

In both cases, since p does not divide $\nu + x_0$, we have that p does not divide $\operatorname{disc}\mathbb{Q}(x_1)$.

Assume by contradiction that p divides the discriminant of $\mathbb{Q}(x_n)$, so that p divides $P_j(0)$ for some $j \in \{1, \dots, n\}$ by Corollary 4.2.5. If $j = 1$, then p divides $\nu + x_0$, which contradicts our hypothesis. Assume $j > 1$. Recall that $P_n(t) = f^{\circ n}(t) - x_0$, where $f(t) = t^2 - \nu$. Therefore, we have

$$P_j(0) = (P_{j-1}(0) + x_0)^2 - (\nu + x_0),$$

which contradicts the hypothesis that $\nu + x_0$ is not a square modulo p. □

Proof of Proposition 4.1.2. We follow the strategy described in the introduction. Let p be a Fermat Prime greater than 3. By Proposition 4.2.6, if $\nu + x_0$ is not a square modulo p, then p does not divide $\operatorname{disc}\mathbb{Q}(x_n)$, so $\zeta_p + \zeta_p^{-1}$ does not lie in $\mathcal{O}^{(\nu,x_0)}$ by Proposition 4.2.3.

Let $s_1 = \sqrt{2}$ and $s_n = \sqrt{2 + s_{n-1}}$. Since

$$\zeta_{2^d} + \zeta_{2^d}^{-1} = \begin{cases} -2 & \text{if } d = 1 \\ s_{d-1} & \text{if } d \geq 2, \end{cases}$$

and $\sqrt{2}$ is not in $\mathcal{O}^{(\nu,x_0)}$ by hypothesis, $\zeta_{2^d} + \zeta_{2^d}^{-1}$ does not lie in $\mathcal{O}^{(\nu,x_0)}$ for any $d \geq 2$. Remark 4.2.1 allows us to conclude. □

4.3 Some non-squares modulo all Fermat primes greater than 3

Lemma 4.3.1. *For all $n \geq 1$, we have*

$$2^{2^n} + 1 \equiv \begin{cases} 3 \pmod 7 & \textit{if } n \textit{ is even} \\ 5 \pmod 7, & \textit{if } n \textit{ is odd,} \end{cases}$$

and

$$2^{2^n} + 1 \equiv 2 \pmod 3.$$

Proof. Since 2^n is congruent to $(-1)^n$ modulo 3, we have $2^n = 1+3k$ for some odd k when n is even, and $2^n = 2+3k$ for some even k when n is odd. Therefore, we have

$$2^{2^n} = \begin{cases} 2^{1+3k} = 2\cdot 8^k \equiv 2 \pmod 7 & \text{if } n \text{ is even} \\ 2^{2+3k} = 4\cdot 8^k \equiv 4 \pmod 7 & \text{if } n \text{ is odd.} \end{cases}$$

and

$$2^{2^n} = \begin{cases} 2^{1+3k} \equiv 2\cdot (-1)^k \equiv 1 \pmod 3 & \text{if } n \text{ is even} \\ 2^{2+3k} \equiv 4\cdot (-1)^k \equiv 1 \pmod 3 & \text{if } n \text{ is odd.} \end{cases}$$

□

Proposition 4.3.2. *The numbers 3 and 7 are not squares modulo all Fermat primes greater than 3.*

Proof. Let $p = 2^{2^n}+1$ be a Fermat prime greater than 3. By the quadratic reciprocity law, since $p \neq 7$, we have

$$\begin{aligned} \left(\frac{7}{p}\right)\left(\frac{p}{7}\right) &= (-1)^{\frac{2^{2^n}\cdot 6}{4}} \\ &= (-1)^{2^{2^n-1}\cdot 3} \\ &= 1, \end{aligned}$$

hence, 7 is a square modulo p if and only if p is a square modulo 7. Since the set of squares modulo 7 is $\{0,1,2,4\}$, we deduce by Lemma 4.3.1 that p is not a square modulo 7.

Similarly, we have $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = 1$, so we can proceed as before. □

4.4 Galois Group of $\mathbb{Q}(x_n)$.

In this section, we assume that $x_0 = 0$ and that ν is not a square. By [Stoll92, Cor. 1.3], each polynomial P_n is the minimal polynomial of x_n.

Let C_2 be the cyclic group of order 2, and denote by $[C_2]^n$ the n-fold wreath product of C_2 — for basic facts about the wreath product, we refer the reader to [Rot95].

Let L_n be the Galois closure of $\mathbb{Q}(x_n)$, and $\mathrm{Gal}(L_n)$ be its Galois group. The following is a particular case of a theorem by M. Stoll [Stoll92, Section 3, p. 243].

Theorem 4.4.1. *If ν is a multiple of 4, then $\mathrm{Gal}(L_n) \cong [C_2]^n$.*

In order to show that $\sqrt{2}$ is not in $\mathbb{Q}(x_n)$, we will show that it is not in L_n. For this we will use a counting argument. First we will show that there are exactly 2^n-1 quadratic subfields of L_n. Then we will construct 2^n-1 quadratic subfields, none of which is $\mathbb{Q}(\sqrt{2})$.

Lemma 4.4.2. *There are 2^n-1 quadratic subfields of L_n.*

Proof. We will give two different proofs. By the Galois correspondence, we need to count how many subgroups H of $[C_2]^n$ are such that the quotient $[C_2]^n/H$ is isomorphic to C_2.

Proof 1. We prove that $[C_2]^n$ has 2^n-1 subgroups of index 2 (they are maximal subgroups). Let M be the set of maximal subgroups of $[C_2]^n$. Since $[C_2]^n$ has order 2^{2^n-1}, it is a 2-group. The groups in M have index 2, so they are normal. The intersection of all the maximal subgroups of $[C_2]^n$ is called the *Frattini subgroup* of $[C_2]^n$ and is denoted by $\phi([C_2]^n)$. By [Rot95, Thm 5.48], the group $\phi = \phi([C_2]^n)$ is normal, and the quotient $[C_2]^n/\phi$ is an $\mathbb{F}_2$-vector space. Let d be the dimension of this vector space.

For every $H \in M$, since $\phi \leq H \leq [C_2]^n$, the quotient H/ϕ is a subspace of $[C_2]^n/\phi$, and every subspace of $[C_2]^n/\phi$ corresponds to a maximal subgroup H. It is easy to see that the number of non-trivial subspaces of a vector space of dimension d over $\mathbb{F}_2$ is $2^d - 1$. So we have $2^d - 1$ maximal subgroups.

On the other hand, by Burnside's basis Theorem [Rot95, Thm. 5.50], all minimal systems of generators of $[C_2]^n$ have the same cardinal, and this cardinal is d. However, the cardinal of a minimal set of generators for wreath products of cyclic groups has been computed by Woryna — see the comments after Theorem 1.1 in [Woryna11]. In our case, we get $d = n$.

Proof 2. We use the following well-known results from Group theory. Let G be a group and $D(G)$ the commutator subgroup of G. Let H be any subgroup of G. The following are true:

1. $D(G)$ is contained in H if and only if H is a normal subgroup of G and G/H is abelian.

2. If $D(G)$ is contained in H, then $(G/D(G))/(H/D(G))$ is isomorphic to G/H.

Moreover, we need the fact that the quotient $[C_2]^n/D([C_2]^n)$ is isomorphic to C_2^n — see [Stoll92, Proof of Lemma 1.5].

Suppose that H is a subgroup of $[C_2]^n$ with $[C_2]^n/H$ isomorphic to C_2. By item 1 above, we deduce that $D([C_2]^n)$ is contained in H. By item 2 and by Lagrange theorem, we have

$$|H/D([C_2]^n)| = \frac{2^n}{2} = 2^{n-1}.$$

Furthermore, the subgroups containing $D([C_2]^n)$ correspond bijectively to subgroups of $[C_2]^n/D([C_2]^n)$. As in the first proof, the group C_2^n is a vector space of dimension n over $\mathbb{F}_2$, and every subgroup of order 2^{n-1} corresponds bijectively to a subspace of dimension $n-1$. This number is well known to be $2^n - 1$. □

For $n \geq q$, let $c_n = P_n(0)$ be the constant term of the minimal polynomial of x_n, and let $c_1 = \nu = -P_1(0)$.

Lemma 4.4.3. *Let p be a prime that divides some c_n. Let $m = \min\{n \geq 1\colon p \text{ divides } c_n\}$ and e be the order of c_m at p. For every n, p divides c_n if and only if p^e divides c_n if and only if m divides n.*

Proof. This is an easy consequence of a theorem by Rice [Rice07, Prop. 3.1 and 3.2]. There is also a simple proof in [Stoll92, proof of Lemma 1.1], inspired by Odoni [Odo85]. We give a very elemental proof for the sake of completeness.

Recall that $P_n(t) = f^{\circ n}(t)$, where $f(t) = t^2 - \nu$. If $n = \ell + m$ for some integer $\ell > 0$, then we have

$$c_n = f^{\circ \ell}(f^{\circ m}(0)) = f^{\circ \ell}(c_m) \equiv c_\ell \pmod{c_m^2},$$

hence, if n is a multiple of m, then c_n has the same order at p as c_m. Conversely, write $n = qm + r$, with $0 \leq r < m$. We have

$$c_n = f^{\circ r}(f^{\circ qm}(0)) \equiv c_r \pmod{c_{qm}^2},$$

hence c_n is congruent to c_r modulo p. So, if p divides c_n, then it divides c_r with $r < m$, which is a contradiction unless $r = 0$. □

We recall that non-zero rational numbers $a_1, \ldots, a_n$ are 2-*independent* if their residue classes in the $\mathbb{F}_2$-vector space $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ are linearly independent. In [Stoll92, Section 1, p. 16], Stoll proves the following theorem.

Theorem 4.4.4. *The group* $\mathrm{Gal}(L_n)$ *is isomorphic to* $[C_2]^n$ *if and only if* $c_1, \ldots, c_n$ *are 2-independent.*

We also need the following simple observation: $\sqrt{c_1}, \ldots, \sqrt{c_n}$ all lie in L_n.

We can now prove our theorem.

Theorem 4.4.5. *Suppose the $\nu = 2^{2m}\mu$, with $\mu \geq 3$ odd and square-free and $m \geq 1$. The field $L = \bigcup_n L_n$ does not contain $\sqrt{2}$ — so in particular $\mathcal{O}^{(\nu,0)}$ does not contain $\sqrt{2}$.*

Proof. From Theorem 4.4.1 and Theorem 4.4.4 the number $c_1, \ldots, c_n$ are 2-independent. There are

$$\binom{n}{1} + \cdots + \binom{n}{n} = 2^n - 1$$

distinct possible products $\sqrt{c_{i_1}} \ldots \sqrt{c_{i_k}}$. By the observation above, each product corresponds to a distinct quadratic extensions in L_n. We conclude with Lemma 4.4.2 that there are no more.

Since $c_1 = \nu$, by Lemma 4.4.3, 2^{2m} is the highest power of 2 which divides c_n for each $n \geq 1$. Hence, in every product of the $\sqrt{c_i}$, an even power of 2 comes out of the square root, and we deduce that $\sqrt{2}$ does not appear in any of the quadratic extensions that we found. □

Here is an example. For $\nu = 12$, we have $L_1 = \mathbb{Q}(\sqrt{12}) = \mathbb{Q}(\sqrt{3})$, and

$$L_2 = L_1\left(\sqrt{12 + \sqrt{12}}, \sqrt{12 - \sqrt{12}}\right) = \mathbb{Q}\left(\sqrt{3}, \sqrt{12 + \sqrt{12}}, \sqrt{12 - \sqrt{12}}\right).$$

We have

$$\sqrt{12 + \sqrt{12}}\sqrt{12 - \sqrt{12}} = \sqrt{12^2 - 12} = \sqrt{12 \cdot 11} = 2\sqrt{33} = \sqrt{c_2}.$$

Hence, in L_2, we have the three following square roots: $\sqrt{3}$, $\sqrt{33}$ and $\sqrt{11}$.

It is still an open problem to characterize the ν for which $\mathrm{Gal}(L_n)$ is $[C_2]^n$ for every n. Note that for $\nu = 3$, the above does not work since $\sqrt{2}$ appears immediately in the tower. Nevertheless, for $\nu = 7$, $\sqrt{2}$ does not appear in the first levels of the tower. This leads to the following question.

Question 4.4.6. *Is $\mathrm{Gal}(L_n)$ equal to $[C_2]^n$ when $\nu = 7$?*

Chapter 5

Conclusion

As a conclusion, we list some of the obvious problems that come naturally from our work. For what has been achieved, we send the reader to the introduction.

1. About Chapter 2: Complete the general picture of the situation by finding the interval and the JR number in the limit case $\nu = 3$.

2. About Chapter 3: Find at least one non-trivial example for which our criterium applies, or show that it never applies.

3. About Chapter 4: Decide, at least for some of the rings, in which case we actually are: the JR number is 4 and is not a minimum, or it is strictly greater than 4.

Bibliography

[Church36] A. Church, *An Unsolvable Problem of Elementary Number Theory*, Amer. J. Math. **58**, no. 2, 345–363 (1936).

[Dries88] L. van den Dries, *Elimination theory for the ring of algebraic integers*, J. Reine Angew. Math. **388**, 189–205 (1988).

[FHV94] M. Fried, D. Haran y H. Völklein, *Real Hilbertianity and the Field of Totally Real Numbers*, Cont. Math., proceedings of Arizona conf. in Geom. **174** 1-34 (1994).

[G98] A. Granville, *ABC Allows Us to Count Squarefrees*, IMRN International Mathematics Research Notices 1998, No. 19.

[JV08] M. Jarden y C. Videla, *Undecidability of Families of Rings of Totally Real Integers*. International Journal of Number Theory **04**, 835-850 (2008).

[Koe14] J. Koenigsmann, *Undecidability in Number Theory*, in: *Model Theory in Algebra, Analysis and Arithmetic, Cetraro, Italy 2012*, Springer, Lecture Notes in Mathematics **2111** (2014).

[Li76] J. J. Liang, *On the integral basis of the maximal real subfield of a cyclotomic field*. J. Reine Angew. Math. 286-287, 223–226 (1976).

[Lu84] H. Lüneburg, *Resultanten von Kreisteilungspolynomen.* (German) [Resultants of cyclotomic polynomials] Arch. Math. (Basel) **42**, no. 2, 139–144 (1984).

[Marcus77] D. Marcus, *Number Fields*. Springer-Verlag, New Yonk (1977).

[Nark04] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers.* Third edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004. xii+708 pp. ISBN: 3-540-21902-1

[Odo85] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*. Proc. London Math. Soc. (3) **51**, no. 3, 385–414 (1985).

[Rice07] B. Rice, *Primitive Prime Divisors in Polynomials Arithmetic Dynamics*. Integers: Electronic Journal of Combinatorial Number Theory (2007).

[Rob49] J. Robinson, *Definability and Decision Problem in Arithmetic*, The Journal of Symbolic Logic, Vol. 14, No2 (Jun., 1949), pp. 98-114 (1949).

[Rob59] J. Robinson, *The Undecidability of Algebraic Rings and Fields*, Proc. Amer. Math. Soc. **10**, 950-957 (1959).

[Rob62] J. Robinson, *On the decision problem for algebraic rings*, The collected works of Julia Robinson, Collected Works **6**, American Mathematical Society, Providence, RI (1996).

[Rot95] J. J. Rotman, *An introduction to the theory of groups.* Fourth edition. Graduate Texts in Mathematics, **148**. Springer-Verlag, New York, 1995. xvi+513 pp. ISBN: 0-387-94285-8.

[Rum80] R. S. Rumely, *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. **262**, no. 1, 195–217 (1980).

[Sh04] A. Shlapentokh, *On Diophantine definability and decidability in some infinite totally real extensions of* $\mathbb{Q}$. Trans. Amer. Math. Soc. **356**, no. 8, 3189–3207 (2004).

[Sh09] A. Shlapentokh, *Rings of algebraic numbers in infinite extensions of* $\mathbb{Q}$ *and elliptic curves retaining their rank.* Arch. Math. Logic **48**, no. 1, 77–114 (2009).

[Sh14] A. Shlapentokh, *First Order Decidability and Definability of Integers in Infinite Algebraic Extensions of Rational Numbers*, arXiv:1307.0743v3.

[Stoll92] M. Stoll, *Galois Group over* $\mathbb{Q}$ *of some iterated polynomials.* Arch. Math., Vol. 59, 239-244 (1992).

[Tarski31] A. Tarski, *Fundamenta Mathematicae* **17**, Issue 1, 210–239 (1931).

[U77] K. Uchida, *When is* $Z[\alpha]$ *the ring of the integers?*, Osaka J. Math. **14**, no. 1, 155–157 (1977).

[VV15] X. Vidaux and C. R. Videla, *Definability of the natural numbers in totally real towers of nested square roots*, Proc. Amer. Math. Soc. **143**, 4463–4477 (2015).

[VV16] X. Vidaux and C. R. Videla, *A note on the Northcott property and undecidability*, Bull. London Math. Soc. **48**, 58–62 (2016), doi: 10.1112/blms/bdv089.

[Videla99] C. R. Videla, *On the constructible numbers*, Proc. Amer. Math. Soc. **127**, no. 3, 851–860 (1999).

[Videla00a] C. R. Videla, *Definability of the ring of integers in pro-p Galois extensions of number fields*, Israel J. Math. **118**, 1–14 (2000).

[Videla00b] C. R. Videla, *The undecidability of cyclotomic towers*, Proc. Amer. Math. Soc. **128**, no. 12, 3671–3674 (2000).

[Woryna11] A. Woryna, *The Rank and Generating Set for Iterated Wreath Products of Cyclic Groups*, Communications in Algebra, Volume 39 - Issue 7 (2011).

[Widmer16] M. Widmer, *Property (N), Decidability, and Diophantine Approximation*, Oberwolfach Reports (2016), https://www.mfo.de/occasion/1615

[Wash82] L. C. Washington, *Introduction to cyclotomic fields.* Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1982. xi+389 pp. ISBN: 0-387-90622-3.