CERO MULTIPLICIDAD DE SUCESIONES LINEALES RECURRENTES TERNARIAS

JOSE LUIS OROZCO GONZALES

UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
SANTIAGO DE CALI
2019

CERO MULTIPLICIDAD DE SUCESIONES LINEALES RECURRENTES TERNARIAS

JOSE LUIS OROZCO GONZALES

Tesis presentada como requisito para optar al título de Magíster en Ciencias Matemáticas

Director
Dr. Carlos Alexis Gómez Ruíz

UNIVERSIDAD DEL VALLE
FACULTAD DE CIENCIAS NATURALES Y EXACTAS
DEPARTAMENTO DE MATEMÁTICAS
SANTIAGO DE CALI
MAYO DE 2018

DEDICATORIA

La presente tesis de Maestría en Ciencias Matemáticas va dedicada a toda mi familia, quienes siempre me han brindado su apoyo.

AGRADECIMIENTOS

Agradezco inicialmente a Dios por la vida, la salud y por permitirme alcanzar una meta más. A la Universidad del Valle por abrirme sus puertas y permitirme crecer en el ámbito profesional y como persona y por el programa de *Asistencia de docencia*, con el cual financié gran parte de mis estudios de maestría. A los profesores que dirigieron mis cursos de posgrado y fueron comprensivos.

Un agradecimiento especial a la Vicerrectoría de investigaciones de la Universidad del Valle, por el apoyo financiero para la culminación de este trabajo, con el proyecto de investigación de financiación interna con centro de información 71135.
Finalmente agradezco a mi director de tesis por la paciencia y por sus enseñanzas.

Introducción.

Una sucesión lineal recurrente de orden k es una sucesión infinita de números complejos $\{u_0, u_1, u_2, \dots\}$ con la siguiente propiedad: existen constantes $a_1, a_2, \dots, a_k \in \mathbb{C}$ tales que

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n \quad \text{para todo } n \geq 0.$$

Si los valores iniciales $u_0, u_1, \dots u_{k-1}$ son dados, la relación de recurrencia define el resto de la sucesión de manera única. El ejemplo más conocido de una sucesión lineal recurrente fue dado por Leonardo de Pisa en el siglo XII: la sucesión de Fibonacci $\{0, 1, 1, 2, 3, 5, 8, 13 \dots\}$, la cual satisface la relación de recurrencia $u_{n+2} = u_{n+1} + u_n$ con valores iniciales $u_0 = 0, u_1 = 1$. El estudio de las sucesiones recurrentes es de interés intrínseco y ha sido una parte central de la teoría de números. Más aún, dichas sucesiones aparecen en mucha parte de las matemáticas y las ciencias de la computación. Para una sucesión lineal recurrente $(u_n)_{n\geq 0}$ de orden k, las siguientes situaciones son llamadas problemas de decisión:

1. $u_n = 0$ para algún n.
2. $u_n \geq 0$ para todo n.
3. $u_n \geq 0$ para todo n, excepto un número finito.

Los problemas anteriores tienen importantes aplicaciones en áreas como: verificación de software especialmente en la terminación de bucles lineales, comprobación de modelos probabilísticos, biología teórica, economía, sistemas dinámicos, combinatoria, entre otras (ver [9]). El problema 1 es conocido como el **problema de Skolem**, al segundo se lo conoce como el problema de *positividad* y al tercero se lo llama el problema de *la última-positividad*.

El punto de partida de la investigación del problema de Skolem fue su artículo [21] de 1934, *Einige Sätze über ge-wisse Reihenentwicklungen und exponentiale Beziehungen mit Anwendung auf diophantische Gleichungen*, donde demostró que el conjunto de índices n de una sucesión lineal recurrente de números racionales tales que $u_n = 0$ consiste de un conjunto finito junto a una unión finita de progresiones aritméticas. Posteriormente, Mahler [15] generalizó el resultado a sucesiones de números algebraicos, y finalmente Lech [13] demostró el resultado para sucesiones de elementos de un campo de característica cero. Sin embrago, las pruebas de este resultado no dan respuesta al problema de Skolem, ya que no proporcionan un algoritmo que permita determinar explícitamente los índices donde se hace cero la sucesión ni tampoco la cantidad de ellos, ya que dicho conjunto incluso podría ser vacío. De ahí que, la decidibilidad del problema de Skolem continue siendo un problema abierto por más de 80 años. En este sentido, ha surgido un gran número de trabajos y publicaciones. El problema de acotar la cero-multiplicidad de sucesiones lineales recurrentes binarias no degeneradas, fue resuelto por varios investigadores, en especial mencionamos el trabajo de Kubota [12], quien demostró que las sucesiones lineales recurrentes binarias no degeneradas tienen cero multiplicidad a lo más 4. Por otro lado, si las raíces del polinomio característico de una sucesión lineal recurrente son todas reales, el problema se vuelve un poco más sencillo de resolver, y en este caso Smiley [22] mostró con un simple argumento apoyado en la ley de signos de Descartes, que la cero multiplicidad para sucesiones recurrentes de orden 3 es a lo más 3 y de manera general cuando el orden de la recurrencia es $k \geq 4$, Hagedorn [11] mostró que la cero multiplicidad es a lo más $2k - 3$. Para el caso ternario en general, en 1957 fue conjeturado por Ward [24] que la cero multiplicidad de una sucesión lineal recurrente ternaria no degenerada es a los sumo cinco, sin embargo, esto no era cierto ya que Berstel [5] presentó la sucesión con relación de recurrencia $B_{n+3} = 2B_{n+2} - 4B_{n+1} + 4B_n$ y valores iniciales $B_0 = B_1 = 0$ y $B_2 = 1$, con lo cual $B_0 = B_1 = B_4 = B_6 = B_{13} = B_{52} = 0$, proporcionando un contraejemplo para la conjetura de Ward. Más adelante Buekers [3] demuestra que 6 es efectivamente la cota superior para la cero multiplicidad de cualquier sucesión recurrente ternaria no degenerada.

Nuestro trabajo constará de tres capítulos y un apéndice. En el Capítulo 1 encontraremos los conceptos fundamentales para el desarrollo de este trabajo. Emperezamos con una serie de definiciones y resultados de la teoría de números algebraica. Después haremos una breve introducción al análisis p-ádico, centrándonos en los valores absolutos no arquimedianos que se pueden definir en un cuerpo numérico $\mathbb{K}$. Continuamos con la revisión de algunas

desigualdades tipo Baker [2], en torno a las formas lineales en logaritmos de números algebraicos, y estableceremos un reciente resultado Matveev [16] el cual será nuestra principal herramienta en el desarrollo del Capítulo 3. Por último, hacemos un breve repaso del concepto de sucesiones lineales recurrentes, especialmente la *cero-multiplicidad*, tema principal de esta investigación.

En el Capítulo 2 realizaremos una revisión monográfica del trabajo de Beukers [3], cuyo principal objetivo es mostrar que una sucesión lineal recurrente ternaria no degenerada de números racionales tiene cero-multiplicidad a lo más seis. Este trabajo ha sido muchas veces referenciado en la literatura matemática concerniente a la cero multiplicidad de las sucesiones lineales recurrentes y ha sido punto de partida de varias investigaciones, por tal razón consideramos pertinente este estudio. Puntualmente describiremos el método de Beukers de manera general y completaremos algunos detalles.

En el Capítulo 3, notando que la recurrencia de Berstel, fue el contra-ejemplo a la conjetura de Ward y que de hecho esta es un ejemplo donde se alcanza la cota para la cero-multiplicidad de recurrencias ternarias no degeneradas, es natural preguntarse por la cero multiplicidad de la familia de sucesiones lineales recurrentes con relación de recurrencia $B_{n+3} = 2B_{n+2} - 4B_{n+1} + 4B_n$ y valores iniciales arbitrarios no todos nulos, las cuales llamaremos sucesiones *tipo Berstel*, y en particular toda esta familia de sucesiones tiene cero-multiplicidad a lo más 6. Como respuesta a este interrogante tenemos el siguiente resultado: *Salvo múltiplo escalar entero o desplazamiento de los subíndices, existen exactamente dos sucesiones lineales recurrentes ternarias tipo Berstel con cero multiplicidad al menos 3. Una de ellas es la sucesión de Berstel* $(B_n)_{n\in\mathbb{Z}}$ *y la otra es la sucesión recurrente tipo Berstel* $(B'_n)_{n\in\mathbb{Z}}$ *con valores iniciales* 0, 1, 4 *la cual tiene cero multiplicidad 3. Es decir, Cualquier sucesión lineal recurrente ternaria tipo Berstel, la cual no es un múltiplo escalar o desplazamiento de los subíndices de* $(B_n)_{n\in\mathbb{Z}}$ *o* $(B'_n)_{n\in\mathbb{Z}}$*, tiene cero-multiplicidad a lo más 2.* Este resultado corresponde a un trabajo de investigación conjunto con C. A. Gómez y F. Luca [14], cabe mencionar que esto fue presentado en el evento llamado ALTENCOA-18 en una ponencia. En el desarrollo de este capítulo demostraremos este resultado, mostrando la técnica utilizada. Este problema nos lleva a resolver una ecuación diofántica exponencial de números algebraicos, la cual es abordada con la teoría de las formas lineales en logaritmos (teoría de Baker), la teoría de aproximación diofántica y también con la ayuda del programa de computo *Mathematica*. Por último, en el Apéndice revisamos algunos aspectos básicos de las fracciones continuas que son necesarios para comprender algunos lemas que utilizamos en el capítulo 3.

Índice general

Capítulo 1

Preliminares

1.1. Introducción

En este capítulo encontraremos los conceptos fundamentales para el desarrollo de este trabajo. Emperezamos con una serie de definiciones y resultados de la teoría de números algebraica, tomando como referencia [18, cap. 2], estos conceptos aparecen de manera natural al tratar con sucesiones lineales recurrentes. Después haremos una breve introducción al análisis p-ádico, centrándonos en los valores absolutos no arquimedianos que se pueden definir en un cuerpo numérico $\mathbb{K}$, las pruebas de los resultados pueden ser consultadas en [7, cap. 4]. En la siguiente sección revisaremos algunas desigualdades tipo Baker [2], en torno a las formas lineales en logaritmos de números algebraicos, y revisaremos un reciente resultado Matveev [16] el cual será nuestra herramienta principal en el desarrollo del capítulo 3. Por último, hacemos un breve repaso del concepto de sucesiones lineales recurrentes, especialmente la *cero-multiplicidad*, tema principal de esta investigación, para esta última sección usamos la referencia [20].

1.2. Teoría de números algebraica

1.2.1. Números algebraicos y enteros.

Conceptos básicos

Un número $\alpha \in \mathbb{C}$ es llamado un *número algebraico* si existe un polinomio no nulo $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ tal que $f(\alpha) = 0$. Si $\alpha \in \mathbb{C}$ es una raíz de un polinomio mónico con coeficientes en $\mathbb{Z}$, decimos que α

es un *entero algebraico*. Claramente todo entero algebraico es un número algebraico. Sin embargo, el recíproco no es cierto, por ejemplo $\sqrt{3}/2$ es un número algebraico, pero este no es un entero algebraico.

Teorema 1.2.1. *Sea α un número algebraico. Entonces existe un único polinomio mónico irreducible $p(x)$ en $\mathbb{Q}[x]$ de grado minimal tal que $p(\alpha) = 0$. Además si $f(x) \in \mathbb{Q}[x]$ y $f(\alpha) = 0$ entonces $p(x) \mid f(x)$.*

El grado de $p(x)$ es llamado el *grado* de α y es denotado por $grad(\alpha)$; $p(x)$ es llamado el *polinomio minimal* de α.
Los números complejos que no son algebraicos son llamados *trascendentes*. Mucho antes de que se conociera un ejemplo de un número trascendente, los matemáticos estaban seguros de su existencia.

Cuerpos numéricos

La teoría de los cuerpo numéricos es vasta y rica. Vamos a mencionar a continuación hechos elementales necesarios para los próximos capítulos. Recordemos que si $A \subseteq B$ son anillos y si $x \in B$, denotamos por $A[x]$ al subanillo más pequeño de B que contiene a A y x. En otras palabras,

$$A[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{N} \text{ y } a_i \in A \text{ para todo } i\}$$

es el conjunto de todos polinomios en x con coeficientes en A.
Por otro lado, si A es un anillo contenido en un cuerpo $\mathbb{K}$ y $\alpha \in \mathbb{K}$, entonces $A(\alpha)$ denota el subcuerpo más pequeño de $\mathbb{K}$ que contiene a A y α. Para cualquier número algebraico α tenemos el siguiente resultado.

Teorema 1.2.2. *Si α es un número algebraico entonces el subanillo $\mathbb{Q}[\alpha] \subseteq \mathbb{C}$ es un cuerpo.*

Este teorema implica que si α es un número algebraico, entonces no hay diferencia entre $\mathbb{Q}[\alpha]$ y $\mathbb{Q}(\alpha)$, luego de ahora en adelante, denotaremos a $\mathbb{Q}[\alpha]$ por $\mathbb{Q}(\alpha)$ cuando α es un número algebraico.
Si $\mathbb{L} \subseteq \mathbb{C}$ es un cuerpo que contiene a $\mathbb{Q}$, entonces $\mathbb{L}$ puede ser visto como un $\mathbb{Q}$-espacio vectorial, a la dimension de $\mathbb{L}$ como $\mathbb{Q}$-espacio vectorial, se la llama la *dimensión* de $\mathbb{L}$ sobre $\mathbb{Q}$.
Un cuerpo $\mathbb{K} \subseteq \mathbb{C}$ es llamado un *cuerpo numérico* si su dimensión sobre $\mathbb{Q}$ es finita. La dimensión de $\mathbb{K}$ sobre $\mathbb{Q}$ es llamada el *grado* de $\mathbb{K}$ y es denotada por $[\mathbb{K} : \mathbb{Q}]$. Si α es un número algebraico de grado n, entonces $\mathbb{Q}(\alpha)$ es un cuerpo numérico de grado n sobre $\mathbb{Q}$.
El siguiente teorema nos dice que todo cuerpo numérico $\mathbb{K}$ es una extensión simple de $\mathbb{Q}$, es decir, una extensión de la forma $\mathbb{Q}(\theta)$ para algún número algebraico θ.

Teorema 1.2.3 (**Teorema del elemento primitivo**). *Sean $\theta_1, \ldots, \theta_n$ números algebraicos, entonces existe un número algebraico θ tal que $\mathbb{Q}(\theta_1, \ldots, \theta_n) = \mathbb{Q}(\theta)$.*

Si $\theta = \theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ son los conjugados de θ, entonces $\mathbb{Q}(\theta^{(i)})$ para $i = 1, \cdots, n$ son llamados los cuerpos conjugados de $\mathbb{Q}(\theta)$. Además, las funciones $\theta \to \theta^{(i)}$ son monomorfismos de $\mathbb{K} = \mathbb{Q}(\theta) \to \mathbb{Q}(\theta^{(i)})$, conocidos como las n inmersiones de $\mathbb{K}$ en $\mathbb{C}$, además estas se dividen en inmersiones reales y complejas, y las complejas vienen por pares conjugados.[1]
Un cuerpo $\mathbb{K}$ es llamado una *extensión de Galois* de $\mathbb{Q}$ si todos los cuerpos conjugados de $\mathbb{K}$ son idénticos a $\mathbb{K}$. Por ejemplo, cualquier extensión cuadrática de $\mathbb{Q}$ es de Galois. Sin embargo, $\mathbb{Q}(\sqrt[3]{2})$ no lo es ya que dos cuerpos conjugados $\mathbb{Q}(\rho\sqrt[3]{2})$ y $\mathbb{Q}(\rho^2\sqrt[3]{2})$ son distintos de $\mathbb{Q}(\sqrt[3]{2})$. (Aquí ρ es una raíz cúbica primitiva de la unidad). Se dice que un cuerpo $\mathbb{K}$ es el *cuerpo de descomposición* de un polinomio $p(x) \in \mathbb{Q}[x]$ si este contiene a todas las raíces de $p(x)$. Con respecto a las extensiones de Galois tenemos la siguiente resultado.

Teorema 1.2.4. *Si $\mathbb{K}$ es cuerpo de descomposición de un polinomio con coeficientes en $\mathbb{Q}$, entones $\mathbb{K}/\mathbb{Q}$ es una extension de Galois.*

El siguiente teorema proporciona distintas caracterizaciones de los enteros algebraicos. De estas, (iii) y (iv) son las más útiles porque determinan una herramienta inmediata para probar si un número algebraico es ó no un entero algebraico.

Teorema 1.2.5. *Sea α un número algebraico, entonces las siguientes afirmaciones son equivalentes:*

(i) *α es un entero algebraico.*

(ii) *El polinomio mínimal de α es mónico y pertenece a $\mathbb{Z}[x]$.*

(iii) *$\mathbb{Z}[\alpha]$ es finitamente generado como $\mathbb{Z}$-módulo.*

(iv) *Existe un $\mathbb{Z}$-módulo finitamente generado $\{0\} \neq M$ de $\mathbb{C}$ tal que $\alpha M \subseteq M$.*

Sea $\mathbb{K}$ un cuerpo numérico. Denotaremos por $\mathcal{O}_\mathbb{K}$ al conjunto de enteros algebraicos de $\mathbb{K}$. Del teorema anterior sabemos que si α y β son enteros algebraicos, entonces $\mathbb{Z}[\alpha]$ y $\mathbb{Z}[\beta]$ son $\mathbb{Z}$-módulos finitamente generados, por tanto $M = \mathbb{Z}[\alpha, \beta]$ también es un $\mathbb{Z}$-módulo finitamente generado, además $(\alpha \pm \beta)M \subseteq M$ y $(\alpha\beta)M \subseteq M$, implicando que:

[1] si σ es una inmersión compleja, entonces $\overline{\sigma}$ dada por $\overline{\sigma}(\alpha) = \overline{\sigma(\alpha)}$ con $\alpha \in \mathbb{K}$, también es una inmersión, aquí la barra denota la conjugación compleja.

Corolario 1.2.1. *Sea $\mathbb{K}$ un cuerpo numérico y $\alpha, \beta \in \mathbb{K}$. Si α y β son enteros algebraicos, entonces $\alpha \pm \beta$ y $\alpha\beta$ también lo son. Esto es, el conjunto de enteros algebraicos de $\mathbb{K}$ es un subanillo de $\mathbb{K}$.*

Es preciso mencionar que por obvias razones $\mathbb{Z} \subseteq \mathcal{O}_{\mathbb{K}}$, además, si $q \in \mathbb{Q}$ es un entero algebraico, entonces necesariamente $q \in \mathbb{Z}$, esto es, $\mathbb{Q} \cap \mathcal{O}_{\mathbb{K}} = \mathbb{Z}$, por esta razón a los elementos de $\mathbb{Z}$ los llamaremos *enteros racionales*.

1.2.2. Bases enteras

A continuación, nos adentramos un poco en la estructura algebraica de $\mathcal{O}_{\mathbb{K}}$. Definiremos la *norma* y la *traza* de un elemento de cualquier cuerpo numérico. También abordaremos un invariante importante de un cuerpo numérico llamado el *discriminante* y finalmente los ideales en el anillo de enteros algebraicos de un cuerpo numérico serán brevemente discutidos.

La norma y la traza

Empezamos definiendo dos importantes números racionales asociados a cualquier número algebraico de un cuerpo numérico $\mathbb{K}$. Recordemos que si $\mathbb{K}$ es un cuerpo numérico, entonces $\mathbb{K}$ puede ser visto como un espacio vectorial de dimensión finita sobre $\mathbb{Q}$. Entonces si $\alpha \in \mathbb{K}$, la función de $\mathbb{K}$ en $\mathbb{K}$ dada por $\Phi_\alpha : v \to \alpha v$, define un operador lineal en $\mathbb{K}$. Definimos la *traza* de α por $Tr_{\mathbb{K}}(\alpha) := Tr(\Phi_\alpha)$ y la *norma* de α por $N_{\mathbb{K}}(\alpha) := \det(\Phi_\alpha)$ (donde Tr y det son las usuales traza y determinante de un operador lineal). Luego, para encontrar la $Tr_{\mathbb{K}}(\alpha)$, escogemos cualquier base[2] de $\mathbb{K}$ sobre $\mathbb{Q}$, $\omega_1, \ldots, \omega_n$ y escribimos

$$\alpha\omega_i = \sum a_{ij}\omega_j \quad \text{para cada } 1 \leq i \leq n,$$

entonces $Tr_{\mathbb{K}}(\alpha) = TrA$ y $N_{\mathbb{K}}(\alpha) = \det A$, donde A es la matriz (a_{ij}).
Con respecto a las definiciones de norma y traza, tenemos el siguiente resultado.

Lema 1.2.1. *Sea $\mathbb{K}$ es un cuerpo numérico de grado n sobre $\mathbb{Q}$. Si $\alpha \in \mathbb{K}$, entonces $N_{\mathbb{K}}(\alpha), Tr_{\mathbb{K}}(\alpha) \in \mathbb{Q}$. Además, si $\alpha \in \mathcal{O}_{\mathbb{K}}$ entonces $Tr_{\mathbb{K}}(\alpha)$ y $N_{\mathbb{K}}(\alpha)$ están en $\mathbb{Z}$.*

[2] Aquí vale la pena mencionar, que la definición de norma y traza es independiente de la $\mathbb{Q}$-base escogida.

Existencia de una base entera

Sea $\mathbb{K}$ un cuerpo numérico de grado n sobre $\mathbb{Q}$, y $\mathcal{O}_{\mathbb{K}}$ su anillo de enteros algebraicos, usando teoría de retículos se puede mostrar que $\mathcal{O}_{\mathbb{K}}$ es un $\mathbb{Z}$-módulo finitamente generado. Decimos que $\omega_1, \ldots, \omega_n$ es una *base entera* de $\mathbb{K}$ si $\omega_i \in \mathcal{O}_{\mathbb{K}}$ para todo i, y $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_n$. El primer resultado respecto a una base entera es precisamente que todo cuerpo numérico $\mathbb{K}$ tiene una.

Lema 1.2.2. *Cualquier cuerpo numérico $\mathbb{K}$ tiene una base entera.*

Sea $\mathbb{K}/\mathbb{Q}$ una extensión de cuerpos, donde $\mathbb{K}$ es un cuerpo numérico de grado n sobre $\mathbb{Q}$. Sean $\sigma_1, \ldots, \sigma_n$ las n inmersiones de $\mathbb{K}$ en $\mathbb{C}$. Para $\alpha_1, \ldots, \alpha_n \in \mathbb{K}$ definimos el discriminante de $\alpha_1, \ldots, \alpha_n$ por

$$d_{\mathbb{K}/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) := [\det(\sigma_i(\alpha_j))]^2.$$

Es preciso mencionar que un cuerpo $\mathbb{K}$ puede tener más de una base entera, sin embargo, un hecho que se cumple para cualquier dos bases enteras con respecto al discriminante definido anteriormente es:

Teorema 1.2.6. *Si $w_1, \ldots, \omega_n$ y $\tilde{\omega}_1, \ldots, \tilde{\omega}_n$ son dos bases enteras distintas de $\mathbb{K}$, entonces $d_{\mathbb{K}/\mathbb{Q}}(\omega_1, \ldots, \omega_n) = d_{\mathbb{K}/\mathbb{Q}}(\tilde{\omega}_1, \ldots, \tilde{\omega}_n)$.*

Por el teorema anterior se tiene que el discriminante de un cuerpo numérico $\mathbb{K}$ es invariante para cualquier base entera de $\mathbb{K}$, por tal motivo definimos el *discriminante* de $\mathbb{K}$, denotado por $d_{\mathbb{K}}$, así:

$$d_{\mathbb{K}} := d_{\mathbb{K}/\mathbb{Q}}(\omega_1, \ldots, \omega_n),$$

donde $\omega_1, \ldots, \omega_n$ es cualquier base entera de $\mathbb{K}$.

Ideales en $\mathcal{O}_{\mathbb{K}}$

Ahora ponemos nuestra atención a los ideales de $\mathcal{O}_{\mathbb{K}}$. Recordemos que un ideal I de un anillo conmutativo con unidad A, es un subgrupo abeliano junto a la propiedad de "absorción de la multiplicación", esto es, para todo $a \in A$, $aI \subseteq I$. En particular, los ideales de $\mathcal{O}_{\mathbb{K}}$ pueden ser vistos como $\mathbb{Z}$-submódulos de $\mathcal{O}_{\mathbb{K}}$. A continuación mencionamos algunas de las propiedades de los ideales de $\mathcal{O}_{\mathbb{K}}$.

Lema 1.2.3. *Si $\mathfrak{a}$ es un ideal no nulo de $\mathcal{O}_{\mathbb{K}}$ entonces $\mathfrak{a} \cap \mathbb{Z} \neq \{0\}$.*

El *índice* de $\mathfrak{a}$ en $\mathcal{O}_{\mathbb{K}}$ denotado por $[\mathcal{O}_{\mathbb{K}} : \mathfrak{a}]$ es el cardinal del anillo cociente $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$.

Lema 1.2.4. *Si $\mathfrak{a}$ es un ideal no nulo de $\mathcal{O}_{\mathbb{K}}$ entonces $[\mathcal{O}_{\mathbb{K}} : \mathfrak{a}]$ es finito.*

El lema anterior nos permite definir la *norma* de un ideal no nulo $\mathfrak{a}$ de $\mathcal{O}_{\mathbb{K}}$ por $N(\mathfrak{a}) := [\mathcal{O}_{\mathbb{K}} : \mathfrak{a}]$. Un ideal de $\mathcal{O}_{\mathbb{K}}$ es un ideal propio si este es distinto de $\mathcal{O}_{\mathbb{K}}$. Un ideal *primo* $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$ es un ideal propio no nulo con la propiedad de que si $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$ son tales que $\alpha\beta \in \mathfrak{p}$ entonces $\alpha \in \mathfrak{p}$ ó $\beta \in \mathfrak{p}$. Un ideal $\mathfrak{m}$ se llama *maximal* si este no está contenido en ningún ideal propio de $\mathcal{O}_{\mathbb{K}}$ distinto de $\mathfrak{m}$.

Lema 1.2.5. *Todo ideal primo de $\mathcal{O}_{\mathbb{K}}$ contiene exactamente un primo racional.*

A este único primo racional con esta propiedad, se le conoce como el primo racional *encima* de $\mathfrak{p}$.
Es bien conocido que todo ideal maximal es un ideal primo, sin embargo, el recíproco no es cierto. En $\mathcal{O}_{\mathbb{K}}$ tenemos:

Lema 1.2.6. *Todo ideal primo de $\mathcal{O}_{\mathbb{K}}$ es maximal.*

De los lemas anteriores podemos deducir que si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_{\mathbb{K}}$, entonces el anillo cociente $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ es un cuerpo finito, por tanto tiene p^f elementos, donde p es exactamente el primo racional del Lema 1.2.5 y $f \in \mathbb{N}$.

1.2.3. Dominios de Dedekind

La noción de dominio de Dedekind es el concepto que necesitamos con el objetivo de establecer la factorización única de ideales como producto de ideales primos. En este camino, nos encontramos con la idea fundamental de anillo Noetheriano, con la noción de dominio integralmente cerrado y una importante propiedades de los ideales primos.

$\mathcal{O}_{\mathbb{K}}$ es integralmente cerrado.

Empezamos con el siguiente lema.

Lema 1.2.7. *Sea α un número algebraico. Entonces existe un entero no nulo $m \in \mathbb{Z}$ tal que $m\alpha$ es un entero algebraico.*

Recordemos que si D es un dominio entero, su *cuerpo de fracciones* $\mathbb{L}$ es el cuerpo más pequeño que contiene a D. Precisamente, tenemos

$$\mathbb{L} = \{x/y : x, y \in D, y \neq 0\}$$

junto con las reglas usuales de adición y multiplicación para fracciones.

Corolario 1.2.2. *Si $\mathbb{K}$ es un cuerpo numérico, entonces $\mathbb{K}$ es el cuerpo de fracciones de $\mathcal{O}_{\mathbb{K}}$.*

Sean A y B anillos con $A \subset B$. Decimos que un elemento $x \in B$ es entero sobre A si este es la raíz de un polinomio mónico con coeficientes en A. Un dominio entero D con cuerpo de fracciones $\mathbb{L}$ es *integralmente cerrado* si cuando $\alpha \in \mathbb{L}$ es entero sobre D, tenemos que $\alpha \in D$.

Lema 1.2.8. *Si $\mathbb{K}$ es un cuerpo numérico, entonces $\mathcal{O}_{\mathbb{K}}$ es integralmente cerrado.*

$\mathcal{O}_{\mathbb{K}}$ es Noetheriano

Un anillo A es llamado *Noetheriano* si todo ideal de A es finitamente generado.

Lema 1.2.9. *Sea A un anillo. Las siguientes afirmaciones son equivalentes a la condición de ser Noetehriano:*

(i) Todo ideal de A es finitamente generado.

(ii) Si $I_0 \subseteq I_1 \subseteq I_2 \subseteq \ldots$ es una cadena creciente de ideales de A, entonces existe n_0 tal que $I_n = I_{n_0}$ para todo $n \geq n_0$.

(iii) Todo conjunto no vacio Σ de ideales de A tiene un elemento maximal.

Una consecuencia del lema anterior y del Lema 1.2.4 es

Corolario 1.2.3. *Si $\mathbb{K}$ es un cuerpo numérico, entonces $\mathcal{O}_{\mathbb{K}}$ es un anillo Noetheriano.*

Factorización única de ideales.

Un *dominio de Dedekind* es un anillo D que satisface las siguientes propiedades:

1. D es un dominio entero.
2. D es Noetheriano.
3. D es integralmente cerrado.
4. Todo ideal primo de D es máximal.

Los resultados de las secciones previas implican:

Teorema 1.2.7. *Si $\mathbb{K}$ es un cuerpo numérico, entonces $\mathcal{O}_{\mathbb{K}}$ es un dominio de Dedekind.*

Un Dominio entero D es un *dominio de ideales principales* (DIP) si todo ideal de D es principal, es decir, es generado por un solo elemento. Mientras que D es un *dominio de factorización única* (DFU) si todo elemento no nulo en D se puede expresar de manera única (salvo orden y asociados) como producto de elementos irreducibles de D. Es bien conocido que todo DIP es DFU. También existen cuerpos numéricos en los cuales su anillo de enteros algebraicos $\mathcal{O}_{\mathbb{K}}$ no es DFU, por ejemplo, con $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$ entonces $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}]$, y en este anillo tenemos que $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, tiene dos factorizaciones en elementos irreducibles distintos. La ventaja de trabajar en dominios de Dedekind es que aunque no siempre se tenga factorización única, siempre se va a tener factorización única en ideales primos.
Recordemos que el producto de dos ideales I, J en un anillo A es definido como el ideal generado por todos los productos ij con $i \in I,\ j \in J$. Si $I = (a_1, \ldots, a_m)$ y $J = (b_1, \ldots, b_n)$ son ideales finitamente generados, entonces

$$IJ = (a_i b_j \mid 1 \leq i \leq m, 1 \leq j \leq n).$$

Decimos que un anillo A admite *factorización única de ideales* si todo ideal propio no nulo de A puede ser escrito de manera única (salvo orden) como producto de ideales primos.

Teorema 1.2.8. *Si D es un dominio de Dedekind, entonces D admite factorización única en ideales.*

De manera recíproca, se puede mostrar que si un dominio D admite factorización única de ideales, entonces D es un anillo de Dedekind. De los hechos anteriores podemos concluir que el anillo de enteros algebraicos de un cuerpo numérico admite factorización única en ideales.
Recordemos que la norma de un ideal $\mathfrak{a}$ no nulo de $\mathcal{O}_{\mathbb{K}}$ es $N(\mathfrak{a}) = [\mathcal{O}_{\mathbb{K}} : \mathfrak{a}]$. Como ya hemos definido el producto de ideales, mencionaremos algunos resultados que involucran la norma y que son consecuencia de la factorización única de ideales.

Lema 1.2.10 (La norma es multiplicativa)**.** *Si $\mathfrak{a}, \mathfrak{b}$ son ideales no nulos de $\mathcal{O}_{\mathbb{K}}$, entonces $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Lema 1.2.11 (Norma de un ideal principal)**.** *Si $\alpha \in \mathcal{O}_{\mathbb{K}}$ y $\mathfrak{a} = (\alpha)$, entonces $N(\mathfrak{a}) = |N_{\mathbb{K}}(\alpha)|$.*

Lema 1.2.12. *Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_{\mathbb{K}}$, entonces $N(\mathfrak{p})$ es una potencia del primo racional del Lema 1.2.5.*

Una consecuencia inmediata de los lemas anteriores es el siguiente resultado fundamental:

Teorema 1.2.9. *Sea $\mathbb{K}$ un cuerpo numérico de grado n y p un primo racional. Consideramos el ideal generado por p en $\mathcal{O}_{\mathbb{K}}$ con factorización*

$$p\mathcal{O}_{\mathbb{K}} = \prod_{i=1}^{r} {\mathfrak{p}_i}^{e_i}$$

donde los $\mathfrak{p}_i$'s son ideales primos distintos. Entones existen números naturales f_i tales que $N(\mathfrak{p}_i) = p^{f_i}$, y además

$$\sum_{i}^{r} e_i f_i = n.$$

Este teorema nos permite introducir una importante terminología concerniente a la factorización de un ideal generado por un primo racional. Sean p, $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ como en el Teorema 1.2.9, llamaremos a los ideales primos $\mathfrak{p}_i$, los ideales primos que están *debajo* de p, así mismo, diremos que p es el único primo racional *encima* de $\mathfrak{p}_i$'s, y los e_i's se los llama el *índice de ramificación* de $\mathfrak{p}_i$'s| p.
También diremos que p es *ramificado* en $\mathcal{O}_{\mathbb{K}}$ si $e_i \geq 2$ para algún i. Además, p es *totalmente ramificado* en $\mathcal{O}_{\mathbb{K}}$ si $(p) = \mathfrak{p}^n$ para algún ideal primo $\mathfrak{p}$. A un primo racional p se le dice *inerte* en $\mathcal{O}_{\mathbb{K}}$ si (p) es un ideal primo y finalmente p se *descompone completamente* en $\mathcal{O}_{\mathbb{K}}$ si $r = n$, así $e_i = f_i = 1$, es decir, si (p) se factoriza como producto de n ideales primos distintos, cada uno con norma p. Por último, tenemos el siguiente resultado importante en torno a esta notación, que relaciona el discriminante de $\mathbb{K}$ definido anteriormente.

Teorema 1.2.10 (Teorema de Dedekind)**.** *Sea $\mathbb{K}$ un cuerpo numérico y p un primo racional, entonces p se ramifica en $\mathcal{O}_{\mathbb{K}}$ si y sólo si $p \mid d_{\mathbb{K}}$.*

Extensiones de Galois y descomposición de primos

Sea $\mathbb{K}/\mathbb{Q}$ una extensión de Galois, donde $\mathbb{K}$ es cuerpo numérico de grado n sobre $\mathbb{Q}$. Si $\sigma_1, \ldots, \sigma_n$ son las n inmersiones de $\mathbb{K}$ en $\mathbb{C}$, entonces estas forman un grupo bajo la composición, denominado el grupo de Galois de $\mathbb{K}/\mathbb{Q}$ y es denotado por $Gal(\mathbb{K}/\mathbb{Q})$. Ahora, si p es un primo racional y descomponemos el ideal generado por p como producto de ideales primos distintos de $\mathcal{O}_{\mathbb{K}}$:

$$p\mathcal{O}_{\mathbb{K}} = {\mathfrak{p}_1}^{e_1}{\mathfrak{p}_2}^{e_2} \cdots {\mathfrak{p}_r}^{e_r},$$

entonces se puede mostrar que $Gal(\mathbb{K}/\mathbb{Q})$ actúa sobre el conjunto $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ mediante la acción $\sigma_i \mathfrak{p}_j \to \sigma_i(\mathfrak{p}_j)$. Respecto a la notación, tenemos dos resultados interesantes que tomamos de [7, sec 3.3.6], los cuales dan una propiedad a la acción definida anteriormente y una condición adicional a la proporcionada por el Teorema 1.2.9.

Lema 1.2.13. *Sea $\mathbb{K}/\mathbb{Q}$ una extensión de Galois, entonces $Gal(\mathbb{K}/\mathbb{Q})$ actúa transitivamente en el conjunto $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$, esto es, para cualquier par $\mathfrak{p}_j, \mathfrak{p}_{j'}$ con $1 \leq j, j' \leq r$, existe $\sigma \in Gal(\mathbb{K}/\mathbb{Q})$ tal que $\mathfrak{p}_j = \sigma \mathfrak{p}_{j'}$.*

En general los e_i's y los f_i's del Teorema 1.2.9 son distintos, pero si $\mathbb{K}/\mathbb{Q}$ es una extensión de Galois, el lema anterior implica:

Teorema 1.2.11. *Sea $\mathbb{K}$ un cuerpo numérico de grado n sobre $\mathbb{Q}$. Si la extensión $\mathbb{K}/\mathbb{Q}$ es de Galois, entonces en notación del Teorema 1.2.9, $e_1 = e_2 = \cdots = e_r$ y $f_1 = f_2 = \cdots = f_r$, luego denotando por e al valor común de los e_i's (resp. los f_i's) tenemos $n = efr$.*

1.3. Breve introducción al análisis p-ádico

Sea $\mathbb{K}$ un cuerpo, un *valor absoluto* en $\mathbb{K}$ es una función $|\ | : \mathbb{K} \longrightarrow \mathbb{R}$ que satisface las siguientes propiedades:

i. $|x| \geq 0$ para todo $x \in \mathbb{K}$ y $|x| = 0$ si y sólo si $x = 0$.

ii. $|xy| = |x|\,|y|$ para todo $x, y \in \mathbb{K}$.

iii. $|x + y| \leq |x| + |y|$ para todo $x, y \in \mathbb{K}$.

Se dice que un valor absoluto en $\mathbb{K}$ es *no-arquimediano* si este satisface la condición adicional

iv. $|x + y| \leq \max\{|x|, |y|\}$ para todo $x, y \in \mathbb{K}$

de lo contrario, diremos que el valor absoluto es *arquimediano*.
Sabemos que dado un valor absoluto $|*|$ definido en $\mathbb{K}$, podemos definir una métrica en $\mathbb{K}$ dada por

$$d(x, y) = |x - y|, \text{ para todo } x, y \in \mathbb{K},$$

y esta métrica induce una topología en $\mathbb{K}$, lo que nos permite hablar de conjuntos abiertos, conjuntos cerrados, sucesiones convergentes, sucesiones de Cauchy, completez, etc. De la definición de valor absoluto tenemos de inmediato:

Lema 1.3.1. *Si $|*|$ un valor absoluto en un cuerpo $\mathbb{K}$, entonces para $a, b \in \mathbb{K}$, $n \in \mathbb{Z}$*

(i.) $|1| = 1$.

(ii.) *Si* $|a|^n = 1$ *entonces* $|a| = 1$.

(iii.) $|-1| = 1$, *y por tanto,* $|-a| = |a|$.

(iv.) *Si* $|*|$ *es no-arquimediano y* $|a| \neq |b|$ *entonces* $|a+b| = \max\{|a|, |b|\}$.

La cuarta propiedad del lema anterior es conocida como la propiedad del *triángulo isósceles*, ya que dice que en un triángulo con dos lados de magnitud $|a|$, $|b|$, el tercer lado $|a+b|$ es de igual magnitud al mayor entre los dos primeros, lo que implica que todos los triángulos son isósceles, siempre que $|\ |$ sea no-arquimediano.
Si $|*|$ y $|*|'$ son dos valores absolutos en un cuerpo $\mathbb{K}$, se dice que estos son *equivalentes* si inducen la misma topología en $\mathbb{K}$. Se puede mostrar que esta relación en el conjunto de valores absolutos en $\mathbb{K}$ define una relación de equivalencia.

Lema 1.3.2. *Dos valores absolutos $|*|$ y $|*|'$ definidos en un cuerpo $\mathbb{K}$ son equivalentes si y sólo si existe una constante $\lambda \in \mathbb{R}^+$, tal que $|*|' = |*|^\lambda$.*

Valores absolutos en $\mathbb{Q}$.

Con $\mathbb{K} = \mathbb{Q}$ el valor absoluto usual es un ejemplo de un valor absoluto arquimediano. Ahora definimos en $\mathbb{Q}$ el valor absoluto *p-ádico* denotado por $|*|_p$. Si $m \in \mathbb{Z}$, el *orden p-ádico* de m, denotado por $ord_p\, m$, es el exponente de la máxima potencia de p que divide a m, y lo extendemos a $\mathbb{Q}$ por la fórmula $ord_p\, a/b = ord_p\, a - ord_p\, b$, entonces para $a \in \mathbb{Q}$ definimos

$$|a|_p := \begin{cases} 0, & \text{si } a = 0, \\ p^{-\,ord_p\, a}, & \text{si } a \neq 0. \end{cases}$$

Es fácil mostrar que $|*|_p$ es un valor absoluto no-arquimediano en $\mathbb{Q}$. También podemos mencionar que $\mathbb{Q}$ junto a la métrica inducida por $|*|_p$ es un espacio métrico no completo, en el sentido de que existen sucesiones de Cauchy que no convergen. La completación[3] de $\mathbb{Q}$ respecto a la métrica inducida por

[3]La completación de un espacio métrico (M, d) es un espacio completo $(\tilde{M}, \tilde{d})$ el cual contiene a M, además M es denso en $\tilde{M}$ y $\tilde{d}|_M = d$. En la referencia [10, cap. 2] podemos ver la prueba de que $(\mathbb{Q}, |\ |_p)$ es un un espacio métrico no completo, la construcción detallada del cuerpo $\mathbb{Q}_p$ y también algunas propiedades algebraicas y topológicas de $\mathbb{Z}_{(p)}$ y $p\mathbb{Z}_{(p)}$.

$|*|_p$ es denotado por $\mathbb{Q}_p$, *el cuerpo de números p-ádicos*. En $\mathbb{Q}_p$ existen dos conjunto importantes,

$$\mathbb{Z}_{(p)} := \left\{ z \in \mathbb{Q}_p : |z|_p \leq 1 \right\},$$

el cual es un subanillo de $\mathbb{Q}_p$, llamado el anillo de enteros p-ádicos, y

$$p\mathbb{Z}_{(p)} = \left\{ z \in \mathbb{Q}_p : |z|_p < 1 \right\},$$

el cual es el único ideal maximal de $\mathbb{Z}_{(p)}$, y por tanto $\mathbb{Z}_{(p)}$ es un anillo local, además

$$\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}.$$

Valores absolutos en $\mathbb{K}$.

Sea $\mathbb{K}$ un cuerpo numérico de grado n sobre $\mathbb{Q}$. Definiremos dos conjuntos importantes de valores absolutos determinados por los ideales primos de $\mathcal{O}_{\mathbb{K}}$ y por las n inmersiones de $\mathbb{K}$ en $\mathbb{C}$.
Si σ es una de las n inmersiones de $\mathbb{K}$ en $\mathbb{C}$, entonces para cualquier $\alpha \in \mathbb{K}$ se define $|\alpha|_\sigma = |\sigma(\alpha)|$, donde $|*|$ es el módulo complejo usual, entonces se sigue de inmediato que $|*|_\sigma$ define un valor absoluto arquimediano en $\mathbb{K}$.
Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_{\mathbb{K}}$, el orden $\mathfrak{p}$-*ádico* de un elemento no nulo $\alpha \in \mathcal{O}_{\mathbb{K}}$, $ord_{\mathfrak{p}}\,\alpha$, es exponente de la máxima potencia $\mathfrak{p}$ que aparece en la factorización en ideales primos del ideal generado por α, si $\alpha \in \mathbb{K}\backslash\mathcal{O}_{\mathbb{K}}$, sabemos que existe $m \in \mathbb{Z}$ tal que $\beta = m\alpha \in \mathcal{O}_{\mathbb{K}}$, entonces $ord_{\mathfrak{p}}\,\alpha = ord_{\mathfrak{p}}\,\beta - ord_{\mathfrak{p}}\,m$. Finalmente definimos para $\alpha \in \mathbb{K}$,

$$|\alpha|_{\mathfrak{p}} := \begin{cases} 0, & \text{si } \alpha = 0, \\ N(\mathfrak{p})^{-\,ord_{\mathfrak{p}}\,\alpha}, & \text{si } \alpha \neq 0, \end{cases}$$

donde $N(\mathfrak{p})$ es la norma de $\mathfrak{p}$. Por ejemplo si $p\mathcal{O}_{\mathbb{K}}$ se descompone como en el Teorema 1.2.9 entonces $|p|_{\mathfrak{p}_i} = N(\mathfrak{p}_i)^{-e_i}$.
Es fácil verificar que $|*|_{\mathfrak{p}}$ es un valor absoluto no arquimediano, llamado el valor absoluto $\mathfrak{p}$-*ádico*, además si $\mathfrak{p}$ y $\mathfrak{q}$ son ideales primos distintos entonces se puede mostrar que $|*|_{\mathfrak{p}}$ y $|*|_{\mathfrak{q}}$ no son equivalentes. Por otro lado, su completación denotada por $\mathbb{K}_{\mathfrak{p}}$ es el cuerpo de números $\mathfrak{p}$-*ádicos*, además $\mathbb{K}_{\mathfrak{p}}$ es una extensión finita de $\mathbb{Q}_p$ donde p es el primo racional encima de $\mathfrak{p}$.
El siguiente teorema caracteriza por completo el conjunto de valores absolutos que se pueden definir en un cuerpo numérico $\mathbb{K}$, los cuales están relacionados con los dos conjuntos definidos anteriormente.

Teorema 1.3.1 (Teorema de Ostrowski)**.** *Sea $\mathbb{K}$ un cuerpo numérico, entonces todo valor absoluto arquimediano de $\mathbb{K}$ es equivalente a uno de los valores absolutos determinados por alguna inmersión de $\mathbb{K}$ en $\mathbb{C}$. Y todo valor absoluto no-arquimediano de $\mathbb{K}$ es equivalente a un valor absoluto $\mathfrak{p}$-ádico $|*|_{\mathfrak{p}}$ determinado por un ideal primo $\mathfrak{p}$ de $\mathcal{O}_{\mathbb{K}}$.*

Enteros algebraicos, unidades y valores absolutos.

Al inicio de este capítulo introducimos la noción de entero algebraico, existe una manera alterna de definirlo utilizando valores absolutos en $\mathbb{K}$, la cual mencionamos en el siguiente teorema y es equivalente a la adoptada inicialmente. Para los últimos retultados de esta sección usamos la referencia [6].

Teorema 1.3.2. *Sea $\mathbb{K}$ un cuerpo numérico y $\alpha \in \mathbb{K}$, las siguientes condiciones son equivalentes:*

(i) α *es un entero algebraico.*

(ii) $|\alpha| \leq 1$ *para todo valor absoluto no-arquimediano en* $\mathbb{K}$.

A un elemento no nulo $u \in \mathcal{O}_{\mathbb{K}}$ se lo llama una *unidad*, si existe $v \in \mathcal{O}_{\mathbb{K}}$ tal que $uv = 1$. Es fácil ver que si u es una unidad, entonces $|u|_{\mathfrak{p}} = 1$ para todo ideal primo de $\mathcal{O}_{\mathbb{K}}$ y por el Teorema de Ostrowki $|u| = 1$ para todo valor absoluto $|*|$ no-arquimediano, la afirmación recíproca también es cierta y adicionalmente tenemos,

Teorema 1.3.3. *Sea $\mathbb{K}$ un cuerpo numérico y $u \in \mathbb{K}$, las siguientes condiciones son equivalentes*

(i) u *es una unidad de* $\mathcal{O}_{\mathbb{K}}$.

(ii) $|u|_{\mathfrak{p}} = 1$ *para todo valor absoluto no-arquimediano de* $\mathbb{K}$.

(iii) $u \in \mathcal{O}_{\mathbb{K}}$ *y* $|N_{\mathbb{K}/\mathbb{Q}}(u)| = 1$.

A un elemento $\alpha \in \mathbb{K}$ se lo llama una *raíz de la unidad* si $\alpha^n = 1$ para algún $n \in \mathbb{Z}^+$. Por el Lema 1.3.1 (ii), si α es una raíz de la unidad, entonces $|\alpha| = 1$ para cualquier valor absoluto $|*|$ en $\mathbb{K}$, como antes la afirmación recíproca también es cierta, esto es,

Teorema 1.3.4. *Sea $\mathbb{K}$ un cuerpo numérico y $\alpha \in \mathbb{K}$, entonces α es una raíz de la unidad si y sólo si $|\alpha| = 1$ para todo valor absoluto $|*|$ en $\mathbb{K}$.*

1.4. Formas lineales en logaritmos

En 1966, A. Baker [2] halló una cota inferior para las formas lineales en logaritmos de números algebraicos; es decir, para una expresión de la forma

$$b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n,$$

donde $\alpha_1, \ldots, \alpha_n$ son números algebraicos y $b_1, \ldots, b_n$ son números racionales. Su resultado marcó el principio de la era de la resolución efectiva de ecuaciones diofánticas[4]. Los primeros resultados al respecto son los siguientes.

Teorema 1.4.1 (A. Baker, 1966)**.** *Sean $\alpha_1, \ldots, \alpha_n$ números algebraicos y $b_1, \ldots, b_n$ números racionales tales que*

$$b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n \neq 0.$$

Entonces

$$|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| > (eB)^C,$$

donde $B := \max\{|b_1|, \ldots, |b_n|\}$ y C es una constante efectivamente calculable que depende sólo de n y $\alpha_1, \ldots, \alpha_n$.

Para un número complejo ω, consideramos $\log \omega := \log |\omega| + i \arg \omega$ donde $\arg \omega$ es tomado en $(-\pi, \pi]$. Ahora, si $|\omega| < 1/2$, entonces tenemos la desigualdad $|\log(\omega + 1)| < 2|\omega|$. Usando este hecho es posible modificar el teorema anterior y eliminar los logaritmos, obteniendo:

Corolario 1.4.1. *Sean $\alpha_1, \ldots, \alpha_n$ números algebraicos y $b_1, \ldots, b_n$ números racionales tales que*

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1.$$

Entonces

$$\left|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1\right| > (eB)^{C_1},$$

donde de nuevo $B := \max\{|b_1|, \ldots, |b_n|\}$ y C_1 es una constante efectivamente calculable que depende sólo de n y $\alpha_1, \ldots, \alpha_n$.

Un caso especial es cuando $b_1, \ldots, b_n$ son enteros. Al respecto se conoce un resultado reciente debido a Matveev [16] donde tenemos explícitamente la cota inferior para $\left|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1\right|$ del Corolario 1.4.1. Antes de presentar

[4] Una ecuación diofántica es una ecuación en la cual su solución debe ser entera, racional o más generalmente en cualquier anillo de enteros de un cuerpo numérico $\mathbb{K}$.

dicho resultado, es necesario introducir dos medidas algebraicas, las cuales están relacionadas entre si y serán usadas en los próximos capítulos.

Sea η un número algebraico de grado d sobre $\mathbb{Q}$ con polinomio minimal primitivo[5] sobre los enteros

$$f(x) := a_0 \prod_{i=1}^{d} (x - \eta^{(i)}) \in \mathbb{Z}[x],$$

donde $a_0 > 0$ y $\eta = \eta^{(1)}, \eta^{(2)}, \ldots, \eta^{(d)}$ son los conjugados de η.
La *altura canónica* de η es dada por

$$H(\eta) := \left(a_0 \prod_{i=1}^{d} \max\{1, |\eta^{(i)}|\} \right)^{1/d}.$$

La *altura logarítmica* de η es dada por

$$h(\eta) := \log H(\eta) = \frac{1}{d} \left(\log a_0 + \sum_{i=1}^{d} \log \max\{|\eta^{(i)}|, 1\} \right).$$

A continuación, presentamos el resultado de Matveev [16], el cual será nuestra herramienta principal para resolver el problema del capítulo 3 de este trabajo.
Sean $\eta_1, \ldots, \eta_n$ elementos no nulos de un cuerpo numérico $\mathbb{K}$ de grado D sobre $\mathbb{Q}$, y sean $b_1, \ldots, b_n$ enteros racionales. Definimos

$$B = \max\{|b_1|, \ldots, |b_n|\},$$

y

$$\Lambda = \eta_1^{b_1} \cdots \eta_n^{b_n} - 1.$$

Sean $A_1, \ldots, A_n$ números reales positivos tales que

$$A_i \geq \max\{Dh(\eta_i),\ |\log \eta_i|,\ 0{,}16\}, \quad i = 1, \ldots, n.$$

Teniendo en cuenta esta notación Matveev probó el siguiente resultado.

Teorema 1.4.2 (Teorema de Matveev [16]). *Si $\Lambda \neq 0$, entonces*

$$|\Lambda| > \exp\left(-3 \cdot 30^{n+4} (n+1)^{5,5} D^2 (1 + \log D)(1 + \log nB) A_1 \cdots A_n\right).$$

En muchos casos esta herramienta permite determinar que un problema diofántico tiene una cantidad finita de soluciones, o equivalentemente que las incógnitas enteras del problema están acotadas.

[5] Un polinomio primitivo es tal que el máximo común divisor de los coeficientes es igual a 1.

1.5. Recurrencias lineales y cero multiplicidad

Como concepto principal de esta investigación, presentamos la definición de *sucesión lineal recurrente* y en relación a esta la noción de *cero multiplicidad*. Presentaremos algunos resultados clásicos en esta teoría los cuales son el punto de partida de este trabajo de investigación.
Sea $k \geq 2$ un entero, una sucesión $(u_n)_{n\geq 0} \subseteq \mathbb{C}$ es una *sucesión lineal recurrente de orden* k si se satisface una relación de recurrencia de la forma

$$u_{n+k} = a_1 u_{n+k-1} + a_2 u_{n+k-2} + \cdots + a_k u_n, \qquad \text{para todo} \quad n \geq 0,$$

con *coeficientes* $a_1, \ldots, a_k$ $(a_k \neq 0)$ y *valores iniciales fijos* $u_0, \ldots, u_{k-1}$ en $\mathbb{C}$. Podemos extender la sucesión a subíndices negativos mediante la fórmula:

$$u_n = (1/a_k)(u_{n+k} - a_1 u_{n+k-1} - a_2 u_{n+k-2} - \cdots - a_{k-1} u_{n+1}), \quad \text{para todo } n < 0.$$

A una sucesión de orden 2 se la llama *binaria*, a una de orden 3 *ternaria*, etc. Cada sucesión lineal recurrente de orden k tiene asociado un polinomio de grado k, llamado el *polinomio característico* de la recurrencia, el cual es dado por

$$f(x) = x^k - a_1 x^{k-1} - \cdots - a_{k-1} x - a_k \in \mathbb{C}[x].$$

Si $\alpha^{(1)}, \ldots, \alpha^{(s)}$ son las raíces distintas de $f(x)$ con multiplicidades $m_1, \ldots, m_s$, respectivamente, entonces mediante el uso de la *función generatriz* $u(z) = \sum_n u_n z^n$ de $(u_n)_{n\geq 0}$, podemos estimar la siguiente fórmula para u_n:

$$u_n = \sum_{i=1}^{s} p_i(n)(\alpha^{(i)})^n, \qquad \text{para todo} \quad n \geq 0, \tag{1.1}$$

donde $p_1(x), \ldots, p_s(x) \in \mathbb{Q}(u_0, \ldots, u_{k-1}, a_1, \ldots, a_k, \alpha^{(1)}, \ldots, \alpha^{(s)})[x]$ y $\deg(p_i) \leq m_i - 1$ para $i = 1, \ldots, s$.
Una sucesión lineal recurrente $(u_n)_{n\geq 0}$ de orden k, se la llama *simple* si las raíces de su polinomio característico son distintas. Si $(u_n)_{\geq 0}$ es simple se obtiene

$$u_n = \sum_{i=1}^{k} c_i(\alpha^{(i)})^n,$$

donde $c_1, \ldots, c_k \in \mathbb{Q}(u_0, \ldots, u_{k-1}, a_1, \ldots, a_k, \alpha^{(1)}, \ldots, \alpha^{(s)})$.
Si en una sucesión lineal recurrente $(u_n)_{n\geq 0}$ sus coeficientes y sus valores iniciales pertenecen a $\mathbb{Z}$, diremos que la sucesión es de números enteros (*resp.* de números racionales, algebraicos o complejos).

En el estudio de las propiedades aritméticas de la sucesiones lineales recurrentes, un problema clásico es determinar la cantidad de veces que aparece cierto valor a en la sucesión $(u_n)_{n\geq 0}$, lo que se conoce como la *a-multiplicidad* de la sucesión. En particular cuando $a = 0$, diremos respectivamente la *cero-multiplicidad* de la sucesión. El siguiente teorema y su corolario proporcionan propiedades de una sucesión lineal recurrente con cero-multiplicidad infinita.

Teorema 1.5.1 (Skolem-Malher-Lech 1953[13]). *Si $(u_n)_{n\geq 0}$ es una sucesión lineal recurrente con cero-multiplicidad infinita, entonces el conjunto de $n's$ para los cuales $u_n = 0$ es un conjunto finito junto a unión finita de progresiones aritméticas.*

Como consecuencia del teorema anterior tenemos el siguiente resultado, el cual es el punto de partida de diversas investigaciones respecto a la cero-multiplicidad de sucesiones lineales recurrentes, ya que proporciona información acerca de la cero-multiplicidad infinita con relación a las raíces de su polinomio característico.

Corolario 1.5.1. *Si una sucesión lineal recurrente tiene cero-multiplicidad infinita, entonces el cociente de dos raíces distintas del polinomio característico es una raíz de la unidad.*

Este corolario motiva a la siguiente definición, una sucesión lineal recurrente es llamada *degenerada* si su polinomio característico tiene dos raíces distintas tales que su cociente es una raíz de la unidad, en otro caso, se la llama *no degenerada*. El siguiente corolario, contrarecíproco del anterior, caracteriza la cero-multiplicidad de las sucesiones lineales recurrentes no degeneradas.

Corolario 1.5.2. *Toda sucesión lineal recurrente no degenerada tiene cero multiplicidad finita.*

Es preciso mencionar que la demostración del Teorema 1.5.1 la cual puede ser consultada en [6], es realizada de forma no constructiva usando métodos del análisis p-ádico. Por tanto la conclusión del Corolario 1.5.2, que caracteriza la cero-multiplicidad de la sucesiones lineales recurrentes no degeneradas, que dice de hecho que es finita, es gran un avance. Pero no es suficiente ya que al no ser constructiva la demostración, no es posible establecer un algoritmo para encontrar los subíndices n donde la sucesión de hace cero. De ahí que, un problema en teoría de sucesiones lineales recurrentes, específicamente en las sucesiones no degeneradas, sea determinar una cota efectiva para su cero multiplicidad.

Capítulo 2

Cero-multiplicidad de sucesiones lineales recurrentes ternarias.

2.1. Introducción

El propósito de este capítulo es mostrar que una sucesión lineal recurrente ternaria no degenerada de números racionales tiene cero-multiplicidad a lo más seis. Si las raíces del polinomio característico de una sucesión lineal recurrente son todas reales, el problema se vuelve un poco más sencillo de resolver, y en este caso Smiley [22] mostró con un simple argumento apoyado en la ley de signos de Descartes, que la cero multiplicidad para sucesiones recurrentes de orden 3 es a lo más 3 y de manera general cuando el orden de la recurrencia es $k \geq 4$, Hagedorn [11] mostró que la cero multiplicidad es a lo más $2k-3$. En 1957 fue conjeturado por Ward en [24] que la cero-multiplicidad de una sucesión lineal recurrente ternaria no degenerada es a lo sumo cinco, sin embargo, esto no era cierto ya que Berstel en [5] mostró que la sucesión con relación de recurrencia $B_{n+3} = 2B_{n+2} - 4B_{n+1} + 4B_n$ y valores iniciales $B_0 = B_1 = 0$ y $B_2 = 1$ tiene cero-multiplicidad 6, ya que $B_0 = B_1 = B_4 = B_6 = B_{13} = B_{52} = 0$. Más adelante Buekers demostró en [3] que 6 es efectivamente la cota superior para la cero multiplicidad de cualquier sucesión recurrente ternaria no degenerada. En este capítulo mostraremos el resultado de Beukers, reproduciendo su método y completando algunos detalles de su trabajo.

Beukers parte de una sucesión lineal recurrente ternaria no degenerada arbitraria de números racionales, digamos $u_{n+3} = Pu_{n+2} + Qu_{n+1} + Ru_n$ con valores iniciales u_0, u_1, u_2 no todos nulos, de ahí, con argumentos propor-

cionados por el análisis p-ádico, muestra que si $\theta_1, \theta_2, \theta_3$ son las raíces del polinomio característico $x^3 - Px^2 - Qx - R$, entonces $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}} = |\theta_3|_{\mathfrak{p}}$ para todos los valores absolutos no arquimedianos de $\mathbb{K} = \mathbb{Q}(\theta_1, \theta_2)$, lo cual permite descartar posibles valores de los coeficientes $P,\ Q,\ R$ de la relación de recurrencia y de los posibles valores iniciales, para obtener una lista de 3 sucesiones lineales recurrentes ternarias no degeneradas, entonces todo se reduce a probar que estas tres sucesiones recurrentes no tienen más de 6 ceros, los cuales son dados explícitamente.

2.2. Algunos lemas técnicos.

Beukers resolvió el problema para a-multiplicidad de sucesiones recurrentes binarias complejas en [4], para lo cual trató la ecuación

$$\lambda\alpha^x + \mu\beta^x = 1, \quad x \in \mathbb{Z} \tag{2.1}$$

donde $\lambda, \alpha, \mu, \beta$ son números algebraicos no nulos en algún cuerpo numérico $\mathbb{K}$ y α, β y α/β no son raíces de la unidad. Usando algunos resultados de este trabajo, Buekers resolvió el problema de la cero-multiplicidad de sucesiones lineales recurrentes ternarias de números racionales, debido a que para resolver este último debemos tratar con la ecuación

$$a_1\theta_1^n + a_2\theta_2^n + a_3\theta_3^n = 0 \text{ con } n \in \mathbb{Z},$$

la cual, como podemos notar es equivalente a (2.1). En efecto, dividiendo esta ecuación por alguno de sus términos, es decir

$$\left(-\frac{a_1}{a_2}\right)\left(\frac{\theta_1}{\theta_2}\right)^n + \left(-\frac{a_3}{a_2}\right)\left(\frac{\theta_3}{\theta_2}\right)^n = 1,$$

$$\left(-\frac{a_1}{a_2}\right)\left(\frac{\theta_2}{\theta 1}\right)^n + \left(-\frac{a_3}{a_2}\right)\left(\frac{\theta_2}{\theta_3}\right)^n = 1.$$

La idea de esta sección es mostrar que la ecuación (2.1) no tiene más de 6 soluciones para un gran conjunto de posibles valores de α y β, con lo cual mostraremos que $a_1\theta_1^n + a_2\theta_2^n + a_3\theta_3^n = 0$ con $n \in \mathbb{Z}$, no tiene más de seis ceros.

Los primeros tres lemas tienen por objetivo crear grandes distancias entre tres soluciones no nulas de la ecuación. Recordemos que si $\mathbb{K}$ es un cuerpo numérico y $\mathcal{O}_{\mathbb{K}}$ es su anillo de enteros algebraicos, y $\mathfrak{p}$ es un ideal primo no nulo de $\mathcal{O}_{\mathbb{K}}$ entonces $|*|_{\mathfrak{p}}$ denota el valor absoluto no-aquimediano en $\mathbb{K}$ definido por $\mathfrak{p}$.

Lema 2.2.1. *Sea $\mathbb{K}$ un cuerpo numérico y $\mathfrak{p}$ un ideal primo de $\mathcal{O}_{\mathbb{K}}$ tal que $|\alpha|_{\mathfrak{p}} < 1$ y $|\beta|_{\mathfrak{p}} = 1$. Asumimos que $0, k, l, m$, con $0 < k < l < m$, son soluciones para x de la ecuación*

$$\lambda\alpha^x + \mu\beta^x = 1, \quad x \in \mathbb{Z},$$

donde $\lambda\alpha\mu\beta \neq 0$, entonces existe un entero positivo d con las siguientes propiedades:

(i) $d > 1$ *y* d *divide* $m - l$ *y* $l - k$.

(ii) Si hay una solución extra n *con* $0 < n < k$, *entonces* $d \geq 4$.

(iii) Si $|\alpha|_{\mathfrak{p}}^k |\beta - 1|_{\mathfrak{p}} < |p|_{\mathfrak{p}}^{1/p-1}$, *donde* p *es el primo racional encima de* $\mathfrak{p}$, *entonces* $|(m-l)/d|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^{l-k}$.

Demostración. Dado que 0 es solución de (2.1) entonces $\lambda + \mu = 1$, luego

$$\begin{aligned} \lambda\alpha^x + \mu\beta^x = 1 \quad &\Rightarrow \quad \lambda\alpha^x + (1-\lambda)\beta^x = 1 \\ &\Rightarrow \quad -\lambda\alpha^x - \beta^x + \lambda\beta^x = -1 \\ &\Rightarrow \quad \lambda\beta^x - \beta^x - \lambda + 1 = \lambda\alpha^x - \lambda \\ &\Rightarrow \quad \beta^x - 1 = \lambda(\lambda-1)^{-1}(\alpha^x - 1). \end{aligned}$$

Ahora tomando valor $\mathfrak{p}$-ádico en la última línea obtenemos

$$|\beta^x - 1|_{\mathfrak{p}} = \left|\lambda(\lambda-1)^{-1}\right|_{\mathfrak{p}} |\alpha^x - 1|_{\mathfrak{p}}. \tag{2.2}$$

Dado que $|\alpha^x - 1|_{\mathfrak{p}} = \max\{|\alpha^x|_{\mathfrak{p}}, 1\} = 1$ para todo $x \in \mathbb{Z}^+$, entonces de la ecuación (2.2) obtenemos que $|\beta^k - 1|_{\mathfrak{p}} = |\beta^l - 1|_{\mathfrak{p}} = |\beta^m - 1|_{\mathfrak{p}}$. Denotamos este valor por B y teniendo en cuenta la propiedad no arquimediana de $|*|_{\mathfrak{p}}$ tenemos que

$$\begin{aligned} B = |\beta^k - 1|_{\mathfrak{p}} &= |\beta - 1|_{\mathfrak{p}} |\beta^{k-1} + \cdots + 1|_{\mathfrak{p}} \\ &\leq |\beta - 1|_{\mathfrak{p}} \cdot \max_{0 \leq j \leq k-1} |\beta|_{\mathfrak{p}}^j \\ &\leq |\beta - 1|_{\mathfrak{p}}, \end{aligned} \tag{2.3}$$

dado que $|\beta|_{\mathfrak{p}} = 1$. Por la eliminación de λ, μ de $\lambda\alpha^x + \mu\beta^x = 1$ con $x = 0, k, l$, se tiene que

$$\lambda(\lambda-1)^{-1} = \frac{\beta^k - 1}{\alpha^k - 1} = \frac{\beta^l - 1}{\alpha^l - 1},$$

reescribiendo la ecuación se obtiene

$$\beta^l - \beta^k = (\beta^l - 1)\alpha^k - (\beta^k - 1)\alpha^l.$$

Tomando valor absoluto $\mathfrak{p}$-ádico a ambos lados de la ecuación anterior obtenemos

$$|\beta^l - \beta^k|_{\mathfrak{p}} = \left|(\beta^l - 1)\alpha^k - (\beta^k - 1)\alpha^l\right|_{\mathfrak{p}},$$

dado que $k < l$, entonces $\left|(\beta^l - 1)\alpha^k\right|_{\mathfrak{p}} \neq \left|(\beta^k - 1)\alpha^l\right|_{\mathfrak{p}}$, luego usando la propiedad del triángulo isósceles de $|*|_{\mathfrak{p}}$ tenemos que

$$\begin{aligned} |\beta^l - \beta^k|_{\mathfrak{p}} &= \text{máx}\{|\alpha|_{\mathfrak{p}}^k |\beta^l - 1|_{\mathfrak{p}},\ |\alpha|_{\mathfrak{p}}^l |\beta^k - 1|_{\mathfrak{p}}\} \\ &= \text{máx}\{|\alpha|_{\mathfrak{p}}^k B,\ |\alpha|_{\mathfrak{p}}^l B\} \\ &= |\alpha|_{\mathfrak{p}}^k B \end{aligned}$$

y como $|\beta|_{\mathfrak{p}} = 1$,

$$|\beta^{l-k} - 1|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^k B. \tag{2.4}$$

De manera análoga,

$$|\beta^{m-l} - 1|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^l B. \tag{2.5}$$

Sea d, el menor entero positivo tal que $|\beta^d - 1|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^k B$, entonces $d > 1$, ya que $d = 1$ implica que $|\beta - 1|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^k B < |\beta - 1|_{\mathfrak{p}}$, lo cual es una contradicción. Además, si para algún $y \in \mathbb{Z}^+$ se tiene que $|\beta^y - 1|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^k Q$ entonces $d \mid y$, en efecto;
Si $d \nmid y$, entonces $y = dt + r$, para algunos $t, r \in \mathbb{Z}^+$ con $0 < r < d$, entonces usando nuevamente la propiedad del triángulo isósceles de $|\ |_{\mathfrak{p}}$ obtenemos

$$\begin{aligned} |\alpha|_{\mathfrak{p}}^k Q \geq |\beta^y - 1|_{\mathfrak{p}} &= |\beta^y - \beta^r + \beta^r - 1|_{\mathfrak{p}} \\ &= \text{máx}\{|\beta^y - \beta^r|_{\mathfrak{p}}, |\beta^r - 1|_{\mathfrak{p}}\} \\ &\geq |\beta^r - 1|_{\mathfrak{p}} \end{aligned}$$

lo que contradice la elección de d. En particular, por (2.4) y (2.5) $d \mid (l-k)$ y $d \mid (m-l)$, lo cual demuestra la primera afirmación. Note también que (2.4) y la propiedad no arquimediana de $|\ |_{\mathfrak{p}}$ implican que $|\beta^d - 1|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^k B$. Para probar la segunda afirmación obtenemos de manera similar como se hizo para (2.4), que $|\beta^{k-n} - 1|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^n B$. Así mismo se escoge el menor entero positivo e tal que $|\beta^e - 1|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^n B$. Por los mismos argumentos anteriores, $e > 1$, si $|\beta^y - 1|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^n Q$ entonces $e \mid y$. Ahora $\left|\beta^d - 1\right|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^k B < |\alpha|_{\mathfrak{p}}^n B$ luego e debe ser un divisor distinto de 1 de d, por tanto $d \geq 4$.

Para probar la tercera afirmación, sea $\beta^d = 1+\gamma$ luego $|\gamma|_{\mathfrak{p}} = \left|\beta^d - 1\right|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^k B$. Fijamos $t = (m-l)/d$, y entonces calculamos $|t|_{\mathfrak{p}}$.
Se tiene que

$$\begin{aligned}\beta^{m-l} - 1 =& (1+\gamma)^t - 1 = t\gamma + \binom{t}{2}\gamma^2 + \cdots + \gamma^t \\ =& t\gamma + t\gamma\left\{\binom{t-1}{1}\frac{\gamma}{2} + \binom{t-1}{2}\frac{\gamma^2}{3} + \cdots \binom{t-1}{t-1}\frac{\gamma^{t-1}}{t}\right\},\end{aligned}$$

luego tomando valor absoluto $\mathfrak{p}$-ádico a ambos lados de la igualdad anterior, se obtiene

$$|\beta^{m-l} - 1|_{\mathfrak{p}} = |t\gamma + t\gamma G|_{\mathfrak{p}} = \max\{|t\gamma|_{\mathfrak{p}}, |t\gamma|_{\mathfrak{p}}|G|_{\mathfrak{p}}\} \tag{2.6}$$

donde, G es la expresión entre las llaves. A continuación, hallamos una estimación para $|G|_{\mathfrak{p}}$

$$|G|_{\mathfrak{p}} \leq \max_{r\geq 2}\left|\frac{\gamma^{r-1}}{r}\right|_{\mathfrak{p}} \leq \max_{s\geq 1}\left\{|\gamma|_{\mathfrak{p}}, \left|\frac{\gamma^{p^s-1}}{p^s}\right|_{\mathfrak{p}}\right\} \leq \max_{s\geq 1}\left\{|\gamma|_{\mathfrak{p}}, \left|\frac{\gamma^{p-1}}{p}\right|_{\mathfrak{p}}^s\right\} < 1,$$

dado que $|\gamma|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^k B \leq |\alpha|_{\mathfrak{p}}^k |\beta - 1|_{\mathfrak{p}} < |p|_{\mathfrak{p}}^{1/p-1}$. Por tanto de la ecuación (2.6) se concluye que

$$|t\gamma|_{\mathfrak{p}} = |\beta^{m-l} - 1|_{\mathfrak{p}} = |\alpha|_{\mathfrak{p}}^l B$$

y finalmente,

$$|t|_{\mathfrak{p}} = \frac{|\alpha|_{\mathfrak{p}}^l B}{|\gamma|_{\mathfrak{p}}} = \frac{|\alpha|_{\mathfrak{p}}^l B}{|\alpha|_{\mathfrak{p}}^k B} = |\alpha|_{\mathfrak{p}}^{l-k}$$

como se había afirmado.

Lema 2.2.2. *Sean $0 \leq x_1 < x_2$ dos soluciones de la ecuación $\lambda\alpha^x + \mu\beta^x = 1$, con $\lambda\alpha\mu\beta \neq 0$. Suponga que existe un entero positivo d tal que x_1+d y x_2+d son también soluciones. Entonces α y β son raíces de la unidad.*

Demostración. Asumimos que x_1, x_2, $x_1 + d$ y $x_2 + d$ son soluciones de $\lambda\alpha^x + \mu\beta^x = 1$ para algún entero d, entonces $(\alpha^{x_1+d} - \alpha^{x_1})\lambda + (\beta^{x_1+d} - \beta^{x_1})\mu = 0$ y $(\alpha^{x_2+d} - \alpha^{x_2})\lambda + (\beta^{x_2+d} - \beta^{x_2})\mu = 0$. Considerando las ecuaciones anteriores como un sistema de ecuaciones lineales en las incógnitas λ y μ, tenemos que el determinante de la matriz

$$\begin{bmatrix}\alpha^{x_1+d} - \alpha^{x_1} & \beta^{x_1+d} - \beta^{x_1} \\ \alpha^{x_2+d} - \alpha^{x_2} & \beta^{x_2+d} - \beta^{x_2}\end{bmatrix}$$

debe ser cero. De ahí que $\beta^{x_1}\alpha^{x_1}(\alpha^d-1)(\beta^d-1)((\beta/\alpha)^{x_2-x_1}-1)=0$. Entonces α es una d-ésima raíz de la unidad o β es una d-ésima raíz de la unidad o β/α es una (x_2-x_1)-ésima raíz de la unidad. Primero, si α es una d-ésima raíz de la unidad entonces se obtiene $\lambda\alpha^{x_1}+\mu\beta^{x_1}=\lambda\alpha^{x_1}+\mu\beta^{x_1+d}$, de donde $\mu\beta_1^x(\beta^d-1)=0$ y por tanto β es una raíz d-ésima de la unidad. Similarmente si β es una raíz d-ésima de la unidad entonces también lo es α. Finalmente si β/α es una raíz (x_2-x_1)-ésima de la unidad, luego $(\beta/\alpha)^{x_2-x_1}=1$ entonces

$$\begin{aligned}1=&\lambda\alpha^{x_2}+\mu\beta^{x_2}\\=&\lambda\alpha^{x_2}(\beta/\alpha)^{x_2-x_1}+\mu\beta^{x_2}\\=&\lambda\alpha^{x_1}\beta^{x_2-x_1}+\mu\beta^{x_2}\\=&(\lambda\alpha^{x_1}+\mu\beta^{x_1})\beta^{x_2-x_1}\\=&\beta^{x_2-x_1},\end{aligned}$$

de ahí que β es una raíz (x_2-x_1)-ésima de la unidad. Como $(\beta/\alpha)^{x_2-x_1}=1$, así $\alpha^{x_2-x_1}=\beta^{x_2-x_1}=1$, y por tanto α también es una raíz de la unidad.

Nota. En otras palabras, el Lema 2.2.2 dice que dada una diferencia entre soluciones de (2.1), esta solo puede ocurrir una vez, a menos de que α y β sean raíces de la unidad. En particular, si α y β no son raíces de la unidad y $x_1<x_2<x_3<\cdots<x_n$ son soluciones de (2.1), entonces

$$x_n-x_1=(x_n-x_{n-1})+\cdots+(x_2-x_1)\geq 1+2+3+\cdots+n=\frac{n(n+1)}{2}=\binom{n}{2}.$$

Lema 2.2.3. *Con la misma notación de los lemas anteriores, sea $\beta=\overline{\alpha}$, $\mu=\overline{\lambda}$[1]. Si $|\alpha|\geq 4/3$ y $0,k,l,m$ son como en el lema anterior, entonces*

(i) Si $k>50$ y $10^{-4}<|\arg(\overline{\alpha}/\alpha)|<\pi-10^{-4}$, entonces $m-k\geq|\alpha|^k$.

(ii) Si $|\alpha|\geq 2{,}1$ y $k\geq 2$, entonces $m-k>2|\alpha|^k$.

Demostración. Eliminamos λ y $\overline{\lambda}$ de la ecuación $\lambda\alpha^x+\overline{\lambda}\overline{\alpha}^x=1$, con $x=0,\ k,\ l,\ m$ para obtener

$$\frac{\overline{\alpha}^k-1}{\alpha^k-1}=\frac{\overline{\alpha}^l-1}{\alpha^l-1}=\frac{\overline{\alpha}^m-1}{\alpha^m-1}. \tag{2.7}$$

[1]Aquí la barra denota la conjugación compleja. Además, el argumento de un número complejo z, denotado por $\arg z$, será tomado en $(-\pi,\pi]$

Si alguno de estos cocientes es igual a uno, entonces α^k sería real y $\overline{\alpha}/\alpha$ una raíz de la unidad, lo cual no es el caso. Sea

$$\eta = \frac{\overline{\alpha}^k - 1}{\alpha^k - 1} - 1.$$

Entonces $\eta \neq 0$ y $|\eta| \leq 2$. Notando que $\eta = \frac{\overline{\alpha}^k - \alpha^k}{\alpha^k - 1}$, concluimos que

$$\begin{aligned} \eta(\alpha^k - 1) = \overline{\alpha}^k - \alpha^k \quad &\Rightarrow \quad \alpha^k(\eta + 1) = \overline{\alpha}^k + \eta \\ &\Rightarrow \quad \frac{\overline{\alpha}^k - 1}{\alpha^k - 1} = \left(\frac{\overline{\alpha}}{\alpha}\right)^k + \frac{\eta}{\alpha^k}, \end{aligned}$$

de manera similar obtenemos

$$\frac{\overline{\alpha}^l - 1}{\alpha^l - 1} = \left(\frac{\overline{\alpha}}{\alpha}\right)^l + \frac{\eta}{\alpha^l} \quad y \quad \frac{\overline{\alpha}^m - 1}{\alpha^m - 1} = \left(\frac{\overline{\alpha}}{\alpha}\right)^m + \frac{\eta}{\alpha^m}.$$

Combinando las identidades en (2.7) y las tres anteriores obtenemos

$$\begin{aligned} \left(\frac{\overline{\alpha}}{\alpha}\right)^{l-k} - 1 &= \eta \left(\frac{\alpha}{\overline{\alpha}}\right)^k \left(\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right) \\ \left(\frac{\overline{\alpha}}{\alpha}\right)^{m-l} - 1 &= \eta \left(\frac{\alpha}{\overline{\alpha}}\right)^l \left(\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right). \end{aligned} \tag{2.8}$$

Un cálculo directo muestra que si estamos en cualquiera de las hipótesis de (i) o (ii), entonces ambos lados derechos de (2.8) son menores que 1 en valor absoluto. Para cualquier número complejo $w \in \mathbb{C}$ tal que $|w| \leq 1$ y $|1 + w| = 1$, se cumple la desigualdad que relaciona al argumento y al valor absoluto de w, $|w| \leq |\arg(1 + w)| \leq (\pi/3)|w|$. Aplicando esto con w igual a los lados derechos de (2.8) obtenemos

$$\begin{aligned} (l-k)\arg\left(\frac{\overline{\alpha}}{\alpha}\right) + 2\pi r &= \arg\left[1 + \eta\left(\frac{\alpha}{\overline{\alpha}}\right)^k \left(\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right)\right] = \theta \left|\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right| |\eta|, \\ (m-l)\arg\left(\frac{\overline{\alpha}}{\alpha}\right) + 2\pi s &= \arg\left[1 + \eta\left(\frac{\alpha}{\overline{\alpha}}\right)^l \left(\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right)\right] = \phi \left|\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right| |\eta|, \end{aligned} \tag{2.9}$$

para algunos $r, s \in \mathbb{Z}$ y $\theta, \phi \in \mathbb{R}$ con $1 \leq |\theta|, |\phi| \leq \pi/3$. Eliminando $\arg(\overline{\alpha}/\alpha)$ de las anteriores igualdades, concluimos que

$$E := (m-l)\theta \left|\frac{1}{\alpha^k} - \frac{1}{\alpha^l}\right| |\eta| - (l-k)\phi \left|\frac{1}{\alpha^l} - \frac{1}{\alpha^m}\right| |\eta| = 2\pi(r-s),$$

debe ser cero o mayor o igual que 2π en valor absoluto. A continuación mostraremos que $E \neq 0$ para los dos casos que estamos tratando. Si suponemos que $E = 0$, debido a que $\eta \neq 0$ entonces

$$(m-l)\theta|\alpha^{l-k}-1| = (l-k)\phi|1-\alpha^{l-m}|.$$

Luego,

$$\frac{|\alpha^{l-k}-1|}{l-k} = \frac{|1-\alpha^{-(m-l)}|}{m-l}\left|\frac{\phi}{\theta}\right|,$$

lo cual lleva a

$$\frac{|\alpha|^{l-k}-1}{l-k} \leq \frac{1+|\alpha|^{-(m-l)}}{m-l}\frac{\pi}{3}. \tag{2.10}$$

Suponga que estamos en la situación del caso (i). Como $|\alpha| \geq 4/3$ y $l > k \geq 50$ podemos ver en los lados derechos de (2.9) que

$$|\theta|\left|\frac{1}{\alpha^k}-\frac{1}{\alpha^l}\right||\eta| < \frac{\pi}{3}((4/3)^{-50}+(4/3)^{-51})\cdot 2 < 10^{-5},$$

y

$$|\phi|\left|\frac{1}{\alpha^l}-\frac{1}{\alpha^m}\right||\eta| < \frac{\pi}{3}((4/3)^{-51}+(4/3)^{-52})\cdot 2 < 10^{-5}.$$

Como $10^{-4} < \arg(\overline{\alpha}/\alpha) < \pi - 10^{-4}$ entonces (2.9) implica que mín$\{l-k, m-l\} \geq 3$. También por el Lema 2.2.2 no se puede tener $m-l = l-k = 3$. Entonces se tiene que $l-k \geq 4$, $m-l \geq 3$ o $l-k \geq 3$, $m-l \geq 4$. Reemplazando estas desigualdades en (2.10) junto con $|\alpha| \geq 4/3$ obtenemos respectivamente

$$0{,}5401\cdots = \frac{(4/3)^4-1}{4} < \frac{|\alpha|^{l-k}-1}{l-k} < \frac{1+|\alpha|^{-(m-l)}}{m-l}\frac{\pi}{3} < \frac{1+(3/4)^3}{3}\frac{\pi}{3} < 0{,}5,$$

y

$$0{,}4567\cdots = \frac{(4/3)^3-1}{3} < \frac{|\alpha|^{l-k}-1}{l-k} < \frac{1+|\alpha|^{-(m-l)}}{m-l}\frac{\pi}{3} < \frac{1+(3/4)^4}{4}\frac{\pi}{3} < 0{,}35,$$

de donde, en cada opción llegamos a una contradicción.
Si estamos en el caso (ii), como $l-k \neq m-l$ se tiene que $l-k \geq 2$, $m-l \geq 1$ o $l-k \geq 1$, $m-l \geq 2$. De nuevo junto con $|\alpha| \geq 2{,}1$ al sustituir en (2.10) obtenemos

$$1{,}705 = \frac{(2{,}1)^2-1}{2} < \frac{|\alpha|^{l-k}-1}{l-k} < \frac{1+|\alpha|^{-(m-l)}}{m-l}\frac{\pi}{3} < \frac{1+(2{,}1^{-1})^1}{1}\frac{\pi}{3} < 1{,}55,$$

y

$$1{,}1 = \frac{(2,1)^1-1}{1} < \frac{|\alpha|^{l-k}-1}{l-k} < \frac{1+|\alpha|^{-(m-l)}}{m-l}\frac{\pi}{3} < \frac{1+(2,1^{-1})^2}{2}\frac{\pi}{3} < 0{,}65,$$

una vez más, llegamos a una contradicción e cada caso.
Dado que hemos mostrado que $E \neq 0$, entonces $2\pi < |E|$ y esto implica que

$$\begin{aligned} 2\pi &\leq (m-l)\frac{\pi}{3}\left|\frac{1}{\alpha^k}-\frac{1}{\alpha^l}\right||\eta| + (l-k)\frac{\pi}{3}\left|\frac{1}{\alpha^l}-\frac{1}{\alpha^m}\right||\eta| \\ &\leq (m-l)\frac{\pi}{3}(|\alpha|^{-k}+|\alpha|^{-l})|\eta| + (l-k)\frac{\pi}{3}(|\alpha|^{-l}+|\alpha|^{-m})|\eta|, \end{aligned}$$

como $0 < k < l < m$, entonces $k+1 \leq l$ y $k+1 \leq m$, por tanto $|\alpha|^{-l} \leq |\alpha|^{-k-1}$ y $|\alpha|^{-m} \leq |\alpha|^{-k-1}$, luego

$$\begin{aligned} 2\pi &\leq (m-l)\frac{\pi}{3}(|\alpha|^{-k}+|\alpha|^{-k-1})2 + (l-k)\frac{\pi}{3}(|\alpha|^{-k}+|\alpha|^{-k-1})2 \\ &= (m-l)\frac{2\pi}{3}((1+|\alpha|^{-1})|\alpha|^{-k}) + (l-k)\frac{2\pi}{3}((1+|\alpha|^{-1})|\alpha|^{-k}) \\ &= (m-k)\frac{2\pi}{3}(1+|\alpha|^{-1})|\alpha|^{-k}. \end{aligned}$$

Por tanto, $m-k \geq M|\alpha|^k$, donde $M = 3(1+|\alpha|^{-1})^{-1}$. Esto concluye el lema ya que si $|\alpha| \geq 4/3$ entonces $M \geq 1$, mientras que si $|\alpha| \geq 2{,}1$ entonces $M \geq 2$.

Para el siguiente lema, recordemos que $H(\alpha)$ es la altura absoluta de α. La demostración de este lema se obtuvo a través de la teoría de *funciones hipergeométricas* y requiere de 6 resultados previos para ser alcanzada por completo, por tal razón es omitida debido a que esta toma elementos por fuera del alcance de este trabajo, el lector interesado en la prueba de este lema puede consultar la referencia [4, Lema 7].

Lema 2.2.4. *Suponga que $m \geq 10l$. Sea $H = \max\{H(\alpha), H(\beta), H(\alpha/\beta)\}$ y suponga que $H > 1$. Entonces*

$$l \leq 27\frac{\log 2}{\log H} + \frac{50}{3}k.$$

Por último, los siguientes Lemas 2.2.5 y 2.2.6 muestran que la ecuación $\lambda\alpha^x + \mu\beta^x = 1$, tiene a lo más seis soluciones para un gran rango de valores de α y β.

Lema 2.2.5. *Sea α un número algebraico tal que $|\alpha| \geq 4$ y $H(\alpha) \geq 2^{1/3}$. Entonces para $\lambda \in \mathbb{C}$, la ecuación*

$$\lambda\alpha^x + \overline{\lambda}\overline{\alpha}^x = 1$$

tiene a lo más seis soluciones para $x \in \mathbb{Z}$.

Demostración. Supongamos que la ecuación $\lambda\alpha^x + \overline{\lambda}\overline{\alpha}^x = 1$ tiene siete soluciones, las cuales podemos asumir que son $x_0 = 0 < x_1 < x_2 < x_3 < x_4 < x_5 < x_6$. Por el Lema 2.2.3 (ii) se tiene $x_6 - x_4 > 2|\alpha|^{x_4}$. Por otro lado, el Lema 2.2.2 garantiza que $x_4 \geq 10$, luego $x_6 > 2|\alpha|^{x_4} + x_4$ implica que $x_6 > 10x_4$. Esto nos permite aplicar el Lema 2.2.4 con $k = x_1$, $l = x_4$, $m = x_6$ y $H \geq 2^{1/3}$ para obtener

$$x_4 < 27\frac{\log 2}{\log 2^{1/3}} + \frac{50}{3}x_1 = 81 + \frac{50}{3}x_1.$$

Usando el Lema 2.2.3 (ii) se tiene que $x_4 \geq x_2 + 2|\alpha|^{x_2}$, combinando esto con la desigualdad anterior queda

$$x_2 + 2|\alpha|^{x_2} < 81 + \frac{50}{3}x_1.$$

Esto implica que $x_1 + 2 \cdot 4^{x_1+1} < 81 + (50/3)x_1$, de ahí que $x_1 = 1$. Así, por el Lema 2.2.2, $x_2 \geq 3$, entonces $3 + 2 \cdot 4^3 < 81 + 50/3$, lo cual es una contradicción.

Lema 2.2.6. *Sean λ, μ, α y β números algebraicos no nulos en cuerpo numérico $\mathbb{K}$ tales que* $\max\{H(\alpha), H(\beta), H(\alpha/\beta)\} > 2^{1/6}$. *Sea $\mathfrak{p}$ un ideal primo de $\mathcal{O}_{\mathbb{K}}$ tal que $|\alpha|_{\mathfrak{p}} < 1$ y $|\beta|_{\mathfrak{p}} = 1$. Sea p el primo racional encima de $\mathfrak{p}$ y supongamos que el índice de ramificación es a lo más 2. Entonces la ecuación $\lambda\alpha^x + \mu\beta^x = 1$ tiene a lo más seis soluciones.*

Demostración. Sean $x_0 = 0 < x_1 < x_2 < x_3 < x_4 < x_5 < x_6$ soluciones de la ecuación $\lambda\alpha^x + \mu\beta^x = 1$. Por el Lema 2.2.2 se tiene que $x_2 \geq 3$, luego $|\alpha|_{\mathfrak{p}}^{x_2} \leq |\alpha|_{\mathfrak{p}}^3$. Dado que $|\alpha|_{\mathfrak{p}} < 1$, entonces $ord_{\mathfrak{p}}\,\alpha \geq 1$, y como índice de ramificación e de $\mathfrak{p}$ es menor que 3, entonces por definición de $|*|_{\mathfrak{p}}$ tenemos que

$$|\alpha|_{\mathfrak{p}}^3 = \left((N\mathfrak{p})^{-\,ord_{\mathfrak{p}}\,\alpha}\right)^3 = (N\mathfrak{p})^{-3\,ord_{\mathfrak{p}}\,\alpha} \leq (N\mathfrak{p})^{-3} < (N\mathfrak{p})^{-e} = |p|_{\mathfrak{p}} \leq |p|_{\mathfrak{p}}^{1/(p-1)}.$$

Luego $|\alpha|_{\mathfrak{p}}^{x_2}\,|\beta - 1|_{\mathfrak{p}} < |\alpha|_{\mathfrak{p}}^3 \cdot 1 < |p|_{\mathfrak{p}}^{1/(p-1)}$. Y esto nos permite aplicar el Lema 2.2.1 (iii) con $k = x_2,\ l = x_3,\ m = x_4$, para obtener

$$\left|\frac{x_4 - x_3}{d}\right|_{\mathfrak{p}} \leq |\alpha|_{\mathfrak{p}}^{x_3 - x_2}, \tag{2.11}$$

para algún $d \geq 4$, lo cual es consecuencia del Lema 2.2.1 (ii) pues tenemos la solución extra $0 < x_1 < k = x_2$. Como $|\alpha|_{\mathfrak{p}} < 1$, de (2.11) se sigue

que $p \mid \frac{x_4-x_3}{d}$, luego $x_4 - x_3 = d \cdot p^t u$ con $t = ord_p\left(\frac{x_4-x_3}{d}\right)$ y $u \in \mathbb{Z}^+$, de donde $x_4 - x_3 \geq d \cdot p^t$. De manera similar como lo hicimos para mostrar que $|\alpha|_{\mathfrak{p}} < |p|_{\mathfrak{p}}^{1/(p-1)}$, usando la definición de $|\ |_{\mathfrak{p}}$, el hecho que $\mathfrak{p} \mid p$ tiene índice de ramificación de $e \leq 2$ y la desigualdad (2.11), no es difícil mostrar que $t \geq \frac{x_3-x_2}{2}$, por tanto

$$x_4 - x_3 \geq d \cdot p^t \geq d \cdot p^{(x_3-x_2)/2} \geq 4 \cdot 2^{(x_3-x_2)/2}. \tag{2.12}$$

De manara análoga,

$$x_5 - x_4 \geq 4 \cdot 2^{(x_4-x_3)/2} \quad y \quad x_6 - x_5 \geq 4 \cdot 2^{(x_5-x_4)/2} \tag{2.13}$$

Por el Lema 2.2.1 (ii) tenemos que $d|(x_3 - x_2)$, luego $x_3 - x_2 \geq 4$. Usando otra vez el Lema 2.2.1, de manera similar como se hizo para obtener (2.12), pero en esta ocasión con $k = x_2$, $l = x_5$ y $m = x_6$, observamos que

$$x_6 - x_2 = x_6 - x_5 + x_5 - x_2 \geq 4 \cdot 2^{(x_5-x_2)/2} + x_5 - x_2,$$

además, por el Lema 2.2.2 sabemos que $x_5 - x_2 \geq \binom{4}{2} = 10$, luego de la ecuación anterior deducimos que $x_6 - x_2 > 10(x_5 - x_2)$, esto nos permite aplicar el Lema 2.2.4 con los datos $k = x_3 - x_2$, $l = x_5 - x_2$ y $m = x_6 - x_2$ y $H \geq 2^{1/6}$ a la ecuación $(\lambda\alpha^{x_2})\alpha^x + (\mu\beta^{x_2})\beta^x = 1$ para obtener

$$x_5 - x_2 \leq 27\frac{\log 2}{\log 2^{1/6}} + \frac{50}{3}(x_3 - x_2) = 162 + \frac{50}{3}(x_3 - x_2). \tag{2.14}$$

Una cota inferior para $x_5 - x_2$ se obtiene combinando (2.12) y (2.13), en efecto

$$x_5 - x_2 > x_5 - x_4 \geq 4 \cdot 2^{(x_4-x_3)/2} \geq 4 \cdot 2^{2 \cdot 2^{(x_3-x_2)/2}} \geq 4^{1+x_3-x_2}.$$

Pero esto contradice (2.14), ya que $x_3 - x_2 \geq 4$.

2.3. Demostración del resultado principal

Sea $(u_n)_{n\in\mathbb{Z}} \subseteq \mathbb{Q}$ una sucesión lineal recurrente ternaria no degenerada de números racionales con polinomio característico $p(x) = x^3 - Px^2 - Qx - R$. Sean θ_1, θ_2, θ_3 las raíces de $p(x)$. Como vimos en el capitulo I, existen a_1, a_2, $a_3 \in \mathbb{Q}(\theta_1, \theta_2)$ tales que

$$u_n = a_1\theta_1^n + a_2\theta_2^n + a_3\theta_3^n, \text{ para todo } n \in \mathbb{Z}.$$

A continuación, mostraremos que la ecuación

$$a_1\theta_1^n + a_2\theta_2^n + a_3\theta_3^n = 0 \quad \text{con } n \in \mathbb{Z}, \tag{2.15}$$

tiene a lo sumo 6 soluciones, el cual es el resultado central de este capítulo, el cual hemos tomado de Bueukers [3].

Teorema Principal. *Sea $(u_n)_{n\in\mathbb{Z}}$ una sucesión lineal recurrente ternaria de números racionales y no degenerada. Entonces su cero multiplicidad es a lo más 6.*

Para la demostración del resultado usaremos los lemas de la sección anterior y dos lemas más. El primer lema es necesario para poder usar el Lema 2.2.6 en algún punto de la demostración. Mientras el otro proporciona herramientas para mostrar que una sucesión lineal recurrente ternaria no degenerada no tiene más ceros que algunos encontrados por una simple inspección.

Lema 2.3.1. *Sea $\mathbb{K}$ el cuerpo de descomposición de un polinomio cúbico $p(x) \in \mathbb{Z}[x]$, con raíces $\theta_1, \theta_2, \theta_3$ y supongamos que $\mathbb{K}$ no es real. Si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_\mathbb{K}$, y tiene índice de ramificación $e \geq 3$, entonces $|\theta_1|_\mathfrak{p} = |\theta_2|_\mathfrak{p} = |\theta_3|_\mathfrak{p}$. Recíprocamente, si $|\theta_1|_\mathfrak{p} = |\theta_2|_\mathfrak{p} = |\theta_3|_\mathfrak{p} \neq 1$ y $\theta_1, \theta_2, \theta_3$ no tienen factores enteros comunes en $\mathcal{O}_\mathbb{K}$, entonces $\mathfrak{p}$ tiene índice de ramificación ≥ 3.*

Demostración. Supongamos que $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_\mathbb{K}$ con índice de ramificación $e \geq 3$. Sean p el primo racional encima de $\mathfrak{p}$ y G el grupo de Galois de $\mathbb{K}/\mathbb{Q}$. Primero supongamos que $p\mathcal{O}_\mathbb{K} = \mathfrak{p}^e$, como la extensión $\mathbb{K}/\mathbb{Q}$ es de Galois, entonces por el Teorema 1.2.13, G actúa transitivamente sobre los ideales primos que dividen a $p\mathcal{O}_\mathbb{K}$, entonces para cualquier $\sigma \in G$ tenemos que $\sigma(\mathfrak{p}) = \mathfrak{p}$. Supongamos que $\sigma \in G$ es tal que $\sigma(\theta_1) = \theta_2$ entonces

$$|\theta_2|_\mathfrak{p} = |\sigma(\theta_1)|_\mathfrak{p} = |\theta_1|_{\sigma^{-1}(\mathfrak{p})} = |\theta_1|_\mathfrak{p},$$

luego $|\theta_1|_\mathfrak{p} = |\theta_2|_\mathfrak{p}$. De manera similar obtenemos que $|\theta_2|_\mathfrak{p} = |\theta_3|_\mathfrak{p}$. Ahora supongamos que $p\mathcal{O}_\mathbb{K} \neq \mathfrak{p}^e$, por el Lema 1.2.11 sabemos que $e|[\mathbb{K} : \mathbb{Q}]$, luego tenemos que $e = 3$ y $[\mathbb{K} : \mathbb{Q}] = 6$, como G actúa transitivamente sobre los ideales primos que dividen a p tenemos que $p\mathcal{O}_\mathbb{K} = \mathfrak{p}^3\mathfrak{p}'^3$, más aún si $\sigma(\mathfrak{p}) = \mathfrak{p}'$ entonces σ es de orden 2, de ahí que $\mathfrak{p}' = \overline{\mathfrak{p}}$ (aquí la barra denota la conjugación compleja), esto implica que si $\sigma \in G$ es de orden 3 entonces $\sigma(\mathfrak{p}) = \mathfrak{p}$. Como $p(x)$ es de grado impar se debe tener que alguno de los $\theta_{i's}$

es real, digamos θ_1. Luego podemos encontrar σ, $\sigma' \in G$ de orden 3 tales que $\sigma(\theta_1) = \theta_2$ y $\sigma'(\theta_2) = \theta_3$. Entonces

$$|\theta_2|_{\mathfrak{p}} = |\sigma(\theta_1)|_{\mathfrak{p}} = |\theta_1|_{\sigma^{-1}(\mathfrak{p})} = |\theta_1|_{\mathfrak{p}}.$$

Por tanto, $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}}$ y de manera similar se muestra que $|\theta_2|_{\mathfrak{p}} = |\theta_3|_{\mathfrak{p}}$.
Para la segunda parte, asumamos que $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_{\mathbb{K}}$ tal que $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}} = |\theta_3|_{\mathfrak{p}} \neq 1$. Sea p el primo racional encima de $\mathfrak{p}$ y como $\mathbb{K}/\mathbb{Q}$ es una extensión de Galois, entonces nuevamente el Teorema 1.2.11 nos permite escribir

$$p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1^e \cdots \mathfrak{p}_k^e$$

para algunos $e, k \in \mathbb{Z}^+$ tales que $e \cdot k | [\mathbb{K} : \mathbb{Q}]$. Sin perdida de generalidad suponemos que $\mathfrak{p} = \mathfrak{p}_1$. Sea G el grupo de Galois de $\mathbb{K}/\mathbb{Q}$, como G actúa transitivamente sobre el conjunto $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$, para cada $1 \leq i \leq k$ existe $\sigma_i \in G$ tal que $\sigma_i(\mathfrak{p}_1) = \mathfrak{p}_i$. Entonces como $|\theta_1|_{\mathfrak{p}_1} = |\theta_2|_{\mathfrak{p}_1} = |\theta_3|_{\mathfrak{p}_1}$ tenemos

$$|\theta_j|_{\mathfrak{p}_i} = |\theta_j|_{\sigma_i(\mathfrak{p}_1)} = |\sigma_i^{-1}(\theta_j)|_{\mathfrak{p}_1},$$

además, como G permuta a θ_1, θ_2, θ_3 tenemos que $|\sigma_i^{-1}(\theta_j)|_{\mathfrak{p}_1} = |\theta_j|_{\mathfrak{p}_1}$, combinado esto con la igualdad anterior obtenemos que

$$|\theta_j|_{\mathfrak{p}_i} = |\theta_j|_{\mathfrak{p}_1}$$

para cada $1 \leq j \leq 3$ y todo $1 \leq i \leq k$. Esto implica que $ord_{\mathfrak{p}_i}\theta_j$ es el mismo para cada $1 \leq j \leq 3$ y $1 \leq i \leq k$, denotaremos este número por a. Como $p(x) \in \mathbb{Z}[x]$, sabemos que a es un entero no negativo, y por hipótesis $|\theta_j|_{\mathfrak{p}_1} \neq 1$ para $1 \leq j \leq 3$, entonces $a \geq 1$ y $\theta_j \in \mathfrak{p}_i$ para cada $1 \leq j \leq 3$ y $1 \leq i \leq k$. Si $e = 1$ entonces tenemos

$$\theta_1, \theta_2, \theta_3 \in \mathfrak{p}_1 \cdots \mathfrak{p}_k = p\mathcal{O}_{\mathbb{K}}$$

por tanto p divide a $\theta_1, \theta_2, \theta_3$ en $\mathcal{O}_{\mathbb{K}}$, lo cual no es posible ya que $\theta_1,\ \theta_2,\ \theta_3$ no tienen factores enteros comunes en $\mathcal{O}_{\mathbb{K}}$. Si $e = 2$ entonces $p\mathcal{O}_{\mathbb{K}} = \mathfrak{p}_1^2 \cdots \mathfrak{p}_k^2$, como $\theta_1\theta_2\theta_3 \in \mathbb{Z}$, y $ord_{\mathfrak{p}_1}(\theta_1\theta_2\theta_3) \geq 1$, tenemos que $p|\theta_1\theta_2\theta_3$, y por tanto $\mathfrak{p}_1^2$ también divide a $\theta_1\theta_2\theta_3$ y esto implica que $2|ord_{\mathfrak{p}_1}(\theta_1\theta_2\theta_3) = 3a$, luego $2|a$, y entonces

$$\theta_1, \theta_2, \theta_3 \in \mathfrak{p}_1^2 \cdots \mathfrak{p}_k^2 = p\mathcal{O}_{\mathbb{K}}$$

lo cual como en el caso $e = 1$ es una contradicción. Por lo tanto debemos tener que $e \geq 3$.

Lema 2.3.2. *Sea $(u_n)_{n\in\mathbb{Z}}$ una sucesión lineal recurrente ternaria y no degenerada de números racionales con polinomio característico x^3-Px^2-Qx-R, el cual tiene raíces distintas $\theta_1,\theta_2,\theta_3$. Suponga que $u_0=0$ y existen $a,b\in\mathbb{Q}-\{0\}$, c y d enteros positivos y un primo racional p tales que*

(i) $\theta_i^d = a+b\theta_i^c$ *para cada* $i=1,2,3$,

(ii) $|b|_p \leq 1/4, |R|_p = |a|_p = 1$ *y* $|u_n|_p \leq 1$ *para todo* $n\in\mathbb{Z}$,

(iii) $|u_r|_p < 1$ *y* $0\leq r\leq d+2c$ *implica que* $u_r = 0$.

Entonces $u_n = 0$ *implica* $0\leq n<d$ *ó* $n=d+r$ *para algún* $0\leq r<d$ *y* $u_r = u_{r+c} = 0$.

Demostración. Supongamos que $u_n = 0$ y $n = qd+r$ con q y r enteros no negativos con $0\leq r<d$. Si $q=0$ el resultado se sigue, entonces asumimos que $q>0$. Dado que

$$u_n = a_1\theta_1^n + a_2\theta_2^n + a_3\theta_3^n$$

y $\theta_j^d = a+b\theta_j^c$, entonces $u_n = 0$ puede ser reescrito como

$$\sum_{i=1}^{3} a_i\left(1+\frac{b}{a}\theta_i^c\right)^q\theta_i^r = 0.$$

Usando expansiones binomiales y reorganizando, obtenemos que la expresión del lado izquierdo tiene la forma

$$u_r + \sum_{j=1}^{q}\binom{q}{j}\left(\frac{b}{a}\right)^j\left(\sum_{i=1}^{3}a_i\theta_i^{r+jc}\right),$$

luego

$$u_r + \sum_{j=1}^{q}\binom{q}{j}\left(\frac{b}{a}\right)^j u_{r+cj} = 0. \tag{2.16}$$

Como $|u_{r+jc}|_p\leq 1$ para todo j y $\left|\frac{b}{a}\right|_p<1$, (2.16) implica que $|u_r|_p<1$, ya que si $|u_r|_p\geq 1$ entonces la propiedad no-arquimediana de $|\ |_p$ y el hecho de que $\left|\binom{q}{j}\right|_p\leq 1$ implican que

$$0 = \max_{j\geq 2}\left\{|u_r|_p, \left|\left(\frac{b}{a}\right)^j u_{r+cj}\right|_p\right\}\geq 1,$$

lo cual no es posible. Entonces por la condición (iii) se concluye que $u_r = 0$, luego de (2.16) tenemos que

$$\sum_{j=1}^{q} \binom{q}{j} \left(\frac{b}{a}\right)^j u_{r+cj} = 0. \tag{2.17}$$

Si $q = 1$ entonces $(b/a)u_{r+c} = 0$, de donde $u_{r+c} = 0$, y por tanto $n = d + r$ con $0 \leq r < d$, $u_r = u_{r+c} = 0$. Nos resta ver que para $q > 1$ se llega a una contradicción. Dividiendo (2.17) por qb/a se obtiene

$$u_{r+c} + \sum_{j=2}^{q} \binom{q-1}{j-1} \frac{1}{j} \left(\frac{b}{a}\right)^{j-1} u_{r+jc} = 0. \tag{2.18}$$

Como $|b|_p < 1/4$ y $|a|_p = 1$, entonces $\left|\frac{1}{j}\left(\frac{b}{a}\right)^{j-1}\right|_p < 1$ para todo $j \geq 2$, como antes de (2.18) se deduce que $|u_{r+c}|_p < 1$ y la condición (iii) implica que $u_{r+c} = 0$. Si $q = 2$ entonces de (2.18) se obtiene que $u_{r+2c} = 0$. Pero $u_r = u_{r+c} = u_{r+2c} = 0$ contradice el Lema 2.2.2 ya que la recurrencia es no degenerada. Si $q \geq 3$, dividiendo a

$$\sum_{j=2}^{q} \binom{q-1}{j-1} \frac{1}{j} \left(\frac{b}{a}\right)^{j-1} u_{r+jc} = 0$$

por $(q-1)b/a$, obtenemos

$$u_{r+2c} + \sum_{j=3}^{q} \binom{q-2}{j-2} \frac{1}{j(j-1)} \left(\frac{b}{a}\right)^{j-2} u_{r+jc} = 0. \tag{2.19}$$

Como antes, dado que $|b|_p \leq 1/4$ y $|a|_p = 1$, se tiene que $\left|\frac{1}{j(j-1)}\left(\frac{b}{a}\right)^{j-2}\right|_p < 1$ para todo $j \geq 3$, entonces (2.19) implica que $|u_{r+2c}|_p < 1$. La condición (iii) implica que $u_{r+2c} = 0$. Pero $u_r = u_{r+c} = u_{r+2c} = 0$ contradice el Lema 2.2.2. Esto completa la prueba de este lema.

Nota. La condición (i) del Lema 2.3.2 podría ser eliminada, tan pronto como se tenga tres soluciones 0, c, d de (2.15), ya que el determinante

$$\begin{vmatrix} 1 & \theta_1^c & \theta_1^d \\ 1 & \theta_2^c & \theta_2^d \\ 1 & \theta_3^c & \theta_3^d \end{vmatrix}$$

debe ser cero. De ahí que sus columnas son linealmente dependientes lo que implica la condición (i). Este lema lo usaremos para mostrar que una sucesión lineal recurrente no tiene más ceros que algunos encontrados por una simple búsqueda, a continuación mostraremos un ejemplo de aplicación de este lema.

Ejemplo 2.3.1. *Consideremos la sucesión lineal recurrente dada por*

$$u_{n+3} = -u_{n+2} + u_n, \quad u_0 = 0,\ u_1 = 1,\ u_2 = 0.$$

Variando $n \in [0, 20]$*, mediante una simple inspección se obtiene que* $u_0 = u_2 = u_3 = u_7 = u_{16} = 0$*. Si* $\theta_1, \theta_2, \theta_3$ *son las raíces de* $x^3 + x^2 - 1$*, con las soluciones* $0,\ c = 2,\ d = 16$ *y con ayuda del sistema de computo Mathematica encontramos que* $\theta_i^{16} = 4 - 7\theta_i^2$ *para* $i = 1, 2, 3$*, luego en notación del Lema 2.3.2 tomamos* $a = 4$ *y* $b = -7$*. Dado que* $|a|_2 < 1$*,* $|b|_3 = |b|_5 = 1$*, entonces tomando* $p = 7$ *, se tiene* $|a|_7 = |R|_7 = 1$*,* $|b|_7 = 1/7 < 1/4$ *y como* $(u_n)_{n\in\mathbb{Z}} \subset \mathbb{Z}$*,* $|u_n|_7 \leq 1$ *para todo* $n \in \mathbb{Z}$*, finalmente para* $n \in [0, 20]$*,* $|u_n|_7 < 1$ *implica que* $u_n = 0$*. Entonces la conclusión del Lema 2.3.2 nos dice que si* $u_n = 0$*, entonces* $0 \leq n < 16$ *ó* $n = 16 + r$ *con* $0 \leq r < 16$*,* $u_r = u_{r+2} = 0$*, pero por el Lema 2.2.2 esto puede pasar sólo para un* r*, y en este caso se puede ver que* $r = 0$ *ya que* $u_0 = u_2 = 0$*. En resumen, se tiene que* $u_n = 0$ *implica que* $0 \leq n \leq 16$*, y por tanto* u_n *sólo se hace cero en* $n = 0, 2, 3, 7, 16$*, es decir, no tiene más ceros que los encontrados originalmente.*

Demostración del resultado principal

La demostración del resultado será dividida en dos casos. En el primero consideramos que $\theta_1, \theta_2, \theta_3$ son todas reales, y en el segundo consideraremos el caso complejo. A su vez, este último caso sera dividido en tres partes. El objetivo en cada subcaso es mostrar que la sucesión lineal recurrente ternaria que resulta tiene cero-multiplicidad a lo más 6, para lo cual usaremos todos los resultados previos.

Caso 1

Primero suponemos que $\theta_1, \theta_2, \theta_3 \in \mathbb{R}$, entonces la ecuación (2.15) puede ser reescrita como

$$a_1 \left(\frac{\theta_1}{\theta_3}\right)^n + a_2 \left(\frac{\theta_2}{\theta_3}\right)^n + a_3 = 0.$$

Si esta ecuación tuviera 5 soluciones, entonces al menos 3 de ellas deberían tener la misma paridad. Pero esto implicaría que

$$a_1\left(\frac{\theta_1}{\theta_3}\right)^{2n} + a_2\left(\frac{\theta_2}{\theta_3}\right)^{2n} + a_3,$$

o

$$a_1\frac{\theta_1}{\theta_3}\left(\frac{\theta_1}{\theta_3}\right)^{2n} + a_2\frac{\theta_2}{\theta_3}\left(\frac{\theta_2}{\theta_3}\right)^{2n} 1 + a_3,$$

vistas como funciones reales, tendrían al menos 3 ceros, y por tanto como mínimo dos puntos críticos al ser funciones derivables. Pero esto no es posible ya que estas funciones tienen a lo más un punto crítico. Por tanto (2.15) tiene a lo más 4 soluciones cuando $\theta_1, \theta_2, \theta_3 \in \mathbb{R}$.

Caso 2

Ahora, asumimos que tenemos una raíz real y dos raíces complejas conjugadas. Existe la opción de que se tenga una raíz racional y las otras sean complejas conjugadas en un campo cuadrático o que sean las raíces de un polinomio cúbico irreducible sobre $\mathbb{Q}$. Consideraremos los valores absolutos no arquimedianos del cuerpo $\mathbb{K} = \mathbb{Q}(\theta_1, \theta_2)$, que por el Teorema de Ostrowsky están determinados por los ideales primos de $\mathcal{O}_\mathbb{K}$. Haremos una nueva separación con respecto a la relación de igualdad de los valores numéricos $|\theta_1|_\mathfrak{p}, |\theta_2|_\mathfrak{p}, |\theta_3|_\mathfrak{p}$, donde $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_\mathbb{K}$.

Subcaso 2.1

Si existe un ideal primo $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$ tal que $|\theta_1|_\mathfrak{p}, |\theta_2|_\mathfrak{p}, |\theta_3|_\mathfrak{p}$ son todos distintos, y si $x \in \mathbb{Z}$ es una solución de (2.15), entonces

$$a_1\theta_1^x + a_2\theta_2^x + a_3\theta_3^x = 0,$$

donde $|a_1\theta_1^x|_\mathfrak{p}, |a_2\theta_2^x|_\mathfrak{p}, |a_3\theta_3^x|_\mathfrak{p}$ no pueden ser todos distintos, ya que la propiedades del triángulo isósceles de $|\ |_\mathfrak{p}$ implica que

$$0 = |a_1\theta_1^x + a_2\theta_2^x + a_3\theta_3^x|_\mathfrak{p} = \max |a_i\theta_i^x|_\mathfrak{p} \neq 0.$$

Por otro lado, para $i \neq j \in \{1, 2, 3\}$, $|a_i\theta_i^x|_\mathfrak{p} = |a_j\theta_j^x|_\mathfrak{p}$ implica que $\left|\frac{a_i}{a_j}\right|_\mathfrak{p} = \left|\frac{\theta_j}{\theta_i}\right|_\mathfrak{p}^x$ y como $|\theta_i|_\mathfrak{p} \neq |\theta_j|_\mathfrak{p}$, entonces $|a_i\theta_i^x|_\mathfrak{p} = |a_j\theta_j^x|_\mathfrak{p}$ solo puede pasar a lo más para un x. Así, podemos concluir que si existe un ideal primo $\mathfrak{p}$ de $\mathcal{O}_\mathbb{K}$ tal que $|\theta_1|_\mathfrak{p}, |\theta_2|_\mathfrak{p}, |\theta_3|_\mathfrak{p}$ son todos distintos, entonces (2.15) tiene a lo sumo 3 soluciones.

Subcaso 2.2

Ahora suponemos que existe un ideal primo de $\mathcal{O}_{\mathbb{K}}$ tal que $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}} \neq |\theta_3|_{\mathfrak{p}}$. En este punto aplicamos el Lema 2.2.6 dado que $|\theta_1/\theta_2|_{\mathfrak{p}} = 1$ y $|\theta_3/\theta_2|_{\mathfrak{p}} < 1$ ó $|\theta_2/\theta_1|_{\mathfrak{p}} = 1$ y $|\theta_2/\theta_3|_{\mathfrak{p}} < 1$, para lo cual resta que el índice de ramificación e de $\mathfrak{p}$ sobre su correspondiente primo racional es menor o igual a 2. En efecto, si suponemos que $e \geq 3$, entonces el Lema 2.3.1 implica que $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}} = |\theta_3|_{\mathfrak{p}}$ lo cual no es el caso.
Así aplicando el Lema 2.2.6 a la ecuación

$$\left(-\frac{a_1}{a_2}\right)\left(\frac{\theta_1}{\theta_2}\right)^n + \left(-\frac{a_3}{a_2}\right)\left(\frac{\theta_3}{\theta_2}\right)^n = 1,$$

si $|\theta_2|_{\mathfrak{p}} > |\theta_3|_{\mathfrak{p}}$, ó a la ecuación equivalente

$$\left(-\frac{a_1}{a_2}\right)\left(\frac{\theta_2}{\theta 1}\right)^n + \left(-\frac{a_3}{a_2}\right)\left(\frac{\theta_2}{\theta_3}\right)^n = 1,$$

si $|\theta_2|_{\mathfrak{p}} < |\theta_3|_{\mathfrak{p}}$, concluimos que la ecuación (2.15) tiene a lo más 6 soluciones.

Subcaso 2.3

Nos queda el caso en que $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}} = |\theta_3|_{\mathfrak{p}}$ para todos los ideales primos de $\mathcal{O}_{\mathbb{K}}$. Sea θ_3 la raíz real entonces θ_1, θ_2 no pueden ser conjugadas en un campo cuadrático complejo, ya que si $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}}$ para todo ideal primo de $\mathcal{O}_{\mathbb{K}}$, entonces el Teorema de Ostrowsky nos permite extender esta igualdad a todo valor absoluto no-arquimediano, además como sólo existen un valor absoluto arquimediano, el módulo complejo usual, entonces esta igualdad se cumple para cualquier valor absoluto en $\mathbb{K}$, luego el Teorema 1.3.4 implica que θ_1/θ_2 es una raíz de la unidad, lo que es una contradicción porque $(u_n)_{n\in\mathbb{Z}}$ es no degenerada. De ahí que $\theta_1, \theta_2, \theta_3$ son raíces de un polinomio cúbico irreducible sobre $\mathbb{Q}$.
Note que si $x \in \mathbb{Z}$ es una solución de (2.15) entonces si se reemplaza cada θ_i por θ_i^{-1} la nueva ecuación tendrá como solución $-x$ y por ende la sucesión lineal recurrente tendrá la misma cero-multiplicidad. Haciendo esta sustitución si fuese necesario, podemos asumir que $|\theta_3| < |\theta_1|$. Además multiplicamos a $\theta_1, \theta_2, \theta_3$ por el mismo entero racional para asegurarnos de que $\theta_3 > 0$ y que $\theta_1, \theta_2, \theta_3$ sean enteros algebraicos sin factores enteros racionales comunes en $\mathcal{O}_{\mathbb{K}}$.
Si $|\theta_1/\theta_3| \geq 4$ entonces aplicamos el Lema 2.2.5 con $\lambda = -a_1/a_3$ y $\alpha = \theta_1/\theta_3$, el cual nos permite concluir que (2.15) tiene a lo más 6 soluciones. Por tanto

Tabla 2.1: Coficientes del polinomio característico para u_n.

P	Q	R	$\lvert\theta_1/\theta_3\rvert$	P	Q	R	$\lvert\theta_1/\theta_3\rvert$	P	Q	R	$\lvert\theta_1/\theta_3\rvert$
2	-3	1	3,545	2	-4	4	1,346	0	-6	6	2,944
5	-25	25	3,677	-2	0	2	1,839	0	-7	7	3,115
3	-6	3	3,104	-3	0	9	1,762	0	-2	1	3,276
2	-4	2	2,769	-2	0	4	1,664	0	-9	9	3,428
4	-8	4	3,383	-2	-1	1	3,148	0	-10	10	3,574
-6	0	36	1,961	-1	0	1	1,525	0	-11	11	3,713
3	-9	9	1,961	0	-1	1	1,774	0	-12	12	3,847
6	-18	18	1,961	0	-2	2	2,089	0	-13	13	3,977
-5	0	25	1,905	0	-3	3	2,342	-1	-1	1	2,494
1	-2	1	2,325	0	-4	4	2,562	-2	-2	2	3,246
5	-10	5	3,627	0	-5	5	2,761	-2	-4	4	3,528

asumiremos en adelante que $|\theta_1/\theta_3| < 4$. Con ayuda de *Mathematica* encontramos el conjunto[2] de polinomios cúbicos irreducibles $x^3 - Px^2 - Qx - R$ con $P, Q, R \in \mathbb{Z}$ y raíces $\theta_1, \theta_2, \theta_3$ donde θ_3 es la raíz real, tales que $|\theta_1|_{\mathfrak{p}} = |\theta_2|_{\mathfrak{p}} = |\theta_3|_{\mathfrak{p}}$ para todos los ideales primos de $\mathcal{O}_{\mathbb{K}}$ y $|\theta_1/\theta_3| < 4$. Tal conjunto es dado en la Tabla 2.1. Note que en cada entrada de la tabla se tiene que $|\theta_1/\theta_3| \geq 4/3$ y $10^{-4} < |\arg(\theta_1/\theta_2)| < \pi - 10^{-4}$.

Entonces, estamos en la situación en que $(u_n)_{n\in\mathbb{Z}}$ está determinada por los coeficientes P, Q, R de cada una de las entradas de la tabla anterior. Para concluir la prueba mostremos que sin importar la elección de los valores iniciales u_0, u_1, u_2 en cada entrada, la ecuación $u_n = 0$ tiene a lo más 6 soluciones.

Como siempre, suponemos que (2.15) tiene siete soluciones, $x_0 = 0 < x_1 < x_2 < x_3 < x_4 < x_5 < x_6$. Primero, asumimos que $x_2 > 100$. Aplicamos el Lema 2.2.3(i) con $m = x_6$, $l = x_5$, $k = x_4$ y $\alpha = \theta_1/\theta_3$ para obtener $x_6 - x_4 > |\theta_1/\theta_3|^{x_4} > (4/3)^{x_4}$. Como $x_4 > x_2 > 100$, la desigualdad anterior implica que $x_6 > 10x_4$ lo cual permite usar el Lema 2.2.4, con

[2]De hecho, este conjunto de polinomios finito debido a que los coeficientes están en $\mathbb{Z}$, y a que la cota del valor absoluto $|\theta_1/\theta_3| < 4$.

$k = x_1,\ l = x_4,\ m = x_6$ y $H > (4/3)^{1/3}$, para obtener

$$x_4 < 27\frac{\log 2}{\log((4/3)^{1/3})} + \frac{50}{3}x_1 \leq 196 + \frac{50}{3}x_1 \left(< 196 + \frac{50}{3}x_2 \right) \qquad (2.20)$$

Por otro lado, del Lema 2.2.3(i) se obtiene que $x_4 - x_2 > |\theta_1/\theta_3|^{x_2} > (4/3)^{x_2}$, de donde $x_4 > (4/3)^{x_2} + x_2$, lo que claramente contradice (2.20) cuando $x_2 > 100$, luego $x_2 \leq 100$. A cada entrada de la Tabla 2.1 le corresponde una relación de recurrencia ternaria para (u_n) con coeficientes $P, Q, R \in \mathbb{Z}$. Con ayuda de *Mathematica*, en la Tabla 2.2 hemos determinado todos los valores iniciales u_0, u_1, u_2 con $u_0 = 0$, tales que $u_n = 0$ para al menos tres soluciones con $0 \leq n < 250$, esto implica que las sucesiones que no están en esta tabla quedan descartadas dado que x_2 resultaría mayor o igual que 250. Entonces la posibilidad para (u_n) queda reducida a esta lista. Si $u_n = 0$

Tabla 2.2: Recurrencias con al menos tres soluciones < 250.

P	Q	R	u_0	u_1	u_2	$0 \leq n < 250$ tal que $u_n = 0$
-3	0	9	0	1	0	0,2,3,9
-2	0	2	0	1	0	0,2,3,26
- 2	0	2	0	2	-1	0,4,12
-2	0	4	0	1	0	0,2,3,8,24
-1	0	1	0	1	0	0,2,3,7,16
-1	-1	1	0	0	1	0,1,4,17
0	-1	1	0	0	1	0,1,3,8
0	-4	3	0	0	1	0,1,3,10
0	-6	6	0	0	1	0,1,3,12
2	-4	2	0	0	1	0,1,4,12
2	-4	4	0	0	1	0,1,4,6,13,52
3	-9	9	0	0	1	0,1,4,9

tuviera cuatro soluciones en n con $0 \leq n \leq 250$, entonces $x_4 > 250$, además la desigualdad (2.20) todavía se cumple. De la Tabla 2.2 se puede inferir que $x_1 \leq 2$ con solo una excepción, y sustituyendo x_1 en (2.20) resulta que $x_4 < 250$, una contradicción. El caso excepcional corresponde a $P = -2$, $Q = 0$, $R = 2$. En este caso $H > (1{,}8)^{1/3}$ y el 196 en (2.20) puede ser reducido a 100, entonces $x_1 = 4$ al ser sustituido en (2.20) resulta de nuevo en

una contradicción.
Por tanto $x_4 < 250$, es decir, la ecuación $u_n = 0$ tiene mínimo cinco soluciones en n con $0 \leq n \leq 250$. Por tal motivo la lista de opciones para los coeficientes de la relación de recurrencia y valores iniciales de (u_n) se reduce a la siguiente tabla.

P	Q	R	u_0	u_1	u_2	n tal que $u_n = 0$
2	-4	4	0	0	1	0,1,4,6,13,52
-1	0	1	0	1	0	0,2,3,7,16
-2	0	4	0	1	0	0,2,3,8,24

Por tanto, si mostramos que cada una de estas sucesiones no tiene más ceros que los listados la prueba del teorema quedaría terminada. Para ello usaremos el Lema 2.3.2 tal como se hizo en el Ejemplo 2.3.1. Para la primer sucesión recurrente tomamos

$$c = 1,\ d = 52\ a = -206,2^{34},\ b = 159{,}2^{34},\ p = 53,$$

para la segunda se toma

$$c = 2,\ d = 16,\ a = 4,\ b = -7,\ p = 7,$$

y para la última tomamos

$$c = 1,\ d = 22,\ a = 26,2^{14},\ b = -23{,}2^{14},\ p = 23.$$

Esto completa la demostración del teorema principal.

Capítulo 3

Cero-multiplicidad de sucesiones lineales recurrentes ternarias tipo Berstel

3.1. Introducción

Del capítulo anterior sabemos que toda sucesión lineal recurrente ternaria no degenerada de números racionales tiene cero-multiplicidad a lo más seis y también se muestra un ejemplo donde esta cota es alcanzada. Este ejemplo corresponde a la sucesión de Berstel $(B_n)_{n\in\mathbb{Z}}$, la cual tiene relación de recurrencia $B_{n+3} = 2B_{n+2} - 4B_{n+1} + 4B_n$ y valores iniciales $B_0 = B_1 = 0$, $B_2 = 1$, por este motivo a una sucesión lineal recurrente ternaria que comparte la misma relación de recurrencia la llamamos una *sucesión tipo Berstel* y en particular toda esta familia de sucesiones tiene cero-multiplicidad a lo más 6. Sin embargo, uno se puede preguntar la por cero-multiplicidad de toda la familia de sucesiones recurrentes ternarias tipo Berstel. Como respuesta a este interrogante tenemos el siguiente resultado:

Teorema Principal. *Salvo múltiplo escalar entero o desplazamiento de los subíndices, existen exactamente dos sucesiones lineales recurrentes ternarias tipo Berstel con cero multiplicidad al menos 3. Una de ellas es la sucesión de Berstel* $(B_n)_{n\in\mathbb{Z}}$ *y la otra es la sucesión recurrente tipo Berstel* $(B'_n)_{n\in\mathbb{Z}}$ *con valores iniciales* 0, 1, 4 *la cual tiene cero multiplicidad 3. Es decir, Cualquier sucesión lineal recurrente ternaria tipo Berstel, la cual no es un*

múltiplo escalar o desplazamiento de los subíndices de $(B_n)_{n\in\mathbb{Z}}$ *o* $(B'_n)_{n\in\mathbb{Z}}$*, tiene cero-multiplicidad a lo más 2.*

Este resultado corresponde a un trabajo conjunto con C. A. Gómez y F. Luca [14]. En el desarrollo de este capítulo demostraremos este resultado, mostrando la técnica utilizada. Este problema nos lleva a resolver una ecuación diofántica exponencial de números algebraicos, la cual es abordada con la teoría de las formas lineales en logaritmos (teoría de Baker), la teoría de aproximación diofántica y también con la ayuda del software *Mahtematica*. En la primera sección observaremos que nuestro problema es equivalente a resolver una ecuación diofántica exponencial en dos variables enteras. En la segunda sección mostramos que las variables de nuestra ecuación diofántica están acotadas superiormente. Sin embargo, estas cotas son enormes para ser manejadas computacionalmente, por tanto en la tercera sección reducimos estas cotas con ayuda de los Lemas A.4.1 y A.4.2 (argumentos de fracciones continuas). Por último, realizamos los cálculos finales en *Mathematica*, mostrando explicitamente las soluciones de nuestra ecuación.

3.2. Primeras observaciones.

Sea $(u_n)_{n\in\mathbb{Z}}$ una sucesión tipo Berstel, con valores iniciales no todos nulos. Su polinomio característico x^3-2x^2+4x-4 es un polinomio irreducible sobre $\mathbb{Q}$, y tiene una raíz real α y dos complejas conjugadas β, γ, donde

$$\alpha = \frac{1}{3}\left(2 - \frac{4\cdot 2^{1/3}}{(13+3\sqrt{33})^{1/3}} + (2(13+3\sqrt{33}))^{1/3}\right) \in (1{,}29, 1{,}3), \tag{3.1}$$

y

$$\beta = 2\alpha^{-1/2}e^{i\omega}, \quad \gamma = 2\alpha^{-1/2}e^{-i\omega}, \quad \text{con} \quad w \in (0, 2\pi). \tag{3.2}$$

Es bien conocido de la teoría clásica de sucesiones lineales recurrentes que el término general de $(u_n)_{n\in\mathbb{Z}}$ es de la forma

$$u_n = a\alpha^n + b\beta^n + c\gamma^n, \quad \text{con} \quad a,\ b,\ c \in \mathbb{Q}(\alpha,\beta) \quad \text{no todos cero.} \tag{3.3}$$

Ahora, como la relación de recurrencia tipo Berstel está en la tabla 2.1, sabemos que $|\alpha|_{\mathfrak{p}} = |\beta|_{\mathfrak{p}} = |\gamma|_{\mathfrak{p}}$ donde $\mathfrak{p}$ es cualquier ideal primo de anillo de enteros de $\mathbb{K} = \mathbb{Q}(\alpha,\beta)$. Dado que $\alpha\beta\gamma = 4$ entonces $\left|\alpha^3\right|_{\mathfrak{p}} = |4|_{\mathfrak{p}}$ luego $\left|4\alpha^{-3}\right|_{\mathfrak{p}} = 1$ para todo ideal primo de $\mathcal{O}_{\mathbb{K}}$, además, el Teorema de Ostrowski nos permite extender esta igualdad a todo valor absoluto no-arquimediano de $\mathbb{K}$, por tanto, el Teorema 1.3.3 implica que $4\alpha^{-3}$ es una unidad de $\mathcal{O}_{\mathbb{K}}$. De

manera análoga podemos mostrar que $4\beta^{-3}$ y $4\gamma^{-3}$ también son unidades de $\mathcal{O}_{\mathbb{K}}$. Si denotamos a estas por $\alpha_1, \beta_1, \gamma_1$ respectivamente, tenemos que

$$\alpha_1 = 4\alpha^{-3}, \qquad \beta_1 = 4\beta^{-3}, \qquad \gamma_1 = 4\gamma^{-3}. \tag{3.4}$$

Un simple cálculo nos muestra que $\alpha_1, \beta_1, \gamma_1$ son las raíces del polinomio $x^3 - x^2 - x - 1$, y estas son dadas por

$$\alpha_1 = \frac{1}{3}\left(1 + (19 - 3\sqrt{33})^{1/3} + (19 + 3\sqrt{33})^{1/3}\right) \in (1{,}83, 1{,}84), \tag{3.5}$$

y

$$\beta_1 = \alpha_1^{-1/2} e^{i\theta} \quad \text{y} \quad \gamma_1 = \alpha_1^{-1/2} e^{-i\theta}, \quad \text{donde} \quad \theta \in (0, 2\pi). \tag{3.6}$$

Usaremos las relaciones entre $\alpha,\ \beta,\ \gamma$ y $\alpha_1,\ \beta_1,\ \gamma_1$ dadas en (3.4), debido a que $\alpha < |\beta| = |\gamma|$, pues como podemos ver las raíces complejas dominan en módulo a la raíz real, mientras que $|\beta_1| = |\gamma_1| < \alpha_1$ y en esta situación la raíz real domina en módulo a las raíces complejas, lo cual será de gran utilidad en la manipulación de la ecuación diofántica que vamos a resolver. Asumimos que u_n tiene cero-multiplicidad al menos 3 y que estos ceros están localizados en los subíndices $n_0,\ n_0 - x,\ n_0 - y$, donde $0 < x < y$. Entonces usando (3.3) tenemos que

$$\begin{cases} u_{n_0} = a\alpha^{n_0} + b\beta^{n_0} + c\gamma^{n_0} = 0, \\ u_{n_0 - x} = a\alpha^{n_0 - x} + b\beta^{n_0 - x} + c\gamma^{n_0 - x} = 0, \\ u_{n_0 - y} = a\alpha^{n_0 - y} + b\beta^{n_0 - y} + c\gamma^{n_0 - y} = 0. \end{cases} \tag{3.7}$$

Podemos considerar a (3.7) como un sistema de ecuaciones lineales homogéneo de tamaño 3×3, el cual tiene una solución no nula $(a\alpha^{n_0}, b\beta^{n_0}, c\gamma^{n_0})$, y por tanto su matriz de coeficientes debe tener determinante nulo, esto es

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha^{-x} & \beta^{-x} & \gamma^{-x} \\ \alpha^{-y} & \beta^{-y} & \gamma^{-y} \end{vmatrix} = 0. \tag{3.8}$$

Con el fin de utilizar las identidades en (3.4), consideramos

$$x = 3x_0 - r_0, \qquad y = 3y_0 - r_1, \quad \text{con} \quad r_0,\ r_1 \in \{0, 1, 2\}. \tag{3.9}$$

Sustituyendo x, y de acuerdo a (3.9) en (3.8), obtenemos

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha^{r_0}\alpha^{-3x_0} & \beta^{r_0}\beta^{-3x_0} & \gamma^{r_0}\gamma^{-3x_0} \\ \alpha^{r_1}\alpha^{-3y_0} & \beta^{r_1}\beta^{-3y_0} & \gamma^{r_1}\gamma^{-3y_0} \end{vmatrix} = 0.$$

En el determinante anterior, multiplicamos la segunda fila por 4^{x_0} y la tercera fila por 4^{y_0}, y usando (3.4), obtenemos

$$\begin{vmatrix} 1 & 1 & 1 \\ b_1\alpha_1^{x_0} & b_2\beta_1^{x_0} & b_3\gamma_1^{x_0} \\ c_1\alpha_1^{y_0} & c_2\beta_1^{y_0} & c_3\gamma_1^{y_0} \end{vmatrix} = 0, \tag{3.10}$$

donde

$$b_1 = \alpha^{r_0}, \;\; b_2 = \beta^{r_0}, \quad b_3 = \gamma^{r_0} \quad \text{y} \quad c_1 = \alpha^{r_1}, \quad c_2 = \beta^{r_1}, \;\; c_3 = \gamma^{r_1}. \tag{3.11}$$

Expandiendo el determinante (3.10) por la primera columna, obtenemos la ecuación

$$b_2\beta_1^{x_0}c_3\gamma_1^{y_0} - b_3\gamma_1^{y_0}c_2\beta_1^{y_0} - b_1\alpha_1^{x_0}(c_3\gamma_1^{y_0} - c_2\beta_1^{y_0}) + c_1\alpha_1^{y_0}(b_3\gamma_1^{x_0} - b_2\beta_1^{x_0}) = 0. \tag{3.12}$$

Dado que todos los pasos anteriores son equivalentes, entonces resolver la ecuación exponencial (3.12), es equivalente a determinar todas las sucesiones tipo Berstel $(u_n)_{n\in\mathbb{Z}}$ con cero-multiplicidad al menos 3 (salvo múltiplos escalares y desplazamiento de los subíndices). Note que si encontramos un rango de solución para (x_0, y_0) entonces vía (3.9) encontramos un rango de solución para (x, y); y para cada solución (x, y), nuestras sucesiones serán un desplazamiento de los subíndices, de la sucesión cuyo termino general está dado por la fórmula (3.3), donde (a, b, c) es un vector en el espacio nulo de la matriz cuyo determinante es mostrado en (3.8).

3.3. Cotas superiores para x_0 e $y_0 - x_0$

Aplicaremos el Teorema 1.4.2 (Teorema de Matveev) para encontrar cotas superiores para x_0 y para $\ell = y_0 - x_0$. Usando las identidades (3.6), podemos reescribir la ecuación (3.12) como

$$\begin{aligned} b_2c_1\alpha_1^{y_0-\frac{x_0}{2}}e^{i\theta x_0}(b_3b_2^{-1}e^{-2i\theta x_0} - 1) &= \alpha_1^{-\frac{x_0+y_0}{2}}(b_3c_2e^{i\theta(y_0-x_0)} - b_2c_3e^{i\theta(x_0-y_0)}) \\ &\quad + b_1\alpha_1^{x_0-\frac{y_0}{2}}(c_3e^{-i\theta y_0} - c_2e^{i\theta y_0}). \end{aligned} \tag{3.13}$$

Dividiendo ambos lados de la ecuación anterior por el número no nulo $b_2c_1\alpha_1^{y_0-\frac{x_0}{2}}$ y tomando valor abosoluto, obtenemos

$$\left|\frac{b_3}{b_2}e^{-2i\theta x_0} - 1\right| < \frac{\alpha_1^{-\frac{x_0+y_0}{2}}R + \alpha_1^{x_0-\frac{y_0}{2}}S}{|b_2||c_1|\alpha_1^{y_0-\frac{x_0}{2}}}, \tag{3.14}$$

donde

$$R := \left|(b_3c_2e^{i\theta(y_0-x_0)} - b_2c_3e^{i\theta(x_0-y_0)})\right| \quad \text{y} \quad S := |b_1| \cdot |c_3e^{-i\theta y_0} - c_2e^{i\theta y_0}|.$$

Usando (3.1), (3.2) y (3.11), tenemos que

$$\begin{aligned} R = |(b_3c_2e^{i\theta(y_0-x_0)} - b_2c_3e^{i\theta(x_0-y_0)})| &\leq |b_3||c_2| + |b_2||c_3| \\ &\leq 2|b_2||c_2| \\ &\leq 2|\beta|^{r_0+r_1} \\ &\leq 2|\beta|^4 < 20. \end{aligned} \tag{3.15}$$

De manera análoga,

$$S = |b_1||c_3e^{-i\theta y_0} - c_2e^{i\theta y_0}| \leq 2\alpha^2|\beta|^2 < 11. \tag{3.16}$$

Sustituyendo las desigualdades (3.15) y (3.16) en (3.14), obtenemos

$$\begin{aligned} \left|\frac{b_3}{b_2}e^{-2i\theta x_0} - 1\right| &\leq \frac{20\alpha_1^{-\frac{x_0+y_0}{2}} + 11\alpha_1^{x_0-\frac{y_0}{2}}}{\alpha_1^{y_0-\frac{x_0}{2}}} \\ &= \frac{20\alpha_1^{-\frac{3}{2}x_0} + 11}{\alpha_1^{\frac{3}{2}(y_0-x_0)}} \\ &\leq \frac{20\alpha_1^{-\frac{3}{2}} + 11}{\alpha_1^{\frac{3}{2}\ell}} \\ &\leq 25\alpha_1^{-\frac{3}{2}\ell}. \end{aligned} \tag{3.17}$$

A continuación usamos una forma lineal en dos logaritmos con los datos

$$t := 2, \quad \eta_1 := \frac{b_3}{b_2}, \quad \eta_2 := e^{2i\theta}, \quad d_1 := 1, \quad d_2 := -x_0.$$

A fin de aplicar el Teorema de Matveev, tomamos $\Lambda_1 := \frac{b_3}{b_2}e^{-2i\theta x_0} - 1$. Así, de (3.17) tenemos que

$$|\Lambda_1| < \alpha_1^{-\frac{3}{2}\ell}. \tag{3.18}$$

Fijamos el cuerpo numérico $\mathbb{K} = \mathbb{Q}(\alpha, \beta)$ el cual contiene a η_1, η_2 y tiene grado $D_{\mathbb{K}} = 6$ sobre $\mathbb{Q}$. Continuamos con el cálculo de la altura logarítmica

de η_1, η_2 y por ende de A_1, A_2. Una simple verificación en *Mathematica* muestra que el polinomio minimal de $\eta_2 = e^{2i\theta} = \beta_1/\gamma_1$ es

$$\prod_{\sigma \in G} (x - \sigma(\beta_1/\gamma_1)) = x^6 + 4x^5 + 11x^4 + 12x^3 + 11x^2 + 4x + 1 \qquad (3.19)$$

con Grupo de Galois G isomorfo a S_3. Por tanto, los conjugados de η_2 son γ_1/β_1, α_1/γ_1, β_1/α_1 y sus recíprocos. De nuevo, por las identidades (3.5) y (3.6), concluimos que

$$|\eta_2| = |\beta_1/\gamma_1| = |\gamma_1/\beta_1| = 1, \qquad |\beta_1/\alpha_1| = |\gamma_1/\alpha_1| = 0{,}4008\ldots,$$

y

$$|\alpha_1/\beta_1| = |\alpha_1/\gamma_1| = 2{,}494\ldots.$$

Luego, $h(\eta_2) = \frac{1}{3}\log|\alpha_1/\beta_1| < 0{,}31$. En la notación del Teorema de Matveev, podemos tomar $A_2 := 2 > \text{máx}\{6h(\eta_2), |\log \eta_2|\}$, dado que $|\log \eta_2| < 1{,}94$. La altura logarítmica cumple las siguientes propiedades

i. $h(\alpha\beta) \leq h(\alpha) + h(\beta)$,

ii. $h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2$,

iii. $h(1/\alpha) = h(\alpha)$,

iv. $h(\alpha^n) = nh(\alpha)$, $n \in \mathbb{Z}^+$.

Ahora note que $\eta_1 = b_3 b_2^{-1} = \beta^{r_0}\gamma^{-r_1}$, $r_0, r_1 \in \{0, 1, 2\}$, luego, usando las propiedades de la altura logarítmica tenemos que

$$\begin{aligned} h(\beta^{r_0}\gamma^{-r_1}) &\leq h(\beta^{r_0}) + h(\gamma^{-r_1}) \\ &= r_0 h(\beta) + r_1 h(\gamma) \\ &= (r_0 + r_1)h(\beta) \leq 4h(\beta) = 1{,}8483\ldots, \end{aligned}$$

donde la última igualdad es dada por los estimativos (3.1) y (3.2), los cuales permiten calcular $h(\alpha) = h(\beta) = h(\gamma) = 1/3\,(\log|\alpha| + \log|\beta| + \log|\gamma|) = 0,462098\ldots$.
Ahora, notando que

$$\max_{0 \leq r_0, r_1 \leq 2} \left|\log\left(\beta^{r_0}\gamma^{-r_1}\right)\right| < 2{,}97,$$

entonces podemos tomar

$$A_1 := 12 > \max_{0 \leq r_0, r_1 \leq 2} \{6h(\eta_1), |\log \eta_1|, 0{,}16\}.$$

Además, como $x_0 \geq 1$, tenemos que $B := x_0$.

Para continuar con la aplicación del Teorema de Matveev, necesitamos mostrar que $\Lambda_1 \neq 0$. Suponiendo lo contrario, obtenemos la ecuación

$$b_3 b_2^{-1} = \frac{\gamma^{r_0}}{\beta^{r_1}} = e^{2i\theta x_0}.$$

Tomando valor absoluto a ambos lados, tenemos $1 = \frac{|\gamma|^{r_0}}{|\beta|^{r_1}}$. De ahí que, $r_0 = r_1$. Luego, $e^{2i\theta x_0} = (\beta_1/\gamma_1)^{x_0} = (\gamma/\beta)^{r_0}$. Usando las identidades en (3.4), obtenemos la ecuación

$$(\gamma/\beta)^x = (\gamma/\beta)^{3x_0 - r_0} = 1.$$

Sin embargo, esto dice que γ/β es una raíz de la unidad, lo que es una contradicción, ya que las sucesiones tipo Berstel son no degeneradas.

El Teorema de Matveev nos proporciona la siguiente desigualdad

$$\exp\left(-3 \cdot 30^5 \cdot 2^{5,5} \cdot 6^2 \cdot (1 + \log 6) \cdot (1 + 2\log x_0) \cdot 2 \cdot 12\right) < |\Lambda_1|,$$

la cual combinada con la desigualdad (3.18) nos lleva a:

$$\exp\left(-3 \cdot 30^5 \cdot 2^{5,5} \cdot 6^2 \cdot (1 + \log 6) \cdot (1 + 2\log x_0) \cdot 2 \cdot 12\right) < 25\alpha_1^{-\frac{3}{2}\ell}.$$

Realizando los respectivos cálculos, obtenemos una cota superior para ℓ en términos de $\log(x_0 + 1)$:

$$y_0 - x_0 = \ell < 7{,}3 \cdot 10^{15} \log(x_0 + 1), \tag{3.20}$$

donde hemos usado el hecho que $1 + \log 2x < 3\log(x+1)$, lo cual se cumple para todo $x \geq 1$.

Con el objetivo de encontrar una cota superior para x_0 en términos de $\log(x_0 + 1)$, regresamos al determinante (3.10), sustituimos $y_0 = x_0 + \ell$ y expandimos el determinante por la primera columna de nuevo, para obtener

$$\begin{aligned} c_1\alpha_1^{x_0+\ell}(b_3\gamma_1^{x_0} - b_2\beta_1^{x_0}) &- b_1\alpha_1^{x_0}(c_3\gamma_1^{x_0+\ell} - c_2\beta_1^{x_0+\ell}) \\ &= b_3c_2\beta_1^{x_0+\ell}\gamma_1^{x_0} - b_2c_3\beta_1^{x_0}\gamma_1^{x_0+\ell}. \end{aligned} \tag{3.21}$$

Reorganizamos la ecuación (3.21) como:

$$b_2c_1\alpha_1^{\ell}\beta_1^{x_0}\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - 1\right) - b_3c_1\alpha_1^{\ell}\gamma_1^{x_0}\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell} - 1\right) = \frac{b_3c_2\beta_1^{\ell} - b_2c_3\gamma_1^{\ell}}{\alpha_1^{2x_0}}.$$

Factorizando en el lado izquierdo el término

$$b_2c_1\alpha_1^{\ell}\beta_1^{x_0}\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right),$$

y tomando valor absoluto a ambos lados, obtenemos:

$$\begin{aligned}\left|\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right| \quad \cdot \quad & \left|\frac{b_3}{b_2}\left(\frac{\gamma_1}{\beta_1}\right)^{x_0}\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell}-1\right)\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right)^{-1}-1\right| \\ \leq \quad & \frac{|b_3c_2|+|b_2c_3|}{\alpha_1^{\frac{3}{2}x_0}|b_2||c_1|} \\ < \quad & \frac{3{,}7}{\alpha_1^{\frac{3}{2}x_0}}. \end{aligned} \tag{3.22}$$

Ahora, tomamos

$$\Lambda_2 := \frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1,$$

y

$$\Lambda_3 := \frac{b_3}{b_2}\left(\frac{\gamma_1}{\beta_1}\right)^{x_0}\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell}-1\right)\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right)^{-1}-1,$$

desde de la ecuación (3.22) obtenemos

$$|\Lambda_2||\Lambda_3| < 3{,}7\cdot\alpha_1^{-\frac{3}{2}x_0}. \tag{3.23}$$

Aplicamos una vez más el Teorema de Matveev a cada valor absoluto del lado izquierdo de la ecuación (3.23).

Para Λ_2, usamos los datos

$$t := 2, \qquad \eta_1 := \frac{b_1}{b_2}\frac{c_2}{c_1}, \qquad \eta_2 := \frac{\beta_1}{\alpha_1}, \qquad d_1 := 1, \qquad d_2 := \ell.$$

Como en la aplicación anterior del Teorema de Matveev, tomamos $\mathbb{K} := \mathbb{Q}(\alpha,\beta)$ con $D_{\mathbb{K}} = 6$ y $A_2 := 2$. Por las propiedades de la altura logarítmica, tenemos

$$\begin{aligned} h(\eta_1) = h\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\right) = h\left(\frac{\alpha^{r_0}\beta^{r_1}}{\beta^{r_0}\alpha^{r_1}}\right) \quad & \leq \quad h(\alpha^{r_0})+h(\beta^{r_1})+h(\beta^{r_0})+h(\alpha^{r_1}) \\ & = \quad r_0h(\alpha)+r_0h(\beta)+r_1h(\alpha)+r_1h(\beta) \\ & = \quad 2(r_0+r_1)h(\beta) \\ & \leq \quad 8h(\beta) < 3{,}7. \end{aligned}$$

Por otra parte,

$$\max_{0\le r_0,r_1\le 2}\left|\log\left(\frac{\alpha^{r_0}\beta^{r_1}}{\beta^{r_0}\alpha^{r_1}}\right)\right| < 3{,}291,$$

Así, podemos tomar $A_1 := 23 > \max\{6h(\eta_1), |\log\eta_1|, 0{,}16\}$. Además $B := \ell$ y Λ_2 no es cero por el mismo argumento usado para mostrar que $\Lambda_1 \neq 0$.

La conclusión del Teorema de Matveev nos lleva a la siguiente desigualdad

$$\exp\left(-1{,}28\cdot 10^{16}\log(\ell+1)\right) < |\Lambda_2|. \tag{3.24}$$

Para Λ_3, tenemos una forma lineal con dos logaritmos con los parámetros

$$t := 2, \quad \eta_1 := \frac{\gamma_1}{\beta_1}, \quad \eta_2 := \frac{b_3}{b_2}\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell} - 1\right)\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - 1\right)^{-1},$$

$$d_1 := x_0, \qquad d_2 := 1.$$

Tomamos de nuevo $A_1 := 2$. De acuerdo a las propiedades de la altura logarítmica

$$h(\eta_2) \le h\left(\frac{b_3}{b_2}\right) + h\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell} - 1\right) + h\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - 1\right).$$

Pero

$$h\left(\frac{b_3}{b_2}\right) \le r_0 h(\gamma) + r_0 h(\beta) = 2r_0 h(\beta) < 1{,}85,$$

y

$$\begin{aligned} h\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell} - 1\right) &\le h\left(\frac{b_1}{b_3}\right) + h\left(\frac{c_1}{c_3}\right) + \ell\cdot h\left(\frac{\gamma_1}{\alpha_1}\right) + \log 2 \\ &\le 1{,}85 + 1{,}85 + 0{,}304\ell + 0{,}7 < 5\ell. \end{aligned}$$

Similarmente

$$h\left(\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - 1\right) < 5\ell.$$

Por tanto, $h(\eta_2) < 12\ell$ y podemos tomar $A_2 := 72\ell$. Finalmente, tomamos $B := x_0$. Para continuar con la aplicación del Teorema de Matveev debemos mostrar que $\Lambda_3 \neq 0$. De otro modo, obtenemos la ecuación

$$\gamma_1^{x_0}\left(\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell} - 1\right) = \beta_1^{x_0}\left(\frac{b_1}{b_3}\frac{c_2}{c_1}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - \frac{b_2}{b_3}\right).$$

Conjugando esta relación con el automorfismo $\sigma:\ \alpha \to \beta,\ \beta \to \gamma,\ \gamma \to \alpha$ (luego, $\alpha_1 \to \beta_1,\ \beta_1 \to \gamma_1,\ \gamma_1 \to \alpha_1,\ b_1 \to b_2,\ b_2 \to b_3,\ b_3 \to b_1$ y $c_1 \to c_2,\ c_2 \to c_3,\ c_3 \to c_1$) y tomando valor absoluto a ambos lados de la igualdad resultante, concluimos que

$$\alpha_1^{\frac{3}{2}x_0}\left|\frac{b_2}{b_1}\frac{c_1}{c_2}\left(\frac{\alpha_1}{\beta_1}\right)^{\ell}-1\right| = \left|\frac{b_2}{b_1}\frac{c_3}{c_2}\left(\frac{\gamma_1}{\beta_1}\right)^{\ell}-\frac{b_3}{b_1}\right|.$$

Usando las identidades (3.2), (3.6) y (3.11), notamos que

$$\begin{aligned}\left|\frac{b_2}{b_1}\frac{c_3}{c_2}\left(\frac{\gamma_1}{\beta_1}\right)^{\ell}-\frac{b_3}{b_1}\right| &\leq \left|\frac{b_2}{b_1}\right|\left|\frac{c_3}{c_2}\right|\left|\frac{\gamma_1}{\beta_1}\right|^{\ell}+\left|\frac{b_3}{b_1}\right| \\ &= \left|\frac{\beta}{\alpha}\right|^{r_0}+\left|\frac{\gamma}{\alpha}\right|^{r_0} \\ &= 2\left(\frac{2}{\alpha^{\frac{3}{2}}}\right)^{2} < 4,\end{aligned}$$

y

$$\begin{aligned}\left|\frac{b_2}{b_1}\frac{c_1}{c_2}\left(\frac{\alpha_1}{\beta_1}\right)^{\ell}-1\right| &\geq \left|\frac{b_2}{b_1}\right|\left|\frac{c_1}{c_2}\right|\left|\frac{\alpha_1}{\beta_1}\right|^{\ell}-1 \\ &= \left|\frac{\alpha}{\beta}\right|^{r_1-r_0}\cdot\left|\frac{\alpha_1}{\beta_1}\right|^{\ell}-1 \\ &= \left(\frac{\alpha^{\frac{3}{2}}}{2}\right)^{r_1-r_0}\alpha_1^{\frac{3\ell}{2}}-1 \\ &> \left(\frac{2}{\alpha^{\frac{3}{2}}}\right)^{2}\cdot\alpha_1^{\frac{3}{2}}-1>3.\end{aligned}$$

Luego,

$$3\cdot\alpha_1^{\frac{3}{2}x_0} < \alpha_1^{\frac{3}{2}x_0}\left|\frac{b_1}{b_3}\frac{c_3}{c_1}\left(\frac{\gamma_1}{\beta_1}\right)^{\ell}-1\right| = \left|\frac{b_1}{b_2}\frac{c_2}{c_1}\left(\frac{\gamma_1}{\beta_1}\right)^{\ell}-\frac{b_2}{b_3}\right| < 4,$$

lo cual es imposible para $x_0 \geq 1$.

El Teorema de Matveev nos lleva a la siguiente desigualdad

$$\exp\left(-4{,}17\cdot 10^{16}\log(x_0+1)\cdot\ell\right) < |\Lambda_3|. \tag{3.25}$$

Luego, de (3.23), (3.24) y (3.25), concluimos que

$$\exp\left(-1{,}28\cdot 10^{16}\log(\ell+1)-4{,}17\cdot 10^{16}\log(x_0+1)\ell\right)<3{,}7\alpha_1^{-\frac{3}{2}x_0}.$$

Tomando logaritmo a cada lado y realizando algunos cálculos, obtenemos

$$x_0<71{,}42\cdot 10^{16}\log(\ell+1)+4{,}6\times 10^{16}\log(x_0+1)\ell. \tag{3.26}$$

Sustituyendo la desigualdad (3.20) en (3.26), obtenemos

$$\begin{aligned} x_0 \;<\; & 1{,}7\cdot 10^{32}\log^2(x_0+1) \\ & +1{,}42\cdot 10^{16}\log\log(x_0+1)+5{,}1\cdot 10^{17}. \end{aligned}$$

Esto nos lleva a $x_0<1{,}2\times 10^{36}$, y regresando a la desigualdad (3.20) obtenemos que $\ell<3\times 10^{17}$. En el siguiente lema resumimos lo que hemos obtenido hasta ahora.

Lema 3.3.1. *Sea $(u_n)_{n\in\mathbb{Z}}$ una sucesión lineal recurrente ternaria tipo Berstel. Si n_0 y $1\le x<y$ son números enteros tales que $u_{n_0}=u_{n_0-x}=u_{n_0-y}=0$, entonces*

$$x<3{,}7\times 10^{36} \quad e \quad y-x<9{,}1\times 10^{17}. \tag{3.27}$$

3.4. Reduciendo las cotas para ℓ y x_0

Ahora, usamos algunos resultados conocidos de fracciones continuas, los cuales mencionamos en el Apéndice, para reducir las cotas dadas en (3.27). Para hacer esto, retornamos a las desigualdades (3.17) y (3.23), y usamos los Lemas A.4.1 y A.4.2.

Reduciendo ℓ.

Primero que todo, hacemos la siguiente observación sobre $|\Lambda_1|$ dada en la ecuación (3.17):

$$\begin{aligned} |\Lambda_1|=\left|\frac{b_3}{b_2}e^{-2i\theta x_0}-1\right| &= \left|\frac{\gamma^{r_0}}{\beta^{r_0}}e^{-2i\theta x_0}-1\right| \\ &= |e^{-2i(x_0\theta+r_0\omega)}-1| \\ &= |(\cos(2(x_0\theta+r_0\omega))-1)-i\sin(2(x_0\theta+r_0\omega))| \\ &\ge |\sin(2(x_0\theta+r_0\omega))|. \end{aligned}$$

Poniendo $m := \lfloor 2(x_0\omega + r_0\theta)/\pi \rceil$, donde $\lfloor y \rceil$ es el entero más cercano al número real y, entonces $-\pi/2 \leq 2(x_0\theta + r_0\omega) - m\pi \leq \pi/2$. Por tanto, de la desigualdad (3.17), obtenemos

$$\begin{aligned} 25 \cdot \alpha_1^{-\frac{3}{2}\ell} > |\sin(2(x_0\theta + r_0\omega)| &= |\sin(2(x_0\theta + r_0\omega) - m\pi)| \\ &\geq 2\left|\frac{2(x_0\theta + r_0\omega)}{\pi} - m\right|, \end{aligned} \tag{3.28}$$

donde hemos usado que $|\sin\phi| = \sin|\phi| \geq \frac{2}{\pi}|\phi|$, lo cual se cumple para todo $-\pi/2 \leq \phi \leq \pi/2$. Luego, podemos concluir de la desigualdad (3.28) que

$$\left|\left(\frac{2\theta}{\pi}\right) x_0 - m + \frac{2r_0\omega}{\pi}\right| < \frac{13}{\alpha_1^{\frac{3}{2}\ell}}. \tag{3.29}$$

Si $r_0 = 0$, entonces desde (3.29)

$$\left|\frac{2\theta}{\pi} - \frac{m}{x_0}\right| < \frac{13}{x_0\alpha_1^{\frac{3}{2}\ell}}. \tag{3.30}$$

En este punto, aplicamos el método de reducción del Lema A.4.1 con $\gamma = 2\theta/\pi$, el cual es un número irracional, ya que de no ser así, θ sería un múltiplo racional de π y por tanto $\beta_1/\gamma_1 = e^{2i\theta}$ sería una raíz de la unidad, luego existe un $n \in \mathbb{N}$ tal que

$$(\beta_1/\gamma_1)^n = 1.$$

Conjugando esta ecuación con el automorfismo $\sigma:\ \alpha \to \beta,\ \beta \to \gamma,\ \gamma \to \alpha$ (luego, $\alpha_1 \to \beta_1,\ \beta_1 \to \gamma_1,\ \gamma_1 \to \alpha_1$) y tomando valor absoluto a cada lado obtenemos

$$|\gamma_1/\alpha_1|^n = 1$$

lo que no es posible ya que $|\gamma_1| < |\alpha_1|$. Usamos *Mathematica* para calcular el inicio de la fracción continua de γ:

$$\begin{aligned} [&\mathbf{1}, \mathbf{2}, \mathbf{1}, \mathbf{1}, \mathbf{2}, \mathbf{6}, \mathbf{1}, \mathbf{5}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{11}, \mathbf{25}, \mathbf{2}, \mathbf{21}, \mathbf{1}, \mathbf{2}, \mathbf{1}, \mathbf{5}, \mathbf{4}, \mathbf{60}, \mathbf{8}, \mathbf{2}, \mathbf{1}, \mathbf{2}, \mathbf{8}, \mathbf{2}, \mathbf{1}, \mathbf{1}, \\ &\mathbf{60}, \mathbf{1}, \mathbf{5}, \mathbf{3}, \mathbf{1}, \mathbf{4}, \mathbf{29}, \mathbf{2}, \mathbf{24}, \mathbf{19}, \mathbf{1}, \mathbf{3}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{2}, \mathbf{1}, \mathbf{12}, \mathbf{2}, \mathbf{1}, \mathbf{1}, \mathbf{3}, \mathbf{1}, \mathbf{3}, \mathbf{12}, \mathbf{8}, \\ &\mathbf{1}, \mathbf{3}, \mathbf{10}, \mathbf{80}, \mathbf{6}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{1}, \mathbf{5}, \mathbf{2}, 2, 39, 8, 5, 1, 6, 3, 1, 1, 2, 1, 2, \dots], \end{aligned}$$

y algunas de sus primeras convergentes, y encontramos que el denominador de C_{68}, $q_{68} = 196227318428967708939906755458317104 4 > 1,2 \times 10^{36} > x_0$,

por tanto en notación del Lema A.4.1, $a_M = \max_{0\leq m\leq 68}\{a_m\} = 80$. La conclusión del Lema A.4.1 nos permite estimar la siguiente desigualdad

$$\frac{1}{(80+2)x_0^2} < \left|\gamma - \frac{m}{x_0}\right|. \tag{3.31}$$

Luego, combinando las desigualdades (3.30) y (3.31) y realizando algunos cálculos obtenemos

$$\alpha_1^{\frac{3}{2}\ell} < 1{,}28 \times 10^{39},$$

por tanto, $\ell \leq 99$.

Ahora, si $r_0 = 1, 2$, tomamos

$$\Gamma_1 := \left(\frac{2\theta}{\pi}\right) x_0 - m + \frac{2r_0\omega}{\pi},$$

el cual no es cero ya que $\Lambda_1 \neq 0$. Si $\Gamma_1 > 0$, entonces por (3.29), obtenemos

$$0 < \left(\frac{2\theta}{\pi}\right) x_0 - m + \frac{2r_0\omega}{\pi} < 13\alpha_1^{-\frac{3}{2}\ell}. \tag{3.32}$$

Tomamos

$$\tau := \frac{2\theta}{\pi}, \qquad \mu := \frac{2r_0\omega}{\pi}, \qquad A := 13, \qquad B := \alpha_1^{3/2}.$$

La desigualdad (3.32) puede ser reescrita como

$$0 < \tau x_0 - m + \mu < AB^{-\ell}. \tag{3.33}$$

Como hemos mostrado antes $\tau = 2\theta/\pi$ es un número irracional. Por último, tomamos $M := 1{,}2 \times 10^{36}$ el cual es una cota superior para x_0 por las desigualdades (3.27). Aplicamos el método de reducción del Lema A.4.2 a la desigualdad (3.33) para $r_0 \in \{1, 2\}$. Con ayuda de *Mathematica*, encontramos que $q_{70} > 6M$ y $\epsilon = 0{,}332563\ldots$ garantizan que el máximo valor de $\lfloor \log(Aq/\epsilon)/\log B \rceil$ es 101, el cual es una cota superior para ℓ, de acuerdo al Lema A.4.2. Esto fue cuando $\Gamma_1 > 0$. Pero si $\Gamma_1 < 0$, entonces de (3.29), obtenemos

$$0 < \left(\frac{\pi}{2\theta}\right) m - x_0 - \frac{r_0\omega}{\theta} < 9{,}4\alpha_1^{-\frac{3}{2}\ell}. \tag{3.34}$$

En este caso, tenemos que

$$0 < \tau m - x_0 + \mu < AB^{-\ell}, \tag{3.35}$$

donde

$$\tau := \frac{\pi}{2\theta}, \qquad \mu := \frac{r_0\omega}{\theta}, \qquad A := 9{,}4, \qquad B := \alpha_1^{3/2}.$$

Claramente τ es un número irracional. Finalmente, tomamos $M := \lfloor 1{,}2 \times 10^{36}(2\theta/\pi) + (2r_0\omega/\pi) + 1 \rceil$ el cual es una cota superior para m y aplicamos de nuevo el Lema A.4.2 para $r_0 \in \{1, 2\}$ a la desigualdad (3.35). Con ayuda de *Mathematica* encontramos que $q_{87} > 6M$ y $\epsilon = 0{,}065199\ldots$ maximizan el valor de $\lfloor \log(Aq/\epsilon)/\log B \rceil$ a 99, el cual es una cota superior para ℓ según el Lema A.4.2. En resumen tenemos que $1 \leq \ell \leq 101$.

Reduciendo la cota de x_0.

En esta sección, asumimos que $x_0 \geq 3$. Note primero que

$$\min_{\substack{0\leq r_0, r_1 \leq 2 \\ 1 \leq \ell \leq 101}} \left| \frac{\alpha^{r_0}}{\beta^{r_0}} \frac{\beta^{r_1}}{\alpha^{r_1}} \left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - 1 \right| > 0{,}8237,$$

luego de la desigualdad (3.23), concluimos que

$$|\Lambda_3| < 4{,}5\alpha_1^{-\frac{3}{2}x_0}. \tag{3.36}$$

Dado que $x_0 \geq 3$, entonces obtenemos que $|\Lambda_3| < 1/2$. Tomando

$$\log z = \log|z| + i \arg z \quad \text{donde} \quad -\pi < \arg z \leq \pi$$

para el logaritmo de un número complejo z, tenemos que

$$\log(1+z) = \sum_{n=1}^{\infty} (-1)^n \frac{z^n}{n}, \qquad z \in \mathbb{C} \qquad \text{con} \qquad |z| < 1.$$

De aquí, fácilmente se muestra que

$$|\log(1+z)| \leq 2|z| \qquad \text{si} \qquad |z| < 1/2.$$

Por tanto, con $z = \Lambda_3$, y recordando que el logaritmo complejo es aditivo módulo $2\pi i$, esto es $\log(\omega\theta) = \log\omega + \log\theta + 2\pi i m$ para algún $m \in \mathbb{Z}$, y que $\log(\gamma_1/\beta_1) = -2\theta i$, concluimos de la desigualdad (3.36) que

$$\left| \log\left[\frac{b_3}{b_2} \left(\frac{b_1}{b_3}\frac{c_3}{c_1} \left(\frac{\gamma_1}{\alpha_1}\right)^{\ell} - 1 \right) \left(\frac{b_1}{b_2}\frac{c_2}{c_1} \left(\frac{\beta_1}{\alpha_1}\right)^{\ell} - 1 \right)^{-1} \right] - 2\theta x_0 i + 2\pi t i \right| < 9\alpha_1^{-\frac{3}{2}x_0}, \tag{3.37}$$

se cumple para algún $t \in \mathbb{Z}$. Usando $|\log(1+\Lambda_3)| \leq 2|\Lambda_3| < 1$ y la desigualdad (3.37) obtenemos

$$|2\pi t i| < 1+|2\theta x_0 i|+\left|\log\left[\frac{\gamma^{r_0}}{\beta^{r_0}}\left(\frac{\alpha^{r_0}}{\gamma^{r_0}}\frac{\gamma^{r_1}}{\alpha^{r_1}}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell}-1\right)\left(\frac{\alpha^{r_0}}{\beta^{r_0}}\frac{\beta^{r_1}}{\alpha^{r_1}}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right)^{-1}\right]\right|. \tag{3.38}$$

Ahora, notando que

$$\max_{\substack{0\leq r_0,r_1\leq 2\\ 1\leq \ell\leq 101}}\left|\log\left[\frac{\gamma^{r_0}}{\beta^{r_0}}\left(\frac{\alpha^{r_0}}{\gamma^{r_0}}\frac{\gamma^{r_1}}{\alpha^{r_1}}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell}-1\right)\left(\frac{\alpha^{r_0}}{\beta^{r_0}}\frac{\beta^{r_1}}{\alpha^{r_1}}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right)^{-1}\right]\right| < 3,03,$$

de la desigualdad (3.38) tenemos que

$$2\pi|t| \leq 1 + 2\theta x_0 + 3,03,$$

y como $x_0 < 1,2 \times 10^{32}$, la desigualdad anterior nos permite concluir que $|t| < 8{,}4 \cdot 10^{35}$. Sea

$$\zeta(r_0, r_1, \ell) := Re\left[-i\log\left(\frac{\gamma^{r_0}}{\beta^{r_0}}\left(\frac{\alpha^{r_0}}{\gamma^{r_0}}\frac{\gamma^{r_1}}{\alpha^{r_1}}\left(\frac{\gamma_1}{\alpha_1}\right)^{\ell}-1\right)\left(\frac{\alpha^{r_0}}{\beta^{r_0}}\frac{\beta^{r_1}}{\alpha^{r_1}}\left(\frac{\beta_1}{\alpha_1}\right)^{\ell}-1\right)^{-1}\right)\right].$$

Observamos de la desigualdad (3.37) que

$$|2\pi t - 2\theta x_0 + \zeta(r_0, r_1, \ell)| < 9\alpha_1^{-\frac{3}{2}x_0}. \tag{3.39}$$

Además, con ayuda de *Mathematica* encontramos que

$$-3{,}0207 < \zeta(r_0, r_1, \ell) < 1{,}33169$$

se cumple para todo $1 \leq \ell \leq 101$ y $0 \leq r_0, r_1, \leq 2$, luego t debe ser un entero positivo, de otro modo la desigualdad (3.39) no se cumple con x_0 suficientemente grande. Así, de ahora en adelante consideraremos la desigualdad (3.39) en el rango donde x_0 y t son enteros positivos $< 1{,}2 \cdot 10^{36}$.

Para cada $1 \leq \ell \leq 101$ y cada $0 \leq r_0, r_1 \leq 2$, usamos el método de reducción del Lema A.4.2. Tomando $\Gamma_2 := 2\pi t - 2\theta x_0 + \zeta(r_0, r_1, \ell)$, tenemos que $\Gamma_2 \neq 0$ ya que $\Lambda_3 \neq 0$. Describimos en paralelo los casos $\Gamma_2 > 0$ y $\Gamma_2 < 0$.

$\Gamma_2 > 0$	$\Gamma_2 < 0$
$0 < \left(\frac{\pi}{\theta}\right)t - x_0 + \frac{\zeta(r_0,r_1,\ell)}{2\theta} < 2{,}1\alpha_1^{-3x_0/2}$	$0 < \left(\frac{\theta}{\pi}\right)x_0 - t - \frac{\zeta(r_0,r_1,\ell)}{2\pi} < 1{,}5\alpha_1^{-3x_0/2}$
$\tau := \pi/\theta, \quad \mu := \zeta(r_0, r_1, \ell)/2\theta$	$\tau := \theta/\pi, \quad \mu := -\zeta(r_0, r_1, \ell)/2\pi$
$A := 2{,}1, \quad B := \alpha_1^{\frac{3}{2}}$	$A := 1{,}5, \quad B := \alpha_1^{\frac{3}{2}}$

Las condiciones sobre x_0 y t en la ecuación (3.39) nos permiten tomar $M := 1{,}2 \cdot 10^{36}$ en ambos casos. Además, por los argumentos mostrados con anterioridad τ es un número irracional en ambos casos. Una nueva implementación del Lema A.4.2 en *Mathematica* nos dice que q_{77} y $\epsilon = 0{,}0006696\ldots$, aseguran que el máximo valor de $\lfloor \log(Aq/\epsilon)/\log B \rceil$ es 105 para $\Gamma_2 > 0$ y también que q_{78} y $\epsilon = 0{,}00027122\ldots$, maximizan el valor de $\lfloor \log(Aq/\epsilon)/\log B \rceil$ a 107, para $\Gamma_2 < 0$. Luego, concluimos que $x_0 \leq 107$.

Finalmente, de (3.9) obtenemos

$$x = 3x_0 - r_0 \leq 321 \quad \text{e} \quad y = 3y_0 - r_1 \leq 3(x_0 + \ell) \leq 624.$$

Resumiendo, hemos demostrado el siguiente resultado.

Lema 3.4.1. *Sea $(u_n)_{n\in\mathbb{Z}}$ una sucesión lineal recurrente ternaria tipo Berstel no nula. Si $1 \leq x < y$ son enteros y n_0 es algún número entero tal que $u_{n_0} = u_{n_0-x} = u_{n_0-y} = 0$, entonces*

$$x \leq 321 \qquad \text{e} \qquad y \leq 624.$$

3.5. Cálculos finales y conclusiones.

Recordemos que la sucesión de Berstel $(B_n)_{n\in\mathbb{Z}}$ tiene cero-multiplicidad 6 con $B_0 = B_1 = B_4 = B_6 = B_{13} = B_{52} = 0$. Una simple búsqueda en *Mathematica* nos muestra que en el rango para (x, y) indicado por el Lema 3.4.1, el determinante (3.8) es cero sólo en los siguientes casos:

x	2	2	3	5	7	7	7	9	9	12	16
y	5	6	4	6	9	12	13	12	13	13	24

x	39	39	39	39	46	46	46	48	48	51
y	46	48	51	52	48	51	52	51	52	52

.

Todas estas soluciones (x, y) excepto $(16, 24)$ provienen de desplazamientos adecuados de los subíndices de la sucesión de Berstel. Para $(x, y) = (16, 24)$, suponemos $n_0 = 24$, luego de (3.7) tenemos que $u_0 = u_8 = u_{24} = 0$. Con el propósito de determinar tal sucesión recurrente ternaria $(u_n)_{n\in\mathbb{Z}}$, asumimos que $u_0 = 0, u_1 = a$ y $u_2 = b$, con $a,\ b$ enteros positivos. Además, como los ceros de u_n permanecen invariante bajo multiplicación por escalar, podemos asumir que $a = 1$.

Ahora calculamos los términos u_8 y u_{24}, con $u_{n+3} = 4u_{n+2} - 4u_{n+1} + 2u_n$ y valores iniciales $u_0 = 0,\ u_1 = 1$ y $u_2 = b$:

$$u_8 = 16(b-4), \qquad \text{y} \qquad u_{24} = -131072(b-4).$$

Esto nos lleva a concluir que el caso $(x, y) = (16, 24)$ corresponde a desplazamientos de los subíndices y múltiplos escalares de la sucesión tipo Berstel $(u_n)_{n\in\mathbb{Z}}$, con valores iniciales $u_0 = 0, u_1 = 1$ y $u_2 = 4$.

Esto completa la prueba de nuestro resultado.

Capítulo 4

Conclusiones

1. En resumen, el método de Beukers expuesto en el Capítulo II para resolver la cero multiplicidad de sucesiones lineales recurrentes ternarias, se basa en apoyarse en un trabajo anterior en el cual resuelve el problema de la $a-$multiplicidad de sucesiones lineales recurrentes binarias. En este resuelve la ecuación $\lambda\alpha^x + \mu\beta^x = 1$, la cual es equivalente a $c_1\theta_1 + c_2\theta_2 + c_3\theta_3 = 0$, siendo esta última la que en realidad necesitamos resolver. Entonces separa la demostración teniendo el cuenta el caso real, el cual es sencillo de tratar, mientras el caso complejo nuevamente lo divide teniendo en cuenta la relación de igualdad de $|\theta_1|_\mathfrak{p}, |\theta_2|_\mathfrak{p}, |\theta_3|_\mathfrak{p}$ donde $\mathfrak{p}$ es un ideal primo del anillo de enteros algebraicos de $\mathbb{K} = \mathbb{Q}(\theta_1, \theta_3)$, luego termina la demostración mostrando que en cada subcaso e la ecuación $c_1\theta_1^x + c_2\theta_2^x + c_3\theta_3^x = 0$ para $x \in \mathbb{Z}$ no tiene más de 6 soluciones.

2. La pregunta natural que podría surgir es si este método de Beukers se puede utilizar para resolver la cero-multiplicidad de sucesiones lineales recurrentes de orden $k \geq 4$. Lamentablemente el método no se ajusta ya que, por ejemplo para $k = 4$, primero que todo se tendría que haber resuelto el problema de la a-multiplicidad de sucesiones lineales recurrentes ternarias, el cual hasta el momento no se ha resuelto. Más aún, si este ya estuviera resuelto, el siguiente paso sería dividir en el caso en que las raíces del polinomio característico sean todas reales o se tenga alguna compleja. Como ya mencionamos, el caso real es fácil de tratar, mientras el caso complejo, siguiendo con la línea de Beukers deberíamos hacer el análisis de la relación de igualdad de los posibles valores de $|\theta_1|_\mathfrak{p}, |\theta_2|_\mathfrak{p}, |\theta_3|_\mathfrak{p}, |\theta_4|_\mathfrak{p}$ donde $\theta_1, \theta_2, \theta_3, \theta_4$ son las 4 raíces del

polinomio característico de una sucesión lineal recurrente de orden 4, lo que produciría un número mayor de subcasos del caso complejo. Esto nos permite concluir que a primera vista, el método de Beukers sólo se ajusta al caso de sucesiones recurrentes ternarias.

3. Usamos el resultado de Matveev [16], el cual proporciona una cota inferior explícita para el valor absoluto de una forma lineal en logaritmos de números algebraicos, para acotar el rango de solución de las variables enteras de la ecuación diofántica exponencial

$$b_2\beta_1^{x_0}c_3\gamma_1^{y_0} - b_3\gamma_1^{y_0}c_2\beta_1^{y_0} - b_1\alpha_1^{x_0}(c_3\gamma_1^{y_0} - c_2\beta_1^{y_0}) + c_1\alpha_1^{y_0}(b_3\gamma_1^{x_0} - b_2\beta_1^{x_0}) = 0.$$

Para después reducir el rango de solución con los métodos de reducción de la sección A.4. Esta forma de proceder puede ser adaptada a diversos problemas en teoría de sucesiones lineales recurrentes. Por ejemplo para un trabajo próximo pensamos explorar este método para resolver la cero-multiplicidad de de la sucesión $k-$*generalizada de Fibonacci* denotada por $(F_n^{(k)})_n$ y definimos para un número entero $k \geq 4$ fijo como sigue

$$F_n^{(k)} = F_{n-1}^{(k)} + F_{n-2}^{(k)} + \cdots + F_{n-k}^{(k)},$$

con valores iniciales $F_0^{(k)} = F_1^{(k)} = \cdots = F_{k-1}^{(k)} = 0, F_k^{(k)} = 1$.

Apéndice A

Fracciones continuas.

Revisamos algunos aspectos básicos de las fracciones continuas que son necesarios para comprender los lemas de reducción que utilizamos en el Capítulo III. Para un tratamiento más completo y consultar las pruebas de los resutados presentados aquí ver la referencia [1].

A.1. Fracciones continuas simples

Una *fracción continua finita* es una expresión de la forma

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} \tag{A.1}$$

donde, $a_0 \in \mathbb{R}$ y $a_i \in \mathbb{R}^+$ para todo $1 \leq i \leq n$. Usaremos la notación $[a_0, a_1, \ldots, a_n]$ para la expresión de arriba. La fracción continua $[a_0, a_1, \ldots, a_n]$ se denomina *simple* si $a_0, \ldots, a_n \in \mathbb{Z}$. La fracción continua $C_k = [a_0, a_1, \ldots, a_k]$ con $0 \leq k \leq n$ se denomina la *k-ésima convergente* de $[a_0, a_1, \ldots, a_n]$.
Es claro que cada fracción continua simple es un número racional. De manera recíproca, usando el algoritmo de Euclides, cada racional se puede representar como una fracción continua simple. En efecto, si p y q son primos entre

si y escribimos

$$\begin{array}{ll} p & = qa_0 + r_1, \qquad 1 \leq r_1 \leq q; \\ q & = a_1 r_1 + r_2, \qquad 1 \leq r_2 \leq r_1; \\ \vdots & \vdots \\ r_{n-1} & = a_n r_n, \end{array}$$

donde $n \geq 0$ es maximal tal que $r_n \geq 1$, se ve fácilmente que la expresión (A.1) es p/q.
Para cada fracción continua $[a_0, a_1, \ldots, a_n]$ definimos $p_0, p_1, \ldots, p_n$ y $q_0, q_1, \ldots, q_n$ mediante las relaciones de recurrencia

$$\begin{array}{ll} p_0 = a_0, & q_0 = 1; \\ p_1 = a_0 a_1 + 1, & q_1 = a_1; \\ p_k = a_k p_{k-1} + p_{k-2}, & q_k = a_k q_{k-1} + q_{k-2}; \end{array}$$

para todo $k = 2, \ldots, n$.
La siguiente proposición resalta propiedades de las convergentes de una fracción continua finita, las cuales son fundamentales a la hora de definir las fracciones continuas infinitas.

Proposición A.1.1. *Con la notación anterior se cumple:*

(i) $C_k = p_k/q_k$, *para* $1 \leq k \leq n$

(ii) $p_k q_{k-1} - p_{k-1} q_k = (-1)^k$ *para todo* $1 \leq k \leq n$,

(iii)

$$C_k - C_{k-1} = \frac{(-1)^{k-1}}{q_k q_{k-1}} \qquad \textit{para} \quad 1 \leq k \leq n.$$

(iv)

$$C_k - C_{k-2} = \frac{(-1)^k a_k}{q_k q_{k-2}} \qquad \textit{para} \quad 2 \leq k \leq n.$$

A.2. Fracciones continuas infinitas.

Las partes (iii) y (iv) de la Proposición A.1 muestran que $C_k < C_{k-2}$ si $k \geq 3$ es impar y $C_k > C_{k-2}$ si $k \geq 2$. Por tanto,

$$C_1 > C_3 > C_5 > \cdots \quad y \quad C_2 < C_4 < C_6 \cdots .$$

Además,

$$C_{2m} - C_{2m-1} = \frac{(-1)^{2m-1}}{q_{2m}q_{2m-1}} < 0,$$

por tanto,

$$C_1 > C_3 > C_5 > \cdots > C_6 > C_4 > C_2.$$

Luego, si $(a_n)_{n\geq 0}$ es una sucesión infinita de enteros con $a_n > 0$ para $n \geq 1$, poniendo $C_k = [a_0, \ldots, a_k]$ deducimos que

(i) La sucesión $(C_{2n+1})_{n\geq 0}$ es decreciente y acotada, en particular convergente.

(ii) La sucesión $(C_{2n})_{n\geq 0}$ es creciente y acotada, en particular convergente.

(iii) La sucesión $C_{2n} - C_{2n-1}$ tiende a cero.

En particular, $(C_n)_{n\geq 0}$ es convergente. Esto nos permite definir correctamente las fracciones continuas infinitas. Sea $(a_n)_{n\geq 0}$ una sucesión infinita de números enteros con $a_n > 0$ para $n \geq 1$. Definimos la fracción continua infinita como el limite de las fracciones continuas finitas

$$[a_0, a_1, a_2, \ldots] := \lim_{n\to\infty} C_n.$$

Es fácil ver que las fracciones continuas infinitas representan siempre números irracionales. Recíprocamente, cualquier número irracional α se puede desarrollar en fracción continua.

Proposición A.2.1. *Dado $\alpha = \alpha_0 \in \mathbb{R} \setminus \mathbb{Q}$, definimos la sucesión $(a_n)_{n\geq 0}$ por*

$$a_k = \lfloor \alpha_k \rfloor, \qquad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \quad \textit{para todo } k \geq 0.$$

Entonces $\alpha = [a_0, a_1, \ldots]$.

A.3. Convergentes

En esta sección, mostraremos que las convergentes p_k/q_k de la fracción continua de un número irracional α son la mejor aproximación diofántica de α por racionales.

Proposición A.3.1. *(i) Sea α un número irracional y sea $C_k = p_k/q_k$ para $k \geq 0$ las convergentes de la fracción continua de α. Si $r, s \in \mathbb{Z}$ con $s > 0$ y k es un entero positivo tal que*

$$|s\alpha - r| < |q_k\alpha - p_k|,$$

entonces $s \geq q_{k+1}$

(ii) Si α es un número irracional y r/s es un número racional con $s > 0$ tal que

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2},$$

entonces r/s es una convergente de α.

La parte (ii) de la Proposición A.3.1 es conocida como el criterio de Legendre, para determinar si un numero racional r/s es una convergente de α.

A.4. Métodos de reducción

Determinar la finitud de las soluciones de un problema diofántico es un gran avance, sin embargo en muchas ocasiones las cotas obtenidas para las incógnitas enteras involucradas siguen siendo demasiado grandes para ser manipuladas aún computacionalmente. Por lo que, se hace necesario la reducción de tales cotas. Para alcanzar este objetivo usamos la teoría de fracciones continuas que hemos abordado.

Los siguientes resultados determinan herramientas efectivas en este propósito. El primer método de reducción es un Lema de Dujella y Pethő [8]. Para un número real x, denotamos la distancia de x al entero más cercano, por $||x|| := \text{mín}\{|x - n| : n \in \mathbb{Z}\}$.

Lema A.4.1. *Sean, M un entero positivo, p/q una convergente de la fracción continua del irracional τ tal que $q > 6M$ y A, B, μ números reales con $A > 0$, $B > 1$ y $\mu \neq 0$. Sea $\epsilon := ||\mu q|| - M||\tau q||$. Si $\epsilon > 0$ entonces no existe ninguna solución de la desigualdad*

$$0 < m\tau - n + \mu < AB^{-m},$$

en enteros positivos m y n con $\log(Aq/\epsilon)/\log B \leq m \leq M$.

Cuando $\mu = 0$, una importante propiedad de la teoría de aproximación diofántica determina un nuevo método de reducción, la cual es una variación del criterio de Legendre.

Lema A.4.2. *Sea τ un número irracional con fracción continua $[a_0, a_1, a_2 \ldots]$ y convergentes p_1/q_1, $p_2/q_2, \ldots$. Si t es un entero positivo tal que $q_t > m$ y $a_M := \text{máx}\{a_i : i = 0, \ldots t\}$, entonces*

$$|\tau - n/m| > \frac{1}{(a_M + 2)m^2}.$$

Bibliografía

[1] T. Andrescu and D. Andrica, *Quadratic diophantine equations*, Springer-Verlag, New York,(2015).

[2] A. Baker, *Linear forms in logarithms of algebraic numbers I, II, III*, Mathematika **13** (1966); 204-216, ibid. **14** (1967), 102-107; ibid. **14** (1967), 220-228.

[3] F. Beukers, *The zero-multiplicity of ternary recurrences*, Compositio Math. **77** (1991), 165-177.

[4] F. Beukers and R. Tijdeman, *The multiplicity of binary recurrences*, Compositio Math. **40** (1980), 251-267.

[5] J. Berstel, *Sur le calcul des termes d'une suite récurrecte linéare, exposé fait à l'I.R.I.A.* (Rocquencourt) en march 1974.

[6] J. W. S. Cassels *Local Fields*, Cambrige University Press, London, (1986).

[7] H. Cohen, *Number Theory Volume I: Tools and Diophantine Equations*, Springer-Verlag, New York, (2007).

[8] A. Dujell and A. Pethő, *A Generalization of a Theorem of Baker and Davenport*, Quart. J. Math. Oxford **49** (1998), 291-306.

[9] G. Everest, A. van der Porten, I. Shparlinski and T. Ward, *Recurrence Secuences*, American Mathematical Society, USA, (2003)

[10] F. Gouvêa, *p-adic numbers: An Introduction*, Springer-Verlac, Berlin Heidelberg, (1993).

[11] T. Hagedorn, *Zeros of a real linear recurrence of degree $n \geq 4$*, C. R. Math. Rep. Acad. Sci. **27**(2) (2005), 41-47.

[12] K. Kubota, *On a conjeture of M. Ward, I, II,* Acta Arith. **33** (1977), 11-28, 29-48.

[13] C. Lech, *A note on recurring series*, Ark. Mat, **2** (1953), 417-421.

[14] C. A. Gómez, F. Luca and J. L Orozco. *The zero-multiplicity of Berstel type sequences,* Bull. Math. Soc. Sci. Math. Roumanie (acepted).

[15] K. Mahler, *Eine arithmetische Eigenschaft der Taylor-Koeffizienten rationaler Funktionen*, Proc. Akad. Wet. Amsterdam **38** (1935), 50-60.

[16] E. Matveev, *An esplicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125-180; traducción en inglés en *Izv Math* **64** (2000), 1217-1269.

[17] A. Vander Poorten and H. Schlickewei, *Zeros of recurrence sequences*, Bull. Austral. Math. Soc, **44** (1991), 215-223.

[18] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, New York, 2nd Ed. (2005).

[19] H. Schlickewei, *Multiplicities of algebraic linear recurrences.* Acta Math., **170** (1993), 151-180.

[20] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge, (1986).

[21] T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen*, Proceedings of the 8th Congress of Scandinavian Mathematicians, Stockholm (1934).

[22] M. Smiley, *On the zeros of a cubic recurrence*, Amer. Math. Monthly, **63** (1956), 171-172.

[23] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, Springer-Verlag, New York, (1991).

[24] M. Ward, *Some diophantine problems connected with linear recurrences,* Report Institute Theory of Numbers (Univ. Colorado) (1959), 250-257.