Una familia de extensiones infinitas de $\mathbb{Q}$ con la propiedad de Bogomolov

por

Benjamín Castillo Córdova

Tesis presentada a la Facultad de Matemáticas
de la Pontificia Universidad Católica de Chile
para optar al grado académico de
Magíster en Matemática.

Supervisor	:	Ricardo Menares
Comisión	:	Natalia Garcia Fritz
		Riccardo Pengo

Marzo, 2024

Santiago, Chile

"There are two kinds of mathematicians.
The matematicians who tackle a difficult problem
and they find a simple solution
and then we can move on and build on that.
There is another type of mathematician
who works on very difficult problems,
and, after the solution is found,
the problems remains very difficult"
Atle Selberg[1]

[1]Esta frase fue mencionada por Enrico Bombieri en el volumen de verano de 2008 de "The Institute Letter", publicado por el Instituto de Estudios Avanzados en Princeton. Además, Bombieri agregó: "*It's clear that Selberg was in the first group. He always looked for simplicity, elegance, and depth.*". Se puede encontrar en https://www.ias.edu/sites/default/files/documents/publications/Summer%202008.pdf.

Agradecimientos

En primer lugar, agradezco al profesor Ricardo Menares por permitirme ser su estudiante, presentarme el tema y poder estudiar sobre la teoría algebraica de números. Siempre estuvo dispuesto a responder todas mis dudas e hizo que este proceso de desarrollar la tesis fuera muy ameno, además de todo lo que aprendí en mi formación como matemático.

Agradezco también a la profesora Natalia Garcia y el profesor Riccardo Pengo por haber leído mi tesis y por sus comentarios al respecto. Valoro profundamente las correcciones y sugerencias realizadas, lo cual permitió mejorar tanto el contenido como la exposición de este trabajo.

Agradezco a mis padres, ya que gracias a ellos nunca me ha faltado nada y he podido dedicarme a todo lo que he querido. En especial a mi madre.

Finalmente, agradezco a mis amigos de la universidad, por las risas y recuerdos que quedaron en estos 7 años de universidad.

Índice general

Introducción

Siguiendo [BZ01], decimos que un conjunto $\mathcal{A}$ de números algebraicos tiene la *propiedad de Bogomolov* (B) si existe un número real positivo T tal que el conjunto

$$\mathcal{A}(T) = \{\alpha \in \mathcal{A} \setminus \{0\} : h(\alpha) < T\}$$

consiste de todas las raíces de la unidad en $\mathcal{A}$, donde $h(\alpha)$ es la altura logarítmica absoluta de Weil. Más precisamente,

Definición. Sea $\alpha \in \overline{\mathbb{Q}}$ un número algebraico y K un cuerpo de números que contiene a α. La *altura absoluta de Weil* de α es

$$H(\alpha) = \prod_{v \in M_K} \max\{1, |\alpha|_v\}^{d_v/d}$$

La *altura logarítmica absoluta de Weil* es

$$h(\alpha) = \log(H(\alpha)) = \sum_{v \in M_K} \frac{d_v}{d} \log^+ |\alpha|_v$$

donde M_K es el conjunto de todos los lugares en K, $\log^+ |\alpha|_v = \log \max\{1, |\alpha|_v\}$, $d_v = [K_v : \mathbb{Q}_v]$ y $d = [K : \mathbb{Q}]$.

Observación. $h(\alpha)$ *no depende de la elección de* K*.*

Un teorema de Kronecker dice que $h(\alpha) = 0$ si y sólo si α es cero o una raíz de la unidad, así que los conjuntos con la propiedad (B) cumplen que el cero está aislado de los valores de $h(\alpha)$.

Todo cuerpo de números cumple la propiedad (B). También existen extensiones algebraicas infinitas de $\mathbb{Q}$ que cumplen (B). Daremos un breve resúmen de los resultados más generales en orden cronológico.

2000: En [AZ00], Francesco Amoroso y Umberto Zannier mostraron que la máxima extensión abeliana K^{ab} de un cuerpo de números K satisface (B). En particular, cada extensión abeliana de K satisface (B).

2001: En [BZ01], Enrico Bombieri y Umberto Zannier probaron que cada extensión de Galois infinita $L/\mathbb{Q}$ con grado local acotado en algún primo racional (ver Definición 2.3.1) tiene la propiedad (B).

2011: En [Hab13], Philipp Habegger introdujo una familia de extensiones Galois infinitas no abelianas de $\mathbb{Q}$ que satisfacen (B). Más concretamente, sea E una curva elíptica definida sobre $\mathbb{Q}$ y E_{tors} el grupo de puntos de torsion en E definido en alguna clausura algebraica de $\mathbb{Q}$. Habegger consideró el cuerpo $\mathbb{Q}(E_{\text{tors}})$ generado por el conjunto de coordenadas de los puntos en E_{tors} respecto a un modelo de Weierstrass de E con coeficientes racionales.

Si E tiene multiplicación compleja, $\mathbb{Q}(E_{\text{tors}})$ cae dentro de la familia de [AZ00] así que satisface (B).

Por lo tanto, el caso interesante es cuando E no tiene multiplicación compleja y en este contexto es donde Habegger demostró que $\mathbb{Q}(E_{\text{tors}})$ también satisface (B) y no está contenido en K^{ab} para ningún cuerpo de números K.

2011: En [ADZ14], Francesco Amoroso, Sinnou David y Umberto Zannier generalizaron [BZ01, Theorem 2] y [AZ00]. Si K es un cuerpo de números y L/K una extensión de Galois infinita con grupo de Galois G, ellos mostraron que si $E \subseteq L$ es el cuerpo fijo por $\mathrm{Z}(G)$ y E/K tiene grado local acotado en algún lugar no arquimedeano v en K acotado por d_0, entonces, L tiene la propiedad (B), con cota inferior uniforme en v, d_0 y $[K : \mathbb{Q}]$. Además, obtuvieron el siguiente corolario: si K es un cuerpo de números y L/K una extensión de Galois infinita con grupo de Galois G tal que $G/\mathrm{Z}(G)$ tiene exponente finito b, entonces L tiene la propiedad (B), de manera uniforme en b y $[K : \mathbb{Q}]$.

2015: En [Gal16], Aurélien Galateau encontro una familia de extensiones Galois infinitas de $\mathbb{Q}$ generadas por invariantes j de ciertas curvas elípticas con mulplicación compleja que satisface (B) y no pertenece a la familia establecida en [ADZ14]. En particular, si G es el grupo de Galois de uno de estos cuerpos, Galateau demostró que $G/\mathrm{Z}(G)$ no tiene exponente finito y encontró una cota inferior explícita para la altura de los elementos de estos cuerpos, que depende sólo de cierto primo racional ligado a su construcción.

En esta tesis exhibiremos una familia de extensiones algebraicas infinitas de $\mathbb{Q}$ que satisfacen (B) pero que no cae dentro de la familia establecida en [ADZ14], [Hab13] y [Gal16].

Más concretamente, fijemos p un número primo impar. Dado K un cuerpo cuadrático, sea H_K su cuerpo de clases de Hilbert, es decir, la máxima extensión abeliana no ramificada de K (ver por ejemplo [Cox14, Theorem 5.18]). Luego, consideremos la colección de cuerpos cuadráticos

$$S_p = \{K/\mathbb{Q} : p \text{ no escinde en } K\}.$$

Sea L_p el compuesto de H_K's donde K varía sobre S_p. Nuestros resultados son los siguientes.

Teorema A. *L_p satisface la propiedad (B).*

Teorema B. *Si E es un cuerpo de números tal que L_p/E es una extensión de Galois infinita, entonces*

$$Gal(L_p/E)/Z(Gal(L_p/E))$$

tiene exponente infinito.

Demostraremos que L_p tiene grado local acotado sobre p (ver Definición 2.3.1) y $L_p/\mathbb{Q}$ es una extensión normal, así que el Teorema A sigue de [BZ01, Theorem 2]. Más aún, haciendo uso de la descripción explícita de extensiones cuadráticas de cuerpos p-ádicos fuimos capaces de usar la efectividad de [BZ01, Theorem 2] respecto al límite inferior de las alturas, obteniendo el siguiente teorema.

Teorema C. *L_p satisface que*

$$\liminf_{\alpha \in L_p} h(\alpha) \geq \frac{\log p}{4(p^2+1)}.$$

Observación. A pesar de que el Teorema A es una consecuencia del Teorema C, la demostración del Teorema A es más simple y representa de mejor manera el porqué L_p tiene la propiedad (B).

Para demostrar el Teorema B, seguimos la misma idea de [Gal16, Proposition 3.2] con la diferencia que explotamos más la estructura de grupos dihedrales generalizados que poseen los grupos de Galois de los cuerpos de clases de Hilbert sobre $\mathbb{Q}$ cuando consideramos cuerpos cuadráticos imaginarios.

Nuestra construcción es similar y extiende la de [Gal16]. En su caso, en vez de tomar el conjunto S_p, consideran el siguiente conjunto ([Gal16, Lemma 3.1]):

$$R_p = \left\{ \mathbb{Q}(\sqrt{-q}) : q \text{ es primo, } q \equiv 3 \bmod 4 \text{ y } \left(\frac{-q}{p}\right) = -1 \right\},$$

para luego construir un cuerpo llamado $L_{\mathcal{P}_p}$ de la misma manera que se construye L_p.

En [Gal16, Proposition 3.3] se demuestra que $L_{\mathcal{P}_p}$ no pertenece a las extensiones establecidas en [Hab13]. Además, tenemos la inclusión $L_{\mathcal{P}_p} \subset L_p$, ya que $R_p \subset S_p$. Luego, el siguiente resultado es una consecuencia inmediata.

Teorema D. *Si E es una curva elíptica definida sobre un cuerpo de números K, entonces $L_p \not\subset K(E_{tor})$.*

Por completitud replicaremos la demostración aquí.

Por contradicción supongamos que $L_p \subset K(E_{\text{tor}})$.

Si E tiene multiplicación compleja, $K(E_{\text{tor}}) \subset K^{\text{ab}}$ con lo cual $\text{Gal}(L_p/L_p \cap K) \simeq \text{Gal}(L_pK/K)$ sería abeliano, lo que contradice el Teorema B.

Si E no tiene multiplicación compleja, sea q un primo que satisface las condiciones de R_p y es suficientemente grande de tal forma que q no ramifica en K, la curva elíptica E tiene buena reducción en todos los primos de K sobre q y es posible ocupar el teorema de imagen abierta de Serre ([Ser72]):

$$\text{Gal}(K(E[q])/K) \simeq \text{GL}_2(\mathbb{F}_q).$$

Si $K_q = \mathbb{Q}(\sqrt{-q})$, la extensión $H_{K_q}/\mathbb{Q}$ ramifica de buena manera en q y no ramifica en otros primos por lo que $H_{K_q} \subseteq K(E[q])$. Además, podemos escoger q tal que

$$\text{Gal}(H_{K_q}/\mathbb{Q}) \simeq C(\mathcal{O}_{K_q}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

no sea abeliano, para esto basta que $C(\mathcal{O}_{K_q})$ no tenga exponente 2 (ver Lema 3.1.1 y Lema 1.1.2).

Es posible incrustar este grupo de Galois como un subgrupo normal de $\mathrm{GL}_2(\mathbb{F}_q)$ que no está contenido en su centro. Al ser $\mathrm{PSL}_2(\mathbb{F}_q)$ un grupo simple, se tiene que $|\mathrm{Gal}(H_{K_q}/\mathbb{Q})| \geq q(q^2-1)$ y por ende

$$|C(\mathcal{O}_{K_q})| \geq \frac{q(q^2-1)}{2}.$$

Siguiendo [Lou92], por la fórmula analítica del número de clases tenemos que

$$|C(\mathcal{O}_{K_q})| = \frac{\omega(K_q)\sqrt{q}}{2\pi} L(1,\chi),$$

donde $\omega(K_q)$ es el número de raíces de la unidad en K_q y χ el caracter asociado a K_q. Sabemos que $\omega(K_q) \leq 6$ y $L(1,\chi) \leq \log(\sqrt{q})+1$, como se observa en [Lou92, p.214]. Luego,

$$|C(\mathcal{O}_{K_q})| \leq \frac{3}{\pi}\sqrt{q}(\log(\sqrt{q})+1)$$

llegando a una contradicción.

Capítulo 1

Preliminares

En este capítulo enunciaremos los resultados precisos que necesitaremos para mostrar que nuestra construcción no cae en los casos previamente establecidos. Las secciones 1.2 y 1.3 se inspiran principalmente de [Gal16, Lemma 3.1] y parte de la demostración de [Gal16, Proposition 3.2].

1.1 Grupos dihedrales generalizados

Dado N un grupo abeliano no trivial queremos entender como es el centro de su grupo dihedral generalizado.

Definición 1.1.1. El grupo dihedral generalizado de N es el producto semidirecto

$$N \rtimes \mathbb{Z}/2\mathbb{Z}$$

donde $\mathbb{Z}/2\mathbb{Z}$ actúa en N invirtiendo elementos, así que la operación de grupo viene dada por

$$(n_1, 0) \cdot (n_2, a) = (n_1 n_2, a)$$
$$(n_1, 1) \cdot (n_2, a) = (n_1 n_2^{-1}, 1 + a)$$

Lo denotamos por $\mathrm{Dih}(N)$.

El único resultado que necesitaremos en este tópico es el siguiente lema.

Lema 1.1.2. *Si N es un grupo abeliano no trivial entonces $Z(Dih(N))$ es un grupo de exponente 2.*

Demostración. Sea $n \in N$.

Si $(n, 0) \in \mathrm{Z}(\mathrm{Dih}(N))$, operando $(n, 0)$ con $(n, 1)$ vemos que

$$(n, 0) \cdot (n, 1) = (n^2, 1) = (e_N, 1) = (n, 1) \cdot (n, 0),$$

con lo cual $n^2 = e_N$ y $(n, 0)$ tiene orden 2.

Por otro lado, es claro que todo elemento en $\mathrm{Dih}(N)$ de la forma $(n, 1)$ tiene orden 2. □

1.2 Densidad analítica de algunos conjuntos de primos

Dado un número primo p, queremos ver que ciertos números módulo p abundan y para eso usaremos el concepto de densidad, aquí seguimos [IR90, Chapter 16, §1].

Definición 1.2.1 (Densidad de Dirichlet)**.** Un conjunto de enteros positivos $\mathcal{P}$ se dice que tiene densidad de Dirichlet si

$$\lim_{s\to 1^+} \frac{\sum_{p\in\mathcal{P}} p^{-s}}{\ln(s-1)^{-1}}$$

existe y en este caso denotamos el límite como $d(\mathcal{P})$ llamándolo densidad de Dirichlet de $\mathcal{P}$.

Lema 1.2.2. *Las siguientes son propiedades básicas provenientes de la definición.*

(a) Si $\mathcal{P}$ es finito entonces $d(\mathcal{P}) = 0$.

(b) Si $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ donde $\mathcal{P}_1$ y $\mathcal{P}_2$ son disjuntos y $d(\mathcal{P}_1)$, $d(\mathcal{P}_2)$ existen entonces

$$d(\mathcal{P}) = d(\mathcal{P}_1) + d(\mathcal{P}_2).$$

Demostración. Ver [IR90, Proposition 16.1.4]. □

Ahora enunciamos el famoso teorema de Dirichlet sobre primos en progresión aritmética en su versión fuerte.

Teorema 1.2.3 (L. Dirichlet)**.** *Sean $a, m \in \mathbb{Z}$ con $(a, m) = 1$. Sea $\mathcal{P}(a; m)$ el conjunto de primos q tal que $q \equiv a \bmod m$. Entonces*

$$d(\mathcal{P}(a; m)) = 1/\phi(m).$$

De esto se desprende el siguiente corolario, que nos será útil más adelante.

Corolario 1.2.4. *Sea p un número primo impar. Si $\mathcal{A}$ es el conjunto de primos que son residuos cuadráticos módulo p y que además son congruentes a 3 módulo 4, entonces $d(\mathcal{A}) = 1/4$.*

Demostración. Si r es un residuo cuadrático módulo p y $r \equiv 3 \bmod 4$, por el teorema chino del resto existe una única clase s en $\mathbb{Z}/4p\mathbb{Z}$ tal que $r \equiv s \bmod 4p$. Por el teorema de Dirichlet $d(\mathcal{P}(s; 4p)) = 1/2(p-1)$. Además, es sabido que la cantidad de residuos cuadráticos módulo p es $(p-1)/2$, así que por la aditividad de la densidad $d(\mathcal{A}) = 1/4$. □

Observación. Lo mismo aplica si cambiamos a residuos no cuadráticos o primos congruentes a 1 módulo 4.

1.3 Exponente del grupo de clases

Dado K un cuerpo de números cuadrático imaginario, el propósito de esta sección es ver que el exponente del grupo de clases $C(\mathcal{O}_K)$ crece a medida que $|d_K|$ lo hace en una colección específica de cuerpos cuadráticos.

Empecemos enunciando un teorema de Francesco Pappalardi [Pap95, Theorem 1.2].

Teorema 1.3.1. *Si d es un entero positivo y $m(d)$ es el exponente del grupo de clases de $\mathbb{Q}(\sqrt{-d})$, para todos los $d < x$ tales que $-d$ es un discriminante se tiene que*

$$m(d) > \frac{\log d/4}{\log\log d},$$

salvo a lo más $O\left(x^{1-A(\log\log x)^{-1}}\right)$ excepciones.

Más precisamente, para cada $A \leq \frac{1}{2}\log 2$ se tiene que

$$\#\left\{d \leq x : m(d) \leq \frac{\log d/4}{\log\log d}\right\} \ll_A x^{1-A(\log\log x)^{-1}}.$$

Observación. En particular, el conjunto de excepciones tiene densidad natural cero y por ende también tiene densidad de Dirichlet cero.

Nos interesa que el exponente vaya creciendo en un grupo específico de cuerpos cuadráticos, pero antes de eso veamos un cálculo.

Lema 1.3.2. *Si A es un número real positivo, entonces*

$$\lim_{x\to+\infty} \frac{x^{A(\log\log x)^{-1}}}{\log x} = +\infty.$$

Demostración. Tomando el logaritmo de la expresión basta calcular

$$\lim_{x\to+\infty} \frac{A\log x}{\log\log x} - \log\log x.$$

Si $t = \log\log x$, obtenemos $\lim_{t\to+\infty} \frac{Ae^t - t^2}{t}$ el cual claramente diverge por la regla de l'Hôpital. □

Proposición 1.3.3. *Sea p un número primo impar. Si $\mathcal{C}$ es la colección de cuerpos cuadráticos $\mathbb{Q}(\sqrt{-q})$ donde q es un primo congruente a 3 módulo 4 y que es residuo cuadrático módulo p, entonces, para todo $n \in \mathbb{N}$ existe $\mathbb{Q}(\sqrt{-q_n}) \in \mathcal{C}$ tal que*

$$m(q_n) > n.$$

Demostración. La condición $q \equiv 3 \bmod 4$ ciertamente hace que $-q$ sea un discriminante. Por el teorema de los números primos $\pi(x) \sim \frac{x}{\log x}$, luego, gracias al Teorema 1.3.1 y Lema 1.3.2 podemos encontrar un primo q suficientemente grande tal que $m(q) > n$. Como esta condición depende del tamaño de q, podemos tomar un q_n tal que $\mathbb{Q}(\sqrt{-q_n}) \in \mathcal{C}$ y $m(q_n) > n$, ya que si esto no fuera posible, quiere decir que los números mayores que q del conjunto $\mathcal{A}$ del Corolario 1.2.4 están todos contenidos en el conjunto de excepciones del Teorema 1.3.1, con lo cual $\mathcal{A}$ tendría densidad de Dirichlet cero, pero esto no es cierto. □

Observación. Lo mismo aplica si consideramos q que no sea residuo cuadrático módulo p.

Capítulo 2

Grados locales

Salvo que se especifique lo contrario, K es un cuerpo de números cuadrático y d_K su discriminante. El objetivo de este capítulo es calcular el grado de ciertas extensiones de $\mathbb{Q}_p$ en términos de el comportamiento de p en K.

2.1 Extensiones cuadráticas

En este contexto, el anillo de enteros $\mathcal{O}_K$ es

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$$

y si p es un primo racional, su comportamiento en K está dado por

$$p\mathcal{O}_K = \begin{cases} \mathfrak{p}^2 & \text{si } p \mid d_K \\ \mathfrak{p} \cdot \mathfrak{p}' & \text{si } \left(\frac{d_K}{p}\right) = 1 \\ p\mathcal{O}_K & \text{se mantiene primo si } \left(\frac{d_K}{p}\right) = -1 \end{cases}$$

donde $\mathfrak{p}$ es un ideal primo, $\mathfrak{p}'$ es el conjugado de $\mathfrak{p}$ bajo $\mathrm{Gal}(K/\mathbb{Q})$ y $\left(\frac{d_K}{p}\right)$ es el símbolo de Kronecker (ver por ejemplo [Cox14, Proposition 5.16]).

Si v_p es la valuación p-ádica y v es el lugar inducido por la valuación, sabemos que

$$2 = \sum_{w|v} [K_w : \mathbb{Q}_p]$$

donde w son los lugares en K que extienden a v, que a su vez provienen de las valuaciones de los primos $\mathfrak{p} \subseteq \mathcal{O}_K$ sobre p.

Fijemos $\mathfrak{p}|p$ y sea w el lugar en K inducido por $\mathfrak{p}$. En vista de la igualdad anterior obtenemos el siguiente lema, el cual nos sera útil en la siguiente sección.

Lema 2.1.1. *Si w es un lugar en K sobre p*

$$[K_w : \mathbb{Q}_p] = \begin{cases} 1 & \text{si } p \text{ se escinde en } K \\ 2 & \text{si } p \text{ ramifica o es inerte en } K \end{cases}$$

2.2 Cuerpo de clases de Hilbert

Sea H/K el cuerpo de clases de Hilbert de K, es decir, la máxima extensión Abeliana no ramificada de K (ver por ejemplo [Cox14, Theorem 5.18]). Por el teorema de reciprocidad de Artin para el cuerpo de clases de Hilbert

$$C(\mathcal{O}_K) \simeq \mathrm{Gal}(H/K) \tag{2.1}$$

y el isomorfismo viene dado por $\mathfrak{q}P_K \to \sigma_\mathfrak{q}$ donde $\mathfrak{q}$ es un ideal primo de $\mathcal{O}_K$, P_K es el subgrupo de ideales fraccionarios principales y $\sigma_\mathfrak{q}$ es el elemento de Frobenius de $\mathfrak{q}$.

El resultado que nos interesa es el siguiente.

Proposición 2.2.1. *Si l es un lugar en H sobre un primo racional p, entonces*

$$[H_l : \mathbb{Q}_p] \leq 4$$

cuando p ramifica o es inerte en K.

Demostración. Sea w el lugar en K bajo l y sean $\mathfrak{P} \subseteq \mathcal{O}_H$, $\mathfrak{p} \subseteq \mathcal{O}_K$ los primos correspondientes a cada lugar.

Por [Nar13, Theorem 5.11] sabemos que $[H_l : K_w] = e_{H/K}(\mathfrak{P}) f_{H/K}(\mathfrak{P})$, así que basta calcular estos invariantes.

H/K es una extensión abeliana no ramificada, por lo que $e_{H/K}(\mathfrak{P}) = 1$ y $f_{H/K}(\mathfrak{P}) = \mathrm{ord}(\sigma_\mathfrak{p}) = \mathrm{ord}(\mathfrak{p}P_K)$ donde la última igualdad viene del isomorfismo (2.1).

Si p es inerte en K entonces $\mathfrak{p} = p\mathcal{O}_K$. Por otro lado, si p ramifica en K entonces $\mathfrak{p}^2 = p\mathcal{O}_K$. Luego,

$$[H_l : K_w] = \mathrm{ord}(\mathfrak{p}P_K) \leq \begin{cases} 2 & \text{si } p \text{ ramifica en } K \\ 1 & \text{si } p \text{ es inerte en } K \end{cases}$$

por lo que el resultado sigue del Lema 2.1.1 y la ley de las torres.

□

2.3 Grado local del compuesto

Por último, veamos que pasa con el grado local cuando tomamos el compuesto de ciertos cuerpos de números. Empecemos con un concepto bastante utilizado en el contexto de cuerpos que satisfacen la propiedad (B).

Definición 2.3.1. Sea K un cuerpo de números, v un lugar no arquimedeano en K y L/K una extensión algebraica. Decimos que L/K tiene *grado local acotado* en v si existe un entero n tal que para cada extensión w de v en L se tiene que $[L_w : K_v] \leq n$.

Como mencionamos en la introducción, Enrico Bombieri y Umberto Zannier demostraron que toda extensión de Galois $L/\mathbb{Q}$ con grado local acotado en algún primo racional satisface la propiedad (B) (ver [BZ01, Theorem 2]). La construcción que realizaremos cae dentro de esta familia, para mostrar aquello necesitaremos la siguiente proposición.

Proposición 2.3.2. *Sea K un cuerpo de números y fijemos un lugar no arquimedeano v en K. Sea $\mathcal{F}$ una familia infinita de extensiones finitas de K. Supongamos que existe un entero d tal que para todo H en $\mathcal{F}$ y para todo lugar $l|v$ en H se tiene que $[H_l : K_v] \leq d$. Entonces, si L es el compuesto de las extensiones en $\mathcal{F}$, L tiene grado local acotado en v.*

Demostración. Básicamente replicamos la demostración de [BZ01, Proposition 1].

Por [Nar13, Corollary 2, p.226] K_v tiene una cantidad finita de extensiones de grado m, lo cual aplica para todo $m \in \mathbb{N}$. Luego, la colección $\mathcal{C}$ de extensiones de K_v de grado a lo más d es finita. En particular, si M es el compuesto de los cuerpos en $\mathcal{C}$ la extensión M/K_v es finita.

Por hipótesis, para cada $H \in \mathcal{F}$ su completación en cualquier lugar $l|v$ está contenido en $\mathcal{C}$, entonces, si w es cualquier lugar en L sobre v, podemos incrustar $L_w \hookrightarrow M$ ya que L es el compuesto de las extensiones en $\mathcal{F}$. Así, $[L_w : K_v] \leq [M : K_v]$ donde el último sólo depende de v y d.

Por lo tanto, L tiene grado local acotado en v. □

Observación. En [BZ01, Proposition 1] se muestra que para cualquier cuerpo números K, el cuerpo $K^{(d)}$ (compuesto de extensiones de K de grado a lo más d) tiene grado local acotado sobre cualquier lugar en K. Nuestro caso es distinto, el grado sobre $\mathbb{Q}$ de los cuerpos de números que consideraremos va ir en incremento, por lo que su compuesto no estará contenido en algún $K^{(d)}$.

Otro resultado interesante se debe a Sara Checcoli. En [Che13, Theorem 1] ella demuestra que si $K/\mathbb{Q}$ es una extensión Galois infinita, K tiene grado local acotado en cada primo (de manera uniforme) si y sólo si $Gal(K/\mathbb{Q})$ tiene exponente finito. De nuevo, en nuestro caso esta propiedad no se satisface.

Capítulo 3

Propiedad de Bogomolov

En este capítulo desarrollamos el resultado principal de esta tesis, el cual es una familia de cuerpos que satisface la propiedad (B) pero no pertenece a la familia establecida en [ADZ14].

3.1 Resultados principales

Fijemos p un número primo impar. Dado K un cuerpo cuadrático, sea H_K su cuerpo de clases de Hilbert y consideremos la colección de cuerpos cuadráticos

$$S_p = \{K/\mathbb{Q} : p \text{ no escinde en } K\}.$$

Sea L_p el compuesto de H_K's donde K varía sobre S_p. La extensión $L_p/\mathbb{Q}$ es Galois como muestra el siguiente lema.

Lema 3.1.1. *Si $K/\mathbb{Q}$ es una extensión Galois, entonces la extensión $H_K/\mathbb{Q}$ es Galois.*

Más aún, si K es un cuerpo cuadrático imaginario, el grupo de Galois de $H_K/\mathbb{Q}$ es un grupo dihedral generalizado

$$Gal(H_K/\mathbb{Q}) \simeq Gal(H_K/K) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

En particular,

$$Gal(H_K/\mathbb{Q}) \simeq C(\mathcal{O}_K) \rtimes \mathbb{Z}/2\mathbb{Z}.$$

Demostración. Sea L/H_K una extensión de cuerpos y $\sigma : H_K \to L$ un morfismo de $\mathbb{Q}$-álgebras.

Notemos que $\sigma(H_K)$ es una extensión abeliana no ramificada de $\sigma(K) = K$, así que $\sigma(H_K) \subseteq H_K$ y por lo tanto $\sigma(H_K) = H_K$. Luego, la extensión $H_K/\mathbb{Q}$ es Galois.

Para probar la segunda afirmación, sea τ la conjugación compleja. Notemos que tenemos la secuencia exacta

$$0 \to \mathrm{Gal}(H_K/K) \to \mathrm{Gal}(H_K/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) \to 0$$

la cual escinde pues $\tau \in \mathrm{Gal}(H_K/\mathbb{Q})$. Entonces,

$$\mathrm{Gal}(H_K/\mathbb{Q}) \simeq \mathrm{Gal}(H_K/K) \rtimes \mathrm{Gal}(K/\mathbb{Q})$$

donde τ actúa en $\mathrm{Gal}(H_K/K)$ conjugando elementos.

Sin embargo, si $\mathfrak{p}$ es un ideal primo de $\mathcal{O}_K$ y $\sigma_{\mathfrak{p}}$ el elemento de Frobenius, es sabido que $\sigma_{\tau(\mathfrak{p})} = \tau \circ \sigma_{\mathfrak{p}} \circ \tau^{-1}$, así que en vista del isomorfismo (2.1), $\mathrm{Gal}(K/\mathbb{Q})$ actúa en $C(\mathcal{O}_K)$ mandando a un primo a su conjugado, que es su inverso pues estamos en una extensión cuadrática. Por lo tanto,

$$\mathrm{Gal}(H_K/\mathbb{Q}) \simeq C(\mathcal{O}_K) \rtimes \mathbb{Z}/2\mathbb{Z}$$

donde $\mathbb{Z}/2\mathbb{Z}$ actua en $C(\mathcal{O}_K)$ inviertiendo elementos. □

Teorema A. *L_p satisface la propiedad (B).*

Demostración. Por la Proposición 2.2.1, L_p es el compuesto de cuerpos de números tal que para cada lugar en ellos sobre p, el grado de su completación sobre $\mathbb{Q}_p$ está acotado por 4. Luego, L_p tiene grado local acotado en p por la Proposición 2.3.2. Como $L_p/\mathbb{Q}$ es una extensión normal, L_p tiene la propiedad (B) por [BZ01, Theorem 2]. □

De hecho, podemos ir un poco más alla y establecer una cota inferior para $\liminf_{\alpha \in L_p} h(\alpha)$. Esto será expuesto en la siguiente sección.

Ahora que L_p satisface (B), veamos que no existe un cuerpo de números E tal que el cociente de $\mathrm{Gal}(L_p/E)$ sobre su centro tiene exponente finito.

Teorema B. *Si E es un cuerpo de números tal que L_p/E es una extensión de Galois infinita, entonces*

$$Gal(L_p/E)/Z(Gal(L_p/E))$$

tiene exponente infinito.

Antes de comenzar con la demostración, centraremos nuestra atención en una colección particular de cuerpos cuadráticos, que son los utilizados en [Gal16].

Consideremos la colección

$$R_p = \left\{ \mathbb{Q}(\sqrt{-q}) : q \text{ es primo, } q \equiv 3 \bmod 4 \text{ y } \left(\frac{-q}{p}\right) = -1 \right\}.$$

Con estas condiciones $-q$ es un discriminante y p es inerte en $\mathbb{Q}(\sqrt{-q})$, por lo que $R_p \subset S_p$.

La ventaja de trabajar con los cuerpos de clases de Hilbert de estos cuerpos cuadráticos es que su intersección a pares es trivial.

Lema 3.1.2. *Si K y K' son cuerpos cuadráticos distintos contenidos en R_p, entonces $H_K \cap H_{K'} = \mathbb{Q}$.*

Demostración. Sea q un número primo.

Notemos que $H_{\mathbb{Q}(\sqrt{-q})}/\mathbb{Q}$ está ramificada sólo en q, ya que $\mathbb{Q}(\sqrt{-q})/\mathbb{Q}$ ramifica sólo en q y $H_{\mathbb{Q}(\sqrt{-q})}/\mathbb{Q}(\sqrt{-q})$ es no ramificada.

Si q y s son primos distintos, la intersección de $H_{\mathbb{Q}(\sqrt{-q})}$ y $H_{\mathbb{Q}(\sqrt{-s})}$ es trivial, pues en caso contrario tendría ramificación (conocido teorema de Minkowski, ver por ejemplo [Neu13, Chapter III, (2.17)]) la cual se extendería sobre estos dos cuerpos. □

Demostración del Teorema B. La demostración será por contradicción, asumamos que este exponente es finito y llamémoslo I.

Al existir una cantidad finita de cuerpos intermedios $E/M/\mathbb{Q}$ sólo puede haber una cantidad finita de $K \in R_p$ tal que $H_K \cap E \neq \mathbb{Q}$, ya que por el Lema 3.1.2 estos cuerpos no pueden repetirse cuando variamos K. Entonces, por la Proposición 1.3.3 podemos fijar un $K \in R_p$ tal que $C(\mathcal{O}_K)$ tiene exponente mayor que $2I$ y $H_K \cap E = \mathbb{Q}$. Con esto,

$$\mathrm{Gal}(H_K E/E) \simeq \mathrm{Gal}(H_K/\mathbb{Q})$$

y por el Lema 3.1.1

$$\mathrm{Gal}(H_K E/E) \simeq C(\mathcal{O}_K) \rtimes \mathbb{Z}/2\mathbb{Z}. \tag{3.1}$$

Tenemos las extensiones $L_p/H_K E/E$ y además la extensión $H_K E/E$ es Galois, por lo que $\mathrm{Gal}(H_K E/E)$ es isomorfo a un cociente de $\mathrm{Gal}(L_p/E)$ que llamaremos C. Notemos que la proyección $\pi : \mathrm{Gal}(L_p/E) \twoheadrightarrow C$ induce un homomorfismo sobreyectivo

$$\mathrm{Gal}(L_p/E)/\mathrm{Z}(Gal(L_p/E)) \twoheadrightarrow C/\mathrm{Z}(C),$$

con lo cual $\mathrm{Gal}(H_K E/E)/\mathrm{Z}(\mathrm{Gal}(H_K E/E))$ tiene exponente menor o igual que I. Luego, el isomorfismo (3.1) y Lema 1.1.2 nos dice que $C(\mathcal{O}_K)$ tiene exponente menor o igual que $2I$, lo cual es una contradicción.

Por lo tanto, I no puede ser finito. □

3.2 Calculando una cota inferior para el límite inferior de las alturas

En esta última sección, realizaremos un análisis más explícito de la Proposición 2.2.1 calculando cuales son los cuerpos H_l, lo que nos permitira refinar el resultado del Teorema A.

Teorema C. *L_p satisface que*

$$\liminf_{\alpha \in L_p} h(\alpha) \geq \frac{\log p}{4(p^2+1)}.$$

Manteniendo la notación de la sección anterior, si p es un primo impar sea $K \in S_p$, $\mathfrak{p} \subseteq \mathcal{O}_K$ el primo sobre p, $\mathfrak{P} \subseteq \mathcal{O}_{H_K}$ cualquier primo sobre $\mathfrak{p}$ y $K_\mathfrak{p}$, $H_\mathfrak{P}$ los cuerpos completos de K y H_K respecto a estos primos.

Proposición 3.2.1. *Para $K_\mathfrak{p}$ tenemos las siguientes posibilidades:*

- *Si p es inerte en K: $K_\mathfrak{p}$ es la extensión cuadrática no ramificada de $\mathbb{Q}_p$.*
- *Si p ramifica en K: $K_\mathfrak{p}$ es una extensión cuadrática completamente ramificada de $\mathbb{Q}_p$.*

Demostración. Ver [Nar13, Theorem 5.11]. □

Por otro lado, siguiendo la demostración de la Proposición 2.2.1 obtenemos lo siguiente:

Proposición 3.2.2. *Para $H_\mathfrak{P}$ tenemos las siguientes posibilidades:*

- *Si p es inerte en K: $H_\mathfrak{P}$ es la extensión cuadrática no ramificada de $\mathbb{Q}_p$.*
- *Si p ramifica en K y $\mathfrak{p}$ es principal: $H_\mathfrak{P}$ es una extensión cuadrática completamente ramificada de $\mathbb{Q}_p$.*
- *Si p ramifica en K y $\mathfrak{p}$ no es principal: $H_\mathfrak{P}$ es una extensión que ramifica de buena manera de $\mathbb{Q}_p$ de grado 4, es decir, $e(H_\mathfrak{P}/\mathbb{Q}_p) = f(H_\mathfrak{P}/\mathbb{Q}_p) = 2$.*

Demostración. Ver demostración de la Proposición 2.2.1. □

Ahora somos capaces de específicar quienes son los cuerpos $H_\mathfrak{P}$.

Proposición 3.2.3. *Sea p un primo impar y $K \in S_p$. Los cuerpos p-ádicos que pueden aparecer al completar H_K respecto a un lugar sobre p son $\mathbb{Q}_p(\sqrt{\zeta})$, $\mathbb{Q}_p(\sqrt{\zeta\pi})$, $\mathbb{Q}_p(\sqrt{\pi})$ y $\mathbb{Q}_p(\sqrt{\pi}, \sqrt{\zeta})$, donde π es un primo en $\mathbb{Z}_p$ y ζ es una raíz primitiva de la unidad de orden $p-1$.*

En particular, el compuesto de todos ellos es $\mathbb{Q}_p(\sqrt{\pi}, \sqrt{\zeta})$.

Demostración. La herramienta clave de la demostración es [Nar13, Proposition 5.31].

El primer y segundo punto de la Proposición 3.2.2 más [Nar13, Proposition 5.31] recaen en las opciones $\mathbb{Q}_p(\sqrt{\zeta})$, $\mathbb{Q}_p(\sqrt{\zeta\pi})$, $\mathbb{Q}_p(\sqrt{\pi})$, donde π es un primo fijo en $\mathbb{Z}_p$ y ζ es una raíz primitiva de la unidad de orden $p-1$

Para el tercer punto de la Proposición 3.2.2, notemos que $H_\mathfrak{P}$ es la extensión cuadrática no ramificada de $K_\mathfrak{p}$ (ver Proposición 2.2.1), así que por [Nar13, Proposition 5.31]

$$H_\mathfrak{P} = K_\mathfrak{p}(\sqrt{\zeta}),$$

donde ζ es la misma de antes pues estamos en el caso en que p ramifica en K. Juntando la Proposición 3.2.1 con [Nar13, Proposition 5.31] tenemos que $K_\mathfrak{p} = \mathbb{Q}_p(\sqrt{\pi})$ ó $K_\mathfrak{p} = \mathbb{Q}_p(\sqrt{\zeta\pi})$. En cualquier caso,

$$H_\mathfrak{P} = \mathbb{Q}_p(\sqrt{\pi}, \sqrt{\zeta})$$

que es la extensión bi-cuadrática de $\mathbb{Q}_p$ por [Nar13, Proposition 5.32]. □

Demostración del Teorema C. Sea $M = \mathbb{Q}_p(\sqrt{\pi}, \sqrt{\zeta})$ la extensión bi-cuadrática de $\mathbb{Q}_p$. En particular, $e(M/\mathbb{Q}_p) = f(M/\mathbb{Q}_p) = 2$ (ver [Nar13, Proposition 5.32]).

L_p es el compuesto de cuerpos de números tal que para cada lugar en ellos sobre p, los cuerpos p-ádicos que aparecen al completar son los listados en la Proposición 3.2.3. Luego, si $v|p$ es cualquier lugar en L_p y $(L_p)_v$ el cuerpo completo respecto a v, podemos incrustar $(L_p)_v \hookrightarrow M$ ya que M es el compuesto de los cuerpos de la lista.

Con esto, $p \in S(L_p)$ donde $S(L_p)$ se define como en [BZ01, Theorem 2]. Como $L_p/\mathbb{Q}$ es una extensión normal (ver Lema 3.1.1) podemos usar la cota inferior de [BZ01, Theorem 2], la cual es

$$\liminf_{\alpha \in L_p} h(\alpha) \geq \frac{1}{2} \sum_{q \in S(L_p)} \frac{\log q}{e_q(q^{f_q} + 1)} \geq \frac{\log p}{4(p^2 + 1)}.$$

□

Bibliografía

[ADZ14] Francesco Amoroso, Sinnou David, and Umberto Zannier. On fields with property (B). *Proceedings of the American Mathematical Society*, 142(6):1893–1910, 2014.

[AZ00] Francesco Amoroso and Umberto Zannier. A relative dobrowolski lower bound over abelian extensions. *Annali della Scuola Normale Superiore di Pisa-Classe di Scienze*, 29(3):711–727, 2000.

[BZ01] Enrico Bombieri and Umberto Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Matematica e Applicazioni*, 12(1):5–14, 2001.

[Che13] Sara Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. *Transactions of the American Mathematical Society*, 365(4):2223–2240, 2013.

[Cox14] D.A. Cox. *Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2014.

[Gal16] Aurélien Galateau. Small height in fields generated by singular moduli. *Proceedings of the American Mathematical Society*, 144(7):2771–2786, 2016.

[Hab13] P. Habegger. Small height and infinite nonabelian extensions. *Duke Mathematical Journal*, 162(11):2027 – 2076, 2013.

[IR90] Kenneth Ireland and Michael Ira Rosen. *A classical introduction to modern number theory*, volume 84. Springer Science & Business Media, 1990.

[Lou92] Stéphane Louboutin. L-functions and class numbers of imaginary quadratic fields and of quadratic extensions of an imaginary quadratic field. *mathematics of computation*, 59(199):213–230, 1992.

[Nar13] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2013.

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

[Pap95] Francesco Pappalardi. On the exponent of the ideal class group of $\mathbb{Q}(\sqrt{-d})$. *Proceedings of the American Mathematical Society*, 123(3):663–671, 1995.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math*, 15:259–331, 1972.