UNIVERSIDAD
DE CHILE

Propiedades de aproximación en cohomología galoisiana de grupos finitos

Tesis entregada a la

Universidad de Chile

en cumplimiento parcial de los requisitos

para optar al grado de

Magíster en Ciencias Matemáticas

Facultad de Ciencias

por

Felipe Camilo Rivera Mesas

Marzo, 2021

Director de tesis: **Dr. Giancarlo Lucchini Arteche**

FACULTAD DE CIENCIAS

UNIVERSIDAD DE CHILE

INFORME DE APROBACIÓN

TESIS MAGÍSTER

Se informa a la Escuela de Postgrado de la Facultad de Ciencias que la Tesis de Magíster presentada por el candidato

Felipe Camilo Rivera Mesas

Ha sido aprobada por la Comisión de Evaluación de la Tesis como requisito para optar al grado de Magíster en Ciencias Matemáticas, en el examen de Defensa de Tesis rendido el día 5 de Marzo de 2021.

Director de Tesis

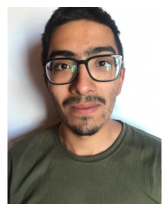
Dr. Giancarlo Lucchini Arteche

Comisión de Evaluación de la Tesis

Dr. Luis Arenas Carmona

Dr. Eduardo Friedman Rafael Eduardo Friedman

Biografía



Crecí en el campo de un pueblo llamado Crucero, ubicado en la comuna de Purranque en la Región de Los Lagos. Hice mis estudios básicos y medios en el Colegio Preciosa Sangre de Purranque. Cuando empezaba mi cuarto medio, supe de la licenciatura en matemáticas y me decidí a estudiar esta carrera. Así, en 2015, entré a estudiar Licenciatura en Matemáticas en la Facultad de Ciencias de la Universidad de Chile. En 2019, después de terminar mi licenciatura, ingresé al programa de Magíster en Ciencias Matemáticas, programa que en el estoy actualmente y para el cual escribo esta tesis.

Agradecimientos

Dedico mi primer y especial agradecimiento a mi mamá y mi papá por apoyarme en mi decisión de estudiar matemáticas. El agradecimiento y admiración que siento por ustedes es inmenso y no creo poder expresar lo que siento. Igualmente, me gustaría agradecer enormente a mis tiazas Mirta, Nuni, Valeska, Carmen y Malela por el cariño y apoyo que siempre que han dado y que me ha hecho sentir tan bien y tranquilo. A les jovenes Babi, Pancho y Rocío, ya tú sabe.

Me gustaría agradecer y reconocer también a mis profesores del colegio. En especial, me gustaría recordar, primeramente, al profesor Luis Oyarzún quien fue el primero en mostrarme una matemática más allá de la matemática del Mineduc y a quien posiblemente le debo mi decisión de estudiar matemáticas. Agradezco también al profesor Eduardo Perez quien alimentó mi interés por las matemáticas y de quien aprecio mucho el apoyo que me brindó en mi sueño de querer ser matemático.

En este punto, me gustaría dar gracias a algunas personas que han influido mucho en mi formación matemática en la universidad. Primero, a mi amigo Sebastián Rivera, quien compartió amablemente conmigo su conocimiento en mis primeros años de licenciatura, además de mostrarme las matemáticas más allá del aula y con quien disfruté largas horas de estudio. Segundo, al profesor Alvaro Castañeda, a quien le debo mi primer paso de abstracción y rigurosidad en mi formación matemática. Finalmente, quiero agradecer a mi tutor Giancarlo Lucchini, a quien reconozco como un gran maestro y de quien he aprendido mucho en matemáticas.

Son muchas las personas a las que me gustaría hacer explícito mis agradecimientos en este texto pero creo que mis palabras serían muy fomes. De todas formas, me gustaría agradecer a todas las personas que alguna vez me dieron comida, alojo, que me enseñaron algo o que me hicieron reír.

Índice general

Resumen

Dado un cuerpo de números k y un k-grupo finito G, el problema de aproximación en G consiste en determinar si la flecha de restricción $H^1(k,G) \to \prod_{v\in\Sigma} H^1(k_v,G)$ es epiyectiva para todo conjunto finito de lugares $\Sigma \subseteq \Omega_k$. Lucchini Arteche ha probado, asumiendo cierta conjetura de Colliot-Thélène, que siempre existe un conjunto finito y explícito $\mathrm{Bad}_G \subseteq \Omega_k$ tal que la flecha de restricción es epiyectiva para todo $\Sigma \subseteq \Omega_k$ disjunto a Bad_G. En esta tesis probamos que dicho resultado es óptimo, en el sentido que Bad_G es minimal. Para esto probamos que existen k-grupos abelianos finitos A donde la flecha $H^1(k,A) \to \prod_{v\in\Sigma_0} H^1(k_v,A)$ no es epiyectiva en un subconjunto $\Sigma_0 \subseteq \mathrm{Bad}_A$ con propiedades particulares, a saber Σ_0 está compuesto por lugares que no dividen al orden de A y que ramifican en la extensión minimal que escinde a A.

Abstract

Given a number field k and a finite k-group G, the Approximation Problem of G asks whether the restriction map $H^1(k, G) \to \prod_{v \in \Sigma} H^1(k_v, G)$ is surjective for every finite set of places $\Sigma \subseteq \Omega_k$. Lucchini Arteche has proved, assuming certain Colliot-Thélène's conjecture, that there exists an explicit finite set $\mathrm{Bad}_G \subseteq \Omega_k$ such that the restriction map is surjective for every finite set $\Sigma \subseteq \Omega_k$ disjoint from Bad_G. In this thesis, we proved that this result is "sharp", in the sense which Bad_G is minimal. For this, we proved that there exists finite abelian k-groups A where the map $H^1(k, A) \to \prod_{v \in \Sigma_0} H^1(k_v, A)$ is not surjective in a subset $\Sigma_0 \subseteq \mathrm{Bad}_A$ with certain properties, namely Σ_0 is composed of places which do not divide the order of A and ramify at the minimal extension splitting A.

Resumen ejecutivo

Los resultados principales de esta tesis son los Teoremas 3.1 y 3.5 del Capítulo 3. En el Capítulo 2 se encuentran ordenados los resultados necesarios para lograr este objetivo. En la sección 2.1 se presentan resultados clásicos en la teoría algebraica de números que están en la base de nuestro trabajo. En la sección 2.2 se presenta un estudio sobre la propiedad de aproximación en k-grupos abelianos. La sección 2.3 tiene por objetivo probar el Lema 2.21 que nos permitirá demostrar los teoremas antes mencionados.

Adicionalmente, en la sección 3.3 se responde a preguntas surgidas a propósito de las construcciones dadas en el Capítulo 3.

§1. Introducción

1.1. Propiedad de aproximación y el problema de Galois inverso

Sea k un cuerpo de números y G un k-grupo finito i.e. un grupo finito con una acción continua del grupo profinito $\mathrm{Gal}(k) := \mathrm{Gal}(\overline{k}/k)$ compatible con la estructura de grupo de G. Un k-grupo finito G tiene aproximación en un conjunto finito Σ de lugares de k si el morfismo de restricción

$$H^1(k, G) \to \prod_{v \in \Sigma} H^1(k_v, G), \tag{1.1}$$

es epiyectivo (ver Definición 2.4). Bajo esta idea, se dice que un k-grupo finito tiene propiedad de aproximación si este k-grupo finito tiene aproximación en cualquier conjunto finito de lugares de k. La propiedad anterior es muy fuerte y no es satisfecha incluso por grupos abelianos. Una propiedad más débil que la precedente es la siguiente: un k-grupo finito tiene aproximación fuera de un conjunto de lugares T si éste tiene aproximación en cualquier conjunto finito de lugares disjunto a T. Esta última noción tiene un vínculo estrecho con el problema de Galois inverso sobre k, el que nos dice que si G es un grupo finito visto como un k-grupo constante (i.e. la acción de $\mathrm{Gal}(k)$ en G es trivial) entonces G es un grupo de Galois sobre k siempre que G tenga aproximación fuera de algún conjunto finito de lugares de k (la hipótesis de esta implicancia puede ser relajada a una noción más débil que aproximación fuera de un conjunto finito, ver [3, Proposición 1, §4]).

1.2. Objetivo: Construcción de ejemplos de no aproximación

Dado un k-grupo finito G, el subconjunto finito $\mathrm{Bad}_G \subseteq \Omega_k$ de lugares de k (ver [2, Definición 2.1]) es la unión del conjunto Bad_G^d compuesto por los lugares de k que dividen al orden de G y el conjunto Bad_G^r compuesto por los lugares que ramifican en la extensión minimal que escinde a G. La historia del problema que estudiaremos puede ser resumida de la siguiente forma:

Primeramente, en [3, Teorema 1] Harari prueba que para todo producto semidirecto iterado de k-grupos abelianos finitos G existe un conjunto finito $T \subset \Omega_k$ tal que G tiene *aproximación fuera de* T (ver Definición 2.4). Esto se logra probando que la obstrucción de Brauer-Manin para el espacio homogéneo SL_n/G es la única obstrucción a la *aproximación débil*, lo que implica la existencia de tal conjunto. Desafortunadamente, esta demostración no permite obtener una descripción precisa del conjunto T. No obstante, es posible predecir el comportamiento de la flecha 1.1 en subconjuntos de T.

Posteriormente, en uno de los principales resultados de [2] (Teorema 1.1) Demarche, Lucchini Arteche y Neftin muestran que si G es un producto semidirecto iterado de grupos abelianos, en particular abeliano, entonces G tiene aproximación fuera de Bad_G. Si bien este resultado describe explícitamente un conjunto finito de lugares donde G tiene aproximación fuera de él, no predice un comportamiento de la flecha en (1.1) en subconjuntos de Bad_G. Por lo que este resultado no puede ser considerado como una mejora al resultado dado en [3] pero sí como un complemento a éste.

Recientemente, en [6] Lucchini Arteche logra un resultado que relaciona a los dos precedentes y es que: dado un k-grupo finito G y asumiendo cierta conjetura de Colliot-Thélène sobre la obstrucción de Brauer-Manin (ver [1, Introducción]), se tiene que G tiene aproximación fuera de Bad_G (ver [6, Corolario 6.3]). Este resultado nos entrega una descripción explícita y general del conjunto de lugares fuera del cual un k-grupo tiene aproximación. Es importante mencionar que la conjetura antes mencionada ha sido probada en una gran variedad de casos, como por ejemplo en productos semidirectos iterados de grupos abelianos finitos por Harari (ver [3, Teorema 1]) y en grupos hípersolubles por Harpaz y Wittenberg (ver [5, Teorema 6.6]).

El objetivo de esta tesis será probar que el resultado obtenido en [6] es *óptimo* en el siguiente sentido: si f asigna a cada k-grupo finito G un subconjunto finito $f(G) \subseteq \Omega_k$ tal que G tiene aproximación fuera de $f(G)$, entonces $f(G)$ no puede tener menos elementos que Bad_G para todo k-grupo finito G. Para esto, probaremos que existen k-grupos abelianos finitos A escindidos por una extensión abeliana tal que el morfismo de restricción

$$H^1(k, A) \to \prod_{v \in \Sigma} H^1(k_v, A)$$

no es epiyectivo en algún subconjunto finito $\Sigma \subseteq \Omega_k$ contenido en Bad_A. Más precisamente, nos preocuparemos de estudiar cómo los subconjuntos Bad_A^d y Bad_A^r afectan a esta epiyectividad, para lo cual precisaremos la búsqueda de Σ en los siguientes dos casos:

1. $\Sigma \subseteq \mathrm{Bad}_A^r \setminus \mathrm{Bad}_A^d$;

2. $\Sigma \subseteq \mathrm{Bad}_A^d \setminus \mathrm{Bad}_A^r$.

Ejemplos de no aproximación en subconjuntos $\Sigma \subseteq \mathrm{Bad}_G^d \setminus \mathrm{Bad}_G^r$ existen y pueden ser construidos a partir de [2, Teorema 5.1]. Estos ejemplos son necesariamente no abelianos y en ellos $\mathrm{Bad}_G^r = \varnothing$. Mostraremos que cuando G es abeliano no existen ejemplos como en el caso 2, por lo que nuestro estudio estará centrado principalmente en el caso 1.

Para efecto de nuestra tesis nos bastará con el estudio de k-grupos abelianos finitos cuyo orden es una potencia de un primo. En efecto, sea A un k-grupo abeliano finito. Como los grupos de cohomología galoisiana son de torsión tenemos que tanto A como $H^1(k, A)$ se descomponen en sus componentes p-primarias. Dado que esta descomposición es única y que los funtores $H^1(k, \cdot)$ conmutan con la suma directa tenemos

$$H^q(k, A)\{p\} = H^q(k, A\{p\}).$$

De esta forma, si A es un k-grupo abeliano finito y $\Sigma \subseteq \Omega_k$ es finito, la restricción

$$H^1(k, A) \to \prod_{v \in \Sigma} H^1(k_v, A)$$

es epiyectiva si y sólo si

$$H^1(k, A\{p\}) \to \prod_{v \in \Sigma} H^1(k_v, A\{p\})$$

es epiyectiva para todo primo p que divida al orden de A. Por lo tanto el estudio de la propiedad de aproximación en k-grupos abelianos finitos se reduce al estudio de esta propiedad en k-grupos abelianos finitos de orden potencia de primo.

1.3. Convenciones y notaciones

En esta tesis k denotará un cuerpo de números y Ω_k el conjunto de lugares de k. Para cada $v \in \Omega_k$ denotaremos por k_v la completación de k en v y, si v es un lugar no arquimediano, $\kappa(v)$ será el cuerpo residual de v. Además para todo cuerpo K denotaremos por $\mathrm{Gal}(K)$ su grupo de Galois absoluto.

Si L/k es una extensión galoisiana con grupo de Galois G, para cada $v \in \Omega_k$ definimos su grupo de descomposición G_v en L/k como el grupo de descomposición $G(w/v)$ en L/k de algún lugar $w \in \Omega_L$ sobre v. En ese caso $\mathrm{Gal}(L_w/k_v) = G_v$, y por ende la flecha de restricción

$$H^1(k, A) \to H^1(k_v, A)$$

se define pasando al límite sobre las extensiones galoisianas finitas. Si bien esta noción depende de la elección de w, esto no trae problema en la primera cohomología, pues si w y w' son lugares sobre v entonces $G(w/v) = g^{-1}G(w'/v)g$ para algún $g \in G$, y por ende los grupos de cohomología $H^1(G(w/v), A)$ y $H^1(G(w'/v), A)$ son canónicamente isormorfos para todo G-grupo A.

Diremos que A es un k-grupo finito si A es un grupo con una acción continua de $\mathrm{Gal}(k)$ compatible con su estructura de grupo. Cuando A sea abeliano diremos que A es un k-grupo abeliano. Además, para cada k-grupo abeliano finito A denotaremos por $\hat{A}$ a su dual de Cartier, i.e. el k-grupo $\mathrm{Hom}(A, \overline{k}^*)$ con la acción $\sigma \cdot f(x) = \sigma \cdot f(\sigma^{-1} \cdot x)$. Por otro lado, diremos que la extensión algebraica L/k escinde a A si $\mathrm{Gal}(L)$ actúa trivialmente en A. Igualmente diremos que A es constante si $\mathrm{Gal}(k)$ actúa trivialmente en A. Notemos que para todo k-grupo finito A existe una extensión galoisiana finita L/k que lo escinde y es la más pequeña con esta propiedad: En efecto, dicha extensión se corresponde con el núcleo del morfismo $\mathrm{Gal}(k) \to \mathrm{Aut}(A)$ dado por la acción de $\mathrm{Gal}(k)$ en A.

§2. Resultados preliminares

2.1. Congruencias y resultados locales

El siguiente resultado es elemental y nos ayudará en la demostración de los teoremas principales de esta tesis.

Lema 2.1. *Sea ℓ un primo. Si p es un primo congruente a 1 módulo ℓ, entonces existe un primo impar q que no es una potencia ℓ-ésima módulo p y tal que*

a) $q \equiv 1 \pmod{8}$ *si* $\ell = 2$*;*

b) $q \equiv 1 \pmod{\ell^2}$ *si* $\ell \neq 2$.

Demostración. Notemos que si $p \equiv 1 \pmod{\ell}$ entonces la función $x \mapsto x^\ell$ de $\mathbb{F}_p$ en $\mathbb{F}_p$ no es biyectiva. Así, el Lema resulta de aplicar el teorema de Dirichlet y el teorema chino de los restos. $\square$

Los siguientes resultados son clásicos en la teoría de cuerpos locales y nos serán muy útiles para construir extensiones cuyos grupos de descomposición en ciertos lugares coincidan con el grupo de Galois de la extensión minimal que escinde a cierto k-grupo abeliano. El segundo resultado se obtiene al aplicar el Lema de Hensel. Para una revisión detallada del primer resultado ver el Corolario de [9, Capítulo I, Proposición 17].

Proposición 2.2. *Sea B un dominio de Dedekind, k su cuerpo de fracciones y $\mathfrak{p}$ un ideal primo de B. Sea $f \in B[x]$ un polinomio de Eisenstein con respecto a $\mathfrak{p}$. Entonces f es irreducible, y si α es una raíz de f, entonces $k(\alpha)$ ramifica totalmente en $\mathfrak{p}$; de hecho $\mathfrak{p}B = \mathfrak{P}^m$ donde $\mathfrak{P} = (\alpha, \mathfrak{p})$ y $m = \mathrm{grado}(f)$.*

Proposición 2.3. *$u \in \mathbb{Z}_p^*$ es una potencia p-ésima en $\mathbb{Q}_p$ si y sólo si $u \equiv 1 \pmod{8\mathbb{Z}_2}$ cuando $p = 2$ y si u es una potencia p-ésima módulo $p^2\mathbb{Z}_p$ cuando $p \neq 2$.*

2.2. Aproximación en k-grupos abelianos

La noción central de esta tesis es la propiedad de aproximación en k-grupos. A continuación presentamos una serie de resultados relativos a esta propiedad que pueden ser encontrados en [2] y [8], junto a observaciones pertinentes a nuestro objetivo.

Definición 2.4. Sea G un k-grupo. Diremos que G *tiene aproximación en* $\Sigma \subseteq \Omega_k$ si el morfismo de restricción

$$H^1(k, G) \to \prod_{v \in \Sigma} H^1(k_v, G),$$

es epiyectivo. Igualmente diremos que G *tiene aproximación fuera de* Σ si éste tiene aproximación en cualquier conjunto finito de lugares de k disjunto a Σ.

Nuestro estudio de esta propiedad se reducirá al caso particular de k-grupos abelianos. En este contexto el siguiente concepto le está estrechamente relacionado y nos será sumamente útil para hacer cálculos.

Definición 2.5. Sea A un k-grupo abeliano y Σ un conjunto de lugares de k. Denotaremos por $Ш^1_\Sigma(k, A)$ al núcleo del morfismo de restricción

$$H^1(k, A) \to \prod_{v \notin \Sigma} H^1(k_v, A).$$

Definimos $Ш^1(k, A) := Ш^1_\varnothing(k, A)$ y $Ш^1_\omega(k, A)$ como la unión de $Ш^1_\Sigma(k, A)$ con Σ finito. Además, si L/k es una extensión de Galois que escinde a A y con grupo de Galois G, denotaremos por $Ш^1_\Sigma(L/k, A)$ al núcleo del morfismo de restricción

$$H^1(G, A) \to \prod_{v \notin \Sigma} H^1(G_v, A),$$

y $Ш^1(L/k, A) := Ш^1_\varnothing(L/k, A)$.

Observación 2.6. El conjunto $Ш^1_\omega(k, A)$ es un grupo pues si α y β son elementos de $Ш^1_\omega(k, A)$ entonces existen Σ y Σ' subconjuntos finitos de Ω_k tales que $\alpha \in Ш^1_\Sigma(k, A)$ y $\beta \in Ш^1_{\Sigma'}(k, A)$, luego $\alpha + \beta \in Ш^1_{\Sigma \cup \Sigma'}(k, A) \subseteq Ш^1_\omega(k, A)$. Otra forma de decir esto es que $Ш^1_\omega(k, A)$ es el límite inductivo $\varinjlim_\Sigma Ш^1_\Sigma(k, A)$ con Σ recorriendo el conjunto de partes finitas de Ω_k e inclusiones como flechas de transición, donde cada objeto $Ш^1_\Sigma(k, A)$ es un subgrupo de $H^1(k, A)$.

El siguiente resultado, que está tomado de [2, Proposición 2.5], nos da la relación antes mencionada entre los dos conceptos precedentes.

Proposición 2.7. *Sea A un k-grupo abeliano, $\hat{A}$ su dual de Cartier y $\Sigma \subseteq \Omega_k$ finito. Entonces hay un emparejamiento,*

$$\prod_{v\in\Sigma} H^1(k_v, A) \times Ш^1_\Sigma(k, \hat{A}) \to \mathbb{Q}/\mathbb{Z},$$

cuyo núcleo derecho es $Ш^1(k, \hat{A})$ y cuyo núcleo izquierdo es la imagen por restricción de

$$H^1(k, A) \to \prod_{v\in\Sigma} H^1(k_v, A).$$

En particular, A tiene aproximación en Σ si y sólo si $Ш^1_\Sigma(k, \hat{A}) = Ш^1(k, \hat{A})$.

Por tanto, primeramente nos concentraremos en entender las propiedades de los grupos $Ш^1_*$. El siguiente resultado, que se encuentra en [8, Lema 1.1] y cuya demostración sigue de aplicar el Teorema de Čebotarev, nos permite hacer eso.

Lema 2.8. *Sea L/k una extensión galoisiana de grupo G, A un k-grupo abeliano finito y Σ un subconjunto finito de Ω_k. Entonces*

a) Si A es constante, entonces $Ш^1_\Sigma(L/k, A) = 0$.

b) Si la extensión L/k escinde a A, tenemos la siguiente reducción

$$Ш^1_\Sigma(k, A) = Ш^1_\Sigma(L/k, A).$$

c) Si G es finito y Σ' es un subconjunto finito de Ω_k formado de lugares cuyos grupos de descomposición en L/k son cíclicos, entonces

$$Ш^1_{\Sigma\cup\Sigma'}(k, A) = Ш^1_\Sigma(k, A).$$

Notemos que si L/k es la extensión minimal que escinde al k-grupo abeliano finito A, el lema anterior nos dice que para que una clase $\alpha \in H^1(k, A)$ se anule localmente en todos los lugares de k basta con que se anule en una cantidad finita de lugares de k, a saber los lugares cuyos grupos de descomposición en L/k no son cíclicos. Esto se resume en el siguiente corolario.

Corolario 2.9. *Sean A un k-grupo abeliano y L/k la extensión minimal que escinde a A. Sea $\Sigma \subseteq \Omega_k$ finito. Si Σ sólo contiene lugares cuyo grupo de descomposición en L/k es cíclico, entonces $Ш^1_\Sigma(k, A) = Ш^1(L/k, A)$.*

Demostración. Por el punto b) del Lema 2.8 tenemos que $Ш^1_\Sigma(k, A) = Ш^1_\Sigma(L/k, A)$. El conjunto Σ sólo contiene lugares de k con grupo de descomposición cíclico en L/k, luego por el punto c) del Lema 2.8 tenemos la igualdad

$$Ш^1_\Sigma(L/k, A) = Ш^1_\varnothing(L/k, A) = Ш^1(L/k, A),$$

obteniendo así la igualdad deseada. $\square$

Observación 2.10. Sea A un k-grupo abeliano finito y $\Sigma \subseteq \mathrm{Bad}^d_A \setminus \mathrm{Bad}^r_A$. El corolario anterior junto con la Proposición 2.7 responde a una de las preguntas de nuestro proyecto de tesis dado que A siempre tendrá aproximación en Σ, pues los grupos de descomposición en L/k de los lugares en Σ serían cíclicos por ser no ramificados en dicha extensión, en consecuencia $Ш^1_\Sigma(k, A) = Ш^1(k, A)$.

En general, si existiese un k-grupo abeliano A y un conjunto finito de lugares de k en donde A no tenga aproximación, entonces ese conjunto debiese contener al menos un lugar cuyo grupo de descomposición en L/k no sea cíclico, o sencillamente sólo debe contener lugares cuyos grupos de descomposición en L/k no sean cíclicos. En particular, estos lugares deben ser ramificados en L/k. Adicionalmente, los lugares arquimedianos no afectan a la aproximación de k-grupos abelianos finitos pues estos tienen grupo de descomposición cíclico. Así, en los sucesivo supondremos que todo conjunto finito $\Sigma \subseteq \Omega_k$ contiene exclusivamente lugares no arquimedianos de k.

A continuación daremos una definición que nos permitirá estudiar la propiedad de aproximación de un k-grupo abeliano A desde un punto de vista puramente algebraico.

Definición 2.11. Sea G un grupo finito. Para un G-módulo A, definimos para $n \geq 0$ el grupo $Ш^n_{\mathrm{cic}}(G, A)$ como el núcleo del morfismo de restricción

$$\hat{H}^n(G, A) \to \prod_{g \in G} \hat{H}^n(\langle g \rangle, A).$$

Observación 2.12. Notar que $Ш^0_{\mathrm{cic}}(G, A)$ está definida sobre la cohomología modificada de Tate (ver [4, Definición 2.5]).

La siguiente proposición, que está tomada de [8, Lema 1.2] y que nuevamente utiliza el Teorema de Čebotarev en su demostración, define un vínculo entre el objeto puramente algebraico $Ш^1_{\mathrm{cic}}$ y el objeto *a priori* aritmético $Ш^1_\omega$.

Proposición 2.13. *Sea A un k-grupo abeliano finito y L/k la extensión minimal que lo escinde con grupo de Galois G. Sea $\Sigma_0 = \Sigma_0(k, A)$ el conjunto de lugares de k cuyo grupo de descomposición en L/k no es cíclico (en particular, Σ_0 sólo contiene lugares que ramifican en L/k). Entonces el grupo $Ш^1_\omega(k, A)$ es un grupo finito e igual a $Ш^1_{\mathrm{cic}}(G, A)$ y podemos escribir*

$$Ш^1_\omega(k, A) = Ш^1_{\Sigma_0}(L/k, A).$$

El conjunto Σ_0 de la proposición anterior será particularmente importante por lo que será bueno definirlo.

Definición 2.14. Sea A un k-grupo abeliano finito. Definimos $\Sigma_0(k, A)$ como el conjunto definido en la Proposición 2.13.

Las Proposiciones 2.7 y 2.13 nos permiten concluir lo siguiente: si el k-grupo abeliano finito A no tiene aproximación en el subconjunto finito $\Sigma \subseteq \Omega_k$ entonces $\Sigma \cap \Sigma_0(k, \hat{A}) \neq \varnothing$. En otras palabras, cuando A es un k-grupo abeliano finito el conjunto de *malos lugares* de A es $\Sigma_0(k, \hat{A})$. Para terminar esta sección mostraremos el siguiente resultado, lo que justifica que más adelante nos concentremos en el conjunto $\Sigma_0(k, \hat{A})$.

Proposición 2.15. *El conjunto $\Sigma_0(k, \hat{A})$ está contenido en* Bad_A

Demostración. Si A es un k-grupo abeliano finito y L/k es la extensión minimal que lo escinde, entonces la extensión minimal que escinde a $\hat{A}$ está contenida en $L(\zeta_e)/k$, donde e es el exponente de A. Por ende, si un lugar $v \in \Omega_k$ ramifica en $L(\zeta_e)/k$ entonces ramifica en L/k o en $L(\zeta_e)/L$, lo que implica necesariamente que v ramifica en L/k o divide a e (en particular divide al orden de A). □

2.3. Resultados previos y herramientas para la construcción de ejemplos de no aproximación

Sea A un k-grupo abeliano finito y $\Sigma \subseteq \Omega_k$ finito. Recordemos que para que A tenga aproximación en Σ es necesario y suficiente que $Ш^1_\Sigma(k, \hat{A})/Ш^1(k, \hat{A}) = 0$ (ver Proposición 2.7). Inspirados en esto, toda esta sección está orientada a probar el Lema 2.21 que nos dará una forma de contruir cocientes $Ш^1_\Sigma(k,\hat{A})/Ш^1(k,\hat{A})$ no triviales.

Notemos que para que A no tenga aproximación en Σ es necesario que $Ш^1_\Sigma(k,\hat{A}) \neq 0$, es decir es necesario que $Ш^1_\omega(k,\hat{A}) \neq 0$. Entonces lo que haremos a continuación es construir k-grupos abelianos finitos A para los cuales $Ш^1_{\text{cic}}(G,A) \neq 0$ (ver Proposición 2.13), donde G es el grupo de Galois de la extensión minimal que escinde a A.

Definición 2.16. Sea G un grupo finito de orden n. El *morfismo de aumentación* del anillo de grupo $\mathbb{Z}/n\mathbb{Z}[G]$ es el morfismo

$$\pi : \mathbb{Z}/n\mathbb{Z}[G] \to \mathbb{Z}/n\mathbb{Z}$$
$$\sum_{g\in G} n_g g \mapsto \sum n_g.$$

Definimos el *ideal de aumentación* del anillo de grupo $\mathbb{Z}/n\mathbb{Z}[G]$ como el núcleo del morfismo π.

Lema 2.17. *Sea G un grupo finito orden n y exponente e. Sea I el ideal de aumentación de $\mathbb{Z}/n\mathbb{Z}[G]$. Entonces, $Ш^1_{\text{cic}}(G,I) \cong \mathbb{Z}/f\mathbb{Z}$ donde $f = n/e$.*

Demostración. Tenemos la sucesión exacta $0 \to I \to \mathbb{Z}/n\mathbb{Z}[G] \to \mathbb{Z}/n\mathbb{Z} \to 0$. Entonces, como el G-módulo $\mathbb{Z}/n\mathbb{Z}[G]$ es cohomológicamente trivial (ver [4, Proposición 1.23]), para todo $H \leq G$ tenemos los isomorfismos $H^1(H,I) \cong \hat{H}^0(H,\mathbb{Z}/n\mathbb{Z})$ (ver [4, Corolario 2.7]). En consecuencia $Ш^1_{\text{cic}}(G,I)$ es isomorfo a $Ш^0_{\text{cic}}(G,B)$. Por otro lado, tenemos que $\hat{H}^0(H,\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z}$ para todo $H \leq G$. Por lo tanto,

$$Ш^1_{\text{cic}}(G,I) \cong \ker\left[\mathbb{Z}/n\mathbb{Z} \to \prod_{g\in G} \mathbb{Z}/|g|\mathbb{Z}\right] \cong \mathbb{Z}/f\mathbb{Z},$$

donde $f = n/e$. □

Para complementar el resultado anterior notemos que para que A no tenga aproximación en Σ es suficiente que las siguientes condiciones se satisfagan

I) $Ш^1_\Sigma(k,\hat{A}) \neq 0$;

II) $Ш^1(k,\hat{A}) = 0$,

por lo que nos interesará saber cuando la última condición es satisfecha en vista de que sabemos construir ejemplos donde la primera condición es satisfecha. El lema siguiente nos ayudará en esta dirección.

Lema 2.18. *Sea L/k la extensión minimal que escinde al k-grupo abeliano A. Supongamos que existe $v \in \Omega_k$ tal que $G_v = G := \mathrm{Gal}(L/k)$. Entonces $Ш^1_\Sigma(k, A) = 0$ para todo $\Sigma \subset \Omega_k$ finito que no contenga a v.*

Demostración. Sea $v \in \Omega_k$ tal que $G_v = G$. Luego, el morfismo de restricción

$$\mathrm{Res}_v : H^1(G, A) \to H^1(G_v, A),$$

es la identidad. Sea $\Sigma \subset \Omega_k$ finito que no contiene a v. Así, si $\alpha \in Ш^1_\Sigma(L/k, A)$ entonces $\mathrm{Res}_v(\alpha) = \alpha = 0$. En consecuencia, $Ш^1_\Sigma(L/k, A) = 0$. Ahora, por el punto b) del Lema 2.8 tenemos que $Ш^1_\Sigma(k, A) = Ш^1_\Sigma(L/k, A)$. Por lo tanto, $Ш^1_\Sigma(k, A) = 0$. □

Los siguientes resultados son inmediatos del lema precedente y nos dan una condición de suficiencia para que $Ш^1(k, A) = 0$.

Corolario 2.19. *Sea L/k la extensión minimal que escinde al k-grupo abeliano A. Para que A no tenga aproximación en Σ es necesario que Σ contenga a todos los lugares cuyo grupo de descomposición en L/k es $\mathrm{Gal}(L/k)$. En particular, si $v \in \Omega_k$ es un lugar cuyo grupo de descomposición en L/k es $\mathrm{Gal}(L/k)$ entonces A tiene aproximación en $\Sigma_0(k, \hat{A}) \setminus \{v\}$.*

Corolario 2.20. *Sea L/k la extensión minimal que escinde al k-grupo abeliano A. Si existe $v \in \Omega_k$ cuyo grupo de descomposición es $G := \mathrm{Gal}(L/k)$, entonces $Ш^1(k, A) = 0$.*

Sea G un grupo de orden n y L/k una extensión galoisiana con grupo de Galois isomorfo a G. Entonces el ideal de aumentación de $\mathbb{Z}/n\mathbb{Z}[G]$ tiene una estructura de k-grupo abeliano; en efecto, $\mathrm{Gal}(L/k)$ actúa en I vía la acción natural de G en I. Luego, extendiendo esta acción a $\mathrm{Gal}(k)$ tenemos que I es un k-grupo abeliano finito. Notemos que cuando $n \geq 3$, la extensión minimal que escinde a I es L/k ya que, en este caso, $\mathrm{Gal}(L/k)$ actúa fielmente en la $\mathbb{Z}$-base $\{g-1 \mid g \in \mathrm{Gal}(L/k)\}$ de I. Para efecto de nuestra tesis, todos las construcciones se harán en el caso $n \geq 3$. De esta forma cabe preguntarnos

¿Existirá una extensión de Galois L/k con grupo de Galois G de orden n donde el k-grupo abeliano I y el conjunto de lugares $\Sigma_0(k, I)$ satisfaga las condiciones I e II?

En este punto es importante notar lo siguiente: si $\Sigma_0(k, I)$ no contiene lugares que dividen a n entonces $\Sigma_0(k, I) \subseteq \mathrm{Bad}^r_{\hat{I}} \setminus \mathrm{Bad}^d_{\hat{I}}$ (por la Proposición 2.15) y por consiguiente el par $(A, \Sigma_0(k, \hat{A}))$, con $A = \hat{I}$, sería un buen candidato a lo buscado.

El siguiente lema concretiza esta pregunta y orientará nuestras construcciones.

Lema 2.21. *Sea L/k una extensión galoisiana con grupo de Galois G de orden n y exponente e tal que $n/e \neq 1$. Sea I un k-grupo abeliano finito definido como el ideal de aumentación de $\mathbb{Z}/n\mathbb{Z}[G]$. Entonces si existe $v \in \Omega_k$ tal que $G_v = G$ se tiene que $Ш^1_{\Sigma_0(k,I)}(k,I)/Ш^1(k,I) \neq 0$.*

Demostración. Sabemos, por la Proposición 2.13 y el Lema 2.17, que $Ш^1_\omega(k,I) = Ш^1_{\Sigma_0(k,I)}(k,I) \neq 0$ pues $n/e \neq 1$. Supongamos que existe $v \in \Omega_k$ tal que $G_v = G$. Entonces por el Corolario 2.20 tenemos que $Ш^1(k,I) = 0$. Así concluimos que el cociente $Ш^1_{\Sigma_0(k,I)}(k,I)/Ш^1(k,I) \neq 0$. $\square$

§3. Resultados

En todo este capítulo usaremos letras latinas (e.g. p) para designar primos en $\mathbb{Q}$ y usaremos letras góticas (e.g. $\mathfrak{p}, \mathfrak{P}$) para designar lugares en cuerpos de números distintos de $\mathbb{Q}$.

3.1. Ejemplos de no aproximación en grupos de torsión ℓ-primaria

El objetivo de esta sección es encontrar una familia de ejemplos de no aproximación en grupos de torsión ℓ-primaria cuando ℓ es dado. Lo que se resume en el siguiente resultado.

Teorema 3.1. *Para todo par de primos ℓ y p con $p \equiv 1 \pmod{\ell^n}$, existe un cuerpo de números k y un k-grupo abeliano A de orden ℓ^a, con $a = (n+1)(\ell^{n+1} - 1)$, tal que*

- *$\Sigma_0(k, \hat{A}) \subseteq \mathrm{Bad}_A^r \smallsetminus \mathrm{Bad}_A^d$ y contiene a todos los lugares sobre p;*
- *A no tiene aproximación en $\Sigma_0(k, \hat{A})$;*
- *A tiene aproximación en $\Sigma_0(k, \hat{A}) \smallsetminus \{\mathfrak{p}\}$ para todo $\mathfrak{p}$ sobre p.*

Sean $n \geq 1$, ℓ un número primo y $k = \mathbb{Q}(\zeta_{\ell^n})$. El siguiente resultado nos permite encontrar explícitamente una extensión de Galois de k en la que el grupo de descomposición de algún lugar de k es todo el grupo de Galois y en donde los lugares que dividen al orden de la extensión tienen grupo de descomposición cíclico.

Lema 3.2. *Sea p un primo congruente a 1 módulo ℓ^n. Entonces existe un primo impar q tal que*

- *$\mathrm{Gal}(k_{\mathfrak{p}}(\sqrt[\ell^n]{p}, \sqrt[\ell]{q})/k_{\mathfrak{p}}) = \mathrm{Gal}(k(\sqrt[\ell^n]{p}, \sqrt[\ell]{q})/k) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, para todo lugar $\mathfrak{p} \in \Omega_k$ sobre p;*
- *$\mathrm{Gal}(k_{\mathfrak{l}}(\sqrt[\ell^n]{p}, \sqrt[\ell]{q})/k_{\mathfrak{l}}) \hookrightarrow \mathbb{Z}/\ell^n\mathbb{Z}$, para todo lugar $\mathfrak{l} \in \Omega_k$ sobre ℓ.*

Demostración. Sea q un primo dado por el Lema 2.1, i.e. un primo impar que no es una potencia ℓ-ésima módulo p y tal que

- $q \equiv 1 \pmod 8$ si $\ell = 2$;
- $q \equiv 1 \pmod{\ell^2}$ si $\ell \neq 2$.

Sea $L = k(\sqrt[\ell^n]{p}, \sqrt[\ell]{q})$. Notemos que $k/\mathbb{Q}$ es una extensión no ramificada en p. Luego el polinomio $x^{\ell^n} - p$ es de Eisenstein sobre $\mathfrak{p}$, para todo $\mathfrak{p}|p$. Por ende $k(\sqrt[\ell^n]{p})/k$ es una extensión galoisiana con grupo de Galois isomorfo a $\mathbb{Z}/\ell^n\mathbb{Z}$. Luego, por la Proposición 2.2, esta extensión es totalmente ramificada en $\mathfrak{p}$ y $k_\mathfrak{p}(\sqrt[\ell^n]{p})/k_\mathfrak{p}$ tiene grupo de Galois isomorfo a $\mathbb{Z}/\ell^n\mathbb{Z}$. Por otro lado, $k(\sqrt[\ell]{q})/k$ no ramifica en $\mathfrak{p}$ (pues $x^\ell - q$ es separable en $\kappa(\mathfrak{p})$). Entonces, $\mathrm{Gal}(k_\mathfrak{p}(\sqrt[\ell]{q})/k_\mathfrak{p}) \cong \mathbb{Z}/\ell\mathbb{Z}$ si y sólo si $[\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = \ell$, donde $\mathfrak{P}$ es algún lugar de $k(\sqrt[\ell]{q})$ sobre $\mathfrak{p}$. Como $p \equiv 1 \pmod{\ell^n}$, éste se descompone completamente en k, luego $\kappa(\mathfrak{p}) = \mathbb{F}_p$ y por ende

$$[\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})] = [\mathbb{F}_p(\sqrt[\ell]{q}) : \mathbb{F}_p] = \ell,$$

ya que q no es una potencia ℓ-ésima módulo p. En consecuencia, $k_\mathfrak{p}(\sqrt[\ell]{q})/k_\mathfrak{p}$ es un extensión cíclica de orden ℓ. Por lo tanto, $L_\mathfrak{p} := k_\mathfrak{p}(\sqrt[\ell^n]{p}, \sqrt[\ell]{q})$ es una extensión ramificada con

$$\mathrm{Gal}(L_\mathfrak{p}/k_\mathfrak{p}) \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \cong \mathrm{Gal}(L/k).$$

Finalmente, por la Proposición 2.3 q es una ℓ-potencia en $\mathbb{Q}_\ell$, por ende

$$\mathrm{Gal}(k_\mathfrak{l}(\sqrt[\ell^n]{p}, \sqrt[\ell]{q})/k_\mathfrak{l}) \hookrightarrow \mathbb{Z}/\ell^n\mathbb{Z},$$

para todo $\mathfrak{l} \in \Omega_k$ sobre ℓ. $\square$

El siguiente resultado es inmediato del lema anterior y nos dice más claramente lo que hemos obtenido.

Lema 3.3. *Sea p un primo congruente a 1 módulo ℓ^n. Entonces existe una extensión galoisiana L/k con grupo de Galois $G = \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ tal que $G_\mathfrak{p} = G$ para todo lugar $\mathfrak{p} \in \Omega_k$ sobre p y $G_\mathfrak{l}$ cíclico para todo lugar $\mathfrak{l} \in \Omega_k$ sobre ℓ.*

Con esto podemos demostrar el teorema del principio de la sección.

Demostración del Teorema 3.1. Sea L/k la extensión dada por el Lema 3.3 y sea $G := \mathrm{Gal}(L/k)$. Sea I el ideal de aumentación de $\mathbb{Z}/\ell^{n+1}\mathbb{Z}[G]$ con la estructura de k-grupo definida por L/k. Así tenemos que $\Sigma_0(k, I)$ contiene a todos los lugares sobre p, no contiene a ningún lugar sobre ℓ y por el Lema 2.21 el cociente $Ш^1_{\Sigma_0(k,I)}(k, I)/Ш^1(k, I)$ es no trivial. Por lo tanto, definiendo $A := \hat{I}$ tenemos, por la Proposición 2.15, que

$$\Sigma_0(k, \hat{A}) = \Sigma_0(k, I) \subseteq \mathrm{Bad}^r_A \setminus \mathrm{Bad}^d_A\,.$$

Además, A no tiene aproximación en $\Sigma_0(k, \hat{A})$ y sí tiene aproximación en $\Sigma_0(k, \hat{A}) \setminus \{\mathfrak{p}\}$ para todo lugar $\mathfrak{p}$ sobre p (ver Corolario 2.19). □

Observación 3.4. Cuando $n = 1$ el conjunto $\Sigma_0(k, I)$ está formado sólo de lugares cuyo grupo de descomposición es $\mathrm{Gal}(L/k)$. De esta forma, tenemos que $\Sigma_0(k, I)$ es el subconjunto de Ω_k más pequeño en donde $\hat{A}$ no tiene aproximación.

Particularmente, si $n = 1$ y $\ell = 2$ tenemos que $k = \mathbb{Q}$ y $\Sigma_0(\mathbb{Q}, I) = \{p, q\}$: en efecto, los únicos lugares de $\mathbb{Q}$ con grupo de descomposición no cíclico en $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})/\mathbb{Q}$ son p y posiblemente q, luego $\Sigma_0(\mathbb{Q}, I) \subset \{p, q\}$. Ahora, por hipótesis q es congruente a 1 módulo 4 y no es un cuadrado módulo p. Luego, por la ley de reciprocidad cuadrática, tenemos que p tampoco es un cuadrado módulo q. En consecuencia, el grupo de descomposición de q en $L/\mathbb{Q}$ es $\mathrm{Gal}(L/\mathbb{Q})$. Por lo tanto, $\Sigma_0(\mathbb{Q}, I) = \{p, q\}$.

3.2. Ejemplos de no aproximación en casi todo lugar de k

Esta sección tiene por objetivo encontrar ejemplos de no aproximación en cualquier cuerpo de números k y en casi cualquier lugar de k. Esto lo resumimos en el siguiente resultado.

Teorema 3.5. *Para todo cuerpo de números k y para todo $\mathfrak{p} \in \Omega_k$ que no divide a 2, existe un k-grupo abeliano finito A tal que*

- $\mathfrak{p} \in \Sigma_0(k, \hat{A}) \subseteq \mathrm{Bad}^r_A \setminus \mathrm{Bad}^d_A$*;*
- *A no tiene aproximación en $\Sigma_0(k, \hat{A})$;*
- *A tiene aproximación en $\Sigma_0(k, \hat{A}) \setminus \{\mathfrak{p}\}$.*

Sea k un cuerpo de números y $\mathfrak{p}$ un lugar de k sobre un primo $p \in \mathbb{Q}$.

Lema 3.6. *Supongamos que p es distinto de 2. Entonces existen $a, b \in \mathcal{O}_k$ tal que*

- $\mathrm{Gal}(k_{\mathfrak{p}}(\sqrt{a}, \sqrt{b})/k_{\mathfrak{p}}) = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*;*
- $\mathrm{Gal}(k_v(\sqrt{a}, \sqrt{b})/k_v) \hookrightarrow \mathbb{Z}/2\mathbb{Z}$*, para todo lugar $v \in \Omega_k$ sobre* 2.

Demostración. Sea $\Sigma_2 \subseteq \Omega_k$ el conjunto de lugares sobre 2. Sea $a_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^* \setminus \mathcal{O}_{\mathfrak{p}}^{*2}$ que no sea un cuadrado en $\kappa(\mathfrak{p})$. Por el teorema de aproximación para un cuerpo de números (ver [7, Capítulo II, Teorema 3.4]), existe $a \in \mathcal{O}_k$ tal que $a - a_{\mathfrak{p}} \in \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ y $a \in \mathcal{O}_v^{*2}$ para todo $v \in \Sigma_2$ pues $\mathcal{O}_v^{*2}$ es un abierto en $\mathcal{O}_v^*$ para todo $v \mid 2$. En particular, a no es un cuadrado módulo $\mathfrak{p}$. En consecuencia, $k_v(\sqrt{a})/k_v$ es trivial y $k_{\mathfrak{p}}(\sqrt{a})/k_{\mathfrak{p}}$ es una extensión cuadrática no ramificada puesto que

$$2 = [\kappa(\mathfrak{p})(\sqrt{a}) : \kappa(\mathfrak{p})] \leq [k_{\mathfrak{p}}(\sqrt{a}) : k_{\mathfrak{p}}] \leq 2.$$

Por otro lado, el conjunto $\{x \in k_{\mathfrak{p}} \mid v_{\mathfrak{p}}(x) = 1\}$ es un abierto de $k_{\mathfrak{p}}$ pues $v_{\mathfrak{p}}$ es una valuación discreta. Luego, existe $b \in k_{\mathfrak{p}}$ tal que $v_{\mathfrak{p}}(b) = 1$, el cual podemos suponer entero. Así, el polinomio $x^2 - b$ es de Eisenstein sobre $\mathfrak{p}$ y por tanto la extensión $k_{\mathfrak{p}}(\sqrt{p})/k_{\mathfrak{p}}$ es cuadrática y totalmente ramificada (por Proposición 2.2). Por lo tanto,

$$\mathrm{Gal}(k_{\mathfrak{p}}(\sqrt{a}, \sqrt{b})/k_{\mathfrak{p}}) = \mathrm{Gal}(k(\sqrt{a}, \sqrt{b})/k) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

y

$$\mathrm{Gal}(k_v(\sqrt{a}, \sqrt{b})/k_v) = \mathrm{Gal}(k_v(\sqrt{b})/k_v) \hookrightarrow \mathbb{Z}/2\mathbb{Z},$$

para todo $v \in \Sigma_2$. □

Observación 3.7. Cuando p no divide al discriminante de la extensión $k/\mathbb{Q}$, entonces el entero b del Lema 3.6 puede ser tomado como p.

El siguiente resultado no es más que una retraducción del lema anterior y nos dice más claramente lo que hemos obtenido.

Lema 3.8. *Supongamos que p es distinto de 2. Entonces existe una extensión bicuadrática L/k tal que $G_{\mathfrak{p}} = \mathrm{Gal}(L/k)$ y G_v es cíclico para todo lugar $v \in \Omega_k$ sobre* 2.

Con esto podemos dar una demostración al teorema del inicio de la sección.

Demostración del Teorema 3.5. Sea L/k la extensión dada por el Lema 3.8 y sea $G := \mathrm{Gal}(L/k)$. Sea I el ideal de aumentación de $\mathbb{Z}/4\mathbb{Z}[G]$ con la estructura de k-grupo abeliano definida por L/k. La demostración sigue igual a la del Teorema 3.1 cambiando ℓ por 2. □

3.3. Algunas observaciones sobre las construcciones precedentes

3.3.1. ¿Se puede obtener un resultado más general usando las mismas construcciones?

En las secciones anteriores dimos ejemplos de no aproximación en:

- k-grupos abelianos de orden ℓ^n para cualquier primo ℓ (Teorema 3.1);
- y en casi todos los lugares (todos salvo una cantidad finita) de un cuerpo de números arbitrario (Teorema 3.5).

En este punto surge una pregunta natural ¿será posible usar las mismas construcciones que permiten demostrar estos teoremas para dar un ejemplo de no aproximación en completa arbitrariedad de elección de ℓ, $\mathfrak{p}$ y k? Más precisamente, dado un primo ℓ, k un cuerpo de números y $\mathfrak{p}$ un lugar de k sobre un primo distinto de ℓ ¿existirá una extensión galoisiana L/k de grupo G y grado una potencia de ℓ tal que $\Sigma_0(k, I) \subseteq \mathrm{Bad}_I^r \setminus \mathrm{Bad}_I^d$ contenga a $\mathfrak{p}$ y $G_\mathfrak{p} = G$? La respuesta es no. En efecto, sea $\mathfrak{P}$ un lugar de L sobre $\mathfrak{p}$. Si suponemos que $G_\mathfrak{p} = \mathrm{Gal}(L/k)$ entonces $L_\mathfrak{P}/k_\mathfrak{p}$ es moderamente ramificada. Sea $T/k_\mathfrak{p}$ la subextensión no ramificada maximal de $L_\mathfrak{P}/k_\mathfrak{p}$, entonces la extensión $L_\mathfrak{P}/T$ está generada por radicales de orden divisible por ℓ (ver [7, Capítulo II, Proposición 7.7]). Lo anterior implica que $\mu_\ell \subseteq T$ y por ende ℓ divide a $|\kappa_T| - 1$, donde κ_T es el cuerpo residual de T. Por lo tanto, no podemos esperar mejoras a los resultados obtenidos en los Teorema 3.1 y 3.5 utilizando las mismas construcciones con libertad de elección en ℓ, $\mathfrak{p}$ y k pues inevitablemente tendríamos la restricción ℓ divide a $|\kappa_T| - 1$.

3.3.2. ¿Qué se puede decir sobre la restricción en $\mathfrak{p}$ en el Teorema 3.5?

La demostración del Teorema 3.5 pasa por el uso del Lema 2.21. Así, la motivación es encontrar una extensión abeliana L/k con grupo de Galois G de orden primo a p y para la cual $G = G_\mathfrak{p}$.

El Lema 3.6 nos permite contruir una tal extensión cuando p es distinto de 2 pero ¿qué ocurre cuando $p = 2$? Evidentemente, el Lema 3.6 no nos sirve en este caso. Entonces debemos encontar otra forma de construir tales extensiones cuando $p = 2$. Lamentablemente, esto no es posible en general pues depende del cuerpo residual de $\mathfrak{p}$. En efecto, la aplicación de reciprocidad de la teoría local de cuerpo de clases nos da una correspondencia entre las extensiones abelianas de $k_\mathfrak{p}$ y los cocientes finitos de $k_\mathfrak{p}^*$ (ver [4, Teorema 9.13]). Por otro lado, recordemos que $k_\mathfrak{p}^* \cong \mathbb{Z} \times U_\mathfrak{p}^1 \times \kappa(\mathfrak{p})^*$ donde $U_\mathfrak{p}^1$ es un pro-2-grupo, i.e. un límite proyectivo de 2-grupos (ver [4, Teorema 7.18]). Por tanto, cuando $\kappa(\mathfrak{p}) = \mathbb{F}_2$ el grupo $k_\mathfrak{p}^*$ tiene un único cociente de orden primo a 2, el cual es cíclico. En consecuencia existe una única extensión abeliana de $k_\mathfrak{p}$ de grado primo a 2, la cual es cíclica. Por tanto, en este caso, no existe una extensión abeliana de grado primo a 2 que satisfaga las hipótesis del Lema 2.21. Así, si quisiésemos usar las mismas construcciones para probar el Teorema 3.5 no podríamos hacerlo en el caso $p = 2$ y $\kappa(\mathfrak{p}) = \mathbb{F}_2$.

Bibliografía

[1] Jean-Louis Colliot-Thélène. Points rationnels sur les fibrations. In *Higher dimensional varieties and rational points (Budapest, 2001)*, volume 12 of *Bolyai Soc. Math. Stud.*, pages 171–221. Springer, Berlin, 2003.

[2] Cyril Demarche, Giancarlo Lucchini Arteche, and Danny Neftin. The Grunwald problem and approximation properties for homogeneous spaces. *Annales de l'Institut Fourier*, 67:1009–1033, 2015.

[3] David Harari. Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini. *Bulletin de la Société Mathématique de France*, 135(4):549–564, 2007.

[4] David Harari. *Cohomologie galoisienne et théorie du corps de classes.* Savoirs Actuels (Les Ulis). EDP Sciences, Les Ulis; CNRS Éditions, Paris, 2017.

[5] Yonatan Harpaz and Olivier Wittenberg. Zéro-cycles sur les espaces homogènes et problème de Galois inverse. *Journal of the American Mathematical Society*, pages 775–805, 2020.

[6] Giancarlo Lucchini Arteche. The unramified Brauer group of homogeneous spaces with finite stabilizer. *Transactions of the American Mathematical Society*, 372(8):5393–5408, 2019.

[7] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften.* Springer-Verlag, Berlin, 1999.

[8] J.-J. Sansuc. Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. *Journal für die reine und angewandte Mathematik*, 327:12–80, 1981.

[9] Jean-Pierre Serre. *Corps locaux.* Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

Financiamiento

Esta tesis fue financiada gracias a las siguientes becas:

- Beca de arancel de desarrollo de tesis 2019, Facultad de Ciencias, Universidad de Chile;
- Beca Magíster Nacional 2020, Anid;
- Beca de arancel redacción de tesis 2020, Facultad de Ciencias, Universidad de Chile.