CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS

DEL INSTITUTO POLITÉCNICO NACIONAL

UNIDAD ZACATENCO

DEPARTAMENTO DE CONTROL AUTOMÁTICO

Campos de géneros extendidos de campos globales y extensiones abelianas imaginarias con número de clases de ideales uno

T E S I S

QUE PRESENTA

Elizabeth Ramírez Ramírez

Para obtener el grado de

Doctora en Ciencias

en la Especialidad de Control Automático

Directora de Tesis:

Dra. Martha Rzedowski Calderón

México, Ciudad de México Abril, 2019

A mis padres y hermanos.

A Eduardo Israel, Abril Paola,
Balam Alejandro, Mabel Itzae y Hanna.

"Algunos misterios siempre escaparán a la mente humana.
Para convencernos de ello, sólo hay que echar un vistazo
a las tablas de los números primos, y ver que no reina
ni orden, ni reglas."
Évariste Galois

"Tenemos mucho tiempo por delante
para crear los sueños que aún
ni siquiera imaginamos soñar."
Steven Spielberg

Agradecimientos

Agradecezco profundamente a la Dra. Martha Rzedowski Calderón por su tiempo, confianza, y por todo el apoyo brindado durante la realización de este trabajo, por su amistad y por animarme siempre a seguir adelante.

Al Dr. Gabriel Villa Salvador por sus enseñanzas y sugerencias para mejorar este trabajo. A mis sinodales, Dra. Petra Wiederhold, Dr. Pablo Lam, Dr. Felipe Zaldívar y Dr. Fausto Jarquín por sus consejos y apoyo.

Al CINVESTAV por el apoyo para asistir a congresos y para graduarme. Al Departamento de Control Automático por la oportunidad brindada.

A mis padres y a mis hermanos Israel, Tere, René y Janet por su apoyo incondicional, por soportarme en los momentos difíciles y por creer en mi siempre.

A quienes de alguna u otra forma me ayudaron a culminar esta etapa de mi vida. En especial a Miguel, Anaid, Carlos, Jonny, y Gabriel por escucharme siempre y por estar cuando más los necesité, por animarme a seguir adelante y por los buenos momentos que pasamos juntos.

Al CONACyT por la beca que me otorgó durante mis estudios de doctorado.

Índice general

Resumen

En la primera parte de la tesis obtenemos el campo de géneros extendido de un campo global. Primero describimos, vía la teoría de campos de clases, el campo de géneros extendido de un campo numérico arbitrario. Segundo, definimos el campo de géneros extendido de un campo de funciones global y obtenemos, también a través de la teoría de campos de clases, la descripción del campo de géneros extendido de un campo de funciones global arbitrario. En la última parte de la tesis consideramos extensiones abelianas imaginarias de un campo de funciones racionales con número de clases de ideales igual a uno.

Abstract

In the first part of the thesis we obtain the extended genus field of a global field. First we describe, via class field theory, the extended genus field of an arbitrary number field. Second, we define the extended genus field of a global function field and we obtain, also via class field theory, the description of the extended genus field of an arbitrary global function field. In the last part of the thesis we consider imaginary abelian function field extensions of a rational function field with ideal class number equal to one.

Introducción

El estudio de *campos de géneros extendidos* se remonta a C.F. Gauss [15], quien introdujo el concepto de género en el contexto de formas cuadráticas. Durante la primera mitad del siglo pasado, el concepto fue importado a campos de números cuadráticos. H. Hasse [16] estudió la teoría de géneros de los campos numéricos cuadráticos. Por medio de la teoría de campos de clases, H. W. Leopoldt [27] generalizó el trabajo de Hasse introduciendo el concepto de campo de géneros para una extensión abeliana finita del campo de números racionales. Leopoldt estudió los campos de géneros extendidos usando la aritmética de los campos abelianos por medio de *caracteres de Dirichlet*. El primero en introducir el concepto de campo de géneros y de campo de géneros extendido de una extensión finita no abeliana del campo de los números racionales fue A. Fröhlich quien definió el concepto de campo de géneros de una extensión finita arbitraria de $\mathbb{Q}$ [11, 12]. Para un campo numérico K, él definió el campo de géneros K (con respecto al campo racional $\mathbb{Q}$) como $K_{\mathfrak{g}} := K\omega$ donde $\omega/\mathbb{Q}$ es la máxima extensión abeliana tal que $K\omega/K$ es no ramificada en todos los primos. Del mismo modo, el campo de géneros extendido es $K_{\mathfrak{g}^+} = K\Omega$ donde $\Omega/\mathbb{Q}$ es la máxima extensión abeliana tal que $K\Omega/K$ es no ramificada en los primos finitos. Numerosos autores han estudiado campos de géneros y campos de géneros extendidos para extensiones finitas $K/\mathbb{Q}$ sobre $\mathbb{Q}$.

En el caso de los campos numéricos, los conceptos de *campo de clases de Hilbert* y de *campo de clases de Hilbert extendido* están definidos sin ninguna ambigüedad. El campo de clases de Hilbert K_H y el campo de clases de Hilbert extendido K_{H^+} de un campo numérico $K/\mathbb{Q}$ se definen como la máxima extensión abeliana no ramificada y como la máxima extensión abeliana no ramificada en los primos finitos de K, respectivamente. De esta manera, los conceptos de campo de géneros y de campo de géneros extendido se definen dependiendo del concepto de campo de clases de Hilbert y de campo de clases de Hilbert extendido, respectivamente. Es decir, tenemos $K \subseteq K_{\mathfrak{g}} \subseteq K_H$ y el grupo de Galois $\mathrm{Gal}(K_H/K)$ es isomorfo al grupo de clases Cl_K de K. El campo de géneros $K_{\mathfrak{g}}$ corresponde a un subgrupo G_K de Cl_K y tenemos $\mathrm{Gal}(K_{\mathfrak{g}}/K) \cong Cl_K/G_K$. El grado $[K_{\mathfrak{g}} : K]$ se llama

el *número de géneros* de K y $\mathrm{Gal}(K_{\mathfrak{g}}/K)$ se llama el *grupo de géneros* de K. De manera similar, $K \subseteq K_{\mathfrak{g}^+} \subseteq K_{H^+}$ y $K_{\mathfrak{g}^+}$ corresponde a un subgrupo G_{K^+} de $\mathrm{Gal}(K_{\mathfrak{g}^+}/K) \cong Cl_{K^+}/G_{K^+}$.

Para campos de funciones globales, la situación es diferente debido al hecho de que hay varios conceptos de campo de clases Hilbert y de campo de clases de Hilbert extendido, dependiendo de en qué aspecto está uno interesado. La definición directa del campo de clases de Hilbert K_H de un campo de funciones global K sobre $\mathbb{F}_q$ como la máxima extensión abeliana no ramificada de K tiene la desventaja de ser grado de grado infinito sobre K debido a las extensiones de constantes. En las extensiones de constantes, cada primo es eventualmente inerte, entonces, si estamos interesados en una definición de un campo de clases de Hilbert de grado finito sobre el campo de base, debemos imponer algunas condiciones sobre las extensiones de constantes. Parece que la primera que consideró el campo de géneros extendido en el caso de campos de funciones fue R. Clement en [8], donde ella estudió el caso de una extensión cíclica moderadamente ramificada $K/\mathbb{F}_q(T)$ de Kummer de grado primo ℓ diferente de la característica p de $\mathbb{F}_q$. Ella desarrolló la teoría a lo largo de las líneas del caso estudiado por Hasse en [16]. Después, S. Bae y J.K. Koo [4] generalizaron los resultados de Clement siguiendo el desarrollo dado por Fröhlich. Ellos definieron el campo de géneros extendido para extensiones de un campo de funciones global arbitrario K definiendo un análogo a las extensiones de campos de funciones ciclotómicos de $\mathbb{F}_q(T)$ dadas por el módulo de Carlitz.

M. Rosen definió en [47] el campo de clases de Hilbert de un campo de funciones global K como la máxima extensión abeliana no ramificada de K tal que un conjunto finito no vacío fijo de divisores primos de K se descomponen totalmente. Usando esta definición de campo de clases de Hilbert, G. Peng [41] encontró el campo de géneros de una extensión de Kummer de grado primo sobre el campo de funciones racionales $k = \mathbb{F}_q(T)$. Su método utilizó el análogo para campos de funciones del hexágono exacto de Conner - Hurrelbrink en los campos numéricos. El caso de una extensión salvaje de grado primo fue presentado por S. Hu e Y. Li en [17] donde ellos describieron explícitamente el campo de géneros de una extensión de Artin - Schreier del campo de funciones racionales. En [5, 30, 32] se desarrolló una teoría de campos de géneros usando el mismo concepto de campo de clases de Hilbert. En estos artículos, se usaron las ideas de Leopoldt usando caracteres de Dirichlet.

En el primer capítulo de esta tesis describimos, utilizando la teoría de campos de clases, el campo de géneros extendido de un campo numérico. Por el Teorema de Kronecker-Weber, cualquier extensión abeliana de $\mathbb{Q}$ es ciclotómica, es decir, está contenida en un campo de números ciclotómico. En este caso, se encontraron las "p - componentes" explícitamente para $p \geq 3$ de-

pendiendo sólo de su grado sobre $\mathbb{Q}$. El caso $p = 2$ no depende sólo de su grado sobre $\mathbb{Q}$ ya que, para $n \geq 3$, el campo ciclotómico $\mathbb{Q}(\zeta_{2^n})$ no es cíclico. Damos un criterio para describir la 2-componente de $K_{\mathfrak{g}^+}$. Un resultado similar fue obtenido por M. Bhaskaran en [6] y por X. Zhang [64]. Finalmente, presentamos algunos resultados sobre el comportamiento del campo de géneros de una composición.

Resulta que el mismo enfoque funciona para las extensiones finitas y separables de $k = \mathbb{F}_q(T)$. En efecto, en el caso del campo numérico, el problema es más simple porque cualquier extensión abeliana finita de $\mathbb{Q}$ es ciclotómica. En el caso de campos de funciones, la máxima extensión abeliana de k consiste de tres componentes: una ciclotómica, una de constantes y una, también ciclotómica, donde el primo infinito es totalmente y salvajemente ramificado y es el único primo ramificado. En el segundo capítulo de esta tesis nos interesa describir, también utilizando la teoría de campos de clases, el campo de géneros extendido de una extensión separable finita de k. B. Anglès y J.-F. Jaulent en [1] establecieron la teoría general de campos de géneros extendidos de campos globales, tanto de funciones como numéricos. Nosotros usamos un concepto de campos de géneros extendido para campos de funciones diferente del definido por Anglès y Jaulent. Con este concepto, cuando describimos las extensiones abelianas finitas Ω de k, donde $K_{\mathfrak{g}^+} = K\Omega$, podemos escribir Ω como la composición de ciertas P-componentes, donde P corre a través de los primos finitos de k. Consideramos la P-componente $\Omega^{(P)}$ como la composición de $E^{(P)}$, la P-componente de la proyección E de Ω en un campo de funciones ciclotómico dado por el módulo de Carlitz, y un campo S que codifica el comportamiento del primo infinito. Más precisamente, S codifica la ramificación salvaje y la inercia del primo infinito de k. Para este fin necesitamos considerar el grupo de idèles correspondiente a un campo de funciones ciclotómico arbitrario.

En el tercer capítulo se buscan las extensiones abelianas imaginarias de un campo de funciones racionales con número de clases de ideales igual a uno. El concepto de número de clases de ideales para campos numéricos también tiene su origen en las *Disquisitiones Arithmeticae* [15] de Gauss (1801), quien lo estudió desde el punto de vista de formas cuadráticas. Este concepto tiene un análogo para extensiones de campos de funciones K/k, donde $k = \mathbb{F}_q(x)$ con x trascendente sobre $\mathbb{F}_q$. Una expresión que relaciona el número de clases de ideales con el número de clases de divisores es la fórmula de Schmidt $h_S r_S = h_K \delta_S$, donde S es el conjunto de primos de K que están arriba del primo infinito $\mathfrak{p}_\infty$, h_S es el número de clases de ideales, h_K es el número de clases de divisores, δ_S es el máximo común divisor de los grados de los primos en S y r_S es el regulador.

En el caso de una extensión cuadrática, R. E. MacRae [28], mostró que bajo isomorfismo hay cuatro extensiones algebraicas con número de clases de divisores uno, género no cero y donde hay

un primo de grado uno.

J. R. Leitzel, M. Madan y C. Queen [26] obtuvieron que hay siete campos de funciones de género no cero con número de clases de divisores uno, clasificaron los campos de funciones congruentes con número de clases de divisores 2 y probaron que hay ocho campos de funciones cuadráticos imaginarios K para los que la cerradura entera de $k[x]$ en K tiene número de clases de divisores 2.

En 1974 D. R. Hayes construyó la máxima extensión abeliana de k desarrollando una idea de L. Carlitz para definir campos de funciones ciclotómicos. M. Kida y N. Murabayashi [21] determinaron los campos de funciones ciclotómicos y los subcampos reales maximales con número de clases de divisores uno.

S. Bae y P.-L. Kang [3] determinaron todos los campos de funciones ciclotómicos con número de clases de divisores relativo igual a uno para q impar.

El problema del número de clases de ideales uno para campos de números ciclotómicos fue resuelto por J. M. Masley y H. L. Montgomery [33] y K. Yamamura [61] determinó todas las extensiones abelianas imaginarias de campos numéricos con número de clases de ideales uno; hay 172 campos de números abelianos imaginarios con número de clases uno.

S. Sémirat [53] determinó todas las extensiones imaginarias finitas separables K/k cuyo orden máximo es un dominio de ideales principales en el caso de que K/k sea una extensión cíclica de género no cero y de grado la potencia de un primo. Hay 42 de tales extensiones. En [54] determinó todos los campos de funciones ciclotómicos con número de clases de ideales uno. Aparte de las de género cero, hay 17 soluciones bajo $\mathbb{F}_q(x)$-isomorfismo, 13 de ellas están definidas sobre $\mathbb{F}_3$ y las 4 restantes están definidas sobre $\mathbb{F}_4$.

D. Le Brigand [25] clasificó todos los campos de funciones algebraicas con número de clases de divisores dos y dio todas las soluciones no cuadráticas. El resultado es que hay ocho campos de funciones algebraicas no cuadráticos de una variable con número de clases de divisores dos. En [24] ella dio todas las extensiones cuadráticas reales del campo de funciones racionales en característica dos. También presentó una aproximación geométrica del algoritmo de expansión de fracciones continuas para calcular el regulador.

H. Jung y J. Ahn [19] determinaron todas las extensiones abelianas de campos de funciones racionales que tienen número de clases de divisores uno y también todas las extensiones abelianas imaginarias con número de clases de divisores relativo uno. En este artículo se sugiere determinar todas las extensiones abelianas imaginarias con número de clases de ideales uno.

A. Picone [42] determinó todos los campos de funciones para los que el número de clases de divisores es tres y mostró que bajo isomorfismo hay sólo 8 de tales campos de funciones. Para $q = 2$ el problema se resolvió bajo la hipótesis adicional de que el campo de funciones es cuadrático.

M. Bilhan, D. Buyruk y F. Özbudak [7] dieron la lista completa de todos los campos de funciones sobre un campo finito con número de clases tres, salvo isomorfismo.

P. Mercuri y C. Stirpe [34] probaron que hay exactamente ocho campos de funciones sobre campos finitos, salvo isomorfismo, con número de clases de divisores uno y género mayor que cero.

Una extensión abeliana imaginaria se define como una extensión finita K/k que está contenida en algún campo de funciones ciclotómico, digamos con conductor N, y tal que si $K^+ = K \cap k(\Lambda_N)^+$ es su máximo subcampo real maximal, entonces $\mathrm{Gal}(K/K^+)$ es no trivial.

Teniendo como base el trabajo de Le Brigand se esperaba encontrar una expresión para el regulador con el fin de encontrar las extensiones abelianas imaginarias con número de clases de ideales $h_S = 1$. Para una extensión abeliana imaginaria se tiene que el grado de los primos en S es 1, luego $h_S r_S = h_K$. Así, si el número de clases de divisores h_K es 1, entonces el número de clases de ideales h_S es 1. El recíproco no es cierto, esto es, si $h_S = 1$, entonces no necesariamente $h_K = 1$. Con la idea de usar h_K conocido y aplicar la fórmula de Schmidt, usamos [34, 7, 42], pero al querer usar las fórmulas del *regulador relativo* r_S^-, notamos que éste puede ser muy grande, pues por ejemplo para el ciclotómico $\mathbb{F}_3(\Lambda_{x^2+1})$, $r_S^- = 2^{12}$. Así que no se pudo encontrar una fórmula que nos diera el valor del regulador. Por ello se decidió analizar diferentes tipos de extensiones usando otros criterios para tratar de encontrar el valor de h_S.

Un resultado general que se tiene es que si $q > 2$, entonces toda extensión ciclotómica es una extensión abeliana imaginaria. De [54], tenemos la clasificación de todas las extensiones ciclotómicas con $h_S = 1$.

Respecto a las p-extensiones abelianas, se tiene que ninguna es una extensión abeliana imaginaria. Se obtuvo que si K/k es una extensión abeliana imaginaria, su campo de géneros $K_{\mathfrak{g}^+}$ también lo es.

Con ayuda de los resultados de [41, 30, 31] referentes a cuál es el campo de géneros de una extensión de Kummer, presentamos extensiones de Kummer de grado primo ℓ y grado ℓ^n. Para las primeras, por [28, 34] hay sólo dos extensiones que son abelianas imaginarias. Para el caso particular de las extensiones cuadráticas, si el género es 1, sólo hay una extensión que es abeliana imaginaria, y si el género es 0, hay muchas extensiones. Para las extensiones de Kummer de grado ℓ^n, la solución se puede encontrar en [53].

Finalmente, es importante mencionar que en el estudio de algunos ejemplos concretos, como el de la Observación 1.2.11, resultaron de gran ayuda las plataformas SAGE y MAGMA.

Capítulo 1

Campos de géneros de campos numéricos

En este capítulo se estudian grupos procíclicos, conjugación compleja, campos numéricos ciclotómicos (para los que se estudian los subcampos de $\mathbb{Q}(\zeta_{2^{n+2}})$ de grado 2^n), caracteres de Dirichlet, campos locales y teoría de campos de clases local y global (se obtienen los grupos de idèles correspondientes a $\mathbb{Q}(\zeta_n)$ y $k(\Lambda_N)$ en los Teoremas 1.1.60 y 1.1.62, respectivamente. Se estudian diversas relaciones entre los campos de clases de Hilbert y de Hilbert extendido y de campos de géneros y de géneros extendido. Todo esto con el fin de presentar el campo de géneros extendido de un campo numérico (Teorema 1.3.2).

1.1. Preliminares

1.1.1. Grupos finitos

Denotaremos por C_n al grupo cíclico con n elementos. Observamos $C_n \cong \mathbb{Z}/n\mathbb{Z}$.

Lema 1.1.1. *Sean G un grupo abeliano finito y G_1, G_2, H subgrupos de G con $|H| = 2$. Entonces*

$$[G_1H \cap G_2H : (G_1 \cap G_2)H] \mid 2.$$

Demostración. Observemos primero que $(G_1 \cap G_2)H \subseteq G_1H \cap G_2H$. Tenemos

$$|G_1H \cap G_2H| = \frac{|G_1H|\,|G_2H|}{|G_1G_2H|} = \frac{\frac{|G_1||H|}{|G_1\cap H|}\frac{|G_2||H|}{|G_2\cap H|}}{\frac{|G_1G_2||H|}{|G_1G_2\cap H|}} = \frac{\frac{|G_1||G_2||H|^2}{|G_1\cap H||G_2\cap H|}}{\frac{|G_1||G_2|}{|G_1\cap G_2|}\frac{|H|}{|G_1G_2\cap H|}} = \frac{|G_1 \cap G_2|\,|G_1G_2 \cap H|}{|G_1 \cap H|\,|G_2 \cap H|}\,|H|$$

y $|(G_1 \cap G_2)H| = \frac{|G_1\cap G_2||H|}{|G_1\cap G_2\cap H|}$. Luego

$\alpha = [G_1H \cap G_2H : (G_1 \cap G_2)H] = \frac{|G_1H \cap G_2H|}{|(G_1 \cap G_2)H|} = \frac{|G_1 \cap G_2||G_1G_2 \cap H||H|}{|G_1 \cap H||G_2 \cap H|} \frac{|G_1 \cap G_2 \cap H|}{|G_1 \cap G_2||H|} = \frac{|G_1G_2 \cap H||G_1 \cap G_2 \cap H|}{|G_1 \cap H||G_2 \cap H|}$.

Como $|H| = 2$, los órdenes de los grupos en la expresión anterior son 1 o 2 y puesto que $\alpha \in \mathbb{N}$, necesariamente $\alpha \mid 2$.

□

Lema 1.1.2. *Sea G un grupo cíclico finito.*

1. *Si $H < G$, entonces H es cíclico.*
2. *Para cada divisor t de $|G|$, existe un único subgrupo de orden t.*
3. *Sean H_1, H_2 subgrupos de G. Entonces $H_1 < H_2$ si y sólo si $|H_1| \Big| |H_2|$ si y sólo si $[G : H_2] \Big| [G : H_1]$.*
4. *Sean H_1, H_2 subgrupos de G. Entonces $H_1 = H_2$ si y sólo si $|H_1| = |H_2|$ si y sólo si $[G : H_2] = [G : H_1]$.*

Demostración. Para 1 y 2 ver [9, Proposición 5, (1) y (3), pág. 57].

Sean $n = |G|$, $n_1 = |H_1|$ y $n_2 = |H_2|$. Entonces $[G : H_2] = \frac{n}{n_2}$ y $[G : H_1] = \frac{n}{n_1}$.

Tenemos $|H_1| \Big| |H_2|$ si y sólo si $n_1 \mid n_2$ si y sólo si $n_2 = n_1 \cdot t$, con $t \in \mathbb{N}$ si y sólo si $\frac{n}{n_2} = \frac{n}{n_1 \cdot t}$, con $t \in \mathbb{N}$ si y sólo si $[G : H_2] \cdot t = [G : H_1]$, con $t \in \mathbb{N}$ si y sólo si $[G : H_2] \Big| [G : H_1]$.

Por el Teorema de Lagrange $H_1 < H_2$ implica que $|H_1| \Big| |H_2|$. Supongamos ahora que $G = \langle \sigma \rangle$. Entonces $H_i = \left\langle \sigma^{\frac{n}{n_i}} \right\rangle$, con $i \in \{1, 2\}$. Tenemos que si $|H_1| \Big| |H_2|$, entonces $n_1 \mid n_2$, es decir, $n_2 = n_1 \cdot t$, con $t \in \mathbb{N}$. Luego $\sigma^{\frac{n}{n_1}} = \sigma^{\frac{n}{n_2 \cdot t}} \in \left\langle \sigma^{\frac{n}{n_2}} \right\rangle$, lo cual implica que $H_1 \subseteq H_2$. Por lo tanto $H_1 < H_2$ si y sólo si $|H_1| \Big| |H_2|$.

El punto 4 se sigue del 2 o del 3. □

Lema 1.1.3. *Sean G un grupo cíclico finito y H_1, H_2 subgrupos de G. Entonces*

$$[G : H_1 \cap H_2] = \operatorname{mcm}([G : H_1], [G : H_2]) \ y \ [G : H_1H_2] = \operatorname{mcd}([G : H_1], [G : H_2]).$$

Demostración. Sean $n = |G|$ y $G = \langle \sigma \rangle = \left\langle \sigma^0, \sigma^1, \ldots, \sigma^{n-1} \right\rangle$. Sea $a_i = \min\{x \mid 1 \leq x \leq n, \sigma^x \in H_i\}$. Entonces $H_i = \langle \sigma^{a_i} \rangle = \left\{ \sigma^0, \sigma^{a_i}, \ldots, \sigma^{\left(\frac{n}{a_i} - 1\right)a_i} \right\}$, con $a_i \mid n$ y $|H_i| = \frac{n}{a_i}$ y $[G : H_i] = a_i$ para $i \in \{1, 2\}$. Sean $a = \operatorname{mcm}[a_1, a_2]$ y $H = \langle \sigma^a \rangle$. Entonces $|H| = \frac{n}{a}$ y $[G : H] = a$. Como $a_i \mid a$, por el Lema 1.1.2, $H \subseteq H_i$, con $i \in \{1, 2\}$. Luego $H \subseteq H_1 \cap H_2$. Tenemos $H_1 \cap H_2 = \left\langle \sigma^b \right\rangle$, donde b es mínimo. Entonces $[G : H_1 \cap H_2] = b$. Como $H_1 \cap H_2 \subseteq H_i$, para $i \in \{1, 2\}$, por el Lema 1.1.2, $a_i \mid b$. Por lo

tanto $a \mid b$ y nuevamente por el Lema 1.1.2, $H_1 \cap H_2 \subseteq H$. Concluimos que $H = H_1 \cap H_2$, de donde $[G : H_1 \cap H_2] = a = \operatorname{mcm}([G : H_1], [G : H_2])$. Luego

$$\begin{aligned}[G : H_1H_2] &= \frac{|G|}{|H_1H_2|} = \frac{|G|}{|H_1||H_2| / |H_1 \cap H_2|} = \frac{|G|}{|H_1|}\frac{|G|}{|H_2|}\frac{|H_1 \cap H_2|}{|G|} \\ &= \frac{[G : H_1][G : H_2]}{[G : H_1 \cap H_2]} = \frac{[G : H_1][G : H_2]}{\operatorname{mcm}([G : H_1], [G : H_2])} = \operatorname{mcd}([G : H_1], [G : H_2]).\end{aligned}$$

□

Por inducción obtenemos el siguiente resultado.

Lema 1.1.4. *Sean G un grupo cíclico finito y $H_1, \ldots, H_n$ subgrupos de G. Entonces*

$$[G : H_1 \cdots H_n] = \operatorname*{mcd}_{1 \le i \le n}([G : H_i]).$$

Lema 1.1.5. *Tenemos*

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z} & si\ p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z} & si\ p = 2, \end{cases}$$

donde p es un número primo.

Demostración. Véase [18, Ejercicio 7]. □

1.1.2. Grupos procíclicos

Las siguientes definiciones y propiedades fueron tomadas de [35] y [45].

Definición 1.1.6. Un *grupo profinito* es un grupo topológico G que es Hausdorff y compacto y tiene una base de vecindades abiertas de la identidad de G que consiste de subgrupos normales.

Ejemplo 1.1.7. Los grupos finitos con la topología discreta son grupos profinitos.

Definición 1.1.8.

1. Un *conjunto dirigido* es un conjunto ordenado I con la propiedad de que para cada $i, i' \in I$ existe $i'' \in I$ con $i, i' \le i''$.

2. Un *sistema proyectivo* de conjuntos (grupos, anillos, etc.) sobre I es una familia $\{G_i, f_{ij} \mid i, j \in I, i \le j\}$ de conjuntos (grupos, anillos, etc.), G_i y mapeos (homomorfismos) $f_{ij} : G_j \to G_i$ tales que $f_{ik} = f_{ij} \circ f_{jk}$, con $i \le j \le k$.

3. El *límite proyectivo (inverso)*, $G = \varprojlim_{i\in I} G_i$ del sistema proyectivo $\{G_i, f_{ij} \mid i, j \in I, i \leq j\}$ se define como el conjunto (grupo, anillo, etc.)

$$G = \left\{ \prod_{i\in I} \sigma_i \in \prod_{i\in I} G_i \mid f_{ij}(\sigma_j) = \sigma_i \text{ si } i \leq j \right\}.$$

Observación 1.1.9. Si los G_i son espacios topológicos y los f_{ij} son mapeos continuos, entonces G es un subespacio cerrado del espacio topológico $\prod_{i\in I} G_i$.

Proposición 1.1.10. *Si G es un grupo profinito y si N corre sobre todos los subgrupos normales, entonces (topológicamente y algebraicamente) $G \cong \varprojlim_N G/N$. Inversamente, si $\left\{G_i, f_{ij}\right\}$ es un sistema proyectivo de grupos finitos G_i, entonces $G = \varprojlim_i G_i$ es un grupo profinito.*

Demostración. Véase [35]. □

Definición 1.1.11. Un *grupo procíclico* es un límite inverso de grupos cíclicos finitos.

Observación 1.1.12. Equivalentemente, un grupo procíclico es un grupo profinito G que es generado topológicamente por un elemento $\sigma \in G$, es decir, G es la cerradura del subgrupo $\langle\sigma\rangle = \left\{\sigma^k \mid k \in \mathbb{Z}\right\}$.

Ejemplo 1.1.13. Si p es un número primo, los anillos $\mathbb{Z}/p^n\mathbb{Z}$, con $n \in \mathbb{N}$, forman un sistema proyectivo con respecto a las proyecciones canónicas $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$, con $n \geq m$. El límite inverso

$$\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

es el *anillo de enteros p-ádicos* y es un grupo procíclico.

Dotamos a cada $\mathbb{Z}/p^n\mathbb{Z}$ con la topología discreta y $\prod_n(\mathbb{Z}/p^n\mathbb{Z})$ por la topología producto. Por el Teorema de Tychonoff este producto es compacto; bajo la restricción $\mathbb{Z}_p$ es compacto, pues $\mathbb{Z}_p$ es cerrado en $\prod_n(\mathbb{Z}/p^n\mathbb{Z})$. El homomorfismo de anillos $\mathbb{Z} \to \prod_n(\mathbb{Z}/p^n\mathbb{Z})$ que lleva a cada elemento a su reducción módulo $p^n\mathbb{Z}$ nos permite ver a $\mathbb{Z}_p$ como la cerradura de $\mathbb{Z} = \langle 1\rangle$ en el producto $\prod_n(\mathbb{Z}/p^n\mathbb{Z})$.

Proposición 1.1.14. *Los subgrupos abiertos de un grupo procíclico G son los grupos nG, con $n \in \mathbb{N}$ (puede ser que $nG = mG$ para $n \neq m$, por ejemplo, $n\mathbb{Z}_p = \mathbb{Z}_p$ para $(n, p) = 1$). De hecho nG es cerrado de índice finito.*

Demostración. Véase [35, Ejemplo 4, pág. 6]. □

Proposición 1.1.15. *Sean p un número primo y n un número natural.*

1. *El grupo $\mathbb{Z}_p$ tiene un único subgrupo cerrado H de índice p^n. Además,*

$$H = p^n\mathbb{Z}_p \cong \mathbb{Z}_p.$$

2. *Cada grupo procíclico de orden p^n aparece como un cociente de $\mathbb{Z}_p$ en una forma única.*

3. *$\mathbb{Z}_p$ no puede escribirse como producto directo de subgrupos no triviales.*

Demostración. Véase [45, Proposición 2.7.1] □

Proposición 1.1.16. *Tenemos*

$$\mathbb{Z}_p^* = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p & si\ p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 & si\ p = 2. \end{cases}$$

Demostración. Usando el Lema 1.1.5, tenemos

$$\mathbb{Z}_p^* = \varprojlim_n (\mathbb{Z}\ p^n\mathbb{Z})^* = \begin{cases} \varprojlim \left(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{n-1}\mathbb{Z}\right) & \text{si } p > 2 \\ \varprojlim \left(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}\right) & \text{si } p = 2 \end{cases}$$

$$= \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \varprojlim \mathbb{Z}_p/p^{n-1}\mathbb{Z} & p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \varprojlim \mathbb{Z}/2^{n-2}\mathbb{Z} & p = 2 \end{cases} = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p & \text{si } p > 2 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 & \text{si } p = 2 \end{cases}$$

□

Como consecuencia tenemos el siguiente resultado.

Corolario 1.1.17. *Para p un número primo:*

1. *$\mathbb{Z}_p^* \cong C_{p-1} \times \mathbb{Z}_p$, si p es impar.*

2. *$\mathbb{Z}_2^* \cong C_2 \times \mathbb{Z}_2 \cong \{\pm 1\} \times \mathbb{Z}_2$.*

Lema 1.1.18. *Sean p un número primo impar, H_1 y H_2 subgrupos cerrados de $\mathbb{Z}_p^*$ con $\left[\mathbb{Z}_p^* : H_i\right] < \infty$ para $i = 1, 2$. Entonces $\left[\mathbb{Z}_p^* : H_1H_2\right] = \text{mcd}\left(\left[\mathbb{Z}_p^* : H_1\right], \left[\mathbb{Z}_p^* : H_2\right]\right)$.*

Demostración. Tenemos que $\mathbb{Z}_p^* \cong C_{p-1} \times \mathbb{Z}_p$, $C_{p-1} = \langle \sigma \rangle$, $H_i = \langle \sigma^{a_i} \rangle \times p^{n_i}\mathbb{Z}_p$, con $n_i \in \mathbb{N} \cup \{0\}$ y $a_i \mid p-1$.

Sea $A = p^{n_1}\mathbb{Z}_p + p^{n_2}\mathbb{Z}_p = \left\{p^{n_1}\alpha_1 + p^{n_2}\alpha_2 \mid \alpha_1, \alpha_2 \in \mathbb{Z}_p\right\}$. Observemos que si $m = \min\{n_1, n_2\}$, entonces $p^m \in A$, luego $p^m\mathbb{Z}_p \subseteq A$. Por otro lado, si $\xi \in A$, entonces $\xi = p^{n_1}\alpha_1 + p^{n_2}\alpha_2 = p^m\left(p^{n_1-m}\alpha_1 + p^{n_2-m}\alpha_2\right) \in p^m\mathbb{Z}_p$. Luego $A = p^m\mathbb{Z}_p$. Tenemos que $\left[\mathbb{Z}_p^* : H_i\right] = a_i p^{n_i}$. Entonces por el Lema 1.1.3, $\left[\mathbb{Z}_p^* : H_1H_2\right] = \operatorname{mcd}(a_1, a_2)\, p^m = \operatorname{mcd}\left(a_1p^{n_1}, a_2p^{n_2}\right) = \operatorname{mcd}\left(\left[\mathbb{Z}_p^* : H_1\right], \left[\mathbb{Z}_p^* : H_2\right]\right)$.

□

Observación 1.1.19. Como consecuencia del lema, tenemos que para p primo impar y $n \in \mathbb{N}$, $\mathbb{Z}_p^*$ tiene un único subgrupo cerrado de índice p^n.

En el siguiente ejemplo se muestra que para $p = 2$ no se cumple el lema anterior.

Ejemplo 1.1.20. En $G = C_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_2^*$ tenemos los subgrupos $H_1 = 2\mathbb{Z}_2$ y $H_2 = C_2 \times 4\mathbb{Z}_2$ tales que $G/H_1 = \frac{C_2\times\mathbb{Z}_2}{2\mathbb{Z}_2} = C_2 \times C_2$ y $G/H_2 = \frac{C_2\times\mathbb{Z}_2}{C_2\times 4\mathbb{Z}_2} = C_4$, por lo que $[G : H_1] = [G : H_2] = 4$, pero $H_1H_2 = C_2 \times 2\mathbb{Z}_2$ por lo que $G/(H_1H_2) = \frac{C_2\times\mathbb{Z}_2}{C_2\times 2\mathbb{Z}_2} \cong C_2$, luego $[G : H_1H_2] = 2 < 4 = \operatorname{mcd}_{1\le i\le 2}[G : H_i]$.

Sea $n \in \mathbb{N}$ y sea $G := \{\pm 1\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2^*$. Consideremos $-1 \in \{\pm 1\}$ y $1 \in \mathbb{Z}_2$, aquí 1 es generador topológico del grupo aditivo $\mathbb{Z}_2$, es decir $\mathbb{Z}_2 = \overline{\langle 1 \rangle}$. Sean $a = (-1, 0)$ y $b = (1, 1) \in G$. Entonces $G = \overline{\langle a, b \rangle}$. A continuación estudiamos los subgrupos cerrados de índice 2^n de G. Sean $\mathcal{A}_n := \{\pm 1\} \times 2^n\mathbb{Z}_2$; $\mathcal{B}_n := 2^{n-1}\mathbb{Z}_2$ y $\mathcal{E}_n := \{\pm 1\}\, 2^{n-1}\mathbb{Z}_2$. Tenemos el siguiente resultado.

Proposición 1.1.21. *Con la notación anterior, los subgrupos cerrados de índice 2^n de G son $\mathcal{A}_n \cong \overline{\langle a, b^{2^n} \rangle}$, $\mathcal{B}_n \cong \overline{\left\langle b^{2^{n-1}} \right\rangle}$ y $\mathcal{E}_n \cong H$, donde $H = \overline{\left\langle a \cdot b^{2^{n-1}} \right\rangle}$ es el grupo procíclico con generador topológico $a \cdot b^{2^{n-1}}$. Los grupos cocientes correspondientes son*

$$\frac{G}{\mathcal{A}_n} = \frac{\overline{\langle a,b\rangle}}{\overline{\left\langle a,b^{2^n}\right\rangle}} = \left\langle b \mod b^{2^n} \right\rangle \cong C_{2^n}.$$

$$\frac{G}{\mathcal{B}_n} = \frac{\{\pm 1\}\times\mathbb{Z}_2}{2^{n-1}\mathbb{Z}_2} = \left\langle a, b \mod b^{2^{n-1}} \right\rangle \cong C_2 \times C_{2^{n-1}}.$$

$$\frac{G}{\mathcal{E}_n} = \frac{\overline{\langle a,b\rangle}}{\overline{\left\langle ab^{2^{n-1}}\right\rangle}} = \langle b \mod H \rangle \cong C_{2^n}.$$

Demostración. Basta verificar que $G/\mathcal{E}_n$ es cíclico de orden 2^n. Los demás casos son claros. Sean $\widetilde{a}$ y $\widetilde{b}$ las clases de a y b módulo H, respectivamente. $\widetilde{a} = a \mod H$, $\widetilde{b} = b \mod H$. Se tiene $G/\mathcal{E}_n = \left\langle \widetilde{a}, \widetilde{b} \right\rangle$. Puesto que $ab^{2^{n-1}} \in H$, $\widetilde{b}^{2^{n-1}} = \widetilde{a}^{-1}$ y $\widetilde{a}^{-1} = \widetilde{a}$, $\widetilde{a} = \widetilde{b}^{2^{n-1}}$. Luego $G/\mathcal{E}_n = \left\langle \widetilde{b} \right\rangle$ y así $G/\mathcal{E}_n$ es cíclico. Notemos que $b^{2^{n-1}} \notin H$ pues si $b^{2^{n-1}} \in H$, entonces $a \in H$, lo cual no es posible pues a es de torsión y H no tiene elementos de torsión. Luego $b^{2^{n-1}} \notin H$. Por otro lado, $b^{2^n} = b^{2^{n-1}}b^{2^{n-1}} \equiv a^{-1}b^{2^{n-1}} \equiv ab^{2^{n-1}} \mod H$, luego $b^{2^n} \in H$ y así $\circ\left(\widetilde{b}\right) = 2^n$. Obtenemos que $G/\mathcal{E}_n$ es cíclico de orden 2^n. □

Observación 1.1.22. Notemos que $-1 \in \mathcal{A}_n$, mientras que $-1 \notin \mathcal{B}_n$ y $-1 \notin \mathcal{E}_n$.

1.1.3. Conjugación compleja

Sea $L/\mathbb{Q}$ una extensión finita de Galois. Entonces para todo $\sigma \in G = \mathrm{Gal}(L/\mathbb{Q})$, $\sigma(L) = L$. Luego L es totalmente real ($\sigma(L) \subseteq \mathbb{R}$ para todo σ encaje de L en $\bar{\mathbb{Q}}$) o totalmente imaginario ($\sigma(L) \nsubseteq \mathbb{R}$ para todo σ encaje de L en $\bar{\mathbb{Q}}$).

Sea $J : \mathbb{C} \to \mathbb{C}$ la conjugación compleja, es decir, $a + bi \mapsto a - bi$ con $a, b \in \mathbb{R}$. Tenemos $J|_L \in G$. Tenemos $\circ(J|_L) \in \{1, 2\}$. Consideremos L^J el campo fijo bajo $J|_L$. Se tiene

$$\mathrm{Gal}(L/L^J) = \langle J|_L \rangle \text{ y } \left|\mathrm{Gal}(L/L^J)\right| 2.$$

Observación 1.1.23.

Tenemos $L^J \subseteq \mathbb{R}$, de hecho $L^J = L \cap \mathbb{R}$. Si $L/\mathbb{Q}$ es abeliana y $L \subseteq \mathbb{Q}(\zeta_n)$, entonces $L^J = L^+ = L \cap \mathbb{Q}(\zeta_n)^+$.

Sean F y L extensiones de Galois de $\mathbb{Q}$ con $F \subseteq L$. Entonces $F^J \subseteq L^J$.

Ejemplo 1.1.24. Sea $L = \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. Tenemos que $L/\mathbb{Q}$ es de Galois con $\mathrm{Gal}(L/\mathbb{Q}) = \langle \alpha, \beta \rangle = C_2 \ltimes C_3 \cong S_3$ y notemos que L es totalmente imaginario. Sin embargo, $L^J = \mathbb{Q}\left(\sqrt[3]{2}\right)$ no es de Galois y no es ni totalmente real ni totalmente imaginaria.

$$\begin{array}{ccc} L^J = \mathbb{Q}\left(\sqrt[3]{2}\right) & \xrightarrow[\langle\alpha\rangle]{C_2} & \mathbb{Q}\left(\zeta_3, \sqrt[3]{2}\right) = L \\ \Big| & & \Big| \\ & & \langle\beta\rangle \Big| C_3 \\ \Big| & & \Big| \\ \mathbb{Q} & \xrightarrow[2]{} & \mathbb{Q}(\zeta_3) \end{array}$$

Los encajes de L^J están dados por

$$\sqrt[3]{2} \mapsto \begin{cases} \sqrt[3]{2} \\ \omega\sqrt[3]{2} \\ \omega^2\sqrt[3]{2}, \end{cases}$$

donde $\omega = \zeta_3$.

Si $L/\mathbb{Q}$ es abeliana, entonces $\langle J|_L \rangle \lhd G$ y por tanto $L^J/\mathbb{Q}$ también es de Galois, de hecho es abeliana y además es totalmente real.

Observación 1.1.25.

1. Si $L/\mathbb{Q}$ es una extensión abeliana y $L^J \subsetneq L$, entonces en L/L^J se ramifican los primos infinitos.

2. Si $L/\mathbb{Q}$ es una extensión de Galois, $F \subsetneq L$, $F/\mathbb{Q}$ también es de Galois y en L/F se ramifican los primos infinitos, entonces $F \subseteq L^J$. En efecto, como hay ramificación de los primos infinitos, se tiene $F \subseteq \mathbb{R}$, luego $F \subseteq \mathbb{R} \cap L = L^J$.

1.1.4. Campos numéricos ciclotómicos

Consideramos [50] y [62] para el desarrollo de campos numéricos ciclotómicos.

Definición 1.1.26. Se define ζ_n por $\zeta_n = \exp\left(\frac{2\pi i}{n}\right)$.

Definición 1.1.27. [50, Definición 3.2.1] Un *campo ciclotómico* $\mathbb{Q}(\zeta_n)$ es la extensión del campo de los números racionales $\mathbb{Q}$ que contiene a todas las raíces primitivas n-ésimas del polinomio $x^n - 1$, donde $n \in \mathbb{N}$.

Observación 1.1.28.

- La extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión finita de Galois.

- Sea $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. Si $\sigma \in G_n$, entonces $\sigma(\zeta_n) = \zeta_n^a$ para algún $a \in \mathbb{N}$ con $\mathrm{mcd}(a, n) = 1$. El grupo de unidades de $\mathbb{Z}/n\mathbb{Z}$ es $U_n = \{t \text{ mód } n \in \mathbb{Z}/n\mathbb{Z} \mid t \in \mathbb{Z} \text{ y } \mathrm{mcd}(t, n) = 1\}$. La función $\varphi : G_n \to U_n$, $\varphi(\sigma_a) = a$ mód n es un monomorfismo de grupos. En particular G_n es un grupo abeliano. De hecho φ es un isomorfismo.

Definición 1.1.29. Sea $x^n - 1 \in \mathbb{Q}[x]$. Las raíces del polinomio $x^n - 1 = 0$ están dadas por $\left\{\zeta_n^j\right\}_{j=0}^{n-1}$, donde $\zeta_n = e^{2\pi i/n}$. El polinomio mínimo de ζ_n es el *polinomio ciclotómico*

$$\Phi_n(x) = \prod_{\substack{i=1 \\ \mathrm{mcd}(i,n)=1}}^{n-1} \left(x - \zeta_n^i\right) \in \mathbb{Z}[x].$$

Se tienen los siguientes resultados para campos ciclotómicos.

Proposición 1.1.30. *Para $n \in \mathbb{N}$ se tiene*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Demostración. [50, Proposición 3.2.3] □

Definición 1.1.31. El *subcampo real maximal* es $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$. Si $K \subseteq \mathbb{Q}(\zeta_n)$, definimos el *subcampo real maximal de K* por

$$K^+ := K \cap \mathbb{Q}(\zeta_n)^+ .$$

Sea p un número primo. Estudiemos las subextensiones del campo ciclotómico $\mathbb{Q}\left(\zeta_{p^m}\right)$.

- Caso $p \neq 2$.

La extensión $\mathbb{Q}\left(\zeta_{p^m}\right)/\mathbb{Q}$ es cíclica de orden $\varphi(p^m) = p^{m-1}(p-1)$.

Proposición 1.1.32. *Con la condición $p \neq 2$ supongamos $L_1, \ldots, L_n \subseteq \mathbb{Q}\left(\zeta_{p^m}\right)$. Entonces*

$$\left[\bigcap_{i=1}^{n} L_i : \mathbb{Q}\right] = \operatorname*{mcd}_{1\leq i\leq n}([L_i : \mathbb{Q}]) .$$

Demostración. Sean $L = \prod_{i=1}^{n} L_i$, $G := \operatorname{Gal}(\bigcap_{i=1}^{n} L_i : \mathbb{Q})$ y $H_i = \operatorname{Gal}(L/L_i)$ para $1 \leq i \leq n$. Entonces $\prod_{i=1}^{n} H_i = \operatorname{Gal}(L/\bigcap_{i=1}^{n} L_i)$. Luego, por Teoría de Galois y el Lema 1.1.4, tenemos $[\bigcap_{i=1}^{n} L_i : \mathbb{Q}] = \left|\operatorname{Gal}(\bigcap_{i=1}^{n} L_i/\mathbb{Q})\right| = \frac{\left|\operatorname{Gal}(L/\mathbb{Q})\right|}{\left|\operatorname{Gal}\left(L/\bigcap_{i=1}^{n} L_i\right)\right|} = \frac{|G|}{\left|\prod_{i=1}^{n} H_i\right|} = \left[G : \prod_{i=1}^{n} H_i\right] = \operatorname*{mcd}_{1\leq i\leq n}([G : H_i]) = \operatorname*{mcd}_{1\leq i\leq n}([L_i : \mathbb{Q}])$. □

Como la extensión $\mathbb{Q}\left(\zeta_{p^m}\right)/\mathbb{Q}$ es cíclica de orden $\varphi(p^m) = p^{m-1}(p-1)$, por el Lema 1.1.2, para cada divisor t de $\varphi(p^m)$ existe un único subcampo $L_{p,t}$ de $\mathbb{Q}\left(\zeta_{p^m}\right)$ de grado t sobre $\mathbb{Q}$.

Como p es totalmente ramificado en $\mathbb{Q}\left(\zeta_{p^m}\right)/\mathbb{Q}$, $e_p\left(L_{p,t}/\mathbb{Q}\right) = \left[L_{p,t} : \mathbb{Q}\right] = t$.

Sea $t = p^{a_p} \cdot b_p$ con $0 \leq a_p \leq m-1$ y $b_p \mid p-1$. Entonces $L_{p.t} = T_{a_p} \cdot M_{b_p}$ con $\mathbb{Q} \subseteq T_{a_p}, M_{b_p} \subseteq L_{p,t}$. $\left[T_{a_p} : \mathbb{Q}\right] = p^{a_p}$ y $\left[M_{b_p} : \mathbb{Q}\right] = b_p$.

La extensión $L_{p,t}/\mathbb{Q}$ está caracterizada totalmente por su grado sobre $\mathbb{Q}$; $L_{p,t}$ es la única extensión cíclica de $\mathbb{Q}$ en la que p se ramifica totalmente y es el único primo ramificado. El conductor de $L_{p,t}$ es p^{a_p+1}. Con esto se tiene que $L_{p,t} \subseteq \mathbb{Q}\left(\zeta_{p^{a_p+1}}\right)$, pero $L_{p,t} \nsubseteq \mathbb{Q}\left(\zeta_{p^{a_p}}\right)$.

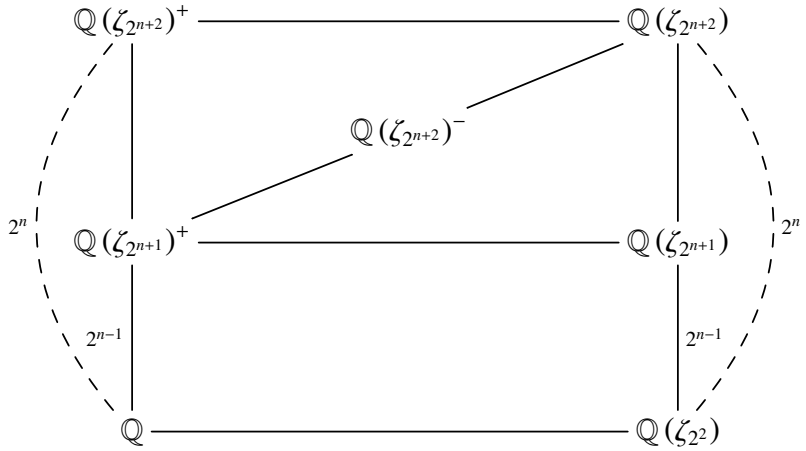
- Caso $p = 2$

En este caso la extensión $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$ en general no es cíclica, de hecho $\operatorname{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}) \cong C_2 \times C_{2^n}$, para $n \geq 1$ y $[\mathbb{Q}(\zeta_{2^{n+2}}) : \mathbb{Q}] = \varphi\left(2^{n+2}\right) = 2^{n+1}$.

Si $n = 0$ se tiene $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ y $\operatorname{Gal}(\mathbb{Q}(i)/\mathbb{Q}) \cong C_2$ y $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Observación 1.1.33. Para $p = 2$ no se cumple la Proposición 1.1.32. Por ejemplo, sean $L_1 = \mathbb{Q}\left(\sqrt{2}\right), L_2 = \mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_8)$. Tenemos $2 = [L_1 : \mathbb{Q}] = [L_2 : \mathbb{Q}] = \text{mcd}([L_1 : \mathbb{Q}], [L_2 : \mathbb{Q}])$, mientras que, como $L_1 \cap L_2 = \mathbb{Q}$, tenemos $[L_1 \cap L_2 : \mathbb{Q}] = 1$.

Cuando $n \geq 1$ hay 3 subcampos de $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$ de grado 2^n, el cual es igual al índice de ramificación de 2.



Estos subcampos son $\mathbb{Q}(\zeta_{2^{n+2}})^+ = \mathbb{Q}\left(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}\right)$, $\mathbb{Q}(\zeta_{2^{n+1}})$ y $\mathbb{Q}(\zeta_{2^{n+2}})^- := \mathbb{Q}\left(\zeta_{2^{n+2}} - \zeta_{2^{n+2}}^{-1}\right)$.

Observación 1.1.34. Con la notación de la Proposición 1.1.21, $G = \{\pm 1\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2^*$ y tomamos $-1 \in \{\pm 1\}$. Identificando la conjugación compleja J con -1, tenemos:

- $\text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})^+/\mathbb{Q}) \cong G/\mathcal{A}_n \cong C_{2^n}$ que es cíclico y con $-1 \in \mathcal{A}_n$.
- $\text{Gal}(\mathbb{Q}(\zeta_{2^{n+1}})/\mathbb{Q}) \cong G/\mathcal{B}_n \cong C_2 \times C_{2^{n-1}}$ que no es cíclico y con $-1 \notin \mathcal{B}_n$.
- $\text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})^-/\mathbb{Q}) \cong G/\mathcal{E}_n \cong C_{2^n}$ que es cíclico y con $-1 \notin \mathcal{E}_n$.

Por otro lado, puesto que $J \in \text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}(\zeta_{2^{n+2}})^+)$, tenemos que la extensión $\mathbb{Q}(\zeta_{2^{n+2}})^+/\mathbb{Q}$ es totalmente real. Como $J \notin \text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}(\zeta_{2^{n+1}})$ tenemos que la extensión $\mathbb{Q}(\zeta_{2^{n+1}})/\mathbb{Q}$ no es real. Finalmente, como $J \notin \text{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}(\zeta_{2^{n+2}})^-)$, la extensión $\mathbb{Q}(\zeta_{2^{n+2}})^-/\mathbb{Q}$ tampoco es real. Podemos visualizar esta información en la tabla 1.1.

Notemos que $\text{Irr}(\zeta_{2^{n+2}}, x, \mathbb{Q}(\zeta_{2^{n+1}})) = x^2 - \zeta_{2^{n+1}}$, $\text{Irr}(\zeta_{2^{n+2}}, x, \mathbb{Q}(\zeta_{2^{n+2}})^+) = x^2 - \alpha x + 1$, donde $\alpha = \zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}$ e $\text{Irr}(\zeta_{2^{n+2}}, x, \mathbb{Q}(\zeta_{2^{n+2}})^-) = x^2 - \beta x - 1$, donde $\beta = \zeta_{2^{n+2}} - \zeta_{2^{n+2}}^{-1}$.

	cíclica	real	conductor
$\mathbb{Q}(\zeta_{2^{n+2}})^+$	sí	sí	2^{n+2}
$\mathbb{Q}(\zeta_{2^{n+1}})$	no	no	2^{n+1}
$\mathbb{Q}(\zeta_{2^{n+2}})^-$	sí	no	2^{n+2}

Tabla 1.1: Análisis de los subcampos de $\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q}$ de grado 2^n

1.1.5. Caracteres de Dirichlet para campos numéricos

Presentamos las definiciones y los resultados básicos referentes a caracteres de Dirichlet. Las demostraciones pueden verse en [60, Capítulo 2].

Definición 1.1.35. Un *caracter de Dirichlet* es un homomorfismo multiplicativo $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$.

Si $n \mid m$, entonces χ induce un homomorfismo $\widetilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$ mediante la composición con el mapeo natural $\varphi_{m,n} : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$. Observamos que χ y $\widetilde{\chi}$ son prácticamente lo mismo. Así podemos considerar χ módulo n o módulo m.

Definición 1.1.36. El *conductor* de χ es el mínimo n tal que χ está definido módulo n. Se denota f_χ.

Observación 1.1.37. Los caracteres de Dirichlet se pueden pensar como caracteres de

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_n\right)/\mathbb{Q}\right) \cong \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

y se llaman *caracteres de Galois*.

Definición 1.1.38. Si $\chi(-1) = 1$ decimos que χ es *par* y si $\chi(-1) = -1$, entonces χ es *impar*.

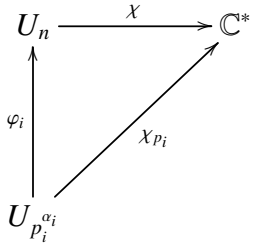
Definición 1.1.39. Sean X un grupo finito de caracteres de Dirichlet, $n := \mathrm{mcm}\{f_\chi \mid x \in X\}$, $H := \bigcap_{x\in X} \mathrm{nuc}\,\chi$ y $K := \mathbb{Q}\left(\zeta_n\right)^H$. Decimos que K es el *campo asociado* a X y si $X = \langle\chi\rangle$, decimos que K es el campo asociado a χ.

Proposición 1.1.40. *Sean X_1, X_2 grupos de caracteres de Dirichlet correspondientes a los campos K_i, $i = 1, 2$. Entonces*

- *$X_1 \subseteq X_2$ si y sólo si $K_1 \subseteq K_2$.*
- *El grupo generado por X_1 y X_2 corresponde a la composición K_1K_2.*

Demostración. Véase [50, Proposición 6.2.41]. □

De [30] tenemos la construcción de caracteres de Dirichlet. Dada $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ una factorización de n como producto de potencias de primos. Entonces para cualquier caracter χ sea $\chi_{p_i} = \chi \circ \varphi_i$, donde $\varphi_i = \phi^{-1} \circ g_{p_i}$, con $\phi : U_n \to \prod_{j=1}^{r} U_{p_j^{\alpha_j}}$, dado por a mód $n \mapsto (a \text{ mód } p_j^{\alpha_j})_j$ y $\chi_{p_i} : U_{p_i^{\alpha_i}} \to \prod_{j=1}^{r} U_{p_j^{\alpha_j}}$, dado por a mód $p_i^{\alpha_i} \mapsto (1, \ldots, a \text{ mód } p_i^{\alpha_i}, \ldots, 1)$.



Sea $n = \prod p^{\alpha}$, consideremos la descomposición $(\mathbb{Z}/n\mathbb{Z})^* \cong \prod (\mathbb{Z}/p^{\alpha}\mathbb{Z})^*$. Podemos escribir entonces un caracter de Dirichlet χ definido módulo n como $\chi = \prod \chi_p$, donde χ_p es un caracter definido mód p^{α}. Si X es un grupo de caracteres de Dirichlet, definimos

$$X_p := \left\{ \chi_p \mid \chi \in X \right\}.$$

Teorema 1.1.41. *Sean X un grupo de caracteres de Dirichlet y K el campo asociado. Sea p un número primo con índice de ramificación e sobre K. Entonces $e = \#\left(X_p\right)$.*

1.1.6. Campos locales

Sea K un campo local, esto es, K es, o bien un campo completo con respecto a una valuación discreta y con campo residual finito, o bien $\mathbb{R}$ o $\mathbb{C}$. Consideremos primero un campo local K que sea completo respecto a una valuación discreta y con campo residual finito. Denotamos por $\mathcal{O}_K$ al anillo de enteros de K. Entonces $\mathcal{O}_K$ es un anillo local con ideal maximal $\wp = (\pi)$ con $v_{\wp}(\pi) = 1$. Sea $A \subseteq \mathcal{O}_K$ un conjunto de representantes de $\mathcal{O}_K/\wp$. Entonces para cada $\alpha \in K^*$, tenemos $\alpha = \sum_{i=N}^{\infty} a_i \pi^i$, donde $a_i \in A$ para todo $i \geq N$ y $a_N \neq 0$ para algún $N \in \mathbb{Z}$. Sean $\mathcal{U}_{\wp}$ el grupo de unidades de $\mathcal{O}_K$ y $\mathcal{U}_{\wp}^{(1)} = \{\zeta \in \mathcal{U}_{\wp} \mid \zeta - 1 \in (\pi)\} = 1 + \pi\mathcal{O}_K = 1 + \wp$ el grupo de 1−unidades. En general, para $n \geq 1, \mathcal{U}_{\wp}^{(n)} = 1 + \wp^n$.

Proposición 1.1.42. *Tenemos $\mathcal{U}_{\wp} \cong \mathbb{F}_q^* \times \mathcal{U}_{\wp}^{(1)}$, donde $\mathbb{F}_q$ es el campo residual.*

Demostración. Sea $\alpha \in \mathcal{U}_\wp$, $\alpha = \sum_{i=0}^{\infty} a_i \pi^i$, $a_0 \in \mathbb{F}_q^*$, luego $\alpha = a_0 \underbrace{\left(1 + \sum_{i=1}^{\infty} a_i a_0^{-1} \pi^i\right)}_{\beta} = a_0 \beta$, con $a_0 \in \mathbb{F}_q^*$ y $\beta \in \mathcal{U}_\wp^{(1)}$. El isomorfismo está dado por $\rho : \mathcal{U}_\wp \to \mathbb{F}_q^* \times \mathcal{U}_\wp^{(1)}$, $\alpha \mapsto (a_0, \beta)$. □

Entonces

$$K^* \cong \mathcal{U}_\wp \times \langle \pi \rangle \cong \mathbb{F}_q^* \times \mathcal{U}_\wp^{(1)} \times \langle \pi \rangle.$$

Ejemplo 1.1.43. Si $K = \mathbb{Q}_p$ es el campo de los números p-ádicos, entonces tenemos $q = p$, $\mathbb{F}_q^* \cong C_{p-1} \cong \mathbb{Z}/(p-1)\mathbb{Z}$, $\mathcal{O}_K = \mathbb{Z}_p = \left\{\sum_{i=0}^{\infty} a_i p^i \mid a_i \in \{0, 1, \ldots, p-1\}\right\}$ es el anillo de los enteros p-ádicos y $\mathcal{U}_p = \mathbb{Z}_p^* = \left\{\sum_{i=0}^{\infty} a_i p^i \in \mathbb{Z}_p, a_0 \neq 0\right\}$.

Observación 1.1.44.

- Si $p > 2$, $\mathcal{U}_p = \mathbb{Z}_p^* \cong C_{p-1} \times \mathbb{Z}_p$ como grupos.
- Para $p = 2$, tenemos $1 + 2\mathbb{Z}_2 \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2)$ y $1 + 4\mathbb{Z}_2 \cong \mathbb{Z}_2$. En particular, $\mathcal{U}_2^{(1)} = \mathcal{U}_2 = \mathbb{Z}_2^* \cong 1 + 2\mathbb{Z}_2 \cong \{\pm 1\} \times (1 + 4\mathbb{Z}_2) \cong \{\pm 1\} \times \mathbb{Z}_2$.

Convenimos en que para el campo local $\mathbb{R}$, el grupo de unidades sea $\mathbb{R}^*$ y el grupo de 1-unidades sea $\mathbb{R}^+$.

1.1.7. Teoría de campos de clases local

Teorema 1.1.45. *(Teorema Fundamental y Mapeo de Artin Local) Sea E/F una extensión abeliana finita de campos locales. Tenemos el mapeo de Artin local*

$$\psi_{E/F} : F^* \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(E/F)$$

es un epimorfismo con núcleo

$$\mathrm{nuc}\, \psi_{E/F} = N_{E/F}(E^*)$$

por lo que

$$F^*/N_{E/F}(E^*) \cong \mathrm{Gal}(E/F),$$

donde $N_{E/F}$ es el mapeo norma.

Observación 1.1.46. Sea $K/\mathbb{Q}$ una extensión abeliana finita. Sea $\wp$ un ideal primo en K y sea p primo tal que $(p) = \wp \cap \mathbb{Q}$. Consideramos las completaciones $K_\wp$ y $\mathbb{Q}_p$. Por el Teorema 1.1.45

$$\mathrm{Gal}\left(K_\wp/\mathbb{Q}_p\right) \cong \mathbb{Q}_p^*/N_{K_\wp/\mathbb{Q}_p} K_\wp^*.$$

De [50, Proposición 17.2.15] tenemos el siguiente diagrama conmutativo correspondiente a una extensión finita arbitraria de campos locales E/F.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{U}_E & \xrightarrow{i} & E^* & \xrightarrow{v_E} & \mathbb{Z} & \longrightarrow & 0 \\ & & \varphi \downarrow N_{E/F} & & \psi \downarrow N_{E/F} & & \downarrow f & & \\ 1 & \longrightarrow & \mathcal{U}_F & \xrightarrow[i]{} & F^* & \xrightarrow[v_F]{} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

donde las filas son exactas y el grado de los campos residuales es $f = [\hat{E} : \hat{F}]$.

Por el Lema de la Serpiente y, como $\operatorname{nuc} f = \{0\}$ y $\operatorname{conuc} f = \mathbb{Z}/f\mathbb{Z}$, tenemos la siguiente sucesión exacta.

$$\operatorname{nuc}\varphi \longrightarrow \operatorname{nuc}\psi \longrightarrow \operatorname{nuc} f = \{0\} \longrightarrow \operatorname{conuc}\varphi \longrightarrow \operatorname{conuc}\psi \longrightarrow \operatorname{conuc} f = \mathbb{Z}/f\mathbb{Z} \longrightarrow \{0\}$$

Luego

$$1 \longrightarrow \mathcal{U}_F/N_{E/F}\mathcal{U}_E \longrightarrow F^*/N_{E/F}E^* \longrightarrow C_f \longrightarrow 1$$

es exacta. Por lo tanto $[F^* : N_{E/F}E^*] = [\mathcal{U}_F : N_{E/F}\mathcal{U}_E] \cdot f$. Observemos que si $f = 1$, entonces

$$F^*/N_{E/F}E^* \cong \mathcal{U}_F/N_{E/F}\mathcal{U}_E. \tag{1.1}$$

Lema 1.1.47. *Si E/F es una extensión abeliana finita de campos locales, entonces el índice de ramificación es*

$$e = [\mathcal{U}_F : N_{E/F}\mathcal{U}_E].$$

Demostración. Como E/F es abeliana, por el Teorema Fundamental de la Teoría de Campos de Clases Local (Teorema 1.1.45), tenemos $ef = [E : F] = [F^* : N_{E/F}E^*]$, donde e es el índice de ramificación de E/F. Por el argumento anterior tenemos $[\mathcal{U}_F : N_{E/F}\mathcal{U}_E] = \frac{[F^*:N_{E/F}E^*]}{f} = \frac{ef}{f} = e$. □

Lema 1.1.48. *Sea E/F una extensión abeliana finita de campos locales. Entonces*

$$\mathcal{U}_F \bigcap N_{E/F}E^* = N_{E/F}\mathcal{U}_E.$$

Demostración. Como $\mathcal{U}_E \subseteq E^*$, se tiene $N_{E/F}\mathcal{U}_E \subseteq N_{E/F}E^*$. Además $N_{E/F}\mathcal{U}_E \subseteq \mathcal{U}_F$. Luego $N_{E/F}\mathcal{U}_E \subseteq \mathcal{U}_F \bigcap N_{E/F}E^*$.

Sea ahora $x \in \mathcal{U}_F \bigcap N_{E/F}E^*$. Entonces $x = N_{E/F}y$ para algún $y \in E^*$. Como $x \in \mathcal{U}_F$, tenemos $y \in \mathcal{U}_E$ y así $x = N_{E/F}y \in N_{E/F}\mathcal{U}_E$. □

Lema 1.1.49. *Sean E/F extensión finita de campos locales y M/F una extensión abeliana finita. Se tiene que EM/E es no ramificada si y sólo si $\psi_{EM/E}(\mathcal{U}_E) = \{1\}$.*

Demostración. Tenemos EM/E es no ramificada si y sólo si, por el Lema 1.1.47, $\mathcal{U}_E = N_{EM/E}\mathcal{U}_{EM}$ si y sólo si el núcleo de $\psi\big|_{\mathcal{U}_E} : \mathcal{U}_E \to \psi(\mathcal{U}_E)$, que por el Lema 1.1.48, es $\mathcal{U}_E \cap N_{EM/E}(EM)^* = N_{EM/E}\mathcal{U}_{EM}$, es igual a $\mathcal{U}_E$ si y sólo si $\psi_{EM/E}(\mathcal{U}_E) = \{1\}$.

□

Lema 1.1.50. *Sea E/F una extensión abeliana finita de campos locales totalmente ramificada. Entonces $[E : F] = [\mathcal{U}_F : N_{E/F}\mathcal{U}_E] = [F^* : N_{E/F}E^*]$. Además $\mathrm{Gal}(E/F) \cong \mathcal{U}_F/N_{E/F}\mathcal{U}_E$.*

Demostración. Como $f = 1$, por la Ecuación 1.1 y el Lema 1.1.47, tenemos

$$[E : F] = ef = e = [\mathcal{U}_F : N_{E/F}\mathcal{U}_E] = [F^* : N_{E/F}E^*].$$

Tenemos también por la Ecuación 1.1 y por el Teorema 1.1.45

$$\mathrm{Gal}(E/F) \cong F^*/N_{E/F}E^* \cong \mathcal{U}_F/N_{E/F}\mathcal{U}_E.$$

□

Teorema 1.1.51. *Sea F un campo local. Sean E_1 y E_2 extensiones abelianas finitas de F. Entonces $E_1 \subseteq E_2$ si y sólo si $N_{E_1/F}E_1^* \supseteq N_{E_2/F}E_2^*$.*

Demostración. Véase [60, Apéndice 3, Teorema 9]. □

Lema 1.1.52. *Sean L/K y L'/K' extensiones abelianas finitas de campos locales con $K \subseteq K'$ y $L \subseteq L'$. Entonces el siguiente diagrama es conmutativo.*

$$\begin{array}{ccc} K'^* & \xrightarrow{\psi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \Big\downarrow{\scriptstyle N_{K'/K}} & & \Big\downarrow{\scriptstyle \mathrm{res}} \\ K^* & \xrightarrow[\psi_{L/K}]{} & \mathrm{Gal}(L/K) \end{array}$$

Demostración. Ver [35, Proposición 2.7, páginas 25-26]. □

Teorema 1.1.53. *Sean F un campo local, E/F una extensión abeliana finita y Δ el subgrupo de F^* correspondiente, esto es $\Delta = N_{E/F}(E^*)$. Sea L/F una extensión finita y separable. Entonces LE/L es una extensión abeliana finita y el grupo de normas correspondiente es $N_{L/F}^{-1}(\Delta)$, (esto es, $N_{LE/L}((LE)^*) = N_{L/F}^{-1}(\Delta)$).*

$$\begin{array}{ccc} L & \xrightarrow{N_{L/F}^{-1}(\Delta)} & LE \\ | & & | \\ F & \xrightarrow[\Delta]{} & E \end{array}$$

Demostración. Sea $\psi_{LE/L} : L^* \to \mathrm{Gal}(LE/L)$ el mapeo de Artin. Por el Teorema Fundamental de la Teoría de Campos de Clases Local (Teorema 1.1.45), el grupo de normas correspondiente a E/F es precisamente $\operatorname{nuc}\psi_{E/F}$ y el de LE/L es precisamente $\operatorname{nuc}\psi_{LE/L}$.

Por el Lema 1.1.52, se tiene el siguiente diagrama conmutativo:

$$\begin{array}{ccc} L^* & \xrightarrow{\psi_{LE/L}} & \mathrm{Gal}\,(LE/L) \\ \downarrow{\scriptstyle N_{L/F}} & & \downarrow{\scriptstyle \mathrm{res}} \\ F^* & \xrightarrow[\psi_{E/F}]{} & \mathrm{Gal}\,(E/F) \end{array}$$

Luego $\mathrm{res} \circ \psi_{LE/L} = \psi_{E/F} \circ N_{L/F}$. Tenemos que $\mathrm{res} : \mathrm{Gal}(LE/L) \to \mathrm{Gal}(E/F)$ es inyectivo pues si $\sigma \in \operatorname{nuc}\mathrm{res}$, entonces $\sigma\,|_E = \mathrm{Id}_E$, luego $\sigma\,|_E = \mathrm{Id}_E$ y $\sigma\,|_L = \mathrm{Id}_L$ y por lo tanto $\sigma = \mathrm{Id}_{LE}$.

Así $x \in \operatorname{nuc}\psi_{LE/L}$ si y sólo si $\psi_{LE/L}(x) = 1$ si y sólo si $\mathrm{res} \circ \psi_{LE/L}(x) = 1$ si y sólo si $\psi_{E/F} \circ N_{L/F}(x) = 1$ si y sólo si $N_{L/F}(x) \in \operatorname{nuc}\psi_{E/F} = \Delta$ si y sólo si $x \in N_{L/F}^{-1}(\Delta)$.

□

1.1.8. Teoría de campos de clases global

Sea K un *campo global*. Esto es, sea K un campo numérico o un campo de funciones en una variable con campo de constantes finito. Denotamos por $\mathbb{P}_K$ al conjunto de lugares primos de K, incluyendo a los primos infinitos, y por $K_\wp$ a la completación de K con respecto al primo $\wp$. Si $\wp$ corresponde a una valuación no arquimediana, denotamos por $\mathcal{O}_\wp$ al correspondiente anillo de

enteros y por $\mathcal{U}_\wp = \mathcal{O}_\wp^*$ al grupo de unidades. Si $\wp$ corresponde a una valuación arquimediana, $\mathcal{U}_\wp = K_\wp^*$.

Definición 1.1.54. [20] El *anillo de adèles* (o reparticiones) $\mathbb{A}_K$ se define como el subanillo de $\prod_{\wp \in \mathbb{P}_K} K_\wp$ dado por:

$$\mathbb{A}_K = \left\{ (a_\wp)_\wp \in \prod_{\wp \in \mathbb{P}_K} K_\wp \;\middle|\; a_\wp \in \mathcal{O}_\wp \text{ para casi todo } \wp \text{ finito} \right\}$$

y el *grupo de idèles* se define como

$$\mathbb{J}_K = \left\{ (a_\wp)_\wp \in \prod_{\wp \in \mathbb{P}_K} K_\wp^* \;\middle|\; a_\wp \in \mathcal{O}_\wp^* \text{ para casi todo } \wp \text{ finito} \right\}.$$

Ejemplo 1.1.55. Tenemos

$$\mathbb{J}_\mathbb{Q} \subseteq \prod_{p \text{ finito}} \mathbb{Q}_p^* \times \mathbb{R}^*.$$

Observamos que $\mathbb{A}_K$ forma un anillo con la suma y multiplicación entrada por entrada y que $\mathbb{J}_K = \mathbb{A}_K^*$ es el grupo de las unidades de $\mathbb{A}_K$.

Se encaja $K^* \hookrightarrow \mathbb{J}_K$ de manera diagonal y la imagen se llama los *idèles principales*. De esta forma K^* consiste de los idèles principales. Similarmente se encaja $K_\wp^* \hookrightarrow \mathbb{J}_K$ con 1 en las demás componentes.

El grupo cociente $\mathcal{C}_K := \mathbb{J}_K / K^*$ se llama el *grupo de clases de idèles*.

De [38], tenemos la topología de idèles como se describe a continuación. El grupo de idèles $\mathbb{J}_K$ de un campo global K es la unión de los grupos $\mathbb{J}_K^S = \prod_{\wp \in S} K_\wp^* \times \prod_{\wp \notin S} \mathcal{U}_\wp$, donde S corre sobre todos los conjuntos finitos de primos de K. Los factores $K_\wp^*$ y $\mathcal{U}_\wp$ están equipados con sus respectivas topologías provenientes de la valuación. Estas inducen la topología de Tychonoff en el producto directo $\mathbb{J}_K^S = \prod_{\wp \in S} K_\wp^* \times \prod_{\wp \notin S} \mathcal{U}_\wp$, así que $\mathbb{J}_K^S$ se vuelve un grupo topológico.

Si $S \subseteq S'$, entonces $\mathbb{J}_K^S \subseteq \mathbb{J}_K^{S'}$ y la topología de Tychonoff en $\mathbb{J}_K^{S'}$ induce la topología de Tychonoff en $\mathbb{J}_K^S$. Por lo tanto se tiene una topología canónica en el grupo de idèles $\mathbb{J}_K = \bigcup_S \mathbb{J}_K^S$ y se llama *topología de idèles*.

También es posible definir la topología de idèles directamente considerando el sistema fundamental de vecindades de la identidad dado por los subconjuntos

$$\prod_{\wp \in S} W_\wp \times \prod_{\wp \notin S} \mathcal{U}_\wp \subseteq \mathbb{J}_K,$$

donde los $W_\wp \subseteq K_\wp^*$ corren sobre un sistema fundamental de vecindades de la identidad de $K_\wp^*$ y S sobre todos los conjuntos finitos de primos de K.

Observación 1.1.56. La extensión E/K de campos globales es no ramificada en el primo $\mathfrak{p}$ si y sólo si $E_\wp/K_\mathfrak{p}$ es no ramificada para todo $\wp \mid \mathfrak{p}$.

Teorema 1.1.57. *(Teorema Fundamental de la Teoría de Campos de Clases, Mapeo de Artin) Sea L/K una extensión abeliana finita de campos globales. Tenemos el mapeo de Artin global*

$$\psi_{L/K} : \mathbb{J}_K \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(L/K)$$

es un epimorfismo con núcleo

$$\mathrm{nuc}\,\psi_{L/K} = K^* N_{L/K}(\mathbb{J}_L)$$

por lo que

$$\mathbb{J}_K/K^* N_{L/K}(\mathbb{J}_L) \cong \mathrm{Gal}(L/K),$$

donde la norma de idèles $N_{L/K} : \mathbb{J}_L \to \mathbb{J}_K$ está dada por

$$N_{L/K}(y)_{\mathfrak{P}\in\mathbb{P}_L} = \left(\prod_{\mathfrak{P}/\mathfrak{p}} N_{L_\mathfrak{P}/K_\mathfrak{p}} y_\mathfrak{P}\right)_{\mathfrak{p}\in\mathbb{P}_K}.$$

Tenemos también el mapeo inducido por ψ

$$\Psi_{L/K} : \mathcal{C}_K \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(L/K)$$

y los isomorfismos

$$\mathcal{C}_K/N_{L/K}\mathcal{C}_L \cong \mathbb{J}_K/K^* N_{L/K}(\mathbb{J}_L) \cong \mathrm{Gal}(L/K),$$

donde $N_{L/K} : \mathcal{C}_L \to \mathcal{C}_K$ es la norma inducida por la norma de los idèles.

Demostración. Véase [60, Apéndice 3, Teorema 11]. □

Teorema 1.1.58. *(Teorema de Existencia) Si $\bar{\Delta}$ es un subgrupo abierto de $\mathcal{C}_K$ de índice finito, entonces hay una única extensión abeliana L/K tal que $N_{L/K}\mathcal{C}_L = \bar{\Delta}$. Equivalentemente, si Δ es abierto de índice finito en $\mathbb{J}_K$ y $K^* \subseteq \Delta$, entonces existe una única extensión abeliana L/K tal que $K^* N_{L/K}\mathbb{J}_L = \Delta$.*

Demostración. Véase [60, Apéndice 3, Teorema 12]. □

Observación 1.1.59. El primo $\wp$ (finito o infinito) es no ramificado en L/K si y sólo si $\mathcal{U}_\wp \subseteq K^* N_{L/K}\mathbb{J}_L$ (recordemos que $\mathcal{U}_\wp$ se encaja en $\mathbb{J}_K$ por medio de $u_\wp \mapsto (\ldots, 1, \ldots, u_\wp, \ldots, 1, \ldots)$, ver [50, Corolario 17.6.47 (2)]).

Teorema 1.1.60. *Sea $n \in \mathbb{N}$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con $p_1, \ldots, p_r$ primos distintos. Entonces el grupo de idèles correspondiente a $\mathbb{Q}(\zeta_n)$ es*

$$\chi_n = \prod_{i=1}^{r} \mathcal{U}_{p_i}^{(\alpha_i)} \times \prod_{\substack{q \text{ primo} \\ q \notin \{p_1, \ldots, p_r\}}} \mathcal{U}_q \times \mathbb{R}^+.$$

Demostración. Sean $G_n := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ y $\mathcal{U}' = \prod_{q \text{ primo}} \mathcal{U}_q \times \mathbb{R}^+$.

Probaremos primero que existe un epimorfismo $\varphi : \mathcal{U}' \to G_n$ con $\operatorname{nuc}\varphi = \chi_n$. Luego $\mathcal{U}'/\chi_n \cong G_n$.

Por otro lado, mostraremos que existe un epimorfismo $\mu : \mathcal{U}' \to \mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^*$ con $\operatorname{nuc}\mu = \chi_n$. Así $\mathcal{U}'/\chi_n \cong \mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^*$. De donde

$$\mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^* \cong G_n,$$

luego el grupo de idèles correspondiente a $\mathbb{Q}(\zeta_n)$ es χ_n.

Primero sea $\vec{\xi} \in \mathcal{U}'$. Entonces $\xi_{p_i} \in \mathcal{U}_{p_i} = \left\{\sum_{j=0}^{\infty} a_j p_i^j \mid a_j \in \mathbb{Z}/(p_i)\right\}$, $1 \le i \le r$. Puesto que $\mathbb{Q}$ es denso en el campo local $\mathbb{Q}_{p_i}$, existe $q_i \in \mathbb{Z}$ tal que $q_i \equiv \xi_{p_i} \bmod p_i^{\alpha_i}$. Por el Teorema Chino del Residuo, existe $c \in \mathbb{Z}$ tal que $c \equiv q_i \bmod p_i^{\alpha_i}$, $1 \le i \le r$, luego $c \equiv \xi_{p_i} \bmod p_i^{\alpha_i}$, $1 \le i \le r$.

Ahora, si $c_1 \in \mathbb{Z}$ es tal que $c_1 \equiv \xi_{p_i} \bmod p_i^{\alpha_i}$, $1 \le i \le r$, tenemos $p_i^{\alpha_i} \mid c - c_1$ para $1 \le i \le r$. Se sigue que $n \mid c - c_1$ y así el entero c es único módulo n. Por otro lado, $v_{p_i}\left(\xi_{p_i}\right) = 0$, por lo que $p_i \nmid \xi_{p_i}$ y por tanto obtenemos $\mathrm{mcd}(c, n) = 1$. Por lo tanto tenemos que c mód n define un elemento de $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

Dado $\sigma \in G_n$, existe $c \in \mathbb{Z}$ tal que $\sigma(\zeta_n) = \zeta_n^c$. Sea $\vec{\xi} \in \mathcal{U}'$ con $\xi_{p_i} = c$, $1 \le i \le r$ y $\xi_{p_\infty} = 1 = \xi_p$ para todo $p \in \mathbb{Z} \setminus \{p_1, \ldots, p_r\}$. Por lo tanto $\vec{\xi} \mapsto c \bmod n$ y φ es suprayectiva. Finalmente $\operatorname{nuc}\varphi = \left\{\vec{\xi} \in \mathcal{U}' \mid \xi_{p_i} \equiv 1 \bmod p_i^{\alpha_i}, 1 \le i \le r\right\} = \chi_n$.

Para la segunda parte tenemos la composición

$$\mathcal{U}' \hookrightarrow \mathbb{J}_\mathbb{Q} \twoheadrightarrow \mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^*, \qquad \mathcal{U}' \xrightarrow{\ \mu\ } \mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^*$$

con $\operatorname{im}\mu = \mathcal{U}'\mathbb{Q}^*/\chi_n\mathbb{Q}^*$ y $\operatorname{nuc}\mu = \mathcal{U}' \cap \chi_n\mathbb{Q}*$.

Veamos que $\mathcal{U}' \cap \chi_n\mathbb{Q}^* = \chi_n$. En efecto, $\chi_n \subseteq \mathcal{U}'$, luego $\chi_n \subseteq \mathcal{U}' \cap \chi_n\mathbb{Q}^*$. Recíprocamente, si $\vec{\xi} \in \mathcal{U}' \cap \chi_n\mathbb{Q}^*$, las componentes de $\vec{\xi}$ son

$$\begin{aligned} \xi_p &= a \cdot \beta_p \text{ para } p \in \mathbb{Z} \\ \xi_\infty &= a \cdot \beta_\infty, \end{aligned}$$

con $\vec{\beta} \in \chi_n$ y $a \in \mathbb{Q}^*$. Como $\xi_p, \beta_p \in \mathcal{U}_p$, tenemos $v_p(\xi_p) = v_p(\beta_p) = 0$ para todo $p \in \mathbb{Z}$. Se sigue que $v_p(a) = 0$ para todo $p \in \mathbb{Z}$. Luego $a \in \{-1, 1\}$. Como $\xi_\infty, \beta_\infty \in \mathbb{R}^+$, necesariamente $a = 1$. Se sigue que $\vec{\xi} \in \chi_n$. Por lo tanto $\operatorname{nuc} \mu = \chi_n$ y se tiene un monomorfismo $\mathcal{U}'/\chi_n \xhookrightarrow{\theta} \mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^*$. Resta probar que θ es suprayectiva.

Veamos que $\mathbb{J}_\mathbb{Q} = \mathcal{U}'\mathbb{Q}^*$. En efecto, $\mathcal{U}'$ corresponde a la máxima extensión abeliana no ramificada de $\mathbb{Q}$, luego $\mathcal{C}_\mathbb{Q} \cong \mathcal{U}'$. Se sigue que $\mathbb{J}_\mathbb{Q}/\mathbb{Q}^* \cong \mathcal{U}'$ y entonces $\mathbb{J}_\mathbb{Q} = \mathcal{U}'\mathbb{Q}^*$. Así $\mathcal{U}'/\chi_n \cong \mathbb{J}_\mathbb{Q}/\chi_n\mathbb{Q}^*$.

□

Corolario 1.1.61. *Sea $n \in \mathbb{N}$, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ con $p_1, \ldots, p_r$ primos distintos. Para un campo ciclotómico $k \subseteq \omega \subseteq \mathbb{Q}(\zeta_n)$, el grupo de idèles correspondiente a ω es de la forma $R_\omega \times \prod_{q \text{ primo}} \mathcal{U}_q \times \mathbb{R}^+$, con R_ω un grupo que satisface $\prod_{i=1}^r \mathcal{U}_{p_i}^{(\alpha_i)} \subseteq R_\omega \subseteq \prod_{i=1}^r \mathcal{U}_{p_i}$.*

Demostración. Por la teoría de campos de clases, se sigue del Teorema 1.1.60. □

Teorema 1.1.62. *Sea $N \in R_T$ con $N = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, con $P_1, \ldots, P_r \in R_T^+$. Sea $R_T' := R_T^+ \setminus \{P_1, \ldots, P_r\}$. Entonces el grupo de idèles correspondiente a $k(\Lambda_N)$ es*

$$\chi_N = \prod_{i=1}^r \mathcal{U}_{P_i}^{(\alpha_i)} \times \prod_{P \in R_T'} \mathcal{U}_P \times \left[(\pi) \times \mathcal{U}_\infty^{(1)}\right],$$

donde $\pi = 1/T$ es un uniformizador para $\wp_\infty$.

Demostración. Análoga a la del Teorema 1.1.60. □

Corolario 1.1.63. *Sea N como en el Teorema 1.1.62. Para un campo ciclotómico $k \subseteq \omega \subseteq k(\Lambda_N)$, el grupo de idèles correspondiente a ω es de la forma $R_\omega \times \prod_{Q \in R_T'} \mathcal{U}_Q \times \left[(\pi) \times \mathcal{U}_\infty^{(1)}\right]$, con R_ω un grupo que satisface $\prod_{i=1}^r \mathcal{U}_{P_i}^{(\alpha_i)} \subseteq R_\omega \subseteq \prod_{i=1}^r \mathcal{U}_{P_i}$.*

Demostración. Nuevamente por la teoría de campos de clases, se sigue del Teorema 1.1.62. □

Teorema 1.1.64. *Sean L_1 y L_2 extensiones abelianas finitas del campo global K. Entonces*

$$L_1 \subseteq L_2 \text{ si y sólo si } K^* N_{L_1/K} \mathbb{J}_{L_1} \supseteq K^* N_{L_2/K} \mathbb{J}_{L_2}.$$

Demostración. Véase [60, Apéndice 3, Teorema 13]. □

Lema 1.1.65. *Sean L/K y L'/K' extensiones abelianas finitas de campos globales con $K \subseteq K'$ y $L \subseteq L'$. Entonces los siguientes diagramas son conmutativos.*

$$\begin{array}{ccc} \mathcal{C}_{K'} & \xrightarrow{\Psi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \downarrow{\scriptstyle N_{K'/K}} & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathcal{C}_K & \xrightarrow[\Psi_{L/K}]{} & \mathrm{Gal}(L/K) \end{array}$$

$$\begin{array}{ccc} \mathbb{J}_{K'} & \xrightarrow{\psi_{L'/K'}} & \mathrm{Gal}(L'/K') \\ \downarrow{\scriptstyle N_{K'/K}} & & \downarrow{\scriptstyle \mathrm{res}} \\ \mathbb{J}_K & \xrightarrow[\psi_{L/K}]{} & \mathrm{Gal}(L/K) \end{array}$$

Demostración. Ver [35, Proposición 2.7, páginas 25-26]. □

Teorema 1.1.66. *Sea E/F una extensión abeliana finita de campos globales correspondiente al subgrupo abierto de índice finito $\bar{\Delta}$ de $\mathcal{C}_F$, esto es $\bar{\Delta} = N_{E/F}(\mathcal{C}_E)$. Sea L/F una extensión finita y separable. Entonces LE/L es una extensión abeliana finita y el grupo de normas correspondiente es $N_{L/F}^{-1}(\bar{\Delta})$, (esto es, $N_{LE/L}(\mathcal{C}_{LE}) = N_{L/F}^{-1}(\bar{\Delta})$).*

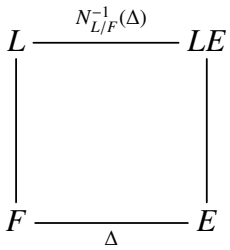
$$\begin{array}{ccc} L & \xrightarrow{N_{L/F}^{-1}(\bar{\Delta})} & LE \\ | & & | \\ F & \xrightarrow[\bar{\Delta}]{} & E \end{array}$$

Demostración. Similar a la del Teorema 1.1.53.

□

Análogamente, tenemos el siguiente resultado.

Teorema 1.1.67. *Sean F un campo global, E/F una extensión abeliana finita y Δ el grupo de idèles que le corresponde a la extensión E/F. Sea L/F una extensión finita y separable. Entonces la extensión abeliana finita LE/L es el campo de clases correspondiente a $N_{L/F}^{-1}(\Delta)$.*



Demostración. Similar a la del Teorema 1.1.53. □

1.2. Campos de clases de Hilbert y de géneros de campos numéricos

Definición 1.2.1. Sea K un campo numérico.

1. El *campo de clases de Hilbert* K_H de K es la máxima extensión abeliana de K no ramificada.
2. El *campo de clases de Hilbert extendido* o *campo de clases de Hilbert en el sentido estricto* K_{H^+} de K es la máxima extensión abeliana de K no ramificada en los primos finitos.
3. El *campo de géneros* $K_{\mathfrak{g}}$ de K es la máxima extensión abeliana de K no ramificada, de manera que $K_{\mathfrak{g}} = K\omega$ con $\omega/\mathbb{Q}$ abeliana.
4. El *campo de géneros extendido* o *campo de géneros en el sentido estricto* $K_{\mathfrak{g}^+}$ de K es la máxima extensión abeliana de K no ramificada en los primos finitos, de manera que $K_{\mathfrak{g}^+} = K\Omega$ con $\Omega/\mathbb{Q}$ abeliana.

Proposición 1.2.2. *Sea $K/\mathbb{Q}$ extensión de Galois. Entonces $K_{H^+}/\mathbb{Q}$ y $K_H/\mathbb{Q}$ son de Galois. También $K_{\mathfrak{g}^+}/\mathbb{Q}$ y $K_{\mathfrak{g}}/\mathbb{Q}$ son de Galois.*

Demostración. Sea $\sigma : K_H \to \bar{\mathbb{Q}}$ un encaje. Entonces $\sigma|_K \in \mathrm{Gal}(K/\mathbb{Q})$. Luego $\sigma(K) = K$. Se tiene que $\sigma(K_H)/K$ es abeliana no ramificada. Por lo tanto $K_H\sigma(K_H)/K$ es abeliana no ramificada. Luego $\sigma(K_H) \subseteq K_H\sigma(K_H) \subseteq K_H$. Por lo tanto $\sigma(K_H) = K_H$ y así $K_H/\mathbb{Q}$ es de Galois. Similarmente para K_{H^+}.

Puesto que K y ω son de Galois sobre $\mathbb{Q}$, $K_{\mathfrak{g}} = K\omega$ es de Galois, análogamente para $K_{\mathfrak{g}}$.

□

Observación 1.2.3. Sea K un campo numérico. Se tiene

1. $K_{\mathfrak{g}} \subseteq K_H$ y $K_{\mathfrak{g}^+} \subseteq K_{H^+}$.

2. $K_H \subseteq K_{H^+}$ y $K_{\mathfrak{g}} \subseteq K_{\mathfrak{g}^+}$.

3. K_H/K, $K_{\mathfrak{g}}/K$, K_{H^+}/K y $K_{\mathfrak{g}^+}/K$ son extensiones abelianas finitas.

4. $\mathrm{Gal}(K_H/K)$ es isomorfo al *grupo de clases* $\mathcal{F}_K/\mathcal{P}_K$, donde $\mathcal{F}_K$ es el grupo de ideales fraccionarios de K y $\mathcal{P}_K = \{(\alpha) \mid \alpha \in K^*\}$ y $\mathrm{Gal}(K_{H^+}/K)$ es isomorfo al *grupo de clases en el sentido estricto* $\mathcal{F}_K/\mathcal{P}_K^{(+)}$, donde $\mathcal{P}_K^+ = \{(\alpha) \mid \alpha \in K^*,\ \alpha \text{ es totalmente positivo}\}$ (un elemento α de K es *totalmente positivo* si $\sigma(\alpha) > 0$ para todos los encajes reales σ de K en $\bar{\mathbb{Q}}$, donde $\bar{\mathbb{Q}}$ es una cerradura algebraica de $\mathbb{Q}$).

Notemos que puede haber varias ω y varias Ω que cumplan la Definición 1.2.1, como podemos observar en el siguiente ejemplo.

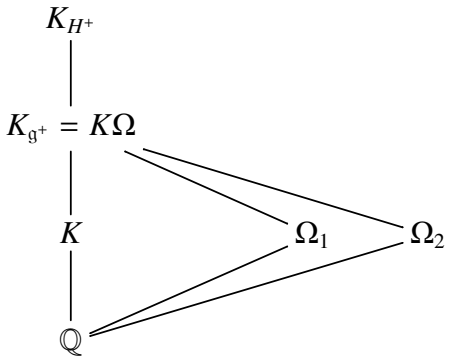
Ejemplo 1.2.4. Sea $K = \mathbb{Q}\left(\sqrt{79}\right)$. Entonces $K_{\mathfrak{g}} = K = \mathbb{Q}\left(\sqrt{79}\right)$ y $K_{\mathfrak{g}^+} = \mathbb{Q}\left(\sqrt{79}, i\right)$. En este caso ω puede ser $\mathbb{Q}$ y puede ser K, mientras que Ω puede ser $\mathbb{Q}(i)$, $\mathbb{Q}\left(\sqrt{-79}\right)$ y $\mathbb{Q}\left(\sqrt{79}, i\right)$ mismo.

Elegimos tomar ω y Ω máximos respecto a las propiedades que los definen. En el ejemplo elegimos $\omega = K$ y $\Omega = \mathbb{Q}\left(\sqrt{79}, i\right)$. Veamos que esto es posible en general.

Proposición 1.2.5. *En las condiciones de arriba se pueden tomar ω y Ω máximos respecto a las propiedades que los definen.*

Demostración. Haremos la demostración para Ω, la demostración para ω es análoga. Puesto que $\Omega \subseteq K_{\mathfrak{g}^+} \subseteq K_{H^+}$, $[\Omega : \mathbb{Q}] < \infty$. Supongamos que las extensiones abelianas sobre $\mathbb{Q}$, Ω_1 y Ω_2, cumplen $K_{\mathfrak{g}^+} = K\Omega_1 = K\Omega_2$. Entonces $K_{\mathfrak{g}^+} = K_{\mathfrak{g}^+}K_{\mathfrak{g}^+} = K\Omega_1 K\Omega_2$. Luego $\Omega = \Omega_1\Omega_2$ también satisface las condiciones.

□



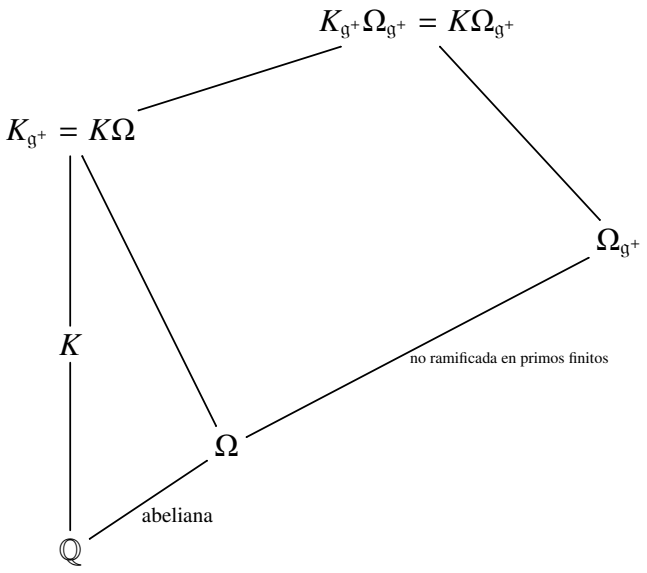
Observación 1.2.6. En adelante tomaremos ω y Ω máximos. En este caso, ω es la máxima extensión abeliana de $\mathbb{Q}$ contenida en K_H y Ω es la máxima extensión abeliana de $\mathbb{Q}$ contenida en K_{H^+}. Como consecuencia tenemos

$$\omega \subseteq \Omega.$$

Proposición 1.2.7. *En las condiciones de arriba tenemos*

1. $\omega_{\mathfrak{g}} = \omega$.
2. $\Omega_{\mathfrak{g}^+} = \Omega$.
3. $\omega_{\mathfrak{g}^+} \subseteq \Omega$.

Demostración. Probaremos solamente el caso 2, el caso 1 es análogo y el caso 3 se sigue de 2.



Tenemos $\Omega \subseteq \Omega_{\mathfrak{g}^+}$ y $\Omega_{\mathfrak{g}^+}/\Omega$ es abeliana ya que $\Omega_{\mathfrak{g}^+}/\mathbb{Q}$ lo es. Como $\Omega_{\mathfrak{g}^+}/\Omega$ es abeliana no ramificada en primos finitos, también $K\Omega_{\mathfrak{g}^+}/K\Omega$ es abeliana y no ramificada en primos finitos. Puesto que $\Omega_{\mathfrak{g}^+}/\mathbb{Q}$ es abeliana, $K\Omega_{\mathfrak{g}^+}/K$ es abeliana y además es no ramificada en primos finitos. Luego $K\Omega_{\mathfrak{g}^+} \subseteq K_{\mathfrak{g}^+} = K\Omega \subseteq K\Omega_{\mathfrak{g}^+}$. Por lo tanto $K\Omega = K\Omega_{\mathfrak{g}^+}$, de donde $\Omega = \Omega_{\mathfrak{g}^+}$.

□

Teorema 1.2.8. *Sea K una extensión abeliana de $\mathbb{Q}$ y sea X el grupo de caracteres de Dirichlet asociado a K. Sea J la máxima extensión abeliana de $\mathbb{Q}$ que contiene a K tal que la extensión J/K es no ramificada en cada primo racional finito. Sea Y el grupo de caracteres de Dirichlet asociado a J. Entonces $Y = \prod_{p \in P} X_p$, donde p recorre el conjunto de primos racionales P.*

Demostración. Véase [30, Teorema 2.1]. □

Lema 1.2.9. *Sea $K/\mathbb{Q}$ una extensión abeliana. Entonces*

1. *$K \subseteq \omega = K_{\mathfrak{g}}$, luego $K_{\mathfrak{g}}$ es la máxima extensión abeliana de $\mathbb{Q}$ contenida en K_H.*

2. *$K \subseteq \Omega = K_{\mathfrak{g}^+}$, luego $K_{\mathfrak{g}^+}$ es la máxima extensión abeliana de $\mathbb{Q}$ contenida en K_{H^+}.*

Demostración. Lo probaremos sólo para Ω, el otro caso es análogo. Como $K/\mathbb{Q}$ es abeliana, por la Observación 1.2.6, $K \subseteq \Omega$. Luego $K_{\mathfrak{g}^+} = K\Omega = \Omega$. □

Proposición 1.2.10. *Sean $K/\mathbb{Q}$ extensión de Galois y J la conjugación compleja. Entonces*

1. *$[K_{H^+} : K_H] \mid 2$.*

2. *Si $J|_K = \mathrm{Id}$, tenemos $K_{H^+}^J = K_H$.*

Demostración. Como $K/\mathbb{Q}$ es de Galois, $K_{H^+}/\mathbb{Q}$ y $K_H/\mathbb{Q}$ son de Galois. Luego $J|_{K_{H^+}} \in \mathrm{Gal}(K_{H^+}/\mathbb{Q})$ y $J|_K \in \mathrm{Gal}(K/\mathbb{Q})$.

Si $J|_K \neq \mathrm{Id}$, entonces K es totalmente imaginario ($K \subsetneq \mathbb{R}$), luego los primos infinitos no se ramifican en K_{H^+}/K y así $K_{H^+} = K_H$.

Si $J|_K = \mathrm{Id}$ entonces $J|_{K_{H^+}} \in \mathrm{Gal}(K_{H^+}/K)$. Si $K_H = K_{H^+}$, entonces $K_{H^+}^J = K_H$. Si $K_H \neq K_{H^+}$, entonces en K_{H^+}/K_H se ramifican los primos infinitos, $K_H \subseteq K_{H^+}^J$. Como $K_H \subseteq K_{H^+}^J \subseteq \mathbb{R}$, necesariamente $K_H = K_{H^+}^J$ y así $[K_{H^+} : K_H] \mid 2$ □

Observación 1.2.11. Sea $K/\mathbb{Q}$ extensión finita. Entonces $\mathrm{Gal}(K_{H^+}/K_H) \cong {C_2}^r$, con $r \leq r_1$, donde r_1 es el número de encajes reales de K (ver [50, comentario después de la Definición 17.7.15]). Es posible que r sea mayor que 1. Por ejemplo, sea $K = \mathbb{Q}(\alpha)$, donde α es una raíz del polinomio $x^5 - 2x^4 - 6x^3 + 8x^2 + 8x + 1$. El grupo de clases de Hilbert es trivial, mientras que el grupo de clases de Hilbert extendido es isomorfo a $C_2 \times C_2$ (ver [10]).

Sea $K/\mathbb{Q}$ extensión finita y consideremos ω y Ω como antes.

Observación 1.2.12. Tenemos ω y Ω son extensiones abelianas de $\mathbb{Q}$. Como $\Omega^J/\mathbb{Q}$ es abeliana y totalmente real, $K\Omega^J/K$ es abeliana no ramificada. Por tanto $\Omega^J \subseteq \omega$. Así pues

$$\Omega^J \subseteq \omega \subseteq \Omega.$$

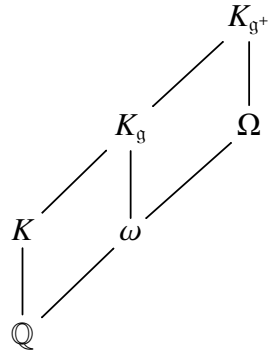
Puesto que $[\Omega : \Omega^J] \mid 2$, tenemos

$$[\Omega : \omega] \mid 2.$$

Proposición 1.2.13. *Sea K una extensión finita de $\mathbb{Q}$. Entonces*

$$[K_{\mathfrak{g}^+} : K_{\mathfrak{g}}] \mid 2.$$

Demostración. Tenemos $[K_{\mathfrak{g}^+} : K_{\mathfrak{g}}] = [K\Omega : K\omega] \mid [\Omega : \omega] \mid 2$.



□

Ejemplos 1.2.14. En el caso de que $K = \mathbb{Q}(\sqrt{79})$, $K_{\mathfrak{g}^+} = \mathbb{Q}(\sqrt{79}, i)$, mientras que $K_{\mathfrak{g}} = K$ por lo que $[K_{\mathfrak{g}^+} : K_{\mathfrak{g}}] = 2$. Si $K = \mathbb{Q}(i)$, $K_{\mathfrak{g}^+} = K_{\mathfrak{g}} = K$ tenemos $[K_{\mathfrak{g}^+} : K_{\mathfrak{g}}] = 1$.

Lema 1.2.15. *Sean K, L campos numéricos con $K \subseteq L$. Entonces*

1. $K_H \subseteq L_H$.

2. $K_{H^+} \subseteq L_{H^+}$.

3. $K_{\mathfrak{g}} \subseteq L_{\mathfrak{g}}$.

4. $K_{\mathfrak{g}^+} \subseteq L_{\mathfrak{g}^+}$.

Demostración. (1) y (2): K_H/K es una extensión abeliana no ramificada, entonces LK_H/L es una extensión abeliana no ramificada. Como $LK_H \subseteq L_H$, se tiene $K_H \subseteq L_H$. De igual forma, como $LK_{H^+} \subseteq L_{H^+}$, tenemos $K_{H^+} \subseteq L_{H^+}$.

(3) y (4):

$$\begin{array}{ccc} L & \text{———} & LK_{\mathfrak{g}} = L\Omega \\ | & & | \\ K & \text{———} & K\Omega = K_{\mathfrak{g}} \\ | & & | \\ \mathbb{Q} & \text{———} & \Omega \end{array}$$

Tenemos que la extensión $K_{\mathfrak{g}}/K$ es abeliana no ramificada. Luego $L\Omega = LK\Omega = LK_{\mathfrak{g}}$ es una extensión de L abeliana no ramificada. Como Ω es abeliana sobre $\mathbb{Q}$, $K_{\mathfrak{g}} \subseteq LK_{\mathfrak{g}} = L\Omega \subseteq L_{\mathfrak{g}}$. Análogamente, $K_{\mathfrak{g}^+} \subseteq L_{\mathfrak{g}^+}$.

□

Del Lema 1.2.15 se sigue el siguiente resultado.

Lema 1.2.16. *Sean K_1 y K_2 campos numéricos y $K = K_1K_2$. Entonces*

1. $(K_1)_H(K_2)_H \subseteq K_H$.

2. $(K_1)_{H^+}(K_2)_{H^+} \subseteq K_{H^+}$.

3. $(K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}} \subseteq K_{\mathfrak{g}}$.

4. $(K_1)_{\mathfrak{g}^+}(K_2)_{\mathfrak{g}^+} \subseteq K_{\mathfrak{g}^+}$.

Proposición 1.2.17. *Sean K_1 y K_2 extensiones abelianas de $\mathbb{Q}$ y $K = K_1K_2$. Entonces*

$$K_{\mathfrak{g}^+} = (K_1)_{\mathfrak{g}^+}(K_2)_{\mathfrak{g}^+}.$$

Demostración. Sea $\mathbb{Q}(\zeta_n)$ campo ciclotómico tal que $K \subseteq \mathbb{Q}(\zeta_n)$. Sean X_1, X_2 y X los grupos de caracteres de Dirichlet asociados a K_1, K_2 y K, respectivamente. Entonces $X = X_1X_2 = \langle X_1X_2 \rangle$. Se tiene $X_p = (X_1)_p(X_2)_p = \langle (X_1)_p(X_2)_p \rangle$. Obtenemos

$$\prod_{p \text{ primo}} X_p = \prod_{p \text{ primo}} \langle X_1X_2 \rangle_p = \prod_{p \text{ primo}} (X_1)_p \prod_{p \text{ primo}} (X_2)_p.$$

Concluimos

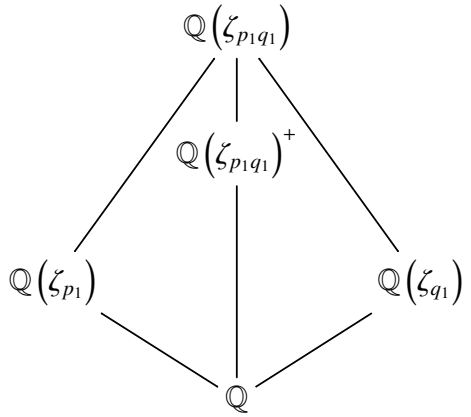
$$K_{\mathfrak{g}^+} = (K_1)_{\mathfrak{g}^+}(K_2)_{\mathfrak{g}^+}.$$

□

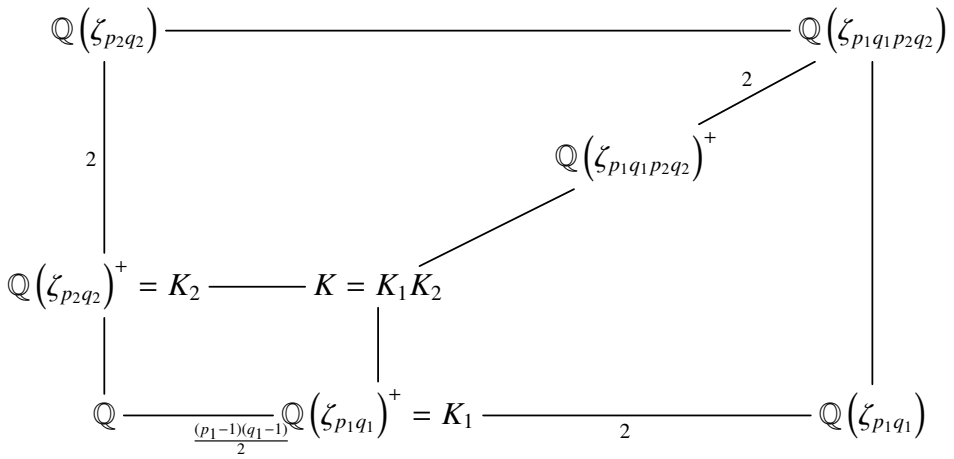
Observación 1.2.18. No necesariamente se tiene que $K_{\mathfrak{g}} = (K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}}$, aún si K_1 y K_2 son extensiones abelianas de $\mathbb{Q}$.

Ejemplo 1.2.19. (Ver [32, Remark 3.7]) Sean p_1, q_1, p_2, q_2 primos impares distintos. Sean $K_1 := \mathbb{Q}\left(\zeta_{p_1q_1}\right)^+$ y $K_2 := \mathbb{Q}\left(\zeta_{p_2q_2}\right)^+$. Tenemos por [27] o [30, Teoremas 2.1 y 3.6] que $(K_1)_{\mathfrak{g}} \subseteq \mathbb{Q}\left(\zeta_{p_1q_1}\right)$ y además, como $p_1 \neq q_1$, $\mathbb{Q}\left(\zeta_{p_1q_1}\right)/\mathbb{Q}\left(\zeta_{p_1q_1}\right)^+$ es ramificada únicamente en los primos infinitos, (ver [50, Teorema 5.3.2]).

Luego $(K_1)_{\mathfrak{g}} = K_1$. Lo mismo para K_2, $(K_2)_{\mathfrak{g}} = K_2$.



Sea $K := K_1K_2$. Tenemos $K = \mathbb{Q}\left(\zeta_{p_1q_1}\right)^+ \mathbb{Q}\left(\zeta_{p_2q_2}\right)^+ \subseteq \mathbb{Q}\left(\zeta_{p_1q_1}\right)\mathbb{Q}\left(\zeta_{p_2q_2}\right) = \mathbb{Q}\left(\zeta_{p_1q_1p_2q_2}\right)$. Luego $K_{\mathfrak{g}} \subseteq \mathbb{Q}\left(\zeta_{p_1q_1p_2q_2}\right)$



La extensión $\mathbb{Q}\left(\zeta_{p_1q_1p_2q_2}\right)^+ / K$ es no ramificada ya que p_1 no es ramificado, pues tenemos $e_{p_1}\left(\mathbb{Q}\left(\zeta_{p_1q_1p_2q_2}\right)/\mathbb{Q}\right) = p - 1 = e_p\left(\mathbb{Q}\left(\zeta_{p_1q_1}\right)^+/\mathbb{Q}\right)$ y lo mismo para q_1, p_2 y q_2.

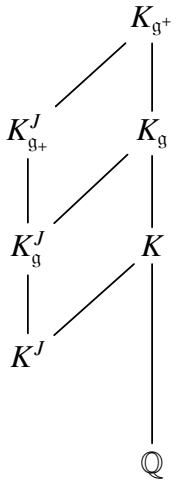
Por lo tanto $(K_1K_2)_{\mathfrak{g}} = \mathbb{Q}\left(\zeta_{p_1q_1p_2q_2}\right)^+$. Tenemos $\left[(K_1K_2)_{\mathfrak{g}} : (K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}}\right] = 2 > 1$.

Lema 1.2.20. *Sea $K/\mathbb{Q}$ una extensión de Galois finita. Entonces*

$$K_{\mathfrak{g}} = K_{\mathfrak{g}^+}^J K.$$

Demostración. Examinemos los diferentes casos:

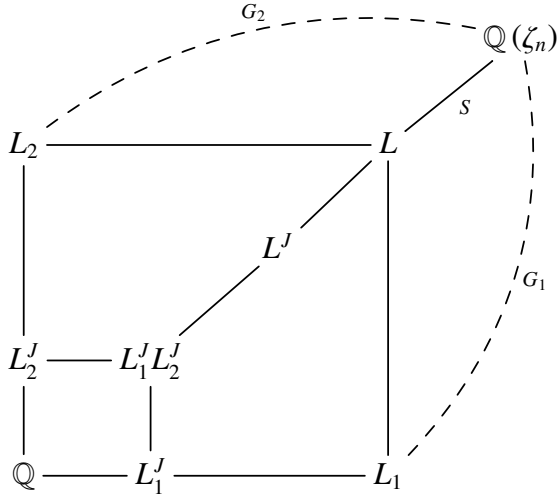
1. $K_{\mathfrak{g}^+} \subseteq \mathbb{R}$, luego $K_{\mathfrak{g}^+}^J = K_{\mathfrak{g}^+}$ y $K_{\mathfrak{g}^+} = K_{\mathfrak{g}}$. Entonces $K_{\mathfrak{g}^+}^J = K_{\mathfrak{g}}$. Así $K_{\mathfrak{g}} = K_{\mathfrak{g}^+}^J K$.
2. $K_{\mathfrak{g}^+} \nsubseteq \mathbb{R}$ y $K \subseteq \mathbb{R}$, entonces $K_{\mathfrak{g}} \subseteq \mathbb{R}$. Así $K_{\mathfrak{g}} = K_{\mathfrak{g}^+}^J$ y por lo tanto $K_{\mathfrak{g}} = K_{\mathfrak{g}^+}^J K$.
3. $K \nsubseteq \mathbb{R}$, se tiene $K_{\mathfrak{g}^+} = K_{\mathfrak{g}}$, luego $K_{\mathfrak{g}^+}^J K = K_{\mathfrak{g}}^J K = K_{\mathfrak{g}}$ pues $K \nsubseteq K_{\mathfrak{g}}^J$.



□

Lema 1.2.21. *Sean L_1 y L_2 extensiones abelianas finitas de $\mathbb{Q}$ y $L = L_1L_2$. Entonces $\left[L^J : L_1^J L_2^J\right] \Big| 2$.*

Demostración. Tenemos que L también es una extensión abeliana de $\mathbb{Q}$. Sea n tal que $L \subseteq \mathbb{Q}(\zeta_n)$.



Sean $S = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/L)$ y $H = \langle J \rangle$. Entonces $L^J = \mathbb{Q}(\zeta_n)^{SH}$. Sean $G_i = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/L_i)$ para $i = 1, 2$. Entonces $L_i^J = \mathbb{Q}(\zeta_n)^{G_iH}$. Como $L = L_1L_2$, tenemos $S = G_1 \cap G_2$. Puesto que $\mathbb{Q}(\zeta_n)^{G_1H \cap G_2H} = \mathbb{Q}(\zeta_n)^{G_1H}\mathbb{Q}(\zeta_n)^{G_2H} = L_1^J L_2^J \subseteq L^J = \mathbb{Q}(\zeta_n)^{SH}$, tenemos que $\mathrm{Gal}\left(L^J/L_1^J L_2^J\right) = \frac{\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/L_1^J L_2^J\right)}{\mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/L^J\right)} \cong \frac{G_1H \cap G_2H}{(G_1 \cap G_2)H}$.

Por el Lema 1.1.1, $\left[L^J : L_1^J L_2^J\right] = [G_1H \cap G_2H : (G_1 \cap G_2)H] \mid 2$.

□

Observación 1.2.22. El Ejemplo 1.2.19 nos ilustra que es posible que $L^J \neq L_1^J L_2^J$, donde $L_1 = \mathbb{Q}\left(\zeta_{p_1q_1}\right)$ y $L_2 = \mathbb{Q}\left(\zeta_{p_2q_2}\right)$.

Teorema 1.2.23. *Sean K_1 y K_2 extensiones abelianas finitas de $\mathbb{Q}$ y sea $K = K_1K_2$. Entonces*

$$[K_{\mathfrak{g}} : (K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}}] \Big| 2.$$

Demostración. Por la Proposición 1.2.17, $K_{\mathfrak{g}^+} = (K_1)_{\mathfrak{g}^+}(K_2)_{\mathfrak{g}^+}$. Por el Lema 1.2.20, $K_{\mathfrak{g}} = K_{\mathfrak{g}^+}^J K$, $(K_1)_{\mathfrak{g}} = (K_1)_{\mathfrak{g}^+}^J K_1$ y $(K_2)_{\mathfrak{g}} = (K_2)_{\mathfrak{g}^+}^J K_2$. Luego $(K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}} = (K_1)_{\mathfrak{g}^+}^J K_1 (K_2)_{\mathfrak{g}^+}^J K_2 = (K_1)_{\mathfrak{g}^+}^J (K_2)_{\mathfrak{g}^+}^J K_1K_2 = (K_1)_{\mathfrak{g}^+}^J (K_2)_{\mathfrak{g}^+}^J K \subseteq \left((K_1)_{\mathfrak{g}^+}(K_2)_{\mathfrak{g}^+}\right)^J K = K_{\mathfrak{g}^+}^J K = K_{\mathfrak{g}}$.

Por el Lema 1.2.21, $\left[\left((K_1)_{\mathfrak{g}^+}(K_2)_{\mathfrak{g}^+}\right)^J : (K_1)_{\mathfrak{g}^+}^J (K_2)_{\mathfrak{g}^+}^J\right] \Big| 2$, tenemos $[K_{\mathfrak{g}} : (K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}}] \Big| 2$.

□

1.3. Campos de géneros extendidos de campos numéricos

Con el objetivo de describir para un campo numérico K su campo de géneros $K_{\mathfrak{g}^+} = K\Omega$, basta conocer el campo Ω, el cual es una extensión abeliana de $\mathbb{Q}$ y por tanto está contenida en un campo ciclotómico.

Sea X el grupo de caracteres de Dirichlet asociado a Ω. Entonces el grupo de caracteres de $\Omega_{\mathfrak{g}^+}$ es

$$Y = \prod_{p \text{ primo finito}} X_p.$$

Por la Proposición 1.2.7, tenemos $\Omega = \Omega_{\mathfrak{g}^+}$, luego $X = Y$.

Sea $\Omega^{(p)}$ el campo asociado a X_p. Tenemos $\Omega = \Omega_{\mathfrak{g}^+} = \prod_p \Omega^{(p)}$. Ahora, para describir $K_{\mathfrak{g}^+}$, se ha reducido el problema a considerar $\Omega^{(p)}$. Notemos que si p es no ramificado en K/k, entonces X_p es trivial y $\Omega^{(p)} = \mathbb{Q}$.

El conductor de X_p es p^{m_p} para algún $m_p \in \mathbb{N} \cup \{0\}$, luego $\Omega^{(p)} \subseteq \mathbb{Q}\left(\zeta_{p^{m_p}}\right)$. Estudiemos las subextensiones del campo ciclotómico $\mathbb{Q}\left(\zeta_{p^{m_p}}\right)$.

- Caso $p \neq 2$.

Recordemos que en este caso $\Omega^{(p)}/\mathbb{Q}$ es una extensión cíclica. Consideremos ahora $\left[\Omega^{(p)} : \mathbb{Q}\right] = t = p^a \cdot b_p$ con $a \in \mathbb{N} \cup \{0\}$ y $\operatorname{mcd}\left(b_p, p\right) = 1$ y sea $\Omega^{(p)\prime} \subseteq \Omega^{(p)}$ con $\left[\Omega^{(p)\prime} : \mathbb{Q}\right] = b_p$. Tenemos que p es moderadamente ramificado en $\Omega^{(p)\prime}/\mathbb{Q}$ y salvajemente ramificado en $\Omega^{(p)}/\Omega^{(p)\prime}$. Sean $\operatorname{con}_{\mathbb{Q}/K} p = \wp_1^{e_1} \cdots \wp_r^{e_r}$; $e_p^* = \operatorname{mcd}(e_1, \ldots, e_r) = p^{c_p} \cdot d_p$ con $c_p \in \mathbb{N} \cup \{0\}$ y $\left(d_p, p\right) = 1$.

Proposición 1.3.1. *En las condiciones de antes*

$$\left[\Omega^{(p)\prime} : \mathbb{Q}\right] = \operatorname{mcd}\left(d_p, p-1\right) = \operatorname{mcd}\left(e_p^*, p-1\right) = \operatorname{mcd}\left(e_1, \ldots, e_r, p-1\right).$$

Demostración. Sea $L \subseteq \mathbb{Q}\left(\zeta_{p^m}\right)$ con $[L : \mathbb{Q}] = d$ y $(d, p) = 1$. Entonces en la extensión $L/\mathbb{Q}$ el primo p es moderadamente ramificado. Sea $\mathfrak{P}$ un primo de KL con $\mathfrak{P} \cap K = \wp_i$. Entonces $\mathfrak{P} \cap \mathbb{Q} = (p)$. Sea $\mathfrak{Q} = \mathfrak{P} \cap L$. Por el Lema de Abhyankar $e(\mathfrak{P}/p) = \operatorname{mcm}\left[e(\wp_i/p), e(\mathfrak{Q}, p)\right] = \operatorname{mcm}\left[e_i, d\right]$. También se tiene $e(\mathfrak{P}/\wp_i) = \frac{e(\mathfrak{P}/p)}{e(\wp_i/p)} = \frac{e(\mathfrak{P}/p)}{e_i}$.

Luego $\mathfrak{P}$ es no ramificado en KL/K si y sólo si $e(\mathfrak{P}/\wp_i) = 1$ si y sólo si $e(\mathfrak{P}/p) = e_i$ si y sólo si $d \mid e_i$.

Por lo tanto, KL/K es no ramificada en ningún primo finito si y sólo si $d \mid e_i$ para $1 \leq i \leq r$ si y sólo si $d \mid \operatorname{mcd}(e_1, \ldots, e_r)$ si y sólo si $d \mid \operatorname{mcd}(e_1, \ldots, e_r, p-1)$ (porque $d \mid p-1$).

Aplicamos lo anterior a $L = \Omega^{(p)'}$ y $d = b_p$; como $K\Omega^{(p)'}/K$ es no ramificada en primos finitos, tenemos $b_p \mid \operatorname{mcd}(e_1, \ldots, e_r, p-1)$.

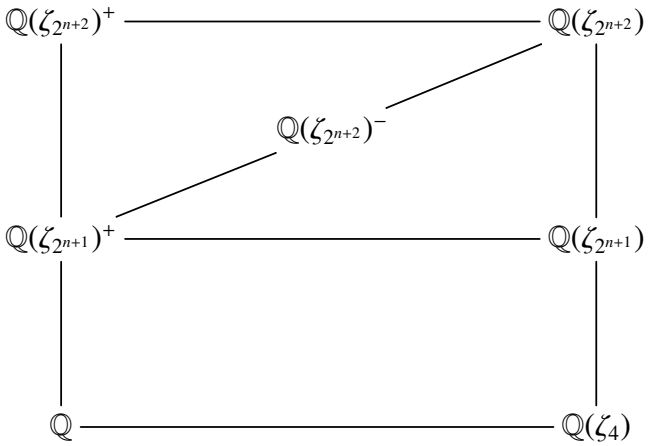
Por otro lado, como $\operatorname{mcd}(e_1, \ldots, e_r, p-1) \mid t$ y $\operatorname{mcd}(\operatorname{mcd}(e_1, \ldots, e_r, p-1), p) = 1$, tenemos que $\operatorname{mcd}(e_1, \ldots, e_r, p-1) \mid b_p$. Luego $b_p = \operatorname{mcd}(e_1, \ldots, e_r, p-1)$.

□

- Caso $p = 2$

Supongamos $[\Omega^{(2)} : \mathbb{Q}] = 2^n$. Entonces $\mathbb{Q}(\zeta_{2^{n+1}})^+ \subseteq \Omega^{(2)} \subseteq \mathbb{Q}(\zeta_{2^{n+2}})$. En la extensión $\Omega^{(2)}/\mathbb{Q}$, el primo 2 es total y salvajemente ramificado.

Tenemos las siguientes posibilidades para $\Omega^{(2)}$. El campo $\Omega^{(2)}$ es uno de $\mathbb{Q}(\zeta_{2^{n+2}})^+$, $\mathbb{Q}(\zeta_{2^{n+1}})$, $\mathbb{Q}(\zeta_{2^{n+2}})^-$.



Las extensiones $\mathbb{Q}(\zeta_{2^{n+2}})^+$ y $\mathbb{Q}(\zeta_{2^{n+2}})^-$ son cíclicas y, por el contrario, $\mathbb{Q}(\zeta_{2^{n+1}})$ no es cíclica. El conductor de $\mathbb{Q}(\zeta_{2^{n+2}})^+$ y $\mathbb{Q}(\zeta_{2^{n+2}})^-$ es 2^{n+2}, mientras que el de $\mathbb{Q}(\zeta_{2^{n+1}})$ es 2^{n+1}.

El siguiente teorema es nuestro resultado principal para campos numéricos. En él se describen los campos $\Omega^{(p)}$, lo que permite determinar el campo de géneros extendido $K_{\mathfrak{g}^+}$ del campo numérico K.

Teorema 1.3.2. *Sea $K/\mathbb{Q}$ una extensión finita. Entonces el campo de géneros extendido de K es $K_{\mathfrak{g}^+} = K\Omega$, donde $\Omega = \prod_p \Omega^{(p)}$, donde p recorre el conjunto de primos finitos ramificados en $K/\mathbb{Q}$, $\mathbb{Q} \subseteq \Omega^{(p)} \subseteq \mathbb{Q}\left(\zeta_{p^{m_p}}\right)$, para algún $m_p \in \mathbb{N}$. Tenemos que $\Omega^{(p)}$ es el campo de clases correspondiente a $\prod_{i=1}^{r} N_{K_{\wp_i}/\mathbb{Q}_p} \mathcal{U}_{\wp_i}$, donde $\operatorname{con}_{\mathbb{Q}/K} p = \wp_1^{e_1} \cdots \wp_r^{e_r}$. Más precisamente $\Omega^{(p)}$, es el campo*

de clases correspondiente al grupo de clases de idèles de $\mathbb{Q}$

$$\left\{\vec{\alpha} \bmod \mathbb{Q}^* \in \mathcal{C}_{\mathbb{Q}} \mid \alpha_p \in \prod_{i=1}^{r} N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i}\right\}.$$

Si $p \geq 3$, $\Omega^{(p)}$ *está unívocamente determinado por la condición*

$$[\Omega^{(p)} : \mathbb{Q}] = \operatorname*{mcd}_{1\leq i\leq r}\left(\mathcal{U}_p : N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i}\right).$$

La parte moderada del índice de ramificación de p *en* $[\Omega^{(p)} : \mathbb{Q}]$ *es* $e_0(p) = \operatorname{mcd}(e_1, \ldots, e_r, p-1)$.

Para $p = 2$, *si* $\left[\Omega^{(2)} : \mathbb{Q}\right] = 2^n$, *para determinar* $\Omega^{(2)}$ *tenemos:*

1. $\Omega^{(2)} = \mathbb{Q}(\zeta_{2^{n+2}})^+$ *si y sólo si* $\mathcal{U}_2/\prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$ *es cíclico y* $-1 \in \bigcap_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$.
2. $\Omega^{(2)} = \mathbb{Q}(\zeta_{2^{n+1}})$ *si y sólo si* $\mathcal{U}_2/\bigcap_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$ *no es cíclico y* $-1 \notin \bigcap_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$.
3. $\Omega^{(2)} = \mathbb{Q}(\zeta_{2^{n+2}})^-$ *si y sólo si* $\mathcal{U}_2/\bigcap_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$ *es cíclico y* $-1 \notin \bigcap_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$.

Demostración. Sea $K_{\mathfrak{g}^+} = K\Omega$ con Ω la máxima extensión abeliana de $\mathbb{Q}$ tal que $K_{\mathfrak{g}^+}/K$ es no ramificada en primos finitos.

Luego

$$\Omega = \prod_{p \text{ primo}} \Omega^{(p)} = \prod_{\substack{p \text{ primo} \\ \text{ram en } K/k}} \Omega^{(p)}$$

Se tiene $\Omega^{(p)} \subseteq \mathbb{Q}\left(\zeta_{p^{m_p}}\right)$ y $p\mathcal{O}_K = \wp_1^{e_1}\cdots\wp_r^{e_r}$. El índice de ramificación es $e_i = e_{K/\mathbb{Q}}(\wp_i/p)$. La extensión $\Omega^{(p)}/\mathbb{Q}$ es totalmente ramificada.

Sea $i \in \{1, \ldots, r\}$. Denotemos a $\wp_i$ por $\wp$ y a $\mathcal{U}_{K_\wp}$ por $\mathcal{U}_\wp$. Tenemos

$$\left[\Omega_\wp^{(p)} : \mathbb{Q}_p\right] = \left[\Omega^{(p)} : \mathbb{Q}\right] = e_{K/k}(\wp/p).$$

Consideremos ahora $M/\mathbb{Q}_p$, $M \subseteq \mathbb{Q}_p\left(\zeta_{p_{m_p}}\right)$ tal que $K_\wp M/K_\wp$ sea no ramificada.

Por el Lema 1.1.49, sabemos que $K_\wp M/K_\wp$ es no ramificada si y sólo si $\psi_{K_\wp M/K_\wp}(\mathcal{U}_\wp) = \{1\}$ y por el Lema 1.1.52, tenemos el siguiente diagrama conmutativo.

$$\begin{array}{ccc} K_\wp^* & \xrightarrow{\psi_{K_\wp M/K_\wp}} & \operatorname{Gal}(K_\wp M/K_\wp) \\ \Big\downarrow{\scriptstyle N_{K_\wp/\mathcal{O}_p}} & & \Big\downarrow{\scriptstyle \text{res}} \\ \mathbb{Q}_p^* & \xrightarrow[\psi_{M/\mathbb{Q}_p}]{} & \operatorname{Gal}\left(M/\mathbb{Q}_p\right) \end{array}$$

Luego, $K_\wp M/K_\wp$ es no ramificada si y solamente si $\operatorname{res}\circ\psi_{K_\wp M/K_\wp}(\mathcal{U}_\wp) = 1$ si y solamente si $\psi_{M/\mathbb{Q}_p}\left(N_{K_\wp/\mathbb{Q}_p}\mathcal{U}_\wp\right) = 1$ si y solamente si $N_{K_\wp/\mathbb{Q}_p}\mathcal{U}_\wp \subseteq \operatorname{nuc}\psi_{M/\mathbb{Q}_p} = N_{M/\mathbb{Q}_p}M^*$

Como siempre se cumple $N_{M/\mathbb{Q}_p}\mathcal{U}_\wp \subseteq \mathcal{U}_p$, tenemos $K_\wp M/K_\wp$ es no ramificada si y sólo si $N_{K_\wp/\mathbb{Q}_p}\mathcal{U}_p \subseteq \mathcal{U}_p \bigcap N_{M/\mathbb{Q}_p}M^*$.

Por el Lema 1.1.48, $\mathcal{U}_p \bigcap N_{M/\mathbb{Q}_p}M^* = N_{M/\mathbb{Q}_p}\mathcal{U}_M$, luego $K_\wp M/K_\wp$ es no ramificada si y sólo si $N_{K_\wp/\mathbb{Q}_p}\mathcal{U}_\wp \subseteq N_{M/\mathbb{Q}_p}\mathcal{U}_M$.

Volvemos a los campos globales. Consideramos la extensión $E/\mathbb{Q}$ con $E \subseteq \mathbb{Q}\left(\zeta_{p^{m_p}}\right)$. Entonces por la Observación 1.1.56, KE/K es no ramificada si y sólo si $(KE)_\mathfrak{P}/K_\wp$ es no ramificada para todo $\mathfrak{P} \mid \wp$ si y sólo si $\prod_{\wp|p} N_{K_\wp/\mathbb{Q}_p}\mathcal{U}_\wp = \prod_{i=1}^{r} N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i} \subseteq N_{K_\wp/\mathbb{Q}_p}\mathcal{U}_E$.

La extensión $K\Omega^{(p)}/K$ es abeliana y no ramificada en primos finitos y $\Omega^{(p)}$ es la máxima extensión de K con esta propiedad. Luego para tener $\Omega_p^{(p)}/\mathbb{Q}_p$ máximo, requerimos $N_{\Omega_p^{(p)}/\mathbb{Q}_p}\mathcal{U}_{\Omega_p^{(p)}}$ mínimo, lo cual corresponde a

$$\prod_{i=1}^{r} N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i} = N_{\Omega_p^{(p)}/\mathbb{Q}_p}\mathcal{U}_{\Omega_p^{(p)}}.$$

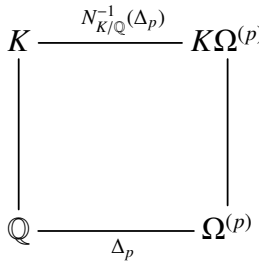
Regresamos al estudio de $\Omega^{(p)}$ para un primo p en general. La extensión $\Omega^{(p)}/\mathbb{Q}$ corresponde a un subgrupo abierto de índice finito Δ_p del grupo de idèles $\mathbb{J}_\mathbb{Q}$. Tenemos $\bar{\Delta}_p = N_{\Omega^{(p)}/\mathbb{Q}_p}\mathcal{C}_{\Omega^{(p)}}$, donde $\bar{\Delta}_p = \Delta_p\mathbb{Q}^*/\mathbb{Q}^*$ y $\operatorname{Gal}(\Omega^{(p)}/\mathbb{Q}) \cong \mathcal{C}_\mathbb{Q}/\bar{\Delta}_p \cong \mathbb{J}_\mathbb{Q}/\Delta_p\mathbb{Q}^*$.

Como en $\Omega^{(p)}$ es ramificado únicamente el primo p y posiblemente $\mathfrak{p}_\infty$, por el Corolario 1.1.61 se tiene

$$\Delta_p = H_p \times \prod_{\substack{q\neq p \\ q \text{ finito}}} \mathcal{U}_q \times \mathbb{R}^+,$$

donde $\mathcal{U}_p^{(m)} \subseteq H_p \subseteq \mathcal{U}_p$.

Por el Teorema 1.1.67, $K\Omega^{(p)}/K$ es el campo de clases correspondiente a $N_{K/\mathbb{Q}}^{-1}(\Delta_p)$.



Tenemos

$$K\Omega^{(p)}/K \longleftrightarrow N_{K/\mathbb{Q}}^{-1}(\Delta_p) \subseteq \left(\prod_{q \text{ finito}} \mathcal{U}_{\mathfrak{q}} \times \prod_{q \text{ real}} \mathbb{R}^*\right) \subseteq \mathbb{J}_K.$$

$$\Omega^{(p)}/\mathbb{Q} \longleftrightarrow \Delta_p \subseteq N_{K/\mathbb{Q}}\left(\prod_{\mathfrak{q} \text{ finito}} \mathcal{U}_{\mathfrak{q}} \times \prod_{\mathfrak{q} \text{ real}} \mathbb{R}^*\right) \subseteq \mathbb{J}_{\mathbb{Q}}.$$

Sea $\vec{\alpha} \in \prod_{q \text{ finito}} \prod_{q|\mathfrak{q}} \mathcal{U}_{\mathfrak{q}} \times \prod_{\mathfrak{q} \text{ real}} \mathbb{R}^*$, $\vec{\alpha} = (\alpha_{\mathfrak{q}})_{\mathfrak{q}}$. Entonces

$$\begin{aligned} N_{K/\mathbb{Q}}\vec{\alpha} &= \left(\prod_{q \text{ finito}} \prod_{\mathfrak{q}|q} N_{K_{\mathfrak{q}}/\mathbb{Q}_q}\alpha_{\mathfrak{q}}\right)\left(\prod_{\mathfrak{q} \text{ real}} N_{\mathbb{R}/\mathbb{R}}\alpha_{\mathfrak{q}}\right) \\ &= \underbrace{\prod_{\mathfrak{p}|p} N_{K_{\wp}/\mathbb{Q}_p}(\alpha_{\wp})}_{\text{en } H_p}\underbrace{\left(\prod_{\substack{q \neq p \\ q \text{ finito}}} \prod_{\mathfrak{q}|q} N_{K_{\mathfrak{q}}/\mathbb{Q}_q}\alpha_{\mathfrak{q}}\right)}_{\text{en } \prod_{\substack{q\neq p \\ q \text{ finito}}} \mathcal{U}_q}\underbrace{\left(\prod_{\mathfrak{q} \text{ real}} N_{\mathbb{R}/\mathbb{R}}\alpha_{\mathfrak{q}}\right)}_{\text{en } \mathbb{R}^*} \end{aligned}$$

Tenemos $\prod_{i=1}^{m_p} N_{K_{\wp_i}/\mathbb{Q}_p}\alpha_{\wp_i} \in H_p$. En efecto, sean $S_i = N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i} \times \prod_{\substack{q\neq p \\ q \text{ primo}}} \mathcal{U}_q \times \mathbb{R}^+ \subseteq \mathcal{U}_p \times \prod \mathcal{U}_q \times \mathbb{R}^+$ y $H_p := \prod_{i=1}^{r} S_i \subseteq$, donde $\operatorname{con}_{\mathbb{Q}/K} p = \wp_1^{e_1} \cdots \wp_r^{e_r}$.

Ahora, S_i corresponde a un campo $R_i \subseteq \mathbb{Q}\left(\zeta_{p^{m_p}}\right)$ y $\Delta_p = \prod_{i=1}^{r} S_i$ corresponde al campo $\bigcap_{i=1}^{r} R_i$, (véase [50, Teorema 17.6.49]). Más precisamente, $\Delta_p = H_p \times \prod_{q\neq p} \mathcal{U}_q \times \mathbb{R}^*$ es el que le corresponde a $\bigcap_{i=1}^{r} R_i$.

Luego

$$\operatorname{Gal}(\Omega^{(p)}/\mathbb{Q}) \cong \mathbb{J}_{\mathbb{Q}}/\Delta_p\mathbb{Q}^* \text{ y } N_{\Omega^{(p)}/\mathbb{Q}_p}\mathcal{C}_{\Omega^{(p)}} = \bar{\Delta}_p.$$

Por lo tanto $\operatorname{Gal}(\Omega^{(p)}/\mathbb{Q}) \cong \mathbb{J}_{\mathbb{Q}}/\Delta_p\mathbb{Q}^* = \frac{\mathcal{U}_p \times \prod_{q\neq p} \mathcal{U}_q \times \mathbb{R}^*}{H_p \times \prod_{q\neq p} \mathcal{U}_q \times \mathbb{R}^*} \cong \mathcal{U}_p/H_p$.

Luego $\operatorname{Gal}(R_i/\mathbb{Q}) \cong \mathcal{U}_p/S_i$. En consecuencia $[R_i : \mathbb{Q}] = \left[(R_i)_{\wp_i} : \mathbb{Q}_p\right] = \left[\mathcal{U}_p : N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i}\right]$ y $[\Omega^{(p)} : \mathbb{Q}] = [\bigcap_{i=1}^{r} R_i : \mathbb{Q}] = [\mathcal{U}_p : H_p]$ y si $p \geq 3$, además $[\Omega^{(p)} : \mathbb{Q}] = \operatorname*{mcd}_{1\leq i\leq r}[R_i : \mathbb{Q}] = \operatorname*{mcd}_{1\leq i\leq r}\left(\mathcal{U}_p : N_{K_{\wp_i}/\mathbb{Q}_p}\mathcal{U}_{\wp_i}\right)$.

Por la Proposición 1.3.1, para $p \geq 3$, si p es moderadamente ramificado precisamente en $\Omega^{(p)}/\Omega^{(p)\prime}$, entonces el índice de ramificación es $\left[\Omega^{(p)\prime} : \mathbb{Q}\right] = \operatorname{mcd}(e_1, \ldots, e_r, p-1)$.

Finalmente, puesto que $\operatorname{Gal}\left(\Omega^{(2)}/\mathbb{Q}\right) \cong \mathcal{U}_2/\prod_{\wp|2} N_{K_{\wp}/\mathbb{Q}}\mathcal{U}_{\wp}$, identificando la conjugación compleja J con $-1 \in \mathcal{U}_2$, tenemos por la Observación 1.1.34:

$\Omega^{(2)} = \mathbb{Q}\left(\zeta_{2^{n+2}}\right)^{+}$ si y sólo si $\mathrm{Gal}\left(\Omega^{(2)}/\mathbb{Q}\right)$ es cíclico y $J \in \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^{n+2}}\right)/\mathbb{Q}\left(\zeta_{2^{n+2}}\right)^{+}\right)$ si y sólo si $\mathcal{U}_2/\prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$ es cíclico y $-1 \in \prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$.

$\Omega^{(2)} = \mathbb{Q}\left(\zeta_{2^{n+1}}\right)$ si y sólo si $\mathrm{Gal}\left(\Omega^{(2)}/\mathbb{Q}\right)$ no es cíclico y $J \notin \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^{n+2}}\right)/\mathbb{Q}\left(\zeta_{2^{n+1}}\right)\right)$ si y sólo si $\mathcal{U}_2/\prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$ no es cíclico y $-1 \notin \prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$.

$\Omega^{(2)} = \mathbb{Q}\left(\zeta_{2^{n+2}}\right)^{-}$ si y sólo si $\mathrm{Gal}\left(\Omega^{(2)}/\mathbb{Q}\right)$ es cíclico y $J \notin \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^{n+2}}\right)/\mathbb{Q}\left(\zeta_{2^{n+2}}\right)^{-}\right)$ si y sólo si $\mathcal{U}_2/\prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$ es cíclico y $-1 \notin \prod_{\wp|2} N_{K_\wp/\mathbb{Q}_2}\mathcal{U}_\wp$.

□

Capítulo 2

Campos de géneros de campos de funciones

En este capítulo se presentan campos de funciones ciclotómicos y caracteres de Dirichlet para campos de funciones. Se ofrece una definición de campo de géneros extendido para campos de funciones (Definiciones 2.2.4, 2.2.7 y 2.2.9). Finalmente, se obtiene el campo de géneros extendido para campos de funciones (2.2.14), en términos de diversos campos auxiliares. Sean $k = \mathbb{F}_q(T)$ un campo de funciones racionales con $q = p^m$, p primo, $R_T = \mathbb{F}_q[T]$ el anillo de polinomios, $R_T^+ = \{P \in R_T \mid P \text{ es un polinomio mónico irreducible}\}$ y $\mathfrak{p}_\infty$, el polo del divisor T en k, el primo infinito de k.

2.1. Preliminares

2.1.1. Campos de funciones ciclotómicos

Lo que sigue fue tomado de [54] y [59].

Sea $k = \mathbb{F}_q(T)$ el campo de funciones racionales sobre el campo finito $\mathbb{F}_q$ con q elementos y sea $R_T = \mathbb{F}_q[T]$ el anillo de polinomios. Sea $\bar{k}$ una cerradura algebraica de k.

Sea $A = \mathrm{End}_{\mathbb{F}_q}(\bar{k}) = \left\{\varphi : \bar{k} \to \bar{k} \mid \varphi(a+b) = \varphi(a) + (b),\ \varphi(\alpha a) = \alpha\varphi(a)\ \forall \alpha \in \mathbb{F}_q \text{ y } \forall a, b \in \bar{k}\right\}$.

Entonces A es una $\mathbb{F}_q$-álgebra que consiste de los $\mathbb{F}_q$ endomorfismos del grupo aditivo de $\bar{k}$. Se consideran los siguientes elementos.

1. Sea φ el automorfismo de Frobenius de $\bar{k}$ sobre $\mathbb{F}_q$, es decir $\varphi : \bar{k} \to \bar{k}$ está dado por $u \mapsto u^q$.

2. Sea μ_T la multiplicación por T, esto es, $\mu_T : \bar{k} \to \bar{k}$ está dado por $u \mapsto Tu$.

Notación 2.1.1. Si $u \in \bar{k}$ y $N \in R_T$, entonces

$$u^N = N(\varphi + \mu_T)(u).$$

Definición 2.1.2. Sea Λ_N el conjunto de elementos en $\bar{k}$ correspondientes a los elementos de N torsión de $\bar{k}$, es decir, $\Lambda_N = \left\{u \in \bar{k} \mid u^N = 0\right\}$= conjunto de ceros del polinomio u^N en u, Λ_N es llamado el *módulo de Carlitz-Hayes de N*.

Proposición 2.1.3. *u^N es un polinomio separable en u de grado q^d, donde $N \in R_T$ es de grado d. Por tanto Λ_N es un $\mathbb{F}_q$-espacio vectorial de dimensión d.*

Demostración. Véase [59, Proposición 12.2.11]. □

Proposición 2.1.4. *Si $N = P^n$, con $P \in R_T$ irreducible y $n \in \mathbb{N}$. Entonces Λ_N es un R_T-módulo cíclico.*

Demostración. Véase [59, Proposición 12.2.14]. □

Teorema 2.1.5. *Para cada $N \in R_T \setminus \{0\}$, el R_T-módulo Λ_N es canónicamente isomorfo a $R_T/(N)$. En particular Λ_N es un R_T-módulo cíclico.*

Demostración. Véase [59, Teorema 12.2.17]. □

Definición 2.1.6. Para $N \in R_T \setminus \{0\}$, se define $\Phi(N) = |(R_T/(N))^*|$. Es decir,

$$\Phi(N) = \left|\{M \in R_T \mid (N, M) = 1,\ \text{gr}\, M < \text{gr}\, N\}\right|$$

es la *cardinalidad del grupo de unidades* de $R_T/(N)$.

Proposición 2.1.7. *El R_T-módulo cíclico Λ_N contiene precisamente $\phi(N)$ generadores. De hecho, si λ es algún generador de Λ_N, entonces para $A \in R_T$, λ^A es un generador si y sólo si $(A, N) = 1$.*

Demostración. Véase [59, Proposición 12.2.21]. □

Observación 2.1.8. Si $N \in R_T \setminus \{0\}$, entonces para $A = \alpha \in \mathbb{F}_q^* \subseteq (R_T/(N))^*$ tenemos $\sigma_A(\lambda) = \sigma_\alpha(\lambda) = \lambda^\alpha = \alpha\lambda$, donde $\lambda = \lambda_N$ es un generador de λ_N.

Definición 2.1.9. Sea $N \in R_T \setminus \{0\}$. Al campo $K_N = k(\Lambda_N) = k(\lambda_N)$ generado sobre $k = \mathbb{F}_q(T)$ al adjuntarle la N-torsión del módulo de Carlitz-Hayes $\Lambda_N = \left\{u \in \bar{K} \mid u^N = 0\right\}$ se le llama el *campo de funciones ciclotómico* determinado por Λ_N sobre k.

Proposición 2.1.10. *$k(\Lambda_N)/k$ es una extensión de Galois.*

Demostración. Véase [59, Proposición 12.3.3] □

Definición 2.1.11. Para $N \in R_T \setminus \{0\}$ sea $G_N := \mathrm{Gal}\ (k(\Lambda_N)/k)$ el *grupo de Galois* de $k(\Lambda_N)/k$.

Proposición 2.1.12. *G_N es un subgrupo de $(R_T/(N))^*$. En particular $k(\Lambda_N)/k$ es una extensión abeliana y $\left[(\Lambda_N) : k\right] \leq \Phi(N)$.*

Demostración. Véase [59, Proposición 12.3.7]. □

Proposición 2.1.13. *Sean $N = P^n$, P polinomio mónico irreducible con $d = \mathrm{gr}\, P$ y $\mathfrak{p}$ el divisor de k asociado a P. Entonces todo divisor primo de k diferente de $\mathfrak{p}$ y $\mathfrak{p}_\infty$ es no ramificado en $k(\Lambda_{P^n})$ y el índice de ramificación de $\mathfrak{p}$ en $k(\Lambda_{P^n})/k$ es $e(\mathfrak{p}) = \Phi(P^n) = q^{nd} - q^{(n-1)d} = q^{(n-1)d}(q^d - 1) = [k(\Lambda_N) : k]$.*

Véase [59, Proposición 12.3.14] y [21].

Teorema 2.1.14. *Sea $N \in R_T \setminus \{0\}$ mónico. Entonces*

1. *$G_N = \mathrm{Gal}\,(k(\Lambda_N)/k) \cong (R_T/(N))^*$.*
2. *$[k(\Lambda_N) : k] = \Phi(N)$.*
3. *Si $N = P^n$, para algún polinomio irreducible P y $\mathfrak{p}$ es el divisor de k asociado a P, entonces $\mathfrak{p}$ es totalmente ramificado en $k(\Lambda_N)/k$.*

Demostración. Véase [59, Teorema 12.3.6]. □

Definición 2.1.15. El *subcampo real maximal* $K_N^+ = K_N^{\mathbb{F}_q^*}$ es el máximo subcampo de K_N en el que $\mathfrak{p}_\infty$ se descompone totalmente. Si $k \subseteq K \subseteq k(\Lambda_N)$, definimos el *subcampo real maximal de K* por

$$K^+ := K \cap k(\Lambda_N)^+ .$$

Proposición 2.1.16. *En un campo ciclotómico hay $\Phi(N)/(q-1)$ lugares de $k(\Lambda_N)$ sobre el lugar infinito $\mathfrak{p}_\infty$ de k, cada uno de grado uno y su índice de ramificación es $e_{\mathfrak{p}_\infty} = 1$. Es decir, el subcampo real maximal $k(\Lambda_N)^+$ de $k(\Lambda_N)$, fijo por el grupo de inercia de cualquier divisor primo $\mathfrak{P}$ de $k(\Lambda_N)$ sobre $\mathfrak{p}_\infty$ es tal que $[k(\Lambda_N) : k(\Lambda_N)^+] = q - 1$ y $\mathfrak{p}_\infty$ se descompone totalmente en $\Phi(N)/(q-1)$ divisores primos en $k(\Lambda_N)^+/k$.*

Demostración. Véase [59, Proposición 12.4.5 y Proposición 12.5.4]. □

En este punto consideramos que sería deseable determinar explícitamente condiciones necesarias y suficientes para que el grupo de Galois del campo ciclotómico $k(\Lambda_{p^\alpha})/k$ sea cíclico, para así tener resultados análogos a los encontrados para campos numéricos.

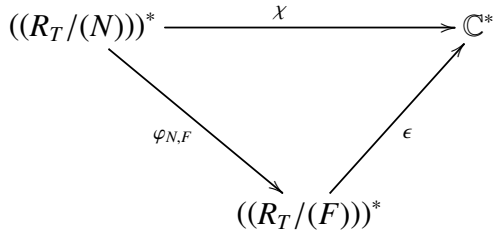
2.1.2. Caracteres de Dirichlet para campos de funciones

De [59] tenemos las siguientes definiciones y propiedades referentes a caracteres de Dirichlet para campos de funciones.

Definición 2.1.17. Sea $N \in R_T \setminus \{0\}$ un polinomio mónico. Un *caracter de Dirichlet* mód N es un homomorfismo

$$\chi : ((R_T/(N)))^* \to \mathbb{C}^*.$$

Teorema 2.1.18. *Dado un caracter de Dirichlet χ, existe un único polinomio mónico F de R_T de grado mínimo que divide a N tal que χ puede ser definido módulo F.*



Definición 2.1.19. Dado un caracter de Dirichlet χ mód N el *conductor* de χ es F si $F \in R_T$ es un polinomio mónico de grado mínimo que divide N tal que χ puede ser definido mód F. Se denota por F_χ.

Definición 2.1.20. Sea G un grupo finito. El *grupo de caracteres de G* es $\hat{G} = \hom(G, \mathbb{C}^*)$.

Proposición 2.1.21. *Cualquier grupo abeliano finito G es isomorfo a su grupo de caracteres $\hat{G}$.*

Definición 2.1.22. Sea $N \in R_T \setminus \{0\}$ y sea $\chi \in \left(\widehat{R_T/(N)}\right)^* \cong \hat{G}_N = \mathrm{Gal}\left(\widehat{K(\Lambda_N)}/K\right)$ un caracter de Dirichlet mód N. Se tiene $\mathbb{F}_q^* \subseteq G_N$. Decimos que χ es *par* si $\chi(\alpha) = 1$ para todo $\alpha \in \mathbb{F}_q^*$, e *impar* en otro caso.

Definición 2.1.23. Sean X un grupo finito de caracteres de Dirichlet, $N := \mathrm{mcm}\{F_\chi \mid x \in X\}$, $H := \bigcap_{x \in X} \mathrm{nuc}\,\chi$ y $K := k(\Lambda_N)^H$. Decimos que K es el *campo asociado* a X y si $X = \langle\chi\rangle$, decimos que K es el campo asociado a χ.

Proposición 2.1.24. *Sean X_1, X_2 dos grupos de caracteres de Dirichlet y sean $K_i = K_{X_i}$, $(i = 1, 2)$ los campos asociados a X_i. Entonces*

- $X_1 \subseteq X_2$ *si y sólo si* $K_1 \subseteq K_2$,
- $K_{\langle X_1, X_2\rangle} = K_1 K_2$.

Sea $N \in R_T \setminus \{0\}$ y sea $N = \prod_{i=1}^{r} P_i^{\alpha_i}$ su descomposición como producto de polinomios irreducibles. Entonces $(R_T/(N))^* \cong \prod_{i=1}^{r} \left(R_T/P_i^{\alpha_i}\right)^*$.

Si χ es un caracter de Dirichlet mód N, entonces tenemos $\chi = \prod_{i=1}^{r} \chi_{P_i}$, donde χ_{P_i} es un caracter mód $P_i^{\alpha_i}$. Es decir, $\chi(A \text{ mód } N) = \prod_{i=1}^{r} \chi_{P_i}\left(A \text{ mód } P_i^{\alpha_i}\right)$.

Definición 2.1.25. Sea X un grupo finito de caracteres de Dirichlet. Entonces para un polinomio mónico irreducible $P \in R_T$ definimos $X_P = \{\chi_P \mid \chi \in X\}$.

Teorema 2.1.26. *Sea X un grupo finito de caracteres de Dirichlet y K_X su campo asociado. Sea $P \in R_T \setminus \{0\}$ un polinomio irreducible y consideremos $(P)_K = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\text{gr}\,P}}$. Sea $\mathfrak{P}$ un divisor primo de K_X que está sobre $\mathfrak{p}$ y sea $e = e(\mathfrak{P} \mid \mathfrak{p})$. Entonces $e = |X_P|$.*

2.2. Campos de géneros de campos de funciones

Definición 2.2.1. Sea K una extensión finita de k y sea S un conjunto finito no vacío de divisores primos de K. El *campo de clases de Hilbert de K relativo a S*, $K_{H,S}$, es la máxima extensión abeliana no ramificada de K, donde cada elemento de S se descompone totalmente. (véase [47])

En lo que sigue, para cualquier extensión finita K de k, consideraremos S como el conjunto de divisores primos de K que dividen a $\mathfrak{p}_\infty$ y escribiremos K_H en vez de $K_{H,S}$.

Definición 2.2.2. Sea K una extensión finita separable de k. El *campo de géneros $K_\mathfrak{g}$ de K con respecto a k* es la máxima extensión de K contenida en K_H que es la composición de K y una extensión abeliana de k. Equivalentemente, $K_\mathfrak{g} = K\omega$, donde ω es la máxima extensión abeliana de k contenida en K_H.

Observación 2.2.3. Como en el caso numérico, existe ω máximo con esta propiedad y así lo tomaremos. También como en el caso numérico, si K/k es abeliana, $K_\mathfrak{g} = \omega$. Además como en el caso numérico, para K/k finita y separable, $\omega_\mathfrak{g} = \omega$.

Definición 2.2.4. Sea E un campo tal que $k \subseteq E \subseteq k(\Lambda_N)$ para algún $N \in R_T$. Sean X el grupo de caracteres asociado a E y $Y = \prod_{P \in R_T} X_P$. Por analogía con el caso de campos numéricos, definimos el *campo de géneros extendido* $E_{\mathfrak{g}^+}$ *de* E *con respecto a* k como el campo asociado a Y.

Observación 2.2.5. Tenemos que $E_{\mathfrak{g}^+}/E$ es la máxima extensión abeliana no ramificada en los primos finitos contenida en $k(\Lambda_N)$. El campo de géneros de E es $E_{\mathfrak{g}} = EE^+_{\mathfrak{g}^+}$, donde $E^+_{\mathfrak{g}^+} = E_{\mathfrak{g}^+} \cap k(\Lambda_N)^+$.

Notación 2.2.6. Sea K una extensión finita separable de k. Para $n \in \mathbb{N} \cup \{0\}$, denotamos ${}_nK := KL_n$, donde L_n es el más grande subcampo del campo ciclotómico $k\left(\Lambda_{\frac{1}{T^{n+1}}}\right)$, donde $\mathfrak{p}_\infty$ es puramente salvaje y totalmente ramificado, de hecho, $L_n = k\left(\Lambda_{1/T^{n+1}}\right)^{\mathbb{F}_q^*}$ y $[L_n : k] = q^n$. Para $m \in \mathbb{N}$, escribimos $K_m := K\mathbb{F}_{q^m}$.

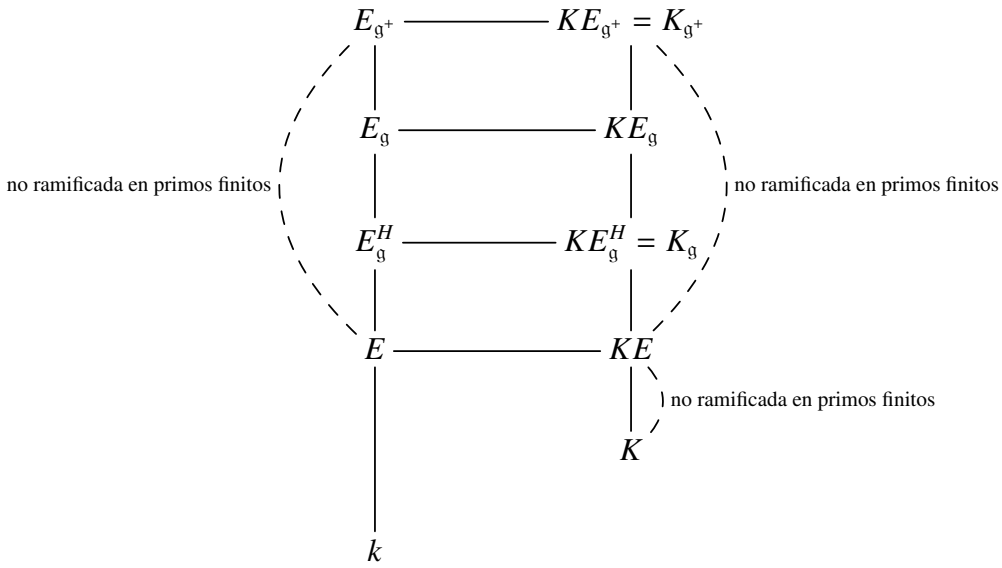
Sea K/k una extensión abeliana finita. Entonces, por el Teorema de Kronecker-Weber, (véase [50, Teorema 13.2.1]) $K \subseteq {}_nk(\Lambda_N)_m$, para algunos $n \in \mathbb{N} \cup \{0\}$, $N \in R_T$ y $m \in \mathbb{N}$. Entonces por [5, Teorema 2.2], $K_{\mathfrak{g}} = KE^H_{\mathfrak{g}}$, donde $E = KM \cap k(\Lambda_N)$, $M = L_nk_m$ y H es la restricción a $E_{\mathfrak{g}}$ del grupo de descomposición de los primos infinitos en $KE_{\mathfrak{g}}/K$. Notemos que $E \subseteq k(\Lambda_N)$.

Definición 2.2.7. Sea K una extensión abeliana finita de k. Con la notación anterior, definimos el *campo de géneros extendido de* K *con respecto a* k por

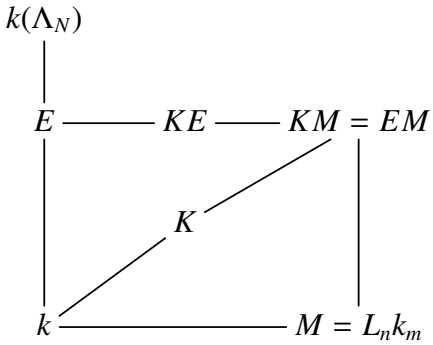
$$K_{\mathfrak{g}^+} := KE_{\mathfrak{g}^+}.$$

Proposición 2.2.8. *Sea* K *una extensión abeliana finita. Con la notación anterior, tenemos* $K_{\mathfrak{g}^+}/K$ *es no ramificada en los primos finitos y es moderadamente ramificada en* $\mathfrak{p}_\infty$ *y* $[K_{\mathfrak{g}^+} : K_{\mathfrak{g}}] \mid q - 1$.

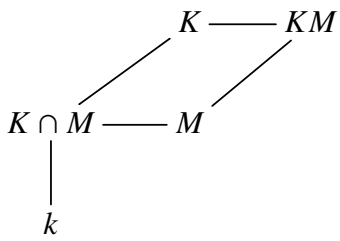
Demostración. Tenemos $E_{\mathfrak{g}^+}/E$ es no ramificada en los primos finitos, luego $K_{\mathfrak{g}^+}/KE$ es no ramificada en los primos finitos.



Veamos que KE/K es no ramificada en los primos finitos. Por [5, demostración del teorema 2.2], tenemos $KM = EM$. Puesto que en M/k el único primo posiblemente ramificado es $\mathfrak{p}_\infty$, $KM = EM/E$ es no ramificada en los primos finitos.



Lo mismo para KM/K.



Como $K \subseteq KE \subseteq KM = EM$, la extensión KE/K también es no ramificada en primos finitos. Concluimos que $K_{\mathfrak{g}^+}/K$ es no ramificada en primos finitos.

Se tiene $E_{\mathfrak{g}^+}/k$ es moderadamente ramificada en $\mathfrak{p}_\infty$, luego $KE_{\mathfrak{g}^+}/K$ lo es. Como $K_{\mathfrak{g}^+} = KE_{\mathfrak{g}^+}$, tenemos $K_{\mathfrak{g}^+}/K$ es moderadamente ramificada en $\mathfrak{p}_\infty$.

Tenemos $e_\infty\left(E_{\mathfrak{g}^+}/E\right) \Big| q-1$ y $H \subseteq I_\infty(E_\mathfrak{g}/k)$, el grupo de inercia de $\mathfrak{p}_\infty$ en la extensión $E_\mathfrak{g}/k$, ya que $f_\infty(E_\mathfrak{g}/k) = 1$. Así pues, tenemos que $\mathfrak{p}_\infty$ es totalmente ramificado en $E_{\mathfrak{g}^+}/E_\mathfrak{g}^H$. Por lo que $\left[E_{\mathfrak{g}^+} : E_\mathfrak{g}^H\right] = e_\infty\left(E_{\mathfrak{g}^+}/E_\mathfrak{g}^H\right) \Big| e_\infty\left(k(\Lambda_N)/k\right) = q-1$. Entonces $\left[E_{\mathfrak{g}^+} : E_\mathfrak{g}^H\right] \Big| q-1$ y por lo tanto $\left[K_{\mathfrak{g}^+} : K_\mathfrak{g}\right] \Big| q-1$. □

Por analogía a la Definión 1.2.1 (4), en el caso de campos numéricos, proponemos la siguiente definición.

Definición 2.2.9. Sea K/k una extensión finita separable. Definimos el *campo de géneros extendido de K con respecto a k* como $K_{\mathfrak{g}^+} := K\omega_{\mathfrak{g}^+}$. Si denotamos $\Omega := \omega_{\mathfrak{g}^+}$, entonces

$$K_{\mathfrak{g}^+} = K\Omega.$$

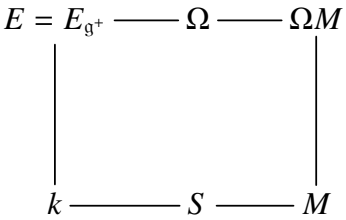
Observación 2.2.10. Notemos que la extensión Ω/k es abeliana y máxima con respecto a esta propiedad.

En adelante, a menos que se diga lo contrario, consideraremos

$$\Omega \subseteq {}_nk\left(\Lambda_N\right)_m$$

con n, N, m mínimos, es decir, para $n \in \mathbb{N} \cup \{0\}, N \in R_T^+$, $m \in \mathbb{N}$, m es el conductor de constantes. Llamamos a (m, N, n) el *conductor* de Ω.

Sean $M := L_nk_m$ y $E := \Omega M \cap k(\Lambda_N)$. Entonces $EM = \Omega M$. Luego $\Omega_\mathfrak{g} = \Omega = \Omega E_{\mathfrak{g}^+}$. Por lo tanto $E_{\mathfrak{g}^+} \subseteq \Omega$ y así $E = E_{\mathfrak{g}^+}$. En efecto, $E_{\mathfrak{g}^+} \subseteq \Omega \subseteq \Omega M = EM$, entonces $E_{\mathfrak{g}^*}M \subseteq EM$, por correspondencia de Galois $E_{\mathfrak{g}^+} \subseteq E$ y por lo tanto $E_{\mathfrak{g}^+} = E$.



Sea $S := \Omega \cap M$. Tenemos $S \subseteq M = L_nk_m$. Como n, m son mínimos $S \nsubseteq L_{n-1}k_m$ y $S \nsubseteq L_nk_r$ con $r \mid m$ y $r < m$, pues si $S \subseteq L_{n_1}k_{m_1}$, entonces $\Omega = SE \subseteq {}_{n_1}k(\Lambda_N)_{m_1}$, luego $m \mid m_1$ y $n \leq n_1$.

Ahora bien, sea $X = Y = \prod_{P\in R_T^+} X_P$ el grupo de caracteres de Dirichlet asociado a $E_{g^+} = E$. Entonces si $E^{(P)}$ es el campo asociado a X_P, con $P \in R_T^+$, $E = \prod_{P\in R_T^+} E^{(P)}$, donde $E^{(P)} = k$ para casi todo P y si $P_1, \ldots, P_r$ son los primos finitos ramificados en E/k, $X_{P_i} \neq \{1\}$, $E^{(P_i)} \neq k$, $E^{(P_i)} \cap \prod_{j\neq i} E^{(P_j)} = k$, $1 \leq i \leq r$ y $E = E^{(P_1)} \ldots E^{(P_r)}$, $\widehat{\mathrm{Gal}(E/k)} \cong X = Y = \prod_{P\in R_T^+} X_P = \prod_{P\in R_T^+} \widehat{\mathrm{Gal}(E^{(P)}/k)} \cong \prod_{i=1}^{r} \widehat{\mathrm{Gal}(E^{(P_i)}/k)}$. Por lo tanto

$$\mathrm{Gal}\,(E/k) \cong \prod_{i=1}^{r} \mathrm{Gal}\left(E^{(P_i)}/k\right).$$

Para calcular Ω necesitamos conocer S, es decir, el comportamiento de $\mathfrak{p}_\infty$ y también cada $E^{(P)}$ para $P \in R_T^+$. Primero tenemos que si $P \in R_T^+$ es no ramificado en K/k, entonces P es no ramificado en E/k y por lo tanto en Ω/k. En efecto, si P es ramificado en Ω/k, entonces se tiene

$$e_P\,(K\Omega/K) = e_P\,(K\Omega/K)\,e_P\,(K/k) = e_P\,(K\Omega/k) = e_P\,(K\Omega/\Omega)\,e_P\,(\Omega/k) > 1,$$

así que $e_P\,(K\Omega/K) > 1$ contrario a la definición de Ω.

$$\begin{array}{ccc} K & \text{———} & K\Omega \\ | & & | \\ | & & | \\ k & \text{———} & \Omega \end{array}$$

Por lo tanto es suficiente conocer $E^{(P_i)}$, $1 \leq i \leq r$, donde $P_1, \ldots, P_r$ son los primos finitos ramificados en K/k y por lo tanto esos son los únicos primos finitos ramificados en E/k y en Ω/k. Ahora, en $E^{(P)}/k$ el único primo finito ramificado es P y $\mathfrak{p}_\infty$ es moderadamente ramificado. Notemos que el índice de ramificación moderada de $\mathfrak{p}_\infty$ en E/k y en Ω/k es el mismo. Esto es consecuencia de que $\Omega = ES$.

Para cualquier subconjunto finito no vacío $\mathcal{A} \subseteq R_T^+$, definimos $E^{(\mathcal{A})} := \prod_{P\in\mathcal{A}} E^{(P)}$. Podemos considerar $E^{(P)}$ como la P-componente de E.

$$\begin{array}{ccccc}
E = \prod\limits_{P\in R_T^+} E^{(P)} = E_{\mathfrak{g}^+} & \longrightarrow & \Omega = ES & \longrightarrow & \Omega M = EM \\
\big| & & \big| & & \big| \\
E^{(P)} & \longrightarrow & \Omega^{(P)} = E^{(P)}S & \longrightarrow & \Omega^{(P)}M = E^{(P)}M \\
\big| & & \big| & & \big| \\
k & \longrightarrow & S = \Omega \cap M & \longrightarrow & M
\end{array}$$

Definimos $\Omega^{(P)} := E^{(P)}M \cap \Omega$. Tenemos que $E^{(P)} \subseteq E \subseteq \Omega$ y $E^{(P)} \subseteq E^{(P)}M$. Por lo que $E^{(P)} \subseteq \Omega^{(P)}$. De la correspondencia de Galois se tiene

$$\Omega^{(P)} = E^{(P)}S.$$

Para cualquier subconjunto finito no vacío $\mathcal{A} \subseteq R_T^+$, tenemos $\Omega^{(\mathcal{A})} := E^{(\mathcal{A})}M \cap \Omega$. De la correspondencia de Galois obtenemos $\Omega^{(\mathcal{A})} = E^{(\mathcal{A})}S$. En particular

$$\Omega^{(\mathcal{A})} = \left(\prod_{P\in\mathcal{A}} E^{(P)}\right)S = \prod_{P\in\mathcal{A}} \left(E^{(P)}S\right) = \prod_{P\in\mathcal{A}} \Omega^{(P)}.$$

Proposición 2.2.11. *Para $A, B \in R_T \setminus \{0\}$, sea $\Omega^{(A)} := E^{(A)}M \cap \Omega$, donde $E^{(A)} := \prod\limits_{\substack{P|A \\ P\in R_T^+}} E^{(P)}$, esto es $E^{(A)} = E^{(\mathcal{A})}$ y $\Omega^{(A)} = \Omega^{(\mathcal{A})}$, donde $\mathcal{A} = \left\{P \in R_T^+ \mid P \mid A\right\}$. Tenemos*

1. $\Omega^{(AB)} = \Omega^{(A)}\Omega^{(B)}$.

2. *Si* $\operatorname{mcd}(A, B) = 1$, *tenemos* $\Omega^{(A)} \cap \Omega^{(B)} = S = \Omega \cap M$.

3. $\Omega^{(A)} \supseteq S$ *para todo* $A \in R_T$ *y* $\Omega^{(A)} = S$ *si y sólo si* $P_i \nmid A$ *para todo* $1 \leq i \leq n$.

Demostración. 1. Se sigue de la discusión anterior.

2. Tenemos $E^{(A)} = \prod\limits_{P|A} E^{(P)}$, $E^{(B)} = \prod\limits_{P|B} E^{(P)}$ y $\left\{P \in R_T^+ \mid P \mid A\right\} \cap \left\{P \in R_T^+ \mid P \mid B\right\} = \emptyset$. Por lo tanto $E^{(A)} \cap E^{(B)} = k$ y $k\Omega \cap M = \Omega \cap M = S$. Por correspondencia de Galois tenemos el resultado.

3. Para $P \in R_T^+$, $\Omega^{(P)} = E^{(P)}M \cap \Omega \supseteq M \cap \Omega = S$ y $\Omega^{(P)} \neq S$ si y sólo si $P \in \{P_1, \ldots, P_r\}$. En efecto, $\Omega^{(P)} = E^{(P)}M \cap \Omega \neq S$ si y sólo si $E^{(P)}M \neq M$ si y sólo si $E^{(P)} \neq k$ si y sólo si $P \in \{P_1, \ldots, P_r\}$.

□

Teorema 2.2.12. *Con la notación anterior se tiene*

$$\Omega = \prod_{P\in R_T^+} \Omega^{(P)} = \prod_{i=1}^{n} \Omega^{(P_i)}.$$

Demostración.

Tenemos

$$\begin{aligned}\Omega = EM \cap \Omega &= \left(\prod_{i=1}^{r} E^{(P_i)}\right) M \cap \Omega = \prod_{i=1}^{r} \left(E^{(P_i)} M \cap \Omega\right) \\ &= \prod_{i=1}^{r} \Omega^{(P_i)} = \prod_{i=1}^{r} \Omega^{(P_i)} \cdot \prod_{P\notin\{P_1,\ldots,P_r\}} S = \prod_{P\in R_T^+} \Omega^{(P)}.\end{aligned}$$

Por lo tanto,

$$\Omega = \prod_{i=1} \Omega^{(P_i)} = \prod_{P\in R_T^+} \Omega^{(P)}.$$

□

Proposición 2.2.13. *Sea K una extensión finita separable de k. Sean $P \in R_T^+$, $d_P = \operatorname{gr} P$ y $e_P(\Omega/k) = e_P^{(0)} e_P^{(S)}$, donde $\operatorname{mcd}\left(p, e_P^{(0)}\right) = 1$ y $e_P^{(S)} = p^{\alpha_P}$ para algún $\alpha_P \geq 0$ y supongamos $\operatorname{con}_{k/K} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_{m_P}^{e_{m_P}}$. Entonces $e_P^{(0)} = \operatorname{mcd}\left(e_1, \ldots, e_{m_P}, q^{d_P} - 1\right)$.*

Demostración. Puesto que Ω/k es abeliana, $e_P^{(0)} \mid q^{d_P} - 1$, (véase [50, Proposición 10.4.8]). Consideremos $k_P^{(0)}/k$ de manera que P es el único primo finito ramificado, $k_P^{(0)} \subseteq \Omega$ y $[k_P^{(0)} : k] = e_P^{(0)}$. Entonces $Kk_P^{(0)} \subseteq K_{\mathfrak{g}^+}$ y $Kk_P^{(0)}/K$ es no ramificada. Sea $\mathfrak{P}$ un primo en $Kk_P^{(0)}$ sobre P. Entonces $\mathfrak{P} \cap K = \mathfrak{p}_i$ para algún i. Luego, por el Lema de Abhyankar, tenemos

$$e_{\mathfrak{P}}\left(Kk_P^{(0)}/k\right) = \operatorname{mcm}\left[e_{\mathfrak{p}_i}(K/k), e_P^{(0)}\right] = \operatorname{mcm}\left[e_i, e_P^{(0)}\right].$$

Por lo tanto, $e_P^{(0)} \mid e_i$ para todo $i = 1, \ldots, m_P$. Puesto que $e_P^{(0)}$ es máximo tenemos

$$e_P^{(0)} = \operatorname{mcd}\left(e_1, \ldots, e_{m_P}, q^{d_P} - 1\right).$$

□

Finalmente, nuestro teorema principal para campos de funciones globales es el siguiente.

Teorema 2.2.14. *Sea K/k una extensión finita y separable, donde $k = \mathbb{F}_q(T)$. Sea $K_{\mathfrak{g}^+} = K\Omega$. Entonces*

$$\Omega = \prod_{P \in R_T^+} \Omega^{(P)},$$

donde $\Omega^{(P)} = E^{(P)}S$, $S = \Omega \cap M$ y $k \subseteq E^{(P)} \subseteq k(\Lambda_{P^{c_P}})$ corresponde a $\prod_{j=1}^{m_P} N_{K_{P_j}/k_P} \mathcal{U}_{P_j}$. En particular

$$\left[E^{(P)} : k\right] = \left[\mathcal{U}_P : \prod_{j=1}^{m_P} N_{K_{\mathfrak{p}}/k_P} \mathcal{U}_{\mathfrak{p}_j}\right],$$

donde $\operatorname{con}_{k/K} P = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_{m_P}^{e_{m_P}}$.

La parte moderadamente ramificada de $\Omega^{(P)}/k$ está dada por

$$e_P^{(0)} = \operatorname{mcd}\left(e_1, \dots, e_{m_P}, q^{d_P} - 1\right),$$

con $d_P = \operatorname{gr}_k P$.

Demostración. Aplicamos el Teorema 1.1.67 al siguiente diagrama

$$\begin{array}{ccc} K & \xrightarrow{N_{K/k}^{-1}(\Delta_P)} & KE^{(P)} \\ | & & | \\ k & \xrightarrow[\Delta_P]{} & E^{(P)} \end{array}$$

esto es, $KE^{(P)}$ es el campo de clases de $N_{K/k}^{-1}(\Delta_P)$.

Como $E^{(P)}$ es máximo en el sentido de que P es el único primo finito ramificado en $E^{(P)}/k$ y $KE^{(P)}/K$ es no ramificado en cada primo finito, tenemos que Δ_P satisface

$$N_{K/k}^{-1}(\Delta_P) \subseteq \prod_{Q \in R_T^+} \prod_{\mathfrak{p}|Q} \mathcal{U}_{\mathfrak{p}} \times \prod_{\mathfrak{P}_\infty|\mathfrak{p}_\infty} K_{\mathfrak{P}_\infty}^* \subseteq \mathbb{J}_K,$$

o equivalentemente,

$$\Delta_P \subseteq N_{K/k}\left(\prod_{Q \in R_T^+} \prod_{\mathfrak{p}|Q} \mathcal{U}_{\mathfrak{p}} \times \prod_{\mathfrak{P}_\infty|\mathfrak{p}_\infty} K_{\mathfrak{P}_\infty}^*\right).$$

Sea $\vec{\alpha} \in \prod_{Q \in R_T^+} \prod_{\mathfrak{p}|Q} \mathcal{U}_{\mathfrak{p}} \times \prod_{\mathfrak{P}_\infty|\mathfrak{p}_\infty} K_{\mathfrak{P}_\infty}^*$, $\vec{\alpha} = (\alpha_{\mathfrak{p}})_{\mathfrak{p}}$. Entonces

$$N_{K/k}\vec{\alpha} = \prod_{Q \in R_T^+} \left(\prod_{\mathfrak{p}|Q} N_{K_{\mathfrak{p}}/k_Q} \alpha_{\mathfrak{p}}\right) \times \prod_{\mathfrak{P}_\infty|\mathfrak{p}_\infty} N_{K_{\mathfrak{P}_\infty}/k_\infty} \alpha_{\mathfrak{P}_\infty}.$$

Para $Q \neq P$, Q es no ramificado en $\Omega^{(P)}/k$, por lo tanto, para $\mathfrak{Q} \mid Q$, $K_{\mathfrak{Q}}/k_Q$ es no ramificado y en particular es una extensión cíclica. Entonces por [50, Teorema 17.2.17], $N_{K_{\mathfrak{Q}}/k_Q}\mathcal{U}_{\mathfrak{Q}} = \mathcal{U}_Q$.

Para $Q = P$ tenemos

$$\prod_{\mathfrak{p}|P} N_{K_{\mathfrak{p}}/k_P}\alpha_{\mathfrak{p}} = \prod_{j=1}^{m_P} N_{K_{\mathfrak{p}_j}/k_P}\alpha_{\mathfrak{p}_j},$$

donde $\mathrm{con}_{k/K} P = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_{m_P}^{e_{m_P}}$.

Se sigue que $\prod_{j=1}^{m_P} N_{K_{\mathfrak{p}_j}/k_P}\alpha_{\mathfrak{p}_j} \in H_P$. En otras palabras, si

$$S_j := N_{K_{\mathfrak{p}_j}/k_P}\mathcal{U}_{\mathfrak{p}_j} \times \prod_{\substack{Q\in R_T^+ \\ Q\neq P}} \mathcal{U}_Q \times \left[(\pi) \times \mathcal{U}_\infty^{(1)}\right] \subseteq \mathcal{U}_P \times \prod_{\substack{Q\in R_T^+ \\ Q\neq P}} \mathcal{U}_Q \times \left[(\pi) \times \mathcal{U}_\infty^{(1)}\right],$$

tenemos

$$\Delta_P = \prod_{j]=1}^{m_P} S_j \text{ y } H_P = \prod_{j=1}^{m_P} N_{K_{\mathfrak{p}_j}/k_P}.$$

Ahora, si S_j está en el grupo de normas del campo $R_j \subseteq {}_nk(\Lambda_{P^{c_j}})_m$ para algún $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N}$ y $c_j \in \mathbb{N}$, entonces $\prod_{j=1}^{m_P} S_j$ es la norma del grupo $\bigcap_{j=1}^{m_P} R_j$.

Se sigue que $\left[C_k : k^*S_j\right] = \left[\mathcal{U}_P : N_{K_{\mathfrak{p}_j}/k_P}\mathcal{U}_{\mathfrak{p}_j}\right]$ y $\mathrm{Gal}\left(R_j/k\right) \cong \mathcal{C}_k/k^*S_j$. Por lo tanto, $\left[R_j : k\right] = \left[\mathcal{C}_k : k^*S_j\right] = \left[\mathcal{U}_P : N_{K_{\mathfrak{p}_j}/k_P}\mathcal{U}_{\mathfrak{p}_j}\right]$. Finalmente tenemos

$$E^{(P)} = \bigcap_{j=1}^{m_P} R_j, \quad \left[E^{(P)} : k\right] = \left[\bigcap_{j=1}^{m_P} R_j : k\right] = \left[\mathcal{U}_P : \prod_{j=1}^{m_P} N_{K_{\mathfrak{p}_j}/k_P}\mathcal{U}_{\mathfrak{p}_j}\right].$$

Para la última parte, por la Proposición 2.2.13 tenemos que la parte moderadamente ramificada de $\Omega^{(P)}/k$ es $e_P^{(0)} = \mathrm{mcd}\left(e_1, \dots, e_{m_P}, q^{d_P} - 1\right)$.

□

Capítulo 3

Extensiones abelianas imaginarias

En este capítulo se estudian algunas familias de extensiones abelianas imaginarias de $k = \mathbb{F}_q(T)$ con número de clases de ideales uno. Para ello se hace uso de la fórmula de Schmidt. Se observa que si K/k es abeliana imaginaria, necesariamente $q > 2$. Se obtiene que si p es la característica de k, entonces las p-extensiones de k no son abelianas imaginarias (Proposición 3.3.5) y que si K es una extensión abeliana imaginaria de k, entonces su campo de géneros $K_{\mathfrak{g}}$ también lo es (Proposición 3.3.29).

3.1. Preliminares

3.1.1. Divisores

Sea $k = \mathbb{F}_q(T)$ el campo de funciones racionales. Considérese K/k una extensión separable con campo de constantes $\mathbb{F}_q$. Sea g_K el género de K. Los lugares de k son $\mathfrak{p}_\infty$, el polo de T y los lugares finitos son los que están en correspondencia biyectiva con los polinomios mónicos irreducibles P de $\mathbb{F}_q[T]$ y se denotan por (P).

Definición 3.1.1. Sea D el grupo abeliano libre generado por todos los lugares en K. A D se le llama *grupo de divisores* de K y a los lugares se les llama *divisores primos* de K.

Tenemos que D es un grupo aditivo.

Consideremos la función grado:

$$\mathrm{gr} : D \to \mathbb{Z}$$

Entonces $D_0 = \text{nuc gr}$ es el *grupo de divisores de grado cero* y $\mathbb{P} = \{(w)_K \mid w \in K^*\}$ es el *grupo de divisores principales* . Tenemos $\mathbb{P} < D_0$ y la siguiente sucesión exacta:

$$1 \longrightarrow D_0 \longrightarrow D \xrightarrow{\text{gr}} \mathbb{Z} \longrightarrow 0$$

Como $D/D_0 = D/\text{ nuc gr} \cong \text{Im gr} = \text{gr}(D) \cong \mathbb{Z}$ y como $\mathbb{Z}$ es libre,

$$D \cong D_0 \oplus \mathbb{Z}.$$

Definición 3.1.2. Decimos que $C = \frac{D}{\mathbb{P}}$ es el *grupo de clases de divisores de K*, $C_0 = \frac{D_0}{\mathbb{P}}$ es el *grupo de clases de divisores de grado cero de K* y $h_K := \left|\frac{D_0}{\mathbb{P}}\right|$ es el *número de clases de divisores de K* .

La siguiente sucesión es exacta para algún $m \in \mathbb{N}$.

$$1 \longrightarrow C_0 \longrightarrow C \xrightarrow{\widetilde{\text{gr}}} m\mathbb{Z} \longrightarrow 0$$

Aquí $m\mathbb{Z} \cong \mathbb{Z}$ y es libre de torsión. Por lo tanto $C \cong C_0 \oplus \mathbb{Z}$. En particular C nunca es finito.

3.1.2. La fórmula de Schmidt

Sea K un campo de funciones. Sea X el conjunto de lugares de K y sea $S \subseteq X$, $S \neq \emptyset$, S finito. Sea $\mathcal{O}(S) = \cap_{\mathcal{P} \notin S} \mathcal{O}_{\mathcal{P}} = \{x \in K \mid v_{\mathcal{P}}(x) \geq 0 \text{ para todo } \mathcal{P} \notin S\}$. Entonces $\mathcal{O}(S)$ es un dominio de Dedekind y por tanto tiene un grupo de clases de ideales $\mathscr{C}_S$. El grupo $\mathscr{C}_S$ es finito y su orden h_S es el *número de clases de ideales* . Sea $\mathcal{I}_S$ el grupo de ideales fraccionarios de $\mathcal{O}(S)$. Entonces hay un epimorfismo de D en $\mathcal{I}_S$ que se obtiene al eliminar los primos que están en S.

Sea $D(S)$ el grupo abeliano libre generado por los elementos de S y considérese la siguiente sucesión exacta:

$$1 \longrightarrow D(S) \longrightarrow D \longrightarrow \mathcal{I}_S \longrightarrow 1$$

Sea $\mathcal{F}_S$ el grupo de ideales fraccionarios principales de $\mathcal{O}(S)$. La preimagen de $\mathcal{F}_S$ en D es el grupo $\mathbb{P}D(S)$. Se tiene entonces que la siguiente sucesión

$$1 \longrightarrow \frac{\mathbb{P}D(S)}{\mathbb{P}} \longrightarrow \frac{D}{\mathbb{P}} \longrightarrow \frac{\mathcal{I}_S}{\mathcal{F}_S} \longrightarrow 1$$

es exacta.

Aplicando el segundo teorema de isomorfismos, se tiene la sucesión exacta

$$1 \longrightarrow \frac{D(S)}{\mathbb{P}\cap D(S)} \longrightarrow \frac{D}{\mathbb{P}} \longrightarrow \frac{\mathcal{I}_S}{\mathcal{F}_S} \longrightarrow 1.$$

Sean $D_0(S) = D(S) \cap D_0$ y $\mathbb{P}(S) = D(S) \cap \mathbb{P} = D_0(S) \cap \mathbb{P}$. Entonces la sucesión

$$1 \longrightarrow \frac{D_0(S)}{\mathbb{P}(S)} \longrightarrow \frac{D_0}{\mathbb{P}} \longrightarrow \frac{\mathcal{I}_S}{D_S}$$

es exacta.

El morfismo del lado derecho no necesariamente es suprayectivo. Para corregir la falla, sea $\mathrm{gr}(D(S)) = \delta_S\mathbb{Z}$, $\delta_S = \mathrm{mcd}_{\mathcal{P}\in S}\,\mathrm{gr}(\mathcal{P})$. Tenemos que $\mathrm{gr}(D) = \mathbb{Z}$. En consecuencia $[D : D_0D(S)] = \delta_S$. Entonces $[\mathcal{I}_S/\mathcal{F}_S : \mathrm{imagen}(D_0/\mathbb{P})] = \delta_S$. En particular $h_S = [\mathcal{I}_S/\mathcal{F}_S : 1]$ es finito. Además $[D_0(S)/\mathbb{P}(S) : 1] = r_S$ es finito por ser isomorfo a un subgrupo del grupo finito $D_0/\mathbb{P}$.

Con esto se ha probado el siguiente teorema.

Teorema 3.1.3. *Sean K/k una extensión separable del campo de funciones racionales $k = \mathbb{F}_q(T)$, h_K su número de clases de divisores, h_S su número de clases de ideales, $\delta_S = \mathrm{mcd}_{\mathcal{P}\in S}\,\mathrm{gr}(\mathcal{P})$ y $r_S = [D_0(S)/\mathbb{P}(S) : 1]$ el regulador . Entonces la fórmula de Schmidt da la relación entre h_K y h_S y es la siguiente:*

$$h_S r_S = h_K \delta_S.$$

Una definición de regulador para campos de funciones dada en [47] es la siguiente:

Sea R_T el anillo de todas las funciones en K cuyos únicos polos están en $S = \{P_1, \ldots, P_s\}$, sean $\{e_1, e_2, \ldots, e_{s-1}\}$ un conjunto fundamental de unidades para R_T^* y considere la matriz $M_{(s-1)\times s}$ cuya i, j-ésima entrada es $\ln \left\|e_j\right\|_{P_i}$, donde $\| \ \|_{P_i}$ denota la valuación normalizada en P_i.

Definición 3.1.4. El *regulador* r_{R_T} de $R_T = k[T]$ está definido como el valor absoluto del determinante de cualquier $s-1 \times s-1$ menor de esta matriz.

Observación 3.1.5. Como la suma de las columnas de la matriz anterior es la columna cero, entonces r_{R_T} está bien definido.

Lo que sigue se hará para ver la relación entre r_S y r_{R_T}.

Corolario 3.1.6. *Se tiene que $\delta_S h_K = [D_0(S) : \mathbb{P}(S)]h_{R_T}$, donde h_K es el número de clases de divisores del campo K.*

Demostración. Véase [47]. □

Se define el mapeo regulador $\lambda : D(S) \to \mathbb{Z}^s$ definido por $\lambda(Q) = (\ldots, -\mathrm{ord}_{\mathcal{P}_i} Q \,\mathrm{gr}\,\mathcal{P}_i, \ldots)$. Entonces λ es un homomorfismo y $[\mathbb{Z}^s : \lambda(D(S))] = \prod_{i=1}^{s} \mathrm{gr}\,\mathcal{P}_i$.

Si $P \in R_T^*$ y (P) es su divisor, entonces $\lambda((P)) = \left(\ldots, \log_q \|P\|_{\mathcal{P}_i}, \ldots\right)$. Sea ahora $R_{R_T}^{(q)}$ el q-regulador definido exactamente como se ha definido r_{R_T}, pero reemplazando el logaritmo natural por el logaritmo en base q. Se tiene $r_{R_T} = R_{R_T}^{(q)} (\ln q)^{S-1}$.

Lema 3.1.7. $[D_0(S) : \mathbb{P}(S)] = \dfrac{\delta r_{R_T}}{\left(\prod_{i=1}^{s} \mathrm{gr}\,\mathcal{P}_i\right)(\ln q)^{s-1}}$.

Demostración. Ver [47, Lema 4.2]. □

El siguiente corolario establece la relación que hay entre la definición del regulador de la Definición 3.1.4 y la de la fórmula de Schmidt.

Corolario 3.1.8. *Si* $\mathrm{gr}\,\mathcal{P}_i = 1$*, para* $i = 1, 2, \ldots, s$*, entonces* $[D_0(S) : \mathbb{P}(S)] = r_{R_T}^{(q)}$.

Demostración. Ver [47]. □

3.1.3. Fórmula del género

Sea $N \in R_T \setminus \{0\}$, N mónico y no constante, esto es $N \notin \mathbb{F}_q^*$. Sean $k = \mathbb{F}_q(T)$ y $K_N = k(\Lambda_N)$ el campo de funciones ciclotómico determinado por N. Sea K_N^+ el subcampo real maximal de K_N. Sea $\mathfrak{D}_{K_N/K}$ el diferente de la extensión K_N/K y sea g_N el género de K_N.

Teorema 3.1.9. ***(Fórmulas del diferente)*** *Sean* $N = \prod_{i=1}^{r} P_i^{n_i}$ *la factorización de* $N \in R_T$ *en potencias de irreducibles y* $d_i = \mathrm{gr}\,P_i$*. Los diferentes* $\mathfrak{D}_{K_N/K}$ *y* $\mathfrak{D}_{K_N/K_N^+}$ *están dados por las siguientes fórmulas:*

$$\mathfrak{D}_{K_N/K} = \prod_{i=1}^{r} \mathrm{con}_{K_{P_i^{n_i}}/K_N} \mathfrak{P}_i^{s_i} \prod_{\mathfrak{B}_\infty | \mathfrak{p}_\infty} \mathfrak{B}_\infty^{q-2}, \tag{3.1}$$

$$\mathfrak{D}_{K_N/K_N^+} = \mathfrak{P}_1^{q-2} \prod_{\mathfrak{B}_\infty | \mathfrak{p}_\infty} \mathfrak{B}_\infty^{q-2} \; si \; r = 1, \tag{3.2}$$

$$\mathfrak{D}_{K_N/K_N^+} = \prod_{\mathfrak{B}_\infty | \mathfrak{p}_\infty} \mathfrak{B}_\infty^{q-2} \; si \; r \geq 2, \tag{3.3}$$

donde $\mathfrak{P}_i$ *es el único divisor primo de* $K_{P_i^{n_i}}$ *sobre* $\mathfrak{p}_i$*, el divisor primo asociado a* P_i *y* $\mathfrak{B}_\infty$ *corre sobre los* $\Phi(N)/(q-1)$ *divisores primos de* K_N *que están sobre* $\mathfrak{p}_\infty$ *y* $s_i = n_i \Phi(P_i^{n_i}) - q^{d_i(n_i-1)}$.

Demostración. Véase [43, Teorema 3.3.1].

□

Corolario 3.1.10. ***(Fórmulas del género)***
Sea $N = \prod_{i=1}^{r} P_i^{n_i}$, donde $P_1, \ldots, P_r$ son polinomios mónicos irreducibles, $n_i \in \mathbb{N}$, $d_i = \operatorname{gr} P_i$ y $r \in \mathbb{N}$. Sean g_N y g_N^+ los géneros de los campos K_N y K_N^+ respectivamente. Entonces los géneros están dados por las siguientes fórmulas:

$$2g_N - 2 = -2\Phi(N) + \sum_{i=1}^{r} s_i \frac{\Phi(N)}{\Phi(P_i^{n_i})} d_i + (q-2)\frac{\Phi(N)}{q-1}, \tag{3.4}$$

$$2g_N^+ - 2 = (dn-2)\frac{\Phi(N)}{q-1} - d\frac{q^{d(n-1)}-1}{q-1} - d \text{ si } r = 1, \tag{3.5}$$

$$2g_N^+ - 2 = \frac{1}{q-1}\left\{(2g_N - 2) - \frac{\Phi(N)}{q-1}(q-2)\right\} \text{ si } r \geq 2. \tag{3.6}$$

En la ecuación (3.5) $d = d_1$ y $n = n_1$.

Demostración. Véase [43, Corolario 3.3.2]. □

3.1.4. Campos de géneros

Recordemos que dados K un campo de funciones con campo de constantes $\mathbb{F}_q$ y S un conjunto finito no vacío de divisores primos de K. El campo de funciones de clases de Hilbert de K relativo a S, $K_{H,S}$, es la máxima extensión abeliana no ramificada de K, donde cada elemento de S se descompone totalmente. En lo que sigue, para cualquier extensión finita K de k, consideraremos S como el conjunto de divisores primos que dividen a $\mathfrak{p}_\infty$, el polo del divisor T en k y escribimos K_H en vez de $K_{H,S}$.

También recordamos que dada K una extensión separable finita de k, el *campo de géneros K_g de K con respecto a k* es la máxima extensión abeliana de K contenida en K_H que es la composición de K y una extensión abeliana de k. Equivalentemente, $K_g = K\Omega$, donde Ω es la máxima extensión abeliana de k contenida en K_H.

Cuando K/k es una extensión abeliana, K_g es la máxima extensión abeliana de k contenida en K_H.

Tenemos las siguientes propiedades para el campo de géneros de extensiones de Kummer de grado primo.

Proposición 3.1.11. *Sea ℓ primo tal que $\ell \mid q-1$. Consideramos $k = \mathbb{F}_q(T)$, D un polinomio mónico, $D = P_1^{e_1} \cdots P_r^{e_r}$, con $1 \leq e_i \leq \ell - 1$. Entonces $K = k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} D} \cdot D}\right) \subseteq k(\Lambda_D)$.*

Demostración. Véase [50, Corolario 9.5.12]. □

Teorema 3.1.12. *Sea $D = P_1^{e_1} \cdots P_r^{e_r}$ un polinomio mónico libre de ℓ-potencias, donde $P_i \in R_T^+$, $1 \leq e_i \leq \ell - 1$, $1 \leq i \leq r$. Sea $0 \leq s \leq r$ tal que $\ell \mid \operatorname{gr} P_i$ para $1 \leq i \leq s$ y $\ell \nmid \operatorname{gr} P_j$ para $s+1 \leq j \leq r$. Sea $K := k\left(\sqrt[\ell]{\gamma D}\right)$, donde $\gamma \in \mathbb{F}_q^*$. Entonces el campo de géneros $K_{\mathfrak{g}}$ está dado por:*

1. $k\left(\sqrt[\ell]{\gamma D}, \sqrt[\ell]{(-1)^{\operatorname{gr} P_1} P_1}, \ldots, \sqrt[\ell]{(-1)^{\operatorname{gr} P_r} P_r}\right)$ *si $\ell \nmid \operatorname{gr} D$ o si $\ell \mid \operatorname{gr} P_i$ para toda $1 \leq i \leq r$,*

2. $k\left(\sqrt[\ell]{\gamma D}, \sqrt[\ell]{P_1}, \ldots, \sqrt[\ell]{P_s}, \sqrt[\ell]{P_{s+1} P_r^{a_{s+1}}}, \ldots, \sqrt[\ell]{P_{r-1} P_r^{a_{r-1}}}\right)$, *donde el exponente a_j satisface $\operatorname{gr} P_j + a_j \operatorname{gr} P_r \equiv 0 \bmod \ell$, $s+1 \leq j \leq r-1$, si $\ell \mid \operatorname{gr} D$ y $\ell \nmid \operatorname{gr} P_r$.*

Demostración. Véase [50, Teorema 14.6.7]. □

Otra versión del mismo resultado es la siguiente.

Teorema 3.1.13. *(Teorema de Peng). Sea $D = P_1^{e_1} \cdots P_r^{e_r} \in R_T$ un polinomio mónico libre de ℓ-potencias, donde $P_i \in R_T^+$, $1 \leq e_i \leq \ell - 1$, $1 \leq i \leq r$. Sea $0 \leq s \leq r$ tal que $\ell \mid \operatorname{gr} P_i$ para $1 \leq i \leq s$ y $\ell \nmid \operatorname{gr} P_j$ para $s+1 \leq j \leq r$. Sea $K := k\left(\sqrt[\ell]{\gamma D}\right)$, donde $\gamma \in \mathbb{F}_q^*$ y sea $\alpha := (-1)^{\operatorname{gr} D}\gamma$ y $a_{s+1}, \ldots, a_{r-1} \in \mathbb{Z}$ que satisface $\operatorname{gr} P_m + a_m \operatorname{gr} P_r \equiv 0 \bmod \ell$, $s+1 \leq m \leq r-1$. Entonces K_g está dado por:*

(a) $k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} P_1} P_1}, \ldots, \sqrt[\ell]{(-1)^{\operatorname{gr} P_r} P_r}\right)$ *si $\alpha \in \left(\mathbb{F}_q^*\right)^\ell$ y $\ell \nmid \operatorname{gr} D$.*

(b) $k\left(\sqrt[\ell]{(P_1}, \ldots, \sqrt[\ell]{P_s}, \sqrt[\ell]{P_{s+1} P_r^{a_s+1}}, \ldots, \sqrt[\ell]{P_{r-1} P_r^{a_r-1}}\right)$ *si $\alpha \in \left(\mathbb{F}_q^*\right)^\ell$, $\ell \mid \operatorname{gr} D$ y $\ell \nmid \operatorname{gr} P_r$.*

(c) $k\left(\sqrt[\ell]{\gamma}, \sqrt[\ell]{P_1}, \ldots, \sqrt[\ell]{P_r}\right)$ *si $\ell \mid \operatorname{gr} P_r$.*

(d) $k\left(\sqrt[\ell]{\gamma D}, \sqrt[\ell]{P_1}, \ldots, \sqrt[\ell]{P_s}, \sqrt[\ell]{P_{s+1} P_r^{a_s+1}}, \ldots, \sqrt[\ell]{P_{r-1} P_r^{a_r-1}}\right)$ *si $\alpha \notin \left(\mathbb{F}_q^*\right)^\ell$ y $\ell \nmid \operatorname{gr} P_r$.*

Demostración. Véase [30, 31, Teorema 5.2]. □

3.2. Algunas propiedades de extensiones abelianas imaginarias

En esta sección se desarrollan algunas propiedades de las extensiones abelianas imaginarias teniendo como base los artículos [19] y [54].

Sean $k = \mathbb{F}_q(T)$ un campo de funciones racionales sobre el campo finito $\mathbb{F}_q$ con q elementos, $R_T = \mathbb{F}_q[T]$ el anillo de polinomios y $\mathfrak{p}_\infty$ el divisor primo de k asociado a $\left(\frac{1}{T}\right)$.

Para cada $N \in R_T$ se consideran el campo de funciones ciclotómico K_N y su subcampo real maximal K_N^+, es decir, el subcampo maximal de K_N en el que $\mathfrak{p}_\infty$ se descompone totalmente.

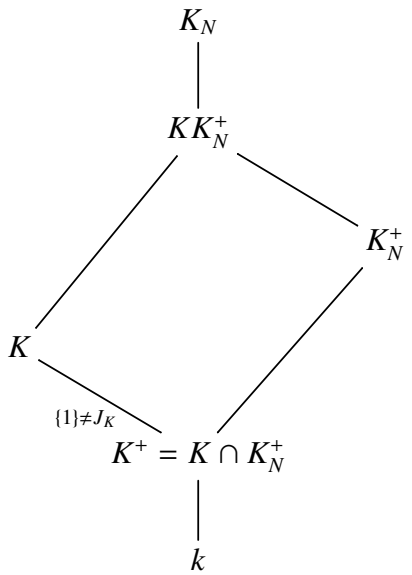
En lo que sigue de esta sección se supone que la extensión finita K de k está contenida en algún campo de funciones ciclotómico.

Definición 3.2.1. El *conductor* de K es el polinomio mónico $N \in R_T$ tal que K_N es el mínimo campo de funciones ciclotómico, en el sentido de contención, que contiene a K.

Definición 3.2.2. Sea $k = \mathbb{F}_q(T)$. Sea K una extensión abeliana finita de k y sean N el conductor de K, $K^+ = K \cap K_N^+$ el subcampo real maximal de K y $J_K = \mathrm{Gal}(K/K^+)$.

- La extensión K/k es *abeliana real* si J_K es trivial.
- La extensión K/k es *abeliana imaginaria* si $J_K \neq \{1\}$.
- Una extensión abeliana imaginaria K/k es *totalmente imaginaria* si $\mathrm{Gal}(K/k) = J_K$.

El siguiente diagrama esquematiza la definición de extensión abeliana imaginaria.



Vamos a reformular la fórmula de Schmidt para el caso abeliano imaginario. Para ello consideremos lo siguiente:

Sean K/k una extensión de campos de funciones, $\mathcal{O}_K$ la cerradura entera de R_T en K y $\mathcal{O}_K^*$ su grupo de unidades. Sea $\mathscr{F}$ el conjunto de ideales fraccionarios y $\mathscr{P}$ el conjunto de ideales fraccionarios principales. Entonces $\mathscr{C} = \mathscr{F}/\mathscr{P}$ es el grupo de clases de ideales y $h_S = |\mathscr{F}/\mathscr{P}|$ es el número de clases de ideales.

Sea $S_k = \{\mathfrak{p}_\infty\}$ y $S = S_K = \{\mathcal{P} \in \mathbb{P}_K \mid \mathcal{P} \text{ está arriba de } \mathfrak{p}_\infty\}$. El *número de clases de ideales* h_S asociado con (K, S) se define como el número de clases del anillo de Dedekind

$$\mathcal{O}_S = \cap_{\mathcal{P} \notin S} \mathcal{O}_\mathcal{P},$$

donde $\mathcal{O}_\mathcal{P} = \{z \in K \mid \mathfrak{v}_\mathcal{P}(z) \geq 0\}$ es el anillo local asociado con la valuación $\mathfrak{v}_\mathcal{P}$ en $\mathcal{P}$. Notemos que $\mathcal{O}_S = \mathcal{O}(S)$ que vimos en la Sección 3.1.2.

Los enteros h_S y h_K están relacionados por la fórmula de Schmidt

$$\delta_S h_K = r_S h_S,$$

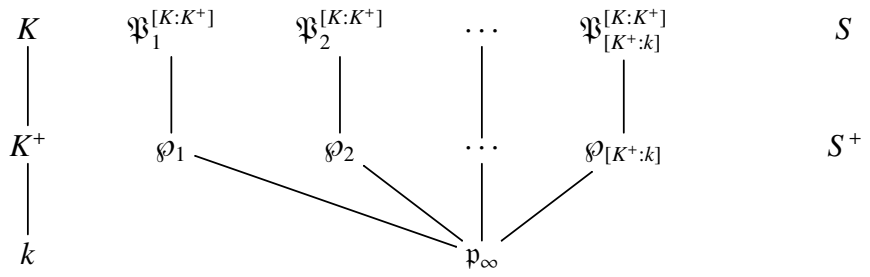
donde $\delta_S = \operatorname{mcd}\{\operatorname{gr}\mathcal{P} \mid \mathcal{P} \in S\}$ y r_S es el *regulador* de (K, S), es decir, el índice del grupo de divisores principales con soporte en S en el grupo de divisores de grado cero con soporte en S.

En nuestro caso, dada K/k una extensión abeliana imaginaria, se tiene $K \subseteq K_N$, $\mathfrak{p}_\infty$ es el primo infinito y S es el conjunto de primos de K que dividen a $\mathfrak{p}_\infty$, entonces el grado de los primos infinitos es 1 y por lo tanto $\delta_S = 1$. Así la fórmula de Schmidt se reduce a:

$$h_K = r_S h_S. \tag{3.7}$$

Nota 3.2.3. *Usando la ecuación anterior podemos concluir que si $h_K = 1$, entonces necesariamente $h_S = 1$.*

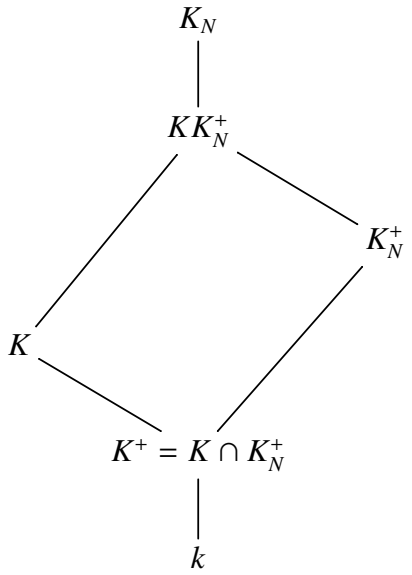
Sean $k = \mathbb{F}_q(T)$ campo de funciones racionales y K/k una extensión abeliana imaginaria. Sea S el conjunto de lugares de K sobre $\mathfrak{p}_\infty$. Sea J_K el grupo de inercia de $\mathfrak{p}_\infty$. Entonces K^+ es el subcampo real maximal de K. Ajustando $S^+ = \{\mathcal{P} \cap K^+ \mid \mathcal{P} \in S\}$ se obtiene el siguiente diagrama:



Observación 3.2.4. Del diagrama se tiene que si una extensión K/k es abeliana imaginaria, entonces $q > 2$, ya que cuando $q = 2$, $K_N^+ = K_N$, de donde $K^+ = K \cap k(\Lambda_N)^+ = K \cap k(\Lambda_N) = K$.

Proposición 3.2.5. *Sea K/k una extensión abeliana totalmente imaginaria y sea $h_S^+ = h_{S^+}$ el número de clases de ideales asociado con (K^+, S^+). Entonces h_{S^+} divide a h_S.*

Demostración. Se considera el siguiente diagrama:



Como K_N/K_N^+ es totalmente ramificada, tenemos KK_N^+/K_N^+ también es totalmente ramificada. Puesto que K es una extensión abeliana imaginaria, en la extensión K/K^+ los primos infinitos son totalmente ramificados.

Por [58, Teorema 3.38], tenemos que $\mathrm{Gal}\,(K/K^+) \cong \mathrm{Gal}\left(KK_N^+/K_N^+\right)$. Con esto tenemos que $e = e_{K/K+} = e_{KK_N^+/K_N^+}$ y por lo tanto $e \mid q-1$.

Se considera el mapeo norma

$$N : \mathscr{C}_{\mathfrak{O}_K} \longrightarrow \mathscr{C}_{\mathfrak{O}_{K^+}}$$

el cual es suprayectivo por [47, Teorema 3.1]. Ahora, por un teorema de isomorfismos, $\frac{\mathscr{C}_{\mathfrak{O}_K}}{\mathrm{nuc}\, N} \cong \mathscr{C}_{\mathfrak{O}_{K^+}}$. Tomando cardinalidad tenemos $\left|\mathscr{C}_{\mathfrak{O}_{K^+}}\right| |\mathrm{nuc}\, N| = \left|\mathscr{C}_{\mathfrak{O}_K}\right|$ y por lo tanto se tiene el resultado. □

Definición 3.2.6. Sea $h_S^+ = h_{S^+}$ el número de clases de ideales asociado con (K^+, S^+). Como K/K^+ es totalmente imaginaria, se tiene h_S^+ divide h_S. El *número de clases de ideales relativo* es

$$h_S^- := h_S / h_S^+.$$

Proposición 3.2.7. *Sea K/k una extensión abeliana totalmente imaginaria, es decir,* $\mathrm{Gal}(K/k) = J_K$. *Entonces dados r_S y r_S^+ los reguladores de K/k y K^+/k respectivamente y $r_S^- := r_S/r_S^+$. El índice de unidades es $Q = [\mathcal{O}_S^* : \mathbb{F}_q^* \mathcal{O}_{S^+}^*]$. Entonces $r_S^- = \frac{[K:K^+]^{|S|-1}}{Q} \in \mathbb{N}$.*

Demostración. Véase [13, Lema 1.15].

□

Proposición 3.2.8. *Con la notación de la Proposición 3.2.7, tenemos que el índice de unidades Q es* 1 *si N es potencia de un primo y $q-1$ en otro caso. Por lo tanto se tiene:*

$$r_S^- = \begin{cases} (q-1)^{|S|-1} & \text{si } N \text{ es potencia de un primo,} \\ (q-1)^{|S|-2} & \text{en otro caso.} \end{cases}$$

Demostración. Véase [54, (2a)].

□

Nota 3.2.9. *Tenemos*

$$h_K^- = r_S^- h_S^-.$$

Observación 3.2.10. Una condición necesaria y suficiente para que en una extensión abeliana imaginaria $h_S = 1$ es que $h_S^- = h_S^+ = 1$.

Proposición 3.2.11. *Sean K_N y K_M dos extensiones ciclotómicas tales que $K_N \subseteq K_M$. Entonces $h_{S_N} \mid h_{S_M}$, donde h_{S_N} y h_{S_M} son los números de clases de ideales de N y M respectivamente.*

Esta proposición se sigue de los siguientes resultados.

Proposición 3.2.12. *Sea $K_N \subseteq K \subseteq K_M$ y K/K_N no ramificada en todos los primos. Entonces $K = K_N$.*

Demostración. Sea X el grupo de caracteres asociado a K_N. Se tiene $X = \prod_p X_P$ pues $\widehat{\mathrm{Gal}(K_N/k)} \cong (R_T/N)^*$ es el grupo de todos los caracteres módulo N. Sea Y el grupo de caracteres asociado a K. Se tiene $X \subseteq Y$ y $X_P \subseteq Y_P$. Como K/K_N es no ramificado, $X_P = Y_P$ para todo P. Luego $\prod_P Y_P = \prod_P X_P = X$. Además $Y \subseteq \prod_P Y_P = X$. Por lo tanto $X = Y$ y así $K = K_N$. □

Proposición 3.2.13. *Sea L/K una extensión finita y separable de campos de funciones tal que no existe una subextensión abeliana no trivial F/K no ramificada en todos los primos y para la que los primos infinitos sean totalmente descompuestos. Denotamos por S_L al conjunto de divisores primos de L que están encima de $\mathfrak{p}_\infty$. Entonces $h_S \mid h_{S_L}$.*

Demostración. Recordemos que S es el conjunto finito no vacío de primos de K que están encima de $\mathfrak{p}_\infty$. Sean $K_{H,S}$ la máxima extensión abeliana no ramificada de K y tal que los primos en S son totalmente descompuestos y sea L_{H,S_L} la máxima extensión abeliana no ramificada de L y tal que los primos en S_L son totalmente descompuestos. Por teoría de campos de clases, el grupo $\mathrm{Gal}(K_{H,S}/K)$ es isomorfo al grupo de clases de ideales de K. (Véase [60, Apéndice 3, Teorema 4]). Como no existe una subextensión abeliana no trivial no ramificada en todos los primos y para la que los primos infinitos sean totalmente descompuestos, tenemos $K_{H,S} \cap L = K$. Con esto se tiene que $\mathrm{Gal}(LK_{H,S}/L) \cong \mathrm{Gal}(K_{H,S}/K)$, vía restricción. Como $LK_{H,S}/L$ es una extensión abeliana no ramificada y es tal que los primos en S_L son totalmente descompuestos, tenemos $LK_{H,S}$ está contenido en L_{H,S_L}.

Por lo tanto

$$\mathrm{Gal}(L_{H,S_L}/L) \longrightarrow \mathrm{Gal}(K_{H,S}/K)$$

es suprayectivo vía restricción. Entonces se tiene el siguiente diagrama conmutativo, donde $\mathscr{C}_{\mathcal{O}_K}$ es el grupo de clases de ideales de K, $\mathscr{C}_{\mathcal{O}_L}$ es el grupo de clases de ideales de L.

$$\begin{array}{ccc} \mathscr{C}_{\mathcal{O}_L} & \xrightarrow[\text{mapeo de Artin}]{\sim} & \mathrm{Gal}(L_{H,S_L}/L) \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \text{rest}} \\ \mathscr{C}_{\mathcal{O}_K} & \xrightarrow[\text{mapeo de Artin}]{\sim} & \mathrm{Gal}(K_{H,S}/K) \end{array}$$

Por el argumento anterior, la flecha de la derecha es suprayectiva, entonces la norma también es suprayectiva. Con esto se tiene que la función del grupo de clases de ideales de L al grupo de clases de ideales de K es suprayectiva y el número de clases de ideales h_S divide al número de clases de ideales h_{S_L}. □

3.3. Estudio de extensiones

En lo que sigue consideramos $k = \mathbb{F}_q(x)$ cuando la extensión K/k se define a través de una ecuación en las variables x, y.

3.3.1. Extensiones ciclotómicas

Observación 3.3.1. Recordemos que los campos ciclotómicos son extensiones abelianas imaginarias si $q > 2$, ya que $K_M = K_M^+$ si y sólo si $q = 2$ y también que los subcampos reales maximales

K_M^+ no son extensiones abelianas imaginarias ya que $K^+ = K_M^+ \cap K_M^+ = K_M^+$ y entonces $J_K = \{1\}$, donde $J_K = \mathrm{Gal}(K/K^+)$.

De los trabajos de Kida-Murabayashi [21] y de Sémirat [54] se tienen los siguientes resultados:

Teorema 3.3.2. *Las soluciones del problema de número de clases de ideales uno para extensiones ciclotómicas imaginarias $k(\Lambda_M)/k$ con $M \in R_T$ y $g_K = 0$ están dadas en la tabla 3.1.*

$M(x)$	q	$\phi(M)$	h_K	h_S
$x - a$, $a \in \mathbb{F}_q$	≥ 3	$q-1$	1	1
$x(x+1)$	3	4	1	1
$x(x-1)$	3	4	1	1
$(x-1)(x+1)$	3	4	1	1

Tabla 3.1: Caso $g_K = 0$

Teorema 3.3.3. *Las soluciones del problema de número de clases de ideales uno para extensiones ciclotómicas imaginarias $k(\Lambda_M)/k$ con $M \in R_T$ y $g_K \geq 1$ están dadas en la tabla 3.2, donde $\langle w \rangle = \mathbb{F}_4^*$.*

$M(x)$	q	$\phi(M)$	g_K	h_K	h_S
x^2	3	6	1	4	1
x^2+1	3	8	2	8	1
$x(x+1)(x+2)$	3	8	1	4	1
$x(x-1)^2$	3	6	4	$2^4 \times 7$	1
$x(x^2+2x+2)$	3	16	7	$2^7 \times 17$	1
$x(x+w)$	4	9	1	3	1
$x(x+w^2)$	4	9	1	3	1

Tabla 3.2: Caso $g_K \geq 1$

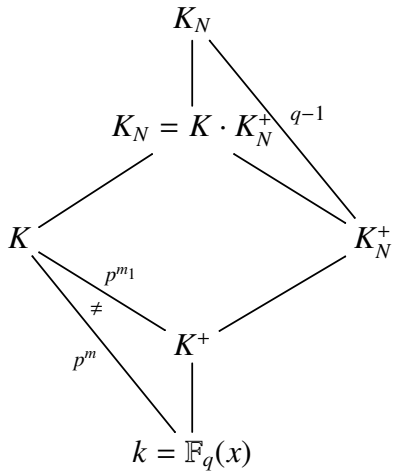
Nota 3.3.4. Del teorema anterior destacamos el caso en que $q = 3$ y $M(x) = x^2 + 1$, el número de clases de ideales es $h_S = 1$ pero $h_K = 8$. Éste es un ejemplo en el que se tiene $h_S = 1$ pero $h_K \neq 1$. Por la fórmula de Schmidt, $r_S = 8$.

3.3.2. p-extensiones

Proposición 3.3.5. *Las p-extensiones abelianas finitas no son extensiones abelianas imaginarias.*

Demostración. Sean K/k una extensión de Galois, $k = \mathbb{F}_q(x)$, $q = p^n$ y la característica de k es p. Sea $G = \mathrm{Gal}(K/k)$. Se considera G un p-grupo abeliano. Entonces $G \cong C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_s}}$ y $|G| = p^{n_1+n_2+\cdots+n_s}$.

Supóngase que K/k es una extensión abeliana imaginaria tal que su grupo de Galois es un p-grupo abeliano G de orden p^m. Se tiene el siguiente diagrama:



Entonces $[K : K^+] = p^{m_1}$, con $m_1 \in \mathbb{N}$. Por teoría de Galois se tiene que $p^{m_1} \mid (q-1)$. Esto es una contradicción. Con esto se concluye que las p-extensiones no son extensiones abelianas imaginarias. □

Corolario 3.3.6. *Las extensiones de Artin-Schreier, las extensiones elementales abelianas y las extensiones de Witt no son extensiones abelianas imaginarias.*

3.3.3. Extensiones de Kummer

La siguiente definición fue tomada de [22]:

Definición 3.3.7. Sea K/F una extensión de Galois de grado n y supóngase que F contiene las n-ésimas raíces de unidad y que la característica de F no es un divisor de n. Entonces K/F es una *extensión de Kummer*.

Observación 3.3.8. Al trabajar en campos de funciones con campo de constantes finito $\mathbb{F}_q$, en las extensiones de Kummer, las n-ésimas raíces de unidad están en el campo de constantes, por lo que $n \mid q-1$. Dada K/k una extensión de Kummer, $K = k\left(\sqrt[n]{D_1}, \ldots, \sqrt[n]{D_t}\right)$, donde $D_1, \ldots, D_t \in R_T$. En el presente trabajo nos restringimos a un radical, luego $K = k\left(\sqrt[n]{D}\right)$, en este caso la extensión es cíclica.

Lo que sigue establece las condiciones para que una extensión de Kummer sea abeliana imaginaria.

Sea K/k una extensión de Kummer contenida en un campo ciclotómico $k(\Lambda_D)$, donde D es un polinomio mónico. Entonces por la Proposición 3.1.11,

$$K = k\left(\sqrt[n]{(-1)^{\operatorname{gr} D} \cdot D}\right) \subseteq k(\Lambda_D).$$

Además, requerimos que $K \neq K^+$. Abordaremos primero el caso en que $n = \ell$ es primo.

Extensiones de Kummer de grado primo ℓ

Sea K una extensión de Kummer de grado primo ℓ. Entonces $K = k(\sqrt[\ell]{(-1)^{\operatorname{gr} D} D})$, donde $\ell \mid q-1$, $\gamma \in \mathbb{F}_q^*$ y $D \in k[T]$, D es libre de ℓ-potencias, es decir, $D = \gamma P_1^{\alpha_1} \ldots, P_r^{\alpha_r}$, P_i es un polinomio mónico irreducible, $0 < \alpha_i < \ell$. Tenemos que K/k es una extensión cíclica de grado ℓ y $K \subseteq k(\Lambda_D)$. Recordemos que $K^+ = K \cap k(\Lambda_D)^+$. Entonces $J_K = \operatorname{Gal}(K/K^+) \neq \{1\}$ si y sólo si $K \neq K^+$, es decir, $K \nsubseteq k(\Lambda_D)^+$. Para que K sea abeliana imaginaria es necesario que $K^+ = k$.

Proposición 3.3.9. *Sea K/k una extensión de Kummer de grado ℓ. El comportamiento de $\mathfrak{p}_\infty$ en K/k es el siguiente:*

(a) Si $\ell \nmid \operatorname{gr} D$, entonces $\mathfrak{p}_\infty$ es ramificado.

(b) Si $\ell \mid \operatorname{gr} D$ y $\gamma \in (\mathbb{F}_q^*)^\ell$, entonces $\mathfrak{p}_\infty$ se descompone.

(c) Si $\ell \mid \operatorname{gr} D$ y $\gamma \notin (\mathbb{F}_q^*)^\ell$, entonces $\mathfrak{p}_\infty$ es inerte.

Demostración. Véase [30, Proposición 5.1]. □

Nota 3.3.10. *Observemos que en una extensión $K = k(\sqrt[\ell]{(-1)^{\operatorname{gr} D} D})$ de Kummer de grado primo ℓ sobre k y abeliana imaginaria debe cumplirse $\ell \nmid \operatorname{gr} D$ y $\mathfrak{p}_\infty$ se ramifica en K/k. Esto se debe a que K está contenido en un campo ciclotómico y en estos campos el primo infinito $\mathfrak{p}_\infty$ no tiene inercia y además, como $K^+ = k$, el primo infinito no se descompone en K/k.*

Nota 3.3.11. *Por [28] y [34], tenemos que hay ocho campos de funciones no isomorfos con número de clases de divisores $h_K = 1$ y género $g_K \geq 1$. Estas ecuaciones fueron dadas inicialmente por MacRae. En nuestro caso sólo consideramos dos, pues en ellos $q \neq 2$.*

(a) Sea K el campo determinado por la ecuación $y^2 + 2x^3 + x + 1 = 0$ con $q = 3$. Usando el cambio de variable $x = -T$:

$$y^2 = -T^3 - 2T + 2 = -(T^3 + 2T - 2) = -(T^3 + 2T + 1)$$

Luego $y = \sqrt{-(T^3 + 2T + 1)}$. Sea $P = T^3 + 2T + 1$. Tenemos $k\left(\sqrt{(-1)^3 P}\right) \subseteq k(\Lambda_P)$, con $k = \mathbb{F}_3(T)$, $\ell = 2$ y $\operatorname{gr} P = 3$. Así, $k(y) \subseteq k(\Lambda_P)$. Como $\ell = 2 \nmid 3 = \operatorname{gr} P$, entonces por la Proposición 3.3.9, $\mathfrak{p}_\infty$ se ramifica. Así $K \neq K^+$ y por lo tanto, la extensión K/k es una extensión de Kummer abeliana imaginaria. Como $h_K = 1$, por la ecuación 3.7, tenemos $h_S = 1$.

(b) Sea ahora K el campo determinado por la ecuación $y^2 + y = x^3 + \alpha$, con $q = 4$ y donde α es un generador del grupo multiplicativo $\mathbb{F}_4^*$. Considerando $k = \mathbb{F}_4(x)$, tenemos $K = k(y)$, la extensión K/k es una extensión de Artin-Schreier y por [30], $\mathfrak{p}_\infty$ se ramifica salvajemente. Así pues, si se considera la extensión K/k de esta manera, no se trata de una extensión abeliana imaginaria. De cualquier modo, como $h_K = 1$, tenemos $h_S = 1$. Notemos que si en la definición de extensión abeliana imaginaria permitimos ramificación salvaje, éste sería un ejemplo.

Pero si consideramos $k = \mathbb{F}_4(y)$, entonces $K = k(x)$ y tendremos una extensión de Kummer de grado 3, donde $x = \sqrt[3]{y^2 + y + \alpha}$, $P = y^2 + y + \alpha$, $\ell = 3$ y $\operatorname{gr} P = 2$. Por la Proposición 3.3.9, como $3 \nmid 2$, $\mathfrak{p}_\infty$ se ramifica. Notemos que en K^+/k, $\mathfrak{p}_\infty$ se descompone, así que $K^+ = k$. Por lo tanto K/k es una extensión abeliana imaginaria. Como $k\left(\sqrt[3]{P}\right) \subseteq k(\Lambda_P)$, tenemos, K/k es una extensión de Kummer abeliana imaginaria. Como antes, de $h_K = 1$ se sigue $h_S = 1$.

Ahora hemos de determinar bajo que condiciones una extensión de Kummer de grado ℓ abeliana imaginaria tiene número de clases de ideales $h_S = 1$. Para esto, nos auxiliamos del campo de géneros K_g de K/k. En nuestro caso $\gamma = (-1)^{\operatorname{gr} D}$ y $\alpha = (-1)^{\operatorname{gr} D}\gamma = (-1)^{\operatorname{gr} D}(-1)^{\operatorname{gr} D} = (-1)^{2\operatorname{gr} D} = 1$. Por lo tanto $\alpha \in \mathbb{F}_q^{*\ell}$. Por el Teorema de Peng 3.1.13, tenemos

$$K_{\mathfrak{g}} = k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} P_1} \cdot P_1}, \ldots, \sqrt[\ell]{(-1)^{\operatorname{gr} P_r} \cdot P_r}\right).$$

Analizando tenemos las siguientes observaciones:

- Si $r \geq 2$, como $K \subsetneq K_{\mathfrak{g}} \subseteq K_H$ y el grado de la extensión K_H/K es h_S, concluimos $h_S > 1$.
- Si $r = 1$, entonces $K_{\mathfrak{g}} = k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} P_1} \cdot P_1}\right)$. Por lo que $K = K_{\mathfrak{g}}$ y entonces no sabemos cuál es el valor de h_S.

En general, dado $D = P^e$, con $1 \leq e \leq \ell - 1$ y P polinomio mónico irreducible, se tiene

$$K = K_{\mathfrak{g}} = k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} P} \cdot P}\right).$$

Podemos suponer que $e = 1$. Luego $D = P$ y $K = k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} P} \cdot P}\right)$.

Ahora debemos encontrar el valor de h_S.

Lema 3.3.12. *Si* $\operatorname{gr} P = 1$ *entonces* $h_S = 1$.

Demostración. Supongamos $\operatorname{gr} P = 1$ y $K = k\left(\sqrt[\ell]{-P}\right) \subseteq k(\Lambda_P)$, entonces se tiene $(P)_{k(x)} = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\operatorname{gr} P}} = \frac{\mathfrak{p}}{\mathfrak{p}_\infty}$ y $\mathfrak{d}_{P(x)} = \mathfrak{p}$. Aquí $\mathfrak{p}_\infty$ se ramifica en K/k por 3.3.10. Luego $\operatorname{con}_{k(x)/k} = \mathfrak{P}$ y $\mathcal{D}_{K/k(x)} = \wp^{\ell-1}\wp_\infty^{\ell-1}$. Así $\operatorname{gr}\left(\mathcal{D}_{K/k}\right) = \operatorname{gr} P(\ell - 1) + \ell - 1 = (\ell - 1)(\operatorname{gr} P + 1)$.

Por la fórmula de Riemann-Hurwitz:

$$\begin{aligned} 2g_K - 2 &= \ell(2g_k - 2) + \operatorname{gr} \mathcal{D}_{K/k} \\ &= \ell(-2) + (\operatorname{gr} P + 1)(\ell - 1) \\ &= -2\ell + \operatorname{gr} P\ell - \operatorname{gr} P + \ell - 1 \\ &= -\ell + \operatorname{gr} P\ell - \operatorname{gr} P - 1 \end{aligned}$$

Se tiene:

$2g_K = \operatorname{gr} P\ell - \ell - \operatorname{gr} P + 1 = \operatorname{gr} P(\ell - 1) - (\ell - 1) = (\ell - 1)(\operatorname{gr} P - 1)$.

Entonces

$$g_K = \frac{1}{2}(\ell - 1)(\operatorname{gr} P - 1) \tag{3.8}$$

y como $\operatorname{gr} P = 1$, se tiene que $g_K = 0$ y así $h_K = 1$. Por la fórmula de Schmidt, $h_S = 1$.

□

Veamos ahora el caso en que $\operatorname{gr} P > 1$:

Sea $K = k\left(\sqrt[\ell]{(-1)^{\operatorname{gr} P} P}\right)$ una extensión abeliana imaginaria, donde P es un polinomio mónico irreducible, $\operatorname{gr} P > 1$, ℓ primo, tal que $\ell \mid q - 1$ y $q > 2$, $q = p^a$.

Notemos que $g_K \neq 0$ por la ecuación 3.8 y por el Lema 3.3.12, tenemos que esto pasa si y sólo si $\operatorname{gr} P = 1$.

Usando [54, Fórmulas (1d), (3a) y (4b)] se tiene: $h_K^+ = 1$ ya que $g_{K^+} = 0$. Por lo tanto $h_K = h_K^-$ y también $h_S^+ = 1$. Por lo tanto $h_S = h_S^-$.

Además tenemos que $h_K^+ = 1$ porque $g_K^+ = 0$. Por lo tanto $h_K = h_K^-$. También $h_S^+ = 1$ y por lo tanto $h_K = h_K^-$.

Por otro lado, por [53] tenemos $r_S^- = \frac{[K:K^+]^{|S|-1}}{Q} \in \mathbb{N}$, donde $|S| = 1$ porque $\mathfrak{p}_\infty$ es totalmente ramificado y la extensión es totalmente imaginaria. Entonces $r_S^- = 1$. Luego $h_K^- = h_S^-$ y $h_K = h_K^-$. Así $h_K = h_S^-$, $h_S^+ = 1$. Por lo tanto $h_K = h_S^- = h_S$ y en consecuencia $h_S = 1$ si y sólo si $h_K = 1$.

Luego como $g_K \neq 0$ y $\operatorname{gr} P > 1$, los casos en que $h_S = 1$ son los casos (a) y (b) de la nota 3.3.11, es decir: $q = 3$, $g = 1$, $T^2 + 2X^3 + X + 1 = 0$ y $q = 4$, $g = 1$, $T^2 + T = X^3 + \alpha$, con $\alpha \in \mathbb{F}_4 - \{0, 1\}$.

Teorema 3.3.13. *Dada una extensión de tipo Kummer de la forma $K = \sqrt[\ell]{(-1)^{\operatorname{gr} D} \cdot D}$, donde D es un polinomio mónico de la forma $D = P_1^{a_1} \cdots P_r^{a_r}$, se tiene:*

- *Si $r \geq 2$, $h_S > 1$.*
- *Si $r = 1$ y $\operatorname{gr} P = 1$, $h_S = 1$.*
- *Si $r = 1$ y $\operatorname{gr} P > 1$, $h_S > 1$, excepto los casos (a) y (b) de la nota 3.3.11.*

Demostración.

- Por el Teorema de Peng, $K \subsetneq K_{\mathfrak{g}}$ y $K_{\mathfrak{g}} \subseteq K_H$, entonces el grado de la extensión K_H/K es h_S y por lo tanto $h_S > 1$.
- Si $\operatorname{gr} P = 1$, entonces K es un campo de funciones racionales y $g_K = 0$, por lo que $h_S = 1$.
- Si $\operatorname{gr} P > 1$, entonces $h_K = h_S$ y $h_S = 1$ si y sólo si K es el caso (a) o el caso (b) de la Nota 3.3.11.

□

Extensiones cuadráticas abelianas imaginarias

Las extensiones cuadráticas son un caso particular de las extensiones de Kummer. Así consideramos $K \subseteq k(\Lambda_N)$. Recordemos que una extensión cuadrática es imaginaria si $\mathfrak{p}_\infty$ se ramifica o es inerte. En particular una extensión cuadrática es abeliana imaginaria si $\mathfrak{p}_\infty$ se ramifica en K/k, pues en los campos ciclotómicos no hay primos infinitos inertes.

Considerando la notación para extensiones de Kummer, en nuestro caso $\ell = 2$, D es un polinomio mónico de grado impar y $K = k\left(\sqrt{(-1)^{\operatorname{gr} D} D}\right)$

Así si K/k es una extensión cuadrática abeliana imaginaria, entonces se tienen las siguientes propiedades:

1. $q > 2$.

2. $\mathfrak{p}_\infty$ se ramifica en K/k.

3. $K \cap k(\Lambda_N)^+ = k$, es decir la extensión K/k es totalmente imaginaria.

4. El grupo de unidades de K es $U_K = \mathbb{F}_q^*$.

5. Dado $K = k\left(\sqrt{f(T)}\right)$, donde $f(T) \in R_T = \mathbb{F}_q[T]$ es libre de cuadrados, $d = \operatorname{gr} f(T)$ y a_d es el coeficiente líder de $f(T)$. Si d es impar, entonces $\mathfrak{p}_\infty$ es ramificado en K. Si d es par y a_d es libre de cuadrados en $\mathbb{F}_q^*$, entonces $\mathfrak{p}_\infty$ se descompone en K. Si d es par y a_d no es libre de cuadrados en $\mathbb{F}_q^*$, entonces $\mathfrak{p}_\infty$ es primo en K.

   Demostración. Véase [48, Proposición 14.6]. □

6. $h_S = h_K$ si $\mathfrak{p}_\infty$ es ramificado, $h_S = 2h_K$ si $\mathfrak{p}_\infty$ es inerte y $h_S \log_q |e|_{\mathfrak{P}_\infty} = h_K$ si $\mathfrak{P}_\infty$ se descompone (e es una unidad fundamental en $\mathcal{O}_S$ y $\mathfrak{P}_\infty$ es el primo sobre $\mathfrak{p}_\infty$ en que e tiene orden negativo). Por lo tanto en nuestro caso $r_S = 1$.

   Demostración. Véase [48, Proposición 14.7]. □

Observación 3.3.14. Si K/k es una extensión cuadrática imaginaria, como $\wp_\infty$ se ramifica, por [48, Proposición 14.7], $h_S = h_K$ y $r_S = 1$.

Proposición 3.3.15. *Sea K una extensión cuadrática. Entonces K es abeliana imaginaria en los siguientes casos:*

1. *Si $g_K = 1$, entonces hay una extensión.*

2. *Si $g_K = 0$, entonces hay muchas extensiones.*

Demostración. 1. Si $g_K = 1$, como $h_K = h_S$ y $h_K = 1$ sólo en el caso (a) de la Nota 3.3.11.

2. Si $g_K = 0$, como $K \subseteq k(\Lambda_M)$, entonces K es un campo de funciones racionales y $h_K = h_S = 1$.

□

Nota 3.3.16. *Por la fórmula de Schmidt, en las extensiones cuadráticas que son abelianas imaginarias, se tiene $h_K = h_S$. Por lo que la única extensión cuadrática con $h_S = 1$ y $g_K = 1$ es la dada por la Nota 3.3.11 (a).*

De la Proposición 3.3.15 y la Nota 3.3.16 se tiene el siguiente resultado.

Teorema 3.3.17. *Sea $k = \mathbb{F}_q(T)$, K/k una extensión cuadrática abeliana imaginaria. Se tiene $h_K = h_S$. Entonces $h_S = 1$ si y sólo si $h_K = 1$ si y sólo si $g_K = 0$ o $g_K = 1$, $q = 3$ y $K = k\left(\sqrt{-(T^3 + 2T + 1)}\right)$.*

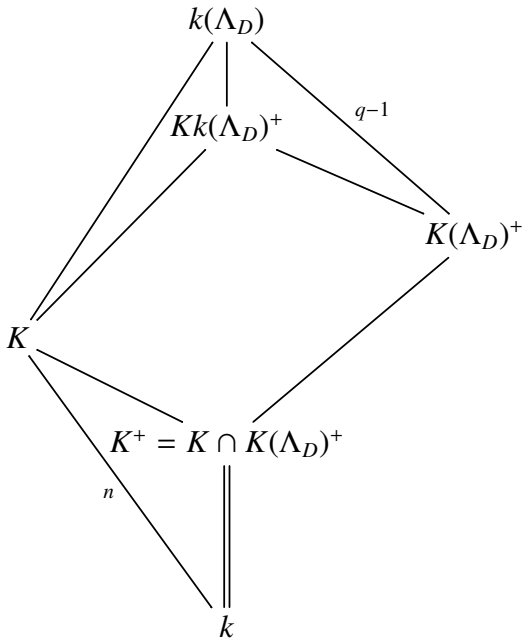
Extensiones de Kummer de grado n

Observación 3.3.18. Lo siguiente se tiene por [53].

- Para el caso de extensiones totalmente imaginarias, aparte de las soluciones de la nota 3.3.11, todos los campos de funciones con número de clases de divisores uno, no tienen lugar racional y por lo tanto tienen número de clases de ideales mayor que uno.

- Para una extensión abeliana imaginaria, no hay solución cuando $[K : K^+] = \ell^3$ y en general, no habrá solución cuando $[K : K^+] = \ell^j$, $j \geq 3$.

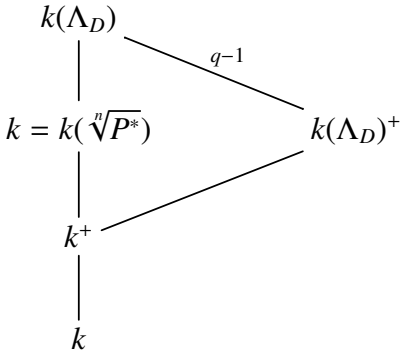
Sea K una extensión de Kummer de grado n, $k = \mathbb{F}_q(T)$. Pedimos que $n \mid q - 1$. Sea D polinomio mónico, $D = P_1^{a_1} \cdots P_r^{a_r}$. Consideramos $K = k(y)$, donde $y^n = (-1)^{\operatorname{gr} D} D$. En nuestro caso necesitamos que $K \subseteq k(\Lambda_D)$. Se tiene que $[K : k] = n$. Entonces K/k es una extensión de Kummer cíclica de grado n. Aquí $G := \operatorname{Gal}(K/k) = \langle \sigma \rangle$. El índice de ramificación es $e_{\wp_i} = \frac{n}{(n,a_i)}$, $e_\infty = \frac{n}{(n,\operatorname{gr} D)}$.



Queremos ver si se puede dar el caso en que se tengan dos extensiones cíclicas, pero que su compuesto no sea cíclico.

Proposición 3.3.19. *Sea* $K = k\left(\sqrt[n]{P^*}\right)$ *una extensión cíclica de grado n, donde* $P^* = (-1)^{\operatorname{gr} P} P$ *y* $\operatorname{gr} P = 1$. *Entonces K es una extensión abeliana imaginaria si K es un campo de funciones racionales y* $h_S = 1$.

Demostración.



Sea $y^n = f(x)$ con $f(x)$ libre de n-potencias y característica que no divida a n. Sea $f(x) = P$, $\operatorname{gr} P = 1$.

$((P(x)))_{k(x)} = \frac{\mathfrak{p}_i}{\mathfrak{p}_\infty^{\operatorname{gr} P}} = \frac{P_i}{\mathfrak{p}_\infty}$ y $\mathfrak{Z}_{P(x)} = \mathfrak{p}$. Como la extensión es abeliana imaginaria, entonces $\mathfrak{p}_\infty$ se ramifica en K/k. Con esto, $\operatorname{con}_{k(x)/K}(\mathfrak{p}) = \mathfrak{P}$ y $\mathfrak{D}_{K/k(x)} = \mathcal{P}^{n-1}\mathcal{P}_\infty^{n-1}$.

$\operatorname{gr} \mathfrak{D}_{K/k} = \operatorname{gr} P(n-1) + (n-1) = 2(n-1)$.

Por la fórmula de Riemann-Hurwitz

$$\begin{aligned} 2g_K - 2 &= n(2g_k - 2) + \operatorname{gr} \mathfrak{D}_{K/k} = n(-2) + (\operatorname{gr} P - 1)(n-1) \\ &= -2n + \operatorname{gr} P(n) - \operatorname{gr} P + n - 1 = -n + \operatorname{gr} P(n) - \operatorname{gr} P - 1 \\ 2g_K &= \operatorname{gr} P(n) - n - \operatorname{gr} P + 1 = \operatorname{gr} P(n-1) - (n-1) = (n-1)(\operatorname{gr} P - 1) \\ g_K &= \frac{1}{2}(n-1)(\operatorname{gr} P - 1) \text{ sustituyendo } \operatorname{gr} P = 1 \\ g_K &= 0 \end{aligned}$$

Con esto concluimos que K es un campo de funciones racionales y por lo tanto $h_S = 1$. □

Proposición 3.3.20. *Sea $K = k\left(\sqrt[n]{P^*}\right)$ una extensión cíclica de grado n, donde $P^* = (-1)^{\operatorname{gr} P} P$ y $\operatorname{gr} P \geq 2$. Entonces $h_S > 1$.*

Demostración. Usamos el siguiente resultado del artículo [30]:

$$K = K_1 K_2 \subsetneq K_{1\mathfrak{g}} K_{2\mathfrak{g}} \subseteq K_{\mathfrak{g}}.$$

Si $\operatorname{gr} P_1 > 1$ y $\operatorname{gr} P_2 > 1$, entonces $K_{i\mathfrak{g}} \supsetneq K_i$, con $i = 1, 2$. Entonces $h_S > 1$. □

Observación 3.3.21. Si el número de primos es mayor o igual que 2 y al menos uno de los primos tiene grado mayor que 1, entonces $K_{\mathfrak{g}} \supsetneq K$ y por lo tanto $h_S > 1$.

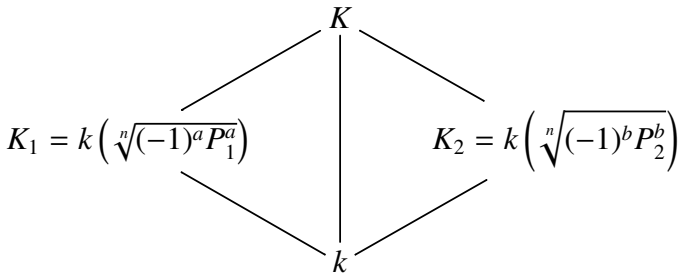
Ahora veremos el caso en que $s \geq 2$ pero todos los primos son de grado 1.

Sea $k = \mathbb{F}_q(T)$, con $n \mid q-1$ y $P^* = (-1)^{\operatorname{gr} P} P$. Notemos que

$$(P_1^*)^a (P_2^*)^b = \left((-1)^{\operatorname{gr} P_1} P_1\right)^a \left((-1)^{\operatorname{gr} P_2} P_2\right)^b = (-1)^{(a \operatorname{gr} P_1) + (b \operatorname{gr} P_2)} P_1^a P_2^b$$

Luego $K = k\left(\sqrt[n]{(-1)^{a+b} P_1^a P_2^b}\right)$.

Se tiene entonces el siguiente diagrama:



K_1/k y K_2/k son campos de funciones racionales.

Observación 3.3.22. Si $s \geq 2$ y todos los primos son de grado 1, entonces K es un campo de funciones racionales, $g_K = 0$ y $h_S = 1$.

En general, si $K = k\left(\sqrt[n]{P_1^* \cdots P_n^*}\right)$, con $\operatorname{gr} P_i = 1$, entonces K es un campo de funciones racionales, $g_K = 0$ y $h_S = 1$.

Teorema 3.3.23. *Sea $K = K_1K_2$, con $K_i = \left((-1)^{\operatorname{gr} P_i} P_i\right)$ y $\operatorname{gr} P_i \geq 2$, entonces $h_S > 1$.*

La prueba se sigue del siguiente resultado:

Lema 3.3.24. *Si $K_1 \subsetneq (K_1)_{\mathfrak{g}}$ o $K_2 \subsetneq (K_2)_{\mathfrak{g}}$, entonces $K \subsetneq K_{\mathfrak{g}}$ y por lo tanto $h_S > 1$.*

Demostración. $(K_1)_{\mathfrak{g}}(K_2)_{\mathfrak{g}} \subseteq (K_1K_2)_{\mathfrak{g}} = K_{\mathfrak{g}}$. Luego $K \subsetneq K_{\mathfrak{g}}$ y así $h_S > 1$. □

Observación 3.3.25. Si $s = 1$ y $\operatorname{gr} P = 1$, entonces $g_K = 0$ y $h_S = 1$.

Observación 3.3.26. Si $s = 1$ y $\operatorname{gr} P \geq 2$, por [54], $h_S = h_K = 1$ sólo en los casos (a) y (b) de la nota 3.3.11.

Los siguientes resultados se prueban en [54].

Teorema 3.3.27. *Sea K/k una extensión cíclica de grado ℓ^n. Las extensiones abelianas imaginarias con número de clases de ideales uno y $g_K \neq 0$ están en la Tabla 3.3.*

$M(x)$	q	g_K	Bajo isomorfismo	h_K
$y^2 + 2x^3 + x + 1 = 0$	3	1	$x \mapsto x + a, a \in \mathbb{F}_3, \xi \leftrightarrow y$	1
$y^8 + y^2(x^3 + x) + x^2 + 1 = 0$	3	2	$x \mapsto ax + b, a \in \mathbb{F}_3^*, b \in \mathbb{F}_3$	8
$y^2 + y + x^3 + w = 0, \langle w \rangle = \mathbb{F}_4^*$	4	1	$x \mapsto x + a, a \in \mathbb{F}_4$	1
$y^4 = x^2 + 3$	5	1	$x \mapsto ax + b, a \in \mathbb{F}_5^*, b \in \mathbb{F}_5$	2
$y^4 = 4(x^2 + 2)$	5	1	$x \mapsto ax + b, a \in \mathbb{F}_5^*, b \in \mathbb{F}_5$	2

Tabla 3.3: Extensiones cíclicas abelianas imaginarias

Teorema 3.3.28. *Sea K/k una extensión cíclica de grado ℓ^n. Las soluciones isomorfas a las ecuaciones de MacRae que son abelianas imaginarias y cumplen $h_K = h_S = 1$ y $g_K \neq 0$ están en la Tabla 3.4.*

$M(x)$	q	g_K	h_K	h_S
$y^2 - x^3 + x + 1 = 0$	3	1	1	1
$y^2 + y + x^3 + w = 0$	4	1	1	1

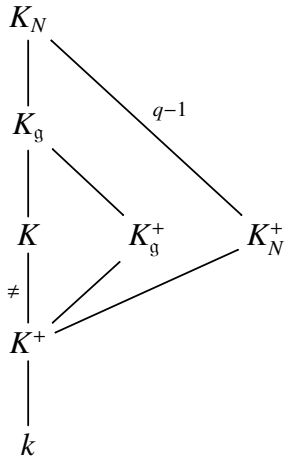
Tabla 3.4: Extensiones cíclicas isomorfas a soluciones de MacRae

3.3.4. Campos de géneros

Proposición 3.3.29. *Sean K una extensión abeliana imaginaria y $K_{\mathfrak{g}}$ su campo de géneros . Entonces $K_{\mathfrak{g}}$ también es una extensión abeliana imaginaria.*

Demostración. Puesto que K es una extensión abeliana imaginaria, $K \subseteq K_N$ para algún $N \in R_T$. Por [30], tenemos que $K_{\mathfrak{g}} \subseteq K_N$.

Consideremos el siguiente diagrama:

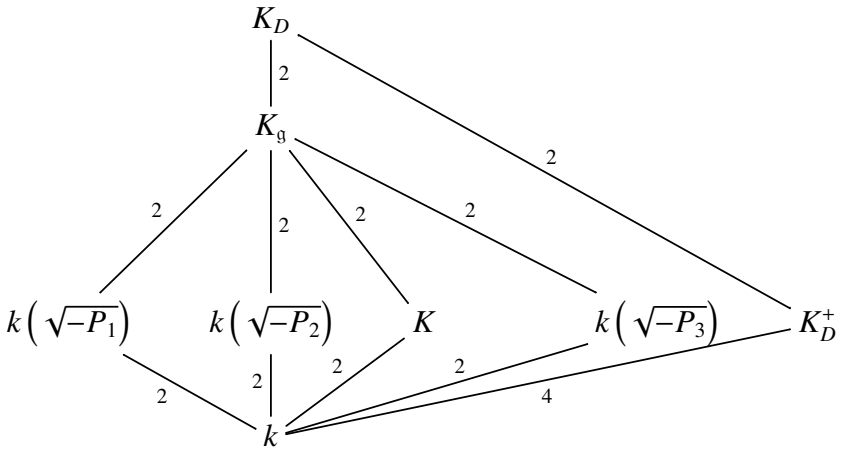


En general se tiene $K^+ = K \cap K_N^+ \subseteq K_{\mathfrak{g}} \cap K_N^+ = K_{\mathfrak{g}}^+$. Para que $K_{\mathfrak{g}}$ sea una extensión abeliana imaginaria es necesario que $K_{\mathfrak{g}} \neq K_{\mathfrak{g}}^+$. En caso de que $K_{\mathfrak{g}} = K_{\mathfrak{g}}^+$, tendríamos $K \subseteq K_{\mathfrak{g}} \subseteq K_N^+$ y puesto que $K \neq K^+$, se tiene $K \nsubseteq K_N^+$, lo cual es absurdo. Por lo tanto $K_{\mathfrak{g}} \neq K_{\mathfrak{g}}^+$.

Se concluye que $K_{\mathfrak{g}}$ es una extensión abeliana imaginaria de K.

□

Ejemplo 3.3.30. Sean $\ell = 2$, $q = 3$, $\alpha = 1$, $P_1 = T$, $P_2 = T + 1$, $P_3 = T - 1$. Con referencia al Teorema 3.1.13, $D = \gamma P_1 P_2 P_3$. Entonces $K = k\left(\sqrt{D}\right)$ y $[K_D : k] = \Phi(D) = \Phi(T)\Phi(T+1)\Phi(T-1) = 2 \cdot 2 \cdot 2 = 8$. Tenemos $K \cap K_D^+ = k$, es decir, K es una extensión abeliana imaginaria y el campo de géneros es $K_{\mathfrak{g}} = k\left(\sqrt{-P_1}\,\sqrt{-P_2}\,\sqrt{-P_3}\right)$. De donde se tiene el siguiente diagrama:


K_D
2
$K_{\mathfrak{g}}$
2
2
2
2
2
$k\left(\sqrt{-P_1}\right)$
$k\left(\sqrt{-P_2}\right)$
K
$k\left(\sqrt{-P_3}\right)$
K_D^+
2
2
2
2
4
k

Conclusiones y perspectivas

En el primer capítulo se obtuvieron los grupos de idèles correspondientes a $\mathbb{Q}(\zeta_n)$ y $k(\Lambda_N)$ en los Teoremas 1.1.60 y 1.1.62, respectivamente y se estudiaron, para el caso de campos numéricos, diversas relaciones entre los campos de clases de Hilbert y de Hilbert extendido y de campos de géneros y de géneros extendido. Finalmente, se presentó el campo de géneros extendido de un campo numérico (Teorema 1.3.2).

En el Capítulo 2 se ofreció una definición de campo de géneros extendido para campos de funciones (Definiciones 2.2.4, 2.2.7 y 2.2.9) y se obtuvo el campo de géneros extendido para campos de funciones (2.2.14), en términos de diversos campos auxiliares. Sería deseable determinar precisamente qué campos ciclotómicos tienen grupo de Galois cíclico con el fin de obtener resultados análogos a los encontrados para campos numéricos. Asimismo sería interesante un estudio comparativo de los distintos conceptos que hay para campos de géneros extendidos en el caso de campos de funciones.

En el tercer capítulo, en la definición de extensión abeliana imaginaria K/k, donde $k = \mathbb{F}_q(T)$, se requirió que $K \subseteq k(\Lambda_N)$ y que el primo al infinito $\mathfrak{p}_\infty$ sea totalmente descompuesto. Otra forma de analizarlas es ver qué es lo que pasa si permitimos que $\mathfrak{p}_\infty$ sea inerte o ramificado salvajemente. Por ejemplo, si K/k es una extensión abeliana en la que $\mathfrak{p}_\infty$ tiene ramificación salvaje, entonces si $h_K = 1$ no necesariamente $h_S = 1$. Con esto se esperaría poder encontrar más soluciones que las que se han mencionado en este trabajo, pues se podría trabajar con extensiones de Artin-Schreier por ejemplo (ver Nota 3.3.11 (b)).

Se obtuvo que si p es la característica de k, entonces las p-extensiones de k no son abelianas imaginarias (Proposición 3.3.5) y que si K es una extensión abeliana imaginaria de k, entonces su campo de géneros $K_{\mathfrak{g}}$ también lo es (Proposición 3.3.29).

Para las extensiones cíclicas de grado ℓ^2 y las bicuadráticas, se esperaba poder dar el comportamiento del primo al infinito en el nivel superior con base en los niveles intermedios, pero por una de las soluciones de Sémirat (ver Tabla 3.3) $y^4 = x^2 + 3$ y considerando $z^2 = x^2 + 3$ y $y^2 = z$, se

tiene lo siguiente:

$$\begin{array}{ll} K = k(y) & g_K = 1 \\ \Big| 2 & \\ K_1 = k\left(\sqrt{x^2+3}\right) & g_{K_1} = 0 \\ \Big| 2 & \\ k = \mathbb{F}_5(x) & \end{array}$$

La extensión K/K_1 tiene $h_S = 2$, mientras que la extensión K/k tiene $h_S = 1$. Así el valor de h_S depende del campo de funciones racionales sobre el que estamos considerando al campo K y en consecuencia el comportamiento de $\mathfrak{p}_\infty$ varía dependiendo del nivel en el que se encuentre. Esto es a diferencia del número de clases de divisores h_K que es un invariante de K, en este caso $h_K = 2$.

Notación

$\mathbb{A}$ anillo de adèles

C grupo de clases de divisores

C_0 grupo de clases de divisores de grado 0

C_n grupo cíclico de n elementos

$\mathcal{C}_K$ grupo de clases de idèles

$\mathscr{C}_S$ grupo de clases de ideales

D grupo de divisores

$\mathfrak{D}_{L/K}$ diferente de la extensión L/K.

D_0 grupo de divisores de grado 0

e_P índice de ramificación del lugar P

$\mathbb{F}_q$ campo finito de q elementos

$\mathcal{F}_S$ grupo de ideales fraccionarios

g_K género de K

gr grado o función grado

Gal(K/k) grupo de Galois de la extensión K/k

h_K número de clases de divisores de K

h_S número de clases de ideales

h_S^+ número de clases de ideales asociado con (K^*, S^+)

h_S^- número de clases de ideales relativos

Im φ imagen de φ

J conjugación compleja

$\mathcal{J}_S$ grupo de ideales fraccionarios

$\mathbb{J}_K$ grupo de idèles

K^+ subcampo real maximal de K

$k = \mathbb{F}_q(T)$ campo de funciones racionales

$K_{H,\mathcal{S}}$ campo de funciones de clases de Hilbert de K

K_H campo de clases de Hilbert

K_H^+ campo de clases de Hilbert extendido.

$K_{\mathfrak{g}}$ campo de géneros

$K_{\mathfrak{g}^+}$ campo de géneros extendido

$K_M = k(\Lambda_M)$ campo de funciones ciclotómico asociado con el polinomio $M(T)$

${}_nK := KL_n$

$K_m := K\mathbb{F}_{q^m}$

$N_{K/L}$ norma de K/L

$\operatorname{nuc}\varphi$ núcleo de φ

$\mathcal{O}_P$ anillo local asociado con la valuación $\mathfrak{v}_P$ en P

$\mathbb{P}$ grupo de divisores principales

$\mathfrak{p}_\infty$ el divisor primo de k asociado a $\left(\frac{1}{T}\right)$

$\mathbb{Q}(\zeta_n)$ campo ciclotómico numérico

r_S regulador

r_S^- regulador relativo

$R_T = \mathbb{F}_q[T]$ anillo de polinomios con coeficientes en T

χ caracter de Dirichlet

Bibliografía

[1] Anglès, Bruno; Jaulent, Jean–François,, *Théorie des genres des corps globaux*, Manuscripta Math. **101**, no. 4 (2000), 513–532.

[2] Artin, Emil; Tate, John, Class field theory, W.A. Benjamin Inc., 1967.

[3] Bae, Sunghan; Kang, Pyung–Lyun, *Class numbers of cyclotomic function fields*, Acta Arithmetica, **102.3** (2002), 251–259.

[4] Bae, Sunghan; Koo, Ja Kyung *Genus theory for function fields*, J. Austral. Math. Soc. (Series A), **60** (1996), 301–310.

[5] Barreto–Castañeda, Jonny Fernando; Montelongo–Vázquez, Carlos Manuel; Reyes–Morales Carlos Daniel; Rzedowski–Calderón, Martha & Villa–Salvador, Gabriel Daniel, *Genus fields of abelian extensions of rational congruence function fields II*, Rocky Mountain Journal of Mathematics, **48**, no. 7 (2018), 2099–2133.

[6] Bhaskaran M., *Construction of genus fields and some applications*, J. Number Theory, **11** (1979), 488–497.

[7] Bilhan, Mehpare, Buyruk, Dilek and Özbudak, Ferruh, *Classification function fields with class number three*, J. Pure and Applied Algebra, **219** (2015), 5097–5116.

[8] Clement, Rosario, *The genus field of an algebraic function field*, J. Number Theory, **40**, no. 3 (1992), 359–375.

[9] Dummit, David S. and Foote, Richard M. Abstract algebra, John Wiley and Sons, Inc., 2004.

[10] Dummit, David S. and Voight, John *The 2-Selmer group of a number field and heuristics for narrow class groups and signature ranks of units*, Proc. London Math. Soc., **117.3** (2018), 682-726.

[11] Fröhlich, Albrecht, *The genus field and genus group in finite number fields*, Mathematika, **6** (1959), 40–46.

[12] Fröhlich, Albrecht, *The genus field and genus group in finite number fields, II*, Mathematika, **6** (1959), 142–146.

[13] Galovich, Steven and Rosen, Michael, *Units and class groups in cyclotomic function fields*, J. Number Theory, **14** (1982), 156–184.

[14] Garzón R. Álvaro and Teherán Herrera, Arnoldo, *Elementary abelian p-extensions and curves with many points*, Rev. Acad. Colomb. Cienc., **36** (2012), 243–252.

[15] Gauss, Carl Friedrich, *Disquisitiones arithmeticae*, 1801.

[16] Hasse, Helmut, *Zur Geschlechtertheorie in quadratischen Zahlkörpern*, J. Math. Soc. Japan **3** (1951), 45–51.

[17] Hu, Su; Li Yan, *The genus fields of Artin-Schreier extensions*, Finite Fields and Their Applications, **16**, no. 4 (2010), 255–264.

[18] Janusz, Gerald J., Algebraic number fields: second edition, Graduate Studies in Mathematics, Volume 7, 1996.

[19] Jung, Hwanyup and Ahn, Jaehyun, *Divisor class number one problem for abelian extensions over rational function fields*, J. Algebra, **310** (2007), 1–14.

[20] Kato, Kazuya; Kurokawa, Nobushige and Saito Takeshi, Number theory: introduction to class field theory, American Mathematical Society, 2011.

[21] Kida, Masanari and Murabayashi, Naoki, *Cyclotomic function fields with divisor class number one*, Tokio J. Math, **14**, No. 1 (1991), 45–56.

[22] Koch, Helmut, Number Theory: Algebraic numbers and functions, American Mathematical Society, Providence, Rhode Island, 2000.

[23] Lang, Serge, Algebraic number theory, Springer-Verlag New York, Inc., 1994.

[24] Le Brigand, Dominique, *Classification of algebraic function fields with divisor class number two*, Finite Fields and Their Applications, **2** (1996), 153–172.

[25] Le Brigand, Dominique, *Real quadratic extensions of the rational function field in charcteristic two*, Séminaires and Congrès, **11** (2005), 143–169.

[26] Leitzel, James R. C., Madan Manohar L. and Queen Clifford S, *Algebraic function fields with small class number*, J. Number Theory, **7** (1975), 11–27.

[27] Leopoldt, Heinrich W., *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr., **9** (1953), 351–362.

[28] MacRae, R. E., *On unique factorization in certain rings of algebraic functions*, J. Algebra, **17** (1971), 243–261.

[29] Madan, M. L. and Queen, C. S., *Algebraic function fields of class number one*, Acta Arith., **20** (1972), 423-432.

[30] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel, *Genus fields of abelian extensions of congruence rational function fields*, Finite Fields and Their Applications, **20** (2013), 40–54.

[31] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel, *Corrigendum to "Genus fields of abelian extensions of rational congruence function fields", [Finite Fields Appl. 20 (2013), 40–54]*, Finite Fields and Their Applications, **33** (2015), 283–285.

[32] Maldonado–Ramírez, Myriam; Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel, *Genus fields of congruence function fields*, Finite Fields and Their Applications, **44** (2017), 56–75.

[33] Masley J. M., Montgomery, H: L. *Cyclotomic fields with unique factorization* J. Reine Angew. Math. (1976).

[34] Mercuri, Pietro and Stirpe, Claudio, *Classification of algebraic function fields with class number one*, J. Number Theory, **154** (2015), 365–374.

[35] Neukirch, Jürgen, Class field theory, Springer-Verlag, Berlin-New York, 1986.

[36] Neukirch, Jürgen, Algebraic number theory, Springer-Verlag, Berlin-New York, 1999.

[37] Neukirch, Jürgen, Schmidt, A., Wingberg, K., Cohomology of number fields, second edition, Springer-Verlag, New York-Berlin-Heidelberg, 2008.

[38] Neukirch, Jürgen, Class field theory, The Bonn Lectures, Edited by Alexander Schmidt, Springer-Verlag, Berlin-New York, 2013.

[39] Newman, M.. *Cyclotomic units and Hilberts Satz 90*, Acta Arithmetica, **XLI**, (1982).

[40] Ngoc, N. and Quan, D., *Representation of units in cyclotomic function fields*, arXiv:1512.05043vI [math.NT] (2015), 1–16.

[41] Peng, Guohua, *The genus fields of Kummer function fields*, J. Number Theory **98**, no. 2 (2003), 221–227.

[42] Picone, Alberto, *On the classification of algebraic function fields of class number three*, Discrete Mathematics, **312** (2012), 637–646.

[43] Ramírez–Ramírez, Elizabeth, *Campos de funciones ciclotómicos con número de clases de divisores uno*, Tesis de maestría, CINVESTAV, 2014.

[44] Ramírez–Ramírez, Elizabeth; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus fields of global fields*, to appear in Palestine Journal of Mathematics.

[45] Ribes, L. and Zalesskii, P., Profinite groups, Springer-Verlag, New York-Berlin-Heidelberg, 2010.

[46] Rosen, Michael, *S-units and S-class group in algebraic function fields*, J. Algebra, **26**, (1973), 98–108.

[47] Rosen, Michael, *The Hilbert class field in function fields*, Exposition Math, **5**, no.4, (1987), 365–378.

[48] Rosen, Michael, Number theory in function fields, GTM 210, Springer-Verlag, New York-Berlin-Heidelberg, 2002.

[49] Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel, *Congruence function fields with class number one*, Palestine Journal of Mathematics, Vol. 5, **1** (2016), 159–165.

[50] Rzedowski–Calderón, Martha and Villa–Salvador, Gabriel, Campos ciclotómicos numéricos y de funciones (segunda versión) con una introducción a la teoría de campos de clase, https://arxiv.org/abs/1407.3238.

[51] Salas-Torres, Julio César and Rzedowski-Calderón, Martha, *Caracteres de Dirichlet en campos de funciones*, Aportaciones Matemáticas Memorias, **36** (2006), 127–144.

[52] Samuel, Pierre, Algebraic theory of numbers, Hermann, Paris, 1970.

[53] Semirat, Stéphan, *Class number one problem for imaginary function field: The cyclic prime power case*, J. Number Theory, **84** (2000), 166–183.

[54] Sémirat, Stéphan, *Cyclotomic function fields with ideal class number one*, J. Algebra, **236** (2001), 376–395.

[55] Serre, Jean Pierre, Local fields, GTM 67, Springer-Verlag, New York-Berlin-Heidelberg, 1979.

[56] Serre, Jean-Pierre, Algebraic groups and class fields, Springer-Verlag, New York-Berlin-Heidelberg, 1988.

[57] Stichtenoth, H., Algebraic function fields and codes, Universitext, Springer-Verlag, Berlin-New York, 1993.

[58] Vargas-Mendoza, J. A., Álgebra Clásica, Publicaciones electrónicas SMM, Serie Textos, Vol.7, México, 2006.

[59] Villa–Salvador, Gabriel, Topics in the theory of algebraic function fields, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.

[60] Washington, Lawrence C., Introduction to Cyclotomic Fields, GTM **83**, Springer-Verlag, New York, 1997.

[61] Yamamura, K. *The determination of the imaginary abelian number fields with class number one*, Math. Comp. 62, **206** (1994), 899–921.

[62] Zaldívar, Felipe, Teoría de Galois, Anthropos, México, 1996.

[63] Zaldívar, Felipe, Campos locales, UAM Iztapalapa, México, 2001.

[64] Zhang, Xianke, *Counterexample and correction about genus fields of number fields*, J. Number Theory, **23**, (1986), 318–321.

Índice alfabético