Centro de Investigación y de Estudios Avanzados
del Instituto Politécnico Nacional

Unidad Zacatenco

Departamento de Control Automático

Cálculo del Campo de Géneros de una Extensión l-elemental Abeliana de $\mathbb{F}_q(T)$

T E S I S

Presenta

Juan Carlos Hernandez Bocanegra

Para obtener el grado de

MAESTRO EN CIENCIAS

En la especialidad de

CONTROL AUTOMÁTICO

Director de la Tesis

Dr. Gabriel Daniel Villa Salvador

Ciudad de México **Abril, 2021**

Dedicatoria

A mis padres, hermanos y Alondra

Agradecimientos

Al Dr. Gabriel Villa y a la Dra. Martha Rzedowski por haberme brindado el conocimiento para poder desarrollar el presente trabajo, así como su paciencia y confianza.

Al Dr. Pablo Lam que me orientó durante la licenciatura para llegar a los estudios de maestría.

Al CINVESTAV y al Departamento de Control Automático por abrirme las puertas para poder realizar mis estudios de maestría, así como al CONACYT por el apoyo otorgado para culminar mis estudios.

A mis padres y hermanos por su paciencia y apoyo incondicional.

Resumen

En el presente trabajo se da la construcción del campo de géneros de una extensión l-elemental abeliana de un campo de funciones racionales, cuyo grupo de Galois es isomorfo a C_l^m. Primero, para el caso Kummer, es decir, $l|q-1$, si K está contenido en un campo de funciones ciclotómico, la construcción se da usando la ideas de Leopoldt mediante caracteres de Dirichlet, mientras que en el caso no ciclotómico, se siguen las ideas del Teorema 2.2 en [2] para describir explícitamente el campos de géneros. Se siguió un proceso análogo para el caso no Kummer.

Abstract

In the present work we give the construction of the genus field of an elementary abelian l-extension of a field of rational functions, whose Galois group is isomorphic to C_l^m. First, in the Kummer case, that is when $l|q-1$, if K is contained in a cyclotomic funtion field, the construction is given using Leopoldt's ideas by means of Dirichlet characters, while in the non-cyclotomic case we use the ideas of Theorem 2.2 in [2] to describe explicitly the genus fields. We follow an analogous process for the non-Kummer case.

Índice general

Capítulo 1

Introducción

El estudio de *campos de géneros* comenzó con C.F. Gauss [7], en el contexto de formas cuadráticas binarias. Fue en la primera mitad del siglo pasado, que el concepto de campos de géneros se introdujo a campos numéricos cuadráticos. Para una extensión finita arbitraria $K/\mathbb{Q}$, el campo de géneros se define como la máxima extensión no ramificada en ningún primo K_{ge} de K tal que K_{ge} es la composición de K y una extensión abeliana k^* de $\mathbb{Q}$, esto es, $K_{ge} = Kk^*$. Esta definición la dio A. Fröhlich [6]. Similarmente para el campo de géneros extendido K_{gex} de K, donde $K_{gex} = KL$ con $L/\mathbb{Q}$ la máxima extensión abeliana tal que KL/K es no ramificada en los primos finitos.

H. Hasse [8] estudió la teoría de campos de géneros para campos numéricos mediante la teoría de campos de clases. Fue H. W. Leopoldt [13] quien determinó el campo de géneros K_{ge} de una extensión abeliana K de $\mathbb{Q}$ mediante el uso de caracteres de Dirichlet, generalizando así el trabajo de Hasse.

En un campo numérico K, donde $[K : \mathbb{Q}] < \infty$, el *campo de clases de Hilbert* K_H de K se define como la máxima extensión abeliana de K no ramificada en ningún primo. El *campo de clases de Hilbert extendido* K_{H^+} se define como la máxima extensión abeliana de K no ramificada en los primos finitos. Se tiene que $K \subseteq K_{ge} \subseteq K_H$ donde $\mathrm{Gal}(K_H/K)$ es isomorfo al grupo de clases Cl_K de K. El campo de géneros K_{ge} corresponde a un subgrupo G_K de Cl_K. Se tiene que $\mathrm{Gal}(K_{ge}/K) \cong Cl_K/G_K$. El grado $[K_{ge} : K]$ es llamado el *número de géneros* de K y al grupo $\mathrm{Gal}(K_{ge}/K)$ se le conoce como *grupo de géneros*. Similarmente para $K \subseteq K_{gex} \subseteq K_{H^+}$.

M. Ishida [11] determinó el campo de géneros K_{ge} para cualquier extensión finita de $\mathbb{Q}$. X. Zhang [22] dio una expresión simple de K_{ge} para cualquier extensión K de $\mathbb{Q}$ usando la teoría de ramificación de Hilbert.

En campos de funciones congruentes, se tiene que dado cualquier campo de funciones congruente $K/\mathbb{F}_q$, donde $\mathbb{F}_q$ es el campo finito de q elementos, $q = p^n$ con p un número primo y n un entero positivo, la máxima extensión abeliana de K contiene a la extensión de constantes $K_m := K\mathbb{F}_{q^m}$ para cualquier entero positivo m. Por tanto la definición directa de campo de clases de Hilbert

como la máxima extensión abeliana no ramificada tiene el inconveniente de ser de grado infinito sobre el campo dado.

M. Rosen [18] dio una definición análoga del campo de clases de Hilbert de K; de un conjunto finito no vacío fijo S_∞ de divisores primos de K, el campo de clases de Hilbert se define como la máxima extensión abeliana de K no ramificada y tal que los primos del conjunto S_∞ se descomponen totalmente. Usando esta definición se puede dar un concepto adecuado del campo de géneros, como en el caso de campos numéricos. Fue R. Clement[4] la primera en considerar una extensión cíclica del campo de funciones racionales $k = \mathbb{F}_q(T)$ de grado un número primo l que divide a $q-1$. Mediante la teoría de campos de clases encontró el campo de géneros. S. Bae y J.K. Koo [1] generalizaron el resultado de Clement usando los métodos de Fröhlich.

G. Peng [17] describió explícitamente el campo de géneros para una extensión cíclica de Kummer de grado primo de un campo de funciones congruentes. Posteriormente S. Hu y Y. Li [9] describieron las clases de ideales ambiguas y el campo de géneros de una extensión de Artin-Schreier de un campo de funciones racionales.

En [15] y [16] se desarrolla la teoría de campos de géneros en un campo de funciones congruentes usando la definición de Rosen de campos de clases de Hilbert. El método que se empleó está basado en las ideas de Leopoldt usando los caracteres de Dirichlet. Se da una descripción general del campo de géneros K_{ge} de una extensión abeliana K de $k = \mathbb{F}_q(T)$ en términos de caracteres de Dirichlet. El método se puede usar como aplicación para encontrar explícitamente K_{ge} de una extensión de grado primo $l|(q-1)$ (Kummer) o $l = p$ donde p es la característica (Artin-Schreier) y también cuando K/k es una extensión p-cíclica (Witt). Después este método fue usado en [3] para describir K_{ge} explícitamente cuando K/k es una extensión cíclica de grado l^n, donde l es un número primo y $l^n|q-1$. En [14] se describe el campo de géneros de una extensión finita y separable de $k = \mathbb{F}_q(T)$ como $K_{ge} = Kk^*$ donde k^* es la composición de dos campos k_1 y k_2 siguiendo el método de Ishida [11].

El estudio de las l-extensiones abelianas elementales finitas ha sido considerado en algunos trabajos, recientemente [2], [15], [16], [3]. En [2] se describe el campo de géneros K_{ge} de una extensión abeliana finita K de $k = \mathbb{F}_q(T)$, aprovechando el estudio de estas extensiones, el camino por el cual se encontró K_{ge} resulta más transparente que en [15].

En el presente trabajo se estudia el campo de géneros de una extensión abeliana K de grado l^m de un campo de funciones racionales congruente $k = \mathbb{F}_q(T)$, donde $K = K_1 \cdots K_m$ con $\mathrm{Gal}(K/k) \cong C_l^m$, y donde C_l es un grupo cíclico de orden l. Usando las ideas que se obtuvieron en [2] se describe el campo de géneros cuando $l|(q-1)$, caso Kummer y cuando $l \nmid (q-1)$, caso no Kummer.

Capítulo 2

Antecedentes

2.1. Teoría de Galois

Se dice que una extensión algebraica de campos F/k es de Galois cuando es normal y separable.

Definición 2.1.1. Dada una extensión arbitraria de campos F/k, definimos el *grupo de Galois*, escrito $\mathrm{Gal}(F/k)$, como el grupo de k-automorfismos de F.

Teorema 2.1.2 (Fundamental de la Teoría de Galois)**.** *Sea F/k una extensión finita de Galois con $G = \mathrm{Gal}(F/k)$. Entonces:*

a) La función que a un campo intermedio E le asocia el grupo H de los E-automorfismos de F, es una biyección del conjunto de los campos intermedios al conjunto de los subgrupos de G cuyo inverso envía cada subgrupo H de G al conjunto de los puntos fijos F^H.

b) La extensión F/E es de Galois para todo campo intermedio E.

c) La extensión E/k es de Galois si y sólo si el subgrupo asociado a E, $\mathrm{Gal}(F/E)$ es normal en G. Cuando esto sucede, $\varphi : G \longrightarrow \mathrm{Gal}(E/k)$ dado por $\varphi(\sigma) = \sigma|_E$ es un epimorfismo de grupos con núcleo $\mathrm{Gal}(F/E)$, de manera que $\mathrm{Gal}(E/k) \cong G/\mathrm{Gal}(F/E)$.

d) Si el campo intermedio E está asociado al subgrupo H de G y $\sigma \in G$ entonces σE es un campo intermedio asociado al subgrupo $\sigma H \sigma^{-1}$ de G.

e) $[F : k] = \circ(G)$.

Demostración. Ver [20, Teorema 3.34]. □

Teorema 2.1.3 (Artin)**.** *Sea F un campo y sea G el grupo finito de automorfismos de F, de orden n. Sea $k = F^G$ el campo dejado fijo por G. Entonces F/k es una extensión finita de Galois, con grupo de Galois $\mathrm{Gal}(F/k) = G$ y $[F : k] = n$.*

Demostración. Ver [12, Chapter VI, Theorem 1.8]. □

A continuación se enuncian dos resultados de la teoría general de Galois finita que son mencionados a lo largo de las demostraciones del Capítulo 3.

Teorema 2.1.4. *a) Si F es una extensión finita de Galois de k con grupo de Galois $G \cong G_1 \times G_2$, entonces los campos $E_1 = F^{G_1}$ y $E_2 = F^{G_2}$ satisfacen $F = E_1E_2$ y $k = E_1 \cap E_2$. Además, las extensiones E_1/k y E_2/k son finitas de Galois.*

b) Recíprocamente, si E_1/k y E_2/k son extensiones finitas de Galois con E_1 y E_2 contenidos en un campo, $k = E_1 \cap E_2$, $H = \mathrm{Gal}(E_1/k)$ y $J = \mathrm{Gal}(E_2/k)$, entonces la extensión E_1E_2 es una extensión finita de Galois de k con grupo de Galois $G \cong H \times J$.

Demostración. Ver [20, Teorema 3.39]. □

Teorema 2.1.5. *(Teorema de Correspondencia de Galois) Sean L/k y F/k extensiones finitas tal que L/k es una extensión de Galois.*

a) La extensión LF/F es de Galois y $\mathrm{Gal}(LF/F) \cong \mathrm{Gal}(L/L\cap F)$ por restricción. En particular,

$$[LF : F] = [L : L \cap F] \ \ y \ \ [LF : k] = \frac{[L : k][F : k]}{[L \cap F : k]}.$$

Entonces $[LF : k] = [L : k][F : k]$ si y sólo si $L \cap F = k$.

b) El conjunto de campos intermedios $\{M \mid F \subseteq M \subseteq LF\}$ y $\{M' \mid L \cap F \subseteq M' \subseteq L\}$ están en correspondencia biyectiva, con biyección $M \mapsto L \cap M$, cuya inversa es $M' \mapsto M'F$. En particular, todo campo entre F y LF tiene la forma $F(\alpha)$ con $\alpha \in L$ y si M y M' están en correspondencia por la biyección, entonces M/F es de Galois si y sólo si $M'/L \cap F$ es de Galois, en dicho caso $\mathrm{Gal}(M/F) \cong \mathrm{Gal}(M'/L \cap F)$ con el isomorfismo dado por restricción.

Demostración. Ver [5, Theorem 2.6]. □

Observación 2.1.6. De aquí en adelante, cuando se hable de una extensión finita, abeliana o cíclica, se entenderá que es de Galois y que el grupo de Galois es finito, abeliano o cíclico respectivamente.

Algunos de los resultados que se deben considerar sobre extensiones de campos finitos son los siguientes

Teorema 2.1.7. *a) La extensión $\mathbb{F}_q/\mathbb{F}_p$ es finita de Galois.*

b) $G = \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ es cíclico, generado por el morfismo de Frobenius.

c) $G = \mathrm{Aut}(\mathbb{F}_q)$

Demostración. Ver [20, Teorema 3.50]. □

Proposición 2.1.8. *Sea K una extensión finita de $\mathbb{F}_q$. Entonces $K/\mathbb{F}_q$ es una extensión de Galois. El grupo de Galois $\mathrm{Gal}(K/\mathbb{F}_q)$ es cíclico.*

Demostración. Ver [10, Proposition 5.10]. □

2.2. Campos de funciones

Cuando se estudian los campos numéricos y los campos de funciones, es fácil notar que existen muchas similitudes, esto cuando el campo de constantes del campo de funciones es finito, pues resulta que los campos residuales también son finitos lo que permite la analogía entre ambos. Sin embargo, note que aun así persisten diferencias que no se deben pasar por alto. Si K es un campo numérico y $\mathfrak{p}$ es un ideal primo en $\mathcal{O}_K$, se tiene que $\mathcal{O}_K/\mathfrak{p}$ es el campo residual y éste es finito, en particular su característica es finita siendo que la característica de K es cero, por lo tanto, K y $\mathcal{O}_K/\mathfrak{p}$ tienen característica distinta. En este capítulo K/k denotará un campo de funciones racionales con k un campo perfecto (Definición 2.2.1). Sea $\mathfrak{p} \in \mathbb{P}_K$, entonces el campo residual $k(\mathfrak{p})$ es una extensión finita de k, y por lo tanto k y $k(\mathfrak{p})$ tienen la misma característica.

Otra notable diferencia es, si dados $a, b, c, d \in k$ con $ad - bc \neq 0$, se tiene que $k(\frac{ax+b}{cx+d}) = k(x)$, por lo que si $y = \frac{ax+b}{cx+d}$, el anillo de polinomios de $k(y)$ es $k[y]$, el cual es isomorfo a $k[x]$, pero no son iguales, a pesar de que los campos de cocientes lo sean. Esto no sucede en $\mathbb{Z}$, pues en dado caso de ser R un subanillo de $\mathbb{Q}$ isomorfo a $\mathbb{Z}$, necesariamente $R = \mathbb{Z}$. Dado que $\mathbb{Q}$ es campo primo, éste no tiene subcampos propios, mientras que $k(x^n) \cong k(x) \cong k(x^{1/n})$, pero se tiene la siguiente torre de campos $k(x^n) \subseteq k(x) \subseteq k(x^{1/n})$, cada una de estas extensiones es de grado n.

A continuación se enuncian algunos resultados generales de campos de funciones sin su demostración. Téngase en cuenta que el propósito del presente trabajo es encontrar el campo de géneros, donde el campo base es un campo de funciones racionales congruente.

Definición 2.2.1. Sea k un campo arbitrario. Un *campo de funciones algebraicas K sobre k* es una extensión finitamente generada de k con grado de trascendencia $r \geqslant 1$, K es llamado un *campo de funciones algebraicas de r- variables.*

Definición 2.2.2. Sea K/k un campo de funciones. La cerradura algebraica de k en K, esto es, el campo $k' = \{\alpha \in K \mid \alpha \text{ es algebraico sobre } k\}$, es llamado el *campo de constantes de K.*

En este trabajo se considera que k algebraicamente cerrado en K, es decir, $k'' = k$.

Definición 2.2.3. Un campo de funciones K/F se llama *campo de funciones global o campo de funciones congruente* si F es un campo finito.

Definición 2.2.4. Sea K un campo arbitrario. Una *valuación discreta* sobre K es una función suprayectiva $v : K^* \longrightarrow \mathbb{Z}$ que satisface

(i) Para $a, b \in K^*$, $v(ab) = v(a) + v(b)$, esto es, v es un epimorfismo de grupos,

(ii) Para $a, b \in K^*$, tales que $a + b \neq 0$, $v(a + b) \geqslant \text{mín}\{v(a), v(b)\}$.

Se entenderá que $v(0) = \infty$. Sean $\mathcal{O}_v = \{x \in K \mid v(x) \geqslant 0\}$ y $\mathfrak{p}_v = \{x \in K \mid v(x) > 0\}$ el anillo de valuación de v y el ideal máximo de $\mathcal{O}_v$ respectivamente. Al campo $k(v) \coloneqq \mathcal{O}_v/\mathfrak{p}_v$ de le llama el campo residual de v y éste es una extensión finita de k. Cuando se hable de valuación, anillo de valuación e ideal máximo, se entenderá indistintamente a los tres como *lugar*.

Sean $k(x)$ un campo de funciones y sea $f(x) \in k[x]$ un polinomio mónico e irreducible de $k[x]$. Entonces si $\alpha(x) \in k(x)^*$, $\alpha(x)$ se puede escribir de manera única como $\alpha(x) = f(x)^s \frac{a(x)}{b(x)}$ donde $a(x), b(x) \in k[x]$ son polinomios primos relativos a $f(x)$ y $s \in \mathbb{Z}$. Entonces se define $v_f(\alpha(x)) \coloneqq s$. Se tiene que v_f es una valuación en K asociada a f. El anillo de valuación y el ideal máximo están dados por:

$$\mathcal{O}_{v_f} = \mathcal{O}_f = \left\{ \frac{a(x)}{b(x)} \in k(x) \mid \operatorname{mcd}(b(x), f(x)) = 1 \right\}$$
$$\mathfrak{p}_{v_f} = \mathfrak{p}_f = \left\{ \frac{a(x)}{b(x)} \in k(x) \mid f(x) | a(x),\ \operatorname{mcd}(b(x), f(x)) = 1 \right\}.$$

Ahora sea $\beta(x) \in k(x)^*$ y $\beta(x) = \frac{h(x)}{g(x)}$ con $h(x), g(x) \in k[x]$. Se define el *grado* de β por: $\operatorname{gr} \beta = \operatorname{gr} h - \operatorname{gr} g$. Sea $v_\infty : k(x)^* \to \mathbb{Z}$, $v_\infty(\beta(x)) = -\operatorname{gr} \beta$. Entonces v_∞ es otra valuación diferente a todas las valuaciones v_f, en este caso

$$\mathcal{O}_{v_\infty} = \mathcal{O}_\infty = \left\{ \frac{h(x)}{g(x)} \in k(x) \mid \operatorname{gr} h - \operatorname{gr} g \leqslant 0 \right\}$$
$$\mathfrak{p}_{v_\infty} = \mathfrak{p}_\infty = \left\{ \frac{h(x)}{g(x)} \in k(x) \mid \operatorname{gr} h - \operatorname{gr} g < 0 \right\}.$$

Teorema 2.2.5. *El conjunto de las valuaciones v sobre $k(x)$ tal que $v(a) = 0$ para $a \in k^*$ es exactamente*

$$\{v_f \mid f(x) \in k[x] \text{ es un polinomio mónico e irreducible}\} \cup \{v_\infty\}.$$

Además, todas ellas son inequivalentes a pares y el campo residual es una extensión finita de k. En caso de que la valuación sea v_f, el grado del campo residual sobre $\mathbb{F}_q$ es igual al grado del polinomio f y en el caso de que sea la valuación v_∞, el grado del campo residual es igual a uno. Finalmente, todas las valuaciones son discretas.

Demostración. Ver [21, página 37]. □

Notación 2.2.6. Si K es un campo de funciones, entonces $\mathbb{P}_K \coloneqq \{\mathfrak{p} \mid \mathfrak{p} \text{ es un lugar de } K\}$. Si $\mathfrak{p} \in \mathbb{P}_K$, la valuación respectiva será denotada por $v_\mathfrak{p}$.

Definición 2.2.7. Sea K un campo de funciones sobre k. El grupo abeliano libre generado por todos los elementos de $\mathbb{P}_K$ se llama *grupo de divisores* de K y se denota por D_K.

Los elementos de D_K se llaman *divisores*. Se escribirán multiplicativamente los elementos de D_K. Sea $\mathfrak{a} \in D_K$, digamos

$$\mathfrak{a} = \prod_{i=1}^{r} \mathfrak{p}_i^{\alpha_i}$$

con $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathbb{P}_K$ y $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$.

Equivalentemente, un divisor es de la forma $\mathfrak{a} = \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$ donde $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$ para todo $\mathfrak{p} \in \mathbb{P}_K$ y $v_\mathfrak{p}(\mathfrak{a}) = 0$ para casi todo $\mathfrak{p}$, es decir $v_\mathfrak{p}(\mathfrak{a}) = 0$ para todo $\mathfrak{p} \in \mathbb{P}_K$ salvo un número finito. El elemento identidad de D_K es el divisor $\mathfrak{N} \in D_K$ tal que $v_\mathfrak{p}(\mathfrak{N}) = 0$ para todo $\mathfrak{p} \in \mathbb{P}_K$. Los elementos de $\mathbb{P}_K$, es decir, los lugares, también reciben el nombre de *divisores primos*.

Definición 2.2.8. El número $f_\mathfrak{p} = d_K(\mathfrak{p}) = [k(\mathfrak{p}) : k]$ es llamado *el grado del lugar* $\mathfrak{p}$ o *el grado de inercia de* $\mathfrak{p}$.

Se define el *grado* de $\mathfrak{a} \in D_K$ por:

$$d_K(\mathfrak{a}) = \sum_{\mathfrak{p}\in\mathbb{P}_K} d_K(\mathfrak{p}) v_\mathfrak{p}(\mathfrak{a}).$$

Teorema 2.2.9. *Si $x \in K^*$, hay un número finito de lugares $\mathfrak{p}$ de K tales que $v_\mathfrak{p}(x) \neq 0$.*

Demostración. Ver [21, Theorem 3.2.1]. □

Note que si $x \in k^*$, $v_\mathfrak{p}(x) = 0$ para todo $\mathfrak{p} \in \mathbb{P}_K$. Se define el *divisor principal* de $x \in K^*$ por:

$$(x)_K := \prod_{\mathfrak{p}\in\mathbb{P}_K} \mathfrak{p}^{v_\mathfrak{p}(x)}.$$

Se tiene que si $x \in K\backslash k$, existe al menos un lugar $\mathfrak{p}$ de K tal que $v_\mathfrak{p}(x) > 0$ y otro lugar $\mathfrak{p}'$ tal que $v_{\mathfrak{p}'}(x) < 0$. También se tiene que si $\mathfrak{Z}_x := \prod_{v_\mathfrak{p}(x)>0} \mathfrak{p}^{v_\mathfrak{p}(x)}$ y $\mathfrak{N}_x := \prod_{v_\mathfrak{p}(x)<0} \mathfrak{p}^{-v_\mathfrak{p}(x)}$ entonces $\mathfrak{Z}_x$ se llama el *divisor de ceros* de x y $\mathfrak{N}_x$ se llama *divisor de polos* de x.

Teorema 2.2.10. *Se tiene que si $x \in k^*$, $\mathfrak{Z}_x = \mathfrak{N}_x = \mathfrak{N}$ y si $x \in K\backslash k$, $d_K(\mathfrak{Z}_x) = d_K(\mathfrak{N}_x) = [K : k(x)]$.*

Demostración. Ver [21, Theorem 3.2.7]. □

Corolario 2.2.11. *Para $x \in K^*$, $d_K((x)_K) = 0$.*

Demostración. Ver [21, Corollary 3.2.9]. □

Sea $d_K : D_K \to \mathbb{Z}$ la función grado. Entonces d_K es un homomorfismo de grupos. Puesto que $d_K \neq 0$, $\operatorname{im} d_K = m\mathbb{Z}$ para algún $m \in \mathbb{N}$. En particular $\operatorname{im} d_K \cong \mathbb{Z}$. Sea $D_{K,0} := \ker d_K = \{\mathfrak{a} \in D_K \mid d_K(\mathfrak{a}) = 0\}$ el cual se llama *grupo de divisores de grado* 0 de K. Además $P_K := \{(x)_K \mid x \in K^*\} \subseteq D_{K,0}$.

Se definen los siguientes grupos:

$$I_K := D_K/P_K = \textit{grupo de clases de divisores de } K,$$
$$I_{K,0} := D_{K,0}/P_K = \textit{grupo de clases de divisores de grado } 0 \textit{ de } K.$$

Note que si $C \in I_K$ y $\mathfrak{a}, \mathfrak{b} \in D_K$ son tales que $\mathfrak{a}, \mathfrak{b} \in C$, entonces $\mathfrak{a} = \mathfrak{b}(x)_K$ para algún $x \in K^*$. En particular $d_K(\mathfrak{a}) = d_K(\mathfrak{b})$. Por tanto es posible definir el *grado* de C por: $\widetilde{d}_K(C) := d_K(\mathfrak{a})$ para $\mathfrak{a} \in C$. Se tiene que $\widetilde{d}_K : I_K \to \mathbb{Z}$ también es homomorfismo de grupos.

Se tienen las siguientes sucesiones exactas:

$$1 \longrightarrow D_{K,0} \longrightarrow D_K \xrightarrow{d_K} \mathbb{Z} \longrightarrow 0\ .$$

$$1 \longrightarrow I_{K,0} \longrightarrow I_K \xrightarrow{d_K} \mathbb{Z} \longrightarrow 0$$

$$1 \longrightarrow P_K \longrightarrow D_{K,0} \longrightarrow I_{K,0} \longrightarrow 0$$

$$1 \longrightarrow P_K \longrightarrow D_K \longrightarrow I_K \longrightarrow 0$$

$$1 \longrightarrow k^* \longrightarrow K^* \longrightarrow P_K \longrightarrow 1$$

$$x \longmapsto (x)_K$$

El siguiente resultado es pilar para el estudio de la teoría de campos de funciones algebraicas:

Teorema 2.2.12 (Riemann-Roch)**.** *Sea K/k un campo de funciones y $C \in C_K$ cualquier clase. Sean W la clase canónica [21, Definition 3.4.13] y g el género de K [21, Definition 3.3.4] . Entonces*

$$N(C) = d(C) - g + 1 + N(WC^{-1}).$$

Equivalentemente, si $\mathfrak{A}$ es cualquier divisor y ω cualquier diferencial [21, Section 3.4] distinta de cero, se tiene

$$l(\mathfrak{A}^{-1}) = d(\mathfrak{A}) - g + 1 + l((\omega)_K^{-1}\mathfrak{A}).$$

Es decir

$$\delta(\mathfrak{A}) = l(\mathfrak{A}^{-1}) + d(\mathfrak{A}^{-1}) + g - 1 = l((\omega)_K^{-1}\mathfrak{A}) = N(WC^{-1})$$

para todo $\mathfrak{A} \in C$.

Demostración. Ver [21, Theorem 3.5.4].

□

2.2.1. Grupo de descomposición y grupo de inercia

Definición 2.2.13. Sean K/k y L/l dos campos de funciones. Se dice que L es una extensión de K si $K \subseteq L$ y $l \cap K = k$.

Sean $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ tal que $\mathfrak{P}$ es una extensión de $\mathfrak{p}$. Se define el *grado relativo* por

$$d_{L/K}(\mathfrak{P}|\mathfrak{p}) = [l(\mathfrak{P}) : k(\mathfrak{p})].$$

Puesto que se tiene el siguiente diagrama

$$\begin{array}{ccc} k(\mathfrak{p}) & \text{——} & l(\mathfrak{P}) \\ | & & | \\ k & \text{————} & l \end{array}$$

y dado que $d_K(\mathfrak{p}) = [k(\mathfrak{p}) : k]$, $d_L(\mathfrak{P}) = [l(\mathfrak{P}) : l]$, se sigue

$$d_{L/K}(\mathfrak{P}|\mathfrak{p}) d_K(\mathfrak{p}) = d_L(\mathfrak{P})[l : k].$$

Como $d_K(\mathfrak{p})$ y $d_L(\mathfrak{P})$ son finitos, se tiene que $d_{L/K}(\mathfrak{P}|\mathfrak{p}) < \infty$ si y sólo si $[l : k] < \infty$.

Definición 2.2.14. Sea $\mathfrak{P} \in \mathbb{P}_L$ y sea $\mathfrak{p}$ la restricción de $\mathfrak{P}$ a K. Entonces $v_{\mathfrak{P}}|_{K*}$ es equivalente a $v_{\mathfrak{p}}$. Se define el *índice de ramificación* de $\mathfrak{P}$ sobre $\mathfrak{p}$ como el número natural $e = e_{\mathfrak{P}|\mathfrak{p}}(L : K)$ tal que $v_{\mathfrak{P}}(\alpha) = e v_{\mathfrak{p}}(\alpha)$ para $\alpha \in K$.

Definición 2.2.15. Si L/l es una extensión de K/k y si $\mathfrak{p} \in \mathbb{P}_K$, entonces si $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ son todos los lugares de L encima de $\mathfrak{p}$ se define la *conorma* de $\mathfrak{p}$ a L por

$$\mathrm{con}_{K/L}\mathfrak{p} = \mathfrak{P}_1^{e_{\mathfrak{P}_1|\mathfrak{p}}(L:K)} \cdots \mathfrak{P}_h^{e_{\mathfrak{P}_h|\mathfrak{p}}(L:K)}.$$

Si $\mathfrak{a}$ es cualquier divisor de D_K, $\mathfrak{a} = \mathfrak{p}_1^{\alpha_1} \cdots \mathfrak{p}_r^{\alpha_r}$ se define la *conorma* de $\mathfrak{a}$ por:

$$\mathrm{con}_{K/L}(\mathfrak{a}) = \prod_{i=1}^{r} \mathrm{con}_{K/L}(\mathfrak{p}_i)^{\alpha_i}$$

Teorema 2.2.16. *Para cualquier extensión L/l de K/k, finita o infinita, sea $\mathfrak{p}$ un lugar de K y sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ los lugares de L sobre $\mathfrak{p}$. Entonces*

$$[L : K] = \sum_{i=1}^{h} e_{\mathfrak{P}_i|\mathfrak{p}}(L : K) d_{\mathfrak{P}_i|\mathfrak{p}}(L : K).$$

Demostración. Ver [21, Theorem 5.1.14]. □

Cuando la extensión es de Galois se tiene que $d_{\mathfrak{P}_i|\mathfrak{p}}(L : K) = d_{\mathfrak{P}_j|\mathfrak{p}}(L : K)$ y $e_{\mathfrak{P}_i|\mathfrak{p}}(L : K) =$

$e_{\mathfrak{P}_j|\mathfrak{p}}(L:K)$ para todo $1 \leqslant i, j \leqslant h$. En este caso si $e = e_{\mathfrak{P}/\mathfrak{p}}(L:K)$ y $d = d_{\mathfrak{P}/\mathfrak{p}}(L:K)$, se tiene $[L:K] = efh$.

Definición 2.2.17. Sea L/K una extensión de Galois con grupo de Galois $G = \mathrm{Gal}(L/K)$. Sean $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ una extensión de $\mathfrak{p}$. Se define

(i) $D_{\mathfrak{P}|\mathfrak{p}}(L:K) \coloneqq \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ el cual es llamado el *grupo de descomposición de* $\mathfrak{P}/\mathfrak{p}$

(ii) $I_{\mathfrak{P}|\mathfrak{p}}(L:K) \coloneqq \{\sigma \in G \mid \sigma x \equiv x \mod \mathfrak{P}\ \forall\ x \in \mathcal{O}_{\mathfrak{P}}\}$ el cual es llamado el *grupo de inercia* de $\mathfrak{P}/\mathfrak{p}$.

Observación 2.2.18. De manera similar como en el caso de campos numéricos se tiene:

- $I_{\mathfrak{P}|\mathfrak{p}}(L:K) \subseteq D_{\mathfrak{P}|\mathfrak{p}}(L:K)$,
- $|I_{\mathfrak{P}|\mathfrak{p}}(L:K)| = e_{\mathfrak{P}|\mathfrak{p}}(L:K)$ y $|D_{\mathfrak{P}|\mathfrak{p}}(L:K)| = e_{\mathfrak{P}|\mathfrak{p}}(L:K)d_{\mathfrak{P}|\mathfrak{p}}(L:K)$,
- $D_{\mathfrak{P}|\mathfrak{p}}(L:K)/I_{\mathfrak{P}|\mathfrak{p}}(L:K) \cong \mathrm{Gal}(l(\mathfrak{P})/k(\mathfrak{p}))$,
- $D_{\mathfrak{P}|\mathfrak{p}}(L:K) \cong \mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$, donde $L_{\mathfrak{P}}$ y $K_{\mathfrak{p}}$ son las completaciones de L y K en $\mathfrak{P}$ y $\mathfrak{p}$ respectivamente.

2.2.2. Diferente y discriminante

Consideremos L un campo con valor absoluto no arquimediano, $v_{\mathfrak{P}}$ la valuación asociada al valor absoluto y $L_{\mathfrak{P}}$ la completación de L respecto al valor absoluto. Sean $\mathcal{O}_{\widehat{\mathfrak{P}}} = \{x \in L_{\mathfrak{P}} \mid v_{\mathfrak{P}}(x) \geqslant 0\}$ la completación de $\mathcal{O}_{\mathfrak{P}}$ y $\widehat{\mathfrak{P}} = \{x \in L_{\mathfrak{P}} \mid v_{\mathfrak{P}}(x) > 0\}$ la completación de $\mathfrak{p}$ en $L_{\mathfrak{P}}$. Si $\mathrm{Tr} = \mathrm{Tr}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ denota la traza de $L_{\mathfrak{P}}$ a $K_{\mathfrak{p}}$ se tiene el siguiente resultado:

Teorema 2.2.19. *Existe $m \geqslant 0$ tal que si $x \in L_{\mathfrak{P}}$ satisface $v_{\mathfrak{P}}(x) \geqslant -m$, entonces $v_{\mathfrak{p}}(\mathrm{Tr}\, x) \geqslant 0$. También, existe x_0 con $v_{\mathfrak{P}}(x_0) < -m$ y $v_{\mathfrak{p}}(\mathrm{Tr}\, x_0) < 0$.*

Demostración. Ver [21, Theorem 5.6.1]. □

Definición 2.2.20. El máximo entero no negativo que satisface las condiciones del Teorema 2.2.19 se denota por $m(\mathfrak{P})$ y es llamado el *exponente diferencial* de $\mathfrak{P}$ con respecto a K.

Teorema 2.2.21. *Se tiene $m(\mathfrak{P}) \geqslant e - 1 = e_{\mathfrak{P}|\mathfrak{p}}(L:K) - 1$. Además, puesto que k es perfecto, $m(\mathfrak{P}) > e - 1$ si y sólo si la característica de k divide a e.*

Demostración. Ver [21, Thoerem 5.6.3]. □

Corolario 2.2.22. *Se tiene que $m(\mathfrak{P}) = 0$ salvo un número finito de lugares $\mathfrak{P}$.*

Demostración. Ver [21, Corollary 5.6.4]. □

Definición 2.2.23. Sean $e = e_{\mathfrak{P}|\mathfrak{p}}(L:K)$ y $k(\mathfrak{p})$ el campo residual $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$. Sea $p = \mathrm{car}\, k(\mathfrak{p})$. Si $p|e$, $\mathfrak{p}$ es llamado *salvajemente ramificado*, y si $p \nmid e$, $\mathfrak{p}$ es llamado *moderadamente ramificado*.

Definición 2.2.24. El divisor $\mathfrak{D}_{L/K} \coloneqq \prod_{\mathfrak{P}\in\mathbb{P}_L} \mathfrak{P}^{m(\mathfrak{P})}$ es llamado el *diferente de la extensión* y se tiene $\mathfrak{P}|\mathfrak{D}_{L/K}$ si y sólo si $\mathfrak{P}$ es ramificado.

El *discriminante* $\mathfrak{d}_{L/K}$ de la extensión L/K se define como la norma del diferente, esto es: $\mathfrak{d}_{L/K} = N_{L/K}(\mathfrak{D}_{L/K})$.

De manera análoga al caso numérico, se tienen los grupos de ramificación y su relación con el diferente.

Definición 2.2.25. Sea $\mathfrak{p} \in \mathbb{P}_K$ y $\mathfrak{P} \in \mathbb{P}_L$ sobre $\mathfrak{p}$. Sean $G_{-2} = G$, $G_{-1} \coloneqq D_{\mathfrak{P}|\mathfrak{p}}(L : K)$, $G_0 \coloneqq I_{\mathfrak{P}|\mathfrak{p}}(L : K)$ y para $i \geqslant 1$ se define el *i-ésimo grupo de ramificación* G_i por:

$$G_i \coloneqq \{\sigma \in G \mid v_{\mathfrak{P}}(\sigma(x) - x) \geqslant i + 1 \text{ para todo } x \in \mathcal{O}_L\}.$$

Entonces $G_i \supseteq G_{i+1}$, cada G_i es un subgrupo normal de G. Además existe i_0 tal que $G_{i_0} = \{\mathrm{Id}\}$.

Definición 2.2.26. Se define la función $i_G : G \longrightarrow \mathbb{Z} \cup \{\infty\}$ por $i_G(\sigma) = v_{\mathfrak{P}}(\sigma x - x)$.

Se tiene el siguiente proposición:

Proposición 2.2.27. *(1) $i_G(\sigma) = \infty$ si y sólo si $\sigma = \mathrm{Id}$,*

(2) $i_G(\sigma) \geqslant i + 1$ si y sólo si $\sigma \in G_i$,

(3) $i_G(g\sigma g^{-1}) = i_G(\sigma)$ para todo $\sigma, g \in G$.

Proposición 2.2.28. *si $m(\mathfrak{P})$ es el exponente diferencial de $\mathfrak{P}$, entonces*

$$m(\mathfrak{P}) = \sum_{\sigma\neq\mathrm{Id}} i_G(\sigma) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

Demostración. Ver [21, Proposition 5.9.8 y Theorem 5.9.9]. □

Teorema 2.2.29. *Si K/k es un campo de funciones congruente, l es una extensión finita de k y $L = Kl$, entonces el campo de constantes de L es l. Además $[L : K] = [l : k]$.*

Demostración. Ver [21, Theorem 6.1.2 y Theorem 6.1.3]. □

Teorema 2.2.30. *Sean k un campo finito y K/k un campo de funciones congruente, sean l/k una extensión finita y $L = Kl$. Entonces L/K es una extensión no ramificada.*

Demostración. Ver [19, Teorema 9.1.3]. □

Teorema 2.2.31. *Sea $\mathfrak{p}$ un lugar de L y sea $\mathcal{P} = \mathfrak{p}|_K$. Entonces los campos residuales satisfacen $l(\mathfrak{p}) = k(\mathcal{P})l$.*

Demostración. Ver [21, Theorem 6.1.4]. □

Se presenta la demostración del siguiente teorema ya que nos brinda información de la descomposición y del grado de inercia de los divisores primos.

Teorema 2.2.32. *Si $\mathfrak{p}$ es un lugar de K, $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ son los lugares de $L = Kl$ sobre $\mathfrak{p}$ y $[l : k] = f$, entonces*

(1) $d_{\mathfrak{P}_i|\mathfrak{p}}(L : K) = \frac{f}{\text{mcd}(d_K(\mathfrak{p}), f)}$,

(2) $h = \text{mcd}(d_K(\mathfrak{p}), f)$,

(3) $d_L(\mathfrak{P}_i) = \frac{d_K(\mathfrak{p})}{\text{mcd}(d_K(\mathfrak{p}), f)}$.

Demostración. Sea $\mathfrak{p} \in \mathbb{P}_L$ y sean $\mathfrak{P}_1, \ldots, \mathfrak{P}_h$ los lugares de L sobre $\mathfrak{p}$. Ahora bien, l/k siempre resulta ser un extensión de Galois, de hecho cíclica con $\text{Gal}(l/k) \cong C_f \cong \mathbb{Z}/f\mathbb{Z}$. Por tanto L/K es una extensión de Galois con $d_{\mathfrak{P}_i|\mathfrak{p}}(L : K) = d$, esto para $1 \leqslant i \leqslant h$.

Se tiene lo siguiente:

$$[L : K] = [l : k] = f = dh.$$

Ahora bien, si $r = d_K(\mathfrak{p}) = [k(\mathfrak{p}) : k]$, entonces $k(\mathfrak{p}) \cong \mathbb{F}_{q^r}$ y si $s = d_L(\mathfrak{P}_i) = [l(\mathfrak{P}_i) : l]$, entonces $l(\mathfrak{P}_i) \cong \mathbb{F}_{q^{fs}}$. Se tiene que $k(\mathfrak{p})l \cong \mathbb{F}_{q^r}\mathbb{F}_{q^f} = \mathbb{F}_{q^{\text{mcm}[r,f]}} = \mathbb{F}_{q^{fs}} \cong l(\mathfrak{P}_i)$. Por lo tanto $fs = \text{mcm}[r, f] = \frac{rf}{\text{mcd}(r,f)}$ y $s = \frac{r}{\text{mcd}(r,f)}$. Esto es,

$$d_L(\mathfrak{P}_i) = s = \frac{d_K(\mathfrak{p})}{\text{mcd}(d_K(\mathfrak{p}), f)}$$

y por tanto se tiene (3). Por otra parte $d_{\mathfrak{P}_i|\mathfrak{p}}(L : K)d_K(\mathfrak{p}) = d_L(\mathfrak{P}_i)[l : k]$, es decir, $dr = sf$ lo cual equivale a $d = \frac{sf}{r} = \frac{r}{\text{mcd}(r,f)}\frac{f}{r} = \frac{f}{\text{mcd}(r,f)}$, esto es (1). Por último $h = \frac{f}{d} = \text{mcd}(r, f)$, que esto es (2).

□

Capítulo 3

Campos de funciones ciclotómicos

3.1. Campos ciclotómicos

Un campo ciclotómico numérico es de la forma $\mathbb{Q}(\zeta_n)$, donde $\zeta_n = \exp(\frac{2\pi i}{n})$ y $\zeta_n^n = 1$. El Teorema de Kronecker-Weber dice que toda extensión abeliana finita de $\mathbb{Q}$ está contenida en una extensión ciclotómica. Equivalentemente, se tiene que si $\mathbb{Q}^{ab}$ es la máxima extensión abeliana de $\mathbb{Q}$, entonces $\mathbb{Q}^{ab} = \bigcup_{n=1}^{\infty} \mathbb{Q}(\zeta_n)$. Note que ζ_n es un elemento de torsión de $\mathbb{Z}$ actuando en $\overline{\mathbb{Q}}^* = \overline{\mathbb{Q}}\backslash\{0\}$, por exponenciación donde $\overline{\mathbb{Q}}$ es la cerradura algebraica de $\mathbb{Q}$. Esto es, si $\alpha \in \overline{\mathbb{Q}}^*$ y $n \in \mathbb{Z}$, la acción está dada por α^n. Entonces

$$\mathbb{Q}^{ab} = \mathbb{Q}(\text{tor}\overline{\mathbb{Q}}^*), \text{ donde } \text{tor}\overline{\mathbb{Q}}^* = \{\alpha \in \overline{\mathbb{Q}}^* \mid \text{existe } n \in \mathbb{N} \text{ con } \alpha^n = 1\}.$$

Se pretende hacer un análogo a todo lo visto en campos numéricos ciclotómicos pero ahora en campos de funciones congruentes. Sean $\mathbb{F}_q$ el campo finito de q elementos y k un campo de funciones racionales sobre $\mathbb{F}_q$: $k = \mathbb{F}_q(T)$. Sea $R_T := \mathbb{F}_q[T]$ el anillo de polinomios sobre $\mathbb{F}_q$, también se tiene a $R_T^+ := \{P \in R_T \mid P \text{ es mónico e irreducible}\}$. Se tiene que k es el campo de cocientes de R_T. Sean $\overline{k}$ una cerradura algebraica de k y A el anillo de endomorfismos de $\overline{k}$ sobre $\mathbb{F}_q$:

$$\begin{aligned} A = \text{End}_{\mathbb{F}_q}(\overline{k}) = \{\varphi : \overline{k} \to \overline{k} \mid \varphi(a+b) = \varphi(a) + \varphi(b), \\ \varphi(\alpha a) = \alpha\varphi(a) \ \forall\ \alpha \in \mathbb{F}_q, \ \forall\ a, b \in \overline{k}\}. \end{aligned}$$

Entonces A es un anillo y un $\mathbb{F}_q$-módulo, es decir, en este caso, un $\mathbb{F}_q$-espacio vectorial, donde la multiplicación de A es la composición. El anillo A tiene dos elementos que se pueden caracterizar de manera sobresaliente:

1. Sea φ el automorfismo de Frobenius de $\overline{k}/\mathbb{F}_q$, es decir:

$$\begin{aligned}\varphi : \overline{k} &\longrightarrow \overline{k}\\ u &\mapsto u^q.\end{aligned}$$

2. Sea μ_T la multiplicación por T:

$$\begin{aligned}\mu_T : \overline{k} &\longrightarrow \overline{k}\\ u &\mapsto Tu.\end{aligned}$$

Sea $\xi : R_T \to A$ la sustitución de T por $\varphi + \mu_T$, es decir, si $f(T) \in R_T$ es un polinomio, $\xi(f(T)) = f(\varphi + \mu_T) \in A$ es el endomorfismo, donde, si

$$f(T) = a_q T^d + \cdots + a_1 T + a_0,$$

entonces

$$f(\varphi + \mu_T)(u) = a_d(\varphi + \mu_T)^d(u) + \cdots + a_1(\varphi + \mu_T)(u) + a_0.$$

Aquí $(\varphi + \mu_T)^d = (\varphi + \mu_T) \circ \cdots \circ (\varphi + \mu_T)$ corresponde a la composición d-veces para $u \in \overline{k}$. Es decir se tiene que si $\xi : R_T \to A$ está dado por $\xi(T) = \varphi + \mu_T$, entonces ξ es un homomorfismo de anillos y, bajo ξ, $\overline{k}$ es un R_T-módulo, donde:

$$(\varphi + \mu_T)^0 = \mathrm{Id}_{\overline{k}}.$$

Note que:

$$\begin{aligned}(\varphi \circ \mu_T)(u) &= \varphi(Tu) = T^q u^q\\ (\mu_T^q \circ \varphi)(u) &= \mu_T^q(u^q) = T^q u^q\end{aligned}$$

lo cual implica que $\varphi \circ \mu_T = \mu_T^q \circ \varphi$ y en particular $\varphi \circ \mu_T \neq \mu_T \circ \varphi$.

Si $u \in \overline{k}$ y $M \in R_T$ se denota la acción de la siguiente forma: $u^M = M(\varphi + \mu_T)(u)$. Esto es, $u^M = M \circ u = \xi(M)(u) = M(\varphi + \mu_T)(u)$. Se tiene que para $u \in \overline{k}$, $M, N \in R_T$,

- $u^{M+N} = u^M + u^N$
- $(u^M)^N = u^{MN} = u^{NM} = (u^N)^M$.

Teorema 3.1.1. *Sea $M = a_d T^d + \cdots + a_1 T + a_0$ con $a_d \neq 0$. Entonces:*

$$u^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i}$$

donde $\begin{bmatrix} M \\ i \end{bmatrix}$ *es un polinomio de* R_T *de grado* $(d-i)^{q^i}$, $\begin{bmatrix} M \\ 0 \end{bmatrix} = M$ *y* $\begin{bmatrix} M \\ d \end{bmatrix} = a_d$.

Demostración. Ver [19, Teorema 9.2.3]. □

La acción, aunque técnicamente complicada, es la correspondiente a $(\overline{\mathbb{Q}})^*$. Más precisamente

$$\begin{array}{ccc} & & \overline{\mathbb{Q}} \\ & & | \\ \mathbb{Z} & \text{——} & \mathbb{Q} \end{array}$$

$\mathbb{Z}$ actúa en $(\overline{\mathbb{Q}})^*$ así: $n \in \mathbb{Z}$, $u \in (\overline{\mathbb{Q}})^*$ tal que $n \circ u = u^n$ y los campos ciclotómicos corresponden a: adjuntar $\mathbb{Q}$

$$\{u \in (\overline{\mathbb{Q}})^* \mid u^n = 1\} = \{\zeta_n^a\}_{a=0}^{n-1}.$$

con $n \in \mathbb{N}$.

En nuestro caso

$$\begin{array}{ccc} & & \overline{k} \\ & & | \\ R_T & \text{——} & k \end{array}$$

R_T actúa en $\overline{k}$ por exponenciación, esto es, para $M \in R_T$ y $u \in \overline{k}$ se tiene $M \circ u = u^M = C_M(u) = M * u$ a esta acción se le conoce como la *acción de Carlitz*. Los campos ciclotómicos corresponden a : adjuntar a k

$$\{u \in \overline{k} \mid u^M = 0\}.$$

con $M \in R_T$.

Definición 3.1.2. Sea Λ_M los elementos de $\overline{k}$ que corresponden a la M-torsión de la acción de R_T, es decir,

$$\Lambda_M = \{u \in \overline{k} \mid u^M = 0\}.$$

Λ_M recibe el nombre de *M-torsión del módulo de Carlitz-Hayes.*

Observación 3.1.3. Se tiene que Λ_M es un R_T-submódulo de $\overline{k}$.

Observación 3.1.4. Si $\alpha \in \mathbb{F}_q^*$, $\Lambda_{\alpha M} = \Lambda_M$ pues $u^{\alpha M} = (u^\alpha)^M = (\alpha u)^M = \alpha u^M = 0 \iff u^M = 0$, por lo que siempre se pueden considerar polinomios mónicos M.

Proposición 3.1.5. *Se tiene que u^M es un polinomio separable en u de grado q^d, donde $M \in R_T\backslash\{0\}$ es de grado d, de donde Λ_M es un conjunto finito de q^d elementos. Más aún es un $\mathbb{F}_q$-espacio vectorial de dimensión d.*

Demostración. Sea $M = a_d T^d + \cdots + a_1 T + a_0$. Entonces

$$u^M = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i},$$

luego al tomar la derivada con respecto a u se obtiene

$$(u^M)' = \frac{d}{du}(u^M) = \begin{bmatrix} M \\ 0 \end{bmatrix} = M \neq 0.$$

De esta forma $(u^M)'$ no tiene raíces múltiples y u^M es separable en u. Observe también que, $\mathrm{gr}_u u^M = q^d$ por lo que $|\Lambda_M| = q^d$. Claramente se ve que Λ_M es un $\mathbb{F}_q$-espacio vectorial y por lo tanto de dimensión d. □

Proposición 3.1.6. *Si $M = \prod_{i=1}^{r} P_i^{\alpha_i}$ es la descomposición de M como producto de irreducibles, entonces*

$$\Lambda_M \cong \prod_{i=1}^{r} \Lambda_{P_i^{\alpha_i}}$$

como R_T-módulos.

Demostración. Sólo es un resultado más de módulos sobre dominios de ideales principales. □

Se probará que Λ_M es R_T-cíclico y con este fin se tiene la siguiente proposición.

Proposición 3.1.7. *Si $M = P^n$, entonces $\Lambda_{P^n} \cong R_T/P^n$ como R_T-módulos y por lo tanto Λ_{P^n} es R_T-cíclico.*

Demostración. Se hará por inducción sobre n. Para $n = 1$, sea $\xi \in \Lambda_P\backslash\{0\}$ y sea $\theta : R_T \to \Lambda_P$ dada por $N \mapsto \xi^N$. Entonces $P \in \ker\theta$ y el ideal $\langle P\rangle$ es maximal pues R_T es un dominio de ideales principales (DIP). Dado que $\theta(1) = \xi \neq 0$, se tiene θ es no trivial, luego $\ker\theta = \langle P\rangle$ y así $R_T/\langle P\rangle \cong \theta(R_T)$ es un submódulo de Λ_P. Puesto que $|R_T/\langle P\rangle| = |\Lambda_P| = q^d$, donde $d = \mathrm{gr}\, P$, se tiene que $R_T/\langle P\rangle \cong \Lambda_P$ y cualquier $\xi \in \Lambda_P\backslash\{0\}$ es generador.

Supóngase que el resultado se tiene para Λ_{P^n} y sea λ un generador de Λ_{P^n}. Se probará que $\Lambda_{P^{n+1}}$ es R_T-cíclico. Sea $\mu : \Lambda_{P^{n+1}} \to \Lambda_{P^n}$ dada por $\xi \mapsto \xi^P$. Entonces $\ker\mu = \Lambda_P$ y además $|\Lambda_{P^{n+1}}/\Lambda_P| = |\Lambda_{P^n}| = q^{nd}$ por lo tanto $\Lambda_{P^{n+1}}/\Lambda_P \cong \Lambda_{P^n}$, es decir:

$$0 \to \Lambda_P \to \Lambda_{P^{n+1}} \to \Lambda_{P^n} \to 0$$

es una sucesión R_T-exacta.

Sea $\xi \in \Lambda_{P^{n+1}}$ tal que $\mu(\xi) = \xi^P = \lambda$, el cual es un generador de Λ_{P^n} como R_T-módulo. Sea A el R_T-módulo generado por ξ es decir $A = R_T \circ \xi = \xi^{R_T}$. Entonces $A \subseteq \Lambda_{P^{n+1}}$ y $A \cong R_T/\ker(\xi)$, donde $\ker(\xi) := \{N \in R_T \mid \xi^N = 0\}$.

Ahora bien $P^{n-1} \notin \ker(\xi)$ pues $\lambda^{P^{n-1}} = \mu(\xi^{P^{n-1}}) \neq 0$. Sea $\alpha \in \Lambda_{P^{n+1}}$ cualquiera. Entonces $\mu(\alpha) = \alpha^P \in \Lambda_{P^n} = R_T \circ \lambda$, lo cual implica que existe $B \in R_T$ tal que $\alpha^P = \lambda^B = \mu(\xi^B) = \xi^{PB}$. Entonces $(\alpha - \xi^B)^P = 0$, es decir, $\alpha - \xi^B \in \Lambda_P = \ker \mu$.

Se tiene que ξ^P genera Λ_{P^n} por lo que $(\xi^P)^{P^{n-1}} = \xi^{P^n} \neq 0$ y $\xi^{Pn} \in \Lambda_P$. Por el caso $n = 1$, ξ^{P^n} genera Λ_P. En particular existe $C \in R_T$ tal que $\xi^{P^n C} = \alpha - \xi^B$ o $\xi^{B+P^n C} = \alpha$, es decir, ξ genera $\Lambda_{P^{n+1}}$ como R_T-módulo.

Finalmente, notemos $\langle P^{n+1}\rangle \subseteq \ker(\xi) \subsetneq \langle P^n\rangle$ y sea $\ker(\xi) = \langle Q\rangle$. Entonces $P^n | Q$ y $Q \neq P^n$ por lo que $Q = P^m Q_1 | P^{n+1}$, es decir $Q_1 | P$ y Q_1 no es unidad. Se sigue que $Q_1 = P$ y $Q = P^{n+1}$, $\ker(\xi) = \langle P^{n+1}\rangle$ y $\Lambda_{P^{n+1}} = R_T \circ \xi \cong R_T/\ker(\xi) = R_T/\langle P^{n+1}\rangle$. □

Teorema 3.1.8. *Para todo $M \in R_T$, $M \neq 0$, Λ_M es un R_T-módulo cíclico y $\Lambda_M \cong R_T/\langle M\rangle$ como R_T-módulos*

Demostración. Considere la descomposición $M = \prod_i^r P_i^{\alpha_i}$. Se tiene por la Proposición 3.1.6 que

$$\Lambda_M \cong \prod_{i=1}^{r} \Lambda_{P_i^{\alpha_i}}$$

Luego, de la Proposición 3.1.7 se tiene que $\Lambda_{P_i^{\alpha_i}}$ es un R_T-módulo cíclico y es la P_i-componente primaria de Λ_M. Por lo tanto Λ_M es un R_T-módulo cíclico (pues los P_i son primos relativos a pares). De hecho si λ_i es generador de $\Lambda_{P_i^{\alpha_i}}$ entonces $\lambda = \lambda_1 + \cdots + \lambda_r$ es generador de Λ_M. Ahora si λ es un generador de Λ_M sea

$$\phi : R_T \longrightarrow \Lambda_M$$

dada por $\phi(A) = \lambda^A$. Entonces ϕ es un epimorfismo y $\Lambda_M \cong R_T/\ker\phi$. Tenemos $\ker\phi = \{A \in R_T \mid \lambda^A = 0\}$. Claramente $M \in \ker\phi$ pues $\lambda \in \Lambda_M$ y por lo tanto $\lambda^M = 0$ de esta manera $\langle M\rangle \subseteq \ker\phi$.

Por otro lado si $d = \operatorname{gr} M$,

$$\left|\frac{R_T}{\langle M\rangle}\right| = q^d = |\Lambda_M|.$$

Por lo tanto $\ker\phi = \langle M\rangle$ y de esta manera se concluye que $\Lambda_M \cong R_T/\langle M\rangle$. □

Proposición 3.1.9. *Sean λ un generador de Λ_M y $A \in R_T$. Entonces λ^A es generador de Λ_M si y sólo si A y M son primos relativos.*

Demostración. Se tiene que λ^A genera a Λ_M si y sólo si $\lambda \in R_T \circ \lambda^A = \{\lambda^{AB} \mid B \in R_T\}$, es decir, si y sólo si existe $C \in R_T$ tal que $\lambda = \lambda^{AC}$ lo cual equivale a que $\lambda^{1-AC} = 0$. Dado que el anulador

de λ es $\{\alpha \in R_T \mid \lambda^\alpha = 0\}$ y satisface, $\mathrm{an}(\lambda) = \langle M \rangle$, se tiene $\lambda^{1-AC} = 0$ si y sólo si $M|1 - AC$ si y sólo si $\mathrm{mcd}(A, M) = 1$. □

Definición 3.1.10. Sea $M \in R_T\backslash\{0\}$ y sea Λ_M la M-torsión del módulo de Carlitz-Hayes. Se define el *campo de funciones ciclotómico* determinado por M al campo $k(\Lambda_M)$.

Teorema 3.1.11. *Se tiene que $k(\Lambda_M)/k$ es una extensión de Galois.*

Demostración. Si λ_M es un generador de Λ_M como R_T-módulo entonces $\lambda_M^{R_T} = \Lambda_M = \{\lambda_M^A \mid A \in R_T\}$ por lo que $k(\Lambda_M) = k(\lambda_M)$ pues cada elemento $\xi \in \Lambda_M$ es de la forma

$$\xi = \lambda_M^A = A(\mu_T + \varphi)(\lambda_M) \in k(\lambda_M^q, \{T^s \lambda_M\}) = k(\lambda_M).$$

Dado que Λ_M es el conjunto de raíces del polinomio $u^M \in R_T[u] \subseteq k[u]$ y u^M es separable (Proposición 3.1.5). $k(\Lambda_M)/k$ es normal y separable, es decir, de Galois. □

Definición 3.1.12. Para $M \in R_T\backslash\{0\}$, G_M denota el grupo de Galois de $k(\Lambda_M)/k$, es decir $G_M := \mathrm{Gal}(k(\Lambda_M)/k)$.

Se tiene, en comparación con el caso numérico, en el que $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$, que en el caso de campos de funciones se podría esperar que $G_M \cong (R_T/\langle M \rangle)^*$ el grupo de unidades del anillo $R_T/\langle M \rangle$. Note que

$$(R_T/\langle M \rangle)^* = \{A \bmod M \mid \mathrm{mcd}(A, M) = 1\}$$

y el número de generadores de Λ_M es precisamente $|(R_T/\langle M \rangle)^*|$. Lo cual motiva la siguiente definición.

Definición 3.1.13. Se define la función *"Fi" de Euler* por:

$$\Phi(M) := |(R_T/\langle M \rangle)^*|$$

para $M \in R_T\backslash\{0\}$.

Proposición 3.1.14. *La función Φ de Euler satisface:*

(1) $\Phi(MN) = \Phi(M)\Phi(N)$ para M, N primos relativos.

(2) $\Phi(P^n) = |R_T/\langle P \rangle|\Phi(P^{n-1}) = q^{nd} - q^{(n-1)d}$ donde P es irreducible, $n \geqslant 1$ y $gr\ P = d$.

(3) Para $1 \leqslant m < n$ y P irreducible, la sucesión

$$0 \longrightarrow D_{P^n,P^m} \longrightarrow (R_T/\langle P^n \rangle)^* \xrightarrow{\varphi} (R_T/\langle P^m \rangle)^* \longrightarrow 1$$

es exacta, donde $D_{P^n,P^m} = \{\overline{A} \in (R_T/\langle P^n \rangle)^* \mid A \equiv 1 \bmod P^m\}$.

(4) $\Phi(M)$ es el número de generadores de Λ_M.

Demostración. Se tiene por el Teorema Chino del Residuo que si M y N son primos relativos, entonces $R_T/\langle MN\rangle \cong R_T/\langle M\rangle \times R_T/\langle N\rangle$ y por lo tanto $(R_T/\langle MN\rangle)^* \cong (R_T/\langle M\rangle)^* \times (R_T/\langle N\rangle)^*$. En particular se tiene (1), es decir, $\Phi(MN) = \Phi(M)\Phi(N)$.

Por otro lado, si P es irreducible se tiene que $R_T/\langle P\rangle$ es el campo de q^d elementos siendo $d = \operatorname{gr} P$. Así $|(R_T/\langle P\rangle)^*| = q^d - 1 = \Phi(P)$. Para $n \geqslant 2$ se tiene que si $\theta : (R_T\langle P^n\rangle)^* \longrightarrow (R_T/\langle P^{n-1}\rangle)^*$ es el mapeo natural, es decir, $\theta(A \bmod Pn) = A \bmod P^{n-1}$ entonces $\ker\theta = \{1 + P^{n-1}B \mid B \in R_T\}$. Se tiene entonces

$$0 \longrightarrow R_T/\langle P\rangle \xrightarrow{\mu} (R_T/\langle P^n\rangle)^* \xrightarrow{\theta} (R_T/\langle P^{n-1}\rangle)^* \longrightarrow 1$$

es exacta, donde $\mu(B \bmod P) = 1 + P^{n-1}B \bmod P^n$. Se obtiene que $\Phi(P^n) = \Phi(P^{n-1})|R_T/\langle P\rangle| = \Phi(P^{n-1})q^d$. Más aún se tiene que $R_T/\langle P\rangle \cong D_{P^n,P^{n-1}} = \{\overline{A} \in (R_T/\langle P^n\rangle)^* \mid A \equiv 1 \bmod P^{n-1}\} = \ker\theta$

Si por inducción se supone que $\Phi(P^n) = q^{nd} - q^{(n-1)d}$, entonces $\Phi(P^{n+1}) = \Phi(P^n)q^d = (q^{nd} - q^{(n-1)d})q^d = q^{(n+1)d} - q^{nd}$. En general se tiene que, para $1 \leqslant m < n$, la sucesión

$$0 \longrightarrow D_{P^n,P^m} \longrightarrow (R_T/\langle P^n\rangle)^* \xrightarrow{\varphi} (R_T/\langle P^m\rangle)^* \longrightarrow 1$$

es exacta, donde $\varphi(A \bmod P^n) = A \bmod P^m$ y

$$D_{P^n,P^m} = \{A \bmod P^n \in (R_T/\langle P^n\rangle)^* \mid A \equiv 1 \bmod P^m\}.$$

Finalmente, puesto que el número de generadores de Λ_M es precisamente $|(R_T/\langle M\rangle)^*| = \Phi(M)$ tenemos (4).

□

Proposición 3.1.15. *La acción de Galois de G_M sobre $k(\Lambda_M)$ conmuta con la acción de R_T, es decir, si $u \in k(\Lambda_M)$ y $\sigma \in G_M$, $N \in R_T$, entonces $\sigma(u^N) = (\sigma(u))^N$.*

Demostración. Si $k \subseteq L \subseteq k(\Lambda_M)$, con L cualquier subcampo y $u \in L$, entonces $u^T = (\varphi + \mu_T)(u) = u^q + Tu \in L$, por lo tanto L es un R_T-módulo. En particular si $u \in k(\Lambda_M)$, $u^N \in k(\Lambda_M)$. Se tiene:

$$\sigma(u^N) = \sigma\Big(\sum_{i=0}^{\operatorname{gr} N} \begin{bmatrix} N \\ i \end{bmatrix} u^{q^i}\Big) = \sum_{i=0}^{\operatorname{gr} N} \sigma\Big(\begin{bmatrix} N \\ i \end{bmatrix}\Big)\sigma(u^{q^i}) = \sum_{i=0}^{\operatorname{gr} N} \begin{bmatrix} N \\ i \end{bmatrix} (\sigma u)^{q^i} = (\sigma u)^N.$$

□

Proposición 3.1.16. *Sea $M \in R_T\backslash\{0\}$. Entonces $G_M \subseteq (R_T/\langle M\rangle)^*$.*

Demostración. Se tiene que si $\lambda = \lambda_M$ es un generador de Λ_M, entonces $k(\Lambda_M) = k(\lambda_M)$. Por lo tanto $\sigma \in G_M$ está determinado por su acción en λ y dado que $\sigma\lambda$ es un conjugado de λ, $\sigma\lambda \in \Lambda_M$.

Si $\sigma\lambda = \beta$, entonces $\lambda = \sigma^{-1}\beta$ y necesariamente $\sigma\lambda$ es generador de Λ_M. Sea $A \in R_T$ tal que $\sigma\lambda = \lambda^A$, entonces $\text{mcd}(A, M) = 1$ y la elección de A no depende de λ. Se denota a σ por σ_A, es decir $\sigma_A\lambda = \lambda^A$ con $\text{mcd}(A, M) = 1$.

Sea $\varphi : G_M \longrightarrow (R_T/\langle M\rangle)^*$, dado por $\sigma_A \mapsto A$ mód M. Es claro que φ es un monomorfismo de grupos. □

Corolario 3.1.17. *Para $M \in R_T\backslash\{0\}$, $[k(\Lambda_M) : k] \leqslant \Phi(M)$.*

Definición 3.1.18. Sea $S \in R_T$ un polinomio mónico. Se define al *polinomio ciclotómico* con respecto a S por:

$$\Psi_S(u) := \prod_{\text{mcd}(B,S)=1} (u - \lambda_s^B)$$

con gr $B <$ gr S y λ_S genera a Λ_S. Entonces $\Psi_S(u) \in k(\Lambda_S)[u]$ y gr $\Psi_S(u) = \Phi(S)$.

Proposición 3.1.19. *Se tiene que $\Psi_S(u) \in k[u]$.*

Demostración. Sea $\sigma_A \in G_S$. Entonces $\sigma_A(\lambda_S) = \lambda_S^A$ y si $\text{mcd}(B, S) = 1$, entonces $\sigma_A(\lambda_s^B) = \lambda_S^{BA}$ con $\text{mcd}(AB, S) = 1$. Por lo tanto

$$\sigma_A(\Psi_S(u)) = \prod_{\text{mcd}(B,S)=1} (u - \lambda_S^{AB}),$$

con gr $B <$ gr S. Tomando AB mód S y notando que la multiplicación por A es un automorfismo de $(R_T/\langle S\rangle)^*$, de aquí $\sigma_A(\Psi_S(u)) = \Psi_S(u)$, con $\sigma_A \in G_M$, por tanto $\Psi_S(u) \in k[u]$. □

Proposición 3.1.20. *(a) Si $M, N \in R_T$ son polinomios mónicos con $M \neq N$, entonces* $\text{mcd}(\Psi_M(u), \Psi_N(u)) = 1$.

(b) $u^M = \prod_{N|M} \Psi_N(u)$, $M, N \in R_T$ mónicos.

(c) $\Psi_M(u) = \prod_{N|M}(u^N)^{\mu(M/N)}$ donde

$$\mu(D) = \begin{cases} 1 & \text{si } D = 1 \\ (-1)^s & \text{si } D = P_1 \cdots P_s \text{ con } P_1, \ldots, P_s \\ & \text{mónicos e irreducibles distintos} \\ 0 & \text{en otro caso} \end{cases}$$

y M es mónico.

Demostración. (a). Sea $D := \text{mcd}(\Psi_M(u), \Psi_N(u))$. Si $D \neq 1$, sea $\lambda \in \overline{k}$ raíz de D. Por lo tanto λ es raíz de $\Psi_M(u)$ y $\Psi_N(u)$, es decir, $\lambda = \lambda_M^A = \lambda_N^B$ con $\text{mcd}(A, M) = 1$, $\text{mcd}(B, N) = 1$ con gr $A <$ gr M y gr $B <$ gr M. Por lo tanto $\lambda = \lambda_{MN}^{AN} = \lambda_{NM}^{BM}$ lo que implica $AN = BM$. Como B y N son primos relativos de igual forma M y A son primos relativos. Se sigue que $B|A$

y $A|B$ por que se concluye que $A = B$ y así $M = N$ lo cual es una contradicción. Por lo tanto $\text{mcd}(\Psi_M(u), \Psi_N(u)) = 1$.

(b) Si $N|M$ claramente se tiene que $\Psi_N(u)|u^M$ y si $N_1 \neq N_2$, $\text{mcd}(\Psi_{N_1}, \Psi_{N_2}) = 1$, de esto se sigue que $\prod_{N|M} \Psi_N(u)|u^M$. Observe que $\text{gr}\Big(\prod_{N|M} \Psi_N(u)\Big) = \sum_{N|M} \Phi(N)$. Veamos que $\sum_{N|M} \Phi(N) = q^{\text{gr } M}$. Si $M = P^n$ con P irreducible y $\text{gr } P = d$, se tiene que:

$$\begin{aligned}\sum_{N|M} \Phi(N) &= \sum_{i=0}^{n} \Phi(P^i) = \sum_{i=1}^{n} (q^{id} - q^{(i-1)d}) + 1 \\ &= q^{nd} - 1 + 1 = q^{nd} = q^{\text{gr } P^n}.\end{aligned}$$

Para el caso general, si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$

$$\begin{aligned}\sum_{N|M} \Phi(N) &= \sum_{i=0}^{n} \Phi(P_1^{\beta_1}) \cdots \Phi(P_r^{\beta_r}) = \prod_{i=1}^{r} \sum_{\beta_i=0}^{\alpha_i} \Phi(P_i^{\beta_i}) \\ &= \prod_{i=1}^{r} q^{\text{gr } P_i^{\beta_i}} = q^{\text{gr } M}.\end{aligned}$$

Por lo tanto $\text{gr}\left(\prod_{N|M} \Psi_N(u)\right) = q^{\text{gr } M} = \text{gr } u^M$. Se concluye entonces que $u^M = \prod_{N|M} \Psi_N(u)$. □

Se estudiará la ramificación en campos de funciones ciclotómicos, de la misma manera que se ve en campos numéricos ciclotómicos.

Definición 3.1.21. Al polo $\mathfrak{p}_\infty$ de T en k se le llama *primo infinito.*

Proposición 3.1.22. *Sea $P \in R_T$ mónico e irreducible de grado d y $M = P^n$, $n \in \mathbb{N}$. Entonces*

(a) Si $\mathfrak{q}$ es cualquier otro divisor primo distinto a $\mathfrak{p}_\infty$ y a $\mathfrak{p}$, donde $\mathfrak{p}$ es el divisor primo asociado a P, entonces $\mathfrak{q}$ es no ramificado.

(b) El índice de ramificación de $\mathfrak{p}$ en $k(\Lambda_M)/k$ es

$$e_{k(\Lambda_M)/k}(\mathfrak{p}_i|\mathfrak{p}) = \Phi(M) = q^{nd} - q^{d(n-1)} = [k(\Lambda_M) : k].$$

Demostración. Sea $\mathcal{O}_M$ la cerradura entera de R_T en $k(\Lambda_M)$. Dado que R_T es un dominio de Dedekind, O_M también lo es. Los primos ramificados en $k(\Lambda_M)/k$ son aquellos que aparecen en el discriminante $\mathfrak{d}_{\mathcal{O}_M/R_T}$. Sea λ un generador de Λ_M, entonces $R_T[\lambda] \subseteq \mathcal{O}_M$.

$$\begin{array}{ccc} \mathcal{O}_M & \text{———} & k(\Lambda_M) \\ | & & | \\ R_T & \text{———} & k \end{array}$$

Sean $g(u) = \mathrm{Irr}(\lambda, u, k) \in k[u]$ y $f(u) = u^M$ y $f(\lambda) = 0$ entonces $g(u)|f(u)$ y así existe $h(u) \in k[u]$ tal que $f(u) = h(u)g(u)$. Se tiene entonces que

$$M = f'(u) = h'(u)g(u) + h(u)g'(u)$$

tomando $u = \lambda$ se tiene

$$M = f'(\lambda) = h'(\lambda)g(\lambda) + h(\lambda)g'(\lambda) = h(\lambda)g'(\lambda)$$

Se sigue que $(g'(\lambda))_{\mathcal{O}_M}|(M)_{\mathcal{O}_M} = P^n\mathcal{O}_M$. Se tiene lo siguiente

$$\mathfrak{D}_{\mathcal{O}_M/R_T} = \langle F'(\alpha) \mid \alpha \in \mathcal{O}_M, k(\Lambda_M) = k(\alpha), F(u) = \mathrm{Irr}(\alpha, u, k)\rangle.$$

En particular $\mathfrak{D}_{\mathcal{O}_M/R_T}|(g'(\lambda))_{\mathcal{O}_M}|P^n$, donde $\mathfrak{p}\mathcal{O}_M = \langle \mathfrak{p}_1 \cdots \mathfrak{p}_h\rangle^e$, entonces $P^n = (\mathfrak{p}_1 \cdots \mathfrak{p}_h)^{ne}$. Por lo tanto los únicos posibles primos ramificados en $k(\Lambda_M)/k$ son $\mathfrak{p}$ y $\mathfrak{p}_\infty$.

Ahora se calcula $e := e_{k(\Lambda_M)/k}(\mathfrak{p}_i|\mathfrak{p})$. Se tiene

$$\begin{aligned} u^{P^n} &= (u^{P^{n-1}})^P = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i} \\ &= u^{P^{n-1}} \Big(\sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i - 1} \Big) = u^{P^{n-1}} t(u). \end{aligned}$$

Observe que

$$t(u) = \frac{u^{P^n}}{u^{P^{n-1}}} = \sum_{i=0}^{d} \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i - 1} = \frac{\prod_{N|P^n} \Psi_N(u)}{\prod_{N|P^{n-1}} \Psi_N(u)}.$$

Se tiene $t(\alpha) = 0 \iff \alpha \in \Lambda_{P^n} \backslash \Lambda_{P^{n-1}} \iff \alpha$ es generador de Λ_{P^n} (recuerde que $\Lambda_{P^n}/\Lambda_{P^{n-1}} \cong \Lambda_P$). Por lo tanto $t(u) = \Psi_{P^n}(u)$. Se sigue que

$$t(u) = \prod_{\mathrm{mcd}(A,M)=1} (u - \lambda^A) = \begin{bmatrix} P \\ 0 \end{bmatrix} + \sum_{i=1}^{d} \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i - 1} = P + \sum_{i=1}^{d} \begin{bmatrix} P \\ i \end{bmatrix} (u^{P^{n-1}})^{q^i - 1}.$$

Para $u = 0$ se tiene

$$t(0) = \pm \prod_{\mathrm{mcd}(A,M)=1} \lambda^A = P.$$

Ahora bien, $u^A = um_A(u)$ con $m_A(u) \in R_T(u)$. En particular $\lambda^A = \lambda F(\lambda) \Rightarrow \lambda|\lambda^A$. Para $\mathrm{mcd}(A, M) = 1$, λ^A es generador y, por simetría, se sigue $\lambda^A|\lambda$, es decir $\lambda = \beta_A\lambda^A$ con $\beta_A \in \mathcal{O}_M^*$. Se tiene que $\pm P = \beta_0\lambda^{\Phi(M)}$ para $\beta_0 \in \mathcal{O}_M$. Se obtiene $\langle P\rangle_{\mathcal{O}_M} = \langle \mathfrak{p}_1 \cdots \mathfrak{p}_h\rangle^e = (\lambda)^{\Phi(M)}$ y en

particular $v_{\mathfrak{P}_i} \geqslant 1$. Por lo tanto $e = v_{\mathfrak{p}_i}((\mathfrak{p}_i \cdots \mathfrak{p}_h)^e) = v_{\mathfrak{p}_i}(\lambda^{\Phi(M)}) \geqslant \Phi(M)$, se tiene entonces:

$$e \geqslant \Phi(M) = |(R_T/\langle M\rangle)^*| \geqslant [k(\Lambda_M) : k] \geqslant e$$

se concluye entonces que $e = \Phi(M) = \Phi(P^n) = [k(\Lambda_{P^n}) : k] = q^{dn} - q^{d(n-1)}$. □

Teorema 3.1.23. *Si $M \in R_T\backslash\{0\}$ un polinomio mónico. Entonces:*

1. *$t(u) = \mathrm{Irr}(\lambda, u, k) = \Psi_M(u)$ donde λ es un generador de Λ_M. En particular $\Psi_M(u)$ es irreducible.*

2. *$G_M = \mathrm{Gal}(k(\Lambda_M)/k) \cong (R_T/\langle M\rangle)^*$*

3. *$[k(\Lambda_M) : k] = \Phi(M)$*

4. *Si $M = P^n$ donde P es irreducible, entonces $\mathfrak{p}$ es totalmente ramificado en $k(\Lambda_M)/k$ donde $\langle P\rangle_k = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\mathrm{gr}\ P}}$.*

Demostración. Si $M = P^n$ por la Proposición 3.1.22 de tiene

$$[k(\Lambda_{P^n}) : k] = \Phi(P^n) = |(R_T/\rangle P^n\langle)^*| = |G_{P^n}|.$$

Se tiene por la Proposición 3.1.6 que $G_M \subseteq (R_T\langle P^n\rangle)^*$. Por lo tanto $G_{P^n} = (R_T\langle P^n\rangle)^*$ y P es totalmente ramificado pues $e_{k(\Lambda_M)/k}(\mathfrak{p}_i|\mathfrak{p}) = \Phi(P^n) = [k(\Lambda_M) : k]$ y se tiene (4). Para el caso general, si $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ con $P_1, \ldots, P_r$ polinomios mónicos e irreducibles distintos, se tiene que $\Lambda_M = \bigoplus \Lambda_{P_i^{\alpha_i}}$. Se probará que $[k(\Lambda_M) : k] = \Phi(M)$ y dado que $G_M \subseteq (R_T/\langle M\rangle)^*$ se tendrán así (2) y (3). Para (1) note que $t(\lambda) = 0$ y $\mathrm{gr}\, t(u) = \Phi(M) = \mathrm{gr}\, \mathrm{Irr}(\lambda, u, k)$ e $\mathrm{Irr}(\lambda, u, k)|t(u)$.

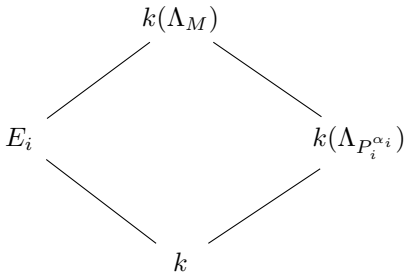
Para probar que $\Phi(M) = [k(\lambda_M) : k]$ se verá que $\mathfrak{p}_i$ es totalmente ramificado en $k(\lambda_{P_i^{\alpha_i}})/k$ y no ramificado en $\prod_{j\neq i} k(\Lambda_{P_j^{\alpha_j}})/k$, y que $k(\Lambda_{P_1^{\alpha_1}}), \ldots, k(\Lambda_{P_r^{\alpha_r}})$ son linealmente disjuntos a pares. Se sigue que

$$[k(\Lambda_M) : k] = \prod_{i=1}^{r} [k(\Lambda_{P_i^{\alpha_i}}) : k] = \prod_{i=1}^{r} \Phi(P_i^{\alpha_i}) = \Phi(M).$$

□

Corolario 3.1.24. *El campo de constantes de $k(\Lambda_M)$ es $\mathbb{F}_q$ y $k(\Lambda_M)/k$ es una extensión geométrica.*

Demostración. Sea $E_i := k(\Lambda_{M/P_i^{\alpha_i}})$ para $1 \leqslant i \leqslant r$ donde $M = P_1^{\alpha_i} \cdots P_r^{\alpha_r}$. Entonces $\mathrm{Gal}(k(\Lambda_M)/E_i) \cong \mathrm{Gal}(k(\Lambda_{P_i^{\alpha_i}})/k)$.



Sea L la máxima extensión no ramificada de k contenida en $k(\Lambda_M)$. Observe que $k(\Lambda_M)/E_i$ es totalmente ramificada en los primos que están sobre $\mathfrak{p}_i$ y E_iL/E_i es no ramificada, por lo tanto $E_iL = E_i$ lo cual implica que $L \subseteq E_i$ para todo $1 \leqslant i \leqslant r$. De esta manera se obtiene que $k \subseteq L \subseteq \bigcap_{i=1}^{r} E_i = k$. Por tanto $L = k$ y así, cada subextensión $k \subsetneq F \subseteq k(\Lambda_M)$ es ramificada. Sea $\mathbb{F}_{q^s}$ el campo de constantes de $k(\Lambda_M)$. Se tiene

$$k = \mathbb{F}_q(T) \subseteq \mathbb{F}_{q^s}(T) \subseteq k(\Lambda_M).$$

Dado que $\mathbb{F}_{q^s}(T)/\mathbb{F}_q(T)$ es no ramificada por el Teorema 2.2.29, se concluye entonces $\mathbb{F}_{q^s}(T) = \mathbb{F}_q(T)$ y por tanto $\mathbb{F}_{q^s} = \mathbb{F}_q$, es decir, $s = 1$.

□

Proposición 3.1.25. *Sea P un polinomio mónico e irreducible en R_T y sea $M = P^n$ para algún $n \geqslant 1$. Entonces*

$$\Psi_{P^n}(u) = \frac{u^{P^n}}{u^{P^{n-1}}}$$

es un polinomio de Einsenstein sobre R_T en P. En otras palabras, si

$$\Psi_{P^n}(u) = u^d + a_{d-1}u^{d-1} + \cdots + a_0 \in R_T[u],$$

entonces P divide a_i para $0 \leqslant i \leqslant d-1$, y P^2 no divide a_0.

Demostración. Ver [21, página 429]. □

Corolario 3.1.26. *El polinomio $\Psi_{P^n}(u) \in R_T$ es irreducible.*

Demostración. Se tiene de la aplicación del criterio de Eisenstein. □

3.2. Aritmética de un campo de funciones ciclotómico

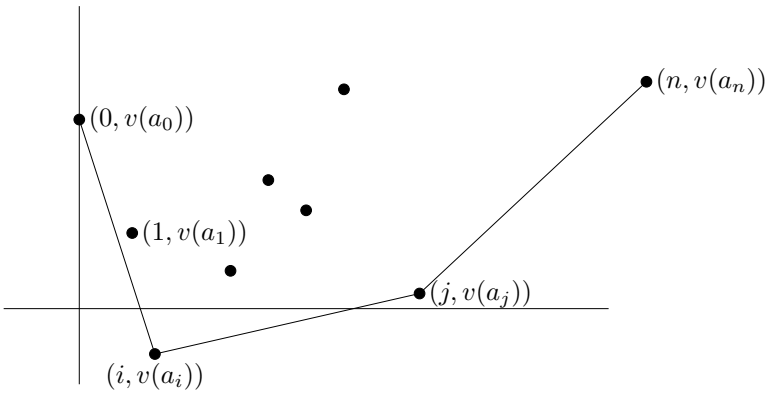
3.2.1. Polígono de Newton

Sea F un campo completo con respecto a una valuación discreta v y con lugar $\mathfrak{p}$. Sean Ω una cerradura algebraica de F y

$$f(x) = a_0 + a_1 x + \cdots a_n x^n \in F[x], \text{ donde } a_0 a_n \neq 0$$

Se asocia a cada término de $f(x)$ un punto de $\mathbb{R} \times (\mathbb{R} \cup \{\infty\})$ de la siguiente manera:

- si $a_i x^i \neq 0$, es decir si $a_i \neq 0$ entonces se toma el punto $(i, v(a_i))$.
- si $a_i x^i = 0$, es decir si $a_i = 0$ entonces se toma el punto $(i, \infty) = (i, v(a_i))$.



Se considera la cubierta convexa inferior del conjunto

$$\{(i, v(a_i)) \mid i = 0, 1, \ldots, n \text{ con } a_i \neq 0\}.$$

Definición 3.2.1. Esta cubierta es llamada el *polígono de Newton*.

En otras palabras, el conjunto de vértices de esta cubierta es

$$\{(0 = i_0, v(a_0)), (i_1, v(a_{i_1})), \ldots, (i_m = n, v(a_n))\}$$

donde $a_0, a_{i_1}, \ldots, a_n$ satisface lo siguiente. Primero, se considera $S = \{i > 0 \mid a_i \neq 0\}$ y sea i_1 el máximo tal que

$$\frac{v(a_{i_1}) - v(a_0)}{i_1 - 0} = \text{mín}\left\{\frac{v(a_j) - v(a_0)}{j - 0} \mid j \in S\right\}.$$

Ahora sea i_2 el máximo tal que

$$\frac{v(a_{i_2}) - v(a_{i_1})}{i_2 - i_1} = \text{mín}\left\{\frac{v(a_j) - v(a_{i_1})}{j - a_{i_1}} \mid j \in S,\ j > i_1\right\}.$$

Teorema 3.2.2. *Sea $[(r, v(a_r)), (s, v(a_s))]$ cualquier segmento del polígono de Newton correspondiente a $f(x)$. Sea $\frac{v(a_s)-v(a_r)}{s-r} = -m$ su pendiente. Entonces $f(x)$ tiene exactamente $s-r$ raíces $\alpha_1, \ldots, \alpha_{s-r}$ satisfaciendo $v(\alpha_1) = \cdots = v(\alpha_{s-r}) = m$.*

Además, se define $f_m(x) = \prod_{i=1}^{s-r}(x - \alpha_i)$. Entonces $f_m(x) \in F[x]$ y $f_m(x)$ divide a $f(x)$.

Demostración. Ver [21, página 431]. □

Teorema 3.2.3 (Lema de Abhyankar)**.** *Sea L/k una extensión finita y separable de campos de funciones. Supóngase que $L = k_1k_2$ con $k \subseteq k_i \subseteq L$. Sea $\mathfrak{p}$ un divisor primo de k y sea $\mathfrak{P}$ un divisor primo en L sobre $\mathfrak{p}$. Sea $\mathfrak{P}_i = \mathfrak{P} \cap k_i$ para $i = 1, 2$. Si al menos una de las dos extensiones k_i/k es moderadamente ramificada en $\mathfrak{p}$, entonces*

$$e_{\mathfrak{P}|\mathfrak{p}}(L : k) = \operatorname{mcm}\big[e_{\mathfrak{P}_1|\mathfrak{p}}(k_1 : k), e_{\mathfrak{P}_2|\mathfrak{p}}(k_2 : k)\big].$$

Demostración. Ver [21, páginas 434-435]. □

3.2.2. Ramificación de $\mathfrak{p}_\infty$

Se enunciarán los resultados que prueban que para cualquier $M \in R_T\backslash\{0\}$ con $R_T = \mathbb{F}_q[T]$, el primo infinito de $k = \mathbb{F}_q(T)$, donde $(T)_k = \frac{\mathfrak{p}_0}{\mathfrak{p}_\infty}$, es moderadamente ramificado en $k(\Lambda_M)/k$.

Teorema 3.2.4. *Sea $u^M \in k[u] \subseteq k_\infty[u]$, donde k_∞ es la completación de k en $\mathfrak{p}_\infty$. Para cada $1 \leqslant i \leqslant d$, con $d = \operatorname{gr} M$, existen exactamente $q^i - q^{i-1}$ raíces $\widetilde{\lambda}$ de u^M/u en $k_\infty[u]$ tales que $v_{\mathfrak{P}}(\widetilde{\lambda}) = e((d - i - \frac{1}{q-1}))$, donde $e = e_{(k(\Lambda_N)/k)}(\mathfrak{P}|\mathfrak{p}_\infty)$.*

Demostración. Se tiene que $v_{\mathfrak{p}_\infty}\Big(\begin{bmatrix} M \\ i \end{bmatrix}\Big) = -q^i(d-i)$ y $v_{\mathfrak{P}}\Big(\begin{bmatrix} M \\ i \end{bmatrix}\Big) = -eq^i(d-i)$. Se considera el polígono de Newton de $\frac{u^M}{u} = \sum_{i=0}^{d} \begin{bmatrix} M \\ i \end{bmatrix} u^{q^i-1}$. Se tendrá la siguiente expresión $\frac{u^M}{u} = \sum_{j=0}^{q^d-1} f_j(T)u^j$, donde $f_j(T) \neq 0 \iff$ existe i tal que $j = q^i - 1$ y, siendo así, se tiene

$$f_j(T) = f_{q^i-1}(T) = \begin{bmatrix} M \\ i \end{bmatrix}, \qquad v_{\mathfrak{p}_\infty}(f_{q^i-1}(T)) = -\operatorname{gr}_T f_{q^i-1}(T) = -q^i(d-1)$$

$$\text{y} \qquad v_{\mathfrak{P}}(f_{q^i-1}(T)) = e(-q^i(d-1)) = eq^i(d-i).$$

Note que los vértices que se deben considerar para el polígono de Newton son:

$$\{\beta_i\}_{i=0}^{d} = \{(q^i - 1, -eq^i(d-1))\}_{0 \leqslant i \leqslant d}.$$

La pendiente entre β_i y β_{i+1}, $0 \leqslant i \leqslant d-1$, es

$$\begin{aligned}\xi_i &= \frac{v_{\mathfrak{P}}(f_{q^{i+1}-1}(T)) - v_{\mathfrak{P}}(f_{q^i-1}(T))}{(q^{i+1}-1)-(q^i-1)} = \frac{v_{\mathfrak{P}}\Big(\begin{bmatrix} M \\ i+1 \end{bmatrix}\Big) - v_{\mathfrak{P}}\Big(\begin{bmatrix} M \\ i \end{bmatrix}\Big)}{q^i(q-1)} \\ &= \frac{-eq^{i+1}(d-(i+1)) - (-eq^i(d-1))}{q^i(d-1)} = \frac{(q^i - q^{i+1})e(d-1) + eq^{i+1}}{q^i(q-1)} \\ &= -e(d-i) + \frac{eq}{q-1} = ei - ed + \frac{eq}{q-1} < e(i-1) - ed + \frac{eq}{q-1} = \xi_{i+1}\end{aligned}$$

esto es $\xi_i < \xi_{i+1}$ para $0 \leqslant i \leqslant d-1$.

Por lo tanto los vértices del polígono de Newton corresponden a $\beta_0, \beta_1, \ldots, \beta_d$ pues se tiene que $\xi_0 < \xi_1 < \cdots < \xi_{d-1}$. Así pues, para $0 \leqslant i \leqslant d-1$, hay $(q^{i+1}-1)-(q^i-1)$ raíces de valuación $-\xi_i = e(d - i - \frac{q}{q-1})$. Es decir hay exactamente $q^{i+1} - q^i$ raíces en $\overline{k}_\infty$ de valuación $-\xi = e(d-(i+1) - \frac{1}{q-1})$.

□

Teorema 3.2.5. *Sea $M \in R_T \backslash \{0\}$ un polinomio mónico. Entonces $\mathfrak{p}_\infty$ es moderadamente ramificado en $k(\Lambda_M)/k$, se tiene $e_\infty = q-1$ y $f_\infty = 1$ y hay exactamente $h_\infty = \Phi(M)/(q-1)$ divisores primos de $k(\Lambda_M)$ sobre $\mathfrak{p}_\infty$.*

Demostración. Ver [21, páginas 437-438]. □

Teorema 3.2.6. *Sea $M \in R_T$ un polinomio no constante. Sean $G_M = \mathrm{Gal}(k(\Lambda_M)/k) \cong (R_T/(M))^*$ y $J := \{\sigma_\alpha \mid \alpha \in \mathbb{F}_q^*\}$, luego $J \cong \mathbb{F}_q^* \subseteq G_M$. Sea $k(\Lambda_M)^+ := k(\Lambda_M)^J = k(\lambda_M^{q-1})$ donde λ_M es un generador de Λ_M. Entonces $\mathfrak{p}_\infty$ se descompone totalmente en $k(\Lambda_M)^+/k$ y si $\mathfrak{P}$ es un primo en $k(\Lambda_M)$ sobre $\mathfrak{p}_\infty$, $\mathfrak{p} = \mathfrak{P} \cap k(\Lambda_M)^+$, entonces $\mathfrak{P}/\mathfrak{p}$ es totalmente ramificado. Esto es,*

$$e_{k(\Lambda_M)^+/k}(\mathfrak{p}|\mathfrak{p}_\infty) = f_{k(\Lambda_M)^+/k}(\mathfrak{p}|\mathfrak{p}_\infty) = 1,$$

$$e_{k(\Lambda_M)/k(\Lambda_M)}(\mathfrak{p}|\mathfrak{p}_\infty) = q-1, \qquad f_{k(\Lambda_M)/k(\Lambda_M)}(\mathfrak{p}|\mathfrak{p}_\infty) = 1.$$

En particular $e_\infty = e_{k(\Lambda_M)/k}(\mathfrak{P}|\mathfrak{p}_\infty) = q-1$ y $f_\infty = f_{k(\Lambda_M)/k}(\mathfrak{P}|\mathfrak{p}_\infty) = 1$. Además $J = \{\sigma_\alpha \in G_M \mid \alpha \in \mathbb{F}_q^*\}$ que es a la vez el grupo de descomposición y el grupo de inercia de $\mathfrak{P}/\mathfrak{p}_\infty$:

$$D_{k(\Lambda_M)/k}(\mathfrak{P}|\mathfrak{p}_\infty) = I_{k(\Lambda_M)/k}(\mathfrak{P}|\mathfrak{p}_\infty) \cong \mathbb{F}_q^*.$$

También se tiene, $k(\Lambda_M)^+ = k(\lambda_M^{q-1})$.

Demostración. Ver [19, páginas 173-174]. □

Definición 3.2.7. El campo $k(\Lambda_M)^+ = k(\Lambda_M^{q-1})$ se llama el *subcampo real o el máximo subcampo real de $k(\Lambda_M)$*.

Observación 3.2.8. Lo anterior es análogo al caso de campos numéricos.

$$\begin{array}{c} \mathbb{Q}(\zeta_n) \\ \{1,J\} \left(\begin{array}{c} | \\ | \end{array} \right) \infty \text{ es totalmente ramificado} \\ \mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n) \cap \mathbb{R} \\ \left. \begin{array}{c} | \\ | \end{array} \right) \infty \text{ es totalmente descompuesto} \\ \mathbb{Q} \end{array}$$

$$\begin{array}{c} k(\Lambda_M) \\ \mathbb{F}_q^* \left(\begin{array}{c} | \\ | \end{array} \right) \infty \text{ es totalmente ramificado} \\ k(\Lambda_M)^+ = k(\Lambda_M^{q-1}) \\ \left. \begin{array}{c} | \\ | \end{array} \right) \infty \text{ es totalmente descompuesto} \\ k \end{array}$$

$\{1, J\} = \{1, -1\} \longleftrightarrow \mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$. $\mathbb{F}_q^*$ juega el papel de $\{\pm 1\}$ (debido a esto, en los campos de funciones se llaman "pares" a los enteros $a \in \mathbb{N}$ tales que $(q-1)|a$).

Observación 3.2.9. Note que $k(\Lambda_M) = k$ si y solamente si $q = 2$ y $M = T$, $M = T + 1$ o $M = T(T + 1)$, para este caso se tiene $\mathbb{F}_q(T)(\Lambda_T)$, $\mathbb{F}_q(T)(\Lambda_{T+1})$, $\mathbb{F}_q(T)(\Lambda_{T(T+1)})$, juegan el papel de $\mathbb{Q}(\zeta_2) = \mathbb{Q}$ en el caso de los campos numéricos. Se debe tener siempre en cuenta esta excepción para el caso de los campos de funciones ciclotómicos.

En particular, para $q = 2$, $\mathfrak{p}_\infty$ no se ramifica en ningún $k(\Lambda_M)/k$ y se tiene que $k(\Lambda_{MT}) = k(\Lambda_M)$ para todo $M \in R_T$ con $T \nmid M$. Similarmente $k(\Lambda_{M(T+1)}) = k(\Lambda_M)$ para todo $M \in R_T$ con $T+1 \nmid M$.

3.2.3. Ramificación en $k(\Lambda_M)/k$

En esta sección se considera $k(\Lambda_M)/k$ donde $M \in R_T \backslash \{0\}$ es un polinomio mónico.

Proposición 3.2.10. *Se tiene que los primos ramificados en $k(\Lambda_M)/k$ son $\mathfrak{p}_\infty$ y los divisores de M con excepción del caso $q = 2$, en el que $\mathfrak{p}_\infty$ es no ramificado y las situaciones analizadas en la Observación 3.2.9.*

Demostración. Se sigue de la Proposición 3.1.22 y del Teorema 3.2.6. □

Sean $\mathfrak{p}$ un lugar en k con $\mathfrak{p} \neq \mathfrak{p}_\infty$ y $\mathfrak{P}$ en $k(\Lambda_M)$ tal que $\mathfrak{P}|\mathfrak{p}$. Sean D e I los grupos de descomposición e inercia respectivamente. Entonces $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p})) \cong D/I$. Si $\mathfrak{p}$ es no ramificado, $I = 1$ y $D \cong \mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$, dado que $k(\mathfrak{P})$ y $k(\mathfrak{p})$ son campos finitos, $\mathrm{Gal}(k(\mathfrak{P})/k(\mathfrak{p}))$ es un grupo cíclico generado por el automorfismo de Frobenius:

$$\sigma_{\mathfrak{p}} : k(\mathfrak{P}) \to k(\mathfrak{P}), \qquad \sigma_{\mathfrak{p}}(x) = x^{|k(\mathfrak{P})|} = x^{N(\mathfrak{p})},$$

donde $N(\mathfrak{p}) = |k(\mathfrak{p})| = |\mathcal{O}_{\mathfrak{p}}/\mathfrak{P}|$.

Definición 3.2.11. El *automorfismo de Frobenius*, el cual se denota por $\left[\frac{k(\Lambda_M)/k}{\mathfrak{P}}\right]$, está caracterizado por la siguiente propiedad

$$\left[\frac{k(\Lambda_M)/k}{\mathfrak{P}}\right](x) \equiv x^{N(\mathfrak{p})} \text{ mód } \mathfrak{P} \quad \forall\, x \in \mathcal{O}_{\mathfrak{P}}.$$

Dado que $k(\Lambda_M)/k$ es abeliana, $\left[\frac{k(\Lambda_M)/k}{\mathfrak{P}}\right]$ es independiente de $\mathfrak{P}$ y sólo depende de $\mathfrak{p}$ y se denota por $\varphi_P = \left(\frac{k(\Lambda_M)/k}{P}\right)$ y se le llama el *símbolo de Artin*, donde $P \in R_T^+$.

Teorema 3.2.12. *Sea P un polinomio irreducible que no divide a M. Entonces el mapeo:*

$$\begin{aligned} \varphi :& \Lambda_M \longrightarrow \Lambda_M \\ & \lambda \mapsto \lambda^P \end{aligned}$$

corresponde al símbolo de Artin $\left(\frac{k(\Lambda_M)/k}{P}\right)$.

Demostración. Sea $(R_T)_{_P} = \{\frac{f}{g} \mid f, g \in R_T,\ P \nmid g\}$ y sea $(P)_k := \frac{\mathfrak{p}}{\mathfrak{p}_\infty}$, es decir, P es un elemento primo de $\mathfrak{p}$. Entonces $k(\mathfrak{p}) = (R_T)_{_P}/P(R_T)_{_P} \cong R_T/\langle P\rangle \cong \mathbb{F}_{q^d}$ donde $d = \operatorname{gr} P$.

Sea $\mathfrak{P}$ un lugar en $k(\Lambda_M)$ sobre $\mathfrak{p}$. Entonces $N(\mathfrak{p}) = |\mathbb{F}_{q^d}| = q^d$ y $k(\Lambda_M) \subseteq \mathcal{O}_{\mathfrak{P}}$. Entonces

$$\left(\frac{k(\Lambda_M)/k}{P}\right)(\lambda) \equiv \lambda^{q^d} \text{ mód } \mathfrak{P}.$$

Se tiene que $u^P = u\Psi_P(u) = u(u^{q^d-1} + \beta_{q^d-2}u^{q^d-2} + \cdots \beta_1 u + \beta_0)$ dado que $\Psi_P(u) = \prod_{\text{mcd}(A,P)=1}(u - \lambda^A)$ con λ generador de Λ_P y $\Psi_P(0) = \pm\prod_{\text{mcd}(A,P)=1}\lambda^A = P$ de aquí se sigue que $P|\beta_i$ para $0 \leqslant i \leqslant q^d - 2$ y de esta manera se tiene $P|\lambda^P - \lambda^{q^d}$ y por tanto $\lambda^P \equiv \lambda^{q^d}$ mód $\mathfrak{P}$.

Ya que $u^M = \prod_{A \text{ mód } M}(u - \lambda^A)$, al tomar la derivada con respecto a u, se tiene que $M = \sum_{A \text{ mód } M}(\prod_{B\neq A}(u - \lambda^B))$ que es constante en u. Sea $u = \lambda^C$. Entonces $M = \prod_{C\neq B}(\lambda^C - \lambda^B)$ y como $P \nmid M$, entonces $\lambda^C \not\equiv \lambda^B$ mód $\mathfrak{P}$ para $C \not\equiv B$ mód M. En particular se tiene $\lambda^P \equiv \lambda^Q$ mód $\mathfrak{P} \Longrightarrow \lambda^P = \lambda^Q$.
Por lo tanto $\lambda^P \equiv \left(\frac{k(\Lambda_M)/k}{P}\right)(\lambda) \equiv \lambda^{q^d}$ mód $\mathfrak{P}$, de aquí se sigue que $\varphi_P = \left(\frac{k(\Lambda_M)/k}{P}\right)$. □

Con la notación usual de e_P = índice de ramificación de P, f_P = grado de inercia y h_P = número de primos encima de P, se tiene:

Proposición 3.2.13. *Sea $M \in R_T\backslash\{0\}$ y sea P un polinomio mónico e irreducible que no divide a M. En $k(\Lambda_M)/k$ se tiene*

- $e_P = 1$
- $f_P = o(P \text{ mód } M)$
- $h_P = \Phi(M)/f_P$

Demostración. Sea λ generador de λ_M, $k(\lambda) = k(\Lambda_M)$. Sea $\mathfrak{P}$ un divisor primo en $k(\Lambda_M)$ dividiendo a $\mathfrak{p}$ donde $(P)_k = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\text{gr } P}}$. Entonces $\mathcal{O}_\mathfrak{P} := \{\xi \in k(\Lambda_M) \mid v_\mathfrak{P}(\xi) \geqslant 0\}$

$$f_P = [\mathcal{O}_\mathfrak{P}/\mathfrak{P} : (R_T)_P/P(R_T)_P] = [(\mathcal{O}_M)_\mathfrak{P}/\mathfrak{P}(\mathcal{O}_M)_\mathfrak{P} : R_T/\langle P\rangle] = [\mathcal{O}_M/\mathfrak{P}\mathcal{O}_M : R_T/\langle P\rangle],$$

donde $\mathcal{O}_M$ es la cerradura entera de R_T en $k(\Lambda_M)$.

Sea $d = \text{gr } P$ y dado que $P \nmid M$, $\mathfrak{p}$ no se ramifica en $k(\Lambda_M)/k$ y el símbolo de Artin $\varphi_P = \left(\frac{k(\Lambda_M)/k}{P}\right)$ en P está dado por $\varphi(\lambda) = \lambda^P$.

Entonces $e_P = 1$ y $h_P = [k(\Lambda_M) : k]/f_P = \Phi(M)/f_P$. Finalmente, el orden de φ_P es f_P, es decir f_P es el mínimo natural tal que $\varphi_P^{f_P} = \text{Id} \in G_M = \text{Gal}(k(\Lambda_M)/k)$. De esta manera $\varphi_P^{f_P} = 1 \iff \varphi_P^{f_P}(\lambda) = \lambda^{P^{f_P}} = \lambda \iff \lambda^{P^{f_P}-1} = 0 \iff M|P^{f_P} - 1$. Se sigue entonces que $f_P = o(P \text{ mód } M)$ es el mínimo número natural tal que $M|P^{f_P} - 1$. □

El resultado general sobre ramificación se enuncia en el siguiente teorema.

Teorema 3.2.14. *Sea $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \in R_T$ donde $P_1, \ldots, P_r$ son polinomios irreducibles y sea $k(\Lambda_M)/k$. Si $P \in R_T$ es distinto de $P_1, \ldots, P_r$ y de $\mathfrak{p}_\infty$ entonces*

$$e_P = 1, \qquad f_P = o(P \text{ mód } M) \quad y \quad h_p = \Phi(M)/f_P.$$

Si $P = P_i$ para $i = 1, \ldots, r$, se tiene

$$e_P = \Phi(P_i^{\alpha_i}), \quad f_P = o(P_i \text{ mód } M/P_i^{\alpha_i}) \;\; y \;\; h_P = \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})f_{P_i}} = \frac{\Phi(M/P_i^{\alpha_i})}{o(P_i \text{ mód } M/P_i^{\alpha_i})}.$$

Finalmente, para $\mathfrak{p}_\infty$ se tiene

$$e_\infty = q - 1, \qquad f_\infty = 1 \quad y \quad h_\infty = \frac{\Phi(M)}{q-1}.$$

Demostración. El teorema se sigue de la Proposición 3.1.22, de la Proposición 3.2.13 y del Teorema 3.2.6 □

Teorema 3.2.15. *Sea $M = P^n$, con $P \in R_T$ irreducible. Entonces $\mathcal{O}_M = R_T[\lambda_M]$ donde $\mathcal{O}_M$ es la cerradura entera de R_T en $k(\Lambda_M)$ y λ_M es un generador de Λ_M.*

Demostración. Ver [19, página 178]. □

Teorema 3.2.16. *Para cualquier $M \in R_T\backslash\{0\}$, se tiene $\mathcal{O}_{k(\Lambda_M)^+} = R_T[\lambda_M^{q-1}]$, donde λ_M es un generador de Λ_M con $k(\Lambda_M)^+ = k(\lambda_M^{q-1})$.*

Demostración. Ver [19, página 179]. □

Observación 3.2.17. El Teorema 3.2.16 se puede generalizar para cualquier subcampo $k(\Lambda_M)^+ \subseteq F \subseteq k(\Lambda_M)$. En efecto, note que $k(\Lambda_M)/k(\Lambda_M)^+$ es una extensión cíclica de Kummer de grado $q-1$, entonces $F = k(\lambda_M^m)$ con $m|q-1$.

3.3. Caracteres de Dirichlet

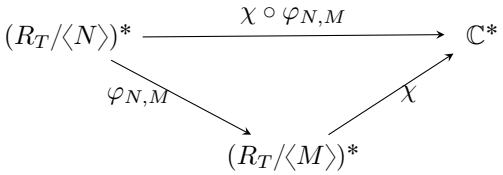
Definición 3.3.1. Sea $M \in R_T\backslash\{0\}$ un polinomio mónico. Un *caracter de Dirichlet módulo M* es un homomorfismo

$$\chi : (R_T/\langle M\rangle)^* \longrightarrow \mathbb{C}^*.$$

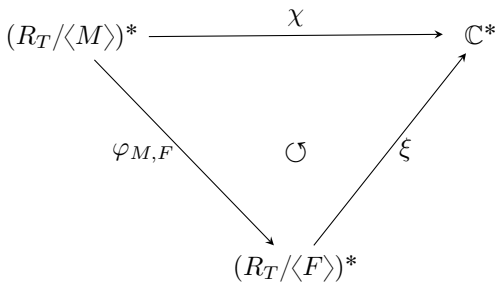
Observación 3.3.2. Si $M|N$ en R_T, se tiene el epimorfismo canónico

$$\begin{aligned} \varphi_{N,M} : (R_T/\langle N\rangle)^* &\longrightarrow (R_T/\langle M\rangle)^* \\ A \text{ mód } N &\longmapsto A \text{ mód } M. \end{aligned}$$

Entonces para todo caracter de Dirichlet módulo M, $\chi : (R_T/\langle M\rangle)^* \longrightarrow \mathbb{C}^*$, $\varphi_{N,M}$ induce un caracter de Dirichlet módulo $N : \chi \circ \varphi_{N,M} : (R_T/\langle N\rangle)^* \longrightarrow \mathbb{C}^*$,



Recíprocamente, si χ es un caracter de Dirichlet módulo M, se dice que se puede definir χ módulo F para $F|M$ si existe $\xi : (R_T/\langle F\rangle)^* \longrightarrow \mathbb{C}^*$ tal que $\xi \circ \varphi_{M,F} = \chi$



Observación 3.3.3. Si ξ es un caracter de Dirichlet definido módulo $M \in R_T$, entonces si $F|M$, $F \in R_T$, se tiene que χ puede definirse módulo F si y solamente si para cualesquiera $A, B \in R_T$ tales que sean primos relativos a M y $A \equiv B$ mód F entonces $\chi(A \text{ mód } M) = \chi(B \text{ mód } M)$.

Teorema 3.3.4 (Existencia del conductor)**.** *Sea χ un caracter de Dirichlet definido módulo M. Entonces existe un polinomio mónico único $F \in R_T$ de grado mínimo que divide a M tal que χ puede ser definido módulo F.*

Demostración. Sea $\chi : (R_T/\langle M\rangle)^* \longrightarrow \mathbb{C}^*$. Sean $A, B \in R_T$ mónicos y tales que χ puede ser definido módulo A y también módulo B, es decir, existen $\chi_A : (R_T/\langle A\rangle)^* \longrightarrow \mathbb{C}^*$ y $\chi_B : (R_T/\langle B\rangle)^* \longrightarrow \mathbb{C}^*$ tales que $\chi = \chi_A \circ \varphi_{M,A}$, $\chi = \chi_B \circ \varphi_{M,B}$.

Sean $C := \text{mcd}(A, B)$ el máximo común divisor de A y B y sea D el producto de todos los polinomios mónicos irreducibles que dividen a M pero no dividen a B. Entonces $C = \text{mcd}(DA, B)$.

Observe que es posible definir χ módulo C. En efecto, sean $U, V \in R_T$ primos relativos a M tales que $U \equiv V$ mód C. Por el Teorema Chino del Residuo, existe $S \in R_T$ tal que $S \equiv U$ mód DA y $S \equiv V$ mód B.

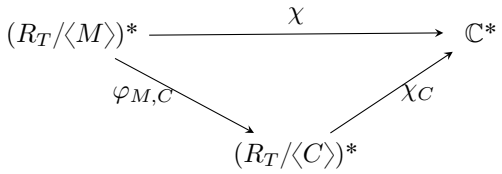
Veamos que S y M son primos relativos. En caso contrario, existiría $P \in R_T$ irreducible tal que divide a S y a M. Sea $S = V + QB$. Entonces si $P|B$, se tendría que $P|V$ y así $P|\text{mcd}(V, M) = 1$ lo cual es absurdo, así que $P \nmid B$. Ahora bien, puesto que $P|M$ y $P \nmid B$ entonces P es un factor de D, de esta manera $P|DA$. Como $P|S$ y por lo tanto $P|U$ y así $P|\text{mcd}(U, M) = 1$ lo cual también es absurdo. Por lo tanto se concluye que $\text{mcd}(S, M) = 1$. Entonces

$$\chi(S) = \chi_A \circ \varphi_{M,A}(S) = \chi_A \circ \varphi_{M,A}(U) = \chi(U)$$

y

$$\chi(S) = \chi_B \circ \varphi_{M,B}(S) = \chi_A \circ \varphi_{M,B}(V) = \chi(V).$$

Por lo tanto $\chi(S) = \chi(U) = \chi(V)$ de aquí se sigue que χ puede definirse módulo C:



Resumiendo, si χ puede definirse módulo F_1 y módulo F_2 con F_1 y F_2 de grado mínimo y F_1, F_2 mónicos, entonces χ puede definirse módulo $C = \text{mcd}(F_1, F_2)$. Dado que $C|F_1$ y $C|F_2$ se concluye que $C = F_1 = F_2$. □

Definición 3.3.5. El polinomio dado en el Teorema 3.3.4 se llama *conductor* de χ y se denota por F_χ. En otras palabras, si χ es un caracter de Dirichlet definido módulo M, entonces F_χ es el único polinomio de grado mínimo que divide a M y tal que χ puede ser definido módulo F_χ.

Observación 3.3.6. Sean $q = 2$ y $M \in R_T\backslash\{0\}$ mónico tal que $\text{mcd}(M, T) = \text{mcd}(M, T+1) = 1$. Se tiene que no existe un caracter de Dirichlet θ tal que tenga conductor $F_\theta = TM$ ni $F_\theta = (T+1)M$. En efecto, dado que $\Phi(TM) = \Phi(T)\Phi(M) = \Phi(M)$ y de manera similar $\Phi((T+1)M) = \Phi(T+1)\Phi(M) = \Phi(M)$ pues $q = 2$. Entonces

$$(R_T/\langle TM\rangle)^* \cong (R_T/\langle (T+1)M\rangle)^* \equiv (R_T/\langle M\rangle)^*.$$

En particular cuando $M = 1$, note que, para $q = 2$ no hay caracter de conductor $T,\ T+1,\ T(T+1)$.

Ejemplo 3.3.7. Sea $q = 2$ y sea $\chi : (R_T/\langle T^3\rangle)^* \longrightarrow \mathbb{C}^*$ dado por

$$\begin{aligned} 1 &\longmapsto 1, \\ T+1 &\longmapsto -1, \\ T^2+1 &\longmapsto 1, \\ T^2+T+1 &\longmapsto -1. \end{aligned}$$

Note que $\chi(T^2+A) = \chi(T^2)$, esto para todo $A \in (R_T/\langle T^3\rangle)^*$. Entonces χ puede definirse módulo T^2 ya que, si $\xi : (R_T/\langle T^2\rangle)^* \longrightarrow \mathbb{C}^*$ dado por $\xi(1) = 1$ y $\xi(T+1) = -1$, sea $\varphi_{T^3,T^2} : (R_T/\langle T^3\rangle)^* \longrightarrow (R_T/\langle T^2\rangle)^*$, entonces

$$\varphi_{T^3,T^2}(1) = \varphi_{T^3,T^2}(T^2+1) = 1$$

$$y$$

$$\varphi_{T^3,T^2}(T+1) = \varphi_{T^3,T^2}(T^2+T+1) = T+1.$$

Se sigue que $\xi \circ \varphi_{T^3,T^2} = \chi$. Por la Observación 3.3.6 se tiene que $F_\chi = T^2$.

Observación 3.3.8. Dado un caracter de Dirichlet χ se puede considerar $\chi : R_T \longrightarrow \mathbb{C}$ definiendo $\chi(Q) = 0$ si $\text{mcd}(Q, F_\chi) \neq 1$. En caso de no especificarse, siempre se considera a un caracter χ definido módulo su conductor F_χ.

Definición 3.3.9. Un caracter de Dirichlet χ definido módulo su conductor se llama *primitivo*. En este caso se hace $\chi(Q) = 0$ tan poco como sea posible.

También se tiene que cuando χ está definido módulo su conductor, $\chi(A + F_\chi) = \chi(A)$, esto es, χ es periódico de período F_χ.

Notación. Siempre que se consideren los caracteres de $(R_T/\langle M\rangle)^*$, $M \in R_T$ o caracteres módulo M se incluirán todos aquellos caracteres cuyos conductores dividan a M. El caracter trivial ε satisface $\varepsilon(Q) = 1$ para todo $Q \in R_T$.

Si G es cualquier grupo, $\widehat{G}$ denota el conjunto de sus caracteres:

$$\widehat{G} := \text{Hom}(G, \mathbb{C}^*) = \{\chi : G \longrightarrow \mathbb{C}^* \mid \chi \text{ es homomorfismo de grupos}\}.$$

Definición 3.3.10. Se dice que un caracter es *par* si $\theta(a) = 1$ para todo $a \in \mathbb{F}_q^*$.

Proposición 3.3.11. *Sea* $X := \{\theta \in \widehat{(R_T/\langle N\rangle)^*} \mid \theta \text{ es par}\}$. *Entonces* X *es subgrupo de* $\widehat{(R_T/\langle N\rangle)^*}$ *de orden* $\frac{\Phi(N)}{q-1}$.

Demostración. Se tiene la sucesión exacta

$$0 \longrightarrow \mathbb{F}_q^* \longrightarrow (R_T/\langle N\rangle)^*.$$

Al tomar duales se obtiene la sucesión exacta

$$(\widehat{R_T/\langle N\rangle})^* \xrightarrow{\mathfrak{X}} \mathbb{F}_q^* \longrightarrow 0.$$

tal que $\mathfrak{X}(\theta) = \theta|_{\mathbb{F}_q^*}$. Por lo tanto $X = \ker \mathfrak{X}$ y así $(\widehat{R_T/\langle N\rangle})^*/X \cong \mathbb{F}_q^*$, de aquí se sigue que

$$|X| = \frac{|(\widehat{R_T/\langle N\rangle})^*|}{|\mathbb{F}_q^*|} = \frac{|(R_T/\langle N\rangle)^*|}{|\mathbb{F}_q^*|} = \frac{\Phi(N)}{q-1}.$$

□

Definición 3.3.12. Sean χ, ϕ dos caracteres de Dirichlet de conductores F_χ y F_ϕ respectivamente. Se define el producto de χ y ϕ de la siguiente manera. Sea $Q := \text{mcm}[F_\chi, F_\phi]$ y se define $\gamma : (R_T/\langle Q\rangle)^* \longrightarrow \mathbb{C}^*$ por $\gamma(A \bmod Q) = \chi(A \bmod Q)\phi(A \bmod Q)$. Entonces el *producto* $\chi\phi$ se define como el caracter primitivo asociado a γ. En particular $F_{\chi\phi}|\text{mcm}[F_\chi, F_\phi]$.

Teorema 3.3.13. *Si* $\text{mcd}(F_\chi, F_\phi) = 1$ *entonces* $F_{\chi\phi} = F_\chi F_\phi$.

Demostración. Sean $N = F_\chi$ y $M = F_\phi$, $S := \text{mcm}[N, M] = NM$. Se define $\gamma : (R_T/\langle S\rangle)^* \longrightarrow \mathbb{C}^*$ dada por $\gamma(A \bmod S) = \chi(A \bmod S)\phi(A \bmod S)$. Observe que $\text{mcm}[S, N] = \text{mcm}[\text{mcm}[N, M], N] = NM = S$, es posible definir $\theta : (R_T/\langle S\rangle)^* \longrightarrow \mathbb{C}^*$ por $\theta(A \bmod S) = \gamma(A \bmod S)\chi^{-1}(A \bmod S)$. Se obtiene $\theta = \phi \bmod S$ lo que implica que $F_\theta = F_\phi = M$. Por lo tanto $M = F_\theta = F_{\gamma\chi^{-1}}|\text{mcm}[F_\gamma, F_{\chi^{-1}}]$. Es decir $M|\text{mcm}[F_\gamma, F_{\chi^{-1}}] = \text{mcm}[F_\gamma, F_\theta] = \frac{F_\gamma N}{\text{mcd}(F_\gamma, N)} = FN_1$ donde $N_1 = \frac{N}{\text{mcd}(F_\gamma, N)}$. Puesto que $\text{mcd}(N, M) = 1$ se sigue que $\text{mcd}(N_1, M) = 1$ y así $M|F_\gamma$. Análogamente $N|F_\gamma$ y puesto que $\text{mcd}(N, M) = 1$ se tiene $NM|F_\gamma$. Por otra parte $F_\gamma = F_{\chi\phi}|\text{mcm}[F_\chi, F_\phi] = \text{mcm}[N, M] = NM$. Se tiene entonces que $F_\gamma = NM = F_\chi F_\phi$. □

Proposición 3.3.14. *Sean* χ, σ *dos caracteres de Dirichlet de conductores* F_χ *y* F_σ *respectivamente. Supóngase que existe* N *tal que* $F_\chi|N$, $F_\sigma|N$ *y* $\chi, \sigma : (R_T/\langle N\rangle)^* \longrightarrow \mathbb{C}^*$ *son iguales módulo* N*, es decir,* $\chi(A \bmod N) = \sigma(A \bmod N)$ *para todo* A *primo relativo a* N*. Entonces* $F_\chi = F_\sigma$ *y* $\chi = \sigma \bmod F_\chi$*, esto es,* $\chi = \sigma$*.*

Demostración. Ver [19, Proposición 9.4.17]. □

Definición 3.3.15. Si χ es un caracter de Dirichlet, se define el *conjugado* $\overline{\chi}$ de χ por $\overline{\chi}(A) = \overline{\chi(A)}$. Note que $\overline{\chi}(A) = \chi(A)^{-1}$ para todo A tal que $\text{mcd}(A, F_\chi) = 1$. Por lo tanto $\chi\overline{\chi}$ es el caracter trivial y $F_{\overline{\chi}} = F_\chi$.

Observación 3.3.16. Se tiene $G_M = \text{Gal}(k(\Lambda_M)/k) \cong (R_T/\langle M\rangle)^*$. Entonces un caracter de Dirichlet módulo M es un caracter de G_M, por lo cual un caracter de Dirichlet puede ser considerado un caracter de Galois.

Definición 3.3.17. Sea χ un caracter de Dirichlet módulo M, esto es, $\chi \in \widehat{G_M} \cong (\widehat{R_T/\langle M\rangle})^*$. Entonces $\ker\chi \subseteq G_M$. Sea $k_\chi := k(\Lambda_M)^{\ker\chi}$. El campo k_χ se llama el *campo que pertenece* a χ o que k_χ está *asociado* a χ.

Ejemplo 3.3.18. Sea $q = 2$ y sea $\chi : (R_T/\langle T^3\rangle)^* \longrightarrow \mathbb{C}^*$ como en el Ejemplo 3.3.7. Entonces

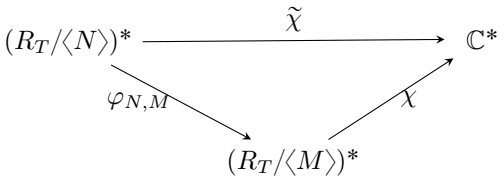
$$\chi : (R_T/\langle T^3\rangle)^* \cong G_{T^3} = \mathrm{Gal}(k(\Lambda_{T^3})/k) \longrightarrow \mathbb{C}^*$$

y

$$\ker\ \chi = \{1 \text{ mód } T^3,\ (T^2+1) \text{ mód } T^3\}.$$

Por lo tanto χ es un caracter de $(R_T/\langle T^3\rangle)^*/\ker\ \chi \cong (R_T/\langle T^2\rangle)^* \cong \mathrm{Gal}(k(\Lambda_{T^2})/k)$ y puede ser considerado como un caracter de $\mathrm{Gal}(k(\Lambda_{T^2})/k)$.

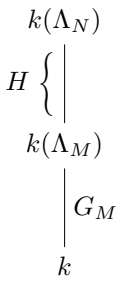
Observación 3.3.19. Sea χ un caracter de Dirichlet definido módulo M y sea $N \in R_T\backslash\{0\}$ múltiplo de M. Sea $\widetilde{\chi}$ el caracter χ definido módulo N, se tiene pues



donde $\widetilde{\chi} = \chi \circ \varphi_{N,M}$. Sean $k_1 = k(\Lambda_M)^{\ker \chi}$ y $k_2 = k(\Lambda_N)^{\ker \widetilde{\chi}}$. Entonces

$$\ker \varphi_{N,M} = D_{N,M} = \{A \text{ mód } N \mid A \equiv 1 \text{ mód } M\}.$$

Observe que $(R_T/\langle N\rangle)^*/\ker \varphi_{N,M} \cong (R_T/\langle M\rangle)^*$ y también se tiene que $G_N \cong (R_T/\langle N\rangle)^*$ y $G_M \cong (R_T/\langle M\rangle)^*$. Sea $H = \mathrm{Gal}(k(\Lambda_N)/k(\Lambda_M))$



Entonces $k(\Lambda_M) = k(\Lambda_N)^H$ y $\ker \varphi_{N,M} \cong \mathrm{Gal}(k(\Lambda_N)/k(\Lambda_M)) \cong H$.

Se tiene que, $\ker \widetilde{\chi} = \varphi_{N,M}^{-1}(\ker \chi)$ y como $\varphi_{N,M}^{-1}(\ker \chi) \supseteq \varphi_{N,M}^{-1}(\{1\}) = \ker \varphi_{N,M}$ se sigue que

$$k_2 = k(\Lambda_N)^{\ker \widetilde{\chi}} \subseteq k(\Lambda_N)^{\ker \varphi_{N,M}} = k(\Lambda_M).$$

Por lo tanto se tiene que

$$k_2 \subseteq k(\Lambda_M)^{\ker \chi} = k_1.$$

Note que

$$\begin{aligned}|\ker\widetilde{\chi}| &= |\varphi_{N,M}^{-1}(\ker\chi)| = |\ker\varphi_{N,M}||\ker\chi| = [k(\Lambda_N):k(\Lambda_M)][k(\Lambda_M):k_1]\\ &= [k(\Lambda_N):k_1]\end{aligned}$$

y dado que $|\ker\widetilde{\chi}| = [k(\Lambda_N):k_2]$. Se concluye que $k_2 = k_1$.

De la observación anterior se deduce que dado cualquier caracter de Dirichlet χ definido módulo M, sin importar su conductor, el campo $k_{\chi,M} = k(\Lambda_M)^{\ker\chi}$ depende únicamente de χ y no de M.

Definición 3.3.20. Sea X cualquier grupo de caracteres de Dirichlet. Sea M el mínimo común múltiplo de $\{F_\chi \mid \chi \in X\}$. Entonces X es un subgrupo de $\widehat{G_M}$. Sean $H = \bigcap_{\chi\in X}\ker\chi$ y $k_X := k(\Lambda_M)^H$. Entonces k_X se le llama *el campo que pertenece a X o campo asociado a X.*

Observación 3.3.21. Sea $k \subseteq L \subseteq k(\Lambda_M)$ y sea X el grupo de caracteres de Dirichlet asociado a L. Entonces $L = k(\Lambda_M)^H \subseteq k(\Lambda_M)^+ = k(\Lambda_M)^{\mathbb{F}_q^*}$, donde $H = \bigcap_{\chi\in X}\ker\chi$, si y sólo si $\mathbb{F}_q^* \subseteq H$ si y sólo si $\chi(a) = 1$ para todo $\chi \in X$ y para todo $a \in \mathbb{F}_q^*$.

Se tiene en general que, dado un grupo de caracteres de Dirichlet asociado a un campo $L \subseteq k(\Lambda_M)$, el grupo de caracteres de Dirichlet asociado a $L^+ = L \cap k(\Lambda_M)^+$ corresponde a $X^+ = X \cap \{\chi \in \widehat{(R_T/\langle M\rangle)}^* \mid \chi(a) = 1\ \forall\ a \in \mathbb{F}_q^*\}$, es decir

$$X^+ := \{\chi \in X \mid \chi(a) = 1\ \forall\ a \in \mathbb{F}_q^*\}.$$

En particular se tiene que un caracter χ es par si y sólo si $\mathfrak{p}_\infty$ de descompone totalmente en k_χ/k.

Se tiene que si X es cíclico, $X = \langle\chi\rangle$, entonces $k_X = k_{\langle\chi\rangle}$.

Observación 3.3.22. Con las notaciones anteriores, se tiene que $H < G_M$ y que $G_M/H \cong \mathrm{Gal}(k_X/k)$. De la teoría general de caracteres, se tiene que $H^\perp \cong \widehat{(G_M/H)} \cong \widehat{\mathrm{Gal}(k_X/k)}$. Dado que G_M es abeliano, $H^\perp \cong \mathrm{Gal}(k_X/k)$.

Teorema 3.3.23. *Existe una correspondencia biyectiva entre $\mathcal{A} = \{Y \mid Y < X\}$ y $\mathcal{B} = \{L \mid L \subseteq k_X\}$ dada por*

$$\begin{aligned}\mathcal{A} &\longleftrightarrow \mathcal{B}\\ Y &\longrightarrow L_Y = k_X^{Y^\perp}\end{aligned}$$

es decir

$$\widehat{\mathrm{Gal}(L/k)} \cong \mathrm{Gal}(k_X/L)^\perp = Y_L \longleftarrow L$$

En particular se tiene una correspondencia uno a uno entre todos los subgrupos de caracteres de Dirichlet y subcampos de campos de funciones ciclotómicos.

Demostración. Ver [19, página 195]. □

Proposición 3.3.24. *Sean X_1, X_2 dos subgrupos de caracteres de Dirichlet y sean $k_i = k_{X_i}$ para $i = 1, 2$, los campos pertenecientes a cada X_i. Entonces*

(1) $X_1 \subseteq X_2$ si y solamente si $k_1 \subseteq k_2$.

(2) $k_{\langle X_1, X_2 \rangle} = k_1 k_2$.

(3) $k_{X_1 \cap X_2} = k_1 \cap k_2$.

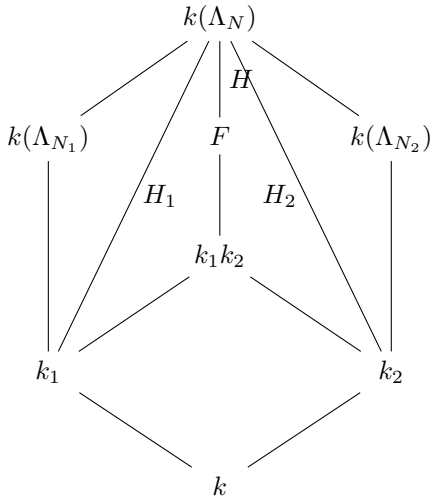
Demostración. Sean $X = \langle X_1, X_2 \rangle$ y sea F el campo correspondiente a X. Sean

$$N := \operatorname{mcm} \{F_\chi \mid \chi \in X\} \qquad N_i := \operatorname{mcm} \{F_\chi \mid \chi \in X_i\} \quad i = 1, 2$$

Entonces $N_i | N$, para $i = 1, 2$. Se denota por

$$H_1 = \bigcap_{\chi \in X_1} \ker \chi, \qquad H_2 = \bigcap_{\chi \in X_2} \ker \chi, \qquad H = \bigcap_{\chi \in X} \ker \chi$$

$$k_1 = k(\Lambda_N)^{H_1}, \qquad k_2 = k(\Lambda_N)^{H_2}.$$



Se tiene que, si $X_1 \subseteq X_2$ entonces $H_2 \subseteq H_1$ y por lo tanto $k(\Lambda_N)^{H_1} \subseteq k(\Lambda_N)^{H_2}$ es decir $k_1 \subseteq k_2$.

Recíprocamente, si $k_1 \subseteq k_2$, entonces $k_1 = k(\Lambda_N)^{H_1} \subseteq k(\Lambda_N)^{H_2} = k_2$ de esta manera se tiene que $H_1 = \operatorname{Gal}(k(\Lambda_N)/k(\Lambda_N)^{H_1}) \supseteq \operatorname{Gal}(k(\Lambda_N)/k(\Lambda_N)^{H_2}) = H_2$. Se probará que $H_1 \supseteq H_2 \iff X_1 \subseteq X_2$ y con esto se tendrá (1).

Del mapeo bilineal $\varphi : \operatorname{Gal}(F/k) \times X \to \mathbb{C}^*$, $\varphi(\sigma, \chi) = \chi(\sigma)$ se obtiene

$$\begin{aligned} X_i^\perp &= \{g \in \operatorname{Gal}(F/k) \mid \chi(g) = 1 \ \forall \ \chi \in X_i\} = \{g \in \operatorname{Gal}(F/k) \mid g \in \ker \chi \ \forall \ \chi \in X_i\} \\ &= \bigcap_{\chi \in X_i} \ker \chi = H_i, \qquad i = 1, 2. \end{aligned}$$

Se tiene pues, $H_i = X_i^{\perp}$. Por lo tanto, si $H_1 \supseteq H_2$, entonces $X_1^{\perp} \supseteq X_2^{\perp}$ lo cual implica que $X_1 \subseteq X_2$, y se tiene (1).

Para probar (2), sea F el campo asociado a $X_1 \cap X_2$, dado que $X_1 \cap X_2 \subseteq X_i$, $i = 1, 2$ se sigue de (1) que $F \subseteq k_1 \cap k_2$. Sea ahora W el grupo de caracteres de Dirichlet asociado a $k_1 \cap k_2$, nuevamente por (1) se sigue que $W \subseteq X_i$, $i = 1, 2$, así que $W \subseteq X_1 \cap X_2$ y por lo anterior se concluye $k_1 \cap k_2 \subseteq F$. Se tiene (2).

Para probar (3) note que, por teoría de Galois se tiene $k_1 k_2 = k(\Lambda_N)^{H_1} k(\Lambda_N)^{H_2} = k(\Lambda_N)^{H_1 \cap H_2}$ y $H_1 \cap H_2 = X_1^{\perp} \cap X_2^{\perp}$. Para concluir la prueba, sólo falta ver que $(X_1 \cup X_2)^{\perp} = \langle X_1, X_2 \rangle^{\perp}$. En efecto, $(X_1 \cup X_2)^{\perp} = \{\sigma \in G \mid \chi(\sigma) = 1 \ \forall \ \sigma \in X_1 \cup X_2\}$, por lo que $\chi(\sigma) = 1$ para todo $\sigma \in \langle X_1, X_2 \rangle$ lo cual prueba que $(X_1 \cup X_2)^{\perp} \subseteq \langle X_1, X_2 \rangle^{\perp}$.

Para la otra contención. Si $\sigma \in \langle X_1, X_2 \rangle^{\perp}$ entonces $\chi(\sigma) = 1$ para todo $\chi \in \langle X_1, X_2 \rangle$ y por tanto $\chi(\sigma) = 1$ para todo $\chi \in X_1 \cup X_2$. Se sigue así $\langle X_1, X_2 \rangle^{\perp} \subseteq (X_1 \cup X_2)^{\perp}$ y se tiene la igualdad.

Dado que $X_i \subseteq X_1 \cup X_2$ se tiene $X_i^{\perp} \supseteq (X_1 \cup X_2)^{\perp}$. Así que $X_1^{\perp} \cap X_2^{\perp} \supseteq (X_1 \cup X_2)^{\perp}$. Recíprocamente, si $\sigma \in X_1^{\perp} \cap X_2^{\perp}$ entonces $\chi_1(\sigma) = 1$ y $\chi_2(\sigma) = 1$ para cualesquiera $\chi_i \in X_i$ $i = 1, 2$. Por lo tanto $\chi(\sigma) = 1$ para todo $\chi \in X_1 \cup X_2$ y en particular $\sigma \in (X_1 \cup X_2)^{\perp}$. Esto prueba que $X_1^{\perp} \cap X_2^{\perp} = (X_1 \cup X_2)^{\perp}$.

Para concluir notemos que ya se demostró que $H_1 \cap H_2 = X_1^{\perp} \cap X_2^{\perp} = (X_1 \cup X_2)^{\perp} = \langle X_1, X_2 \rangle^{\perp} = X^{\perp}$, de donde se sigue que $k_1 k_2$ corresponde a $X = \langle X_1, X_2 \rangle$. □

Proposición 3.3.25. *Sean A un grupo abeliano finito y $B < A$. Entonces A contiene un subgrupo isomorfo a A/B y viceversa.*

Demostración. Directamente de la estructura de grupos abelianos finitamente generados o bien $A/B \cong \widehat{A/B} \cong B^{\perp} \subseteq A^{\perp} \cong A$. □

3.3.1. Aritmética en campos de funciones ciclotómicos usando caracteres de Dirichlet

Se darán algunas aplicaciones de los caracteres de Dirichlet para el estudio de campos de funciones ciclotómicos.

Sea $M \in R_T \backslash \{0\}$ mónico tal que $M = \prod_{i=1}^{r} P_i^{\alpha_i}$ es su descomposición como producto de polinomios irreducibles, por lo que

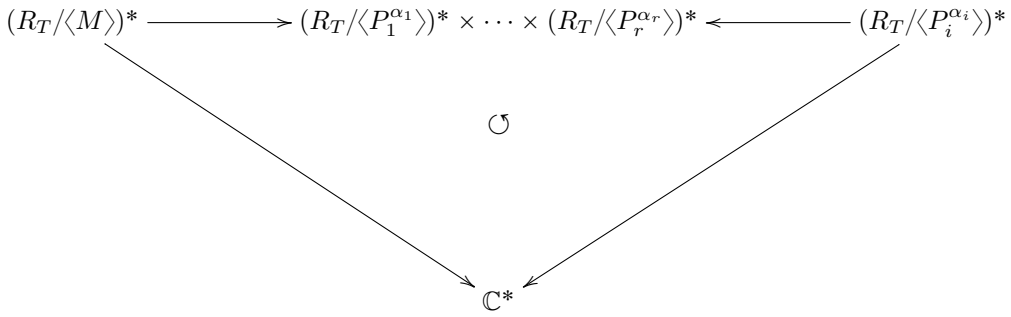
$$(R_T/\langle M \rangle)^* \cong \prod_{i=1}^{r} (R_T/\langle P_i^{\alpha_i} \rangle)^*, \tag{3.1}$$

con el isomorfismo φ descrito más adelante. Si χ es un caracter de Dirichlet módulo M, por lo que, de acuerdo a (3.1), se tiene $\chi = \prod_{i=1}^{r} \chi_{P_i}$, donde χ_{P_i} es un caracter módulo $P_i^{\alpha_i}$, esto es:

$$\chi(A \bmod M) = \prod_{i=1}^{r} \chi_{P_i}(A \bmod P_i^{\alpha_i}),$$

donde $\chi_{P_i} = \chi \circ \varphi^{-1} \circ g_{P_i}$ y $g_{P_i} : (R_T/\langle P_i^{\alpha_i}\rangle)^* \longrightarrow \prod_{j=1}^{r}(R_T/\langle P_j^{\alpha_j}\rangle)^*$, está dado por $g_{P_i}(A) = (1, \ldots, 1, A, 1, \ldots, 1)$.

El isomorfismo $\varphi : (R_T/\langle M\rangle)^* \longrightarrow \prod_{j=1}^{r}(R_T/\langle P_j^{\alpha_j}\rangle)^*$ está dado por el Teorema Chino del Residuo.

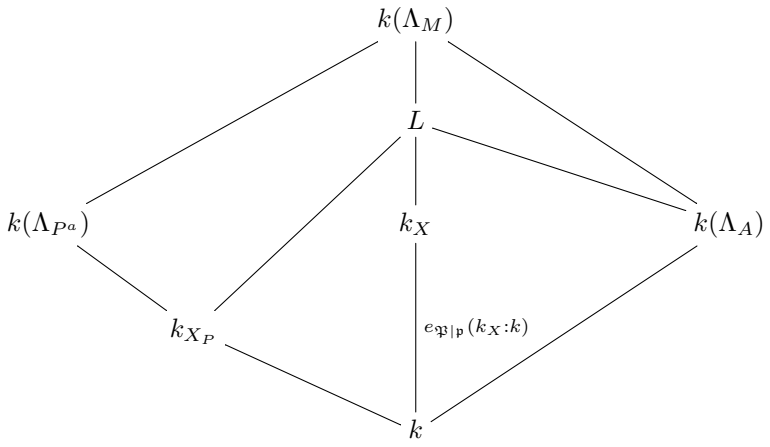


Definición 3.3.26. Sea X un grupo finito de caracteres. Entonces para un polinomio mónico e irreducible $P \in R_T$ se define $X_P := \{\chi_P \mid \chi \in X\}$.

Como se ha mencionado anteriormente, las similitudes entre campos de funciones ciclotómicos y campos numéricos son bastantes y una herramienta que tienen en común son los caracteres de Dirichlet para el estudio de extensiones abelianas.

Teorema 3.3.27. *Sean X un grupo finito de caracteres de Dirichlet y k_X su campo asociado. Sea $P \in R_T\backslash\{0\}$ un polinomio irreducible y sea $(P)_k = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\mathrm{gr}P}}$. Sea $\mathfrak{P}$ un divisor primo de k_X sobre $\mathfrak{p}$ y sea $e := e_{\mathfrak{P}|\mathfrak{p}}(k_X : k)$. Entonces $e = |X_P|$.*

Demostración. Sea M el mínimo común múltiplo de $\{F_\chi \mid \chi \in X\}$. Entonces $k_X \subseteq k(\Lambda_M)$. Ahora sea $M = P^a A$ donde $A \in R_T$ y P no divide a A. Sea $L = k_X(\Lambda_A) = k_X k(\Lambda_A)$. Considérese el siguiente diagrama



Por la Proposición 3.3.22 se tiene $L = k_X k(\Lambda_A) = k_X k_{\widehat{G_A}} = k_{\langle \widehat{X, G_A}\rangle}$.

Así que L es el campo asociado al grupo generado por X y $\widehat{G_A}$, esto es, el grupo de caracteres de L está generado por X y por los caracteres de Dirichlet de G_M cuyo conductor es primo relativo a P. Por tanto, se tiene que $\langle X, \widehat{G_A}\rangle \cong X_P \times \widehat{G_A}$ así que $\mathfrak{p}$ es no ramificado en $k(\Lambda_A)/k$, por lo que índice de ramificación de $\mathfrak{p}$ en k_X/k es el mismo que el de L/k. Por otro lado, se tiene L/k_{X_P} es no ramificado en los divisores primos que están encima de $\mathfrak{p}$ y, por el Teorema 3.1.23 (4), se tiene que $\mathfrak{p}$ es totalmente ramificado en k_{X_P}/k. Se concluye que

$$e = [k_X : k] = [k_{X_P} : k] = |X_P|.$$

□

Corolario 3.3.28. *Sea χ un caracter de Dirichlet. Entonces $\mathfrak{p}$ se ramifica en k_χ/k si y sólo si $\chi(P) = 0$ o, equivalentemente, P divide a F_χ. Si X es cualquier grupo finito de caracteres de Dirichlet, entonces P es no ramificado en k_X/k si y sólo si $\chi(P) \neq 0$ para todo $\chi \in X$.*

Demostración. Ver [19, Corolario 9.5.7]. □

Al igual que en el caso numérico se tiene que los grupos de inercia y descomposición están relacionados con los caracteres de Dirichlet. Se tiene el siguiente resultado:

Teorema 3.3.29. *Sea X un grupo finito de caracteres de Dirichlet y sea k_X su campo asociado. Sean $P \in R_T$, $Y = \{\chi \in X \mid \chi(P) \neq 0\}$ y $Z = \{\chi \in X \mid \chi(P) = 1\}$. Si $(P)_k = \frac{\mathfrak{p}}{\mathfrak{p}_\infty^{\mathrm{gr}P}}$, se considera $\mathfrak{P}$ un divisor primo de k_X sobre $\mathfrak{p}$. Entonces*

$$X/Y \cong \widehat{I(\mathfrak{P}|\mathfrak{p})} \cong I(\mathfrak{P}|\mathfrak{p}) \quad y \quad X/Z \cong \widehat{D(\mathfrak{P}|\mathfrak{p})} \cong D(\mathfrak{P}|\mathfrak{p})$$

En particular, $e = e_{\mathfrak{P}|\mathfrak{p}}(k_X : k) = [X : Y]$, $f = d_{\mathfrak{P}|\mathfrak{p}}(k_X : k) = [Y : Z]$ y $h = [Z : 1] = |Z|$ donde h es el número de divisores primos en k_X sobre $\mathfrak{p}$. Finalmente, el grupo Y/Z es cíclico de orden f.

Demostración. Sea L el subcampo de k_X que corresponde a Y. Por el Corolario 3.3.28 se tiene que L es el máximo subcampo de k_X en donde $\mathfrak{p}$ es no ramificado. Por lo tanto L es el subcampo dejado fijo por el grupo de inercia $I(\mathfrak{P}|\mathfrak{p})$.

$$\begin{array}{c} k_X \\ \Big| \Big\}_{I(\mathfrak{P}|\mathfrak{p})=\mathrm{Gal}(k_X/L)} \\ L \\ \Big| \ \mathfrak{p} \text{ no ramificado} \\ k \end{array}$$

Se tiene que $L = k_X^{Y^\perp}$, $Y = \mathrm{Gal}(k_X/L)^\perp$. Por lo tanto $I(\mathfrak{P}|\mathfrak{p}) \cong Y^\perp \cong \widehat{(X/Y)}$, de esta manera se tiene que $X/Y \cong \widehat{\mathrm{Gal}(k_X/L)} = \widehat{I(\mathfrak{P}|\mathfrak{p})}$. En particular se tiene $e = |I(\mathfrak{P}|\mathfrak{p})| = |\widehat{I(\mathfrak{P}|\mathfrak{p})}| = |X/Y| =$

$[X : Y]$. Ahora bien, $Y \cong \widehat{\mathrm{Gal}(L/k)}$. Sea $M := \mathrm{mcm}\{F_\chi \mid \chi \in Y\}$. Dado que $\mathfrak{p}$ es no ramificado en L, $\mathfrak{p} \nmid F_\chi$, para todo $\chi \in Y$ y por lo tanto $\mathfrak{p} \nmid M$.

Ahora, se tiene $L \subseteq k(\Lambda_M)$. El automorfismo de Frobenius φ_P en $k(\Lambda_M)$ es el que corresponde a $\varphi_P(\lambda_M) = \lambda_M^P$, donde λ_M es un generador de Λ_M. Por lo tanto el automorfismo de Frobenius de $\mathfrak{p}$ en L es:

$$\varphi_P \text{ mód } \mathrm{Gal}(k(\Lambda_M)/L) = \overline{\varphi_P} = \varphi_P \text{ mód } H,$$

donde $H := \mathrm{Gal}(k(\Lambda_M)/L)$.

Con la identificación $\mathrm{Gal}(k(\Lambda_M)/L) \cong H$, se sigue que $\overline{\varphi_P} = P$ mód H donde se considera $H \subseteq (R_T/\langle M\rangle)^*$. Si $\chi \in Y$, entonces $\chi(\mathrm{Gal}(k(\Lambda_M)/L)) = 1$, es decir, $\chi(H) = 1$, de otra forma $H \subseteq \ker\chi$. Se sigue que $\chi(\overline{\varphi_P}) = \chi(\varphi_P)$ y por tanto $\chi(\overline{\varphi_P}) = 1 \iff \chi(P) = 1$.

De lo anterior se obtiene que:

$$\langle\overline{\varphi_P}\rangle^\perp = \{\chi \in Y \mid \chi(P) = 1\} = Z$$

en el mapeo bilineal

$$\mathrm{Gal}(L/k) \times Y \to \mathbb{C}^*.$$

Ahora bien,$\langle\overline{\varphi_P}\rangle$ es un grupo cíclico de orden f generado por $\overline{\varphi}_P$. Se sigue que

$$\frac{\widehat{\mathrm{Gal}(L/k)}}{\langle\overline{\varphi_P}\rangle^\perp} = \frac{Y}{\langle\overline{\varphi_P}\rangle^\perp} \cong \frac{Y}{Z} \cong \widehat{\langle\overline{\varphi_P}\rangle} \cong \langle\overline{\varphi_P}\rangle.$$

Por lo tanto se tiene el siguiente diagrama:

$$\begin{array}{l} k_X \\ \Big| \Big\} X/Y \to e \to \text{ grupo de inercia} \\ L \\ \Big| \Big\} Y/Z \to f \text{ inercia} \\ E = L^{\langle\overline{\varphi_P}\rangle} \\ \Big| \Big\} Z \to g \text{ descomposición} \\ k \end{array}$$

El campo fijo del automorfismo de Frobenius $E = L^{\overline{\langle\varphi_P\rangle}}$ corresponde al campo de descomposición de P. Por lo tanto E corresponde a Z y $g = [E : k] = |Z|$ o simplemente,

$$efg = [k_X : k] = |X| = [X : Y][Y : Z][Z : 1] = ef[Z : 1],$$

por lo tanto $g = [Z : 1] = [Z]$. Se sigue que $X/Z \cong \widehat{D(\mathfrak{P}|\mathfrak{p})}$. □

Ejemplo 3.3.30. Sea $q = 2$ y sea χ mód $T^2(T^2+1)$ dado por

$$\chi(1) = 1, \quad \chi(T^2+T+1) = 1, \quad \chi(T^3+T^2+1) = -1, \quad \chi(T^3+T+1) = -1.$$

El conductor de χ satisface que $F_\chi \in \{1, T^2, T^2+1, T^2(T^2+1)\}$. Al tener dos elementos tales que $\chi(T^3+T^2+1) = -1 = \chi(T^3+T+1)$ se tiene $F_\chi \neq 1$.

Como $T^3+T^2+1 \bmod T^2 = 1$ y dado que $\chi(T^3+T^2+1) = -1$ y de manera similar, T^3+T^2+1 mód $T^2+1 = 1$ pero $\chi(T^3+T^2+1) = -1$, se sigue que el conductor F_χ no puede ser ni T^2 ni T^2+1. Por tanto $F_\chi = T^2(T^2+1)$.

Sea ahora φ definido mód T^2 por $\varphi(1) = 1$, $\varphi(1+T) = -1$. Por lo tanto el conductor de φ corresponde a $F_\varphi = T^2$. Sea $\phi := \chi\varphi$, donde ϕ está definido módulo T^2+1. Dado que $\chi = (\chi\varphi)\varphi^{-1} = \phi\varphi^{-1}$, y ϕ está definido módulo T^2+1 de tal forma que estos caracteres de Dirichlet están definidos módulo su conductor, esto es, $\chi_{T^2} = \varphi^{-1} = \varphi$ y $\chi_{T^2+1} = \phi$.

Sea Φ la función Fi de Euler. Se tiene $\Phi(T^2) = \Phi(T^2+1) = q^{dn} - q^{d(n-1)} = 2^{1(2)} - 2^{1(1)} = 4-2 = 2$. Entonces, las extensiones son de grado 2, esto es, $[k(\Lambda_{T^2}) : k] = 2 = [k(\Lambda_{T^2+1}) : k]$. De la acción de Carlitz se tiene

$$u^{T^2} = \sum_{i=0}^{2} \begin{bmatrix} T^2 \\ i \end{bmatrix} u^{q^i} = T^2u + \begin{bmatrix} T^2 \\ 1 \end{bmatrix} u^q + uq^2,$$

donde

$$\begin{bmatrix} T^2 \\ 1 \end{bmatrix} = T \begin{bmatrix} T \\ 1 \end{bmatrix} + \begin{bmatrix} T \\ 0 \end{bmatrix}^2 = T + T^q = T + T^2$$

pues $\begin{bmatrix} T \\ 1 \end{bmatrix} = 1$. Por lo tanto

$$u^{T^2} = T^2u + (T+T^2)u^2 + u^4$$

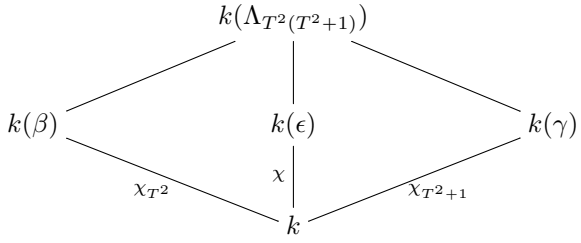
El polinomio ciclotómico es:

$$\Psi_{T^2}(u) = \frac{u^{T^2}}{u^T} = \frac{T^2 + (T+T^2)u^2 + u^4}{Tu+u^2} = u^2 + Tu + T,$$

donde cada raíz α de $\Psi_{T^2} = (u)$ es de la forma $(\frac{\alpha}{T})^2 + (\frac{\alpha}{T}) = -\frac{1}{T} = \frac{1}{T}$. Entonces, $k(\Lambda_{T^2}) = k(\beta)$ donde β es raíz de la extensión de Artin-Schreier que cumple $\beta^2 - \beta = \frac{1}{T}$.

Análogamente para $k(\Lambda_{T^2+1}) = k(\gamma)$ donde $\gamma^2 + \gamma = \frac{1}{T+1}$. Ahora, se tiene que $k_\chi = k(\epsilon)$ con

$\epsilon^2 - \epsilon = \frac{1}{T(T+1)}$, esto es:



Para finalizar se tiene que, en $k(\epsilon)/k$ los primos ramificados son T y $T+1$. En $k(\beta)/k$, T es el único primo ramificado y en $k(\gamma)/k$, el único primo ramificado es $T+1$.

A continuación se enuncia una proposición que está ligada a resolver el problema inverso de la teoría de Galois para el caso particular de un grupo abeliano. El teorema, así como su demostración, brinda información de cómo construir extensiones no ramificadas en ningún primo. Esto nos servirá más adelante cuando se esté calculando el campo de géneros de una extensión abeliana.

Proposición 3.3.31. *Sea $P \in R_T$ un polinomio irreducible mónico de grado d y sea $n = p^t$. Entonces $(R_T/\langle P^n\rangle)^*$ contiene un subgrupo cíclico de orden $p^t a$ para cualquier a que divide a $q^d - 1$.*

Demostración. Ver [19, Proposición 9.5.9]. □

Teorema 3.3.32. *Sea G un grupo abeliano finito. Entonces existen campos de funcione congruentes E y F tales que*

(I) $\mathrm{Gal}(F/E) \cong G$

(II) F/E es no ramificada en todos los divisores primos.

(III) F/k es abeliana y E/k es cíclica.

(IV) El campo de constantes, tanto de E como de F es $\mathbb{F}_q$.

Demostración. Sea $G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$. Sea $m_i = p^{t_i}a_i$ donde p y a_i primos relativos, p primo racional y $t_i \geqslant 0$ para $1 \leqslant i \leqslant r$. Sea $d_i' = \circ(p \bmod a_i)$, esto es, $p^{d_i'} \equiv 1 \bmod a_i$, donde d_i' es mínimo con esta propiedad. Es posible elegir $d_1 < d_2 < \cdots d_r$ con $d_i \in \mathbb{N}$ y cada $d_i'|d_i$.

Sea $P_i \in R_T$ un polinomio mónico e irreducible de grado d_i. Este polinomio existe pues si $\mathbb{F}_{q^{d_i}} = \mathbb{F}_q(\alpha_i)$ para algún α_i, entonces $P_i = \mathrm{Irr}(\alpha_i, T, \mathbb{F}_q)$ es de grado d_i y $\mathbb{F}_q(\alpha_i) \cong R_T/\langle P_i\rangle$, esto es, P_i resulta ser el polinomio irreducible de una extensión de grado d_i.

De la proposición anterior, se sigue que $(R_T/\langle P_i^{p^{t_i}}\rangle)^*$ contiene un elemento de orden $p^{t_i}a_i = m_i$. Dado el siguiente isomorfismo (no directo) $(R_T/\langle P_i^{p^{t_i}}\rangle)^* \cong \widehat{(R_T/\langle P_i^{p^{t_i}}\rangle)^*}$, existe un caracter $\chi_i \bmod P_i^{t_i}$ de orden m_i, esto es $\circ(\chi) = m_i$ y además el conductor del caracter χ_i, satisface $F_{\chi_i} = P_i^{s_i}$, donde $s_i \leqslant t_i$. Todo esto es para $1 \leqslant i \leqslant r$.

Sea P_{r+1} otro polinomio mónico e irreducible de grado $d_{r+1} > d_r$ tal que $a_1 \cdots a_r | q^{d_{r+1}} - 1$. Tal d_{r+1} existe pues $\text{mcd}(a_1, \ldots, a_r, q) = 1$.

Ahora, sea χ_{r+1} el caracter de Dirichlet definido módulo $P_{r+1}^{p^t}$ donde $t = t_1 + \cdots + t_r$ y de orden $m_{r+1} = p^t(q^{d_{r+1}} - 1)$. Entonces $m_1 \cdots m_r = a_1 \cdots a_r p^{t_1+\cdots+t_r} | m_{r+1}$.

Sea $\chi := \chi_1 \cdots \chi_r \chi_{r+1}$ y $E := k_X$ el campo asociado a $X ::= \langle \chi \rangle$. Sean $Y := \langle \chi_1, \ldots, \chi_r, \chi_{r+1} \rangle$ y $F := k_Y$ el campo asociado Y. Se tiene la siguiente torre de campos:

$$k \subseteq E = k_X \subseteq k_Y = F \subseteq k(\Lambda_M)$$

donde $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r} P_{r+1}^{\alpha_{r+1}}$ con $\alpha_i = p^{t_i}$ para $1 \leqslant i \leqslant r$ y $\alpha_{r+1} = p^t$. Por el Corolario 3.1.24 se tiene que el campo de constantes, tanto de E como de F es $\mathbb{F}_q$ esto prueba (IV) y puesto que Y es abeliano, se sigue F/k es una extensión abeliana.

Por otro lado, dado que $\text{Gal}(E/k) \cong X \cong \langle \chi \rangle$ el cual es un grupo cíclico, resulta ser que E/k es una extensión cíclica. Con esto se ha probado (III). Ahora bien, $Y = \langle \chi_1, \ldots, \chi_r, \chi_{r+1} \rangle = \langle \chi_1, \ldots, \chi_r, \chi \rangle$ y $\circ(\chi) = \circ(\chi_{r+1}) = m_{r+1}$ y puesto que $m_1 \cdots m_r | m_{r+1}$, se sigue que χ es de orden máximo en Y.

Por lo tanto $Y/X = Y/\langle \chi \rangle \cong \langle \chi_1, \ldots, \chi_r \rangle$ y

$$Y/X \cong \frac{\widehat{\text{Gal}(k_Y/k)}}{\widehat{\text{Gal}(k_X/k)}} \cong \frac{\widehat{\text{Gal}(k_Y/k)}}{\frac{\widehat{\text{Gal}(k_Y/k)}}{\widehat{\text{Gal}(k_Y/k_X)}}} \cong \widehat{\text{Gal}(k_Y/k_X)} \cong \widehat{\text{Gal}(F/E)} \cong \text{Gal}(F/E).$$

Por lo tanto $\text{Gal}(F/E) \cong \langle \chi_1, \ldots, \chi_r \rangle \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z} \cong G$, con esto se ha probado (I).

Para probar (II), como $(P_i)_k = \frac{\mathfrak{p}_i}{\mathfrak{p}_\infty^{\text{gr}P_i}}$, del Teorema 3.2.14 se tiene que los primos ramificados son $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{p}_{r+1}, \mathfrak{p}_\infty$. Note que $e_\infty(E : k) = e_\infty(F : k)$ pues E es el campo asociado a χ y dado que $q-1 | \circ(\chi)$ y por la Proposición anterior, se sigue que $(R_T/\langle P_{r+1}^{p^t} \rangle)$ contiene un único subgrupo de orden $q-1$, del Teorema 3.2.6 este subgrupo cíclico es el grupo de inercia de $\mathfrak{p}_\infty$. Por lo tanto $\mathfrak{p}_\infty$ es no ramificado en F/E. Para finalizar, observe que $Y_{P_i} = \langle \chi_i \rangle = X_{P_i}$. Por el Teorema 3.3.24 se tiene que el índice de ramificación de cada divisor primo de F sobre $\mathfrak{p}_i$ es $\frac{|Y_{P_i}|}{|X_{P_i}|} = 1$. Por lo tanto F/E es no ramificada en ningún primo. □

El problema a tratar en el presente trabajo, como se había mencionado, es calcular el campo de géneros de una l-extensión elemental abeliana, la cual se separa en dos casos, a saber, el caso Kummer y el caso no Kummer. Una ventaja del caso Kummer es que es posible tener una representación explícita de estos campos, es decir, extensiones radicales. A continuación, se presentan dos resultados los cuales dan las condiciones necesarias para que una extensión de Kummer esté contenida en un campo ciclotómico.

Proposición 3.3.33. *Para un polinomio $P \in R_T^+$ de grado d, se tiene que $k(\sqrt[n]{(-1)^d P}) \subseteq k(\Lambda_P)$, donde n es cualquier divisor de $q-1$.*

Demostración. Ver [19, Proposición 9.5.11]. □

Corolario 3.3.34. *Sea $D \in R_T$ un polinomio mónico. Entonces*

$$k(\sqrt[n]{(-1)^{\mathrm{gr}D} D}) \subseteq k(\Lambda_D)$$

para cualquier n tal que $n|q-1$.

En resumen, se considera una extensión de Kummer: $k(\sqrt[n]{\gamma D})/k$, donde $n|q-1$ y $D \in R_T$ y tal que $\mathrm{gr}D$ es libre de n-potencias. Entonces $k(\sqrt[n]{\gamma D}) \subseteq k(\Lambda_D)$ si y sólo si $\gamma \equiv (-1)^{\mathrm{gr}D}$ mód $(\mathbb{F}_q)^t$.

Proposición 3.3.35. *Sean L/k una extensión abeliana finita de campos de funciones globales, $P \in R_T^+$ y $d = \mathrm{gr}P$. Supóngase que P es moderadamente ramificado en L/k. Si e denota el índice de ramificación de P en L/k entonces $e|q^d - 1$, donde el campo de constantes de k es $\mathbb{F}_q$.*

Demostración. Ver [19, Proposición 10.4.8]. □

3.4. Campos de clases de Hilbert y campos de géneros

En esta sección se dan algunos resultados de la teoría de campos de clases, con el fin de hablar del campo de clases de Hilbert y del campo de géneros. En el caso de campos numéricos, si $[K : \mathbb{Q}] < \infty$, el *campo de clases de Hilbert* K_H de K se define como la máxima extensión abeliana de K no ramificada. Esto es, ningún primo finito o infinito de K se ramifica en K_H. De la teoría de campos de clases, se tiene que K_H/K es una extensión finita y que $\mathrm{Gal}(K_H/K)$ es isomorfo al grupo de clases de K.

El *campo de géneros* se define como la máxima extensión no ramificada K_{ge} de K tal que K_{ge} es la composición de K y una extensión abeliana k^* de $\mathbb{Q}$: $K_{ge} = Kk^*$. Esta definición fue dada por A. Fröhlich. Se tiene $K \subseteq K_{ge} \subseteq K_H$. El *campo de clases de Hilbert extendido* K_H^+ se define como la máxima extensión abeliana de K tal que los primos finitos no sean ramificados.

Ejemplo 3.4.1. (Teorema del Género de Gauss). Sea $K = \mathbb{Q}(\sqrt{d})$ una extensión cuadrática de $\mathbb{Q}$, donde $d \in \mathbb{Z}$ es libre de cuadrados. Sea m el número de factores primos distintos de δ_K, el discriminante de K. Sean $p_1, \ldots, p_m$ los primos distintos que dividen a δ_K, en caso de que $2|\delta_K$, se tendrá $p_1 = 2$.

Se denota por $\mathbb{P}_\mathbb{Q}$ al conjunto de números primos en $\mathbb{Q}$. Sea χ el caracter cuadrático asociado a K. Como los primos ramificados son los factores del discriminante de K, entonces $\chi_{p_i} \neq 1$ para $1 \leqslant i \leqslant m$, mientras que $\chi_q = 1$ para $q \in \mathbb{P}_\mathbb{Q} \backslash \{p_1, \ldots, p_m\}$. Para $p_i \neq 2$, χ_{p_i} es único con $\chi_{p_i}(-1) = (-1)^{(p_i-1)/2}$. Para este caso el campo asociado a χ_{p_i} es $\mathbb{Q}(\sqrt{(-1)^{(p_i-1)/2} p_i})$, ya que, éste es el subcampo dentro del campo ciclotómico $\mathbb{Q}(\zeta_{p_i})$. Para p_1 se tiene que, si $p_1 = 2$, entonces hay tres caracteres cuadráticos χ_2. Si $d \equiv 2$ mód 4, entonces $f_{\chi_2} = 8$ y χ_2 puede corresponder a $\mathbb{Q}(\sqrt{2})$ si $\chi_2(-1) = 1$, esto es, χ_2 es real o $\mathbb{Q}(\sqrt{-2})$ cuando $\chi_2(-1) = -1$, aquí χ_2 es imaginario. Si $d \equiv 3$ mód 4, entonces $f_{\chi_2} = 4$ y χ_2 corresponde a $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$, también χ_2 es imaginario

pues $\chi_2(-1) = -1$. Se sigue que la máxima extensión abeliana de $\mathbb{Q}$ que es no ramificada en ningún primo finito sobre K es:

$$J = \begin{cases} \mathbb{Q}\big(\sqrt{(-1)^{(p_1-1)/2}p_1}, \ldots, \sqrt{(-1)^{(p_m-1)/2}p_m}\big) & \text{si } p_1 \neq 2, \\ \mathbb{Q}\big(\sqrt{2}, \sqrt{(-1)^{(p_2-1)/2}p_2}, \ldots, \sqrt{(-1)^{(p_m-1)/2}p_m}\big) & \text{si } p_1 = 2,\ f_{\chi_2} = 8 \text{ y } \chi_2 \text{ es real} \\ \mathbb{Q}\big(\sqrt{-2}, \sqrt{(-1)^{(p_2-1)/2}p_2}, \ldots, \sqrt{(-1)^{(p_m-1)/2}p_m}\big) & \text{si } p_1 = 2,\ f_{\chi_2} = 8 \text{ y } \chi_2 \text{ es imaginario} \\ \mathbb{Q}\big(\sqrt{-1}, \sqrt{(-1)^{(p_2-1)/2}p_2}, \ldots, \sqrt{(-1)^{(p_m-1)/2}p_m}\big) & \text{si } p_1 = 2,\ f_{\chi_2} = 4 \end{cases}$$

Se tiene que $[J : \mathbb{Q}] = 2^m$ y que $[J : K] = 2^{m-1}$. Ahora $K_{ge} = J$ excepto en el caso de que K sea real y J imaginario y esto ocurre cuando $\delta_K > 0$ y existe $p_i \equiv 3$ mód 4. Aquí, en este último caso $K_{ge} = J^+ := J \cap \mathbb{R}$ con $[J^+ : K] = 2^{m-2}$

De aquí en adelante k denotará el campo global de funciones racionales, es decir, $k = \mathbb{F}_q(T)$. Se denota para cualquier campo de funciones congruente K la extensión de constantes de grado m como: $K_m = K\mathbb{F}_{q^m}$.

Para campos de funciones congruentes no hay una noción general de campo de clases de Hilbert. Se usará la noción de campos de clases de Hilbert que introdujo M. Rosen, la cual se fija en un conjunto finito no vacío S_∞ de primos de K.

Definición 3.4.2. Sea K un campo de funciones con campo de constantes $\mathbb{F}_q$. Sea S_∞ cualquier 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.

Definición 3.4.3. Sea E una extensión finita de k. El *campo de géneros* E_{ge} de E sobre k es la máxima extensión abeliana de E contenida en E_{H,S_∞} que sea la composición de E y una extensión abeliana de k. Equivalentemente, $E_{ge} = Ek^*$ donde k^* es la máxima extensión abeliana de k contenida en E_{H,S_∞}.

EL problema que se trata en el Capítulo 4 es dar la descripción del campo de géneros de una extensión K abeliana finita de un campo de funciones congruente, mediante el uso de caracteres de Dirichlet, que es un análogo a la teoría de campos de géneros de Leopoldt desarrollada para campos numéricos. Se considera a S_∞ como el conjunto de primos infinitos de K, es decir, los primos de K que se encuentran encima de $\mathfrak{p}_\infty$, el divisor de polos de T en el campo de funciones racionales $k = \mathbb{F}_q(T)$.

El siguiente resultado es un análogo al Teorema de Leopoldt [86] de campos numéricos.

Teorema 3.4.4. *Si $K \subseteq k(\Lambda_N)$ y el grupo de caracteres asociado a K es X, entonces la máxima extensión abeliana L de K no ramificada en ningún primo finito $P \in R_T^+$, contenida en una*

extensión ciclotómica, es el campo asociado a

$$Y = \prod_{P \in R_T^+} X_P = \prod_{P|N} X_P.$$

Demostración. Observe que para todo polinomio mónico irreducible $P \in R_T^+$, $Y_P = X_P$ por lo que $|Y_P| = |X_P|$, del Teorema 3.3.27 se sigue que, $e_p(L : K) = 1$ y por lo tanto L/K es no ramificado en ningún primo finito.

Sea ahora, E/K una extensión no ramificada en ningún primo finito y E/K abeliana. Sea Z el grupo de caracteres de Dirichlet asociado a E. Entonces $|X_P| = |Y_P|$ y $Z \supseteq X$. Por lo cual se tiene $Z_P = X_P$ y así $Z \subseteq \prod_P Z_P = \prod_P X_P = X = Y$ y se concluye que, $E \subseteq L$. □

Capítulo 4

Cálculo del campo de géneros para una extensión l-elemental abeliana

En este capítulo k denotará un campo de funciones racionales congruente, es decir, el campo de constantes de k es finito, esto es, $k = \mathbb{F}_q(T)$ y K/k una extensión abeliana tal que $\mathrm{Gal}(K/k) = C_l \times \cdots \times C_l = C_l^m$, donde C_l es el grupo cíclico de orden l, con l número primo racional distinto de la característica de K y $m \in \mathbb{N}$. Sea $K = K_1 \cdots K_m$ tal que para cada $1 \leqslant i \leqslant m$ se tiene $\mathrm{Gal}(K_i/k) = C_l$. En esta sección se describe el campo de géneros para el caso Kummer es decir $l|q-1$ y el caso no Kummer, es decir $l \nmid q-1$. A continuación se enuncia el Teorema de Peng [10] que describe explícitamente el campo de géneros de una extensión de Kummer cíclica de grado primo de campos de funciones:

Teorema 4.0.1 (G. Peng). *Sea $D = P_1^{e_1} \cdots P_r^{e_r} \in R_T$ un polinomio mónico libre de l potencias, donde $P_i \in R_T^+$, $1 \leqslant e_i \leqslant l-1$, $1 \leqslant i \leqslant r$. Sea $1 \leqslant s \leqslant r$ tal que $l|\mathrm{gr}\, P_i$ para $1 \leqslant i \leqslant s$ y $l \nmid \mathrm{gr}\, P_j$ para $s+1 \leqslant j \leqslant r$. Sea $K \coloneqq k(\sqrt[l]{\gamma D})$ donde $\gamma \in \mathbb{F}_q^*$. Sean $\alpha \coloneqq (-1)^{\mathrm{gr}\, D}\gamma$ y $a_{s+1}, \ldots, a_{r-1} \in \mathbb{Z}$ que satisfacen $\mathrm{gr}\, P_m + a_m \mathrm{gr}\, P_r \equiv 0 \bmod l$, $s+1 \leqslant m \leqslant r-1$. Entonces el campo de géneros K_{ge} está dado por:*

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

(b).- $k(\sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}})$ *si* $\alpha \in (\mathbb{F}_q^*)$, $l|\mathrm{gr}\, D$ *y* $l \nmid \mathrm{gr}\, P_r$.

(c).- $k(\sqrt[l]{\gamma}, \sqrt[l]{P_1}, \ldots, \sqrt[l]{P_r})$ *si* $l|\mathrm{gr}\, P_r$.

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

Demostración. Ver [17, página 225]. □

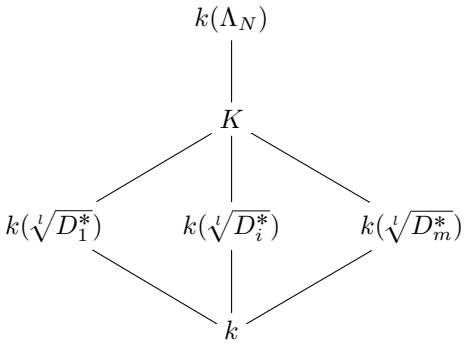
Proposición 4.0.2. *Si K/k es una extensión abeliana tal que $\mathfrak{p}_\infty$ es moderadamente ramificado, existen $N \in R_T$ y $m \in \mathbb{N}$ tales que $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$.*

Demostración. Ver [19, Proposición 14.3.8]. □

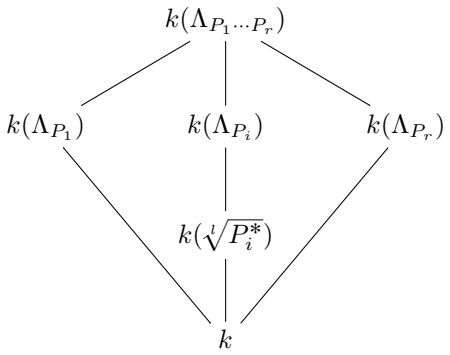
4.1. Caso Kummer

En el caso Kummer se puede escribir cada K_i en forma de radicales de la siguiente manera: $K_i = k(\sqrt[l]{\gamma_i D_i})$ para todo $1 \leqslant i \leqslant m$, donde $\gamma_i \in \mathbb{F}_q^*$ y $D_i \in R_T = \mathbb{F}_q[T]$ un polinomio mónico. Note que, se tendrán dos subcasos más, a saber, si K está contenido o no en un campo ciclotómico. Se verá en primer lugar cuando K está contenido en un campo ciclotómico. Dadas estas condiciones, del Corolario 3.3.34, se tiene que $K_i = k(\sqrt[l]{\gamma_i D_i}) \subseteq k(\Lambda_{D_i})$ si y solamente si $\gamma_i \equiv (-1)^{\mathrm{gr}\, D_i}$ mód $(\mathbb{F}_q^*)^l$ lo cual equivale a que $\xi_i := (-1)^{\mathrm{gr}\, D_i}\gamma_i \in (\mathbb{F}_q^*)^l$. En este caso se denota a K_i como $k(\sqrt[l]{\gamma_i D_i})$, para todo $1 \leqslant i \leqslant m$. Note también que, si $l | \mathrm{gr}\, D_i$, entonces $k(\sqrt[l]{D}) \subseteq k(\Lambda_D)$. Se tendrá la siguiente notación, para todo $A \in R_T$, $K(\sqrt[l]{(-1)^{\mathrm{gr}\, A} A}) = K(\sqrt[l]{A^*})$

Sea $K \subseteq k(\Lambda_N)$ para algún $N \in R_T$, nuestro objetivo es encontrar el campo de géneros de K y para esto se estudia la aritmética de K usando la herramienta que proporcionan los caracteres de Dirichlet . Sean χ_i el caracter asociado a K_i, es decir, $K_i = k(\Lambda_N)^{\chi_i^{\perp}}$ con $\chi_i \in \mathrm{Gal}(\widehat{k(\Lambda_N)}/k)$ para cada $1 \leqslant i \leqslant m$ y $X := \langle \chi_1, \ldots, \chi_m \rangle$ el grupo de caracteres asociado a K. Dado que χ_i es el caracter asociado a K_i/k, la cual es una extensión cíclica de grado l con $\mathrm{Gal}(K_i/k) \cong \langle \chi_i \rangle$ por lo que $\circ(\chi_i) = l$ y por tanto $X \cong C_l^m$, lo cual era de esperarse pues $G := \mathrm{Gal}(K/k) = C_l^m$, por lo que, ya se tiene otra representación de las extensiones K_i/k en términos de caracteres de Dirichlet.



Sea $S := \{P \in R_T^+ \mid P | D_i, \text{ para algún } 1 \leqslant i \leqslant m\}$, el conjunto de polinomios irreducibles divisores de algún D_i, para $1 \leqslant i \leqslant m$. Se tiene que S es finito y nos permite escribir al conjunto S como $S = \{P_1, \ldots, P_r\}$. Se considera la P_i-parte de cada caracter χ_j, es decir, $\chi_j = \prod_{i=1}^{r} (\chi_j)_{P_i}$ para cada $1 \leqslant j \leqslant m$, donde χ_j es el caracter asociado a $K_j = k(\sqrt[l]{D_j^*})$. Note que, es posible que para algún $1 \leqslant i \leqslant r$, $P_i | D_j$ para algunos $1 \leqslant j \leqslant m$, por lo cual $(\chi_j)_{P_i}$ aparece como factor en algunos χ_j. Dado que $k \subseteq K \subseteq k(\Lambda_N)$, si $k(\sqrt[l]{P_i^*})$ es el campo que corresponde a $(\chi_j)_{P_i}$, se tiene que K está contenido en la composición de estos campos, esto es, $K \subseteq k(\sqrt[l]{P_1^*}) \cdots k(\sqrt[l]{P_r^*}) \subseteq k(\Lambda_N)$.



donde $k(\sqrt[l]{P_i^*})$ es el campo correspondiente a $(\chi_j)_{P_i}$ y se denota a este caracter por χ_{P_i}

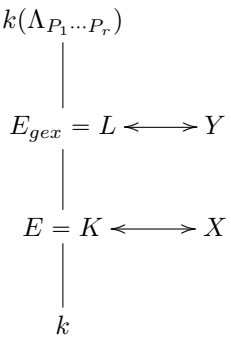
Sea $X_P = \{\chi_P \mid \chi \in X\}$. Note que el conductor de cada χ_{P_i} es precisamente F_{P_i} (ver Definición 3.3.5), y como $X_{P_i} = \langle \chi_{P_i} \rangle$, se tiene

$$Y = \prod_{P \in S} X_P = \prod_{i=1}^{r} \langle \chi_{Pi} \rangle.$$

Sea L el campo asociado a $Y \subseteq \mathrm{Gal}(\widehat{k(\Lambda_N)}/k)$, es decir, $L = k(\Lambda_N)^{Y^\perp}$. Por la Proposición 3.3.24 se sigue que $L = k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*})$. Sea $E := K_{m_0} \cap k(\Lambda_N)$, donde $K_{m_0} = K\mathbb{F}_{q^{m_0}}(T)$, en el caso de que K esté contenido en el campo ciclotómico, se tiene que $K = E \subseteq k(\Lambda_N)$. El objetivo es determinar el campo de géneros de E (sobre k) E_{ge}, para esto se sabe que el campo de géneros extendido E_{gex}, es la máxima extensión abeliana de E no ramificada en ningún primo finito y contenida en un campo ciclotómico. Observe que, $X, Y \subseteq (R_T/\widehat{\langle P_1 \cdots P_r \rangle})^*$ donde este último es el grupo de caracteres del grupo $\mathrm{Gal}(k(\Lambda_{P_1\cdots P_r})/k)$ y ya que los únicos primos finitos ramificados son los elementos de S, del Teorema 3.3.27 se tiene que $e_{P_i}(L|k) = |Y_{P_i}|$, recuérdese que $Y = \prod_{i=1}^{r} X_{P_i}$ por tanto $|Y_{P_i}| = |X_{P_i}|$, es decir

$$e_{P_i}(L : k) = |Y_{P_i}| = |X_{P_i}| = e_{P_i}(E : k)$$

entonces $e_{P_i}(L : E) = 1$, esto para todo $P_i \in S$ y dado que ningún primo finito es ramificado en L/E se tiene $E_{gex} = L$.



Del Teorema 3.2.14 se tiene que, no hay inercia en una extensión ciclotómica, esto es $f_\infty(k(\Lambda_N)|k) =$

1 y además $e_\infty(k(\Lambda_N)|k) = q-1$. Note que,

$$\frac{D_\infty(L:k)}{I_\infty(L:k)} \cong \mathrm{Gal}((\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty)/(\mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty))$$

dado que $1 = f_\infty = [\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty \ : \ \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty] = \frac{|D_\infty(L:k)|}{|I_\infty(L:k)|}$ se tiene que $I_\infty(L:k) = D_\infty(L:k)$ y como $(\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty)/(\mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty)$ es una extensión cíclica, pues ésta resulta ser una extensión de Galois de un campo finito, y como los únicos subgrupos de $\mathrm{Gal}(L/k)$ que son cíclicos son precisamente $\langle \mathrm{Id} \rangle$ y C_l, de esto se concluye que

$$e_\infty(L:k)|l\ , \qquad e_\infty(E_{ge}:k)|l \quad \text{y} \quad e_\infty(E:k)|l.$$

Los caracteres de Dirichlet nos proporcionaron información de la ramificación de los primos finitos, falta ver el comportamiento de $\mathfrak{p}_\infty$ en la torre de campos $k \subseteq E \subseteq L$. La siguiente proposición nos brinda información del comportamiento de $\mathfrak{p}_\infty$ en una extensión de Kummer $k(\sqrt[l]{\gamma D})$ con $\gamma \in \mathbb{F}_q^*$ y $D \in R_T$..

Proposición 4.1.1. *El comportamiento de $\mathfrak{p}_\infty$ en $k(\sqrt[l]{\gamma D})/k$ es el siguiente:*

1. *si $l \nmid \mathrm{gr}\, D$, $\mathfrak{p}_\infty$ es totalmente ramificado.*

2. *si $l|\mathrm{gr}\, D$ y $\gamma \in (\mathbb{F}_q^*)^l$, $\mathfrak{p}_\infty$ se descompone completamente.*

3. *si $l|\mathrm{gr}\, D$ y $\gamma \notin (\mathbb{F}_q^*)^l$, $\mathfrak{p}_\infty$ es inerte.*

Demostración. Ver [17, Lemma 3]. □

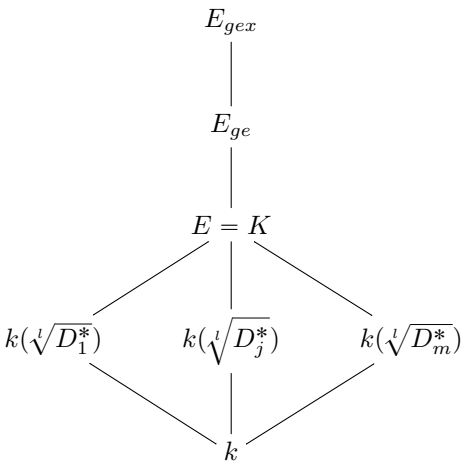
Gracias a esta proposición ya se está encaminado a determinar el campo de géneros de E.

4.1.1. Campo de géneros cuando K es ciclotómico

Caso 1: $l|\mathrm{gr}\, P_j$ para todo $1 \leqslant j \leqslant r$.

Por la proposición anterior, $\mathfrak{p}_\infty$ no se ramifica en $k(\sqrt[l]{P_j^*})/k$, es decir $e_\infty(k(\sqrt[l]{P_j^*}:k)) = 1$ para todo $1 \leqslant j \leqslant r$. Se tiene pues que, en todas las extensiones $k(\sqrt[l]{P_j^*})/k$, $\mathfrak{p}_\infty$ no se ramifica y por tanto no se ramifica en $k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*})/k$, ya que la composición de extensiones no ramificadas en un primo dado, da como resultado una extensión que no se ramifica en este mismo primo. Se sabe que E_{ge} es la máxima extensión abeliana de E no ramificada en ningún primo finito y tal que los primos infinitos se descomponen totalmente. De lo anterior se sigue que en L/E no se ramifica ningún primo finito y como $\mathfrak{p}_\infty$ se descompone totalmente en L/k y por lo tanto en L/E, pues no hay inercia, es decir, $f_\infty(L:k) = 1$. En este caso se concluye que $L = E_{gex} = E_{ge}$.

Caso 2: $l \nmid \operatorname{gr} D_j$ **para algún** $1 \leqslant j \leqslant m$**.**



Se tiene de la Proposición 4.1.1 que $\mathfrak{p}_\infty$ se ramifica en $k(\sqrt[l]{D_j^*})/k$, y como

$$l = [k(\sqrt[l]{D_j^*}) : k] = e_\infty(K_j : k) f_\infty(K_j : k) h_\infty(K_j : k),$$

necesariamente $e_\infty(K_j : k) = l$, $f_\infty(K_j : k) = 1$ y $h_\infty(K_j : k) = 1$. Note también que, para los demás $i \in \{1, \ldots, m\}$ con $i \neq j$ tal que $l | \operatorname{gr} D_i$ se tiene que $e_\infty(K_i : k) = 1$. Ahora, del Lema de Abhyankar se sigue

$$e_\infty(E : k) = \operatorname{mcm}[e_\infty(K_1 : k), \ldots, e_\infty(K_j : k), \ldots, e_\infty(K_m : k)] = l.$$

Por lo tanto $\mathfrak{p}_\infty$ es ramificado en E/k esto es, $e_\infty(E : k) = l$. Puesto que $e_\infty(L : k) | l$ se tiene que $e_\infty(L : E) = 1$, así que se tiene $E_{ge} = E_{gex} = L$.

Caso 3: $l | \operatorname{gr} D_j \ \forall\ 1 \leqslant j \leqslant m$**,** $l | \operatorname{gr} P_i$ **para** $1 \leqslant i \leqslant s$ **y** $l \nmid \operatorname{gr} P_j$ **para** $s \leqslant j \leqslant r$ **con** $s < r$**.**

Bajo estas condiciones se tiene que $\mathfrak{p}_\infty$ se descompone en K_i/k para todo $1 \leqslant i \leqslant m$ y por lo tanto $\mathfrak{p}_\infty$ se descompone en E/k. Ahora, dado que $l \nmid \operatorname{gr} P_r$ se tiene que $\mathfrak{p}_\infty$ se ramifica en $k(\sqrt[l]{P_r^*})/k$ y por lo tanto en L/k. Para encontrar E_{ge} se procede de la siguiente manera, sean $a_{s+1}, \ldots, a_{r-1} \in \mathbb{Z}$ tales que $l | \operatorname{gr}(P_i P_r^{a_i})$, es decir, $\operatorname{gr} P_i + a_i \operatorname{gr} P_r \equiv 0 \bmod l$ para $s+1 \leqslant i \leqslant r-1$. Sea

$$F = k\Big(\sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1} P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1} P_r^{a_{r-1}}}\Big) \subseteq k(\Lambda_{P_1 P_2 \cdots P_r}).$$

Puesto que $E = E_1 \cdots E_m$, donde $E_t = k(\sqrt[l]{D_t^*})$, en este caso $k(\sqrt[l]{D_t^*}) = k(\sqrt[l]{D_t})$ pues $l | \operatorname{gr} D_t$. De manera análoga $k(\sqrt[l]{P_i^*}) = k(\sqrt[l]{P_i})$ para $1 \leqslant i \leqslant s$ y $k(\sqrt[l]{(P_{s+j} P_r^{a_{s+j}})^*}) = k(\sqrt[l]{P_{s+j} P_r^{a_{s+j}}})$ para $s+1 \leqslant j \leqslant r-1$. Observe que $E \subseteq F \subsetneq L$ y $L = F(\sqrt[l]{P_r^*})$, así que $[L : F] = l$, además $l | \operatorname{gr} P_i$ para

$1 \leqslant i \leqslant s$ y $l|\text{gr}\,(P_j P_r^{a_{s+j}})$ para $s+1 \leqslant j \leqslant r-1$, de esta manera se tiene que $\mathfrak{p}_\infty$ no se ramifica en F/E y por lo tanto para este caso se concluye que el campo de géneros de E es:

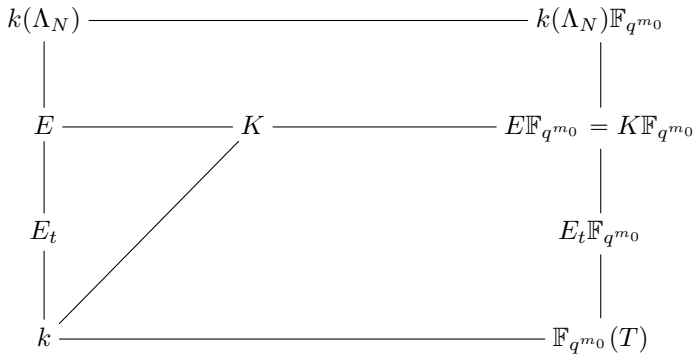
$$E_{ge} = k\Big(\sqrt[l]{P_1}, \ldots, \sqrt[l]{P_s}, \sqrt[l]{P_{s+1}P_r^{a_{s+1}}}, \ldots, \sqrt[l]{P_{r-1}P_r^{a_{r-1}}}\Big).$$

4.1.2. Campo de géneros cuando K no es ciclotómico

Ahora se verá el caso no ciclotómico, es decir, $K \nsubseteq k(\Lambda_N)$. Al ser K/k una extensión abeliana donde $\mathfrak{p}_\infty$ se ramifica moderadamente, de la Proposición 4.0.2 se tiene que, existen $N \in R_T$ y $m_0 \in \mathbb{N}$ tal que $K \subseteq k(\Lambda_N)\mathbb{F}_{q^{m_0}}$ (más adelante se verá que basta con $m_0 = l$). Se usa la siguiente notación. Sean $D_t = P_1^{\beta_{1_t}} \cdots P_r^{\beta_{r_t}}$, donde $0 \leqslant \beta_{v_t} \leqslant l-1$ y $1 \leqslant v \leqslant r$, $1 \leqslant t \leqslant m$. Sea $K = K_1 \cdots K_m$ donde $K_t = k(\sqrt[l]{\gamma_t D_t})$ y $\gamma_t \in \mathbb{F}_q^*$, para $1 \leqslant t \leqslant m$. Se tiene que $P_1, \ldots, P_r$ son los primos finitos ramificados en K/k.
Dada la definición anterior de $E := K_{m_0} \cap k(\Lambda_N)$, donde $K_{m_0} = K\mathbb{F}_{q^{m_0}}(T)$, note que $K_{m_0} = K_1 \cdots K_m \mathbb{F}_{q^{m_0}}(T)$. Por lo tanto

$$E = K_{m_0} \cap k(\Lambda_N) = (K_1 \cdots K_m \mathbb{F}_{q^{m_0}}(T)) \cap k(\Lambda_N).$$

Así, es posible reescribir al campo E de la siguiente manera $E = E_1 \cdots E_m$ donde, $E_t = K_t\mathbb{F}_{q^{m_0}} \cap k(\Lambda_N)$, $1 \leqslant i \leqslant m$. Sea $E' = E_1' \cdots E_m'$ con $E_t' = k(\sqrt[l]{(-1)^{\text{gr}\,D_t} D_t}) = k(\sqrt[l]{D_t^*}) \subseteq k(\Lambda_N)$, para cada $1 \leqslant t \leqslant m$. Se probará que E_t es igual a E_t', es decir, $E_t = k(\sqrt[l]{D_t^*})$, para todo $1 \leqslant t \leqslant m$. En efecto, se tiene el siguiente cuadro de Galois



Dado que $k(\Lambda_N) \cap \mathbb{F}_{q^{m_0}} = k$, de la correspondencia de Galois entre $k(\Lambda_N)/k$ y $k(\Lambda_N)\mathbb{F}_{q^{m_0}}/\mathbb{F}_{q^{m_0}}(T)$, se tiene que E_t corresponde a $K_t\mathbb{F}_{q^{m_0}}$ pues $E_t = K_t\mathbb{F}_{q^{m_0}} \cap k(\Lambda_N)$ y puesto que $E_t\mathbb{F}_{q^{m_0}}$ corresponde a E_t, se sigue que $K_t\mathbb{F}_{q^{m_0}} = E_t\mathbb{F}_{q^{m_0}}$.
Observe que un posible candidato a ser $E_t = K_t\mathbb{F}_{q^{m_0}} \cap k(\Lambda_N)$ es precisamente $E_t' = k(\sqrt[l]{D_t^*})$, si se prueba que al agregarle constantes estos coinciden, es decir

$$E_t'\mathbb{F}_{q^{m_0}} = K_t\mathbb{F}_{q^{m_0}} = E_t\mathbb{F}_{q^{m_0}},$$

lo cual es equivalente a probar

$$k(\sqrt[l]{D_t^*})\mathbb{F}_{q^{m_0}} = k(\sqrt[l]{\gamma_t D_t})\mathbb{F}_{q^{m_0}}.$$

De la correspondencia de Galois, se seguirá que $E_t = E_t'$ es decir, $E_t = k(\sqrt[l]{D_t^*})$. Puesto que, $\gamma_t \in \mathbb{F}_q^* \subseteq (\mathbb{F}_{q^{m_0}})^l$, se sigue que $\gamma_t = \alpha^l$ con $\alpha \in \mathbb{F}_{q^{m_0}}$, es decir $\sqrt[l]{\gamma_t} = \alpha \in \mathbb{F}_{q^{m_0}}^*$, del hecho $m_0 \in \mathbb{N}$ se tiene que $\sqrt[l]{-1} \in \mathbb{F}_{q^{m_0}}$ y por tanto $\sqrt[l]{-\gamma_t} = \sqrt[l]{-1}\sqrt[l]{\gamma_t} \in \mathbb{F}_{q^{m_0}}^*$. Dado que $(-1)^{\mathrm{gr}\, D_t} = \pm 1$, en caso de que $(-1)^{\mathrm{gr}\, D_t} = -1$ se tiene:

$$\sqrt[l]{\gamma_t D_t} = \sqrt[l]{-\gamma_t(-1)^{\mathrm{gr}\, D_t} D_t} = \sqrt[l]{D_t^*} \cdot \sqrt[l]{-\gamma_t} \in k(\sqrt[l]{D_t^*})\mathbb{F}_{q^{m_0}}.$$

De manera similar, si $(-1)^{\mathrm{gr}\, D_t} = 1$ se tiene

$$\sqrt[l]{\gamma_t D_t} = \sqrt[l]{D_t^*} \cdot \sqrt[l]{\gamma_t} \in k(\sqrt[l]{D_t^*})\mathbb{F}_{q^{m_0}}.$$

Por lo tanto de ambos casos se concluye que $k(\sqrt[l]{\gamma_t D_t})\mathbb{F}_{q^{m_0}} \subseteq k(\sqrt[l]{D_t^*})\mathbb{F}_{q^{m_0}}$. Para ver la otra contención se procede de la misma manera, es decir, nuevamente se supone primero que $(-1)^{\mathrm{gr}\, D_t} = -1$,

$$\sqrt[l]{(-1)^{\mathrm{gr}\, D_t} D_t} = \frac{\sqrt[l]{\gamma_t D_t}}{\sqrt[l]{-\gamma_t}} \in k(\sqrt[l]{\gamma_t D_t})\mathbb{F}_{q^{m_0}}.$$

Ahora, si $(-1)^{\mathrm{gr}\, D_t} = 1$ se tiene

$$\sqrt[l]{(-1)^{\mathrm{gr}\, D_t} D_t} = \frac{\sqrt[l]{\gamma_t D_t}}{\sqrt[l]{\gamma_t}} \in k(\sqrt[l]{\gamma_t D_t})\mathbb{F}_{q^{m_0}}.$$

De ambos casos se obtiene $k(\sqrt[l]{D_t^*})\mathbb{F}_{q^{m_0}} \subseteq k(\sqrt[l]{\gamma_t D_t})\mathbb{F}_{q^{m_0}}$.

Se ha probado la igualdad requerida, es decir, $k(\sqrt[l]{D_t^*})\mathbb{F}_{q^{m_0}} = k(\sqrt[l]{\gamma_t D_t})\mathbb{F}_{q^{m_0}}$, luego de la correspondencia de Galois se sigue que $E_t = E_t' = k(\sqrt[l]{D_t^*})$ para todo $1 \leqslant t \leqslant m$. Por tanto $E\mathbb{F}_{q^{m_0}} = K\mathbb{F}_{q^{m_0}} = E'\mathbb{F}_{q^{m_0}}$. Así pues, se tiene que el candidato propuesto E' es el correspondiente a K en la extensión $k(\Lambda_N)/k$, esto es

$$E = E' = k(\sqrt[l]{D_1^*}, \ldots, \sqrt[l]{D_m^*}).$$

Sean ahora $P_1, \ldots, P_r$ los primos finitos ramificados arreglados de tal forma que, $l | \mathrm{gr}\, P_i$ para $1 \leqslant i \leqslant s$ y $l \nmid \mathrm{gr}\, P_j$ para $s+1 \leqslant j \leqslant r$. Si $s < r$ se eligen $a, b \in \mathbb{Z}$ tales que $al + b\mathrm{gr}\, P_r = 1$. En adelante se denotará $d_i = \mathrm{gr}\, P_i$ para $1 \leqslant i \leqslant r$ y se define $Q_i := P_i P_r^{-bd_i}$ para $1 \leqslant i \leqslant r-1$. Note que, $l | \mathrm{gr}\, Q_i$ en efecto

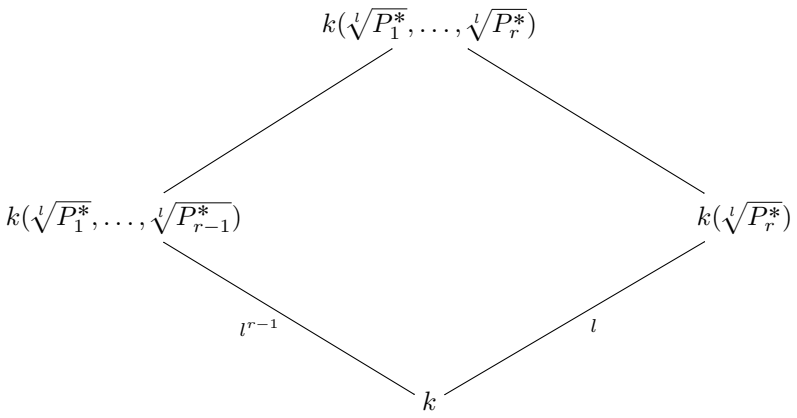
$$\mathrm{gr}\, Q_i = \mathrm{gr}\, P_i + (-bd_i)\mathrm{gr}\, P_r = d_i + (-bd_i)d_r = d_i(1 - bd_r).$$

Dado que $al + bdr = 1$ observe que $\operatorname{gr} Q_i = d_i(al)$ y por lo tanto $l | \operatorname{gr} Q_i$, para todo $1 \leqslant i \leqslant r-1$.

Sean $L = k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*}) \subseteq k(\Lambda_{P_1 \cdots P_r})$ y $M := k(\sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_{r-1}})$. Se probará que L es una extensión de M de grado l (cuando $s < r$). La prueba comenzará primero con ver que $M \subseteq L$. Puesto que $Q_i = P_i P_r^{-bd_i}$, $\sqrt[l]{Q_i} = \sqrt[l]{P_i P_r^{-bd_i}}$. Entonces, se tiene

$$\begin{aligned}
\sqrt[l]{Q_i} &= \sqrt[l]{P_i P_r^{-bd_i}} \\
&= (-1)^{d_i a}(-1)^{d_i a}\sqrt[l]{P_i P_r^{-bd_i}} \\
&= (-1)^{d_i a}\sqrt[l]{(-1)^{d_i al} P_i P_r^{-bd_i}} \\
&= (-1)^{d_i a}\sqrt[l]{(-1)^{d_i(1-bd_r)} P_i P_r^{-bd_i}} \qquad \text{pues} \qquad al + bd_r = 1 \\
&= (-1)^{d_i a}\sqrt[l]{(-1)^{d_i} P_i (-1)^{-d_i bd_r} P_r^{-bd_i}} \\
&= (-1)^{d_i a}\sqrt[l]{(-1)^{d_i} P_i ((-1)^{d_r} P_r)^{-bd_i}} \\
&= (-1)^{d_i a}\sqrt[l]{(-1)^{d_i} P_i}\left(\sqrt[l]{(-1)^{d_r} P_r}\right)^{-bd_i} \\
&= \pm 1 \sqrt[l]{P_i^*}\sqrt[l]{P_r^*}^{-bd_i} \ \in \ L,
\end{aligned}$$

esto para $1 \leqslant i \leqslant r-1$, y por lo tanto $M = Q(\sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_{r-1}}) \subseteq k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*}) = L$. Ahora, dado que $[M : k] \leqslant l^{r-1}$, para probar que $[L : M] = l$ primero se probará que $[L : k] = l^r$. La prueba se hará por inducción sobre $r \in \mathbb{N}$ y a través de los índices de ramificación. Para $r = 1$ se considera la extensión $k(\sqrt[l]{P_1^*})/k$ donde el primo P_1 es totalmente ramificado. Así $l = [k(\sqrt[l]{P_1^*}) : k] = e_{P_1}(k(\sqrt[l]{P_1^*}) : k)$. Supóngase el resultado cierto para $r-1$, es decir $[k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_{r-1}^*}) : k] = l^{r-1}$. Ahora se probará para $k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*})$ que $[k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*}) : k] = l^r$.



Por el caso $r = 1$ se tiene que P_r se ramifica totalmente en $k(\sqrt[l]{P_r^*})/k$, y además no se ramifica en $k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_{r-1}^*})/k$, por lo tanto de la hipótesis de inducción y del caso $r = 1$ se tiene que P_r se ramifica en $k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*})/k$, de esta manera se concluye $[k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*}) : k] = l^r$, es decir $[L : k] = l^r$. Para ver que $[L : M] = l$ basta probar que $M \neq L$ y $M(\sqrt[l]{P_r^*}) = L$, es decir al agregar un elemento cuyo irreducible es de grado l a M se obtiene L. Supóngase que $\sqrt[l]{P_r^*} \in M$,

luego para cada $1 \leqslant i \leqslant r-1$, se tiene

$$\begin{aligned} M \ni \sqrt[l]{Q_i}(\sqrt[l]{P_r^*})^{bd_i} &= \sqrt[l]{P_i P_r^{-bd_i}}(\sqrt[l]{(-1)^{d_r} P_r})^{bd_i} \\ &= \sqrt[l]{P_i P_r^{-bd_i} P_r^{bd_i} (-1)^{d_r bd_i}} \\ &= \sqrt[l]{(-1)^{d_r bd_i} P_i} \\ &= \sqrt[l]{(-1)^{d_i - d_i al} P_i} \\ &= \sqrt[l]{(-1)^{-d_i al}(-1)^{d_i} P_i} \\ &= (-1)^{-d_i a}\sqrt[l]{(-1)^{d_i} P_i} \\ &= \pm\sqrt[l]{P_i^*}. \end{aligned}$$

Por lo tanto $\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*} \in M$, por lo que se tendría $L \subseteq M$, luego $L = M$, pero note que

$$[L : k] = l^r > l^{r-1} \geqslant [M : k]$$

lo cual es una contradicción. Por lo tanto se tiene que $L \neq M$ y $L = M(\sqrt[l]{P_r^*})$, esto implica que $[L : M] = l$. Hasta el momento se ha probado que $M \subseteq L$, se sabe también que $E = E_1 \cdots E_m$ donde $E_i = k(\sqrt[l]{D_i^*})$ para todo $1 \leqslant i \leqslant m$. Téngase en cuenta que nuestro principal objetivo es encontrar el campo de géneros de K. Para el caso ciclotómico ya se tiene una representación.

A continuación se dará otra descripción de E_{ge} cuando $E_{ge} \neq E_{gex} = L$. En este caso se tendrá $E_{ge} = M$, para esto se probará que $E \subseteq M$ y que los índices de ramificación coinciden, es decir $e_{P_i}(M : k) = e_{P_i}(E : k)$. Si $E_{ge} \neq E_{gex}$, se probó en el Caso 3 que esto sucede si y sólo si $l | \text{gr}\, D_t$ para todo $1 \leqslant t \leqslant m$ y $l \nmid \text{gr}\, P_r$.

Dado que $D_t = P_1^{\beta_{1_t}} \cdots P_r^{\beta_{r_t}}$, por lo que $\text{gr}\, D_t = \beta_{1_t} d_1 + \cdots + \beta_{r_t} d_r$, y como $l | \text{gr}\, D_t$ esto implica $l | \beta_{1_t} d_1 + \cdots + \beta_{r_t} d_r$, es decir existe $q_t \in \mathbb{Z}$ tal que

$$l q_t - \beta_{r_t} d_r = \beta_{1_t} d_1 + \cdots + \beta_{r-1_t} d_{r-1}. \tag{4.1}$$

Además, se tiene $l \nmid d_r$. Como los primos finitos ramificados $P_1, \ldots, P_r$ están arreglados de tal forma que, $l | \text{gr}\, P_i$ para $1 \leqslant i \leqslant s$ y $l \nmid \text{gr}\, P_j$ para $s+1 \leqslant j \leqslant r$, necesariamente se tendría que $l \nmid d_{r-1}$, pues en caso contrario, si $l | d_{r-1}$ entonces $l | d_i$ para todo $1 \leqslant i \leqslant r-1$ y ya que

$$l | \beta_{1_t} d_1 + \cdots + \beta_{r-1_t} d_{r-1} \Longrightarrow \quad l | l q_t - \beta_{r_t} d_r \Longrightarrow \quad l | \beta_{r_t} d_r.$$

Esto es una contradicción pues l es número primo y así $l | \beta_{r_t}$ o $l | d_r$ pero $1 \leqslant \beta_{r_t} \leqslant l-1$ y $l \nmid d_r$. Por lo tanto $l \nmid d_{r-1}$. Entonces existen al menos dos P_j tales que, su grado no es divisible por l. Ahora para probar que $E \subseteq M$ basta ver que $E_t \subseteq M$ para todo $1 \leqslant t \leqslant m$. Observe que en este

caso, si $l|\text{gr } D_t$ entonces $E_t = k(\sqrt[l]{D_t^*}) = k(\sqrt[l]{D_t})$ para todo $1 \leqslant t \leqslant m$. Note lo siguiente

$$\begin{aligned} Q_1^{\beta_{1_t}} \cdots Q_{r-1}^{\beta_{r-1_t}} &= (P_1 P_r^{-bd_1})^{\beta_{1_t}} \cdots (P_{r-1} P_r^{-bd_{r-1}})^{\beta_{r-1_t}} \\ &= P_1^{\beta_{1_t}} P_r^{-bd_1\beta_{1_t}} \cdots P_{r-1}^{\beta_{r-1_t}} P_r^{-bd_{r-1}\beta_{r-1_t}} \\ &= P_1^{\beta_{1_t}} \cdots P_{r-1}^{\beta_{r-1_t}} \cdot P_r^{-b(\beta_{1_t}d_1 + \cdots + \beta_{r-1_t}d_{r-1})}. \end{aligned} \tag{4.2}$$

Así pues de la Ecuación (4.1) se sigue que $-b(\beta_{1_t}d_1 + \cdots + \beta_{r-1_t}d_{r-1}) = -b(lq_t - \beta_{r_t}d_r)$ y dado que $al + bd_r = 1$, se sigue $bd_r = 1 - al$, por tanto

$$-blq_t + \beta_{r_t}bd_r = -blq_t + \beta_{r_t}(1 - al) = -blq_t + \beta_{r_t} - \beta_{r_t}al = \beta_{r_t} + l(-bq_t - \beta_{r_t}a) = \beta_{r_t} + l\delta.$$

Reescribiendo la Ecuación (4.2) se obtiene

$$\begin{aligned} Q_1^{\beta_{1_t}} \cdots Q_{r-1}^{\beta_{r-1_t}} &= P_1^{\beta_{1_t}} \cdots P_{r-1}^{\beta_{r-1_t}} \cdot P_r^{-b(\beta_{1_t}d_1 + \cdots + \beta_{r-1_t}d_{r-1})} = P_1^{\beta_{1_t}} \cdots P_{r-1}^{\beta_{r-1_t}} \cdot P_r^{\beta_{r_t} + l\delta} \\ &= P_1^{\beta_{1_t}} \cdots P_{r-1}^{\beta_{r-1_t}} \cdot P_r^{\beta_{r_t}} P_r^{l\delta}. \end{aligned}$$

Tomando la raíz l-ésima en ambos miembros se tiene

$$Q_1^{\frac{\beta_{1_t}}{l}} \cdots Q_{r-1}^{\frac{\beta_{r-1_t}}{l}} = P_1^{\frac{\beta_{1_t}}{l}} \cdots P_{r-1}^{\frac{\beta_{r-1_t}}{l}} \cdot P_r^{\frac{\beta_{r_t}}{l}} P_r^{\delta} = \sqrt[l]{D_t} \cdot P_r^{\delta},$$

con $P_r^{\delta} \in k$. Por tanto $E_t = k(\sqrt[l]{D_t}) \in M$ para todo $1 \leqslant t \leqslant m$. De esto se concluye que $E = E_1 \cdots E_m \subseteq M$. Para probar que $E_{ge} = M$ sólo falta probar que $e_{P_i}(M : k) = e_{P_i}(E : k)$. Note que la siguiente torre de campos $k \subseteq E \subseteq M \subseteq E_{gex}$, como $e_{P_i}(E_{gex} : E) = 1$ se tiene $e_{P_i}(M : E) = 1$ y por lo tanto $e_{P_i}(M : k) = e_{P_i}(E : k)$ por lo tanto ningún primo finito se ramifica en M/E, más aún se probará que $[E_{gex} : M] = l = [E_{gex} : E_{ge}]$ y como se está en el caso ciclotómico, necesariamente $M = E_{ge}$.

Continuando con el caso $K \neq E$, es decir $\gamma_t \not\equiv (-1)^{\text{gr } D_t} \mod (\mathbb{F}_q^*)^l$ para algún t. Anteriormente ya se había definido $\xi_t = (-1)^{\text{gr } D_t}\gamma_t$. Se probará a continuación que EK es una extensión de constantes de grado l tanto de E como de K , es decir:

$$EK = E(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_r}) = K(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_r}).$$

Se tiene que, $\sqrt[l]{\xi_i} = \frac{\sqrt[l]{(-1)^{\text{gr } D_i} D_i}}{\sqrt[l]{\gamma_i D_i}} \in EK$, para todo $1 \leqslant i \leqslant m$, por lo tanto

$$E(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_r}) \subseteq EK, \quad K(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_r}) \subseteq EK.$$

Para probar las otras contenciones se tiene lo siguiente, dado que $K_i(\sqrt[l]{\xi_i}) = k(\sqrt[l]{\gamma_i D_i}\sqrt[l]{\xi_i})$, se tiene

$$\sqrt[l]{D_i^*} = \frac{\sqrt[l]{\gamma_i D_i}}{\sqrt[l]{(-1)^{\text{gr } D_i}}\sqrt[l]{\gamma_i}} = \frac{\sqrt[l]{\gamma_i D_i}}{\sqrt[l]{\xi_i}} \in K_i(\sqrt[l]{\xi_i}).$$

Por lo tanto $E_i = k(\sqrt[l]{D_i^*}) \subseteq K_i(\sqrt[l]{\xi_i})$, así que $E_iK_i \subseteq K_i(\sqrt[l]{\xi_i})$ para $1 \leqslant i \leqslant m$, luego

$$\begin{aligned} EK &= E_1 \cdots E_m K_1 \cdots K_m = E_1K_1 \cdots E_mK_m \\ &\subseteq K_1(\sqrt[l]{\xi_1}) \cdots K_m(\sqrt[l]{\xi_m}) = K_1 \cdots K_m(\sqrt[l]{\xi_1}, \ldots \sqrt[l]{\xi_m}) \\ &= K(\sqrt[l]{\xi_1}, \ldots \sqrt[l]{\xi_m}). \end{aligned}$$

Para ver la última contención, note primero que:

$$\sqrt[l]{(-1)^{\mathrm{gr}\ D_i} D_i} \cdot \sqrt[l]{\xi_i} = \sqrt[l]{(-1)^{\mathrm{gr}\ D_i} D_i} \cdot \sqrt[l]{(-1)^{\mathrm{gr}\ D_i} \gamma_i} = \sqrt[l]{(-1)^{2\mathrm{gr}\ D_i} \gamma_i D_i} = \sqrt[l]{\gamma_i D_i}.$$

Por lo tanto $k(\sqrt[l]{\gamma_i D_i}) \subseteq k(\sqrt[l]{D_i^*})(\sqrt[l]{\xi_i})$, es decir, $K_i \subseteq E_i(\sqrt[l]{\xi_i})$, por lo que $E_iK_i \subseteq E_i(\sqrt[l]{\xi_i})$, esto para todo $1 \leqslant i \leqslant m$. Se sigue pues:

$$\begin{aligned} EK &= E_1 \cdots E_m K_1 \cdots K_m = E_1K_1 \cdots E_mK_m \\ &\subseteq E_1(\sqrt[l]{\xi_i}) \cdots E_m(\sqrt[l]{\xi_m}) = E_1 \cdots E_m(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_m}) = E(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_m}). \end{aligned}$$

Resumiendo, de las contenciones anteriores se concluye que

$$EK = E(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_r}) = K(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_r}).$$

Se tiene lo siguiente, $EK = K\mathbb{F}_q(\sqrt[l]{\xi_1}, \ldots, \sqrt[l]{\xi_m})$. De la hipótesis se tiene que al menos un $\gamma_i \not\equiv (-1)^{\mathrm{gr}\ D_i} \mod (\mathbb{F}_q^*)^l$, es decir $(-1)^{\mathrm{gr}\ D_i}\gamma_i \notin (\mathbb{F}_q^*)^l$ por lo que $\mathbb{F}_q(\sqrt[l]{\xi_i}) = \mathbb{F}_{q^l}$. Resumiendo se tiene: $EK = E\mathbb{F}_{q^l} = K\mathbb{F}_{q^l}$, es decir, $E_l = K_l$.

Ahora se analiza el comportamiento de $\mathfrak{p}_\infty$ en la extensión K/k, cuando $E \neq K$. Dado que $G = \mathrm{Gal}(K/k) = C_l^m$ y puesto que $f_\infty(K:k) = \frac{|D_\infty(K:k)|}{|I_\infty(K:k)|}$, donde

$$\frac{D_\infty(K:k)}{I_\infty(K:k)} \cong Gal\Big(\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty : \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty\Big).$$

Dado que la extensión de campos residuales es una extensión de un campo finito, por lo que, resulta ser cíclica, se sigue de la igualdad anterior que $D_\infty(K:k)/I_\infty(K:k)$ es un subgrupo cíclico de $G = \mathrm{Gal}(K/k) = C_l^m$ pero los únicos subgrupos cíclicos son precisamente $\langle \mathrm{Id} \rangle$ y C_l. Se sigue entonces que $f_\infty(K:k)|l$.

Esto también se sigue para $e_\infty(K:k)|l$. En efecto, ya que para cada $1 \leqslant i \leqslant m$, se tiene que $l = [K_i : k] = e_{\infty_i}(K:k)f_{\infty_i}(K:k)h_{\infty_i}(K:k)$ por lo que $e_{\infty_i}(K:k)|l$. Puesto que cada una de estas extensiones es moderadamente ramificada, al aplicar el Lema de Abhyankar se tiene:

$$e_\infty(K:k) = \mathrm{mcm}[e_{\infty_1}(K_1:k), \ldots, e_{\infty_m}(K_m:k)].$$

De esta manera se concluye $e_\infty(K:k)|l$.

A continuación se probará que la cantidad de subcampos $k \subseteq F \subseteq K$ tales que $[F : k] = l$, es precisamente $\frac{l^m-1}{l-1}$. Para esto se trabajará con los grupos cíclicos $C_l \subseteq \mathrm{Gal}(K/k) = C_l^m$. Sea $C_l = \{a_1 = e, a_2, \ldots, a_l\}$ el grupo cíclico de orden l, como l es un número primo se tiene, $\circ(a_j) = l$ para cada $j \in \{2, \ldots, m\}$, como consecuencia hay $\varphi(l) = l - 1$ generadores. Entonces, para cada elemento de G tal que $(a_{i_1}, \ldots, a_{i_l}) \neq (e, \ldots, e)$ con $i_j \in \{1, 2, \ldots, l\}$, también es de orden l. Sea $A_i = \langle (a_{i_1}, \ldots, a_{i_l}) \rangle < G$ cuyo orden es l, pues es generado por un elemento de orden l, se sigue pues que A_i es un grupo cíclico de orden l con $\varphi(l) = l - 1$ generadores. Si $(b_{i_1}, \ldots, b_{i_l}) \in A_i$ es tal que $(b_{i_1}, \ldots, b_{i_l}) \neq (e, \ldots, e)$, resulta que también es generador de A_i, es decir

$$A_i = \langle (b_{i_1}, \ldots, b_{i_l}) \rangle = \langle (a_{i_1}, \ldots, a_{i_l}) \rangle.$$

Note que, por cada subgrupo A_i existen $l - 1$ subgrupos de orden l tales que forman el mismo subgrupo de $G = \mathrm{Gal}(K : k)$. De esta manera se tiene que, la cantidad de subgrupos de orden l en G es precisamente $\frac{l^m-1}{l-1}$. Se sigue de la Proposición 3.3.25 que existen $\frac{l^m-1}{l-1}$ subgrupos en G tales que son isomorfos a G/A_i, es decir si $B_i \subseteq G$

$$B_i \cong G/A_i \quad \text{con} \quad i \in [\![1, \frac{l^m - 1}{l - 1}]\!]. \tag{4.3}$$

La cardinalidad de estos subgrupos es $|B_i| = l.^{m-1}$ Llámese F_i al campo dejado fijo por B_i

$$\begin{array}{c} K \\ {\scriptstyle l^{m-1}}\big| \\ F_i = K^{B_i} \\ {\scriptstyle l}\big| \\ k \end{array}$$

De la teoría de Galois, se concluye que existen ${}^{l^m - 1}\!/_{l - 1}$ subcampos de K/k tales que $[F_i : k] = l$. Se tiene que $e_\infty(K : k)|l$, a continuación se verá que una condición necesaria y suficiente para que $e_\infty(K : k) = l$ es que, en la red de subcampos de la extensión K/k exista al menos un $k \subseteq F_j \subseteq K$ con $[F_j : k] = l$ tal que $\mathfrak{p}_\infty$ se ramifique totalmente, es decir $e_\infty(F_i : k) = l$.
Supóngase que $e_\infty(K : k) = l$, y puesto que

$$K_i \in \mathcal{A} \coloneqq \{F_j \mid [F_j : k] = l, \quad j \in [\![1, \frac{l^m - 1}{l - 1}]\!]\}.$$

Así pues, $K = F_1 \cdots F_{\frac{l^m-1}{l-1}}$. Dado que todas estas extensiones son moderadamente ramificadas, por el Lema de Abhyankar, se sigue que

$$l = e_\infty(K : k) = \mathrm{mcm}[e_\infty(F_1 : k), \ldots, e_\infty(F_{\frac{l^m-1}{l-1}} : k)].$$

Se obtiene que existe al menos un $j \in [\![1, \frac{l^m-1}{l-1}]\!]$ tal que $e_\infty(F_j : k) = l$.

Recíprocamente, si se supone que $e_\infty(F_j : k) = l$ para algún $j \in [\![1, \frac{l^m-1}{l-1}]\!]$, nuevamente por el Lema de Abhyankar se sigue

$$e_\infty(K : k) = \text{mcm}[e_\infty(F_1 : k), \ldots, e_\infty(F_{\frac{l^m-1}{l-1}} : k)]$$

lo que implica $e_\infty(K : k) = l$. En resumen se tiene:

$$e_\infty(K : k) = l \Longleftrightarrow \exists\ j \in \left[\!\!\left[1, \frac{l^m - 1}{l - a}\right]\!\!\right] \text{ tal que } e_\infty(F_j : k) = l. \tag{4.4}$$

El resultado análogo es para el grado de inercia de $\mathfrak{p}_\infty$, es decir:

$$f_\infty(K : k) = l \Longleftrightarrow \exists\ j \in \left[\!\!\left[1, \frac{l^m - 1}{l - a}\right]\!\!\right] \text{ tal que } f_\infty(F_j : k) = l. \tag{4.5}$$

Se probará la necesidad. Supóngase que existe tal j con $f_\infty(F_j : k) = l$. Dado que los grados de inercia en una torre de campos se multiplican

$$f_\infty(K : k) = f_\infty(K : F_j) f_\infty(F_j : k)$$

y del hecho de que $f_\infty(K : k)|l$ se tiene necesariamente que $f_\infty(K : k) = l$. Para probar la suficiencia se procede por inducción sobre m. Para $m = 1$ campos de grado l que generan a K, se vio que la cantidad de campos de grado l sobre k es $\frac{l^m-1}{l-1} = \frac{l-1}{l-1} = 1$, a saber este campo corresponde a $F_1 = K$, por lo que

$$f_\infty(F_j : k) = f_\infty(K : k) = l.$$

Ahora si se supone el resultado cierto para $m - 1$ campos de grado l que generan a K, es decir, si $f_\infty(K : k) = l$ entonces existe $j \in [\![1, \frac{l^{m-1}-1}{l-1}]\!]$ tal que $f_\infty(F_j : k) = l$ y se prueba el resultado para m campos que generan a K de grado l sobre k. Las hipótesis que se tienen son, $f_\infty(K : k) = l$ y que $e_\infty(K : k)|l$ consecuentemente se obtienen dos casos. Primeramente se estudia el caso $e_\infty(K : k) = 1$, lo cual implica que $D_\infty(K : k) \cong C_l$, pues $I_\infty(K : k) = \langle \text{Id} \rangle$.
Sea $H_1 < G$ con

$$|H_1| = l \quad \text{y} \quad H_1 \neq D_\infty(K : k).$$

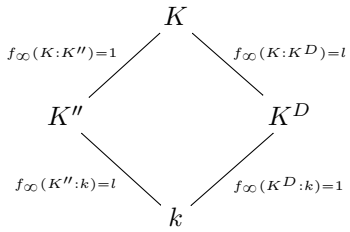
Se denota por K' al campo fijo por H_1, es decir, $K' = K^{H_1}$. Por hipótesis, $H_1 \neq D_\infty(K : k)$ lo que implica $f_\infty(K : K') = 1$ y $f_\infty(K' : k) = l$, dado que K' es el campo generado por $m - 1$ subcampos de grado l sobre k, por la hipótesis de inducción se tiene que existe $j \in [\![1, \frac{l^{m-1}-1}{l-1}]\!]$ con $[F_j : k] = l$ de tal forma que $f_\infty(F_j : k) = l$, en particular este campo F_j pertenece a la red de subcampos de grado l sobre k y se tiene el resultado.

Si $e_\infty(K : k) = l$ se tiene en este caso que $D_\infty(K : k) \cong C_l \times C_l$ puesto que $I_\infty(K : k) \cong C_l$.

Dado que

$$\frac{D_\infty(K:k)}{I_\infty(K:k)} \cong \mathrm{Gal}\Big(\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty : \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty\Big) \cong C_l$$

sea $D \cong \mathrm{Gal}\Big(\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty : \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty\Big)$. Se elige $H_2 < G$ de tal forma que $|H_2| = l$ y además $H_2 \neq D$. Si $K'' = K^{H_2}$, se tiene que $f_\infty(K : K'') = 1$ y $f_\infty(K'' : k) = l$. Ahora como K'' es el campo generado por $m-1$ subcampos de grado l sobre k, se tiene el siguiente diagrama



Nuevamente, por hipótesis de inducción, se tiene que existe $j \in [\![1, \frac{l^{m-1}-1}{l-1}]\!]$ con $k \subseteq F_J \subseteq K'' \subseteq K$ tal que $[F_j : k] = l$ y $f_\infty(F_j : k) = l$. En particular este F_j pertenece a la red de subcampos de grado l sobre k de la extensión K/k.

A continuación se da una representación de los campos F_j. Para esto se reescribe a G de la siguiente manera $G = \mathrm{Gal}(K/k) = \langle \sigma_1, \ldots, \sigma_m \rangle$, donde $\sigma_i(\sqrt[l]{\gamma_j D_j}) = \zeta_l^{\delta_{ij}} \sqrt[l]{\gamma_j D_j}$ y

$$\delta_{ij} = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{si } i \neq j \end{cases}$$

es la delta de Kronecker y ζ_l una raíz l-ésima primitiva de la unidad, pues en el caso Kummer se tiene $\langle \zeta_l \rangle \subseteq k$. En adelante se denotará $\mu_j := \sqrt[l]{\gamma_j D_j}$ y $\zeta = \zeta_l$ por lo que se tiene entonces $\sigma_i(\mu_j) = \zeta^{\delta_{ij}} \mu_j$. Sean $\overrightarrow{\alpha}, \overrightarrow{\beta} \in \mathbb{F}_l^m$ con $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_m)$ y $\overrightarrow{\beta} = (\beta_1, \ldots, \beta_m)$ donde $1 \leqslant \alpha_i, \beta_j \leqslant l-1$ para todo $i, j \in \{1, \ldots, m\}$. Se definen la siguientes aplicaciones:

$$\Lambda(\overrightarrow{\alpha}) := \mu_1^{\alpha_1} \cdots \mu_m^{\alpha_m}$$

$$y$$

$$\sigma(\overrightarrow{\beta}) := \sigma_1^{\beta_1} \cdots \sigma_m^{\beta_m}.$$

Puesto que $\zeta \in k$, los elementos de G lo dejan fijo, es decir, si $\sigma \in G$ se tiene $\sigma(\zeta) = \zeta$. Se hace notar lo que representa $\sigma_i^v(\mu_j^w)$, para esto primeramente observe que:

$$\sigma_i^v(\mu_j) = \overbrace{\sigma_i \cdots \sigma_i}^{v-veces}(\mu_j) = \sigma_i \cdots \sigma_i(\sigma_i(\mu_j)) = \underbrace{\sigma_i \cdots \sigma_i}_{v-1-veces}(\zeta^{\delta_{ij}}\mu_j) \ \cdots = \zeta^{v\delta_{ij}}\mu_j. \tag{4.6}$$

Ahora, si se tiene lo siguiente

$$\sigma_i(\mu_j^w) = \overbrace{\sigma_i(\mu_j)\cdots\sigma_i(\mu_j)}^{w-veces} = \zeta^{\delta_{ij}}\cdots\zeta^{\delta_{ij}}\mu_j = \zeta^{w\delta_{ij}}\mu_j^w, \tag{4.7}$$

de las Ecuaciones 4.6 y 4.7 se sigue que $\sigma_i^v(\mu_j^w) = \zeta^{vw\delta_{ij}}\mu_j^w$. Al combinar las aplicaciones se obtiene lo siguiente:

$$\begin{aligned}
\sigma(\overrightarrow{\beta})\cdot\Lambda(\overrightarrow{\alpha}) &= \sigma_1^{\beta_1}\cdots\sigma_m^{\beta_m}(\mu_1^{\alpha_1}\cdots\mu_m^{\alpha_m}) \\
&= \sigma_1^{\beta_1}\cdots\sigma_{m-1}^{\beta_{m-1}}(\sigma_m^{\beta_m}(\mu_1^{\alpha_1}\cdots\mu_m^{\alpha_m})) \\
&= \sigma_1^{\beta_1}\cdots\sigma_{m-1}^{\beta_{m-1}}(\sigma_m^{\beta_m}(\mu_1^{\alpha_1})\cdots\sigma_m^{\beta_m}(\mu_m^{\alpha_m})) \\
&= \sigma_1^{\beta_1}\cdots\sigma_{m-1}^{\beta_{m-1}}(\zeta^{\beta_m\alpha_1\delta_{m1}}\mu_1^{\alpha_1}\cdots\zeta^{\beta_m\alpha_m\delta_{mm}}\mu_m^{\alpha_m}) \\
&= \sigma_1^{\beta_1}\cdots\sigma_{m-1}^{\beta_{m-1}}(\mu_1^{\alpha_1}\cdots\mu_{m-1}^{\alpha_{m-1}}\cdot\zeta^{\beta_m\alpha_m}\mu_{\alpha_m}) \\
&\ \ \vdots \\
&= \zeta^{\alpha_1\beta_1}\mu_1^{\alpha_1}\cdots\zeta^{\beta_m\alpha_m}\mu_m^{\alpha_m} \\
&= \zeta^{\beta_1\alpha_1+\cdots+\beta_m\alpha_m}\mu_1^{\alpha_1}\cdots\mu_m^{\alpha_m} \\
&= \zeta^{\langle\overrightarrow{\alpha},\overrightarrow{\beta}\rangle}\Lambda(\overrightarrow{\alpha})
\end{aligned}$$

donde $\langle\overrightarrow{\alpha},\overrightarrow{\beta}\rangle = \alpha_1\beta_1+\cdots+\alpha_m\beta_m$. En resumen, se ha obtenido una expresión para las aplicaciones

$$\sigma(\overrightarrow{\beta})\Lambda(\overrightarrow{\alpha}) = \zeta^{\langle\overrightarrow{\alpha},\overrightarrow{\beta}\rangle}\Lambda(\overrightarrow{\alpha}). \tag{4.8}$$

Note que si $\langle\overrightarrow{\alpha},\overrightarrow{\beta}\rangle \equiv 0 \mod l$, entonces $\zeta^{\langle\overrightarrow{\alpha},\overrightarrow{\beta}\rangle} = 1$ donde se obtiene la siguiente condición

$$\sigma(\overrightarrow{\beta})\Lambda(\overrightarrow{\alpha}) = \Lambda(\overrightarrow{\alpha}) \Longleftrightarrow \langle\overrightarrow{\alpha},\overrightarrow{\beta}\rangle \equiv 0 \mod l.$$

Sean $\overrightarrow{\beta}_1,\ldots,\overrightarrow{\beta}_{m-1} \in \mathbb{F}_l^m$ vectores linealmente independientes sobre el campo $\mathbb{F}_q$ y defínase

$$B := \langle\sigma(\overrightarrow{\beta}_1),\ldots,\sigma(\overrightarrow{\beta}_{m-1})\rangle.$$

Observación 4.1.2. Dado que $G \cong C_l^m$, es posible ver a G como un espacio vectorial sobre $\mathbb{F}_l$ y en este caso la red de subgrupos de G coincide con la red de subespacios vectoriales de $\mathbb{F}_l^m$.

Nótese que B es isomorfo al subespacio vectorial generado por $\{\overrightarrow{\beta}_1,\ldots\overrightarrow{\beta}_{m-1}\}$ el cual se denota por V. Sea pues:

$$\begin{aligned}
T : V &\longrightarrow B \\
\gamma_1 &\mapsto \sigma(\gamma_1)
\end{aligned}$$

donde $\gamma_1 = a_1\overrightarrow{\beta}_1 + \cdots + a_{m-1}\overrightarrow{\beta}_{m-1}$ con $a_i \in \mathbb{F}_q$ para $1 \leqslant i \leqslant m-1$. Puesto que $\sigma(\overrightarrow{\beta}_i) \in G$ para

todo $1 \leqslant i \leqslant m-1$, se sigue que $\sigma(a) = a$ para todo $a \in \mathbb{F}_l$, por lo que

$$\begin{aligned} T(a\gamma_1) &= T(a(a_1\overrightarrow{\beta}_1 + \cdots + a_{m-1}\overrightarrow{\beta}_{m-1})) = T(aa_1\overrightarrow{\beta}_1 + \cdots + aa_{m-1}\overrightarrow{\beta}_{m-1}) \\ &= \sigma(aa_1\overrightarrow{\beta}_1 + \cdots + aa_{m-1}\overrightarrow{\beta}_{m-1}) = a\sigma(a_1\overrightarrow{\beta}_1) + \cdots a\sigma(a_{m-1}\overrightarrow{\beta}_{m-1}) \\ &= a\sigma(a_1\overrightarrow{\beta}_1 + \cdots a_{m-1}\overrightarrow{\beta}_{m-1}) = a\sigma(\gamma_1) = aT(\gamma_1). \end{aligned}$$

Sean ahora $\gamma_1 = a_1\overrightarrow{\beta}_1 + \cdots + a_{m-1}\overrightarrow{\beta}_{m-1}$ y $\gamma_2 = b_1\overrightarrow{\beta}_1 + \cdots + b_{m-1}\overrightarrow{\beta}_{m-1}$. Se tiene

$$\begin{aligned} T(\gamma_1+\gamma_2) &= T(a_1\overrightarrow{\beta}_1 + \cdots + a_{m-1}\overrightarrow{\beta}_{m-1} + b_1\overrightarrow{\beta}_1 + \cdots + b_{m-1}\overrightarrow{\beta}_{m-1}) \\ &= T((a_1+b_1)\overrightarrow{\beta}_1 + \cdots + (a_{m-1}+b_{m-1})\overrightarrow{\beta}_{m-1}) \\ &= \sigma((a_1+b_1)\overrightarrow{\beta}_1 + \cdots + (a_{m-1}+b_{m-1})\overrightarrow{\beta}_{m-1}) \\ &= (a_1+b_1)\sigma(\overrightarrow{\beta}_1) + \cdots + (a_{m-1}+b_{m-1})\sigma(\overrightarrow{\beta}_{m-1}) \\ &= a_1\sigma(\overrightarrow{\alpha}_1) + \cdots a_{m-1}\sigma(\overrightarrow{\beta}_{m-1}) + b_1\sigma(\overrightarrow{\beta}_1) + \cdots + b_{m-1}\sigma(\overrightarrow{\beta}_{m-1}) \\ &= T(\gamma_1) + T(\gamma_2). \end{aligned}$$

Claramente se tiene que T es una transformación lineal biyectiva y por lo tanto se concluye $V \cong B$ como $\mathbb{F}_l$-espacios vectoriales. Ahora, dado que $\dim(V) = l^{m-1}$ se tiene $B \cong \mathbb{F}_l^{m-1}$ y por tanto $|B| = l^{m-1}$. Continuando con el espacio vectorial $\mathbb{F}_l^m$ sobre $\mathbb{F}_l$ se tiene que la cantidad de subespacios cuya dimensión es $m-1$ es precisamente:

$$\begin{aligned} \frac{(l^m-1)(l^m-l)\cdots(l^m-l^{m-2})}{(l^{m-1}-1)(l^{m-1}-l)\cdots(l^{m-1}-l^{m-2})} &= \frac{(l^m-1)l(l^{m-1}-1)\cdots l(l^{m-1}-l^{m-3})}{(l^{m-1}-1)(l^{m-1}-l)\cdots(l^{m-1}-l^{m-2})} \\ &= \frac{l^{m-2}(l^m-1)(l^{m-1}-1)\cdots(l^{m-1}-l^{m-3})}{(l^{m-1}-1)(l^{m-1}-l)\cdots(l^{m-1}-l^{m-2})} \\ &= \frac{l^{m-2}(l^m-1)}{l^{m-1}-l^{m-2}} = \frac{l^m-1}{l-1}. \end{aligned}$$

En resumen se tiene que existen $\frac{l^m-1}{l-1}$ subespacios de $\mathbb{F}_l^m$ cuya dimensión es l^{m-1}, luego por la Observación 4.1.2 se concluye que existen $\frac{l^m-1}{l-1}$ subgrupos de G tales que tienen orden l^{m-1}.

Téngase en cuenta, que $\Lambda(\overrightarrow{\alpha}) = \mu_1^{\alpha_1}\cdots\mu_m^{\alpha_m} \in K$, y de la Ecuación (4.8) se obtuvo una condición, en la cual estos elementos de K son dejados fijos bajo el subgrupo B, es decir

$$\begin{aligned} &\{\Lambda(\overrightarrow{\alpha}) \mid \sigma(\overrightarrow{\beta}_i)\Lambda(\overrightarrow{\alpha}) = \Lambda(\overrightarrow{\alpha}) \text{ para todo } 1 \leqslant i \leqslant m-1\} \\ =&\{\Lambda(\overrightarrow{\alpha}) \mid \langle\overrightarrow{\alpha}, \overrightarrow{\beta}_i\rangle \equiv 0 \mod l \text{ para todo } 1 \leqslant i \leqslant m\} \\ =&\{\Lambda(\overrightarrow{\alpha}) \mid \langle\overrightarrow{\alpha}, \overrightarrow{\beta}_i\rangle = 0 \text{ para todo } 1 \leqslant i \leqslant m\}, \end{aligned} \tag{4.9}$$

donde $\overrightarrow{\beta_i} = (\beta_{1i}, \ldots \beta_{mi})$ para todo $1 \leqslant i \leqslant m-1$, y $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_m)$. Además, recordando lo que representa $\langle\overrightarrow{\alpha}, \overrightarrow{\beta}_i\rangle$, note que se está obteniendo de la igualdad anterior un sistema de ecuaciones

lineales, a saber:

$$\begin{aligned}
&\beta_{11}\alpha_1 + \cdots + \beta_{m1}\alpha_m = 0\\
&\beta_{12}\alpha_1 + \cdots + \beta_{m2}\alpha_m = 0\\
&\vdots\\
&\beta_{1m-1}\alpha_1 + \cdots + \beta_{mm-1}\alpha_m = 0,
\end{aligned}$$

el cual es posible representar en forma matricial, es decir

$$\underbrace{\begin{bmatrix} \beta_{11} & \cdots & \beta_{m1} \\ \beta_{12} & \cdots & \beta_{m2} \\ . & & \\ . & & \\ . & & \\ \beta_{1m-1} & \cdots & \beta_{mm-1} \end{bmatrix}}_{C} \underbrace{\begin{bmatrix} \alpha_1 \\ \alpha_2 \\ . \\ . \\ . \\ \alpha_m \end{bmatrix}}_{X} = \begin{bmatrix} 0 \\ 0 \\ . \\ . \\ . \\ 0 \end{bmatrix}.$$

De la elección de los vectores $\overrightarrow{\beta}_1, \ldots, \overrightarrow{\beta}_{m-1}$ linealmente independientes, se tiene que la matriz C es de rango $m-1$, por lo que la dimensión del espacio solución del sistema de ecuaciones lineales homogéneo $CX = 0$ es $m-(m-1) = 1$ donde m es el número de incógnitas y $m-1$ el rango de la matriz de coeficientes que en este caso corresponde a la matriz C. Entonces el espacio solución tiene rango 1 sobre $\mathbb{F}_l$, es decir, existe $\overrightarrow{\alpha}_0 \neq 0$ solución de $CX = 0$.

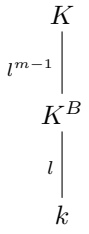
Resumiendo, se ha obtenido que, para cualquier conjunto de $m-1$-vectores linealmente independiente $\{\overrightarrow{\beta}_1, \ldots, \overrightarrow{\beta}_{m-1}\}$ de $\mathbb{F}_l^m$ es posible formar un subespacio vectorial, el cual se puede asociar a un subgrupo de G de orden l^{m-1} a saber $B = \langle \sigma(\overrightarrow{\beta}_1), \ldots, \sigma(\overrightarrow{\beta}_{m-1}) \rangle$. Se probó la existencia de un vector $\overrightarrow{\alpha}_0$ que da solución al sistema de ecuaciones lineales que se obtuvo del desarrollo en 4.9 el cual nos describe los elementos de K que son dejados fijos por el subgrupo B, es decir

$$\begin{aligned}
&\{\Lambda(\overrightarrow{\alpha}_0) \mid \langle \overrightarrow{\alpha}_0, \overrightarrow{\beta}_i \rangle = 0 \text{ para todo } 1 \leqslant i \leqslant m-1\}\\
=&\{\mu_1^{\alpha_{10}} \cdots \mu_m^{\alpha_{m0}} \mid \langle \overrightarrow{\alpha}_0, \overrightarrow{\beta}_i \rangle = 0 \text{ para todo } 1 \leqslant i \leqslant m-1\}.
\end{aligned}$$

Entonces el campo fijo de K bajo B es

$$F_{\overrightarrow{\alpha}_0} = K^B = k(\mu_1^{\alpha_{10}} \cdots \mu_m^{\alpha_{m0}}).$$

Recordando que $\mu_i = \sqrt[l]{\gamma_i D_i}$, se sigue que $F_{\overrightarrow{\alpha}_0} \neq k$,

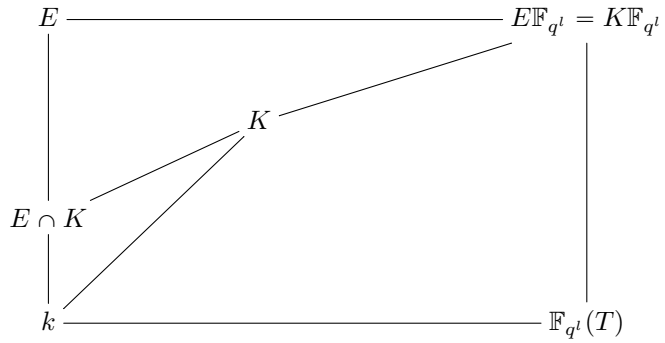


Todos estos subcampos tienen la particularidad de que son de grado l sobre k, es decir $[K^B : k] = l$. Ahora de (4.6) y de la red de subgrupos de G que son de orden l^{m-1} se sigue que todos los subcampos $k \subseteq F_j \subseteq K$ tales que $[F_j : k] = l$ son de la forma

$$F_j = k(\mu_1^{\alpha_1} \cdots \mu_m^{\alpha_m}),$$

donde $(\alpha_1, \ldots, \alpha_m) \neq (0, \ldots, 0)$ y $j \in [\![1, \frac{l^{m-1}-1}{l-1}]\!]$.

Continuando con el caso $E \neq K$, esto es, cuando existe al menos un $1 \leqslant i \leqslant m$ tal que $\gamma_i \not\equiv (-1)^{\mathrm{gr}\, D_i} \mod (\mathbb{F}_q^*)^l$, se probó EK es una extensión de constantes tanto de E como de K, es decir $EK = K_l = E_l$.



Se sabe del Teorema 3.2.14 que $f_\infty(E : k) = 1$ pues $k \subseteq E \subseteq k(\Lambda_N)$. Del Teorema 2.2.32 se sigue:

$$f_\infty(\mathbb{F}_{q^l}(T) : k) = \frac{l}{\mathrm{mcd}(d_k(\mathfrak{p}_\infty), l)}$$

y como $d_k(\mathfrak{p}_\infty) = 1$ se sigue que $f_\infty(\mathbb{F}_{q^l}(T) : k) = l$, es decir $\mathfrak{p}_\infty$ es totalmente inerte en $\mathbb{F}_{q^l}(T)/k$. Puesto que $K\mathbb{F}_{q^l}(T)/k$ es una extensión l-elemental abeliana, se sabe que el grupo de inercia debe ser un grupo cíclico y que

$$\frac{D_\infty(K\mathbb{F}_{q^l}(T) : k)}{I_\infty(K\mathbb{F}_{q^l}(T) : k)} \cong \mathrm{Gal}\Big(\mathcal{O}_{\mathfrak{P}_\infty}/\mathfrak{P}_\infty : \mathcal{O}_{\mathfrak{p}_\infty}/\mathfrak{p}_\infty\Big)$$

se tiene que $f_\infty(K\mathbb{F}_{q^l}(T) : k) = 1$ o l, pero, en el párrafo anterior se tiene que $f_\infty(\mathbb{F}_{q^l}(T) : k) = l$,

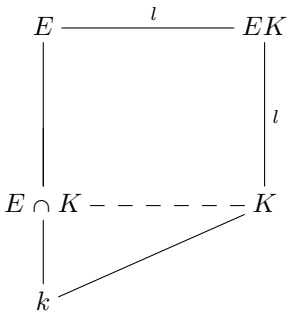
lo cual implica que $f_\infty(K\mathbb{F}_{q^l}(T) : k) = l$. Considérese la siguiente torre de campos $k \subseteq K \subseteq EK = K\mathbb{F}_{q^l}$, de esta manera se tienen las siguientes condiciones:

$$f_\infty(EK : k) = l \Longleftrightarrow f_\infty(K : k) = 1. \tag{4.10}$$

Sea $H' := D_\infty(EK : K)$ así que $f_\infty(EK : K) = |H'|$, se sigue entonces de (4.10) que

$$|H'| \neq 1 \Longleftrightarrow f_\infty(K : k) = 1.$$

Considere el siguiente cuadro de Galois



Puesto que las extensiones E/k y EK/K son de grados l^m y l respectivamente, de la correspondencia de Galois, K corresponde a $E \cap K$ en la extensión E/k y por lo tanto $[E \cap K : k] = l^{m-1}$.

Para el cálculo del campo de géneros de K es necesario entender el comportamiento de $\mathfrak{p}_\infty$, para lo cual se analiza primeramente el comportamiento del primo infinito en el caso ciclotómico, lo que ya se estudió en la sección anterior. Entonces, si $f_\infty(EK : K) = l$ y dado que no hay inercia en el caso ciclotómico, es decir $f_\infty(E : k) = 1$, si se considera $H|_E$ necesariamente se debe tener $H|_E = I_\infty(E : k)$, en efecto

$$1 = f_\infty(E : k) = \Big|\frac{D_\infty(E : k)}{I_\infty(E : k)}\Big|$$

entonces $D_\infty(E : k) = I_\infty(E : k)$ y por lo tanto $H|_E = I_\infty(K : k)$ y en particular $e_\infty(E : k) = l$. Del Caso 2 se obtuvo el campo de géneros cuando $\mathfrak{p}_\infty$ se ramifica en E/k, es decir, cuando $e_\infty(E : k) = l$ y esté corresponde a $E_{ge} = L = k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*})$. Entonces, si $f_\infty(EK : K) = l$ se tiene $H' \cong C_l$. Así el subcampo $E_{ge}^{H_1}$ que es dejado fijo por subgrupo H_1 de $\mathrm{Gal}(E_{ge}/k)$ que es isomorfo a H' es una subextensión de E_{ge} de grado l, es decir, $[E_{ge} : E_{ge}^{H'}] = l$.

Anteriormente se probó que $M = k(\sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_{r-1}})$ es un subcampo de la extensión L/E de tal forma que $[L : M] = l$. A continuación se da una representación del subcampo $E_{ge}^{H_1}$ y para esto se prueba que $M = E_{ge}^{H_1}$ para lo cual basta con ver $M \subseteq E_{ge}^{H_1}$. Recuérdese que cada $Q_i = P_i P_r^{-bd_i}$, donde $d_i = \mathrm{gr}\, P_i$. También se probó que $l | \mathrm{gr}\, Q_i$ para todo $1 \leqslant i \leqslant r-1$, por lo que $\mathfrak{p}_\infty$ se descompone en M/E. Ahora bien $H = D_\infty(EK : k)$ y $H|_E = I_\infty(E : k)$, dado que se está en una extensión ciclotómica. Se sigue que $\mathfrak{p}_\infty$ no se ramifica en $E_{ge}^{H_1}/E$ existiendo únicamente descomposición. De esta manera se tiene $M \subseteq E_{ge}^{H_1}$ y al ser subextensiones de E_{ge} de grado l, se

concluye que

$$E_{ge}^{H_1} = L^{H_1} = M. \tag{4.11}$$

El resultado que se escribe a continuación nos dice cómo está dado el campo de géneros de una extensión abeliana finita K/k.

Teorema 4.1.3. *Sea K una extensión geométrica finita y abeliana de k donde $\mathfrak{p}_\infty$ es moderadamente ramificado. Sea*

$$E \coloneqq K\mathbb{F}_{q^m}(T) \cap k(\Lambda_N).$$

Entonces

$$K_{ge} = E_{ge}^{H_1} K = (E_{ge}K)^H \tag{4.12}$$

donde H es el grupo de descomposición de cualquier primo en $S_\infty(K)$, que corresponde al conjunto de primos infinitos de K encima de $\mathfrak{p}_\infty$ en $E_{ge}K/K$, $H_1 \coloneqq H|_{E_{ge}}$ y $H_2 \coloneqq H_1|E$.
Sea $d \coloneqq f_\infty(EK : K)$. Se tiene $H \cong H_1 \cong H_2 \cong C_d$ y $d|q-1$. También se tiene que $E_{ge}K/K_{ge}$ y $EK/E^{H_2}K$ son extensiones de constantes de grado d. Finalmente, el campo de constantes de K_{ge} es $\mathbb{F}_{q^t}$, donde t es el grado de $S_\infty(K)$ en K.

Demostración. Ver [2, Theorem 2.2]. □

Ahora se tiene la herramienta necesaria para describir todos los casos del campo de géneros de $K = k(\sqrt[l]{D_1}) \cdots k(\sqrt[l]{D_m})$. Antes de comenzar se recuerda parte de la notación que se da al principio, con el objetivo de facilitar su comprensión. Sea $K = K_1 \cdots K_m$ donde cada $K_i = k(\sqrt[l]{\gamma_i D_i})$ para $1 \leqslant i \leqslant m$ y cada $D_i = P_1^{\beta_{1i}} \cdots P_r^{\beta_{ri}}$ donde $1 \leqslant \beta_{ij} \leqslant l-1$, además $\gamma_1, \ldots, \gamma_m \in \mathbb{F}_q^*$. Se denota por S al conjunto de polinomios irreducibles que dividen a algún D_j, es decir, $S = \{P_1, \ldots, P_r\}$. Esta extensión abeliana tiene como grupo de Galois a $G = \mathrm{Gal}(K/k) \cong C_l^m$, por otro lado se recuerda que estos $P_i's$ se arreglan de tal forma que $l|\mathrm{gr}\ P_i$ para $1 \leqslant i \leqslant s$ y $l \nmid \mathrm{gr}\ P_j$ para $s+1 \leqslant j \leqslant r$ con $0 \leqslant s \leqslant r$, especificando que $s = 0$ significa que $l \nmid \mathrm{gr}\ P_1$. Sean $n_i = \mathrm{gr}\ D_i$ y $d_j = \mathrm{gr}\ P_j$ con $1 \leqslant i \leqslant m$ y $1 \leqslant j \leqslant r$.

Cuando $s \leqslant r-1$, esto es, si $l \nmid \mathrm{gr}\ P_r$, sea $Q_i = P_1 P_r^{-bd_i}$ para $1 \leqslant i \leqslant r-1$ y sean $a, b \in \mathbb{Z}$ tales que $al + bd_r = 1$ y $M = k(\sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_{r-1}})$. Con estas notaciones ahora nos es posible describir todos los casos del campo de géneros de K cuando existe algún i tal que $\xi_i \notin (\mathbb{F}_q^*)^l$, esto es, cuando $E \neq K$.

Caso 4: $l|\mathrm{gr}\ P_i$ para todo $1 \leqslant i \leqslant r$.

En el Caso 1 se probó que el campo de géneros de E es $E_{ge} = E_{gex} = L$. Como $\mathfrak{p}_\infty$ se descompone totalmente en E_{ge}/K entonces $H|_{E_{ge}} = \langle \mathrm{Id} \rangle$ y dado que $H_1 = H|_{E_{ge}}$, se concluye que

$$K_{ge} = E_{ge}^{H_1} K = LK.$$

Caso 5: $l|n_j$ **para todo** $1 \leqslant j \leqslant m$ **y** $s < r$**.**

En el Caso 3 se probó que el campo de géneros de E es $E_{ge} = M$. Nuevamente en este caso tenemos que $\mathfrak{p}_\infty$ se descompone totalmente en E_{ge}/E y al ser $H_1 = H|_{E_{ge}}$ se sigue que H_1 es el subgrupo identidad. Así que

$$K_{ge} = E_{ge}^{H_1} K = MK.$$

Note que las subextensiones F_j/k de K/k de grado l sobre k juegan un papel importante para describir en ciertos casos el campos de géneros de K. Sea $F_j = k(\mu_1^{\alpha_{1j}} \cdots \mu_m^{\alpha_{mj}})$ donde $(\alpha_{1j}, \ldots, \alpha_{mj}) \in \mathbb{F}_l^m \backslash \{\overrightarrow{0}\}$ y $\mu_i = \sqrt[l]{\gamma_i D_i}$, para $1 \leqslant i \leqslant m$, por lo que

$$\operatorname{gr}\left((\mu_1^{\alpha_{1j}} \cdots \mu_m^{\alpha_{mj}})\right) = \sum_{i=1}^{m} \frac{\alpha_{ij} n_i}{l}.$$

Al considerar esta extensión, note que

$$l = [F_j : k] = e_\infty(F_j : k) f_\infty(F_j : k) h_\infty(F_j : k).$$

Dado que l es primo, solamente se tienen tres posibilidades y éstas son: $e_\infty(F_j : k) = l$, es decir, $\mathfrak{p}_\infty$ se ramifica en F_j/k, $f_\infty(F_j : k) = l$, es decir, $\mathfrak{p}_\infty$ es inerte en F_j/k y $h_\infty(F_j : k) = l$, es decir, $\mathfrak{p}_\infty$ se descompone en F_j/k. A continuación se presentan el campo de géneros de K considerando el comportamiento de $\mathfrak{p}_\infty$ en las extensiones F_j/k.

Caso 6: $l \nmid n_j$ **para algún** $1 \leqslant j \leqslant m$ **y** $\mathfrak{p}_\infty$ **se ramifica o es inerte para alguna extensión** F_j/k **con** $j \in [\![1, \frac{l^m - 1}{l-1}]\!]$**.**

Del Caso 2 se obtuvo que el campo de géneros de E es $E_{ge} = E_{gex} = L$. Note que, si para algún $F_j = k(\mu_1^{\alpha_{1j}} \cdots \mu_m^{\alpha_{mj}})$, donde $(\alpha_{1j}, \ldots, \alpha_{mj}) \in \mathbb{F}_l^m \backslash \{0\}$ y $\mu_i = \sqrt[l]{\gamma_i D_i}$ para $1 \leqslant i \leqslant m$, es tal que:

1. Si $l \nmid \sum_{i=1}^{m} \frac{\alpha_{ij} n_i}{l}$ entonces $\mathfrak{p}_\infty$ se ramifica en F_j/k y de la torre de campos $k \subseteq F_j \subseteq K \subseteq E_{ge}K$ se tiene que el grupo de descomposición de $\mathfrak{p}_\infty$ en $E_{ge}K/K = \langle \mathrm{Id} \rangle$.

2. Si $l | \sum_{i=1}^{m} \frac{\alpha_{ij} n_i}{l}$ y $\gamma_1^{\alpha_1 j} \cdots \gamma_m^{\alpha_{mj}} \notin (\mathbb{F}_q^*)^l$, entonces $\mathfrak{p}_\infty$ es totalmente inerte en F_j/k, es decir, $f_\infty(F_j : k) = l$. Luego de (4.5) y (4.10) se sigue que $f_\infty(EK : K) = 1$, lo que es equivalente a que $H = \langle \mathrm{Id} \rangle$.

De ambos casos se concluye que el campo de géneros de K corresponde a

$$K_{ge} = E_{ge}^{H_1} K = LK.$$

Caso 7: $l \nmid n_j$ para algún $1 \leqslant j \leqslant m$ y $\mathfrak{p}_\infty$ se descompone en todas la extensiones F_j/k con $j \in [\![i, \frac{l^m-1}{l-1}]\!]$.

En el Caso 3 se probó que $E_{ge} = L$ y como $\mathfrak{p}_\infty$ se descompone en todas las extensiones F_j/k, se tiene que $f_\infty(F_j : k) = 1$ para todo $j \in [\![1, \frac{l^m-1}{l-1}]\!]$. De (4.5) se sigue $f_\infty(K : k) = 1$ y de (4.10) se sigue que $f_\infty(EK : k) = l$ por lo tanto $H_1 \cong D_\infty(EK : k) \cong C_l$. De la Ecuación (4.11) se sigue que, el campo de géneros de K es

$$K_{ge} = E_{ge}^{H_1} K = L^{H_1} K = MK.$$

En resumen y para finalizar con el caso Kummer se tiene el siguiente teorema donde se describen a continuación todos los posibles campos de géneros de K:

Teorema 4.1.4. *Sea K/k una extensión de campos de funciones congruentes, donde $K = K_1 \cdots K_m$ con $K_t = k(\sqrt[l]{\gamma_t D_t})$ y $\gamma_t \in \mathbb{F}_q^*$ con $\mathrm{Gal}(K/k) = C_l^m$. Sean $\xi_t := (-1)^{\mathrm{gr}\, D_t}\gamma_t$ y $S = \{P_1, \ldots, P_r \in R_T^+ \mid P_i | D_t \quad \text{para algún} \quad 1 \leqslant t \leqslant m\}$. Se denota por $n_t = \mathrm{gr}\, D_t$ y $d_i = \mathrm{gr}\, P_i$ para $1 \leqslant t \leqslant m$ y $1 \leqslant i \leqslant r$. Sean*

$$E := K\mathbb{F}_{q^{m_0}} \cap k(\Lambda_N)$$

y

$$L = k(\sqrt[l]{P_1^*}, \ldots, \sqrt[l]{P_r^*}).$$

Los $P_i's$ están arreglados de tal forma que $l | d_i$ $1 \leqslant i \leqslant s$ y $l \nmid P_j$, $s+1 \leqslant j \leqslant r$, $0 \leqslant s \leqslant r$. Si $s \leqslant r-1$, esto es, si $l \nmid d_r$, sea $Q_i := P_i P_r^{-bd_i}$, $1 \leqslant i \leqslant r-1$ con $al + bd_r = 1$ y sea $M = k(\sqrt[l]{Q_1}, \ldots, \sqrt[l]{Q_{r-1}})$. Entonces el campo de géneros K_{ge} de K es:

(a) Si $\xi_i \in (\mathbb{F}_q^*)^l$ $\forall\, 1 \leqslant i \leqslant m$ y $s = r$, entonces $K_{ge} = E_{ge} = L$.

(b) Si $\xi_i \in (\mathbb{F}_q^*)^l$ $\forall\, 1 \leqslant i \leqslant m$, $s < r$ y $l \nmid n_j$ para algún $1 \leqslant j \leqslant m$, entonces $K_{ge} = E_{ge} = L$.

(c) Si $\xi_i \in (\mathbb{F}_q^*)^l$ $\forall\, 1 \leqslant i \leqslant m$, $s < r$ y $l | n_j$ para toda $1 \leqslant j \leqslant m$ entonces $K_{ge} = E_{ge} = M$.

(d) Si $\xi_i \notin (\mathbb{F}_q^*)^l$ para algún $1 \leqslant i \leqslant m$ y $s = r$, entonces $K_{ge} = E_{ge}K = LK$.

(e) Si $\xi_i \notin (\mathbb{F}_q^*)^l$ para algún $1 \leqslant i \leqslant m$ y $l | n_j$ para todo $1 \leqslant j \leqslant m$, $(s < r)$, entonces $K_{ge} = E_{ge}K = MK$.

(f) Si $\xi_i \notin (\mathbb{F}_q^*)^l$ para algún $1 \leqslant i \leqslant m$ y $l \nmid n_j$ para algún $1 \leqslant j \leqslant m$, $(s < r)$, y $l \nmid \sum_{i=1}^m \frac{\alpha_{ij} n_i}{l}$ o si $l | \sum_{i=1}^m \frac{\alpha_{ij} n_i}{l}$ y $\gamma_1^{\alpha_{1j}} \cdots \gamma_m^{\alpha_{mj}} \notin (\mathbb{F}_q^*)^l$ para algún $(\alpha_{1j}, \ldots \alpha_{mj}) \in \mathbb{F}_l^m \backslash \{\overrightarrow{0}\}$, entonces $K_{ge} = E_{ge}K = LK$.

(g) Si $\xi_i \notin (\mathbb{F}_q^*)^l$ para algún $1 \leqslant i \leqslant m$ y $l \nmid n_j$ para algún $1 \leqslant j \leqslant m$, $(s < r)$, y $l | \sum_{i=1}^m \frac{\alpha_{ij} n_i}{l}$ y $\gamma_1^{\alpha_{1j}} \cdots \gamma_m^{\alpha_{mj}} \in (\mathbb{F}_q^*)^l$ para todo $(\alpha_{1j}, \ldots \alpha_{mj}) \in \mathbb{F}_l^m \backslash \{\overrightarrow{0}\}$, entonces $K_{ge} = E_{ge}^{H_1} K = MK$.

4.2. Caso no Kummer

Para el caso no Kummer, es decir cuando $l \nmid q-1$, dado que K/k es una extensión de Galois moderadamente ramificada de campos de funciones congruentes, se tiene que el grupo de inercia de cualquier primo resulta ser un grupo cíclico pues, éste es isomorfo al grupo de Galois de los campos residuales de K/k y a su vez ésta es una extensión de un campo finito. Puesto que $G = \mathrm{Gal}(K/k) = C_l^m$, $I_\infty(K:k) = C_l$ o $\langle \mathrm{Id} \rangle$ ya que éstos son los únicos subgrupos cíclicos de G. El siguiente resultado nos dará información de la ramificación de $\mathfrak{p}_\infty$ en la extensión K/k

Proposición 4.2.1. *Sea K/k una extensión abeliana finita de campos de funciones globales, $P \in R_T^+$ y $d = \mathrm{gr}\, P$. Suponga que P es moderadamente ramificada en K/k. Si $e = e_P(K:k)$ denota el índice de ramificación de P en K/k, entonces $e|q^d-1$, donde el campo de constantes de K es $\mathbb{F}_q$.*

Demostración. Ver [19, Proposición 10.4.8]. □

Tenemos que el grupo de inercia de $\mathfrak{p}_\infty$ en la extensión K/k es isomorfo a C_l o es la identidad. Suponga que $I_\infty(K:k) \cong C_l$. Entonces $e_\infty(K:k) = l$ y dado que $\mathrm{gr}\,\mathfrak{p}_\infty = 1$ lo que implica $l|q^1-1$, lo cual es una contradicción, a la hipótesis que es $l \nmid q-1$. Por lo tanto $e_\infty(K:k) = 1$, es decir $\mathfrak{p}_\infty$ no es ramificado en K/k. Ahora, observe que nuevamente se presentan dos casos más, esto es si K está contenido o no en un campo ciclotómico.

4.2.1. Campo de géneros cuando K es ciclotómico

Sea ahora $K \subseteq k(\Lambda_N)$ para algún $N \in R_T$. Sea $E \coloneqq K\mathbb{F}_{q^m}(T) \cap k(\Lambda_N)$, con $m_0 \in \mathbb{N}$. En la Sección 4.1 se obtuvo que en el caso ciclotómico se tiene $E = K = K_1 \cdots K_m$ y se denota $E_i = K_i$, donde E_i/k es una extensión de grado l y tal que $\mathrm{Gal}(E_i/k) \cong C_l$, para todo $1 \leqslant i \leqslant m$, así $G = \mathrm{Gal}(E/k) \cong C_l^m$. Sea $\chi_i \in \widehat{G}$ el caracter de Dirichlet asociado a E_i y sea $X \coloneqq \langle \chi_1, \ldots, \chi_m \rangle$ el grupo de caracteres de Dirichlet asociado a E. Al ser χ_i el caracter que corresponde a E_i, es decir $E_i = k(\Lambda_N)^{\langle \chi_i \rangle^\perp}$ y puesto que E_i/k es una extensión cíclica de grado l con $\mathrm{Gal}(E_i/k) \cong \langle \chi_i \rangle$ de manera no directa, se tiene que $\circ(\chi_i) = l$, esto para todo $1 \leqslant i \leqslant m$. Sea $X_P = \{\chi_P \mid \chi \in X\}$, con $P \in R_T^+$. Si χ_P aparece como factor no trivial en algún $\chi \in X$, entonces $X_P = \langle \chi_P \rangle$ y por tanto $\circ(X_P) = l$. Si χ_P no aparece como factor no trivial para todo $\chi \in X$, entonces $X_P = \langle 1 \rangle$ y por tanto $\circ(X_P) = 1$. Note que en ambos casos $\circ(X_P)|l$ para todo $P \in R_T^+$.

Sean el conjunto S y L el campo asociado a Y, esto es $L = k(\Lambda_N)^{Y^\perp}$, como en la Sección 4.1. Se sigue que $e_P(L:E) = 1$, más aún, se tiene $e_\infty(L:k) = 1$, es decir en L/E ningún primo se ramifica y puesto que K es ciclotómico, se tiene que $f_\infty(k(\Lambda_N):k) = 1$. Se sigue que $\mathfrak{p}_\infty$ se descompone totalmente en L/k, por lo cual se concluye que $E_{ge} = L$. Cabe señalar que en el caso Kummer se tiene explícitamente el campo de géneros de K, pues las extensiones de Kummer se expresan por medio de extensiones radicales. Para el caso actual se dará una representación mediante la aritmética de los caracteres de Dirichlet. Dado que la cantidad de primos ramificados en E/k es

finita, sea entonces $S = \{P_1, \ldots, P_r\}$ el conjunto de los primos de k ramificados en K/k, luego, para cada $P_i \in S$ se tiene

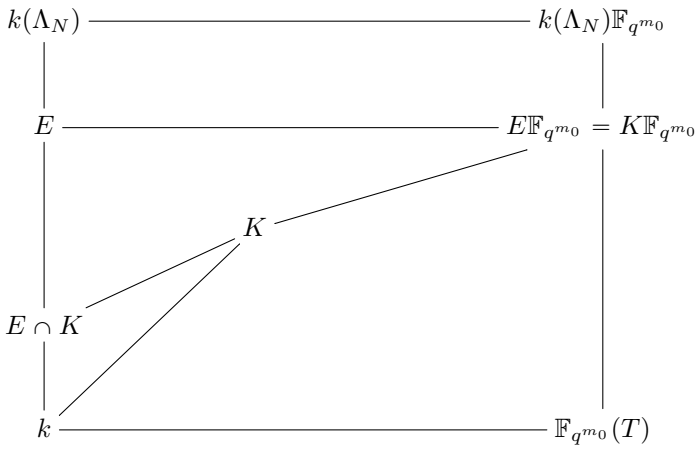
$$\begin{array}{c} k(\Lambda_{P_i}) \\ | \\ k(\Lambda_{P_i})^{X_{P_i}^{\perp}} \\ | \\ k \end{array}$$

donde $k(\Lambda_{P_i})/k$ es la extensión ciclotómica de grado $[k(\Lambda_{P_i}) : k] = \Phi(P_i) = q^{\operatorname{gr} P_i} - 1$, con P_i el único primo ramificado. Se define $F_i \coloneqq k(\Lambda_{P_i})^{X_{P_i}^{\perp}}$. Entonces F_i es el único subcampo de $k(\Lambda_{P_i})/k$ de grado l sobre k, es decir, $k \subseteq F_i \subseteq k(\Lambda_{P_i})$ es tal que $[F_i : k] = l$ la cual es una extensión cíclica. Por lo tanto $l | q^{\operatorname{gr} P_i} - 1$, esto para todo $1 \leqslant i \leqslant r$. En resumen F_i/k es una extensión cíclica de grado l sobre k donde F_i es el campo asociado a X_{P_i} y por tanto $F_1 \cdots F_r \subseteq k(\Lambda_{P_1 \cdots P_r})$ donde los elementos de S son los únicos primos ramificados en L/k con índice de ramificación $e_{P_i}(F_1 \cdots F_r : k) = |X_{P_i}| = e_{P_i}(E : k) = l$. Por tanto en $F_1 \cdots F_r/E$ no se ramifica ningún primo. Se concluye que

$$E_{ge} = F_1 \cdots F_r.$$

4.2.2. Campo de géneros cuando K no es ciclotómico

Ahora, supóngase que K no está contenido en ningún campo ciclotómico, por lo que $EK \neq K$, donde E está dado como antes.



Se mencionó anteriormente que EK/K es una extensión de constantes por lo que ningún primo se ramifica. Sea $H' = D_\infty(EK : K)$ el grupo de descomposición de $\mathfrak{p}_\infty$ en EK/K. También se tiene que $H'|_E = I_\infty(E : k)$, de manera similar al Caso 6 se sabe que $e_\infty(E : k) = 1$ por lo que $H' = \langle \mathrm{Id} \rangle$ y como $H_1 \cong H'$, del Teorema 4.1.3 se concluye

$$K_{ge} = E_{ge}^{H_1} K = E_{ge} K = LK.$$

Resumiendo, para el caso $l \nmid q-1$ se tiene el siguiente teorema donde se describe el campo de géneros de K.

Teorema 4.2.2. *Sea K/k una extensión de campos de funciones congruentes, donde $K = K_1 \cdots K_m$ con $\mathrm{Gal}(K/k) = C_l^m$ con $l \nmid q-1$. Sea $S = \{P_1, \ldots, P_r\} \subseteq R_T^+$ el conjunto de primos de k ramificados en K. Entonces el campo de géneros de K está dado de la siguiente forma*

(a) Si $K \subseteq k(\Lambda_N)$, entonces

$$K_{ge} = E_{ge} = L,$$

donde $L = F_1 \cdots F_r$ con F_i el campo asociado al caracter χ_{P_i} para $1 \leqslant i \leqslant r$.

(b) Si $K \subsetneq k(\Lambda_N)$, entonces

$$K_{ge} = E_{ge}K = LK,$$

donde $L = F_1 \cdots F_r$ con F_i el campo asociado al caracter χ_{P_i} para $1 \leqslant i \leqslant r$.

Capítulo 5

Conclusiones y perspectivas

Las técnicas usadas por Leopoldt mediante la herramienta de caracteres de Dirichlet, se emplearon en el resultado central del presente trabajo, que fue el cálculo explícito del campo de géneros de una extensión l-elemental abeliana de un campo de funciones racionales contenida en un campo ciclotómico. Así mismo se siguen las ideas del Teorema 2.2 de [2] para el caso no ciclotómico.

El Teorema 4.1.4 generaliza el Teorema de Peng a extensiones de Kummer más generales, donde se obtienen los diversos campos de géneros, dada la relación de los grados de de los polinomios P_i's y D_j's con respecto al primo l.

En el Teorema 4.2.2 resulta ser que no existe ramificación de $\mathfrak{p}_\infty$ en la extensión K/k, lo cual da lugar a sólo dos casos para campo de géneros. En este caso no se tiene una representación explícita del campo de géneros, como en el caso Kummer, como extensiones radicales.

Es interesante pensar una extensión abeliana K/k donde el grupo de Galois sea isomorfo a $C_{l_1} \times C_{l_2}$ con l_1 y l_2 números primos diferentes y distintos de la característica de k. Otro caso interesante para estudiar sería si $l_1 | q-1$ mientras que $l_2 \nmid q-1$, es decir se combinarían los casos Kummer y no Kummer.

Bibliografía

[1] S. Bae and J. K. Koo. Genus theory for function fields. *Journal of the Australian Mathematical Society*, 60(3):301–310, 1996.

[2] J. F. Barreto-Castaneda, C. Montelongo-Vazquez, C. D. Reyes-Morales, M. Rzedowski-Calderón, and G. Villa-Salvador. Genus fields of abelian extensions of rational congruence function fields, II. *Rocky Mountain Journal of Mathematics*, 48(7):2099–2133, 2018.

[3] V. Bautista-Ancona, M. Rzedowski-Calderón, and G. Villa-Salvador. Genus fields of cyclic l-extensions of rational function fields. *International Journal of Number Theory*, 9(05):1249–1262, 2013.

[4] R. Clement. The genus field of an algebraic function field. *Journal of Number Theory*, 40(3): 359–375, 1992.

[5] K. Conrad. The Galois correspondence at work. *Expository work. https://kconrad. math. uconn. edu/blurbs/galoistheory/galoiscorrthms. pdf.*

[6] A. Fröhlich. Central extensions, Galois groups, and ideal class groups of number fields. *Contemporary Mathematics, American Mathematical Society Providence, RI*, 24, 1983.

[7] C. F. Gauss. *Disquisitiones arithmeticae*. 1801.

[8] H. Hasse. Zur Geschlechtertheorie in quadratischen Zahlkörpern. *J. Math. Soc. Japan*, 3(1): 45–51, 1951.

[9] S. Hu and Y. Li. The genus fields of Artin-Schreier extensions. *Finite Fields and Their Applications*, 16(4):255–264, 2010.

[10] T. W. Hungerford. Algebra. *Springer Verlag*, 1974.

[11] M. Ishida. The genus fields of algebraic number fields. *Lecture Notes in Mathematics*, 555, 2006.

[12] S. Lang. *Algebra*. Springer, 2002.

[13] H. W. Leopoldt. Zur Geschlechtertheorie in abelschen Zahlkörpern. *Mathematische Nachrichten*, 9(6):351–362, 1953.

[14] M. Maldonado-Ramírez, M. Rzedowski-Calderón, and G. Villa-Salvador. Genus fields of congruence function fields. *Finite Fields and Their Applications*, 44:56–75, 2017.

[15] M. Maldonado-Ramírez, M. Rzedowski-Calderón, and G. Villa-Salvador. Genus fields of abelian extensions of rational congruence function fields. *Finite Fields and Their Applications*, 20:40 – 54, 2013.

[16] M. Maldonado-Ramírez, M. Rzedowski-Calderón, and G. Villa-Salvador. Corrigendum to "Genus fields of abelian extensions of rational congruence function fields" [finite fields appl. 20 (2013) 40–54]. *Finite Fields and Their Applications*, 33:283 – 285, 2015.

[17] G. Peng. The genus fields of Kummer function fields. *Journal of Number Theory*, 98(2): 221–227, 2003.

[18] M. Rosen. The Hilbert class field in function fields. 5(4):365–378, 1987.

[19] M. Rzedowski Calderón and G. Villa-Salvador. Campos ciclotómicos, segunda versión. *arXiv:1407.3238*, 2017.

[20] J. A. Vargas Mendoza. Álgebra abstracta. *Editorial Limusa*, 1986.

[21] G. Villa-Salvador. *Topics in the theory of algebraic function fields*. Birkhäuser Boston, Inc., Boston, MA,, 2006.

[22] X. K. Zhang. A simple construction of genus fields of abelian number fields. *Proceedings of the American Mathematical Society*, 94(3):393–395, 1985.