CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS
DEL INSTITUTO POLITÉCNICO NACIONAL

Unidad Zacatenco

Departamento de Control Automático

Campos de géneros de extensiones abelianas de campos de funciones congruentes y extensiones cíclicas de Kummer de grado ℓ^n

TESIS

Que presenta

M. en C. Carlos Daniel Reyes Morales

para obtener el grado de
Doctor en Ciencias

en la especialidad de
Control Automático

Director de Tesis:

Dr. Gabriel Daniel Villa Salvador

Ciudad de México Abril, 2021

Agradecimientos

Con especial agradecimiento a mis Maestros Gabriel Villa y Martha Rzedowski, por todo su incondicional apoyo, confianza, paciencia y por compartir conmigo su conocimiento y experiencia, así como el gran amor por las matemáticas que me mostraron día a día durante todo mi doctorado, los llevare en mi corazón toda la vida.

A mis sinodales, por el tiempo dedicado en la revisión de mi trabajo, así como sus valiosos comentaros.

Al departamento de Control Automático, por acogerme en sus aulas y darme los grandes amigos que encontré allí.

Agradezco al Consejo Nacional de Ciencia y Tecnología, CONACyT, por la beca que me otorgó para la realización de mis estudios de doctorado por el periodo Enero 2017 - Diciembre 2020.

A mis seres amados por todo su cariño y apoyo incondicional en los momentos mas críticos de mi vida, sus consejos y muestras de bondad, sin ustedes no seria quien ahora soy, Arturo, Loo, Juan Carlos, Jessy, Najmeh, Ana gracias por existir.

Ciudad de México
Abril 2021

Carlos Daniel Reyes Morales

Resumen

Presentamos una nueva forma de calcular el campo de géneros de una extensión abeliana de un campo de funciones congruentes. Además definimos el concepto de **conductor de constantes** y observamos su relación en términos de otros invariantes de extensiones abelianas. En segundo lugar encontramos de manera explícita el campo de géneros de una extensión cíclica de Kummer de grado una potencia de primo en general, de un campo de funciones racionales.

Abstract

We present a new way to compute the genus field of an abelian extension of a congruent functions field. Furthermore we define the concept of **constant conductor** and we observe its connection with other invariants of abelian extensions. Second, we found explicitly the genus field of a cyclic Kummer extension of degree a prime power in general, of a rational function field.

Índice general

Introducción

El concepto de campo de géneros se remonta a C. F. Gauss [13] en el contexto de formas cuadráticas binarias. Para cualquier extensión finita $K/\mathbb{Q}$, el campo de géneros está definido como la máxima extensión no ramificada $K_{\mathfrak{ge}}$ de K tal que $K_{\mathfrak{ge}}$ es la composición de K y una extensión abeliana k^* de $\mathbb{Q}$, $K_{\mathfrak{ge}} = Kk^*$. Esta definición se debe a A. Fröhlich [12]. Si K_H denota el campo de clases de Hilbert de K, se tiene $K \subseteq K_{\mathfrak{ge}} \subseteq K_H$. Originalmente la definición de campo de géneros fue dada para extensiones cuadráticas de $\mathbb{Q}$.

H. W. Leopoldt [19] determinó el campo de géneros $K_{\mathfrak{ge}}$ de una extensión abeliana K de $\mathbb{Q}$ usando caracteres de Dirichlet, generalizando el trabajo de H. Hasse [15] quien introdujo la teoría de géneros para extensiones cuadráticas en campos numéricos.

M. Ishida describió el campo de géneros $K_{\mathfrak{ge}}$ para cualquier extensión finita de $\mathbb{Q}$ [18].

X. Zhang [31] dio una expresión simple de $K_{\mathfrak{ge}}$ para cualquier extensión finita K de $\mathbb{Q}$ usando la teoría de ramificación de Hilbert.

Para campos de funciones, la noción de campo de clases de Hilbert como la máxima extensión abeliana de un campo de funciones congruente $K/\mathbb{F}_q$ no es apropiada, pues esta última contiene a $K_m := K\mathbb{F}_{q^m}$ para todo número natural m y por tanto la máxima extensión abeliana no ramificada de K es de grado infinito sobre K.

M. Rosen [24] dio una definición de un análogo del campo de clases de Hilbert de K fijando un conjunto finito no vacío S de divisores primos de K. Usando esta definición, se puede dar un concepto adecuado del campo de géneros similar al caso clásico.

R. Clement [8] consideró una extensión cíclica de $k := \mathbb{F}_q(T)$ de grado un número primo l divisor de $q - 1$ y halló el campo de géneros usando teoría de campos de clases.

Más adelante, S. Bae y J. K. Koo [4] generalizaron los resultados de Clement siguiendo los métodos de Fröhlich [12].

G. Peng [23] describió explícitamente el campo de géneros para extensiones de Kummer de grado primo de campos de funciones racionales. Recientemente S. Hu y Y. Li [17] describieron explícitamente las clases de ideales ambiguas y el campo de géneros de una extensión de Artin–Schreier de un campo de funciones racionales congruente.

En [20, 21] se desarrolló una teoría de campos de géneros de campos de funciones congruentes usando la definición de Rosen del campo de clases de Hilbert: dado un conjunto finito no vacío S de lugares de un campo de funciones global K, el campo de clases de Hilbert (relativo a S) $K_{H,S}$ de K se define como la máxima extensión abeliana no ramificada de K tal que los lugares de S se descomponen totalmente en $K_{H,S}$. El campo de géneros $K_{\mathfrak{ge}}$ con respecto a k, es la máxima extensión de K tal que $K \subseteq K_{\mathfrak{ge}} \subseteq K_{H,S}$ con $K_{\mathfrak{ge}} = Kk^*$ y tal que k^*/k es una extensión abeliana. Cuando la extensión K/k es abeliana, $K_{\mathfrak{ge}}$ simplemente es la máxima extensión abeliana no ramificada de K tal que los primos en S se descomponen totalmente en $K_{\mathfrak{ge}}$. Los métodos usados allí se basan en las ideas de Leopoldt usando caracteres de Dirichlet y dando una descripción general de $K_{\mathfrak{ge}}$ en términos de los caracteres de Dirichlet. El campo de géneros $K_{\mathfrak{ge}}$ fue obtenido para una extensión abeliana K de k y S el conjunto de primos infinitos. El método se usó para dar $K_{\mathfrak{ge}}$ explícitamente cuando K/k es una extensión cíclica de grado primo $l \mid q-1$ (Kummer) o $l = p$ en donde p es la característica (Artin–Schreier) y también cuando K/k es una extensión p–cíclica (Witt). Posteriormente, el método fue usado en [5] para describir $K_{\mathfrak{ge}}$ explícitamente cuando K/k es una extensión cíclica de grado l^n, en donde l es un número primo, $l^n \mid q-1$ y K es un subcampo de un campo ciclotómico.
Este trabajo tiene dos objetivos. En primer lugar, encontramos el campo de géneros de una extensión abeliana finita de un campo de funciones racionales global. Introduciremos el concepto de conductor de constantes para estas extensiones y lo determinaremos en términos de otros invariantes.

En segundo lugar determinamos explícitamente el campo de géneros de una extensión cíclica de Kummer K/k de grado una potencia de un número primo. Este resultado generaliza lo encontrado en [5] haciendo explícito el campo $K_{\mathfrak{ge}}$ sin las restricciones impuestas ahí. Esta parte generaliza el resultado de G. Peng [23] el cual describe el campo de géneros de una extensión cíclica de Kummer del campo de funciones racionales de grado primo.

En el Capítulo 1 introducimos las definiciones y notación que usaremos durante el desarrollo de este trabajo. En el Capítulo 2 presentamos el primer cálculo del campo de géneros de una extensión abeliana finita de un campo de funciones racionales global. Iniciamos atendiendo el caso cuando el campo K está contenido en un campo ciclotómico para posteriormente dar el resultado en campos de funciones con tipo de ramificación general de $\mathcal{P}_\infty$. En el Capítulo 3 se presentan nuevas demostraciones a las que hallamos en el Capítulo 2, dichas demostraciones hacen uso de un enfoque distinto del problema y simplifican las anteriores. En este mismo capítulo introducimos el concepto de conductor de constantes y exhibimos algunas de sus propiedades. En el Capítulo 4 estudiamos las extensiones de tipo $(K_1K_2)_{\mathfrak{ge}}/(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$, partiendo del resultado obtenido en el capítulo anterior, analizamos la relación entre estos campos, para conocer los factores que impiden la igualdad entre ellos. Finalmente,e en el Capítulo 5 generalizamos el resultado de Peng [23], damos de forma

explícita el campo de géneros para las extensiones cíclicas de Kummer de grado ℓ^n, donde ℓ es un número primo.

Capítulo 1

Preliminares

En este trabajo usaremos la siguiente notación. Sea $k = \mathbb{F}_q(T)$ un campo de funciones racionales global de característica p, en donde $\mathbb{F}_q$ es el campo finito de q elementos, $q = p^\ell$ con p un número primo y $\ell \in \mathbb{N}$. Sea $R_T = \mathbb{F}_q[T]$ el anillo de los polinomios. Sea R_T^+ que denota el conjunto de todos los polinomios mónicos e irreducibles en R_T. Para $N \in R_T$, por $k(\Lambda_N)$ denotamos el N–ésimo campo de funciones ciclotómico de Carlitz. Sea $\mathcal{P}_\infty$ el polo del divisor principal (T) en k, al cual llamamos el *primo infinito*. El máximo subcampo real $k(\Lambda_N)^+$ de $k(\Lambda_N)$ es el campo de descomposición del primo infinito. Para todo campo L tal que $k \subseteq L \subseteq k(\Lambda_N)$, el subcampo real L^+ de L es $L^+ := k(\Lambda_N)^+ \cap L$.

1.1. Caracteres de Dirichlet en campos de funciones

Definición 1.1. Un **caracter de Dirichlet en campos de funciones** es un homomorfismo

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

con $N \in R_T \setminus \{0\}$ mónico. Decimos que χ está definido módulo N. Ahora, si $N \mid M$ con $N, M \in R_T \setminus \{0\}$ mónicos, se define

$$\Phi_{M,N} : (R_T/(M))^* \to (R_T/(N))^*,$$

dada por $A + (M) \mapsto A + (N)$. Notemos que $\Phi_{M,N}$ es un epimorfismo. Si $\chi : (R_T/(N))^* \to \mathbb{C}^*$, y $N \mid M$, tenemos $\chi \circ \Phi_{M,N}$ es un caracter módulo M y "casi" es el mismo que χ. Por lo tanto χ puede considerarse módulo N o módulo M. El mínimo N (en tanto a grado) módulo el cual χ puede definirse se llama el **conductor** de χ y se denota por F_χ.

En general, sea χ un caracter módulo N. Entonces χ es un caracter de $\mathrm{Gal}(k(\Lambda_N)/k)$. Sea $K = k(\Lambda_N)^{\ker \chi} \subseteq k(\Lambda_N)$. Tenemos K sólo depende de χ y se llama el **campo**

asociado a χ. Si N es minimal, $N = F_\chi$. Más generalmente, si X es un grupo de caracteres de Dirichlet, sea

$$N := \mathrm{mcd}(F_\chi \,|\, \chi \in X),$$

donde mcd denota el **máximo común divisor**. Así X es un subconjunto de los caracteres de $\mathrm{Gal}(k(\Lambda_N)/k)$. Sean

$$H := \bigcap_{\chi \in X} \ker \chi \subset (R_T/(N))^*$$

y $K = k(\Lambda_N)^H$, K es el **campo asociado a** X. Entonces X es el conjunto de homomorfismos $\mathrm{Gal}(K/k) \to \mathbb{C}^*$ y $[K : k] = |X|$. De hecho

$$X \cong \mathrm{Gal}(K/k).$$

Sea $N = P_1^{\alpha_1} \cdots P_h^{\alpha_h}$ con $P_i \in R_T$, $\alpha_i \in \mathbb{N}$. Tenemos $(R_T/(N))^* \cong \prod_{i=1}^{h} (R_T/(P_i^{\alpha_i}))^*$, por lo tanto, si $\chi : (R_T/(N))^* \to \mathbb{C}^*$, entonces $\chi = \prod_{i=1}^{h} \chi_{P_i}$, donde $\chi_{P_i} : (R_T/(P_i^{\alpha_i}))^* \to \mathbb{C}^*$, $\chi_{P_i} = \chi \circ \Phi^{-1} \circ G_i$, $\Phi : (R_T/(N))^* \to \prod_{i=1}^{h} (R_T/(P_i^{\alpha_i}))^*$ es el homomorfismo natural y

$$G_i : (R_T/(P_i^{\alpha_i}))^* \to \prod_{i=1}^{h} (R_T/(P_i^{\alpha_i}))^*,$$

dado por $A \mapsto (1, \ldots, 1, A, 1, \ldots, 1)$. En efecto, si $A \in R_T$, $(A, N) = 1$, entonces

$$\chi_{P_i}(A) = \chi\Phi^{-1}((1, \ldots, 1, A, 1, \ldots, 1)) = \chi(B_i)$$

donde $B_i \equiv 1 \bmod P_j^{\alpha_j}$, $j \neq i$, $B_i \equiv A \bmod P_i^{\alpha_i}$, luego

$$(\prod_{i=1}^{h} \chi_{P_i})(A) = \prod_{i=1}^{h} \chi_{P_i}(A) = \prod_{i=1}^{h} \chi(B_i) = \chi(\prod_{i=1}^{h} B_i) = \chi(A).$$

Para X un conjunto de caracteres de Dirichlet en campos de funciones y P un polinomio irreducible, se denota: $X_P = \{\chi_P \,|\, \chi \in X\}$.

1.2. El campo de géneros

Sea K/k una extensión abeliana finita. Del Teorema de Kronecker–Weber [25], tenemos que existen $m \in \mathbb{N}$, $n \in \mathbb{N} \cup \{0\}$ y $N \in R_T$ tales que

$$K \subseteq {}_nk(\Lambda_N)_m := L_nk(\Lambda_N)k_m,$$

en donde L_n denota al subcampo de $k(\Lambda_{1/T^{n+1}})$ de grado q^n y $k_m := \mathbb{F}_{q^m}(T)$ es la extensión de constantes de k de grado m. Tenemos que $\mathcal{P}_\infty$ es total y salvajemente ramificado en L_n/k. También tenemos que $\mathcal{P}_\infty$ es totalmente inerte en k_m/k.
Para cualquier extensión abeliana finita F de k, $S_\infty(F)$ denota el conjunto de divisores primos en F encima de $\mathcal{P}_\infty$. Para cualquier extensión abeliana finita E/F, $e_\infty(E/F)$, $f_\infty(E/F)$ y $h_\infty(E/F)$ denotan al índice de ramificación, al grado de inercia y al número de descomposición de $S_\infty(F)$ en E respectivamente. Para $P \in R_T^+$, $e_P(E/F)$ denota el índice de ramificación de cualquier primo encima de P en E/F. Para cualquier extensión F/k, $F_{\mathfrak{ge}}$ denota al campo de géneros de F sobre k, , para $S = S_\infty(F)$. Cuando F/k es una extensión abeliana finita, $F_{\mathfrak{ge}}$ es la máxima extensión abeliana contenida en el campo de clases de Hilbert de F. El símbolo C_d denotará al grupo cíclico de d elementos.
Sea $M := L_n k_m$. Entonces

$$e_\infty(M/k) = q^n, \quad f_\infty(M/k) = m \quad \text{y} \quad h_\infty(M/k) = 1. \tag{1.1}$$

Tenemos que $M \cap k(\Lambda_N) = k$. Los resultados generales acerca de los campos de géneros necesarios a lo largo de este trabajo, se pueden encontrar en [20, 21].

1.3. p–extensiones abelianas

Para un campo F, $W_v(F)$ denotará el anillo de vectores de Witt de longitud v. Las operaciones de Witt se denotaran por $\overset{\bullet}{+}$ y $\overset{\bullet}{-}$. Ahora, consideremos el campo $K = k(\vec{y})$ en donde

$$\vec{y}^{p^u} \overset{\bullet}{-} \vec{y} = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r$$

con $\vec{\delta}_i = (\delta_{i,1}, \ldots, \delta_{i,v})$ para algún $v \in \mathbb{N}$, en donde $\delta_{i,j} = \frac{Q_{i,j}}{P_i^{e_{i,j}}}$, $e_{i,j} \geq 0$, $Q_{i,j} \in R_T$ y si $e_{i,j} > 0$, entonces $e_{i,j} = \lambda_{i,j} p^{m_{i,j}}$, $\operatorname{mcd}(\lambda_{i,j}, p) = 1$, $0 \leq m_{i,j} < n$, con n como en (1.1), $\operatorname{mcd}(Q_{i,j}, P_i) = 1$ y $\operatorname{gr}(Q_{i,j}) < \operatorname{gr}(P_i^{e_{i,j}})$, y $\gamma_j = f_j(T) \in R_T$ con $\operatorname{gr} f_j = \nu_j p^{m_j}$ y $\operatorname{mcd}(q, \nu_j) = 1$, $0 \leq m_j < n$ cuando $f_j \notin \mathbb{F}_q$. Aquí vamos a suponer que $\mathbb{F}_{p^u} \subseteq \mathbb{F}_q$ y que $K \subseteq k(\Lambda_N)$ para algún $N \in R_T$.

Para más resultados sobre la teoría de los vectores de Witt se puede consultar [29] (o [20]).

Capítulo 2

Campos de géneros de campos de funciones congruentes

En este capítulo obtendremos de una primera forma, el campo de géneros $K_{\mathfrak{ge}}$ de un campo de funciones racionales K/k usando los caracteres de Dirichlet, resultado que posteriormente contrastaremos con los presentados en el Capítulo 3, donde se cambiara a otros dos enfoques que nos arrojan más información aritmética de este tipo de extensiones. Pero antes, presentaremos un resultado fundamental, que es el análogo en campos de funciones al Teorema de Leopoldt, en campos numéricos [19].

Proposición 2.1. *Si $K \subseteq k(\Lambda_N)$ y el grupo de caracteres asociado a K es X, entonces la máxima extensión abeliana J de K no ramificada en ningún primo finito $P \in R_T^+$, contenida en una extensión ciclotómica, es el campo asociado a*

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

Demostración. Sea L el campo asociado a Y. Notemos que para todo $P \in R_T^+$, $Y_P = X_P$ por lo que $e_P(L/k) = |Y_P| = |X_P| = e_P(K/k)$, de donde $e_P(L/K) = 1$. Como $L \subseteq k(\Lambda_N)$, se sigue que $L \subseteq J$.
Ahora, sea E/K una extensión no ramificada en ningún primo finito y E contenido en un campo de funciones ciclotómico. Sea Z el grupo de caracteres de Dirichlet asociado a E. Entonces $|X_P| = |Z_P|$ y $Z \supseteq X$. Por lo tanto $Z_P = X_P$ y se sigue que $Z \subseteq \prod_P Z_P = \prod_P X_P = Y$ y por lo tanto $E \subseteq L$. En particular $J \subseteq L$ y por tanto $J = L$. □

Nota 2.2. Dado un campo $K \subseteq k(\Lambda_N)$, denotaremos por $K_{\mathfrak{g}ex}$, a la máxima extensión abeliana no ramificada en ningún primo finito $P \in R_T^+$.

Antes de continuar nuestro estudio en campos de funciones, hagamos un paréntesis para ver el Teorema de Géneros de Gauss. Pero antes tenemos la siguiente observación en campos numéricos respecto al Teorema de Leopoldt.
Con una definición análoga a la Definición 1.1 de los caracteres de Dirichlet pero en campos numéricos (ver [28, Chapter 3]) tenemos que:

Observación 2.3. Sea K un campo numérico y J como en la Proposición 2.1. Cuando los primos infinitos son no ramificados en J/K tenemos que $K_{\mathfrak{ge}} = J$. En otro caso, si K es real y J imaginario, entonces $K_{\mathfrak{ge}} = J^+$ donde $J^+ := J \cap \mathbb{R}$ y el grupo de caracteres de Dirichlet asociado a J^+ es $Y^+ := \{\chi \in Y \mid \chi(-1) = 1\}$. Finalmente $[J : J^+] = [Y : Y^+] = 2$.

Ejemplo 2.4 (Teorema de Géneros de Gauss)**.** Sea $K = \mathbb{Q}(\sqrt{d})$ una extensión cuadrática de $\mathbb{Q}$, con $d \in \mathbb{Z}$ libre de cuadrados. Sea m el número de factores primos distintos de $\mathfrak{d}_K$, el discriminante de K. Si $p_1, \ldots, p_m$ son dichos factores, escogemos $p_1 = 2$ si $2 \mid \mathfrak{d}_K$.
Sea χ el caracter cuadrático asociado a K. Entonces $\chi_{p_i} \neq 1$, $1 \leq i \leq m$ y $\chi_q = 1$ para todo primo q, $q \notin \{p_1, \ldots, p_m\}$. Para $p_i \neq 2$, χ_{p_i} es único y $\chi_{p_i}(-1) = (-1)^{(p_i-1)/2}$. En este caso, el campo asociado a χ_{p_i} es $\mathbb{Q}\big(\sqrt{(-1)^{(p_i-1)/2}p_i}\big)$. Si $p_1 = 2$, entonces hay tres caracteres cuadráticos $\chi_{p_1} = \chi_2$; dos de ellos con conductor 8, uno real y otro imaginario, y el otro de conductor 4. Si χ_2 es real, $\chi(-1) = 1$ y el campo asociado es $\mathbb{Q}(\sqrt{2})$. Si χ_2 es imaginario de conductor 8, $\chi(-1) = -1$ y el campo asociado es $\mathbb{Q}(\sqrt{-2})$. Finalmente, si χ_2 es de conductor 4, $\chi(-1) = -1$ y el campo asociado a χ_2 es $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. De esto se sigue que la máxima extensión abeliana de $\mathbb{Q}$ no ramificada en todos los primos finitos es $J = \mathbb{Q}\big(\sqrt{\varepsilon}, \sqrt{(-1)^{(p_2-1)/2}p_2}, \ldots, \sqrt{(-1)^{(p_m-1)/2}p_m}\big)$ donde $\varepsilon = (-1)^{(p_1-1)/2}p_1$ si $p_1 \neq 2$ y $\varepsilon = 2, -2$ o -1 si $p_1 = 2$.
Así obtenemos que $[J : \mathbb{Q}] = 2^m$ y $[J : K] = 2^{m-1}$. Luego $K_{\mathfrak{ge}} = J$ excepto cuando K es real y J es imaginario, este caso ocurre cuando $\mathfrak{d}_K > 0$ ($d > 0$) y existe $p_i \equiv 3 \pmod 4$. En ese caso, $[J^+ : K] = 2^{m-2}$.
Para la extensión cuadrática $K = \mathbb{Q}(\sqrt{-14})$ de $\mathbb{Q}$, tenemos que $K_{\mathfrak{ge}} = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ y para $K = \mathbb{Q}(\sqrt{79})$ obtenemos que $J = \mathbb{Q}(\sqrt{-79}, i)$ y $K_{\mathfrak{ge}} = J^+ = J \cap \mathbb{R} = \mathbb{Q}(\sqrt{79}) = K$.

Regresando a nuestro estudio de los campos de funciones, tenemos los siguientes resultados.

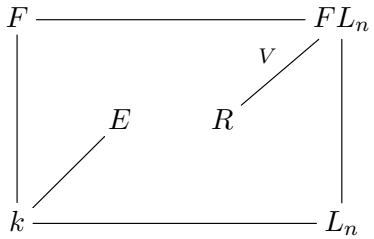
Lema 2.5. *Si K/k es una extensión abeliana y el grado de cualquier divisor primo en $S_\infty(K)$ es t, entonces el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$.*

Demostración. Considere la extensión de constantes $K_r := K\mathbb{F}_{q^r}$ de K. Entonces el número de primos en K_r encima de cualquier primo en $S_\infty(K)$ es $h = (d_K(S_\infty(K)), r)$ = (t, r) ver [25, Teorema 9.1.4]. Por lo tanto $S_\infty(K)$ se descompone totalmente en K_r/K si y sólo si $h = r$ y esto es equivalente a $r \mid d_K(S_\infty(K)) = t$. Se sigue que la

máxima extensión de constantes de K donde $S_\infty(K)$ se descompone totalmente es $K_t = K\mathbb{F}_{q^t}$. Así el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$. □

Proposición 2.6. *Si E/k es una extensión abeliana tal que $\mathfrak{p}_\infty$ es moderadamente ramificado, entonces existen $N \in R_T$ y $m \in \mathbb{N}$ tales que $E \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$.*

Demostración. Por el Teorema de Kronecker–Weber, tenemos $E \subseteq k(\Lambda_N)\mathbb{F}_{q^m}L_n = {}_nk(\Lambda_N)_m$ para algunos $N \in R_T$ y $m \in \mathbb{N}$, $n \in \mathbb{N} \cup \{0\}$.



Sea $F := k(\Lambda_N)\mathbb{F}_{q^m} = k(\Lambda_N)_m$ y sea $V = \{\sigma \in D(\mathfrak{P} \,|\, \mathcal{P}_\infty) \,|\, \sigma a - a \in \mathfrak{P}^2, \forall a \in \mathcal{O}_{FL_n}\}$ el primer grupo de ramificación de $\mathcal{P}_\infty$ en FL_n/k. Entonces $R := (FL_n)^V$ es la máxima extensión de k contenida en FL_n donde $\mathfrak{p}_\infty$ es moderadamente ramificado y como consecuencia tenemos que $S_\infty(R)$ es salvajemente ramificado en FL_n/R.
Puesto que $\mathcal{P}_\infty$ es moderadamente ramificado en E/k, se sigue que $E \subseteq R$. Ahora, $\mathcal{P}_\infty$ es moderadamente ramificado en F/k y $S_\infty(F)$ es total y salvajemente ramificado en FL_n/F. Luego FL_n/F es de grado $|V|$. Por tanto $R = F$ y $E \subseteq F$. □

Proposición 2.7. *Con las hipótesis de la Proposición* 2.1*, en el caso de que $e_{\mathcal{P}_\infty}(K|k) = q - 1$, se tiene $K_{\mathfrak{ge}} = J$.*

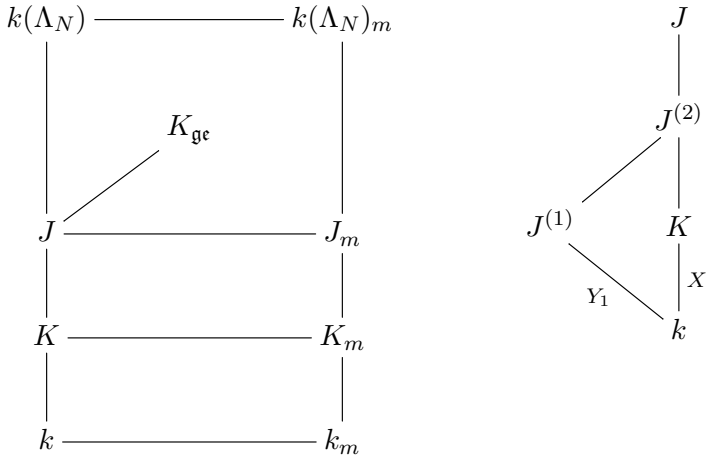
Demostración. Puesto que $e_{\mathcal{P}_\infty}(J|K) = \frac{e_{\mathcal{P}_\infty}(J|k)}{e_{\mathcal{P}_\infty}(K|k)} = \frac{q-1}{q-1} = 1$, $\mathcal{P}_\infty$ se descompone totalmente en J/K y por tanto $J \subseteq K_{\mathfrak{ge}}$.
Ahora bien, el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_q$ (ver [24] o simplemente si $\mathbb{F}_{q^m}$ es el campo de constantes de $K_{\mathfrak{ge}}$, $K \subseteq K_m \subseteq K_{\mathfrak{ge}}$ y $\mathcal{P}_\infty$ es totalmente inerte en K_m, es decir $f_\infty = [K_m : K] = m$; puesto que $\mathcal{P}_\infty$ y los primos en $S_\infty(K)$ no tienen inercia en ninguno de K/k o J/K, $m = 1$).
Puesto que $\mathcal{P}_\infty$ se descompone totalmente en $K_{\mathfrak{ge}}/K$ y $\mathcal{P}_\infty$ es moderadamente ramificado en K/k, por la Proposición 2.6 tenemos que $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$ para algunos $N \in R_T$ y $m \in \mathbb{N}$.
En todas las extensiones k_m/k, K_m/K, J_m/J y $k(\Lambda_N)_m/k(\Lambda_N)$ los primos infinitos son totalmente inertes ya que todos tienen grado 1 (ver [27, Theorem 6.2.1]). En las extensiones K_m/k_m y K/k el índice de ramificación de los primos infinitos es $q - 1$, esto es, el máximo posible. Se sigue que en J_m/K_m, J/K, $k(\Lambda_N)/J$ y $k(\Lambda_N)_m/J_m$, $S_\infty(K_m)$, $S_\infty(K)$, $S_\infty(J)$ y $S_\infty(J_m)$ son totalmente descompuestos. Finalmente, en $k(\Lambda_N)_m/J$ (y por tanto en $k(\Lambda_N)_m/K_{\mathfrak{ge}}$), $S_\infty(J)$ es no ramificado.

Sea $G := \mathrm{Gal}(k(\Lambda_N)_m/J)$. Para $S_\infty(J)$ tenemos que en esta extensión el índice de ramificación e, el grado de inercia f y el número de descomposición h son $e = 1$, $f = m$ y $h = \frac{|G|}{m}$. Por lo tanto el grupo de descomposición $\mathfrak{D}$ de $\mathcal{P}_\infty$ es de orden m y es cíclico. Debemos tener $\mathfrak{D} = \mathrm{Gal}(k(\Lambda_N)_m/k(\Lambda_N))$ ya que $S_\infty(k(\Lambda_N))$ es totalmente inerte de grado m en $k(\Lambda_N)_m/k(\Lambda_N)$. Puesto que los primos en $S_\infty(J)$ tienen grado de inercia 1 en $K_{\mathfrak{ge}}/J$, se sigue que $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Por tanto $K_{\mathfrak{ge}} = J$. □

Finalmente tenemos el siguiente resultado.

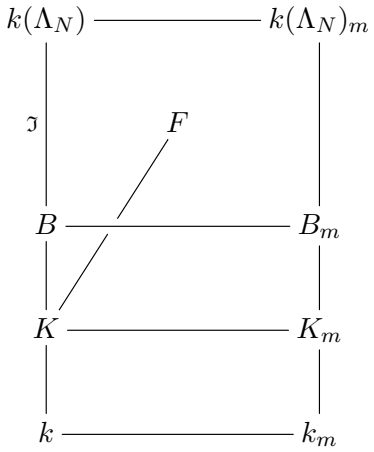
Teorema 2.8. *Supongamos que $k \subseteq K \subseteq k(\Lambda_N)$ para algún polinomio N. Sean X el grupo de caracteres de Dirichlet asociado a K, $Y = \prod_{P|N} X_P$, $Y_1 = \{\chi \in Y \mid \chi(a) = 1$ para todo $a \in \mathbb{F}_q^*\}$ y $J^{(1)}$ el campo asociado a Y_1 ($J^{(1)} = J \cap k(\Lambda_N)^+$). Entonces el campo de géneros $K_{\mathfrak{ge}}$ de K satisface $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$ y $K_{\mathfrak{ge}} = KJ^{(1)}$.*

Demostración. Ahora, $e_{\mathcal{P}_\infty}(K|k)$ no necesariamente es igual a $q-1$. Usaremos la notación de la Proposición 2.1. En este caso $S_\infty(K)$ puede ser ramificado en J/K. Tenemos que $J^{(1)} \subseteq J$ puesto que $Y_1 \subseteq Y$, aunque no necesariamente $J^{(1)} \subseteq K$ o $K \subseteq J^{(1)}$. Sea $J^{(2)} := KJ^{(1)}$.
Entonces $J^{(2)}$ es el campo asociado al grupo de caracteres XY_1. Puesto que $\mathcal{P}_\infty$ se descompone totalmente en $J^{(1)}/k$, $S_\infty(K)$ se descompone totalmente en $J^{(2)}$. Más aún $S_\infty(J^{(1)})$ es totalmente ramificado en $J/J^{(1)}$. Por tanto $S_\infty(J^{(2)})$ es totalmente ramificado en $J/J^{(2)}$.



Obtenemos que $J^{(2)}/K$ es una extensión abeliana no ramificada con $J^{(2)} \subseteq k(\Lambda_N)$ y $S_\infty(K)$ se descompone totalmente en $J^{(2)}/K$. Se sigue que $J^{(2)} = J^{\mathfrak{D}}$ donde $\mathfrak{D}$ es el grupo de descomposición de $S_\infty(J)$ con respecto al grupo $\mathrm{Gal}(J/K)$. Por tanto $J^{(2)} \subseteq K_{\mathfrak{ge}}$
Ahora consideremos cualquier extensión abeliana no ramificada F/K tal que $S_\infty(K)$ se descompone totalmente en F. Por la Proposición 2.6, $F \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$ para algunos

$N \in R_T$ y $m \in \mathbb{N}$. En el caso de que $F \subseteq k(\Lambda_N)$, sea Z el grupo de caracteres de Dirichlet asociado a F. Puesto que F/K es no ramificada, se sigue que $X \subseteq Z \subseteq Y$ debido a la Proposición 2.1 y por tanto $F \subseteq J$. Puesto que $J^{(2)} = J^{\mathfrak{D}}$, obtenemos que $F \subseteq J^{(2)}$.



Para el caso $k \subseteq F \subseteq k(\Lambda_N)\mathbb{F}_{q^m}$, esto es, F no necesariamente está contenido en un campo de funciones ciclotómico, sea $\mathfrak{I}$ el grupo de inercia de $S_\infty(K)$ en $k(\Lambda_N)/K$ y sea $B := k(\Lambda_N)^{\mathfrak{I}}$. Entonces los primos en $S_\infty(B)$ son totalmente inertes en B_m debido a que tienen grado 1 y son totalmente ramificados en $k(\Lambda_N)/B$. Como $S_\infty(K)$ se descompone totalmente en B, B es el campo de descomposición de $S_\infty(K)$ en $k(\Lambda_N)_m/K$ entonces $F \subseteq B \subseteq k(\Lambda_N)$.
De la primera parte, obtenemos que $F \subseteq J^{(2)}$. Por tanto $K_{\mathfrak{ge}} \subseteq J^{(2)}$ y $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. □

2.1. Campos de funciones congruentes con tipo de ramificación general de $\mathcal{P}_\infty$

Ahora, presentamos el primer cálculo del campo de géneros de una extensión abeliana congruente con tipo de ramificación general de $\mathcal{P}_\infty$. La idea principal tras este resultado fue, dada una extensión abeliana K/k con $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}L_n$, usando caracteres de Dirichlet obtener el campo de géneros de un cierto campo con ciertas propiedades $F \in k(\Lambda_N)$, $N \in \mathbb{N}$ con el cual "aproximar" el campo de géneros de K.

Teorema 2.9. *Sea K/k una extensión abeliana finita con $K \subseteq k(\Lambda_N)\mathbb{F}_{q^m}L_n$. Sean $F = KL_n \cap k(\Lambda_N)\mathbb{F}_{q^m}$ y $E = k(\Lambda_N) \cap F\mathbb{F}_{q^m} \subseteq k(\Lambda_N)$. Entonces el campo de géneros de K es*

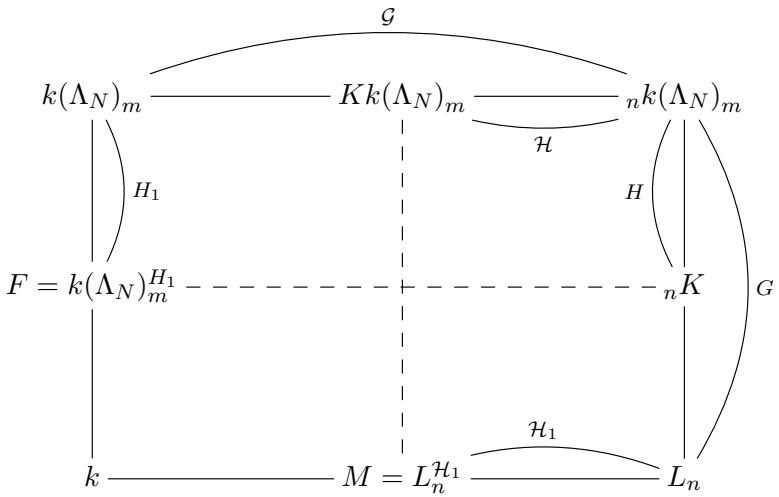
$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1}FK$$

donde $E_{\mathfrak{ge}}$ es el campo de géneros de E, H es el grupo de descomposición de $S_\infty(F)$ en $E_{\mathfrak{ge}}F/F$ y $H_1 = H|_{E_{\mathfrak{ge}}}$. Además $E_{\mathfrak{ge}}FK/K_{\mathfrak{ge}}$ es una extensión de constantes de grado $d = |H|$ y d divide a $q-1$. Finalmente

$$E_{\mathfrak{ge}}FK = K_{\mathfrak{ge}}\mathbb{F}_{q^{td}}$$

donde t es el grado de $S_\infty(K)$.

Demostración. Consideremos $M := Kk(\Lambda_N)_m \cap L_n$ y $F = KL_n \cap k(\Lambda_N)_m$. Sean $\mathcal{G} := \mathrm{Gal}({}_nk(\Lambda_N)_m/k(\Lambda_N)_m)$, $\mathcal{H} := \mathrm{Gal}({}_nk(\Lambda_N)_m/Kk(\Lambda_N)_m)$ y $\mathcal{H}_1 := \mathcal{H}|_{L_n}$. Sean $G := \mathrm{Gal}({}_nk(\Lambda_N)_m/L_n)$, $H := \mathrm{Gal}({}_nk(\Lambda_N)_m/{}_nK)$, $H_1 := H|_{k(\Lambda_N)_m}$. Veamos que $M = L_n^{\mathcal{H}_1}$. Ya que $\mathcal{G} \cong \mathrm{Gal}(L_n/k)$ se sigue que $|\mathcal{H}_1| = |\mathcal{H}|$, luego $L_n^{\mathcal{H}_1} = Kk(\Lambda_N)_m \cap L_n = M$. De forma análoga tenemos que $F = k(\Lambda_N)_m^{H_1}$ pues del isomorfismo $G \cong \mathrm{Gal}(k(\Lambda_N)_m/k)$ se obtiene que $|H_1| = |H|$. Luego $k(\Lambda_N)_m^{H_1} = {}_nK \cap k(\Lambda_N)_m = F$.



(2.1)

Ahora, como $F \subseteq {}_nK$ tenemos que ${}_nF \subseteq {}_nK$, por otro lado $[{}_nk(\Lambda_N)_m : {}_nF] = [k(\Lambda_N)_m : F] = [k(\Lambda_N)_m : k(\Lambda_N)_m^{H_1}] = |H_1| = |H| = [{}_nk(\Lambda_N)_m : {}_nK]$. Se sigue que ${}_nF = {}_nK$. Similarmente como $M \subseteq Kk(\Lambda_N)_m$ tenemos $Mk(\Lambda_N)_m \subseteq Kk(\Lambda_N)_m$. Por otro lado $[{}_nk(\Lambda_N)_m : Mk(\Lambda_N)_m] = [L_n : M] = [L_n : L_n^{\mathcal{H}_1}] = |\mathcal{H}_1| = |\mathcal{H}| = [{}_nk(\Lambda_N)_m : Kk(\Lambda_N)_m]$. Se sigue que $Mk(\Lambda_N)_m = Kk(\Lambda_N)_m$.

Sea $A \subseteq \mathcal{G} \times G$ tal que $K = {}_nk(\Lambda_N)_m^A$. Observemos en el diagrama (2.1), por las respectivas correspondencias de los grupos de Galois se tiene que $F = {}_nk(\Lambda_N)_m^{\mathcal{G}\times H}$ y $M = {}_nk(\Lambda_N)_m^{\mathcal{H}\times G}$. Entonces, si denotamos $R = {}_nk(\Lambda_N)_m$, tenemos

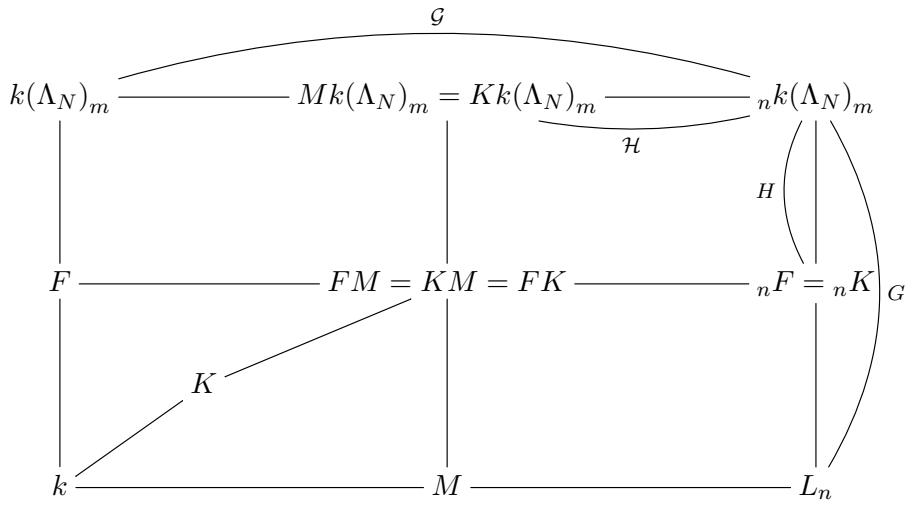
$$\begin{aligned} R^{A\cap(\mathcal{G}\times 1)} &= R^A R^{\mathcal{G}\times 1} = Kk(\Lambda_N)_m = Mk(\Lambda_N)_m \\ &= R^{\mathcal{H}\times G}R^{\mathcal{G}\times 1} = R^{(\mathcal{H}\times G)\cap(\mathcal{G}\times 1)} = R^{\mathcal{H}\times 1}. \end{aligned}$$

Se sigue que $A \cap (\mathcal{G} \times 1) = \mathcal{H} \times 1$. De forma análoga se obtiene $A \cap (1 \times G) = 1 \times H$.

Por lo tanto

$$\begin{aligned} FM &= R^{\mathcal{G}\times H}R^{\mathcal{H}\times G} = R^{(\mathcal{G}\times H)\cap(\mathcal{H}\times G)} = R^{\mathcal{H}\times H}, \\ KM &= R^{A}R^{\mathcal{H}\times G} = R^{A\cap(\mathcal{H}\times G)}, \\ FK &= R^{\mathcal{G}\times H}R^{A} = R^{(\mathcal{G}\times H)\cap A}. \end{aligned}$$

Veamos que $(\mathcal{G}\times H)\cap A = A\cap(\mathcal{H}\times G) = \mathcal{H}\times H$. Sea $(h,g)\in\mathcal{H}\times H\subseteq\mathcal{H}\times G$. Entonces $(1,g)\in 1\times H = A\cap(1\times G)$. En particular obtenemos que $(1,g)\in A$. Por otro lado, $(h,1)\in\mathcal{H}\times 1 = A\cap(\mathcal{G}\times 1)$, en particular $(h,1)\in A$, así $(h,g)\in A$, luego $(h,g)\in A\cap(\mathcal{H}\times G)$. Al tomarse (h,g) arbitrario, se sigue que $\mathcal{H}\times H\subseteq A\cap(\mathcal{H}\times G)$. Ahora, sea $(h,g)\in A\cap(\mathcal{H}\times G)$. Como $(h,1)\in\mathcal{H}\times 1 = A\cap(\mathcal{G}\times 1)$, en particular $(h,1)\in A$ y $(h,1)\in\mathcal{H}\times G$, se sigue que $(h,1)\in A\cap(\mathcal{H}\times G)$. Se tiene $(h,1)(1,g) = (h,g)\in A\cap(\mathcal{H}\times G)$. Luego $(1,g)\in A\cap(\mathcal{H}\times G)$. En particular $(1,g)\in A$ y puesto que $(1,g)\in 1\times G$ se tiene que $(1,g)\in A\cap(1\times G) = 1\times H$, es decir, $g\in H$. Por tanto $(h,g)\in\mathcal{H}\times H$, luego $\mathcal{H}\times H = A\cap(\mathcal{H}\times G)$.
Análogamente obtenemos que $\mathcal{H}\times H = A\cap(\mathcal{G}\times H)$. Por tanto se sigue $FM = KM = FK$. En resumen tenemos el siguiente diagrama



Dado que $F_{\mathfrak{ge}}/F$ es no ramificada y $S_\infty(F)$ se descompone totalmente en $F_{\mathfrak{ge}}/F$, obtenemos que ${}_nF_{\mathfrak{ge}}/{}_nF = {}_nFF_{\mathfrak{ge}}/{}_nF = {}_nKF_{\mathfrak{ge}}/{}_nK$ es no ramificada y que $S_\infty({}_nF)$ se descompone totalmente en ${}_nk(\Lambda_N)_m$. Ahora, en ${}_nK/K$, los únicos primos posiblemente ramificados son aquellos en $S_\infty(K)$ y si es así, se ramifican salvajemente. Se sigue que en ${}_nKF_{\mathfrak{ge}}/K$ los únicos primos posiblemente ramificados son los elementos de $S_\infty(K)$ y de serlo, se ramifican salvajemente. En particular, como $K\subseteq KF_{\mathfrak{ge}}\subseteq {}_nKF_{\mathfrak{ge}}$, en $F_{\mathfrak{ge}}K/K$ los únicos primos posiblemente ramificados son aquellos en $S_\infty(K)$ y, si son ramificados, se ramifican salvajemente.

Nuevamente, dado que la extensión $F_{\mathfrak{ge}}/F$ es no ramificada y $S_\infty(F)$ se descompone totalmente, $F_{\mathfrak{ge}}K/FK$ es no ramificada y $S_\infty(FK)$ se descompone totalmente en

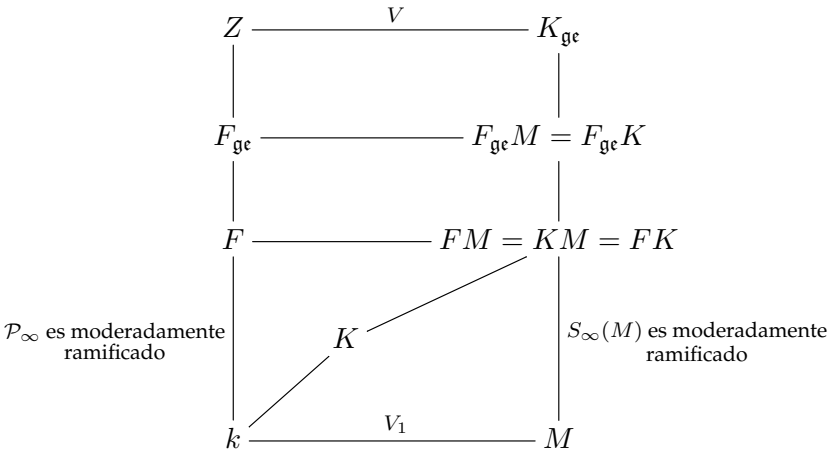
$F_{\mathfrak{ge}}K/FK$. Ya que $k \subseteq F \cap K \subseteq F \subseteq k(\Lambda_N)_m$ y en la extensión $F/(F \cap K)$, $S_\infty(F \cap K)$ es moderadamente ramificado, como para los grupos de inercia

$$I(S_\infty(FK) \mid S_\infty(K))|_F \subseteq I(S_\infty(F) \mid S_\infty(F \cap K)),$$

se tiene en particular para los índices de ramificación

$$e(S_\infty(FK) \mid S_\infty(K)) \mid e(S_\infty(F) \mid S_\infty(F \cap K)).$$

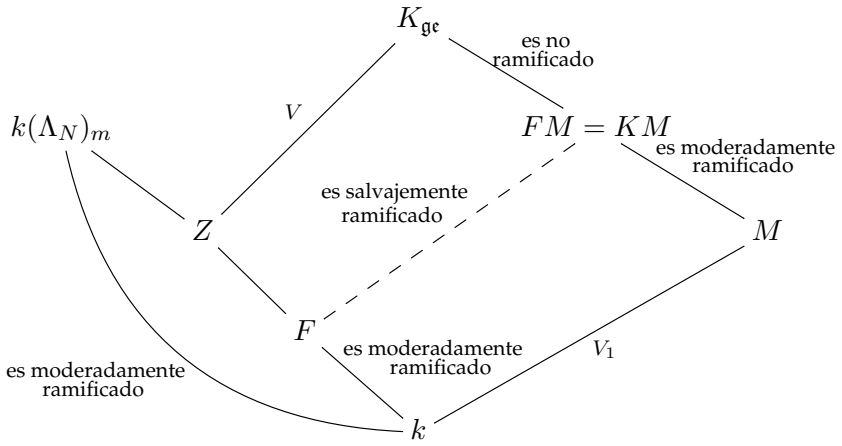
Por tanto $S_\infty(K)$ es moderadamente ramificado en FK/K. Es decir, de los razonamientos previos resulta que en FK/K, $S_\infty(K)$ es moderada y salvajemente ramificado a la vez. Por lo tanto $S_\infty(K)$ se descompone totalmente en FK/K. En resumen, tenemos $F_{\mathfrak{ge}}K \subseteq K_{\mathfrak{ge}}$. Puesto que $FM = FK$, se tiene $F_{\mathfrak{ge}}M = F_{\mathfrak{ge}}K \subseteq K_{\mathfrak{ge}}$.
Sea V el primer grupo de ramificación de $\mathcal{P}_\infty$ en $K_{\mathfrak{ge}}/k$. Sea $Z := K_{\mathfrak{ge}}^V$. Entonces $\mathcal{P}_\infty$ es moderadamente ramificado en Z/k y por lo tanto $Z \subseteq k(\Lambda_N)_m$.
Como $\mathcal{P}_\infty$ es total y salvajemente ramificado en M/k, $M \cap Z = k$. Ahora, siendo V el primer grupo de ramificación de $\mathcal{P}_\infty$ en la extensión $K_{\mathfrak{ge}}/k$, $V_1 = V|_{L_n}$ lo es en M/k. Ya que $k \subseteq M \subseteq F_{\mathfrak{ge}}M \subseteq K_{\mathfrak{ge}}$ y $\mathcal{P}_\infty$ es total y salvajemente ramificado precisamente en la extensión M/k de dicha torre de campos, se tiene $|V_1| = |V|$, por lo que se sigue que $\mathcal{P}_\infty$ y $S_\infty(M)$ son moderadamente ramificados en Z/k y en $K_{\mathfrak{ge}}/M$ respectivamente. Además $S_\infty(F)$ es total y salvajemente ramificado en la extensión $FK = FM/F$. Finalmente, como $K_{\mathfrak{ge}}/K$ es no ramificada, se sigue que $K_{\mathfrak{ge}}/KM$ es no ramificada, es decir $K_{\mathfrak{ge}}/FM$ es no ramificada.



Ahora $[K_{\mathfrak{ge}} : k] = [K_{\mathfrak{ge}} : Z][Z : k] = |V|[Z : k] = |V_1|[Z : k] = [M : k][Z : k] = [ZM : k]$. Se sigue que $K_{\mathfrak{ge}} = ZM$. Como $F \subseteq k(\Lambda_N)_m$ y $F_{\mathfrak{ge}}/F$ es moderadamente ramificada se sigue que

$$F_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}^V = Z.$$

Puesto que $\mathcal{P}_\infty$ es el único primo ramificado en M/k, los únicos primos ramificados en $FK = FM/F$ son aquéllos en $S_\infty(F)$ y justo como lo hemos mencionado, éstos son salvajemente ramificados. Entonces tenemos lo siguiente con respecto a $\mathcal{P}_\infty$:



Ahora bien, se tiene que $S_\infty(F)$ no se ramifica en Z/F ya que de ramificarse tendría que ser moderadamente ramificado pero como se vio antes, en $FM = KM/F$ es salvajemente ramificado y en $K_{\mathfrak{ge}}/KM = FM$ es no ramificado. Además Z/F es no ramificada en todos los demás primos, pues $K_{\mathfrak{ge}}/F$ es ramificada a lo más en los divisores primos de $S_\infty(F)$. Se sigue que

$$Z \subseteq F_{\mathfrak{ge}} \quad \text{y por lo tanto} \quad Z = F_{\mathfrak{ge}}.$$

Así

$$K_{\mathfrak{ge}} = ZM = F_{\mathfrak{ge}}M = F_{\mathfrak{ge}}K. \tag{2.2}$$

Para terminar, necesitamos calcular $F_{\mathfrak{ge}}$.

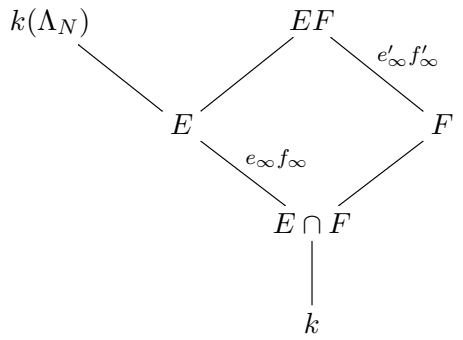
Dado que $k(\Lambda_N)/k$ es una extensión geométrica y k_m/k es una extensión de constantes, dichas extensiones de k son linealmente disjuntas. Por tanto $k(\Lambda_N) \cap k_m = k$. Puesto que $\mathcal{P}_\infty$ es moderadamente ramificado en $F_{\mathfrak{ge}}/k$, sin pérdida de generalidad podemos suponer que $F_{\mathfrak{ge}} \subseteq k(\Lambda_N)_m$.

Definamos $E := F_m \cap k(\Lambda_N) \subseteq F_m$. Como $k_m \subseteq F_m$ se tiene que $E_m = Ek_m \subseteq F_m$. Además, como $F \subseteq k(\Lambda_N)_m$ se tiene que $F_m \subseteq k(\Lambda_N)_m$. Así $F_m \subseteq F_m \cap k(\Lambda_N)_m = E_m$. Por lo tanto $E_m = F_m$.
Por otro lado $m[F : k] = [F_m : k_m][k_m : k] = [E_m : k_m][k_m : k] = [E_m : k_m]m = m[E : k]$. Así $[E : k] = [F : k]$. Por lo tanto,

$$E_m = F_m \quad \text{y} \quad [E : k] = [F : k]. \tag{2.3}$$

En otras palabras, E juega un papel similar al de F pero E está contenido en una extensión ciclotómica.
Puesto que $E = F_m \cap k(\Lambda_N)$, tenemos $E \cap F = (F_m \cap k(\Lambda_N)) \cap F = k(\Lambda_N) \cap F$. Como en particular $E \subseteq k(\Lambda_N)$, se tiene que $E_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Se sigue que $E \cap F \subseteq E_{\mathfrak{ge}} \cap F \subseteq k(\Lambda_N) \cap F = E \cap F$. Por lo tanto $E \cap F = E_{\mathfrak{ge}} \cap F = k(\Lambda_N) \cap F$.
Ya que F_m/F es no ramificada y $EF \subseteq E_m = F_m$, tenemos que EF/F es no ramificada y como $E_{\mathfrak{ge}}/E$ es no ramificada, obtenemos que $E_{\mathfrak{ge}}F/EF$ es no ramificada, en consecuencia, la extensión $E_{\mathfrak{ge}}F/F$ es no ramificada. También, como $S_\infty(E)$ se descompone totalmente en $E_{\mathfrak{ge}}$, $S_\infty(EF)$ se descompone totalmente en $E_{\mathfrak{ge}}F$.

Sean $D(S_\infty(F))$ el grupo de descomposición de cualquier primo de $S_\infty(F)$ en EF/F y $D(S_\infty(E \cap F))$ el grupo de descomposición de cualquier primo de $S_\infty(E \cap F)$ en $E/(E \cap F)$. Sabemos que $D(S_\infty(F))|_E \subseteq D(S_\infty(E \cap F))$. Se tiene que $|D(S_\infty(F))| = e'_\infty f'_\infty$ y $|D(S_\infty(E \cap F))| = e_\infty f_\infty$, donde e'_∞ y f'_∞ indican los respectivos índices de ramificación e inercia de $S_\infty(F)$ en EF/F, e_∞ y f_∞ indican los respectivos índices ramificación e inercia de $S_\infty(E \cap F)$ en $E/(E \cap F)$, además $e'_\infty f'_\infty \mid e_\infty f_\infty$.

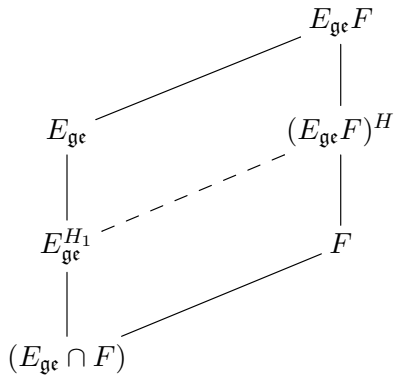


Ya que EF/F es no ramificada, $e'_\infty = 1$. Puesto que $k \subseteq E \cap F \subseteq E \subseteq k(\Lambda_N)$ y $\mathcal{P}_\infty$ tiene índice de ramificación $q-1$ y grado de inercia igual a 1 en $k(\Lambda_N)/k$, se sigue que $e_\infty \mid q-1$ y $f_\infty = 1$. Definiendo $d := f'_\infty$ se tiene que $d \mid q-1$ y como $I(S_\infty(E \cap F))$, el grupo de inercia de $S_\infty(E \cap F)$ en $E/(E \cap F)$, es subgrupo de $D(S_\infty(E \cap F))$ y $|I(S_\infty(E \cap F))| = e_\infty$, se sigue que $D(S_\infty(E \cap F)) = I(S_\infty(E \cap F))$. Si denotamos por $I(\mathcal{P}_\infty)$ el grupo de inercia de $\mathcal{P}_\infty$ en $k(\Lambda_N)/k$, se tiene que $D(S_\infty(F))$ es un subgrupo de orden d de $I(S_\infty(E \cap F)))$ que a su vez es subgrupo de $I(\mathcal{P}_\infty) \cong C_{q-1}$.

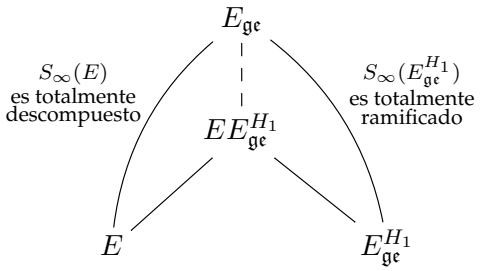
Sea H el grupo de descomposición de $S_\infty(F)$ en $E_{\mathfrak{ge}}F/F$, puesto que $E_{\mathfrak{ge}}F/EF$ es no ramificada, tenemos que H coincide con $D(S_\infty(F))$, por tanto

$$|H| = |D(S_\infty(F))| = d = f'_\infty.$$

Así tenemos que H es un grupo cíclico de orden d que corresponde a la inercia de $S_\infty(F)$ en $E_{\mathfrak{ge}}F/F$. Si $H_1 := H|_{E_{\mathfrak{ge}}}$, puesto que $\mathrm{Gal}(E_{\mathfrak{ge}}/(E_{\mathfrak{ge}} \cap F)) \cong \mathrm{Gal}(E_{\mathfrak{ge}}F/F)$, por la correspondencia de Galois, obtenemos que $(E_{\mathfrak{ge}}F)^H = E_{\mathfrak{ge}}^{H_1}F$.



Ahora, como $S_\infty(E)$ es totalmente descompuesto en $E_{\mathfrak{ge}}/E$ y $S_\infty(E_{\mathfrak{ge}}^{H_1})$ es totalmente ramificado en $E_{\mathfrak{ge}}/E_{\mathfrak{ge}}^{H_1}$, resulta que



$S_\infty(EE_{\mathfrak{ge}}^{H_1})$ es totalmente descompuesto y totalmente ramificado en $E_{\mathfrak{ge}}/EE_{\mathfrak{ge}}^{H_1}$, por lo tanto $E_{\mathfrak{ge}} = EE_{\mathfrak{ge}}^{H_1}$.
En resumen

$$(E_{\mathfrak{ge}}F)^H = E_{\mathfrak{ge}}^{H_1}F \subseteq F_{\mathfrak{ge}} \qquad \text{y} \qquad EE_{\mathfrak{ge}}^{H_1} = E_{\mathfrak{ge}} \tag{2.4}$$

Finalmente, sea $C := F_{\mathfrak{ge},m} \cap k(\Lambda_N)$. De (2.3) tenemos $E \subseteq E_m = F_m \subseteq F_{\mathfrak{ge},m}$ y $E \subseteq k(\Lambda_N)$. Por lo tanto $E \subseteq C$. De (2.4) obtenemos ${E_{\mathfrak{ge}}}^{H_1} \subseteq {E_{\mathfrak{ge}}}^{H_1}F \subseteq F_{\mathfrak{ge}} \subseteq F_{\mathfrak{ge},m}$, además ${E_{\mathfrak{ge}}}^{H_1} \subseteq E_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Por lo tanto ${E_{\mathfrak{ge}}}^{H_1} \subseteq F_{\mathfrak{ge},m} \cap k(\Lambda_N) = C$. También tenemos que $E_{\mathfrak{ge}} = E{E_{\mathfrak{ge}}}^{H_1} \subseteq C$.

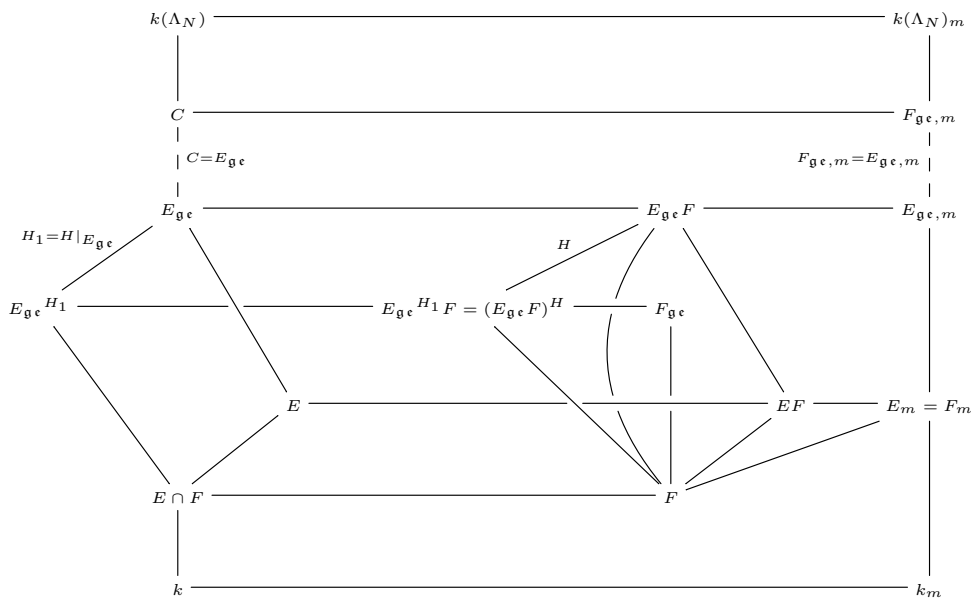
Por definición $F_{\mathfrak{ge}}/F$ es no ramificada. Luego $F_{\mathfrak{ge},m}/F_m$ es no ramificada. Puesto que $F_m = E_m = (EF)_m$, se sigue que la extensión F_m/E es una extensión de constantes, por tanto es no ramificada. Luego $F_{\mathfrak{ge},m}/E$ es no ramificada. Ahora, como $E \subseteq C \subseteq F_{\mathfrak{ge},m}$, tenemos que C/E es no ramificada, tal que $C \subseteq k(\Lambda_N)$. Se sigue que $S_\infty(E)$ se descompone totalmente en C/E. Así $C \subseteq E_{\mathfrak{ge}}$. Por lo tanto $E_{\mathfrak{ge}} = C$.

Como $k(\Lambda_N)_m = k(\Lambda_N)k_m$ y $k(\Lambda_N) \cap k_m = k$, por la correspondencia de Galois, obtenemos que $E_{\mathfrak{ge},m} = E_{\mathfrak{ge}}k_m = CE_m = (F_{\mathfrak{ge},m} \cap k(\Lambda_N))k_m = F_{\mathfrak{ge},m} \cap k(\Lambda_N)_m =$

$F_{\mathfrak{ge},m}$ pues $F_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. En resumen

$$C = E_{\mathfrak{ge}} \quad \text{y} \quad E_{\mathfrak{ge},m} = Ck_m = F_{\mathfrak{ge},m}. \tag{2.5}$$

(2.6)

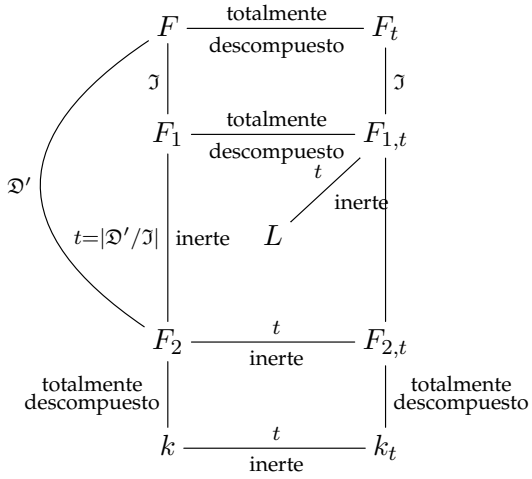


De (2.4) tenemos $E_{\mathfrak{ge}}^{H_1}F \subseteq F_{\mathfrak{ge}} \subseteq F_{\mathfrak{ge},m}$ y

$$({E_{\mathfrak{ge}}}^{H_1}F)_m = {E_{\mathfrak{ge}}}^{H_1}F_m = {E_{\mathfrak{ge}}}^{H_1}E_m = ({E_{\mathfrak{ge}}}^{H_1}E)_m = E_{\mathfrak{ge},m} = F_{\mathfrak{ge},m}.$$

Así $F_{\mathfrak{ge},m} = (E_{\mathfrak{ge}}^{H_1}F)_m/E_{\mathfrak{ge}}^{H_1}F$ es una extensión de constantes. Del Lema 2.5, el campo de constantes de $F_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$, por lo que $F_{\mathfrak{ge}} = (E_{\mathfrak{ge}}^{H_1}F)_t$. Si probamos que $\mathbb{F}_{q^t} \subseteq E_{\mathfrak{ge}}^{H_1}F$, se seguirá que $F_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1}F$.

Sea $\mathfrak{I}$ el grupo de inercia de cualquier elemento de $S_\infty(F)$ en la extensión F/k, $|\mathfrak{I}| = e(S_\infty(F) \mid \mathcal{P}_\infty) = e$, y sea $\mathfrak{D}'$ el grupo de descomposición de $S_\infty(F)$ en F/k. Como $t = d_F(S_\infty(F))$, tenemos que $|\mathfrak{D}'| = et$, puesto que $\mathfrak{D}'/\mathfrak{I} \cong \mathrm{Gal}(F(S_\infty(F))/k(\mathcal{P}_\infty)) \cong C_t$. En el siguiente diagrama el tipo de descomposición es con referencia a los divisores primos infinitos.



Aquí $F_1 := F^{\mathfrak{I}}$, $F_2 := F^{\mathfrak{D}'}$ y L es el campo fijo del grupo de descomposición de $\mathcal{P}_\infty$ en $F_{1,t}/k$. Se sigue que $\mathcal{P}_\infty$ es totalmente descompuesto en L/k. Por lo tanto $L \subseteq k(\Lambda_N)$. Nuevamente, como t es el grado de inercia de cualquier elemento de $S_\infty(F)$ en F/k, se tiene que el grado de inercia de $S_\infty(F_2)$ en F_1/F_2 es t. Además tenemos que $\mathrm{Gal}(F_{1,t}/F_2) \cong C_t \times C_t$. Se sigue que $S_\infty(L)$ es totalmente descompuesto e inerte en $F_{1,t}/LF_1$, por lo tanto $F_{1,t} = LF_1$ (o también, se sigue de que $LF_1 \subseteq F_{1,t}$ con $[LF_1 : F_2] = t^2$). Así $L \cap F_1 = F_2$ y LF_1/F_2 es una extensión de Galois de grado t^2 con grupo de Galois $C_t \times C_t$.
Puesto que $L \subseteq F_t \subseteq F_m$ y $L \subseteq k(\Lambda_N)$ se sigue que $L \subseteq F_m \cap k(\Lambda_N) = E$. Ya que $\mathcal{P}_\infty$ se descompone totalmente en L/k, se sigue en particular que $L \subseteq {E_{\mathfrak{ge}}}^{H_1}$. Por tanto $\mathbb{F}_{q^t} \subseteq k_t F_1 = F_{1,t} = LF_1 \subseteq LF \subseteq {E_{\mathfrak{ge}}}^{H_1} F$. Luego

$$F_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1} F. \tag{2.7}$$

Por lo tanto de (2.2) y (2.7) concluimos que

$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1} FM = E_{\mathfrak{ge}}^{H_1} FK. \tag{2.8}$$

Ahora, de (2.4) obtenemos que $E_{\mathfrak{ge}}^{H_1} F = F_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}} F \subseteq (E_{\mathfrak{ge}} F)_m = E_{\mathfrak{ge}} F_m = {E_{\mathfrak{ge}}}^{H_1} EF_m = {E_{\mathfrak{ge}}}^{H_1} EE_m = {E_{\mathfrak{ge}}}^{H_1} E_m = {E_{\mathfrak{ge}}}^{H_1} F_m = ({E_{\mathfrak{ge}}}^{H_1} F)_m$. En particular, $E_{\mathfrak{ge}} F/F_{\mathfrak{ge}}$ es una extensión de constantes. Ya que $E_{\mathfrak{ge}} \cap F = E \cap F$, de la correspondencia de Galois tenemos

$$[E_{\mathfrak{ge}} F : F_{\mathfrak{ge}}] = [E_{\mathfrak{ge}} F : {E_{\mathfrak{ge}}}^{H_1} F] = [E_{\mathfrak{ge}} : {E_{\mathfrak{ge}}}^{H_1}] = |H_1| = |H| = d$$

(recordemos que d corresponde a la inercia de $S_\infty(F)$ en $E_{\mathfrak{ge}} F/F$) y como el campo de constantes de $F_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$, se sigue que el campo de constantes de $E_{\mathfrak{ge}} F$ es $\mathbb{F}_{q^{td}}$. Así

$$E_{\mathfrak{ge}}F = F_{\mathfrak{ge}}\mathbb{F}_{q^{td}}. \tag{2.9}$$

Finalmente, de (2.5) tenemos que, al ser $F_{\mathfrak{ge},m}/F_{\mathfrak{ge}}$ una extensión de constantes, en particular es cíclica, y como $\mathbb{F}_{q^t}$ es el campo de constantes de $F_{\mathfrak{ge}}$, dicha extensión es de orden $\frac{m}{t}$. Si $\mathfrak{D}$ denota el grupo de descomposición de los divisores primos en $S_\infty(F)$ en $E_{\mathfrak{ge},m} = F_{\mathfrak{ge},m}/F$, se sigue que $F_{\mathfrak{ge}} = E^{\mathfrak{D}}_{\mathfrak{ge},m} = F^{\mathfrak{D}}_{\mathfrak{ge},m}$. Observe además que $|\mathfrak{D}| = [F_{\mathfrak{ge},m} : F^{\mathfrak{D}}_{\mathfrak{ge},m}] = [E_{\mathfrak{ge},m} : F_{\mathfrak{ge}}] = [F_{\mathfrak{ge},m} : F_{\mathfrak{ge}}] = \frac{m}{t}$ donde t es el grado de cualquier primo en $S_\infty(F)$. □

Observemos en particular, de (2.9) si $(t, d) = 1$ entonces $E_{\mathfrak{ge}}F = F_{\mathfrak{ge}}\mathbb{F}_{q^d}$.

Capítulo 3

Nuevo cálculo del campo de géneros de campos de funciones congruentes y el conductor de constantes

En este capítulo se calcula el campo de géneros de una extensión abeliana congruente K desde otro enfoque, dando por resultado una expresión mucho más transparente para $K_{\mathfrak{ge}}$. Considerando el enfoque de caracteres de Dirichlet usado en el Teorema 2.9, nos preguntamos que información extra nos podría proveer "partiendo" el campo ${}_nk(\Lambda_N)_m = k(\Lambda_N)k_mL_n$ de diferentes formas, esto es, ${}_nk(\Lambda_N)_m = k(\Lambda_N)({}_nk_m)$ y ${}_nk(\Lambda_N)_m = ({}_nk(\Lambda_N))k_m$.

3.1. Nuevos cálculos

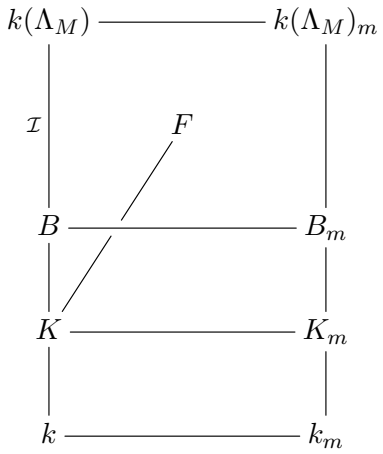
Primero, presentamos una nueva prueba del hecho de que si $K \subseteq k(\Lambda_N)$, entonces $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$, es decir, del Teorema 2.8.

Teorema 3.1. *Sea $k \subseteq K \subseteq k(\Lambda_N)$ para algún $N \in R_T^+$. Entonces $K_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Más aún, si el grupo de caracteres de Dirichlet de K es X y si L es el campo asociado a $Y = \prod_{P \in R_T^+} X_P$, entonces*

$$K_{\mathfrak{ge}} = KL^+.$$

Demostración. Sea F/K una extensión abeliana no ramificada tal que los elementos de $S_\infty(K)$ son totalmente descompuestos en F/K. En particular $\mathcal{P}_\infty$ es moderadamente ramificado.
Por el Teorema de Kronecker–Weber, tenemos que $F \subseteq K(\Lambda_M)_m$ para algunos $M \in R_T^+$ y $m \in \mathbb{N}$.

Sea $\mathcal{I}$ el grupo de inercia de $S_\infty(K)$ en $k(\Lambda_M)/K$ y sea $B = k(\Lambda_M)^{\mathcal{I}}$.



Como los elementos de $S_\infty(B)$ son de grado 1, son totalmente inertes en B_m/B. Más aún, los elementos de $S_\infty(B)$ son totalmente ramificados en $k(\Lambda_M)/B$. Ahora, los elementos de $S_\infty(K)$ son totalmente descompuestos en B/K entonces obtenemos que B es el campo de descomposición de $S_\infty(K)$ en $k(\Lambda_M)_m/K$. Se sigue que $F \subseteq B \subseteq k(\Lambda_M)$.

Sea Z el grupo de caracteres de Dirichlet asociado a F. Como F/K es no ramificada, se sigue que $X \subseteq Z \subseteq Y$, esto es, $F \subseteq L$ puesto que L es la máxima extensión abeliana contenida en algún campo ciclotómico tal que L/K es no ramificada en los primos finitos. En particular, podemos tomar $M = N$. Por lo tanto $K_{\mathfrak{ge}} = L^{\mathcal{D}}$ en donde $\mathcal{D}$ es el grupo de descomposición de $S_\infty(K)$ en L/K.

Ahora, $S_\infty(K)$ se descompone totalmente en KL^+/K ya que $\mathcal{P}_\infty$ se descompone totalmente en L^+/k. Como L/K es no ramificada, tenemos que $KL^+ \subseteq L$ y KL^+/K es no ramificada. Por lo tanto $KL^+ \subseteq K_{\mathfrak{ge}}$ y obtenemos que $KL^+ \subseteq K_{\mathfrak{ge}} \subseteq L$.

Finalmente, podemos ver que $S_\infty(KL^+)$ es totalmente ramificado en la extensión L/KL^+. De hecho esto se sigue del hecho de que $L^+ \subseteq KL^+ \subseteq L$ y de que $S_\infty(L^+)$ es totalmente ramificada en L/L^+. Como $KL^+ \subseteq K_{\mathfrak{ge}} \subseteq L$ y $K_{\mathfrak{ge}}/KL^+$ es no ramificado, se sigue que $K_{\mathfrak{ge}} = KL^+ \subseteq k(\Lambda_N)$. □

Teorema 3.2. *Sean K/k una extensión abeliana finita con $K \subseteq k(\Lambda_N)k_mL_n$ y $M := L_nk_m$. Sea*

$$E := KM \cap k(\Lambda_N).$$

Entonces

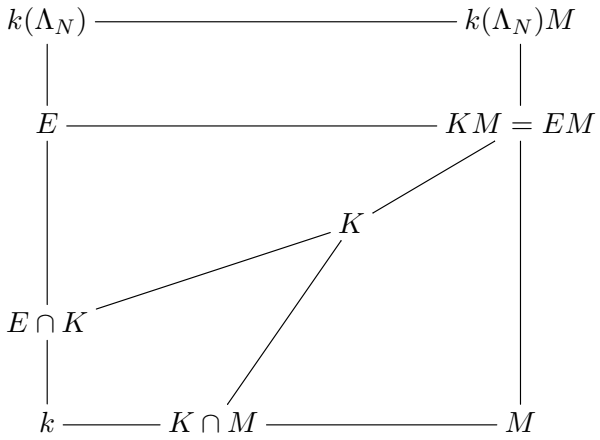
$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H_1}K = (E_{\mathfrak{ge}}K)^H,$$

en donde H es el grupo de descomposición de algún elemento primo de $S_\infty(K)$ en $E_{\mathfrak{ge}}K/K$, $H_1 := H|_{E_{\mathfrak{ge}}}$ y $H_2 := H_1|_E$.

Sea $d := f_\infty(EK/K)$, tenemos que $H \cong H_1 \cong H_2 \cong C_d$ y $d|q-1$. También tenemos que $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ y $EK/E^{H_2}K$ son extensiones de constantes de grado d. Finalmente, el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$, en donde t es el grado de $S_\infty(K)$ en K.

Demostración. Como $k(\Lambda_N) \cap M = k$ y $E = KM \cap k(\Lambda_N)$, por la correspondencia de Galois, entre $k(\Lambda_N)/k$ y $k(\Lambda_N)M/M$, E corresponde a KM. Por lo tanto $KM = EM$ corresponde a E. Así

$$KM = EM.$$



Ahora $E \cap K \subseteq E_{\mathfrak{ge}} \cap K \subseteq k(\Lambda_N) \cap K = (KM \cap k(\Lambda_N)) \cap k(\Lambda_N) \cap K = E \cap k(\Lambda_N) \cap K = E \cap K$. Por lo tanto

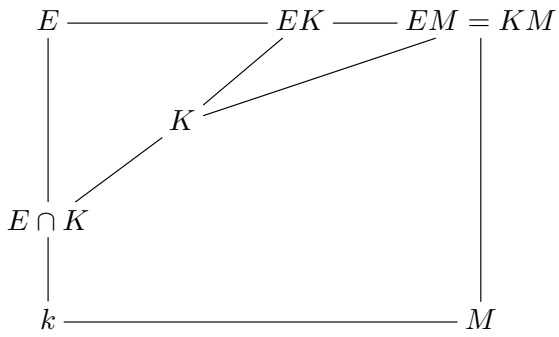
$$E \cap K = E_{\mathfrak{ge}} \cap K = k(\Lambda_N) \cap K.$$

Tenemos que $[E : k] = [EM : M] = [KM : M] = [K : K \cap M]$. Así

$$[K : k] = [E : k][K \cap M : k]. \tag{3.1}$$

Después, probaremos que EK/K es no ramificada. Primero note que $E \subseteq EK \subseteq EKM = E \cdot EM = EM$. En la extensión M/k, $\mathcal{P}_\infty$ es el único primo ramificado. Por lo tanto, en KM/E los únicos posibles primos ramificados son aquellos en $S_\infty(E)$. También tenemos que en la extensión KM/K los únicos posibles primos ramificados son los elementos de $S_\infty(K)$ y como $K \subseteq EK \subseteq EM = KM$, los únicos posibles

primos ramificados en EK/K son aquellos en $S_\infty(K)$.



De (1.1) tenemos que

$$e_\infty(EK/K) \mid e_\infty(M/K \cap M) \quad \text{y} \quad e_\infty(M/K \cap M) \mid e_\infty(M/k) = q^n.$$

Por otro lado, tenemos que

$$e_\infty(EK/K) \mid e_\infty(E/E \cap K) \quad \text{y} \quad e_\infty(E/E \cap K) \mid e_\infty(k(\Lambda_N)/k) = q - 1.$$

Así

$$e_\infty(EK/K) \mid \operatorname{mcd}(q^n, q-1) = 1$$

y por tanto EK/K es una extensión no ramificada. Ahora, tenemos que

$$e_\infty(EK/K) f_\infty(EK/K) \mid e_\infty(E/E \cap K) f_\infty(E/E \cap K),$$

y $e_\infty(EK/K) = 1$, $f_\infty(E/E \cap K) = 1$. Por lo tanto, $f_\infty(EK/K) \mid e_\infty(E/E \cap K)$ y $e_\infty(E/E \cap K) \mid q - 1$. Así $f_\infty(EK/K) \mid q - 1$.
Por lo tanto tenemos que EK/K es no ramificada, el grado de inercia de $S_\infty(K)$ en EK/K es $d = f_\infty(EK/K)$ y $d \mid q - 1$. Como $E_{\mathfrak{ge}}/E$ es no ramificada y $S_\infty(E)$ se descompone totalmente en $E_{\mathfrak{ge}}/E$, lo mismo se tiene en $E_{\mathfrak{ge}}K/EK$. En este caso obtenemos que $E_{\mathfrak{ge}}K/K$ es una extensión no ramificada y el grado de inercia de $S_\infty(K)$ es d.
Recordemos que H es el grupo de descomposición de algún primo en $S_\infty(K)$ en $E_{\mathfrak{ge}}K/K$ y $H_1 = H|_{E_{\mathfrak{ge}}}$. Observe que $|H| = d$. Como $E_{\mathfrak{ge}} \cap K = E \cap K$, de la correspondencia de Galois obtenemos que $H \cong H_1$, $|H| = |H_1|$ y $E_{\mathfrak{ge}}^{H_1} K = (E_{\mathfrak{ge}}K)^H$. Análogamente, $H_2 \cong H_1$. Más aún, $H_1 \subseteq I_\infty(k(\Lambda_N)/k) \cong C_{q-1}$, en donde $I_\infty(k(\Lambda_N)/k)$ denota el grupo de inercia de $\mathcal{P}_\infty$. Por lo tanto H es un grupo cíclico, $H \cong H_1 \cong H_2 \cong C_d$. Como $S_\infty(K)$ se descompone totalmente en $E_{\mathfrak{ge}}^{H_1}K/K$, se sigue que

$$E_{\mathfrak{ge}}^{H_1} K \subseteq K_{\mathfrak{ge}}.$$

Sea $E_1 := EE_{\mathfrak{ge}}^{H_1} \subseteq E_{\mathfrak{ge}}$. Ahora $H_1 \subseteq I_\infty(E/E\cap K)$, entonces $S_\infty(E_{\mathfrak{ge}}^{H_1})$ es totalmente ramificado en $E_{\mathfrak{ge}}/E_{\mathfrak{ge}}^{H_1}$. Por lo tanto $S_\infty(E_1)$ es totalmente ramificado en $E_{\mathfrak{ge}}/E_1$. Por otro lado, $S_\infty(E)$ se descompone totalmente en $E_{\mathfrak{ge}}/E$. Por lo tanto $S_\infty(E_1)$ se descompone totalmente en $E_{\mathfrak{ge}}/E_1$. Esto es, $S_\infty(E_1)$ se ramifica y se descompone totalmente en $E_{\mathfrak{ge}}/E_1$. Por lo tanto

$$E_{\mathfrak{ge}} = E_1 = EE_{\mathfrak{ge}}^{H_1}.$$

Se sigue que

$$(E_{\mathfrak{ge}}K)^H = E_{\mathfrak{ge}}^{H_1}K \subseteq K_{\mathfrak{ge}} \quad \text{y} \quad EE_{\mathfrak{ge}}^{H_1} = E_{\mathfrak{ge}}.$$

Para probar la otra contención, definimos $C := K_{\mathfrak{ge}}M \cap k(\Lambda_N)$. Tenemos que

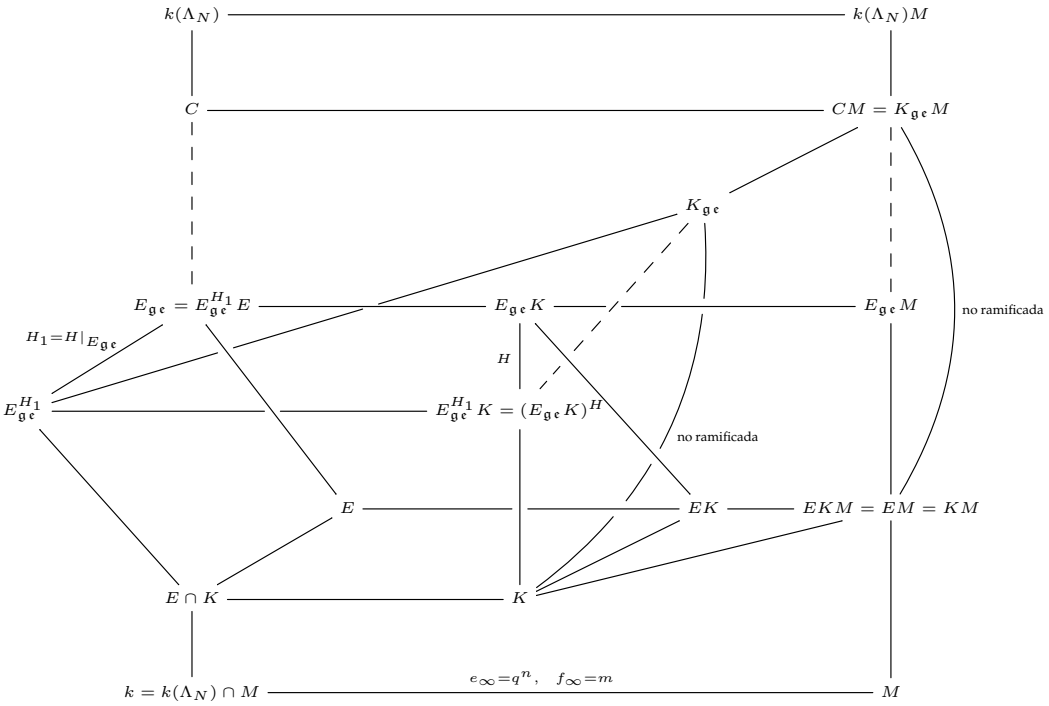
$$E \subseteq EM = KM \subseteq K_{\mathfrak{ge}}M, \quad E \subseteq k(\Lambda_N).$$

por lo tanto

$$E \subseteq K_{\mathfrak{ge}}M \cap k(\Lambda_N) = C, \quad \text{esto es} \quad E \subseteq C.$$

Más aún, $E_{\mathfrak{ge}}^{H_1} \subseteq E_{\mathfrak{ge}}^{H_1}K \subseteq K_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}M$ y $E_{\mathfrak{ge}}^{H_1} \subseteq E_{\mathfrak{ge}} \subseteq k(\Lambda_N)$. Así $E_{\mathfrak{ge}}^{H_1} \subseteq K_{\mathfrak{ge}}M \cap k(\Lambda_N) = C$. Luego $E_{\mathfrak{ge}}^{H_1} \subseteq C$. Por lo tanto

$$E_{\mathfrak{ge}} = EE_{\mathfrak{ge}}^{H_1} \subseteq C. \tag{3.2}$$



Como $C = K_{\mathfrak{ge}}M \cap k(\Lambda_N)$, por la correspondencia de Galois tenemos que $CM = K_{\mathfrak{ge}}M$. Ahora, como $K_{\mathfrak{ge}}/K$ es no ramificada y $S_\infty(K)$ se descompone totalmente, se sigue que

$$CM/KM \text{ es no ramificada y } S_\infty(KM) \text{ se descompone totalmente.} \tag{3.3}$$

Ahora probaremos que C/E es no ramificada. De (3.3) se sigue que CM/KM es no ramificada. Ahora, en $KM = EM$ sobre E, los únicos primos ramificados son aquellos en $S_\infty(E)$ y éstos tienen índice de ramificación igual a q^n. Se sigue que los únicos primos ramificados en CM/E son aquellos en $S_\infty(E)$. Por tanto, los únicos posibles primos ramificados en C/E son aquellos en $S_\infty(E)$. Ahora

$$e_\infty(C/E) \mid e_\infty(CM/E) = q^n \quad \text{y} \quad e_\infty(C/E) \mid e_\infty(k(\Lambda_N)/k) = q-1$$

de modo que

$$e_\infty(C/E) \mid \operatorname{mcd}(q^n, q-1) = 1.$$

Por lo tanto C/E es una extensión no ramificada.
Por otro lado, al ser $S_\infty(E)$ no ramificado en C/E, $S_\infty(E)$ se descompone totalmente en C/E puesto que $C \subseteq k(\Lambda_N)$. Se sigue que $C \subseteq E_{\mathfrak{ge}}$. De esto y de la ecuación (3.2), obtenemos que

$$C = E_{\mathfrak{ge}} \quad \text{y} \quad E_{\mathfrak{ge}}M = CM = K_{\mathfrak{ge}}M.$$

Como $K_{\mathfrak{ge}}/K$ es no ramificada y $S_\infty(K)$ se descompone totalmente en $K_{\mathfrak{ge}}$, lo mismo tenemos en la extensión $E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K$. En particular $h_\infty(E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K) = [E_{\mathfrak{ge}}K_{\mathfrak{ge}} : E_{\mathfrak{ge}}K]$.
Ahora, en la extensión $E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}$, los únicos primos ramificados son aquellos en $S_\infty(E_{\mathfrak{ge}})$ y tenemos que $e_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}) = q^n$ y $f_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}) = m$ pues $e_\infty(E_{\mathfrak{ge}}/k) \mid q-1$ el cual es primo relativo con q, $f_\infty(E_{\mathfrak{ge}}/k) = 1$, $e_\infty(M/k) = q^n$ y $f_\infty(M/k) = m$.

$$\begin{array}{ccc} E_{\mathfrak{ge}} & \text{———————} & E_{\mathfrak{ge}}M \\ | & & | \\ E_{\mathfrak{ge}} \cap M = k & \xrightarrow[e_\infty = q^n,\, f_\infty = m]{\text{———————}} & M \end{array}$$

Sean F_1 y F_2 dos campos tales que $k \subseteq F_1 \subseteq F_2 \subseteq M$. Sea $R_i = E_{\mathfrak{ge}}F_i$, $i = 1, 2$. Como $f_\infty(E_{\mathfrak{ge}}/k) = 1$ y $e_\infty(E_{\mathfrak{ge}}/k) \mid q-1$, se sigue de la correspondencia de Galois entre M/k y $E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}$ que $e_\infty(R_i/E_{\mathfrak{ge}}) = e_\infty(F_i/k)$ y que $f_\infty(R_i/E_{\mathfrak{ge}}) = f_\infty(F_i/k)$, $i = 1, 2$. Por lo tanto $e_\infty(F_2/F_1) = e_\infty(R_2/R_1)$ y $f_\infty(F_2/F_1) = f_\infty(R_2/R_1)$.
Como $h_\infty(M/k) = 1$, tenemos que $h_\infty(R_2/R_1) = 1$. En particular

$$\begin{aligned} R_1 \neq R_2 &\iff F_1 \neq F_2 \iff e_\infty(F_2/F_1) > 1 \text{ o } f_\infty(F_2/F_1) > 1 \\ &\iff e_\infty(R_2/R_1) > 1 \text{ o } f_\infty(R_2/R_1) > 1. \end{aligned} \tag{3.4}$$

Como

$$E_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M,$$

$S_\infty(E_{\mathfrak{ge}}K)$ es no ramificado en $E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K$ y $S_\infty(E_{\mathfrak{ge}}K)$ se descompone totalmente, por lo que obtenemos que $e_\infty(E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K) = 1$ y $f_\infty(E_{\mathfrak{ge}}K_{\mathfrak{ge}}/E_{\mathfrak{ge}}K) = 1$. De (3.4), se sigue que

$$E_{\mathfrak{ge}}K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K.$$

Por lo tanto $K_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$. Como $E_{\mathfrak{ge}}K/K$ es no ramificada, si $\mathcal{D}$ es el grupo de descomposición de $S_\infty(K)$ en $E_{\mathfrak{ge}}K/K$, entonces obtenemos que $K_{\mathfrak{ge}} = (E_{\mathfrak{ge}}K)^{\mathcal{D}}$. Así, tenemos que

$$f_\infty(E_{\mathfrak{ge}}K/K) = f_\infty(E_{\mathfrak{ge}}K/EK)f_\infty(EK/K) = 1 \cdot d = d.$$

Por lo tanto $\mathcal{D} = H$ y $K_{\mathfrak{ge}} = (E_{\mathfrak{ge}}K)^{\mathcal{D}} = (E_{\mathfrak{ge}}K)^H = E_{\mathfrak{ge}}^{H_1}K$.

Finalmente, queda por demostrar que $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ y $EK/E^{H_2}K$ son extensiones de constantes de grado d.

Como $K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M$ y $E_{\mathfrak{ge}}K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$, tenemos que

$$K_{\mathfrak{ge}} = (E_{\mathfrak{ge}}K)^H \subseteq E_{\mathfrak{ge}}K \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M.$$

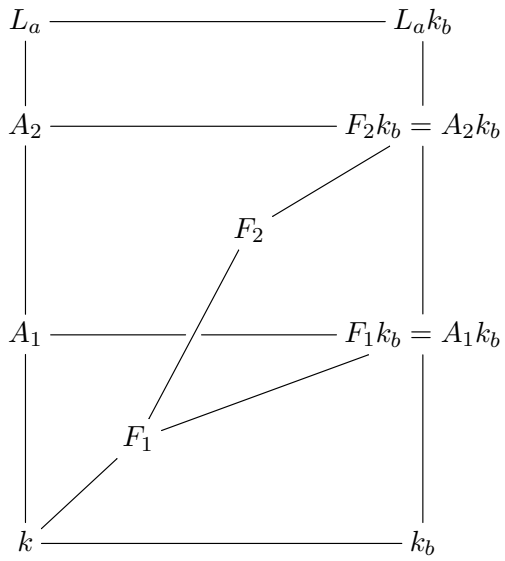
Sean $F_1 = K_{\mathfrak{ge}} \cap M$ y $F_2 = E_{\mathfrak{ge}}K \cap M$. Tenemos que $d = [E_{\mathfrak{ge}}K : K_{\mathfrak{ge}}] = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}) = [F_2 : F_1] = e_\infty(F_2/F_1)f_\infty(F_2/F_1)h_\infty(F_2/F_1)$. Como $e_\infty(F_2/F_1) \mid q^n$ y $h_\infty(F_2/F_1) = 1$, se sigue que

$$e_\infty(F_2/F_1) = e_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}) = 1 \quad \text{y} \quad f_\infty(F_2/F_1) = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}) = d.$$

Por lo tanto $k \subseteq F_1 \subseteq F_2 \subseteq M$ y $e_\infty(F_2/F_1) = 1$.

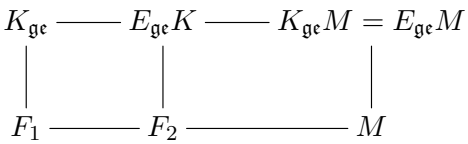
Sean a y b tal que $F_2 \subseteq F_1k_bL_a$. Sea $A_i = F_ik_b \cap L_a$, $i = 1, 2$. Teniendo en cuenta que $e_\infty(F_2/F_1) = 1$ y $F_ik_b = A_ik_b/A_i$, $i = 1, 2$, son extensiones de constantes, tenemos

que $e_\infty(A_2/A_1) = 1$.



$$e_\infty(F_2k_b/F_1k_b) = e_\infty(F_2/F_1) = e_\infty(A_2/A_1) = 1.$$

Como L_a/k es totalmente ramificada en $\mathcal{P}_\infty$, se sigue que $A_1 = A_2$. Por lo tanto $F_2k_b = F_1k_b$ y F_2/F_1 es una extensión de constantes.
Recordemos que $F_1 = K_{\mathfrak{ge}} \cap M$. Consideremos $K_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K \subseteq K_{\mathfrak{ge}}M = E_{\mathfrak{ge}}M$:



Por lo tanto $K_{\mathfrak{ge}} \subseteq F_2K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$. Se sigue que $E_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ es una extensión de constantes de grado $[E_{\mathfrak{ge}}K : K_{\mathfrak{ge}}] = |H| = d$.

Finalmente, probaremos que $EK/E^{H_2}K$ es una extensión de constantes.

Siguiendo el análisis anterior, tomamos ahora $F_1 := E^{H_2}K \cap M$ y $F_2 := EK \cap M$, obtenemos como resultado que la extensión F_2/F_1 resulta ser de constantes, luego por correspondencia de Galois se sigue el resultado.

□

Teorema 3.3. *Sea K/k una extensión abeliana finita $K \subseteq k(\Lambda_N)k_mL_n$. Sea*

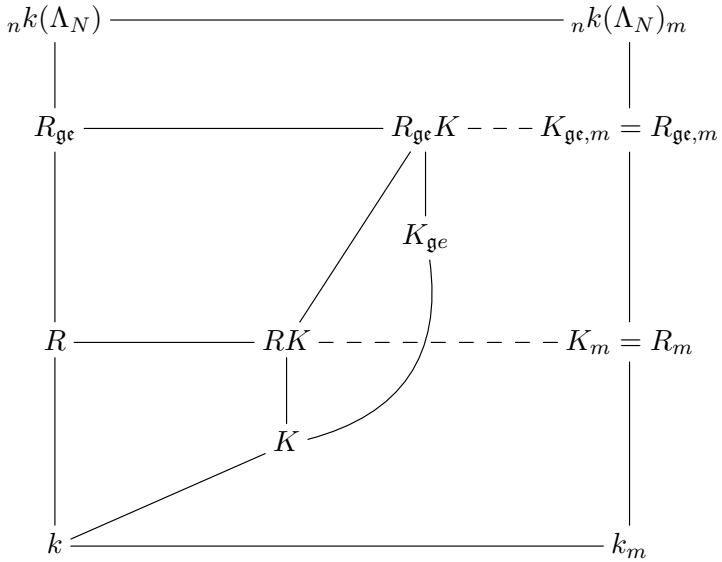
$$R := K_m \cap {}_nk(\Lambda_N).$$

Entonces

$$K_{\mathfrak{ge}} = R_{\mathfrak{ge}}^{\mathcal{H}_1}K = (R_{\mathfrak{ge}}K)^{\mathcal{H}},$$

en donde $\mathcal{H}$ es el grupo de descomposición de $S_\infty(K)$ en $R_{\mathfrak{ge}}K/K$, $\mathcal{H}_1 := \mathcal{H}|_{R_{\mathfrak{ge}}}$ y $\mathcal{H}_2 := \mathcal{H}_1|_R$.
Sea $d^* := f_\infty(RK/K)$. Tenemos que $\mathcal{H} \cong \mathcal{H}_1 \cong \mathcal{H}_2 \cong C_{d^*}$ y $d^*|q-1$. También tenemos que $R_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ y $RK/R^{\mathcal{H}_2}K$ son extensiones de constantes de grado d^*. Finalmente, el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$, en donde t es el grado de $S_\infty(K)$ en K.

Demostración. Como $R = K_m \cap {}_nk(\Lambda_N)$, tenemos el siguiente diagrama:



En donde $R_{\mathfrak{ge}}$ se calcula como en la ecuación (2.2) del Teorema 2.9 (poniendo $m = 1$ en dicho resultado). Por otro lado, como K_m/K es no ramificada y puesto que $K \subseteq RK \subseteq K_m = R_m$ se tiene que RK/K es una extensión no ramificada. Al ser $R_{\mathfrak{ge}}/R$ una extensión no ramificada, se obtiene que la extensión $R_{\mathfrak{ge}}K/K$ es no ramificada y procediendo de forma similar al Teorema 3.2 se obtiene que $R_{\mathfrak{ge}}K_{\mathfrak{ge}} = R_{\mathfrak{ge}}K$.

Ahora, sea $\mathcal{H}$ el grupo de descomposición de $S_\infty(K)$ en $R_{\mathfrak{ge}}K/K$. Como la extensión $R_{\mathfrak{ge}}K/RK$ es no ramificada, resulta que

$$|\mathcal{H}| = |D(S_\infty(K))| = f_\infty(R_{\mathfrak{ge}}K/K) = f_\infty(RK/K) = d^*,$$

donde $d^* \mid q-1$.
Puesto que $\mathcal{H}_1 = \mathcal{H}|_{R_{\mathfrak{ge}}}$ y $\mathcal{H}_2 = \mathcal{H}|_R$, se tiene que

$$K_{\mathfrak{ge}} = (R_{\mathfrak{ge}}K)^{\mathcal{H}} = R_{\mathfrak{ge}}^{\mathcal{H}_1}K \quad \text{y} \quad (RK)^{\mathcal{H}} = R^{\mathcal{H}_2}K$$

y que $\mathcal{H} \cong \mathcal{H}_1 \cong \mathcal{H}_2 \cong C_{d^*}$, teniéndose así que $K_{\mathfrak{ge}} \subseteq R_{\mathfrak{ge}}K \subseteq K_{\mathfrak{ge},m}$ y $K \subseteq R^{\mathcal{H}_2}K \subseteq RK \subseteq K_m$, resultando que las extensiones $R_{\mathfrak{ge}}K/K_{\mathfrak{ge}}$ y $RK/R^{\mathcal{H}_2}K$, son extensiones de constantes.

Finalmente, para ver que el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$, en donde t es el grado de $S_\infty(K)$ en K, ver el Lema 2.5. □

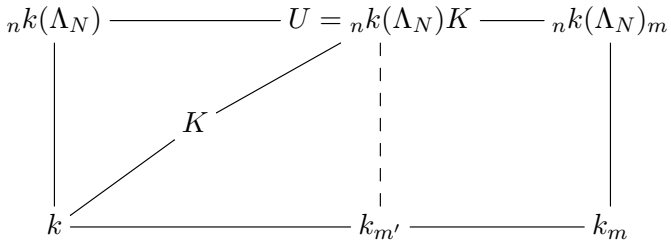
3.2. Conductor de constantes

Sea K una extensión abeliana finita de k. Por el Teorema de Kronecker–Weber tenemos que existen $m \in \mathbb{N}$, $n \in \mathbb{N} \cup \{0\}$ y $N \in R_T$ tal que $K \subseteq {}_nk(\Lambda_N)_m$. Los mínimos n y N que satisfacen esta condición están dados por la teoría de campos de clases por medio del conductor local de la extensión K/k: n para $\mathcal{P}_\infty$ y N para los primos finitos.

En esta subsección, determinaremos el mínimo m que satisface la condición anterior y veremos que este m está relacionada con el número d dado en el Teorema 3.2. El número m será llamado *el conductor de constantes* de la extensión abeliana K/k.

Note que en general $\mathbb{F}_{q^m}$ no es necesariamente el campo de constantes de K ni el de $K_{\mathfrak{ge}}$. Por ejemplo, sea $q \equiv 3 \bmod 4$. Como $\sqrt{-1} \notin \mathbb{F}_q$, tenemos que $k(\sqrt{-T}) \neq K := k(\sqrt{T})$. El campo de constantes de K es $\mathbb{F}_q$ y K no es ciclotómico. De hecho $K \subseteq k(\Lambda_T)\mathbb{F}_{q^2}$ y $m = 2$ es el conductor de constantes de K. También tenemos en este caso que $K_{\mathfrak{ge}} = K$.

Ahora, sean $m \in \mathbb{N}$, $n \in \mathbb{N} \cup \{0\}$ y $N \in R_T$ tales que $K \subseteq {}_nk(\Lambda_N)_m$ y en donde m es el mínimo con respecto a esta condición. Note que m podría depender de n y N. Considere el siguiente diagrama de extensiones de Galois



Esto es, sean $U := {}_nk(\Lambda_N)K$ y $k_{m'} := U \cap k_m$. Por la correspondencia de Galois, tenemos que $U = {}_nk(\Lambda_N)K = {}_nk(\Lambda_N)k_{m'} = {}_nk(\Lambda_N)_{m'} \supseteq K$.

Como m es mínimo, obtenemos que $m' = m$. Esto es, m está determinado por la igualdad

$$ {}_nk(\Lambda_N)K = {}_nk(\Lambda_N)_m. \tag{3.5}$$

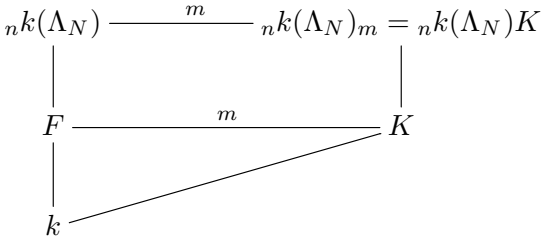
Ahora, veremos que m es independiente de n y de N. Sean $n_i \in \mathbb{N}$, $N_i \in R_T$ y $m_i \in \mathbb{N}$ el mínimo tal que $K \subseteq {}_{n_i}k(\Lambda_{N_i})_{m_i}$, $i = 1, 2$.

Sean $n_0 := \max\{n_1, n_2\}$, $N_0 = \operatorname{mcm}[N_1, N_2]$ y $m_0 \in \mathbb{N}$ mínimo tal que $K \subseteq {}_{n_0}k(\Lambda_{N_0})_{m_0}$.

De (3.5), se sigue que

$$\begin{aligned} {}_{n_0}k(\Lambda_{N_0})K &= L_{n_0}\big({}_{n_i}k(\Lambda_{N_i})k(\Lambda_{N_0})\big)K = L_{n_0}\big({}_{n_i}k(\Lambda_{N_i})K\big)k(\Lambda_{N_0}) \\ &= L_{n_0}\big({}_{n_i}k(\Lambda_{N_i})_{m_i}k(\Lambda_{N_0})\big) = {}_{n_0}k(\Lambda_{N_0})_{m_i}, \quad \text{y} \\ {}_{n_0}k(\Lambda_{N_0})K &= {}_{n_0}k(\Lambda_{N_0})_{m_0}. \end{aligned}$$

Por lo tanto $m_1 = m_2 = m_0$.
Entonces, consideremos $K \subseteq {}_nk(\Lambda_N)_m$ con m mínimo. Sea $F := K \cap {}_nk(\Lambda_N)$ y consideremos el siguiente diagrama (ver (3.5))



Sea t el grado de $S_\infty(K)$ en K. Esto es, $t = f_\infty(K/k)$. Tenemos que

$$e_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) = 1, \quad f_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) = m.$$

En particular

$$\begin{aligned} \{1\} = I_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) \subseteq I_\infty(K/F), \\ C_m \cong D_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) \subseteq D_\infty(K/F). \end{aligned}$$

Como $[K : F] = m$ y $m \leq |D_\infty(K/F)| \leq [K : F] = m$, se sigue que $|D_\infty(K/F)| = m$ y que $D_\infty(K/F) \cong C_m$. En particular tenemos que

$$h_\infty(K/F) = 1 \quad \text{y} \quad h_\infty({}_nk(\Lambda_N)_m/{}_nk(\Lambda_N)) = 1.$$

Por otro lado, tenemos que

$$t = f_\infty(K/k) = f_\infty(K/F)f_\infty(F/k) = f_\infty(K/F) \cdot 1 = f_\infty(K/F),$$

esto es, $f_\infty(K/F) = t$. Además

$$e_\infty(K/F)f_\infty(K/F)h_\infty(K/F) = e_\infty(K/F) \cdot t \cdot 1 = m,$$

así que $e_\infty(K/F) = \frac{m}{t}$. Por tanto

$$m = [K : F] = f_\infty(K/F)e_\infty(K/F) = te_\infty(K/F) = t\frac{e_\infty(K/k)}{e_\infty(F/k)}. \tag{3.6}$$

Ahora, hallaremos la relación entre los números m mínimo y $d = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}})$ dados en el Teorema 3.2. Recordemos que $M = L_n k_m$, $E = KM \cap k(\Lambda_N)$ y que $EM = KM$. Tenemos que

$$E_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}K \subseteq E_{\mathfrak{ge}}KL_n \subseteq E_{\mathfrak{ge}}KM = E_{\mathfrak{ge}}EM = E_{\mathfrak{ge}}M.$$

Sea $A := E_{\mathfrak{ge}}K \cap M$ y $B := E_{\mathfrak{ge}}KL_n \cap M$. Por la correspondencia de Galois tenemos que $E_{\mathfrak{ge}}K = E_{\mathfrak{ge}}A$ y $E_{\mathfrak{ge}}KL_n = E_{\mathfrak{ge}}B$.

$$\begin{array}{ccccccc} E_{\mathfrak{ge}} & \text{——} & E_{\mathfrak{ge}}K & \text{——} & E_{\mathfrak{ge}}KL_n & \text{——} & E_{\mathfrak{ge}}M \\ | & & | & & | & & | \\ k & \text{————} & A & \text{————} & B & \text{————} & M \end{array}$$

Tenemos que $L_n \subseteq E_{\mathfrak{ge}}KL_n \cap M = B \subseteq M = L_n k_m$. Por lo tanto B/L_n es una extensión de constantes. Digamos que $B = L_n k_{m'}$ con $m'|m$. Por la correspondencia de Galois, obtenemos que

$$K \subseteq E_{\mathfrak{ge}}KL_n = E_{\mathfrak{ge}}B = E_{\mathfrak{ge}}L_n k_{m'} \subseteq k(\Lambda_N)L_n k_{m'} = {}_nk(\Lambda_n)_{m'}.$$

Ya que m es el mínimo, $m' = m$, $B = M$ y $E_{\mathfrak{ge}}KL_n = E_{\mathfrak{ge}}M$.
Ahora, $E_{\mathfrak{ge}}(AL_n) = (E_{\mathfrak{ge}}A)L_n = (E_{\mathfrak{ge}}K)L_n = E_{\mathfrak{ge}}M$. Por la correspondencia de Galois se sigue que $AL_n = M$. Consideremos el siguiente cuadro de Galois:

$$\begin{array}{ccc} L_n & \text{———} & AL_n = M = L_n k_m \\ | & & | \\ A \cap L_n & \text{————————} & A \end{array}$$

Tenemos que $f_\infty(AL_n/L_n) = f_\infty(M/L_n) = m$ y $e_\infty(AL_n/L_n) = e_\infty(M/L_n) = 1$. Así

$$\begin{aligned} &\{1\} = I_\infty(AL_n/L_n) \subseteq I_\infty(A/A \cap L_n) \quad \text{y} \\ &C_m \cong D_\infty(AL_n/L_n) \subseteq D_\infty(A/A \cap L_n). \end{aligned}$$

Puesto que $[A : A \cap L_n] = [M : L_n] = m$, se sigue que $D_\infty(A/A \cap L_n) \cong C_m$, $e_\infty(A/A \cap L_n) = 1$ y $f_\infty(A/A \cap L_n) = m$. Por lo tanto

$$f_\infty(E_{\mathfrak{ge}}K/k) = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}})f_\infty(K_{\mathfrak{ge}}/K)f_\infty(K/k) = d \cdot 1 \cdot t = td.$$

Así

$$f_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}K) = \frac{f_\infty(E_{\mathfrak{ge}}M/k)}{f_\infty(E_{\mathfrak{ge}}K/k)} = \frac{m}{td}.$$

Finalmente

$$\begin{aligned} \frac{m}{td} &= f_\infty(E_{\mathfrak{ge}}M/E_{\mathfrak{ge}}K)|[E_{\mathfrak{ge}}M : E_{\mathfrak{ge}}K] = [M : A] \\ &= [L_n : A \cap L_n]|[L_n : k] = q^n. \end{aligned}$$

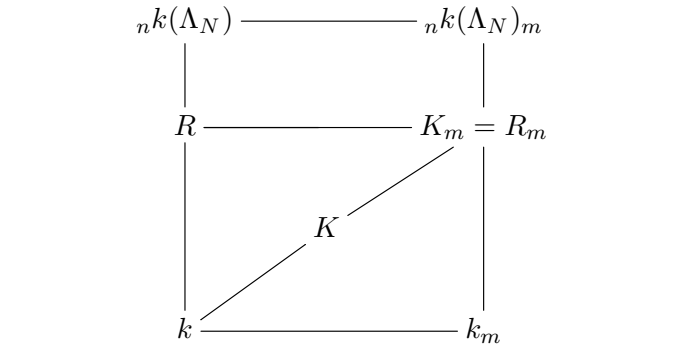
Se sigue que

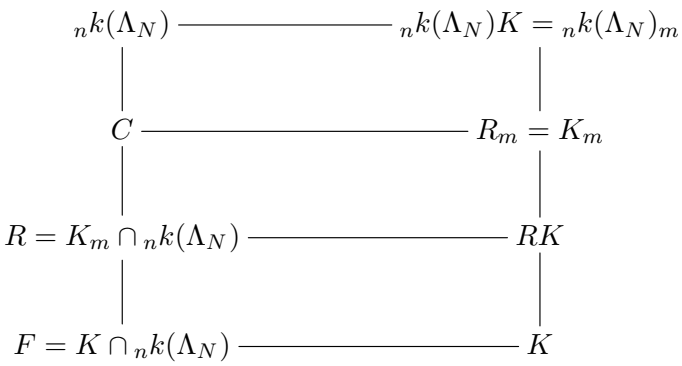
$$m = tdp^s$$

para algún $s \in \mathbb{N} \cup \{0\}$.
Además, $f_\infty(K_m/K) = \frac{m}{t} = e_\infty(K/F)$. Note que

$$td = f_\infty(K/k)f_\infty(EK/K) = f_\infty(EK/k).$$

Calculemos m de otra forma. Recordemos $F = K \cap {}_nk(\Lambda_N)$, sea $R = K_m \cap {}_nk(\Lambda_N)$, se sigue que $K_m = R_m$. Ahora, $K, R \subseteq RK \subseteq K_m = R_m$. Tenemos los siguientes cuadros de Galois





Note que en general $R \neq F$. Por ejemplo, si $q \equiv 3 \pmod 4$, $\sqrt{-1} \notin \mathbb{F}^*$ y si $K := k(\sqrt{T})$, entonces $n = 0, m = 2, N = T$ y $F = K \cap {}_nk(\Lambda_N) = k(\sqrt{T}) \cap k(\Lambda_T) = k$, $R = K_m \cap {}_nk(\Lambda_N) = \mathbb{F}_{q^2}(\sqrt{T}) \cap k(\Lambda_T) = k(\sqrt{-T}) \neq k$.
Sea $C := K_m \cap {}_nk(\Lambda_N)$. Entonces $C = R$ y por la correspondencia de Galois, obtenemos que $RK = R_m = K_m$.
Se sigue que el campo de constantes de RK es $\mathbb{F}_{q^m}$. El campo de constantes de $RK_{\mathfrak{ge}}$ es también $\mathbb{F}_{q^m}$.
Ahora, el campo de constantes de $K_{\mathfrak{ge}}$ es $\mathbb{F}_{q^t}$. Por otro lado, tenemos que

$$RK_{\mathfrak{ge}}/R_{\mathfrak{ge}}^{\mathcal{H}_1}K$$

es una extensión de constantes de grado $d^* = |\mathcal{H}_1|$, recordemos que $d^* = |\mathcal{H}|$ y $\mathcal{H}_1 = \mathcal{H}|_{R_{\mathfrak{ge}}}$ con $\mathcal{H}$ el grupo de descomposición de $S_\infty(K)$ en $R_{\mathfrak{ge}}K/K$. Así, el campo de constantes de $RK_{\mathfrak{ge}}$ es $\mathbb{F}_{q^{td^*}}$. Se sigue que $td^* = m$. Entonces tenemos el siguiente resultado.

Teorema 3.4. (Conductor de Constantes) *Sea K una extensión abeliana finita de k. Sea $m \in \mathbb{N}$, $n \in \mathbb{N} \cup \{0\}$ y $N \in R_T$ tal que $K \subseteq {}_nk(\Lambda_N)_m$ y tal que m es mínimo con respecto a esta propiedad. Entonces m es independiente de n y N. Sea $t = f_\infty(K/k)$ el grado de los primos infinitos de K.*

(a).- *Sean $M = L_nk_m$, $E = KM \cap k(\Lambda_N)$, $F = K \cap {}_nk(\Lambda_N)$ y $d = f_\infty(EK/K) = f_\infty(E_{\mathfrak{ge}}K/K_{\mathfrak{ge}})$. Entonces*

$$ {}_nk(\Lambda_N)K = {}_nk(\Lambda_N)_m $$

y

$$ m = [K : F] = te_\infty(K/F) = tdp^s = f_\infty(EK/k)p^s $$

para algún $s \geq 0$. En particular

$$ e_\infty(K/F) = dp^s = f_\infty(K_m/K). $$

(b).- *Sean $R = K_m \cap {}_nk(\Lambda_N)$ y $d^* = f_\infty(RK/K)$. Entonces*

$$ m = te_\infty(K/F) = td^* = f_\infty(RK/k). $$

En particular

$$ d^* = f_\infty(RK/K) = e_\infty(K/F). $$ □

Nota 3.5. Cuando $p \nmid \frac{m}{t}$, en particular cuando K/k es moderadamente ramificada en $\mathcal{P}_\infty$, tenemos que $s = 0$ y $m = td$. Cuando K/k no es moderadamente ramificada tenemos que $s \geq 1$.

Nota 3.6. De los Teoremas 3.2 y 3.3 se sigue que si $K \subseteq {}_nk(\Lambda_N)_m$, entonces $K_{\mathfrak{ge}} \subseteq {}_nk(\Lambda_N)_m$. En particular el conductor de constantes de K y el de $K_{\mathfrak{ge}}$ son el mismo.

Capítulo 4

Extensiones de tipo $(K_1K_2)_{\mathfrak{ge}}/(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$

Un resultado que se deriva de forma limpia usando el nuevo cálculo del campo de géneros, es el dado por el Teorema 4.6. Pero veamos primero los siguientes resultados.

Para una extensión abeliana K/k, la descripción explícita de $K_{\mathfrak{ge}}$, esto es, una descripción en términos de la ecuación generada de $K_{\mathfrak{ge}}$, depende de la descripción explícita de $E_{\mathfrak{ge}}$ (Teorema 3.2). En esta primera parte presentamos algunos detalles con el fin de hallar $E_{\mathfrak{ge}}$. Para resultados y notación relativa a los caracteres de Dirichlet usamos como referencia [27, Chapter 12]. Aquí K denota un campo $k \subseteq K \subseteq k(\Lambda_N)$ para algún $N \in R_T$ y $k = \mathbb{F}_q(T)$.

Observación 4.1. Sea $k \subseteq K \subseteq k(\Lambda_N)$ y sea X el grupo de caracteres de Dirichlet asociado a K. Si L es el campo asociado a $\prod_{P \in R_T^+} X_P$, entonces

$$K_{\mathfrak{ge}} = L^{\mathcal{D}},$$

donde $\mathcal{D}$ es el grupo de descomposición de cualquier primo $\mathfrak{p} \in S_\infty(K)$ en L/K.

Proposición 4.2. *Con la notación anterior, sea X el grupo de caracteres de Dirichlet correspondiente a K. Fijamos $P \in R_T^+$. Sea Y un grupo de caracteres de Dirichlet tal que $Y = Y_P$, esto es, para cualquier $\chi \in Y$, el conductor de χ es una potencia de P: $\mathcal{F}_\chi = P^{\alpha_\chi}$ para algún $\alpha_\chi \in \mathbb{N} \cup \{0\}$. Sea L el campo asociado a $\langle X, Y\rangle$, esto es, si F es el campo asociado a Y, entonces $L = KF$. Si KF/K es no ramificada en P, entonces $Y \subseteq X_P$.*

Demostración. Tenemos que

$$|\langle X, Y\rangle_P| = e_P(KF/k) = e_P(KF/K)e_P(K/k) = e_P(K/k) = |X_P|.$$

Puesto que $X_P \subseteq \langle X, Y\rangle_P$, se sigue que $X_P = \langle X, Y\rangle_P$. Ya que $Y_P \subseteq \langle X, Y\rangle_P$, el resultado se sigue. □

Corolario 4.3. *En el contexto de la Proposición 4.2, si* $|Y| = |X_P|$*, entonces* $Y = X_P$*.* $\square$

Sea K/k una p–extensión abeliana finita. Recordemos que $k = \mathbb{F}_q(T)$, digamos $q = p^\ell$ para algún $\ell \in \mathbb{N}$. Supondremos que $\mathbb{F}_{p^u} \subseteq \mathbb{F}_q$, es decir, $u \mid \ell$. Sea $v \in \mathbb{N}$
Entonces tenemos que

$$\mathrm{Gal}(K/k) \cong \left(\mathbb{Z}/p^{\alpha_1}\mathbb{Z}\right) \times \cdots \times \left(\mathbb{Z}/p^{\alpha_u}\mathbb{Z}\right) \quad \text{con}$$
$$1 \leq \alpha_1 \leq \cdots \leq \alpha_u = v.$$

Existen $\vec{w}_1, \ldots, \vec{w}_u \in W_v(\bar{k})$ tales que $\vec{w}_i^{\,p} \overset{\bullet}{-} \vec{w}_i = \vec{\xi}_i \in W_v(k)$, con $K = k(\vec{w}_1, \cdots, \vec{w}_v)$.
También tenemos que existe $\vec{y}_0 \in W_v(\bar{k})$ tal que $K = k(\vec{y}_0)$ con

$$\vec{y}_0^{\,p^u} \overset{\bullet}{-} \vec{y}_0 = \vec{\xi}_0 \quad \text{para algún} \quad \vec{\xi}_0 \in W_v(k)$$

(vea [6, Theorem 8.5]). Aquí $\bar{k}$ denota una cerradura algebraica de k.
Sean $P_1, \ldots, P_r \in R_T^+$ los primos finitos de k ramificados en K. De [6, Theorem 8.10] se sigue que $\vec{\xi}_0$ se puede descomponer como

$$\vec{\xi}_0 = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r \overset{\bullet}{+} \vec{\gamma}, \tag{4.1}$$

en donde $\delta_{i,j} = \frac{Q_{i,j}}{P_i^{e_{i,j}}}$, $e_{i,j} \geq 0$, $Q_{i,j} \in R_T$ y si $e_{i,j} > 0$, entonces $e_{i,j} = \lambda_{i,j}p^{m_{i,j}}$, $\mathrm{mcd}(\lambda_{i,j}, p) = 1$, $0 \leq m_{i,j} < n$, $\mathrm{mcd}(Q_{i,j}, P_i) = 1$ y $\mathrm{gr}\,(Q_{i,j}) < \mathrm{gr}\,(P_i^{e_{i,j}})$, y $\gamma_j = f_j(T) \in R_T$ con $\mathrm{gr}\, f_j = \nu_j p^{m_j}$ y $\mathrm{mcd}(q, \nu_j) = 1$, $0 \leq m_j < n$, con n como en (1.1), cuando $f_j \notin \mathbb{F}_q$.
Si el índice de ramificación de P_i es $p^{a_i} < p^v$, podemos escribir $\vec{\delta}_i = (\delta_{i,1}, \ldots, \delta_{i,v}) = (0, \ldots, 0, \delta_{i,(v-a_i+1)}, \ldots, \delta_{i,v})$. En particular $\mathcal{P}_\infty$ se descompone totalmente en $k(\vec{y}_i)/k$, donde $\vec{y}_i^{\,p^u} \overset{\bullet}{-} \vec{y}_i = \vec{\delta}_i$ (ver [6, Theorem 8.13]).
Sea $\vec{z}^{\,p^u} \overset{\bullet}{-} \vec{z} = \vec{\gamma}$. En $k(\vec{z})/k$, el único posible primo ramificado es $\mathcal{P}_\infty$. Note que si

$$\vec{y} = \vec{y}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{y}_r, \quad \text{entonces} \quad \vec{y}^{\,p^u} \overset{\bullet}{-} \vec{y} = \vec{\xi}_0 \overset{\bullet}{-} \vec{\gamma} = \vec{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_r$$

y $\mathcal{P}_\infty$ se descompone totalmente en $k(\vec{y})/k$.
Observemos que $\vec{y}_0 = \vec{y} \overset{\bullet}{+} \vec{z}$, $k(\vec{z}) \subseteq M$ y $k(\vec{y} \overset{\bullet}{+} \vec{z}) \subseteq k(\vec{y})k(\vec{z})$.

Tenemos el siguiente resultado.

Proposición 4.4. *Sea* K/k *una* p*–extensión abeliana finita con grupo de Galois* $\mathrm{Gal}(K/k) = G \cong G_1 \times \cdots \times G_s$ *con* $G_i \cong \mathbb{Z}/p^{\alpha_i}\mathbb{Z}$, $1 \leq i \leq s$*. Sea* K *la composición* $K = K_1 \cdots K_s$ *tal que* $\mathrm{Gal}(K_i/k) \cong G_i$*. Sean* $P_1, \ldots, P_r$ *los primos finitos ramificados en* K/k*. Sea* $K_i = k(\vec{w}_i)$ *dado por la ecuación*

$$\vec{w}_i^{\,p} \overset{\bullet}{-} \vec{w}_i = \vec{\xi}_i, \quad 1 \leq i \leq s.$$

Escribiendo cada $\vec{\xi}_i$ como en [20, Theorem 5.5] *esto es,*

$$\vec{\xi}_i = \vec{\delta}_{i,1} \overset{\bullet}{+} \cdots \overset{\bullet}{+} \vec{\delta}_{i,r} \overset{\bullet}{+} \vec{\gamma}_i,$$

tal que todos los componentes de $\vec{\delta}_{i,j}$ son escritos de manera que el grado del numerador es menor que el grado del denominador, el soporte del denominador es al lo más $\{P_j\}$ y las componentes de $\vec{\gamma}_i$ son polinomios. Sean

$$\vec{w}_{i,j}^{\,p} \overset{\bullet}{-} \vec{w}_{i,j} = \vec{\delta}_{i,j}, \quad 1 \leq i \leq s, \quad 1 \leq j \leq r$$

y

$$\vec{z}_i^{\,p} \overset{\bullet}{-} \vec{z}_i = \vec{\gamma}_i, \quad 1 \leq i \leq s.$$

Entonces

$$K_{\mathfrak{ge}} = k\big(\vec{w}_{i,j}, \vec{z}_i \mid 1 \leq i \leq s, 1 \leq j \leq r\big).$$

Demostración. Ver [7, Corolary 6.7]. □

Proposición 4.5. *Sean $E \subseteq k(\Lambda_N)$ una extensión cíclica de k de grado t primo relativo con $p(q-1)$. Sea $P_1, \ldots, P_r \in R_T^+$ los primos de k ramificados en E. Entonces*

$$E_{\mathfrak{ge}} = \prod_{j=1}^{r} F_j,$$

en donde $k \subseteq F_j \subseteq k(\Lambda_{P_j})$ es el subcampo de grado a_j sobre k, a_j es el orden de χ_{P_j}, y χ es el caracter asociado a E.

Demostración. Consideremos una extensión cíclica K/k de grado t tal que $\mathrm{mcd}(t, p(q-1)) = 1$. Tenemos que $E = KM \cap k(\Lambda_N)$ satisface que $[E : k]$ es primo relativo con $q-1$. Por la observación 4.1, tenemos que $E'_{\mathfrak{ge}} = E_{\mathfrak{ge}}$ y $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K$.
El resultado se sigue del hecho de que $X = \langle \chi \rangle$ es el grupo de caracteres de Dirichlet asociado a E, $E_{\mathfrak{ge}}$ es el campo correspondiente a $\prod_{j=1}^{r} X_{P_j}$, $X_{P_j} = \langle \chi_{P_j} \rangle$ (ver la Proposición 4.2) y F_j es el campo asociado a χ_{P_j}. □

4.1. Ejemplo $(K_1K_2)_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$

De lo anterior, tenemos el siguiente resultado:

Teorema 4.6. *Sea K/k una extensión abeliana de grado t con $\mathrm{mcd}(t, q-1) = 1$. Sean $P_1, \ldots, P_r \in R_T^+$ los primos de k ramificados en K. Sea $E = KM \cap k(\Lambda_N) = E_0E_1 \cdots E_s$ donde E_i/k es una extensión cíclica de grado t_i, $\mathrm{mcd}(t_i, p(q-1)) = 1$, $1 \leq i \leq s$ y E_0/k es una p–extensión abeliana. Entonces*

$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}K, \quad \textit{donde} \quad E_{\mathfrak{ge}} = (E_0)_{\mathfrak{ge}}(E_1)_{\mathfrak{ge}} \cdots (E_s)_{\mathfrak{ge}},$$

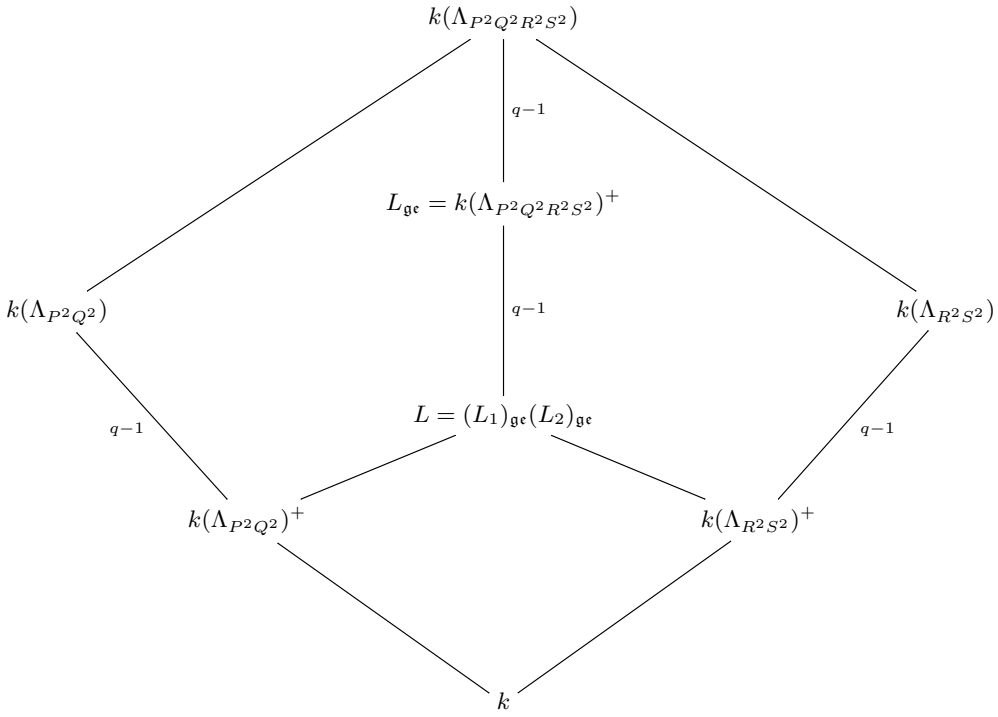
$(E_0)_{\mathfrak{ge}}$ está dado por la Proposición 4.4 y $(E_i)_{\mathfrak{ge}} = \prod_{j=1}^{r} F_{i,j}$ está dado por la Proposición 4.5, $1 \leq i \leq s$.

Más aún, sea $b_{i,j} := [F_{i,j} : k]$. Entonces $L_j := \prod_{i=1}^{s} F_{i,j}$ es el subcampo de $k(\Lambda_{P_j})$ de grado $b_j := \mathrm{mcm}[b_{i,j}, 1 \leq i \leq s]$ sobre k. Tenemos que

$$K_{\mathfrak{ge}} = (E_0)_{\mathfrak{ge}}\Big(\prod_{j=1}^{r} L_j\Big)K. \qquad \square$$

Respecto al Teorema 4.6, en general si $L := L_1L_2$, entonces $(L_1)_{\mathfrak{ge}}(L_2)_{\mathfrak{ge}} \subseteq L_{\mathfrak{ge}}$, pero la contención contraria no siempre se tiene:

Ejemplo 4.7. Sean $q > 2$ y $P, Q, R, S \in R_T$ cuatro polinomios irreducibles en k. Sean $L_1 := k(\Lambda_{P^2Q^2})^+$ y $L_2 := k(\Lambda_{R^2S^2})^+$. Entonces $L_1 = (L_1)_{\mathfrak{ge}}$ y $L_2 = (L_2)_{\mathfrak{ge}}$. Sea $L := L_1L_2$. Entonces $L_{\mathfrak{ge}} = k(\Lambda_{P^2Q^2R^2S^2})^+$ y $[L_{\mathfrak{ge}} : L] = q - 1 > 1$. Así $L_{\mathfrak{ge}} = (L_1L_2)_{\mathfrak{ge}} \neq (L_1)_{\mathfrak{ge}}(L_2)_{\mathfrak{ge}} = L$.



Entonces, dado un campo L tal que $L = L_1L_2$, estudiaremos condiciones que garanticen se de la igualdad $L_{\mathfrak{ge}} = (L_1)_{\mathfrak{ge}}(L_2)_{\mathfrak{ge}}$. En general, estudiaremos la extensión $L_{\mathfrak{ge}}/(L_1)_{\mathfrak{ge}}(L_2)_{\mathfrak{ge}}$.

4.2. Caso general de las extensiones $(K_1K_2)_{\mathfrak{ge}}/(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$

En esta sección estudiaremos el comportamiento de las extensiones tipo

$$(K_1K_2)_{\mathfrak{ge}}/(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}},$$

con el fin de saber si nos proveen alguna ventaja al estudiar campos de tipo $K = K_1K_2$, con K_1 y K_2 campos de funciones sobre $k = \mathbb{F}_q(T)$.

Sea $K := K_1K_2$ con K_1, K_2 como antes y supongamos que $K \subseteq {}_nk(\Lambda_N)_m$. Sea $E := E_1E_2$, con $E_i := {}_n(K_i)_m \cap k(\Lambda_N)$, $i = 1, 2$. Entonces tenemos que $E \subseteq {}_nK_m \cap k(\Lambda_N)$.

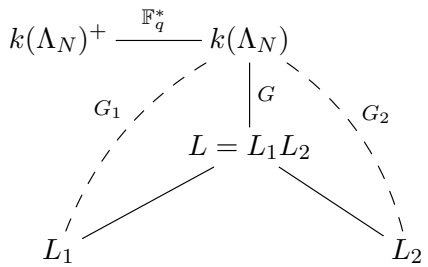
Proposición 4.8. *Sean* $L_1, L_2 \subseteq k(\Lambda_N)$, $L := L_1L_2$, $L^+ := L \cap k(\Lambda_N)^+$ *y* $L_i^+ := L_i \cap k(\Lambda_N)^+$, $i = 1, 2$. *Entonces*

$$[L^+ : L_1^+L_2^+] \,|\, q - 1.$$

Demostración. Sean $G := \mathrm{Gal}(k(\Lambda_N)/L)$, $G_1 := \mathrm{Gal}(k(\Lambda_N)/L_1)$ y $G_2 := \mathrm{Gal}(k(\Lambda_N)/L_2)$. Tenemos que $G = G_1 \cap G_2$. Sean $L^+ = L \cap k(\Lambda_N)^+ = k(\Lambda_N)^{G\mathbb{F}_q^*}$, $L_1^+ = L_1 \cap k(\Lambda_N)^+ = k(\Lambda_N)^{G_1\mathbb{F}_q^*}$ y $L_2^+ = L_2 \cap k(\Lambda_N)^+ = k(\Lambda_N)^{G_2\mathbb{F}_q^*}$. Como $G\mathbb{F}_q^* < G_1\mathbb{F}_q^* \cap G_2\mathbb{F}_q^*$, tenemos que

$$L_1^+L_2^+ = k(\Lambda_N)^{G_1\mathbb{F}_q^*}k(\Lambda_N)^{G_2\mathbb{F}_q^*} = k(\Lambda_N)^{G_1\mathbb{F}_q^* \cap G_2\mathbb{F}_q^*} \subseteq k(\Lambda_N)^{G\mathbb{F}_q^*} = L^+,$$

veamos el siguiente diagrama:



Así

$$\begin{aligned}
[L^+ : L_1^+L_2^+] &= |G_1\mathbb{F}_q^* \cap G_2\mathbb{F}_q^* : G\mathbb{F}_q^*| = \frac{|G_1\mathbb{F}_q^* \cap G_2\mathbb{F}_q^*|}{|G\mathbb{F}_q^*|} \\
&= \frac{\frac{|G_1\mathbb{F}_q^*||G_2\mathbb{F}_q^*|}{|G_1G_2\mathbb{F}_q^*|}}{\frac{|G||\mathbb{F}_q^*|}{|G\cap\mathbb{F}_q^*|}} = \frac{|G_1\mathbb{F}_q^*||G_2\mathbb{F}_q^*||G\cap\mathbb{F}_q^*|}{(q-1)|G||G_1G_2\mathbb{F}_q^*|} \\
&= \frac{|G_1||\mathbb{F}_q^*||G_2||\mathbb{F}_q^*||G\cap\mathbb{F}_q^*|}{(q-1)|G||G_1\cap\mathbb{F}_q^*||G_2\cap\mathbb{F}_q^*||G_1G_2\mathbb{F}_q^*|} \\
&= \frac{(q-1)^2}{(q-1)}\frac{|G_1||G_2||G\cap\mathbb{F}_q^*|}{|G||G_1G_2\mathbb{F}_q^*||G_1\cap\mathbb{F}_q^*||G_2\cap\mathbb{F}_q^*|} \\
&= (q-1)\frac{|G_1||G_2|}{|G|}\frac{|G\cap\mathbb{F}_q^*|}{|G_1\cap\mathbb{F}_q^*||G_2\cap\mathbb{F}_q^*|}\frac{1}{|G_1G_2\mathbb{F}_q^*|} \\
&= (q-1)\frac{|G_1||G_2|}{|G_1\cap G_2|}\frac{1}{|G_1G_2\mathbb{F}_q^*|}\frac{|G\cap\mathbb{F}_q^*|}{|G_1\cap\mathbb{F}_q^*||G_2\cap\mathbb{F}_q^*|} \\
&= (q-1)\frac{|G_1G_2|}{|G_1G_2\mathbb{F}_q^*|}\frac{|G\cap\mathbb{F}_q^*|}{|G_1\cap\mathbb{F}_q^*||G_2\cap\mathbb{F}_q^*|} \\
&= (q-1)\frac{1}{|(G_1\cap\mathbb{F}_q^*)(G_2\cap\mathbb{F}_q^*)|}\frac{1}{[L_1\cap L_2 : L_1^+\cap L_2^+]}.
\end{aligned}$$

Sea $\alpha := |(G_1\cap\mathbb{F}_q^*)(G_2\cap\mathbb{F}_q^*)|[L_1\cap L_2 : L_1^+\cap L_2^+]$. Ya que $[L^+ : L_1^+L_2^+] \in \mathbb{Z}$ se sigue que $\alpha \mid q-1$ y $[L^+ : L_1^+L_2^+] \mid q-1$. □

Proposición 4.9. *Sea $L \subseteq k(\Lambda_N)$. Si $k(\Lambda_N)^+ \subseteq L \subseteq k(\Lambda_N)$, entonces $L_{\mathfrak{ge}} = L$.*

Demostración. Tenemos que $L_{\mathfrak{ge}_{\mathfrak{x}}} = k(\Lambda_N)$ entonces de [7, Theorem 2.1] se sigue que $L_{\mathfrak{ge}} = L^+_{\mathfrak{ge}_{\mathfrak{x}}}L = k(\Lambda_N)^+L = L$. □

Sea $E = E_1E_2 \subseteq k(\Lambda_N)$. Sean Y_1 y Y_2 los grupos de caracteres de Dirichlet asociados con $(E_1)_{\mathfrak{ge}_{\mathfrak{x}}}$ y $(E_2)_{\mathfrak{ge}_{\mathfrak{x}}}$ respectivamente. Entonces, del Teorema de Leopoldt [25, Proposición 14.4.1], tenemos que $Y = Y_1Y_2$ es el grupo de caracteres asociado a $E_{\mathfrak{ge}_{\mathfrak{x}}}$, en donde Y_1Y_2 es el grupo de caracteres de Dirichlet asociado al campo $(E_1)_{\mathfrak{ge}_{\mathfrak{x}}}(E_2)_{\mathfrak{ge}_{\mathfrak{x}}}$ [25, Proposición 9.4.33], es decir, $E_{\mathfrak{ge}_{\mathfrak{x}}} = (E_1)_{\mathfrak{ge}_{\mathfrak{x}}}(E_2)_{\mathfrak{ge}_{\mathfrak{x}}}$. De la Proposición 4.8 obtenemos que

$$[E^+_{\mathfrak{ge}_{\mathfrak{x}}} : (E_1)^+_{\mathfrak{ge}_{\mathfrak{x}}}(E_2)^+_{\mathfrak{ge}_{\mathfrak{x}}}] \mid q-1.$$

Tenemos los siguientes resultados.

Proposición 4.10. *Sea $K_1, K_2 \subseteq {}_nk(\Lambda_N)_m$, $K = K_1K_2$ y E_1, E_2 como antes. Si $K_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$, entonces $E_{\mathfrak{ge}} = (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$.*

Demostración. Sean $K = K_1K_2 \subseteq {}_nk(\Lambda_N)_m$ y $E := E_1E_2 \subseteq k(\Lambda_N)$. Consideremos los campos $(K_{\mathfrak{ge}})_m$ y $(E_{\mathfrak{ge}})_m$. Ahora, de [7, Theorem 2.2] tenemos $(E_{\mathfrak{ge}})_m = (K_{\mathfrak{ge}})_m$ y $((K_i)_{\mathfrak{ge}})_m = ((E_i)_{\mathfrak{ge}})_m$, $i = 1, 2$. Por lo tanto

$$\begin{aligned}(E_{\mathfrak{ge}})_m = (K_{\mathfrak{ge}})_m &= ((K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}})_m = ((K_1)_{\mathfrak{ge}})_m((K_2)_{\mathfrak{ge}})_m \\ &= ((E_1)_{\mathfrak{ge}})_m((E_2)_{\mathfrak{ge}})_m = ((E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}})_m.\end{aligned}$$

Finalmente, de la correspondencia de Galois, se sigue que

$$E_{\mathfrak{ge}} = (E_{\mathfrak{ge}})_m \cap k(\Lambda_N) = ((E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}})_m \cap k(\Lambda_N) = (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}.$$

□

El recíproco de la Proposición 4.10 no es cierto en general, es decir, si $E_{\mathfrak{ge}} = (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$, entonces la igualdad $K_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$ puede fallar.

Ejemplo 4.11. *Consideremos los campos $K_1 = k(\sqrt[\ell]{P_1})$, $K_2 = k(\sqrt[\ell]{\gamma P_2})$ y $K = K_1K_2$ tales que $P_1, P_2 \in R_T^+$ son polinomios diferentes, con ℓ primo, $\operatorname{gr} P_1 = a$, $1 \leq a < \ell$, $\operatorname{gr} P_2 = \ell - a$ y $\gamma \notin (\mathbb{F}_q^*)^\ell$. Entonces tenemos $E_i = k(\sqrt[\ell]{(P_i)^*})$, $i = 1, 2$ y $E = E_1E_2$. Si χ_{P_i} es el grupo de caracteres de Dirichlet asociado al campo E_i, $i = 1, 2$, por el Teorema de Leopoldt ([25, Proposición 14.4.1]) tenemos $E_i = (E_i)_{\mathfrak{ge}}$, $i = 1, 2$ y $E_{\mathfrak{ge}} = E_1E_2 = E$. Por lo tanto $E_{\mathfrak{ge}} = E = E_1E_2 = (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$.*
Ahora, ya que $\mathcal{P}_\infty$ es ramificado en K_i/k, $i = 1, 2$, tenemos que $\mathcal{P}_\infty$ es de grado 1 en K_i y $(K_i)_{\mathfrak{ge}} = K_i$. Por otro lado, por el Lema de Abhyankar, la ramificación de $\mathcal{P}_\infty$ en K/k es igual a $\operatorname{mcm}[e_\infty(K_1/k), e_\infty(K_2/k)] = \ell$. Como $k(\sqrt[\ell]{\gamma P_1P_2}) \subseteq K$, con $\operatorname{gr} P_1P_2 = \operatorname{gr} P_1 + \operatorname{gr} P_2 = \ell$, luego, $\ell \mid \operatorname{gr} P_1P_2$ y $\gamma \notin (\mathbb{F}_q^*)^\ell$, $f_\infty(K/k) = \ell$. También, tenemos que $[K : k] = \ell^2 = f_\infty(K/k)e_\infty(K/k)$. Se sigue que $h_\infty(K/k) = 1$ y $\operatorname{gr}(S_\infty(K)) = f_\infty(K/k) = \ell$. Así $[K\mathbb{F}_{q^\ell} : K] = \ell$ y $K \subsetneq K\mathbb{F}_{q^\ell} \subseteq K_{\mathfrak{ge}}$, es decir, $K_{\mathfrak{ge}} \neq K = K_1K_2 = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$.

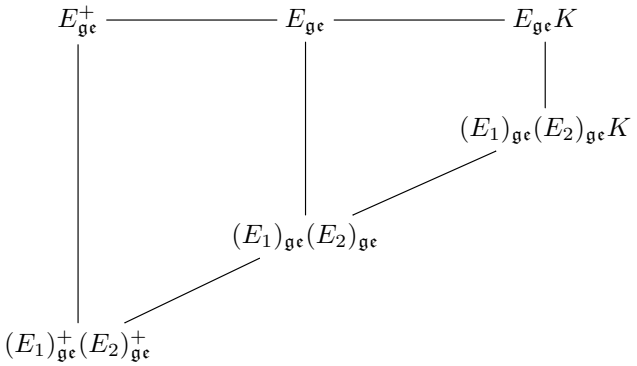
El resultado principal de esta sección es el siguiente teorema.

Demostración. Tenemos que $K_1, K_2 \subseteq {}_nk(\Lambda_N)_m$ para algunos $m \in \mathbb{N}$, $n \in \mathbb{N} \cup \{0\}$ y $N \in R_T$. Sea $K = K_1K_2 \subseteq {}_nk(\Lambda_N)_m$. Sean $E_i = {}_n(K_i)_m \cap k(\Lambda_N)$, $i = 1, 2$ y $E = {}_nK_m \cap k(\Lambda_N)$. Entonces $E = E_1E_2$. Ahora, ya que $E^+_{\mathfrak{gex}} \cap E_{\mathfrak{ge}} = E_{\mathfrak{gex}} \cap k(\Lambda_N)^+ \cap E_{\mathfrak{ge}} = E_{\mathfrak{gex}} \cap E^+_{\mathfrak{ge}} = E^+_{\mathfrak{ge}}$, tenemos el siguiente cuando de Galois.

$$\begin{array}{ccc} E^+_{\mathfrak{gex}} & \text{——} & E^+_{\mathfrak{gex}}E_{\mathfrak{ge}} \\ | & & | \\ E^+_{\mathfrak{ge}} & \text{———} & E_{\mathfrak{ge}} \end{array}$$

De [7, Theorem 2.1] tenemos que $E_{\mathfrak{ge}} = E^+_{\mathfrak{gex}}E$, entonces, por la correspondencia de Galois, tenemos que $E^+_{\mathfrak{ge}} = E^+_{\mathfrak{gex}}$. Similarmente tenemos que $(E_i)^+_{\mathfrak{ge}} = (E_i)^+_{\mathfrak{gex}}$, $i =$

$1,2$. Luego $[E^+_{\mathfrak{ge}_\mathfrak{x}} : (E_1)^+_{\mathfrak{ge}_\mathfrak{x}}(E_2)^+_{\mathfrak{ge}_\mathfrak{x}}] \,|\, q-1$. En particular $[E^+_{\mathfrak{ge}} : (E_1)^+_{\mathfrak{ge}}(E_2)^+_{\mathfrak{ge}}] = [E^+_{\mathfrak{ge}_\mathfrak{x}} : (E_1)^+_{\mathfrak{ge}_\mathfrak{x}}(E_2)^+_{\mathfrak{ge}_\mathfrak{x}}] \,|\, q-1$. Finalmente, obtenemos el siguiente diagrama.



Se sigue que

$$[E_{\mathfrak{ge}}K : (E_1)_{\mathfrak{ge}}(E_1)_{\mathfrak{ge}}K] \,|\, [E_{\mathfrak{ge}} : (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}] \,|\, [E^+_{\mathfrak{ge}} : (E_1)^+_{\mathfrak{ge}}(E_2)^+_{\mathfrak{ge}}].$$

Por lo tanto $[E_{\mathfrak{ge}}K : (E_1)_{\mathfrak{ge}}(E_1)_{\mathfrak{ge}}K] \,|\, q-1$.

Por otra parte, de [7, Theorem 2.2] tenemos que la extensiones $(E_i)_{\mathfrak{ge}}K_i/(K_i)_{\mathfrak{ge}}$, $i = 1,2$, son extensiones de constantes de orden $|H_i| \,|\, q-1$, $i = 1,2$, en donde H_i es el grupo de descomposición de $S_\infty(K_i)$ en $(E_i)_{\mathfrak{ge}}K_i$, $i = 1,2$. También, si $t_i := \operatorname{gr} S_\infty(K_i)$, entonces $(E_i)_{\mathfrak{ge}}K_i = (K_i)_{\mathfrak{ge}}\mathbb{F}_{q^{t_i|H_i|}}$, $i = 1,2$. Se sigue que

$$\begin{aligned}
(E_1)_{\mathfrak{ge}}K_1(E_2)_{\mathfrak{ge}}K_2 &= (K_1)_{\mathfrak{ge}}\mathbb{F}_{q^{t_1|H_1|}}(K_2)_{\mathfrak{ge}}\mathbb{F}_{q^{t_2|H_2|}} \\
&= (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}\mathbb{F}_{q^{\operatorname{mcm}[t_1|H_1|,t_2|H_2|]}} \\
&\subseteq (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}\mathbb{F}_{q^{\operatorname{mcm}[t_1(q-1),t_2(q-1)]}} \\
&= (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}\mathbb{F}_{q^{\operatorname{mcm}[t_1,t_2](q-1)}}.
\end{aligned}$$

Así $\mathbb{F}_{q^{\operatorname{mcm}[t_1,t_2]}} \subseteq (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$, es decir, el campo $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}\mathbb{F}_{q^{\operatorname{mcm}[t_1,t_2](q-1)}}$ es una extensión de campos de constantes de $(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$ de grado a lo más $q-1$. Entonces tenemos que

$$(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} \subseteq (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}K \subseteq (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}\mathbb{F}_{q^{\operatorname{mcm}[t_1,t_2](q-1)}}.$$

Por lo tanto, $(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}K/(K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$ es una extensión de campos de constantes de grado a lo más $(q-1)$. Finalmente, tenemos

$$[E_{\mathfrak{ge}}K : (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}K] \,|\, [E_{\mathfrak{ge}} : (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}] \,|\, q-1.$$

Por lo tanto

$$[K_{\mathfrak{ge}} : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}] \,|\, [E_{\mathfrak{ge}}K : (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}K][(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}K : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}] \,|\, (q-1)^2.$$

Entonces

$$[K_{\mathfrak{ge}} : (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}] \leq (q-1)^2$$

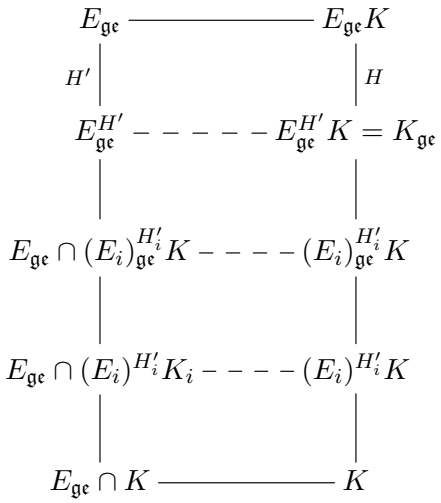
□

Sean H, H_1 y H_2, los grupos de descomposición de $\mathcal{P}_\infty$ en $E_{\mathfrak{ge}}K/K$, $(E_1)_{\mathfrak{ge}}K_1/K_1$ y $(E_2)_{\mathfrak{ge}}K_2/K_2$ respectivamente y sean $H' := H|_{E_{\mathfrak{ge}}}$, $H'_i := H_i|_{(E_i)_{\mathfrak{ge}}}$, $i = 1, 2$.

Proposición 4.12. *Con la notación anterior, tenemos que*

$$(E_1)_{\mathfrak{ge}}^{H'_1}(E_2)_{\mathfrak{ge}}^{H'_2} \subseteq E_{\mathfrak{ge}}^{H'}.$$

Demostración. Ya que $K = K_1K_2$, tenemos $(K_i)_{\mathfrak{ge}} \subseteq K_{\mathfrak{ge}}$, $i = 1, 2$. Como $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H'}K$ y $(K_i)_{\mathfrak{ge}} = (E_i)_{\mathfrak{ge}}^{H'_i}K_i$, $i = 1, 2$, se sigue que $(E_i)_{\mathfrak{ge}}^{H'_i}K \subseteq E_{\mathfrak{ge}}^{H'}K$, $i = 1, 2$. Ahora, puesto que $E_i \subseteq (E_i)_{\mathfrak{ge}}$ por correspondencia de Galois se sigue que $E_i^{H'_i} \subseteq (E_i)_{\mathfrak{ge}}^{H'_i}$, $i = 1, 2$. Por tanto $E_i^{H'_i}K \subseteq (E_i)_{\mathfrak{ge}}^{H'_i}K \subseteq E_{\mathfrak{ge}}^{H'}K$. Así, obtenemos el siguiente cuadro de Galois.



De la correspondencia de Galois, obtenemos que $E_{\mathfrak{ge}} \cap (E_i)^{H'_i}K \subseteq E_{\mathfrak{ge}} \cap (E_i)^{H'_i}K \subseteq E_{\mathfrak{ge}} \cap (E_i)_{\mathfrak{ge}}^{H'_i}K \subseteq E_{\mathfrak{ge}} \cap K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H'}$ y $(E_i)_{\mathfrak{ge}}^{H'_i} \subseteq E_{\mathfrak{ge}} \cap (E_i)_{\mathfrak{ge}}^{H'_i}K$. Por lo tanto $(E_i)_{\mathfrak{ge}}^{H'_i} \subseteq E_{\mathfrak{ge}}^{H'}$, $i = 1, 2$. □

Teorema 4.13. *Con la notación de antes, tenemos que* $|H| \,|\, \mathrm{mcm}[|H_1|, |H_2|]$.

Demostración. Tenemos que $\mathcal{P}_\infty$ es totalmente ramificado en la extensión $E_{\mathfrak{ge}}/E_{\mathfrak{ge}}^{H'}$ y $\mathcal{P}_\infty$ es totalmente descompuesto en $E_{\mathfrak{ge}}/(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$ ya que

$$E = E_1E_2 \subseteq (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}} \subseteq E_{\mathfrak{ge}}.$$

Se sigue que $E_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H'}(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$, ya que si $L := E_{\mathfrak{ge}}^{H'}(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$, en la extensión $E_{\mathfrak{ge}}/L$, $\mathcal{P}_\infty$ es totalmente ramificado y totalmente descompuesto a la vez.

Ahora, $(E_1)_{\mathfrak{ge}}/(E_1)_{\mathfrak{ge}}^{H_1'}$ es totalmente ramificada en $\mathcal{P}_\infty$ con índice de ramificación $|H_1'|$, tal que

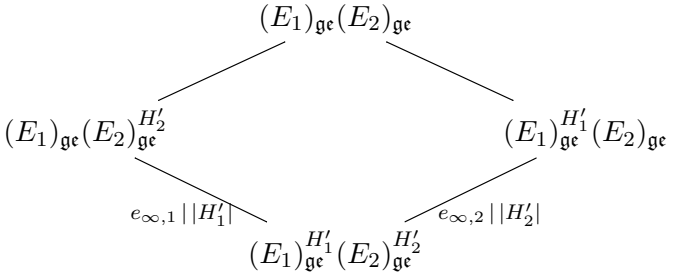
$$e_\infty((E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}/(E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}}) \,|\, |H_1'|$$

$$\begin{array}{ccc} (E_1)_{\mathfrak{ge}} & \text{——} & (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}^{H_2'} \\ {\scriptstyle |H_1'|}\Big| & & \Big|{\scriptstyle e_{\infty,1}\,|\,|H_1'|} \\ (E_1)_{\mathfrak{ge}}^{H_1'} & \text{——} & (E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}}^{H_2'} \end{array}$$

Similarmente $e_\infty((E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}/(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}^{H_2'}) \,|\, |H_2'| \,|\, e_\infty((E_2)_{\mathfrak{ge}}/(E_2)_{\mathfrak{ge}}^{H_2'}) = [(E_2)_{\mathfrak{ge}} : (E_2)_{\mathfrak{ge}}^{H_2'}]$

$$\begin{array}{ccc} (E_2)_{\mathfrak{ge}} & \text{——} & (E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}} \\ {\scriptstyle |H_2'|}\Big| & & \Big|{\scriptstyle e_{\infty,2}\,|\,|H_2'|} \\ (E_2)_{\mathfrak{ge}}^{H_2'} & \text{——} & (E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}}^{H_2'} \end{array}$$

Tenemos $(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}} = ((E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}^{H_2'})((E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}})$ y el siguiente diagrama



Por el Lema de Abhyankar

$$e_\infty((E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}/(E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}}^{H_2'}) = e_0 := \operatorname{mcm}[e_{\infty,1}, e_{\infty,2}] \,|\, \operatorname{mcm}[|H_1'|, |H_2'|].$$

Finalmente, $\mathcal{P}_\infty$ es totalmente ramificado en $E_{\mathfrak{ge}}/E_{\mathfrak{ge}}^{H'}$ y totalmente descompuesto en $E_{\mathfrak{ge}}/(E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}$.

$$\begin{array}{ccc} E_{\mathfrak{ge}}^{H'} & \overset{|H'|}{\text{——————}} & E_{\mathfrak{ge}} \\ \Big| & & \Big|{\scriptstyle \mathcal{P}_\infty \text{ totalmente descompuesto}} \\ (E_1)_{\mathfrak{ge}}^{H_1'}(E_2)_{\mathfrak{ge}}^{H_2'} & \underset{e_0}{\text{——}} & (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}} \end{array}$$

Luego $|H'|\,|\,[E_{\mathfrak{ge}} : (E_1)_{\mathfrak{ge}}(E_2)_{\mathfrak{ge}}]\,e_0$. Así $|H'|\,|\,e_0$ y $e_0\,|\,\mathrm{mcm}[|H_1'|, |H_2'|]$. Por lo tanto

$$|H'|\,|\,\mathrm{mcm}[|H_1'|, |H_2'|].$$

□

Teorema 4.14. *Sean* $K_1, K_2 \subseteq {}_nk(\Lambda_N)_m$, $K = K_1K_2$, $F := {}_nK \cap k(\Lambda_N)_m$ *y* $F_i := {}_nK_i \cap k(\Lambda_N)_m$, $i = 1, 2$. *Entonces*

$$K_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} \textit{ si y sólo si } F_{\mathfrak{ge}} = (F_1)_{\mathfrak{ge}}(F_2)_{\mathfrak{ge}}$$

Demostración. Como $K = K_1K_2$, tenemos ${}_nK = {}_n(K_1K_2) = {}_nK_1{}_nK_2$. De la correspondencia de Galois se sigue que $F = F_1F_2$.

De [20, Theorem 4.4] tenemos que $K_{\mathfrak{ge}} = MF_{\mathfrak{ge}}$ con $M := Kk(\Lambda_N)_m \cap L_n$ y $M \cap F_{\mathfrak{ge}} = k$ pues $\mathcal{P}_\infty$ es moderadamente ramificado en $F_{\mathfrak{ge}}/k$ y salvajemente ramificado en M/k. Entonces $K_{\mathfrak{ge}} = MF_{\mathfrak{ge}}$ y $(K_i)_{\mathfrak{ge}} = M_i(F_i)_{\mathfrak{ge}}$, $M_i := K_ik(\Lambda_N)_m \cap L_n$, $i = 1, 2$. Por tanto $[K_{\mathfrak{ge}} : M] = [F_{\mathfrak{ge}} : k]$. Luego, por la correspondencia de Galois $F_{\mathfrak{ge}} = K_{\mathfrak{ge}} \cap k(\Lambda_N)_m$.

Primero, supongamos que $K_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}$. Entonces

$$MF_{\mathfrak{ge}} = K_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}} = M_1(F_1)_{\mathfrak{ge}}M_2(F_2)_{\mathfrak{ge}} = M_1M_2((F_1)_{\mathfrak{ge}}(F_2)_{\mathfrak{ge}}).$$

En particular $Mk(\Lambda_N)_m = M_1k(\Lambda_N)_mM_2k(\Lambda_N)_m = M_1M_2k(\Lambda_N)_m$. Por tanto, por la correspondencia de Galois $M = M_1M_2$. Así

$$MF_{\mathfrak{ge}} = M_1M_2((F_1)_{\mathfrak{ge}}(F_2)_{\mathfrak{ge}}) = M((F_1)_{\mathfrak{ge}}(F_2)_{\mathfrak{ge}}).$$

Entonces, por correspondencia de Galois, se sigue que $F_{\mathfrak{ge}} = (F_1)_{\mathfrak{ge}}(F_2)_{\mathfrak{ge}}$.

Por el contrario, supongamos que $F_{\mathfrak{ge}} = (F_1)_{\mathfrak{ge}}(F_2)_{\mathfrak{ge}}$. Entonces

$$K_{\mathfrak{ge}} = MF_{\mathfrak{ge}} = M(F_1)_{\mathfrak{ge}}M(F_2)_{\mathfrak{ge}} = (K_1)_{\mathfrak{ge}}(K_2)_{\mathfrak{ge}}.$$

□

Capítulo 5

Campo de géneros de extensiones cíclicas de Kummer de grado ℓ^n

El teorema principal de este capítulo, Teorema 5.5, bajo el enfoque de los caracteres de Dirichlet, generaliza el resultado obtenido por G. Peng [23]. En dicho resultado, determinamos de forma explícita el campo de géneros para extensiones cíclicas de Kummer de grado potencia de un número primo. Este trabajo, resuelve por completo las ideas expuestas en [5], donde bajo restricciones, se obtuvo para un caso particular el campo de géneros para estas extensiones.

Sea ℓ un número primo tal que $\ell^n \mid q-1$. Sea $D \in R_T$, $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ con $P_1, ..., P_r \in R_T^+$ diferentes, $r \geq 1$, $\alpha_1, ..., \alpha_r \in \mathbb{N}$ y $1 \leq \alpha_j \leq \ell^n - 1$, $1 \leq j \leq r$. Sea $E := k(\sqrt[\ell^n]{(-1)^{\operatorname{gr} D} D})$. Tenemos que $E \subseteq k(\Lambda_D)$ [25, Corolario 9.5.12]. Denotamos por $D^* = (-1)^{\operatorname{gr} D} D$, luego

$$k(\sqrt[\ell^n]{(-1)^{\operatorname{gr} D} D}) = k(\sqrt[\ell^n]{D^*}).$$

Notemos que si $\ell^n \mid \operatorname{gr} D$, entonces $k = k(\sqrt[\ell^n]{(-1)^{\operatorname{gr} D}})$ y por lo tanto $k(\sqrt[\ell^n]{D^*}) = k(\sqrt[\ell^n]{D})$.

Sea $\alpha_j = b_j \ell^{a_j}$ con $\operatorname{mcd}(b_j, \ell) = 1$ y $\operatorname{gr} P_j = c_j \ell^{d_j}$ con $\operatorname{mcd}(c_j, \ell) = 1$, $1 \leq j \leq r$. Para cada $1 \leq j \leq r$, definimos $E_j := k(\sqrt[\ell^n]{(P_j^{\alpha_j})^*})$. Tenemos que $E_j \subseteq k(\Lambda_{P_j})$, $1 \leq j \leq r$. Notemos que $\sqrt[\ell^n]{(-1)^{\operatorname{gr} P_j^{\alpha_j}} P^{\alpha_j}} = \sqrt[\ell^n]{(-1)^{b_j \ell^{a_j} \operatorname{gr} P_j} P_j^{b_j \ell^{a_j}}} = \sqrt[\ell^{n-a_j}]{(-1)^{\operatorname{gr} P_j^{b_j}} P_j^{b_j}}$. Además $\sqrt[\ell^{n-a_j}]{(-1)^{\operatorname{gr} P_j^{b_j}} P_j^{b_j}} = (\sqrt[\ell^{n-a_j}]{(-1)^{\operatorname{gr} P_j} P_j})^{b_j} \in k(\sqrt[\ell^{n-a_j}]{(-1)^{\operatorname{gr} P_j} P_j})$. Tenemos que $P_j^{b_j}$ es libre de ℓ-potencias y así P_j es completamente ramificado en

$$k(\sqrt[\ell^{n-a_j}]{(-1)^{\operatorname{gr} P_j^{b_j}} P_j^{b_j}})/k.$$

Por lo tanto

$$[k(\sqrt[\ell^{n-a_j}]{(-1)^{b_j \operatorname{gr} P_j} P_j^{b_j}}) : k] = \operatorname{gr}(X^{\ell^{n-a_j}} - (-1)^{b_j \operatorname{gr} P_j} P_j^{b_j}) \\ = \operatorname{gr}(X^{\ell^{n-a_j}} - (-1)^{\operatorname{gr} P_j} P_j) = [k(\sqrt[\ell^{n-a_j}]{(-1)^{\operatorname{gr} P_j} P_j}) : k].$$

Se sigue que $E_j = k(\sqrt[\ell^{n-a_j}]{P_j^*})$.

Definamos $\mathcal{M} := E_1 \cdots E_r$. Tenemos que $\mathcal{M}/k$ es la máxima extensión no ramificada de E en todo primo finito contenida en un campo de funciones ciclotómico [20, Proposition 3.3], esto es, $\mathcal{M} = E_{\mathfrak{ge}}$. En particular $E_{\mathfrak{g}} \subseteq \mathcal{M}$. Tenemos que $\mathcal{P}_\infty$ es completamente ramificado en $\mathcal{M}/E_{\mathfrak{g}}$. El campo $\mathcal{M}$ es conocido como el *campo de géneros extendido* de E. Por el Lema de Abhyankar [27, Theorem 12.4.4], tenemos que

$$e_\infty(E_{\mathfrak{ge}}/k) = \operatorname{mcm}[e_\infty(E_j/k) \mid 1 \le j \le r] =: \ell^m.$$

Como $\mathcal{P}_\infty$ es no ramificado en la extensión $E_{\mathfrak{g}}/E$, es decir, $e_\infty(E_{\mathfrak{g}}/E) = 1$, tenemos en general

$$[E_{\mathfrak{ge}} : E_{\mathfrak{g}}] = e_\infty(E_{\mathfrak{ge}}/E_{\mathfrak{g}}) e_\infty(E_{\mathfrak{g}}/E) = e_\infty(E_{\mathfrak{ge}}/E).$$

Sean $P \in R_T$ y $F := k(\sqrt[\ell^n]{(P^\alpha)^*})$ con $\alpha = b\ell^a$, $\operatorname{mcd}(b, \ell) = 1$. Denotaremos por $e_P(F/k)$ el índice de ramificación del polinomio P en la extensión $k(\sqrt[\ell^n]{(P^\alpha)^*})/k$. Por $e_\infty(E/k)$ denotaremos el índice de ramificación del primo infinito $\mathcal{P}_\infty$, en la extensión $k(\sqrt[\ell^n]{(P^\alpha)^*})/k$.

Tenemos la siguiente proposición.

Proposición 5.1. *Sean $P \in R_T$ y $k(\sqrt[\ell^n]{(P^\alpha)^*}) = k(\sqrt[\ell^{n-a}]{P^*})$. Entonces*

$$e_P(k(\sqrt[\ell^n]{(P^\alpha)^*})/k) = \frac{\ell^n}{\operatorname{mcd}(\alpha, \ell^n)} = \ell^{n-a} \quad \text{y}$$
$$e_\infty(k(\sqrt[\ell^n]{(P^\alpha)^*})/k) = \frac{\ell^n}{\operatorname{mcd}(\ell^n, \operatorname{gr} P^\alpha)} = \frac{\ell^{n-a}}{\operatorname{mcd}(\ell^{n-a}, \operatorname{gr} P)}.$$

Demostración. Ver [22, Subsección 5.2] o [25, Teorema 10.3.1]. □

Sea $\operatorname{gr} P = c\ell^d$ con $\operatorname{mcd}(c, \ell) = 1$. Entonces $\operatorname{mcd}(\ell^{n-a}, \operatorname{gr} P) = \ell^{\min\{n-a,d\}}$. De la Proposición 5.1 se sigue que

$$e_\infty(k(\sqrt[\ell^{n-a}]{P^*})/k) = \ell^{n-a-\min\{n-a,d\}}.$$

Así

$$e_\infty(E_j/k) = \ell^{n-a_j-\min\{n-a_j,d_j\}} \mid \ell^m = e_\infty(E_{\mathfrak{ge}}/k),\ 1 \le j \le r.$$

5.1. Caso ciclotómico ℓ^n

Vamos a iniciar con la siguiente proposición que marca los límites del tipo de ramificación en las ℓ^n-extensiones de Kummer.

Proposición 5.2. *Sean $P, Q \in R_T^+$ y los campos $J := k(\sqrt[\ell^n]{(P^\alpha)^*})$ y $F := k(\sqrt[\ell^n]{(Q^\beta)^*})$. Supongamos que $e_P(J/k) \leq e_Q(F/k)$ y $e_\infty(F/k) \leq e_\infty(J/k)$ con $1 < e_\infty(J/k)$. Entonces $\nu_\ell(\operatorname{gr} P) \leq \nu_\ell(\operatorname{gr} Q)$.*

Demostración. Ya que $e_P(J/k) \leq e_Q(F/k)$, tenemos que $1 \leq \frac{e_Q(F/k)}{e_P(J/k)}$. Por otro lado, de $e_\infty(F/k) \leq e_\infty(J/k)$ obtenemos que

$$\frac{e_Q(F/k)}{\operatorname{mcd}(\operatorname{gr} Q, e_Q(F/k))} = e_\infty(F/k) \leq e_\infty(J/k) = \frac{e_P(J/k)}{\operatorname{mcd}(\operatorname{gr} P, e_P(J/k))}.$$

Como $e_\infty(J/k) \neq 1$, se sigue que $\nu_\ell(\operatorname{gr} P) < e_P(J/k)$, y $\operatorname{mcd}(\operatorname{gr} P, e_P(J/k)) = l^{\nu_\ell(\operatorname{gr} P)}$. Además, ya que $\operatorname{mcd}(\operatorname{gr} Q, e_Q(F/k)) \mid \operatorname{gr} Q$, obtenemos

$$\frac{e_Q(F/k)}{l^{\nu_\ell(\operatorname{gr} Q)}} \leq \frac{e_Q(F/k)}{\operatorname{mcd}(\operatorname{gr} Q, e_Q(F/k))} \leq \frac{e_P(J/k)}{\operatorname{mcd}(\operatorname{gr} P, e_P(J/k))} = \frac{e_P(J/k)}{l^{\nu_\ell(\operatorname{gr} P)}}.$$

Por lo tanto

$$1 \leq \frac{e_Q(F/k)}{e_P(J/k)} \leq l^{\nu_\ell(\operatorname{gr} Q) - \nu_\ell(\operatorname{gr} P)}.$$

Entonces $0 \leq \nu_\ell(\operatorname{gr} Q) - \nu_\ell(\operatorname{gr} P)$, es decir, $\nu_\ell(\operatorname{gr} P) \leq \nu_\ell(\operatorname{gr} Q)$. □

El resultado principal para el caso de las ℓ^n-extensiones cíclicas de Kummer es el siguiente teorema.

Teorema 5.3. *Sea $E = k(\sqrt[\ell^n]{D^*})$, con $\ell^n \mid q-1$, $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, $1 \leq \alpha_j \leq \ell^n - 1$ y $\alpha_j = b_j \ell^{a_j}$ con $\operatorname{mcd}(b_j, \ell) = 1$, $1 \leq j \leq r$, $P_1, ..., P_r \in R_T^+$ diferentes tal que $\operatorname{gr} P_j = c_j \ell^{d_j}$ para $\operatorname{mcd}(c_j, \ell) = 1$, $1 \leq j \leq r$. Ordenamos los polinomios $P_1, ..., P_r$ de tal forma que $0 = a_1 \leq \cdots \leq a_r \leq n-1$.*

Sea $E_{\mathfrak{ger}} := E_1 \cdots E_r$ con $E_j = k(\sqrt[\ell^{n-a_j}]{P_j^*})$, $1 \leq j \leq r$. Sean

$$e_\infty(E/k) = \ell^t \text{ con } \ t = n - \min\{n, \nu_\ell(\operatorname{gr} D)\},$$

$$e_\infty(E_{\mathfrak{ger}}/k) = \ell^m \text{ con } \ m = \max\{n - a_j - \min\{n - a_j, d_j\} \mid 1 \leq j \leq r\}.$$

Sea i_0, $1 \leq i_0 \leq r$, tal que $n - a_{i_0} - \min\{n - a_{i_0}, d_{i_0}\} = m$ y $n - a_j - d_j < m$ para $j > i_0$. Para $m > 0$ tenemos $\operatorname{mcd}(\operatorname{gr} P_{i_0}, \ell^n) = \ell^{d_{i_0}}$, y por tanto existen $a, b \in \mathbb{Z}$ tal que $a \operatorname{gr} P_{i_0} + b\ell^n = \ell^{d_{i_0}}$. Para $j < i_0$, tenemos que $d_{i_0} \leq d_j$. Sea $z_j := -ac_j \ell^{d_j - d_{i_0}}$. Para

$j > i_0$, sea $y_j \equiv -c_j c_{i_0}^{-1} \mod \ell^n \in \mathbb{Z}$.

Entonces

$$E_{\mathfrak{ge}} = F_1 \cdots F_r,$$

donde $F_j = E_j$ con $1 \leq j \leq r$ si $m = t$, es decir, $E_{\mathfrak{ge}} = E_{\mathfrak{ger}}$, y si $m > t \geq 0$, entonces

$$F_j := \begin{cases} k\left(\sqrt[\ell^{n-a_j}]{P_j P_{i_0}^{z_j}}\right) & \text{si } j < i_0, \\ k\left(\sqrt[\ell^{d_{i_0}+t}]{P_{i_0}^*}\right) & \text{si } j = i_0, \\ k\left(\sqrt[\ell^{n-a_j}]{P_j P_{i_0}^{y_j \ell^{d_j - d_{i_0}}}}\right) & \text{si } j > i_0 \text{ y } d_j \geq d_{i_0}, \\ k\left(\sqrt[\ell^{n-a_j+d_{i_0}-d_j}]{P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j}}\right) & \text{si } j > i_0 \text{ y } d_{i_0} > d_j. \end{cases} \tag{5.1}$$

Demostración. Primero supongamos que $m = t$. Entonces

$$[E_{\mathfrak{ger}} : E_{\mathfrak{ge}}] = e_\infty(E_{\mathfrak{ger}}/E_{\mathfrak{ge}}) = \frac{e_\infty(E_{\mathfrak{ger}}/k)}{e_\infty(E/k)} = \ell^{m-t} = 1.$$

Por lo tanto

$$E_{\mathfrak{ger}} = E_{\mathfrak{ge}}.$$

Ahora, supongamos que $m > t$. Sea i_0 como antes. De (5.1) tenemos

$$e_\infty\left(k\left(\sqrt[\ell^{n-a_{i_0}}]{P_{i_0}^*}\right)/k\right) = \frac{\ell^{n-a_{i_0}}}{\operatorname{mcd}(\operatorname{gr} P_{i_0}, \ell^{n-a_{i_0}})} = \ell^{n-a_{i_0}-\min\{d_{i_0}, n-a_{i_0}\}} = \ell^m \neq 1.$$

Por lo tanto, $\operatorname{mcd}(\operatorname{gr} P_{i_0}, \ell^{n-a_{i_0}}) = \ell^{d_{i_0}}$, luego $n - a_{i_0} - \min\{n-a_{i_0}, d_{i_0}\} = n - a_{i_0} - d_{i_0} = m > t \geq 0$.

Ya que $\operatorname{mcd}(\operatorname{gr} P_{i_0}, \ell^n) = \ell^{d_{i_0}}$, existen $a, b \in \mathbb{Z}$, tales que

$$a \operatorname{gr} P_{i_0} + b\ell^n = \ell^{d_{i_0}}. \tag{5.2}$$

En particular $ac_{i_0} + b\ell^{n-d_{i_0}} = 1$ y por tanto $\operatorname{mcd}(a, \ell) = 1$. Por la Proposición 5.2 para $1 \leq j \leq i_0 - 1$ se tiene que $\ell^{d_{i_0}} = \nu_\ell(\operatorname{gr} P_{i_0}) \leq \nu_\ell(\operatorname{gr} P_{i_0})$, luego $\ell^{d_{i_0}} \mid \operatorname{gr} P_j$, entonces de (5.2) al multiplicar por $\operatorname{gr} P_j$ obtenemos que

$$\operatorname{gr} P_j + \left(-a\frac{\operatorname{gr} P_j}{\ell^{d_{i_0}}}\right) \operatorname{gr} P_{i_0} = \operatorname{gr} P_j + (-ac_j \ell^{d_j - d_{i_0}}) \operatorname{gr} P_{i_0} = (b \operatorname{gr} P_j)\ell^{n-d_{i_0}}.$$

Observemos que $-a\frac{\operatorname{gr} P_j}{\ell^{d_{i_0}}} \in \mathbb{Z}$ con $\operatorname{mcd}(a, \ell) = 1$. Para $1 \leq j \leq i_0 - 1$, definamos $Q_j := P_j P_{i_0}^{z_j}$. Puesto que para $1 \leq j \leq i_0 - 1$, $d_j \geq d_{i_0}$, por construcción tenemos

que $\ell^n \mid \operatorname{gr} P_j + z_j \operatorname{gr} P_{i_0} = \operatorname{gr} Q_j$. Por tanto, $\mathcal{P}_\infty$ es no ramificado en $k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)/k$, es decir,

$$e_\infty\left(k\left(\sqrt[\ell^{n-a_{i_0}}]{P_{i_0}^*}\right)/k\right) = \frac{\ell^{n-a_{i_0}}}{\operatorname{mcd}(\operatorname{gr} P_{i_0}, \ell^{n-a_{i_0}})} = \ell^{n-a_{i_0}-\min\{d_{i_0}, n-a_{i_0}\}} = \ell^m \neq 1.$$

$e_\infty\left(k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)/k\right) = 1$, (Proposición 5.1). Además, para $j < i_0$, tenemos

$$\begin{aligned} e_{P_j}\left(k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)/k\right) &= \ell^{n-a_j}, \\ e_{P_{i_0}}\left(k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)/k\right) &= \frac{\ell^{n-a_j}}{\operatorname{mcd}(z_j, \ell^{n-a_j})} = \ell^{n-a_j-\min\{n-a_j, d_j-d_{i_0}\}}. \end{aligned} \tag{5.3}$$

Ahora $d_j - d_{i_0} \geq \min\{n-a_j, d_j-d_{i_0}\}$ de modo que $n-a_j-\min\{n-a_j, d_j-d_{i_0}\} \leq n-a_j-d_j+d_{i_0} \leq n-a_{i_0}-d_{i_0}+d_{i_0} = n-a_{i_0}$ pues $e_\infty(E_j/k) = \ell^{n-a_j-d_j} \mid e_\infty(E_{i_0}/k) = \ell^{n-a_{i_0}-d_{i_0}}$. Por tanto

$$e_{P_{i_0}}\left(k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)/k\right) \leq \ell^{n-a_{i_0}}. \tag{5.4}$$

Ahora consideremos $j > i_0$. Tenemos dos posibilidades: $d_{i_0} \leq d_j$ o $d_{i_0} > d_j$.

En general, deseamos poder definir un polinomio $Q_j = P_j^{\alpha_j} P_{i_0}^{\beta_j}$, $\operatorname{mcd}(\alpha_j, \beta_j) = 1$ de tal forma que

$$e_\infty\left(k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)/k\right) \leq \ell^t.$$

Esto es,

$$\begin{aligned} \operatorname{gr} Q_j &= \alpha_j \operatorname{gr} P_j + \beta_j \operatorname{gr} P_{i_0} \\ &= \alpha_j c_j \ell^{d_j} + \beta_j c_{i_0} \ell^{d_{i_0}} = A\ell^B, \text{ con } \operatorname{mcd}(Ac_jc_{i_0}, \ell) = 1, \end{aligned}$$

de manera que $n - a_j - \min\{n-a_j, B\} \leq t$. Es decir, necesitamos que $n-a_j-t \leq \min\{n-a_j, B\} \leq B$.

Primero supondremos que $d_{i_0} \leq d_j$. Consideremos el polinomio $Q_j = P_j P_{i_0}^{y_j \ell^\gamma}$, es decir, tomando $\alpha_j = 1$ y $\beta_j = y_j \ell^\gamma$. Tenemos que

$$\begin{aligned} \operatorname{gr} Q_j &= \operatorname{gr} P_j + \beta_j \operatorname{gr} P_{i_0} = c_j \ell^{d_j} + y_j c_{i_0} \ell^{d_{i_0}+\gamma} \\ &= \ell^{d_{i_0}}(c_j \ell^{d_j-d_{i_0}} + y_j c_{i_0} \ell^\gamma) = A\ell^B. \end{aligned}$$

Por tanto $c_j \ell^{d_j-d_{i_0}} + y_j c_{i_0} \ell^\gamma = A\ell^{B-d_{i_0}}$, $\operatorname{mcd}(A, \ell) = 1$. Ahora, queremos que γ e y_j sean tales que

$$\nu_\ell(c_j \ell^{d_j-d_{i_0}} + y_j c_{i_0} \ell^\gamma) = B - d_{i_0}.$$

Observemos que tomando $\gamma := d_j - d_{i_0}$, tenemos $\ell^{d_j-d_{i_0}}(c_j + y_j c_{i_0}) = \ell^{B-d_{i_0}}$, luego $c_j + y_j c_{i_0} = \ell^{B-d_{i_0}+d_{i_0}-d_j} = \ell^{B-d_j}$. Podemos escoger $B \geq n + d_j$, esto es equivalente a que $c_j + y_j c_{i_0} \equiv 0 \mod \ell^n$, lo cual es posible ya que $\mathrm{mcd}(c_{i_0}c_j, \ell) = 1$ con $B - d_j \geq n > 0$.

Finalmente, de $\mathrm{mcd}(c_{i_0}c_j, \ell) = 1$, elegimos $y_j \equiv -c_j c_{i_0}^{-1} \mod \ell^n \in \mathbb{Z}$. Notemos en particular que $\mathrm{mcd}(y_j, \ell) = 1$. Así, definimos $F_j := k\left(\sqrt[\ell^{n-a_j}]{Q_j}\right)$ con $Q_j := P_j P_{i_0}^{y_j \ell^{d_j-d_{i_0}}}$. Tenemos entonces $\mathrm{gr}\, Q_j = A\ell^B$ con $B \geq n$, de donde

$$e_{P_j}(F_j/k) = e_{P_j}(E_j/k) = \ell^{n-a_j}, \tag{5.5}$$

$$e_{P_{i_0}}(F_j/k) = \frac{\ell^{n-a_j}}{\mathrm{mcd}(y_j\ell^{d_j-d_{i_0}}, \ell^{n-a_j})} = \ell^{n-a_j-\min\{n-a_j, d_j-d_{i_0}\}} \leq \ell^{n-a_{i_0}} = e_{P_{i_0}}(E_{i_0}/k) \tag{5.6}$$

$$\text{y} \quad e_\infty(F_j/k) = \frac{\ell^{n-a_j}}{\mathrm{mcd}(\mathrm{gr}\, Q_j, \ell^{n-a_j})} = \ell^{n-a_j-n+a_j} = 1. \tag{5.7}$$

Ahora, supongamos que $d_j < d_{i_0}$. En este caso, si tomáramos $Q_j = P_j P_{i_0}^{y_j\ell^{d_j-d_{i_0}}}$ como antes, esto es, $\gamma = d_j - d_{i_0}$ tendríamos $\gamma < 0$, entonces $Q_j \notin R_T$, pero

$$Q_j = P_j P_{i_0}^{y_j\ell^{d_j-d_{i_0}}} = (P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j})^{\ell^{d_{i_0}-d_j}} = \sqrt[\ell^{d_{i_0}-d_j}]{P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j}},$$

con $P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j} \in R_T$. Por estas observaciones, definimos $Q'_j := P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j}$, con y_j como antes, esto es, $y_j \equiv -c_j c_{i_0}^{-1} \mod \ell^n$, $Q'_j \in R_T$. Definimos

$$F_j := k\left(\sqrt[\ell^{n-a_j+d_{i_0}-d_j}]{P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j}}\right).$$

Tenemos que

$$e_{P_j}(F_j/k) = \frac{\ell^{n-a_j+d_{i_0}-d_j}}{\mathrm{mcd}(\ell^{d_{i_0}-d_j}, \ell^{n-a_j+d_{i_0}-d_j})} = \ell^{n-a_j+d_{i_0}-d_j-d_{i_0}+d_j} = \ell^{n-a_j} = e_{P_j}(E_j/k), \tag{5.8}$$

y

$$e_{P_{i_0}}(F_j/k) = \frac{\ell^{n-a_j+d_{i_0}-d_j}}{\mathrm{mcd}(y_j, \ell^{n-a_j+d_{i_0}-d_j})} = \ell^{n-a_j+d_{i_0}-d_j}. \tag{5.9}$$

Como $n - a_j - d_j < m = n - a_{i_0} - d_{i_0}$, entonces $n - a_j - d_j + d_{i_0} < n - a_{i_0}$. Se sigue que

$$e_{P_{i_0}}(F_j/k) < \ell^{n-a_{i_0}} = e_{P_{i_0}}(E_{i_0}/k). \tag{5.10}$$

Finalmente, recordando que $B \geq n + d_j$, notemos que

$$\begin{aligned}\operatorname{gr} Q'_j &= \operatorname{gr} P_j^{\ell^{d_{i_0}-d_j}} P_{i_0}^{y_j} = \ell^{d_{i_0}-d_j} \operatorname{gr} P_j + y_j \operatorname{gr} P_{i_0} \\ &= \ell^{d_{i_0}-d_j} c_j \ell^{d_j} + y_j c_{i_0} \ell^{d_{i_0}} = \ell^{d_{i_0}} (c_j + y_j c_{i_0}) \\ &= \ell^{d_{i_0}} (A\ell^{n-d_j}) = A\ell^{n+d_{i_0}-d_j}.\end{aligned}$$

Tenemos $A\ell^{n+d_{i_0}-d_j} = A\ell^{n-d_j+d_{i_0}}$, con $\nu_\ell(A) = 0$ y $n - d_j + d_{i_0} > n$. Se sigue que

$$e_\infty(F_j/k) = \frac{\ell^{n-a_j+d_{i_0}-d_j}}{\operatorname{mcd}(A\ell^{n+d_{i_0}-d_j}, \ell^{n-a_j+d_{i_0}-d_j})} = \ell^{n-a_j+d_{i_0}-d_j-n+a_j-d_{i_0}+d_j} = 1. \quad (5.11)$$

Sea $L := F_1 \cdots F_{i_0-1} F_{i_0+1} \cdots F_r$. De (5.3) – (5.11) obtenemos que $L \subseteq E_{\mathfrak{ge}}$. Probaremos que $E_{\mathfrak{ge}} = LF_{i_0}$, con F_{i_0} como en (5.1). Considere los conjuntos

$$\mathcal{J} = \{j \in \{1, 2, ..., r\} \,|\, j > i_0,\ n - a_j - d_j > t \ \ y \ \ d_{i_0} > d_j\}$$

y $\mathcal{I} = \{1, 2, ..., r\} \setminus (\mathcal{J} \cup \{i_0\})$. Ordenamos los elementos de $\mathcal{J} = \{j_1, ..., j_s\}$ tal que $d_{i_0} - d_{j_1} \leq d_{i_0} - d_{j_2} \leq \cdots \leq d_{i_0} - d_{j_s}$. Para $j_u \in \mathcal{J}$ tenemos

$$F_{j_u} = k(\sqrt[\ell^{n-a_{j_u}+d_{i_0}-d_{j_u}}]{P_{j_u}^{\ell^{d_{i_0}-d_{j_u}}} P_{i_0}^{y_{j_u}}}).$$

Sea I_j el grupo de inercia del primo P_j en F_j/k para $1 \leq j \leq r$. Tenemos $|I_j| = e_{P_j}(F_j/k) = \ell^{n-a_j}$, $j \neq i_0$. Sea $F'_j := F_j^{I_j}$. Si $j_u \in \mathcal{J}$, de (5.9) observamos que la máxima extensión contenida en F_j no ramificada en P_j es el campo $F_j^{I_j} = k(\sqrt[\ell^{d_{i_0}-d_{j_u}}]{P_{i_0}^*})$, esto es, $F'_{j_u} = k(\sqrt[\ell^{d_{i_0}-d_{j_u}}]{P_{i_0}^*})$, $1 \leq u \leq s$, y por el orden tomado para los índices en $\mathcal{J}$, se sigue que $F'_{j_1} \subseteq F'_{j_2} \subseteq \cdots \subseteq F'_{j_s}$. Si $j \in \mathcal{I}$ tenemos que $F'_j = k$.

Antes de continuar, observemos que para F_i y F_j dados como en (5.1) con $i \neq j$, por teoría clásica de Galois ([9, Proposition 21]) tenemos que

$$\operatorname{Gal}(F_iF_j/F_i \cap F_j) \cong \operatorname{Gal}(F_i/F_i \cap F_j) \times \operatorname{Gal}(F_j/F_i \cap F_j).$$

Además, tenemos que

$$\begin{aligned}|\operatorname{Gal}(F_i/F'_i)| &= |\operatorname{Gal}(F_i/F_i^{I_i})| = |I_i| = e_{P_i}(F_i/k) = \ell^{n-a_i} \ y \\ |\operatorname{Gal}(F_j/F'_j)| &= |\operatorname{Gal}(F_j/F_j^{I_j})| = |I_j| = e_{P_j}(F_j/k) = \ell^{n-a_j}.\end{aligned}$$

Por tanto $\operatorname{Gal}(F_iF_j/F_i \cap F_j) \cong I_i \times I_j$.

Ahora, del Lema de Abhyankar [27, Theorem 12.4.4], tenemos que

$$e_{P_i}(F_iF_j/k) = \operatorname{mcm}[e_{P_i}(F_i/k), e_{P_i}(F_j/k)] = \operatorname{mcm}[e_{P_i}(F_i/k), 1] = e_{P_i}(F_i/k) = |I_i|.$$

Similarmente $e_{P_j}(F_iF_j/k) = e_{P_j}(F_j/k) = |I_j|$. Sean I_i' y I_j' el grupo de inercia de P_i, P_j en F_iF_j/k respectivamente. Entonces $I_i \times \{e\} < I_i'$ y $\{e\} \times I_j < I_j'$ son tales que $|I_i \times \{e\}| = |I_i'|$ y $|\{e\} \times I_j| = |I_j'|$. Por tanto, la máxima subextensión no ramificada en P_i y P_j de F_iF_j/k es $(F_iF_j)^{I_iI_j} = (F_iF_j)^{I_i \times I_j}$.
Además, note que para $i, j \in \mathcal{J}$, $i \neq j$, tenemos que P_i y P_j no son ramificados en $F_i \cap F_j$. En efecto, supongamos que P_j es ramificado en $F_i \cap F_j$ y como $F_i \cap F_j \subseteq F_i$, se sigue que P_j es ramificado en F_i lo cual es imposible.
Por tanto $F_i \cap F_j \subseteq F_i'$. Similarmente $F_i \cap F_j \subseteq F_j'$. Así $F_i \cap F_j \subseteq F_i' \cap F_j' \subseteq F_i \cap F_j$. Por lo tanto $F_i \cap F_j = F_i' \cap F_j'$. Si suponemos que $i < j$, entonces $F_i \cap F_j = F_i'$. Por lo tanto

$$\begin{aligned}[F_iF_j : k] &= [F_iF_j : F_i \cap F_j][F_i \cap F_j : k] = [F_iF_j : F_i'][F_i' : k] \\ &= [F_iF_j : F_j'][F_j' : F_i'][F_i' : k] = [F_iF_j : F_j][F_j : F_j'][F_j' : k] \\ &= [F_i : F_i'][F_j : F_j'][F_j' : k].\end{aligned}$$

Enumeremos los elementos de $\mathcal{I}$ como $\mathcal{I} = \{i_1, ..., i_{s'}\}$. Probaremos que para los campos F_{i_w}, con $i_w \in \mathcal{I}$, para $1 \leq w \leq s'$ satisfacen

a.1.- $F_{i_1} \cdots F_{i_{w-1}} \cap F_{i_w} = k$,

b.1.- $I_{i_1} \cdots I_{i_w} \cong I_{i_1} \times \cdots \times I_{i_w}$,

c.1.- $[F_{i_1} \cdots F_{i_w} : k] = \prod_{j=1}^{w} [F_{i_j} : k] = \prod_{j=1}^{w} \ell^{n-a_{i_j}}$,

d.1.- $(F_{i_1} \cdots F_{i_w})^{I_{i_1} \cdots I_{i_w}} = k$.

Similarmente, los campos F_{j_w}, $1 \leq w \leq s$, con $j_w \in \mathcal{J}$, satisfacen

a.2.- $F_{j_1} \cdots F_{j_{w-1}} \cap F_{j_w} = F'_{j_{w-1}}$,

b.2.- $I_{j_1} \cdots I_{j_w} \cong I_{j_1} \times \cdots \times I_{j_w}$,

c.2.- $[F_{j_1} \cdots F_{j_w} : k] = (\prod_{n=1}^{w-1} [F_{j_n} : F'_{j_n}])[F'_{j_w} : k] = (\prod_{n=1}^{w-1} \ell^{n-a_{j_n}})\ell^{d_{i_0}-d_w}$,

d.2.- $(F_{j_1} \cdots F_{j_w})^{I_{j_1} \cdots I_{j_w}} = F'_{j_w}$.

Observemos que, por definición, de F_{i_w}, los campos satisfacen $F'_{i_w} = k$, $i_w \in \mathcal{I}$, el análisis para probar a.2, b.2, c.2, d.2 a su vez prueba de forma análoga los casos a.1, b.1, c.1, d.1.

Por simplicidad de notación, consideremos los campos F_w en representación de F_{j_w}, $j_w \in \mathcal{J}$. Análogamente lo haremos para los grupos de inercia, esto es, escribiremos I_w en lugar de I_{j_w}, $j_w \in \mathcal{J}$. Con esto en mente, tenemos

a.2.- $F_1 \cdots F_{w-1} \cap F_w = F'_{w-1}$:

En efecto, por la definición de los campos F'_j, $j \in \mathcal{J}$, tenemos que $F'_1 \subseteq \cdots \subseteq F'_w$, por tanto $F'_{w-1} \subseteq F_1 \cdots F_{w-1} \cap F_w$. Por otro lado, dado un subcampo $A \neq k$ de $F_1 \cdots F_{w-1} \cap F_w$ se tiene que, en A/k el único primo finito que puede ramificarse es P_{i_0}, ya que si algún P_j, $\leq j \leq w-1$ se ramificara, en particular, puesto que $A \subseteq F_w$, se tendría P_j con $j \neq w$ se ramificaría, lo cual es imposible. De igual forma P_w es no ramificado en $F_1 \cdots F_{w-1}$, en particular $A := F_1 \cdots F_{w-1} \cap F_w$. Ahora, por el Lema de Abhyankar se sigue que $e_{P_{i_0}}(F_1 \cdots F_{w-1}/k) = \mathrm{mcm}[e_{P_{i_0}}(F_1/k), \cdots, e_{P_{i_0}}(F_{w-1}/k)] = e_{P_i}(F_{w-1}/k) = |I_{w-1}|$. Así $F'_{w-1} \subseteq F'_w \subseteq F_w$, es decir, el máximo campo común con P_{i_0} el único primo finito ramificado entre los campos $F_1 \cdots F_{w-1}$ y F_w es F'_{w-1}. Por tanto $F_1 \cdots F_{w-1} \cap F_w \subseteq F'_{w-1}$.

b.2.- $I_1 \cdots I_w \cong I_1 \times \cdots \times I_w$:

Procederemos por inducción. Con anterioridad probamos que se cumple para dos grupos de inercia, esto es $I_1 I_2 \cong I_1 \times I_2$. Supongamos ahora que se cumple $I_1 \cdots I_n \cong I_1 \times \cdots \times I_n$. Entonces consideremos $I_1 \cdots I_{n+1} = I_1 \cdots I_n I_{n+1}$. Sean $H := I_1 \cdots I_n \cong I_1 \times \cdots \times I_n$. Tenemos de forma análoga al caso de dos grupos que, $H I_{k+1} = H \times I_{k+1}$. Entonces por la hipótesis de inducción

$$I_1 \cdots I_{k+1} \cong I_1 \times \cdots \times I_{k+1}.$$

c.2.- $[F_1 \cdots F_w : k] = (\prod_{n=1}^{w-1} [F_n : F'_n])[F'_w : k] = (\prod_{n=1}^{w-1} \ell^{n-a_{j_n}})\ell^{d_{i_0}-d_w}$:

Se sigue de que $F'_1 \subseteq \cdots \subseteq F'_w$ y del inciso a.2, aplicados sobre la igualdad

$$\begin{aligned}[F_1 \cdots F_w : k] &= \frac{\prod_{j=1}^{w} [F_j : k]}{\prod_{j=1}^{r} [F_1 \cdots F_{j-1} \cap F_j : k]} = \frac{\prod_{j=1}^{w} [F_j : k]}{\prod_{j=1}^{w} [F'_{j-1} : k]} \\ &= \prod_{j=1}^{w} [F_{j-1} : F'_{j-1}][F'_w : k].\end{aligned}$$

d.2.- $(F_1 \cdots F_w)^{I_1 \cdots I_w} = F'_w$:

Primero observemos que por teoría clásica de Galois, si $F := F_1 \cdots F_w$ entonces $(F_1 \cdots F_w)^{I_1 \cdots I_w} = F^{I_1} \cap \cdots \cap F^{I_w}$, tal que

$$F^{I_j} = F^{\{e\} \times I_j \times \{e\}} = F_1 \cdots F_{j-1} F'_j F_{j+1} \cdots F_w.$$

En otras palabras, de b.2 tenemos que

$$(F_1 \cdots F_w)^{I_1 \cdots I_w} = F_1^{I_1} \cdots F_1^{I_w} = F'_1 \cdots F'_w = F'_w.$$

Sea $L = \prod_{i\in\mathcal{I}} F_i \prod_{j\in\mathcal{J}} F_j$. Veremos que $(\prod_{i\in\mathcal{I}} F_i) \cap (\prod_{j\in\mathcal{J}} F_j) = k$. De otra manera, sea $A \neq k$ un subcampo propio de $\prod_{i\in\mathcal{I}} F_i$. Entonces, al menos uno de los P_i con $i \in \mathcal{I}$ podría ramificarse en A, ya que de otra forma tendríamos por b.1 y d.1 que $A \subseteq (\prod_{i\in\mathcal{I}} F_i)^{\prod_{i\in\mathcal{I}} I_i} = k$. Por tanto, en todo subcampo propio no trivial de $\prod_{i\in\mathcal{I}} F_i$ al menos un P_i con $i \in \mathcal{I}$ se ramifica. Ahora, en todo subcampo de $\prod_{j\in\mathcal{J}} F_j$ se tiene que algún $P_j, j \in \mathcal{J}$ o P_{i_0} es ramificado, pero ninguno de éstos es ramificado en $\prod_{i\in\mathcal{I}} F_i$. Se sigue que $(\prod_{i\in\mathcal{I}} F_i) \cap (\prod_{j\in\mathcal{J}} F_j)$ no tiene subcampos propios distintos de k. En consecuencia, de c.1 y c.2 obtenemos

$$\begin{aligned}[L:k] &= [F_{i_1}\cdots F_{i_{s'}} : k][F_{j_1}\cdots F_{j_s} : k] \\ &= \prod_{j=1}^{s'} \ell^{n-a_{i_j}} (\prod_{n=1}^{s-1} \ell^{n-a_{j_n}})\ell^{d_{i_0}-d_s} = (\prod_{\substack{j=1\\ j\neq i_0}}^{r} \ell^{n-a_j})\ell^{d_{i_0}-d_s} \end{aligned} \tag{5.12}$$

A continuación veremos que $L \cap F_{i_0} = F'_s$. Sea $C := L \cap F_{i_0}$. Tenemos que $F'_s \subseteq C$. Como $C \subseteq F_{i_0}$ todo primo P_j con $1 \leq j \leq r$, $j \neq i_0$, es no ramificado en C. Sea $I = \prod_{\substack{j=1\\ j\neq i_0}}^{r} I_j$. De b.1 y b.2 obtenemos que $C \subseteq L^I$. De d.1 y d.2 se sigue

$$L^I = (F_{i_1}\cdots F_{i_{s'}})^{I_{i_1}\cdots I_{i_{s'}}} (F_{j_1}\cdots F_{j_s})^{I_{j_1}\cdots I_{j_s}} = F'_s.$$

Por tanto $C = L^I = F'_s$.

Finalmente, notemos que $[M : E_{\mathfrak{gc}}] = [M : LF_{i_0}]$. Por la correspondencia de Galois tenemos que $[LF_{i_0} : L] = [F_{i_0} : L \cap F_{i_0}]$. Así

$$[F_{i_0} : L \cap F_{i_0}] = [k(\sqrt[\ell^{d_{i_0}+t}]{P_{i_0}}) : k(\sqrt[\ell^{d_{i_0}-d_s}]{P^*_{i_0}})] = \frac{[k(\sqrt[\ell^{d_{i_0}+t}]{P_{i_0}}) : k]}{[k(\sqrt[\ell^{d_{i_0}-d_s}]{P^*_{i_0}}) : k]} = \ell^{d_{i_0}+t-d_{i_0}+d_s}.$$

Se sigue que $[LF_{i_0} : L] = [F_{i_0} : L \cap F_{i_0}] = [F_{i_0} : F'_{i_0}] = \ell^{d_{i_0}+t-d_{i_0}+d_s} = \ell^{d_s+t}$. De la ecuación (5.12) obtenemos

$$\begin{aligned}[M : LF_{i_0}] = \frac{[M:k]}{[LF_{i_0}:k]} = \frac{[M:k]}{[LF_{i_0}:L][L:k]} &= \frac{\prod_{j=1}^{r} \ell^{n-a_j}}{\ell^{d_s+t}(\prod_{\substack{j=1\\ j\neq i_0}}^{r} \ell^{n-a_j})\ell^{d_{i_0}-d_s}} \\ &= \frac{\ell^{n-a_{i_0}}}{\ell^{d_{i_0}+t}} = \ell^{n-a_{i_0}-d_{i_0}-t}.\end{aligned}$$

Por otro lado tenemos $m = n - a_{i_0} - d_{i_0}$. Por tanto $[M : LF_{i_0}] = \ell^{m-t} = [M : E_{\mathfrak{ge}}]$ y por construcción tenemos que $L(\sqrt[\ell^{d_{i_0}+t}]{P^*_{i_0}}) \subseteq E_{\mathfrak{ge}}$. Se sigue que $E_{\mathfrak{ge}} = L(\sqrt[\ell^{d_{i_0}+t}]{P^*_{i_0}})$. $\square$

Nota 5.4. En la definición de F_j dada en (5.1), para $j < i_0$ si $1 \leq n - a_j - \min\{n - a_j, d_j\} \leq t$, podemos definir simplemente $F_j = E_j$.

5.2. Caso general ℓ^n

Sea H el grupo de descomposición de $\mathcal{P}_\infty$ en $E_{\mathfrak{ge}}K/K$ (ver diagrama (2.6)).

Teorema 5.5. *Sea $K = k(\sqrt[\ell^n]{\gamma D^*}) \subseteq k(\Lambda_D)_u$, con $\ell^n \mid q-1$, $\gamma \in \mathbb{F}_q^*$, $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$, $1 \leq \alpha_j \leq \ell^n - 1$, $\alpha_j = b_j \ell^{a_j}$ con $\operatorname{mcd}(b_j, \ell) = 1$, $1 \leq j \leq r$, $P_1, ..., P_r \in R_T^+$ polinomios diferentes. Ordenamos los polinomios $P_1, ..., P_r$ tales que $0 = a_1 \leq \cdots \leq a_r \leq n-1$. Sea $E = K_u \cap k(\Lambda_D)$, t como en el Teorema 5.3 y $\alpha = \nu_\ell(|H|)$. Sea $H' := H \mid_{E_{\mathfrak{ge}}}$. Entonces $E_{\mathfrak{ge}}^{H'} = F_1 \cdots F_{i_0-1} F_{i_0+1} \cdots F_r(\sqrt[\ell^{d_{i_0}+(t-\alpha)}]{P^*_{i_0}})$ donde F_j está dado en (5.1) para toda j. Así*

$$K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H'} K = \prod_{\substack{i=1 \\ i \neq i_0}}^{r} F_i K(\sqrt[\ell^{d_{i_0}+(t-\alpha)}]{P^*_{i_0}}).$$

Más aún, si $d = \min\{n, \nu_\ell(\operatorname{gr} D)\}$, tenemos

$$|H| = \ell^\alpha = [\mathbb{F}_q(\sqrt[\ell^n]{(-1)^{\operatorname{gr} D}\gamma}) : \mathbb{F}_q(\sqrt[\ell^d]{(-1)^{\operatorname{gr} D}\gamma})].$$

Demostración. Del Teorema 5.3 tenemos $e_\infty(F_j/k) = 1$ para $j \neq i_0$ (es decir, $e_\infty(L/k) = 1$). Por tanto $e_\infty(E_{\mathfrak{ge}}/k) = \operatorname{mcm}[e_\infty(F_j/k) \mid 1 \leq j \leq r] = e_\infty(F_{i_0}/k) = \ell^t$. Esto es, la ramificación de $\mathcal{P}_\infty$ en $E_{\mathfrak{ge}}/k$ depende sólo de la ramificación de $\mathcal{P}_\infty$ en la extensión F_{i_0}/k. Ya que $E_{\mathfrak{ge}}/E_{\mathfrak{ge}}^+$ es una extensión cíclica, $E_{\mathfrak{ge}}^+ \subseteq E_{\mathfrak{ge}}^{H'} \subseteq E_{\mathfrak{ge}}$, y se tiene

$$[E_{\mathfrak{ge}} : E_{\mathfrak{ge}}^{H'}] = [E_{\mathfrak{ge}} : F_1 \cdots F_{i_0-1} F_{i_0+1} \cdots F_r(\sqrt[\ell^{d_{i_0}+(t-\alpha)}]{P^*_{i_0}})],$$

se sigue que

$$E_{\mathfrak{ge}}^{H'} = F_1 \cdots F_{i_0-1} F_{i_0+1} \cdots F_r(\sqrt[\ell^{d_{i_0}+(t-\alpha)}]{P^*_{i_0}}).$$

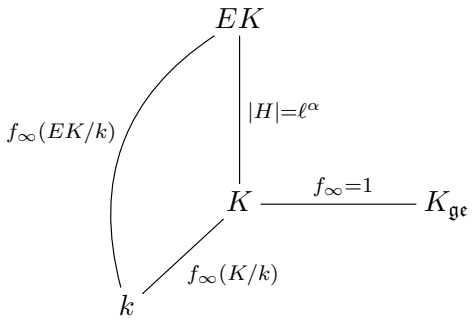
Tenemos que $EK = K(\sqrt[\ell^n]{(-1)^{\operatorname{gr} D}\gamma})$ y EK/K es no ramificada, de hecho, EK/K es una extensión de constantes [22, Subsección 5.3]. De [27, Theorem 6.2.1], tenemos que

$$f_\infty(EK/k) = [\mathbb{F}_q(\sqrt[\ell^n]{(-1)^{\operatorname{gr} D}\gamma}) : \mathbb{F}_q]$$

y de [5, Proposition 2.8] se sigue que

$$f_\infty(K/k) = [\mathbb{F}_q(\sqrt[\ell^d]{(-1)^{\operatorname{gr} D}\gamma}) : \mathbb{F}_q] \text{ con } d = \min\{n, \nu_\ell(\operatorname{gr} D)\}.$$

Entonces $f_\infty(EK/k) = f_\infty(EK/K)f_\infty(K/k)$ en donde $f_\infty(EK/K) = |H| = \ell^\alpha$.



Por lo tanto

$$\begin{aligned} |H| = \ell^\alpha = \frac{f_\infty(EK/k)}{f_\infty(K/k)} &= \frac{[\mathbb{F}_q(\sqrt[\ell^n]{(-1)^{\mathrm{gr}\, D}\gamma}) : \mathbb{F}_q]}{[\mathbb{F}_q(\sqrt[\ell^d]{(-1)^{\mathrm{gr}\, D}\gamma}) : \mathbb{F}_q]} \\ &= [\mathbb{F}_q(\sqrt[\ell^n]{(-1)^{\mathrm{gr}\, D}\gamma}) : \mathbb{F}_q(\sqrt[\ell^d]{(-1)^{\mathrm{gr}\, D}\gamma})]. \end{aligned}$$

□

Corolario 5.6. (Caso $n = 1$, G. Peng [20]) *Sea $K := k(\sqrt[\ell]{\gamma D})$ con $\gamma \in \mathbb{F}^*$, donde $D = P_1^{\alpha_1} \cdots P_r^{\alpha_r} \in R_T$ es un polinomio mónico libre de ℓ–potencias, $P_i \in R_T^+$ y $d_j = \nu_\ell(\mathrm{gr}\, P_j)$, $1 \leq \alpha_j \leq \ell - 1$, $1 \leq j \leq r$. Sean $m = \mathrm{máx}\{1 - \mathrm{mín}\{1, d_j\} \,|\, 1 \leq j \leq r\}$ y $d = \mathrm{mín}\{1, \nu_\ell(\mathrm{gr}\, D)\}$. Supondremos que $m = 1 - \mathrm{mín}\{1, d_r\}$. Entonces*

$$K_{\mathfrak{ge}} = \begin{cases} E_1 \cdots E_r K & \text{si } m = 1 - d,\ E = K \text{ o } E \neq K \text{ y } d = 1 \\ F_1 \cdots F_{r-1} K & \text{si } m > 1 - d,\ E = K \text{ o } E \neq K \text{ y } d = 0 \text{ o } 1 \end{cases}, \tag{5.13}$$

en donde $E_j = k(\sqrt[\ell]{P_j^*})$, $1 \leq j \leq r$, $F_j = k(\sqrt[\ell]{P_j P_r^{z_j}})$ $1 \leq j \leq r - 1$, $z_j = -a\, \mathrm{gr}\, P_j$, con $a\, \mathrm{gr}\, P_r + b\ell = 1$, cuando $d_r = 0$ para algún b.

Demostración. Pongamos $\alpha_j = b_j \ell^{a_j}$, $1 \leq j \leq r$, tenemos que $0 = a_1 = \cdots = a_r$. Sea i_0 como en el Teorema 5.5, esto es, i_0, $1 \leq i_0 \leq r$, es tal que $n - a_{i_0} - \mathrm{mín}\{n - a_{i_0}, d_{i_0}\} = m$. Entonces $i_0 = r$.

Por otro lado, tenemos dos casos, si escribimos $\epsilon := (-1)^{\mathrm{gr}\, D}\gamma$, entonces

$a)$ $\epsilon \in (\mathbb{F}^*)^\ell$

$b)$ $\epsilon \notin (\mathbb{F}^*)^\ell$

$a)$ Tenemos que si $K = E$ (ver [21, Theorem 4.2]), entonces $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}$. Si $m = t$, entonces $E_{\mathfrak{ge}} = E_1 \cdots E_r$, con $E_j = k(\sqrt[\ell]{P_j^*})$, $1 \leq j \leq r$, así $K_{\mathfrak{ge}} = E_1 \cdots E_r$. Si $m > t$,

tenemos que $m = 1$ y $t = 0$, del Teorema 5,3 tenemos $E_{\mathfrak{ge}} = F_1 \cdots F_r$, donde si $z_j := -ac_j\ell^{d_j - d_r}$ entonces

$$F_j := \begin{cases} k\left(\sqrt[\ell]{P_j P_r^{z_j}}\right) & \text{si } j < r, \\ k\left(\sqrt[\ell^{d_r+t}]{(-1)^{\operatorname{gr} P_r} P_r}\right) & \text{si } j = r. \end{cases} \tag{5.14}$$

Notemos que $d_r = 0$ y puesto que $t = 0$, tenemos $F_r = k$. Por tanto $K_{\mathfrak{ge}} = F_1 \cdots F_{r-1}$.

b) Tenemos que $K \neq E$ y $K_{\mathfrak{ge}} = E_{\mathfrak{ge}}^{H'} K$, donde H está dado como en el Teorema 5.5, y con $E_{\mathfrak{ge}}$ como en el caso a). También tenemos que $|H'| = \ell^\alpha = [\mathbb{F}(\sqrt[\ell]{(-1)^{\operatorname{gr} D}\gamma}) : \mathbb{F}(\sqrt[\ell^d]{(-1)^{\operatorname{gr} D}\gamma})]$, en donde $\alpha = 0$ o 1, esto es $|H'| = 1$ o ℓ.

Si $d = 1$, entonces $|H'| = 1$, esto es $\alpha = 0$. Así $K_{\mathfrak{ge}} = E_{\mathfrak{ge}} K$, con $E_{\mathfrak{ge}}$ en a). Por lo tanto $K_{\mathfrak{ge}} = E_1 \cdots E_r K$ si $m = t$ y $K_{\mathfrak{ge}} = F_1 \cdots F_{r-1} K$ si $m > t$ con F_j como en (5.14).

Si $d = 0$, tenemos que $|H'| = \ell$, esto es $\alpha = 1$. Ya que $d = 1 - t$, tenemos $1 = t \leq m \leq 1$. Por tanto $\ell \nmid \operatorname{gr} P_r$, esto es $d_r = 0$. Del Teorema 5.5 y de $d_r + t - \alpha = 0$, obtenemos

$$E_{\mathfrak{ge}}^{H'} = F_1 \cdots F_{r-1}(\sqrt[\ell^{d_{i_0}+(t-\alpha)}]{P_r^*}) = F_1 \cdots F_{r-1}.$$

Por tanto $K_{\mathfrak{ge}} = F_1 \cdots F_{r-1} K$. □

A continuación veamos un ejemplo que ilustra el Teorema 5.5

Ejemplo 5.7. *Sea* $K = \mathbb{F}(\sqrt[\ell^n]{\gamma D})$ *con* $\gamma = 5$, $\ell = 3$, $n = 10$, $q = 472393$ *y* $D = P_1^{\alpha_1} P_2^{\alpha_2} P_3^{\alpha_3} P_4^{\alpha_4}\ P_5^{\alpha_5} P_6^{\alpha_6} P_7^{\alpha_7} P_8^{\alpha_8}$, *donde* $\alpha_j = b_j \ell^{a_j}$, $\operatorname{gr} P_j = c_j \ell^{b_j}$, $1 \leq j \leq 8$. *Sea* $a_1 = 0$, $a_2 = 1$, $a_3 = 3$, $a_4 = 3$, $a_5 = 4$, $a_6 = 7$, $a_7 = 8$ *y* $a_8 = 9$. *Sea* $d_1 = 5$, $d_2 = 7$, $d_3 = 2$, $d_4 = 3$, $d_5 = 2$, $d_6 = 0$, $d_7 = 10$ *y* $d_8 = 0$. *Ya que* $\operatorname{mcd}(b_j c_j, \ell) = 1$, $1 \leq j \leq 8$, *podemos elegir* $c_1 = 2$, $b_1 = b_2 = b_4 = b_5 = b_6 = b_7 = b_8 = c_2 = c_4 = c_6 = c_7 = c_8 = 1$ *y* $b_3 = c_3 = c_5 = 5$. *Tenemos que* $m = \max\{n - a_j - \min\{n - a_j, d_j\} \mid 1 \leq j \leq r\} = \max\{5, 2, 5, 4, 4, 3, 0, 1\} = 5$ *y* $t = 10 - \min\{10, \nu_\ell(\operatorname{gr} D)\}$ *donde* $\operatorname{gr} D = \ell^5(\ell^3(b_2c_2 + b_7c_7\ell^{10} + b_8c_8\ell) + b_1c_1 + b_3c_3 + \ell(b_4c_4 + b_5c_5 + b_6c_6\ell))$, *tal que* $\nu_\ell(b_1c_1 + b_3c_3 + \ell(b_4c_4 + b_5c_5 + b_6c_6\ell)) = 3$. *Así* $\nu_\ell(\operatorname{gr} D) = 8$, $\operatorname{gr} D = 387459855$ *y* $t = 2$. *Tenemos que* $i_0 = 3$, $F_3 = k\left(\sqrt[\ell^4]{P_3^*}\right)$ *y*

$$F_1 = k\left(\sqrt[\ell^{10}]{P_1 P_3^{z_1}}\right),\ F_2 = k\left(\sqrt[\ell^9]{P_2 P_3^{z_2}}\right),\ F_4 = k\left(\sqrt[\ell^7]{P_4 P_3^{y_4 \ell}}\right),$$
$$F_5 = k\left(\sqrt[\ell^6]{P_5 P_3^{y_5 \ell^0}}\right),\ F_6 = k\left(\sqrt[\ell^5]{P_6^{\ell^2} P_3^{y_6}}\right),\ F_7 = k\left(\sqrt[\ell^2]{P_7 P_3^{y_7 \ell^8}}\right),$$
$$F_8 = k\left(\sqrt[\ell^3]{P_8^{\ell^2} P_3^{y_8}}\right),$$

con $z_1 = -2a\ell^3$, $z_2 = -a\ell^5$ *y* $y_j \equiv -c_j 5^{-1} \mod \ell^{10} = -c_j 11810 \mod 3^{10}$, $4 \leq j \leq 8$, *donde* $a5 + b\ell^8 = 1$. *Elegimos* $y_4 = y_6 = y_7 = y_8 = 47239$, $y_5 = 59048$, $a = -1312$ *y* $b = 1$. *Por lo tanto*

$$K_{\mathfrak{ge}} = K(\sqrt[3^{10}]{P_1 P_3^{70848}}, \sqrt[3^9]{P_2 P_3^{318816}}, \sqrt[3^7]{P_4 P_3^{141717}}, \sqrt[3^6]{P_5 P_3^{59048}}, \sqrt[3^5]{P_6^9 P_3^{47239}}, \sqrt[3^2]{P_7 P_3^{309935079}}, \sqrt[3^3]{P_8^9 P_3^{47239}}, \sqrt[3^{4-\alpha}]{P_3^*}).$$

con

$$|H'| = 3^\alpha = [\mathbb{F}(\sqrt[3^{10}]{-\gamma}) : \mathbb{F}(\sqrt[3^8]{-\gamma})].$$

De [1, Theorem 4 (1)], $5 \notin (\mathbb{F}^*)^\ell$ *y* $[\mathbb{F}(\sqrt[3^{10}]{-\gamma}) : \mathbb{F}(\sqrt[3^8]{-\gamma})] = 3^2$. *Por lo tanto* $\alpha = 2$ *y* $\sqrt[3^{4-\alpha}]{P_3^*} = \sqrt[3^2]{P_3^*}$.

Notación

A lo largo del trabajo se usa la siguiente notación:

Sea p un número primo, entonces

$$\begin{aligned}
\mathbb{N} &= \{1, 2, \dots\}, \\
\mathbb{Z} &= \text{anillo de números enteros}, \\
\mathbb{Q} &= \text{campo de números racionales}, \\
\mathbb{R} &= \text{campo de números reales}, \\
\mathbb{C} &= \text{campo de números complejos}, \\
\mathbb{F}_p &= \text{campo finito de } p \text{ elementos } \mathbb{Z}/p\mathbb{Z}, \\
\mathbb{F}_q &= \text{campo finito de } q = p^r \text{ elementos}, \\
C_m &= \text{grupo cíclico de orden } m.
\end{aligned}$$

Para $m, n \in \mathbb{Z}$, $m \mid n$ significa que m divide a n, es decir, $n \in m\mathbb{Z}$, $\mathrm{mcd}(m, n)$ denota el *máximo común divisor* de m y n. Y $\mathrm{mcm}[m, n]$ denota el *mínimo común múltiplo* de m y n.

El cardinal de un conjunto S es denotado por $|S|$ (entonces $|S|$ es el número de elementos en S cuando S es finito). Sean I y A dos conjuntos; una familia de elementos de A indexada por I, denotada por $\{a_i\}_{i \in I}$, es una función $\varphi : I \to A$ tal que $\varphi(i) = a_i$.

$\emptyset$ denota al conjunto vacío;

$X \subseteq Y$ X es subconjunto de Y;

$X \subsetneq Y$ X es un subconjunto propio de Y;

$X := Y$ X está definido como Y, o es igual a Y por definición;

$X \cong Y$ X es isomorfo a Y;

$X \neq Y$ X es distinto de Y;

$x \in Y$ x es elemento de Y;

$X \setminus Y$ denota el conjunto de los $x \in X$ tal que $x \notin Y$;

$F[T]$ denota el anillo de polinomios en la variable T con coeficientes en F;

$\prod$ denota "producto";

$\oplus$ denota "suma directa";

ν_ℓ denota la valuación respecto a ℓ, un número primo;

$\mathcal{O}_K$ denota el anillo de enteros de campo K;

$D(\mathfrak{P} \mid \mathfrak{p})$ denota el grupo de descomposición del ideal $\mathfrak{P}$ sobre el ideal $\mathfrak{p}$;

$I(\mathfrak{P} \mid \mathfrak{p})$ denota el grupo de inercia del ideal $\mathfrak{P}$ sobre el ideal $\mathfrak{p}$;

$e(\mathfrak{P} \mid \mathfrak{p})$ denota el índice de ramificación del ideal $\mathfrak{P}$ sobre el ideal $\mathfrak{p}$;

$f(\mathfrak{P} \mid \mathfrak{p})$ denota el grado de inercia del ideal $\mathfrak{P}$ sobre el ideal $\mathfrak{p}$;

$e_P(E/F)$ denota el índice de ramificación de cualquier primo sobre P en E/F;

$S_\infty(K)$ denota el conjunto de primos de K sobre $\mathcal{P}_\infty$;

$e_\infty(E/F)$ denota el índice de ramificación de $S_\infty(F)$ en E;

$f_\infty(E/F)$ denota el grado de inercia de $S_\infty(F)$ en E;

$h_\infty(E/F)$ denota al número de descomposición de $S_\infty(F)$ en E;

$\square$ indica fin de la demostración;

$\mathfrak{d}_{L/K}$ denota el discriminante de la extensión L/K;

$\mathfrak{d}_L$ denota el discriminante de la extensión $L/\mathbb{Q}$;

k denota el campo de funciones racionales $\mathbb{F}_q(T)$;

R_T denota el anillo de polinomios $\mathbb{F}_q[T]$;

R_T^+ denota el conjunto de polinomios mónicos e irreducibles en R_T;

$\mathcal{P}_\infty$ denota al primo infinito en k;

S denota un conjunto no vacío de divisores primos de un campo K (en este trabajo en general $S := \{\mathfrak{P}$ primo en $K \mid \mathfrak{P}$ sobre $\mathcal{P}_\infty\}$);

$K_{H,S}$ denota el campo de clases de Hilbert de K respecto a S (en campos numéricos se denota simplemente K_H);

F_χ denota el conductor del caracter χ;

Λ_N denota la N-torsión del modulo de Carlitz para $N \in R_T \setminus \{0\}$;

$K_{\mathfrak{ge}}$ denota el campo de géneros del campo K;

$K_{\mathfrak{gex}}$ denota el campo de géneros extendido de K;

$k(\Lambda_N)$ denota el campo de funciones ciclotómico de N sobre k;

$k(\Lambda_N)^+$ denota el máximo subcampo real de $k(\Lambda_N)$;

L_n denota el campo fijo por $\mathbb{F}_q^*$ contenido en $k(\Lambda_{T^{-n-1}})$;

K_m denota al campo $K\mathbb{F}_{q^m}$;

${}_nK$ denota al campo KL_n;

${}_nK_m$ denota al campo $K\mathbb{F}_{q^m}L_n$;

$[L : K]$ denota el grado de la extensión de campos L/K, es decir, la dimensión de L como espacio vectorial sobre K.

De forma estándar se usan el abecedario gótico fraktur (mathfrak) para ideales:

$\mathfrak{a}$	$\mathfrak{b}$	$\mathfrak{c}$	$\mathfrak{f}$	$\mathfrak{m}$	$\mathfrak{p}$	$\mathfrak{q}$	$\mathfrak{A}$	$\mathfrak{B}$	$\mathfrak{C}$	$\mathfrak{M}$	$\mathfrak{P}$	$\mathfrak{Q}$
a	b	c	f	m	p	q	A	B	C	M	P	Q

al igual que el abecedario caligráfico (mathcal) para grupos, ideales o ciertos anillos:

$\mathcal{D}$	$\mathcal{G}$	$\mathcal{H}$	$\mathcal{O}$	$\mathcal{P}$
D	G	H	O	P

Para un vector $\mathbf{x} = (x_1, x_2, \dots)$ con una cantidad a lo más numerable de componentes x_n, en característica 0, se definen las *componentes fantasmas* de x por

$$x^{(t)} = x_1^{p^{t-1}} + px_2^{p^{t-2}} + \cdots + p^{t-1}x_t = \sum_{i=1}^{t} p^{i-1}x_i^{p^{t-i}}, \quad t = 1, 2, \dots$$

Recíprocamente, x_t puede ser calculado recursivamente como un polinomio en $x^{(1)}$, $x^{(2)}$, $\dots$, $x^{(t)}$. Esta correspondencia puede ser expresada como

$$\mathbf{x} = (x_1, x_2, x_3, \dots \mid x^{(1)}, x^{(2)}, x^{(3)}, \dots).$$

La *suma* $\overset{\bullet}{+}$, la *diferencia* $\overset{\bullet}{-}$ y el *producto* $\overset{\bullet}{\cdot}$ *de Witt* se definen por

$$\mathbf{x} \overset{\bullet}{\pm} \mathbf{y} = (?, ?, \dots \mid x^{(1)} \overset{\pm}{\cdot} y^{(1)}, x^{(2)} \overset{\pm}{\cdot} y^{(2)}, \dots).$$

Referencias

[1] Aabrandt, Andreas; Lundsgaard–Hansen, Vagn, *A note on powers in finite fields*, International Journal of Mathematical Education in Science and Technology **47**, no. 6, 987-991, (2016).

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

[3] Artin, Emil; Tate John, *Class field theory*, Benjamin, New York, 1967.

[4] Bae, Sunghan; Koo, Ja Kyung, *Genus theory for function fields*, J. Austral. Math. Soc. Ser. A **60**, no. 3, 301–310, (1996).

[5] Bautista–Ancona, Víctor; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Genus fields of cyclic l–extensions of rational function fields*, International Journal of Number Theory **9**, no. 5, 1249–1262, (2013).

[6] Barreto–Castañeda, Jonny Fernando; Jarquín–Zárate, Fausto; Rzedowski–Calderón, Martha; Villa–Salvador, Gabriel, *Abelian p–extensions and additive polynomials*, International Journal of Mathematics, Vol. **28**, no. 14, 1–32, (2017).

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

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

[9] Dummit, David; Foote Richardt, *Abstract Algebra*, Tercera edición. Wiley, 2004.

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

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

[12] Fröhlich, Albrecht, *Central extensions, Galois groups and ideal class groups of number fields*, Contemporary Mathematics, **24**, American Mathematical Society, Providence, RI, 1983.

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

[14] Garcia, Arnaldo; Stichtenoth, Henning, *Elementary Abelian p–Extensions of Algebraic Function Fields*, manuscripta math. **72**, 67–79 (1991).

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

[16] Hayes, David, Explicit Class Field Theory for Rational Function Fields, Trans. Amer. Math. Soc. **189**, 77–91, (1974).

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

[18] Ishida, Makoto, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, Vol. **555**, Springer-Verlag, Berlin-New York, 1976.

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

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

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

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

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

[24] Rosen, Michael, *The Hilbert class field in function fields*, Exposition. Math. **5**, no. 4, 365–378, (1987).

[25] Rzedowski Calderón, Martha; Villa Salvador, Gabriel, *Campos ciclotómicos* (versión preliminar), arXiv: 1407.3238v1, 11 de julio de 2014.

[26] Schmid, Hermann Ludwig, *Zur Arithmetik der zyklischen p-Körper*, J. Reine Angew. Math. **176**, 161–167, (1936).

[27] Villa Salvador, Gabriel Daniel, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

[28] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Springer-Verlag, Second edition, GTM 83, 1997.

[29] Witt, Ernst, *Zyklische Körper und Algebren der Characteristik p von Grad p^n*, J. Reine Angew. Math. **176**, (1936), 126-140.

[30] Wittmann, Christian, *l–class groups of cyclic function fields of degree l*, Finite Fields Appl. **13**, no. 2, 327–347, (2007).

[31] Zhang, Xianke, *A simple construction of genus fields of abelian number fields*, Proc. Amer. Math. Soc. **94**, no. 3, 393–395, (1985).