Casa abierta al tiempo

Universidad Autónoma Metropolitana
Ciencias Básicas e Ingeniería
Unidad Iztapalapa
Posgrado en Matemáticas

UNA DEMOSTRACIÓN COMBINATORIA DEL TEOREMA DE KRONECKER-WEBER EN CAMPOS DE FUNCIONES

Tesis que presenta

Julio Cesar Salas Torres

para obtener el grado de
Doctor en Ciencias (Matemáticas)

Asesora de Tesis: Dra. Martha Rzedowski Calderón

Jurado Calificador:

Presidenta: Dra. Martha Rzedowski Calderón

Secretario: Dr. Carlos Enrique Signoret Poillon

Vocal: Dr. Fernando Barrera Mora

Vocal: Dr. Pedro Luis del Ángel Rodríguez

Vocal: Dr. Mario Pineda Ruelas

México, D. F.
Julio de 2014

Dedicatoria

A Keni, Tonalli y Tina
A mis padres y hermanos
A mis sobrinos Osiris, Shivaya y a mis ahijados

A Dalila, tía Imelda y mis abuelos †

Me lo contaron y lo olvidé; lo vi y lo entendí; lo hice y lo aprendí.

La lectura nunca fue un hábito
mas me acostumbré por la necesidad
por el hambre y mi pobreza.
Mi familia fue mi decisión
la fuerza que me dio en la voluntad
la energía que el pan no me daba
y la lucha contra la miseria.
La decisión hace la realidad
el sueño nos hace miserables
y la perseverancia nos lleva al triunfo.

Tircis Salas Torres

Agradecimientos

Por su amistad y por ser un ejemplo a seguir, agradezco:

A mi asesora de tesis la Doctora Martha Rzedowski Calderón, por haber confiado en mi motivándome a seguir adelante sin bajar los brazos, haberme tenido paciencia y guiarme en la realización de este trabajo...

Un agradecimiento muy especialmente al Doctor Gabriel Villa Salvador por su apoyo incondicional que me ha brindado...

A los Doctores Fernando Barrera Mora, Pedro Luis del Ángel Rodríguez, Mario Pineda Ruelas y Carlos Enrique Signoret Poillon por la revisión de este trabajo...

A mis profesores por sus enseñanzas...

A la Universidad Autónoma Metropolitana por las enseñanzas y el apoyo recibidos...
A la Escuela Superior de Física y Matemáticas del IPN por sus enseñanzas y las facilidades otorgadas...
A la Universidad Autónoma de la Ciudad de México por darme la oportunidad de superarme...
Al Departamento de Control Automático del Cinvestav del IPN por el apoyo académico y la flexibilidad extendida...

A mis padres por la confianza y el apoyo que siempre me han mostrado, a mi hermana Anahi por su paciencia y constancia...

A mis profesores de inglés, especialmente a la Maestra Patricia Arenas Chiang.
A la Maestra María Iseo González Christen por su apoyo...

Resumen

El objetivo principal de este trabajo fue obtener una demostración del Teorema de Kronecker-Weber en campos de funciones sin usar la teoría de campos de clases.

Como resultados preliminares se prueban el encaje de las extensiones de Artin-Schreier y el encaje de las extensiones cuadráticas de un campo de funciones racionales con campo de constantes finito en las extensiones ciclotómicas compuestas con extensiones de constantes. Se demuestra el teorema, primero para el caso de extensiones moderadamente ramificadas y después se estudian las p-extensiones cíclicas en característica p a través de los vectores de Witt.

Se presenta una prueba de tipo combinatorio del Teorema de Kronecker-Weber para campos globales de característica positiva. Las principales herramientas son el uso de los vectores de Witt y su desarrollo aritmético por H. L. Schmid. La clave fue obtener, usando argumentos de conteo, cuántas p-extensiones existen de grado fijo y conductor acotado donde sólo un divisor primo se ramifica. Comparando este número con el número de subextensiones de campos de funciones ciclotómicos del mismo tipo se verifica que los dos números son iguales.

Introducción

El Teorema de Kronecker-Weber establece que toda extensión abeliana de los números racionales está contenida en un campo ciclotómico. El primero en enunciarlo fue Leopold Kronecker en 1853 pero su demostración era incompleta. En la demostración de Heinrich Weber de 1886 había todavía un hueco y no fue sino hasta 1896 que David Hilbert dio una demostración completa, misma que se basa en los grupos de ramificación. Este teorema es una consecuencia sencilla de la teoría de campos de clases y también se puede probar usando una versión local del Teorema de Kronecker-Weber. Para el caso de campos de funciones racionales sobre un campo de constantes finito, David Hayes en 1974 obtuvo una demostración del análogo al Teorema de Kronecker-Weber basada en la teoría de campos de clases.

El objetivo de la tesis es obtener una demostración en el espíritu de la demostración de Hilbert del análogo en campos de funciones al Teorema de Kronecker-Weber. Se considerarán separadamente los casos de ramificación moderada y ramificación salvaje.

En el presente escrito se presentan como resultados preliminares el encaje de las extensiones cuadráticas en las extensiones ciclotómicas compuestas con extensiones de constantes y, para el caso de ramificación salvaje, el encaje de las extensiones de Artin-Schreier sobre un campo de funciones racionales con campo de constantes finito en las extensiones ciclotómicas compuestas con extensiones de constantes. En el primer capítulo se introduce la notación y se presentan algunos resultados acerca de los campos ciclotómicos sobre campos de funciones, se introducen resultados generales acerca de las extensiones cíclicas de Kummer y las extensiones de Artin-Schreier y se dan algunos ejemplos; se estudian los vectores de Witt y su relación con las p-extensiones cíclicas de grado p^n cuando la característica de los campos es p (Teorema 1.6) y finalmente, en la última sección, se escribe un resultado auxiliar que nos va ser de gran utilidad. En el Capítulo 2 se estudian las

extensiones de Artin-Schreier, se cuentan las extensiones de Artin-Schreier en las que hay solamente un divisor primo ramificado (Corolario 2.8) y se estima el número de tales extensiones que están contenidas en la composición de un campo ciclotómico y una extensión de constantes (Proposición 2.12). A continuación se utilizan los resultados anteriores para obtener el encaje de las extensiones de Artin-Schreier en la composición de un campo ciclotómico y una extensión de constantes (Teorema 2.15). En cuanto a las extensiones cuadráticas, se estudia primero el caso moderadamente ramificado y se obtiene el encaje de las extensiones cuadráticas moderadamente ramificadas en la composición de un campo ciclotómico y una extensión de constantes (Proposición 2.4) y, como consecuencia del Teorema 2.15, se obtiene el encaje de las extensiones cuadráticas salvajemente ramificadas en la composición de un campo ciclotómico y una extensión de constantes (Corolario 2.16). En el Teorema 2.17 se presentan juntos ambos casos. Por último, en el Capítulo 3 se consideran separadamente los casos de ramificación moderada y ramificación salvaje. Primeramente, toda extensión abeliana finita moderadamente ramificada de un campo de funciones racionales con campo de constantes finito está contenida en el compuesto de un campo ciclotómico y una extensión de constantes (Corolario 3.4). Para el caso de ramificación salvaje, primero se reduce el problema, con ayuda de los vectores de Witt, a estudiar las extensiones cíclicas de grado p^n en las que se ramifica totalmente un solo divisor primo finito y el primo infinito se descompone totalmente. Se prueba el resultado con argumentos de conteo y por inducción sobre n, siendo el caso $n = 1$ el de las extensiones de Artin-Schreier. También con ayuda de los vectores de Witt, se obtiene el paso de inducción. Alternativamente, se usan los vectores de Witt de una manera simbólica para dar otra demostración, más directa, del resultado en este caso.

Índice general

Capítulo 1

Preliminares

En la primera sección de este capítulo se trata el tema de campos ciclotómicos dentro del contexto de campos de funciones. Más adelante introducimos la teoría de las extensiones de Artin-Schreier, después estudiamos los vectores de Witt y su relación con las extensiones cíclicas de grado p^n. Por último, probaremos un resultado que nos será de gran utilidad en el tercer capítulo.

1.1. Campos de funciones ciclotómicos

Sea $\mathbb{F}_q$ el campo finito de q elementos, $q = p^t$, p primo. Sea K un campo de funciones racionales sobre $\mathbb{F}_q$, esto es $K = \mathbb{F}_q(T)$ y sea $R_T = \mathbb{F}_q[T]$. Denotamos por R_T^+ al conjunto de polinomios irreducibles mónicos en R_T y por $\mathcal{P}$ al divisor primo asociado al polinomio mónico e irreducible P, esto es

$$(P)_K = \frac{\mathcal{P}}{\mathcal{P}_\infty^d},$$

donde $d = \mathrm{gr}P$ y $\mathcal{P}_\infty$ es el divisor primo infinito. En ocasiones nos referiremos al polinomio P y a su divisor asociado $\mathcal{P}$ de manera indistinta.
Denotamos por K^{ac} a una cerradura algebraica de K. Sea $\mathcal{A} = \mathrm{End}_{\mathbb{F}_q}(K^{ac}) = \{\rho : K^{ac} \to K^{ac} \mid \rho(u+v) = \rho(u) + \rho(v),\ \rho(au) = a\ \rho(u)$ para todo $a \in \mathbb{F}_q$ y para todos $u, v\ \in K^{ac}\}$. Es decir, $\mathcal{A}$ es la $\mathbb{F}_q$-álgebra ($\mathbb{F}_q$-módulo + anillo) de los $\mathbb{F}_q$-endomorfismos del grupo aditivo de K^{ac}.
Vamos a considerar dos elementos de $\mathcal{A}$:

(1) Sea φ el homomorfismo de Fröbenius de K^{ac} sobre $\mathbb{F}_q$, es decir $\varphi : K^{ac} \to K^{ac}$ donde

$$\varphi(u) = u^q.$$

(2) Sea μ_T la multiplicación por T, $\mu_T : K^{ac} \to K^{ac}$ donde

$$\mu_T(u) = Tu.$$

Tenemos un homomorfismo de anillos $\xi : R_T \to \mathcal{A}$, $\xi(T) = \varphi + \mu_T$, $\xi(f(T)) = f(\varphi + \mu_T)$. Así pues, K^{ac} obtiene una estructura de R_T-módulo de la manera siguiente: si $u \in K^{ac}$, $M \in R_T$, usamos la notación

$$u^M := M(\varphi + \mu_T)(u).$$

Notemos que si $M, N \in R_T$, entonces $u^{N+M} = u^N + u^M$ y $u^{NM} = (u^N)^M$. Si $a \in \mathbb{F}_q$, $u \in K^{ac}$, $u^a = a(\varphi + \mu_T)^0(u) = a(u) = au$, por lo tanto la estructura de R_T-módulo respeta la estructura de $\mathbb{F}_q$-álgebra de K^{ac}. Se tienen los siguientes resultados:

(1) Si $M = a_d T^d + \cdots + a_1 T + a_0 \in R_T$, $a_d \neq 0$, entonces

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

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

(2) Sea $M \in R_T \backslash \{0\}$. Denotamos por Λ_M al conjunto de elementos de K^{ac} que corresponden a la M-torsión de K^{ac}. Esto es

$$\Lambda_M = \{u \in K^{ac} | u^M = 0\}$$

el conjunto de ceros del polinomio u^M en la variable u. Como polinomio en u sobre K, u^M es separable de grado q^d, $d = \operatorname{gr}_T M$. Por tanto Λ_M es finito con q^d elementos. Más aún, Λ_M es un espacio vectorial de dimensión d sobre $\mathbb{F}_q$. Tenemos

$$\Lambda_M \cong R_T/(M)$$

como R_T-módulos. En particular, Λ_M es R_T-cíclico. Denotamos por $\lambda = \lambda_M$ a un generador de Λ_M.

(3) Sea $M \in R_T \backslash \{0\}$. Al campo $K(\Lambda_M)$, que es el campo generado sobre K al adjuntarle Λ_M, se le llamará el **campo de funciones ciclotómico determinado por** M **sobre** K. Tenemos que la cerradura entera de R_T en $K(\Lambda_M)$ es

$$\vartheta_M = R_T[\lambda].$$

La extensión $K(\Lambda_M)/K$ es abeliana con grupo de Galois

$$G_M = \text{ Gal } (K(\Lambda_M)/K) \cong (R_T/(M))^*.$$

El **polinomio ciclotómico determinado por** M es el polinomio irreducible $\psi(u) = \text{ Irr } (\lambda, u, K)$. La **función** Φ **de Euler** está dada por

$$\Phi(M) = |(R_T/(M))^*|.$$

Tenemos las siguientes propiedades:

(a) Si $M = P^n$ para algún polinomio irreducible P, entonces

$$\Phi(P^n) = q^{dn} - q^{d(n-1)},$$

donde $d = \text{ gr } P$.

(b) Si $(M, N) = 1$, entonces $(R_T/(MN))^* \cong (R_T/(M))^* \times (R_T/(N))^*$, luego

$$\Phi(MN) = \Phi(M)\Phi(N).$$

Además $K(\Lambda_M)/K$ es una extensión geométrica, es decir, el campo de constantes de $K(\Lambda_M)$ es el mismo que el de K.

(4) Sea $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ la factorización de M como producto de potencias de polinomios irreducibles. Sea P un polinomio irreducible en R_T. Si $P \notin \{P_1, \ldots, P_r\}$ entonces $e_P = 1$, $f_P = o(P \text{ mód } M)$, $h_P = \Phi(M)/f_P$ son el índice de ramificación, el grado relativo y el número de primos de $K(\Lambda_M)$ que están encima de P, respectivamente. Si $P = P_i$ para algún $1 \leq i \leq r$, entonces $e_{P_i} = \Phi(P_i^{\alpha_i})$, $f_{P_i} = o\left(P_i \text{ mód } \dfrac{M}{P_i^{\alpha_i}}\right)$ y $h_{P_i} = \dfrac{\Phi(M)}{\Phi(P_i^{e_i}) f_{P_i}}$. Para el divisor primo $\mathcal{P}_\infty$, tenemos $e_\infty = q-1$, $f_\infty = 1$, $h_\infty = \Phi(M)/(q-1)$. El diferente de la extensión $K(\Lambda_M)/K$ está dado por

$$\mathfrak{D}_M = \prod_{i=1}^{r} \Big(\prod_{\mathfrak{p}|\mathcal{P}_i} \mathfrak{p} \Big)^{s_i} \prod_{\mathfrak{P}|\mathcal{P}_\infty} \mathfrak{P}^{q-2},$$

donde $\mathfrak{p}$ y $\mathfrak{P}$ son divisores primos en $K(\Lambda_M)$, $d_i = \text{gr}\,(P_i)$ y $s_i = \alpha_i\Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i-1)}$ para $1 \leq i \leq r$. Los primos que se ramifican en $K(\Lambda_M)/K$ son $\mathcal{P}_\infty$ y los polinomios $P \in R_T^+$ tales que $P|M$, excepto en el caso extremo $q = 2$, $M \in \{T, T+1, T(T+1)\}$ porque en este caso tenemos $K(\Lambda_M) = K$.

(5) Sean $M \in R_T$, $M \neq 0$, y G_0 el grupo de inercia de cualquier divisor primo de $K(\Lambda_M)$ sobre $\mathcal{P}_\infty$. El campo $K(\Lambda_M)^+ = K(\Lambda_M)^{G_0}$, se llama el **subcampo real maximal** de $K(\Lambda_M)$. Sea $J = \{\sigma_a \in \text{Gal}\,(K(\Lambda_M)/K) | a \in \mathbb{F}_q^*\}$ donde, para $a \in \mathbb{F}_q^*$, $\sigma_a : K(\Lambda_M) \to K(\Lambda_M)$ está dado por $\sigma_a(\lambda) = \lambda^a = a\lambda$. Tenemos que $K(\Lambda_M)^+$ es el campo fijo bajo J, es decir $G_0 = J \cong \mathbb{F}_q^*$. Se tiene que $[K(\Lambda_M) : K(\Lambda_M)^+] = q-1$ y $\mathcal{P}_\infty$ se descompone totalmente en $K(\Lambda_M)^+/K$ en $\Phi(M)/(q-1)$ divisores primos.

1.2. Divisores primos en extensiones de constantes

Sea E/k un campo de funciones congruente, esto es, su campo de constantes k es finito y sea $L = E\ell$ una extensión de constantes. El campo de constantes de L es ℓ. Dado que ℓ/k es una extensión de Galois (de hecho cíclica), L/E es una extensión de Galois. Además L/E es no ramificada. Sean $\mathcal{P}$ un lugar en E, $\text{con}_{E/L}\mathcal{P} = \mathfrak{p}_1 \cdots \mathfrak{p}_h$ y $d = d_{L/E}(\mathfrak{p}_i|\mathcal{P})$ para $1 \leq i \leq h$. Tenemos $dh = [L : E] = [\ell : k]$.

Teorema 1.1. *Sean E/k un campo de funciones congruente y $L = E\ell$ una extensión de constantes. Sean $\mathcal{P}$ un lugar en E, $\mathfrak{p}_1, ..., \mathfrak{p}_h$ los lugares de L sobre $\mathcal{P}$ y $[\ell, k] = m$. Entonces:*

(a) $d_{L/E}(\mathfrak{p}_i|\mathcal{P}) = \dfrac{m}{(d_E(\mathcal{P}), m)}$,

(b) $h = (d_E(\mathcal{P}), m)$,

(c) $d_L(\mathfrak{p}_i) = \dfrac{d_E(\mathcal{P})}{(d_E(\mathcal{P}), m)}$.

Demostración. Ver [23, Theorem 6.2.1]. □

Ejemplo 1.1. Sean $K = \mathbb{F}_3(T)$, $L = \mathbb{F}_9(T)$ y $P = T^3 - T + 1 \in R_T^+$. Consideremos $(T^3 - T + 1)_K = \dfrac{\mathcal{P}}{\mathcal{P}_\infty^3}$. Observamos que $\mathcal{P}$ es inerte en L/K pues $h = (3, 2) = 1$.

$$K = \mathbb{F}_3(T) \overset{2}{\text{———}} \mathbb{F}_9(T) = L$$

$$\mathcal{P} \text{———————} \mathfrak{p}$$

Ejemplo 1.2. Sean ahora $K = \mathbb{F}_3(T)$, $L = \mathbb{F}_{27}(T)$ y $P = T^3 - T + 1 \in R_T^+$. Nuevamente, $(T^3 - T + 1)_K = \dfrac{\mathcal{P}}{\mathcal{P}_\infty^3}$. Esta vez $\mathcal{P}$ es totalmente descompuesto en L/K pues $h = (3, 3) = 3$.

$$K = \mathbb{F}_3(T) \overset{3}{\text{———}} \mathbb{F}_{27}(T) = L$$

$$\mathcal{P} \text{———————} \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$$

Ejemplo 1.3. Sean $K = \mathbb{F}_3(T)$, $L = \mathbb{F}_{27}(T)$ y $M = T^4 - T^2 \in R_T$. Consideremos $(T^4 - T^2)_K = \dfrac{\mathcal{P}_0^2\mathcal{P}_{-1}\mathcal{P}_1}{\mathcal{P}_\infty^4}$. Observamos que $\mathcal{P}_\infty, \mathcal{P}_0, \mathcal{P}_{-1}$, y $\mathcal{P}_1$ son inertes en L/K pues $h = (1, 3) = 1$.

$$K = \mathbb{F}_3(T) \overset{3}{\text{———}} \mathbb{F}_{27}(T) = L$$

$$\mathcal{P}_\infty \text{———————} \mathfrak{p}_\infty$$

1.3. Extensiones cíclicas de Kummer y extensiones de Artin-Schreier

Empezamos esta sección con un teorema debido a Kummer y a Dedekind que establece la descomposición de un ideal primo, bajo ciertas condiciones.

Teorema 1.2 (Kummer-Dedekind)**.** *Sea E/k un campo de funciones y sea $\mathcal{P}$ un lugar de E. Supongamos que $F = E(\alpha)$, donde α es entero sobre $\vartheta_\mathcal{P}$, el anillo de valuación inducido por $\mathcal{P}$. Sea $f(X) = \text{Irr}\,(\alpha, X, E) \in \vartheta_\mathcal{P}[X]$ el*

polinomio mínimo de α sobre E, y sea

$$\bar{f}(X) := f(X) \text{ mód } \mathcal{P} = \prod_{i=1}^{r} \bar{f}_i(X)^{a_i}$$

la descomposición de $\bar{f}(X)$ en $k(\mathcal{P})[X]$, donde $k(\mathcal{P}) = \vartheta_{\mathcal{P}}/\mathcal{P}$ es el campo residual. Sea $f_i(X) \in \vartheta_{\mathcal{P}}[X]$ tal que gr $f_i(X) =$ gr $\bar{f}_i(X)$ *y $f_i(X)$* mód $\mathcal{P} = \bar{f}_i(X)$ *para $1 \leq i \leq r$.*
Entonces existen r lugares diferentes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ de F sobre $\mathcal{P}$ tales que $f_i(\alpha) \in \mathfrak{P}_i$ y $d_{F/E}(\mathfrak{P}_i|\mathcal{P}) \geq$ gr $\bar{f}_i(X)$.
Supongamos que $a_i = 1$ para $1 \leq i \leq r$ o $\{1, \alpha, ..., \alpha^{n-1}\}$ es una base entera para $\mathcal{P}$, donde $n = [F : E]$. Entonces $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ son todos los lugares de F sobre $\mathcal{P}$,

$$\text{con } {}_{E/F}\mathcal{P} = \prod_{i=1}^{r} \mathfrak{P}_i^{a_i}, \quad \vartheta_{\mathfrak{P}_i}/\mathfrak{P}_i \cong \frac{k(\mathcal{P})[X]}{(\bar{f}_i(X))},$$

y por lo tanto $d_{F/E}(\mathfrak{P}_i|\mathcal{P}) =$ gr $\bar{f}_i(X)$.

Demostración. Ver [23, Theorem 5.8.2]. □

Ahora presentamos algunos hechos básicos acerca de las extensiones cíclicas de Kummer y de Artin-Schreier.

Teorema 1.3 (Extensiones cíclicas de Kummer)**.** *Sean* car$E = p \geq 0$ *y $n \in \mathbb{N}$ tal que $p \nmid n$ (n se elige arbitrariamente en el caso $p = 0$). Supongamos que E contiene una raíz primitiva de la unidad ζ_n. Entonces F/E es una extensión cíclica de grado n si y sólo es una extensión cíclica de Kummer, esto es, si existe $z \in F$ tal que $F = E(z)$ y*

$$\text{Irr}\,(z, X, E) = X^n - a \in E[X].$$

Demostración. Ver [23, Theorem 5.8.5]. □

Sean $E = K = \mathbb{F}_q(T)$ y $F = K(y)$ una extensión cíclica de grado n sobre K, de manera que $p \nmid n$ si $p =$ car F (o bien car $F = 0$). Supongamos que F contiene las raíces n-ésimas de la unidad. Entonces, dado que F/K es una

extensión de Kummer, podemos suponer $y^n = f(T)$ con $f(T) \in R_T$ y $f(T)$ no es divisible por ninguna n-ésima potencia. Sea

$$(f(T))_K = \frac{\mathcal{P}_1^{\alpha_1} \cdots \mathcal{P}_s^{\alpha_s}}{\mathcal{P}_\infty^d}, \quad \text{donde} \quad d = \operatorname{gr} f(T) \quad \text{y} \quad 0 < \alpha_i < n.$$

Los primos finitos ramificados en F/E son precisamente $\mathcal{P}_1, \ldots, \mathcal{P}_s$ y $\mathcal{P}_\infty$ es ramificado si y sólo si $n \nmid d$. Observamos que en este tipo de extensiones la ramificación siempre es moderada.

Ejemplo 1.4. Sean $K = \mathbb{F}_3(T)$, $F = K(y)$ con $y^2 = T^3 - T + 1$. En la extensión cíclica de Kummer F/K tenemos $(T^3 - T + 1)_K = \dfrac{\mathcal{P}}{\mathcal{P}_\infty^3}$, donde $P = T^3 - T + 1$. Los lugares $\mathcal{P}$ y $\mathcal{P}_\infty$ son los lugares ramificados.
El diferente está dado por

$$\mathfrak{D}_{F/K} = \mathfrak{P}\mathfrak{P}_\infty.$$

Sean los lugares $\mathcal{P}_0, \mathcal{P}_{-1}$, $\mathcal{P}_1$ y $\mathcal{Q}$ correspondientes a los polinomios irreducibles T, $T+1$, $T-1$ y T^2+1, respectivamente. El polinomio $f(X) = X^2 - (T^3 - T + 1)$ es el polinomio mínimo de y. Tenemos que $\bar{f}(X) := f(X)$ mód $\mathcal{P}_i$ $= X^2 - 1 = (X-1)(X+1)$ es la descomposición de $\bar{f}(X)$ en $\mathbb{F}_3(\mathcal{P}_i)[X]$, para $i \in \{0, -1, 1\}$ y $\bar{f}(X) := f(X)$ mód $\mathcal{Q} = X^2 - (T+1)$ es irreducible en $\mathbb{F}_3(\mathcal{Q})[X]$. Por el Teorema de Kummer-Dedekind, $\mathcal{P}_0, \mathcal{P}_{-1}$, y $\mathcal{P}_1$ son totalmente descompuestos y $\mathcal{Q}$ es inerte en la extensión F/K.

$$\begin{array}{ccc} F = K(y) & & \mathfrak{P}^2 \\ \Big| & & \Big| \\ 2 & & \\ \Big| & & \Big| \\ K = \mathbb{F}_3(T) & & \mathcal{P} \end{array}$$

Sea E un campo de característica $p > 0$. Para $a \in E$ y $A \subseteq E$, definimos

$$\wp a = a^p - a \quad \text{y}$$
$$\wp(A) = \{a^p - a | a \in A\}.$$

La extensión F/E es llamada **extensión de Artin-Schreier** si existe un $z \in F$ tal que $F = E(z)$, donde

$$z^p - z = a$$

para algún $a \in E$ con $a \notin \wp(E)$.

Teorema 1.4 (Extensiones de Artin-Schreier)**.** *Sea E un campo de característica $p > 0$. Entonces la extensión F/E es cíclica de grado p si y sólo si es una extensión de Artin-Schreier, esto es, si existe $z \in F$ tal que $F = E(z)$ con $\mathrm{Irr}\,(z, X, E) = X^p - X - a \in E[x]$ con $a \notin \wp(E)$. Las raíces del polinomio anterior son de la forma $z + i$, donde $0 \leq i \leq p - 1$.*

Demostración. Ver [23, Theorem 5.8.4]. □

Consideremos ahora $E = k(T)$, un campo de funciones racionales, donde k es un campo perfecto de característica $p > 0$. Sea F/E una extensión cíclica de grado p. Entonces $F = E(y)$, donde es posible elegir y de tal manera que y satisface una ecuación de la forma

$$y^p - y = s(T),$$

con $s(T) \in k(T)$, $s(T) \notin \wp(E)$ y se tiene que $\mathrm{Irr}\,(y, X, k(T)) = X^p - X - s(T)$, donde

$$(s(T))_E = \frac{\mathfrak{C}}{\mathcal{P}_1^{\alpha_1} \cdots \mathcal{P}_r^{\alpha_r}},$$

donde $\mathcal{P}_i$ es un divisor primo en E, $\alpha_i \in \mathbb{N}$, $(\alpha_i, p) = 1$, $\mathfrak{C}$ es un divisor entero primo relativo a $\mathcal{P}_i$ para todo $i \in \{1, ..., r\}$. El divisor primo $\mathcal{P}_\infty$ puede o no estar incluido en este conjunto de divisores.
Conocemos a esta ecuación de Artin-Schreier como **ecuación de Artin-Schreier en su forma normal**. Los primos ramificados en F/E son precisamente $\mathcal{P}_1, ..., \mathcal{P}_r$ y son ramificados total y salvajemente (ver [4]). El diferente de F/E es

$$\mathfrak{D}_{F/E} = \prod_{i=1}^{r} \mathfrak{P}_i^{(\alpha_i+1)(p-1)}$$

donde $\mathfrak{P}_i$ es el divisor en F que divide a $\mathcal{P}_i$, para todo $i \in \{1, ..., r\}$ (ver [23, páginas 172-176]).

Con ayuda del algoritmo de la división y usando fracciones parciales, las extensiones de Artin-Schreier F/K se pueden ver de la siguiente forma. Tenemos $F := K(y)$ donde y satisface la ecuación normalizada

$$y^p - y = \sum_{i=1}^{r} \frac{Q_i}{P_i^{e_i}} + f(T), \tag{1.1}$$

donde $P_i \in R_T^+$, $Q_i \in R_T$, $(Q_i, P_i) = 1$, $e_i > 0$, $p \nmid e_i$, $\text{gr}\, Q_i < \text{gr}\, P_i^{e_i}$, $1 \leq i \leq r$, $\text{gr}\, Q_i < \sum_{i=1}^{r} \text{gr}\, P_i^{e_i}$, $f(T) \in R_T$, con $p \nmid \text{gr}\, f$ cuando $f(T) \notin \mathbb{F}_q$ y $f(T) \notin \wp(\mathbb{F}_q)$ cuando $f(T) \in \mathbb{F}_q^*$.

Tenemos que los primos finitos ramificados en F/K son precisamente, $P_1, \ldots,$ P_r (ver [4]). Con respecto a $\mathcal{P}_\infty$ tenemos el siguiente resultado, que es bien conocido y del cual ofrecemos una demostración.

Proposición 1.5. *Sea $F = K(y)$ dado por* (1.1)*. Entonces el primo $\mathcal{P}_\infty$ es*

(a) *descompuesto si $f(T) = 0$,*

(b) *inerte si $f(T) \in \mathbb{F}_q$ y $f(T) \notin \wp(\mathbb{F}_q) = \{a^p - a | a \in \mathbb{F}_q\}$,*

(c) *ramificado si $f(T) \notin \mathbb{F}_q$ (así $p \nmid \text{gr}\, f$).*

Demostración. Primero consideramos el caso $f(T) = 0$. Entonces $\nu_{\mathcal{P}_\infty}(\alpha) = \text{gr}\, (P_1^{e_1}, \ldots, P_r^{e_r}) - \text{gr}\, Q > 0$. Por lo tanto $\mathcal{P}_\infty$ es no ramificado. Ahora $y^p - y = \prod_{i=0}^{p-1}(y - i)$. Sea $\mathfrak{P}_\infty$ primo en F que divide a $\mathcal{P}_\infty$. Entonces

$$\nu_{\mathfrak{P}_\infty}(y^p - y) = \sum_{i=0}^{p-1} \nu_{\mathfrak{P}_\infty}(y - i) = e(\mathfrak{P}_\infty | \mathcal{P}_\infty)\nu_{\mathcal{P}_\infty}(\alpha) = \nu_{\mathfrak{P}_\infty}(\alpha) > 0.$$

Por lo tanto, existe $0 \leq i \leq p-1$ tal que $\nu_{\mathfrak{P}_\infty}(y-i) > 0$. Sin pérdida de generalidad podemos suponer que $i = 0$. Sea $\sigma \in \text{Gal}\,(F/K)\backslash\{\text{Id}\}$. Supongamos que $\mathfrak{P}_\infty^\sigma = \mathfrak{P}_\infty$. Tenemos que $y^\sigma = y - j$, $j \neq 0$. Así, por un lado tenemos

$$\nu_{\mathfrak{P}_\infty}(y - j) = \nu_{\mathfrak{P}_\infty}(y^\sigma) = \nu_{\sigma(\mathfrak{P}_\infty)}(y) = \nu_{\mathfrak{P}_\infty}(y) > 0.$$

Por otro lado, dado que $\nu_{\mathfrak{P}_\infty}(y) > 0 = \nu_{\mathfrak{P}_\infty}(j)$, se sigue que

$$\nu_{\mathfrak{P}_\infty}(y - j) = \text{mín}\{\nu_{\mathfrak{P}_\infty}(y), \nu_{\mathfrak{P}_\infty}(j)\} = 0.$$

Esta contradicción muestra que $\mathfrak{P}_\infty^\sigma \neq \mathfrak{P}_\infty$. Así que $\mathcal{P}_\infty$ se descompone en F/K.

Ahora consideremos el caso $f(T) \neq 0$. Si $f(T) \notin \mathbb{F}_q$, entonces $\mathcal{P}_\infty$ se ramifica pues está en la forma normal descrita por Hasse [4].

El último caso es cuando $f(T) \in \mathbb{F}_q$, $f(T) \notin \wp(\mathbb{F}_q)$. Sea $b \in \mathbb{F}_{q^p}$ con $b^p - b = a = f(T)$. Dado que $\operatorname{gr} \mathcal{P}_\infty = 1$, $\mathcal{P}_\infty$ es inerte en la extensión de constantes $K(b)/K$ (ver [23, Theorem 6.2.1]). Suponiendo que $\mathcal{P}_\infty$ se descompone en $K(y)/K$, tendríamos el siguiente diagrama.

$$\begin{array}{ccc} & K(y) & \xrightarrow[\text{inerte}]{\mathfrak{P}_\infty} K(y,b) \\ \mathcal{P}_\infty \text{ se descompone} \Big| & & \Big| \\ & K & \xrightarrow[\text{inerte}]{\mathcal{P}_\infty} K(b) \end{array}$$

El grupo de descomposición de $\mathcal{P}_\infty$ en $K(y,b)/K$ es el grupo de Galois $\operatorname{Gal}(K(y,b)/K(b))$. Por lo tanto $\mathcal{P}_\infty$ es inerte en cualquier campo de grado p sobre K el cual es diferente al campo $K(y)$. Dado que los campos de grado p son $K(y+ib)$, $K(b)$, $0 \leq i \leq p-1$, en $K(y+b)/K$ tenemos

$$(y+b)^p - (y+b) = (y^p - y) + (b^p - b) = \alpha - a = \frac{Q}{P_1^{e_1}, \ldots, P_r^{e_r}}$$

con $\operatorname{gr}(\alpha - a) < 0$. Por lo tanto, por la primera parte, $\mathcal{P}_\infty$ se descompone en $K(y+b)/K$ y en $K(y)/K$ lo cual es imposible. Así $\mathcal{P}_\infty$ es inerte en $K(y)/K$. □

Ejemplo 1.5. Sean $K = \mathbb{F}_3(T)$ y $F = K(y)$ con $y^3 - y = T$. La extensión F/K es de Artin-Schreier. Tenemos

$$(T)_K = \frac{\mathcal{P}_0}{\mathcal{P}_\infty}.$$

$$\begin{array}{ccc} F = K(y) & & \mathfrak{P}_\infty^2 \\ \Big| & & \Big| \\ {\scriptstyle 3} & & \\ \Big| & & \Big| \\ K = \mathbb{F}_3(T) & & \mathcal{P}_\infty \end{array}$$

El único primo ramificado es $\mathcal{P}_\infty$, es ramificado total y salvajemente. El diferente está dado por

$$\mathfrak{D}_{F/K} = \mathfrak{P}_\infty^4.$$

Ejemplo 1.6. Sean $K = \mathbb{F}_3(T)$ y $F = K(y)$ con $y^3 - y = \frac{1}{T^3-T+1}$. La extensión F/K es de Artin-Schreier. Tenemos

$$\left(\frac{1}{T^3 - T + 1}\right)_K = \frac{\mathcal{P}_\infty^3}{\mathcal{P}}.$$

El lugar $\mathcal{P}$, asociado al polinomio mónico irreducible $P = T^3 - T + 1$, es el único primo ramificado y es total y salvajemente ramificado.
El diferente está dado por

$$\mathfrak{D}_{F/K} = \mathfrak{P}^4.$$

Consideremos los lugares $\mathcal{P}_0, \mathcal{P}_{-1}$, $\mathcal{P}_1$ y $\mathcal{Q}$ correspondientes a los polinomios irreducibles T, $T+1$, $T-1$ y T^2+1, respectivamente. El polinomio $f(X) = X^3 - X - \left(\frac{1}{T^3-T+1}\right)$ es el polinomio mínimo de y. Tenemos que $\bar{f}(X) := f(X)$ mód $\mathcal{P}_i = X^3 - X - 1$ es irreducible en $\mathbb{F}_3(\mathcal{P}_i)[X]$, para $i \in \{0, -1, 1\}$ y $\bar{f}(X) := f(X)$ mód $\mathcal{Q} = X^3 - X - \frac{1}{T+1}$ es irreducible en $\mathbb{F}_3(\mathcal{Q})[X]$. Por el Teorema de Kummer-Dedekind, $\mathcal{P}_0, \mathcal{P}_{-1}$, $\mathcal{P}_1$ y $\mathcal{Q}$ son inertes en la extensión F/K. El primo infinito $\mathcal{P}_\infty$ es totalmente descompuesto en F/K.

$$\begin{array}{ccc} F = K(y) & & \mathfrak{P}^3 \\ \Big| & & \Big| \\ {\scriptstyle 3} & & \\ \Big| & & \Big| \\ K = \mathbb{F}_3(T) & & \mathcal{P} \end{array}$$

Ejemplo 1.7. Sean $K = \mathbb{F}_3(T)$ y $F = K(y)$ con $y^3 - y = T^4 - T^2$. La extensión L/K es de Artin-Schreier. Tenemos

$$(T^4 - T^2)_K = \frac{\mathcal{P}_0^2 \mathcal{P}_{-1} \mathcal{P}_1}{\mathcal{P}_\infty^4}.$$

El lugar $\mathcal{P}_\infty$ es el único primo ramificado y es total y salvajemente ramificado. El diferente está dado por

$$\mathfrak{D}_{F/K} = \mathfrak{P}_\infty^{10}.$$

Consideremos los lugares $\mathcal{P}_0, \mathcal{P}_{-1}$, $\mathcal{P}_1$ y $\mathcal{Q}$, correspondientes a los polinomios irreducibles T, $T+1$, $T-1$ y T^2+1, respectivamente. El polinomio $f(X) = X^3 - X - (T^4 - T^2)$ es el polinomio mínimo de y. Tenemos que $\bar{f}(X) := f(X)$ mód $\mathcal{P}_i = X^3 - X = X(X-1)(X+1)$ es la descomposición de $\bar{f}(X)$ en $\mathbb{F}_3(\mathcal{P}_i)[X]$, para $i \in \{0, -1, 1\}$ y $\bar{f}(X) := f(X)$ mód $\mathcal{Q} = X^3 - X + 1$ es irreducible en $\mathbb{F}_3(\mathcal{Q})[X]$. Por el Teorema de Kummer-Dedekind, $\mathcal{P}_0, \mathcal{P}_{-1}$ y $\mathcal{P}_1$ se descomponen completamente y $\mathcal{Q}$ es inerte en la extensión F/K.
Sea $T' = \frac{1}{T}$. Observamos que $K = \mathbb{F}_3(T) = \mathbb{F}_3(T')$.

$$\begin{array}{ccc} F = K(y) & & \mathfrak{P}_\infty^3 \\ \Big| & & \Big| \\ {\scriptstyle 3} & & \\ \Big| & & \\ K = \mathbb{F}_3(T') & & \mathcal{P}_\infty \end{array}$$

1.4. Vectores de Witt

Sea p un número primo fijo y sea $n \in \mathbb{N}$. Para un vector

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$$

con **componentes usuales** a_m formamos las **componentes fantasmas**

$$a^{(i)} = a_1^{p^{i-1}} + p a_2^{p^{i-2}} + \cdots + p^{i-1} a_i \tag{1.2}$$

y, abusando de la notación, expresamos esta situación de la siguiente manera

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_n | a^{(1)}, a^{(2)}, \ldots, a^{(n)}).$$

Recíprocamente, a_i se puede calcular recursivamente de la ecuación (1.2) como un polinomio con coeficientes racionales en $a^{(1)}, ..., a^{(i)}$. Un vector $\boldsymbol{a}$ está completamente determinado por sus componentes fantasmas.
Las componentes fantasmas se operan término a término y las componentes usuales se calculan a partir del resultado que se obtenga en las componentes fantasmas.
Lo anterior puede precisarse de la siguiente forma. Consideremos tres familias $\{x_i, y_j, z_l\}_{i,j,l=1}^{n}$ donde $n \in \mathbb{N}$, de indeterminadas independientes y consideremos el anillo $R = \mathbb{Q}[x_i, y_j, z_l]_{i,j,l}$. Sea R^n el producto $\underbrace{R \times \cdots \times R}_{n}$.

Denotamos por R^n al anillo que como conjunto base tiene al conjunto R^n y cuyas operaciones son término a término (esto correspondería a las componentes fantasmas) y sea R_n el anillo que como conjunto sigue siendo R^n pero con las siguientes operaciones de Witt: sea $\varphi : R_n \to R^n$ dado por $\varphi(a_1, a_2, \ldots, a_n) = (a^{(1)}, a^{(2)}, \ldots, a^{(n)})$ donde

$$a^{(i)} := a_1^{p^{i-1}} + pa_2^{p^{i-2}} + \cdots + p^{i-1}a_i, \quad i = 1, 2, \ldots, n.$$

Se tiene que φ es un mapeo biyectivo y el inverso $\psi : R^n \to R_n$ está dado por $\psi(a^{(1)}, a^{(2)}, \ldots, a^{(n)}) = (a_1, a_2, \ldots, a_n)$ donde

$$a_i := \frac{1}{p^{i-1}}(a^{(i)} - a_1^{p^{i-1}} - pa_2^{p^{i-2}} - \cdots - p^{i-2}a_{i-1}^{p}), \quad i = 1, 2, \ldots, n.$$

Definimos **la suma, la diferencia y la multiplicación de dos vectores**, componente a componente.

$$\boldsymbol{a} \underset{\times}{\overset{\bullet}{\pm}} \boldsymbol{b} = (?, \ldots, ?|a^{(1)} \underset{\times}{\pm} b^{(1)}, \ldots, a^{(n)} \underset{\times}{\pm} b^{(n)}). \tag{1.3}$$

Esto es, las operaciones $\overset{\bullet}{+}$, $\overset{\bullet}{-}$, $\overset{\bullet}{\times}$ sobre R^n están dadas por

$$\boldsymbol{a} \underset{\times}{\overset{\bullet}{\pm}} \boldsymbol{b} := (\boldsymbol{a}^{\varphi} \underset{\times}{\pm} \boldsymbol{b}^{\varphi})^{\varphi^{-1}} = (\boldsymbol{a}^{\varphi} \underset{\times}{\pm} \boldsymbol{b}^{\varphi})^{\psi} \tag{1.4}$$

En otras palabras, dados dos vectores en R_n, los trasladamos a R^n y ahí los operamos de la manera usual, es decir, componente por componente y el resultado lo volveremos a R_n. Como R^n es conmutativo con identidad, R_n también es conmutativo con identidad. Por ejemplo si $n = 2$, tenemos

$$\boldsymbol{a} = (a_1, a_2|a^{(1)}, a^{(2)}) = (a_1, a_2|a_1, a_1^p + pa_2),$$
$$\boldsymbol{b} = (b_1, b_2|b^{(1)}, b^{(2)}) = (b_1, b_2|b_1, b_1^p + pb_2),$$

se tiene que

$$\begin{aligned}\boldsymbol{c} = \boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b} &= (c_1, c_2 | c^{(1)}, c^{(2)}) = (c_1, c_2 | c_1, c_1^p + pc_2) \\ &= (?, ? | a_1 + b_1, a_1^p + pa_2 + b_1^p + pb_2).\end{aligned}$$

Esto es $c_1 = a_1 + b_1$, $c_1^p + pc_2 = a_1^p + pa_2 + b_1^p + pb_2$. Luego

$$\begin{aligned}c_2 &= \frac{1}{p}(a_1^p + pa_2 + b_1^p + pb_2 - (a_1 + b_1)^p) \\ &= \frac{1}{p}(pa_2 + pb_2 - \sum_{i=1}^{p-1} \binom{p}{i} a_1^i b_1^{p-i}) \\ &= a_2 + b_2 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} a_1^i b_1^{p-i}.\end{aligned}$$

Por lo tanto

$$\begin{aligned}&\boldsymbol{c} = \boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b} \\ =&(a_1 + b_1, a_2 + b_2 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} a_1^i b_1^{p-i} | a_1 + b_1, a_1^p + pa_2 + b_1^p + pb_2).\end{aligned}$$

Usaremos

$$\boldsymbol{a}^p = (a_1^p, a_2^p, \ldots, a_n^p). \tag{1.5}$$

Nótese que $\boldsymbol{a}^p$ no es la p-ésima potencia en el sentido de multiplicación de vectores.
Nuevamente abusando de la notación, usaremos $(\boldsymbol{a})^{(i)}$ para denotar lo mismo que $a^{(i)}$, a saber, la i-ésima componente fantasma del vector $\boldsymbol{a}$. Similarmente, usaremos $(\boldsymbol{a})_i$ para denotar a_i, la i-ésima componente de $\boldsymbol{a}$.

Ejemplo 1.8. Aquí vemos el caso $n = 2$, $p = 3$, $\boldsymbol{a} = (a_1, a_2)$ y $\boldsymbol{b} = (b_1, b_2)$. Tenemos que

$$\begin{aligned}(\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_1 &= a_1 + b_1 \\ (\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_2 &= a_2 + b_2 - a_1 b_1 (a_1 + b_1)\end{aligned}$$

y

$$\begin{aligned}(\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_1 &= a_1 b_1 \\ (\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_2 &= a_1^3 b_2 + a_2 b_1^3 + 3a_2 b_2.\end{aligned}$$

Para cuando $\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b} = (0,0)$, $a_1 + b_1 = 0$, $a_1 = -b_1$ y $a_2 = -b_2 - b_1^2$ por lo que

$$\overset{\bullet}{-}\boldsymbol{b} = (-b_1, -b_2),$$

luego

$$\boldsymbol{a} \overset{\bullet}{-} \boldsymbol{b} = (a_1 - b_1, a_2 - b_2 + a_1 b_1 (a_1 - b_1)),$$

de donde, si $\boldsymbol{b}^3 = (b_1^3, b_2^3)$, tenemos

$$\boldsymbol{b}^3 \overset{\bullet}{-} \boldsymbol{b} = (b_1^3 - b_1, b_2^3 - b_2 + b_1^7 - b_1^5).$$

Ejemplo 1.9. Para $n = 2$ y $p = 2$, tenemos que

$$\begin{aligned} \boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b} &= (a_1 + b_1,\ a_2 + b_2 - a_1 b_1), \\ \overset{\bullet}{-}\boldsymbol{b} &= (-b_1,\ -b_2 - b_1^2), \\ \boldsymbol{b}^2 \overset{\bullet}{-} \boldsymbol{b} &= (b_1^2 - b_1,\ b_2^2 - b_2 - b_1^2 + b_1^3). \end{aligned}$$

Si $\overset{\bullet}{\underset{\times}{\pm}}$ denota a $\overset{\bullet}{+}$, $\overset{\bullet}{-}$ ó $\overset{\bullet}{\times}$, entonces $(a \overset{\bullet}{\underset{\times}{\pm}} b)_i$ es un polinomio con coeficientes enteros en las variables $a_1, b_1, a_2, b_2, \ldots, a_i, b_i$. Denotemos

$$\begin{aligned} (\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_i &= s_i(a_1, b_1, \ldots, a_i, b_i) \quad \text{y} \\ (\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_i &= m_i(a_1, b_1, \ldots, a_i, b_i), \end{aligned}$$

para cada $i \in \{1, 2, \ldots, n\}$.

Sea $\mathfrak{A}$ una álgebra conmutativa sobre el campo finito $\mathbb{F}_p$. Sea

$$W_n(\mathfrak{A}) = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in \mathfrak{A}, i = 1, 2, \ldots, n\}.$$

Si $\boldsymbol{a}, \boldsymbol{b} \in W_n(\mathfrak{A})$, con $\boldsymbol{a} = (a_1, a_2, \ldots, a_n)$ y $\boldsymbol{b} = (b_1, b_2, \ldots, b_n)$, entonces

$$\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b} = ((\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_1, (\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_2, \ldots, (\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_n),$$

con

$$(\boldsymbol{a} \overset{\bullet}{+} \boldsymbol{b})_i = \bar{s}_i(a_1, b_1, \ldots, a_i, b_i),$$

donde

$$\bar{s}_i(a_1, b_1, \ldots, a_i, b_i) = s_i(a_1, b_1, \ldots, a_i, b_i) \text{ mód } p$$

y

$$\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b} = ((\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_1, (\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_2, \ldots, (\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_n),$$

con

$$(\boldsymbol{a} \overset{\bullet}{\times} \boldsymbol{b})_i = \bar{m}_i(a_1, b_1, \ldots, a_i, b_i),$$

donde

$$\bar{m}_i(a_1, b_1, \ldots, a_i, b_i) = m_i(a_1, b_1, \ldots, a_i, b_i) \text{ mód } p.$$

Tenemos que $W_n(\mathfrak{A})$ es un anillo conmutativo, llamado el anillo de vectores de Witt de longitud n sobre $\mathfrak{A}$.

Ejemplo 1.10. Consideramos elementos de $W_2(K)$, donde $K = \mathbb{F}_3(T)$. De acuerdo con las reglas transformamos las componentes usuales en componentes fantasmas, operamos normalmente y regresamos a las componentes usuales. Tenemos

$$\begin{array}{llll} a^{(1)} & = a_1 & a_1 & = a^{(1)} \\ a^{(2)} & = a_1^3 + 3a_2 & a_2 & = \frac{1}{3}(a^{(2)} - a_1^3). \end{array}$$

Obtengamos $\left(0, \dfrac{1}{T}\right) \overset{\bullet}{+} \left(\dfrac{-1}{T-1}, 0\right) \overset{\bullet}{+} \left(\dfrac{1}{T+1}, 0\right)$.

$$\begin{array}{ccc} \text{Usuales} & & \text{Fantasmas} \\ \left(0, \dfrac{1}{T}\right) & \mapsto & \left(0, \dfrac{3}{T}\right), \\ \left(\dfrac{-1}{T-1}, 0\right) & \mapsto & \left(\dfrac{-1}{T-1}, \dfrac{-1}{(T-1)^3}\right), \\ \left(\dfrac{1}{T+1}, 0\right) & \mapsto & \left(\dfrac{1}{T+1}, \dfrac{1}{(T+1)^3}\right). \end{array}$$

$$\begin{array}{l} \text{Fantasmas} \\ \left(0, \dfrac{3}{T}\right) + \left(\dfrac{-1}{T-1}, \dfrac{-1}{(T-1)^3}\right) + \left(\dfrac{1}{T+1}, \dfrac{1}{(T+1)^3}\right) \\ \qquad = \left(\dfrac{-1}{T-1} + \dfrac{1}{T+1}, \dfrac{3}{T} + \dfrac{-1}{(T-1)^3} + \dfrac{1}{(T+1)^3}\right) \\ \qquad = \left(\dfrac{-2}{T^2-1}, \dfrac{3T^6 - 9T^4 - 6T^3 + 9T^2 - 2T - 3}{T(T^2-1)^3}\right). \end{array}$$

$$\begin{aligned}
&\text{Usuales}\\
\left(0,\frac{1}{T}\right) &\overset{\bullet}{+} \left(\frac{-1}{T-1},0\right) \overset{\bullet}{+} \left(\frac{1}{T+1},0\right) = \left(\frac{-2}{T^2-1},\right.\\
&\left.\frac{1}{3}\left(\frac{3T^6-9T^4-6T^3+9T^2-2T-3}{T(T^2-1)^3}\right)-\left(-\frac{2}{(T^2-1)^3}\right)\right)\\
&= \left(\frac{-2}{T^2-1},\frac{T^6-3T^4-2T^3+3T^2+2T-1}{T(T^2-1)^3}\right)\\
&= \left(\frac{1}{T^2-1},\frac{T^6+T^3-T-1}{T(T^2-1)^3}\right).
\end{aligned}$$

1.5. Extensiones Cíclicas y Vectores de Witt

Sea E un campo arbitrario de característica p. Queremos obtener extensiones cíclicas de grado p^n sobre E. Estas extensiones son análogas a las extensiones cíclicas de Kummer y también son una generalización de las de Artin-Schreier. Del mismo modo que se introdujo la notación $\wp a = a^p - a$ para ser usada en las extensiones de Artin-Schreier, introducimos la siguiente para los vectores de Witt

$$\wp \boldsymbol{a} = \boldsymbol{a}^p \overset{\bullet}{-} \boldsymbol{a} = (a_1^p,\ldots,a_n^p) \overset{\bullet}{-} (a_1,\ldots,a_n).$$

Tenemos el siguiente resultado que vincula a los vectores de Witt con las extensiones cíclicas de grado p^n de un campo de característica p. Como referencias ver [26, Satz 13] y [13, Teoremas 1.2.2 y 1.2.3 y Corolario 1.2.1].

Teorema 1.6. *Sean E un campo de característica $p>0$, $n\geq 1$ un entero y F/E una extensión algebraica de campos. Entonces F/E es una extensión cíclica de grado p^n si y sólo si existen $y_1,y_2,\ldots,y_n \in F$ tales que $F = E(y_1,y_2,\ldots,y_n)$ y $\boldsymbol{y}=(y_1,\ldots,y_n)\in W_n(F)$ satisface $\boldsymbol{y}^p \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta}$, con $\boldsymbol{\beta} = (\beta_1,\beta_2,\ldots,\beta_n)\in W_n(E)$ y $\beta_1 \neq b^p - b$, para todo $b\in E$.* □

1.6. Un resultado auxiliar

El siguiente resultado nos será de utilidad tanto en el estudio de las extensiones de Artin-Schreier, en el Capítulo 2, como en el caso de extensiones

cíclicas de grado p^n, donde p es la característica de los campos, las cuales se tratan en el Capítulo 3.

Denotamos por $[x]$ a la parte entera del número real x y por $\lceil x \rceil$ al techo de x, esto es, el mínimo entero mayor o igual que x.

Lema 1.7. *Sean $\alpha \in \mathbb{Z}$, p un número primo y $s \in \mathbb{N}$. Se cumple:*

(a) $\left[\frac{\left[\frac{\alpha}{p^s}\right]}{p}\right] = \left[\frac{\left[\frac{\alpha}{p}\right]}{p^s}\right] = \left[\frac{\alpha}{p^{s+1}}\right]$.

(b) $\left\lceil \frac{\alpha}{p^s} \right\rceil = \left[\frac{\alpha-1}{p^s}\right] + 1$.

Demostración. (a) Primero probamos $\left[\frac{\left[\frac{\alpha}{p^s}\right]}{p}\right] = \left[\frac{\alpha}{p^{s+1}}\right]$. En efecto, para el caso cuando $s = 0$ se cumple la igualdad. Ahora, sea $\alpha = tp^{s+1} + r$ con $0 \leq r \leq p^{s+1}-1$, donde $r = lp^s + r'$ con $0 \leq r' \leq p^s - 1$. Note que $0 \leq l \leq p-1$. De donde $\left[\frac{\alpha}{p^s}\right] = tp + l$, y $\frac{\left[\frac{\alpha}{p^s}\right]}{p} = t + \frac{l}{p}$, $0 \leq l \leq p-1$. Por lo que se tiene $\left[\frac{\left[\frac{\alpha}{p^s}\right]}{p}\right] = t = \left[\frac{\alpha}{p^{s+1}}\right]$. Ahora, probaremos la otra igualdad $\left[\frac{\left[\frac{\alpha}{p^s}\right]}{p}\right] = \left[\frac{\left[\frac{\alpha}{p}\right]}{p^s}\right]$. Para cuando $s = 0$ ó $s = 1$ se tiene el resultado. Ahora, sea $\alpha = mp + r''$ donde $0 \leq r'' \leq p-1$. Tenemos $\left[\frac{\alpha}{p}\right] = m$, y $m = hp^s + r'''$ con $0 \leq r''' \leq p^s - 1$, luego $\left[\frac{\left[\frac{\alpha}{p}\right]}{p^s}\right] = h$. Por otro lado, tenemos $\alpha = (hp^s + r''')p + r'' = hp^{s+1} + r'''p + r''$ con $0 \leq r'''p + r'' \leq p^{s+1} - p + p + 1 = p^{s+1} - 1$, lo cual implica que $\left[\frac{\alpha}{p^{s+1}}\right] = h$. Para probar (b) consideramos $\alpha - 1 = p^s q + r$, donde $0 \leq r \leq p^s - 1$, por lo que $1 \leq r + 1 \leq p^s$ y $\alpha = p^s q + r + 1$. Luego, cuando $r + 1 < p^s$, se sigue $\left[\frac{\alpha - 1}{p^s}\right] = q$ y $\left\lceil \frac{\alpha}{p^s} \right\rceil = q + 1$, lo cual se quería probar. Y en el caso cuando $r + 1 = p^s$, $\alpha = p^s q + r + 1 = p^s q + p^s = p^s(q + 1)$ luego $\left[\frac{\alpha-1}{p^s}\right] = q$ y $\left\lceil \frac{\alpha}{p^s} \right\rceil = q + 1$, de donde se sigue el resultado. □

Capítulo 2

Extensiones cuadráticas y de Artin-Schreier

En este capítulo estudiaremos extensiones cuadráticas y extensiones de Artin-Schreier. Estos son casos particulares del resultado general, pero los incluimos ya que son útiles como ejemplos concretos del caso general. Las extensiones cuadráticas moderadamente ramificadas son un tipo de extensiones cíclicas de Kummer. Dejamos al final las extensiones cuadráticas en general puesto que las extensiones cuadráticas salvajemente ramificadas son un caso particular de las extensiones de Artin-Schreier.

2.1. Extensiones cuadráticas moderadamente ramificadas

Dado que estamos considerando extensiones moderadamente ramificadas, en esta sección se supone que la característica p de los campos es diferente de 2. Necesitamos algunos lemas.

Lema 2.1. *Sea $K = \mathbb{F}_q(T)$, donde $\mathbb{F}_q$ es el campo finito con q elementos, q impar. Sea F/K una extensión cuadrática. Entonces $F = K(\sqrt{M})$, donde $M = \alpha \prod_{i=1}^{r} P_i$ es un polinomio no cero libre de cuadrado, $\alpha \in \mathbb{F}_q^*$, $P_i \in R_T^+$ es un polinomio mónico irreducible para $i \in \{1, ..., r\}$ con $P_i \neq P_j$ para $i \neq j$.*

Demostración. Puesto que la característica de K es diferente de 2, $F = K(y)$, donde y satisface $y^2 + b_1 y + b_0 = 0$, para algunos b_0, $b_1 \in K$, lue-

go $y = \dfrac{-b_1 \pm \sqrt{b_1^2 - 4b_0}}{2}$, por tanto $F = K(\sqrt{b_1^2 - 4b_0}) = K\left(\sqrt{\dfrac{f(T)}{g(T)}}\right) = K(\sqrt{f(T)g(T)}) = K(\sqrt{M})$, donde M es un polinomio no cero libre de cuadrado, $M = \alpha \prod_{i=1}^{r} P_i$, $\alpha \in \mathbb{F}_q^*$, $P_i \in R_T^+$ es un polinomio mónico irreducible para $i \in \{1, ..., r\}$ con $P_i \neq P_j$ para $i \neq j$. □

Lema 2.2. *Sean $K = \mathbb{F}_q(T)$ con q impar y $P \in R_T^+$ polinomio mónico e irreducible de grado d. Entonces:*

(*a*) *Para d par se tiene $K(\sqrt{P}) \subseteq K(\Lambda_P)$,*

(*b*) *Para d impar se cumple $K(\sqrt{-P}) \subseteq K(\Lambda_P)$.*

Demostración. Como q es impar, existe $l \in \mathbb{N}$ tal que $q - 1 = 2l$. Por [16, Exercise 5, página 303] tenemos dos casos:

(*a*) Para d par tenemos $K(\sqrt[q-1]{P}) \subseteq K(\Lambda_P)$, entonces $P^{\frac{1}{2}} = P^{\frac{l}{q-1}} = \left(P^{\frac{1}{q-1}}\right)^l$, luego $K(\sqrt{P}) \subseteq K(\Lambda_P)$.

(*b*) Para d impar tenemos $K(\sqrt[q-1]{-P}) \subseteq K(\Lambda_P)$, luego $(-P)^{\frac{1}{2}} = (-P)^{\frac{l}{q-1}} = \left((-P)^{\frac{1}{q-1}}\right)^l$, por lo que $K(\sqrt{-P}) \subseteq K(\Lambda_P)$. □

Lema 2.3. *Sean $K = \mathbb{F}_q(T)$ con q impar y $P \in R_T^+$ polinomio mónico e irreducible de grado d. Entonces se cumple*

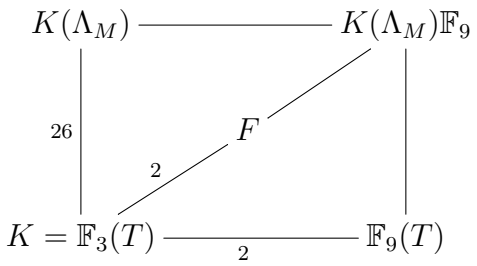
$$K(\sqrt{P}) \subseteq K(\Lambda_P)\mathbb{F}_{q^2}.$$

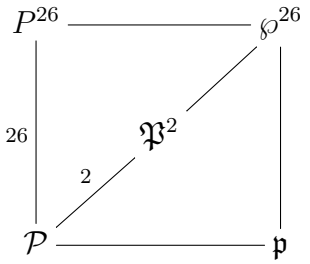
Demostración. Para el caso cuando d es impar, tenemos $K(\sqrt{P}) = K(\sqrt{-1}\sqrt{-P}) \subseteq K(\sqrt{-1}, \sqrt{-P}) = K(\sqrt{-1})K(\sqrt{-P}) \subseteq K\mathbb{F}_{q^2} \cdot K(\Lambda_P) = K(\Lambda_P)\mathbb{F}_{q^2}$ y para cuando d es par tenemos $K(\sqrt{P}) \subseteq K(\Lambda_P) \subseteq K(\Lambda_P)\mathbb{F}_{q^2}$. □

Proposición 2.4. *Sea $K = \mathbb{F}_q(T)$, donde q es impar. Sea F/K una extensión cuadrática. Entonces $F = K(\sqrt{M}) \subseteq K(\Lambda_M)\mathbb{F}_{q^2}$, donde $M = \alpha \prod_{i=1}^{r} P_i$ es un polinomio no cero libre de cuadrado, $\alpha \in \mathbb{F}_q^*$, $P_i \in R_T^+$ es un polinomio mónico e irreducible para $i \in \{1, ..., r\}$ con $P_i \neq P_j$ para $i \neq j$.*

Demostración. Por los Lemas 2.1 y 2.3 existe $M = \alpha \prod_{i=1}^{r} P_i$ polinomio no cero libre de cuadrado, donde $\alpha \in \mathbb{F}_q^*$, $P_i \in R_T^+$ es un polinomio mónico irreducible para $i \in \{1, ..., r\}$ con $P_i \neq P_j$ para $i \neq j$, tal que $F = K(\sqrt{M})$. Se tiene $\mathbb{F}_q(\sqrt{\alpha}) \subseteq \mathbb{F}_{q^2}$. Tomando $\sqrt{M} = \sqrt{\alpha}\sqrt{P_1} \cdots \sqrt{P_r} \in \mathbb{F}_{q^2} K(\sqrt{P_1}) K(\sqrt{P_2}) \cdots K(\sqrt{P_r})$ el cual está contenido en $K(\Lambda_{P_1}) \cdots K(\Lambda_{P_r})\mathbb{F}_{q^2} = K(\Lambda_{P_1 \cdots P_r})\mathbb{F}_{q^2} = K(\Lambda_{\alpha P_1 \cdots P_r})\mathbb{F}_{q^2} = K(\Lambda_M)\mathbb{F}_{q^2}$, luego $F = K(\sqrt{M}) \subseteq K(\Lambda_M)\mathbb{F}_{q^2}$. □

Ejemplo 2.1. Viene de los Ejemplos 1.1 y 1.4. Sean $K = \mathbb{F}_3(T)$, $F = K(y)$ con $y^2 = T^3 - T + 1$. El polinomio $M = T^3 - T + 1$ es irreducible módulo 3. La extensión F/K es de Kummer cuadrática, luego por la Proposición 2.4 tenemos $F \subseteq K(\Lambda_M)\mathbb{F}_9$.





2.2. Extensiones de Artin-Schreier

En esta sección se dará una prueba tipo combinatoria de que cualquier extensión de Artin-Schreier de un campo funciones racionales congruente está contenido en el compuesto de un campo de funciones ciclotómico y una extensión de campo de constantes que se describirán explícitamente.

La demostración se hará como sigue: primero consideraremos extensiones de Artin-Schreier con un único primo ramificado. Calcularemos el número de tales extensiones cuyo conductor es un divisor de una potencia dada del primo ramificado. Después, probaremos que este número es el mismo que el número de extensiones de Artin-Schreier contenidas en el compuesto de un campo de funciones ciclotómico generado por la misma potencia del primo ramificado y una extensión de constantes de grado p. Finalmente, el caso general se sigue inmediatamente de este caso usando la descomposición de una función racional en fracciones parciales.

La siguiente proposición presenta las diferentes formas de generar una extensión de Artin-Schreier.

Proposición 2.5. *Sea $p > 0$ la característica de E y sean $F_1 = E(y)$, $F_2 = E(z)$, extensiones cíclicas de grado p sobre E dadas por $y^p - y = a_1 \in E$, $z^p - z = a_2 \in E$. Entonces los siguientes enunciados son equivalentes:*

(*a*) $F_1 = F_2$.

(*b*) $z = jy + b$ *para* $1 \leq j \leq p-1$ *y* $b \in E$.

(*c*) $a_2 = ja_1 + (b^p - b)$ *para* $1 \leq j \leq p-1$ *y* $b \in E$.

Demostración. Ver [23, Proposition 5.8.6]. □

Ahora consideremos extensiones de Artin-Schreier donde precisamente un divisor primo se ramifica. Primero tratemos el caso cuando el divisor corresponde al polinomio mónico e irreducible P.

Proposición 2.6. *Sean $K = \mathbb{F}_q(T)$, $q = p^t$, $P \in R_T^+$, $d = \operatorname{gr} P$, $F_1 = K(y)$, donde*

$$y^p - y = \frac{f(T)}{P^\alpha},$$

$f(T) \in R_T, \operatorname{gr} f(T) \leq d\alpha$, $(f(T), P) = 1$, $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$, $\alpha_0 := \left[\frac{\alpha}{p}\right]$, *la parte entera de* $\frac{\alpha}{p}$ *y* $F_2 = K(z)$, *donde*

$$z^p - z = \frac{g(T)}{P^\alpha},$$

$g(T) \in R_T, \operatorname{gr} g(T) \leq d\alpha$, $(g(T), P) = 1$. *Tenemos que los siguientes enunciados son equivalentes:*

(a) $F_1 = F_2$.

(b) $z = jy + c$, *donde* $j \in \{1, ..., p-1\}$, $c = \dfrac{h(T)}{P^{\alpha_0}}$ *con* $h(T) \in R_T$, *donde* $h(T) = 0$ *o* $\operatorname{gr} h(T) \leq d\alpha_0$.

(c) $\dfrac{g(T)}{P^\alpha} = j\dfrac{f(T)}{P^\alpha} + c^p - c$, *donde* $j \in \{1, ..., p-1\}$, $c = \dfrac{h(T)}{P^{\alpha_0}}$ *con* $h(T) \in R_T$, *donde* $h(T) = 0$ *o* $\operatorname{gr} h(T) \leq d\alpha_0$.

Demostración. Las equivalencias se siguen de la Proposición 2.5. Verifiquemos las condiciones que debe cumplir c.

Sea $Q \in R_T^+$, $P \neq Q$. Tenemos $\nu_Q(c) \geq 0$ pues si $\nu_Q(c) < 0$ tendríamos

$$\begin{aligned} 0 \leq \nu_Q\left(\frac{g(T)}{P^\alpha}\right) &= \nu_Q\left(j\frac{f(T)}{P^\alpha} + c^p - c\right) \\ &= \min\left\{\nu_Q\left(\frac{f(T)}{P^\alpha}\right), p\nu_Q(c), \nu_Q(c)\right\} = p\nu_Q(c) < 0, \end{aligned}$$

lo cual es una contradicción. Análogamente, se tiene $\nu_\infty(c) \geq 0$. Finalmente, tenemos $c = 0$ ó $\nu_P(c) \leq 0$ pues $\nu_P(c) > 0$ implica $0 \geq \operatorname{gr}(c) = \sum_{Q \in \mathcal{P}_K} \nu_Q(c) > 0$, lo cual es una contradicción.
Por lo tanto, tenemos las siguientes posibilidades:

(*i*) $c = 0$.

(*ii*) $c \neq 0$, $\nu_P(c) = 0$, lo cual implica $c \in \mathbb{F}_q^*$.

(*iii*) Si $\nu_P(c) < 0$, sea $\gamma := -\nu_P(c)$. Dado que $(\alpha, p) = 1$, tenemos $\nu_P(c^p - c) = \min\{p\nu_P(c), \nu_P(c)\} = -p\gamma \neq -\alpha$. Luego

$$\begin{aligned} -\alpha = \nu_P\left(\frac{g(T)}{P^\alpha}\right) &= \nu_P\left(j\frac{f(T)}{P^\alpha} + c^p - c\right) \\ &= \min\left\{\nu_P\left(j\frac{f(T)}{P^\alpha}\right), \nu_P(c^p - c)\right\} = \min\{-\alpha, -p\gamma\}. \end{aligned}$$

Lo cual implica $-\alpha < -p\gamma$, luego $p\gamma < \alpha$. Por lo tanto $\gamma < \dfrac{\alpha}{p}$. Así $\gamma \leq \alpha_0 = \left[\dfrac{\alpha}{p}\right]$, luego $c = \dfrac{h_1(T)}{P^\gamma}$ con $h_1(T) \in \mathbb{F}_q[T]$, $(h_1(T), P) = 1$, $\operatorname{gr} h_1(T) \leq d\gamma$ y $\gamma \leq \alpha_0$, lo cual implica que $c = \dfrac{h_1(T)P^{\alpha_0-\gamma}}{P^{\alpha_0}}$.

En los primeros dos casos, ponemos $h(T) = cP^{\alpha_0}$ y en el tercero $h(T) = h_1(T)P^{\alpha_0-\gamma}$.

Concluimos que $c = \dfrac{h(T)}{P^{\alpha_0}}$ con $h(T) = 0$ ó $\operatorname{gr} h(T) \leq d\alpha_0$. □

Corolario 2.7. *Sean $K = \mathbb{F}_q(T)$, $q = p^t$, $P \in R_T^+$, $d = \operatorname{gr} P$. Sea $F = K(y)$ una extensión de Artin-Schreier dada en forma normal, esto es,*

$$y^p - y = \frac{f(T)}{P^\alpha},$$

donde $f(T) \in R_T, \operatorname{gr} f(T) \leq d\alpha$, $(f(T), P) = 1$, $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$, $\alpha_0 = \left[\dfrac{\alpha}{p}\right]$. Entonces hay $(p-1)q^{(d\alpha_0+1)}$ elementos $z \in F$ tales que $F = K(z)$ está también dada en forma normal

$$z^p - z = \frac{g(T)}{P^\alpha}. \tag{2.1}$$

Además, estos elementos z están dados por $z = jy + c$, donde $1 \leq j \leq p-1$ y $c = \dfrac{h(T)}{P^{\alpha_0}}$, con $h(T) \in R_T$, $\operatorname{gr} h(T) \leq d\alpha_0$.

Aún más, hay

$$\frac{p-1}{p}q^{(d\alpha_0+1)}$$

distintas ecuaciones de la forma (2.1) con $g(T) \in R_T$, $\operatorname{gr} g(T) \leq d\alpha$, $(g(T), P) = 1$, de manera que z es como se indica arriba y además $\dfrac{g(T)}{P^\alpha} = j\dfrac{f(T)}{P^\alpha} + c^p - c$.

Demostración. Por la Proposición 2.6 el número de posibilidades para j es $p-1$ y el número de posibilidades para $h(T)$ es $q^{(d\alpha_0+1)}$, así, el número de posibles z es $(p-1)q^{(d\alpha_0+1)}$. Para obtener el número de posibles ecuaciones,

sólo basta observar que $c^p - c = d^p - d$ si y sólo si $(c-d)^p = c - d$ si y sólo si $c - d \in \mathbb{F}_p$. □

Corolario 2.8. *Sean $K = \mathbb{F}_q(T)$, $q = p^t$, $P \in R_T^+$. Entonces el número de diferentes extensiones de Artin-Schreier $F = K(y)$, donde*

$$y^p - y = \frac{f(T)}{P^\alpha}$$

con $f(T) \in R_T, \operatorname{gr} f(T) \leq d\alpha$, $(f(T), P) = 1$, $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$, es

$$N_\alpha := \frac{p}{p-1}\Phi\left(P^{\alpha-\alpha_0}\right),$$

donde $\alpha_0 = \left[\frac{\alpha}{p}\right]$.

Demostración. Por el Algoritmo de la División tenemos que $f(T) = aP^\alpha + h(T)$, donde $a \in \mathbb{F}_q$, $h(T) \in R_T$, con $\operatorname{gr} h(T) \leq d\alpha - 1$ y $(h(T), P) = 1$ ó bien $h(T) = 0$. Luego $y^p - y = a + \frac{h(T)}{P^\alpha}$. El número de ecuaciones de este tipo es

$$q\Phi(P^\alpha) = q \cdot q^{(\alpha-1)d}(q^d - 1).$$

Por el Corolario 2.7 tenemos que hay

$$N_\alpha = \frac{q \cdot q^{(\alpha-1)d}(q^d-1)}{\frac{p-1}{p}q^{(d\alpha_0+1)}} = \frac{p}{p-1}q^{(\alpha-\alpha_0-1)d}(q^d-1) = \frac{p}{p-1}\Phi(P^{\alpha-\alpha_0})$$

distintas extensiones cíclicas F de grado p sobre K en las que P es el único primo ramificado y aparece a la potencia α en la ecuación de Artin-Schreier en su forma normal. □

Lema 2.9. *Sean $K = \mathbb{F}_q(T)$, p un número primo, $q = p^t$, $P \in R_T^+$, $d = \operatorname{gr} P$ y $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$.*

(a) Sea $F = K(y)$, donde

$$y^p - y = \frac{f(T)}{P^\alpha}$$

con $f(T) \in R_T$, $\operatorname{gr} f(T) \leq \alpha d$, y $(f(T), P) = 1$.

Suponemos $F \subseteq K(\Lambda_M)$ *para algún* $M \in R_T \setminus \{0\}$. *Entonces* $F \subseteq K(\Lambda_{P^{\alpha+1}})$ *pero* $F \nsubseteq K(\Lambda_{P^\alpha})$.

(*b*) *Recíprocamente, si* F/K *es una extensión de Artin-Schreier tal que* $F \subseteq K(\Lambda_{P^{\alpha+1}})$ *pero* $F \nsubseteq K(\Lambda_{P^\alpha})$, *entonces* $F = K(y)$, *donde*

$$y^p - y = \frac{f(T)}{P^\alpha}$$

con $f(T) \in R_T$, $\operatorname{gr} f(T) \leq \alpha d$ *y* $(f(T), P) = 1$.

Demostración. (*a*) Tenemos que $\mathcal{P}$, el divisor primo asociado al polinomio P, es el único divisor primo ramificado en F/K y el diferente de F/K es

$$\mathfrak{D}_{F/K} = \mathfrak{P}^{(\alpha+1)(p-1)},$$

donde $\mathfrak{P}$ es el único divisor primo en F que divide a $\mathcal{P}$. Entonces el discriminante de F/K es

$$\delta_{F/K} = \mathcal{P}^{(\alpha+1)(p-1)}.$$

Puesto que F está contenido en un campo ciclotómico y la extensión F/K es cíclica, F es el campo asociado a algún caracter Θ de orden p y de conductor $\mathfrak{F}_\Theta$ (ver [23, Chapter 12]).
Por la Fórmula del Conductor-Discriminante (ver [21, página 104]) tenemos que

$$\delta_{F/K} = \prod_{\varphi \in \langle \Theta \rangle} \mathfrak{F}_\varphi = \mathfrak{F}_{\Theta^0} \mathfrak{F}_{\Theta^1} \cdots \mathfrak{F}_{\Theta^{p-1}} = \mathfrak{F}_\Theta^{p-1}.$$

Luego $\mathcal{P}^{(\alpha+1)(p-1)} = \mathfrak{F}_\Theta^{p-1}$, por lo que $\mathfrak{F}_\Theta = \mathcal{P}^{(\alpha+1)}$. De donde concluimos que $F \subseteq K(\Lambda_{P^{\alpha+1}})$ pero $F \nsubseteq K(\Lambda_{P^\alpha})$ (ver [23, Chapter 12]).

(*b*) Dado que $F \subseteq K(\Lambda_{P^{\alpha+1}})$, $\mathcal{P}$ es el único divisor primo ramificado en F/K. Entonces $F = K(y)$, donde

$$y^p - y = \frac{f(T)}{P^\beta}$$

con $f(T) \in R_T$, $\operatorname{gr} f(T) \leq \beta d$, y $(f(T), P) = 1$. Se sigue de (*a*) que $\beta = \alpha$. $\square$

Proposición 2.10. *Sean* $K = \mathbb{F}_q(T)$, $q = p^t$, $P \in R_T^+$, $d =$ gr P, $\beta \in \mathbb{N}$ *y* $\beta \geq 2$. *Entonces el número de extensiones de Artin-Schreier contenidas en el campo ciclotómico* $K(\Lambda_{P^\beta})$ *es*

$$\mathcal{N}_\beta := \frac{q^{\left(\beta - \lceil \frac{\beta}{p} \rceil\right)d} - 1}{p-1}.$$

Demostración. Puesto que la red de subgrupos de un grupo abeliano es simétrica, por Teoría de Galois tenemos que $\mathcal{N}_\beta$, que es igual al número de subgrupos de grado p, también es igual al número de subgrupos de orden p del grupo de Galois $\left(R_T/P^\beta\right)^*$ de la extensión $K(\Lambda_{P^\beta})/K$. Sea r_p el número de elementos de orden p en $\left(R_T/P^\beta\right)^*$. Consideramos la sucesión exacta

$$1 \longrightarrow D_{P^\beta,P} \longrightarrow \left(R_T/P^\beta\right)^* \longrightarrow (R_T/P)^* \longrightarrow 1\ .$$

$$A \text{ mód } P^\beta \longmapsto A \text{ mód } P.$$

Puesto que los órdenes de $D_{P^\beta,P}$ y $(R_T/P)^*$ son primos relativos, tenemos

$$\left(R_T/P^\beta\right)^* \cong D_{P^\beta,P} \times (R_T/P)^*.$$

Tenemos $D_{P^\beta,P} = \{A \text{ mód } P^\beta | A \equiv 1 \text{ mód } P\} = \{A \text{ mód } P^\beta | A = 1 + h(T)P,$ donde $h(T) \in R_T$ y gr $h(T) \leq (\beta-1)d - 1\}$.
Observemos que $|D_{P^\beta,P}| = q^{(\beta-1)d}$. También notemos que A mód $P^\beta \equiv 1$ mód P^β si y sólo si $h(T) = 0$. Por lo que A mód P^β es de orden p si y sólo si $h(T) \neq 0$ y $(1+h(T)P)^p = 1 + h(T)^p P^p \equiv 1$ mód P^β si y sólo si $P^\beta | h(T)^p P^p$. Tenemos dos casos:

(*i*) Si $\beta \leq p$, lo anterior se cumple para todo A mód $\left(R_T/P^\beta\right)^* \in D_{P^\beta,P}$ y así $r_p = q^{(\beta-1)d} - 1$.

(*ii*) Si $\beta > p$, tenemos $P^\beta g(T) = h(T)^p P^p$, para algún $g(T) \in R_T$. Luego $P^{\beta-p} g(T) = h(T)^p$. Así $h(T) = P^\gamma h_1(T)$ para algún $\gamma \in \mathbb{N}$ y $h_1(T) \in R_T$ con $(h_1(T), P) = 1$. Tenemos $P^{\beta-p} g(T) = P^{\gamma p} h_1(T)^p$. Luego $\gamma p \geq \beta - p$,

$\gamma \geq \dfrac{\beta}{p} - 1$, $\gamma + 1 \geq \dfrac{\beta}{p}$. Así, $\gamma + 1 \geq \left\lceil \dfrac{\beta}{p} \right\rceil$. Por lo tanto $h(T) = P^{\left(\left\lceil \frac{\beta}{p} \right\rceil - 1\right)} h_2(T)$, donde

$$\begin{aligned} \operatorname{gr} h_2(T) &= \operatorname{gr} h(T) - \left(\left\lceil \frac{\beta}{p} \right\rceil - 1 \right) d \\ &\leq (\beta - 1)d - 1 - \left(\left\lceil \frac{\beta}{p} \right\rceil - 1 \right) d \\ &= \left(\beta - \left\lceil \frac{\beta}{p} \right\rceil \right) d - 1, \end{aligned}$$

luego $r_p = q^{\left(\beta - \left\lceil \frac{\beta}{p} \right\rceil\right)d} - 1$ es el número de elementos de orden p de $\left(R_T/P^\beta\right)^*$.

Entonces, en cualquier caso, el número de subgrupos de orden p de $\left(R_T/P^\beta\right)^*$ es

$$\mathcal{N}_\beta = \frac{r_p}{p-1} = \frac{q^{\left(\beta - \left\lceil \frac{\beta}{p} \right\rceil\right)d} - 1}{p-1}. \qquad \square$$

Corolario 2.11. *Sean* $K = \mathbb{F}_q(T)$, $q = p^t$, $P \in R_T^+$, $d = \operatorname{gr} P$, $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$, $\alpha_0 = \left\lceil \dfrac{\alpha}{p} \right\rceil$. *Entonces el número de extensiones de Artin-Schreier contenidas en* $K(\Lambda_{P^{\alpha+1}})$ *pero no en* $K(\Lambda_{P^\alpha})$ *es*

$$\frac{\Phi(P^{\alpha - \alpha_0})}{p-1}.$$

Demostración. Por la Proposición 2.10 tenemos que el número de extensiones de Artin-Schreier contenidas en $K(\Lambda_{P^{\alpha+1}})$ pero no en $K(\Lambda_{P^\alpha})$ es igual a

$$\begin{aligned}
\mathcal{N}_{\alpha+1} - \mathcal{N}_\alpha &= \frac{q^{\left(\alpha+1-\left\lceil\frac{\alpha+1}{p}\right\rceil\right)d} - 1}{p-1} - \frac{q^{\left(\alpha-\left\lceil\frac{\alpha}{p}\right\rceil\right)d} - 1}{p-1} \\
&= \frac{q^{\left(\alpha+1-\left\lceil\frac{\alpha+1}{p}\right\rceil\right)d} - q^{\left(\alpha-\left\lceil\frac{\alpha}{p}\right\rceil\right)d}}{p-1} \\
&= \frac{q^{\alpha d}\left(q^{\left(1-\left\lceil\frac{\alpha+1}{p}\right\rceil\right)d} - q^{-\left\lceil\frac{\alpha}{p}\right\rceil d}\right)}{p-1} = \frac{q^{\alpha d} q^{-\left\lceil\frac{\alpha}{p}\right\rceil d}(q^d-1)}{p-1} \\
&= \frac{q^{\left(\alpha-\left\lceil\frac{\alpha}{p}\right\rceil\right)d}(q^d-1)}{p-1} = \frac{q^{\left(\alpha-\left[\frac{\alpha}{p}\right]-1\right)d}(q^d-1)}{p-1} \\
&= \frac{\Phi\left(P^{\alpha-\alpha_0}\right)}{p-1},
\end{aligned}$$

pues como $p \nmid \alpha$, $\left\lceil\dfrac{\alpha+1}{p}\right\rceil = \left\lceil\dfrac{\alpha}{p}\right\rceil$ y, por el Lema 1.7, $\left\lceil\dfrac{\alpha}{p}\right\rceil = \left[\dfrac{\alpha}{p}\right] + 1$. □

Proposición 2.12. *Sean* $K = \mathbb{F}_q(T)$, $q = p^t$, $P \in R_T^+$, $d = \operatorname{gr} P$, $\alpha \in \mathbb{N}$, $(\alpha, p) = 1$, $\alpha_0 = \left[\dfrac{\alpha}{p}\right]$. *Consideramos extensiones de Artin-Schreier* $F = K(y)$ *de* K *donde*

$$y^p - y = \frac{f(T)}{P^\alpha} \tag{2.2}$$

con $f(T) \in R_T$, $\operatorname{gr} f(T) \leq \alpha d$ *y* $(f(T), P) = 1$. *Entonces existen al menos*

$$N_\alpha = \frac{p}{p-1}\Phi(P^{\alpha-\alpha_0})$$

extensiones F *del tipo descrito en* (2.2) *contenidas en* $K(\Lambda_{P^{\alpha+1}})\mathbb{F}_{q^p}$.

Demostración. Consideremos el siguiente diagrama:

$$\begin{array}{ccc}
K(\Lambda_{P^{\alpha+1}}) & \text{——} & K(\Lambda_{P^{\alpha+1}})\mathbb{F}_{q^p} \\
| & & | \\
F & \text{————————} & F\mathbb{F}_{q^p} \\
{\scriptstyle p}\,| & & | \\
K & \underset{p}{\text{————————}} & K\mathbb{F}_{q^p}
\end{array}$$

Tenemos $\mathbb{F}_{q^p} = \mathbb{F}_q(\xi)$, donde $\xi^p - \xi = \rho$ para $\rho \in \mathbb{F}_q \backslash \wp(\mathbb{F}_q)$.
Debido al Corolario 2.11, existen $\dfrac{\Phi(P^{\alpha-\alpha_0})}{p-1}$ extensiones de Artin-Schreier F/K contenidas en $K(\Lambda_{P^{\alpha+1}})$ pero no en $K(\Lambda_{P^\alpha})$. Por el Lema 2.9, tal F es del tipo (2.2). De una tal F, obtenemos p campos $F_i = K(y_i)$, donde $y_i = y + i\xi$ para $0 \leq i \leq p-1$, de grado p sobre K y contenidos en $K(\Lambda_{P^{\alpha+1}})\mathbb{F}_{q^p}$. Verifiquemos que estos campos son del tipo prescrito, que son distintos y también que si $E, F \subseteq K(\Lambda_{P^{\alpha+1}})$ son del tipo requerido y $E \neq F$, entonces $F_i \neq E_j$, para todo $i, j \in \{0, ..., p-1\}$. Con lo anterior, se concluye que hay al menos $\dfrac{p}{p-1}\Phi(P^{\alpha-\alpha_0})$ extensiones F del tipo indicado contenidas en alguna extensión ciclotómica compuesta con la extensión de constantes.
Tenemos

$$\begin{aligned}(y+i\xi)^p - (y+i\xi) &= y^p - y + i^p\xi^p - i\xi = y^p - y + i(\xi^p - \xi) \\ &= \frac{f(T)}{P^\alpha} + i\rho = \frac{f(T) + i\rho P^\alpha}{P^\alpha} = \frac{g_i(T)}{P^\alpha}\end{aligned}$$

con $g_i(T) \in R_T$, gr $g_i(T) \leq \alpha$ para todo $i \in \{0, ..., p-1\}$.
Luego $F_i = K(y+i\xi)$ es una extensión del tipo prescrito. Supongamos ahora que $0 \leq i, j \leq p-1$, $i \neq j$ y $F_i = F_j$. Entonces $y + i\xi$, $y + j\xi \in F_i = F_j$, entonces $(i-j)\xi \in F_i = F_j$, por tanto $\xi \in F_i = F_j$, por lo que $y \in F_i = F_j = F$. Así $\xi \in F_i = F_j = F$, lo cual es una contradicción pues el campo de constantes de F es $\mathbb{F}_q$.
Finalmente, supongamos que F y E son extensiones del tipo requerido, contenidas en $K(\Lambda_{P^{\alpha+1}})$ con $E \neq F$ y $F_i = E_j$ para algunos $i, j \in \{0, ..., p-1\}$. Digamos que $F = K(y)$ con $y^p - y = \dfrac{f(T)}{P^\alpha}$, $f(T) \in R_T$, gr $f(T) \leq \alpha$ y $E = K(z)$ con $z^p - z = \dfrac{g(T)}{P^\alpha}$, $g(T) \in R_T$, gr $g(T) = \alpha$.
Tenemos $i \neq 0$, $j \neq 0$, pues de otra manera $\xi \in K(\Lambda_{P^{\alpha+1}})$, lo cual es una contradicción pues el campo de constantes de $K(\Lambda_{P^{\alpha+1}})$ es $\mathbb{F}_q$. Sea $l = i^{-1}j$. Tenemos $ly + j\xi = l(y + i\xi)$, $z + j\xi \in F_i = E_j$. Entonces $z - ly \in F_i = E_j$. Pero $z - ly \notin K$, pues $F \neq E$. Por tanto, $\mathbb{F}_{q^p} \subseteq F_i = E_j = K(z - ly) \subseteq K(\Lambda_{P^{\alpha+1}})$, lo cual es una contradicción. □

El siguiente lema es primordial para probar el resultado principal (Teorema 2.15) de esta sección. Probaremos que cualquier extensión cíclica de grado p sobre K en la cual $\mathcal{P}$, el divisor asociado al polinomio P, es el único divisor primo ramificado y aparece a la potencia α en la ecuación de Artin-Schreier en su forma normal está contenida en algún campo ciclotómico compuesto con una extensión de constantes.

Lema 2.13. *Sean p un número primo, $q = p^t$ y $P \in R_T^+$, $d =$ gr P. Sean $K = \mathbb{F}_q(T)$ y $F = K(y)$, donde*

$$y^p - y = \frac{f(T)}{P^\alpha}$$

con $f(T) \in R_T$, gr $f(T) \leq \alpha d$, $(f(T), P) = 1$, $\alpha \in \mathbb{N}$, y $(\alpha, p) = 1$. Entonces

$$F \subseteq K(\Lambda_{P^{\alpha+1}})\mathbb{F}_{q^p}.$$

Demostración. Por el Corolario 2.8 y la Proposición 2.12, tenemos que el número de extensiones cíclicas de grado p sobre K en las cuales $\mathcal{P}$ es el único divisor primo ramificado y aparece a la potencia α en la ecuación de Artin-Schreier en su forma normal debe ser igual al número de tales extensiones contenidas en el compuesto de la extensión ciclotómica y la extensión de constantes mencionados arriba. Por lo tanto, concluimos que cualquier tal extensión F está contenida en el compuesto $K(\Lambda_{P^{\alpha+1}})\mathbb{F}_{q^p}$. □

En el siguiente resultado se consideran las extensiones de Artin-Schreier en las que el divisor primo infinito es el único divisor primo ramificado.

Lema 2.14. *Sean p un número primo y $q = p^t$. Sean $K = \mathbb{F}_q(T)$ y $F = K(y)$, donde $y^p - y = f(T) \in R_T$, gr $f(T) = \alpha$, $\alpha \in \mathbb{N}$, y $(\alpha, p) = 1$. Entonces*

$$F \subseteq K(\Lambda_{\frac{1}{T^{\alpha+1}}})\mathbb{F}_{q^p}.$$

Demostración. Se sigue del Lema 2.13 dado que $K(T) = K\left(\frac{1}{T}\right)$. □

Observamos que para simplificar el enunciado de los resultados, hemos venido incluyendo al campo $K(\Lambda_{\frac{1}{T^{\alpha+1}}})$ entre los campos ciclotómicos.

Teorema 2.15. *Sean p un número primo y $q = p^t$. Sean $K = \mathbb{F}_q(T)$ y F/K una extensión de Artin-Schreier, es decir, $F = K(y)$, donde*

$$y^p - y = s(T),$$

con $s(T) \in K$, $s(T) \notin \wp(K)$,

$$(s(T))_K = \frac{\mathfrak{C}}{\mathcal{P}_1^{\alpha_1} \cdots \mathcal{P}_r^{\alpha_r}},$$

donde $\mathcal{P}_i$ es un divisor primo en K, $\alpha_i \in \mathbb{N}$, $(\alpha_i, p) = 1$, $\mathfrak{C}$ es un divisor entero primo relativo a $\mathcal{P}_i$ para $i \in \{1, ..., r\}$.

(*a*) *Si el divisor primo $\mathcal{P}_\infty$ no se ramifica en F/K, es decir, si $\mathcal{P}_\infty$ no es factor de $\prod_{i=1}^{r} \mathcal{P}_i^{\alpha_i}$, entonces $F \subseteq K(\Lambda_{\prod_{i=1}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^p}$.*

(*b*) *Si $\mathcal{P}_\infty$ se ramifica en F/K, es decir, si $\mathcal{P}_\infty = \mathcal{P}_1$ es factor de $\prod_{i=1}^{r} \mathcal{P}_i^{\alpha_i}$, entonces se cumple $F \subseteq K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})K(\Lambda_{\prod_{i=2}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^p}$.*

Los divisores $\mathcal{P}_i$ corresponden a los polinomios P_i, para $i \in \{1, \ldots, r\}$ en el caso (a) y para $i \in \{2, \ldots, r\}$ en el caso (b).

Demostración. (*a*) Por el método de fracciones parciales tenemos:

$$s(T) = \frac{f(T)}{P_1^{\alpha_1} \cdots P_r^{\alpha_r}} = \frac{f_1(T)}{P_1^{\alpha_1}} + \cdots + \frac{f_r(T)}{P_r^{\alpha_r}},$$

donde $f_i(T) \in R_T$ y $\operatorname{gr} f_i(T) \leq \alpha_i \operatorname{gr} P_i$ para todo $i \in \{1, ..., r\}$. Consideramos $F_i = K(y_i)$, donde $y_i^p - y_i = \frac{f_i(T)}{P_i^{\alpha_i}}$ para $i \in \{1, ..., r\}$. Por el Lema 2.13, se obtiene que $F_i \subseteq K(\Lambda_{P_i^{\alpha_i+1}})\mathbb{F}_{q^p}$ para $i \in \{1, ..., r\}$. Observamos que podemos poner $y = y_1 + \cdots + y_r$ pues $y^p - y = y_1^p - y_1 + \cdots + y_r^p - y_r = \frac{f(T)}{P_1^{\alpha_1} \cdots P_r^{\alpha_r}}$. Entonces

$$\begin{aligned} F = K(y) &\subseteq K(\Lambda_{P_1^{\alpha_1+1}}) \cdots K(\Lambda_{P_r^{\alpha_r+1}})\mathbb{F}_{q^p} \\ &= K(\Lambda_{P_1^{\alpha_1+1} \cdots P_r^{\alpha_r+1}})\mathbb{F}_{q^p}. \end{aligned}$$

(b) En este caso $\mathcal{P}_\infty = \mathcal{P}_1$ y tenemos

$$y^p - y = s(T) = \frac{g(T)}{P_2^{\alpha_2} \cdots P_r^{\alpha_r}}$$

con gr $\left(\dfrac{g(T)}{P_2^{\alpha_2} \cdots P_r^{\alpha_r}}\right) = \alpha_1 \in \mathbb{N}$, $g(T) \in R_T$ y $P_2, ..., P_r \in R_T$. Por el Algoritmo de la División

$$g(T) = (P_2^{\alpha_2} \cdots P_r^{\alpha_r})h(T) + l(T),$$

con $h(T)$, $l(T) \in R_T$, gr $h(T) = \alpha_1$ y ya sea gr $l(T) < \displaystyle\sum_{i=2}^{r} \alpha_i \text{gr } P_i$ o bien $l(T) = 0$. Entonces

$$y^p - y = h(T) + \frac{l(T)}{\displaystyle\prod_{i=2}^{r} P_i^{\alpha_i}}.$$

Consideramos $F_1 = K(y_1)$, donde $y_1^p - y_1 = h(T)$. Como en el caso (a), por el método de fracciones parciales tenemos:

$$\frac{l(T)}{\displaystyle\prod_{i=2}^{r} P_i^{\alpha_i}} = \frac{l_2(T)}{P_2^{\alpha_2}} + \cdots + \frac{l_r(T)}{P_r^{\alpha_r}}$$

donde $l_i(T) \in R_T$ y gr $l_i(T) \leq \alpha_i d_i$ para todo $i \in \{2, ..., r\}$. Por los Lemas 2.13 y 2.14 tenemos

$$F_1 \subseteq K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})\mathbb{F}_{q^p},$$
$$F_i \subseteq K(\Lambda_{\frac{1}{P_i^{\alpha_i+1}}})\mathbb{F}_{q^p} \text{ para todo } i \in \{2, ..., r\}.$$

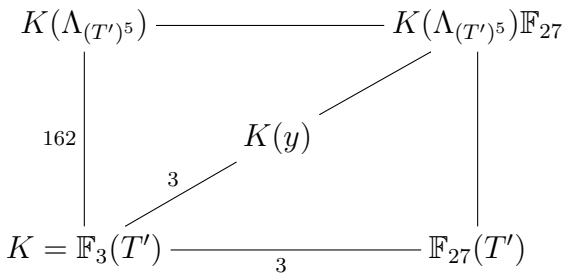
Tenemos $y = y_1 + \cdots + y_r$ pues $y^p - y = y_1^p - y_1 + \cdots + y_r^p - y_r = h(T) + \dfrac{l(T)}{\displaystyle\prod_{i=2}^{r} P_i^{\alpha_i}}$.

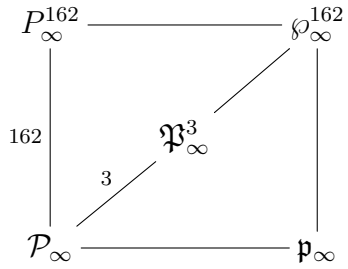
Concluimos

$$\begin{aligned} F = K(y) &\subseteq K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})K(\Lambda_{P_2^{\alpha_2+1}})\cdots K(\Lambda_{P_r^{\alpha_r+1}})\mathbb{F}_{q^p} \\ &= K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})K(\Lambda_{P_2^{\alpha_2+1}\cdots P_r^{\alpha_r+1}})\mathbb{F}_{q^p} \\ &= K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})K(\Lambda_{\prod_{i=2}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^p}. \end{aligned}$$

□

Ejemplo 2.2. Viene de los Ejemplos 1.3 y 1.6. Sean $K = \mathbb{F}_3(T)$ y $L = K(y)$ con $y^3 - y = T^4 - T^2$. La extensión L/K es de Artin-Schreier. Sea $T' = \dfrac{1}{T}$ y $L = K(y)$,





2.3. Extensiones cuadráticas

Como caso particular del Teorema 2.15 tenemos el siguiente resultado.

Corolario 2.16. *Sean $K = \mathbb{F}_q(T)$, donde q es una potencia de 2. Sea F/K una extensión cuadrática, $F = K(y)$ donde*

$$y^2 - y = s(T),$$

con $s(T) \in K$, $s(T) \notin \wp(K)$,

$$(s(T))_K = \frac{\mathfrak{C}}{\mathcal{P}_1^{\alpha_1} \dots \mathcal{P}_r^{\alpha_r}},$$

donde $\mathcal{P}_i$ *es un divisor primo en* K, $\alpha_i \in \mathbb{N}$, $(\alpha_i, 2) = 1$, $\mathfrak{C}$ *es un divisor entero primo relativo a* $\mathcal{P}_i$ *para todo* $i \in \{1, ..., r\}$.

(a) *Si el divisor primo* $\mathcal{P}_\infty$ *no se ramifica en* F/K, *es decir, si* $\mathcal{P}_\infty$ *no es factor de* $\prod_{i=1}^{r} \mathcal{P}_i^{\alpha_i}$, *entonces* $F \subseteq K(\Lambda_{\prod_{i=1}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^2}$ *se cumple.*

(b) *Si* $\mathcal{P}_\infty$ *se ramifica en* F/K, *es decir, si* $\mathcal{P}_\infty = \mathcal{P}_1$ *es factor de* $\prod_{i=1}^{r} \mathcal{P}_i^{\alpha_i}$, *entonces se cumple* $F \subseteq K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})K(\Lambda_{\prod_{i=2}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^2}$.

Demostración. Tomando $p = 2$ en el Teorema 2.15 se sigue el resultado. □

Finalmente, enunciamos el resultado general, análogo al caso de campos numéricos, para extensiones cuadráticas sobre un campo de funciones racionales.

Teorema 2.17. *Sea* $K = \mathbb{F}_q(T)$ *y* F/K *una extensión cuadrática. Entonces* F *está contenido en el compuesto de una extensión ciclotómica y la extensión de constantes* $\mathbb{F}_{q^2}$. *Más precisamente:*

(a) *Si* q *es impar,* $F = K(\sqrt{M}) \subseteq K(\Lambda_M)\mathbb{F}_{q^2}$, *para algún* $M \in \mathbb{F}_q[T]$ *no cero y libre de cuadrado.*

(b) *Si* q *es par,* $F = K(y)$, *donde*

$$y^2 - y = s(T),$$

con $s(T) \in K$, $s(T) \notin \wp(K)$,

$$(s(T))_K = \frac{\mathfrak{C}}{\mathcal{P}_1^{\alpha_1} \dots \mathcal{P}_r^{\alpha_r}},$$

donde $\mathcal{P}_i$ *es un divisor primo en* K, $\alpha_i \in \mathbb{N}$, $(\alpha_i, 2) = 1$, $\mathfrak{C}$ *es un divisor entero primo relativo a* $\mathcal{P}_i$ *para todo* $i \in \{1, ..., r\}$.

(*i*) *Si el divisor primo* $\mathcal{P}_\infty$ *no se ramifica en* F/K*, es decir, si* $\mathcal{P}_\infty$ *no es factor de* $\prod_{i=1}^{r} \mathcal{P}_i^{\alpha_i}$*, entonces se cumple* $F \subseteq K(\Lambda_{\prod_{i=1}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^2}$.

(*ii*) *Si* $\mathcal{P}_\infty$ *se ramifica en* F/K*, es decir, si* $\mathcal{P}_\infty = \mathcal{P}_1$ *es factor de* $\prod_{i=1}^{r} \mathcal{P}_i^{\alpha_i}$*, entonces* $F \subseteq K(\Lambda_{\frac{1}{T^{\alpha_1+1}}})K(\Lambda_{\prod_{i=2}^{r} P_i^{\alpha_i+1}})\mathbb{F}_{q^2}$ *se cumple.*

Demostración. El resultado se sigue de la Proposición 2.4 y el Corolario 2.16. □

Capítulo 3

La máxima extensión abeliana

3.1. La máxima extensión abeliana de K

El objetivo principal de este trabajo es probar el siguiente resultado.

Teorema 3.1. (Kronecker-Weber,[6],[23, Theorem 12.8.31]) *La máxima extensión abeliana de $K = \mathbb{F}_q(T)$ es $A = K_T E L_\infty$.*

Denotamos por A a la máxima extensión abeliana de $K = \mathbb{F}_q(T)$, la cual se construye explícitamente (ver [23]), es decir, A es generada por ciertas extensiones de grado finito sobre K, cada una de las cuales está generada por las raíces de ciertos polinomios dados explícitamente.
La extensión A es la composición de tres extensiones linealmente disjuntas: E/K, K_T/K, y L_∞/K. Las dos primeras son $E = \bigcup_{m=1}^{\infty} \mathbb{F}_{q^m}(T)$ y $K_T = \bigcup_{M \in R_T} K(\Lambda_M)$. Nótese que EK_T no puede ser la máxima extensión abeliana de K puesto que $\mathcal{P}_\infty$ es moderadamente ramificado en EK_T/K. Necesitamos una extensión en la cual $\mathcal{P}_\infty$ sea salvajemente ramificado. Sea L_n la máxima subextensión de $K(\Lambda_{1/T^{n+1}})$ donde $\mathcal{P}_\infty$ es total y salvajemente ramificado, $n \in \mathbb{N} \cup 0$. Esto es, $L_n = K(\Lambda_{1/T^{n+1}})^{\mathbb{F}_q^*}$. Sea $L_\infty := \bigcup_{n \in \mathbb{N}} L_n$.

Para probar el Teorema 3.1 es suficiente mostrar que cualquier extensión abeliana finita de K está contenida en $K(\Lambda_N)\mathbb{F}_{q^m} L_n$ para algunos $N \in R_T$, $m, \in \mathbb{N}$ y $n \in \mathbb{N} \cup 0$.
Sean $K = \mathbb{F}_q(T)$ y F/K una extensión abeliana finita. Sea $G := \mathrm{Gal}\,(F/K)$. Por el Teorema Fundamental de los Grupos Abelianos Finitamente Genera-

dos tenemos

$$G \cong C_{n_1} \times \cdots \times C_{n_l} \times C_{p^{a_1}} \times \cdots \times C_{p^{a_h}},$$

donde C_n denota al grupo cíclico de n elementos, $(n_i, p) = 1$ para $1 \leq i \leq l$ y $a_j \in \mathbb{N}$ para $1 \leq j \leq h$. Sea $S_i \subseteq F$ tal que $\mathrm{Gal}\,(S_i/K) \cong C_{n_i}$ para $1 \leq i \leq l$ y sea $R_j \subseteq F$ tal que $\mathrm{Gal}\,(R_j/K) \cong C_{p^{a_j}}$, $1 \leq j \leq h$. Para probar el Teorema 3.1 basta con mostrar que cada S_i y cada R_j están contenidos en $K(\Lambda_N)\mathbb{F}_{q^m}L_n$ para algunos $N \in R_T$ y $m, n \in \mathbb{N}$. Por lo tanto, podemos suponer que F/K es una extensión cíclica de grado h donde ya sea $(h, p) = 1$ o bien $h = p^n$ para algún $n \in \mathbb{N}$.

3.2. Extensiones moderadamente ramificadas

En esta sección se probara la suficiencia del Teorema 3.1 para el caso particular de una extensión moderadamente ramificada. Sea F/K una extensión abeliana finita. Sean $P \in R_T$ polinomio mónico irreducible de grado d y $\mathcal{P}$ el divisor primo asociado a P.

Proposición 3.2. *Sea $\mathcal{P}$ moderadamente ramificado en F/K. Si e denota el índice de ramificación de $\mathcal{P}$ en F. Entonces $e|(q^d - 1)$.*

Demostración. Primero consideremos en general una extensión abeliana finita F/K. Sean $G_{-1} = D$ el grupo de descomposición de $\mathcal{P}$, $G_0 = I$ el grupo de inercia y G_i, con $i \geq 1$, los grupos de ramificación. Sea $\mathfrak{P}$ un divisor primo en F que divide a $\mathcal{P}$. Entonces, si $\mathcal{O}_{\mathfrak{P}}$ denota el anillo de valuación de $\mathfrak{P}$, tenemos

$$U^{(i)} = 1 + \mathfrak{P}^i \subseteq \mathcal{O}_{\mathfrak{P}}^* = \mathcal{O}_{\mathfrak{P}} \setminus \mathfrak{P},\ i \geq 1,\ U^{(0)} = \mathcal{O}_{\mathfrak{P}}^*.$$

Sea $l(\mathfrak{P}) = \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}$ el campo residual de $\mathfrak{P}$. Los siguientes son monomorfismos:

$$\begin{aligned} G_i/G_{i+1} \overset{\varphi_i}{\hookrightarrow} U^{(i)}/U^{(i+1)} &\cong \begin{cases} l(\mathfrak{P})^*, & i = 0 \\ \mathfrak{P}^i/\mathfrak{P}^{i+1} \cong l(\mathfrak{P}), & i \geq 1 \end{cases} \\ \overline{\sigma} &\mapsto [\sigma\pi/\pi] \end{aligned}$$

donde π denota un elemento primo para $\mathfrak{P}$.

Probaremos que si $G_{-1}/G_1 = D/G_1$ es abeliano, entonces

$$\varphi = \varphi_0 : G_0/G_1 \to U^{(0)}/U^{(1)} \cong (\mathcal{O}_\mathfrak{P}/\mathfrak{P})^*$$

satisface que $\operatorname{Im}\varphi \subseteq \mathcal{O}_\mathcal{P}/\mathcal{P} \cong R_T/(P) \cong \mathbb{F}_{q^d}$. En particular se seguirá que $|G_0/G_1|$ divide a $|\mathbb{F}_{q^d}^*| = q^d - 1$.

Para probar esta afirmación, notemos que

$$\begin{aligned}\text{Aut } ((\mathcal{O}_\mathfrak{P}/\mathfrak{P})/(\mathcal{O}_\mathcal{P}/\mathcal{P})) &\cong \text{Gal } ((\mathcal{O}_\mathfrak{P}/\mathfrak{P})/(\mathcal{O}_\mathcal{P}/\mathcal{P})) \\ &= D/I = G_{-1}/G_0\end{aligned}$$

(ver [23, Corollary 5.2.12]).
Sean $\sigma \in G_0$ y $\varphi(\bar{\sigma}) = \varphi(\sigma \text{ mód } G_1) = [\alpha] \in (\mathcal{O}_\mathfrak{P}/\mathfrak{P})^*$. Entonces $\sigma\pi \equiv \alpha\pi$ mód $\mathfrak{P}^2$.
Sea $\theta \in G_{-1} = D$ arbitrario y sea $\pi_1 := \theta^{-1}(\pi)$. Entonces π_1 es un elemento primo para $\mathfrak{P}$. Dado que φ es independiente del elemento primo, se sigue que $\sigma\pi_1 \equiv \alpha\pi_1$ mód $\mathfrak{P}^2$, esto es, $\sigma\theta^{-1}\pi \equiv \alpha\theta^{-1}\pi$ mód $\mathfrak{P}^2$. Dado que G_{-1}/G_1 es un grupo abeliano, tenemos

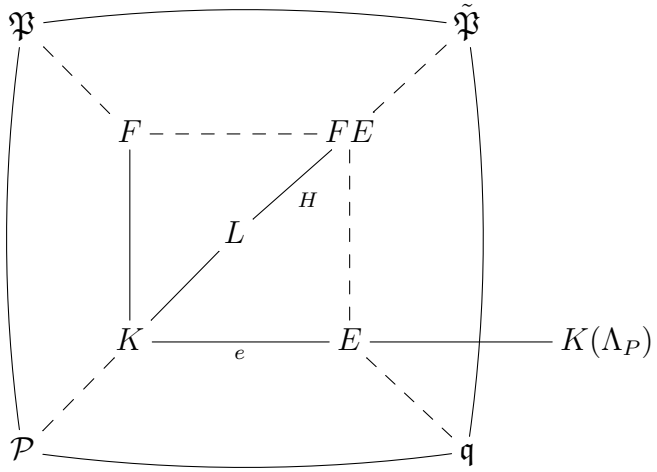
$$\sigma\pi = (\theta\sigma\theta^{-1})(\pi) \equiv \theta(\alpha)\pi \text{ mód } \mathfrak{P}^2.$$

Así $\sigma\pi \equiv \theta(\alpha)\pi$ mód $\mathfrak{P}^2$ y $\sigma\pi \equiv \alpha\pi$ mód $\mathfrak{P}^2$. De aquí se sigue que $\theta(\alpha) \equiv \alpha$ mód $\mathfrak{P}$ para todo $\theta \in G_{-1}$.
Si escribimos $\tilde{\theta} = \theta \text{ mód } G_0$, $\tilde{\theta}[\alpha] = [\alpha]$, esto es, $[\alpha]$ es un elemento fijo bajo la acción de grupo $G_{-1}/G_0 \cong \text{Gal } ((\mathcal{O}_\mathfrak{P}/\mathfrak{P})/(\mathcal{O}_\mathcal{P}/\mathcal{P}))$. Obtenemos que $[\alpha] \in \mathcal{O}_\mathcal{P}/\mathcal{P}$. Por lo tanto $\operatorname{Im}\varphi \subseteq (\mathcal{O}_\mathcal{P}/\mathcal{P})^*$ y $|G_0/G_1|||(\mathcal{O}_\mathcal{P}/\mathcal{P})^*| = q^d - 1$. Finalmente, dado que F/K es abeliana y $\mathcal{P}$ es ramificado moderadamente, $G_1 = \{1\}$, se sigue que $e = |G_0| = |G_0/G_1||(q^d - 1)$. □

Ahora consideramos una extensión abeliana finita ramificada moderadamente F/K donde $P_1, \ldots, P_r$ son los primos finitos ramificados. Sean $P \in \{P_1, \ldots, P_r\}$ y $\text{gr } P = d$. Sea e el índice de ramificación de $\mathcal{P}$ en F. Por la Proposición 3.2 tenemos $e|q^d - 1$. Ahora bien, $\mathcal{P}$ es totalmente ramificado en $K(\Lambda_P)/K$ con

índice de ramificación $q^d - 1$. En esta extensión $\mathcal{P}_\infty$ tiene índice de ramificación igual a $q - 1$.

Sea $K \subseteq E \subseteq K(\Lambda_P)$ con $[E : K] = e$. Sea $\tilde{\mathfrak{P}}$ un divisor primo en FE que divide a $\mathcal{P}$. Sean $\mathfrak{q} := \tilde{\mathfrak{P}}|_E$ y $\mathfrak{P} := \mathfrak{P}|_F$.



Tenemos $e = e_{F/K}(\mathfrak{P}|\mathcal{P}) = e_{E/K}(\mathfrak{q}|\mathcal{P})$. Por el Lema de Abhyankar (ver [23, Theorem 12.4.4]) obtenemos

$$e_{FE/K}(\tilde{\mathfrak{P}}/\mathcal{P}) = [e_{F/K}(\mathfrak{P}|\mathcal{P}), e_{E/K}(\mathfrak{q}|\mathcal{P})] = [e, e] = e.$$

Sea $H \subseteq \mathrm{Gal}(FE/K)$ el grupo de inercia de $\tilde{\mathfrak{P}}/\mathcal{P}$. Sea $L := (FE)^H$. Entonces $\mathcal{P}$ es no ramificado en L/K. Queremos ver que $F \subseteq LK(\Lambda_P)$. En efecto, tenemos $[FE : L] = e$ y $E \cap L = K$ dado que $\mathcal{P}$ es totalmente ramificado en E/K y no ramificado en L/K. Se sigue que $[LE : K] = [L : K][E : K]$. Por lo tanto

$$\begin{aligned}[FE : K] = [FE : L][L : K] &= e\frac{[LE : K]}{[E : K]} \\ &= e\frac{[LE : K]}{e} = [LE : K].\end{aligned}$$

Dado que $LE \subseteq FE$ se sigue que $FE = LE = EL \subseteq K(\Lambda_P)L$. Así que $F \subseteq K(\Lambda_P)L$. En L/K los primos finitos ramificados son a lo más $\mathcal{P}_2, \ldots, \mathcal{P}_r$. En caso de que $r - 1 \geq 1$, podemos aplicar el argumento anterior a L/K y obtenemos L_2/K tal que a lo más $r - 2$ primos finitos son ramificados y $L \subseteq K(\Lambda_{P_2})L_2$, así $F \subseteq K(\Lambda_{P_1})L \subseteq K(\Lambda_{P_1})K(\Lambda_{P_2})L_2 = K(\Lambda_{P_1P_2})L_2$.

Realizando el proceso anterior a lo más r veces tenemos

$$F \subseteq K(\Lambda_{P_1 \cdots P_r}) L_0, \tag{3.1}$$

donde en la extensión L_0/K posiblemente el primo infinito $\mathcal{P}_\infty$ sea el único que se ramifique. Con ayuda de la siguiente proposición veremos que no es el caso que haya primos ramificados en L_0/K.

Proposición 3.3. *Sean $K = \mathbb{F}_q(T)$ y F/K una extensión abeliana finita donde a lo más un primo $\mathcal{P}_0$ de grado 1 se ramifica y lo hace moderadamente. Entonces F/K es una extensión de constantes (por lo que de hecho $\mathcal{P}_0$ no se ramifica en F/K).*

Demostración. Por la Proposición 3.2 tenemos $e := e_{F/K}(\mathcal{P}_0) | q-1$. Supongamos $e > 1$. Sea H el grupo de inercia de $\mathcal{P}_0$. Entonces H es cíclico, $|H| = e$ y $\mathcal{P}_0$ es no ramificado en $E := F^H/K$. Por lo tanto E/K es una extensión no ramificada. Así E/K es una extensión de constantes.

Sea $m = [E : K]$. Entonces, si $\mathfrak{P}_0$ es un divisor primo en E el cual divide a $\mathcal{P}_0$, tenemos que el grado relativo $d_{E/K}(\mathfrak{P}_0|\mathcal{P}_0)$ es igual a m, el número de divisores primos en E/K es 1 y el grado de $\mathfrak{P}_0$ es 1 (ver el Teorema 1.1). Por lo tanto $\mathfrak{P}_0$ es el único divisor primo ramificado en F/E y éste es de grado 1 y totalmente ramificado. Además $[F : E] = e | q-1 = |\mathbb{F}_q^*|$.

Las raíces $(q-1)$-ésimas de 1 pertenecen a $\mathbb{F}_q \subseteq K$. Luego K contiene a las raíces e-ésimas de la unidad. Así, F/E es una extensión de Kummer. Luego $F = E(y)$ con $y^e = \alpha$ (ver el Teorema 1.3) con $\alpha \in E = K\mathbb{F}_{q^m} = \mathbb{F}_{q^m}(T)$. Escribimos α en su forma normal como lo prescribe Hasse [4]: $(\alpha)_E = \frac{\mathfrak{P}_0^a \mathfrak{a}}{\mathfrak{b}}$ con $0 < a < e$. Como, por otro lado, el grado de $(\alpha)_E$ es 0, esto no es posible, pues $\mathrm{gr}(\mathfrak{a})_E$ o $\mathrm{gr}(\mathfrak{b})_E$ no es múltiplo de e, por lo que hay al menos otro primo ramificado en F/K, lo cual contradice que $\mathcal{P}_0$ es el único primo ramificado. Por lo tanto F/K es una extensión de constantes. □

Como un corolario de (3.1) y la Proposición 3.3 obtenemos

Corolario 3.4. *Sean $K = \mathbb{F}_q(T)$ y F/K una extensión abeliana moderadamente ramificada donde los divisores primos finitos ramificados son $\mathcal{P}_1, \ldots, \mathcal{P}_r$. Entonces $F \subseteq K(\Lambda_{P_1 \cdots P_r})\mathbb{F}_{q^m}$ para algún $m \in \mathbb{N}$.*

Demostración. Puesto que no hay primos ramificados salvajemente, se sigue de (3.1) que existe una extensión abeliana finita no ramificada M_0/K tal que $F \subseteq K(\Lambda_{P_1 \cdots P_r})M_0$ en la cual tal vez el primo infinito es ramificado moderadamente. Por la Proposición 3.3, tenemos que M_0/K es una extensión de constantes, es decir $M_0 = \mathbb{F}_{q^m}(T)$ para algún $m \in \mathbb{N}$. Por lo tanto tenemos $F \subseteq K(\Lambda_{P_1 \cdots P_r})\mathbb{F}_{q^m}$. □

3.3. Ramificación en Extensiones de Witt

Como una consecuencia del Corolario 3.4, el Teorema 3.1 se seguirá si lo demostramos para el caso particular de una extensión de Witt, esto es, una extensión cíclica K_n/K de grado p^n para algún $n \in \mathbb{N}$. Se sigue del Teorema 1.6 que este tipo de extensión K_n/K está dada por un vector de Witt $\boldsymbol{\beta} \in W_n(K)$, esto es $K_n = K(\boldsymbol{y})$ donde

$$\boldsymbol{y}^p \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta},$$

la operación es la diferencia de Witt.

El siguiente resultado fue probado en [14]. El objetivo es "separar" a los divisores primos ramificados.

Teorema 3.5. *Sea K_n/K una extensión cíclica de grado p^n donde $\mathcal{P}_1, \ldots, \mathcal{P}_r \in R_T^+$ y posiblemente $\mathcal{P}_\infty$, son los divisores primos ramificados. Entonces $K_n = K(\boldsymbol{y})$ donde*

$$\boldsymbol{y}^p \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta} = \boldsymbol{\delta}_1 \overset{\bullet}{+} \cdots \overset{\bullet}{+} \boldsymbol{\delta}_r \overset{\bullet}{+} \boldsymbol{\mu},$$

con $\boldsymbol{\delta} = (\delta_{i1}, \ldots, \delta_{in})$, $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_n)$, $\delta_{ij} = \dfrac{Q_{ij}}{P_i^{e_{ij}}}$, $e_{ij} \geq 0$, $Q_{ij} \in R_T$,

(a) *si $e_{ij} = 0$ entonces $Q_{ij} = 0$;*

(b) *si $e_{ij} > 0$, entonces $p \nmid e_{ij}$, $(Q_{ij}, P_i) = 1$ y $\operatorname{gr} Q_{ij} < \operatorname{gr} P_i^{e_{ij}}$ y $\mu_j = f_j(T) \in R_T$ con*

(c) $p \nmid \operatorname{gr} f_j$ *cuando* $f_j \notin \mathbb{F}_q$ *y*

(d) $\mu_j \notin \wp(\mathbb{F}_q) := \{a^p - a | a \in \mathbb{F}_q\}$ *cuando* $\mu_j \in \mathbb{F}_q^*$. □

El siguiente ejemplo ilustra la descomposición del Teorema 3.5

Ejemplo 3.1. Viene del Ejemplo 1.10.

Sean $K = \mathbb{F}_3(T)$ y $n = 2$. Consideremos $K_2 = K(\boldsymbol{y})$ donde

$$\boldsymbol{y}^{3\,\bullet} - \boldsymbol{y} = \boldsymbol{\beta} \text{ con } \boldsymbol{\beta} = \left(\frac{1}{T^2-1}, \frac{T^6+T^3-T-1}{T(T^2-1)^3}\right).$$

Usando fracciones parciales tenemos las componentes usuales

$$\begin{aligned}
\beta_1 &= \frac{1}{T^2-1} = \frac{-1}{T-1} + \frac{1}{T+1}, \\
\beta_2 &= \frac{T^6+T^3-T-1}{T(T^2-1)^3} = \frac{1}{T} - \frac{1/4}{T-1} + \frac{1}{(T-1)^2} + \frac{1/4}{T+1} - \frac{1/2}{(T+1)^2}.
\end{aligned}$$

Pasamos a las componentes fantasmas

$$\begin{aligned}
\beta^{(1)} &= \frac{-1}{T-1} + \frac{1}{T+1}, \\
\beta^{(2)} &= \left(\frac{-1}{T-1} + \frac{1}{T+1}\right)^3 \\
&\quad + 3\left(\frac{1}{T} - \frac{1/4}{T-1} + \frac{1}{(T-1)^2} + \frac{1/4}{T+1} - \frac{1/2}{(T+1)^2}\right) \\
&= \frac{-1}{(T-1)^3} + \frac{3}{(T-1)^2(T+1)} + \frac{-3}{(T-1)(T+1)^2} + \frac{1}{(T+1)^3} \\
&\quad + 3\left(\frac{1}{T} - \frac{1/4}{T-1} + \frac{1}{(T-1)^2} + \frac{1/4}{T+1} - \frac{1/2}{(T+1)^2}\right) \\
&= \frac{3}{T} + \frac{-9/4}{T-1} + \frac{9/2}{(T-1)^2} + \frac{-1}{(T-1)^3} + \frac{9/4}{T+1} + \frac{1}{(T+1)^3}.
\end{aligned}$$

Luego

$$\begin{aligned}
(\beta^{(1)}, \beta^{(2)}) &= \left(0, \frac{3}{T}\right) \\
&\quad + \left(\frac{-1}{T-1}, \frac{-9/4}{T-1} + \frac{9/2}{(T-1)^2} + \frac{-1}{(T-1)^3}\right) \\
&\quad + \left(\frac{1}{T+1}, \frac{9/4}{T+1} + \frac{1}{(T+1)^3}\right).
\end{aligned}$$

Tenemos

$$\gamma_1 = \left(0, \frac{3}{T}\right),$$
$$\gamma_2 = \left(\frac{-1}{T-1}, \frac{-9/4}{T-1} + \frac{9/2}{(T-1)^2} + \frac{-1}{(T-1)^3}\right),$$
$$\gamma_3 = \left(\frac{1}{T+1}, \frac{9/4}{T+1} + \frac{1}{(T+1)^3}\right).$$

Volvemos a componentes usuales

$$\delta_1 = \left(0, \frac{1}{T}\right),$$
$$\delta_2 = \left(\frac{-1}{T-1}, \frac{-3/4}{T-1} + \frac{3/2}{(T-1)^2}\right) = \left(\frac{-1}{T-1}, 0\right),$$
$$\delta_3 = \left(\frac{1}{T+1}, \frac{3/4}{T+1}\right) = \left(\frac{1}{T+1}, 0\right).$$

Finalmente recuperamos

$$\boldsymbol{y}^3 \overset{\bullet}{-} \boldsymbol{y} = \left(0, \frac{1}{T}\right) \overset{\bullet}{+} \left(\frac{-1}{T-1}, 0\right) \overset{\bullet}{+} \left(\frac{1}{T+1}, 0\right).$$

Consideremos el campo $L = K(\boldsymbol{y})$ donde $\boldsymbol{y}^p \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta}$, con $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$ y se cumplen las siguientes condiciones

$$\begin{aligned} &\beta_i = \frac{Q_i}{P^{\lambda_i}},\ P \in R_T^+,\ Q_i \in R_T \text{ tal que } \lambda_i \geq 0, \\ &\text{si } \lambda_i = 0 \text{ entonces } Q_i = 0, \\ &\text{si } \lambda_i > 0 \text{ entonces } (\lambda_i, p) = 1,\ (Q_i, P) = 1 \text{ y gr } Q_i < \text{gr } P^{\lambda_i}, \\ &\lambda_1 > 0. \end{aligned} \tag{3.2}$$

Un caso particular del Teorema 3.5 adecuado para nuestro estudio se presenta en la siguiente proposición.

Proposición 3.6. *Supongamos que cualquier extensión L/K que cumpla las condiciones* (3.2) *satisface que $L \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$. Sea K_n/K una extensión definida por $K_n = K(\boldsymbol{y})$ donde $\wp(\boldsymbol{y}) = \boldsymbol{y}^p \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta}$ con $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$, β_i dado en su forma normal: $\beta_i \in \mathbb{F}_q$ o bien $\beta_i = \dfrac{Q_i}{P^{\lambda_i}}$, con $Q_i \in R_T$ y $\lambda_i > 0$, $(\lambda_i, p) = 1$, $(Q_i, P) = 1$ y gr $Q_i <$ gr P^{λ_i}. Entonces $K_n \subseteq \mathbb{F}_{q^{p^n}} K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{F}_q$.*

Demostración. Del Teorema 3.5 tenemos que podemos descomponer el vector $\boldsymbol{\beta}$ como $\boldsymbol{\varepsilon} \overset{\bullet}{+} \boldsymbol{\gamma}$ con $\varepsilon_i \in \mathbb{F}_q$ para todo $1 \leq i \leq n$ y $\gamma_i = 0$ o bien $\gamma_i = \dfrac{Q_i}{P^{\lambda_i}}$, con $Q_i \in R_T$ y $\lambda_i > 0$, $(\lambda_i, p) = 1$, $(Q_i, P) = 1$ y $\operatorname{gr} Q_i < \operatorname{gr} P^{\lambda_i}$.

Supongamos $\gamma_1 = \cdots = \gamma_r = 0$ y $\gamma_{r+1} \notin \mathbb{F}_q$. Tenemos $K_n \subseteq K(\boldsymbol{\varepsilon})K(\boldsymbol{\gamma})$. Ahora bien, $K(\boldsymbol{\gamma}) = K(0, \ldots, 0, \gamma_{r+1}, \ldots, \gamma_n)$ y $K(\boldsymbol{\varepsilon}) \subseteq \mathbb{F}_{q^{p^n}}$.

Para cualquier vector de Witt $\boldsymbol{x} = (x_1, \ldots, x_n)$ tenemos la descomposición dada por el mismo Witt (ver [26]).

$$\begin{aligned}\boldsymbol{x} =& (x_1, \ldots, 0) \overset{\bullet}{+} (0, x_2, \ldots, 0) \overset{\bullet}{+} \cdots \overset{\bullet}{+} (0, \ldots, 0, x_j, 0, \ldots, 0) \\ & \overset{\bullet}{+} (0, \ldots, 0, x_{j+1}, \ldots, x_n)\end{aligned}$$

para cada $0 \leq j \leq n-1$. Se sigue que $K(\boldsymbol{\gamma}) = K(\gamma_{r+1}, \ldots, \gamma_n)$. Dado que este campo cumple las condiciones (3.2), tenemos $K(\boldsymbol{\gamma}) \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$. El resultado se sigue. □

Observación 3.1. El primo $\mathcal{P}_\infty$ se puede manejar de la misma manera. Las condiciones (3.2) para $\mathcal{P}_\infty$ son las siguientes. Sea $K_n = K(\boldsymbol{\mu})$ con $\mu_j = f_j(T) \in R_T$, con $f_j(0) = 0$ para todo j y cada $f_j(T) = 0$ o $f_j(T) \neq 0$ y $p \nmid \operatorname{gr} f_j(T)$. La condición $f_j(0) = 0$ significa que el primo infinito para $T' = 1/T$ o bien se descompone o bien se ramifica en cada nivel, esto es, su grado de inercia es 1 en K_n/K. En este caso, con el cambio de variable $T' = 1/T$, las hipótesis en la Proposición 3.6 dicen que cualquier campo que cumpla estas condiciones satisface $K_n \subseteq K(\Lambda_{T'^m}) = K(\Lambda_{T^{-m}})$ para algún $m \in \mathbb{N}$. Sin embargo, dado que el grado de la extensión K_n/K es una potencia de p debemos tener $K_n \subseteq K(\Lambda_{T^{-m}})^{\mathbb{F}_q^*} = L_{m-1}$.

Observación 3.2. Con la notación del Teorema 3.5 obtenemos que si $\boldsymbol{z}_i^p \overset{\bullet}{-} \boldsymbol{z}_i = \boldsymbol{\delta}_i$, $1 \leq i \leq r$ y $\boldsymbol{v}^p \overset{\bullet}{-} \boldsymbol{v} = \boldsymbol{\mu}$, entonces $K_n = K(\boldsymbol{y}) \subseteq K(\boldsymbol{z}_1, \ldots, \boldsymbol{z}_r, \boldsymbol{v}) = K(\boldsymbol{z}_1) \cdots K(\boldsymbol{z}_r)K(\boldsymbol{v})$. Por lo tanto, si el Teorema 3.1 se tiene para cada $K(\boldsymbol{z}_i)$, $1 \leq i \leq r$ y para $K(\boldsymbol{v})$, entonces se tiene para K_n.

Del Teorema 3.5, la Proposición 3.6 y la Observación 3.1, obtenemos que para la prueba del Teorema 3.1 es suficiente mostrar que cualquier extensión

de campos K_n/K que cumpla con las condiciones (3.2) satisface o bien que $K_n \subseteq K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$ o bien que $K_n \subseteq L_m$ para algún $m \in \mathbb{N}$. Es suficiente estudiar el caso para $P \in R_T$.

A continuación estudiaremos el comportamiento de $\mathcal{P}_\infty$ en una extensión cíclica arbitraria K_n/K de grado p^n.

Proposición 3.7. *Sea K_n/K dada como en el Teorema 3.5. Supongamos $\mu_1 = \cdots = \mu_s = 0$, $\mu_{s+1} \in \mathbb{F}_q^*$, $\mu_{s+1} \notin \wp(\mathbb{F}_q)$ y sea $t+1$ el primer índice para el cual $f_{t+1} \notin \mathbb{F}_q$(y por tanto $p \nmid \operatorname{gr} f_{t+1}$). Entonces el índice de ramificación de $\mathcal{P}_\infty$ es p^{n-t}, el grado de inercia de $\mathcal{P}_\infty$ es p^{t-s} y el número de descomposición de $\mathcal{P}_\infty$ es p^s. Es decir, si $\operatorname{Gal}(K_n/K) = \langle\sigma\rangle \cong C_{p^n}$, entonces el grupo de inercia de $\mathcal{P}_\infty$ es $\mathfrak{J} = \langle\sigma^{p^t}\rangle$ y el grupo de descomposición de $\mathcal{P}_\infty$ es $\mathfrak{D} = \langle\sigma^{p^s}\rangle$.*

Demostración. Dado que la extensión K_n/K es una extensión cíclica de grado potencia de un número primo, el campo de inercia es aquél a partir del cual $\mathcal{P}_\infty$ se ramifica. El primer nivel donde esto sucede tiene índice $t+1$. Por otra parte, por la misma razón, el campo de descomposición es aquél a partir del cual $\mathcal{P}_\infty$ empieza a ser inerte y el primer nivel donde esto sucede es el $s+1$. □

Proposición 3.8. *Si K_n es un campo definido por una ecuación del tipo dado en (3.2), entonces K_n/K es una extensión de grado p^n, $\mathcal{P}$ es el único primo ramificado, totalmente ramificado y $\mathcal{P}_\infty$ es totalmente descompuesto. Análogamente, si $K_n = K(\boldsymbol{v})$ donde $v_i = f_i(T) \in R_T$, $f_i(0) = 0$ para todo $1 \leq i \leq n$ y $f_1(T) \notin \mathbb{F}_q$, $p \nmid \operatorname{gr} f_1(T)$, entonces $\mathcal{P}_\infty$ es el único primo ramificado en K_n/K, es totalmente ramificado y el divisor de ceros de T, el cual es el primo infinito en $R_{1/T}$, es totalmente descompuesto.*

Demostración. De las Proposiciones 1.5 y 3.7 obtenemos el resultado. □

Hemos reducido la prueba del Teorema 3.1 a demostrar que cualquier extensión del tipo dado en la Proposición 3.8 está contenida en $K(\Lambda_{P^\alpha})$ para algún $\alpha \in \mathbb{N}$ o en L_m para algún $m \in \mathbb{N}$. El segundo caso es una consecuencia del primero con el cambio de variable $T' = 1/T$.

Sean $n,\ \alpha \in \mathbb{N}$. Denotamos por $v_n(\alpha)$ al número de grupos cíclicos de orden p^n contenidos en $(R_T/(P^\alpha))^* \cong \mathrm{Gal}\,(K(\Lambda_{P^\alpha})/K)$. Tenemos que $v_n(\alpha)$ es el número de extensiones cíclicas K_n/K de grado p^n tales que $K_n \subseteq K(\Lambda_{P^\alpha})$. Cualquier tal extensión satisface que su conductor $\mathfrak{F}_{K_n}$ divide a $\mathcal{P}^\alpha$.

Sea $t_n(\alpha)$ el número de extensiones cíclicas K_n/K de grado p^n tales que $\mathcal{P}$ es el único primo ramificado y es totalmente ramificado, $\mathcal{P}_\infty$ es totalmente descompuesto y su conductor $\mathfrak{F}_{K_n}$ es un divisor de $\mathcal{P}^\alpha$. Dado que cualquier extensión cíclica K_n/K de grado p^n tal que $K \subseteq K_n \subseteq K(\Lambda_{P^\alpha})$ satisface las condiciones, tenemos $v_n(\alpha) \leq t_n(\alpha)$. Si probamos que $t_n(\alpha) \leq v_n(\alpha)$ entonces habremos probado que cualquier extensión que satisface las condiciones (3.2) está contenida en una extensión ciclotómica y el Teorema 3.1 se sigue.

Por lo tanto, para demostrar el Teorema 3.1 es suficiente demostrar

$$t_n(\alpha) \leq v_n(\alpha) \text{ para todos } n,\ \alpha \in \mathbb{N}. \tag{3.3}$$

3.4. Extensiones salvajemente ramificadas

En esta sección probaremos (3.3) por inducción sobre n. Primero calcularemos $v_n(\alpha)$ para todos $n,\ \alpha \in \mathbb{N}$.

Proposición 3.9. *El número $v_n(\alpha)$ de grupos cíclicos de orden p^n contenidos en $(R_T/P^\alpha)^*$ es*

$$v_n(\alpha) = \frac{q^{d(\alpha-\lceil \frac{\alpha}{p^n} \rceil)} - q^{d(\alpha-\lceil \frac{\alpha}{p^{n-1}} \rceil)}}{p^{n-1}(p-1)} = \frac{q^{d(\alpha-\lceil \frac{\alpha}{p^{n-1}} \rceil)}(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1)}{p^{n-1}(p-1)}.$$

Demostración. Tenemos el isomorfismo $\mathrm{Gal}(K(\Lambda_{P^\alpha})/K) \cong (R_T/(P^\alpha))^*$ y la sucesión exacta

$$0 \longrightarrow D_{P,P^\alpha} \longrightarrow (R_T/(P^\alpha))^* \xrightarrow{\varphi} (R_T/(P))^* \longrightarrow 0\ , \tag{3.4}$$

donde

$$\varphi : (R_T/(P^\alpha))^* \to (R_T/(P))^*$$
$$A \text{ mód } P^\alpha \mapsto A \text{ mód } P$$

y $D_{P,P^\alpha} = \{N \text{ mód } P^\alpha | N \equiv 1 \text{ mód } P\}$. Podemos considerar $D_{P,P^\alpha} = \{1 + hP | h \in R_T,\ \mathrm{gr}\, h < \mathrm{gr}\, P^\alpha = d\alpha\}$.

Tenemos $(R_T/(P^\alpha))^* \cong (R_T/(P))^* \times D_{P,P^\alpha}$ y $(R_T/(P))^* \cong C_{q^d-1}$. Primero calculamos el número de elementos de orden p^n contenidos en $(R_T/(P^\alpha))^*$. Estos elementos pertenecen a D_{P,P^α}. Sea $A = 1 + hP \in D_{P,P^\alpha}$ de orden p^n. Escribimos $h = gP^\gamma$ con $g \in R_T$ $(g, P) = 1$ y $\gamma \geq 0$. Dado que A es de orden p^n, se tiene

$$A^{p^n} = 1 + g^{p^n} P^{p^n(1+\gamma)} \equiv 1 \text{ mód } P^\alpha, \tag{3.5}$$

y

$$A^{p^{n-1}} = 1 + g^{p^{n-1}} P^{p^{n-1}(1+\gamma)} \not\equiv 1 \text{ mód } P^\alpha. \tag{3.6}$$

de (3.5) y (3.6) se sigue que

$$p^{n-1}(1+\gamma) < \alpha \leq p^n(1+\gamma) \tag{3.7}$$

lo cual es equivalente a

$$\left\lceil \frac{\alpha}{p^n} \right\rceil - 1 \leq \gamma < \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 1 \tag{3.8}$$

Observemos que para la existencia de al menos un elemento de orden p^n necesitamos $\alpha > p^{n-1}$.

Ahora, para cada γ que satisface (3.7) tenemos $(g, P) = 1$ y $\operatorname{gr} g + d(1+\gamma) < d\alpha$, esto es, $\operatorname{gr} g < d(\alpha - \gamma - 1)$. Así existen $\Phi(P^{\alpha-\gamma-1})$ tales $g's$.

Por lo tanto, el número de elementos de orden p^n en D_{P,P^α} es

$$\sum_{\gamma=\left\lceil \frac{\alpha}{p^n} \right\rceil - 1}^{\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 2} \Phi(P^{\alpha-\gamma-1}) = \sum_{\gamma'=\alpha-\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil + 1}^{\alpha - \left\lceil \frac{\alpha}{p^n} \right\rceil} \Phi(P^{\gamma'}). \tag{3.9}$$

Notemos que para cualquier $1 \leq r \leq s$ tenemos

$$\begin{aligned} \sum_{i=r}^{s} \Phi(P^i) &= \sum_{i=r}^{s} q^{d(i-1)}(q^d - 1) = (q^d - 1)q^{d(r-1)} \sum_{j=0}^{s-r} q^{dj} \\ &= (q^d - 1)q^{d(r-1)} \frac{q^{d(s-r+1)} - 1}{q^d - 1} = q^{ds} - q^{d(r-1)}. \end{aligned}$$

Por lo tanto (3.9) es igual a

$$q^{d(\alpha-\lceil\frac{\alpha}{p^n}\rceil)}-q^{d(\alpha-\lceil\frac{\alpha}{p^{n-1}}\rceil)}=q^{d(\alpha-\lceil\frac{\alpha}{p^{n-1}}\rceil)}(q^{d(\lceil\frac{\alpha}{p^{n-1}}\rceil-\lceil\frac{\alpha}{p^n}\rceil)}-1).$$

Puesto que cada grupo cíclico de orden p^n tiene $\varphi(p^n)=p^{n-1}(p-1)$ generadores, obtenemos el resultado. □

Nótese que si F/K es cualquier campo contenido en $K(\Lambda_{P^\alpha})$ entonces el conductor $\mathfrak{F}_F$ de F es un divisor de $\mathcal{P}^\alpha$.

En el curso de la demostración de la Proposición 3.10 calculamos $t_1(\alpha)$, es decir, el número de extensiones cíclicas F/K de grado p tales que $\mathcal{P}$ es el único primo ramificado, $\mathcal{P}_\infty$ se descompone en F/K y $\mathfrak{F}_F|\mathcal{P}^\alpha$ y obtenemos (3.3) para el caso $n=1$. Ya hemos resuelto este caso en el Lema 2.13. Aquí presentamos otra prueba, que es más adecuada para la generalización al caso de extensiones cíclicas de grado p^n.

Proposición 3.10. *Cualquier extensión cíclica F/K de grado p tal que el primo finito $\mathcal{P}$ es el único primo ramificado, $\mathcal{P}_\infty$ es totalmente descompuesto y $\mathfrak{F}_F|\mathcal{P}^\alpha$, está contenida en $K(\Lambda_{P^\alpha})$.*

Demostración. De la teoría de Artin-Schreier (ver la Sección 1.3), tenemos que el campo F está dado por $F=K(y)$ con la ecuación de Artin-Schreier de y normalizada como describe Hasse (ver [4]). Esto es

$$y^p-y=\frac{Q}{P^\lambda},$$

donde $P\in R_T^+$, $Q\in R_T$, $(P,Q)=1$, $\lambda>0$, $p\nmid\lambda$, $\operatorname{gr}Q<\operatorname{gr}P^\lambda$. Ahora bien, el conductor $\mathfrak{F}_F$ satisface $\mathfrak{F}_F=\mathcal{P}^{\lambda+1}$, luego $\lambda\leq\alpha-1$.

Tenemos que si $F=K(z)$ con $z^p-z=a$ entonces existen $j\in\mathbb{F}_q^*$ y $c\in K$ tales que $z=jy+c$ y $a=j\dfrac{Q}{P^\lambda}+\wp(c)$, donde $\wp(c)=c^p-c$ (ver la Proposición 2.6). Si a también está dado en su forma normal entonces $c=\dfrac{h}{P^\gamma}$ con $p\gamma\leq\lambda$ (de hecho $p\gamma<\lambda$ dado que $(\lambda,p)=1$) y $\operatorname{gr}h<\operatorname{gr}P^\gamma$ o bien $h=0$. Sea $\gamma_0:=\left[\dfrac{\lambda}{p}\right]$. Entonces cualquier tal c puede escribirse como $c=\dfrac{hP^{\gamma_0-\gamma}}{P^{\gamma_0}}$. Por lo tanto $c\in\mathcal{G}:=\{\dfrac{h}{P^{\gamma_0}}|h\in R_T,\ \operatorname{gr}h<\operatorname{gr}P^{\gamma_0}=d\gamma_0\text{ o }h=0\}$.

Si $c \in \mathcal{G}$ y $j \in \{1, 2, \ldots, p-1\}$ tenemos

$$\begin{aligned} a = j\frac{Q}{P^\lambda} + \wp(c) &= j\frac{Q}{P^\lambda} + \frac{h^p}{P^{p\gamma_0}} + \frac{h}{P^{\gamma_0}} \\ &= \frac{jQ + P^{\lambda - p\gamma_0}h^p + P^{\lambda-\gamma_0}h}{P^\lambda} = \frac{Q_1}{P^\lambda}, \end{aligned}$$

con gr $Q_1 <$ gr P^λ. Dado que $\lambda - p\gamma_0 > 0$ y $\lambda - \gamma_0 > 0$, tenemos que $(Q_1, P) = 1$. Por lo tanto a está en su forma normal.

Se sigue que el mismo campo tiene $|\mathbb{F}_p^*||\wp(\mathcal{G})|$ diferentes representaciones en forma estándar. Ahora, $\mathcal{G}$ y $\wp(\mathcal{G})$ son grupos aditivos y $\wp : \mathcal{G} \to \wp(\mathcal{G})$ es un epimorfismo de grupos cuyo núcleo es $\ker \wp = \mathcal{G} \cap \{c|\wp(c) = c^p - c = 0\} = \mathcal{G} \cap \mathbb{F}_p = \{0\}$. Tenemos $|\wp(\mathcal{G})| = |\mathcal{G}| = |R_T/(P^{\gamma_0})| = q^{d\gamma_0}$.

De lo anterior obtenemos que el número de diferentes extensiones cíclicas F/K de grado p tales que el conductor de K es $\mathfrak{F}_F = \mathcal{P}^{\lambda+1}$, es igual a

$$\begin{aligned} \frac{\Phi(P^\lambda)}{|\mathbb{F}_p^*||\wp(\mathcal{G})|} &= \frac{q^{d(\lambda-1)}(q^d-1)}{(p-1)q^{d\gamma_0}} = \frac{q^{d(\lambda-[\frac{\lambda}{p}]-1)}(q^d-1)}{p-1} \\ &= \frac{\Phi(P^{\lambda-[\frac{\lambda}{p}]})}{p-1}. \end{aligned} \tag{3.10}$$

Por lo tanto, el número de diferentes extensiones cíclicas F/K de grado p tales que el conductor $\mathfrak{F}_F$ de K es un divisor de $\mathcal{P}^\alpha$ está dado por $t_1(\alpha) = \frac{w(\alpha)}{p-1}$ donde

$$w(\alpha) = \sum_{\substack{\lambda=1 \\ (\lambda,p)=1}}^{\alpha-1} \Phi(P^{\lambda-[\frac{\lambda}{p}]}). \tag{3.11}$$

Para obtener $w(\alpha)$ escribimos $\alpha - 1 = pt_0 + r_0$, $t_0 \geq 0$ y $0 \leq r_0 \leq p-1$. Ahora $\{\lambda|1 \leq \lambda \leq \alpha - 1,\ (\lambda, p) = 1\} = \mathcal{A} \cup \mathcal{B}$ donde $\mathcal{A} = \{pt + r|0 \leq t \leq t_0 - 1,\ 1 \leq r \leq p-1\}$ y $\mathcal{B} = \{pt_0 + r|1 \leq r \leq r_0\}$.
Entonces

$$w(\alpha) = \sum_{\lambda \in \mathcal{A}} \Phi(P^{\lambda - [\frac{\lambda}{p}]}) + \sum_{\lambda \in \mathcal{B}} \Phi(P^{\lambda - [\frac{\lambda}{p}]}).$$

Donde entenderemos que si un conjunto $\mathcal{A}$ o $\mathcal{B}$ es vacío, la suma respectiva es cero. Luego

$$\begin{aligned} w(\alpha) &= \sum_{\substack{0 \le t \le t_0 - 1 \\ 1 \le r \le p-1}} q^{d(pt+r-t-1)}(q^d - 1) + \sum_{r=1}^{r_0} q^{d(pt_0 + r - t_0 - 1)}(q^d - 1) \\ &= (q^d - 1)\left[(\sum_{t=0}^{t_0 - 1} q^{d(p-1)t})(\sum_{r=1}^{p-1} q^{d(r-1)}) + q^{d(p-1)t_0} \sum_{r=1}^{r_0} q^{d(r-1)} \right] \\ &= (q^d - 1)\left[\frac{q^{d(p-1)t_0} - 1}{q^{d(p-1)} - 1} \frac{q^{d(p-1)} - 1}{q^d - 1} + q^{d(p-1)t_0} \frac{q^{dr_0} - 1}{q^d - 1} \right] \\ &= q^{d(p-1)t_0} - 1 + q^{d(p-1)t_0 + dr_0} - q^{d(p-1)t_0} = q^{d((p-1)t_0 + r_0)} - 1 \\ &= q^{d(pt_0 - t_0 + r_0)} - 1 = q^{d(\alpha - 1 - [\frac{\alpha - 1}{p}])} - 1. \end{aligned} \tag{3.12}$$

Por lo tanto, el número de diferentes extensiones cíclicas F/K de grado p tal que $\mathcal{P}$ es el único primo ramificado, $\mathfrak{F}_F | \mathcal{P}^\alpha$ y $\mathcal{P}_\infty$ se descompone, es

$$t_1(\alpha) = \frac{w(\alpha)}{p-1} = \frac{q^{d(\alpha - 1 - [\frac{\alpha - 1}{p}])} - 1}{p-1}.$$

Por el Lema 1.7 (b) se sigue que

$$t_1(\alpha) = \frac{w(\alpha)}{p-1} = \frac{q^{d(\alpha - 1 - \lceil \frac{\alpha}{p} \rceil + 1)} - 1}{p-1} = \frac{q^{d(\alpha - [\frac{\alpha}{p}])} - 1}{p-1} = v_1(\alpha). \tag{3.13}$$

Luego de (3.13), tenemos la demostración de la Proposición 3.10. □

La Proposición 3.10 prueba (3.3) para $n = 1$ y para todo $\alpha \in \mathbb{N}$.

Ahora consideremos cualquier extensión cíclica K_n/K de grado p^n tal que $\mathcal{P}$ es el único primo ramificado y es totalmente ramificado, $\mathcal{P}_\infty$ es descompuesto totalmente en K_n/K y $\mathfrak{F}_{K_n} | \mathcal{P}^\alpha$. Queremos probar que $K_n \subseteq K(\Lambda_{P^\alpha})$, esto es, (3.3): $t_n(\alpha) \le v_n(\alpha)$. Esto se demostrará por inducción sobre n. El caso $n = 1$ es la Proposición 3.10. Supongamos que cualquier extensión cíclica K_{n-1} de grado p^{n-1}, $n \ge 2$ tal que $\mathcal{P}$ es el único primo ramificado y es totalmente ramificado, $\mathcal{P}_\infty$ es descompuesto totalmente en K_{n-1}/K y $\mathfrak{F}_{K_{n-1}} | \mathcal{P}^\delta$ está contenido en $K(\Lambda_{P^\delta})$, donde $\delta \in \mathbb{N}$.

Sea K_n cualquier extensión cíclica de grado p^n tal que $\mathcal{P}$ es el único primo ramificado y es totalmente ramificado, $\mathcal{P}_\infty$ es descompuesto totalmente en K_n/K y $\mathfrak{F}_{K_n}|\mathcal{P}^\alpha$. Sea K_{n-1} el subcampo de K_n de grado p^{n-1} sobre K. Ahora consideramos K_n/K generada por el vector de Witt $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_{n-1}, \beta_n)$, esto es,

$$\wp(\boldsymbol{y}) = \boldsymbol{y}^p \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta}$$

y suponemos que $\boldsymbol{\beta}$ está en su forma normal descrita por Schmid (ver [20] y el Teorema 3.5). Entonces K_{n-1}/K está dada por el vector de Witt $\boldsymbol{\beta}' = (\beta_1, \ldots, \beta_{n-1})$.

Si $\boldsymbol{\lambda} := (\lambda_1, \ldots, \lambda_{n-1}, \lambda_n)$ es el vector de parámetros de Schmid, esto es, cada β_i está dado por

$$\begin{aligned} \beta_i = \frac{Q_i}{P^{\lambda_i}}, \text{ donde } Q_i = 0 \text{ (esto es, } \beta_i = 0) \text{ y } \lambda_i = 0 \text{ o bien} \\ (Q_i, P) = 1, \operatorname{gr} Q_i < \operatorname{gr} P^{\lambda_i},\ \lambda_i > 0 \text{ y } (\lambda_i, p) = 1. \end{aligned}$$

Dado que $\mathcal{P}$ es totalmente ramificado tenemos $\lambda_1 > 0$.

Ahora se calcula la cantidad de extensiones diferentes K_n/K_{n-1} que pueden ser construidas por medio de β_n.

Lema 3.11. *Para un campo fijo K_{n-1} el número de campos diferentes K_n es menor que o igual a*

$$\frac{1 + w(\alpha)}{p} = \frac{1}{p} q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}. \tag{3.14}$$

Demostración. Para $\beta_n \neq 0$, cada ecuación en forma normal está dada por

$$y_n^p - y_n = z_{n-1} + \beta_n, \tag{3.15}$$

donde z_{n-1} es el elemento en K_{n-1} obtenido por la generación de Witt de K_{n-1} por el vector $\boldsymbol{\beta}'$ (ver [20, página 161]). De hecho z_{n-1} está dado, formalmente, por

$$z_{n-1} = \sum_{i=1}^{n-1} \frac{1}{p^{n-i}} \left[y_i^{p^{n-i}} + \beta_i^{p^{n-i}} - (y_i + \beta_i + z_{i-1})^{p^{n-i}} \right],$$

con $z_0 = 0$.

Como en el caso $n = 1$, tenemos que existen $\Phi(P^{\lambda_n})$ diferentes β_n con $\lambda_n > 0$. Con el cambio de variable $y_n \to y_n + c$, $c \in \mathcal{G}_{\lambda_n} := \left\{ \frac{h}{P^{\gamma_n}} | h \in R_T, \text{ gr } h < \text{ gr } P^{\gamma_n} = d\gamma_n \text{ o } h = 0 \right\}$ donde $\gamma_n = \left[\frac{\lambda_n}{p} \right]$, obtenemos $\beta_n \to \beta_n + \wp(c)$, también en forma normal. Por lo tanto, el número de elementos diferentes β_n que proveen el mismo campo K_n con este cambio de variable es $q^{d[\frac{\lambda_n}{p}]}$. Por lo tanto, obtenemos a lo más $\Phi(P^{\lambda_n - [\frac{\lambda_n}{p}]})$ posibles campos K_n para cada $\lambda_n > 0$ (ver 3.10). Más precisamente, si para cada β_n con $\lambda_n > 0$ proponemos $\overline{\beta}_n := \{\beta_n + \wp(c) | c \in \mathcal{G}_{\lambda_n}\}$, entonces cualquier elemento de $\overline{\beta}_n$ da el mismo campo K_n.

Sean

$$\mathcal{A}_{\lambda_n} := \{\overline{\beta_n} | v_{\mathcal{P}}(\beta_n) = -\lambda_n\},$$
$$\mathcal{A} := \bigcup_{\substack{\lambda_n = 1 \\ (\lambda_n, p) = 1}}^{\alpha - 1} \mathcal{A}_{\lambda_n}.$$

Entonces cualquier campo K_n está dado por $\beta_n = 0$ o $\overline{\beta}_n \in \mathcal{A}$. De (3.12) tenemos que el número de campos K_n que contienen al campo fijo K_{n-1} que obtenemos en (3.15) es menor que o igual a

$$\begin{aligned} 1 + |\mathcal{A}| = 1 + w(\alpha) &= q^{d(\alpha - 1 - [\frac{\alpha - 1}{p}])} = q^{d(\alpha - 1 - \lceil \frac{\alpha}{p} \rceil + 1)} \\ &= q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}. \end{aligned} \tag{3.16}$$

Ahora, con la sustitución $y_n \to y_n + j y_1$, $j = 0, 1, \ldots, p - 1$, en (3.15) obtenemos

$$(y_n + j y_1)^p - (y_n + j y_1) = y_n^p - y_n + j(y_1^p - y_1) = z_{n-1} + \beta_n + j\beta_1.$$

Por lo tanto cada una de las extensiones obtenidas en (3.15) son repetidas al menos p veces, esto es, para cada β_n, obtenemos la misma extensión con $\beta_n, \beta_n + \beta_1, \ldots, \beta_n + (p-1)\beta_1$. Vamos a probar que los diferentes $\beta_n + j\beta_1$ corresponden a diferentes elementos de $\{0\} \cup \mathcal{A}$.

Fijamos β_n. Modificamos cada $\beta_n + j\beta_1$ para llevarlo a su forma normal: $\beta_n + j\beta_1 + \wp(c_{\beta_n, j})$ para algún $c_{\beta_n, j} \in K$. De hecho, $\beta_n + j\beta_1$ está siempre en

su forma normal, con la posible excepción en que $\lambda_n = \lambda_1$ y en este caso se tiene para a lo más un índice $j \in \{0, 1, \ldots, p-1\}$: si $\lambda_n \neq \lambda_1$,

$$v_{\mathcal{P}}(\beta_n + j\beta_1) = \begin{cases} -\lambda_n & \text{si } j = 0 \\ -\max\{-\lambda_n, -\lambda_1\} & \text{si } j \neq 0. \end{cases}$$

Cuando $\lambda_n = \lambda_1$ y si $v_{\mathcal{P}}(\lambda_n + j\lambda_1) = u > -\lambda_n = -\lambda_1$ y $p|u$, tenemos para $i \neq j$, $v_{\mathcal{P}}(\beta_n + j\beta_1) = v_{\mathcal{P}}(\beta_n + j\beta_1 + (i-j)\beta_1) = -\lambda_n = -\lambda_1$. En otras palabras $c_{\beta_n,j} = 0$ con muy pocas excepciones.

Cada $\mu = \beta_n + j\beta_1 + \wp(c_{\beta_n,j})$, $j \in \{0, 1, \ldots, p-1\}$ satisface ya sea $\mu = 0$ o bien $\overline{\mu} \in \mathcal{A}$. Veremos que todos estos elementos dan diferentes elementos de $\{0\} \cup \mathcal{A}$.

Si $\beta_n = 0$, entonces para $j \neq 0$, $v_{\mathcal{P}}(j\beta_1) = -\lambda_1$, así $\overline{j\beta}_1 \in \mathcal{A}$. Ahora, si $\overline{j\beta}_1 = \overline{i\beta}_1$, entonces

$$j\beta_1 = \beta'_n + \wp(c_1) \text{ y } i\beta_1 = \beta'_n + \wp(c_2)$$

para algún $\beta'_n \neq 0$ y algunos $c_1\, c_2 \in \mathcal{G}_{\lambda_1}$. Se sigue que $(j-i)\beta_1 = \wp(c_2 - c_1) \in \wp(K)$. Esto no es posible por la elección de β_1, a menos que $j = i$.

Sea $\beta_n \neq 0$. El caso $\beta_n + j\beta_1 = 0$ para algún índice $j \in \{0, 1, \ldots, p-1\}$ ya se ha considerado en el primer caso. Así, consideramos el caso $\beta_n + j\beta_1 + \wp(c_{\beta_n,j}) \neq 0$ para todo j. Si para algunos $i, j \in \{0, 1, \ldots, p-1\}$ tenemos $\overline{\beta_n + j\beta_1 + \wp(c_{\beta_n,j})} = \overline{\beta_n + i\beta_1 + \wp(c_{\beta_n,i})}$ entonces existen β'_n y $c_1\ c_2 \in K$ tales que

$$\beta_n + j\beta_1 + \wp(c_{\beta_n,j}) = \beta'_n + \wp(c_1) \text{ y } \beta_n + i\beta_1 + \wp(c_{\beta_n,i}) = \beta'_n + \wp(c_2)$$

Se sigue que $(j-i)\beta_1 = \wp(c_1 - c_2 + c_{\beta_n,i} - c_{\beta_n,j}) \in \wp(K)$ así que $i = j$.

Luego cada campo K_n es representado por al menos p diferentes elementos de $\{0\} \cup \mathcal{A}$. El resultado se sigue. □

De acuerdo con Schmid (ver [20, página 163]), el conductor de K_n es $\mathcal{P}^{M_n+1}$, donde $M_n = \max\{pM_{n-1}, \lambda_n\}$ y $\mathcal{P}^{M_{n-1}+1}$ es el conductor de K_{n-1}. Dado que

$\mathfrak{F}_{K_n}|\mathcal{P}^\alpha$ tenemos $M_n \leq \alpha - 1$. Luego $pM_{n-1} \leq \alpha - 1$ y $\lambda_n \leq \alpha - 1$. Por lo tanto $\mathfrak{F}_{K_{n-1}}|\mathcal{P}^\delta$ con

$$\delta = \left[\frac{\alpha - 1}{p}\right] + 1.$$

Proposición 3.12. *Recordemos que para n, $\alpha \in \mathbb{N}$, denotamos por $v_n(\alpha)$ al número de grupos cíclicos de orden p^n contenidos en $(R_T/(P^\alpha))^*$. Tenemos*

$$\frac{v_n(\alpha)}{v_{n-1}(\delta)} = \frac{q^{d(\alpha - \lceil \frac{\alpha}{p} \rceil)}}{p}, \quad \text{donde} \quad \delta = \left[\frac{\alpha - 1}{p}\right] + 1.$$

Demostración. De la Proposición 3.9 obtenemos

$$\begin{aligned} v_n(\alpha) &= \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1)}{p^{n-1}(p-1)} \\ &= \frac{q^{d(\alpha - \lceil \frac{\alpha}{p^{n-1}} \rceil)}}{p^{n-1}(p-1)}(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1) \quad \text{y} \\ v_{n-1}(\delta) &= \frac{q^{d(\delta - \lceil \frac{\delta}{p^{n-2}} \rceil)}(q^{d(\lceil \frac{\delta}{p^{n-2}} \rceil - \lceil \frac{\delta}{p^{n-1}} \rceil)} - 1)}{p^{n-2}(p-1)} \\ &= \frac{q^{d(\delta - \lceil \frac{\delta}{p^{n-2}} \rceil)}}{p^{n-2}(p-1)}(q^{d(\lceil \frac{\delta}{p^{n-2}} \rceil - \lceil \frac{\delta}{p^{n-1}} \rceil)} - 1) \end{aligned}$$

Del Lema 1.7 tenemos

$$\begin{aligned} \left[\frac{\delta}{p^{n-2}}\right] - \left[\frac{\delta}{p^{n-1}}\right] &= \left(\left[\frac{\delta - 1}{p^{n-2}}\right] + 1\right) - \left(\left[\frac{\delta - 1}{p^{n-1}}\right] + 1\right) \\ &= \left[\frac{\delta - 1}{p^{n-2}}\right] - \left[\frac{\delta - 1}{p^{n-1}}\right] = \left[\frac{\left[\frac{\alpha - 1}{p}\right]}{p^{n-2}}\right] - \left[\frac{\left[\frac{\alpha - 1}{p}\right]}{p^{n-1}}\right] \\ &= \left[\frac{\alpha - 1}{p^{n-1}}\right] - \left[\frac{\alpha - 1}{p^n}\right] = \left(\left[\frac{\alpha}{p^{n-1}}\right] - 1\right) - \left(\left[\frac{\alpha}{p^n}\right] - 1\right) \\ &= \left[\frac{\alpha}{p^{n-1}}\right] - \left[\frac{\alpha}{p^n}\right], \end{aligned}$$

$$\begin{aligned}\delta - \left\lceil \frac{\delta}{p^{n-2}} \right\rceil &= \left(\left[\frac{\alpha - 1}{p} \right] + 1 \right) - \left(\left[\frac{\delta - 1}{p^{n-2}} \right] + 1 \right) \\ &= \left[\frac{\alpha - 1}{p} \right] - \left[\frac{\delta - 1}{p^{n-2}} \right] = \left[\frac{\alpha - 1}{p} \right] - \left[\frac{\left[\frac{\alpha - 1}{p} \right]}{p^{n-2}} \right] \\ &= \left[\frac{\alpha - 1}{p} \right] - \left[\frac{\alpha - 1}{p^{n-1}} \right].\end{aligned}$$

Luego

$$v_{n-1}(\delta) = \frac{q^{d\left(\left[\frac{\alpha-1}{p}\right] - \left[\frac{\alpha-1}{p^{n-1}}\right]\right)}}{p^{n-2}(p-1)} \left(q^{d\left(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil\right)} - 1 \right)$$

Por lo tanto, de nuevo por el Lema 1.7,

$$\begin{aligned}\frac{v_n(\alpha)}{v_{n-1}(\delta)} &= \frac{\frac{q^{d\left(\alpha - \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil\right)}}{p^{n-1}(p-1)} \left(q^{d(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil)} - 1 \right)}{\frac{q^{d\left(\left[\frac{\alpha-1}{p}\right] - \left[\frac{\alpha-1}{p^{n-1}}\right]\right)}}{p^{n-2}(p-1)} \left(q^{d\left(\lceil \frac{\alpha}{p^{n-1}} \rceil - \lceil \frac{\alpha}{p^n} \rceil\right)} - 1 \right)} = \\ &= \frac{1}{p} q^{d\left(\alpha - \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - \left[\frac{\alpha-1}{p}\right] + \left[\frac{\alpha-1}{p^{n-1}}\right]\right)} \\ &= \frac{1}{p} q^{d\left(\alpha - \left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - (\lceil \frac{\alpha}{p} \rceil - 1) + \left(\left\lceil \frac{\alpha}{p^{n-1}} \right\rceil - 1\right)\right)} = \frac{1}{p} q^{d\left(\alpha - \lceil \frac{\alpha}{p} \rceil\right)}.\end{aligned}$$

Esto prueba el resultado. □

Por lo tanto, de la Proposición 3.12 y del Lema 3.11 (3.14) y como, por la hipótesis de inducción, $t_{n-1}(\delta) = v_{n-1}(\delta)$, obtenemos

$$t_n(\alpha) \leq t_{n-1}(\delta)(\frac{1}{p} q^{d\left(\alpha - \lceil \frac{\alpha}{p} \rceil\right)}) = v_{n-1}(\delta)(\frac{1}{p} q^{d\left(\alpha - \lceil \frac{\alpha}{p} \rceil\right)}) = v_n(\alpha).$$

Esto prueba (3.3) y, por lo tanto, el Teorema 3.1.

3.5. Demostración alternativa

Mantenemos la misma notación que en la secciones anteriores. Sea F/K que satisface las condiciones (3.2) y con conductor un divisor de $\mathcal{P}^\alpha$. Daremos

una demostración alternativa de (3.3), la cual tiene la ventaja de ser más directa. Tenemos $\mathfrak{F}_F = \mathcal{P}^{M_n+1}$ donde

$$M_n = \text{máx}\{p^{n-1}\lambda_1, p^{n-2}\lambda_2, \ldots, p\lambda_{n-1}, \lambda_n\},$$

(ver [20]). Por lo tanto

$$\mathfrak{F}_F|\mathcal{P}^\alpha \text{ si y sólo si } M_n + 1 \leq \alpha \text{ si y sólo si } p^{n-i}\lambda_i \leq \alpha - 1, \quad i = 1, \ldots, n.$$

Así $\lambda_i \leq \left[\dfrac{\alpha-1}{p^{n-i}}\right]$. Estas condiciones nos dan todas las extensiones cíclicas de grado p^n donde $P \in R_T^+$ es el único primo ramificado, es totalmente ramificado, $\mathfrak{p}_\infty$ es descompuesto totalmente y su conductor divide a $\mathcal{P}^\alpha$. Ahora estimaremos el número de formas diferentes de generar a F.

Sea $F = K(\boldsymbol{y})$. Primero, nótese que con el cambio de variable y_i por $y_i + c_i$ para cada $i, c_i \in K$, obtenemos la misma extensión. Para estas nuevas formas de generar a F satisfaciendo (3.2), debemos tener:

(1) Si $\lambda_i = 0$, $c_i = 0$.

(2) Si $\lambda_i > 0$, entonces $c_i \in \{\frac{h}{P^{\gamma_i}} | h \in R_T,\ \text{gr}\, h < \text{gr}\, P^{\gamma_i} = d\gamma_i \text{ o } h = 0\}$, donde $\gamma_i = \left[\frac{\lambda_i}{p}\right]$. Luego tenemos a lo más $\Phi(P^{\lambda_i - \left[\frac{\lambda_i}{p}\right]})$ extensiones para este λ_i (ver (3.10)). Dado que $1 \leq \lambda_i \leq \left[\frac{\alpha-1}{p^{n-i}}\right]$ y $(\lambda_i, p) = 1$, si definimos $\delta_i := \left[\frac{\alpha-1}{p^{n-i}}\right] + 1$, de (3.11)) y (3.12)) obtenemos que hay a lo más

$$w(\delta_i) = \sum_{\substack{\lambda_i = 1 \\ (\lambda_i, p) = 1}}^{\delta_i - 1} \Phi(P^{\lambda_i - \left[\frac{\lambda_i}{p}\right]}) = q^{d\left(\delta_i - 1 - \left[\frac{\delta_i - 1}{p}\right]\right)} - 1 \tag{3.17}$$

diferentes expresiones para todos los posibles $\lambda_i > 0$.
Ahora por el Lema 1.7 tenemos

$$\delta_i - 1 - \left[\frac{\delta_i - 1}{p}\right] = \left[\frac{\alpha-1}{p^{n-i}}\right] - \left[\frac{\left[\frac{\alpha-1}{p^{n-i}}\right]}{p}\right] = \left[\frac{\alpha-1}{p^{n-i}}\right] - \left[\frac{\alpha-1}{p^{n-i+1}}\right].$$

Por lo tanto

$$w(\delta_i) = q^{d\left(\left[\frac{\alpha-1}{p^{n-i}}\right] - \left[\frac{\alpha-1}{p^{n-i+1}}\right]\right)} - 1. \tag{3.18}$$

Cuando $\lambda_i = 0$, tenemos a lo más $w(\delta_i) + 1$ extensiones con parámetro λ_i. Por lo tanto, dado que $\lambda_1 > 0$ y $\lambda_i \geq 0$ para $i = 2, \ldots, n$, tenemos que el número de extensiones que satisfacen las condiciones (3.2) y con conductor un divisor de $\mathcal{P}^\alpha$ es a lo más

$$s_n(\alpha) := w(\delta_1) \cdot \prod_{i=2}^{n} (w(\delta_i) + 1).$$

De (3.18) obtenemos

$$s_n(\alpha) = (q^{d\left(\left[\frac{\alpha-1}{p^{n-1}}\right]-\left[\frac{\alpha-1}{p^n}\right]\right)} - 1) \cdot \prod_{i=2}^{n} q^{d\left(\left[\frac{\alpha-1}{p^{n-i}}\right]-\left[\frac{\alpha-1}{p^{n-i+1}}\right]\right)}.$$

Luego $\prod_{i=2}^{n}(w(\delta_i)+1) = q^{d\mu}$, donde

$$\begin{aligned}\mu &= \sum_{i=2}^{n}\left(\left[\frac{\alpha-1}{p^{n-i}}\right] - \left[\frac{\alpha-1}{p^{n-i+1}}\right]\right) = \sum_{i=2}^{n}\left[\frac{\alpha-1}{p^{n-i}}\right] - \sum_{j=1}^{n-1}\left[\frac{\alpha-1}{p^{n-j}}\right] \\ &= \left[\frac{\alpha-1}{p^{n-n}}\right] - \left[\frac{\alpha-1}{p^{n-1}}\right] = \alpha - 1 - \left[\frac{\alpha-1}{p^{n-1}}\right].\end{aligned}$$

Por lo tanto

$$\begin{aligned}s_n(\alpha) &= (q^{d\left(\left[\frac{\alpha-1}{p^{n-1}}\right]-\left[\frac{\alpha-1}{p^n}\right]\right)} - 1) \cdot q^{d\left(\alpha-1-\left[\frac{\alpha-1}{p^{n-1}}\right]\right)} \\ &= q^{d\left(\left[\frac{\alpha-1}{p^{n-1}}\right]-\left[\frac{\alpha-1}{p^n}\right]+\alpha-1-\left[\frac{\alpha-1}{p^{n-1}}\right]\right)} - q^{d\left(\alpha-1-\left[\frac{\alpha-1}{p^{n-1}}\right]\right)} \\ &= q^{d\left(\alpha-1-\left[\frac{\alpha-1}{p^n}\right]\right)} - q^{d\left(\alpha-1-\left[\frac{\alpha-1}{p^{n-1}}\right]\right)}.\end{aligned}$$

Del Lema 1.7 (b) obtenemos

$$\alpha - 1 - \left[\frac{\alpha-1}{p^n}\right] = \alpha - \left[\frac{\alpha}{p^n}\right] \quad \text{y} \quad \alpha - 1 - \left[\frac{\alpha-1}{p^{n-1}}\right] = \alpha - \left[\frac{\alpha}{p^{n-1}}\right].$$

Así, por la Proposición 3.9

$$s_n(\alpha) = q^{d\left(\alpha-\left\lceil\frac{\alpha}{p^n}\right\rceil\right)} - q^{d\left(\alpha-\left\lceil\frac{\alpha}{p^{n-1}}\right\rceil\right)} = p^{n-1}(p-1)v_n(\alpha).$$

Finalmente, como en el caso Artin-Schreier, el cambio de variable $\boldsymbol{y} \to \boldsymbol{j} \overset{\bullet}{\times} \boldsymbol{y}$ con $\boldsymbol{j} \in W_n(\mathbb{F}_p)^* \cong (\mathbb{Z}/p^n\mathbb{Z})^*$ da el mismo campo y tenemos $\boldsymbol{\beta} \to \boldsymbol{j} \overset{\bullet}{\times} \boldsymbol{\beta}$. Por lo tanto

$$t_n(\alpha) \leq \frac{s_n(\alpha)}{\varphi(p^n)} = \frac{s_n(\alpha)}{p^n(p-1)} = v_n(\alpha).$$

Esto prueba (3.3) y, por lo tanto, el Teorema 3.1. Finalmente, presentamos dos ejemplos que ilustran el resultado y las técnicas usadas.

Ejemplo 3.2. Viene del Ejemplo 1.5. Consideremos $n = 2$, $q = p = 3$ y $\boldsymbol{y} = (y_1, y_2)$ de manera que

$$\boldsymbol{y}^3 \overset{\bullet}{-} \boldsymbol{y} = (T, 0).$$

Tenemos

$$\begin{array}{cc} K_2 = K_1(y_2) & \mathfrak{P}_\infty^9 \\ \Big| 3 & \Big| \\ K_1 = K_0(y_1) & \mathfrak{p}_\infty^3 \\ \Big| 3 & \Big| \\ K = K_0 = \mathbb{F}_3(T) & \mathcal{P}_\infty \end{array}$$

Entonces $y_1^3 - y_1 = T$ donde $(T)_{K_0} = \frac{\mathcal{P}_0}{\mathcal{P}_\infty}$, y $y_2^3 - y_2 + y_1^7 - y_1^5 = 0$, $y_2^3 - y_2 = -y_1^4 \cdot T$ donde $(-y_1^4 \cdot T)_{K_1} = \frac{\mathfrak{A}}{\mathfrak{p}_\infty^4 \mathfrak{p}_\infty^3} = \frac{\mathfrak{A}}{\mathfrak{p}_\infty^7}$ pues $\nu_{\infty,1}(y_1^3 - y_1) = -3$, luego $\nu_{\infty,1}(y_1) = -1$.

La contribución de $\mathfrak{P}_\infty$ al diferente $\mathfrak{D}_{K_2/K}$ es $\mathfrak{P}_\infty$ a la potencia

$$(p-1)\sum_{i=1}^{n}(M_{i+2-n}+1)p^{i-1},$$

(ver [12, Proposition 1]). Como $n = 2$, $\lambda_2 = 0$, y $\lambda_1 = 1$, tenemos $M_1 = \lambda_1 = 1$ y $M_2 = \text{máx}\{3^{2-1}(1), \lambda_2\} = 3$. Se tiene

$$\mathfrak{D}_{K_2/K} = \mathfrak{P}_\infty^{28}.$$

El exponente en el conductor es $M_2 + 1$ (ver [20, página 163]). Luego el conductor es

$$\mathfrak{F}_{K_2} = \mathcal{P}_\infty^4.$$

Por la Proposición 3.6, la extensión de constantes relevante corresponde a $\mathbb{F}_{q^{p^n}} = \mathbb{F}_{3^{3^2}} = \mathbb{F}_{3^9}$, por lo tanto,

$$K_2 \subseteq \mathbb{F}_{3^9}(T)(\Lambda_{1/T^4}).$$

Obtengamos en qué ciclotómico se encaja K_1. Por el Lema 2.13 tenemos $K_1 \subseteq \mathbb{F}_{q^p}(T)(\Lambda_{1/T^{\lambda_1+1}})$, por lo tanto

$$K_1 \subseteq \mathbb{F}_{27}(T)(\Lambda_{1/T^2}).$$

Ejemplo 3.3. Viene del Ejemplo 3.1.
Sean $K = \mathbb{F}_3(T)$ y $n = 2$. Consideremos $K_2 = K(\boldsymbol{y})$ donde

$$\boldsymbol{y}^3 \overset{\bullet}{-} \boldsymbol{y} = \boldsymbol{\beta} \text{ con } \boldsymbol{\beta} = \left(\frac{1}{T^2-1}, \frac{T^6+T^3-T-1}{T(T^2-1)^3}\right).$$

Por la Observación 3.2, tenemos $K_2 = K(\boldsymbol{y}) \subseteq K(z_1, z_2, z_3)$ donde

$$\begin{aligned} z_1^3 \overset{\bullet}{-} z_1 &= \left(0, \frac{1}{T}\right), \\ z_2^3 \overset{\bullet}{-} z_2 &= \left(\frac{-1}{T-1}, 0\right), \\ z_3^3 \overset{\bullet}{-} z_3 &= \left(\frac{1}{T+1}, 0\right). \end{aligned}$$

Estudiaremos separadamente las tres extensiones.

1. $z_{11}^3 - z_{11} = 0$ y $z_{12}^3 - z_{12} + z_{11}^7 - z_{11}^5 = \frac{1}{T}$. Podemos tomar $z_{11} = 0$, luego $z_{12}^3 - z_{12} = \frac{1}{T}$. $M_1 = \lambda_1 = 0$ y $\lambda_2 = 1$, así $M_2 = \text{máx}\{3^{2-1}(0), 1\} = 1$. Entonces la aportación de $\mathcal{P}_0$ al conductor es $\mathcal{P}_0^2$.

2. $z_{21}^3 - z_{21} = \frac{-1}{T-1}$ y $z_{22}^3 - z_{22} + z_{21}^7 - z_{21}^5 = 0$, luego $z_{22}^3 - z_{22} = \frac{1}{T-1} z_{21}^4$. Tenemos $M_1 = \lambda_1 = 1$ y $\lambda_2 = 0$, así $M_2 = \text{máx}\{3^{2-1}(1), 0\} = 3$. La aportación de $\mathcal{P}_1$ al conductor es $\mathcal{P}_1^4$.

3. $z_{31}^3 - z_{31} = \frac{1}{T+1}$ y $z_{32}^3 - z_{32} + z_{31}^7 - z_{31}^5 = 0$, luego $z_{32}^3 - z_{32} = \frac{-1}{T+1} z_{31}^4$. Tenemos $M_1 = \lambda_1 = 1$ y $\lambda_2 = 0$, así $M_2 = \text{máx}\{3^{2-1}(1), 0\} = 3$. La aportación de $\mathcal{P}_{-1}$ al conductor es $\mathcal{P}_{-1}^4$.

La extensión de constantes relevante corresponde a $\mathbb{F}_{q^{p^n}} = \mathbb{F}_{3^9}$. Concluimos que en este caso

$$K_2 \subseteq \mathbb{F}_{3^9}(T)(\Lambda_{T^2(T^2-1)^4}).$$

Conclusiones y perspectivas

Se consideraron separadamente los casos de ramificación moderada y ramificación salvaje. La prueba del teorema en el caso moderadamente ramificado es similar a la de Hilbert. Por otro lado, el hecho de que, a diferencia del caso clásico, para campos de funciones haya una infinidad de extensiones cíclicas de grado p sobre $\mathbb{F}_q(T)$ donde precisamente un divisor primo fijo es ramificado, hizo necesaria la búsqueda de una nueva estrategia. Un primer paso fue, para el caso de ramificación salvaje, el encaje de las extensiones de Artin-Schreier en extensiones ciclotómicas compuestas con extensiones de constantes y, en general, el encaje de las extensiones cuadráticas en extensiones ciclotómicas compuestas con extensiones de constantes. El siguiente objetivo fue estudiar los vectores de Witt con el fin de encajar las p-extensiones cíclicas en extensiones ciclotómicas compuestas con extensiones de constantes. La experiencia con las extensiones de Artin-Schreier fue provechosa para las demostraciones del caso de extensiones cíclicas de grado p^n, tanto en el argumento por inducción sobre n como en el directo.

Se plantea a futuro el estudio de caracteres sobre campos de funciones en una variable con campo de constantes finito y no sólo sobre campos de funciones racionales, para lo cual es necesario abordar el estudio de la máxima extensión abeliana de un campo de funciones arbitrario. Puesto que uno de los objetivos de los módulos de Drinfeld es la generalización del Teorema de Kronecker-Weber a este tipo de campos, será importante tener en mente la estrategia de conteo que resultó fructífera en el caso de campos de funciones racionales, para la exploración de este tema.

Bibliografía

[1] Dummit, David S. & Foote, Richard M., *Abstract Algebra*, John Wiley and Sons, Inc., 2^{nd} ed., 1999.

[2] Galovich, S. and Rosen, M. *The class number of cyclotomic function fields*, J. Number Theory 13, (1981), 363-375.

[3] Galovich, S. and Rosen, M. *Units and class groups in cyclotomic function fields*, J. Number theory 14,(1982), 156-184.

[4] Hasse, Helmut, *Theorie der relativ–zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*, J. Reine Angew. Math. 172, (1934), 37-54.

[5] Harald Niederreiter and Chaoping Xing, *Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places*, Acta Arith. 79 (1997), no. 1, 59-76.

[6] Hayes, David, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. 189, (1974), 77-91.

[7] Hilbert, David *The Theory of Algebraic Number Fields*, Springer-Verlag, Berlin Heidelberg New York, 1998.

[8] Lam Estrada, Pablo, *Campos de funciones ciclotómicos y extensiones seudo-cogalois*, Tesis doctoral, CINVESTAV-IPN, México 1997.

[9] Lam-Estrada, Pablo and Villa-Salvador, Gabriel Daniel, *Some remarks on the theory of cyclotomic function fields*, Rocky Mountain J. Math., 31, (2001), 483-502.

[10] Lang, Serge, *Cyclotomic Fields*, Springer-Verlag, New York, GTM 59, 1978.

[11] Lang, Serge, *Algebraic Number Theory*, Springer-Verlag, New York, GTM 110, 1986.

[12] Madden, Daniel J., *Arithmetic in Generalized Artin-Schreier Extensions of $k(x)$*, Journal of Number Theory 10, No. 3 (1978), 303-323.

[13] Maldonado Ramírez, Myriam Rosalía, *Sobre p-extensiones de campos de funciones con mapeo de Hasse-Witt nulo*, Tesis doctoral, CINVESTAV-IPN, México 2008.

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

[15] Rosen, Michael, *The Hilbert class field in function fields*, Expos. Math, 5, (1987), 365-378.

[16] Rosen, Michael, *Number Theory in Function Fields*, Springer-Verlag, New York, GTM 210, 2002.

[17] Salas-Torres, Julio Cesar, Rzedowski-Calderón, Martha and Villa-Salvador, Gabriel, *Tamely ramified extensions and cyclotomic fields in characteristic p*, Palestine Journal of Mathematics, 2, No. 1 (2013), 1-5.

[18] Salas-Torres, Julio Cesar, Rzedowski-Calderón, Martha and Villa-Salvador, Gabriel, *Artin-Schreier and Cyclotomic Extensions*, JP Journal of Algebra, Number Theory and Applications, 30, No. 2 (2013), 173-190.

[19] Salas-Torres, Julio Cesar, Rzedowski-Calderón, Martha and Villa-Salvador, Gabriel, *A combinatorial proof of the Kronecker-Weber Theorem in positive characteristic*, Finite Fields and Their Applications, 26, (2014), 144-161.

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

[21] Serre, Jean-Pierre, *Local Fields*, Springer-Verlag, New York, GTM 67, 1979.

[22] Villa Salvador, Gabriel Daniel, *Introducción a la Teoría de las Funciones Algebraicas*, México, Fondo de Cultura Económica, 2003.

[23] Villa Salvador, Gabriel Daniel, *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, Boston, 2006.

[24] Gabriel Daniel Villa-Salvador, *Vectores de Witt*, Boletín del Departamento de Matemáticas de la Universidad de Sonora (1989).

[25] Washington, Lawrence C., *Introduction to Cyclotomic Fields*, Springer-Verlag, Second edition, GTM 83, 1982.

[26] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. Reine Angew. Math. **176** (1936), 126-140.