UNIVERSIDAD AUTÓNOMA METROPOLITANA
IZTAPALAPA
DEPARTAMENTO DE MATEMÁTICAS

TEORÍA DE COGALOIS SOBRE CAMPOS DE FUNCIONES

Tesis que presenta
M. en C. Marco Antonio Sánchez Mirafuentes
para obtener el grado de
Doctor en ciencias (Matemáticas)

Jurado:

Presidente: Dr. Florian Luca

Secretario: Dr. Felipe de Jesús Zaldívar Cruz

Vocal: Dr. Pedro Luis del Ángel Rodriguez

Vocal: Dr. Rogelio Fernández Alonso Gonzalez

Vocal: Dr. Mario Pineda Ruelas

México, D.F. Marzo de 2014

Índice general

PARA KARLA ...

Agradecimientos

Quisiera agradecer en primer lugar a mi familia, en especial a mi madre Adriana Mirafuentes Valencia, mi tía Ángela Mirafuentes Valencia y mi hermano Jorge José Sánchez Mirafuentes, por el apoyo brindado para terminar esta tarea. Por otro lado agradezco profundamente al Dr. Gabriel Daniel Villa Salvador por el apoyo y guía para la realización de esta tesis doctoral, sus consejos fueron valiosos para el desarrollo de las ideas aquí plasmadas. También agradezco a mis sinodales Dr. Pedro Luis del Ángel Rodriguez, Dr. Rogelio Fernández Alonso Gonzales, Dr. Florian Luca, Dr. Mario Pineda Ruelas y Dr. Felipe de Jesús Zaldívar Cruz, por las sugerencias hechas para mejorar este trabajo. Finalmente agradezco al CONACYT por el apoyo económico dado por medio de la beca que se me asigno.

Resumen

En este trabajo estudiaremos algunos aspectos algebraicos de las extensiones de campos de funciones $L/\mathbb{F}_q$, es decir una extensión de campos de $\mathbb{F}_q$, finitamente generada, con grado de trascendencia 1. Nos restringiremos a considerar campos de funciones $L/\mathbb{F}_q$ tales que $\mathbb{F}_q(T) \subseteq L \subseteq \overline{\mathbb{F}_q(T)}$, donde $\overline{\mathbb{F}_q(T)}$ denota la cerradura algebraica de $\mathbb{F}_q(T)$. En particular nos fijaremos en la acción de Carlitz-Hayes, la cual ha servido para definir análogos a los campos ciclotómicos clásicos en campos de funciones. Un aspecto, importante, que se considera aquí, es del estudiar el módulo de torsión de una extensión de campos de funciones L/K, es decir

$$T(L/K) = \{u \in L \mid \text{existe un polinomio } M \in \mathbb{F}_q[T] \text{ tal que } u^M \in K\}$$

y las extensiones de campos de funciones L/K de la forma

$$L = K(T(L/K)).$$

Parte del trabajo hecho en esta tesis esta publicado en [22].

Introducción

En la teoría de campos de funciones, es decir, extensiones de campos L/k tales que L es finitamente generado sobre k y el grado de trascendencia de L sobre k es uno, a mediados de los años 1930's, al menos en el caso $L = \mathbb{F}_q(T)$ y $k = \mathbb{F}_q$, L. Carlitz estudia análogos a la funciones exponencial, que denota por $\psi(u)$, y logarítmica, en la completación de $K = \mathbb{F}_q(T)$ y encuentra la relación siguiente: $\psi(Mu) = \omega_M(\psi(u))$, donde ω_M es un polinomio aditivo con coeficientes en $\mathbb{F}_q[T]$, determinado únicamente por $M \in \mathbb{F}_q[T]$, ver [4]. En [5], continuación del artículo anterior, Carlitz estudia los polinomios ω_M y descubre análogos de los polinomios ciclótomicos.

Muchos años después, D. Hayes, da estructura de $\mathbb{F}_q[T]$-módulo a la cerradura algebraica de $\mathbb{F}_q(T)$, $\overline{\mathbb{F}_q(T)}$, conocida como *la acción de Carlitz-Hayes* como sigue: sean $u \in \overline{\mathbb{F}_q(T)}$ y $M \in \mathbb{F}_q[T]$ se define $M \cdot u = \omega_M(u)$.

Se demuestra que, en efecto, se tiene que esta definición da a $\overline{\mathbb{F}_q(T)}$ estructura de $\mathbb{F}_q[T]$-módulo (ver [25] Capítulo 12). Por otra parte, esto da

lugar a los análogos de los campos ciclotómicos sobre el campo $\mathbb{F}_q(T)$, y a una teoría de campos de clases sobre L (ver [13]).

En este trabajo se intenta, en primer lugar, generalizar la teoría de cogalois, utilizando la acción de Carlitz-Hayes. Dada una extensión arbitraria de campos, L/K, se define el grupo

$$T(L/K) = \{u \in L^* \mid \text{existe un entero positivo } n, \text{ tal que } u^n \in K\}$$

donde $L^* = L\backslash\{0\}$.

Al grupo cociente $\text{cog}(L/K) := T(L/K)/K^*$ se le llama *grupo de cogalois* de L/K.

Se dice que L/K es una extensión de *cogalois* si:
(1) $L = K(T(L/K))$ y
(2) $card(\text{cog}(L/K)) \leq [L : K]$,
ver [10] y [2].

En este contexto se tiene una definición de lo que se entiende por una extensión *radical ciclotómica*. En primer lugar, una extensión L/K se dice *radical* si $L = K(\alpha_1, \ldots, \alpha_r)$ y existen $N_i \in \mathbb{F}_q[T]$ tales que $\alpha_i^{N_i} \in K$, $i = 1, \ldots, r$. En segundo lugar, una extensión L/K es *pura* si para cada polinomio mónico irreducible $M \in \mathbb{F}_q[T]$ y cada $u \in L$ tal que $u^M = 0$ se tiene que $u \in K$. Así diremos que L/K es radical ciclotómica si es separable, radical y pura.

La extensiones radicales L/K tienen propiedades análogas a la extensiones radicales, en el sentido de [1], o las extensiones coseparables, en el sentido de [10]. Por lo tanto si L/K es radical y Galois, entonces dado un $\overline{\alpha} \in \text{cog}(L/K)$, cuyo orden es M, se tiene que si λ_M denota un generador de Λ_M, entonces $\lambda_M \in L$, ver proposición 2.7, lema 2.6 y la definición 2.1.

También, en algunas extensiones radicales L/K, es posible encontrar un elemento primitivo, $\alpha \in L$, de tal manera que existe $M \in \mathbb{F}_q[T]$ tal que $\alpha^M \in K$, ver proposición 2.8.

Por otra parte, se tienen algunos resultados análogos a los presentados en [24] lema 2.1, ver lema 1.31 y en [12] lema 1, lema 5 y lema 9, ver lema 2.11, lema 2.12 y la proposición 2.13.

Por otro lado, las extensiones radicales tienen propiedades como:
- Si L'/K es pura y L es un campo intermedio, entonces L'/L y L/K son puras y recíprocamente, ver lema 2.14.
- Un análogo parcial del teorema 1.6 de [10], ver proposición 2.15.
- La proposición 2.23, junto con la proposición 1.7, muestra que bajo ciertas circunstancias, el módulo $\text{cog}(L/K)$ es finito.
- En la subsección 3.4, de este trabajo, se consideraron las retículas con el orden la contención usual entre conjuntos siguientes:

Sea E/L una extensión de Galois con grupo de Galois Γ. Por lo que tenemos las reticulas

$$\{L' \mid L' \text{ es una extensión de } L \text{ contenida en } E\}$$

y

$$\{U \mid U \text{ es subgrupo de } Z^1(\Gamma, \mu(E))\}.$$

Así la proposición 2.30 relaciona las retículas anteriores y da una condición necesaria y suficiente para que una extensión L'/L con $L' \subseteq E$ sea radical. Este resultado a su vez muestra la proposición 2.31 de este trabajo.

- Además se tiene que si L/K es radical ciclotómica, entonces existe $m \in \mathbb{N}$ tal que $[L : K] = p^m$, ver teorema 2.39 y teorema 2.40.

- Finalmente, se obtiene una cota superior de la cardinalidad de $\mathrm{cog}(L/K)$, ver teorema 2.57.

En segundo lugar, se trata de estudiar extensiones análogas a las extensiones de Kummer, pero usando la acción de Carlitz-Hayes, siguiendo, en primer lugar el trabajo de W. Chi [6] y usando la teoría clásica de Kummer, ver [18]. Para la teoría de Kummer empezamos con un campo K que contenga al grupo μ_n de las raíces n-ésimas de la unidad, con n primo relativo a la caracteristica de K, así una *extensión de Kummer de exponente* n de K es un campo de la forma

$$L = K(\sqrt[n]{\Delta})$$

donde Δ es un subgrupo de K^* que contiene al subgrupo $(K^*)^n$, ver [26] Capítulo 5.

Notación

C_m denota al grupo cíclico de orden m.

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

$\overline{k}$ denota la cerradura algebraica del campo k.

R_T denota al anillo $\mathbb{F}_q[T]$.

$\mu(K)$ denota el conjunto de raíces de Carlitz contenidas en el campo K, es decir es el conjunto $\{u \in K \mid \text{existe } M \in R_T talque u^M = 0\}$.

$\mu(K)(N)$ denota al conjunto de $x \in \mu(K)$ tales que $x^N = 0$, donde $N \in R_T$.

$[M, N]$ denota el mínimo común múltiplo de los polinomios M y N.

(M, N) denota al máximo común divisor de los polinomios M y N.

$\mathfrak{L}_p(A, B)$ denota al conjunto de transformaciones lineales de A en B, sobre $\mathbb{F}_p$.

$\mathfrak{M}_{\mathfrak{m}\times\mathfrak{n}}(\mathbb{F}_\mathfrak{p})$ denota al conjunto de matrices, de tamaño m por n, con entradas en $\mathbb{F}_p$.

$(G : H)$ denota el índice del grupo H en G.

$(M : N)$ denota el índice del módulo N en M.

Capítulo 1

Preliminares algebraicos.

1.1. El módulo de Carlitz-Hayes

Como se mencionó en la introducción, usaremos la acción de Carlitz-Hayes, que definiremos a continuación.

Sea p un número primo, $q = p^n$, $n \in \mathbb{N}$. Sean $\varphi : \overline{k} \to \overline{k}$ el automorfismo de Frobenius, $\varphi(u) = u^q$, y $\mu_T : \overline{k} \to \overline{k}$, denota al endomorfismo multiplicar por T, es decir, $\mu_T(u) = Tu$.

DEFINICIÓN 1.1. Se define una acción de R_T en $\overline{k}$ de la forma siguiente: si $M \in R_T$, $u \in \overline{k}$, entonces

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

es decir, si $M = a_0 + a_1T + \cdots + a_dT^d$, se tiene que

$$u^M = a_0u + a_1(\varphi + \mu_T)(u) + \cdots + a_d(\varphi + \mu_T)^d(u).$$

Esta acción tiene las siguientes propiedades (ver [25] Capitulo 12):

Para cada $M, N \in R_T$ y $u, v \in \overline{k}$ se tiene

$(u + v)^M = u^M + v^M$ y $u^{M+N} = u^M + u^N$

$u^{MN} = (u^M)^N$ y $u^1 = u$

Así $\overline{k}$ tiene estructura de R_T-módulo, llamado *módulo de Carlitz-Hayes*.

Por otro lado, si $M \in R_T$ es conveniente tener la definición siguiente

DEFINICIÓN 1.2. Se define Λ_M como el conjunto de puntos de M-torsión de $\overline{k}$, es decir

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

Obsérvese que Λ_M es un R_T-submódulo de $\overline{k}$.

OBSERVACIÓN 1.3. El módulo Λ_M es el análogo a la n-torsión definida sobre $\overline{\mathbb{Q}}^*$. Así como la n-torsión es un $\mathbb{Z}$-módulo cíclico, puesto que son las raíces de la unidad, es posible demostrar que Λ_M es R_T-módulo cíclico, ver [25] Capítulo 12. Denotamos por λ_M un generador de Λ_M, y a veces diremos que λ_M es una raíz primitiva de Carlitz.

Por otro lado, en un contexto más general, es posible definir una función, *la exponencial de Carlitz*, dada por la serie

$$\mathrm{ex}(u) = \sum_{j=0}^{\infty} \frac{u^{q^j}}{D_j}$$

donde

(i) Para cada $j \in \mathbb{N}$ se define

$$[j] = T^{q^j} - T$$

(ii) Para $j = 0$ definimos $D_0 = 1$ y si $j \in \mathbb{N}$ definimos

$$D_j = [j][j-1]^q \cdots [1]^{q^{i-1}}$$

ver [8] Capítulo 3.

Esta función tiene las siguientes propiedades

(i) ex es aditiva
(ii) Sea $\xi = \lambda\xi_*$ donde λ es cualquier raíz de la ecuación $x^{q-1} = -[1]$ y

$$\xi_* = \prod_{j=1}^{\infty}(1 - \frac{[j]}{[j+1]})$$

Entonces ex admite una representación en forma de producto infinito, es decir

$$ex(u) = u \prod_{\alpha \in \xi R_T \setminus \{0\}} (1 - \frac{u}{\alpha})$$

Además los únicos ceros de ex son 0 y todos los elementos de $\xi R_T \setminus \{0\}$, ver [8] Capítulo 3.
(iii) Satisface la ecuación funcional

$$\mathrm{ex}(Tu) = (\mathrm{ex}(u))^T = \mathrm{ex}(u)^q + T\mathrm{ex}(u)$$

Ver [8] Capítulo 3 para más detalles.

Por otro lado, si $M \in R_T$ entonces $\lambda_M = \mathrm{ex}(\frac{\xi}{M})$ es un generador de Λ_M, ver [7] Teorema 6.5.

DEFINICIÓN 1.4. Si $M \in R_T$, $M \neq 0$, $\Phi(M)$ denota el número de elementos de $(R_T/(M))^*$, las unidades de $(R_T/(M))$.

Se tiene que

$$\Phi(M) = \text{card}(\{N + (M) \mid (N) + (M) = 1\}) = \text{card}((R_T/(M))^*).$$

Por lo tanto Φ es el análogo a la función φ de Euler.

En el caso de campos numéricos, $\mathbb{Q}(\zeta_n)$ es el campo ciclótomico de las n-raíces de la unidad, $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es una extensión de Galois de grado $\varphi(n)$, con grupo de Galois $(\mathbb{Z}/n\mathbb{Z})^*$. El análogo para campo de funciones será:

TEOREMA 1.5. *Si $M \in R_T$, entonces $k(\Lambda_M)/k$ es una extensión de Galois de grado $\Phi(M)$ y grupo de Galois $(R_T/M)^*$. En particular $k(\Lambda_M)/k$ es una extensión abeliana.*

Ver [25] Capítulo 12, para más detalles.

Si $M = \zeta Q_1^{\alpha_1} \cdots Q_s^{\alpha_s}$, donde los Q_i son mónicos irreducibles y $\zeta \in (\mathbb{F}_q)^*$, entonces

$$\Phi(M) = \Phi(Q_1^{\alpha_1}) \cdots \Phi(Q_s^{\alpha_s}) = N(M) \prod_{Q_i} (1 - \frac{1}{N(Q_i)}). \tag{1.1}$$

donde $N(M) = q^{\deg(M)}$.

LEMA 1.6. *Sean $A, B \in R_T \setminus \{0\}$. Entonces*

$$\Phi(AB)\Phi((A,B)) = \Phi(A)\Phi(B)N((A,B)).$$

Demostración. Podemos suponer que ambos polinomios son no constantes. Considere los conjuntos

$$D_A = \{\pi \in R_T \mid \pi \text{ es mónico e irreducible y divide a } A\}$$

y

$$D_B = \{\mu \in R_T \mid \mu \text{ es mónico e irreducible y divide a } B\}.$$

Sean $D_{A\setminus B} = \{\pi \in D_A \mid \pi \nmid B\}$ y $D_{B\setminus A} = \{\mu \in D_B \mid \mu \nmid A\}$. Entonces por (1.1) se puede escribir:

$$\Phi(A)\Phi(B) = N(A) \prod_{\pi \in D_A} (1 - \frac{1}{N(\pi)}) N(B) \prod_{\mu \in D_B} (1 - \frac{1}{N(\mu)}).$$

Por la definición de $N(M)$ se sigue que $N(A)N(B) = N(AB)$. Por otro lado utilizando los conjuntos $D_{A\setminus B}$ y $D_{B\setminus A}$ el producto $\prod_{\pi \in D_A}(1 - \frac{1}{N(\pi)}) \prod_{\mu \in D_B}(1 - \frac{1}{N(\mu)})$ se puede escribir como:

$$\prod_{\pi \in D_{A\setminus B}} (1 - \frac{1}{N(\pi)}) \prod_{\pi \notin D_{A\setminus B}} (1 - \frac{1}{N(\pi)}) \prod_{\mu \in D_{B\setminus A}} (1 - \frac{1}{N(\mu)}) \prod_{\mu \notin D_{B\setminus A}} (1 - \frac{1}{N(\mu)}).$$

Notamos que $D_A \setminus D_{A\setminus B} = D_B \setminus D_{B\setminus A}$, de este modo los tres primeros términos del producto anterior, junto con $N(AB)$, dan lugar a $\Phi(AB)$. Finalmente, si al último término lo multiplicamos y dividimos por $N((A,B))$, se obtiene $\frac{\Phi((A,B))}{N((A,B))}$, de donde se sigue el resultado. □

PROPOSICIÓN 1.7. *Sean $q > 2$, $M \in R_T$ no constante. Considere la extensión $k(\Lambda_M)/k$. Entonces $\mu(k(\Lambda_M)) = \Lambda_M$.*

Demostración. Bastará mostrar la contención $\mu(k(\Lambda_M)) \subseteq \Lambda_M$. Sea $u \in \mu(k(\Lambda_M))$, existe un $S \in R_T$ tal que

$$X^S = \prod_{\substack{N|S \\ N \text{ es mónico}}} \Psi_N(X)$$

y $u^S = 0$ ver [25] proposición 12.3.13. Digamos que $\Psi_N(u) = 0$. Como la extensión $k(\Lambda_M)/k$ es de Galois, se sigue que el generador de Λ_N, λ_N, está en $k(\Lambda_M)$.

Así $k(\Lambda_M)$ contiene un generador de Λ_N. Sea $R = [M,N]$. Entonces, puesto que $R = \frac{MN}{(M,N)}$ y $(M,N) = P_1M + Q_1N$, se tiene que

$$\lambda_R = \lambda_{MN}^{(M,N)} = \lambda_{MN}^{P_1M+Q_1N} = \lambda_{MN}^{MP_1} + \lambda_{MN}^{NQ_1} = \lambda_N^{P_1} + \lambda_M^{Q_1}$$

así se tiene que $\lambda_R \in k(\Lambda_M)$.

Obsérvese que $\Lambda_R = \Lambda_M + \Lambda_N$, ya que claramente si $u \in \Lambda_M$ y $v \in \Lambda_N$, entonces dado que $R = SM$ y $R = QN$, se tiene $(u+v)^R = u^R + v^R = u^{SM} + v^{QN} = (u^M)^S + (v^N)^Q = 0$, es decir $u + v \in \Lambda_R$.

Por otro lado si $w \in \Lambda_R$, sean $M' = \frac{M}{(M,N)}$ y $N' = \frac{N}{(M,N)}$. Se tiene que $(M', N') = 1$ por lo que

$$w = w^1 = w^{M'S'+N'Q'} = w^{M'S'} + w^{N'Q'}.$$

En la suma anterior, el primer sumando pertenece a Λ_N y el segundo sumando a Λ_M, de aquí se sigue que $w \in \Lambda_M + \Lambda_N$.

En particular $\Lambda_M \subseteq \Lambda_R$, es decir, $k(\Lambda_R) \supseteq k(\Lambda_M)$ y como, claramente, $k(\Lambda_R) \subseteq k(\Lambda_M)$ se tiene que $k(\Lambda_R) = k(\Lambda_M)$. Entonces $\Phi(M) = \Phi(R)$. Además, existe un $Q \in R_T$ tal que $R = MQ$. Por el Lema 1.6 se obtiene:

$$\Phi(R) = \Phi(MQ) = \Phi(M)\Phi(Q)\frac{N((MQ))}{\Phi((M,Q))} \geq \Phi(M)\Phi(Q).$$

Puesto que $\Phi(M) = \Phi(R)$ la anterior desigualdad implica $1 \geq \Phi(Q) \geq 1$, es decir, $\Phi(Q) = 1$. Se afirma que Q es un polinomio constante, pues en caso contrario si P es un factor irreducible de Q, es decir, $Q = P^\alpha Q'$ y tal que

P no divide a Q', $\alpha \geq 1$, y $\Phi(P^\alpha) = q^{\alpha m} - q^{(\alpha-1)m} = q^{(\alpha-1)m}(q^m - 1) > 1$, donde m denota el grado de P.

Por lo tanto, por (1.1), se tiene que $\Phi(Q) > 1$, lo cual es una contradicción. Así pues $N \mid M$ y, por lo tanto, si $M = QN$. Se tiene que:

$$\lambda_M^Q = \lambda_{QN}^Q = \lambda_N \in \Lambda_M.$$

Puesto que $u = \lambda_N^{N_1}$, para algún $N_1 \in R_T$, entonces $u \in \Lambda_M$. □

OBSERVACIÓN 1.8. Excluimos el caso $q = 2$ ya que en la demostración de la proposición 1.7 se usa que si $q > 2$ entonces los únicos polinomios P que producen $\Phi(P) = 1$, son los polinomios constantes no nulos. Sin embargo si $q = 2$ puede ocurrir que $\Phi(P) = 1$ sin que $P \in (\mathbb{F}_2)^*$. Por ejemplo $P = T$ satisface que (ver [25] Capítulo 12) $\Phi(P) = 1$. Desafortunadamente este mismo hecho hace que el Teorema 5.2 de [7] sea falso si $p = 2$, pues basta tomar $M = T$ y $N = T + 1$.

Por lo tanto se tiene que $k(\Lambda_M) = k$ si y sólo si $q = 2$ y $M \in \{T, T + 1, T(T + 1)\}$.

1.2. Teoría de módulos

En lo que resta de este capítulo, a menos que se indique otra cosa, todos los módulos y homomorfismos de módulos considerados se refieren a R_T-módulos y R_T-homomorfismos respectivamente. Siguiendo [18] definimos los siguientes conceptos:

Sea A un módulo, y $a \in A$. Sea

$$\varphi_a : R_T \to A$$

el homomorfismo definido por

$$\varphi_a(M) = Ma.$$

DEFINICIÓN 1.9. Diremos que A es *cíclico*, si existe $a \in A$ tal que el homomorfismo φ_a es suprayectivo.

La definición anterior es equivalente a pedir la existencia de $a \in A$ tal que $A = (a)$.

DEFINICIÓN 1.10. Un módulo cíclico A es de *orden* M, si M es un polinomio monico no constante con coeficientes en $\mathbb{F}_q$ y $\ker(\varphi_a) = (M)$.

OBSERVACIÓN 1.11. Si A es un módulo cíclico, entonces existe $a \in A$ tal que el homomorfismo φ_a es suprayectivo. Por lo tanto existe un polinomio M con coeficientes en $\mathbb{F}_q$ tal que

(i) $\ker(\varphi_a) = (M)$ y
(ii) $R_T/(M) \cong A$.

Si M es un polinomio no constante, entonces A es finito, por (ii). En este caso podemos reemplazar a M por un polinomio mónico. Por lo que A es un modulo ciclico de orden M, en el sentido de la definición 1.10.

DEFINICIÓN 1.12. Sea $a \in A$. Diremos que a tiene *orden infinito* si el núcleo de φ_a es cero. Diremos que a tiene *orden finito* M, M polinomio mónico, si $\ker(\varphi_a)$ es distinto de cero y $\ker(\varphi_a) = (M)$.

DEFINICIÓN 1.13. Si A es un módulo, un *exponente* de A es $M \in R_T$, no nulo tal que $Ma = 0$ para cada $a \in A$.

LEMA 1.14. *Sean A un módulo cíclico de orden M, $a \in A$ un generador de A y $B \subseteq A$ un submódulo no trivial. Entonces existe un polinomio mónico N con coeficientes en $\mathbb{F}_q$, tal que $B = (Na)$ y $N \mid M$.*

Demostración. Sea $\mathcal{C} = \{N \in R_T \mid Na \in B\}$. Sea $N \in \mathcal{C}$ un polinomio no constante, mónico de grado mínimo. Veamos que $B = (Na)$. Sea $N'a \in B$ y supongamos que $N \nmid N'$. Por lo tanto se puede escribir $N' = QN + R$ con el grado de R menor que el grado de N, lo cual implica $N'a = QNa + Ra$. Por lo tanto $Ra \in B$.

Si R fuera una constante no nula, entonces $a \in B$, pero esto es una contradicción ya que $B \neq A$. Por lo tanto si $R \neq 0$ se tiene que R es polinomio no constante, pero esto lleva a una contradicción con la elección de N. Por lo tanto $N \mid N'$, de este modo $N'a \in (Na)$.

Por otro lado si $N \nmid M$ se tiene que $M = NQ + R$ y $\mathrm{gr}(R) < \mathrm{gr}(N)$, por lo tanto $0 = Ma = NQa + Ra$ pero esto implica que $Ra = -NQa \in B$, en contradicción con la elección de N. □

El lema anterior es el análogo a la proposición de que todo subgrupo de un grupo cíclico es cíclico.

LEMA 1.15. *Sean A un R_T-módulo cíclico de orden N y N_1 un divisor mónico de N. Entonces existe un R_T-submódulo de A, cuyo orden es N_1.*

Demostración. Sea N_1 un divisor mónico de N, digamos $N = N_1Q_1$. Ahora como A es cíclico existe $a \in A$, tal que el homomorfismo φ_a es suprayectivo. Sean $b = \varphi(Q_1)$ y $B = (b)$ y se define $\psi_b : R_T \to B$ por $\psi_b(M) = Mb$. Entonces ψ_b es un homomorfismo suprayectivo.

Además si $\psi_b(M) = 0 = \varphi_a(MQ_1)$, entonces, existe $Q \in R_T$ tal que $MQ_1 = NQ = N_1QQ_1$. Por lo tanto $M = N_1Q$ luego $\ker(\psi_b) \subseteq (N_1)$.

Por otra parte si $M \in (N_1)$, M es de la forma QN_1 y $\psi_b(QN_1) = QN_1\varphi_a(Q_1) = Q\varphi_a(N_1Q_1) = 0$. Por lo tanto $(N_1) \subseteq \ker(\psi_b)$. De este modo, B es R_T-submódulo cíclico de A de orden N_1. □

En base a los lemas 1.14 y 1.15 se tiene la siguiente proposición.

PROPOSICIÓN 1.16. *Sea A un módulo cíclico de orden M. Entonces para cada divisor mónico N de M existe un único submódulo cíclico de A, de orden N.*

Ahora sea A un módulo cíclico con exponente M. Denotamos por C_M, en analogía a los grupos cíclicos C_m, al módulo $R_T/(M)$, que es cíclico de orden M.

DEFINICIÓN 1.17. Se denota por $\hat{A}$ o $\mathrm{Hom}_{R_T}(A, C_M)$, al grupo de homomorfismos de A en C_M, el *módulo dual respecto al exponente M* de A.

Supongamos que $f : A \to B$ es un homomorfismo, y que ambos módulos tienen exponente M. Se tiene un homomorfismo

$$\widehat{f} : \widehat{B} \to \widehat{A}$$

definido por $\widehat{f}(\psi) = \psi \circ f$. La categoría R_T-módulos de exponente M, es una subcategoría plena de la categoría R_T-módulos. Además nótese que $\widehat{()}$ es un funtor contravariante, es decir

$$\widehat{()} : R_T - \text{módulos de exponente } M \to R_T - \text{módulos}$$

es tal que si $f : A \to B$ y $g : B \to C$ son homomorfismos, entonces
(1) $\widehat{g \circ f} = \widehat{f} \circ \widehat{g}$ y
(2) $\widehat{1} = 1$.

LEMA 1.18. *Sean A un módulo finito, con exponente M, B y C módulos tales que $A = B \times C$. Entonces $\widehat{A}$ es isomorfo a $\widehat{B} \times \widehat{C}$.*

Demostración. En primer lugar, $B \times C$ es un módulo de exponente M, ya que $M(b, c) = (Mb, Mc) = (0, 0)$. De las proyecciones naturales $\pi_1 : B \times C \to B$ y $\pi_2 : B \times C \to C$, se obtiene los homomorfismos $\widehat{\pi}_1 : \widehat{B} \to \widehat{B \times C}$ y $\widehat{\pi}_2 : \widehat{C} \to \widehat{B \times C}$, por lo que definimos $\theta : \widehat{B} \times \widehat{C} \to \widehat{B \times C}$ por medio de:

$$\theta(\psi_1, \psi_2) = \widehat{\pi_1}(\psi_1) + \widehat{\pi_2}(\psi_2)$$

donde $(\psi_1, \psi_2) \in \widehat{B} \times \widehat{C}$. Se tiene que θ es homomorfismo. Por otra parte si $\psi \in \widehat{B \times C}$ entonces, puesto que ψ es homomorfismo, $\psi(x, y) = \psi(x, 0) + \psi(0, y)$ para todo $(x, y) \in B \times C$. Ahora si definimos $\psi_1 : B \to A_M$ y $\psi_2 : C \to A_M$ por

$$\psi_1(x) = \psi(x, 0)$$

y

$$\psi_2(y) = \psi(0, y)$$

entonces ψ_1 y ψ_2 son homomorfismos. Esto induce una función

$$\delta : \widehat{B \times C} \to \widehat{B} \times \widehat{C}$$

dada por

$$\delta(\psi) = (\psi_1, \psi_2)$$

que es homomorfismo de módulos y cuya inversa es θ. Esto termina la demostración. □

PROPOSICIÓN 1.19. *Un módulo finito A, con exponente M, es isomorfo a su dual. En otras palabras*

$$A \cong \widehat{A} = \mathrm{Hom}_{R_T}(A, C_M).$$

Demostración. Sea A un módulo finito de exponente M y hagamos la siguiente observación: Por el teorema 4.7, Capítulo 5 de [14], A se puede escribir como

$$A \cong \oplus_P A_P$$

la suma anterior es sobre todos los mónicos irreducibles P y A_P denota los elementos de A que tiene orden una potencia de P. Ahora por el teorema 4.9, Capítulo 5 de [14], cada A_P se puede escribir como

$$A_P \cong C_{P^{\alpha_1}} \oplus \cdots \oplus C_{P^{\alpha_k}}$$

donde $\alpha_1 \geq \ldots \geq \alpha_k \geq 1$ y cada $C_{P^{\alpha_i}}$ es un módulo cíclico cuyo generador tiene orden P^{α_i}, así cada $C_{P^{\alpha_i}}$ tiene orden P^{α_i}. Nótese que cada A_P y cada $C_{P^{\alpha_i}}$ tiene exponente M.

Por la observacion anterior y el lema 1.18, podemos suponer que A es cíclico generado por a con orden P^α, con $\alpha \in \mathbb{N}$ y $P \in R_T$ irreducible. Por lo tanto la función φ_a es un homomorfismo suprayectivo y $(P^\alpha) = \ker(\varphi_a)$.

Como M es un exponente de A, se tiene que $\varphi_a(M) = Ma = 0$ por lo tanto $M \in \ker(\varphi_a)$, es decir, $P^\alpha \mid M$.

De la proposición 1.16, se tiene que C_M tiene un único submódulo cíclico de orden P^α, que denotamos por C_{P^α}. El homomorfismo $\varphi_a : R_T \to A$ induce un isomorfismo, que seguiremos denotando por $\overline{\varphi_a}$

$$R_T/(P^\alpha) \to A$$

Al inverso del isomorfismo φ_a, lo denotaremos por $\psi : A \to C_{P^\alpha}$. Sea $y = \psi(a)$, entonces y es un generador de C_{P^α}. Al componer ψ con la inclusión natural $C_{P^\alpha} \hookrightarrow C_M$, se obtiene un elemento de $\widehat{A}$, que seguiremos denotando por ψ.

Ahora sea $\varphi \in \widehat{A}$, así $\varphi : A \to C_M$ es homomorfismo. Nótese que $\mathrm{Im}(\varphi) \subseteq C_M$ es submódulo cíclico de orden N. Así, existe $w \in \mathrm{Im}(\varphi)$, $w = \varphi(a_w)$ con $a_w \in A$, que genera a $\mathrm{Im}(\varphi)$ y su orden es N.

Puesto que

$$P^\alpha w = P^\alpha \varphi(a_w) = \varphi(P^\alpha a_w) = 0$$

se tiene que $P^\alpha \in (N)$. Por lo tanto $P^\alpha = ND$, para algún $D \in R_T$. Por lo que $N = P^\gamma$ además $\gamma \leq \alpha$, es decir, w tiene orden P^γ y como w genera a $\mathrm{Im}(\varphi)$, se tiene que $\mathrm{Im}(\varphi) \subseteq C_{P^\alpha}$.

Por otro lado φ esta determinado completamente por su acción en a, donde $a \in A$ es un generador de A, pero $\varphi(a) \in C_{P^\alpha}$ y y es un generador de C_{P^α}. Por lo tanto $\varphi(a) = Ny$. Si $\psi_N = N\psi$ entonces

$$\psi_N(a) = N\psi(a) = Ny = \varphi(a),$$

es decir $\varphi = \psi_N \in (\psi)$.

Así $\widehat{A} = (\psi)$ y contiene $q^{\deg(P^\alpha)}$ elementos. Por lo tanto $A \cong \widehat{A}$. □

Sean A y B módulos.

DEFINICIÓN 1.20. Una *función bilineal* de $A \times B$ en un módulo C es una función

$$A \times B \to C$$

denotada por $(a, b) \mapsto < a, b >$, que tiene la propiedad siguiente: para cada $a \in A$, la función $b \mapsto < a, b >$ es un homomorfismo y, para cada $b \in B$, la función $a \mapsto < a, b >$ es un homomorfismo. Un $a \in A$ se dice *ortogonal* a $S \subseteq B$ si $< a, b >= 0$ para cada $b \in S$.

De modo análogo tenemos la definición de que $b \in B$ sea ortogonal a $S \subseteq A$. El *núcleo izquierdo* de la función bilineal es el submódulo de A, que denotamos por N_I, ortogonal a B, es decir

$$N_I = \{a \in A \mid < a, b >= 0 \,\text{para todo}\, b \in B.\}$$

El *núcleo derecho* de la función bilineal es el submódulo de B, que denotamos por N_D, ortogonal a A, es decir

$$N_D = \{b \in B \mid < a, b >= 0 \,\text{para todo}\, a \in A.\}$$

$b \in B$ da lugar a un elemento de $\mathrm{Hom}_{R_T}(A, C)$, dado por $a \mapsto < a, b >$, que denotamos por ψ_b. Entonces ψ_b se anula en N_I, es decir, $\psi_b(a) = 0$ para cada $a \in N_I$. Así, ψ_b induce un homomorfismo $A/N_I \to C$, dado por

$$a + N_I \mapsto \psi_b(a)$$

Por otro lado si $b \equiv b' \bmod N_D$ entonces $\psi_b = \psi_{b'}$, esto da lugar, en primer lugar a un homomorfismo $\psi : B/N_D \to \mathrm{Hom}_{R_T}(A/N_I, C)$, dado por

$$\psi(b + N_D) = \psi_b$$

y en segundo lugar a la sucesión exacta de módulos

$$0 \to B/N_D \to \mathrm{Hom}_{R_T}(A/N_I, C). \tag{1.2}$$

De modo similar se obtiene

$$0 \to A/N_I \to \mathrm{Hom}_{R_T}(B/N_D, C). \tag{1.3}$$

Supongamos que C es cíclico de orden M, entonces para cada $b \in B$ se tiene $M\psi_b = \psi_{Mb} = 0$, por lo tanto B/N_D tiene exponente M. De modo similar A/N_I tiene exponente M.

PROPOSICIÓN 1.21. *Sea $A \times A' \to C$ una función bilineal de módulos, con C cíclico de orden $M \neq 0$. Sean B y B' los núcleos izquierdos y derecho respectivamente. Supongamos que A'/B' es finito. Entonces A/B es finito y A'/B' es isomorfo al módulo dual de A/B.*

Demostración. De las sucesiones exactas (1.2) y (1.3), se deduce que las sucesiones siguientes son exactas

$$0 \to A'/B' \to \mathrm{Hom}_{R_T}(A/B, C) \tag{1.4}$$

y

$$0 \to A'/B' \xrightarrow{\psi} \mathrm{Hom}_{R_T}(A/B, C) \tag{1.5}$$

Por otro lado como C es cíclico de orden M, entonces $C \cong R_T/(M)$. Por lo tanto C es finito. Puesto que A'/B' es finito por hipótesis, entonces $\mathrm{Hom}_{R_T}(A'/B', C)$ es finito. De la sucesión exacta (1.5) deducimos que $\mathrm{card}(A/B) \leq \mathrm{card}(\mathrm{Hom}_{R_T}(A/B, C))$. Por lo tanto de la proposición 1.19 se tiene que $\mathrm{card}(A/B) \leq \mathrm{card}(A'/B')$.

Por otra parte de la sucesión (1.4) y de la proposición 1.19 deducimos $\mathrm{card}(A'/B') \leq \mathrm{card}(A/B)$. Por lo tanto $\mathrm{card}(A'/B') = \mathrm{card}(A/B)$. Puesto que ψ es inyectiva, entonces de la proposición 1.19 concluimos

$$\mathrm{Hom}_{R_T}(A/B, C) \cong A/B \cong A'/B' \cong \mathrm{Hom}_{R_T}(A'/B', C).$$

□

1.3. Algunos resultados sobre torsión

DEFINICIÓN 1.22. Sean A un R_T-módulo y $N \in R_T$. Definimos $N \cdot A = \{Na \mid a \in A\}$. Por otro lado si A es un módulo de torsión escribiremos

$$\mathcal{O}_A = \{\text{orden}(a) \mid a \in A\}.$$

DEFINICIÓN 1.23. Un módulo A se dice *acotado* si A es un módulo de torsión y existe un numero natural m tal que para cada $M \in \mathcal{O}_M$ se tiene $\deg(M) \leq m$.

LEMA 1.24. *Sea A un módulo.*

(1) Para cada $M \in \mathcal{O}_M$ y todo $N \in R_T$, tal que $N \mid M$, se tiene que $N \in \mathcal{O}_A$.

(2) Para todo $M, N \in \mathcal{O}_A$ se tiene que $[M, N] \in \mathcal{O}_A$.

(3) Sea A un módulo acotado y $M \in \mathcal{O}_A$ de grado máximo, entonces todo elemento de $\mathcal{O}_A$ divide a M.

Demostración. (1) Sean $M \in \mathcal{O}_A$ y $N \mid M$. Entonces existe $a \in A$ tal que $M = \text{orden}(a)$, por lo tanto N es el orden de $b = \frac{M}{N}a$ ya que $Nb = (\frac{M}{N})Na = Ma = 0$. Por otra parte, si N_1 es el orden de b, entonces se tiene que $N_1 b = \frac{MN_1}{N}a = 0$ de aquí se sigue que existe $N_2 \in R_T$ tal que $N_1 = N_2 N$. Por lo tanto $\text{orden}(b) = N$.

(2) Se observa que si $(M, N) = 1$, entonces $MN \in \mathcal{O}_A$. Para mostrar la afirmación anterior, sean $a_M, a_N \in A$, con ordenes M y N respectivamente y $b = a_M + a_N$. Entonces $MNb = MN(a_M + a_N) = N(Ma_M) + M(Na_N) = 0$. Así, $MN \in (\widetilde{N})$, donde $\widetilde{N} = \text{orden}(b)$.

Por otro lado $\widetilde{N}b = \widetilde{N}(a_M + a_N) = \widetilde{N}a_M + \widetilde{N}a_N = 0$, de esto se sigue que $\widetilde{N}a_M = -\widetilde{N}a_N$. Por lo tanto $M\widetilde{N}a_N = 0$, de aquí se sigue que $\widetilde{N}M = R_1 N$. Ahora si $N = P_1^{\alpha_1} \dots P_r^{\alpha_r}$, de la hipótesis hecha sobre M y N se sigue que $P_i^{\alpha_i} \mid \widetilde{N}$.

Como $N\widetilde{N}a_M = 0$, siguiendo un razonamiento análogo al parrafo anterior ahora con $M = Q_1^{\beta_1} \dots Q_s^{\beta_s}$, se tendrá que $Q_j^{\beta_j} \mid \widetilde{N}$. Por lo tanto se tiene que $\widetilde{N} = MNN_2$, es decir, $\text{orden}(h) = MN$.

Por inducción podemos mostrar que si $M_1, \dots, M_r \in \mathcal{O}_G$ satisfacen que

$$(M_i, M_j) = 1$$

para $i \neq j$, entonces $M_1 \cdot \dots \cdot M_r \in \mathcal{O}_G$.

Falta mostrar que si $M, N \in \mathcal{O}_G$, entonces $[M, N] \in \mathcal{O}_G$. Podemos suponer que

$$M = P_1^{\alpha_1} \cdot \dots \cdot P_s^{\alpha_s} \text{ y } N = P_1^{\beta_1} \cdot \dots \cdot P_s^{\beta_s}$$

con $P_1, \cdots, P_s$ irreducibles distintos y $\alpha_i, \beta_j \in \mathbb{N} \cup \{0\}$. Nótese que $P_i^{\max(\alpha_i,\beta_i)}$ divide a M o N, así por (1), se tiene que $P_i^{\max(\alpha_i,\beta_i)} \in \mathcal{O}_G$. Por lo que $[M,N] = P_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot P_s^{\max(\alpha_s,\beta_s)} \in \mathcal{O}_G$.

(3) Sea $N \in \mathcal{O}_A$. Entonces por (2) se tiene que $[N,M] \in \mathcal{O}_A$, por lo que

$$\deg([N,M]) \leq \deg(M).$$

Pero $\deg(M) \leq \deg([N,M])$, por lo tanto $M = [N,M]$ y, así, $N \mid M$. □

COROLARIO 1.25. *Sea A un módulo acotado, y $M = máx(\mathcal{O}_A)$, esto último es una abreviatura de la frase: M es un polinomio que pertenece a $\mathcal{O}_A$ de grado máximo. Entonces $M \cdot A = \{0\}$.*

Demostración. Aplicar el lema 1.24. □

DEFINICIÓN 1.26. El módulo A se dice *N-acotado* si es acotado y $N \in R_T$ es monico y es el polinomio de menor grado tal que $N \cdot A = \{0\}$.

LEMA 1.27. *Sea A un módulo N-acotado. Si $M \cdot A = \{0\}$ para algún $M \in R_T$ no constante, entonces $N \mid M$.*

Demostración. Por el algoritmo de la división se puede escribir $M = NA + R$ de tal modo que $R = 0$ o $\deg(R) \leq \deg(N)$. Por lo tanto $R \cdot A = \{0\}$ y por la minimalidad de N se tendrá que $R = 0$. □

PROPOSICIÓN 1.28. *Sean A un módulo N-acotado, $M = máx(\mathcal{O}_A)$ y R el mínimo común múltiplo del conjunto $\mathcal{O}_A$. Entonces $N = M = R$.*

Demostración. Por el corolario 1.25 se tiene que $R \mid M$. Puesto que $M \in \mathcal{O}_A$ se tiene que $M \mid R$, de aquí se obtiene la igualdad $M = R$.

Ahora se tiene que $M \cdot A = \{0\}$, por el corolario 1.25, así por el lema 1.27 se tendrá que $N \mid M$. Por otro lado existe $a_0 \in A$ tal que $M = \text{orden}(a_0)$, así pues $Ma_0 = 0$ y de aquí inferimos que $M \mid N$. Por lo tanto $N = M$. □

Denotamos por $\mathbb{P}_N$ al conjunto de polinomios irreducibles que dividen a N.

PROPOSICIÓN 1.29. *Sea A un módulo N-acotado. Entonces para cada $D \in R_T$, tal que $D \mid N$, existe $a_D \in A$ con orden D. En particular, para cada $P \in \mathbb{P}_N$ existe $a_P \in A$ de orden P.*

Demostración. En primer lugar se tiene que $N = M = \max(\mathcal{O}_A)$, por la proposición 1.28. Puesto que $M \in \mathcal{O}_A$, se deduce que $D \mid N = M$. Por lo tanto se tiene que $D \in \mathcal{O}_A$ por lema 1.24. Así existe $a_G \in A$ de orden D. □

El siguiente resultado es un análogo al siguiente lema, (ver lema 2.1 de [24]).

LEMA 1.30. *Sean F un campo y m, n numeros naturales tales que el máximo común divisor de m y n es 1. Si $a = b_1^m = b_2^n$, con $b_1, b_2 \in F$, entonces existe $b \in F$ tal que $a = b^{mn}$*

Para el lema análogo, que es el siguiente, K es un campo tal que $k \subseteq K \subseteq \overline{k}$ y el grado de trascendencia de la extensión $K/\mathbb{F}_q$ es uno. En este lema consideramos la acción de Carlitz-Hayes.

LEMA 1.31. *Sean $a, b_1, b_2 \in K$ y $M, N \in R_T$, $(M, N) = 1$, tales que $a = b_1^M = b_2^N$. Entonces existe $b \in K$ tal que $b^{MN} = a$.*

Demostración. Sea $M_1 = M + N$. Entonces $(MN, M_1) = 1$ puesto que, en caso contrario, se considera un irreducible Q que divide a MN y M_1, se tendrá que $Q \mid M$ y $Q \mid N$, lo cual contradice que M y N son primos relativos. Por lo tanto podemos escribir $1 = D_1M_1 - D_2MN$, con $D_1, D_2 \in R_T$. Sea $b = (b_1 + b_2)^{D_1} - a^{D_2}$. Entonces

$$\begin{aligned} b^{MN} &= (b_1 + b_2)^{MND_1} - a^{D_2MN} \\ &= b_1^{MND_1} + b_2^{MND_1} - a^{MND_2} \\ &= a^{ND_1} + a^{MD_1} - a^{MND_2} \\ &= a^{M_1D_1 - MND_2} \\ &= a. \end{aligned}$$

□

Capítulo 2

Extensiones radicales ciclotómicas

2.1. Extensiones radicales ciclotómicas.

En lo que sigue, a menos que se especifique otra cosa, las extensiones de campos de funciones consideradas $L/\mathbb{F}_q$ satisfacen que $k \subseteq L \subseteq \overline{k}$ y L/k es una extensión algebraica. Por otra parte, si $L/\mathbb{F}_q$ y $K/\mathbb{F}_q$ son campos de funciones y $K \subseteq L$, entonces L es una extensión de K, en el sentido de campos de funciones, ya que ambos campos contiene a $\mathbb{F}_q$. A menudo un campo de funciones $L/\mathbb{F}_q$ lo denotaremos solo por L. Por otro lado a las extensiones anteriores se les da estructura de R_T-módulo, usando la acción de Carlitz-Hayes definida anteriormente.

El primer objeto a considerar, asociado a la extensión L/K es el siguiente:

$$T(L/K) = \{u \in L \mid \text{existe un } M \in R_T \setminus \{0\} \text{ tal que } u^M \in K\}.$$

Nótese que $T(L/K) \subseteq L$ es subgrupo del grupo *aditivo* L. Por otro lado $T(L/K)$ es R_T - módulo y el R_T-módulo $T(L/K)/K$ es de R_T-torsión. A este último R_T - módulo lo denotamos por $\mathrm{cog}(L/K)$. Se tiene que $\mathrm{cog}(L/K)$ es el análogo al grupo $T(L/K)/K^*$, en el caso de una extensión L/K de campos donde $T(L/K)$ denota el grupo de torsión usual asociado a la extensión L/K, es decir $T(L/K) = \{u \in L \mid \text{existe } n \in \mathbb{N} \text{ tal que } u^n \in K\}$ (ver [10] p.1).

DEFINICIÓN 2.1. Diremos que una extensión L/K es *radical* si existe $A \subseteq T(L/K)$ tal que $L = K(A)$; diremos que una extensión L/K es *separable* si cada $x \in L$ es raíz de un polinomio P, con coeficientes en K, sin raíces multiples; decimos que L/K es *pura* si para cada polinomio mónico irreducible $M \in R_T$ y cada $u \in L$ tal que $u^M = 0$ se tiene que $u \in K$; finalmente diremos que L/K es una extensión *radical ciclotómica* si:

(1) es radical,

(2) separable y

(3) pura.

Al módulo $\mathrm{cog}(L/K) = T(L/K)/K$ lo llamaremos *módulo de cogalois de la extensión.*

EJEMPLO 2.2. La extensión $k(\Lambda_M)/k$, con $M \in R_T$, es radical ya que existe $W = \Lambda_M \subseteq T(k(\Lambda_M)/k)$ tal que $k(\Lambda_M) = k(W)$, es separable, pero no pura, ya que por la Proposición 1.7, se tiene que la únicas raíces de Carlitz que estan en $k(\Lambda_M)$ son Λ_M y si Q es un factor irreducible de M, $\lambda_Q \in \Lambda_M$, pero no está en k. Por lo tanto $k(\Lambda_M)/k$ no es una extensión radical ciclotómica. □

El siguiente ejemplo muestra la existencia de extensiones radicales ciclotómicas.

EJEMPLO 2.3. Sean p un primo impar y $M = T$. Considere la extensión $k(\Lambda_M)/k$ cuyo grado es $p-1$. Se ha visto en el ejemplo 2.2 que $k(\Lambda_M)/k$ no es pura. Ahora considere el polinomio

$$F(X) = X^T - 1 = X^p + XT - 1$$

Se afirma que $1 \in k(\Lambda_M) \setminus k(\Lambda_M)^M$, ya que si ocurre lo contrario, existe $u \in k(\Lambda_M)$ tal que $u^M = 1$. Sea α un generador de Λ_M. Nótese que $[k(\alpha) : k] = p-1$, por lo que $\{1, \alpha, \alpha^2, \ldots, \alpha^{p-2}\}$ es una base de $k(\Lambda_M)$ sobre k.

Por lo tanto u se puede escribir como $u = a_0 + a_1\alpha + \cdots + a_{p-2}\alpha^{p-2}$ con $a_0, a_1, \ldots, a_{p-2} \in k$. Por lo que

$$\begin{aligned} u^T &= a_0^T + (a_1\alpha)^T + \cdots + (a_{p-2}\alpha^{p-2})^T \\ &= (a_0^p + a_0T) + (a_1^p\alpha^p + a_1\alpha T) + \cdots \\ &+ (a_{p-2}^p\alpha^{p(p-2)} + a_{p-2}\alpha^{p-2}T) \end{aligned} \tag{2.1}$$

Como $\alpha^T = \alpha^p + \alpha T = 0$ entonces $\alpha^p = -\alpha T$. Por lo tanto, puesto que $u^T = 1$, de las igualdades 2.1 se obtiene

$$\begin{aligned} 1 &= (a_0^p + a_0T) + (a_1^p\alpha^p + a_1\alpha T) + \cdots + (a_{p-2}^p\alpha^{p(p-2)} + a_{p-2}\alpha^{p-2}T) \\ &= (a_0^p + a_0T) + (-a_1^p\alpha T + a_1\alpha T) + \cdots + (-a_{p-2}^p\alpha^{p-2}T^{p-2} + a_{p-2}\alpha^{p-2}T) \end{aligned}$$

es decir

$$0 = (a_0^p + a_0T - 1) + c_1\alpha + c_2\alpha^2 + \cdots + c_{p-2}\alpha^{p-2}$$

donde $c_i = (-1)^i a_i^p T^i + a_i T$, $i = 1, \ldots, p-2$, pertenecen a k.

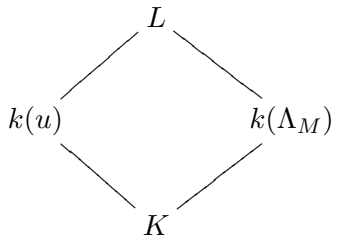
Por lo tanto llegamos a la ecuación

$$0 = a_0^p + a_0 T - 1$$

ya que $\{1, \alpha, \alpha^2 \ldots, \alpha^{p-2}\}$ es base de $k(\Lambda_M)$ sobre k. Pero $a_0 = \frac{f(T)}{g(T)}$, con $(f(T), g(T)) = 1$, de aquí derivamos la ecuación $f^p(T) + f(T)g^{p-1}(T)T = g^p(T)$ sin embargo esto contradice el que $(f(T), g(T)) = 1$.

Sea L el campo de descomposición de $F(u)$, sobre $k(\Lambda_M)$, entonces la extensión $L/k(\Lambda_M)$ es separable. Como la extension $L/k(\Lambda_M)$ es de Carlitz-Kummer (ver [23]), entonces por la proposición 2.3 de [23], se tiene que $[L : k(\Lambda_M)] = p^t$, con $t \geq 1$. Si β es una raíz de $F(u)$ se tiene que $L = k(\Lambda_M)(\beta)$, así la extensión anterior es radical. Nótese que como el irreducible de β divide a $F(u) = u^p + uT - 1$, entonces tal irreducible es $F(u)$. En particular de esto se deduce que $t = 1$.

Para mostrar que la extensión $L/k(\Lambda_M)$ es radical ciclotómica, bastará mostrar que es pura, puesto que se ha mostrado que es radical y separable. Para este fin considere polinomios mónicos irreducibles N, con grado de $N > 1$ y sea $u \in L$ tal que $u^N = 0$, se afirma que $u = 0$, en caso contrario u es un generador de Λ_N y se puede considerar el diagrama



Ahora $[k(u) : k] = p^{\mathrm{gr}(N)} - 1 \geq p(p-1) = [L : k]$, pero esto contradice que $[k(u) : k] \mid [L : k]$. Por lo tanto $u = 0 \in k(\Lambda_M)$. Esto muestra la propiedad (3) de la definición 2.1, para los polinomios de grado mayor que 1.

Resta mostrar la propiedad (3) de la definición 2.1 para los polinomios de grado 1. Para ello se consideran los polinomios $T, T+1, \ldots, T+(p-1)$, bastará considerar, por ejemplo, $N = T + 1$. Sea $u \in L$ tal que $u^{T+1} = 0$ y supongamos que $u \notin k(\Lambda_M)$, en particular $u \neq 0$; de esta manera $\mathrm{irr}(u, k(\Lambda_M)) \mid (u^{p-1} + T + 1)$, pero por nuestra suposición $\deg(\mathrm{irr}(u, k(\Lambda_M))) = p$, una contradicción. Por lo tanto $u \in k(\Lambda_M)$.

□

Para el siguiente ejemplo necesitamos la siguiente proposición

PROPOSICIÓN 2.4. *Sean $q > 2$, $P \in R_T$ mónico e irreducible y $n \in \mathbb{N}$. Entonces la extensión $k(\Lambda_{P^n})/k(\Lambda_P)$ es pura.*

Demostración. Sea $z \in k(\Lambda_{P^n})$ tal que existe un polinomio mónico irreducible $Q \in R_T$, de modo que $z^Q = 0$. Así existe un N tal que $z = \lambda_Q^N$ y

podemos suponer que $Q \nmid N$, ya que si $Q \mid N$ se tendrá que $z = \lambda_P^N = 0$. Por otra parte, de la proposición 1.7 se tiene que $\mu(k(\Lambda_{P^n})) = \Lambda_{P^n}$, por lo que $z^{P^n} = 0$.

Así, por la Observación 1.3, existe un $M \in R_T$ tal que $NP^n \frac{\xi}{Q} = M\xi$, con la hipótesis sobre Q, se deduce que $Q \mid P^n$. Por lo tanto $Q = P$, es decir, $z \in k(\Lambda_P)$ lo deseado. □

EJEMPLO 2.5. La extensión $k(\Lambda_{P^n})/k(\Lambda_P)$ es radical ciclotómica, ya que claramente, es radical y es separable ya que el polinomio, con coeficientes en R_T, U^{P^n}, es separable y por el lema 2.4 la extensión es pura. □

2.2. Propiedades de las extensiones radicales.

La extensiones radicales, en el sentido de este trabajo L/K tienen propiedades análogas a las extensiones radicales en el sentido de [10] o [1]. Sea A un R_T-módulo de torsión. Considere $\mathcal{O}_A$ el conjunto dado en la definición 1.22. Supongamos que A es un R_T-módulo acotado, en el sentido de la definición 1.23. Al mínimo común múltiplo de los elementos de $\mathcal{O}_A$, lo llamaremos el *R_T-anulador de A* y lo denotamos por anulador(A).

Ahora sea E/F una extensión radical, no necesariamente finita. Existe $A \subseteq T(E/F)$ tal que $E = F(A)$. Podemos reemplazar A por el submódulo de E generado por A y F, que seguiremos denotando por A. Es decir, puede suponerse que $F \subseteq A$.

Ahora A/F es R_T-módulo de torsión, así tiene sentido considerar $\mathcal{O}_{A/F}$. Diremos que una extensión de R_T-torsión, E/F, es una *extensión acotada* si A/F es R_T-módulo acotado, en este caso si $N =$ anulador(A/F), diremos que E/F es una extensión N *acotada*.

LEMA 2.6. *Sean A un R_T-módulo, bajo la acción de Carlitz-Hayes, $a \in A$ de orden finito $M = P_1^{k_1} \cdots P_r^{k_r}$. Entonces, si $Q_i = P_i^{k_i}$, $i = 1, \ldots, r$, A tiene elementos de orden Q_i.*

Demostración. Considere $a_i = a^{N_i}$, donde $N_i = \prod_{j \neq i} P_j^{k_j}$. Nótese que $a_i \neq 0$, ya que en caso contrario $N_i \in (M)$, es decir, N_i es divisible por M, lo cual es una contradicción.

Sea $\theta_{a_i} : R_T \to A$ definido por $\theta_{a_i}(N) = a_i^N$. De esta manera $\theta_{a_i}(Q_i) = 0$, por lo que $Q_i \in \ker(\theta_{a_i}) = (\widetilde{N_i})$, es decir, $\widetilde{N_i} \mid Q_i$. Por lo tanto $\widetilde{N_i} = P_i^{\alpha_i}$, con $\alpha_1 \geq 1$. Dado que $a_i^{P_i^{\alpha_i}} = a^{P_i^{\alpha_i} N_i} = 0$, se tiene que $M \mid N_i P_i^{\alpha_i}$. Lo cual implica que $\alpha_i \geq k_i$. Finalmente puesto que $a_i^{P_i^{k_i}} = 0$, se tiene que $\widetilde{N_i} = Q_i = P_i^{k_i}$. □

En este contexto se tiene la siguiente proposición.

PROPOSICIÓN 2.7. *Sea E/F una extensión radical, no necesariamente finita, acotada, y sea $N = \text{anulador}(A/F)$. Entonces E/F es de Galois si y sólo si $\lambda_M \in E$ para todo $M \in \mathcal{O}_{A/F}$.*

Demostración. Sea $\alpha \in E$ cuyo orden es $M \in R_T$, así tenemos que $\alpha^M = a \in F$. Considere $f(u) = u^M - a = \prod_N (u - (\alpha + \lambda_M^N)) \in F[u]$, por lo tanto los conjugados de α son

$$\{\alpha + \xi_1, \ldots, \alpha + \xi_s\}$$

para algunos $\xi_i \in \Lambda_M$.

Sea B el R_T-módulo generado por $\{\xi_1, \ldots, \xi_s\}$. Entonces $B \subseteq E$ y existe $M' \in R_T$, que divide a M, tal que $B = \Lambda_{M'}$. Si $M' \neq M$, entonces $\alpha^{M'} = a' \in F$ lo cual es una contradicción. Por lo tanto $M' = M$ y $\lambda_M \in E$.

Ahora supongamos que $\lambda_M \in E$ para todo $M \in \mathcal{O}_{A/F}$. Sea $u \in A$ y $M = \text{orden}(u)$. Como todo conjugado de u sobre F es de la forma $u + \lambda_M^N \in E$, se sigue que la extensión E/F es normal, y como los u son separables sobre F, entonces E/F es de Galois. □

En algunas extensiones radicales L/K, es posible encontrar un elemento primitivo *explícito* y que pertenezca $\text{cog}(L/K)$, como lo muestra la siguiente Proposición

PROPOSICIÓN 2.8. *Sea L/K una extensión tal que $L = K(\alpha, \beta)$ y existen $M, N \in R_T$ con $\alpha^M = a$, $\beta^N = b$, $a, b \in K$, M y N primos relativos. Entonces $L = K(\alpha + \beta)$, es decir, $\alpha + \beta$ es un elemento primitivo.*

Demostración. Puesto que $\alpha + \beta \in K(\alpha, \beta)$ entonces $K(\alpha + \beta) \subseteq K(\alpha, \beta)$. Por otro lado $(\alpha + \beta)^M = \alpha^M + \beta^M = a + \beta^M \in K(\alpha + \beta)$ y $(\alpha + \beta)^N = \alpha^N + \beta^N = \alpha^N + b \in K(\alpha + \beta)$. Por lo tanto se tiene que $\beta^M, \alpha^N \in K(\alpha + \beta)$.

Ahora puesto que $1 = MS_1 + NS_2$ se tiene que

$$\alpha = \alpha^1 = \alpha^{MS_1 + NS_2} = a^{S_1} + (\alpha^N)^{S_2} \in K(\alpha + \beta)$$

y

$$\beta = \beta^1 = \beta^{MS_1 + NS_2} = (\beta^N)^{S_1} + b^{S_2} \in K(\alpha + \beta)$$

Así pues $K(\alpha, \beta) = K(\alpha + \beta)$, más aún

$$(\alpha + \beta)^{MN} = (\alpha^M)^N + (\beta^N)^M \in K.$$

□

Nótese que el argumento anterior se puede generalizar a extensiones de la forma L/K, con $L = K(\alpha_1, \ldots, \alpha_s)$ de modo que existen $M_i \in R_T$ con $\alpha_i^{M_i} = a_i \in K$ y los polinomios M_i primos a pares.

Tenemos una serie de lemas, análogos a los lemas 1 y 5 de [12]. El objetivo de enunciar y demostrar tales lemas, es tratar de establecer el análogo, en el sentido de este trabajo, de la siguiente proposición (ver [12] Satz 2).

PROPOSICIÓN 2.9. *Sean L/K una extensión finita separable, $n \in \mathbb{N}$ tal que $(n, \mathrm{car}(K))$, donde $\mathrm{car}(K)$ la caracteristica del campo K, y sea G un grupo tal que $K^* \subseteq G \subseteq L^*$ y $G^n \subseteq L$. Entonces*

(1) $(G^* : K^n) \mid [L : K]$

(2) G/K^* *es finito.*

El análogo sería:

PROPOSICIÓN 2.10. *Sea L/K una extensión finita y separable, $n \in \mathbb{N}$ primo relativo a la caracteristica de K y C un grupo con $K^* \subseteq C \subseteq L^*$ tal que $C^n \subseteq K$. Entonces*

(1) $(C^n : K^{*n}) \mid [L : K]$

(2) Los grupos C^*/K^* *y* C^n/K^{*n} *son finitos.*

Empezamos definiendo para una extensión L/K y $N \in R_T$ no constante

$$T(N) = \{x \in L \mid x^N \in K\}$$

LEMA 2.11. *Sea $x \in T(N) \backslash K$ y M el orden de x. Supongamos que $Q \mid M$, Q irreducible, y que $\Lambda_Q \subseteq K$. Entonces $x^M \notin K^Q$.*

Demostración. Supongamos lo contrario. Sea $x^M \in K^Q$. Así $x^M = y^Q$, para algún $y \in K$. Ahora se tiene que $x^{\frac{M}{Q}}$ satisface

$$(x^{\frac{M}{Q}})^Q = x^M = y^Q$$

es decir, $(x^{\frac{M}{Q}} - y)^Q = 0$. Por lo tanto, existe $B \in R_T$ tal que

$$x^{\frac{M}{Q}} - y = \lambda_Q^B \in K.$$

Esto último implica que $x^{\frac{M}{Q}} \in K$, lo cual es absurdo. Por lo tanto

$$x^M \notin K^Q.$$

□

Para el siguiente lema, sea C un R_T-módulo, tal que $K \subseteq C \subseteq L$ y $C^N \subseteq K$. Por otro lado, sea $N = N_1 N_2$ de modo tal que $(N_1, N_2) = 1$. Definimos, para $i = 1, 2$,

$$C_{(N_i)} = \{x \in C \mid x^{N_i} \in K\}.$$

Nótese que $C^N \subseteq C_{(N_i)}^{N_i}$ para $i = 1, 2$, puesto que si $x \in C^N$, entonces existe $c \in C$ tal que $x = c^N = (c^{N_2})^{N_1}$. Ahora, puesto que $c^{N_2} \in C$ debido

a la naturaleza de la acción de Carlitz-Hayes, se tiene que $c^N \in C_{(N_1)}^{N_1}$. De modo análogo se demuestra que $c^N \in C_{(N_2)}^{N_2}$.

Por otro lado se tiene que $K^N = K^{N_1} \cap K^{N_2}$, puesto que si $x \in K^N$, existe $y \in K$ tal que $x = y^N$, por lo que $x = y^N = (y^{N_2})^{N_1} \in K^{N_1}$ y $x = y^N = (y^{N_1})^{N_2} \in K^{N_2}$. Además si $x \in K^{N_1} \cap K^{N_2}$, se tiene que $x = x_1^{N_1}$ y $x = x_2^{N_2}$, por otra parte $1 = N_1D_1 + N_2D_2$, así que

$$\begin{aligned} x &= x^1 \\ &= x^{N_1D_1+N_2D_2} = x^{N_1D_1} + x^{N_2D_2} \\ &= (x_1^{N_2N_1})^{D_1} + (x_2^{N_2N_1})^{D_2} \\ &= (x_1^{D_1} + x_2^{D_2})^N \end{aligned}$$

De aquí se sigue que $x \in K^N$ puesto que $x_1^{D_1} + x_2^{D_2} \in K$. Por otro lado se define

$$\theta : C^N \to C_{(N_1)}^{N_1} \times C_{(N_2)}^{N_2}$$

como $\theta(x^N) = (x^N, x^N)$.

Esta función θ induce una función

$$\varphi : C^N/K^N \to C_{(N_1)}^{N_1}/K^{N_1} \times C_{(N_2)}^{N_2}/K^{N_2}$$

dada por $\varphi(x^N + K^N) = (x^N + K^{N_1}, x^N + K^{N_2})$. Puesto que $K^N \subseteq K^{N_i}$, para $i = 1, 2$, se tiene que φ está bien definida.

LEMA 2.12. *La función φ definida anteriormente, es un isomorfismo. Por lo tanto*

$$\text{card}(C^N/K^N) = \text{card}(C_{(N_1)}^{N_1}/K^{N_1})\text{card}(C_{(N_2)}^{N_2}/K^{N_2})$$

Demostración. Se tiene que φ es una función inyectiva, puesto que si se tiene $\varphi(x^N + K^N) = (0, 0)$ entonces $x^N \in K^{N_i}$ para $i = 1, 2$ y esto implica que $x^N \in K^N$.

Por otro lado, supongamos que

$$(x_1^{N_1} + K^{N_1}, x_2^{N_2} + K^{N_2}) \in C_{(N_1)}^{N_1}/K^{N_1} \times C_{(N_2)}^{N_2}/K^{N_2}.$$

Puesto que $(N_1, N_2) = 1$, existen $A_1, A_2 \in R_T$ tales que

$$A_1N_1 \equiv 1 \text{ mód } N_2 \text{ y } A_2N_2 \equiv 1 \text{ mód } N_1.$$

Sea $w = x_1^{A_2N} + x_2^{A_1N} + K^N$. Entonces $x_1^{A_2N} = x_1^{A_2N_2N_1} = x_1^{N_1} + x^{S_1N_1}$ y $x_2^{A_1N} = (x_2^{S_2})^{N_1}$. Por lo tanto φ es suprayectiva. □

PROPOSICIÓN 2.13. *Sea L/K una extensión finita tal que existe $x \in L$ con $L = K(x)$ y tal que $\overline{x} = (x + K)$ tiene orden $N \in R_T$, no constante. Supongamos que $a = x^N \in K$ no pertenece a K^N y que $\Lambda_N \cap K = 0$. Sea M un divisor de N de tal modo que $x^N \in K^M$ pero si M' es otro divisor de N, de grado mayor al de M, se tenga que $x^N \notin K^{M'}$. Entonces*

(1) $\lambda_M \in L$.

(2) $K(\lambda_M)/K$ *es abeliana.*

(3) $((K, x)^N : K^N) = q^{\deg(\frac{N}{M})}$.

Aquí $(M : N)$ *denota el índice del módulo* N *en el módulo* M.

Demostración. (1) Existe $z \in K$ tal que $x^N = z^M$. Entonces $(x^{\frac{N}{M}} - z)^M = x^N - z^M = 0$. Por lo que $x^{\frac{N}{M}} - z = \lambda_M^B$. Supongamos que $(B, M) \neq 1$. Entonces $B/M = B'/M'$, con $(B', M') = 1$ y $\mathrm{gr}(M') < \mathrm{gr}(M)$. Por lo que

$$(x^{\frac{N}{M}} - z)^{M'} = (\lambda_{M'}^{B'})^{M'} = 0.$$

Pero $\mathrm{gr}(\frac{NM'}{M}) < \mathrm{gr}(N)$ y $z^{M'} \in K$, lo cual contradice la elección de N. Por lo tanto $(B, M) = 1$ así $\lambda_M \in L$.

(2) Considere el diagrama siguiente

$$\begin{array}{ccc} k(\lambda_M) & \text{——} & k(\lambda_M)K = K(\lambda_M) \\ | & & | \\ k & \text{————————} & K \end{array}$$

Sea $\widetilde{K} = k(\lambda_M) \cap K$. Puesto que $k(\lambda_M)/k$ es una extensión de Galois, se tiene que $K(\lambda_M)/K$ es una extensión de Galois, de tal modo que

$$H = \mathrm{Gal}(k(\lambda_M)/\widetilde{K}) \cong \mathrm{Gal}(K(\lambda_M)/K).$$

Por otro lado si $G = \mathrm{Gal}(k(\lambda_M)/k)$, entonces $H \subseteq G$ es un subgrupo y G es abeliano. Esto muestra que $K(\lambda_M)/K$ es abeliana.

(3) Considere el módulo (K, x) generado por K y x, así que $K \subseteq (K, x)$. Se sigue que $K^N \subseteq (K, x)^N$. Ahora si $A = (K, x)^N/K^N$, se afirma que $(\overline{a}) = A$, donde $\overline{a} = a + K^N$, ya que si $w \in A$ entonces

$$w = ((\sum a_i^{B_i}) + x^C)^N + K^N = \sum a_i^{NB_i} + x^{CN} + K^N = a^C + K^N.$$

Por lo tanto $A \subseteq (\overline{a})$.

Ahora sea D el orden de $\overline{a}$. Entonces

$$(x^N)^{\frac{N}{M}} = (x^{\frac{N}{M}})^N = (z + \lambda_M)^N = z^N \in K.$$

Por lo tanto $D \mid \frac{N}{M}$.

Por otra parte, de $x^N = z^M$ se sigue que $x^{ND} = z^{MD}$, pero se tiene que $x^{ND} = a^D \in K^N$, por la definición del orden de $\overline{a}$. Por lo tanto existe $u \in K$ tal que $z^{MD} = u^N$. Por otro lado, puesto que $D \mid \frac{N}{M}$, existe $S_1 \in R_T$ tal que $N = DS_1M$. Ahora

$$\begin{aligned}(u^{\frac{N}{MD}} - z)^N &= U^{\frac{N^2}{MD}} - z^N \\ &= u^{NS_1} - z^N \\ &= u^{NS_1} - z^{\frac{N}{S_1}S_1} \\ &= (u^N - z^{\frac{N}{S_1}})^{S_1} \\ &= (u^N - z^{MD})^{S_1} \\ &= 0.\end{aligned}$$

Por lo tanto $z = u^{\frac{N}{MD}}$, ya que $u^{\frac{N}{MD}} \in K$ y por la hipótesis. Por otro lado

$$x^N = z^M = (u^{\frac{N}{MD}})^M = u^{\frac{N}{D}} = u^{MS_1} \in K^{MS_1}.$$

Por la condición impuesta a M se sigue que $S_1 = 1$. En consecuencia el orden de $\overline{a}$ es $\frac{N}{M}$. □

2.3. Extensiones radicales ciclotómicas

Las extensiones radicales ciclotómicas tiene algunas propiedades, análogas a las propiedades de las extensiones cogalois clásicas. Necesitamos primero un lema.

LEMA 2.14. *Sea $K \subseteq L \subseteq L'$ una torre de campos. Entonces L'/K es pura si y sólo si L'/L y L/K son puras.*

Demostración. Supongamos que L'/K es pura, sean $\lambda \in L'$ y $P \in R_T$, mónico e irreducible, tal que $\lambda_P^P = 0$. Entonces $\lambda_P \in K \subseteq L$, puesto que L'/K es pura. Por lo tanto L'/L es pura. De modo completamente análogo se prueba que L/K es pura.

Por otro lado supongamos que L'/L y L/K son puras, sean $\lambda_P \in L'$ y $P \in R_T$, mónico e irreducible, tal que $\lambda_P^P = 0$, entonces, como L'/L es pura, $\lambda_P \in L$ y como L/K es pura, entonces $\lambda_P \in K$. □

PROPOSICIÓN 2.15. *Sea $K \subseteq L \subseteq L'$ una torre de campos, entonces*

(1) Existe una sucesión exacta de R_T-módulos

$$0 \to \mathrm{cog}(L/K) \to \mathrm{cog}(L'/K) \to \mathrm{cog}(L'/L)$$

(2) Si la extensión L'/K es radical ciclotómica, entonces la extensión L'/L es radical ciclotómica.

(3) Si la extensión L'/K es radical, y las extensiones L'/L y L/K son radicales ciclotómicas, entonces L'/K es radical ciclotómica.

Demostración. (1) El homomorfismo canónico

$$\operatorname{cog}(L'/K) \to \operatorname{cog}(L'/L),\ x + K \mapsto x + L$$

es un R_T-homomorfismo con núcleo $\operatorname{cog}(L/K)$. Esto prueba que la sucesión de R_T-módulos

$$0 \to \operatorname{cog}(L/K) \to \operatorname{cog}(L'/K) \to \operatorname{cog}(L'/L)$$

es exacta.

(2) Como L'/K es separable, entonces L'/L es separable y, por el lema 2.14, L'/L es pura. Finalmente puesto que $T(L'/K) \subseteq T(L'/L)$ entonces L'/L es radical.

(3) Como L'/L y L/K son radicales ciclotómicas, entonces ambas son separables y puras, por lo tanto, por el lema 2.14, la extensión L'/K es pura, además separable, por lo tanto L'/K es radical ciclotómica. □

La proposición anterior sería la análoga al teorema 1.6 de [10] que enunciamos a continuación.

TEOREMA 2.16. *Supongamos que L/K es cogalois.*

(1) Para todo campo intermedio $K \subseteq F \subseteq L$, L/F y F/K son cogalois.

(2) Para todo campo intermedio $K \subseteq F \subseteq L$, tenemos que $L_{\operatorname{cog}(F/K)} = F$.

(3) Para todo subgrupo $H \subseteq \operatorname{cog}(L_H/K) = H$.

(4) Las funciones $\operatorname{cog}(-)/$ y $L_{(-)}$ son isomorfismos inversos de retículas.

(5) $\operatorname{cog}(L/F)$ es canonicamente isomorfo a $\operatorname{cog}(L/K)/\operatorname{cog}(F/K)$.

Sin embargo el análogo al inciso (a) del teorema 2.16, no es válido en general, es decir, existe una extensión radical ciclotómica L/K y un campo $\widetilde{K}$, con $K \subseteq \widetilde{K} \subseteq L$ tal que $\widetilde{K}/K$ no es radical ciclotómica. Para empezar necesitamos algunas definiciones y un lema.

DEFINICIÓN 2.17. Sean G un grupo y M un G-módulo. Una función $f : G \to M$ se dice que es un *homomorfismo cruzado de G con coeficientes en M* si para cada $\sigma, \tau \in G$ se tiene que $f(\sigma \circ \tau) = f(\sigma) + \sigma \cdot f(\tau)$.

Al conjunto de homomorfismos cruzados lo denotamos por

$$Z^1(G, M).$$

DEFINICIÓN 2.18. Sean G un grupo y M un G-módulo. Una función $f : G \to M$ se dice que es un *homomorfismo cruzado principal de G con coeficientes en M* si existe $x \in M$ tal que $f(\sigma) = \sigma x - x$, para cada $\sigma \in G$. Al conjunto de homomorfismos cruzados principales lo denotamos por

$$B^1(G, M).$$

Nótese que si L/K es una extensión de Galois de campos, entonces $\mu(L)$ es un $G = \mathrm{Gal}(L/K)$-módulo mediante la acción siguiente: dado $\sigma \in G$ y $u \in \mu(L)$ pongamos $\sigma \cdot u = \sigma(u)$; ya que la acción de Carlitz-Hayes conmuta con σ, $\sigma \cdot u$ está bien definida.

LEMA 2.19. *Sean L/K una extensión Galois tal que $[L : K] = p^2$, $\mu(L) = \mu(K)$ y $G = \mathrm{Gal}(L/K) \cong C_{p^2}$. Entonces L/K no es una extensión radical.*

Demostración. Supongamos que L/K es radical. Considere el grupo

$$H^1(G, \mu(L)).$$

Puesto que $\mu(L) = \mu(K)$ se tiene que $B^1(G, \mu(L)) = \{1\}$ (ver definición 2.18) y, por lo tanto,

$$H^1(G, \mu(L)) = Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong \mathrm{Hom}(G, \mu(L))$$

(ver [26] Capítulo 1).

En consecuencia, por la proposición 2.23, se tendrá

$$\mathrm{cog}(L/K) \cong \mathrm{Hom}(G, \mu(K)).$$

Por el teorema de Cauchy, existe un elemento de orden p, digamos τ, en G. Sean $H = (\tau)$ y $L' = L^H$. Nótese que, al ser H normal en G, se tiene que L'/K es una extensión normal y, por lo tanto, de Galois. Además $G' = \mathrm{Gal}(L'/K)$ es isomorfo a C_p. Nótese que $\mu(L') = \mu(K)$. Así

$$\mathrm{cog}(L'/K) \cong \mathrm{Hom}(G', \mu(K)).$$

Nótese que la cardinalidad de $\mathrm{cog}(L/K) \cong \mathrm{Hom}(G, \mu(K))$ es $\mid \mu(K) \mid$. Para ver ésto sea $a \in G \cong C_{P^2}$ un generador. Un homormorfismo $\psi : G \to \mu(K)$ queda completamente determinado por su acción en a, por lo tanto hay $\mid \mu(K) \mid$ homomorfismos de G en $\mu(K)$. Del mismo modo podemos mostrar que la cardinalidad de $\mathrm{cog}(L'/K) \cong \mathrm{Hom}(G', \mu(K))$ es $\mid \mu(K) \mid$.

Por otro lado tenemos que $\mathrm{cog}(L'/K) \subseteq \mathrm{cog}(L/K)$ (ver proposición 2.15 inciso (1)). Entonces, por cardinalidad, se tiene $\mathrm{cog}(L'/K) = \mathrm{cog}(L/K)$, pero de esto se sigue que $L = L'$, ya que si $\alpha_1, \ldots, \alpha_s$ generan a L sobre K, entonces por lo mostrado se tendrá que $\alpha_1, \ldots, \alpha_s \in L'$ y de aquí la afirmación. Pero se tendría que $[L : K] = p^2 = [L' : K] = p$ lo cual es una contradicción. □

EJEMPLO 2.20. Sea $M = P^n$, $n \in \mathbb{N}$ y $P \in R_T$ irreducible. Considere la extensión $k(\Lambda_M)/k(\lambda_P)$. Sea $t \in \mathbb{N}$ de tal modo que $p^{t-1} < n \leq p^t$ y n_0 la parte entera de $\frac{n}{p^{t-1}}$.

Del corolario 1 de [17], se obtiene

$$H_M \cong (\mathbb{Z}/p^t\mathbb{Z})^\alpha \times \mathbb{Z}/p^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_s}\mathbb{Z}$$

con $t > n_1 \geq \ldots \geq n_s \geq 0$.

Sean $n = 5$ y $p = 3$. Si $t = 2$ se cumple que $p^{t-1} < n \leq p^t$, además $n_0 = 1$, el valor de α está dado por el corolario 1 de [17].

Se puede escoger un subgrupo de H_M de la forma

$$H = (\mathbb{Z}/p^t\mathbb{Z})^{\alpha-1} \times \mathbb{Z}/p^{n_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p^{n_s}\mathbb{Z}$$

y $L' = L^H$, así $\mathrm{Gal}(L'/k(\lambda_P)) \cong C_{p^2}$. Nótese también que $\mu(k(\lambda_P)) = \mu(L')$, esto es posible, escogiendo adecuadamente $q = p^s$.

Por el lema 2.19, $L'/k(\lambda_P)$ no es radical. Por lo tanto $k(\lambda_{P^5})/k(\lambda_P)$ es una extensión Galois radical ciclotómica, pero no cumple la propiedad de que si L es un campo tal que $k(\lambda_P) \subseteq L \subseteq k(\lambda_{P^5})$, entonces $L/k(\lambda_P)$ es radical.

En este aspecto sería mejor considerar la extensión $k(\lambda_{T^4})/k(\lambda_T)$, con $q = p^r$, $p = 3$ y $r = 3$. Su grupo de Galois es isomorfo a

$$(\mathbb{Z}/p^2\mathbb{Z})^3 \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

ver [17], en especial el corolario 1 al lema 2.

Por otra parte, de la proposición 7.1.2. de [16], es posible encontrar $\alpha \in \mathbb{F}_q \setminus \{0, 1, 2\}$, de modo que $\alpha^2 \neq 2$.

Por lo tanto se consideran los polinomios, módulo T^4, $1 + T^2$, $1 + \alpha T^2$ y $1 + \alpha T^3$ de orden p y los polinomios $1 + T(T+1)$, $1 + T^2(T+1)$ y $1 + T(T^2+1)$ de orden p^2. Si se considera el campo $L = k(\lambda_{T^4})^H$, donde H es el subgrupo de $\mathrm{Gal}(k(\lambda_{T^4})/k(\lambda_T))$, generado por

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

entonces la extensión $L/k(\lambda_T)$ cumple la hipótesis del lema 2.19, así $L/k(\lambda_T)$ no es radical.

PROPOSICIÓN 2.21. *Sean K/F y L/F extensiones de campos tales que $L \cap K = F$. Entonces* $\mathrm{cog}(K/F) \subseteq \mathrm{cog}(KL/L)$

Demostración. Nótese que $F \subseteq T(K/F) \cap L \subseteq K \cap L = F$, es decir, $T(K/F) \cap L = F$. Por otro lado $T(K/F) \subseteq T(KL/L)$.

Así $\mathrm{cog}(KL/L) \supseteq (T(K/F) + L)/L$ y por los teoremas de isomorfismo, se tiene que

$$(T(K/F) + L)/L \cong T(K/F)/(T(K/F) \cap L) = T(K/F)/F = \mathrm{cog}(K/F).$$

Esto prueba lo deseado. □

PROPOSICIÓN 2.22. *Sean K/F y L/F extensiones de campos tales que $L \cap K = F$ y KL/F es pura. Entonces KL/F es una extensión radical ciclotómica y se tiene un monomorfismo* $\mathrm{cog}(L/F) \times \mathrm{cog}(K/F) \hookrightarrow \mathrm{cog}(KL/F)$.

Demostración. Por definición se tiene que $L = F(T(L/F))$ y $K = F(T(K/F))$. Por lo tanto $KL = F(T(L/F), T(K/F))$. Se sigue que KL/F es radical. Además como las extensiones L/F y K/F son separables se sigue que KL/L es separable y, por hipótesis, KL/L es pura. Por lo tanto KL/L es una extensión radical ciclotómica.

Para mostrar la última parte de la proposición se define

$$\varphi : \mathrm{cog}(K/F) \times \mathrm{cog}(L/F) \to \mathrm{cog}(KL/F)$$

como $\varphi(\overline{x}, \overline{y}) = \overline{x + y}$. Por lo tanto la condición $L \cap K = F$ implica que φ es un monomorfismo, lo cual prueba la proposición. □

Para algunas extensiones L/K se tiene que el R_T-módulo $\mathrm{cog}(L/K)$ es finito. Por lo tanto en este punto conviene definir

$$\mu(L) = \{u \in L \mid \text{existe un } M \in R_T \setminus \{0\} \text{ tal que } u^M = 0\}.$$

Observamos que éste es el análogo a $\mu(L)$, las raíces de la unidad de L, ver [2].

Por otra parte, considere L/K una extensión de Galois de campos, con grupo de Galois $G = \mathrm{Gal}(L/K)$. Nótese que $\mu(L)$ es un G-módulo, mediante la acción siguiente: dado $\sigma \in G$ y $u \in \mu(L)$ pongamos $\sigma \cdot u = \sigma(u)$; ya que la acción de Carlitz-Hayes conmuta con σ, $\sigma \cdot u$ está bien definida.

TEOREMA 2.23. *Sean L/K una extensión de Galois y G su grupo de Galois. Entonces la función $\phi : \mathrm{cog}(L/K) \to Z^1(G, \mu(L))$ dada por $\phi(u + K) = f_u$ donde $f_u(\sigma) = \sigma(u) - u$, es un isomorfismo de grupos.*

Demostración. Se define $\theta : T(L/K) \to Z^1(G, \mu(L))$ mediante $\theta(u) = f_u$. Obsérvese que $f_u(\sigma \circ \tau) = \sigma(\tau(u)) - u$, además $f_u(\sigma) = \sigma(u) - u$ y $f_u(\tau) = \tau(u) - u$ aplicando a esta última ecuación σ se obtiene $\sigma(f(\tau)) = \sigma(\tau(u)) -$

$\sigma(u)$, al sumar esta ecuación con la primera se obtiene que f_u es un homomorfismo cruzado. Nótese de paso que si $\sigma \in G$ entonces $f_u(\sigma) = \sigma(u) - u$ está en $\mu(L)$, puesto que existe un $N \in R_T$ tal que $u^N \in K$. Por lo tanto $(\sigma(u) - u)^N = (\sigma(u))^N - u^N = \sigma(u^N) - u^N = 0$.

Además

$$\theta(u + v) = f_{u+v}$$

Por lo tanto

$$\begin{aligned} f_{u+v}(\sigma) &= \sigma(u + v) - (u + v) \\ &= \sigma(u) + \sigma(v) - u - v \\ &= \sigma(u) - u + \sigma(v) - v, \end{aligned}$$

es decir

$$\theta(u + v) = \theta(u) + \theta(v).$$

Por lo tanto θ es homomorfismo. Por otra parte sea $u \in \ker(\theta)$, así $\theta(u) = f_u = 0$, es decir, $f_u(\sigma) = \sigma(u) - u = 0$, y como L/K es de Galois, entonces $u \in K$.

Recíprocamente si $u \in K$, claramente $\theta(u) = 0$, así $\ker(\theta) = K$ y por lo tanto tenemos un monomorfismo de grupos abelianos

$$\phi : \mathrm{cog}(L/K) \to Z^1(G, \mu(L)).$$

Por otro lado $Z^1(G, \mu(L)) \subseteq Z^1(G, L)$ y por el teorema 90 de Hilbert aditivo que afirma que $H^1(G, L)) = Z^1(G, L)/B^1(G, L) = 0$, se tiene que

$$Z^1(G, L) = B^1(G, L) = \{f \in Z^1(G, L) \mid \text{existe un } u \in L \text{ tal que } f = f_u\}.$$

Entonces, dado $f \in Z^1(G, \mu(L))$ existe $u \in L$ tal que $f = f_u$, por lo que para cada $\sigma \in G$, $f(\sigma) = f_u(\sigma) = \sigma(u) - u \in \mu(L)$. Ahora, u es algebraico sobre K, y se puede considerar la cerradura de Galois K' de $K(u)/K$. Se tiene que $K \subseteq K(u) \subseteq K' \subseteq L$.

Sea $H = \mathrm{Gal}(L/K')$, entonces $H \lhd G$ y $\mathrm{card}(G/H)$ es finita. Los conjugados de u son $\{\overline{\sigma}(u) \mid \overline{\sigma} \in \overline{G} = G/H\}$, así

$$\overline{\sigma}(u) = \sigma(u) = u + z_\sigma \text{ con } z_\sigma \in \mu(L).$$

Como sólo hay un número finito de elementos $\overline{\sigma} \in \overline{G} = \{\sigma_1 H \dots \sigma_s H\}$ existen $N_{\sigma_1}, \dots, N_{\sigma_s} \in R_T$ tales que $(z_{\sigma_i})^{N_{\sigma_i}} = 0$. Sea $N = N_{\sigma_1} \cdots N_{\sigma_s}$. Entonces

$$\overline{\sigma}(u^N) = (u + z_\sigma)^N = u^N + z_\sigma^N = u^N + (z_\sigma^{N_\sigma})^{P_\sigma} = u^N.$$

Como la extensión K'/K es de Galois, esto implica que $u^N \in K$, es decir, ϕ es suprayectiva. □

En el contexto de la proposición 2.23 se tiene

PROPOSICIÓN 2.24. *Sean E/F una extensión finita de Galois, $\Gamma = \mathrm{Gal}(E/F)$ y $\Delta \lhd \Gamma$. Entonces la sucesión canónica de grupos abelianos*

$$0 \to Z^1(\Gamma/\Delta, \mu(E/F)^\Delta) \xrightarrow{\theta_1} Z^1(\Gamma, \mu(E/F)) \xrightarrow{\theta_2} Z^1(\Delta, \mu(E/F))$$

es exacta, donde $\mu(E/F)^\Delta = \{\zeta \in \mu(E/F) \mid \sigma(\zeta) = \zeta, \forall \sigma \in \Delta\}$

Demostración. Supongamos que $\theta_1(f) = 0$. Entonces si $\overline{\sigma} \in \Gamma/\Delta$, se tiene que $f(\overline{\sigma}) = \theta_1(f)(\sigma) = 0$. De este modo θ_1 es inyectiva. Por otro lado $\mathrm{im}(\theta_1) \subseteq \ker(\theta_2)$ ya que si $f = \theta_1(f')$, con $f' \in Z^1(\Gamma/\Delta, \mu(E/F)^\Delta)$, entonces $\theta_2(f)(\sigma) = \theta_1(f')(\sigma) = f'(\overline{\sigma}) = 0$.

Ahora si $f \in \ker(\theta_2)$, entonces para cada $\sigma \in \Delta$, se tiene que $f(\sigma) = 0$. Por lo se puede definir $f' : \Gamma/\Delta \to \mu(E/F)$ mediante $f'(\overline{\sigma}) = f(\sigma)$. Por la condición impuesta a f, f' está bien definida y es un morfismo cruzado. Finalmente si $\tau \in \Delta$, entonces

$$\tau(f'(\overline{\sigma})) = \tau(f(\tau^{-1} \circ \sigma)) = \tau(f(\sigma)) = f'(\overline{\sigma}),$$

es decir $f' \in Z^1(\Gamma/\Delta, \mu(E/F)^\Delta)$ y $f = \theta_1(f')$. □

COROLARIO 2.25. *Sea L/K una extensión como en la proposición 2.23. Si la cardinalidad de $\mu(L)$ es finita entonces el R_T-módulo $\mathrm{cog}(L/K)$ es finito.*

Demostración. Se sigue del teorema 2.23. □

LEMA 2.26. *Si K es un campo tal que $k \subseteq K \subseteq \overline{k}$ y K/k finita, entonces $\mu(K)$ es finito.*

Demostración. Sólo hay un número finito de polinomios ciclótomicos Ψ_M tales que $\Phi(M) \leq [K : k]$. Puesto que hay sólo un número finito de polinomios de grado dado, entonces los ceros de estos polinomios, son los únicos elementos de $\mu(K)$. □

PROPOSICIÓN 2.27. *Sea L/K una extensión radical ciclotómica tal que L/k sea finita. Entonces $\mid \mathrm{cog}(L/K) \mid$ es finito.*

Demostración. Considere la cerradura normal de la extensión L/k. Sea E/k tal cerradura, por lo tanto E/k es Galois y contiene a la extensión L/K. El lema 2.26 muestra que $\mu(E)$ es un conjunto finito y, puesto que $\mu(L) \subseteq \mu(E)$, la proposición 2.23 muestra que $\mid \mathrm{cog}(L/K) \mid$ es finito. □

DEFINICIÓN 2.28. Sea A un conjunto. Una relación $\leq$ en A es un *orden parcial* si reflexiva, transitiva y antisimétrica. Una *retícula* es un par $(A, \leq)$ donde $\leq$ es un orden parcial.

En la siguiente proposición consideramos una extsnsión de Galois E/L, con grupo de Galois Γ, junto con los conjuntos

$$C_{\mathrm{cog}(E/L)} = \{H \mid H \text{ es submódulo de } T(E/L) \text{ y contiene a } L\}$$

y

$$D_{Z^1(\Gamma,\mu(E))} = \{U \mid U \text{ es subgrupo de } Z^1(\Gamma, \mu(E))\}.$$

Ambos conjuntos son retículas, con el orden inducido por la inclusión de conjuntos. Así tenemos el siguiente corolario de la proposición 2.23.

COROLARIO 2.29. *Si E/L es finita y de Galois, con grupo de Galois Γ, entonces la función:*

$$\Psi : C_{\mathrm{cog}(E/L)} \to D_{Z^1(\Gamma,\mu(E))},$$

dada por $\Psi(H) = \{\phi(\alpha + L) \in Z^1(\Gamma, \mu(E))|\alpha \in H\}$, es un isomorfismo de retículas.

Demostración. Se sigue del isomorfismo dado en la proposición 2.23. □

2.4. Retículas asociadas a extensiones radicales

En esta parte consideramos relaciones entre ciertas retículas asociadas a las extensiones radicales ciclotómicas. En esta sección las retículas $(A, \leq)$ que se consideran son inducidas por la contención usual entre conjuntos, a menos que se diga otra cosa. Para empezar sea E/L una extensión de Galois con grupo de Galois $\mathrm{Gal}(E/L) = \Gamma$, definimos

$$f : \mathrm{Gal}(E/L) \times \mathrm{cog}(E/L) \to \mu(E)$$

mediante $f(\sigma, \overline{u}) = \sigma(u) - u$. Como sabemos que $\mathrm{cog}(E/L) \to Z^1(\Gamma, \mu(E))$ es un isomorfismo, se tiene la función evaluación

$$<,>: \Gamma \times Z^1(\Gamma, \mu(E)) \to \mu(E)$$

dado por $< \sigma, h >= h(\sigma)$.

Solo en esta sección usaremos las siguientes notaciones: $\Delta \leq \Gamma$ para denotar que Δ es subgrupo de Γ, $U \leq Z^1(\Gamma, \mu(E))$ para denotar que U es subgrupo de $Z^1(\Gamma, \mu(E))$ y si F y G son R_T-módulos, $F \leq G$ indica que F es submódulo del módulo G.

Ahora para cada $\Delta \leq \Gamma$, $U \leq Z^1(\Gamma, \mu(E))$ y $\chi \in Z^1(\Gamma, \mu(E))$ definimos:

$$\Delta^{\perp} = \{h \in Z^1(\Gamma, \mu(E)) \mid < \sigma, h >= 0 \text{ para cada } \sigma \in \Delta\}$$

$$U^{\perp} = \{\sigma \in \Gamma \mid < \sigma, h >= 0 \text{ para cada } h \in U\}$$

$$\chi^{\perp} = \{\sigma \in \Gamma \mid < \chi, h >= 0\}$$

así $\Delta^{\perp} \leq Z^1(\Gamma, \mu(E))$ y $U^{\perp} \leq \Gamma$.

PROPOSICIÓN 2.30. *Sea E/L una extensión finita y de Galois, $\Gamma = \mathrm{Gal}(E/L)$, y sea L' una extensión intermedia de E/L. Entonces L'/L es radical si y solamente si existe un $U \leq Z^1(\Gamma, \mu(E))$ tal que $\mathrm{Gal}(E/L') = U^\perp$.*

Demostración. Si L'/L es radical existe $\widetilde{G} \subseteq T(E/L)$ tal que $L' = L(\widetilde{G})$. Podemos reemplazar $\widetilde{G}$ por el subgrupo *aditivo* generado por $\widetilde{G}$ y L, que denotamos por G, así $L \leq G \leq T(E/L)$ y $L' = L(G)$. Sea

$$U = \phi(G) = \{f_\alpha \mid \alpha \in G\} \leq Z^1(\Gamma, \mu(E)),$$

donde ϕ es la función dada en el corolario 2.29. Entonces

$$\begin{aligned} U^\perp &= \{\sigma \in \Gamma \mid <\sigma, f_\alpha> = 0 \text{ para cada } f_\alpha \in U\} \\ &= \{\sigma \in \Gamma \mid f_\alpha(\sigma) = 0 \text{ para cada } f_\alpha \in U\} \\ &= \{\sigma \in \Gamma \mid \sigma(\alpha) = \alpha \text{ para cada } f_\alpha \in U\} \\ &= \{\sigma \in \Gamma \mid \sigma(x) = x \text{ para cada } x \in L(G)\} \\ &= \mathrm{Gal}(E/L(G))) = \mathrm{Gal}(E/L'). \end{aligned}$$

Recíprocamente, si existe $U \leq Z^1(\Gamma, \mu(E))$ tal que $\mathrm{Gal}(E/L') = U^\perp$, entonces veamos que $\mathrm{Gal}(E/L') = U^\perp = \mathrm{Gal}(E/L(G)))$, con $G = \{\alpha \in E \mid f_\alpha \in U\} = \phi^{-1}(U)$ donde ϕ es la función del corolario 2.29.

Para mostrar las igualdades anteriores sólo debemos mostrar

$$U^\perp = \mathrm{Gal}(E/L(G)).$$

Para este fin consideremos $\tau \in U^\perp = \{\sigma \in \Gamma \mid h(\sigma) = 0 \text{ para cada } h \in U\}$. Si $\alpha \in G$, entonces $f_\alpha \in U$, en particular, $f_\alpha(\tau) = 0 = \tau(\alpha) - \alpha$. Por lo tanto, para todo $\alpha \in G$, $\tau(\alpha) = \alpha$ y, de este modo, τ fija a $L(G)$ así que $\tau \in \mathrm{Gal}(E/L(G))$.

Ahora si $\tau \in \mathrm{Gal}(E/L(G))$, sea $h \in U$. Entonces existe $\alpha \in G$ tal que $h = f_\alpha$, por la definición de G y el hecho de que ϕ es biyectiva. Se sigue que $h(\sigma) = f_\alpha(\sigma) = 0$ por lo que $\tau \in U^\perp$. Ahora por teoría de Galois, se tiene que $L' = L(G)$ □

El siguiente resultado es una aplicación de la proposición anterior, ver [3]. El símbolo $\sqrt[N]{\alpha}$ denota una raíz del polinomio $u^N - \alpha$ donde $\alpha \in \overline{k}$.

PROPOSICIÓN 2.31. *Sean K/F una extensión finita y separable, y E la cerradura normal de K/F. Supongamos que existe una extensión finita L/F tal que*

(1) $E(\lambda_N) \cap L = F$ donde $N \in R_T$ es un polinomio no constante.

(2) $KL = L(\sqrt[N]{\alpha})$ para algún $\alpha \in L$ distinto de 0.

Entonces $K = F(\sqrt[N]{\alpha})$.

Demostración. Se considera el diagrama siguiente

$$\begin{array}{ccc} E(\lambda_N) & \text{——} & E(\lambda_N)L \\ | & & | \\ K & \text{————} & KL \\ | & & | \\ F & \text{————} & L \end{array}$$

Puesto que la extensión $E(\lambda_N)/F$ es de Galois, entonces, por teoría de Galois, se tiene que $E(\lambda_N)L/L$ es de Galois y de la hipótesis (1) se tiene

$$G = \mathrm{Gal}(E(\lambda_N)/F) \cong \mathrm{Gal}(E(\lambda_N)L/L) = G_1.$$

Por la hipótesis (2) se tiene $KL = L(\sqrt[N]{\alpha})$. Sea $\beta = \sqrt[N]{\alpha}$ y considere $\sigma \in \mathrm{Gal}(E(\lambda_N)L/KL)$, entonces

$$(\sigma(\beta) - \beta)^N = \sigma(\beta^N) - \beta^N = \sigma(\alpha) - \alpha = 0. \tag{2.2}$$

Definimos $\chi : G_1 \to \mu(E(\lambda_N)L)$ por

$$\chi(\sigma) = \sigma(\beta) - \beta.$$

Entonces $\mathrm{Gal}(E(\lambda_N)L/KL) = \ker(\chi)$, ya que si $\sigma \in \mathrm{Gal}(E\lambda_N)L/KL)$ se tiene que $\chi(\sigma) = \sigma(\beta) - \beta = 0$ y viceversa. Además de (2.2) se tiene que χ toma valores en Λ_N. Puesto que G y G_1 son isomorfos, χ puede ser definido en G.

Por lo anterior χ puede pensarse como elemento de $Z^1(G, E(\lambda_N))$ y $\ker(\chi)$ es $\mathrm{Gal}(E(\lambda_N)/K)$, puesto que G y G_1 son isomorfos. Por la proposición 2.30 K/F es radical. □

Sea E/F finita de Galois, con grupo de Galois G. Sea L/F otra extensión tal que $L \cap E = F$, considere la composición EL. Utilizando la proposición 3.18 de [20], la función de restricción

$$\mathrm{Gal}(EL/L) \to \mathrm{Gal}(E/F), \;\; \sigma \mapsto \sigma \mid_E$$

es un isomorfismo de grupos. Denotamos por $S(L_1/L_2)$ al subconjunto de subextensiones de L_1 que contienen a L_2, entonces por teoría de Galois, se tiene que las funciones

$$\varepsilon : S(E/F) \to S(EL/L), \;\; K'/F \mapsto LK'/L$$

y

$$\lambda : S(EL/L) \to S(E/F), \;\; K_1/L \mapsto (K_1 \cap E)/F$$

son isomorfismo de retículas, inversas una de la otra.

Denotamos por $\mathrm{Rad}(E/F)$ al conjunto de todas las subextensiones K'/F de E/F que son radicales. Entonces para todo $K'/F \in \mathrm{Rad}(E/F)$ existe un R_T-módulo G, no necesariamente único, tal que $F \leq G \leq T(E/F)$ y $K' = F(G)$. Pongamos $G_1 = G + L$. Entonces $LK' = L(G_1)$, ya que $LK' = L(G)$, $L \leq G_1 \leq T(EL/L)$ y G_1 es un R_T-módulo. Por lo que $\varepsilon(K'/L) \in \mathrm{Rad}(EL/L)$. De este modo la restricción de ε a las extensiones radicales da lugar a una función inyectiva

$$\rho : \mathrm{Rad}(E/F) \to \mathrm{Rad}(EL/L)$$

definida por

$$F(G)/F \mapsto F(G)L/L = L(G+L)/L$$

donde G es un R_T-módulo tal que $F \leq G \leq T(E/F)$.

PROPOSICIÓN 2.32. *Sea E/F una extensión finita de Galois con grupo de Galois Γ, y sea L/F una extensión arbitraria, con $L \leq \overline{k}$, tal que*

$$E \cap L = F.$$

Si $\mu(EL) = \mu(E)$, entonces se tiene:

(1) $(G + L) \cap E = G$ para todo R_T-módulo G con $F \leq G \leq T(E/F)$

(2) $G_1 = (G_1 \cap E) + L$ para todo R_T-módulo G_1, con $L \leq G_1 \leq T(EL/L)$.

(3) La función

$$\rho : ST(E/F) \to ST(EL/L)$$

$$F(G)/F \mapsto L(G+L)/L, \;\; F \leq G \leq T(E/F)$$

es biyectiva, y la función

$$ST(EL/L) \to ST(E/F),$$

$$L(G_1)/L \mapsto F(G_1 \cap E)/F, \;\; L \leq G_1 \leq T(EL/L)$$

es su inversa.

Demostración. (1) Sea $w \in (G + L) \cap E$. Así $w = x + y$ donde $x \in G$ y $y \in L$, por lo que $y = w - x \in E$. Así $y \in F$ ya que $E \cap L = F$. Por lo tanto $x \in G$.

Recíprocamente si $x \in G$ claramente $x \in (G + L) \cap E$.

(2) Denotamos por Γ_1 al grupo de Galois de EL/L. Hemos visto anteriormente que se tiene un isomorfismo de grupos

$$\Gamma_1 \to \Gamma, \;\; \sigma_1 \to \sigma_1 \mid E \tag{2.3}$$

Como $\mu(EL) = \mu(E)$, el isomorfismo anterior induce un isomorfismo de grupos

$$\upsilon : Z^1(\Gamma, \mu(E)) \to Z^1(\Gamma_1, \mu(EL))$$

dado como sigue: sea $h \in Z^1(\Gamma, \mu(E))$. Si $\sigma_1 \in \Gamma_1$ se tiene que $\sigma_1 \mid_E \in \Gamma$, y definimos $\upsilon(h)(\sigma_1) := h(\sigma_1 \mid_E)$. Ahora

$$\upsilon(h)(\sigma_1 \circ \sigma_2) = h(\sigma_1 \circ \sigma_2 \mid_E) = h(\sigma_1 \mid_E \circ \sigma_2 \mid_E)$$

Así $\upsilon(h)$ es un homomorfismo cruzado. Por construcción υ es un homomorfismo de grupos, y por (2.3) se tiene que υ es un isomorfismo de grupos.

Sea G_1 con $L \leq G_1 \leq T(EL/L)$. Ahora si $w \in (G_1 \cap E) + L$ entonces $w = x+y$ con $x \in (G_1 \cap E)$ y $y \in L$, así $w \in G_1$. Ahora sea $a_1 \in G_1$. Entonces $f_{a_1} \in Z^1(\Gamma_1, \mu(EL)$. Tenemos que existe $f \in Z^1(\Gamma, \mu(E))$ tal que $f_{a_1} = \upsilon(f)$. De la proposición 2.23 existe $a \in T(E/F)$ tal que $f_{a_1} = \upsilon(f = f_a)$.

Se tiene que $f_{a_1}(\sigma_1) = f_a(\sigma_1 \mid_E)$ para todo $\sigma_1 \in \Gamma_1$, de aquí se sigue que $\sigma_1(a_1) - a_1 = \sigma_1(a) - a$, es decir, $\sigma_1(a_1 - a) = a_1 - a$ para cada $\sigma_1 \in \Gamma_1$. Se sigue $a_1 - a \in L$. Por lo tanto $a_1 = a + b$ donde $b \in L$ y, además, $a \in G_1$ de donde $a \in (G_1 \cap E) + L$.

(3) Por la observación hecha previamente a esta proposición se tiene que ρ es inyectiva, por lo que basta mostrar que ρ es suprayectiva. Para ello, sea $K_1/L \in \mathrm{Rad}(EL/L)$, entonces $K_1 = L(G_1)$ para algún G_1 con

$$L \leq G_1 \leq T(EL/L).$$

Por lo tanto si ponemos $G = G_1 \cap E$, entonces $F(G)/F$ pertenece a $ST(E/F)$ y

$$\rho(F(G)/F) = L(F(G))/L = L(F(G_1 \cap E))/L = L(L + (G_1 \cap E))/L$$

y, por (2), se tiene que

$$L(L + (G_1 \cap E)) = L(L + G) = L(G_1) = K_1.$$

□

OBSERVACIÓN 2.33. (1) El isomorfismo υ definido en la prueba de la proposición 2.32 induce un isomorfismo de retículas

$$\begin{array}{rcl} \{U \mid U \leq Z^1(\Gamma, \mu(E))\} & \to & \{U_1 \mid U_1 \leq Z^1(\Gamma_1, \mu(EL))\} \\ U & \mapsto & U_1 = \upsilon(U). \end{array} \tag{2.4}$$

Por el corolario 2.29, existen isomorfismos de retículas

$$\{U \mid U \leq Z^1(\Gamma, \mu(E))\} \to \{G \mid F \leq G \leq T(E/F)\}$$

$$U \mapsto G = \{\alpha \in E \mid f_\alpha \in U\}.$$

y

$$\{U \mid U \leq Z^1(\Gamma, \mu(EL))\} \to \{G \mid F \leq G \leq T(EL/L)\}$$
$$U_1 \mapsto G_1 = \{\alpha_1 \in EL \mid f_{\alpha_1} \in U_1\}.$$

Ahora usando (2.4), se obtiene un isomorfismo de retículas

$$\upsilon : \{G \mid F \leq G \leq T(E/F)\} \to \{G_1 \mid L \leq G_1 \leq T(EL/L)\}$$
$$G \mapsto G_1 = \{\alpha_1 \in EL \mid f_{\alpha_1} \in \upsilon(\{f_\alpha\} \mid \alpha \in G)\}.$$

Se afirma que $\upsilon(G) = G + L$ para cada submódulo G que satisface que $F \leq G \leq T(E/F)$. Para ver esto, pongamos $G_1 = \upsilon(G)$, ahora sea $\alpha_1 \in (EL)^*$. Entonces

$$\begin{aligned}
\alpha_1 \in G_1 &\Leftrightarrow \text{existe } \alpha \in G \text{ tal que para cada } \sigma_1 \in \Gamma_1; f_{\alpha_1}(\sigma_1) = f_\alpha(\sigma_1 \mid_E) \\
&\Leftrightarrow \text{existe } \alpha \in G \text{ tal que para cada } \sigma_1 \in \Gamma_1; \sigma_1(\alpha_1) - \alpha_1 = \sigma_1(\alpha) - \alpha \\
&\Leftrightarrow \text{existe } \alpha \in G \text{ tal que para cada } \sigma_1 \in \Gamma_1; \sigma_1(\alpha_1 - \alpha) = \alpha_1 - \alpha \\
&\Leftrightarrow \text{existe } \alpha \in G, \text{ tal que } \alpha_1 - \alpha \in L,
\end{aligned}$$

este último paso se sigue de que la extensión EL/L es de Galois. Por lo tanto $\upsilon(G) = G + L$.

2.5. Algunos teoremas de estructura.

PROPOSICIÓN 2.34. *Sea L/K una extensión de campos tal que*

$$[L : K] = q$$

con q un primo diferente a $p = \text{car}(k)$. Entonces L/K no es radical ciclotómica.

Demostración. Supongamos que L/K es radical ciclotómica. Por lo tanto $\text{cog}(L/K)$ es no trivial. Sea $\overline{\alpha} \in \text{cog}(L/K)$ distinto de 0, esto significa que $\alpha \notin K$. Así, existe $M \in R_T$ tal que $\alpha^M \in K$. Podemos suponer que M es mónico y que es el polinomio de grado mínimo con tal propiedad, es decir el orden de $\overline{\alpha}$ es M, por lo que es posible suponer que existe un irreducible Q, reemplazando a α si es necesario, tal $\alpha^Q = a \in K$.

Sea $f(u) = \text{irr}(\alpha, K) \in K[u]$. Puesto que $u^Q - a = \prod(u - (\alpha + \lambda_Q^A)) \in K[u]$ entonces $f(u) \mid u^Q - a$. Por lo tanto $f(u) = \prod(u - (\alpha + \lambda_Q^B))$, para ciertos $B \in R_T$. Obsérvese que $\deg(f(u)) = q$, además $\sum(\alpha + \lambda_Q^B) = q\alpha + \lambda_Q^{\sum B} \in K$. Por otro lado puesto que $q \neq p$ entonces $q \neq 0$ en K. Así pues $D = \sum B$ se puede suponer no nulo, pues en caso contrario $\alpha \in K$ por lo que podemos suponer que el grado de D es menor que el grado de Q.

Por otra parte $\lambda_Q^D \notin K$, pero $\lambda_Q^D \in L$ y, por pureza, $\lambda_Q^D \in K$, lo cual es una contradicción. Por lo tanto, L/K no es radical ciclotómica. □

COROLARIO 2.35. *Sea L/K una extensión de Galois tal que*

$$[L : K] = p^s n$$

con $p \nmid n$ y $n > 1$. Entonces L/K no es radical ciclotómica.

Demostración. Por el teorema de Cauchy el grupo $G = \mathrm{Gal}(L/K)$ tiene un elemento de orden q, digamos g, donde q es un primo que divide a n. Considere el subgrupo $H = (g)$ de G. Si L/K fuese radical ciclotómica entonces, por la proposición 2.15, la extensión L/L', donde $L' = L^H$, es radical ciclotómica. Pero $[L : L'] = q$ y por la proposición 2.34 tal extensión no es radical ciclotómica. Por lo tanto L/K no es radical ciclotómica. □

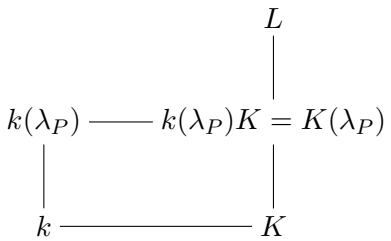
Nótese que podemos inferir de lo anterior el

COROLARIO 2.36. *Si L/K es Galois y radical ciclotómica, entonces $[L : K]$ es de la forma p^s, con $s \in \mathbb{N}$.*

Demostración. Si ocurre lo contrario, se tendrá que $[L : K] = p^n m$, con n entero y ≥ 0, $p \nmid m$ y $m > 1$. Sin embargo por el corolario 2.35 L/K no sería radical ciclotómica, lo cual es una contradicción. □

LEMA 2.37. *Sea L/K una extensión tal que $[L : K] = p^s$ con $s \in \mathbb{N}$. Entonces L/K es pura.*

Demostración. Supongamos que L/K no es pura, así existe $a = \lambda_P \in L$, $P \in R_T$ irreducible tal que $a^P = 0$ pero $a \notin K$. Considere el diagrama siguiente



Sea $\widetilde{K} = K \cap k(\lambda_P)$. Entonces por teoría de Galois se tiene que $K(\lambda_P)/K$ es Galois, con grupo de Galois G isomorfo a $\mathrm{Gal}(k(\lambda_P)/\widetilde{K})$. Por otro lado

$$\mid G \mid\mid [L : K] = p^s \text{ y } \mid G \mid\mid (q^d - 1)$$

donde $d = \deg(P)$. Por lo tanto $\mid G \mid = 1$, es decir, $\lambda_P \in K$. □

EJEMPLO 2.38. Una extensión de *Carlitz-Kummer*, ver [23], es una extensión L/K tal que

(1) K es una extensión finita de $k(\Lambda_M)$, para algún $M \in R_T$.

(2) L es campo de descomposición del polinomio $f(u) = u^M - z \in K[u]$, sobre K, donde $z \in K \setminus K^M$.

Por la proposición 2.3 inciso (4) de [23], se tiene que $[L : K] = p^t$. Ahora el lema 2.37 muestra que las extensiones de Carlitz-Kummer son extensiones radicales ciclotómicas.

Por otro lado, en base a los resultados anteriores, se tiene el

TEOREMA 2.39. *Una extensión de Galois L/K es radical ciclotómica si y sólo si es radical, separable y $[L : K] = p^s$ con $s \in \mathbb{N}$.*

En este contexto se tiene el siguiente teorema, en el cual no suponemos que L/K sea una extensión de Galois:

TEOREMA 2.40. *Si L/K es radical ciclotómica, entonces $[L : K] = p^n$ para alguna $n \geq 0$*

Demostración. Sea L/K radical ciclotómica. Entonces $L = K(\alpha_1, \ldots, \alpha_t)$, de tal modo que $\alpha_i^{M_i} = a_i \in K$ donde $M_i \in R_T$. Tomando $M_i = P_1^{\varepsilon_{1,i}} \cdots P_{r_i}^{r_i,i}$, $\delta_{i,j} = \alpha_i^{\frac{M_i}{P_{i,j}}}$ se tiene que $\delta_{i,j}^{P_{i,j}} = a_i$. Por lo que se tiene una torre de campos

$$K \subseteq K(\beta_1) \subseteq K(\beta_1, \beta_2) \subseteq \cdots \subseteq K(\beta_1, \cdots \beta_s) = L$$

donde para cada $i = 1, \ldots, s$ se tiene que $\beta_i^{P_i} = b_i \in K(\beta_1, \ldots, \beta_{i-1})$ y

$$[L : K] = \prod_{i=1}^{s} [K(\beta_1, \ldots, \beta_i) : K(\beta_1, \ldots, \beta_{i-1})]. \tag{2.5}$$

Es suficiente mostrar, en virtud de la ecuación (2.5), que si $L = K(\alpha)$, con $\alpha^P = a \in K$ y $P \in R_T$ mónico e irreducible, de tal manera que L/K sea radical ciclotómica, entonces $[L : K] = p^m$ para algún $m \in \mathbb{N}$.

Si $\lambda_P \in L$, entonces L/K es de Galois y, por el corolario 2.36, L/K es una p-extensión.

Ahora se considera el diagrama

$$\begin{array}{ccccc}
 & & L = K(\alpha) & \xrightarrow{\ a\ } & L(\lambda_P) = K(\lambda_P, \alpha) \\
 & & {\scriptstyle b}\big| & & \big|{\scriptstyle b} \\
 & K & \xrightarrow{\ d\ } K(\alpha) \cap K(\lambda_P) & \xrightarrow{\ a\ } & K(\lambda_P) \\
 & {\scriptstyle c}\big| & {\scriptstyle c}\big| & & \big|{\scriptstyle c} \\
k & \longrightarrow K \cap k(\lambda_P) & \xrightarrow{\ d\ } K(\alpha) \cap k(\lambda_P) & \xrightarrow{\ a\ } & k(\lambda_P)
\end{array}$$

Puesto que $K(\lambda_P, \alpha)/K(\lambda_P)$ es Galois además, por las proposiciones 2.2 y 2.3 de [23], se tiene que $N = \mathrm{Gal}(L(\lambda_P)/K(\lambda_P))$ puede pensarse

como un subgrupo de Λ_P, es decir, N es un p-grupo elemental abeliano y $\mid N \mid = b = p^n$.

Como

$$[L : K] = [L : K(\alpha) \cap K(\lambda_P)][K(\alpha) \cap K(\lambda_P) : K] = bd = p^n d$$

basta mostrar que $d = 1$.

Sean $H = \mathrm{Gal}(L(\lambda_P)/(K(\alpha) \cap K(\lambda_P)))$, $G = \mathrm{Gal}(L(\lambda_P)/K)$ y N denota al grupo $\mathrm{Gal}(L(\lambda_P)/K(\lambda_P))$. Nótese que N es subgrupo normal de G.

Se tiene que

$$G/N \cong \mathrm{Gal}(K(\lambda_P)/K) < \mathrm{Gal}(k(\lambda_P)/k) \cong C_{q^d-1} (= \mathbb{Z}/(q^d - 1)\mathbb{Z})$$

Así pues G/N es grupo cíclico de orden $q^d - 1$, primo relativo a p. Además se tiene que $\mid G/N \mid = ad$

Por el teorema de Hall, ver [11] Teorema 9.3.1., como G es soluble, existe R subgrupo de G, R cíclico de orden ad, tal que $G = NR$ (de hecho se tiene que, $G \cong N \rtimes R$ ya que $(\mid R \mid, \mid N \mid) = 1$).

Por el mismo teorema de Hall, todo subgrupo de orden un divisor de $\mid R \mid = ad$ esta contenido en un conjugado R' de R y se tiene que $G = NR' \cong N \rtimes R'$.

Sea $S = \mathrm{Gal}(L(\lambda_P)/K(\alpha)) \cong C_a$. Por lo tanto podemos suponer $S \subseteq R$ y $\mid R/S \mid = d$, nótese que $(d, p) = 1$.

Sea $E = L(\lambda_P)^R$. Observe que $L(\lambda_P)^S = K(\alpha) = L$. Por lo tanto $K \subseteq E \subseteq L$, $[L : E] = [R : S] = d = \mid R/S \mid$, además como L/K es radical ciclotómica lo es también L/E. Por lo tanto $d = 1$.

□

COROLARIO 2.41. *Con las notaciones del Teorema 2.40*

$$K(\alpha) \cap K(\lambda_P) = K, [L : K] = [L(\lambda_P) : K(\lambda_P)]$$

y

$$\mathrm{Irr}(u, \alpha, K) = \mathrm{Irr}(u, \alpha, K(\lambda_P)) = F_1(u) = \prod (u - (\alpha + \lambda_P^A)).$$

Demostración. Se sigue de la demostración del teorema 2.40. □

El siguiente corolario es análogo al teorema 2.39 excepto que no suponemos que L/K sea una extensión de Galois.

COROLARIO 2.42. *Una extensión L/K es radical ciclotómica si y sólo si es separable, radical y $[L : K] = p^m$ para algún $m \in \mathbb{N}$.*

Demostración. Se sigue del teorema 2.40 y el Lema 2.37. □

2.6. El análisis de algunos módulos cog.

En esta parte trataremos de encontrar, si es posible, la estructura de $\mathrm{cog}(L/K)$, donde L/K es una extensión radical separable, en particular radical ciclotómica. Antes de estudiar algunos casos particulares, mostraremos un lema que será de utilidad.

LEMA 2.43. *Sea L/K una extensión finita de Galois radical ciclotómica. Entonces*

$$B^1(G, \mu(L)) \cong \mu(L)/\mu(K).$$

donde $G = \mathrm{Gal}(L/K)$.

Demostración. Se define $\psi : \mu(L) \to B^1(G, \mu(L))$ como sigue: $\psi(u) = f_u$, donde $u \in \mu(L)$ y $f_u = \sigma(u) - u$ para cada $\sigma \in G$. Nótese que $\psi(u + v) = \psi(u) + \psi(v)$ ya que

$$\begin{aligned}(f_u + f_v)(\sigma) &= f_u(\sigma) + f_v(\sigma)\\ &= \sigma(u) - u + \sigma(v) - v\\ &= \sigma(u + v) - (u - v)\\ &= (f_{u+v})(\sigma).\end{aligned}$$

y si $M \in R_T$ se tendrá que $\psi(u^M) = f_u^M$, ya que

$$\begin{aligned}f_{u^M}(\sigma) &= \sigma(u^M) - u^M\\ &= (\sigma(u))^M - u^M\\ &= (\sigma(u) - u)^M\\ &= (f_u(\sigma))^M.\end{aligned}$$

Por lo tanto ψ es un homomorfismo de R_T-módulos, suprayectivo por la definición de $B^1(G, \mu(L))$. Puesto que $\ker(\psi) = \mu(K)$, por ser L/K de Galois, del primer teorema de isomorfismo sobre módulos, se tiene que ψ es un isomorfismo. □

EJEMPLO 2.44. Considere la extensión $k(\Lambda_P)/k$, con $P \in R_T$ mónico e irreducible. Sea $G = \mathrm{Gal}(k(\Lambda_P)/k)$. Ahora por el teorema 4.7 de [14] Capítulo 5, se tiene que

$$\mathrm{cog}(k(\Lambda_P)/k) \cong \oplus_Q \mathrm{cog}(k(\Lambda_P)/k)_Q$$

donde la suma anterior es sobre todos los polinomios mónicos irreducibles, Q, de R_T, y $\mathrm{cog}(k(\Lambda_P)/k)_Q$ denota el subconjunto de $\mathrm{cog}(k(\Lambda_P)/k)$ que tiene orden una potencia de Q.

Se mostrará que si $Q \neq P$ es mónico e irreducible, entonces

$$\mathrm{cog}(k(\Lambda_P)/k)_Q = \{0\}.$$

Supongamos lo contrario, así existe $\overline{\beta} \in \mathrm{cog}(k(\Lambda_P)/k)$, $\overline{\beta} \neq 0$, de orden Q^r, con $r \geq 1$. Por lo tanto de la proposición 2.7 se tiene que $\lambda_{Q^r} \in k(\Lambda_P)$.

Por otro lado se ha mostrado (ver proposición 1.7) que $\mu(K(\Lambda_M)) = \Lambda_M$, en particular, $\mu(K(\Lambda_P)) = \Lambda_P$. Así $\lambda_{Q^r}^P = 0$, es decir, $Q = P$ lo cual es una contradicción. Por lo tanto

$$\mathrm{cog}(k(\Lambda_P)/k) \cong \mathrm{cog}(k(\Lambda_P)/k)_P.$$

Puesto que $\mathrm{cog}(k(\Lambda_P)/k)$ es finito, por el teorema 4.9 de [14] Capítulo 5, se puede escribir

$$\mathrm{cog}(k(\Lambda_P)/k) \cong C_{P^{n_1}} \oplus \ldots \oplus C_{P^{n_k}}$$

donde $C_{P^{n_i}}$ es un R_T-módulo cíclico de orden P^{n_i}, para $1 \leq i \leq r$.

Por otro lado, puesto que $H^1(G, \Lambda_P) = \{0\}$ (ver [6] proposición 2.7) y $\mathrm{cog}(k(\Lambda_P)/k) \cong Z^1(G, \Lambda_P)$ (ver proposición 2.23) se tendrá, a partir del Lema 2.43

$$\mid \mathrm{cog}(k(\Lambda_P)/k) \mid = \mid H^1(G, \Lambda_P) \mid \frac{\mid \mu(k(\Lambda_P)) \mid}{\mid \mu(k) \mid} = \mid \Lambda_P \mid .$$

EJEMPLO 2.45. En este ejemplo, a menos que se especifique otra cosa, $q = p \geq 3$. Considere la extensión $L/k(\Lambda_T)$, donde L es el campo de descomposición del polinomio $f(X) = X^T - 1$, con coeficientes en $k(\Lambda_T)$, el grado de esta extensión es $[L : k(\Lambda_T)] = p$ (ver ejemplo 2.3). Trataremos de determinar la estructura de $\mathrm{cog}(L/k(\Lambda_T))$.

Supongamos que $\overline{\beta} \in \mathrm{cog}(L/k(\Lambda_T))$ tiene orden Q^r, con Q mónico irreducible, $r \geq 1$ y $Q \neq T$. Por la proposición 2.7 se tiene que $\lambda_{Q^r} \in L$. Puesto que $\lambda_Q = \lambda_{Q^r}^{Q^{r-1}} \in L$, por pureza se tiene que $\lambda_Q \in k(\Lambda_T)$, pero esto implica que $Q = T$ lo cual es una contradicción. Por lo tanto

$$\mathrm{cog}(L/k(\Lambda_T)) \cong \mathrm{cog}(L/k(\Lambda_T))_T,$$

donde $\mathrm{cog}(L/k(\Lambda_T))_T$ es el conjunto de elementos de $\mathrm{cog}(L/k(\Lambda_T))$ cuyo orden es una potencia de T.

Necesitaremos un lema para obtener la cardinalidad de $\mathrm{cog}(L/k(\Lambda_T))$. Para empezar sea $z \in k$, $z \neq 0$, y $N \in R_T$ un polinomio no constante. Considere $f(X) = X^N - z \in k(\Lambda_N)[X]$. El campo de descomposición de $f(X)$ sobre k es de la forma $L = k(\alpha, \lambda_N)$ donde α es una raíz arbitraria de $f(X)$ y λ_N un generador de Λ_N. Como el polinomio $f(X)$ es separable la extensión L/k es de Galois.

Sea $G = \mathrm{Gal}(L/k)$. Entonces dado $\sigma \in G$ se tiene que $\sigma(\alpha) = \alpha + \lambda^{M_\sigma}$ y $\sigma(\lambda) = \lambda^{N_\sigma}$, donde M_σ y N_σ se determinan salvo un múltiplo de N, y N_σ es primo relativo a N.

Por otro lado considere $G(N)$ el subgrupo de $GL_2(R_T/(N))$ de todas las matrices de la forma

$$\begin{pmatrix} 1 & 0 \\ \overline{B} & \overline{A} \end{pmatrix}$$

donde $\overline{B} \in R_T/(N)$ y $\overline{A} \in (R_T/(N))^*$. De esta descripción se sigue que $\text{card}(G(N)) = q^{\deg(N)}\Phi(N)$, por lo tanto es posible definir $\theta : G \to G(N)$ como sigue:

$$\theta(\sigma) = \begin{pmatrix} 1 & 0 \\ \overline{M_\sigma} & \overline{N_\sigma} \end{pmatrix}$$

LEMA 2.46. *Sea L/k la extensión anteriormente descrita y θ la función anteriormente definida. Entonces θ es un monomorfismo de grupos. Por otra parte si $N = P$, P mónico e irreducible, $z \in R_T$ como antes y la ecuación $f(X) = 0$ no tiene soluciones en R_T, entonces θ es un isomorfismo de grupos.*

Demostración. Sea $\sigma, \tau \in G$. Se tiene que

$$\begin{aligned} \sigma(\tau(\alpha)) &= \sigma(\alpha + \lambda^{M_\tau}) \\ &= \alpha + \lambda^{M_\sigma} + \lambda^{M_\tau N_\sigma} \end{aligned}$$

además $\sigma(\tau(\lambda)) = \sigma(\lambda^{N_\tau}) = \lambda^{N_\sigma N_\tau}$, por lo tanto

$$\theta(\sigma \cdot \tau) = \begin{pmatrix} 1 & 0 \\ M_\sigma + M_\tau N_\sigma & N_\sigma N_\tau \end{pmatrix}$$

pero esta última matriz es la multiplicación de las matrices

$$\theta(\sigma) = \begin{pmatrix} 1 & 0 \\ M_\sigma & N_\sigma \end{pmatrix} \quad \text{y} \quad \theta(\tau) = \begin{pmatrix} 1 & 0 \\ M_\tau & N_\tau \end{pmatrix}.$$

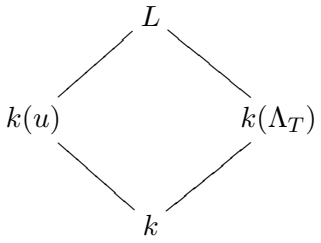
Por lo tanto θ es un homomorfismo de grupos. Si $\theta(\sigma)$ es la matriz identidad se tiene que M_σ es un múltiplo de N y $N_\sigma = 1 + NQ$, así $\sigma = e$, es decir, θ es un monomorfismo de grupos.

Si $N = P$, P mónico e irreducible, $z \in R_T$ como antes y la ecuación $f(X) = 0$ no tiene soluciones en R_T, entonces por el teorema 1.7 (3) de [15], se tiene que $\text{Gal}(L/k(\lambda_P))$ tiene cardinalidad $q^{\deg(P)}$, es decir, el monomorfismo anterior es un isomorfismo. □

Se mostrará que $\mu(L) = \Lambda_T$. Para empezar, claramente $\Lambda_T = \mu(k(\Lambda_T)) \subseteq \mu(L)$. Por otro lado sea $u \in \mu(L)$ no nulo, así, existe un $N \in R_T$ tal que $u^N = 0$. Por lo tanto u es de la forma λ_N^M. Podemos suponer que $(M, N) = 1$, así por la proposición 12.2.21 de [25], podemos afirmar que $\lambda_N \in L$. Sea

$N = P_1^{\alpha_1} \cdots P_s^{\alpha_s}$, entonces $\lambda_{P_i} = \lambda_N^{P_1^{\alpha_1} \cdots P_i^{\alpha_i - 1} \cdots P_s^{\alpha_s}} \in L$, y por pureza tendremos que $\lambda_{P_i} \in k(\Lambda_T)$. Así $P_i = T$. Por lo tanto $N = T^n$ con $n \geq 1$ y $n \in \mathbb{N}$.

Supongamos que $n \geq 2$ y considere el diagrama



Del diagrama anterior obtenemos $[L : k(u)]\Phi(T^n) = p(p-1)$. Puesto que $\Phi(T^n) = p^{n-1}(p-1)$, se sigue que $[L : k(u)]p^{n-1} = p$. Si $n \geq 3$ entonces $n-2 \geq 1$, así $[L : k(u)]p^{n-2} = 1$ lo cual es una contradicción. Solo resta considerar el caso $n = 2$, que implica que $L = k(u)$, pero del lema 2.46 se tiene que $\mathrm{Gal}(L/k)$ es no abeliano, lo cual contradice que el grupo $\mathrm{Gal}(k(\Lambda_{T^2})/k)$ es abeliano. Por lo tanto $n = 1$ y $u = \lambda_T^M \in k(\Lambda_T)$.

Por lo anterior

$$H^1(G, \mu(L)) = Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong \mathrm{Hom}(G, \mu(L)),$$

y por el lema 2.43 se tiene que $B^1(G, \mu(L)) = \{0\}$. De esta manera, utilizando la demostración del lema 2.19, se tiene que

$$| \operatorname{cog}(L/k(\Lambda_T)) | = [L : k(\Lambda_T)] = p$$

.

EJEMPLO 2.47. Considere la extensión $k(\Lambda_{P^n})/k(\Lambda_P)$ con $P \in R_T$ mónico e irreducible. La extensión es radical ciclotómica (ver ejemplo 2.5). Considere el R_T-módulo

$$\operatorname{cog}(k(\Lambda_{P^n})/k(\Lambda_P)).$$

Si denotamos por $\operatorname{cog}(k(\Lambda_{P^n})/k(\Lambda_P))_Q$ al subconjunto de

$$\operatorname{cog}(k(\Lambda_{P^n})/k(\Lambda_P))$$

cuyos elementos tienen orden una potencia de Q, entonces, por el teorema 4.7 de [14] Capítulo 5, se tiene que

$$\operatorname{cog}(k(\Lambda_{P^n})/k(\Lambda_P)) \cong \oplus_Q \operatorname{cog}(k(\Lambda_{P^n})/k(\Lambda_P))_Q$$

donde la suma anterior es sobre todos los mónicos irreducibles Q.

Se afirma que si $Q \neq P$ es mónico irreducible, entonces

$$\operatorname{cog}(k(\Lambda_{P^n})/k(\Lambda_P))_Q = \{0\}.$$

En caso contrario, existe $\overline{w} \in \mathrm{cog}(k(\Lambda_{P^n})/k(\Lambda_P))_Q$, no cero, cuyo orden es Q^m. Ahora por la Proposición 2.7, se tiene que $\lambda_{Q^m} \in k(\Lambda_{P^n})$, lo que lleva a que $Q = P$, una contradicción con la elección de Q.

Por otra parte, se observa que, ver [14] Capítulo 5, teorema 4.9

$$\mathrm{cog}(k(\Lambda_{P^n})/k(\Lambda_P)) \cong C_{P^{\alpha_1}} \oplus \ldots \oplus C_{P^{\alpha_m}}, \quad \alpha_1 \geq \ldots \geq \alpha_m \geq 1$$

y los $C_{P^{\alpha_i}}$ son módulos cíclicos, cuyo generadores tienen orden P^{α_i}, respectivamente.

En cuanto a la determinación de la cardinalidad del módulo

$$\mathrm{cog}(k(\Lambda_{P^n})/k(\Lambda_P))$$

sólo tenemos el siguiente caso especial. Sea $P(T) = T$, $q = p > 2$ y $n = 2$. Entonces $\mathrm{card}(H_{T^2}) = q^{d(n-1)} = p$, con $d = \deg(P(T)) = 1$, donde H_{T^2} es el grupo definido en la proposición 1 de [17]. Por lo tanto el grupo H_{T^2} es cíclico. Usando el corolario 2.21, Capítulo 1 de [26], se tiene que

$$H^1(H_{T^2}, \Lambda_{T^2}) \cong \ker(N_{H_{T^2}})/D\Lambda_{T^2}$$

donde definimos $N_{H_{T^2}} : \Lambda_{T^2} \to \Lambda_{T^2}$ y $D : \Lambda_{T^2} \to \Lambda_{T^2}$ como (ver [19] Capítulo 2)

$$N_{H_{T^2}}(x) = x + \sigma \cdot x + \ldots + \sigma^{p-1} \cdot x$$
$$D(x) = \sigma \cdot x - x$$

donde $\sigma = 1 + T + (T^2)$ es un generador de H_{T^2} y $x \in \Lambda_{T^2}$. Por otro lado si $x = \lambda_{T^2}^M$ se tiene que

$$\begin{aligned} N_{H_{T^2}}(x) &= \lambda_{T^2}^M + \lambda_{T^2}^{M(T+1)} + \cdots \lambda_{T^2}^{M(1+(p-1)T)} \\ &= \lambda_{T^2}^{pM+(1+2+\cdots+p-1)MT} = 0. \end{aligned}$$

Se observa que $1 + 2 + \cdots + (p-1) = 0$ ya que tal suma es igual a $\frac{p(p-1)}{2}$ y $2 \neq 0$ en $\mathbb{F}_p$. De esta manera se tiene que $\ker(N_{H_{T^2}}) = \Lambda_{T^2}$. Obsérvese también que $D(x) = \lambda_{T^2}^{M(T+1)} - \lambda_{T^2}^M = \lambda_T^M$, de aquí se sigue que

$$D\Lambda_{T^2} = \Lambda_T.$$

Por lo tanto $H^1(H_{T^2}, \Lambda_{T^2}) = \Lambda_{T^2}/\Lambda_T$. Por otra parte del Lema 2.43 se tiene que $\mathrm{card}(B^1(H_{T^2}, \Lambda_{T^2})) = \mathrm{card}(\Lambda_{T^2}/\Lambda_T)$ y recordando que

$$H^1(H_{T^2}, \Lambda_{T^2}) = Z^1(H_{T^2}, \Lambda_{T^2})/B^1(H_{T^2}, \Lambda_{T^2})$$

se obtiene, por la proposición 2.23

$$\mathrm{card}(\mathrm{cog}(K(\Lambda_{T^2})/K(\Lambda_T))) = \mathrm{card}(Z^1(H_{T^2}, \Lambda_{T^2})) = [K(\Lambda_{T^2}) : K(\Lambda_T)]^2.$$

El siguiente lema es crucial para mostrar que si tenemos una extensión K/k pura y separable, en el sentido de C. Greither y D. K. Harrison (ver [10]), entonces la extensión K/k es cogalois en el sentido clásico.

LEMA 2.48. *Supongamos que $K = k(\alpha)$, $\alpha^p = a \in k$, $[K : k] = p$ primo, y K/k es pura y separable. Entonces K/k es cogalois.*

La demostración del lema anterior consta de tres pasos, a saber

(1) Si q es un primo diferente de p, entonces $\mathrm{cog}(K/k)$ no tiene elementos de orden q.

(2) $\mathrm{cog}(K/k)$ no tiene elementos de orden p^2.

(3) αk^* genera a $\mathrm{cog}(K/k)$.

El lema que a continuación probaremos recoge parte de la hipótesis del lema 2.48, en el sentido de este trabajo, sin embargo no siempre es válido en general.

LEMA 2.49. *Considere la extensión $L/k(\lambda_P)$, donde L es campo de descomposición del polinomio $X^P - a$, $P \in R_T$ es irreducible y $a \in k(\lambda_P) \setminus k(\lambda_P)^P$. El módulo $\mathrm{cog}(L/k(\lambda_P))$ no tiene elementos de orden Q, un irreducible, distinto de P. Además si $\nu_{\mathfrak{p}}(a) \geq q^d$, donde $d = \deg(P)$, se tiene que $\mathrm{cog}(L/K)$ no tiene elementos de orden P^2.*

Demostración. Supongamos que $\mathrm{cog}(L/k(\lambda_P))$ tiene un elemento de orden Q irreducible. Entonces como $L/k(\lambda_P)$ es Galois, se tiene que $\lambda_Q \in L$ y como $L/k(\lambda_P)$ es radical ciclotómica, se tendrá que $\lambda_Q \in \mu(K) = \Lambda_P$, por la proposición 1.7, por lo tanto $Q = P$.

Ahora supongamos que $\mathrm{cog}(L/k(\lambda_P))$ tiene un elemento de orden P^2, es decir, existe $\widehat{\beta} \in \mathrm{cog}(L/K)$ tal que $\beta^{P^2} = b \in K$. Entonces, como $L/k(\lambda_P)$ es radical, se tiene que por la proposición 2.7, $\lambda_{P^2} \in L$. Entonces se considera el diagrama siguiente

$$\begin{array}{ccc}
\mathcal{O}_L & \longrightarrow & L \\
\downarrow & & \downarrow \\
\mathcal{O}_{K(\lambda_{P^2})} & \longrightarrow & K(\lambda_{P^2}) \\
\downarrow & & \downarrow \\
\mathcal{O}_K & \longrightarrow & K \\
\downarrow & & \downarrow \\
R_T & \longrightarrow & k
\end{array}$$

Ahora el índice de ramificación del primo P, en la extensión $K(\lambda_{P^2})/K$, es $\Phi(P^2)$ (ver [25] Capítulo 12 proposición 12.3.14.) así el índice de ramificación de P en la extensión L/k es $\widetilde{d}\Phi(P^2)$, donde $\widetilde{d} = e_{L/K(\lambda_{P^2})}$; pero del

teorema 3.9. de [23] el índice de ramificación es $\Phi(P)$. En otras palabras, $d\Phi(P^2) = \Phi(P)$, lo cual es absurdo, de aquí se tiene la afirmación. □

El siguiente ejemplo muestra que si L/K es pura y separable con $[L : K] = p$, $L = K(\alpha^P)$ y P un polinomio irreducible, entonces $\mathrm{cog}(L/K)$ contiene un elemento de orden Q, Q polinomio irreducible distinto de P. Así el paso (1) del lema 2.48 en el sentido de este trabajo no siempre es cierto.

EJEMPLO 2.50. Sean $P, Q \in R_T$, irreducibles y distintos. Considere la extensión $L = k(\Lambda_{P^2Q^2})/k$, nótese que $L = k(\lambda_{P^2}, \lambda_{Q^2})$. Sea $\sigma = 1 + PQ \in G = \mathrm{Gal}(L/k)$. Se observa que $\sigma \neq 1$ puesto que $\lambda_{P^2Q^2}^{1+PQ} = \lambda_{P^2Q^2} + \lambda_{PQ} \neq \lambda_{P^2Q^2}$.

Obsérvese que $\sigma(\lambda_{PQ}) = \lambda_{PQ}^{1+PQ} = \lambda_{PQ}$, por lo tanto si K es el campo fijo de (σ), se tiene que $\lambda_{PQ} \in K$.

Por otro lado se tiene que $\sigma^p = (1 + PQ)^p = 1 + P^pQ^p \equiv 1 \text{ mód } P^2Q^2$, es decir, el orden de σ es p. Por lo tanto $[L : K] = p$.

Por otra parte $\alpha = \lambda_{P^2} \notin K$, puesto que $\sigma(\lambda_{P^2}) = \lambda_{P^2} + \lambda_P^Q \neq \lambda_{P^2}$. De modo análogo se puede mostrar que $\beta = \lambda_{Q^2} \notin K$.

Ahora, como $[L : K] = p$, se tiene que $L = K(\alpha) = K(\beta)$, además $\alpha^P = \lambda_P$ y $\beta^Q = \lambda_Q$. Por lo tanto el módulo $\mathrm{cog}(L/K)$, tiene elementos de orden P y de orden Q.

El siguiente ejemplo muestra que si L/K es pura y separable con $[L : K] = p$, $L = K(\alpha^P)$ y P un polinomio irreducible, entonces $\mathrm{cog}(L/K)$ contiene un elemento de orden P^2. Así el paso (2) del lema 2.48 en el sentido de este trabajo no siempre es cierto.

EJEMPLO 2.51. Sea $L = k(\Lambda_{P^3})$ y $\sigma = 1+P \in \mathrm{Gal}(L/k(\Lambda_P))$. Obsérvese que $\sigma^p = (1 + P)^p \equiv 1 \text{ mód } P^3$, aquí suponemos que $q = p^s$ con $p \geq 3$. Además $\sigma \neq 1$ ya que $\sigma(\lambda_{P^3}) = \lambda_{P^3} + \lambda_{P^2} \neq \lambda_{P^3}$.

Sea $K = L^{(\sigma)}$, se tiene que $[L : K] = p$. Por otra parte $\sigma(\lambda_{P^2}) = \lambda_{P^2} + \lambda_P \neq \lambda_{P^2}$. Por lo tanto $\alpha = \lambda_{P^2} \notin K$. Así $L = K(\alpha)$ y $\alpha^P = a \in K$.

Pero $\lambda_{P^3} \in L$ tiene orden P^2, ya que $\lambda_{P^3}^{P^2} \in K$ y $\lambda_{P^3}^P \notin K$. Por lo tanto el módulo $\mathrm{cog}(L/K)$ tiene elementos de orden P^2.

2.7. Una estimación para $|\mathrm{cog}(L/K)|$

En esta sección establecemos una cota superior para la cardinalidad del módulo $\mathrm{cog}(L/K)$, con L/K una extensión arbitraria. En lo que sigue se tiene que $q = p^s$.

OBSERVACIÓN 2.52. Si L/K es Galois y radical ciclotómica tal que $\mu(K) = \mu(L)$, entonces al ser radical L es de la forma $K(\rho_1, \ldots, \rho_t)$, con $\rho^{M_i} = a_i \in K$, para algunos $M_i \in R_T$. Por otra parte, las raíces de $X^{M_i} - a_i$ son $\{\rho_i + \lambda_{M_i}^A\}_{A \in R_T}$. Por lo tanto $\mathrm{Gal}(K(\rho_i)/K) \subseteq \Lambda_{M_i}$. De esta manera $\mathrm{Gal}(K(\rho_i)/K)$ es elemental abeliano.

Puesto que se tiene una inyección

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_{i=1}^{t} \mathrm{Gal}(K(\rho_i)/K).$$

se sigue que $\mathrm{Gal}(L/K)$ es elemental abeliano.

Por otra parte, nótese que si L/K es una extensión, entonces $\mu(L) = \Lambda_M$ y $\mu(K) = \Lambda_N$, para algunos $M, N \in R_T$. Por lo tanto definimos

$$\deg(\mu(L)) = \deg(M).$$

PROPOSICIÓN 2.53. *Sea L/K una extensión Galois y radical ciclotómica. Supongamos que $\mu(L) = \mu(K)$, así por la observación 2.52 se tiene que $\mathrm{Gal}(L/K) \cong C_p^m$, para algún $m \in \mathbb{N}$. Entonces*

$$|\mathrm{cog}(L/K)| = q^{m \deg(\mu(L))}.$$

Demostración. Puesto que $B^1(G, \mu(L)) = \{0\}$ y $H^1(G, \mu(L)) \cong \mathrm{Hom}(G, \mu(L))$ (ver [26] Capítulo 1), entonces de la proposición 2.23, se tiene que

$$\mathrm{cog}(L/K) \cong Z^1(G, \mu(L))/B^1(G, \mu(L)) \cong H^1(G, \mu(L)) \cong \mathrm{Hom}(G, \mu(L))$$

además $\mu(L) \cong C_p^{s \deg(\mu(L))}$. Por lo tanto

$$\begin{aligned} \mathrm{Hom}(G, \mu(L)) &= \mathrm{Hom}(C_p^m, C_p^{s\deg(\mu(L))}) \\ &= \mathfrak{L}_p(\mathbb{F}_p^m, \mathbb{F}_p^{s\deg(\mu(L))}) \\ &= \mathfrak{M}_{m \times s\deg(\mu(L))}(\mathbb{F}_p) \end{aligned}$$

Por lo que $|\mathrm{Hom}(G, \mu(L))| = q^{m \deg(\mu(L))}$.

□

PROPOSICIÓN 2.54. *Sea L/K una extensión Galois y radical ciclotómica y supongamos que $L = K(\mu(L))$. Entonces $|\mathrm{cog}(L/K)| \leq q^{m \deg(\mu(L))}$.*

Demostración. Obsérvese que, en primer lugar, $[L : K] = p^m$ para algún $m \in \mathbb{N}$ (ver corolario 2.36). Ahora la demostración es por inducción sobre m. Sea L/K Galois y radical ciclotómica, tal que $L = K(\mu(L))$ y $[L : K] = p$. Por lo tanto L/K es cíclica de grado p. Considere los polinomios $M = P_1^{\alpha_1} \cdots P_r^{\alpha_r}$ y $N = P_1^{\beta_1} \cdots P_r^{\beta_r}$, con $1 \leq \beta_i \leq \alpha_i$, donde $i = 1, \ldots, r$.

Sea $G = (\sigma)$, así pues $\sigma(\lambda_M) = \lambda_M^A$, puesto que la acción de Carlitz-Hayes conmuta con σ. Nótese que $\sigma(\lambda_M) \neq \lambda_M$, en caso contrario esto implicaría que $\lambda_M \in K$, es decir, $L = K$ lo cual es una contradicción. Por lo tanto $M \nmid (A-1)$, y como $\sigma(\lambda_N) = \lambda_N$ se tiene que $N \mid (A-1)$. Para ver esta última afirmación, se observa que $M = ND$, por lo tanto $\lambda_N = \lambda_N^D$, de esta manera se tiene que

$$\lambda_N = \sigma(\lambda_N) = \sigma(\lambda_M^D) = (\sigma(\lambda_M))^D = \lambda_M^{AD} = \lambda_N^A.$$

así $\lambda_N^{A-1} = 0$, es decir, $N \mid (A-1)$.

Por otro lado

$$\begin{aligned}\mathrm{Tr}_G(\lambda_M) &= \lambda_M + \lambda_M^A + \lambda_M^{A^2} + \cdots + \lambda_M^{A^{p-1}} \\ &= \lambda_M^{1+A+A^2+\cdots+A^{p-1}} = \lambda_M^{\frac{A^p-1}{A-1}} \\ &= \lambda_M^{(A-1)^{p-1}}.\end{aligned}$$

donde la última igualdad se debe a que $\frac{A^p-1}{A-1} = \frac{(A-1)^p}{A-1}$.

Por lo tanto $\mathrm{Tr}_G(\lambda_M) \in K \cap \Lambda_M = \Lambda_N$. De aquí se obtiene que existe un $C \in R_T$ tal que $\lambda_M^{(A-1)^{p-1}} = \lambda_N^C$. Como se tiene la igualdad $\sigma^p = 1$ se sigue que $\sigma^p(\lambda_M) = \lambda_M^{A^p} = \lambda_M$, es decir, $\lambda_M^{A^p-1} = 0$ y como $A^p - 1 = (A-1)^p$, se tendrá que $M \mid (A-1)^p$.

Nótese que podemos escribir $A-1 = P_1^{\gamma_1} \cdots P_r^{\gamma_r} Q$ con $(Q, P_1 \cdots P_r) = 1$. Ahora si $\beta_i < \alpha_i$ se tiene que $\lambda_{NP_i} \in L \setminus K$ por lo tanto

$$\sigma(\lambda_{NP_i}) = \sigma(\lambda_M^D) = (\sigma(\lambda_M))^D = (\lambda_M^A)^D = \lambda_{NP_i}^A \neq \lambda_{NP_i}.$$

Así $NP_i \nmid (A-1)$. De aquí se sigue lo siguiente:

(i) Puesto que $M \nmid (A-1)$ se tiene que $\gamma_{i_0} < \alpha_{i_0}$ para algún $i_0 \in \{1, \ldots, r\}$.

(ii) Puesto que $N \mid (A-1)$ se tiene que $\beta_i \leq \gamma_i$. Ya que $NP_i \nmid (A-1)$, entonces $\beta_i + 1 > \gamma_i$. Por lo tanto $\beta_i = \gamma_i$.

(iii) Como $\lambda_M^{(A-1)^{p-1}} = \lambda_N^C$ se tiene que $\alpha_i - (p-1)\gamma_i \leq \beta_i$, para $1 \leq i \leq r$.

(iv) De $M \mid (A-1)^p$ se sigue que $\alpha_i \leq p\gamma_i$, para $1 \leq i \leq r$.

Ahora $\mathrm{Tr}_G(\lambda_M^B) = (\mathrm{Tr}(\lambda_M))^B = \lambda_M^{B(A-1)^{p-1}}$, la igualdad intermedia se da porque la acción de Carlitz-Hayes conmuta.

Sea $B = P_1^{\delta_1} \cdots P_r^{\delta_r} R$ con $(R, P_1 \cdots P_r) = 1$. Se tiene

$$\begin{aligned}\lambda_M^B \in \operatorname{Ker}\operatorname{Tr}_G &\Leftrightarrow \delta_i + (p-1)\gamma_i \geq \alpha_i \text{ para cada } i \\ &\Leftrightarrow \delta_i \geq 0 \text{ y } \delta_i + (p-1)\gamma_i \geq \alpha_i \text{ para cada } i \\ &\Leftrightarrow \delta_i \geq \max\{0, \alpha_i - (p-1)\gamma_i\} \text{ para cada } i.\end{aligned}$$

Por lo tanto $\operatorname{Ker}\operatorname{Tr}_G = (\lambda_M^B)$ con $B = P_1^{\delta_1} \cdots P_r^{\delta_r}$ y

$$\delta_i = \max\{0, \alpha_i - (p-1)\gamma_i\}$$

con $1 \leq i \leq r$. Así $(\lambda_M^B) = (\lambda_{M'})$, con $M' = P_1^{\mu_1} \cdots P_r^{\mu_r}$ donde

$$\mu_i = \max\{0, \alpha_i - \delta_i\}$$

y $1 \leq i \leq r$.

Además $I_G(\lambda_M) = ((\sigma - 1)\lambda_M) = (\lambda_M^{A-1})$, donde $I_G : \mu(L) \to \mu(L)$ es el homomorfismo definido por $I_G(u) = \sigma(u) - u$. Por otro lado

$$I_G(\lambda_M) = (\lambda_{M''})$$

con $M'' = P_1^{\varphi_1} \cdots P_r^{\varphi_r}$, donde $\varphi_i = \max\{\alpha_i - \gamma_i, 0\}$ y $1 \leq i \leq r$.

Nótese que $\varphi_i = \alpha_i - \beta_i$ si $\beta_i < \alpha_i$, esto se sigue de (ii). Si $\alpha_i = \beta_i$, de (ii) se obtiene que $\alpha_i - \gamma_i \leq 0$. Por lo tanto $\varphi_i = \alpha_i - \beta_i$.

Así pues, del corolario 2.21 de [26], se tiene que

$$|H^1(G, \mu(L))| = \frac{|(\lambda_{M'})|}{|(\lambda_{M''})|} = |(\lambda_{M'''})|$$

con $M''' = P_1^{\varepsilon_1} \cdots P_r^{\varepsilon_r}$ de tal modo que

$$\varepsilon_i = \mu_i - \varphi_i = \max\{0, \alpha_i - \delta_i\} - (\alpha_i - \beta_i) \; 1 \leq i \leq r$$

Por otro lado $\alpha_i - \delta_i = \min\{\alpha_i, (p-1)\beta_i\} > 0$, además

$$\mu_i = \max\{0, \alpha_i - \delta_i\} = \alpha_i - \delta_i = \min\{\alpha_i, (p-1)\beta_i\}.$$

Por lo tanto $\varepsilon_i = \min\{\alpha_i, (p-1)\beta_i\} - (\alpha_i - \beta_i)$. De lo anterior se sigue que:

(i) Si $\alpha_i \leq (p-1)\beta_i$, entonces $\varepsilon_i = \beta_i$

(ii) Si $(p-1)\beta_i < \alpha_i$, entonces $\varepsilon_i = p\beta_i - \alpha_i < \beta_i$
De (i) y (ii) se obtiene que $\varepsilon_i \leq \beta_i$.

Por lo que

$$|H^1(G, \mu(L))| = q^{\deg M'''} \leq q^{\deg N}$$

y

$$\begin{aligned}|\mathrm{cog}(L/K)| =& |H^1(G,\mu(L))||B^1(G,\mu(L))| \\ =& |H^1(G,\mu(L))|\ \frac{|\mu(L)|}{|\mu(K)|} \\ =& q^{\deg M'''} q^{\deg M - \deg N} \\ \leq& q^{\deg M} = q^{\deg(\mu(L))}\end{aligned}$$

la segunda igualdad se da por el lema 2.43.

Ahora sea $L = K(\mu(L))$, L/K Galois y radical ciclotómica. Así, por el Teorema 2.57, se tiene que $[L : K] = p^m$ para algún $m \in \mathbb{N}$. Sea H un subgrupo de G con orden p^{m-1}. Si $E = L^H$, entonces $K \subseteq E \subseteq L$. Nótese que $[E : K] = p$, $[L : E] = p^{m-1}$ y $L = E(\mu(L))$.

Si E/K no fuera radical ciclotómica, entonces $\mathrm{cog}(E/K) = \{0\}$, ya que en caso contrario existe $\overline{\alpha} \in \mathrm{cog}(E/K) \neq \{0\}$ no cero, en particular esto implica que $\alpha \notin K$. De esta manera $E = K(\alpha)$, pero esto implica que E/K es radical ciclotómica, lo cual es absurdo.

Si E/K es radical ciclotómica se tienen dos casos a considerar
(i) $\mu(E) \neq \mu(K)$ y
(ii) $\mu(E) = \mu(K)$.
En el caso (i), por lo demostrado para el caso $[E : K] = p$ se tiene que

$$|\mathrm{cog}(E/K)| \leq q^{\deg(\mu(E))}.$$

En el caso (ii), por la proposición 2.53 se tiene que

$$|\mathrm{cog}(E/K)| = q^{\deg(\mu(E))}.$$

Así, en cualquier caso,

$$|\mathrm{cog}(E/K)| \leq q^{\deg(\mu(E))} \leq q^{\deg(\mu(L))}.$$

Por lo tanto, puesto que $L = E(\mu(L))$ y $[L : E] = p^{m-1}$, por inducción se tiene que $|\ \mathrm{cog}(L/E)\ | \leq q^{(m-1)\deg(\mu(L))}$. Por lo tanto de la sucesión exacta

$$0 \to \mathrm{cog}(E/K) \to \mathrm{cog}(L/K) \to \mathrm{cog}(L/E)$$

se tiene que

$$|\mathrm{cog}(L/K)| \leq |\mathrm{cog}(E/K)||\mathrm{cog}(L/E)| \leq q^{m\deg(\mu(L))}.$$

□

De la demostración de la proposición 2.54, para el caso $m = 1$, se tiene el siguiente teorema

TEOREMA 2.55. *Sean L/K cíclica de grado p, $L = K(\alpha)$ tal que $\overline{\alpha}$ pertenece a $\mathrm{cog}(L/K)$. Entonces L/K es radical ciclotómica, $|\mathrm{cog}(L/K)|= p^{st}$, donde $q = p^s$ y*

$$t = \begin{cases} \deg(\mu(L)) - \deg(\mu(K)) + \deg(\frac{B-1}{C}) & si\ \mu(L) \neq \mu(K), \\ \deg(\mu(L)) & si\ \mu(L) = \mu(K). \end{cases}$$

donde $\sigma(\lambda_M) = \lambda_M^B$, donde C es de grado mínimo tal que $C \mid (B-1)$ y $M \mid C(B-1)^{p-1}$.

Demostración. Esto se sigue de la demostración de la proposición 2.54, para el caso $m = 1$. □

PROPOSICIÓN 2.56. *Sea L/K Galois radical ciclotómica. Entonces*

$$|\mathrm{cog}(L/K)| \leq q^{m \deg(\mu(L))}.$$

donde $[L : K] = p^m$.

Demostración. Sea $E = K(\mu(L))$ con $K \subseteq E \subseteq L$. Entonces

$$|\mathrm{cog}(L/K)| \leq |\mathrm{cog}(E/K)||\mathrm{cog}(L/E)| \leq q^{m\deg(\mu(L))}$$

por la proposición 2.54. □

TEOREMA 2.57. *Sea L/K radical ciclotómica. Entonces si $\widetilde{L}$ es la cerradura de Galois de L, se tendrá*

$$|\mathrm{cog}(L/K)| \leq q^{m \deg(\mu(\widetilde{L}))}$$

donde $[\widetilde{L} : K] = p^m$.

Demostración. Sean $G = \mathrm{Gal}(\widetilde{L}/K) = HN$ con H un subgrupo normal de G, N el p subgrupo de Sylow de G. Sea $F = \widetilde{L}^H$. Se puede suponer, cambiando H por un conjugado, que $F = L$. De aquí tenemos el diagrama

$$\begin{array}{ccc} L & \overset{H}{\text{——}} & \widetilde{L} \\ | & & | N \\ K & \text{——} & E \end{array}$$

Sea $\overline{\alpha} \in \mathrm{cog}(L/K)$, distinto de cero. Así existe $N \in R_T$ tal que $\alpha^N = a \in K$. Puesto que $\alpha \in \widetilde{L}$, $\alpha^N \in K \subseteq E$, es decir, $\overline{\alpha} \in \mathrm{cog}(\widetilde{L}/E)$. Si $\overline{\alpha} = 0$ en $\mathrm{cog}(\widetilde{L}/E)$, entonces $\alpha \in E \cap L = K$, así $\alpha = 0$ en $\mathrm{cog}(L/K)$ una contradicción.

Por lo anterior $\mathrm{cog}(L/K) \subseteq \mathrm{cog}(\widetilde{L}/E)$ y

$$|\mathrm{cog}(L/K)| \leq |\mathrm{cog}(\widetilde{L}/E)| \leq q^{m \deg(\mu(\widetilde{L}))}.$$

□

Se esperaría que $|\mathrm{cog}(L/E)| = [L:E]^{s\deg(\mu(L))}$, pero se tiene el ejemplo siguiente.

EJEMPLO 2.58. Sea $L = k(\Lambda_{P^{2p-1}})$, con $P \in R_T$ irreducible, y considere $\sigma = 1 + P^2 \in \mathrm{Gal}(k(\Lambda_{P^{2p-1}})/k)$. Se tiene

$$\sigma(\lambda_{2p-1}) = \lambda_{P^{2p-1}} + \lambda_{P^{2p-3}} \neq \lambda_{P^{2p-1}}$$

de este modo $\sigma \neq 1$.

Por otro lado $\sigma^p = (1+P^2)^p = 1 + P^{2p}$, de esta manera

$$\sigma^p(\lambda_{P^{2p-1}}) = \lambda_{P^{2p-1}} + \lambda_{P^{2p-1}}^{P^{2p}} = \lambda_{P^{2p-1}}.$$

Por lo tanto $\sigma^p = 1$ y el orden de σ es p.

Si $E = L^{(\sigma)}$, entonces $[L:E] = p$ y L/E es radical ciclotómica. Observe que $\sigma(\lambda^M_{P^{2p-1}}) = \lambda^M_{P^{2p-1}} + \lambda^M_{P^{2p-3}} = \lambda_{P^{2p-1}}$ si y sólo si el exponente de P en la descomposición de M es mayor o igual que $2p-3$. En este caso $\lambda_{P^{2p-1}}^{P^{2p-3}} = \lambda_{P^2} \in E$. Nótese que $\lambda_{P^3} \notin E$. Por lo tanto $\mu(E) = \Lambda_{P^2}$, y $\mu(L) = \Lambda_{P^{2p-1}}$.

Ahora, $N_{\mu(L)}(\lambda^M_{P^{2p-1}}) = \lambda_{P^{2p-1}}^{M(\frac{(1+P^2)^p-1}{(1+P^2)-1})} = \lambda^{MP^{2p-2}}_{P^{2p-1}} = \lambda^M_P = 0$ si y sólo si P divide a M. Así $\ker N_{\mu(L)} = (\lambda^P_{P^{2p-1}}) = \Lambda_{P^{2p-2}}$. Por otro lado

$$I_G(\mu(L)) = (\sigma(\lambda_{P^{2p-1}}) - \lambda_{P^{2p-1}}) = (\lambda_{P^{2p-3}}) = \Lambda_{P^{2p-3}}.$$

Por lo tanto

$$|\,\mathrm{cog}(L/E)\,| = |\,H^1(G,\mu(L))\,|\,\frac{|\,\mu(L)\,|}{|\,\mu(E)\,|} = \frac{|\,\Lambda_{P^{2p-2}}\,|}{|\,\Lambda_{P^{2p-3}}\,|}\frac{|\,\Lambda_{P^{2p-1}}\,|}{|\,\Lambda_{P^2}\,|} = q^{d(2p-2)},$$

donde $d = \deg(P)$. Por lo que $[L:E]^{s\deg\mu(L)} = q^{d(2p-1)}$ y $|\mathrm{cog}(L/E)| \neq [L:E]^{s\deg(\mu(L))}$.

Perspectivas y conclusiones

Los conceptos de ser *radical* y *pura*, definidos en las extensiones L/K utilizando la acción de Carlitz-Hayes, dan lugar a las llamadas extensiones *radical ciclotómicas*, objeto de estudio de la primera parte de la tesis. Estas tiene propiedades análogas a las que tienen las llamadas extensiones *cogalois*. Por ejemplo

(1) La extensión $k(\Lambda_{P^n})/k(\Lambda_P)$, donde $P \in R_T$ es irreducible, es radical ciclotómica, ejemplo 2.5. En analogía a que la extensión $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_p)$, con p un primo impar, es cogalois.

(2) El teorema 2.23 es análogo al teorema 7 de [2].

(3) El corolario 2.25 es análogo al corolario 8 de [2].

Por otro lado las extensiones radical ciclotómicas L/K cumplen que $[L : K] = p^s$, donde $p = \mathrm{char}(k)$, ver teorema 2.40. Sin embargo, aunque las extensiones cogalois L'/K' cumplen la siguiente propiedad: si K'' es cualquier campo intermedio de L'/K' entonces L'/K'' y K''/K' son extensiones cogalois, las extensiones radical ciclotómicas no cumplen la propiedad anterior, ver ejemplo 2.20.

Así pues las extensiones radical ciclotómicas no son análogas a las extensiones cogalois. Sin embargo todavía queda trabajo por hacer, por ejemplo

(1) Describir el módulo $\mathrm{cog}(k(\Lambda_{P^n})/k(\Lambda_P))$ con $P \in R_T$ irreducible.

(2) Encontrar soluciones *explícitas* de ecuaciones de la forma $X^M - a = 0$, donde $M \in R_T$ y $a \in \overline{k}$.

En la segunda parte de la tesis se pudo establecer un análogo parcial al siguiente teorema de Kummer (ver el teorema 5.17 de [26]).

TEOREMA 2.59. *Sea K un campo que contiene al grupo μ_n de las raíces n-ésimas de la unidad, con n primo relativo a la característica de K. Entonces:*

(1) Si L/K es una extensión de Kummer de exponente n, entonces L/K es normal (Galois, no necesariamente finita) y $Gal(L/K)$ es abeliano de exponente n.

(2) Reciprocamente, si L/K es una extensión abeliana de exponente n, entonces $L = K(\sqrt[n]{\Delta})$ con $\Delta = L^{*n} \cap K^*$, es decir L/K es una extensión de Kummer de exponente n.

Para ello seguimos algunas definiciones dadas en [18]: Sean $M \in R_T$ un polinomio no constante y $\varphi : K \to K$ definido por $\varphi(u) = u^M$, donde $K = k(\Lambda_M)$. Entonces φ es un R_T-homomorfismo. Por otra parte considere un R_T-submódulo B de K bajo la acción de Carlitz-Hayes que contenga a $K^M = \varphi(K)$.

Denotamos por K_B la composición de todos los campos $K(\sqrt[M]{a})$ con $a \in B$. Esto último quiere decir que adjuntamos a K una raíz arbitraria α de la ecuación $z^M - a = 0$, donde $\alpha \in \overline{k}$. Puesto que las M-raíces de Carlitz están en K, tal campo no depende de la elección de la raíz α, y por lo tanto K_B es de Galois sobre K.

DEFINICIÓN 2.60. Diremos que una extensión de Galois L/K, con grupo G, es una extensión *R_T-abeliana* si G tiene estructura de R_T-módulo. Una extensión R_T-abeliana L/K se dice que tiene *exponente* $M \in R_T$ si $M \cdot \sigma = 1$ para cada $\sigma \in G$, (ver [6]).

Es posible probar la siguiente proposición.

PROPOSICIÓN 2.61. *(1) Sea B un R_T-módulo de K, que contiene a K^M y sea K_B la composición de todos los campos $K(\sqrt[M]{a})$, para cada $a \in B$. Entonces K_B/K es Galois y abeliana.*

(2) Supongamos que K_B/K es una extensión R_T-abeliana y de exponente M. Entonces existe una función bilineal:

$$G \times B \to \Lambda_M \text{ dada por } (\sigma, a) \mapsto < \sigma, a >$$

donde $< \sigma, a >= \sigma(\alpha) - \alpha$ y α satisface $\alpha^M = a$. El núcleo izquierdo es 1 y el núcleo derecho es K^M.

(3) Con las hipótesis del inciso (2), la extensión K_B/K es finita si y sólo si $(B : K^M)$ es finito. Si esto ocurre, entonces

$$B/K^M \cong \widehat{G}.$$

En particular se tiene que

$$[K_B : K] = (B : K^M).$$

Aquí el símbolo $\widehat{G}$ denota el módulo dual de G (ver definición 1.21).

Para mostrar la proposición siguiente se necesitaron algunas definiciones. Recordamos que las extensiones de campos L/K están contenidas en la extensión $\overline{k}/k$ (ver [6]).

DEFINICIÓN 2.62. Una extensión R_T-abeliana L/K se dice que es *R_T-cíclica* si $\mathrm{Gal}(L/K)$ es un R_T-módulo cíclico. En este caso si

$$\mathrm{Gal}(L/K) \cong R_T/(M)$$

con M un polinomio mónico, diremos que L/K es una *extensión cíclica de orden M*.

El análogo al teorema 2.59 es la siguiente proposición:

PROPOSICIÓN 2.63. *Con las notaciones de la Proposición 2.61, la función θ definida por $\theta(B) = K_B$ entre el conjunto de R_T-submódulos de K que contienen a K^M y las extensiones R_T-abelianas de K, con exponente M, es inyectiva. Además si L/K es una extensión R_T-abeliana, finita, de exponente M entonces existe un R_T-submódulo B, de K, que contiene a K^M, tal que $L = K_B$.*

Demostración. Para mostrar la inyectividad de la función anterior bastara probar que si $K_{B_1} \subseteq K_{B_2}$, entonces $B_1 \subseteq B_2$. Sea $b \in B_1$. Se tiene que $K(b^{\frac{1}{M}}) \subseteq K_{B_2}$ por lo que $K(b^{\frac{1}{M}})$ esta contenido en una subextensión finitamente generada de K_{B_2}, es decir, existen un número finito de $b_i \in B_2$ de modo que $K(b^{\frac{1}{M}}) \subseteq K(b_1, \ldots, b_m)$. Así podemos suponer que B_2/K^M es finitamente generada y, por ser radical, finito.

Sea B_3 el submódulo de L generado por B_2 y b. Entonces probaremos que $K_{B_2} = K_{B_3}$. Tenemos que $K_{B_2} \subseteq K_{B_3}$. Para mostrar la otra contención, sea α una raíz M-ésima de $c \in B_3$. Si $c \in B_2$, entonces $K(\alpha) \subseteq K_{B_2}$. Si c es de la forma $b^N + \sum b_i^{N_i}$, con $b_i \in B_2$, entonces $\alpha^M = b^N + \sum b_i^{N_i} = \beta^{MN} + \sum \beta_i^{MN_i}$, es decir, $\alpha - \beta^N - \sum \beta_i^{N_i} = \lambda^A$. Por lo que $K(\alpha) \subseteq L_{B_2}$. De aquí se sigue la contención deseada.

Por lo tanto $(B_2 : K^M) = (B_3 : K^M)$, de esta manera $b \in B_2$, por lo que $B_1 \subseteq B_2$.

Por otro lado, sea K' una extensión R_T-abeliana de K de exponente M, finita. Sea G el grupo de Galois de tal extensión. Entonces, por [14] p. 187, G es suma directa finita de R_T-submódulos de exponente M. Aplicando Teoría de Galois podemos suponer que la anterior extensión es cíclica de exponente M. Ahora por la Proposición 2.6 de [6], toda extensión cíclica, con exponente M, se obtiene adjuntando una M-raíz de un elemento de K. Así K' es la adjunción de M-raíces, es decir, existen $\{b_j\} \subseteq K$ y $\{\alpha_j\} \subseteq K'$ tales que $\alpha_j^M = b_j$ y $K' = K(\{\alpha_j\})$. Sea B el submódulo de K generado por los b_j y K^M. Entonces $K' \subseteq K_B$. Por otro lado considere una raíz M-ésima

de $b + a^M$, digamos α. Así $\alpha^M = b + a^M$. Se observa que $(\alpha - a)^M = b$ y que $K(\alpha) \subseteq K(\alpha - a) \subseteq K'$, de esto se sigue que $K_B \subseteq K'$. Esto termina la demostración. □

Sin embargo también en esta parte queda trabajo por hacer, por ejemplo

(1) ¿Es posible que en la proposición 2.63 la función θ sea biyectiva, no solo inyectiva.?

Bibliografía

[1] T. Albu, *Cogalois theory*, Marcel Dekker Series, New York, 2003.

[2] F. Barrera-Mora, M. Rzedowski-Calderon, and G. Villa-Salvador, "On cogalois extensions", *J. Pure Appl. Algebra.* **76** (1991), 1-11.

[3] F. Barrera-Mora, W Yslas-Velez, "Some results on radical extensions", *J. of Algebra.* **162** (1993), 295-301.

[4] L. Carlitz, "On certain functions connected with polynomials in a Galois field", *Duke Math. J.* **1** (1935), 137-168.

[5] L. Carlitz, "A class of polynomials", *Trans. Amer. Math. Soc.* **43** (1938), 167-182.

[6] W. Chi, A. Li, "Kummer theory of division", *J. Pure Appl. Algebra.* **156** (2001), no. 2-3, 171-185.

[7] K. Conrad, "Carlitz Extensions", *www.math.uconn.edu/ kconrad/.*

[8] D. Goss, *Basic structures of function field arithmetic*, Springer Verlag, Berlin Heidelberg, 1996.

[9] G. Gras. *Class field theory*, Springer Verlag, Berlin Heidelberg, 2003.

[10] C. Greither and D.K. Harrison, "A Galois correspondence for radical extensions of fields", *1. Pure Appl. Algebra.* **43** (1986), 257-270.

[11] M. Hall, Jr. *Teoría de los grupos*, F. Trillas, México, 1969.

[12] F. Halter-Koch, "Über Radikalerweiterungen", *Acta Arithmetica.* **36** (1980), 43-58.

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

[14] P. Hilton, Y. Wu. *Curso de álgebra moderna*, Reverte, Barcelona, 1982.

[15] Hsu, Chih-Nung, "On Artin conjecture for the Carlitz module", *Compositio Mathematica.* **106** (1997), 247-266.

[16] Ireland, K; Rosen M, *A Classical Introduction to Modern Number Theory*, Springer Verlag New York, 1990.

[17] P. Lam-Estrada and G. D. Villa-Salvador, "Some remarks on the theory of cyclotomic function fields", *Rocky Mountain Journal of Mathematics.* **31** (2001), 2, 483-502.

[18] S. Lang, *Algebra 3rd ed*, Addison-Wesley. Co, Reading, Mass, 1993.

[19] J. S. Milne, "Class Field Theory", *www.jmilne.org/math/.*

[20] J. S. Milne, "Fields and Galois theory", v4.00 (19 de febrero 2005), www.jmilne.org/math/.

[21] D. Marcus, *Number fields*, Springer-Verlag, New York, 1977.

[22] M. Sánchez-Mirafuentes and G. Villa-Salvador, "Radical extensions for the Carlitz module", *Journal of Algebra*, **398** (2014), 284-302.

[23] F. Schultheis, "Carlitz-Kummer Function Fields", *Journal of number theory.* **36** (1990), 133-144.

[24] W. Y. Velez, "On normal binomials", *Acta Arithmetica.* **36** (1980), 113-124.

[25] G. D. Villa Salvador, *Topics in the Theory of Algebraic Function Fields*, Birkhäuser, Boston, 2006.

[26] F. Zaldivar, *Cohomología de galois de campos locales*, Sociedad Matemática Mexicana, México, 2001.

Índice alfabético