Universitat Autònoma de Barcelona

Facultat de Ciències

EXTENSIONS CICLOTÒMIQUES SOBRE COSSOS DE FUNCIONS: EL GÈNERE DEL MÒDUL DE CARLITZ

Treball de Fi de Grau

Niels Knudsen Esquerda

Juny 2022

Índex

1 Introducció

En la Teoria de Nombres clàssica anomenem extensions ciclotòmiques aquelles extensions dels nombres racionals $\mathbb{Q}$ que consisteixen en afegir una arrel n-èssima primitiva de la unitat ξ_n. Aquestes extensions són de Galois i el grup de Galois és abelià. A més, pel Teorema de Kronecker-Weber, tota extensió de Galois abeliana sobre $\mathbb{Q}$ està continguda en alguna extensió ciclotòmica.

Leonard Carlitz va construir als anys 1930 un anàleg per les extensions ciclotòmiques pel cos de funcions racionals $K = \mathbb{F}_q(t)$ sobre el cos finit $\mathbb{F}_q$ [Car38][Car35]. Aquesta construcció es coneix amb el nom de Mòdul de Carlitz i es pot trobar a la secció 7. L'objectiu del treball és estudiar l'extensió $K(n)$ que correspon a afegir els punts n-torsió del mòdul al cos K, i que és la que comparteix moltes similituds amb les extensions ciclotòmiques sobre $\mathbb{Q}$ (veure Teorema 10).

L'objectiu del treball és trobar el gènere de l'extensió $K(n)$. Aquí el que estem fent és identificar l'extensió $K(n)$ amb una corba algebraica tal i com s'explica en el capítol 5. Aleshores el gènere, que és una propietat geomètrica, es pot trobar gràcies a les eines algebraiques com són la ramificació, la diferent o altres conceptes de geometria algebraica. Més concretament, gràcies a la Fórmula de Riemann-Hurwitz donem al capítol 8 una fórmula pel gènere de $K(n)$ tal i com la va donar Alice Keller [Kel01] l'any 1999. Observem que en el cas de les extensions ciclotòmiques sobre $\mathbb{Q}$ no podem parlar de gènere ja que per poder-ho fer necessitem una variable lliure, o el que és el mateix, un element transcendent sobre el cos base.

Per últim, hem volgut investigar el Mòdul de Carlitz Twistat tal i com el va presentar Gekeler en [Gek16]. S'ha inclòs un apèndix 8.3 on es recopilen els resultats que hem obtingut per aquest cas, tot i que encara són incomplets pel cas general.

2 Conceptes bàsics

Sigui p un nombre primer, n un nombre natural i $q = p^n$. Denotem per $\mathbb{F}_q$ el cos finit de q elements. Aquest cos té característica p i és perfecte. Sigui K una extensió transcendent pura sobre $\mathbb{F}_q$ de grau de transcendència 1, és a dir, $K = \mathbb{F}_q(t)$ amb t transcendent sobre $\mathbb{F}_q$. Aleshores anomenem K el *cos de funcions racionals* sobre $\mathbb{F}_q$. Una extensió finita L de K es diu que és un *cos de funcions algebraiques* sobre $\mathbb{F}_q$ en la variable t.

Definició 1 (Anell de valoració discreta)**.** *Diem que un anell A és un anell de valoració discreta si és un domini d'ideals principals (DIP) amb un únic ideal primer no trivial.* $\mathfrak{p}$.

De la definició anterior es dedueix que en un anell de valoració discreta només existeix un únic element irreductible π que s'anomena l'*uniformitzador* de A. Per tant els ideals no nuls de A són de la forma $\mathfrak{p}(A) = \pi^n A$ i per tant per qualsevol $x \in A$ no nul el podem escriure com $x = \pi^n u$, on u és un invertible. L'enter n s'anomena l'ordre de x i es denota per $v(x)$. Ara podem estendre la definició anterior al cos de fraccions de A, que anomenarem Frac(A):

Definició 2. *L'aplicació $v : Frac(A)^* \to \mathbb{Z}$ rep el nom de valoració discreta. El coneixement de v determina l'anell A: és el conjunt de $x \in Frac(A)^*$ tals que $v(x) \geq 0$. Anàlogament, l'únic ideal primer $\mathfrak{p}$ de A és el conjunt de $x \in Frac(A)$ tals que $v(x) > 0$. A s'anomena l'anell de valoració discreta associat a la valoració v i al cos $K = Frac(A)$.*

Les valoracions discretes no trivials sobre K (resp. L) que són trivials sobre $\mathbb{F}_q$ (i.e. $v|_{\mathbb{F}_q} = 0$) formen classes d'equivalència, on podem escollir les valoracions normalitzades com a representants de cada classe. Dues valoracions v_1, v_2 són equivalents si $v_1 = c \cdot v_2$ per algun nombre real positiu c. Una classe de valoracions s'anomena una *plaça de K* (resp. L). El conjunt de totes les places de K (resp. L) es denotarà per $S(K)$ (resp. $S(L)$). Un element de $S(K)$ (resp. $S(L)$) es denotarà per $\mathfrak{p}$ (resp. $\mathfrak{P}$ i la corresponent valoració discreta normalitzada per $v_\mathfrak{p}$ (resp. $v_\mathfrak{P}$).
Cada valoració $v_\mathfrak{p}$ sobre K i $v_\mathfrak{P}$ sobre L se li associa de manera única els anells de valoració $o_{(\mathfrak{p})} \subset K$ i $\mathcal{O}_{(\mathfrak{P})} \subset L$. L'anell $o_{(\mathfrak{p})}$ conté l'ideal maximal

$$\mathfrak{p} := \{x \in K | v_\mathfrak{p}(x) > 0\}$$

i de la mateixa manera l'anell $\mathcal{O}_{(\mathfrak{P})}$ conté l'ideal maximal

$$\mathfrak{P} := \{x \in L | v_\mathfrak{P}(x) > 0\}$$

El cos $o_{(\mathfrak{p})}/\mathfrak{p}$ és el *cos residual* de K sota la valoració $v_\mathfrak{p}$ i $\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P}$ l'anàleg sobre L.

Abans de continuar donarem també la definició de *domini de Dedekind* ja que apareixerà diverses vegades al llarg del treball.

Definició 3. *Un domini de Dedekind és*

1. *Un domini d'integritat on tots els ideals propis no nuls factoritzen com a producte d'ideals primers (i per tant de forma única llevat d'ordre).*

   Observació 1. *La definició anterior és equivalent a la que donem a continuació:*

2. *Un domini d'integritat, noetherià, de dimensió de Krull 1 íntegrament tancat al seu cos de fraccions.*

Per una caracterització més detallada dels Dominis de Dedekind vegeu [Lor96]. Denotem per $\mathfrak{P}$ tant l'ideal maximal d'un anell de valoració discreta com les places i els divisors primers ja que existeix una correspondència bijectiva entre ells (veure [Lor96]).

2.1 El grup de divisors

Definició 4 (Grup de divisors)**.** *El grup de divisors d'un cos de funcions algebraiques L sobre $\mathbb{F}_q$ es defineix com el grup abelià lliure:*

$$Div(L) := \left\{ \sum_{\mathfrak{P} \in S(L)} n_{\mathfrak{P}} \mathfrak{P} : n_{\mathfrak{P}} \in \mathbb{Z} \text{ i } n_{\mathfrak{P}} = 0 \text{ per quasi tot } \mathfrak{P} \right\}$$

Els elements del grup s'anomenen divisors. Un divisor $\mathfrak{D}$ es diu primer exactament quan és de la forma

$$\mathfrak{D} = \mathfrak{P} \text{ per un } \mathfrak{P} \in S(L)$$

Per a un divisor $\mathfrak{D} = \sum_{\mathfrak{P} \in S(L)} n_{\mathfrak{P}} \mathfrak{P}$ tenim $v_{\mathfrak{P}}(\mathfrak{D}) := n_{\mathfrak{P}}$ per tot $\mathfrak{P} \in S(L)$. A cada element $\alpha \in L^*$ se li assigna el seu divisor principal

$$div(\alpha) := \sum_{\mathfrak{P} \in S(L)} v_{\mathfrak{P}}(\alpha) \mathfrak{P}$$

Es diu que un divisor $\mathfrak{A} \in S(L)$ divideix un altre divisor $\mathfrak{B} \in S(L)$ quan

$$\mathfrak{A} = \sum_{\mathfrak{P} \in S(L)} a_{\mathfrak{P}} \mathfrak{P} \quad i \quad \mathfrak{B} = \sum_{\mathfrak{P} \in S(L)} b_{\mathfrak{P}} \mathfrak{P}$$

i es compleix $a_{\mathfrak{P}} \leq b_{\mathfrak{P}}$.

Exemple 1. *Considerem per al nostre cas una funció racional $f \in \mathbb{F}_q(t)$. L'ideal generat per f es pot escriure com*

$$(f) = \frac{\prod \mathfrak{p}^{n_i}}{\prod \mathfrak{q}^{m_i}}$$

on $\mathfrak{p}_i, \mathfrak{q}_i$ *són polinomis irreductibles de* $\mathbb{F}_q[t]$*. Aleshores*

$$div(f) = \sum n_i \mathfrak{p}_\mathfrak{i} - \sum m_i \mathfrak{q}_i$$

i per tant veiem que els divisors del cos $\mathbb{F}_q(t)$ *ens donen una manera de controlar on tenim els zeros i els pols d'una funció racional i els* n_i, m_i *són els ordres dels zeros o els pols.*

Definició 5. *Sigui* $\mathfrak{P} \in S(L)$ *un divisor primer amb la propietat* $o_{(\mathfrak{p})} \subset \mathcal{O}_{(\mathfrak{P})}$*. Aleshores es diu que* $\mathfrak{P}$ *està sobre* $\mathfrak{p}$ *o que* $\mathfrak{P}$ *divideix* $\mathfrak{p}$ *i s'escriu* $\mathfrak{P}|\mathfrak{p}$*. La valoració* $v_\mathfrak{P}$ *de* L *es defineix com l'extensió de la valoració* $v_\mathfrak{p}$*.*
El nombre $e_\mathfrak{P}(L/K)$ *definit per*

$$e_\mathfrak{P}(L/K)(v_\mathfrak{p}(x)) = v_\mathfrak{P}(x) \ , \ x \in K$$

és l'índex de ramificació de $\mathfrak{P}$ *a* L/K*. També definim l'índex d'inèrcia de* $\mathfrak{P}$ *a* L/K *com*

$$f_\mathfrak{P}(L/K) = [\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P} : o_{(\mathfrak{p})}/\mathfrak{p}]$$

(i) Si $e_\mathfrak{P}(L/K) = f_\mathfrak{P}(L/K) = 1$ *per tot* $\mathfrak{P}|\mathfrak{p}$ *es diu que l'extensió és completament* split *en* $\mathfrak{p}$ *o que descomposa totalment en* $\mathfrak{P}$*.*

(ii) Si $f_\mathfrak{P}(L/K) > 1$ *es diu que l'extensió és inerta en* $\mathfrak{P}$*.*

(iii) Si $e_\mathfrak{P}(L/K) = 1$ *es diu que l'extensió és no ramificada en* $\mathfrak{P}$*.*

(iv) Si $f_\mathfrak{P}(L/K) = 1$ *es diu que l'extensió és totalment ramificada en* $\mathfrak{P}$*.*

Teorema 1. *Es compleix:*

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P}(L/K) f_\mathfrak{P}(L/K)$$

La demostració d'aquest teorema es pot trobar a [Lor96, Sec. III.8]. La ramificació serà el principal objecte d'estudi en aquest treball. Ara, seguint de les definicions d'anells de valoració discreta tenia sentit definir l'índex d'aquesta manera. Tanmateix, és equivalent a donar la següent definició, sense utilitzar la teoria d'anells locals:

Definició 6. *Un ideal primer* $\mathfrak{p}$ *d'un domini* A *ramifica a* $K/Frac(A)$*, on* K *és una extensió separable de* $Frac(A)$*, si es compleix la següent igualtat a* B*, la clausura entera de* A

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}$$

on $\mathfrak{P}_i$ *són ideals primers de* B *i* ***almenys un dels*** e_i ***és més gran que 1****.*

2.2 Extensions de cossos i completacions

Per a cada plaça $\mathfrak{p} \in S(K)$ existeix una completació del cos K respecte la valoració discreta $v_\mathfrak{p}$. Tota valoració indueix un valor absolut (no arquimedià) a través de $|a| := c^{-v_\mathfrak{p}(a)}$ on c és una constant positiva $c > 1$. Així podem parlar de mètrica que alhora ens dóna una estructura d'espai topològic i podem definir-hi les successions de Cauchy de la manera usual. D'aquí surt el concepte de completació que consisteix en agafar l'anell de les successions de Cauchy i identificar totes les successions amb el mateix límit completant d'aquesta manera el cos K. Si denotem per $K_\mathfrak{p}$ la completació de K és clar que K s'injecta a $K_\mathfrak{p}$ a través de $a \mapsto (a, a, \dots)$ i $v_\mathfrak{p}$ s'estén de manera única a $K_\mathfrak{p}$.

Si denotem per $o_\mathfrak{p}$ l'anell de valoracions i per π un element uniformitzador de $o_\mathfrak{p}$ podem descriure $o_\mathfrak{p}$ a partir del límit projectiu

$$o_\mathfrak{p} = \varprojlim o_\mathfrak{p}/\pi^n o_\mathfrak{p}$$

i els elements de $x \in K_\mathfrak{p}$ són de la forma

$$x = \sum_{i=n}^{\infty} a_i \pi^i, \qquad a_i \in \mathbb{F}_{q^m}, m = [o_\mathfrak{p}/\mathfrak{p} : \mathbb{F}_q], n \in \mathbb{Z}$$

i per tant $K_\mathfrak{p} = \mathbb{F}_{q^m}((\pi))$. [MF 69, Cap. 10][Ser79, Sec. II.4]

Les nocions que acabem de presentar s'estenen exactament igual a L/K i les denotarem anàlogament $L_\mathfrak{P}, \mathcal{O}_\mathfrak{P}$. Sigui ara L/K una extensió separable de cossos de grau n i $r_\mathfrak{p}(L/K)$ el nombre de places diferents sobre de $\mathfrak{p} \in S(K)$. Les denotem per $\mathfrak{P}_i, i = 1, 2, \dots, r_\mathfrak{p}(L/K)$ i els associem els seus respectius índexs de ramificació e_i i d'inèrcia f_i. Aleshores les completacions $L_{\mathfrak{P}_i}$ compleixen

(i) $L_{\mathfrak{P}_i}$ és una extensió de $K_\mathfrak{p}$ de grau $n_i = e_i f_i$.

(ii) La valoració $v_{\mathfrak{P}_i}$ és l'única extensió de $v_\mathfrak{p}$ a $L_{\mathfrak{P}_i}$ i a més

$$e_i = e_{\mathfrak{P}_i}(L_{\mathfrak{P}_i}/K_\mathfrak{p}) = e_{\mathfrak{P}_i}(L/K)$$
$$f_i = f_{\mathfrak{P}_i}(L_{\mathfrak{P}_i}/K_\mathfrak{p}) = f_{\mathfrak{P}_i}(L/K)$$

(iii) El morfisme canònic

$$\phi : L \otimes_K K_\mathfrak{p} \longrightarrow \prod_{i=1}^{r_\mathfrak{p}(L/K)} L_{\mathfrak{P}_i}$$

és un isomorfisme. [Ser79, Sec. II.3]

2.2.1 La Diferent

Sigui L/K una extensió finita separable, i sigui $\mathfrak{p}$ (resp. $\mathfrak{P}$) una plaça de K (resp. L) complint $\mathfrak{P}|\mathfrak{p}$ i $K_\mathfrak{p}$ (resp. $L_\mathfrak{P}$) les corresponents completacions. Considerant $L_\mathfrak{P}$ com un $K_\mathfrak{p}$-espai vectorial, es pot definir l'aplicació

$$T(x,y) = Tr_{K_\mathfrak{p}}^{L_\mathfrak{P}}(xy)$$

que és bilineal i no degenarada [Ser79, Sec. III.3]. Gràcies a aquesta aplicació, podem assignar a cada ideal $\mathfrak{a}$ de $L_\mathfrak{P}$ l'ideal associat

$$\hat{\mathfrak{a}} = \{x \in L_\mathfrak{P} : Tr_{K_\mathfrak{p}}^{L_\mathfrak{P}}(x\mathfrak{a}) \subset o_\mathfrak{p}\}$$

La diferent de $L_\mathfrak{P}/K_\mathfrak{p}$ es defineix com l'invers de l'ideal associat

$$\hat{\mathcal{O}_\mathfrak{P}} = \{x \in L_\mathfrak{P} : Tr_{K_\mathfrak{p}}^{L_\mathfrak{P}}(x\mathcal{O}_\mathfrak{P}) \subset o_\mathfrak{p}\}$$

Escriurem $\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Definició 7. *L'ideal $\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$ s'anomena la diferent local de L/K respecte $\mathfrak{P}$. La diferent $\mathcal{D}_{L/K}$ de L/K es pot expressar com el divisor:*

$$\mathcal{D}_{L/K} := \sum_{\mathfrak{P} \in S(L)} v_\mathfrak{P}(\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}})\mathfrak{P}$$

Propietats de la diferent

(i) Un divisor primer $\mathfrak{P}$ de L ramifica sobre K exactament quan $v_\mathfrak{P}(\mathcal{D}_{L/K}) \geq 1$.

(ii) Si π és un uniformitzador de l'extensió local $L_\mathfrak{P}/K_\mathfrak{p}$, aleshores π satisfà el polinomi d'Eisenstein

$$f_\pi(\pi) = \pi^e + \alpha_1\pi^{e-1} + \cdots + \alpha_e = 0$$

amb $e = e_\mathfrak{P}(L/K)$, i per la diferent local es compleix

$$\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}} = (f'_\pi(\pi))$$

(iii) Per un divisor $\mathfrak{P}$ amb índex de ramificació e es compleix

$$v_\mathfrak{P}(\mathcal{D}_{L/K}) = e-1, \quad \text{si } \mathfrak{P} \text{ és dòcilment ramificat, és a dir, } p \nmid e$$
$$v_\mathfrak{P}(\mathcal{D}_{L/K}) > e-1, \quad \text{si } \mathfrak{P} \text{ és salvatgement ramificat, és a dir, } p|e$$

2.2.2 Extensions de Galois

Si l'extensió L/K és finita i de Galois sabem que el grup de Galois $\mathrm{Gal}(L/K)$ actua transitivament sobre el conjunt de totes les places diferents que estan sobre una plaça $\mathfrak{p}$ de K. A més, els índexs de ramificació i els graus residuals depenen només de $\mathfrak{p}$ i escriurem $e_{\mathfrak{p}}(L/K)$ i $f_{\mathfrak{p}}(L/K)$ respectivament.

Si $r_{\mathfrak{p}}(L/K)$ és el nombre de places que divideixen $\mathfrak{p}$ (i.e. les places que estan a sobre) llavors podem descriure el Teorema 1 com

$$[L:K] = r_{\mathfrak{p}}(L/K) \cdot e_{\mathfrak{p}}(L/K) \cdot f_{\mathfrak{p}}(L/K)$$

Sigui $\mathfrak{P} \in S(L)$ tal que $\mathfrak{P}|\mathfrak{p}$. Definim

$$Z_{\mathfrak{P}}(L/K) = \{\sigma \in G(L/K) | \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

Es pot comprovar que és un subgrup del grup de Galois $\mathrm{Gal}(L/K)$, anomenat el grup de descomposició de $\mathfrak{P}$ a L/K. També definim el grup d'inèrcia $T_{\mathfrak{P}}(L/K)$ com el nucli de l'aplicació

$$\begin{aligned} Z_{\mathfrak{P}}(L/K) &\longrightarrow G(\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P}/o_{(\mathfrak{p})}/\mathfrak{p}) \\ \sigma &\longmapsto \overline{\sigma} \qquad\qquad \text{amb } \overline{\sigma}(x+\mathfrak{P}) = \sigma(x) + \mathfrak{P} \end{aligned}$$

Per simplificar la notació posem

$$\begin{aligned} Z(L/K) &:= Z_{\mathfrak{P}}(L/K) \qquad T(L/K) := T_{\mathfrak{P}}(L/K) \\ e &:= e_{\mathfrak{p}}(L/K), \qquad f := f_{\mathfrak{p}}(L/K), \qquad r := r_{\mathfrak{p}}(L/K) \end{aligned}$$

Proposició 1. *[Ser79, Sec. I.7]*

(i) Si L^Z és el cos fix de $Z(L/K)$ a L/K, llavors es té

$$[L^Z : K] = r, \qquad [L : L^Z] = ef, \qquad G(L/L^Z) = Z$$

(ii) L'extensió de cossos residuals $\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P}/o_{(\mathfrak{p})}/\mathfrak{p}$ és separable i si L^T és el cos fix pel grup d'inèrcia $T(L/K)$ es compleix

$$[L : L^T] = e \quad \text{ i també } \quad [L^T : L^Z] = f$$

(iii) En el cas que l'extensió de cossos residuals sigui separable, la plaça $\mathfrak{p}$ esplita *completament a l'extensió L^Z/K i no ramifica a l'extensió L^T/K. Per últim totes les places que es troben sobre $\mathfrak{p}$ a L^T ramifiquen totalment a l'extensió L/L^T.*

Observació 2. *Si l'extensió de Galois L/K és abeliana, aleshores si $\mathfrak{P}, \mathfrak{P}'$ són dues places de L que es troben sobre $\mathfrak{p} \in S(K)$ tenim*

$$Z_{\mathfrak{P}}(L/K) = Z_{\mathfrak{P}'}(L/K) \qquad T_{\mathfrak{P}}(L/K) = T_{\mathfrak{P}'}(L/K)$$

ja que els grups de descomposició de les diferents places que divideixen $\mathfrak{p}$ són conjugats entre ells, és a dir, són iguals en el cas d'una extensió abeliana. Per tant en aquest cas escrivim:

$$Z_{\mathfrak{p}}(L/K) := Z_{\mathfrak{P}}(L/K) \qquad T_{\mathfrak{p}}(L/K) = T_{\mathfrak{P}}(L/K)$$

2.2.3 El principi Local-Global per a cossos

Considerem ara un extensió de cossos L/K, una valoració $v_{\mathfrak{p}}$ i la seva corresponent extensió $v_{\mathfrak{P}}$ amb $\mathfrak{P}|\mathfrak{p}$. Diem que un cos F és cos global si és una extensió finita de $\mathbb{Q}$ o de $\mathbb{F}_q(t)$ i diem que un cos $\mathcal{F}$ és local si és complet respecte una valoració discreta no trivial i té un cos residual finit. El principi local-global per a cosos consisteix en la transició de l'extensió "global" L/K cap a l'extensió "local" $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Aquí estem fent servir el fet que l'extensió canònica de la valoració $v_{\mathfrak{P}}$ de L a $L_{\mathfrak{P}}$ és l'única extensió de la valoració $v_{\mathfrak{p}}$ a $K_{\mathfrak{p}}$ a l'extensió $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. Finalment si L/K és de Galois, llavors $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ també és de Galois amb grup de Galois

$$G(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = Z_{\mathfrak{P}}(L/K)$$

2.2.4 Composició de cossos

Considerem una extensió de cossos separable L/K i tres cossos intermedis K', K_1, K_2 de manera que $K' \subset K_1$ i també $K' \subset K_2$. Sigui $\mathfrak{Q}$ una plaça de K_1K_2 i $\mathfrak{Q}', \mathfrak{Q}_1, \mathfrak{Q}_2$ les respectives places a sota de $\mathfrak{Q}$ a K', K_1 i K_2 respectivament. Llavors es compleix

$$(K_1K_2)_{\mathfrak{Q}} = K_{1,\mathfrak{Q}_1}K_{2,\mathfrak{Q}_2}$$

En particular d'aquest fet es dedueixen els següents resultats: [Neu99]

(i) Si $\mathfrak{Q}'$ *esplita* tant a K_1 i K_2 també ho fa a K_1K_2.

(ii) Tota plaça de K' que no ramifiqui ni a K_1 ni K_2 tampoc ramifica a K_1K_2.

(iii) Si K_1 i K_2 són linealment independents sobre K', $\mathfrak{Q}_1$ *esplita* a K_1 i $\mathfrak{Q}_2$ ramifica totalment a l'extensió K_2/K' aleshores totes les places de K_1 que es troben a sobre de $\mathfrak{Q}_1$ ramifiquen totalment a K_1K_2

3 El cos $\mathbb{F}_q(t)$

Fixem un element transcendent t sobre $\mathbb{F}_q$ i definim $K = \mathbb{F}_q(t)$. El cos de fraccions de l'anell $A = \mathbb{F}_q[t]$ correspon a $\mathbb{F}_q(t)$. Aquest cos és una representació del cos de funcions racionals sobre $\mathbb{F}_q$ i isomorf a qualsevol altra representació del cos de funcions racionals sobre el cos finit $\mathbb{F}_q$. Vegem ara com definim totes les valoracions sobre aquest cos:

(i) Sigui $P \in A$ un polinomi irreductible (mònic). Definim la valoració associada a l'ideal maximal $\mathfrak{p} := (P)$ com

$$\begin{aligned} v_{\mathfrak{p}} : \mathbb{F}_q(t)^* &\to \mathbb{Z} \\ x = \frac{P^n a}{P^m b} &\mapsto n - m \end{aligned}$$

on $n, m \in \mathbb{N} \cup \{0\}$, $a, b \in A \setminus \{0\}$, $\mathrm{mcd}_T(a, P) = \mathrm{mcd}_T(b, P) = 1$ i per definició

$$v_{\mathfrak{p}}(0) := \infty$$

Es dedueix a partir de la definició que

$$v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$$

i també

$$v_{\mathfrak{p}}(x + y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}, \quad \text{amb igualtat si } v_{\mathfrak{p}}(x) \neq v_{\mathfrak{p}}(y)$$

Sabem que A és un domini d'ideals principals i per tant també és un domini de Dedekind. Els ideals primers són generats pels polinomis irreductibles. La localització de A en $\mathfrak{p}$,

$$A_{(\mathfrak{p})} := \left\{ \frac{a}{b} \in \mathbb{F}_q(t) : a, b \in A, b \notin \mathfrak{p} \right\}$$

també és un domini d'ideals principals amb exactament un ideal maximal $\mathfrak{p}A_{(\mathfrak{p})}$, on $A_{(\mathfrak{p})}$ és també un anell de valoració discreta. En efecte,

$$\begin{aligned} \{x \in \mathbb{F}_q(t) | v_{\mathfrak{p}} \geq 0\} &= \left\{ \frac{a}{b} | a, b \in A, b \neq 0, v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(b) \right\} \\ &= \left\{ \frac{a}{b} | a, b \in A, b \notin \mathfrak{p} \right\} = A_{(\mathfrak{p})} \end{aligned}$$

També obtenim el cos residual sobre $\mathfrak{p}$

$$A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})} \cong A/\mathfrak{p} = \mathbb{F}_{q^{\mathrm{grau}(P)}}$$

(ii) També podem definir la valoració en la plaça de l'infinit

$$v_\infty : \mathbb{F}_q(t)^* \longrightarrow \mathbb{Z}, v_\infty(\frac{a}{b}) := \mathrm{grau}(b) - \mathrm{grau}(a)$$

on $a, b \in A \setminus \{0\}$, $\mathrm{mcd}_T(a, b) = 1$ i $v_\infty(0) := \infty$. D'aquesta manera tenim que

$$A_\infty := \left\{ \frac{a}{b} \in \mathbb{F}_q(t) : \mathrm{grau}(a) \leq \mathrm{grau}(b) \right\}$$

és l'anell de valoracions i el seu ideal maximal és

$$\mathfrak{m}_\infty = \left\{ \frac{a}{b} \in \mathbb{F}_q(t) : \mathrm{grau}(a) < \mathrm{grau}(b) \right\}$$

i en aquest cas el cos residual és

$$A_\infty/\mathfrak{m}_\infty \cong \mathbb{F}_q$$

El conjunt de totes les valoracions normalitzades del cos $\mathbb{F}_q(t)$ es troba en bijecció amb el conjunt [Lor96]

$$\{\mathfrak{p}|\mathfrak{p} \neq 0 \text{ ideal primer }, \mathfrak{p} \subset A\} \cup \{\infty\}$$

i també amb el conjunt de totes les places $S(\mathbb{F}_q(t))$, on adoptem el símbol $\mathfrak{p}$ per designar-ne els seus elements. Finalment, també es compleix ([Lor96, Sec. II.9])

$$A = \bigcap_{\mathfrak{p} \in S(\mathbb{F}_q(t)), \mathfrak{p} \neq \infty} A_{(\mathfrak{p})}$$

3.1 Completació a la plaça de l'infinit

De la mateixa manera que podem completar cossos en qualsevol plaça finita, també ho podem fer per la plaça de l'infinit a través de v_∞. Així obtenim

$$\mathbb{F}_q(T)_\infty = \mathbb{F}_q\left(\left(\frac{1}{T}\right)\right) = \left\{ f(T) = \sum_{i=-\infty}^{n} a_i T^i : n \in \mathbb{Z}, a_i \in \mathbb{F}_q \right\}$$

$\mathbb{F}_q(T)_\infty$ és un cos local, és a dir, és complet respecte d'una valoració discreta no trivial i té un cos residual finit. Denotem ara per C la completació de la clausura algebraica de $\mathbb{F}_q(T)_\infty$.

Teorema 2. *C és algebraicament tancat.*

3.2 Extensions finites de $\mathbb{F}_q(T)$

Considerem $L/\mathbb{F}_q(T)$ una extensió finita i separable. La clausura entera de l'anell $A = \mathbb{F}_q[T]$ a L, la qual denotem per $\mathcal{O}$ és un domini de Dedekind. En particular això vol dir que podem obtenir totes les places finites de L considerant els ideals maximals de $\mathcal{O}$. Pel que fa a les places infinites, són les places de L que es troben sobre la plaça de l'infinit, $(\frac{1}{T})$, de $\mathbb{F}_q(T)$. Un plaça finita $\mathfrak{P} \in S(L)$ divideix una altra plaça $\mathfrak{p} \in S(\mathbb{F}_q(T))$ exactament quan $\mathfrak{p}\mathcal{O} \subset \mathfrak{P}$.

Definició 8. *Sigui $\mathfrak{A} \subset \mathcal{O}$ un ideal de la forma*

$$\mathfrak{A} = \prod_{i=1}^{s} \mathfrak{P}_i$$

amb $s \in \mathbb{N}$ i $\mathfrak{P}_i$ ideals maximals de $\mathcal{O}$. Aleshores definim la norma de $\mathfrak{A}$ com

$$N_{\mathbb{F}_q(T)}^{L}(\mathfrak{A}) = \prod_{i=1}^{s} \mathfrak{p}_i^{f_{\mathfrak{p}_i}(L/\mathbb{F}_q(T))}$$

on $\mathfrak{p}_i = \mathfrak{P}_i \cap A$. *Fent servir la norma definim el discriminant* $D_{\mathcal{O}/A}$ *com el producte de les normes de les diferents locals* $\mathcal{D}_{L_{\mathfrak{P}}/\mathbb{F}_q(T)_{\mathfrak{p}}}$, *on* $\mathfrak{p} \in S(\mathbb{F}_q(T))$ *és una plaça finita:*

$$D_{\mathcal{O}/A} := N^L_{\mathbb{F}_q(T)} \left(\prod_{\substack{\mathfrak{P} \subset \mathcal{O} \\ \mathfrak{P} \text{ ideal maximal}}} \mathcal{D}_{L_{\mathfrak{P}}/\mathbb{F}_q(T)_{\mathfrak{p}}} \right)$$

4 Grups de ramificació superiors

En aquesta secció presentem les definicions i també un seguit de resultats que ens permeten calcular la diferent d'una extensió separable amb ramificació salvatge, cosa que necessitem més endavant a l'hora de calcular el gènere de corbes sobre un cos finit (veure secció 5). Aquests resultats són tots recopilats a [Ser79, Sec. IV.1]. A continuació presentem les definicions i hipòtesis que farem servir en aquest capítol.

Sigui $\mathcal{K}$ un cos complet respecte una valoració discreta $v_{\mathcal{K}}$. Denotem per $\mathcal{O}_{\mathcal{K}}$ el corresponent anell de valoracions, per $\mathfrak{p}_{\mathcal{K}}$ el seu únic ideal maximal i per $\kappa = \mathcal{O}_{\mathcal{K}}/\mathfrak{p}_{\mathcal{K}}$ el cos residual.

Sigui ara $\mathcal{L}/\mathcal{K}$ una extensió de Galois finita amb grup de Galois G i sigui $\mathcal{O}_{\mathcal{L}}$ la clausura entera de $\mathcal{O}_{\mathcal{K}}$ a $\mathcal{L}$. Així $\mathcal{O}_{\mathcal{L}}$ és també un anell de valoració discreta i definim anàlogament $v_{\mathcal{L}}, \mathfrak{p}_{\mathcal{L}}$ i λ. En tot el capítol suposarem que l'extensió residual λ/κ és separable.

Conseqüentment, $\mathcal{O}_{\mathcal{L}}$ admet una base sobre $\mathcal{O}_{\mathcal{K}}$ que consisteix de potències d'un sol element x.[Ser79, Sec. III.6]. Denotant com habitualment l'índex de ramificació i el d'inèrcia tenim

$$e_{\mathcal{L}/\mathcal{K}} f_{\mathcal{L}/\mathcal{K}} = [\mathcal{L} : \mathcal{K}]$$

Fixem ara $x \in \mathcal{O}_{\mathcal{L}}$ de manera que x és un generador de $\mathcal{O}_{\mathcal{L}}$ com a $\mathcal{O}_{\mathcal{K}}$-àlgebra.

Lema 1. *Sigui* $\sigma \in G$, $-1 \leq i \in \mathbb{Z}$. *Aleshores les tres condicions següents són equivalents:*

(i) σ *actua trivialment sobre l'anell quocient* $\mathcal{O}_{\mathcal{L}}/\mathfrak{p}^{i+1}$.

(ii) $v_{\mathcal{L}}(\sigma(a) - a) \geq i + 1$ *per tot* $a \in \mathcal{O}_{\mathcal{L}}$

(iii) $v_{\mathcal{L}}(\sigma(x) - x) \geq i + 1$.

Definició 9. *Per tot enter* $i \geq 1$ *definim* G_i *com el conjunt de* $\sigma \in G$ *tal que compleix algunes de les tres condicions equivalents del lema.* G_i *s'anomena l'*i***-èssim grup de ramificació*** *de* $\mathcal{L}/\mathcal{K}$.

Proposició 2. *Per a cada enter $i \geq -1$ els grups G_i formen una seqüència decreixent de subgrups normals de G. En particular $G_{-1} = G$, G_0 és el subgrup d'inèrcia de G i $G_i = \{1\}$ per i prou gran.*

Proposició 3. *Sigui $H \leq G$ un subgrup del grup de Galois i sigui $\mathcal{K}'$ el cos fix per H, $\mathcal{K} \subset \mathcal{K}' \subset \mathcal{L}$. Aleshores $H = G(\mathcal{L}/\mathcal{K}')$ i es compleix*

$$H_i = G_i \cap H$$

Corol·lari 1. *Sigui $\mathcal{K}_r$ la subextensió no ramificada més gran de $\mathcal{L}$ sobre $\mathcal{K}$, i H el corresponent subgrup de G. Aleshores H és igual al grup d'inèrcia G_0, i els grups de ramificació de G amb índex ≥ 0 són iguals als de H. A més, l'extensió $\mathcal{L}/\mathcal{K}_r$ és totalment ramificada.*

Proposició 4. *Si $H = G_j$ per algun enter $j \geq 0$, llavors $(G/H)_i = G_i/H$ per $i \leq j$ i $(G/H)_i = \{1\}$ per $i \geq j$.*

Amb aquestes proposicions ja estem en condicions de poder determinar la diferent d'una subextensió de $\mathcal{L}/\mathcal{K}$:

Proposició 5. *Si $\mathcal{D}_{\mathcal{L}/\mathcal{K}}$ és la diferent de $\mathcal{L}/\mathcal{K}$, aleshores*

$$v_{\mathcal{L}}(\mathcal{D}_{\mathcal{L}/\mathcal{K}}) = \sum_{i=0}^{\infty}(|G_i| - 1)$$

on $|G_i|$ és l'ordre (finit) del grup. Observem que la suma és finita ja que $|G_i| - 1 = 0$ per i prou gran.

4.1 Cas global

El Principi Local-Global per a cossos ofereix la possibilitat de traslladar els resultats vists a la secció anterior al cas global. Sigui K'/K una extensió finita de Galois amb grup de Galois G. Suposem en tota aquesta secció que tant K' com K són cossos globals. Sigui $\mathfrak{p}$ una plaça de K i $K_{\mathfrak{p}}$ la seva corresponent completació i de la mateixa manera $K'_{\mathfrak{P}}$ la completació de K' respecte $\mathfrak{P}$, on suposem $\mathfrak{P}|\mathfrak{p}$. Aleshores l'$i$-èssim grup de ramificació $G_i(\mathfrak{P})$ de G respecte a $\mathfrak{P}$ és justament l'i-èssim grup de ramificació de $\mathfrak{P}$ a l'extensió de cossos locals $K'_{\mathfrak{P}}/K_{\mathfrak{p}}$. És a dir:

$$G_i(\mathfrak{P}) := (G(K'_{\mathfrak{P}}/K_{\mathfrak{p}}))_i$$

Per qualsevol $\sigma \in G$ es compleix la relació

$$\sigma \in G_i(\mathfrak{P}) \iff \sigma(a) \equiv a \mod \mathfrak{P}^{i+1}, \forall a \in \mathcal{O}_{(\mathfrak{P})}$$

Si $\mathfrak{P}$ i $\mathfrak{A}$ són dues places de K' que es troben sobre $\mathfrak{p}$ aleshores tenim

$$|G_i(\mathfrak{P})| = |G_i(\mathfrak{A})|, \forall i \in \mathbb{Z}, i \geq -1$$

i com que el grup de Galois actua transitivament sobre les places que divideixen $\mathfrak{p}$, si $\tau \in G$ és tal que $\tau(\mathfrak{P}) = \mathfrak{A}$, llavors

$$\tau \circ \sigma \circ \tau^{-1} \in G_i(\mathfrak{A}), \forall \sigma \in G_i(\mathfrak{P})$$

Per tant, en el cas global escriurem $g_i(\mathfrak{p}) := |G_i(\mathfrak{P})|$ per a tota plaça $\mathfrak{P}$ que es trobi sobre $\mathfrak{p}$.

4.2 Propietats dels grups de ramificació

(i) El grup G_0/G_1 és cíclic i el seu ordre és coprimer amb la característica del cos residual λ.

(ii) El grup G_0 és resoluble. Si a més, κ és finit, aleshores G també és resoluble.

(iii) Si G és abelià i $i \in \mathbb{Z}$ no és divisble per $|G_0/G_1|$ llavors $G_i = G_{i+1}$

Per als enunciats que vénen ara $\text{char}(\lambda) = l \neq 0$.

(iv) Els quocients G_i/G_{i+1}, per tot $i \geq 1$ són abelians i són productes directes de grups cíclics d'ordre l. En particular el grup G_1 és un l-grup.

(v) El grup d'inèrcia és el producte semidirecte d'un grup cíclic d'ordre coprimer amb l amb un subgrup normal d'ordre l^r, per algun r.

(vi) Els enters $i \geq 1$ tals que $G_i \neq G_{i+1}$ són tots congruents $\mod l$.

4.3 La funció φ de Herbrand

Sigui $u \geq 1$ un nombre real i denotem per G_u el grup de ramificació G_i amb i el menor enter tal que $i \geq u$. Per tant

$$\sigma \in G_u \iff v_{\mathcal{L}}(\sigma(x) - x) \geq u + 1$$

Denotem també l'índex del subgrup H dins de G per $|G : H|$ i definim

$$\varphi_{\mathcal{L}/\mathcal{K}} : [-1, \infty) \longrightarrow \mathbb{R}, \qquad \varphi_{\mathcal{L}/\mathcal{K}}(u) = \int_0^u \frac{dt}{|G_0 : G_t|}$$

on per convenció si $t = -1$, llavors $|G_0 : G_t| = |G_{-1} : G_0|^{-1}$ i si $-1 < t \leq 0$ llavors $|G_0 : G_0|^{-1} = 1$. De fet, es pot donar una expressió explícita com una suma de la funció φ, si $m \leq u \leq m + 1$, on m és un enter positiu, aleshores

$$\varphi(u) = \frac{1}{g_0}(g_1 + \cdots + g_m + (u - m)g_{m+1}), \text{ amb } g_i = |G_i|$$

i en particular

$$\varphi(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i$$

Ara es pot veure que l'aplicació φ és un homeomorfisme de la semirecta $[-1, \infty)$ en ella mateixa i per tant denotem ψ l'aplicació inversa [Ser79, Sec. IV.3]. Aleshores

(i) La funció φ és contínua, lineal a trossos, creixent i còncava.

(ii) $\varphi(0) = 0$

(iii) La funció ψ és contínua, lineal a trossos, creixent i convexa.

(iv) $\psi(0) = 0$.

(v) Si $v = \varphi(u)$ és un enter aleshores $u = \psi(v)$ també és un enter.

(vi) En una torre d'extensions de Galois $\mathcal{K} \subset \mathcal{K}' \subset \mathcal{L}/$ es compleix

$$\varphi_{\mathcal{L}/\mathcal{K}} = \varphi_{\mathcal{K}'/\mathcal{K}} \circ \varphi_{\mathcal{L}/\mathcal{K}'} \text{ i també } \psi_{\mathcal{L}/\mathcal{K}} = \psi_{\mathcal{K}'/\mathcal{K}} \circ \psi_{\mathcal{L}/\mathcal{K}'}$$

Ara gràcies al quart punt de llista anterior podem definir una *numeració superior*. Posem

$$G^v = G_{\psi(v)}$$

o equivalentment

$$G^{\varphi(u)} = G_u$$

Així tenim $G^{-1} = G, G^0 = G_0$ i $G^v = \{1\}$ per v prou gran. Els tres resultats a continuació es poden trobar a [Ser79, Sec IV.3].

Proposició 6. *Sigui H un subgrup normal del grup de Galois $G = Gal(L/K)$, aleshores per tot v*

$$(G/H)^v = G^v H/H$$

Lema 2. *Sigui $\mathcal{K} \subset \mathcal{K}' \subset \mathcal{L}/$ el cos fix pel subgrup $H \leq G$ i $v = \phi(u)$ per algun $u \neq -1$. Aleshores*

$$G_u H/H = (G/H)_v$$

Teorema 3 (Hasse-Arf)**.** *Si G és un grup abelià, i v és un salt en la filtració*[1] *G^v aleshores v és un enter. Dit d'una altra manera, si $G_i \neq G_{i+1}$ aleshores $\varphi(i)$ és un enter.*

[1] Una filtració és una seqüència decreixent de subgrups normals de G

4.4 Exemple: Extensions ciclotòmiques sobre el cos $\mathbb{Q}_p$

Donem el nom d'extensió ciclotòmica a aquelles extensions de $\mathbb{Q}$ on afegim una arrel de la unitat. El seu estudi és fonamental en la teoria de nombres algebraica. Un clar exemple és el Teorema de Kronecker-Weber que afirma que tota extensió abeliana sobre $\mathbb{Q}$ està continguda en alguna extensió ciclotòmica.

Sigui doncs p un nombre primer, n un nombre natural i ξ_n una arreal n-èssima primitva de la unitat. Els cossos $\mathbb{Q}$ i $\mathbb{Q}(\xi_n)$ no són complets respecte la valoració p-àdica. Com hem mencionat ja, però, l'estratègia consisteix en inspeccionar el cas local. L'índex de ramificació de l'ideal primer (p) és independent de la tria de n. De fet es compleix que si $\gcd(n,p) = 1$ aleshores (p) no ramifica a $\mathbb{Q}_p(\xi_n)/\mathbb{Q}_p$. En aquest exemple ens centrarem en el cas $n = p^m$. Llavors l'extensió $\mathbb{Q}_p(\xi_n)/\mathbb{Q}_p$ té grau $\varphi(n) = p^{m-1}(p-1)$ i el grup de Galois és justament el grup d'invertibles de $\mathbb{Z}/n\mathbb{Z}$ (el denotem per $G(n)$) i (p) és completament *split*. L'element $1-\xi_n$ és un uniformitzador per $\mathbb{Q}_p(\xi_n)$. Finalment, els grups de ramificació superiors són

$$\begin{aligned} &G_0 = G; \\ &G_u = G(n)^1 && \text{si } 1 \leq u \leq p-1, \\ &G_u = G(n)^2 && \text{si } p \leq u \leq p^2-1, \\ &\quad\vdots && \quad\vdots \\ &G_u = G(n)^m = \{1\} && \text{si } p^{m-1} \leq u,, \end{aligned}$$

on $G(n)^i := \{x \in G(n) | x \equiv 1 \mod p^i\}$. Es pot veure que els salts en la filtració ocorren quan $u = p^k - 1$ amb $0 \leq k \leq m-1$ i $\varphi_{\mathbb{Q}_p(\xi_n)/\mathbb{Q}_p}(p^k-1) = k$ per tot $0 \leq k \leq m-1$. Tenint en compte tot això,

$$\begin{aligned} G^v = G(n)^v \text{ per } 0 \leq v \leq m, \\ G^v = \{1\} \text{ per } v \geq m \end{aligned}$$

5 Corbes algebraiques

Sigui k un cos perfecte qualsevol i denotem per $\overline{k}$ la seva clausura algebraica i F un cos intermedi. El conjunt $\mathbb{A}^n(F) := F^n$ és el conjunt de punts de l'espai afí de dimensió n amb coordenades a F.
Sigui $f(x,y) \in k[x,y]$ un polinomi en dues variables de grau total $\text{grau}(f) = d$. El conjunt de zeros de f amb coordenades a F es defineix com

$$Z_f(F) := \{(a,b) \in F \times F | f(a,b) = 0\}$$

5.1 Punts i ideals

A partir d'ara f serà un polinomi irreductible a $\overline{k}[x,y]$. L'anell $C_f := \overline{k}[x,y]/(f)$ és un domini d'integritat. Posem $K_f := \text{Frac}(C_f)$ i denotem

per $\mathrm{Max}(C_f)$ el conjunt d'ideals maximals de C_f. Ara, l'aplicació

$$\begin{aligned} I_f : Z_f(\overline{k}) &\longrightarrow \mathrm{Max}(C_f) \\ (a,b) &\mapsto (x-a, y-b) \end{aligned}$$

és de fet una bijecció entre els punts de la corba $Z_f(\overline{k})$ i els ideals maximals de C_f [Lor96, Sec. II.3]. Aquests ideals maximals estan formats per totes les funcions que s'anul·len en (a,b), és a dir, el valor de tal polinomi és precisament 0 a la plaça (a,b).

5.2 Punts singulars

Un punt (a,b) de $Z_f(\overline{k})$ es diu que és singular si

$$\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0$$

Si això no passa direm que el punt és no singular. Si (a,b) és un punt singular diem que la corba $Z_f(\overline{k})$ té una singularitat en (a,b) o simplement que és singular en (a,b). Diem que una corba és no singular si no té cap punt singular. Els resultats que vénen a continuació es poden veure a [Lor96, Cap. II]

Teorema 4. *Sigui $(a,b) \in Z_f(\overline{k})$ un punt i sigui $\mathfrak{m} \subset C_f$ l'ideal maximal corresponent. Aleshores el punt (a,b) és no singular si i només si l'ideal maximal de la localització $(C_f)_{(\mathfrak{m})}$ està generat per un element.*

Teorema 5. *Sigui $f \in \overline{k}[x,y]$ un polinomi irreductible. Aleshores l'anell $C_f := \overline{k}[x,y]/(f)$ és íntegrament tancat al seu cos de fraccions $\overline{k}(Z_f)$ si i només si la corba $Z_f(\overline{k})$ és no singular.*

Corol·lari 2. *C_f és un domini de Dedekind si i només si $Z_f(\overline{k})$ és no singular.*

Demostració. Pel Teorema de la base de Hilbert C_f és una $\overline{k}$-àlgebra finitament generada i per tant és noetheriana. D'altra banda es pot veure que C_f té dimensió de Krull 1. Ara pel Teorema 5 és íntegrament tancat si i només si $Z_f(\overline{k})$ és no singular. Recordant la definició 3 tenim que C_f és un domini de Dedekind si i només si $Z_f(\overline{k})$ és no singular. □

5.3 Corbes completes no singulars

Sigui L/k una extensió de cossos finitament generada de grau de transcendència 1. El conjunt de totes les valoracions discretes de L que són trivials sobre k es denota per $\mathcal{V}(L/k)$.

Definició 10. *Sigui k un cos qualsevol. Una corba completa no singular X/k sobre k és una parella $(X, k(X))$ que consisteix d'un cos de grau de transcendència 1 sobre k i un conjunt X el qual es troba en bijecció amb $\mathcal{V}(k(X)/k)$. Un element P de X s'anomena un punt i el cos $k(X)$ s'anomena el cos de funcions racionals de X. Cada punt P se li associa una valoració v_P de $\mathcal{V}(k(X)/k)$ i un anell local de valoració discreta $\mathcal{O}_P$ amb ideal maximal $\mathfrak{m}_P$. L'anell $\mathcal{O}_P$ s'anomena l'anell de funcions racionals definides en P. Una funció $\alpha \in \mathcal{O}_P$ s'anul·la en P si $\alpha \in \mathfrak{m}_P$. El nombre $v_P(\alpha)$ s'anomena el grau del zero de α. Per últim, si $\alpha \in k(X) \setminus \mathcal{O}_P$ aleshores α té un pol en P de grau $|v_P(\alpha)|$.*

Cada extensió de cossos L/k de grau de transcendència 1 genera una corba completa no singular, només cal considerar la parella $(\mathcal{V}(k(X)/k), L/k)$.

Definició 11. *Una recta projectiva sobre k és una corba completa no singular $\mathbb{P}^1/k$ amb la propietat que el cos $k(\mathbb{P}^1)$ és isomorf al cos de funcions racionals en una variable com a k-àlgebres.*

Com a exemple podem prendre la recta projectiva $\mathbb{P}^1/k$ associada al cos de funcionals $k(x)/k$, on x és una indeterminada. Aleshores es compleix

$$\mathcal{V}(k(X)/k) = \mathbb{P}^1 = \{v_{g(x)} | g(x) \in k[x] \text{ irreductible i mònic } \} \cup \{\infty\}$$

Per tant acabem de trobar una corba algebraica adequada pel cos que ens interessa, $\mathbb{F}_q(t)$.

6 Cossos de funcions algebraiques

En aquest capítol introduïm la noció de gènere d'un cos de funcions algebraiques com també la fórmula de Riemann-Hurwitz que s'utilitza per calcular el gènere d'una extensió.

Sigui $K = \mathbb{F}_q(t)$ el cos de funcions racionals sobre el cos finit $\mathbb{F}_q$ i L/K una extensió finita i separable de K.

Definició 12. *Sigui $\mathfrak{p}$ (resp. $\mathfrak{P}$) una plaça del cos K (resp. L). El grau de $\mathfrak{p}$ (resp. $\mathfrak{P}$) es defineix com*

$$deg\mathfrak{p} = [o_{(\mathfrak{p})}/\mathfrak{p} : \mathbb{F}_q]$$

i el grau d'un divisor $\mathfrak{a}$ (resp. $\mathfrak{A}$) de K, (resp. L) com

$$deg\mathfrak{a} = \sum_{\mathfrak{p} \in S(K)} v_{\mathfrak{p}}(\mathfrak{a}) \cdot deg\mathfrak{p}$$

6.1 El gènere

Hi ha una equivalència entre corbes algebraiques sobre un cos k i extensions de grau de transcendència 1 sobre k. En particular, una corba (anomenada superfície topològica) té associat sobre $\mathbb{C}$ la característica d'Euler i el gènere que correspon al nombre de forats. Aquí donem alguns detalls d'aquesta relació quan k és un cos global de característica positiva, o més concretament k és un cos finit.

Definició 13. *El grup de Picard $Pic(L)$ és el quocient de $Div(L)$ pel grup dels divisors principals. El grau d'un divisor $\overline{D} \in Pic(L)$ és el grau d'algun dels seus representants $D \in Div(L)$.*

Per tal d'enunciar el Teorema de Riemann-Roch introduïm la següent definició:

Definició 14. *Sigui k un cos i sigui X/k una corba completa no-singular. Definim el k-espai vectorial*

$$H^0(D) = \{\alpha \in k(X) | div(\alpha) + D \geq 0\}$$

i $h^0(D) = \dim_k(H^0(D))$.

Teorema 6 (Riemann-Roch)**.** *Sigui k un cos i X/k una corba completa no singular. Aleshores existeix un divisor $W \in Div(X)$ tal que es compleix*

$$h^0(D) = deg(D) + 1 - g(X) + h^0(W - D)$$

El divisor W s'anomena el divisor canònic. [Lor96, Sec. IX.4]

El nombre $g(X)$ es coneix com el gènere de la corba X/k. En particular el teorema ens dóna

$$\deg(W) = 2g(X) - 2$$

Vegem ara que $\mathbb{F}_q(t)$ té gènere 0 a partir del Teorema de Riemann-Roch.

Corol·lari 3. *Sigui k un cos, X/k una corba completa no-singular. Sigui $\mathcal{L} \in Pic(X/k)$. Si $\deg(L) \geq 2g(X) - 1$ aleshores $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g(X)$*

Demostració. Sigui D un representant de $\mathcal{L}$. Com que $\deg(D) > \deg(K)$ tenim que $\deg(W - D) < 0$. Ara pel Teorema de Riemann-Roch $h^0(D) \geq deg(D) + 1 - g(X)$ i per tant

$$h^0(W - D) = \deg(W - D) + 1 - g(X) + h^0(D)$$

cosa que implica $h^0(D) \geq g(X)$ i així

$$h^0(W - D) = h^0(D) + g(X) - 1 - \deg(D) \leq 2g(X) - 1 - \deg(D) \leq 0$$

Per tant $h^0(W - D) = 0$ i $h^0(\mathcal{L}) = \deg(\mathcal{L}) + 1 - g(X)$. □

Corol·lari 4. *Sigui k un cos. La recta projectiva $\mathbb{P}^1/k$ té gènere 0.*

Demostració. Identifiquem $k(\mathbb{P}^1)$ amb $k(x)$. Sigui ∞ el punt corresponent a la plaça de l'infinit. Es pot veure que $\{1, x, \ldots, x^n\}$ és una base per $H^0(n\infty)$ de manera que $h^0(n\infty) = n + 1$. Pel Corol·lari anterior, si n és prou gran tenim $h^0(n\infty) = n + 1 - g(k(x))$. Per tant $g(k(x)) = 0$. □

Suposem que la característica de $\mathbb{F}_q$ diferent de 2 i 3. Vegem ara alguns exemples de gèneres:

1. (Cossos de funcions el·líptiques) Considerem $y^2 = f(T)$, on $f \in A$ és un polinomi de grau 3 lliure de quadrats. Aleshores el cos $\mathbb{F}_q(y, T)$ té gènere $g = 1$.

2. Si $f \in A$ és un polinomi de grau 5 lliure de quadrats i $y^2 = f(T)$ aleshores el cos $\mathbb{F}_q(y, T)$ té gènere $g = 2$.

Donem ara la fórmula de Riemann-Hurwitz que relaciona el gènere de la corba X amb el gènere de la corba $\mathbb{P}^1$ i la ramificació d'un morfisme entre les dues corbes (pensat de manera geomètrica). Abans però, definim el cos de constants $\underline{l}$ d'un cos de funcions L com

$$\underline{l} = \{x \in L | x \text{ és algebraic sobre } \mathbb{F}_q\}$$

Teorema 7 (Fórmula de Riemann-Hurwitz)**.** *Sigui L'/L una extensió finita i separable del cos de funcions L. Siguin $\underline{l}, \underline{l}'$ els respectius cossos de constants a L, L'. Aleshores es compleix:*

$$2g(L') - 2 = \frac{[L' : L]}{[\underline{l}' : \underline{l}]}(2g(L) - 2) + deg\mathcal{D}_{L'/L}$$

Demostració. Veure [Ros01, Cap. 7] □

6.2 Extensions de constants

En general el cos $\mathbb{F}_q$ no és algebraicament tancat a L. Sigui ara L un cos de funcions algebraiques sobre $\mathbb{F}_q$ amb cos de constants $\underline{l}$. Si ara suposem que $\underline{l}'$ és una extensió algebraica de $\underline{l}$ que contingui la clausura algebraica de L, llavors el composat $L' = L\underline{l}'$ és un cos de funcions algebraiques sobre $\underline{l}'$. Les propietats més importants sota aquestes hipòtesis estan recollides en aquest teorema: [Ros01, Cap. 8]

Teorema 8. *(i) $\underline{l}'$ és el cos de constants de L'.*

(ii) Tot subconjunt $\underline{l}$-linealment independent de L també ho és sobre $\underline{l}'$.

(iii) Per a cada $x \in L \setminus \underline{l}'$ tenim $[L' : \underline{l}'(x)] = [L : \underline{l}(x)]$.

(iv) L'/L és no ramificada a cada plaça $\mathfrak{P}' \in S(L')$

(v) L' *té el mateix gènere que* L*.*

(vi) El cos residual d'una plaça $\mathfrak{P}'$ *de* L' *és el composat del cos* $\underline{l}'$ *amb el cos residual d'una plaça* $\mathfrak{P}$ *tal que* $\mathfrak{P}'|\mathfrak{P}$*.*

Aquest teorema ens permet considerar la clausura algebraica d'un cos a l'hora de calcular el seu gènere o els índexs de ramificació, sempre i quan $\mathbb{F}_q$ sigui el cos de constants, ja que són invariants per extensió de constants.

Aquest teorema facilita nombrosos càlculs. En especial per al nostre cas és certament important que a $\overline{\mathbb{F}_q}[T]$, tots els polinomis descomponen en factors de grau 1 i per tant només existeixen polinomis primers de grau 1. Pel que fa al cos de constants tenim que està contingut al cos residual $\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P}$ per una plaça $\mathfrak{P}$. Alhora, el cos residual és una extensió algebraica del cos de constants i per tant això implica la igualtat entre $\overline{\mathbb{F}_q}$ i i qualsevol extensió algebraica del cos de constants.

D'aquesta manera la fórmula de Riemann-Hurwitz se simplifica. Fent servir les notacions del Teorema 8 tenim que $\underline{l} = \overline{\mathbb{F}_q}$ i $\underline{l}' = \underline{l}$ i per tant

$$2g(L') - 2 = [L' : L](2g(L) - 2) + deg\mathcal{D}_{L'/L}$$

i també se'ns simplifica el grau de la diferent

$$deg\mathcal{D}_{L'/L} = \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'/L}) \cdot deg\mathfrak{P}' = \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'/L})$$

Això ens porta a enunciar un altre cop la fórmula de Riemann-Hurwitz de la manera que la farem servir d'ara endavant.

Teorema 9 (Fórmula de Riemann-Hurwitz)**.** *Sigui* L *un cos de funcions algebraic amb un cos de constants algebraicament tancat i sigui* L'/L *una extensió finita i seperable. Aleshores*

$$2g(L') - 2 = [L' : L](2g(L) - 2) + \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'/L})$$

Si a més la extensió L'/L *és de Galois de grau* m*, aleshores*

$$2g(L') - 2 = m(2g(L) - 2) + \sum_{\mathfrak{P}' \in S(L')} \frac{m}{e_{\mathfrak{P}}(L'/L)} \sum_{i=0}^{\infty} (g_i(\mathfrak{P}) - 1)$$

Demostració. Recordem que la diferent d'una extensió global és la suma de les diferents locals, per tant

$$\mathcal{D}_{L'/L} = \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'_{\mathfrak{P}'}/L_{\mathfrak{P}'}})\mathfrak{P}'$$

i la valoració de la diferent a una plaça $\mathfrak{P}'$ resulta

$$v_{\mathfrak{P}'}(\mathcal{D}_{L'/L}) = v_{\mathfrak{P}'}(\mathcal{D}_{L'_{\mathfrak{P}'}/L_{\mathfrak{P}'}}) = \sum_{i=0}^{\infty}(|G_i(\mathfrak{P}')| - 1)$$

En particular, en una extensió de Galois els ordres dels grups de ramificació superiors respecte una plaça $\mathfrak{P}'$ de L' queden determinats pels ordres dels grups de ramificació de les places $\mathfrak{P}$ que es troben a sota. Per tant només depenen de $r_{\mathfrak{P}}(L'/L)$. Per últim, com que el grau d'inèrcia d'una plaça és 1 perquè el cos de constants és algebraicament tancat, fent servir el Teorema 1 ens dóna la fórmula desitjada. □

7 El mòdul de Carlitz

En aquesta secció definirem el mòdul de Carlitz. Per fer-ho de la manera més simple possible començarem definint els *polinomis* de Carlitz [Con09].

Sigui $a \in \mathbb{F}_q[T]$ un polinomi i denotem per $\rho_a(X)$ el seu *polinomi de Carlitz* associat. Per definir $\rho_a(X)$, considerem $\rho_1(X) := X$ i

$$\rho_T(X) := X^q + TX$$

Per a un polinomi qualsevol definim el polinomi de Carlitz recursivament i forçant linealitat tal com es resumeix en els punts a continuació:

(i) $\rho_T(X) = TX + X^q$

(ii) $\rho_{T^n}(X) = \rho_T(\rho_{T^{n-1}}(X)) = [\rho_{T^{n-1}}(X)]^q + T \cdot \rho_{T^{n-1}}(X)$

(iii) $\rho_{a+b}(X) = \rho_a(X) + \rho_b(X)$, amb $a, b, \in A$

(iv) Per tot $c \in \mathbb{F}_q$ es té $\rho_{cT^n}(X) = c \cdot \rho_{T^n}(X)$

Veiem-ne uns exemple per entendre-ho millor.

Exemple 2. *(Polinomis de Carlitz)*

(i)

$$\begin{aligned}\rho_{T^2}(X) = \rho_T(\rho_T(X)) &= (TX + X^q)^q + T(TX + X^q) \\ &= X^{q^2} + (T^q + T)X^q + T^2X\end{aligned}$$

(ii)

$$\rho_{T^2-c}(X) = \rho_{T^2}(X) - \rho_c(X) = X^{q^2} + (T^q + T)X^q + (T^2 - c)X$$

(iii)

$$\begin{aligned}\rho_{T^3}(X) &= \rho_T(\rho_{T^2}(X)) \\ &= (X^{q^2} + (T^q + T)X^q + T^2X)^q + T(X^{q^2} + (T^q + T)X^q + T^2X) \\ &= X^{q^3} + (T^{q^2} + T^q + T)X^{q^2} + (T^{2q} + T^{q+1} + T^2)X^q + T^3X\end{aligned}$$

Ara ja estem en condicions de definir el mòdul de Carlitz.

Definició 15. *Sigui $L/\mathbb{F}_q(T)$ una extensió de cossos. Ara donem al grup additiu de K una estructura de $\mathbb{F}_q[T]$-mòdul a través dels polinomis de Carlitz. És a dir, si $a \in \mathbb{F}_q[T]$ i $\alpha \in L$, definim*

$$a \cdot \alpha := \rho_a(\alpha)$$

*Diem que aquesta és l'*acció *de Carlitz de $\mathbb{F}_q[T]$ sobre L.*

Considerem ara un polinomi mònic $n \in A$ i la seva descomposició en factors irreductibles a A:

$$n = \prod_{\nu=1}^{s} p_\nu^{r_\nu}$$

Aleshores definim els punts de n-torsió com el conjunt

$${}_n\rho = \{\lambda \in \overline{\mathbb{F}_q(T)} | \rho_m(\lambda) = 0\}$$

on $\overline{\mathbb{F}_q(T)}$ és la clausura algebraica de $\mathbb{F}_q(T)$. Denotem per $K(n) := K({}_n\rho)$ el cos de descomposició del polinomi $\rho_n(X)$ que correspon a afegir els punts de n-torsió al cos base $K = \mathbb{F}_q(T)$. Diem que λ és una arrel primitiva de n-torsió si l'A-mòdul ${}_n\rho$ està generat per λ. Com que els polinomis $\rho_n(X)$ són separables per tot $n \in A$ (ja que tots els termes de X que apareixen són de la forma X^{q^i}, amb $i \geq 0$ i el polinomi és no nul quan $i \neq 0$) tenim que l'extensió $K(n)/K$ és de Galois. Ara podem enunciar el teorema més important per a la caracterització d'aquestes extensions:

Teorema 10. *(i) L'extensió $K(n)/K$ és de Galois amb grup de Galois abelià isomorf a $(A/(n))^*$.*

(ii) Si $m = P^r$, potència d'un primer P aleshores l'extensió $K(n)/K$ ramifica totalment en $\mathfrak{p} = (P)$ i no ramifica en cap altra plaça finita $\mathfrak{q} \neq \mathfrak{p}, \mathfrak{q} \neq \infty$.

*(iii) Sigui $K_+(n)$ el cos fix per l'*embedding $\mathbb{F}_q^* \hookrightarrow (A/(n))^*$. *Aleshores la plaça de l'infinit* esplita *completament a $K_+(n)$ i totes les places que es troben sobre la plaça de l'infinit de $K_+(n)$ ramifiquen totalment a l'extensió $K(n)/K_+(n)$.*

(iv) Sigui n el producte de s factors primers de A. Aleshores $K(n)$ és el composat dels cossos $K(p_\nu^{r_\nu})$, per $\nu = 1, \ldots, s$, i tots els cossos $K(p^{r_\nu})$ són linealment independents dos a dos.

(v) Sigui $\mathcal{O}(n)$ la clausura entera de A a $K(n)$ i $\lambda \in_n \rho$ una arrel primitiva de n-torsió. Aleshores

$$\mathcal{O}(n) = A[\lambda]$$

Demostració. Veure [Ros01, Cap.12] □

Observació 3. *Aquest Teorema ens mostra les similituds que mencionàvem a la Introducció. Més concretament veiem que el grup de Galois $(\mathbb{Z}/(n))^\times$ de $\mathbb{Q}(\xi_n)$ correspon al grup de Galois $(A/(n))^\times$ de $K(n)$. El subcòs $K_+(n)$ correspon a l'extensió real més gran continguda a $\mathbb{Q}(\xi_n)$ i l'anell d'enters $\mathcal{O}(n)$ correspon a l'anell $\mathbb{Z}[\xi_n]$.*

Corol·lari 5. *$\mathbb{F}_q$ és algebraicament tancat a $K(n)$*

Demostració. Siguin $\mathfrak{p}_\infty$ i $\mathfrak{P}_\infty$ les places que es troben a sobre de la plaça de l'infinit ∞ de K a $K_+(n)$ i $K(n)$ respectivament. Aleshores $f(\mathfrak{p}_\infty/\infty) = 1$ (*esplita* completament) implica que el cos residual a $\mathfrak{p}_\infty$ és $\mathbb{F}_q$. Com que $\mathfrak{p}_\infty/\mathfrak{P}_\infty$ és totalment ramificada també tenim $f(\mathfrak{p}_\infty/\mathfrak{P}_\infty) = 1$ i per tant el cos residual de $\mathfrak{P}_\infty$ també és $\mathbb{F}_q$. Ara, com que el cos de constants de $K(n)$ s'injecta dins el cos residual de $\mathfrak{P}_\infty$, el cos de constants de $K(n)$ és $\mathbb{F}_q$. □

8 Càlcul del gènere

8.1 Notacions i hipòtesis

Tornem a recordar i a establir les notacions que farem servir a partir d'ara. Designem per $A := \mathbb{F}_q[T]$ i per $K = \mathbb{F}_q(T)$. També posem

$$K' := \overline{\mathbb{F}_q}K = \overline{\mathbb{F}}_q(T)$$

on K' és l'extensió del cos de constants a través de la transició cap a la clausura algebraica $\overline{\mathbb{F}_q} \subset C$ de $\mathbb{F}_q$. Sigui $n \in A$ un polinomi mònic. Aleshores n té una descomposició en factors primers, concretament

$$n = \prod_{\nu=1}^{s} P_\nu^{r_\nu}$$

on $s, r_\nu \in \mathbb{N}$ i els P_ν són tots mònics irreductibles, coprimers dos a dos i de grau ≥ 1. A més, definim

$$d_\nu := deg(P_\nu), q_\nu := q^{d_\nu}$$
$$n_\nu := P_\nu^{r_\nu}, m_\nu := \frac{n}{n_\nu}$$

i

$$\varphi(n) := |(A/(n))^*|$$

Pel Teorema Xinès del Residu tenim que

$$(A/(n))^* \simeq \prod_{\nu=1}^{s} (A/(n_\nu))^*$$

i per tant que

$$\varphi(n) = \prod_{\nu=1}^{s} \varphi(n_\nu) \text{ amb } \varphi(n_\nu) = (q_\nu - 1)q_\nu^{r_\nu - 1}$$

Aquí es pot veure clarament l'analogia amb la funció φ d'Euler. També designem per $\mathfrak{p}_\nu := (P_\nu)$ els ideals principals per $\nu = 1, \ldots, s$ i per $1 \leq \alpha \leq r_\nu$ definim

$$G(n_\nu)^\alpha := \{b \in (A/(n_\nu))^* | b \equiv 1 \mod P_\nu^\alpha\}$$

Pel que fa als punts de torsió definim

$${}_n\rho :=_n \rho(C)$$

com el conjunt de punts de n-torsió de C i pel que fa al cos de descomposició de $\rho_n(X)$ escriurem $K(n) := K({}_n\rho)$. Aleshores designem l'extensió del cos de constants de $K(n)$ per

$$K'(n) := \overline{\mathbb{F}_q} K(n)$$

Pel que hem vist al capítol 6.2, el grau, l'índex de ramificació i el gènere no canvien a través d'extensions del cos de constants ja que $\mathbb{F}_q$ és el cos de constants de $K(n)$ pel Corol·lari 5. Per tant per una extensió de Galois d'un cos de funcions algebraiques, els ordres dels grups de ramificació superiors tampoc canvien per extensions del cos de constants. Així tenim:

$$[K'(n) : K'] = [K(n) : K] = \varphi(n)$$
$$e_{\mathfrak{p}'}(K'(n) : K') = e_{\mathfrak{p}}(K(n) : K) \text{ i per tant } g(K'(n)) = g(K(n))$$

on $\mathfrak{p}' \in S(L')$ amb $\mathfrak{p}'|\mathfrak{p}$.

Finalment sigui $K \subset L \subset K(n)$ i sigui $L' = \overline{\mathbb{F}_q} L$. Aleshores si $\mathfrak{q} \in S(L)$ i $\mathfrak{q}' \in S(L')$ amb $\mathfrak{q}'|\mathfrak{q}$ posem

$$g_i(\mathfrak{q}') := |(G(K'(n)/L'))_i(\mathfrak{q}')| = |G(K(n)/L))_i(\mathfrak{q})|$$

com l'ordre del i-èssim grup de ramificació a l'extensió $K'(n)/L'$

A partir d'aquí la nostra intenció serà trobar una fórmula tancada per al gènere del mòdul de Carlitz. Començarem pel cas $K(P^r)$, és a dir, per potències d'elements primers i després ho estendrem recursivament fent servir que $K(n_\nu)$ i $K(m_\nu)$ són linealment independents.

8.2 El gènere de $K(P^r)$

A partir d'aquesta secció, com que estem inspeccionant un sol polinomi P^r, tenim que $s = 1$. Per claredat també escriurem $P_1 = P$, $r_1 = r$, i $d_1 = d$. El grup de Galois serà G com habitualment.

Gràcies a la fórmula de Riemann-Hurwitz podem calcular el gènere del cos $K(P^r)$

$$2g(K(P^r)) - 2 = [K(P^r) : K](2g(K) - 2) + \sum_{\mathfrak{p} \in S(K')} \sum_{i=0}^{\infty} (g_i(\mathfrak{p}) - 1)$$

Tanmateix, ens falta conèixer l'ordre dels grups de ramificació superior per poder determinar el gènere completament. La següent secció abordarà exactament això. Tots els resultats sobre el gènere de $K(P^r)$ i $K(n)$ són deguts a [Kel01].

8.2.1 Grups de ramificació superior de $K(P^r)$

Recordem que pel Teorema 10 totes les places que es troben sobre la plaça de l'infinit són dòcilment ramificades amb índex de ramificació $e_\infty(K(P^r)/K) = q - 1$. Els grups de ramificació superiors són trivials i d'aquesta manera l'expressió per la diferent local se simplifica

$$\sum_{i=0}^{\infty} (g_i(\infty) - 1) = e_\infty(K(P^r)_{\mathfrak{Q}}/K_\infty) - 1 = q - 2$$

on $\mathfrak{Q} \in S(K(P^r))$ és un plaça sobre de ∞. A més, com a conseqüència del Teorema 10 tenim que $\mathfrak{p} = (P)$ és l'única plaça finita que ramifica en aquesta extensió. Com que és totalment ramificada tenim que l'índex és

$$e_{\mathfrak{p}}(K(P^r)/K) = |(A/\mathfrak{p})^*| = \varphi(P^r) = q^{d(r-1)}(q^d - 1)$$

Denotant per $K_{\mathfrak{p}}$ i per $K(P^r)_{\mathfrak{P}}$ les respectives completacions dels cossos K i $K(P^r)$ en les places pertinents amb $\mathfrak{P}|\mathfrak{p}$ sabem per la secció 2.2.3 que el grup de Galois de $K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ és exactament el grup de descomposició de $\mathfrak{P}$

$$G((K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}})) = Z_{\mathfrak{P}}(K(P^r)/K)$$

Com que $\mathfrak{p}$ ramifica totalment, els grups de Galois de $K(P^r)/K$ i $K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ coincideixen i el grup d'inèrcia de $\mathfrak{P}$ és exactament el grup de Galois.

Denotem ara l'i-èssim grup de ramificació de $\mathfrak{P}$ a l'extensió $K(P^r)/K$ i $K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ com

$$G_i := \{\sigma \in G | v_{\mathfrak{P}}(\sigma(a) - a) \geq i + 1, \forall a \in \mathcal{O}_{(\mathfrak{P})}\}$$

per tot $i \geq -1$. Aleshores tenim la proposició següent

Proposició 7. *Els grups de ramificació de* $K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ *són*

$$\begin{aligned} G_0 &= G(K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}), \\ G_i &= G(P^r)^1, \ \textit{per } 1 \leq i \leq q^d - 1 \\ G_i &= G(P^r)^2, \ \textit{per } q^d \leq i \leq q^{2d} - 1 \end{aligned}$$

i en general

$$\begin{aligned} G_i &= G(P^r)^\alpha, \ \textit{per } q^{d(\alpha-1)} \leq i \leq q^{d\alpha} - 1, 1 \leq \alpha \leq r-1 \\ G_i &= G(P^r)^r = \{1\}, \ \textit{per } q^{d(r-1)} \leq i \end{aligned}$$

Demostració. És clar que $G_0 = T_{\mathfrak{P}}(K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) = G(K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}})$ per ser totalment ramificat. Sigui ara R^* un sistema generador minimal per $(A/(P^r))^*$ i λ_0 un generador del A-mòdul ${}_{P^r}\rho$. Aleshores l'aplicació

$$\begin{aligned} R^* &\longrightarrow G(K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) \\ b &\longmapsto \sigma_{\overline{b}} \end{aligned}$$

amb $\sigma_{\overline{b}}(\lambda_0) = \rho_b(\lambda_0)$ és una bijecció. Per $b \in R^*$ tenim

$$\rho_b(\lambda_0) = b \cdot \lambda_0 + (\ldots)\lambda_0^q + \cdots + \lambda_0^{q^{deg(b)}}$$

A més a més tenim

$$\rho_b(\lambda_0) - \lambda_0 = \rho_{b-1}(\lambda_0)$$

i

$$v_{\mathfrak{P}}(\rho_b(\lambda_0) - \lambda_0) = v_{\mathfrak{P}}(\rho_{b-1}(\lambda_0))$$

Ara provem un lema que ens ajudarà a acabar la demostració

Lema 3. *Si per* $0 \leq \alpha \leq r-1$ *tenim* $b \equiv 1 \mod P^\alpha$ *i* $b \not\equiv 1 \mod P^{\alpha+1}$, *aleshores* $\rho_{b-1}(\lambda_0)$ *és una arrel primitiva de* $\rho_{P^{r-\alpha}}$*-torsió.*

Demostració. Siguin

$$f_{p^r}(X) := \frac{\rho_{P^r}(X)}{\rho_{P^{r-1}}(X)} = \prod_{\substack{\lambda \in {}_{P^r}\rho \\ \lambda \text{primitiva}}} (X - \lambda)$$

i

$$f_{P^{r-\alpha}}(X) := \frac{\rho_{P^{r-\alpha}}(X)}{\rho_{P^{r-\alpha-1}}(X)} = \prod_{\substack{\lambda \in {}_{P^{r-\alpha}}\rho \\ \lambda \text{primitiva}}} (X - \lambda)$$

Ambdós polinomis són Eisenstein i també el polinomi irreductible de les extensions $K(P^r)$ i $K(P^{r-\alpha})$ respectivament.

Ara com que $P^\alpha|(b-1)$ i $P^{\alpha+1} \nmid (b-1)$, existeix $\tilde{b} \in R^*$ tal que $b-1 = \tilde{b}\cdot P^\alpha$ amb $\gcd(\tilde{b}, p) = 1$. Així obtenim

$$\rho_{P^{r-\alpha}}(\rho_{b-1}(\lambda_0)) = \rho_{(b-1)P^{r-\alpha}}(\lambda_0) = \rho_{\tilde{b}P^r}(\lambda_0) = \rho_{P^r}(\rho_{\tilde{b}}(\lambda_0)) = 0$$

i

$$\rho_{P^{r-\alpha-1}}(\rho_{b-1}(\lambda_0)) = \rho_{\tilde{b}P^{r-1}}(\lambda_0) \neq 0$$

ja que $\rho_{\tilde{b}}(\lambda_0)$ és una arrel primitiva de ρ_{P^r}-torsió. Per tant $f_{P^{r-\alpha}}(\rho_{b-1}(\lambda_0)) = 0$ i per tant $\rho_{b-1}(\lambda_0)$ és una arrel primitiva de $\rho_{P^{r-\alpha}}$-torsió com volíem. □

Finalment recordant que ramifica totalment tenim

$$v_{\mathfrak{P}}(\rho_{b-1}(\lambda_0)) = [K(P^r)_{\mathfrak{P}} : K(P^{r-\alpha})_{\mathfrak{q}}] \cdot v_{\mathfrak{q}}(\rho_{b-1}(\lambda_0)) = q^{d\alpha} \cdot 1 = q^{d\alpha}$$

on $\mathfrak{q}$ és l'ideal primer de la clausura entera de $K(P^{r-\alpha})$ que divideix $\mathfrak{p}$, és a dir, $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{P}$. D'aquí surt $\sigma_{\overline{b-1}} \in G_i$ per tot $i \leq q^{d\alpha} - 1$ i $\sigma_{\overline{b-1}} \notin G_i$ per $i \geq q^{d\alpha}$. Per tant queda demostrada la Proposició. □

Proposició 8. *Per tot $1 \leq \alpha \leq r$ es compleix*

$$|G(P^r)^\alpha| = q^{d(r-\alpha)}$$

Demostració. Considerem la projecció

$$(A/(P^r))^* \longrightarrow (A/(P^\alpha))^*$$

que té com a nucli el grup $G(P^r)^\alpha$. D'aquí veiem que tenim la següent seqüència exacta

$$1 \longrightarrow G(P^r)^\alpha \longrightarrow (A/(P^r))^* \longrightarrow (A/(P^\alpha))^* \longrightarrow 1$$

Per tant l'ordre del nucli és

$$|G(P^r)^\alpha| = \frac{\varphi(P^r)}{\varphi(P^\alpha)} = q^{d(r-\alpha)}$$

□

Proposició 9. *La filtració de grups descrita a la Proposició 7 concorda amb la numeració superior dels grups de ramificació. En concret,*

$$G_i = G^\alpha = G(P^r)^\alpha \text{ amb } \varphi_{K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(i) = \alpha$$

Demostració. Recordem que si G^v és un salt en la filtració (G^v) aleshores, pel Teorema de Hasse-Arf el nombres v és un enter. Per tant primer haurem de determinar els $v \in \mathbb{R}$ tals que v és un enter. Recordem també l'expressió que teníem per la funció φ

$$\varphi_{K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i$$

on g_i són els ordres dels grups de ramificació superior i m un nombre natural. Per tant, per $q^{d(\alpha-1)} \leq m \leq q^{d\alpha} - 1$ tenim

$$\begin{aligned}
\varphi_{K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(m) &= \frac{1}{g_0}\left(\sum_{k=1}^{\alpha-1}\sum_{i=q^{d(k-1)}}^{q^{kd}-1} q^{d(r-k)} + \sum_{i=q^{d(\alpha-1)}}^{m} q^{d(r-\alpha)}\right) \\
&= \frac{1}{g_0}\left((\alpha-1)(q^d-1)q^{d(k-1)}q^{d(r-k)} + (m - q^{d(\alpha-1)} + 1)q^{d(r-\alpha)}\right) \\
&= \alpha - 1 + \frac{m - q^{d(\alpha-1)} + 1}{(q^d-1)q^{d(r-1)}} \cdot q^{d(r-\alpha)} \\
&= \begin{cases} \alpha, m = q^{d\alpha} - 1 \\ \notin \mathbb{N}, \text{ en altre cas} \end{cases}
\end{aligned}$$

Per tant els salts en la filtració concorden amb la numeració superior

$$G_{q^{d\alpha}-1} = G^{\alpha} \simeq G(P^r)^{\alpha} \text{ per } 1 \leq \alpha \leq r-1$$

ja que $\varphi_{K(P^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(q^{d\alpha} - 1) = \alpha$. □

A partir d'ara escriurem $G(n)$ tant per designar $(A/(n))^*$ com per designar el grup de Galois $G(K(n)/K)$ ja que els podem identificar a través d'un isomorfisme.

8.2.2 Càlcul de gènere

Ara ja tenim tots els ingredients per substituir a la Fórmula de Riemann-Hurwitz. Tenim

$$\begin{aligned}
2g(K(P^r)) - 2 &= [K(P^r) : K](2g(K) - 2) + \sum_{\mathfrak{q} \in S(K')}\sum_{i=0}^{\infty}(g_i(\mathfrak{q}) - 1) \\
&= \varphi(P^r)(2g(K) - 2) + \frac{\varphi(P^r)}{q-1}\left(e_{\infty}(K(P^r)/K) - 1\right) \\
&\quad + d \cdot \sum_{i=0}^{\infty}(g_i(\mathfrak{p}) - 1) \\
&= -2 \cdot \varphi(P^r) + \frac{\varphi(P^r)}{q-1}(q-2) + d \cdot \sum_{i=0}^{\infty}(g_i(\mathfrak{p}) - 1)
\end{aligned}$$

on a la última igualtat hem fet servir que el gènere d'un cos de funcions racionals és 0 (grau de transcendència 1). Tenint en compte tot el que s'ha

provat en aquesta secció:

$$\begin{aligned}\sum_{i=0}^{\infty}(g_i(\mathfrak{p})-1) &= \sum_{i=0}^{q^{d(r-1)}}(g_i(\mathfrak{p})-1)\\ &= |g_0(\mathfrak{p})|-1+\sum_{\alpha=1}^{r-1}\sum_{i=q^{d(\alpha-1)}}^{q^{d\alpha}-1}(|G(P^r)^\alpha|-1)\\ &= |g_0(\mathfrak{p})|-1+\sum_{\alpha=1}^{r-1}(q^{d\alpha}-q^{d(\alpha-1)})(q^{d(r-\alpha)}-1)\\ &= |g_0(\mathfrak{p})|-1+\sum_{\alpha=1}^{r-1}(q^{d\alpha}-q^{d(\alpha-1)})q^{d(r-\alpha)}-\sum_{\alpha=1}^{r-1}(q^{d\alpha}-q^{d(\alpha-1)})\\ &= q^{d(r-1)}(q^d-1)-1+(r-1)q^{d(r-1)}(q^d-1)-(q^{d(r-1)}-1)\\ &= q^{d(r-1)}(rq^d-r-1).\end{aligned}$$

on hem fet servir

- Primer igualtat: $G_i(\mathfrak{P})=\{1\}$ si $i\geq q^{d(r-1)}$.
- Segona igualtat: $G_i(\mathfrak{P})=G(P^r)^\alpha$ si $q^{d(\alpha-1)}\leq i\leq q^{d\alpha}-1$.
- Tercera igualtat: $|G(P^r)^\alpha|=q^{d(r-\alpha)}$.

Només falta combinar-ho tot per obtenir

$$2g(K(P^r))-2=-2(q^d-1)q^{d(r-1)}+\frac{q-2}{q-1}q^{d(r-1)}(q^d-1)+dq^{d(r-1)}(rq^d-r-1)$$

i per tant aïllant ens queda

$$g(K(P^r))=1+\frac{1}{2}(q^d-1)q^{d(r-1)}\left(-2+\frac{q-2}{q-1}+d\frac{rq^d-r-1}{q^d-1}\right)$$

Per tant podem enunciar-ho com a un resultat ja

Teorema 11. *El gènere del cos $K(P^r)$ és*

$$g(K(P^r))=1+\frac{1}{2}\varphi(p^r)\left(-2+\frac{q-2}{q-1}+d\frac{rq^d-r-1}{q^d-1}\right)$$

8.3 El gènere de $K(n)$

Teorema 12. *El gènere de $K(n)$ és*

$$2g(K(n))-2=\varphi(n)\left(-2+\frac{q-2}{q-1}+\sum_{\nu=1}^{s}d_\nu\frac{r_\nu q_\nu-r_\nu-1}{q_\nu-1}\right)$$

Demostració. (i) El càlcul del gènere es pot fer recursivament:

$$g(K(n)) = [K(n) : K(m_\nu)](2g(K(m_\nu)) - 2) + \sum_{\tilde{\mathfrak{p}} \in S(K'(m_\nu))} \sum_{i=0}^{\infty} (g_i(\tilde{\mathfrak{p}}) - 1)$$

(ii) Els cossos $K(n_\nu)$ són linealment independents pel Teorema 10, i entre les totes les places que ramifiquen a $K(n_\nu)$, només la plaça $\mathfrak{p}_\nu$ és no ramificada a $K'(m_\nu)$. Les places de $K'(m_\nu)$ que es troben sobre $\mathfrak{p}_\nu$ són completament *split*, i així tenim que el grau de descomposició de les places $\mathfrak{p}_\nu$ per $\nu = 1, \ldots, s$ a $K'(n)$ és $d_\nu \cdot \varphi(m_\nu)$ (veure secció 2.2.4).

(iii) L'índex de ramificació de la plaça de l'infinit a $K(n)$ i $K(m_\nu)$ són iguals per $s \geq 2$, és a dir, no existeix més ramificació a la plaça de l'infinit a l'extensió $K(n)/K(m_\nu)$.

(iv) Denotem per $H_i(\mathfrak{P}_\nu)$ l'i-èssim grup de ramificació d'una plaça $\mathfrak{P}_\nu \in S(K(n))$ que es trobi sobre $\mathfrak{p}_\nu$. Aleshores tenim

$$H_i(\mathfrak{P}_\nu) = G(K(n)/K(m_\nu)) \cap G_i(\mathfrak{P}_\nu) = G_i(\mathfrak{P}_\nu)$$

ja que $G(K(n)/K(m_\nu)) = G(K(n_\nu)/K) = G(n_\nu)$.

(v) Finalment fent servir l'equació del punt (i) i els comentaris anteriors ens queda la següent expressió per $s \geq 2$:

$$2g(K(n)) - 2 = \varphi(n_\nu)(2g(K(m_\nu)) - 2) + d_\nu \varphi(m_\nu) \sum_{i=0}^{\infty} g_i(\mathfrak{p}_\nu)$$

Per acabar la demostració només cal fer inducció sobre s. Pêr $s = 1$ tenim exactament la fórmula del $g(K(P^r))$. Suposem ara que és cert per a $s - 1$ i fem servir (v) per provar el cas s:

$$\begin{aligned}
2g(K(n)) - 2 &= \varphi(n_s)(2g(K(m_s)) - 2) + d_s \varphi(m_s) \sum_{i=0}^{\infty} g_i(\mathfrak{p}_s) \\
&= \varphi(n_s)\varphi(m_s) \left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s-1} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1} \right) \\
&+ d_s \varphi(m_s) q_s^{r_s - 1}(r_s q_s - r_s - 1) \\
&= \varphi(n) \left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s-1} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1} \right) \\
&+ d_s \varphi(n) \frac{r_s q_s - r_s - 1}{q_s - 1} \\
&= \varphi(n) \left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1} \right)
\end{aligned}$$

□

Per tant el gènere de $K(n)$ és: [Kel01]

$$g(K(n)) = 1 + \frac{1}{2}\varphi(n)\left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1}\right)$$

Apèndix: Extensions abelianes considerant el twistat del mòdul de Carltiz

Considerem el mòdul de Carlitz twistat sobre $\mathbb{F}_q(T) = K$ definit per $\rho^{\Delta}_T(X) = \Delta X^q + TX$ amb $\Delta \in \mathbb{F}_q[T]$.

Fixem una clausura separable de K, denotem-la $\overline{K}$. De manera similar al mòdul de Carlitz podem considerar els punts de g-torsió de ρ^{Δ} amb $g \in A = \mathbb{F}_q[T]$ via

$$ {}_g\rho^{\Delta}\{\alpha \in \overline{K} | \rho^{\Delta}_g(\alpha) = 0\}.$$

Tenim el següent enunciat a Gekeler [Gek16]:

Teorema 13. *L'extensió $K(g) := K({}_g\rho^{\Delta})/K$ és una extensió finita de Galois i abeliana i a més hi ha un morfisme injectiu*

$$\psi : Gal(K(g)/K) \hookrightarrow (A/(g))^*.$$

Exemple 3. *Considerem $\rho^{\Delta}_T(X) = TX + \Delta X^q$ i $rho^{\Delta}_{T^2}(X) = T^2X + \Delta(T + T^q)X^q + \Delta^{q+1}X^{q^2}$, tenim llavors que $K({}_T\rho^{\Delta}) = K(\sqrt[q-1]{\frac{-T}{\Delta}})$ i $K({}_{T^2}\rho^{\Delta})$ és el cos de descomposició del polinomi irreductible sobre $\mathbb{F}_q[T]$: $T + \Delta(TX + \Delta X^q)^{q-1}$ sobre K i l'extensió té grau $q(q-1)$. Observeu que*

$$\rho^{\Delta}_{T^2}(X) = T(TX + \Delta X^q) + \Delta(T^q X^q + \Delta^q X^{q^2}) =$$

$$(TX + \Delta X^q)(T + \Delta(TX + \Delta X^q)^{q-1}).$$

El següent resultat és ben conegut en la literatura, veieu per exemple [Ros01, Cap. 12].

Teorema 14. *Suposem $\Delta \in \mathbb{F}_q^*$, i per simplificar suposem que g és un polinomi irreductible de $\mathbb{F}_q[T]$. La clausura entera de $\mathbb{F}_q[T]$ en $K({}_{g^n}\rho^{\Delta})$ és $\mathbb{F}_q[T][\alpha]$ on $Irr(\alpha, K)[X]$ és $\rho^{\Delta}_{g^n}(X)/\rho^{\Delta}_{g^{n-1}}$.*

I en particular l'extensió $K({}_{g^n}\rho^{\Delta})/K$ ramifica totalment en (g) (per tant de grau $q^{deg_T(g)n}(q^{deg_T(g)} - 1)$ i moderadament ramificat en ∞ amb grau $q-1$ en ∞, no ramificant en cap altre primer.

Proposició 10. *Sigui $\Delta \in \mathbb{F}_q[T] \setminus \mathbb{F}_q$ i g un polinomi irreductible de $\mathbb{F}_q[T]$ coprimer amb Δ. Llavors $\rho^{\Delta}_g(X)/X$ és irreductible i el polinomi $h(X) = \rho^{\Delta}_g(X/\Delta) \cdot \Delta^s$, és mònic en $\mathbb{F}_q[T][X]$, per algun $s \in \mathbb{N}$ adequat, i per tant $\Delta\alpha$ és un element de la clausura entera $\mathcal{O}$ de $\mathbb{F}_q[T]$ en $K({}_g\rho^{\Delta})$, i per tant $\mathbb{F}_q[T][\Delta\alpha] \subseteq \mathcal{O}$. Aquí α és una arrel qualsevol del polinomi $\rho^{\Delta}_g(X)/X$*

Demostració. Que $\rho^{\Delta}_g(X)/X$ és irreductible surt de considerar el cas sense twistat, on sabem que $\rho_g(X)/X$ és Eisenstein en g. Si Δ és coprimer amb g, $\rho^{\Delta}_g(X)/X$ també és Eisenstein. Falta escriure la resta.

□

Tenim el següent resultat que podem trobar al llibre del Lorenzini [Lor96]

Teorema 15. *Si $C_g = \mathbb{F}_q[T][X]/g(X)$ amb $g(X)$ irreductible mònic a coeficients en $\mathbb{F}_q[T]$, i $g(X)$ és no-singular llavors C_g és integrament tancat en $\mathbb{F}_q(T)[X]/g(X)$.*

És té el següent resultat sobre ramificació en extensions de cossos, veieu [Neu99].

Teorema 16. *Sigui $F/K = \mathbb{F}_q(T)$ una extensió finita separable i escrivim $F = K(\alpha)$, sigui $\mathcal{O}_F$ la clausura entera de $A = \mathbb{F}_q[T]$ en K i suposem α és A-enter, (és a dir $g(X) := Irr(\alpha, K)[X] \in A[X]$ mònic), clarament $A[\alpha] \subseteq \mathcal{O}_F$. Tenim que si és un primer $\mathcal{P}$ de F sobre A, ramifica sobre F/K si $\mathcal{P} \cap A = \mathfrak{p}$ divideix la Resultant de g i g'. A més a més si $\mathcal{O}_F = A[\alpha]$ i la resultant de g i g' és l'ideal de A: $\mathfrak{p}_1^{m_1} \cdot \ldots \cdot \mathfrak{p}_r^{m_r}$ llavors els únics primers de L/K sobre A ramificats són $\mathfrak{p}_\mathfrak{i}$ on $m_i = [L : K](1 - 1/e_i)$ si $\mathfrak{p}_i$ es debilment ramificat on e_i és l'index de ramificació.*

En el cas de ramificació salvatge en l'ideal $\mathfrak{p}_i$ llavors m_i és igual a

$$[F : K] \cdot \left(\sum_{i=0}^{\infty} \frac{|I_n| - 1}{|I_0|} \right).$$

on I_0 el grup d'inèrcia i I_1 el grup inèrcia salvatge i I_n l'n-èssim grup grup d'inèrcia superior.

Demostració. Tant sols l'última part és menys coneguda. Quan tenim aquesta situació la resultant coincideix amb la different i tenim que

$$Res(g, g') = \prod \mathfrak{p}_1^{m_1} \ldots \cdot {\mathfrak{p}_\mathfrak{r}}^{m_r}$$

□

Exemple 4. *Amb el cas $\Delta \notin \mathbb{F}_q^*$, anterior anell $A[\alpha]$ no coincideix amb $\mathcal{O}$. Per exemple si $g(X) = T^2 + 2T + 2 \in \mathbb{F}_3[T]$, irreductible, i $\Delta = T + 1$ aleshores*

$$\rho_g^\Delta(X)/X = \Delta^4 X^8 + (T^4 + T^3 + T^2 + 2)X^2 + T^2 + 2T + 2$$

Ara, fent el canvi $X \leftrightarrow \Delta X$ i tornant a multiplicar per Δ^4 queda

$$r(X) = X^8 + (T^6 + T^4 + T + 2)X^2 + T^6 + T^4 + T + 2$$

i la resultant $Res(r, r') = \Delta^{28} g^7$.

De Gekeler [Gek16], i prenem $\mathfrak{n}$ primer de A i coprimer amb Δ tenim que $K({}_\mathfrak{n}\rho^\Delta)/K$ sol pot ser ramificat en ∞, $\mathfrak{n}$ i primers sobre Δ, per tant pel càlcul del gènere de $g(K({}_\mathfrak{n}\rho^\Delta))$ sol falta estudiar la ramificació sobre aquests tres primers.

Sota la hipòtesi $(\Delta, \mathfrak{n}) = 1$ i pensem Δ primer, Gekeler demostra en [Gek16] que el cos de constants per a $K({}_{\mathfrak{n}}\rho^{\Delta})$ és $\mathbb{F}_q$ on $K = \mathbb{F}_q(T)$, d'on d'un argument similar al cas no twistat hauria de sortir que ∞ és moderadament ramificat amb index $q - 1$.

Pel primer $\mathfrak{n}$, per Gekeler, es prova que té el mateix index de ramficiacions en tots els grups i-èssims de grups inèrcia per tant contribuieix de la mateixa manera amb la diferent.

Falta estudiar amb detall l'extensió de Kummer i la ramificació sobre Δ.

Referències

[Car35] Leonard Carlitz. "On certain functions connected with polynomials in a Galois field". A: *Duke Mathematical Journal* 1.2 (1935), pàg. 137 - 168. DOI: 10.1215/S0012-7094-35-00114-4. URL: https://doi.org/10.1215/S0012-7094-35-00114-4.

[Car38] L. Carlitz. "A class of polynomials". A: *Transactions of the American Mathematical Society* 43 (1938), pàg. 167 - 182.

[MF 69] I.G. MacDonald M.F. Atiyah. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. CRC Press, 1969. ISBN: 978-0-201-40751-8.

[Ser79] Jean-Pierre Serre. *Local Fields*. Graduate Texts in Mathematics. Springer-Verlag, 1979. ISBN: 0-387-90424-7.

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry*. Graduate Studies in Mathematics. American Mathematical Society, 1996. ISBN: 0-8218-0267-4.

[Neu99] J. Neukirch. *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, 1999. ISBN: 0-387-90424-7.

[Kel01] Alice Keller. "Cyclotomic Function Fields with Many Rational Places". A: *Finite Fields and Applications*. Ed. de Dieter Jungnickel i Harald Niederreiter. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, pàg. 293 - 302.

[Ros01] Michael Rosen. *Number Theory in Function Fields*. Graduate Texts in Mathematics. Springer, 2001. ISBN: 0-387-95335-3.

[Con09] Keith Conrad. *Carlitz Extensions*. 2009. URL: https://kconrad.math.uconn.edu/blurbs/gradnumthy/carlitz.pdf. (consultat: 18.06.2022).

[Gek16] Ernst-Ulrich Gekeler. "The Galois image of twisted Carlitz modules". A: *Journal of Number Theory* 163 (2016), pàg. 316 - 330. DOI: https://doi.org/10.1016/j.jnt.2015.11.021.