Grup de classes d'ideals sobre cossos globals

Treball de fi de Grau de Matemàtiques

Autor:
Sergi Arjó Segovia

Tutor:
Francesc Bars Cortina

Juny 2021

Índex

1 Introducció **2**

2 Grup de classes d'ideals **3**
2.1 Clausura entera i dominis de Dedekind 3
2.2 Factorització única d'ideals i ramificacions 9
2.3 Norma d'un ideal 13
2.4 Valoracions i anàlisi no arquimedià 15
2.5 Grup de classes d'ideals i la seva finitud 18

3 El grup de classes de divisors i les S-unitats **24**
3.1 Divisors i Teorema de Riemann-Roch 24
3.2 Teorema de les unitats de Dirichlet en cossos globals en característica positiva . . . 25
3.3 Relació entre Cl_K, Cl_S i grup de classes d'ideals d'un domini de Dedekind 27

4 La conjectura de Brumer-Stark **28**
4.1 Preàmbul i Teorema de Stickelberger 28
4.1.1 Cas extensió ciclotòmica en cossos de nombres 28
4.1.2 Cas extensions abelianes sobre cos finit en característica positiva 29
4.2 La conjectura de Brumer-Stark per a cossos globals 30
4.2.1 Cas extensió ciclotòmica 31
4.2.2 Cos de global en característica p>0 31

5 Alguns resultats referents al nombre de classes per a cossos globals ciclotòmics. **35**
5.1 Extensions de cossos constants 35
5.2 Extensions ciclotomiques dels racionals 36
5.3 Extensions Carlitz-ciclotòmiques 38

Apèndixs **41**

A Extensions ciclotòmiques en cossos globals **41**
A.1 Extensions ciclotòmiques en cossos numèrics 41
A.2 Extensions ciclotòmiques en cossos globals de característica positiva 41

B Relació de corbes amb cossos de funcions d'una variable **43**

1 Introducció

Comencem definint que és un cos global, que seràn els cossos amb els quals treballarem al llarg de tot el treball.

Definició 1.1 *Un cos global K és un cos que compleix una de les següents possibilitats*

(i) és una extensió finita de $\mathbb{Q}$, i en aquest cas parlem de cos numèric o cos de nombres.

(ii) és una extensió finita de $\mathbb{F}_q(T) = \mathbb{F}(T)$, el cos de fraccions de l'anell de polinomis $\mathbb{F}[T]$, on $q = p^r$, p primer i $r \in \mathbb{N} \geq 1$, és a dir, el cos de funcions d'una corba algebraica sobre un cos finit.

En particular, és molt interessant el cas de característica positiva $\mathbb{F}[T]$, i el paral·lelisme entre $\mathbb{Z}$ i $\mathbb{F}[T]$: són dominis d'ideals principals, tenen grup d'unitats finits, tenen la propietat que l'anell de quocients mòdul un ideal diferent del zero té un nombre finit d'elements, etc. De fet, $\mathbb{F}[T] \subseteq \mathbb{F}(T)$ té diferents analogies amb $\mathbb{Z} \subset \mathbb{Q}$. Així doncs, també treballarem amb aquestos. Una bona font d'informació són les notes del llibre [TN].

L'objectiu principal del treball és la demostració de la finitud del grup de classes d'ideals en el context dels dominis de Dedekind dins cossos globals en característica $p > 0$, i tot el background necessàri per fer-ho. Una vegada demostrat aquest fet, vam anar ampliant el treball, on el capítol 3 resulta clau pels conceptes que introduim i la relació amb l'objectiu principal. Finalment, els capítols 4 i 5 són aplicacions o alguns dels darrers resultats relacionats amb el que hem estudiat al llarg del treball.

En un primera part del treball, concretament durant tot el capítol 2, el nostre objectiu és definir el grup de classes d'ideals i veure que és finit en el context dels dominis de Dedekind dins cossos globals en característica $p > 0$. En aquesta primera part, introudïrem tots els conceptes, eïnes i resultats necessàris fent la demostració de finitud. Una motivació darrere d'això és l'idea de mesurar com de lluny es troba l'anell amb el treballem de ser un domini d'ideals principals. La teoria de grup de classes d'ideals va ser introduïda per Kummer,en particular, en el cas del l'anell d'enters ciclotòmic $\mathbb{Z}[e^{2\pi i/p}]$ a mitjans del segle XIX, tot i que, van aparèixer breument abans en la teoria de formes quadràtiques per Gauss. Kummer va demostrar que si p no divideix l'ordre del nombre de classes de $\mathbb{Z}[e^{2\pi i/p}]$ l'equació de Fermat $x^p+y^p = z^p$ no tenia solucions no trivials.

En el capítol 3, introduïm el concepte de divisors i el grup de classes de divisors relacionat amb geometria aritmètica que relaciona cossos de trascendència 1 amb corbes algebraiques (veiem [Lor] Capítol 10). Veurem com aquest darrer grup esta relacionat amb el grup que hem treballat anteriorment, per certs anells de Dedekind dins un cos global de característica positiva. Parlarem de les S-unitats i veurem la seva relació directa amb la clausura entera d'un cert domini de Dedekind.

Finalment, en el capítol 4 estudiarem la conjectura de Brumer-Stark en un cassos particulars en l'estudi del grup de classes como un $\mathbb{Z}$-mòdul de Galois, i el capítol 5 mostrant fòrmules pel càlcul del nombre de classes en uns exemples concrets, relacionats amb extensions abelianes.

Per acabar la introducció i donar una raó inicial de l'analogia entre (i) i (ii) de la definició 1.1, tenim l'anàleg del Teorema d'Euler en el cas de $F_q[T]$.

Lema 1.1 *Sigui $A = \mathbb{F}[T]$. Si $f \in A, f \neq 0$, i $a \in A$ és relativament primer amb f, llavors*

$$a^{\phi(f)} \equiv 1 \, (mod\, f),$$

on $\phi(f)$ està definit com el nombre d'elements en el grup $(A/fA)^*$ o, alternativament, el nombre de polinomis diferents del zero de grau inferior a grau(f) i relativament primer amb f.[1]

Demostració. El grup $(A/fA)^*$ té $\phi(f)$ elements. La classe lateral de a mòdul f, $\bar{a}$, cau en aquest grup. Per tant, $\bar{a}^{-\phi(f)} = \bar{1}$, i això és equivalent a la congrüencia que tenim a la proposició.

□

[1] Per veure una fòrmula explícita de $\phi(f)$ veure pàgina 5, Proposició 1.7 de [Ros]

2 Grup de classes d'ideals

L'objectiu d'aquesta secció serà definir que és un grup de classes d'ideals per a dominis de Dedekind i demostrarem que és finit en el cas del cossos de funcions sobre $\mathbb{F}_q(T) = \mathbb{F}(T)$, on tenim que $q = p^r$, p primer i $r \in \mathbb{N} \geq 1$. Per a demostrar-ho introduïm conceptes previs que dividirem en 4 subseccions: clausura entera i domini de Dedekind, factorització única d'ideals i ramificacions, norma d'un ideal, i finalment valoracions i anàlisi no arquimedià.

2.1 Clausura entera i dominis de Dedekind

De manera general, en aquesta secció treballarem amb la següent tripleta: Sigui A un domini commutatiu amb unitat, K el seu cos de fraccions i sigui L/K una extensió finita. Llavors la clausura entera B de A en L és un domini B associat de manera canònica a la tripleta (A,K,L) tal que B $\subseteq$ L i tal que L és el cos de fraccions de B, definit via $B = \{\alpha \in L \mid Irr(\alpha, K)[x] \in A[x]\}$ (veure demostració [Lor], pàgina 15, Proposició 2.19, part (i)), on $Irr(\alpha, K)[x]$ és un polinomi irreductible de α sobre $K[x]$.

Definim ara els conceptes element enter, clausura entera i enterament tancat.

Definició 2.1.1 *Sigui A un subanell d'un cos L. Un element α de L s'anomena enter sobre A si és arrel d'un polinomi mònic $f(y)$ en $A[y]$.*

Fet: *Sigui A un subanell d'un cos L. La clausura entera B de A en L és el domini dins L format per elements de L enters sobre A.*

Definició 2.1.2 *Un domini A amb cos de fraccions K, s'anomena integrament tancat si la seva clausura entera de A en K és A.*

Ara enunciarem una proposició i un corol·lari que ens permetran veure que la clausura entera és enterament tancada i que conté una base del K-espai vectorial L.

Proposició 2.1.1 *Sigui A un domini. Sigui K el seu cos de fraccions. Sigui L/K una extensió finita. Sigui B la clausura entera de A en L. Aleshores:*

(i) Sigui $\alpha \in L$. Llavors, existeix $b \in B$ i $a \in A$ tal que $\alpha = b/a$. En particular, L és el cos de fraccions de B.

(ii) B és integrament tancat.

Demostració.

(i) Sigui $\alpha \in L$. Sigui $g(y) \in K[y]$ el seu polinomi mínim. Com K és el cos de fraccions de A, podem escriure:

$$g(y) = y^n + \frac{c_{n-1}}{d_{n-1}} y^{n-1} + ... + \frac{c_0}{d_0}, on\ c_i, d_i \in A, d_i \neq 0, \forall i = 0, ..., n-1$$

Sigui ara $d := \prod_{i=0}^{n-1} d_i$. Com $d^n g(\alpha) = 0$, tenim que

$$(d\alpha)^n + \frac{c_{n-1}}{d_{n-1}} d(d\alpha)^{n-1} + ... + \frac{c_0}{d_0} d^n = 0.$$

Per construcció tenim que $(\frac{c_i}{d_i})d \in A, \forall i = 0, ..., n-1$, així doncs l'equació anterior ens dona una relació entera per $d\alpha$ sobre A. Per tant, $b := d\alpha \in B$, i $\alpha = b/d$, amb $b \in B$ i $d \in A$.

(ii) Això es demostra fàcilment si tenim tres dominis A,B,C amb A $\subseteq$ B $\subseteq$ C, on es té C és enter sobre A si i només si C és enter sobre B i B és enter sobre A. Com que B és la clausura entera de A en L i L és el cos de fraccions de B, B és integrament tancat.

□

Corol·lari 2.1.1 *Sigui A un domini. Sigui K el seu cos de fraccions. Sigui L/K una extensió finita de grau n. Sigui B la clausura entera de A en L. Llavors B conte una base $\{e_1, ..., e_n\}$ del K-espai vectorial L.*

Demostració. Sigui $(f_1, ..., f_n) \in L$ una base qualsevol de L sobre K. Per l'apartat (i) de la proposició anterior, tenim que podem trobar $c_1, ..., c_n$ en A i $e_1, ..., e_n$ en B tal que $f_i := e_i/c_i, \forall i = 1, ..., n$. Llavors, $(e_1, ..., e_n)$ és una base de L continguda en B. □

Exemple 2.1.1 *Veiem que $\mathbb{Z}$ és integrament tancat en $\mathbb{Q}$: per veure això agafem un element qualsevol de $\mathbb{Q}$ que sigui enterament tancat sobre $\mathbb{Z}$, i ho expressem de forma reduïda tal que sigui de la forma a/b, on $a, b \in \mathbb{Z}$ són relativament primers. Llavors,*

$$(\frac{a}{b})^n + z_1\frac{a}{b}^{n-1} + \cdots + z_n = 0$$
$$a^n + z_1a^{n-1}b + \cdots + z_nb^n = 0$$

i la darrera equació implica que b divideix a^n. Per tant, $b = \pm 1$, i per tant, per tot $a \in \mathbb{Z}$ tenim que és enter sobre $\mathbb{Z}$, verificant el que volíem.

De manera anàloga veiem que $\mathbb{F}[T]$ és integrament tancat en $\mathbb{F}(T)$: per veure això agafem un element qualsevol de $\mathbb{F}(T)$ que sigui α enter sobre $\mathbb{F}[T]$. Escrivim α per p/q, on $p, q \in \mathbb{F}[T]$ són relativament primers. Llavors,

$$(\frac{p}{q})^n + h_1\frac{p}{q}^{n-1} + \cdots + h_n = 0$$
$$p^n + h_1p^{n-1}q + \cdots + h_nq^n = 0$$

i de la darrera equació s'obté que q divideix p^n. Per tant com que p i q són relativament primers, $q = 1$, i per tant, $p \in \mathbb{F}[T]$ obtenim que és enter sobre $\mathbb{F}[T]$, verificant el que volíem.

Exemple 2.1.2 *Considerem $f(x, y) = y^2 - x^3 \in \overline{k}(x)[y]$, on k cos, $\overline{k}$ la seva clausura algebraica, $\overline{k}[x]$ l'anell de polinomi en x amb coeficients a $\overline{k}$, $\overline{k}(x)$ el cos de fraccions de $\overline{k}[x]$, $\overline{k}[x, y]$ l'anell de polinomis en x, y amb coeficients a $\overline{k}$, i $\overline{k}(x)[y]$ l'anell de polinomis en y amb coeficients en $\overline{k}(x)$. Podem veure que $f(x, y)$ és irreductible a $\overline{k}(x)[y]$, ja que, com un polinomi en y amb coeficients en $\overline{k}[x]$ observem la descomposició*

$y^2 - x^3 = (y - g_1(x))(y + g_2(x)), g_1(x), g_2(x) \in \overline{k}[x]$, *amb* $grau(g_1(x)) = 1$ *o* 2 *i* $grau(g_2(x)) = 2$ *o* 1.

Seguint aquest raonament, s'observa que $g_1(x) = g_2(x)$ cosa que no pot ser, ja que $g_1^2(x) \neq x^3, g_1 \in \overline{k}[x]$. Per tant, és irreductible sobre $\overline{k}[x][y]$ pel lema de Gauss. Denotem per $A = \overline{k}[x]$,$K = \overline{k}(x)$, i $L = \overline{k}(x)[y]/(f) = K[y]/(f(x))$.

Tenim ara el domini $C_f := \overline{k}[x, y]/(f)$ dins el cos L. Podríem pensar que C_f és la clausura entera de A en L, però veurem que C_f no és integrament tancat en L, i per tant, no és la clausura entera per la Proposició 2.1.1.

En C_f tenim que $y^2 - x^3 = 0$, i per tant, en L,

$$x^2((y/x)^2 - x) = 0.$$

Com que $x \neq 0$ en L, trobem $(y/x)^2 - x = 0$. Així podem veure que l'element y/x és enter sobre $\overline{k}[x]$. Demostrem que $y/x \notin C_f$. És suficient veure $y = xg(x, y) + h(x, y)f(x, y)$ no té solucions en $\overline{k}[x, y]$, ja que, si $y/x \in C_f$, $y/x = g(x, y)\ mod(C_f)$, llavors $y = xg(x, y) + h(x, y)f(x, y)$. Substituint f(x,y)=0 en C_f i

$$y = y^2h(x, y) + x(g(x, y) - x^2h(x, y)) \Rightarrow h = g/x^2, (\ en\ \ C_f)$$

obtenim

$$y^2g(x, y)/x^2 = y \Rightarrow g(x, y) = x^2/y \notin \overline{k}[x, y].$$

Ara com que C_f és un domini d'integritat, podem buscar la clausura entera en el seu cos de fraccions L. Substituim $x = t^2$,$y = t^3$, tenim que C_f és isomorf a $\overline{k}[t^2, t^3]$, amb cos de fraccions $\overline{k}(t)$. Això és a causa de que $1/t = t^2/t^3 = x/y$. Però com que $\overline{k}[t]$ és un domini de factorització única, tenim que és integrament tancat en $\overline{k}(t)$ (Proposició 2.1.1). Així, la clausura entera serà $\overline{k}[t] = \overline{k}[y/x]$. I com que $\overline{k}[y/x]$ té com a cos de fraccions L, i $\overline{k}[y/x]$ és enterament tancat, concloem que $\overline{k}[y/x]$, on $y^2 = x^3$, és la clausura entera de $\overline{k}[x]$ en L.

Amb el darrer exemple, podem notar que hi ha una relació entre la no-singularitat d'una corba[2] i com serà la seva clausura entera relacionada.

Teorema 2.1.1 *Sigui $f \in \overline{k}[x, y]$ un polinomi irreductible. L'anell $C_f := \overline{k}[x, y]/(f)$ és integrament tancat si i només si $f(x, y) = 0$ és no singular, és a dir, no té cap punt singular.*

Exemple 2.1.3 *Un altre exemple utilitzant la mateixa notació que a l'exemple anterior. Sigui ara $f(x, y) = y^2 - x^3 - x^2$. Tenim que és irreductible pel criteri d'Eisentein amb x+1, ja que, x+1 és primer en $\overline{k}[x]$ i divideix $x^3 + x^2$ amb multiplicitat 1. Sigui $C_f := \overline{k}[x, y]/(f)$ com abans. La relació*

$$x^2((y/x)^2 - (x + 1)) = 0$$

en L demostra que $(y/x)^2 - (x + 1) = 0$ i, per tant, que y/x és un element enter en L sobre $\overline{k}[x]$. Fent un raonament similar al de l'exemple anterior, podem veure que C_f no serà la clausura entera de $\overline{k}[x]$ en L.

Ara considerem les inclusions $C_f \subset C_f[x][y/x] \subset L$. Per definició, L és el cos de fraccions de C_f, així L és també el cos de fraccions de $\overline{k}[x][y/x]$.En L, C_f és el subanell generat per $\overline{k}$,$\overline{x}$ i $\overline{y}$. Com que $(\overline{y}/\overline{x})^2 = \overline{x} + 1$ i $(\overline{y}/\overline{x})\overline{x} = \overline{y}$, trobem que $C_f[x][y/x] = \overline{k}[x][\overline{y}/x]$, el subanell de L generat per $\overline{k}$,x i $\overline{y}/x$.

Com que $\overline{k}[x][y/x]$ és un domini de factorització única amb cos de fraccions L, tenim que $\overline{k}[x][y/x]$ és enterament tancat en L. Com tot element de $\overline{k}[x][\overline{y}/x], y^2 = x^3 + x^2$ és enter sobre $\overline{k}[x]$, trobem que

$$\overline{k}[x] \subseteq C_f \subseteq \overline{k}[x][\overline{y}/x] \subseteq \textit{clausura entera de } \overline{k}[x] \textit{ en } L.$$

Com que $\overline{k}[x][y/x]$ és integrament tancat, podem concloure que $\overline{k}[x][\overline{y}/x]$ és la clausura entera de $\overline{k}[x]$ en L.

Ara que ja hem definit el terme clausura integral, volem definir el terme domini de Dedekind, però abans d'això, caldrà que introduïm dos conceptes prèviament: noetherià i dimensió de Krull.

Definició 2.1.3 *Sigui I un ideal en un domini commutatiu A, diem que I està finitament generat si existeix un nombre finit d'elements $c_1, ..., c_r$ en I tal que:*

$$I = \{a_1c_1 + ... + a_rc_r | a_i \in A, i = 1, ..., r\}.$$

Observació: *Observem que en el cas $r = 1$, correspon a ideals principals.*

Definició 2.1.4 *Un domini commutatiu noetherià A és un domini A tal que tot ideal de A està finitament generat.*

Abans de parlar de la dimensió de Krull, enunciarem i demostrarem un teorema sobre dominis noetherians, però necessitem un parell de proposicions per a demostrar-ho.

Definició 2.1.5 *Sigui A un domini. Un A-mòdul M de A s'anomena noetherià si tot submòdul és finitament generat.*

Proposició 2.1.2 *Sigui A un domini noetherià. Llavors tot submòdul M d'un A-mòdul[3] finitament generat és finitament generat, és a dir, és noetherià.*

[2] $f(x, y) = 0$, $(a, b) \in k^2$ és un punt singular si i només si $\frac{\partial f}{\partial x}(a, b) = \frac{\partial f}{\partial y}(a, b) = 0$

[3] Remarquem que si A és un cos llavors un A-mòdul és un espai vectorial.

La demostració de la darrera proposició no la emularem aquí, però la podem trobar a [Lor], pàgina 26, o la podem veure de la definició anterior.

Proposició 2.1.3 *Sigui A un domini, integrament tancat en el seu cos de fraccions K. Sigui L/K una extensió separable de grau n. Sigui B la clausura entera de A en L.Sigui $\{e_1, ..., e_n\} \subset B$ una base per L sobre K. Aleshores existeix un element no nul $d \in A$ tal l'A-mòdul B està contingut en el A-mòdul lliure generat per $e_1/d, ..., e_n/d$; és a dir,*

$$Ae_1 \oplus ... \oplus Ae_n \subseteq B \subseteq Ae_1/d \oplus ... \oplus Ae_n/d \subseteq L.$$

Demostració. Existeix una base $(e_1, ..., e_n) \subset B$ de L sobre K (veiem Corol·lari 2.1.1). Sigui $\alpha \in B$ un element qualsevol. Aquest element es pot expressar de manera única de la següent forma

$$\alpha = x_1e_1 + ... + x_ne_n, \ amb \ x_i \in K$$

Sigui $d \in A$ un element no nul. Escrivim

$$\alpha = dx_1(e_1/d) + ... + dx_n(e_n/d).$$

Hem de veure l'existència d'un element no nul d tal que $dx_i \in A, \forall i = 1, ..., n$, independent de l'element α triat de B. Fixem una clausura algebraica $\overline{K}$ de K. L'extensió L/K és separable per hipòtesis. Siguin $\sigma_1, ..., \sigma_n$ els diferents n embeddings de L en $\overline{K}$(n el grau de l'extensió). Sigui $M := (\sigma_i(e_j))_{1 \leq i,j \leq n}$. Considerem les següents relacions

$$\begin{pmatrix} \sigma_1(\alpha) \\ \cdot \\ \cdot \\ \cdot \\ \sigma_n(\alpha) \end{pmatrix} = (\sigma_i(e_j))_{1 \leq i,j \leq n} \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = M \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix}.$$

Sigui ara M^* la matriu d'adjunts de M. Per construcció,

$$M^* \begin{pmatrix} \sigma_1(\alpha) \\ \cdot \\ \cdot \\ \cdot \\ \sigma_n(\alpha) \end{pmatrix} = M^*M(\sigma_i(e_j))_{1 \leq i,j \leq n} \begin{pmatrix} x_1 \\ \cdot \\ \cdot \\ \cdot \\ x_n \end{pmatrix} = \begin{pmatrix} det(M)x_1 \\ \cdot \\ \cdot \\ \cdot \\ det(M)x_n \end{pmatrix}$$

Com les entrades de M^* són els $(n-1) \times (n-1)$ menors de M, aquests són enters sobre A. Com $\alpha \in B$, cada $\sigma_i(\alpha), i = 1, ..., n$, és enter enter sobre A. Per tant, cada element $det(M)x_i$ és enter sobre A.

Tenim que det(M) és enter sobre A, ja que, tenim que $det : M_n(B) \to B$, per tant $det(M) \in B$ i així és enter sobre A, però det(M) no necessàriament és un element de K. Així, det(M) pot no ser enter sobre K. Sense pèrdua de generalitat, suposem que L està contingut en $\overline{K}$, i que cada embedding σ_i és la restricció en L d'un automorfisme τ_i en $\overline{K}$. Aleshores, per tot automorfisme τ de $\overline{K}$ tal que $\tau_{|K} = id_{|K}$, existeixen $i \in \{1, ..., n\}$ tal que $\tau_{|L} = \sigma_i$. Sota aquestes condicions extra, podem trobar que $\tau_i(det(M)) = \pm det(M)$, ja que, aplicant un automorfisme τ_i sobre la matriu M permuta les seves col·lumnes. Això indica que det(M) pot no pertanyer a K. Però l'element $d := det(M)^2$ existeix a K, ja que, és invariant sota tots els automorfismes τ de $\overline{K}$ tal que $\tau_K = id_K$. Com A és integrament tancat i d existeix en K i és enter sobre A, tenim que d és un element de A. Així veiem que l'element dx_i existeix en K. L'element dx_i també és enter sobre A, ja que, $d_i = det(M) \cdot (det(M)x_i)$. Per tant, com A és enterament tancat, $dx_i \in A, \forall i = 1, ..., n$. Ara, cal veure que $d \neq 0$. Per teoria de Galois, sabem que $\{e_1, ..., e_n\}$ és una base per L/K, i per tant, $det(M) \neq 0$. Així, veiem que aquest $d \neq 0$, és l'element buscat en l'enunciat. □

Teorema 2.1.2 *Sigui A un domini noetherià, integrament tancat en el seu cos de fraccions K. Sigui L/K una extensió finita separable. Llavors la clausura entera B de A en L és un A-mòdul finitament generat. En particular, B és un anell noetherià.*

Demostració. Per la proposició 2.1.2 demostra que per veure que B és un A-mòdul finitament generat, és suficient veure que B és un A-submòdul d'un A-mòdul finitament generat. Això queda demostrat a la proposicio 2.1.3.

□

La noció que introduirem a continuació és una manera de mesurar la complexitat d'un anell commutatiu amb unitat. Ens centrarem principalment en treballar amb dimensió 1.

Definició 2.1.6 *Sigui R un anell commutatiu amb unitat. Una cadena d'ideals primers de longitud n en R és un conjunt de n+1 ideals primers diferents $P_0, ..., P_n$ de R tal que $P_n \subset ... \subset P_1 \subset P_0$. L'altura d'un ideal primer P, ht(P), és el suprem de les longituds de les cadenes de primers en R amb $P_0 = P$. La dimensió de Krull de R es defineix com*

$$dim\, R := sup\{ht(P) \mid P\, ideal\, primer\, de\, R\}$$

En aquest treball, ens referirem a la dimensió de Krull de R simplement com la dimensió de R. Podem veure que un domini d'integritat R té dimensió 1 si i només si R conté un ideal primer diferent del cero i tot ideal primer diferent del cero de R és maximal.

Proposició 2.1.4 *Sigui A un domini de dimensió 1. Sigui B un domini que conté A i tal que cada element de B és enter sobre A. Llavors B té dimensió 1.*

Demostració. Sigui $\mathfrak{B}$ un ideal primer propi de B. Sigui $P = \mathfrak{B} \cap A$. Notem que $P \neq A$, ja que, $P \subseteq B$. L'ideal P és un ideal primer de A, perquè A/P s'injecta en B/$\mathfrak{B}$ i, per tant, A/P és un domini d'integritat.

Anem a veure que $P \neq (0)$. Sigui $\alpha \in \mathfrak{B}, \alpha \neq 0$. Com que α és enter sobre A, existeix un polinomi mònic $f(y) \in A[y]$ de grau mínim tal que

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + ... + a_1\alpha + a_0 = 0.$$

Afirmem que $a_0 \neq 0$. En efecte, si tenim que $a_0 = 0$, llavors

$$\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + ... + a_1) = 0.$$

Obtenint contradicció amb la minimalitat del grau de $f(y)$, i per tant, $a_0 \neq 0$. Llavors, tenim que $a_0 = -\alpha^n - ... - a_1\alpha \in \mathfrak{B}$, i trobem que $(0) \neq (a_0) \subset P$. Com que A té dimensió 1 per hipòtesis, un ideal primer diferent del zero P és maximal.

Ara veiem que $\mathfrak{B}$ és maximal, o equivalentment, veure que B/$\mathfrak{B}$ és un cos. El domini B/$\mathfrak{B}$ conté el cos A/P. Com tot element de B és enter sobre A, tot element de B/$\mathfrak{B}$ és enter sobre A/P. Sigui $0 \neq \gamma \in B/\mathfrak{B}$ un element diferent del cero. Hem de veure que γ és un element invertible en B/$\mathfrak{B}$. Tenim que

$$\gamma^n + c_{n-1}\gamma^{n-1} + ... + c_1\gamma + c_0 = 0$$

una relació entera sobre A/P per γ, de grau mínim. Argumentant com abans, tenim que $c_0 \neq 0$, ja que, si tenim que $c_0 = 0$ tindríem contradicció amb la minimalitat de la relació anterior. Així, $c_0 \neq 0$, i per tant, c_0 és invertible en A/P i podem escriure

$$\gamma(-c_0^{-1}\gamma^{n-1} - c_0^{-1}c_{n-1}\gamma^{n-2} - ... - c_0^{-1}c_1) = 1.$$

Per tant, γ és invertible, tal i com volíem veure. Així, B/$\mathfrak{B}$ és un cos, i, equivalentment, $\mathfrak{B}$ és maximal. □

Com a corol·lari de la proposició anterior, tenim el següent.

Corol·lari 2.1.2 *Sigui K el cos de fraccions d'un domini A de dimensió 1. Sigui L/K una extensió finita. Llavors, la clausura entera B de A en L té dimensió 1.*

Ara presentem la definició de domini de Dedekind, i un teorema sobre aquests i la clausura integral.

Definició 2.1.7 *Sigui A un domini d'integritat. L'anell A s'anomena domini de Dedekind si verifica les següents tres propietats:*

(i) A és noetherià.

(ii) A té dimensió (de Krull) 1.

(iii) A és integrament tancat.

Teorema 2.1.3 *Sigui A un domini de Dedekind. Sigui L/K una extensió finita separable del cos de fraccions K de A. Aleshores, la clausura entera B de A en L és un domini de Dedekind.*

Demostració. Apliquem el teorema 2.1.1, proposició 2.1.4, i l'apartat (ii) de la proposició 2.1.1. □

Exemple 2.1.4 *Anem a veure que $\mathbb{Z}$ i k[x], on k cos, són dominis de Dedekind. Ho veurem més en general, de fet, veurem que tot domini d'ideals principals és un domini de Dedekind.*

Observem que un domini d'ideals principals, és noetherià, ja que, en un domini d'ideals principals tot ideal es generat per un element i per tant, en particular, és finitament generat. Obviament té dimensió 1 perquè conté un ideal primer propi, i tot ideal primer en un domini d'ideals principals és maximal.

Així, només hem de veure que un domini d'ideals principals és enterament tancat, i per veure-ho, veurem que tot domini de factorització única és enterament tancat.

Sigui K el cos de fraccions del domini de factorització única A. Sigui $z \in K$ enter sobre A. Suposem que $z = a/b$, amb a,b elements coprimers en A. Així, com z és enter sobre A, a/b serà arrel d'un polinomi de la forma

$$(a/b)^n + m_{n-1}(a/b)^{n-1} + \cdots + m_1(a/b) + a_0 = 0, \text{ amb } m_i \in A.$$

Llavors

$$-a^n = b(m_{n-1}a^{n-1} + \cdots + m_1ab^{n-2} + a_0b^{n-1}).$$

Com A és un domini de factorització única, tot factor primer de c divideix b. Com b i c són coprimers, tenim que c és una unitat en A i, per tant, $z \in A$.

Així, tot domini d'ideals principals és un domini de Dedekind.

Observació: *Generalment un domini de Dedekind no és un domnini d'ideals principals. Per exemple, podem pensar $\mathbb{Z} \subset \mathbb{Q}$ amb $\mathbb{Q}(e^{\frac{2\pi i}{p}})/\mathbb{Q}$ una extensió finita, tenim que la clausura entera B de $\mathbb{Z}$ en $\mathbb{Q}(e^{\frac{2\pi i}{p}})$ quasi mai és un domini d'ideals principals, on $B = \mathbb{Z}[e^{\frac{2\pi i}{p}}]$ (podeu consultar [Was] Capítol 1).*

Proposició 2.1.5 *Sigui A un domini de Dedekind amb un nombre finit d'ideals primers, llavors és un domini d'ideals principals.*

Podem veure la demotració de la darrera proposició a [Lor], pàgina 29, Proposició 5.5. Acabem la secció amb una darrera proposició i un exemple.

Exemple 2.1.5 *Recordant els exemples 2.1.2 i 2.1.3, anem a veure quan $C_f = \overline{k}[x,y]/(f)$ és un domini de Dedekind, on k cos, $\overline{k}$ la seva clausura algebraica i f un polinomi irreductible en $\overline{k}[x,y]$. Per fer això, veurem quan és la clausura entera, que estarà relacionat amb la no-singularitat.*

Recordem notació: $A = \overline{k}[x]$, $K = \overline{k}(x)$, $L = \overline{k}(x)[y]/(f)$. Sigui $f(x,y) = y^n + a_{n-1}(x)y^{n-1} + \cdots + a_0(x) \in \overline{k}[x,y]$ irreductible. Anem a veure que C_f és la clausura entera de A en L si i només si f(x,y)=0 és no singular, és a dir, no te cap punt singular. És directe que tot element de C_f és enter sobre $\overline{k}[x]$, ja que, tot element de C_f verifica una relació entera. Per tant, només queda veure que C_f és la clausura entera de A en L si i només si C_f és integralment tancat en L. Ara apliquem el Teorema 2.1.1, i així, si f(x,y)=0 és no singular tenim que serà integralment tancat, i

per tant, serà la clausura entera de A.

Aplicant el teorema 2.1.3, si A és un domini de Dedekind, aleshores C_f és un domini de Dedekind si i només si f(x,y)=0 és no singular (f irreductible en $\overline{k}[x,y]$).

2.2 Factorització única d'ideals i ramificacions

En aquesta secció, introduïrem la propietat de factorització única d'ideals per ideals primers i el concepte de ramificació.

Definició 2.2.1 *Un domini d'integritat R diem que té la propietat de factorització única d'ideals si tot ideal propi $I \subseteq R$ es pot escriure com $I = \mathfrak{P}_1, ..., \mathfrak{P}_s$, on $\mathfrak{P}_i, i = 1, .., s$ és un ideal primer de R, i aquesta factorització és única, llevat de permutacions(i multiplicacions d'unitats en R).*

A continuació, enunciem el següent teorema d'àlgebra commutativa. I la demostració es pot trobar a [Lor] a la pàgina 91, Teorema 2.8.

Teorema 2.2.1 *Sigui R un domini noetherià de dimensió (de Krull) 1. L'anell R és un domini de Dedekind si i només si R té la propietat de factorització d'ideals única.*

Observació: *A vegades, per aquesta propietat s'anomenen "primers ideals"de l'anell R als ideals primers.*

Fixem-nos que, amb les hipòtesis que tenim al teorema 2.2.1, només cal veure que un domini noetherià de dimensió 1 té la propietat de factorització d'ideals única si i només si és integrament tancat.

Abans de parlar del concepte de ramificació, cal comentar que utilitzarem diverses vegades l'eina de la localització, i donarem per conegudes certes propietats o resultats. Podeu consultar la informació necessària a diferents llibres com a la secció II.6 de [Lor], al llarg de [AtiMac], a la secció I.1 de [Lan] i/o al Capítol 6 de [Kem].

Sigui A un domini de Dedekind i denotem per K el seu cos de fraccions. Sigui B la clausura entera de A en una extensió finita L de K. Suposarem que B és A-mòdul finitament generat, o equivalentment, que la extensió L/K és separable (Teorema 2.1.1). Anem a estudiar la relació entre ideals de A amb els de B, i la seva factorització en ideals primers diferents del zero, en aquesta situació es té $A = B \cap K$.

Lema 2.2.1 *Sigui A un domini de Dedekind i denotem per K el seu cos de fraccions. Sigui B la clausura entera de A en una extensió finita L de K. Sigui P un ideal maximal de A. Aleshores $PB \neq B$.*

Demostració. Comencem en el cas que P és un ideal principal de A. Sigui p un generador de P. Suposem que PB = B. Llavors existeix $b \in B$ tal que $pb = 1$. Com que $P \neq A$, s'obté que $b \notin A$. Sigui $f(y) \in A[y]$ un polinomi mònic de grau mínim $n > 1$ tal que $f(b) = 0$. Escrivim $f(y) = y^n + a_{n-1}y^{n-1} + ... + a_0$. Com tenim que $pb = 1$, trobem que $pf(b) = b^{n-1} + a_{n-1}b^{n-2} + ... + a_0 p = 0$. Per tant, hem trobat una relació entera amb b sobre A amb un grau menor que n, contradient la minimalitat del grau n. Així, no pot existir un element com b, i per tant, $PB \neq B$.
Ara suposem que P no és principal. No podem argumentar com abans, però reduïm la nostra demostració al cas on P és principal utilitzant localització. Sigui $S := A \setminus P$, S és multiplicatiu per ser P primer. Llavors, $PB \neq B$ si i només si $S^{-1}PS^{-1}B \neq S^{-1}B$ ([AtiMac], pàgina 39, corol·lari 3.4). L'anell $A_P = S^{-1}A$ és un domini de Dedekind ([Lor], pàgina 63, corol·lari 6.20), llavors A_P és un domini d'ideals principals.[4] □

Com ara sabem que PB és un ideal propi en el domini de Dedekind B, podem factoritzar PB en un producte d'ideals maximals:

$$PB = M_1^{e_1} \cdots M_s^{e_s}, e_i \in \mathbb{Z}, e_i \geq 1,$$

[4] A_P té solament (0) i P com ideals primers, i utilizant la Proposició 2.1.5, obtenim el resultat.

i observem que $PM_i \cap A = P$.L'enter $e_{M_i/P} := e_i$ s'anomena **índex de ramificació** de M_i sobre P. I com que $M_i \cap A = P$, l'inclusió $A \subseteq B$ indueix l'injecció

$$A/P \to B/M_i, \text{ per a } i = 1, ..., s.$$

Com B és un A-mòdul finitament generat, el cos B/M_i és una extensió finita del cos A/P. Denotem per $f_{M_i/P} := [B/M_i : A/P]$ la dimensió de B/M_i com a (A/P)-espai vectorial. Quan no hi hagi confusió, escriurem $f_{M_i/P} = f_i$. Anem a definir més formalment.

Definició 2.2.2 *El cos A/P s'anomena el cos residual de A en P. El natural positiu $f_{M_i/P}$ s'anomena el grau residual de M_i sobre P.*

Ara enunciem i demostrem un resultat que relaciona el índexos de ramificació amb el grau n d'una extensió.

Teorema 2.2.2 *Sigui A un domini de Dedekind. Sigui L/K una extensió finita del cos de fraccions K de A. Sigui B la clausura entera de B en L. Si B és un A-mòdul finitament generat, llavors*

$$[L : K] = \sum_{M|PB} e_{M/P} f_{M/P}.$$

Demostració. Sigui $PB = \prod_{i=1}^{s} M_i^{e_i}$. Com els ideals $M_i^{e_i}, i = 1, ..., s$, son coprimers dos a dos, trobem que hi ha un isomorfisme d'anells

$$B/PB \cong \prod_{i=1}^{s} B/M_i^{e_i}.$$

Cada un dels anells B/PB i $B/M_i^{e_i}, i = 1, ..., s$, també poden ser considerats com (A/P)-espais vectorials. Per demostrar el teorema, veurem que:

(i) $dim_{A/P}(B/PB) = [L : K]$, i que

(ii) $dim_{A/P}(B/M_i^{e_i}) = e_i \cdot dim_{A/P}(B/M_i) = e_i f_i, \forall i = 1, ..., s.$

Primer farem la demostració de les dues afirmacions quan A i B són dominis d'ideals principals. Com B és A-mòdul finitament generat sense torsió, per teoria d'estructura de mòduls sobre dominis d'ideals principals tenim que B és un A-mòdul lliure de rang $n := [L : K]$ (és a dir, $B = A^n$). Sigui π un generador del ideal P en A. Llavors:

$$B/PB \cong (A \oplus \cdots \oplus A)/(\pi A \oplus \cdots \oplus \pi A) \cong (A/P)^n.$$

Per tant, el (A/P)-espai vectorial B/PB té dimensió n sobre A/P.

Assumim ara que $P \subseteq M^e$, tal que B/M^e és un (A/P)-espai vectorial. Ara procedim per inducció sobre e de M, per a obtenir

$$dim_{A/P}(B/M^e) = e \cdot dim_{A/P}(B/M).$$

Per al cas $e = 1$ és clar. Ara considerem la seqüencia exacta de (A/P)-espais vectorials:

$$0 \to M^{e-1}/M^e \to B/M^e \to B/M^{e-1} \to 0.$$

Per propietats de successions exactes i hipòtesi d'inducció:

$$\begin{aligned} dim_{A/P}(B/M^e) &= dim_{A/P}(B/M^{e-1}) + dim_{A/P}(M^{e-1}/M^e) \\ &= (e-1) dim_{A/P}(B/M) + dim_{A/P}(M^{e-1}/M^e). \end{aligned}$$

Per a concloure la demostració demostrem que M^{e-1}/M^e és un (B/M)-espai vectorial de dimensió 1 o, equivalentment, un (A/P)-espai vectorial de dimensió $dim_{A/P}(B/M)$. Sigui m un generador de l'ideal maximal M de B que conté P. L'aplicació natural

$$\begin{aligned} \nu : B &\to M^{e-1}/M^e \\ 1 &\to [m^{e-1}], \end{aligned}$$

on $[m^{e-1}]$ és la classe de m^{e-1}, és exhaustiva e indueix un isomorfisme de (B/M)-espais vectorials: $\nu' : B/M \to M^{e-1}/M^e$. Per tant, $dim_{B/P}(M^{e-1}/M^e) = 1$, i l'afirmació (ii) està demostrada quan A i B són dominis d'ideals principals.

Sigui A un domini de Dedekind qualsevol. Sigui $S := A\backslash P$. El conjunt S és un conjunt multiplicatiu en A i B. Com A és un domini de Dedekind, l'anell $S^{-1}A = A_P$ és un domini d'ideals principals, amb cos de fraccions K (Proposició 2.1.5). Aplicant el corol·lari 6.19 de la pàgina 63 de [Lor], obtenim que la clausura entera de A_P en L és l'anell $S^{-1}B$. Com que $M_1, ..., M_s$ són els únics ideals maximals de B que no intersecten amb S, trobem que $S^{-1}B$ és un domini de Dedekind que té només un nombre finit d'ideals maximals. Així, $S^{-1}B$ és un domini d'ideals principals, per la Proposició 2.1.5. A més, com els ideals $S^{-1}M_i, i = 1, ..., s$, son ideals propis maximals en $S^{-1}B$, concloem que

$$(S^{-1}P)(S^{-1}B) = \prod_{i=1}^{s}(S^{-1}M_i)^{e_i}$$

és la factorització de $(S^{-1}P)(S^{-1}B)$ en $(S^{-1}B)$. Per tant, com tant $(S^{-1}B)$ i $(S^{-1}A)$ són dominis d'ideals principals, aplicant l'argument anterior obtenim la següent igualtat:

$$[L : K] = \sum_{i=1}^{s} e_i f_i',$$

on $f_i' := dim_{(S^{-1}A/S^{-1}P)}(S^{-1}B/S^{-1}M_i)$. Llavors, per un resultat de localitzacions es demostra que A/P i $S^{-1}A/S^{-1}P$ són isomorfs. Així, obtenim

$$[L : K] = \sum_{i=1}^{s} e_i f_i.$$

□

Teorema 2.2.3 *Sota les hipòtesis del Teorema 2.2.2 i suposem, a més, L/K és Galois, llavors donat P ideal primer de A, $PB = M_1^{e_1} \cdots M_s^{e_s}$, es té $e_1 = \cdots = e_s$ i $f_1 = \cdots = f_s$, i per tant, $[L : K] = s \cdot e_1 \cdot f_1$.*

Podeu trobar una desmostració del teorema anterior a la pàgina 116, Teorema 8.1, [Lor].

Definició 2.2.3 *Sigui L/K una extensió finita. Sigui A un domini de Dedekind amb cos de fraccions K. Denotem per B la clausura entera en L. Suposem que B és un A-mòdul finitament generat. Sigui M un ideal maximal de B. Sigui $P := M \cap A$. L'ideal M és ramificat sobre P (o sobre A) si $e_{M/P} > 1$ o l'extensió B/M no és separable sobre A/P. Si l'ideal M no és ramificat sobre P, llavors diem que és no-ramificat sobre P (o sobre A).*
Un ideal maximal P de A ramifica en B si PB està contingut en un ideal maximal M de B que és ramificat sobre A. Quan no hi ha cap ideal maximal de B ramificat sobre A, l'extensió B/A s'anomena no-ramificada.

Ara presentem un parell d'exemples.

Exemple 2.2.1 *Sigui $f(t) = t^3 - 9t - 6$ polinomi irreductible sobre $\mathbb{Q}[x]$, i sigui α una arrel de f(t) que pensem dins de $\mathbb{C}$, com tots els cossos els pensem sobre $\mathbb{C}$ en aquests exemples d'aquesta subsecció. Denotem $K = \mathbb{Q}(\alpha)$, on $K/\mathbb{Q}$ no és de Galois. Observem $6 = \alpha^3 - 9\alpha = \alpha(\alpha-3)(\alpha+3)$. Per $m \in \mathbb{Z}$, $\alpha+m$ té el polinomi mínim $f(t-m) \in \mathbb{Q}[t]$, així $N_{K/\mathbb{Q}}(\alpha+m) = -f(-m) = m^3-9m+6$ (veurem aquest concepte de norma en la següent secció) i l'ideal principal $\alpha - m$ té norma*

$$N(\alpha - m) = |m^3 - 9m + 6|.$$

Per tant, $N(\alpha) = 6, N(\alpha-3) = 6$, i $N(\alpha+3) = 6$. Com té dos primers a $\mathbb{Z}$ que divideix la norma, ha de succeir que $(\alpha) = \mathfrak{p}_2\mathfrak{p}_3$, $(\alpha-3) = \mathfrak{p}_2'\mathfrak{p}_3$, i $(\alpha+3) = \mathfrak{p}_2'\mathfrak{p}_3$. Així

$$(2)(3) = (6) = (\alpha)(\alpha-3)(\alpha+3) = \mathfrak{p}_2\mathfrak{p}_2'^2\mathfrak{p}_3^3,$$

per tant, $(2) = \mathfrak{p}_2^2\mathfrak{p}_3'$ i $(3) = \mathfrak{p}_3^3$. Per tant, 2 i 3 són ramificats en K.

Exemple 2.2.2 *Sigui p un primer senar, i* $\zeta = \zeta_p = e^{\frac{2\pi i}{p}}$ *una arrel p-éssima primitiva de l'unitat. Considerem el cos ciclotòmic* $K = \mathbb{Q}(\zeta)$*. A partir de que l'extensió* $K/\mathbb{Q}$ *és una extensió de Galois i utilitzant el discriminant d'una extensió, trobem la següent identitat*

$$p = (\zeta - 1)(\zeta^2 - 1)...(\zeta^{p-1} - 1),$$

i veure el fet que $(\zeta - 1)\mathscr{O}_K \cap \mathbb{Z} = p\mathbb{Z}$*. Podem veure que per tot enter i no divisible per p, podem trobar un enter j tal que* $ij \equiv 1(modp)$*, i per tant* $(\zeta^i - 1)/(\zeta - 1) = 1 + \zeta + ... + \zeta^{i-1} \in \mathbb{Z}[\zeta]$*, i la seva inversa* $(\zeta - 1)/(\zeta^i - 1) = (\zeta^i j - 1)/(\zeta^i - 1)$ *també està en* $\mathbb{Z}[\zeta]$*. Per tant, la fracció* $(\zeta^i - 1)/(\zeta - 1)$ *és una unitat en* $\mathbb{Z}[\zeta]$*. Conseqüentment,* $(\zeta^i - 1)$ *i* $(\zeta - 1)$ *generen el mateix ideal, ho denotem per* P_1*. Ara amb la igualtat anterior i el teorema 2.2.2, podem veure* $p\mathbb{Z}[\zeta] = P_1^{p-1}$ *i* P_1 *és un ideal primer. Per tant, podem veure que estem en el cas* $f_1 = 1$ *i* $e_1 = p - 1 = [K : \mathbb{Q}]$*.*

Aquest darrer exemple, ens permet escriure d'una manera alternativa el concepte totalment ramificat: un ideal propi primer P de A s'anomena totalment ramificat en L (o en B) si $PB = \mathfrak{p}^n$, per algun ideal primer $\mathfrak{p}$ de B, i $[L : K] = n$.

Per acabar aquesta secció presentem unes definicions relacionades amb la següent secció i que donaràn informació sobre els primers on ramifica L/K finita.

Definició 2.2.4 *Sigui A un domini commutatiu, i siguin* $f(y) := a_n y^n + \cdots + a_0$ *i* $g(y) := b_m y^m + \cdots + b_0$ *dos polinomis en A[y], amb* $a_n b_m \neq 0$*. La resultant de f i g és l'element de A*

$$Res(f,g) := det \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & \\ & a_n & a_{n-1} & \cdots & a_0 & \\ & & \ddots & & & \\ & & & a_n & a_{n-1} & a_0 \\ b_m & b_{m-1} & & \cdots & b_0 & \\ & \ddots & \ddots & & & \\ & & b_m & b_{m-1} & & b_0 \end{pmatrix}$$

Definició 2.2.5 *Sigui A un domini commutatiu, i sigui* $g(y) \in A[y]$ *un polinomi. Sigui* $g'(y)$ *la derivada de* $g(y)$ *en* $A[y]$*. La resultant de* $g(y)$ *i* $g'(y)$ *depèn només dels coeficients de* $g(y)$ *i s'anomena discriminant de* $g(y)$*. Ho denotem per disc(g).*

Proposició 2.2.1 *Sigui A un domini de Dedekind. Sigui* $f(y) \in A[y]$ *un polinomi mònic irreductible. Suposem que* $C_f := A[y]/(f(y))$ *és un domini de Dedekind. Llavors* $P \in Max(A)$*(conjunt ideals maximals de A) ramifica en* C_f *si i només si* $disc(f) \in P$*.*

Podem trobar la demostració de la darrera proposició a la pàgina 133, Proposició 1.2 del [Lor].

Definició 2.2.6 *Sigui A un domini de Dedekind. Sigui K el seu cos de fraccions. Sigui B la clausura entera de A en una extensió finita L/K. Sigui* $d_{B/A}$ *l'ideal de B generat per els elements de la forma* $f'(\alpha)$*, on f(y) és el polinomi mínim d'un element* $\alpha \in B$ *tal que* $L = K(\alpha)$*. Si l'extensió L/K no és simple, llavors definim* $d_{B/A} = (0)$[5]*. L'ideal* $d_{B/A}$ *s'anomena l'ideal diferent de B/A. Sigui* $\delta_{B/A}$ *l'ideal de A generat per els elements de la forma disc(f), on f(y) és el polinomi mínim d'un element* $\alpha \in B$ *tal que* $L = K(\alpha)$*. Si l'extensió L/K no és simple, llavors definim* $\delta_{B/A} = (0)$*.*

Proposició 2.2.2 *Sigui A un domini de Dedekind. Sigui K el seu cos de fraccions. Sigui B la clausura entera de A en una extensió finita i separable L/K. Llavors*

(1) Si $M \in Max(B)$ *és ramificat sobre A, llavors* $d_{B/A} \subseteq M$*.*

(2) Si $P \in Max(A)$ *ramifica en B, llavors* $\delta_{B/A} \subseteq P$*.*

Podem trobar la demostració de la darrera proposició a la pàgina 143, Proposició 5.2 del [Lor].

[5]Recordem que tota extensió L/K finita i separable és simple

Exemple 2.2.3 *Sigui $A = \mathbb{Z}$, i considerem l'extensió $\mathbb{Q}(\alpha)/\mathbb{Q}$, on $\alpha^4 + \alpha + 1 = 0$. Tenim que $f(x) = x^4 + x + 1 \in \mathbb{Z}[x]$ és mònic irreductible. Calculem el discriminant de f:*

$$disc(f) = det \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 4 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 1 \end{pmatrix} = 229.$$

Així per la Proposició 2.2.1 tenim que l'únic primer que ramifica és 229. Ara sigui B la clausura entera de A en L. Obtenim també que l'ideal diferent és $d = 4\alpha^3 + 1$, i $\delta = (229)$. Per la Proposició 2.2.2 un ideal primer P de A ramificarà en B si $229 \in P$, i un ideal primer M de B és ramificat en A si $(4\alpha^3 + 1) \subseteq M$.

2.3 Norma d'un ideal

Definició 2.3.1 *Sigui F un cos. Sigui R un F-espai vectorial de dimensió n. Sigui $r \in R$. Sigui $\mu_r : R \to R$, amb $x \mapsto \mu_r(x) := rx$, i així denotem l'aplicació "multiplicació per r". Fàcilment, l'aplicació μ_r és un morfisme de F-espais vectorials. L'aplicació*

$$\begin{aligned} Norm_{R/F} : & R \to F \\ & r \mapsto det(\mu_r), \end{aligned}$$

s'anomena (l'aplicació) norma de R a F.

Sigui A un domini de Dedekind, amb cos de fraccions K. Sigui L/K una extensió finita de grau n. Sigui B la clausura entera de A en L, i suposem que L/K és separable, és a dir, B és un A-mòdul finitament generat. Definirem:

$$N_{B/A} : I_B := \{ideals\ de\ B\} \to I_A := \{ideals\ de\ A\}$$

tal que, quan L/K sigui separable, compleixi que $\forall \alpha \in B$,

$$N_{B/A}(\alpha B) = N_{L/K}(\alpha)A.$$

Abans, donarem una expressió alternativa a l'aplicació norma en el cas que L/K sigui una extensió de Galois amb el grup de Galois $G = \{\sigma_1, ..., \sigma_n\}$: $N_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = Norm_{L/K}(\alpha)$ (de la definició 2.3.1). Aquesta darrera expressió de $N_{L/K}(\alpha)$ ens suggereix que definim pel cas Galois i per un ideal I de B:

$$N_{B/A}(I) := (\prod_{i=1}^{n} \sigma_i(I)) \cap A. \tag{1}$$

Proposició 2.3.1 *Sigui L/K una extensió de Galois. Sigui $\alpha \in B$. Llavors $N_{B/A}(\alpha B) = N_{L/K}(\alpha)A$.*

Demostració. Agafant l'expressió de $N_{B/A}(I)$ donada en (1) tenim:

$$N_{B/A}(\alpha B) = (\prod_{i=1}^{n} \sigma_i(\alpha)B) \cap A = (\prod_{i=1}^{n} \sigma_i(\alpha))B \cap A = N_{L/K}(\alpha)B \cap A.$$

Com que $N_{L/K}(\alpha) \in A$, obtenim $N_{L/K}(\alpha)B \cap A = N_{L/K}(\alpha)A$. □

Ara que ja hem vist un resultat que relaciona la norma que habíem definit, amb la que volem definir (la norma que porta ideals de B a ideals de A), i abans de continuar amb els lemes i resultat final, definim el concepte norma-ideal quan L/K no és de Galois.

Definició 2.3.2 *Considerem (A,K,B,L) com hem definit al principi. Definim l'aplicació norma-ideal $N_{B/A} : I_B \to I_A$, on I_R denota el conjunt d'ideals d'un domini de Dedekind R, via:*

(i) Si $\mathfrak{B} \in Max(B) := \{ideals\, maximals\, de\, B\}$, *llavors* $N_{B/A}(\mathfrak{B}) := (\mathfrak{B} \cap A)^{f_{\mathfrak{B}/\mathfrak{B}\cap A}}$.

(ii) Sigui $N_{B/A}(\mathfrak{B}_1^{a_1} \cdots \mathfrak{B}_r^{a_r}) := \prod_{i=1}^{r} N_{B/A}(\mathfrak{B}_i)^{a_i}$.

(iii) Sigui $N_{B/A}(B) := A$ *i* $N_{B/A}((0)) = (0)$.

L'aplicació $N_{B/A} : I_B \to I_A$ *definida així és multiplicativa. Quan no hi ha confusió, anomenarem l'aplicació norma-ideal simplement com aplicació norma.*

Notació 2.3.1 *(A,K,B,L) denota un A domini de Dedekind amb cos de fraccions K, L/K extensió finita i separable, B clausura entera de A en L amb B domini de Dedekind, i [L:K]=n.*

Lema 2.3.1 *Sigui (A,K,B,L) com abans. Sigui n el grau de L/K. Llavors la composició* $N_{B/A} \circ i_{B/A} : I_A \to I_B$ *és l'aplicació n-éssima potència en* I_A, *on* $i_{B/A}$ *és la inclusió d'un ideal de A en B via extensió.*

Demostració. És clar que $(N_{B/A} \circ i_{B/A})(0) = (0)$. Com ambdós $N_{B/A}$ i $i_{B/A}$ són aplicacions multiplicatives, només hem de veure, per demostrar el lema, que

$$\forall P \in Max(A), (N_{B/A} \circ i_{B/A})(P) = P^n.$$

Escrivim $i_{B/A}(P) = PB = \prod_{i=1}^{s} \mathfrak{B}_i^{e_i}$. Llavors

$$N_{B/A}(PB) = \prod_{i=1}^{s} N_{B/A}(\mathfrak{B}_i)^{e_i} = P^{\sum_{i=1}^{s} e_i f_{\mathfrak{B}_i/P}} = P^n.$$

□

Lema 2.3.2 *Siguin L/K i M/L dues extensions finites de cossos. Sigui A un domini de Dedekind amb cos de fraccions K. Sigui B (respectivament, C) la clausura entera de A en L (respectivament, en M). Suposem que B i C són A-mòduls finitament generats. Llavors* $N_{C/A} = N_{B/A} \circ N_{C/B}$.

Demostració. Com les aplicacions norma són multiplicatives, només hem de veure que, $\forall \mathfrak{B} \in Max(C)$,

$$N_{C/A}(\mathfrak{B}) = N_{B/A}(N_{C/B}(\mathfrak{B})).$$

Sigui $\mathfrak{B}_B := \mathfrak{B} \cap B$ i $\mathfrak{B}_A := \mathfrak{B} \cap A$. Per definició, $N_{C/A}(\mathfrak{B}) = \mathfrak{B}_A^{f_{\mathfrak{B}/\mathfrak{B}_A}}$, i així podem veure

$$N_{B/A}(N_{C/B}(\mathfrak{B})) = \mathfrak{B}_A^{f_{\mathfrak{B}/\mathfrak{B}_B} f_{\mathfrak{B}_B/\mathfrak{B}_A}}.$$

Per la multiplicitat de f en les torres, obtenim el resultat que volíem. □

Proposició 2.3.2 *Sigui (A,K,B,L) com abans. Llavors,* $\forall \alpha \in B$,

$$N_{L/K}(\alpha)A = N_{B/A}(\alpha B).$$

Demostració. Sigui M/L una extensió de Galois de L tal que M/K és també una extensió de Galois. Sigui C la clausura entera de A en M. Sigui $\alpha \in B$. Llavors

$$\begin{aligned} N_{C/A}(\alpha C) &= N_{B/A}(N_{C/B}(\alpha C)) \ (Lema\, 2.3.2) \\ &= N_{B/A}((\alpha B)^{[M:L]}) \ (Lema\, 2.3.1) \\ &= N_{B/A}(\alpha B)^{[M:L]}. \end{aligned}$$

Similarment, utilitzant la transitivitat de la norma, podem veure que $\forall \alpha \in B$,

$$N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha)) = N_{L/K}(\alpha^{[M:L]}) = N_{L/K}(\alpha)^{[M:L]}.$$

Com que M/K és de Galois, per la proposició 2.3.1, tenim que $N_{C/A}(\alpha C) = N_{M/K}(\alpha)A$. Per tant, concloem que

$$N_{B/A}(\alpha B)^{[M:L]} = (N_{L/K}(\alpha)A)^{[M:L]}.$$

Com que l'anell A té la propietat de la factorització única d'ideals (recordem que A és un domini de Dedekind), tenim que $N_{B/A}(\alpha B) = N_{L/K}(\alpha)A$. □

2.4 Valoracions i anàlisi no arquimedià

En aquesta secció introduirem el concepte de valoració i presentarem resultats de l'ànalisi no arquimedià. Ho farem de manera breu, referenciant al lector [Goss] Capítol 2 i/o [Lor] Capítol 5.

Comencem parlant de valoracions i valors absoluts.

Definició 2.4.1 *Sigui L un cos qualsevol. Una aplicació* $||: L \to \mathbb{R}^+$ *s'anomena un valor absolut de L si es verifiquen les següents tres condicions:*

(i) $|x| = 0$ *si i només si x=0.*

(ii) $|xy| = |x||y|, \forall x, y \in L.$

(iii) $|x + y| \leq |x| + |y|, \forall x, y \in L.$

Definició 2.4.2 *Sigui L un cos qualsevol. Una valoració de L és una aplicació* $\upsilon : L^* \to \mathbb{Z}$ *tal que es verifiquen les següents propietats:*

(i) $\upsilon(xy) = \upsilon(x) + \upsilon(y), \forall x, y \in L^*.$

(ii) $\upsilon(x + y) \geq min(\upsilon(x), \upsilon(y)), \forall x, y \in L^*.$

Extenem υ *a L definint* $\upsilon(0) := +\infty$.

Considerem una valoració en cossos globals, en particular correspon a la generalització del valor absolut p-àdic en $\mathbb{Q}$, definit per $\alpha = p^i \frac{n}{m} \in \mathbb{Q}$, on $(n, m) = 1$,$(n, p) = 1$,$(m, p) = 1$, via $|\alpha|_p = \frac{1}{p^i}$.

Exemple 2.4.1 *Valoració P-àdica: Sigui A un domini de Dedekind, i sigui K el seu cos de fraccions. Sigui* $P \subset A$ *un ideal maximal. Associem a P la valoració exhaustiva* $\upsilon_P : K^* \to \mathbb{Z}$ *que definida per* $x \in A$*, llavors escrivim la factorització de l'ideal (x) en A com*

$$(x) := \prod_{P \in Max(A)} P^{ord_P(x)}.$$

Definim $\upsilon_P(x) := ord_P(x)$*, quan* $x = a/b \in K, a, b \in A$*,* $b \neq 0$*, definim*

$$\upsilon_P(x) := \upsilon_P(a) - \upsilon_P(b).$$

És fàcil comprobar υ_P *satisfà la definició 2.4.2. Ara, quan A té quocients finits (ho definirem més endavant, però explicat de manera ràpida és quan* $\forall P \in Max(A)$*, el cos residual A/P és un cos finit), definim el valor absolut estandaritzat* $||_P$ *associat a* υ_P *com:*

$$\begin{aligned} ||_P :& K \to \mathbb{R}^+ \\ & x \mapsto |x|_P := |A/P|^{-\upsilon_P(x)}, if\, x \neq 0, \end{aligned}$$

i $||0||_P = 0$*. On* $|A/P|$ *denota la cardinalitat del cos A/P, que és finit quan A té quocients finits.*

Exemple 2.4.2 $\mathbb{Z}$ *i* $\mathbb{F}_q[t]$*, i les clausures integres en extensions finites i separables de* $\mathbb{Q}$ *i* $\mathbb{F}_q(t)$ *són de quocient finit. Per exemple,* $\mathbb{F}_5[t]$ *i agafem el polinomi mònic irreductible* $t^3 + t + 1$*, llavors si considerem l'ideal maximal* $(t^3 + t + 1)$*, obtenim el cos residual finit* $\mathbb{F}_5[t]/(t^3 + t + 1) \cong \mathbb{F}_{5^3}$ *amb cardinalitat 125.*

Sigui ara L/K una extensió finita, i sigui B la clausura entera de A en L. Suposem que B és un A-mòdul finitament generat. Com que B és un domini de Dedekind, volem associar a cada ideal maximal $\mathfrak{B}$ de B la valoració $\upsilon_{\mathfrak{B}} : L^* \to \mathbb{Z}$. Quan A té quocients finits, llavors B també té quocients finits, i associem a $\upsilon_{\mathfrak{B}}$ un valor absolut $\|\|_{\mathfrak{B}}$:

$$\begin{aligned} \|\|_{\mathfrak{B}} :& L \to \mathbb{R}^+ \\ & x \mapsto \| \, x \, \|_{\mathfrak{B}} := |B/\mathfrak{B}|^{-\upsilon_{\mathfrak{B}}(x)}, si\, x \neq 0, \end{aligned}$$

i $|0|_{\mathfrak{B}} = 0$. El valor absolut $\|\|_{\mathfrak{B}}$ és el que anomenem el valor absolut estandaritzat de L associat a $\mathfrak{B}$. Ara sigui, $P := \mathfrak{B} \cap A$, i sigui $PB = \prod_{\mathfrak{B}|P} \mathfrak{B}^{e_{\mathfrak{B}/P}}$. Definim

$$\begin{aligned} ||_{\mathfrak{B}} : & L \to \mathbb{R}^+ \\ & x \mapsto |x|_{\mathfrak{B}} := |A/P|^{-\frac{\upsilon_{\mathfrak{B}}(x)}{e_{\mathfrak{B}/P}}}, si\, x \neq 0, \\ & 0 \mapsto 0. \end{aligned}$$

Podem extendre el valor absolut de $||_{\mathfrak{B}}$ de L al valor absolut $||_P$ de K: $\forall x \in K, |x|_P = |x|_{\mathfrak{B}}$. De fet, si $x \in K$, llavors $\upsilon_{\mathfrak{B}}(x) = e_{\mathfrak{B}/P}\upsilon_P(x)$. Notem que

$$\|\|_{\mathfrak{B}} = (||_{\mathfrak{B}})^{e_{\mathfrak{B}/P} f_{\mathfrak{B}/P}}.$$

Per simplificar notació, definim $n_{\mathfrak{B}/P} := e_{\mathfrak{B}/P} \cdot f_{\mathfrak{B}/P}$.

Lema 2.4.1 *Sigui A un domini de Dedekind amb cos de fraccions K. Sigui L/K una extensió finita de grau n. Sigui B la clausura entera de A en L, i suposem que B és un A-mòdul finitament generat. Llavors*

(i) $\sum_{\mathfrak{B}|P} n_{\mathfrak{B}/P} = n = [L : K]$.

(ii) Sigui $x \in B$. *Llavors* $\upsilon_P(N_{L/K}(x)) = \sum_{\mathfrak{B}|P} f_{\mathfrak{B}/P}\upsilon_{\mathfrak{B}}(x)$.

(iii) Suposem que A té quocients finits. Sigui $x \in L$. *Sigui* $||_P$ *el valor absolut estandaritzat associat a* $P \in Max(A)$. *Llavors,* $|N_{L/K}(x)|_P = \prod_{\mathfrak{B}|P} |x|_{\mathfrak{B}}^{n_{\mathfrak{B}/P}}$.

Demostració. L'apartat (i) s'obté directament del teorema 2.2.2. Per veure l'apartat (ii), escrivim

$$(xB) := \prod_{P \in Max(A)} (\prod_{\mathfrak{B}|P} \mathfrak{B}^{\upsilon_{\mathfrak{B}|P}(x)}).$$

Per definició, $N_{B/A}(xB) = \prod_{P \in Max(A)} P^{\sum_{\mathfrak{B}|P} f_{\mathfrak{B}/P}\upsilon_{\mathfrak{B}}(x)}$. Com que $N_{B/A}(xB) = N_{L/K}(x)A$ per la proposició 2.3.2, ja tenim l'apartat (ii). Ara com els valors absoluts i les normes són funcions multiplicatives, és suficient demostrar l'apartat (iii) quan $x \in B$. Sigui $x \in B$. Utilitzant la factorització de (xB) i l'apartat (ii), trobem que

$$\prod_{\mathfrak{B}|P} |x|_{\mathfrak{B}}^{n_{\mathfrak{B}/P}} = |A/P|^{-\sum_{\mathfrak{B}|P} f_{\mathfrak{B}/P}\upsilon_{\mathfrak{B}}(x)} = |A/P|^{-\upsilon_P(N_{L/K}(x))} = |N_{L/K}(x)|_P.$$

Concloent la demostració de l'apartat (iii). □

Ara definirem quan un valor absolut és arquimedià o no, i acabarem enunciant la fòrmula del producte pel cas dels cossos numèrics, que no demostrarem aquí, però podem trobar la demostració a [Lor], pàgina 175, Proposició 7.7.

Definició 2.4.3 *Diem que un valor absolut* $||_\bullet$ *de K és un valor absolut no arquimedià quan satisfà a més la desigualtat*

$$|x + y|_\bullet \leq max(|x|_\bullet, |y|_\bullet), \forall x, y \in K,$$

on $||_\bullet$ *és un valor absolut associat a una valoració* υ *del cos K.*

Recordem la funció grau, $grau : k[x] \setminus \{0\} \to \mathbb{N}$, amb $f(x) \mapsto grau(f(x))$. Podem extendre aquesta funció a $k(x) \setminus \{0\}$ així: si $r(x) = p(x)/q(x)$ amb $p(x), q(x) \in k[x]$, i $grau(r(x)) := grau(p(x)) - grau(q(x))$. És clar que

$$\begin{aligned} grau(f \cdot g) &= grau(f) + grau(g) \\ grau(f + g) &\leq max(grau(f), grau(g)). \end{aligned}$$

Fixem $grau(0) = \infty$. Llavors, d'aquestes propietats podem veure que l'aplicació υ_∞ definida a continuació és una valoració de k(x):

$$\begin{aligned} \upsilon_\infty : k(x) \setminus \{0\} &\to \mathbb{Z} \\ f &\mapsto -grau(f). \end{aligned}$$

Quan k és un cos finit amb q elements, cas corresponent a cos global de característica $p > 0$, associem a la valoració υ_∞ de k(x) el valor absolut

$$|f(x)|_\infty := q^{-\upsilon_\infty(f)} = q^{grau(f)}.$$

Definició 2.4.4 *Denotarem per $V(k(x))$ el conjunt de valors absoluts de k(x) que consisteixen en el valor absolut no arquimedià $||_\infty$, i en els valors absoluts no arquimedians estandaritzats associats als ideals maximal de k[x]. Denotarem un element de $V(k(x))$ per υ abans que per $||_\upsilon$.*

Ara enunciem pero no demostrarem la fòrmula del producte (es pot trobar a [Lor], pàgina 177, Lema 8.2) per al cas $\mathbb{F}_q(x)$.

Lema 2.4.2 *(Fòrmula del producte per $\mathbb{F}(x)$) Sigui $f(x) \in \mathbb{F}^*$. Llavors*

$$\prod_{\upsilon \in V(\mathbb{F}(x))} |f(x)|_\upsilon = 1.$$

El següent lema ens portarà un resultat clau per fer la demostració de la fòrmula del producte de cossos de funcions sobre cossos finits.[6]

Lema 2.4.3 *Sigui k un cos qualsevol. La valoració υ_∞ de k(x) és igual a la valoració υ_P de k(x) associada a l'ideal maximal $P := (1/x)k[1/x]$ de k[1/x].*

Demostració. Considerem l'inclusió $k[1/x] \subset k(1/x) = k(x)$. L'anell k[1/x] és un domini d'ideals principals en el seu cos de fraccions k(x). Sigui $f(x) = \sum_{i=0}^{grau(f)} a_i x^i$, amb $a_{grau(f)} \neq 0$, un element qualsevol de k[x]. Com que k(x) és el cos de fraccions de k[1/x], podem escriure f(x) com un quocient de g(1/x)/h(1/x), amb $g(1/x)/h(1/x) \in k[1/x]$. Així, escrivim

$$\begin{aligned} f(x) &= (1/x)^{-grau(f)}\Big(\sum_{i=0}^{grau(f)} a_i \frac{1}{(x)^{grau(f)-i}}\Big) = \\ &= \frac{a_{grau(f)} + a_{grau(f)-1}(1/x) + ... + a_0(1/x)^{grau(f)}}{(1/x)^{grau(f)}}. \end{aligned}$$

Podem veure que en el domini d'ideals principals k[1/x], l'element $a_{grau(f)} + a_{grau(f)-1}(1/x) + ... + a_0(1/x)^{grau(f)}$ no és divisible per 1/x. Per tant, per la definició donada de valoració P-àdica υ_P associada a $P := (1/x)$ tenim que

$$\upsilon_P(f(x)) := ord_P(f(x)) = ord_P((1/x)^{-grau(f)}) = -grau(f).$$

Per tant, $\upsilon_P = \upsilon_\infty$. Per veure que $||_\infty = ||_P$, és suficient fixar-nos que $k[1/x]/P \cong k$. Per tant, $|k| = q, |f|_P := q^{\upsilon_P(f)} = |f|_\infty$. □

Sigui k un cos finit i L/k(x) una extensió separable de grau finit n. Volem determinar el conjunt de valors absoluts $\{||_i, i = 1, ..., s\}$ de L que extenen al valor absolut $||_\infty$ de k(x). Pel lema anterior, sabem que podem trobar un conjunt de valoracions de L associades a υ_∞.

De manera general, sigui B' la clausura entera de k[1/x] in L. Suposem que B' és una k[1/x]-àlgebra finitament generada. Com que B' que és llavors un domini de Dedekind, l'ideal $(1/x)B'$ factoritza en un producte d'ideals maximals

$$(1/x)B' := \mathfrak{B}_1^{e\mathfrak{B}_{1/P}} \cdots \mathfrak{B}_s^{e\mathfrak{B}_{s/P}}.$$

[6] En el cas d'un cos de nombres L la fòrmula és $\prod_{w \in V(L)} |x|_w^{n_{w/\upsilon}} = 1$, on $x \in L^*$

Denotem per $v_{\mathfrak{B}_i}$ la valoració de L associada a $\mathfrak{B}_i$, i per $||_{\mathfrak{B}_i}$, $i = 1, ..., s$, els valors absoluts de L associats a $v_{\mathfrak{B}_i}$. Pel que hem vist anteriorment, cada valor absolut $||_{\mathfrak{B}_i}$ de L extén al valor absolut $||_\infty = ||_P$ de k(x). Sigui

$$n_{\mathfrak{B}_i/P} = n_i := e_{\mathfrak{B}_i/P} \cdot f_{\mathfrak{B}_i/P}.$$

Pel teorema 2.2.2 sabem que $\sum_{i=1}^{s} n_{\mathfrak{B}_i/P} = n = [L : k(x)]$. Pel lema 2.4.1 tenim que $\forall \alpha \in B, |N_{L/k(x)}(\alpha)|_\infty = \prod_{i=1}^{s} |\alpha|_{\mathfrak{B}_i}^{n_i}$. Pel fet que ideals maximals diferents, tenen valoracions associades diferents tenim que les valoracions exhaustives $v_{\mathfrak{B}_i}, i = 1, ..., s$, són totes diferents.

Tornem al cas de k cos finit. Sigui L una extensió finita de k(x). Denotem per V(L) el conjunt que consisteix en tots els valors absoluts $||_{\mathfrak{B}}$ de L associats als ideals maximals $\mathfrak{B}$ de B, i els valors absoluts $||_{\mathfrak{B}_i}, i = 1, ..., s$ extenen al valor absolut $||_\infty$ de k(x). Denotem un element de V(L) per $||_w$, o simplement per w. Si $||_w$ exten a un valor absolut $||_v$ de V(k(x)), diem que w divideix v, i ho denotem per $w|v$. Si $||_w = ||_{\mathfrak{B}}$ per algun $\mathfrak{B} \in Max(B)$, llavors escrivim $||_v = ||_{\mathfrak{B}\cap k[x]}$, i $n_{w/v} = n_{\mathfrak{B}/\mathfrak{B}\cap k[x]}$ (podeu veure apèndix B per més informació).

Fet: *En les condicions anteriors, V(L) consisteix en tots els valors absoluts possibles de en el cos L ([Art] Capítol 9).*

Proposició 2.4.1 *(Fòrmula del producte per cossos de funcions sobre cossos finits)Sigui k un cos finit. Sigui L/k(x) una extensió finita separable. Sigui $f \in L^*$. Llavors*

$$\prod_{w \in V(L)} |f|_w^{n_{w/v}} = 1.$$

Demostració. Siguin B i B^* les clausures enteres en L de k[x] i k[1/x], respectivament. Suposem que B i B^* són k[x]-mòduls i k[1/x]-mòduls finitament generats, respectivament. Llavors,

$$\begin{aligned}\prod_{w \in V(L)} |f|_w^{n_{w/v}} &= \prod_{v \in V(k(x))} \Big(\prod_{w|v, w \in V(L)} |f|_w^{n_{w/v}} \Big) \\ &= \prod_{v \in V(k(x))} |N_{L/K}(f)|_v \, (Lemma\, 2.4.1) \\ &= 1. \, (Lemma\, 2.4.2)\end{aligned}$$

□

Corol·lari 2.4.1 *Sigui $||_{\mathfrak{B}_i}, i = 1, ..., s$, els valors absoluts de L que extenen $||_\infty$. Si $f \in B \setminus \{0\}$, llavors $\| f \|_B = \prod_{i=1}^{s} |f|_{\mathfrak{B}_i}^{n_i}$, on els n_i són els definits anteriorment $n_i := e_{\mathfrak{B}_i/P} \cdot f_{\mathfrak{B}_i/P}$.*

Demostració. Sigui f un element diferent del zero de B. Factoritzem

$$(fB) = \prod_{M \in Max(B)} M^{v_M(f)}.$$

Per definició,

$$\| fB \|_B = |B/fB| = \prod_{M \in Max(B)} |B/M|^{v_M(f)} = \frac{1}{\prod_{M \in Max(B)} |f|_{n_{M/M\cap k[x]}}^{M}}.$$

Aplicant la fòrmula del produte, obtenem el que volíem. □

2.5 Grup de classes d'ideals i la seva finitud

En aquest apartat associarem a un domini de Dedekind A un grup abelià, anomenat grup de classes d'ideals $Cl(A)$. A continuació, demostrarem que és un grup finit quan A és un anell de funcions sobre un cos finit (recordem que es conegut quan A és anell d'enters d'un cos de nombres que $Cl(A)$

és finit).

Sigui A un domini. El conjunt $\mathscr{M}(A)$, que consisteix en tots els ideals diferent del zero de A, és un monoide commutatiu quan es dotat amb la llei de composició de multiplicació d'ideals:

(i) Donats $I, J \in \mathscr{M}(A), IJ \in \mathscr{M}(A)$.

(ii) L'ideal unitat $(1) = A$ és l'element identitat per la multiplicació d'ideals.

Definició 2.5.1 *Sigui $\mathscr{M}$ un monoide qualsevol amb element unitat 1. Una relació de congrüencia en $\mathscr{M}$ és una relació d'equivalència $\equiv$ tal que, per tot $I, I', J, J' \in \mathscr{M}$ amb $I \equiv J$ i $I' \equiv J'$, $II' \equiv JJ'$.*

Definició 2.5.2 *Sigui A un domini commutatiu qualsevol. Considerem la següent relació en el monoide $\mathscr{M}(A)$:*

$$I \equiv J \Leftrightarrow \exists \alpha, \beta \in A \setminus \{0\} \, tal \, que \, (\alpha)I = (\beta)J.$$

Com que $\equiv$ és una relació d'equivalència associada a un submonoide de $\mathscr{M}(A)$ (concretament, el conjunt d'ideals principals diferents del zero de A), és una relació de congruència en $\mathscr{M}(A)$. Denotem per $Cl(A)$ el monoide $\mathscr{M}(A)/\equiv$.

Quan A és un domini de Dedekind, llavors $Cl(A)$ és un grup abelià amb l'element identitat la classe del (1), com podem veure a [Lor], pàgina 159. Anem a veure l'invers, I^{-1}, de $I \in Cl(A)$, $I \neq A$. Sigui $\alpha \in I, \alpha \neq 0$. Com que els ideals no trivials de A tenen factorització única en un producte d'ideals maximals, podem escriure $(\alpha) = IJ$ per algún ideal J de $\mathscr{M}(A)$. Per tant, $IJ \equiv (1)$, i la classe de J és l'invers de la classe de I en $Cl(A)$, $I^{-1} = J$.

Definició 2.5.3 *Sigui A un domini de Dedekind. El grup $Cl(A)$ s'anomena el grup de classes d'ideals de A.*

Definició 2.5.4 *Diem que un domini de Dedekind A té quocients finits si, per tot $P \in Max(A)$, el cos residual A/P és un cos finit.*

Definició 2.5.5 *Sigui A un domini de Dedekind amb quocients finits. Definim la norma d'un ideal diferent del zero com*

$$\| I \|_A := \, cardinalitat \, de \, A/I.$$

Notem que $\| I \|_A = 1$ si i només si I=A.

Exemple 2.5.1 *L'anell A=k[x], on k és un cos finit amb $q = p^r$ elements té quocients finits. Sigui I=(g(x))un ideal qualsevol diferent del zero. Llavors*

$$\| I \|_A := |k[x]/(g(x))| = q^{grau(g(x))}.$$

De fet, k[x]/(g(x)) és un k-espai vectorial de dimensió igual al grau de g(x).

Exemple 2.5.2 *L'anell $A = \mathbb{Z}$ té quocients finits. Sigui $I = (a)$ un ideal diferents del zero. Llavors*

$$\| I \|_A := |\mathbb{Z}/a\mathbb{Z}| = a|.$$

Proposició 2.5.1 *Sigui A un domini de Dedekind amb quocients finits. Sigui K el seu cos de fraccions. Sigui L/K una extensió finita. Suposem que la clausura entera B de A en L és un A-mòdul finitament generat. Llavors, B és un domini de Dedekind amb els quocients finits. A més, si $I \subset B$ és un ideal diferent del zero , llavors $\| I \|_B = \| N_{B/A}(I) \|_A$.*

Demostració. Anteriorment ja hem vist que B és un domini de Dedekind. Sigui $M \in Max(B)$. Sigui $P := M \cap A$. Llavors B/M és un (A/P)-espai vectorial de dimensió $f_{M/P}$. Per tant, B/M és un cos finit, i

$$\| M \|_B = |B/M| = |A/P|^{f_{M/P}} = \| P^{f_{M/P}} \|_A = \| N_{B/A}(M) \|_A \, .$$

Com que $N_{B/A}$ és una funció multiplicativa, trobem que per tot ideal I de B,

$$\| I \|_B = \| N_{B/A}(I) \|_A \, .$$

□

En el següents tres lemas, denotarem per A=k[x], on k és un cos finit amb q elements. Denotarem per L una extensió finita i separable de grau n del cos de fraccions K de A, i denotarem per B la clausura entera de A en L. La proposició anterior mostra que B té quocients finits.

Lema 2.5.1 *Fixem un $\lambda \in \mathbb{R}$. Llavors, existeixen únicament un nombre finit d'ideals I de B amb $\| I \|_B \leq \lambda$.*

Demostració. Un ideal I en $\mathscr{M}(B)$ té norma $\| I \|_B = 1$ si i només si I=B. Com la funció norma en B és multiplicativa i positiva, per veure el lema només cal veure que B conté només un nombre finit d'ideals maximals M amb $\| M \|_B \leq \lambda$. Com un ideal maximal de A és contingut només en un nombre finit d'ideals maximals de B, i com que

$$\| M \|_B = \| M \cap A \|_A^{f_{M/M\cap A}} \geq \| M \cap A \|_A,$$

és suficient veure que donat un $\lambda \in \mathbb{R}$, llavors existeixen només un nombre finit de ideals P de A amb $\| P \|_A \leq \lambda$. Això és clar per l'exemple 2.5.1, i 2.5.2. □

Lema 2.5.2 *El grup Cl(B) és finit si i només si existeix un nombre $\lambda \in \mathbb{R}$, depenent de B, tal que tota classe d'ideal de B conté un ideal I amb $\| I \|_B \leq \lambda$.*

Demostració. Suposem que el grup Cl(B) és finit i sigui $Cl(B) := \{C_1, ..., C_h\}$. Com tota classe d'ideal conté un ideal, podem agafar un ideal I_i en cada classe C_i. El nombre $\lambda := max\{\| I_i \|_B , i = 1, ..., h\}$ satisfà l'afirmació del lema.
Ara del lema 2.5.1 obtenim que únicament hi ha un nombre finit d'ideals I de B tals que $\| I \|_B \leq \lambda$. Així, quan tota classe d'ideal de B correspon a un ideal I amb $\| I \|_B \leq \lambda$, provant que Cl(B) és finit. □

Lema 2.5.3 *Sigui $\lambda \in \mathbb{R}$. Tota classe d'ideals de B conté un ideal amb $\| I \|_B \leq \lambda$ si tot ideal diferent del zero J de B conté un element α amb $\| (\alpha) \|_B \leq \lambda \| J \|_B$.*

Demostració. Sigui $C \neq (1)$ una classe d'ideal de B. Fixem un ideal J en la classe de C^{-1}, l'invers de C en Cl(B). Sigui $\alpha \in J$ tal que $\| (\alpha) \|_B \leq \lambda \| J \|_B$. Com que $\alpha \in J$, podem escriure $(\alpha) = IJ$, per algun ideal I de A. Com que $(\alpha) = IJ$, veiem que l'ideal I pertany a la classe de C. La desigualtat $\| IJ \|_B = \| (\alpha) \|_B \leq \lambda \| J \|_B$ demostra que $\| I \|_B \leq \lambda$. □

Teorema 2.5.1 *Sigui A=k[x], amb k un cos finit. Sigui L una extensió finita i separable de grau n del cos de fraccions K de A, i sigui B la clausura entera de A en L. Llavors existeix un nombre real λ, depenent només de B, tal que tot ideal diferent de zero I de B conté un element α diferent del zero amb $\| (\alpha) \|_B \leq \lambda \| J \|_B$. En particular, el grup de classes d'ideals de B és finit.*

Demostració. Tenim k un cos finit amb q elements. Suposarem que la clausura entera B és un A-mòdul finitament generat. Com que A és un domini d'ideals principals, podem agafar una base $\{\alpha_1, ..., \alpha_n\}$ per B sobre A. Sigui I un ideal diferent de zero de B. Com que $\| I \|_B = \| N_{B/A}(I) \|_A$, i com que la norma de qualsevol ideal diferent del zero de A és igual a una potència de q, concloem que $\| I \|_B$ és una potència de q. Sigui $d \geq 0$ l'únic enter tal que

$$(q^d)^n \leq \| I \|_B < (q^{d+1})^n.$$

Com que $(q^{d+1})^n > \| I \|_B = |B/I|$, trobem que dos dels $(q^{d+1})^n$ elements diferents de B de la forma

$$\sum_{i=1}^{n} m_i \alpha_i, m_i \in A, \ i \ m_i = 0 \ o \ 0 \leq grau(m_i) \leq d,$$

han de ser congruents mòdul I. Per tant, l'ideal I conté un element diferent del zero α de la forma

$$\alpha = \sum_{i=1}^{n} \alpha_i, m_i \in A, \ i \ m_i = 0 \ o \ 0 \leq grau(m_i) \leq d.$$

Ara necessitem de l'existència de n aplicacions:

$$||_i : L \to \mathbb{R}^+, i = 1, ..., n,$$

que han de satisfer les següents propietats:

(i) $\forall \alpha \in B, \alpha \neq 0, \| (\alpha B) \|_B = \prod_{i=1}^{n} |\alpha|_i$.

(ii) $|\sum_{j=1}^{n} m_j \alpha_j|_i \leq \sum_{j=1}^{n} |m_j \alpha_j|_i$.

(iii) $|m_j \alpha_j|_i = |m_j|_i \cdot |\alpha_j|_i$.

Aquestes aplicacions venen donades en la construcció final de la secció anterior. Recordem el que vam fer, vam definir una valoració v_∞ a k(x), i després vam associar a aquesta valoració un valor absolut, i vam veure una fòrmula producte i un corol·lorari com a conseqüencia d'aquesta.

Recordem tenim k un cos finit d'ordre q. Tenim $A = k[x]$, i denotem per K el seu cos de fraccions. Sigui L/K una extensió de grau n. Suposem que les clausures enteres B i B' de k[x] i k[1/x] en L són k[x]-mòduls i k[1/x]-mòduls finitament generats, respectivament. Denotem per $||_i := ||_{\mathfrak{B}_i}, i = 1, ..., s$, els s valors absoluts de L, definits anteriorment, que extenen al valor absolut $||_\infty$ de K. Denotem per $n_i := n_{\mathfrak{B}_i/P}, i = 1, ..., s$, les multiplicitats associades. Com A és un domini d'ideals principals, podem agafar una base $\{\alpha_1, ..., \alpha_n\}$ per B sobre A. Sigui

$$\lambda := \prod_{i=1}^{s} (\sum_{j=1}^{n} |\alpha_j|_i)^{n_i}.$$

Anem a veure que ideal diferent de zero I de B conté un element diferent del zero α tal que $\| (\alpha) \|_B \leq \lambda \| I \|_B$. Sigui I un ideal diferent del zero de B. Denotem per $d \geq 0$ l'únic enter tal que

$$(q^d)^n \leq \| I \| < (q^{d+1})^n.$$

Com que $(q^{d+1})^n > \| I \|_B = |B/I|$, trobem que dos dels $(q^{d+1})^n$ elements diferents de B de la forma $\sum_{i=1}^{n} m_i \alpha_i$, amb $m_i \in A$ i $|m_i|_\infty \leq q^d$, són congruents mòdul I. Per tant, l'ideal I conté un element α de la forma

$$\alpha = \sum_{i=1}^{n} m_i \alpha_i, \, amb \, m_i \in A, \, i \, |m_i|_\infty \leq q^d.$$

Utilitzant el corol·lari 2.4.1, i propietats dels valors absoluts podem veure que

$$\begin{aligned} \| (\alpha) \|_B &= \prod_{i=1}^{s} |\alpha|_i^{n_i} \\ &\leq \prod_{i=1}^{s} (\sum_{j=1}^{n} |m_j \alpha_j|_i)^{n_i} = \prod_{i=1}^{s} (\sum_{j=1}^{n} |m_j|_\infty \cdot |\alpha_j|_i)^{n_i} \\ &\leq (q^d)^{\sum_{i=1}^{s} n_i} \cdot \prod_{i=1}^{s} (\sum_{j=1}^{n} |\alpha_j|_i)^{n_i} = (q^d)^n \cdot \lambda \\ &\leq \| I \|_B \cdot \lambda. \end{aligned}$$

I obtenim el resultat del teorema. I pels lemes anteriors al teorema, veiem que el grup de classes d'ideals és finit. □

Ara definirem la cota Minkowski pel cas de cossos numèrics, i donarem un exemple molt senzill sobre aquesta cota. Després, veurem un cos on el grup de classes d'ideals és infinit.

Teorema 2.5.2 *(Cota de Minkowski) Sigui K un cos numèric. Sigui D el discriminant del cos K sobre K, n el grau de K sobre $\mathbb{Q}$, i $2r_2 = n - r_1$ el nombre d'embeddings complexos on r_1 és el nombre d'embeddings reals. Llavors, tota classe del grup d'ideals de classe de K conté un ideal I diferent de zero amb la norma tal que*

$$N(I) \leq \sqrt{|D|} (\frac{4}{\pi})^{r_2} \frac{n!}{n^n}$$

Podem veure una demostració d'aquest teorema a [Mil] a la pàgina 70 Teorema 4.3, i al llarg de la mateixa secció podem trobar més aplicacions d'aquest.

Corol·lari 2.5.1 *Sigui K cos de nombres, $\mathscr{O}_K$ l'anell d'enters que és la clausura entera de $\mathbb{Z}$ en K, es té $Cl(\mathscr{O}_K)$ finit.*

Demostració. Hi ha un nombre finit d'enters menors o iguals a $\sqrt{|D|}(\frac{4}{\pi})^{r_2}\frac{n!}{n^n}$, i pel Lema 2.5.1 i 2.5.2 obtenim el resultat de la finitud de $Cl(\mathscr{O}_K)$. □

Exemple 2.5.3 *Sigui $K=\mathbb{Q}(\sqrt{5})$, un cos numèric, llavors $r_1=2$, $r_2=0$, $n=2$, i $|D|=5$. Així*

$$N(I)\leq\frac{1}{2}\sqrt{5}\approx 1.118<2.$$

Per tant, N(I)=1 i així $I=\mathscr{O}_K$. Per tant, tot ideal de $\mathscr{O}_K$ és principal i $Cl(\mathscr{O}_K)=\{1\}$.

Proposició 2.1 *Sigui k un cos i $f(x,y)\in k[x,y]$ un polinomi en dos variables irreductible. Sigui $f(x,y)=0$ no-singular, llavors $C_f:=\overline{k}[x,y]/(f)$ és un domini de Dedekind. A més, si k és un cos finit, llavors C_f és un domini amb quocients finits.*

Podeu trobar la demostració del resultat anterior a la pàgina 229, Corol·lari 2.7, [Lor].

Exemple 2.5.4 *Considerem la corba el·líptica afí $y^2=x^3-x$. Fixem-nos que és no singular i per tant, la clausura entera és $B=\mathbb{C}[x,y]/(y^2-x^3+x)$. En aquest cas, el grup de classes d'ideals és infinit.*

La raó d'això és que els ideals maximals de B corresponen als ideals maximals de $\mathbb{C}[x,y]$ que contenen (y^2-x^3+x). Els ideal maximals de $\mathbb{C}[x,y]$ són de la forma (x-a,y-b) i aquest conté (y^2-x^3+x) si i només si b^2-a^3+a. Així, els ideals maximals de B corresponen al punts de la corba $y^2=x^3-x$.

Pel teorema dels zeros de Hilbert (Hilbert's Nullstellensatz)[7] tenim que tot ideal d'una corba com la que tenim és de la forma (x-a,y-b) on $b^2=a^3-a$, que satisfà l'equació $y^2=x^3-x$. Això ho podem fer, ja que, estem en un cos algebraicament tancat, $\mathbb{C}$. Així doncs, tenim infinits punts i per tant, infinits ideals maximals. Ara anem a veure si dos ideals maximals poden estar relacionats per una funció f. Per fer això, utilitzarem teoria del Capítol 5 de Ros[1], que introduïrem en la següent secció, però que per aquest exemple donarem per donada. Llavors tenim que $Div(f)=\mathscr{D}_{(f)}=P-Q$, on P ideal maximal de la forma $(x-a_1,y-b_1)$ i Q ideal maximal de la forma $x-a_2,y-b_2$, i per tant, el grau del divisor serà zero, però té un zero i un pol, i això vol dir que la corba té gènere zero, i la nostra corba és una corba el·líptica de gènere 1, arribant així a contradicció. Per tant, no poden haver-hi aquest divisors, i tots aquests ideals maximals no estàn relacionats i llavors hi ha un nombre no finit d'elements en Cl(B).

Veiem un fet relacionat amb el següent exemple i acabem amb una definició.

Fet: *Si tenim (A,K,B,L), on L/K separable i Galois, $Cl(B)$ és un $\mathbb{Z}$[Gal(L/K)]-mòdul via acció β ideal primer de B, $\sigma\in$Gal(L/K), $\sigma\cdot\beta=\sigma(\beta)$ ideal primer de L.*

Observació: $[\beta]\in Cl(B)$, $n\in\mathbb{Z}$ *actua via* $n[\beta]::=[\beta^n]$. *Per* $[\beta]\in Cl(B)$, $\sigma\in Gal(L/K)$ *actua via* $\sigma[\beta]:=[\sigma(\beta)]$. *Per tant,* $(\sum_{i=1}^k n_i\sigma_i)\in\mathbb{Z}[Gal(L/K)]$ *actua via* $(\sum_{i=1}^k n_i\sigma_i)[\beta]=[\prod_{i=1}^k\sigma_i(\beta)^{n_i}]$.

Exemple 2.5.5 *Sigui $A=\mathbb{F}_2[t]$, $K=\mathbb{F}_2(t)$, $f(t,x)=x^2+tx+t$ i $L=\mathbb{F}_2(t)[x]/(x^2+tx+t)$. Observem que L/K abeliana i Galois amb $Gal(L/K)\cong\mathbb{Z}/(2)$. Estem en la següent situació:*

$$\begin{array}{ccc} B & \subseteq & L \\ | & & | \\ \mathbb{F}_2[t] & \subseteq & \mathbb{F}_2(t) \end{array}$$

$B=\mathbb{F}_q[t,x]/(x^2+tx+t)$ és la clausura entera de A en L, ja que, $f(t,x)$ és no singular,

[7] Per més detall sobre el teorema, mirar el Capítol I de Kem[1], i en particular, el Teorema 1.7 de la pàgina 21, on s'explicita aquesta correspondència.

$$\frac{\partial f}{\partial x} = 2x + t = t$$
$$\frac{\partial f}{\partial t} = x + 1$$

$Cl(B) \neq \langle id \rangle$, i és un $\mathbb{Z}[Gal(L/K)]$-mòdul no trivial. Ara calculem el discriminant de f en x

$$disc(f) = det \begin{pmatrix} 1 & t & t \\ t & 0 & 0 \\ 0 & t & 0 \end{pmatrix} = t^3.$$

Així, per la Proposició 2.2.1 i 2.2.2, tenim que (t) ramifica en B (ja que, $disc(f) = t^3 \in (t)$. Per tant, $(t) = \beta^2$ on β ideal de B. Suposem que β és principal, llavors

$$\beta = (u(t)x + v(t)), \quad u(t), v(t) \in B$$
$$t = \beta^2 = u^2(t)x^2 + v^2(t) = u^2(t)tx + u^2(t)t + v^2(t),$$

on $u^2(t) = 0$ per tant, $u(t) = 0$, llavors $v^2(t) = t$ per tant, $v(t) = \sqrt{t}$. Però $\sqrt{t} \notin B$[8], d'on obtenim $Cl(B) \neq \{id\}$.

Definició 2.5.6 *Sigui A un domini de Dedekind amb cos de fraccions K (un cos global), denotem per h_A el nombre d'elements del grup finit $Cl(A)$.*

[8] L'extensió $\sqrt{t}$ no hi és ja que seria inseparable sobre $\mathbb{F}(t)$ i la nostra extensió és separable

3 El grup de classes de divisors i les S-unitats

En aquesta secció introduim uns conceptes relacionats amb geometria més estretament, relacionats amb el grup de classes d'ideals. En particular, obtenim un anàleg del teorema de Dirichlet per les unitats en cossos globals en característica $p > 0$.

3.1 Divisors i Teorema de Riemann-Roch

Un cos de funcions en una variable sobre F és un cos K, que conté F i amb $x \in$K trascendental sobre F, tal que $K/F(x)$ és una extensió finita algebraica separable. Per a K/F cos de funcions en una variable parlem del cos de constants per $\overline{F} \cap K = E$, on $\bar{F}$ és la clausura separable de F.

Veiem breument que la clausura separable de F en K és finita sobre F, és a dir, $E = \overline{F} \cap K$ és una extensió finita separable de F. Com E un subcòs de K, que és algebraic i separable sobre F, tenim

$$[E : F] = [E(x) : F(x)] \leq [K : F(x)].$$

Així, canviant F amb la seva clausura separable en K, si fos necessàri, suposem que F és algebraicament tancat en K, és a dir, tot $\bar{K} \cap F = K$, on $\bar{K}$ la clausura de K. En aquest cas, F seria el cos de constants de K. A partir d'ara K/F(x) finita separable, pensarem que el cos de constants és F.

El grup de divisors de K, $\mathscr{D}_K$, és per definició el grup lliure abelià generat pels primers de K[9]. Escriurem aquest de manera additiva tal que un divisor qualsevol serà de la forma $D = \sum_P a(P)P$, on P denota sempre en aquesta secció un primer de K. Els coeficients, $a(P)$, estàn únicament determinats per D i els denotarem a vegades com $ord_P(D)$. El grau de tal divisor es defineix com $grau(D) = \sum_P a(P)grau(P)$. Això ens dòna un morfisme de $\mathscr{D}_K$ a $\mathbb{Z}$, amb el nucli denotat per $\mathscr{D}_K^o$, el grup de divisors de grau zero.
Ara sigui $a \in K^*$. El divisor de a, (a) o div(a), es defineix com $\sum_P ord_P(a)P$. L'aplicació $a \to (a)$ és un morfisme de grups de K^* a $\mathscr{D}_K$. L'imatge d'aquest morfisme es denota per $\mathscr{P}_K$ i s'anomena el grup de divisors principals. Es pot demostrar que el grau d'un divisor principal és zero ([Sil], pàgina 32, Proposició 3.1).
Si P és un primer tal que $ord_P(a) = m > 0$, diem que P és un zero de a d'ordre m de (a) o de la funció a. Si P és un primer tal que $ord_P(a) = -n < 0$, diem que P és un pol de a d'ordre n (de (a) o de la funció a). Sigui

$$(a)_o = \sum_{P|ord_P(a)>0} ord_P(a)P\,,\ (a)_\infty = -\sum_{P|ord_P(a)<0} ord_P(a)P.$$

El divisor $(a)_o$ s'anomena el divisor de zeros de a, i el divisor $(a)_\infty$ s'anomena el divisor de pols de a. Observem $(a) = (a)_o - (a)_\infty$ en $\mathscr{D}_K$.

Dos divisors D_1 i D_2 són linealment equivalents, denotat per $D_1 \sim D_2$, si la seva diferència és principal, és a dir, $D_1 - D_2 = (a)$ per algun $a \in K^*$.

Definició 3.1.1 *Definim ara, $Cl_K = \mathscr{D}_K/\mathscr{P}_K$, el grup de classes de divisors del cos K. Com el grau d'un divisor principal és zero, la funció grau ens dòna un morfisme de Cl_K a $\mathbb{Z}$. El nucli d'aquest morfisme es denota per Cl_K^o, el grup de classes divisors de grau 0.*

Ara donarem dues definicions i enunciarem un teorema que no demostrarem, però si que treballarem amb certes conseqüencies d'aquest teorema.

Definició 3.1.2 *Un divisor, $D = \sum_P a(P)P \in \mathscr{D}_K$, diem que és un divisor efectiu si per a tot P, es té $a(P) \geq 0$. El denotem per $D \geq 0$.*

Fet: *Sigui D un divisor. Definim $L(D) = \{x \in K^* | (x) + D \geq\} \cup \{0\}$. Podem veure que L(D) té estructura d'espai vectorial sobre F i que és de dimensió finita sobre F. La dimensió de L(D) sobre F és denota per l(D).*

[9] Per un cos global K un primer $\mathfrak{p}$ del cos denota una V(K), una valoració discreta, o equivalentment un primer $\mathfrak{B}$ de la clausura entera de F[x] en K o en la clausura entera de F[1/x] en K.

Lema 3.1.1 *Si D_1 i D_2 són divisors linealment equivalents, llavors $L(D_1)$ i $L(D_2)$ són isomorfs. En particular, $l(D_1) = l(D_2)$.*

Demostració. Suposem que D_1=D_2+(h). L'aplicació K^* $x \to xh$ és un isomorfisme de L(D_1) a L(D_2). □

Lema 3.1.2 *Si $grau(D_1) \leq 0$, llavors $l(D_1) = 0$, llevat que $D_1 \sim 0$ en aquest cas tindríem que $l(D_1)$=1.*

Demostració. Si tenim que grau(D)<0 i $x \in L(D)$, llavors grau((x)+D) es menor que 0 i més o igual que zero, que és una contradicció. Per tant, $l(D) = 0$. Ara si grau(D)=0 i L(D) no és buit, sigui $x \in L(D)$. LLavors $(x) + D \geq 0$ i té grau zero, així doncs, ha de ser el divisor zero. Per tant, $D \sim 0$. En canvi, si $D \sim 0$, llavors $l(D) = l(0) = 1$, ja que, L(0)=F perquè $x \in L(0)$ implica que x no té pols ni zeros, i per tant, $x \in F$, les funcions constants. □

El primer lema enunciat i demostrat ens diu que les constants $l(D)$ depèn només de la classe de D en Cl_K. De manera similar, el grau(D) depèn només en la classe de D. La demostració del següent teorema es pot trobar al capítol 6 de [Ros], pàgina 73.

Teorema 3.1.1 *(Riemann-Roch) Existeix un enter $g \geq 0$ i un divisor de classe $\mathfrak{D}$ tal que per $\omega^v \in \mathfrak{D}_K$ i per a tot $D \in \mathscr{D}_K$ es té*

$$l(D) = grau(D) - g + 1 + l(\omega^v - D).$$

L'enter g és únicament determinat per K, i s'anomena el gènere de K.

Ara procedim a enunciar els següents corol·laris del teorema de Riemann-Roch.

Corol·lari 3.1.1 *(Desigualtat de Riemann)Per tots el divisors de D, es té $l(D) \geq grau(D) - g + 1$.*

Corol·lari 3.1.2 *El $\omega^v \in \mathfrak{D}$ compleix $l(\omega^v) = g$, ω^v s'anomena el divisor canònic.*

Corol·lari 3.1.3 *Per a $\omega^v \in \mathfrak{D}$ tenim que $grau(\omega^v) = 2g - 2$.*

Demostració. Posem D=0 en el teorema, i a continuació, apliquem el corol·lari anterior. □

Corol·lari 3.1.4 *Si $grau(D) \geq 2g - 2$, llavors $l(D) = grau(D) - g + 1$, excepte en el cas que $grau(D) = 2g - 2$ i $D \in \mathfrak{D}$.*

Demostració. Si tenim que $grau(D) \geq 2g - 2$, llavors $grau(\omega^v - D) \leq 0$. Ara aplicant el Lema 3.1.2 obtenim el resultat. □

Per a llegir més sobre aquest apartat podeu consultar [Lor] Capítol 9, [Har] Capítol 4 (en concret secció 4.19), i [Ros] Capítols 5 i 6.

3.2 Teorema de les unitats de Dirichlet en cossos globals en característica positiva

Sigui K/F un cos de funcions algebraiques sobre el cos de constants $F = \mathbb{F}$ finit. L'anell $A = \mathbb{F}[x] \subset k = \mathbb{F}(x)$ té una certa analogia a la parella $\mathbb{Z} \subset \mathbb{Q}$ en la teoria de nombres. K és una extensió algebraica de $\mathbb{F}$(x) i l'anàleg de l'anell d'enters en un cos algebraic numèric és la clausura entera de $A = \mathbb{F}[x]$ en K. Anomenarem aquest anell com B, i com hem vist anteriorment és un domini de Dedekind. Estudiarem el seu grup d'unitats.

Denotarem per ∞ el primer a l'infinit en el subcós $k = \mathbb{F}(x)$, corresponent a l'ideal primer $\frac{1}{x}$ en $\mathbb{F}[\frac{1}{x}]$ suposem sempre K/F separable, i denotarem per $S_\infty = S$ al conjunt finit de primers $\mathfrak{p}$ de K que es troben sobre ∞ (és a dir, $\mathfrak{p} \cap \mathbb{F}[\frac{1}{x}] = (\frac{1}{x})$). Denotem per S_K el conjunt de tots el primers en K. Per a $S \subset S_K$ un conjunt finit qualsevol de primers, definim

$$\mathscr{O}_S = \{a \in K | ord_P(a) \geq 0, \forall P \notin S\},$$

l'anell dels S-enters, i el grup de les S-unitats com

$$E(S) = \{a \in K^* | ord_P(a) = 0, \forall P \notin S\} \subseteq \mathscr{O}_S,$$

és a dir, les funcions de k sense zeros ni pols en S. És clar que $E(S) = \mathscr{O}_S^*$, les unitats de l'anell dels S-enters.

Com que K està fixat denotarem per $\mathscr{D}_K$ el seu grup de divisors, per $\mathscr{P}_K$ el subgrup de divisors principals, i per $Cl_K = \mathscr{D}_K/\mathscr{P}_K$ el grup de classes de divisors. El grup dels S-divisors, $\mathscr{D}_S$, es defineix com el subgrup de $\mathscr{D}_K$ generat pels primers en $S_K - S$. Donat un element $a \in K^*$, definim el seu S-divisor com

$$(a)_S = div(a)_S = \sum_{P \notin S} ord_P(a)P.$$

Un divisor de la forma $(a)_S$ per algun $a \in K^*$ s'anomena un S-divisor principal. Els S-divisors principals formen un subgrup de $\mathscr{D}_S$, que es denota per $\mathscr{P}_S$. El grup quocient $Cl_S = \mathscr{D}_S/\mathscr{P}_S$ s'anomena grup de S-classes. Finalment, definim $\mathscr{D}_K(S)$ com el subgrup de $\mathscr{D}_K$ generat pels primers en S i $\mathscr{P}_K(S) = \mathscr{P}_K \cap \mathscr{D}_K(S)$.

Teorema 3.2.1 *(F.K. Schmidt) Considerem l'aplicació grau : $\mathscr{D}_K \to \mathbb{Z}$. L'imatge d'aquest aplicació és un ideal principal $i\mathbb{Z}$. L'enter i és el màxim comú divisor de tots els elements del conjunt $\{grau(P)|P \in S_K\}$. Quan el cos constant és un cos finit, llavors i=1.*

Per una referència al teorema anterior podeu consultar [Roq] Secció 8.1, i en la mateixa font podeu trobar més resultats de F.K. Schmidt al llarg d'aquesta.

Com que $\mathscr{D}_K(S)$ és un subgrup de $\mathscr{D}_K$, pel teorema anterior de F.K. Schmidt, l'imatge de $\mathscr{D}_K(S)$ sota l'aplicació anterior és també un ideal principal en $\mathbb{Z}$ que denotem per $d\mathbb{Z}$. L'enter d és caracteritza com el màxim comú divisor de tots els elements en $\{grau(P)|P \in S\}$. Clarament, i divideix d.

Proposició 3.2.1 *Obtenim que les següents seqüencies són exactes per cos K/F en la notació d'aquesta secció (és a dir, K/F extensió finita separable amb cos de constants $\mathbb{F}_q$):*

(a) $(0) \to F^* \to E(S) \to \mathscr{P}_K(S) \to (0)$,

(b) $(0) \to \mathscr{D}_K(S)^o/\mathscr{P}_K(S) \to Cl_K^o \to Cl_S \to C \to (0)$,

on C és un grup cíclic d'ordre d/i.

Demostració. Comencem per (a). Notem primer $F^* \subseteq E(S)$, i assignar-hi l'aplicació de E(S) a $\mathscr{P}_K(S)$ ve donada d'agafar una S-unitat al seu divisor. L'aplicació és exhaustiva per definició de $\mathscr{P}_K(S)$. Si una S-unitat e va cap al divisor zero, llavors $ord_P(e) = 0, \forall P \in S_K$, i per tant ha de ser una constant. Amb això queda vist que (a) és una seqüencia exacta (ja que div(F^*) dincs E(S) va a zero $\mathscr{P}_K(S)$).

Per (b): definim l'aplicació $\tau : \mathscr{D}_K \to \mathscr{D}_S$ via:

$$\tau(D) = \sum_{P \notin S} ord_P(D)P.$$

Aquesta aplicació és un epimorfisme amb nucli $\mathscr{D}_S$. L'imatge de $\mathscr{P}_K$ sota τ és $\mathscr{P}_S$. Per tant, τ indueix a un morfisme de $Cl_K \to Cl_S$ amb nucli $(\mathscr{D}_K(S) + \mathscr{P}_K)/\mathscr{P}_K \cong \mathscr{D}_K(S)/\mathscr{P}_K(S)$. D'aquí deduïm la seqüència exacta

$$(0) \to \mathscr{D}_K(S)^o/\mathscr{P}_K(S) \to Cl_K^o \to Cl_S,$$

i només queda veure que el cokernel de la darrera fletxa és un grup cíclic d'ordre d/i.

Per fer això, utilitzem de nou el fet que τ indueix un morfisme de $\mathscr{D}_K/(\mathscr{P}_K + \mathscr{D}_K(S))$ a Cl_S. El grup que busquem també pot ser descrit com el cokernel de l'aplicació natural de $\mathscr{D}_K^o/\mathscr{P}_K$ a $\mathscr{D}_K/(\mathscr{P}_K + \mathscr{D}_K(S))$. Aquest cokernel el podem veure com isomorf a $\mathscr{D}_K/(\mathscr{D}_K^o + \mathscr{D}_K(S))$ (utilitzant el fet que $\mathscr{P}_K \subseteq \mathscr{D}_K^o$). L'aplicació grau ens dòna un isomorfisme de $\mathscr{D}_K/(\mathscr{D}_K^o + \mathscr{D}_K(S))$ amb $i\mathbb{Z}/d\mathbb{Z} \cong \mathbb{Z}/(d/i)\mathbb{Z}$ (utilizant el teorema de Schmidt). □

Com una conseqüència directa de la part (b) de la proposició anterior, podem enunciar el següent:

Corol·lari 3.2.1 *Cl_S és un grup finit si Cl_K^o és un grup finit. També, Cl_S és un grup de torsió si Cl_K^o és un grup de torsió.*

Proposició 3.2.2 *(Ànaleg al teorema de Dirichlet[10] en cossos globals en característica positiva) Sigui K/F un cos de funcions sobre un cos finit F. Llavors, per tots els subconjunts finits $S \subset S_K$ tenim que Cl_S és un grup finit i $E(S)/F^*$ és un grup lliure amb $|S|-1$ generadors.*

Demostració. Fixemnos que Cl^o en aquest cas és el grup de classes d'ideals que hem estudiat en la secció anterior, i com hem vist, és finit. Llavors pel corol·lari anterior tenim que Cl_S és finit. Per la seqüencia exacta (b) en la proposició anterior podem veure que $\mathscr{D}(S)^o/\mathscr{P}(S)$ és finit també. Això demostra que $\mathscr{P}$ és abelià lliure en $|S|-1$ generadors. □

A continuació veurem que $Cl_S \cong Cl(\mathscr{O}_S)$, on $\mathscr{O}_S$ és un domini de Dedekind en cos global en característica positiva. Podeu trobar també al final de l'apèndix B, un exemple relacionant el Capítol 2 d'aquest treball amb tot el que hem vist en el Capítol 3.

3.3 Relació entre Cl_K, Cl_S i grup de classes d'ideals d'un domini de Dedekind

Teorema 3.3.1 *Sigui K/F un cos de funcions amb cos constant $F = \mathbb{F}$ i sigui S un conjunt finit no buit de primers. Existeixen elements $x \in K$ tal que els pols de x consisteixen precisament en el elements de S. Per tot element x d'aquesta forma, la clausura entera de $F[x]$ en K és $\mathscr{O}_S$. $\mathscr{O}_S$ és un domini de Dedekind i hi ha un correspondència un a un entre els ideals primers diferents del zero de $\mathscr{O}_S$ i els primers de K que no es troben en S. Les S-unitats $E(S)$ són equivalents a les unitats de $\mathscr{O}_S$ i el grup de classes de $\mathscr{O}_S$, $Cl(\mathscr{O}_S)$, és isomorf a Cl_S.*

Demostració. Primerament, denotem els primers en S, $S = \{P_1, P_2, ..., P_s\}$. Per un enter positiu gran M considerem els espais vectorials $L(MP_i) = \{x \in K^* | (x) + MP_i \geq 0\}$. Quan tenim que M és suficientment gran ($M > 2g-2$) pel corol·lari 3.1.4 obtingut del Teorema de Riemann-Roch, tenim que la dimensió d'aquest espai és $Mgrau(P_i) - g + 1$. Segueix que $L(MP_i)$ es contingut en $L((M+1)P_i)$. Agafem un element x_i que està en el darrer conjunt, però no en el conjunt original. Llavors x_i té un pol d'ordre M+1 en P_i i no altres pols. Ara considerem $x = x_1 x_2 \cdots x_s$. Llavors, x te cada element de S com un pol i no altres pols.

Amb x seleccionat de manera que té pols en els elements de S, i en cap lloc més, sigui R la clausura entera de F[x] en K. Suposem doncs que $K/F(x)$ és una extensió separable, llavors pel que hem vist al Teorema 2.1.2 tenim que l'anell R és un domini de Dedekind.[11] Si P és un primer de K que no està en S, llavors $x \in \mathscr{O}_P$ i segueix que $R \subseteq \mathscr{O}_P$. Per tant,

$$R \subseteq \bigcap\nolimits_{P \notin S} \mathscr{O}_P = \mathscr{O}_S.$$

Anem a veure que $R = \mathscr{O}_S$. Sigui $P \notin S$ un primer de K i considerem $P \cap R$. No podem tenir que $P \cap R = (0)$, ja que, del contrari el cos de fraccions de R, K, injectaria en el cos de classe residu $\mathscr{O}_P/P$. Malgrat això, $\mathscr{O}_P/P$ és finit sobre F. Per tant, $P \cap R = \mathfrak{p}$ és un ideal maximal de R, i $R_\mathfrak{p} \subseteq \mathscr{O}_P$. Això ha de ser una igualtat, ja que, $R_\mathfrak{p}$ és un anell de valoració discreta i així és un subanell maximal de K. Per altra banda, si $\mathfrak{p}$ és un ideal maximal de R llavors $R_\mathfrak{p}$ és un anell de valoració discreta i $(\mathfrak{p}R_\mathfrak{p}, R_\mathfrak{p})$ és un primer de K que conté x. Això demostra que $\mathfrak{p} \to (\mathfrak{p}R_\mathfrak{p}, R_\mathfrak{p})$ és una correspondència un a un entre els ideals maximals de R i els primers de K que no són a S. Utilizant altra vegada el fet que R és un domini de Dedekind, podem trobar que

$$R = \bigcap\nolimits_{\mathfrak{p} \subset R} R_\mathfrak{p} = \bigcap\nolimits_{P \notin S} \mathscr{O}_P = \mathscr{O}_S.$$

Per una explicació més detallada del resultat anterior, veure la secció 10.4, pàgines 634 i 635, de [Jac]. Així, acabem de veure que $\mathscr{O}_S$ és un domini de Dedekind i que hi ha una correspondència un a un entre els ideals maximals de $\mathscr{O}_S$ i els primers de K que no són a S, tal i com volíem. □

[10] Teorema de Dirichlet:Donat $\mathscr{O}_K$ anell d'enters del cos numèric K, $\mathscr{O}_K^*$ és un grup abelia lliure, i es té $rank_\mathbb{Z}\mathscr{O}_K^* = r_1 + r_2 - 1$, on r_1 és el nombre de les inmersions reals de K i r_2 és el nombre de les inmersions complexes.

[11] També podem veure que això es verifica si K/F(x) és inseparable en [SamZar], pàgines 281 i 282, Teorema 19.

4 La conjectura de Brumer-Stark

En aquesta secció el nostre objetiu serà enunciar la conjectura de Brumer-Stark i en el treball aportem unes demostracions d'aquestes en cassos particulars, un d'ells relacionat amb cossos globals en característica $p > 0$. Introduim també un teorema de Stickelberger.

4.1 Preàmbul i Teorema de Stickelberger

4.1.1 Cas extensió ciclotòmica en cossos de nombres

Comencem fixant notació que utilizarem durant tota la secció. Recordem, pel teorema de Kronecker-Weber, que afirma que tota extensió abeliana finita $L/\mathbb{Q}$, compleix $L \subseteq \mathbb{Q}(\zeta_n)$ per a un cert n(veure [Lan], pàgina 210, corol·lari 3). Per tot enter positiu m, denotem per ζ_m el nombre complex $e^{\frac{2\pi i}{m}}$. Sigui $K_m = \mathbb{Q}(\zeta_m)$ i denotem per D_m l'anell dels enters algebraics en K_m. Es demostra que D_m està generat, com anell, per ζ_m, i tenim $D_m = \mathbb{Z}[\zeta_m]$ (Proposició 1.2, pàgina 1 de [Was]). Podem suposar que $m \not\equiv 2\,(mod\ 4)$, ja que si $m \equiv 2\,(mod\ 4)$ llavors $\zeta_{m/2} = \zeta_m^2$ i $\zeta_m = -\zeta_{m/2}^{\frac{m+2}{4}}$ i per tant, $K_m = K_{m/2}$. Amb aquesta convenció, un primer $p \in \mathbb{Z}$ és ramificat en K_m si i només si $p|m$ (Teorema 2, pàgina 74 de [Lan]).

Suposem que $p \in \mathbb{Z}$ és un primer que no divideix m i que $P \subset D_m$ és un ideal primer que sobre $p\mathbb{Z}$ en K_m. D_m/P és un cos finit amb $N(P) = p^f$ elements[12], on f és l'enter positiu més petit tal que $p^f \equiv 1\,(mod\ m)$([IreRos, pàgina 194, Proposició 13.2.2]). Si $\alpha \notin P$ hi ha un enter únic i amb $0 \leq i < m$ complint

$$\alpha^{\frac{N(P)-1}{m}} \equiv \zeta_m^i\,(mod\ P).$$

Definim $(\alpha/P)_m := \zeta_m^i$ i anomenem $(\alpha/P)_m$ l'm-èssim símbol de residu potència [13]. Si $\alpha \in P$, definim $(\alpha/P)_m = 0$. Un fet molt important és que $\alpha \to (\alpha/P)_m$ indueix a un morfisme de $(D_m/P)^* \to (\zeta_m)$, és a dir, un caràcter del grup multiplicatiu de D_m/P dins els complexes. Sigui Tr_P l'aplicació traça de D_m/P a $\mathbb{Z}/p\mathbb{Z}$ (podeu consultar definició en [IreRos, pàgina 172]) i definim

$$g(P) = \sum_{\alpha \in (D_m/P)^*} (\alpha/P)_m^{-1} \zeta_p^{Tr_P(\alpha)}.$$

La quantitat $g(P)$ s'anomena suma de Gauss associada amb l'ideal primer P. A més, definim $\phi(P) := g(P)^m$.

Proposició 4.1.1 *En les notacions anteriors, la suma de Gauss verifica:*

(1) $g(P) \in \mathbb{Q}(\zeta_m, \zeta_p)$.

(2) $|g(P)|^2 = N(P)$.

La part (1) s'obté directament de la definició. La part (2) s'obté de les propietats de les sumes de Gauss, i podem veure la demostració explícita a [IreRos], pàgina 209, Proposició 14.3.1.

El primer objectiu és la descomposició en primers de $\phi(P)$ en D_m on P és un ideal primer que no conté m. De la part (2) de la proposició 4.1.1 tenim $\phi(P)\phi(\bar{P}) = N(P^m) = p^{fm}$. Segueix que els primers que divideixen $(\phi(P))$ són primers en D_m sobre $p\mathbb{Z}$. Com que $\mathbb{Q}(\zeta_m)$ és una extensió de Galois, el primers sobre $p\mathbb{Z}$ són tots conjugats de P. Denotem $G_m = Gal(K_m/\mathbb{Q})$ i el elements del grup de Galois per σ_i, i recordem que, en aquest cas, tenim que $(\mathbb{Z}/m\mathbb{Z})^* \cong G_m$. Ara podem enunciar:

Teorema 4.1.1 *(L.Stickelberger):*

$$(\phi(P)) = \prod_{t=1,(t,m)=1}^{m-1} (\sigma_t^{-1}P)^t = (\sum_{t=1,(t,m)=1}^{m-1} t\sigma_t^{-1})P.$$

[12] Observem que denotem per, en aquesta secció, N(P) com el nombre d'elements en D_m/P.
[13] És una generalització símbol de Legendre

Corol·lari 4.1.1 *L'element*

$$\sum_{t=1,(t,m)=1}^{m-1} t\sigma_t^{-1} \in \mathbb{Z}[G_m]$$

aniquila el grup de classes Cl_{K_m}, recordem Cl_{K_m} és un $\mathbb{Z}[G_m]$-mòdul.

La demostració del teorema la podem llegir [IreRos], pàgina 209, Teorema 2, i per la demostració del corol·lari (i més resultats sobre l'element i el teorema) podem veure [Lan2], Capítol 1.2, o [Was], Capítol 6.2.[14]

4.1.2 Cas extensions abelianes sobre cos finit en característica positiva

L'objectiu de la conjectura de Brumer-Stark és generalitzar el resultats en la Secció 4.1.1 per una extensió abeliana arbitrària de cossos globals K/k. Si $G = Gal(K/k)$, busquem un element de $\mathbb{Z}[G]$ definit d'una manera canónica que aniquila el grup de classes de K, en el cas de cossos numèrics, i el grup de classes divisors de K, en el cas de cossos de funcions. A continuació, i per acabar, donem les eines per a poder enunciar la conjectura.

Introduim breument la m-torsió del mòdul de Carlitz que utilitzarem més endavant. Donarem per conegudes algunes nocions, tot i així, podeu consultar el Capítol 2 de [Gos], ja que, seguirem la mateixa notació, o el Capítol 2 de [TN]. Definint $k = \mathbb{F}(T)$, $\overline{k}$ la clausura separable de k i $C_a(X)$ el polinomi de Carlitz en a ([TN], pàgina 20, proposició 2.2.1).

Definició 4.1.1 *Sigui K una extensió de $\mathbb{F}(T)$, definim l'acció de Carlitz de $\mathbb{F}[T]$ sobre K fent que $\mathbb{F}[T]$ actui sobre K amb els polinomis de Carlitz, on $M \in \mathbb{F}[T]$ i $\alpha \in K$,*

$$M \cdot \alpha = C_M(\alpha).$$

Definim el mòdul de Carlitz com el $\mathbb{F}[T]$-mòdul per l'acció de Carlitz $C(\overline{\mathbb{F}(T)})$, on $\overline{\mathbb{F}(T)}$ és la clausura separable de $\mathbb{F}(T)$.

Definició 4.1.2 *Definim la m-torsió del mòdul de Carlitz com, on m ideal de $\mathbb{F}[T]$,*

$$\Lambda_m = \{\lambda \in \overline{k} | C_a(\lambda) = 0,\, a \in m\}.$$

Exemple 4.1.1 *Veiem l'exemple de T^2-torsió del mòdul de Carlitz, on $\mathbb{F}$ té p elemets. Com $C_{T^2}(X) = X^{p^2} + (T^p + T)X^p + T^2X = X(X^{p^2-1} + (T^p + T)X^{p-1} + T^2)$. Obtenim que*

$$\Lambda_{T^2} = \{\lambda \in \overline{\mathbb{F}(T)} | = \lambda^{p^2} + (T^p + T)\lambda^p + T^2\lambda) = 0\} = \{0\} \cup \{\lambda \mid \lambda^{p^2-1} = -(T^p + T)\lambda^{p-1} - T^2\} =$$
$$= \{0\} \cup \{\lambda \mid \lambda^{1-p}(\lambda^{-p} + T^2) = -(T^p + T)\}.$$

Teorema 4.1.2 *(Teorema de Carlitz, 1930) Donada $L/\mathbb{F}(T)$ Galois, finita i abeliana, on L té cos de constants $\mathbb{F}$ i l'ideal primer $1/T = \infty$ esplita totalment en L llavors existeix un ideal m de $\mathbb{F}[t]$ complint que $L \subseteq \mathbb{F}(t)[\Lambda_m]$. Si $1/T$ no esplita completament, també hi ha un resultat dins un cos $\mathbb{F}(T)$(torsio Carlitz) on L està a dins.*

Observeu que el teorema de Carlitz és l'anàleg del teorema de Weber per les extensions abelians de $\mathbb{Q}$ que estan dins $\mathbb{Q}(e^{\frac{2\pi i}{n}})$ per cert n. Drinfeld i Hayes generalitza el resultat de Carlitz per L/k cossos globals de característica $p > 0$ on $k \neq \mathbb{F}(T)$ durant els 1970's.

Sigui K/k una extensió abeliana de cossos globals de grau n, i G el seu grup de Galois. Sigui S un conjunt no buit finit de primers de k que conté tots els primers que ramifiquen en K, i en el cas de cossos numèrics, tots els primers arquimedians.

[14] Cal remarcar que, en aquestes demostracions, utilitzen eines diferents: [Lan2] usa el caràcter de Teichmüller i [Was] treballa amb l'ideal de Stickelberger.

Ara, escriurem $\theta_{K/k,S}(w) = \theta(w) \in \mathbb{C}[G]$, anomenada la L-funció evaluadora, en termes de funcions zeta parcials. Per $\sigma \in G$ la definició de la funció zeta parcial $\zeta_S(s,\sigma)$, amb $s \in \mathbb{C}$ i $\sigma \in G$ fixat, ve donada per

$$\zeta_S(s,\sigma) = \sum_{D,(D,S)=1,(D,K/k)=\sigma} N(D^{-s}).$$

En tots els casos, la suma és absolutament convergent en la regió $Re(s) > 1$, i totes aquestes funcions tenen extensió analítica al pla complex sencer amb, com a màxim, un pol simple en $s = 1$. En el cas del cos de funcions la suma és sobre tots el divisors que el seu suport no conté primers en S i el seu símbol d'Artin, $(D, K/k)$, és igual a σ (podeu veure més detalls del símbol d'Artin amb la mateixa notació en [Lan], Secció 10.1, pàgina 197). En el cas del cos numèric la suma és sobre tots els ideals integrals en l'anell d'enters de k que són primers a S i que el símbol d'Artin,$(D, K/k)$, és igual a σ.

En la definició següent veiem una expressió de $\theta(w)$, i els preliminars necessàries en [Ros], pàgina 266, Proposició 15.11, amb la Proposició 15.10 del mateix llibre i un repàs de les L-funcions.

Definició 4.1.3

$$\theta(w) := \theta_{K/k,S}(w) := \sum_{\sigma \in G} \zeta_S(w,\sigma)\sigma^{-1}.$$

Els valors de la funció zeta parcial $\zeta_S(w,\sigma)$ en $w = 0$ són especialment importants. De fet, són nombres racionals i tenim un bon control dels seus denominadors. Més detalladament, enunciem el següent teorema.

Teorema 4.1.3 *Sigui W_K el nombre d'arrels de la unitat en K, es té*

(1) $\theta_S(0,\sigma) \in \mathbb{Q}$.

(2) $W_K\theta_S(0,\sigma) \in \mathbb{Z}$.

La part (1) va ser primerament demostrada, en el cas de cossos numèrics, per Carl Ludwig Siegel en *Berechnung Von Zetafunktionen an Ganzzahligen Stellen*(1969), i la part (2), va ser primerament demostrada per Pierre Deligne i Ken Ribet en *Values of abelianL-functions at negative integers over totally real fields*(1980).

Definició 4.1.4 *Definim $\theta_{K/k,S} := \theta_{K/k,S}(0)$ i $\omega_{K/k,S} = W_K\theta_{K/k,S}$. L'element $\omega_{K/k,S}$ s'anomena l'element de Brumer de K/k relatiu a S.*

S'obté de la Proposició 4.1.1 i del Teorema 4.1.3 que $\theta_{K/k,S} \in \mathbb{Q}[G]$ i que $\omega_{K/k,S} \in \mathbb{Z}[G]$. Observem que Cl_K és un $\mathbb{Z}[G]$-mòdul.

4.2 La conjectura de Brumer-Stark per a cossos globals

Ara estem en la posició de enunciar la conjectura de Brumer-Stark en els cassos de cossos numèrics i cossos de funcions, recordem S és un conjunt finit de primers de k no buits i K/k Galois.

Conjectura de Brumer-Stark *(Cas de Cossos Numèrics) Suposem $|S| > 1$. Llavors, existeix $\omega \in \mathbb{Z}[Gal(K/k)]$, on per tot ideal fraccionari D de K (és a dir, existeix $k \in K^*$ on kD ideal de $\mathcal{O}_K$ l'anell d'enters de K) es té $\omega D = (\alpha_D)$ on $\alpha_D \in K^*$ i α_D té valor absolut 1 en tots els valors absoluts arquimedians. A més a més, si λ_D és una arrel W_K-éssima de α_D, es té $K(\lambda_D)/k$ és una extensió abeliana, on W_K és el nombre d'arrels de la unitat en K.*

Conjectura de Brumer-Stark *(Cas de Cossos Globals de característica p>0) Suposem $|S| > 1$, existeix $\omega \in \mathbb{Z}[Gal(K/k)]$, complint que per tot divisor D de K, es té $\omega D = (\alpha_D)$ amb $\alpha_D \in K^*$. Si λ_D és una W_K-éssima arrel de α_D, llavors $K(\lambda_D)/k$ és una extensió abeliana, on W_K és el nombre d'arrels de la unitat en K.*

La conjectura que ω aniquila el grup de classes és gràcies a Brumer, i la conjectura que $K(\lambda_D)/k$ és abelià és gràcies a Stark. Ara presentarem un esbòs de la seva demostració en dos cassos.

4.2.1 Cas extensió ciclotòmica

Suposem que m és un enter positiu que és senar o divisible per 4, i considerem el cos ciclotòmic $K_m = \mathbb{Q}(\zeta_m)$. Sigui S el conjunt de primers que divideixen m juntament amb els primers arquimedians de $\mathbb{Q}$. La primera tasca que tenim serà trobar l'element $s = s_{S,K_m/\mathbb{Q}}$.

Sigui $t \in \mathbb{Z}$ relativament primer amb m i $1 \leq t < m$. Sigui σ_t l'element corresponent a $Gal(K_m/\mathbb{Q})$ a $\xi_m \mapsto \xi_m^t$. Si $n > 0$ és relativament primer amb m, $\sigma_n = ((n), K_m/\mathbb{Q}) = \sigma_t$ si i només si $n \equiv t\ (mod\, m)$. Per tant,

$$\zeta_S(s, \sigma_t) = \sum_{n=1, n\equiv t(mod\, m)}^{\infty} \frac{1}{n^s} = \sum_{h=0}^{\infty} \frac{1}{(t+hm)^s},$$

amb $s \in \mathbb{C}, Re(s) >> 0$. Per a tot nombre real b amb $0 < b \leq 1$, la funció zeta de Hurwitz està definida per la fòrmula, per $Re(s) > 1$,

$$\zeta(s, b) = \sum_{h=0}^{\infty} \frac{1}{(b+h)^s}.$$

Les funcions $\zeta_S(s, \sigma_t)$, $\zeta_S(s, b)$ tenen continuació analítica a tot $\mathbb{C}$. Segueix que $\zeta_S(s, \sigma_t) = m^{-s}\zeta(s, t/m)$. Una propietat coneguda de la funció zeta de Hurwitz és que per tot enter $n \geq 1$ tenim que $\zeta(1-n, b) = -B_n(b)/n$, on $B_n(b)$ és l'n-éssim polinomi de Bernoulli (podem veure més informació al Capítol 2.2 de [Lan2]). Per $n = 1$ tenim que $B_1(b) = b - \frac{1}{2}$. S'obté

$$\zeta_S(0, \sigma_t) = \zeta(0, t/m) = \zeta(1-1, t/m) = -B_1(t/m) = \frac{1}{2} - \frac{t}{m},$$

i així

$$\theta := \theta(0) = \sum_{t=1,(t,m)=1}^{m-1} (\frac{1}{2} - \frac{t}{m})\sigma_t^{-1}.$$

Suposarem primer que m és senar. Llavors, $W_{K_m} = 2m$ i definim

$$\omega := W_{K_m}\theta = \sum_{t=1,(t,m)=1}^{m-1} (m-2t)\sigma_t^{-1} = m\mathscr{N} - 2\sum_{t=1,(t,m)=1}^{m-1} t\sigma_t^{-1}.$$

on, $\mathscr{N} = \sum_{\sigma\in G}\sigma$ és l'aplicació norma. Sigui ara P un primer de K_m coprimer amb m. Llavors, utilitzant l'expressió explícita de que hem trobat de ω i el teorema de Stickelberger 4.1.1, trobem que

$$\omega P = (\frac{\mathscr{N}(P^m)}{\phi(P)^2}) = (\frac{\mathscr{N}(P^m)}{g(P)^{2m}})$$

Això verifica la primera part de la conjectura de Brumer-Stark quan $D = P$ és un ideal primer coprimer amb m on $\alpha_P = \mathscr{N}(P^m)/g(P)^{2m}$.

Per la Proposició 4.1.1, part 2, α_P té valor absolut igual a 1. Podem verificar utilitzant les propietats les propietats de Galois de les sumes de Gauss, que tot conjugat de Galois de α_P té també valor absolut 1. Això verifica la segona part de la conjectura. Finalment, com que $W_K = 2m$ en el cas que estem considerant, trobem que $\lambda_P = \mathscr{N}(P^{1/2})/g(P)$ tal que $K_m(\lambda_P) \subseteq \mathbb{Q}(\zeta_m, \zeta_p, \sqrt{\mathscr{N}(P)})$ que és abelià sobre $\mathbb{Q}$. Si m és senar, la conjectura de Brumer-Stark sencera per qualsevol divisor D primer amb m s'obté. Altres casos són petites modificacions que no explicitarem aquí.

4.2.2 Cos de global en característica p>0

Ara centrarem la nostra atenció al cas de cossos de funcions. Per facilitar l'explicació ens restringirem a les extensions abelianes K/k que són geomètriques, és a dir, ambós K i k tenen el mateix cos constant,$\mathbb{F}$, que és el cos finit amb q elements. Sota aquesta condició, el grup d'unitats de K

es justament $\mathbb{F}^*$, així doncs $W_K = q-1$.

Abans però, enunciem un teorema de John Tate que no demostrarem, però la seva demostració es pot trobar a [Ros], de la pàgina 275 fins la 277, i sugerim llegir la pàgina 269 del mateix llibre.

Teorema 4.2.1 *Sigui K/k una extensió finita geomètrica (és a dir, K i k tenen el mateix cos de constants $\mathbb{F}$ finit) i abeliana de cossos de funcions global amb característica $p>0$ i grup de Galois G. Sigui $\omega = (q-1)\theta(0) \in \mathbb{Z}[G]$ l'element de Brumer. Llavors, per a tot divisor D de K de grau 0, es té $\omega D = (\alpha_D)$, un divisor principal de K. En altres paraules, ω aniquila el grup de classes de divisors de grau 0, Cl_K^o.*

La nostra tasca següent és utilitar aquest resultat per demostrar a la conjectura de Brumer-Stark sencera pel cas de els cossos de funcions ciclotòmics $K_m = k(\Lambda_m)$ i $K_m^+ = k(\Lambda_m)^+$, el subcós real maximal de K_m, que consisteix en el cos fix de $\{\sigma_\alpha \in Gal(K_m/k) | \alpha \in \mathbb{F}^*\}$ (podeu trobar més detalls a pàgina 212, Teorema 12.14, i pàgina 213 de [Ros]). Observem que K_m denota ara el cos de funcions ciclotòmic generat per afegir la m-torsió en el mòdul de Carlitz al cos de funcions racionals $k = \mathbb{F}(T)$. Aquí m és un polinomi no constant mònic de grau $M \geq 1$ en l'anell $A = \mathbb{F}[T]$.

El conjunts S i S^+ corresponents a K_m/k i K_m^+/k consistiràn en els primers ramificats, que correspon a $S = \{P : P|m\} \cup \{\infty\}$, i $S^+ = \{P : P|m\}$. Per la Proposició 12.4 de la pàgina 201 de [Ros], sabem que ∞ és ramificat en K_m i esplita completament en K_m^+ (és a dir, $\infty B = \infty_1 \cdots \infty_k$ on B és la clausura entera de $\mathbb{F}[1/t]$ en K_m^+, i $f_{\infty_i/\infty} = 1$ per $i = 1, ..., k$). Ara volem calcular $\theta := \theta_{K_m/k,S}$ i $\theta^+ := \theta_{K_m^+/k,S^+}$.

Proposició 4.2.1 *Amb les definicions i notacions anteriors s'obté: per a $a \in \mathbb{F}[t]$, $\sigma_a \in Gal(K_m/k)$:*

(1) $\theta = \sum_{a\, monic, grau(a)<M,(a,m)=1} \sigma_a^{-1} - \frac{1}{q-1}N$.

(2) $\theta^+ = \sum_{a\, monic, grau(a)<M,(a,m)=1} (M - grau(a) - 1)\sigma_a^{-1} - \frac{1}{q-1}N^+$.

En la part 1, $N = \sum_{\sigma \in Gal(K_m/k)} \sigma$, i la part 2, $N^+ = \sum_{\sigma \in Gal(K_m^+/k)} \sigma$, és a dir, les aplicacions norma.

Demostració. Recordem que $Gal(K_m/k) = \{\sigma_a | (a,m) = 1\, i\, grau(a) < M\}$. Sigui λ_m el generador de Λ_m com un $\mathbb{F}[t]$-mòdul. Si $\sigma \in Gal(K_m/k)$, llavors $\sigma\lambda_m$ és un altre generador. Per tant, existeix $a \in A = \mathbb{F}[t]$ amb $(a,m) = 1$ tal que $\sigma(\lambda_m) = C_a(\lambda_m)$. L'automorfisme σ queda totalment determinat per aquesta relació, ja que, λ_m genera K_m sobre k. Observem a és determina fins un múltiple de m. Escrivim $\sigma = \sigma_a$. L'aplicació $\sigma \to a$ és un isomorfisme de $Gal(K_m/k) \to (A/mA)^*$ (veure apèndix A.2). Així es té que per qualsevol $a \in A$, coprimer amb m, hi ha un únic automorfisme $\sigma_a \in Gal(K_m/k)$ tal que $\sigma_a\lambda_m = C_a(\lambda_m)$. A més, $((a), K_m/k) = \sigma_a$.

Com que S consisteix en tots el primers dividint m i ∞, en la definició donada de funció zeta parcial nosaltres sumem sobre els divisors efectius relativament primers amb m sense component a ∞. Això és el mateix que sumar sobre els ideals de A que són primers respecte m. Tot ideal D té un únic generador mònic d i $N(D) = |d| = q^{grau(d)}$. Per tant, suposant que a és mònic, tenim que

$$\begin{aligned}\zeta_S(s,\sigma_a) &= \sum_{(D,S)=1,(D,K_m/k)=\sigma_a} \frac{1}{N(D)^s} = \sum_{d\, monic,(d,m)=1,\sigma_d=\sigma_a} |d|^{-s} \\ &= |a|^{-s} + \sum_{h\in A, h\, monic} |a+hm|^{-s} = |a|^{-s} + |m|^{-s} \sum_{h\, monic} |h|^{-s} \\ &= |a|^{-s} + |m|^{-s} \frac{1}{1-q^{1-s}}.\end{aligned}$$

Si a no és mònic, el càlcul és exactament el mateix però el terme $|a|^{-s}$ no apareix. Per tant, $\zeta_S(0,\sigma_a) = 1-(q-1)^{-1}$ si a és mònic i $\zeta_S(0,\sigma_a) = -(q-1)^{-1}$ si a no és mònic. L'expressió per θ donada en la part 1 s'obté directament d'aquests resultats.

Recordem ara que K_m^+ és el cos fixat de $\{\sigma_\alpha | \alpha \in \mathbb{F}^*\}$, grup inertia de K_m/k en $\infty = \frac{1}{t}$. Segueix que $Gal(K_m^+/k) = \{\sigma_a | (a,m) = 1, grau(a) < M, a\, monic\}$. Aquí identifiquem σ_a amb la seva restricció en K_m^+. Com automorfisme de K_m^+ tenim que $\sigma_d = \sigma_a$ si i només si $d \equiv \alpha a \ (mod\, m)$ per algun $\alpha \in \mathbb{F}^*$.
Com que S^+ consisteix solament en els primers dividint m, en la definició de la funció zeta parcial nosaltres sumem sobre tots els divisors efectius de la forma $D = D_f + i\infty$, on D_f és un divisor efectiu primer respeccte m i ∞, on i és un enter no negatiu. Com abans, D_f correspon a un ideal de $A = \mathbb{F}[t]$ amb un genereador mónic d que es primer respecte m.
Com que ∞ esplita completament en K_m^+ tenim que $(\infty, K_m^+/k) = e$. Per tant, per a mònic obtenim

$$\zeta_{S^+}(s, \sigma_a) = \sum_{(D,S^+)=1,(D,K_m^+/k)=\sigma_a} \frac{1}{N(D)^s} = \sum_{i=0}^{\infty} \sum_{(D_f,K_m^+/k)=\sigma_a} \frac{1}{N(D_f + i\infty)^s}.$$

Ara, $N(D_f + i\infty) = N(D_f)N(\infty)^i = |d|q^i$. Per tant, podem reescriure l'expressió com

$$\zeta_{S^+}(s, \sigma_a) = \sum_{i=0}^{\infty} \sum_{d\, monic, \sigma_d = \sigma_a} |d|^{-s} q^{-is} = \frac{1}{1 - q^{-s}} \sum_{d\, monic, \sigma_d = \sigma_a} |d|^{-s}.$$

on d recorre els polinomis mònics de $\mathbb{F}[t]$ coprimers amb m i complint $\sigma_d = \sigma_a$. Com hem comentat, aquesta condició es compleix si i només si $d \equiv \alpha a \ (mod\, m)$ per algun $\alpha \in \mathbb{F}^*$, que és equivalent a la condició $\alpha^{-1} d \equiv a \ (mod\, m)$. En altres paraules, podem sumar sobre tot $d \in A$ (no únicament els mònics) amb $d \equiv a \ (mod\, m)$. Per tant,

$$\sum_{d\, monic, \sigma_d = \sigma_a} |d|^{-s} = \sum_{d \in A, d \equiv a \, (mod\, m)} |d|^{-s} = |a|^{-s} + \sum_{h \in A, h \neq 0} |a + hm|^{-s} =$$

$$= |a|^{-s} + (q-1)|m|^{-s} \sum_{h\, monic} |h|^{-s} = |a|^{-s} + \frac{q-1}{1 - q^{1-s}} |m|^{-s}.$$

Ajuntat-ho tot, obtenim

$$\zeta_{S^+}(s, \sigma_a) = (1 - q^{-s})^{-1} (|a|^{-s} + (q-1)(1 - q^{1-s})^{-1} |s|^{-s})$$
$$= \frac{(1 - qu) u^{grau(a)} + (q-1) u^{grau(m)}}{(1-u)(1-qu)},$$

substituint $u = q^{-s}$. Hem de evaluar la funció en $s = 0$, o equivalentment en $u = 1$. Si fem la substitució de $u = 1$ en l'expressió anterior, el numerador i el denominador s'anul·len. Apliquem doncs, la regla d'Hôpital, diferenciant el numerador i el denominador i llavors substituïnt $u = 1$. El resultat és

$$\zeta_{S^+}(0, \sigma_a) = grau(m) - grau(a) - 1 - \frac{1}{q-1},$$

d'on sobté la segona part. □

Definim ara,

$$\eta = \sum_{a\, monic, grau(a) < M, (a,m)=1} \sigma_a^{-1}, \ \eta^+ = \sum_{a\, monic, grau(a) < M, (a,m)=1} (M - grau(a) - 1) \sigma_a^{-1}.$$

Ara podem escriure $\theta = \eta - (q-1)^{-1} \mathscr{N}$ i $\theta^+ = \eta^+ - (q-1)^{-1} \mathscr{N}^+$. També, pels elements de Brumer tenim que $\omega = (q-1)\theta = (q-1)\eta - \mathscr{N}$ i $\omega^+ = (q-1)\eta^+ - \mathscr{N}^+$.

Proposició 4.2.2 *L'element η aniquila $Cl^o_{K_m}$ i l'element η^+ aniquila $Cl^o_{K_m^+}$.*

La demostració d'aquest teorema es demostra com un corol·lari de la demostració del Teorema 4.2.1 i la podem trobar a [Ros], a les pàgines 277 i 278.

L'últim recurs que necessitem per a demostrar la conjectura de Brumer-Stark per K_m/k i K_m^+/k és la descomposició en primers d'un punt de m-torsió primitiu en el mòdul de Carlitz. El fet clau és que aquesta descomposició ve donada essencialment per l'element de Brumer ω^+, l'element de la conjectura.

Proposició 4.2.3 *Sigui $\mathfrak{B}_\infty$ un primer de K_m sobre ∞ en $\mathbb{F}(t)$. Llavors existeix un punt de m-torsió primitiu $\lambda \in \Lambda_m$ tal que*

$$(\lambda) = ((q-1)\eta^+ - \eta)\mathfrak{B}_\infty + \mathfrak{B}_m.$$

L'element η^{q-1} està en K_m^+. Com element de K_m^+ la seva descomposició en primers ve donada per

$$(\lambda^{q-1}) = \omega^+\mathfrak{B}_\infty^+ + \mathfrak{B}_m^+.$$

Aquí, $\mathfrak{B}_m$ és l'únic primer de K_m que cau sobre P si $m = P^s$ és una potència d'un primer i és el divisor del zero altrament. $\mathfrak{B}_m^+$ és el primer de K_m^+ que cau en $\mathfrak{B}_m$. Finalment, $\mathfrak{B}_\infty^+$ és el primer de K_m^+ que cau en $\mathfrak{B}_\infty$ (recordem que K_m/k és totalment ramificat en el primers p de $\mathbb{F}(t)$ amb $(m,p) = p$).

El lector interessat en la demostració consulteu [Ros], pàgines 272 i 273, Proposició 15.17.

Ara hem introduit el preliminars necessàris per demostrar la conjectura de Brumer-Stark per a K_m/k i K_m^+/k.

Teorema 4.2.2 *Sigui $k = \mathbb{F}(t)$, $K_m = k(\Lambda_m)$, i $K_m^+ = k(\Lambda_m)^+$. La conjectura Brumer-Stark és vàlida per a K_m/k i K_m^+/k.*

Demostració. Sigui D un divisor qualsevol de K_m. Com que $\mathfrak{B}_\infty$ té grau 1 podem escriure $D = D_0 + t\mathfrak{B}_\infty$, on $t = grau(D)$ amb D_0 de grau zero. Com que el grup de descomposició de $\mathfrak{B}_\infty$ és $\{\sigma_\alpha | \alpha \in \mathbb{F}^*\}$ s'obté $N(\mathfrak{B}_\infty) = (q-1)\eta\mathfrak{B}_\infty$. Per tant, recordem $\omega = (q-1)\eta - \mathscr{N}$,

$$\omega\mathfrak{B}_\infty = ((q-1)\eta - \mathscr{N})\mathfrak{B}_\infty = \mathscr{N}(\mathfrak{B}_\infty) - \mathscr{N}(\mathfrak{B}_\infty) = 0.$$

Pel Teorema 4.2.1 s'obté $\omega D = \omega D_0 = (\alpha_D)$ per algún $\alpha_D \in K_m^*$. Això prova la primera part de la conjectura per K_m/k. Per la segona part, demostrarem el resultat següent. Considerem que ηD_0 principal, escrivim $\eta D_0 = (\beta_D)$. Notem també que $N(D_0) = (d)$ on $d \in k^*$, ja que Cl_k^o és trivial (k=$\mathbb{F}(t)$ correspon a linia projectiva sobre $\mathbb{F}$ i fàcilment, Cl_k^o és trivial). Per tant,

$$\omega D = \omega D_0 = (q-1)\eta D_0 - N(D_0) = (\beta_D^{q-1}) - (d) = (\beta_D^{q-1}d^{-1}).$$

Triem $\alpha_D = \beta_D^{q-1}d^{-1}$, observem que cos generat per $\lambda_D = \sqrt[q-1]{\alpha_D}$ sobre K_m és el mateix que el cos generat sobre K_m per $\sqrt[q-1]{d}$. Ara, $k(\sqrt[q-1]{d})/k$ és una extensió de Kummer[15]. Per tant, $K_m(\lambda_D)$ és la composició de dues extensions abelianes de k, en particular, K_m i $k(\sqrt[q-1]{d})$, i així és també una extensió abeliana de k per ser disjuntes sobre k. Això completa la demostració per K_m/k.

Ara considerem el cas K_m^+/k. Una vegada més, sigui D un divisor qualsevol de K_m^+ pot ser expressat de la forma $D_0 + t\mathfrak{B}_\infty^+$, on $t = grau(D)$. Pel Teorema 4.2.1, on recordem $\omega^+ = (q-1)\eta^+ - \mathscr{N}^+$, trobem que $\omega^+ D_0 = (\alpha_{D_0})$ és principal. De la Proposició 4.2.3, tenim que $\omega^+\mathfrak{B}_\infty^+ = (\lambda^{q-1}) - \mathfrak{B}_m^+$. Per tant,

$$\omega^+ D = (\alpha_{D_0}\lambda^{(q-1)t}) - t\mathfrak{B}_m^+,$$

que verifica la primera part de la conjectura de Brumer-Stark per K_m^+/k. Ara, per demostrar la segona part de la conjectura utilitzarem la Proposició 4.2.2 per veure que $\eta^+ D_0 = (\beta_{D_0})$ és principal. Segueix que

$$\omega^+ D_0 = ((q-1)\eta^+ - N^+)D_0 = (\beta_{D_0}^{q-1}d^{-1}),$$

on $d \in k^*$ tal que $N^+(D_0) = (d)$. Per tant, podem agafar $\alpha_{D_0} = \beta_{D_0}^{q-1}d^{-1}\lambda^{(q-1)t}$. D'això podem veure que λ_D^+, que és l'(q-1) arrel de α_D, genera el mateix cos sobre K_m com $\sqrt[q-1]{d}$. Per tant, $K_m^+(\lambda_D^+)$ està contingut en $K_m(\sqrt[q-1]{d})$, que és abelià sobre k similarment com K_m/k. Finalitzant la prova per $K_m^+/\mathbb{F}(t) = k$.

□

[15] Una extensió de Kummer és una extensió de cossos L/K, on donat un enter $n > 1$ verifica que K conté n diferents arrels n-éssimes de l'unitat((n,p)=1 per no trivials), i L/K té un grup de Galois abelià d'exponent n

5 Alguns resultats referents al nombre de classes per a cossos globals ciclotòmics.

Un dels problemes clàssics en Teoria de Nombres era estudiar les solucions de l'equació de Fermat $X^p + Y^p = Z^p$ amb p primer ≥ 5. Kummer va fer el primer avenç important quan va demostrar que si p no divideix l'ordre del grup de classes de $\mathbb{Z}[e^{2\pi i/p}]$ (anell d'enters del cos de nombres $K_p = \mathbb{Q}(e^{2\pi i/p})$) llavors el teorema de Fermat era correcte, i per tant l'equació diofantina anterior no tenia solució amb $XYZ \neq 0$.
Aquest fet va inspirar a estudiar l'ordre de grups de classes en extensions, i Iwasawa va començar amb la extensió de posar arrels de la unitat sobre una corba algebraica sobre un cos finit $\mathbb{F} = \mathbb{F}_q$ de q elements, on $q = p^n$, és a dir un cos global K_0 de característica positiva $p > 0$ amb cos de constants $\mathbb{F}$, és a dir va començar a estudiar com es comporta l'ordre del grup de classes d'ideals en $K_n = K_0\mathbb{F}_{q^n}$ on va trobar-ne una condició lineal, fixem-nos que posem a K_0 les arrels de $\mathbb{F}_{q^n}$ que són les arrels de la unitat $X^{q^n-1} - 1$ en un cos de característica $p > 0$.
Iwasawa trasllada doncs estudi a l'extensió de $\mathbb{Q}$ d'introduir les arrels de la unitat. Fixeu-vos que aquestes extensions son abelianes sobre el cos base, K_0 o $\mathbb{Q}$ respectivament. No obstant en el mon de característica positiva hi ha una altra manera de traslladar les arrels de la unitat. Podem pensar que afegir les arrels de l'unitat corresponen a posar la torsió del grup lineal $GL_1(\overline{K})$ on $\overline{K}$ es la clausura separable de un cos K, en el cas $K = \mathbb{Q}$ pensem $\overline{\mathbb{Q}} \subset \mathbb{C}$, i en K_0 correspon a les extensions K_n. En característica positiva Carlitz va descobrir que posar la torsió del grup additiu aconseguia extensions de cossos de $K_0 = \mathbb{F}_q(T)$, Galois i abelianes amb propietats de ramificació i comportament com l'extensió ciclotòmica de $\mathbb{Q}$. Aquesta torsió a afegir a $\mathbb{F}_q(T)$ consistia a posar arrels de polinomis aditius (es dir $P(X + Y) = P(X) + P(Y)$) definits pel que s'anomena mòdul de Carlitz, que sobre $\mathbb{F}_q[T]$ (domini de Dedekind dins $\mathbb{F}_q(T)$), on aquests polinomis venen definits via $C : \mathbb{F}_q[T] \to \mathbb{F}_q[T]\{\tau\}$ via $C(T) := T\tau^0 + \tau = Tid + \tau$ on C és $\mathbb{F}_q$-lineal i morfisme d'anells on $\tau f = f^q\tau$ per a $f \in \mathbb{F}_q[T]$. El polinomi additiu corresponent a $C(f)$ s'obté de substituir τ per X^q, i $\tau^0 = X$ (penseu $\mathbb{F}_q[T]\{\tau\}$ correspon als endomorfismes del grup additiu). Per tant es natural comparar el grup de classes en aquesta extensió Carlitz-ciclotòmica, i comparar-ne els resultats amb els de la torre ciclotòmica. L'estudi d'aquests grups de classes, en el cas Carlitz-ciclotòmica i ciclotòmica són encara tema de recerca.
Lamentablement, en aquest treball, just enunciaré alguns dels resultats inicials i el resultat de Iwasawa, qui va primer traslladar de corbes sobre cossos finits a característica zero, però que recentment en torna a característica positiva en cossos globals estudiant l'extensió Carlitz-ciclotòmica o altres donades per Hayes-Drinfeld.

5.1 Extensions de cossos constants

Marcarem la notació i després donarem la fòrmula per aquest cas, sense demostració, i alguns resultats relacionats. Sigui K un cos global de característica $p > 0$ i cos de constants $\mathbb{F}$ amb q elements. Fixem una clausura algebraica $\bar{\mathbb{F}}$ de $\mathbb{F}$, i sigui $\mathbb{F}_n$ l'únic subcòs de $\bar{\mathbb{F}}$ tal que $[\mathbb{F}_n : \mathbb{F}] = n$ (recordem que aquesta seria extensió ciclotòmica amb arrels de l'unitat de $x^{q^n} - x = 0$ on $q = |\mathbb{F}|$). Sigui $K_n = K\mathbb{F}_n$ l'extensió de cossos constant de K per $\mathbb{F}_n$ i $h(K_n)$ el nombre de classes per K_n. Per definició, $h(K_n)$ és el nombre d'elements de $Cl^o_{K_n}$.

La fòrmula en aquesta cas ve donada per

$$h(K_n) = \prod_{i=1}^{2g}(1 - \pi_i^n),$$

on g denota el gènere de K, i π_i són les arrels d'un cert polinomi L_K de grau doble que el gènere i coeficients enters amb terme constant 1. La demostració d'aquesta fòrmula es pot trobar a [Ros], pàgina 110, Proposició 8.16, però caldrà una lectura sencera del Capítol 8. Un fet curiós, es que, per l'hipòtesis de Riemann, $|\pi_i| = \sqrt{q}$ per $1 \leq i \leq 2g$. Utilitzant això i la fòrmula anterior, podem trobar una cota inferior per $h(K_n)$:

$$h(K_n) \geq (q^{n/2} - 1)^{2g}.$$

Si $K = \mathbb{F}_q(T)$ es té $h_K = 1$ (de $Cl(K) \cong Cl(\mathbb{F}_q[T])$, $q = p^n$). Considerem aquí K_1 una extensió finita separable de K i $K_n := K_1\mathbb{F}_{q^n}$, i per a ℓ un primer coprimer amb p. Denotem per $d(\ell)$ al minim comú multiple dels nombres $\ell^k - 1$ per a $1 \leq k \leq 2g$ on g és el gènere de la corba associat al cos K_1 (veieu el capítol 2).

Lema 5.1.1 *Sigui ℓ un primer diferent de p que no divideix h_K amb $mcd(n, d(\ell)) = 1$ llavors ℓ no divideix h_{K_n}.*

Lema 5.1.2 *Sigui ℓ un primer diferent de p que divideix h_K. Si ℓ divideix $n \cdot \frac{q^n-1}{q-1}$ llavors ℓ divideix h_{K_n}/h_K.*

Lema 5.1.3 *Sigui n el natural més petit complint que ℓ divideix h_{K_n}. Llavors n divideix $d(\ell)$.*

Amb l'estudi de la torre $K_1 \subseteq K_2 \subset \ldots$, Iwasawa als anys 1960's demostra el següent resultat (que després ho traslladarà a l'extensió ciclotòmica)

Teorema 5.1.1 *(Iwasawa) Sigui e_n el ordre o la valoració en ℓ de $h_{K_{\ell^n}}$, on ℓ un primer racional coprimer amb p. Existeixen invariants λ_ℓ i ν_ℓ complint que existein un natural n_0 on per a tot $n \geq n_0$ es té*

$$e_n = \lambda_\ell \cdot n + \nu_\ell$$

i per tant els nombres e_n creixen linealment en n.

Podeu trobar una demostració d'aquests resultats a [Ros], capítol 11.

5.2 Extensions ciclotomiques dels racionals

Considerem el cossos ciclotòmics $K_m = \mathbb{Q}(\zeta_m)$ i $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, fix per la conjugació complexa, cos real.. Denotem el nombre de classes de K_m per h_m, i el nombre de classes de K_m^+ per h_m^+. Es demostrar que $h_m^+ | h_m$ ([Ros], pàgina 300) i escrivim $h_m = h_m^+ h_m^-$, on h_m^- és un enter anomenat nombre de classes relatiu.

Per a coprimer amb m, sigui $\sigma_a \in Gal(K_m/\mathbb{Q})$ l'automorfisme $\zeta_m \mapsto \zeta_m^a$. Això indueix a un isomorfisme $(\mathbb{Z}/m\mathbb{Z})^* \cong Gal(K_m/\mathbb{Q})$. Fixem-nos que σ_{-1} és la conjugació complexa. Qualsevol caràcter de $Gal(K_m/\mathbb{Q})$ pot ser pensat com un caràcter en $(\mathbb{Z}/m\mathbb{Z})^*$ via isomorfisme. Anomenem χ un caràcter parell si $\chi(-1) = 1$ i un caràcter senar si $\chi(-1) = -1$. Com que -1 correspon a la conjugació complexa , podem veure que els caràcters parells estàn en correspondència un a un amb els caràctes de $Gal(K_m^+/\mathbb{Q})$.

Ara ens restringirem, en el següents 2 teoremes en el cas on $m = p$, un primer senar. Aquests teoremes els enunciarem però no demostrarem.

Teorema 5.2.1 *Sigui h_p^- el nombre de classes relatiu de $\mathbb{Q}(\zeta_p)$. Llavors,*

$$h_p^- = 2p \prod_{\chi \, senar} (-\frac{1}{2} \sum_{a=1}^{p-1} \chi(a) \frac{a}{p}),$$

on el produce és sobre tots els caràcters senars de $(\mathbb{Z}/m\mathbb{Z})^*$.

El resultat anterior és gràcies a Kummer.

Per un resultat de cossos de funcions ciclotòmics (Secció 3.5, pàgina 84 de [Lan2]), sabem que $\frac{\zeta_p^a - 1}{\zeta_p - 1}$ són unitats en el cos K_p. Suposant que $K_p \subset \mathbb{C}$ podem agafar $\zeta_p = e^{\frac{2\pi i}{p}}$. Llavors

$$\frac{\zeta_p^a - 1}{\zeta_p - 1} = e^{\frac{\pi i}{p}(a-1)} \frac{sin(\pi a/p)}{sin(\pi/p)}.$$

L'element $e^{\frac{\pi i}{p}(a-1)}$ és una arrel $2p$-éssima de l'unitat i per tant, és una unitat de K_p. Per tant, els elements

$$\frac{sin(\pi a/p)}{sin(\pi/p)} \; per \; a = 2, 3, ..., p-1$$

són unitats en K_p i, de fet, són unitats en K_p^+.

Teorema 5.2.2 *Sigui C_p^+ el subgrup d'unitats en K_p^+ generat per les unitats*

$$\frac{sin(\pi a/p)}{sin(\pi/p)} \; per \; 1 < a < \frac{p}{2},$$

i per ± 1. Sigui E_p^+ el grup sencer d'unitats de K_p^+. Llavors, $h_p^+ = [E_p^+ : C_p^+]$.

La demostració la podem trobar a [Lan2], Capítol 3, Secció 5.

Sigui $r \in \mathbb{R}$ un nombre real qualsevol. Llavors, hi ha un únic enter $n \in \mathbb{Z}$ tal que $0 \leq r - n \leq 1$. Definim $n = [r]$, i $r - n = \langle r \rangle$. La darrera quantitat s'anomena la part fraccional de r. Notem que si $a, m \in \mathbb{Z}$ i $m \neq 0$, llavors $\langle \frac{a}{m} \rangle$ depèn només en el residu de classe de a mòdul m. Escriurem $G_m = (\mathbb{Z}/m\mathbb{Z})^*$ i $G_m^+ = G_m/(\pm 1)$.

Sigui χ un caràcter senar de $(\mathbb{Z}/p\mathbb{Z})^*$ i definim el nombre de Bernoulli generalitzat com

$$B_{1,\chi} = \sum_{a=1}^{p-1} \chi(a) \langle \frac{a}{p} \rangle.$$

Com que $\chi(a)$ i $\langle \frac{a}{p} \rangle$ només depèn en a mòdul p podem reescriure com

$$B_{1,\chi} = \sum_{a \in G_p} \chi(a) \langle \frac{a}{p} \rangle.$$

En l'expressió substituim $-a$ per a i utilitzant el fet que χ és senar obtenim que

$$B_{1,\chi} = \sum_{a \in G_p} -\chi(a) \langle \frac{-a}{p} \rangle.$$

Ara, sumant les dues expressions per $B_{1,\chi}$ i trobem

$$B_{1,\chi} = \frac{1}{2} \sum_{a \in G_p} \chi(a) (\langle \frac{a}{p} \rangle - \langle \frac{-a}{p} \rangle).$$

Ara com els termes a sumar són invariants sota la substitució $a \to -a$, obtenim l'expressió final per $B_{1,\chi}$,

$$B_{1,\chi} = \sum_{a \in G_p^+} \chi(a) (\langle \frac{a}{p} \rangle - \langle \frac{-a}{p} \rangle).$$

Observació: *Podem trobar una altra fòrmula que es pot obtenir del teorema 5.1.1 i l'expressió que hem trobat pel nombre de Bernoulli generalitzat, podem veure que*

$$h_p^- = \pm \frac{2p}{2^{\frac{p-1}{2}}} \prod_{\chi \; senar} \sum_{a \in G_p^+} \chi(a) (\langle \frac{a}{p} \rangle - \langle \frac{-a}{p} \rangle) = \pm \frac{2p}{2^{\frac{p-1}{2}}} \prod_{\chi \; senar} B_{1,\chi} = \pm \frac{2p}{2^{\frac{p-1}{2}}} \prod_{1 \leq k \leq \frac{p-1}{2}} B_{1,\omega^{2k+1}},$$

on hem utilitzat la notació de ω^{2k+1} per designar el caràcters senars.

Exemple 5.2.1 *Volem calcular el nombre de classes de $\mathbb{Q}(\zeta_{23})$. Per fer-ho utilitzarem que $h_{23} = h_{23}^- h_{23}^+$. La raó la veurem a continuació, amb l'ajuda del Magma.*
Pel càlcul de h_{23}^+, utilitzarem el Magma de la següent forma:

```
R<x> := PolynomialRing(IntegerRing());
C<c> := CyclotomicField(23);C;
f := MinimalPolynomial(c + c^-1);
M<m> := NumberField(f);M; //aqui creem el subcos real maximal

MinkowskiBound(C);
MinkowskiBound(M);

ClassNumber(M);
```

On obtenim que $h_{23}^{+} = 1$. Una raó de perquè podem calcular-lo ve donat per la cota de Minkowski. La cota de Minkowski per $\mathbb{Q}(\zeta_{23} + \zeta_{23}^{-1})$ és 90, mentre que la cota per $\mathbb{Q}(\zeta_{23})$ és 9324406. Llavors, amb un ordinador, podem calcular la factorització de primers en el rang en un cas, però en l'altre no (tot i que, aquest mètode servira fins p=31, on p primer senar).
Per calcular, el nombre de classes relatiu, tenim les fòrmules que hem vist anteriorment. Inclòs podem utilitzar una en termes dels nombrs de Bernoulli generalitzats que s'obté del Teorema 5.1.1 i la definició d'aquests nombres. Llavors podem veure:

$$h_{23}^{-} = -\frac{23}{2^{10}} \prod_{1 \leq k \leq 11} B_{1,\omega^{2k+1}}$$

Tot i així, l'implementació del càlcul dels nombres de Bernoulli generalitzats encara no està feta. Per obtenir aquest terme he consultat [New], i podem veure que $h_{23}^{-} = 3$. A [New] arriba al càlcul fins $p < 200$, però hi han altres autors com S. Pajunen o D.H.Lehmer i J.M.Masley, que han arribar fins $p < 521$.[16]
Així, el nombre de classes de $\mathbb{Q}(\zeta_{23})$ és $h_{23} = h_{23}^{-} h_{23}^{+} = 3 \cdot 1 = 3$.

Teorema 5.2.3 *Es té: $p \nmid h_p$ si i només si $p \nmid h_p^{-}$*

Per tant, és molt important pels primers que $p \nmid h_p$ estudiar h_p^{-}. Considerem la torre $K = \mathbb{Q} \subset K_p \subset \ldots \subset K_{p^n} \subset \ldots$, on $K_n = \mathbb{Q}(e^{2\pi i/n})^{+}$, (fixem-nos $Gal(K_{p^n}/K) \cong \mathbb{Z}/p^n$). Iwasawa inspirat pel cas de corbes en característica positiva en l'extensió constant demostra els anys 1960 a 1970 (ho anunciem per $K = \mathbb{Q}$ però ho va demostrar per a qualsevol cos de nombres com a K),

Teorema 5.2.4 *(Iwasawa) Donat p un primer enter fix, existeixen constants μ_p, λ_p i ν_p naturals complint*

$$ord_p h_{\mathbb{Q}(e^{2\pi i/p^n} + e^{-2\pi i/p^n})} = \mu_p \cdot p^n + \lambda_p \cdot n + \nu_p$$

per a n suficientment gran. A més per $K = \mathbb{Q}$ tenim $\mu_p = 0$.

Podeu trobar una prova en el capítol 12 de [Was]. El cas $K = \mathbb{Q}$ que és el que treballem tenim

Teorema 5.2.5 *(Washington) En el teorema anterior amb $K = \mathbb{Q}$ es té que $\mu_p = 0$, i per tant per n suficientment gran h_{p^n} és constant la seva p-valoració.*

Podeu consultar una prova en el capítol 10 de [Was].

5.3 Extensions Carlitz-ciclotòmiques

L'objectiu d'aquesta secció serà donar una anàleg al Teorema 5.2.1, en el cas de cossos de funcions ciclotòmics.

Sigui $A = \mathbb{F}[T]$, $k = \mathbb{F}(T)$, $\Lambda_m :=$ els punts de m-torsió en el mòdul de Carlitz ($m \in A$, un polinomi mònic), $K_m = k(\Lambda_m)$, i, O_m, la clausura entera de A en K_m. Tenim un isomorfisme $a \to \sigma_a$ de $(A/mA)^* \to G_m = Gal(K_m/k)$, on σ_a està caracteritzat per $\sigma_a(\lambda) = C_a(\lambda), \forall \lambda \in \Lambda_m$.

[16] Aquest terme creix molt ràpid, per exemple $h_{109}^{-} = 17 \cdot 1009 \cdot 9431866153$

Sigui $J = \{\sigma_\alpha | \alpha \in \mathbb{F}^*\}$. El cos fix de J es denota per K_m^+ i s'anomena el subcòs real maximal de K_m. Denotem per O_m^+ la clausura entera de A en K_m^+.

Amb la notació ja introduïda, donarem uns conceptes i enunciarem un teorema sense demostració, previs a l'anàleg qie hem dit. Podem definir el conductor d'un caràcter és un enter associat al caràcter d'una representació del grup de Galois d'una extensió finita en un cos. Ara concretarem la definició per la nostra situació. Sigui $G_m(\chi) \subseteq G_m$ el nucli de χ i sigui $K_m(\chi)$ el corresponent subcòs de K_m. Llavors, el conductor de χ ve donat per l'ideal $(m_\chi) \subseteq A$, on m_χ és un divisor mònic de m de grau com a mínim tal que $K_m(\chi) \subseteq K_{m_\chi} \subseteq K_m$. Com que $Gal(K_m/K_{m_\chi}) \subseteq G_m(\chi)$ podem veure χ com un caràcter en $G_{m_\chi} \cong (A/m_\chi A)^*$. Definim $M_\chi = grau(m_\chi)$. Ara podem enunciar el següent teorema.

Teorema 5.3.1 *Tenim que es verifica:*

$$(i)\ h_{K_m} = \prod_{\chi\ senar} \Big(\sum_{a\ monic, grau(a)<M_\chi} \chi(a) \Big) \prod_{\chi\ parell, \chi\neq\chi_o} \Big(\sum_{a\ monic, grau(a)<M_\chi} -grau(a)\chi(a) \Big).$$

$$(ii)\ h_{K_m}^+ = \prod_{\chi\ parell, \chi\neq\chi_o} \Big(\sum_{a\ monic, grau(a)<M_\chi} -grau(a)\chi(a) \Big).$$

Podem veure la demostració al [Ros], pàgina 291, Teorema 16.8. Ara, farem un darrera definició abans d'anar al nostre objectiu.

Definició 5.3.1 *El nombre de classes relatiu, h_m^-, està definit com $h_{K_m}/h_{K_m^+}$.*

D'on

$$h_m^- = \prod_{\chi\ senar} \Big(\sum_{a\ monic, grau(a)<M_\chi} \chi(a) \Big).$$

Suposem que $m = P$ un mònic irreductible de grau d. L'expressió anterior és simplifica a

$$h_P^- = \prod_{\chi\ senar} \Big(\sum_{a\ monic, grau(a)<d} \chi(a) \Big).$$

Per ser precisos, el producte es sobre els caràcters senars de $(A/PA)^*$. Definim, ara, $t = (q^d - 1)/(q-1)$. Llavors t és de la mida del conjunt $\mathscr{M}$, el conjunt de polinomis mònics grau menor que d. Per cada caràcter $\psi \in \mathbb{F}^*$ construïm una matriu $t \times t$, $C(\psi)$, tal que:

$$C(\psi) = [\psi(sgn\langle ab\rangle)].$$

Més conretament, escrivim $ab = cP + r$, on $r \in A$ i $grau(r) < grau(d)$. L'element r no pot ser zero, ja que, ni a ni b són divisibles per P. Llavors, $sgn(\langle ab\rangle) = sgn(r) :=$ el coeficient principal de r. Ara enunciem l'anàleg que habíem dit.

Teorema 5.3.2 *Amb tot lo anterior, tenim que*

$$h_P^- = \pm \prod_{\psi\in\mathbb{F}^*, \psi\neq\psi_o} det(C(\psi)).$$

L'extensió $K(C[f^n])$ (definida com a l'introducció l'aplicació C) amb f irreductible o primer, amb$K = \mathbb{F}(T)$ és únicament ramificada en l'ideal primer (f) que és totalment ramificada, i en el primer de infinit $1/T$ que és moderadament ramificada amb grup d'inercia i ramificació els $(a, K(C[f^n])/K)$ amb a en $\mathbb{F}^*$. En fer fix per J es fixa per la inercia de ∞, i per tant, $K(C[f^n])^+$ sol ramifica totalment en f i enlloc més.
Sigui, ara, p primer i q una potència de p. Sigui $\mathbb{F}$ un cos finit amb q elements. Per tot polinomi $Q(T) \in \mathbb{F}[T] = A$ un pot utilitzar el mòdul de Carlitz per construïr una extensió abeliana de $\mathbb{F}(T) = k$, anomenada extensió ciclotòmica de Carlitz.

Per tot polinomi $P \in A$, utilitzant el mòdul de Carlitz podem construïr una extensió $k(P)$ de k. Fixem un polinomi P, i sigui n un enter. Les extensions ciclotòmiques de k associades a P^n via mòdul de Carlitz formen una torre

$$k(P) = k(\Lambda_P) \subset k(P^2) = k(\Lambda_{P^2}) \subset \cdots k(P^n) = k(\Lambda_{P^n}) \subset \cdots .$$

Podem descompondre $h(k(P^n))$ en $h^+(k(P^n))$ i $h^-(k(P^n))$. Ara, sigui p l'únic primer que divideix q. Un resultat principal és el següent, que podem trobar demostrat a [GuoShu] pàgina 4450-4451, Teorema 2.3 i Teorema 2.4.

Teorema 5.3.3 *Si el grau del polinomi P(T) és 1, llavors $h^+(k(P^n))$ i $h^-(k(P^n))$ són congrüents amb 1 mòdul p.*

Proposició 5.3.1 *Sigui P un polinomi de grau 1. El nombre de classes $h(k(P^2))$ és asimptòtic a $q^{q(q-2)/2}$ per q prou gran.*

La demostració del darrer resultat es pot trobar també a [GuoShu] pàgina 4453, corol·lari 2.1. Podeu consultar la mateixa font per trobar més resultats sobre aquest cas en particular. Presentem una petita taula d'alguns resultats obtinguts, al calcular $h(k(P^n)), grau(P) = 1$.

n	p	h^+	h^-
1	2	1	1
2	3	1	2^2
2	5	1	$2^8 \cdot 41$
2	7	1	$2^9 \cdot 3^6 \cdot 13^2 \cdot 118147$
3	3	$2^2 \cdot 7^2$	$2^8 \cdot 7$
3	5	$2^4 \cdot 71^4$	$2^64 \cdot 3^8 \cdot 11^4 \cdot 41^3 \cdot 61^2 \cdot 101 \cdot 401 \cdot 701 \cdot 821$

En introduir la torre $K = \mathbb{F}(T)$ i f un irreductible de $\mathbb{F}[T]$ i considerar les torres de K donades per $K_{f^n} = K(C[f^n])$ d'introduir la f^n-torsió, es té $Cl(K_{f^n})$ estan relacionats amb certs θ introduïts en la secció 4 i es demostra un anàleg que l'invariant μ és igual a zero (Anglès, Bandini, Bars, Longhi, Iwasawa main conjecture for the Carlitz cyclotomic extension and applications. Math. Ann. Journal Profile 376, No. 1-2, 475-523 (2020). No obstant és massa complicat per introduir-ho en aquest treball.

Apèndixs

A Extensions ciclotòmiques en cossos globals

A.1 Extensions ciclotòmiques en cossos numèrics

Comencem per les extensions de $\mathbb{Q}$ i recordant notació. Sigui $m > 2$ un enter positiu i $\zeta_m \in \mathbb{C}$ una arrel primitiva m-èssima de l'unitat. Tenim $K_m := \zeta_>$ una extensió de Galois de $\mathbb{Q}$. Si $\sigma \in Gal(K_m/\mathbb{Q}$, llavors $\sigma(\zeta_m) = \zeta_m^a$, on és coprimer amb m. Sabem que $Gal(K_m/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ per Teoria de Galois. Si $a \in (\mathbb{Z}/m\mathbb{Z})^*$, denotem per σ_a el corresponent automorfisme, caracterizat per $\sigma_a(\zeta_m) = \zeta_m^a$. El següent teorema conté els resultats necessàris per al treball, la seva demostració es pot llegir a la pàgina 194 i 195 de [Ros].

Teorema A.1.1 *Sigui m>0 un enter que no és el doble d'un nombre senar. Sigui $\zeta_m \in \mathbb{C}$ una arrel primitiva m-èssima de l'unitat i $K_m = \zeta_>$. Llavors $K_m/\mathbb{Q}$ és una extensió abeliana de grau $\phi(m)$. El grup de Galois és isomorf a $(\mathbb{Z}/m\mathbb{Z})^*$. Un primer racional p és ramificat en K_m si i només si p|m. Si p>0 no divideix m, l'automorfisme d'Artin corresponent a l'ideal primer $P = p\mathbb{Z}$ porta ζ_m a ζ_m^p. Sigui f l'enter positiu més petit que verifica $p^f \equiv 1\ (mod\ m)$. Llavors, $P = p\mathbb{Z}$ esplita en $\phi(m)/f$ primers de grau f en K_m. Finalment, sigui $\mathcal{O}_m$ l'anell d'enters en K_m, llavors $\mathcal{O}_m = \mathbb{Z}[\zeta_m]$.*

L'extensió $\mathbb{Q}(e^{2\pi/p^m})$ és unicament ramificada i totalment en el primer p sobre $\mathbb{Q}$ dels primers de l'anell d'enters. Té ramificació en les valoracions dels valors absoluts (inmersions reals). Ara veiem els primers a l'infinit. El cos dels nombres racionals $\mathbb{Q}$ només té un primer arquimedià donat pel valor absolut usual. El cos K_m és tal que tot embedding en $\mathbb{C}$ és complexe, ja que, les úniques arrels de l'unitat en els nombres real $\mathbb{R}$ són ± 1. Considerem el subcòs $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$. Aquest cos és real i també ho és tot embedding d'aquest cos als nombres complexos. A més, té índex 2 en K_m, ja que, ζ_m satisfà l'equació $x^2(\zeta_m + \zeta_m^{-1})x + 1 = 0$. Per tant, el primer a l'infinit en $\mathbb{Q}$ esplita en $\phi(m)/2$ primers reals en K_m^+, i cadascun d'aquests ramifica en un primer complex en K_m. El grup de Galois de K_m/K_m^+ és generat per σ_{-1}, la conjugació complexa. Per tant, σ_{-1} pot ser el generador del grup d'inertia dels dels primers a l'infinit en K_m.

A.2 Extensions ciclotòmiques en cossos globals de característica positiva

Comencem recordant notació. $\mathbb{F}$ denota el cos finit amb $q = p^r$ elements. Definim $A = \mathbb{F}[T]$ i $k = \mathbb{F}(T)$. Comencem amb unes definicions, podeu consultar més informació d'aquestes en el Capítol 4 de [Gos].

Definició A.2.1 *Un mòdul de Drinfeld per A definit sobre k és un morfisme $\rho : A \to k\langle\tau\rangle$, amb la seva imatge no contenida en k, tal que per tot $a \in A$ el terme constant de ρ_a és a.*

Definició A.2.2 *Considerem l'A-mòdul $\overline{k}_\rho$ i el seu submòdul torsió*

$$\Lambda_\rho = \{\lambda \in \overline{k} | \rho_a(\lambda) = 0\ \ per\ \ algun\ \ a \in A, a \neq 0\}.$$

Per qualsevol $a \in A, a \neq 0$, definim el submòdul $\Lambda_\rho[a] \subset \Lambda_\rho$ com

$$\Lambda_\rho[a] = \{\lambda \in \overline{k} | \rho_a(\lambda) = 0\}.$$

Proposició A.2.1 *Definim per $K_{\rho,a}$ com el cos $k(\Lambda_\rho[a])$. Llavors $K_{\rho,a}/k$ és una extensió de Galois i existeix un morfisme*

$$Gal(K_{\rho,a}/k) \to GL_r(A/mA),$$

on r és el rank del mòdul de Drinfeld ρ.

Recordem les definicions del mòdul de Carlitz, i observem que és un mòdul de Drinfeld de rank 1.

Definició A.2.3 *Sigui K una extensió de $\mathbb{F}(T)$, definim l'acció de Carlitz de $\mathbb{F}[T]$ sobre K fent que $\mathbb{F}[T]$ actui sobre K amb els polinomis de Carlitz, on $M \in \mathbb{F}[T]$ i $\alpha \in K$,*

$$M \cdot \alpha = C_M(\alpha).$$

Definim el mòdul de Carlitz com el $\mathbb{F}[T]$-mòdul per l'acció de Carlitz $C(\overline{\mathbb{F}(T)})$, on $\overline{\mathbb{F}(T)}$ és la clausura separable de $\mathbb{F}(T)$.

Definició A.2.4 *Definim la m-torsió del mòdul de Carlitz com, on m ideal de $\mathbb{F}[T]$,*

$$\Lambda_m = \{\lambda \in \overline{k} | C_a(\lambda) = 0,\, a \in m\}.$$

Definim ara $K_m = k(\Lambda_m)$, per la següent proposició.

Proposició A.2.2 *K_m/k és una extensió de Galois i hi ha un monomorfisme*

$$Gal(K_m/k) \to GL_1(A/mA).$$

Observem que $GL_1(A/mA) = (A/mA)^*$. El nostre objectiu és veure $Gal(K_m/k) \cong (A/mA)^*$. De la proposició anterior, veiem $\Lambda_m \cong A/mA$ com un A-mòdul. Sigui λ_m el generador. Llavors, $C_a(\lambda_m), a \in \mathbb{F}[T]$, és un generador si i només si $(a, m) = 1$. Així Λ_m té $\Phi(m)$ generadors ($\Phi(m)$ és l'anàleg de la funció ϕ d'Euler). Alternativament, $\Phi(m)$ és el nombre d'elements en $(A/mA)^*$ (recordem Lema 1.1).

Com λ_m és un generador de Λ_m, obtenim que $K_m = k(\lambda_m)$. Sigui $\mathscr{O}_m$ la clausura entera de A en K_m. Sigui ara $m \in A$ un polinomi de grau positiu amb $m = \alpha P_1^{e_1} \cdots P_t^{e_t}$ la seva descomposició en primers, on $P_i \in A$ mònics irreductibles i e_i enters positius.

Teorema A.2.1 *K_m és el compositum dels cossos $K_{P_i^{e_i}}$. El únics ideal en A ramificats en $\mathscr{O}_m$ són P_iA amb $1 \leq i \leq t$. Aleshores, $[K_m : k] = \Phi(m)$, i*

$$Gal(K_m/k) \cong (A/mA)^*.$$

Ara veiem com els primers en A espliten en $\mathscr{O}_m$. Recordem, sigui λ_m el generador de Λ_m com un A-mòdul. Si $\sigma \in Gal(K_m/k)$, llavors $\sigma\lambda_m$ és un altre generador. Per tant, existeix $a \in A$ amb $(a, m) = 1$ tal que $\sigma(\lambda_m) = C_a(\lambda_m)$. L'automorfisme σ queda totalment determinat per aquesta relació, ja que, λ_m genera K_m sobre k. Observem a és determina fins un múltiple de m. Escrivim $\sigma = \sigma_a$. L'aplicació $\sigma \to a$ és un isomorfisme de $Gal(K_m/k) \to (A/mA)^*$ (veure apèndix). Pel Teorema A.2.1 es té que per qualsevol $a \in A$, coprimer amb m, hi ha un únic automorfisme $\sigma_a \in Gal(K_m/k)$ tal que $\sigma_a\lambda_m = C_a(\lambda_m)$.

Proposició A.2.3 *Sigui $\mathscr{O}_m$ la clausura entera de A en K_m, llavors $\mathscr{O}_m = A[\lambda_m]$.*

Teorema A.2.2 *Sigui $m \in A$ un polinomi de grau positiu i $P \in A$ un polinomi mònic irreductible que no divideix m. Llavors, l'automorfisme d'Artin de l'ideal primer PA en l'extensió K_m/k és l'automorfisme σ_P que porta λ_m a $C_P(\lambda_m)$. Sigui f l'enter positiu més petit que verifica $P^f \equiv 1\ (mod\ m)$. Llavors, $P\mathscr{O}_m$ és el producte de $\Phi(m)/f$ ideals primers de grau f. En particular, PA esplita completament en si i només si $P \equiv 1\ (mod\ m)$.*

Per acabar, veiem com esplita el primer a l'infinit de k en l'extensió K_m. Aqui enunciem el resultat, la demostració d'aquests i els preliminars es poden trobar a [Ros] pàgines 209-213.

Teorema A.2.3 *Sigui $J = \{\sigma_a \in Gal(K_m/k) | \alpha \in \mathbb{F}^*\}$ i denotem K_m^+ com el cos fix de J. Llavors ∞ esplita completament en K_m^+ i tot primer sobre ∞ en K_m^+ és totalment ramificat en K_m.*

Ara, per acabar la secció, estudiem breument l'extensió constant $K_n = K\mathbb{F}_{q^{p^n}}$ que és ciclotòmica, on $\mathbb{F}_q$ és el cos de constant per K. Llavors, K_n/K no ramifica enlloc. Podeu trobar la demostració d'aquest fet en [Ros], pàgina 103, Proposició 8.5. Podem pensar aquesta darrera extensió com l'extensió de posar arrels de la unitat sobre una corba algebraica sobre un cos finit (recordem l'introducció del Capítol 5).

B Relació de corbes amb cossos de funcions d'una variable

Es conegut que corbes no-singulars projectives algebraiques C sobre un cos arbitrari k correspon a extensions finites L del cos $k(x)$ on x és transcendent sobre k (o pensar x com una variable).
Hi ha tres aproximacions equivalents a l'estudi de corbes algebraiques (o varietats algebraiques) sobre un cos k:

1. la clàssica, referent a estudi de conjunt de zeros de polinomis, per exemple si $f \in k[x,y]$ un polinomi en dues variables x, y, considera el conjunt de zeros de f

   $$Z_f = V(f) := \{(x,y) \in \overline{k}^2 | f(x,y) = 0\}$$

   on $\overline{k}$ és la clausura separable de k amb l'acció de $Gal(\overline{k}/k)$.

   Consulteu el primer capítol del Harshorne "Algebraic Geometry".

2. usant teoria d'esquemes, introduit per Grothendieck els anys 1960, mireu el segon capítol del Harshorne "Algebraic Geometry".

3. usant teoria de valoracions, introduïda per Zariski (anterior a Grothendieck), actualment en treball de nou, per exemple en geometria tropical.

En aquest treball, usem la versió Zariski, comentant alguna relació amb la versió clàssica de corbes no-singulars.
Podeu trobar les demostracions al capítol 5 §9 i §10 del llibre de'n Lorenzini.

Proposició B.1 *K un cos arbitrari, i $v : K^* \to \mathbb{Z}$ una valoració no trivial. L'anell $\mathscr{O}_v := \{\alpha \in K^* | v(\alpha) \geq 0\} \bigsqcup \{0\}$ és un domini d'ideals primers amb un únic ideal maximal $\mathscr{M}_v := \{\alpha \in K^* | v(\alpha) > 0\} \bigsqcup \{0\}$. L'aplicació $v \mapsto \mathscr{O}_v$ és una bijecció entre valoracions no trivials i exhaustives de K i el conjunt de dominis d'ideals principals que conté K*

Proposició B.2 *Sigui A un domini de Dedekind, K el cos de fraccions de A. Hi ha una bijecció entre valoracions no trivials i exhaustives de A amb els ideals maximals de A, més concretament per cada ideal maximal $\mathfrak{m} \subset A$ defineix una valoració $v_\mathfrak{m}$ e K (la valoració M-àdica) complint que $v_\mathfrak{m}(A) \geq 0$, i $\mathfrak{m} \mapsto v_\mathfrak{m}$ és l'aplicació inversa de $v \mapsto \mathscr{M}_v \cap A$. A més es té $A = \cap_{\{v | v(A) \geq 0\}} \mathscr{O}_v$, i es té $k_{v_\mathfrak{m}} := \mathscr{O}_{v_\mathfrak{m}} / \mathscr{M}_{v_\mathfrak{m}} \cong A/\mathfrak{m}$.*

Definició B.1 *Sigui k un cos i L/k una extensió de cossos (finita o no). Diem que una valoració $v : L^* \to \mathbb{Z}$ és trivial en k si $v(k^*) = \{0\}$. Denotem per $\mathscr{V}(L/k)$ el conjunt de valoracions exhaustives $v : L^* \to \mathbb{Z}$ trivials en el cos k.*

Definició B.2 *Sigui k un cos. Un cos L contenint k s'anomena un cos de trascendència de grau n si existeixen $x_1, \ldots, x_n$ en L complinte que $L/k(x_1, \ldots, x_n)$ és finita i $k(x_1, \ldots, x_n)$ és isomorf al cos de fraccions de l'anell de polinomis a coeficients en k amb n variables.*

Donem finalment la definició de corba no-singular projectiva sobre un cos arbitrari k que usem en aquest treball.

Definició B.3 *Sigui k un cos arbitrari. Una corba no-singular completa (o projectiva) sobre k (denotada per X/k) és una parella $(X, k(X)/k)$ consisting en un cos $k(X)/k$ de grau de trascendència 1, i un conjunt X que s'identifica via una bijecció amb el conjunt $\mathscr{V}(k(X)/k)$. Un element P de X s'anomena un punt. El cos $k(X)$ s'anomena el cos de les funcions racionals en X. Per a cada punt P corresponent a la valoració $v_P \in \mathscr{V}(k(X)/k)$, té associat un anell d'ideals primers $\mathscr{O}_P = \mathscr{O}_{v_P} \subset k(X)$ amb únic ideal maximal $\mathfrak{m}_P$. Una funció $\alpha \in \mathscr{O}_P$ es diu que s'anul.la en P, o té un zero en P, si $\alpha \in \mathfrak{m}_P$. L'enter $v_P(\alpha)$ s'anomena l'ordre d'anul.lació en P. Una funció $\alpha \in k(X) \setminus \mathscr{O}_P$ es diu que té un pol en P i el natural $|v_P(\alpha)|$ s'anomena l'ordre del pol de α en P. El domini de $\alpha \in k(X)$, és el conjunt de punts de X on α es definit. Si $U \subset X$, llavors $\mathscr{O}_X(U) := \cap_{P \in U} \mathscr{O}_P$ es el domini anomenat l'anell de funcions en X definit a tot U.*
Al X introduïm la topologia de Zariski, on un conjunt T és tancat si i només si T és buit, tot X o un conjunt finit de punts de X.

Definició B.4 *Un conjunt obert U de X s'anomena afí si l'anell $\mathscr{O}_X(U)$ es un domini de Dedekind i una algebra finit generada, és a dir és de la forma $k[X_1,\dots,X_N]/(f_1,\dots,f_m)$ on X_i variables i $f_i \in k[X_1,\dots,X_N]$, i a més hi l'aplicació $P \mapsto \mathfrak{m}_P \cap \mathscr{O}_X(U)$ entre U i ideals maximals de $\mathscr{O}_X(U)$ és una bijecció.*

Definició B.5 *Una linea projectiva sobre k ś una corba no-singular completa $\mathbb{P}^1_{|k}$ complint que el cos de funcions $k(\mathbb{P}^1)$ és isomorf al cos de les funcions racionals en una variable x_1, és a dir isomorf a $k(x_1)$.*

Observem si k un cos arbitrari. Sigui $\mathbb{P}^1_{|k}$ la linea projectiva associada a l'extensió $k(x_1)/k$. Llavors

$$\mathbb{P}^1 = \{v_{g(x_1)} | g(x_1) \in [x_1] \ irreductible \ monic\} \bigsqcup \{v_\infty\}$$

Efectivament si $v \in \mathscr{V}(k(x_1)/k)$, com v exhaustiva, existeix $h(x_1) \in k[x_1]$ amb $v(h(x)) \neq 0$. Si $v(h(x)) < 0$ correspon a v_∞ (la valoració del grau o uniformitzant, generador del DIP és $1/x_1$). Si $v(h(x)) > 0$, llavors $v = v_{g(x_1)}$ on g és un dels factors irreductibles mònics de $h(x_1)$.
Abans de posar un exemple que expliquiciti la relació amb teoria esquemes i el cas clàssic de geometria, comentem més coses que es deriven de les definicions anteriors.

Proposició B.3 *Sigui X/k una corba no-singular completa associada a $k(X)/k$. Sigui $\beta \in k(X)$ complint que $K(X)/k(\beta)$ és una extensió finita. Denotem per U el domini de x en X. Llavors U és un obert afí de X i $\mathscr{O}_X(U)$ es igual a la clausura entera de $k[\beta]$ en $k(X)$. El complement de U en X es el conjunt de punts P complint $k[1/\beta]_{(1/\beta)} \subseteq \mathscr{O}_P$. En particular $X = U \cup U'$ on U' és el domini de $1/\beta$ en X, i per tant tota corba no-singular completa X/k és la unió de dos conjunts oberts afins. A més es té*

$$\mathscr{V}(k(X)/k) = \{v_{\mathfrak{B}} | \mathfrak{B}, ideal \ \ maximal \ \ de \ \mathscr{O}_X(U)\} \bigsqcup \{v_{\mathfrak{B}_1},\dots,v_{\mathfrak{B}_k}\}$$

on $\frac{1}{\beta}\mathscr{O}_X(U') = \prod_{i=1}^k \mathfrak{B}_i^{e_i}$.

Proposició B.4 *Donada X/k una corba no-singular completa associada a $k(X)/k$, i sigui $\gamma \in k(X)^*$. Llavors el conjunt $\{v \in \mathscr{V}(k(X)/k) | v(\gamma) \neq 0\}$ és un conjunt finit.*

Aquest resultat és clau en definir el divisor d'un element de $k(X)$ en la secció 3, on a més si es compta multiplicitats de zeros i pols, aquesta suma dona zero.
En el treball assumeix en molts casos que el cos de constants de $k(X)/k$ és k, és a dir que les corbes no-singulars completes $k(X)/k$ satisfant que $\mathscr{O}_X(X) = k$.
Per una petita relació amb la formulació clàssica de corbes enunciem-ho el resultat següent:

Definició B.6 *Definim la corba plana projectiva no-singular com*

$$X_f := (f(x,y) = 0) \sqcup \{P_1, ..., P_s\},$$

on els punts $P_1, ..., P_s$ s'anomenen els punts a l'infinit de la corba $f(x,y) = 0$, que provenen del polinomi homogeni $f(x,y,z) \in k[x,y,z]$ irreductible i no-singular.

Teorema B.1 *Sigui $f \in k[x_0,x_1,x_2]$ un polinomi homogèni. Suposem que la corba plana projectiva X_f en $\mathbb{P}^2(\overline{k})$ és no singular, i $P \in X_f$. Llavors l'aplicació*

$$\begin{aligned} X_f &\to V(\overline{k}(X_f)/\overline{k}) \\ P &\mapsto \upsilon_P \end{aligned}$$

és bijectiva.

Recordem el següent resultat

Teorema B.2 *Tota corba plana no-singular projectiva X sobre un cos k de característica zero amb cos de constants k. Llavors té un model plà afí: $f(x,y) = 0$ amb $f(x,y) \in k[x,y]$. Aquest model plà usualment és singular.*

Demostració. Sigui $k(X)/k$ el cos de trascendència 1, i per tant triem $\beta \in K(X) \setminus k$ i tenim que $K(X)/k(\beta)$ és finita i separable, per estar en característica zero, per tant per teoria de Galois existeix $\gamma \in K(X)$ on $K(X) = K(\beta)[\gamma])$ i $Irr(\gamma, k(\beta))[Y]$ és un polinomi mónic a coeficients en $k(\beta)$, $Y^n + \frac{a_{n-1}}{b_{n-1}}Y^{n-1} + \ldots + \frac{a_0}{b_0}$ amb $a_i, b_i \in k[\beta]$, per tant la corba ve definida per

$$(\prod_{i=0}^{n-1} b_i(x))y^n + (\prod_{i=1}^{n-2} b_i(x))a_{n-1}(x)y^{n-1} + \ldots + a_0(x)(\prod_{i=2}^{n-1} b_i(x) = 0.$$

□

Fem finalment un exemple, recordo de nou el següent resultat que ens serà útil, pels conceptes anteriors

Un exemple:

Considerem $L = \mathbb{Q}(x)[y]/(y^2 - (x^3 + 2))$ o estudiem $f(x, y) = y^2 - (x^3 + 2) = 0$. Fixem-nos que $f(x, y) \in \mathbb{Q}[x, y]$ és no singular. Aquí $\mathbb{Q}(x)$ és el cos de fraccions en la variable x i y també és una variable (o element trascendent) sobre $\mathbb{Q}(x)$.
Si L és un cos clarament, té grau de trascendencia 1 sobre $\mathbb{Q}$ perquè $\mathbb{Q} \subset \mathbb{Q}(x) \subset L$ i x trascendent sobre $\mathbb{Q}$ i $[L : \mathbb{Q}(x)] = 2$, i per tant pensem $L = \mathbb{Q}(X)$, i anem a veure aquesta X (observem $y^2 - (x^3 + 2) \in \mathbb{Q}(x)[y]$ és irreductible en $\mathbb{Q}(x)[y]$ ja que $x^3 + 2 \in \mathbb{Q}[x]$ és irreductible i pel criteri d'Eisenstein finalitzem (també és irreductible a la clausura algebraica de $\mathbb{Q}$ o als complexos, ja que llavors $x^3 + 1$ trenca en polinomis de grau 1 sense arrels repetides i per tant aplicant Eisenstein és irreductible $y^2 - (x^3 + 2)$ en $\overline{\mathbb{Q}}(x)[y]$).
Per tant L és un cos de trascendencia 1 sobre $\mathbb{Q}$ i per tant defineix una corba no-singular completa sobre $\mathbb{Q}$ (i es fàcil veure que L no pot ser la recta projectiva sobre $\mathbb{Q}$, exercici al lector).
També es pot demostrar que el cos de constants de L és $\mathbb{Q}$, exercici al lector (és a dir $L \cap \overline{\mathbb{Q}} = \mathbb{Q}$.
Anem a estudiar qui és X on $L = \mathbb{Q}(X)$.
Hem de recordar aquest resultat

Proposició B.5 *Sigui $f(x, y) \in k[x, y]$ un polinomi en dos variables irreductible i $f(x, y) = 0$ no-singular. Suposem que $f(x, y)$ és irreductible en $\overline{k}[x, y]$, llavors $k[x, y]/f(x, y)$ és un domini de Dedekind.*

Pel lema de Gauss tenim que $y^2 - (z^3 + 2)$ és irreductible en $\overline{\mathbb{Q}}[x, y]$ per tant
$\mathbb{Q}[x, y]/(y^2 - (x^3 + 2)) \subset L$ és un domini de Dedekind i considerant l'extensió de grau 2 $\mathbb{Q}(x) \subset L$ tenim $\mathbb{Q}[x] \subset C_{y^2-(x^3+2)}\mathbb{Q}[x, y]/(y^2 - (x^3 + 2))$ amb cos de fraccions L, d'on $C_{y^2-(x^3+2)}$ és la clausura entera de $k[x]$ en L, $y^2 - (x^3 + 2) = 0$ és no-singular, i per tant una corba afí U associada a X de L és $y^2 - (x^3 + 2) = 0$ on $\mathscr{O}_X(U) = \mathbb{Q}[x, y]/(y^2 - (x^3 + 2))$, l'altra vindrà d'estudiar la clausura de $k[1/x]$ en L.
Per a determinar els punts de X, val estudiar valoracions però donat $h(x) \in \mathbb{Q}[x]$ irreductible tenim

$$h(x)C_{y^2-(x^3+2)} = \begin{cases} \mathfrak{B}^2 & ramifica \\ \mathfrak{B}_1\mathfrak{B}_2 & esplita \\ h(x)C_{y^2-(x^3+2)} = \mathfrak{B} & inert \end{cases}$$

on $\mathfrak{B}$'s son ideals primers de $C_{y^2-(x^3+2)}$ i per tant pel capítol 2 valoracions exhaustives amb $\mathbb{Q}$-trivial $v_{\mathfrak{B}}$. Finalment falta determinar les valoracions que falten al conjunt X que provenen de la factorització en primers en C de $\frac{1}{x}C$ on C és la clausura entera de $\mathbb{Q}[1/x]$ en L, que sera un nombre finit, les valoracions sobre la valoració de ∞.
El treball estudia defineix el grup de classes $Cl(C_{y^2-(x^3+2)})$ i $Cl^0(L)$, però es centra amb cos base $\mathbb{F}_q$ enlloc de $\mathbb{Q}$ en aquest exemple. Sobre $\mathbb{F}_q$ sempre que l'anterior sigui correcte (és dir característica diferent de 2 i 3) es té $Cl(C_{y^2-(x^3+2)})$ és finita i $Cl^0(\mathbb{F}_7(x)[y]/(y^2 - (x^3 + 2)))$ també és finita. Això es demostra en el capítol 3.
Continuant amb l'exemple anterior sobre $\mathbb{Q}$ de $Cl(C_{y^2-(x^3+2)})$ o $Cl^0(\mathbb{F}_7(x)[y]/(y^2 - (x^3 + 2)))$, bé relacionat la seva finitut o no en el rank de la corba de gènere 1: $y^2 = x^3 + 2$, on tenir rang positiu

implicarà que són grups no finits. El càlcul del rang per a corbes el.líptiques és computable i en el nostre cas té rank 1

```
Input:Rank(EllipticCurve([0, 0, 0, 0, 2]))
```

```
Output: 1 true
```

i per tant aquests grups de classes no són grups finits com a corba sobre els racionals.

Referències

[Art] A. Travesa , *Teoria de Nombres*, UB, 1991

[AtiMac] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra*, CRC Press, 1994

[GuoShu] L. Guo, L. Shu , *Class Numbers of Cyclotomic Function Fields*, Transactions of the American Mathematical Society Vol. 351, No. 11 , 1999, pp. 4445-4467

[Gos] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer, 1998

[Har] R. Hartshorne, *Algebraic Geometry*, Springer, 1977

[IreRos] K. Ireland, M.Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990

[Jac] N. Jacobson, *Basic Algebra Volume II*, W.H.Freeman and Company, New York, 1989

[Kem] G. Kemper, *A Course in Commutative Algebra*, Springer, 2010

[Lan] S. Lang, *Algebraic Number Theory*, Springer, 1994

[Lan2] S. Lang, *Cyclotomic Fields I and II*, Springer, 1990

[Lau] L. Soler, *Estudi d'extensions abelianes finites de* $\mathbb{F}_p[T]$, UAB, 2018

[Lor] D. Lorenzini, *An Invitation to Arithmetic Geometry*, American Mathematical Society, 1996

[Mil] J.S. Milne, *Algebraic Number Theory*, Course Notes, 2020

[New] M. Newman, *A table of the first factor for prime cyclotomic fields*, Math. Com. 24, 1996, 215-219

[Roq] P. Roquette, *Class Field Theory in Characteristic p, its Origin and Development*, Advanced Studies in Pure Mathemathics 30, Class Field Theory - Its Centenary and Prospect, 2001, pp. 549-631

[Ros] M. Rosen, *Number Theory in Function Fields*, Springer, 2002

[SamZar] P. Samuel, O. Zariski, *Commutative Algebra Volume I*, Springer, 1960

[Sil] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer New York, 1986

[TN] P. Bayer E. Nart J. Quer, *Notes del Seminari de Teoria de Nombres (UB-UAB-UPC): "Mòduls de Drinfeld"editat per X. Xarles dins la cole·lecció STNB*, Barcelona, 2004, `http://www.ub.edu/tn/notes/vol09-drinfeld.pdf`

[Was] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1997