Grau de Matemàtiques

Treball Final de Grau

Estudi d'extensions abelianes finites de $\mathbb{F}_p(T)$

Autora:
Laura Soler Riba

Tutor:
Francesc Bars Cortina

Setembre de 2018

Abstract

L'objectiu d'aquest treball és l'anàlisi d'extensions abelianes finites de $\mathbb{F}_p(T)$. Per fer-ho, ens centrarem en l'estudi dels polinomis de Carlitz i les seves característiques i veurem com les arrels d'aquests polinomis confereixen a $\mathbb{F}_p(T)$ propietats anàlogues a les propietats que transfereixen a $\mathbb{Q}$ arrels dels polinomis ciclotòmics.

Agraïments

Aquest treball no hagués estat possible sense la guia i l'ajuda del meu tutor, en Francesc Bars. Voldria agrair-li sincerament totes les hores que m'ha dedicat en les reunions que hem fet durant tots aquests mesos, explicant-me els passos a seguir del treball, proporcionant-me bibliografia i revisant i corregint els continguts.

També vull agrair el suport que he rebut per part de la família, amics i companys, per creure en mi, acompanyar-me en aquest viatge i fer-lo més fàcil.

Índex

Conceptes previs

En aquesta secció repassarem alguns conceptes i resultats que ens seran útils al llarg del treball, com són algunes nocions de Teoria de Galois. Com que aquests termes són ben coneguts, no hi entrarem de manera exhaustiva i no farem cap demostració, tot i que en donarem alguna referència durant el treball:

Definició i. Sigui A un anell commutatiu, un *A-mòdul* és un grup abelià M (escrit additivament) sobre el qual A actua linealment: de manera més precisa, és un parell (M, μ), on M és un grup abelià i μ és una aplicació $A \times M$ a M tal que, representant per "ax" a $\mu(a, x)$ $(a \in A, x \in M)$, se satisfan els següents axiomes:

- $a(x + y) = ax + ay$
- $(a + b)x = ax + bx$
- $(ab)x = a(bx)$
- $1x = x$

amb $(a, b \in A, x, y \in M)$.

Criteri d'Eisenstein. Sigui R un DFU, $p(x) = a_n x^n + \cdots + a_0 \in R[X]$ i p primer de R tal que:

- $p | a_i \ \forall i = 0, \ldots, n-1$
- $p \nmid a_n$
- $p^2 \nmid a_0$

Aleshores, $p(x)$ és irreductible a $K[x]$, on K=Quot(R).

Extensions de cossos

Definició ii. Sigui $K \subseteq F$ una extensió de cossos i $\alpha \in F$, considerem el morfisme avaluació:

$$\begin{array}{rccl} ev_\alpha\colon & K[x] & \longrightarrow & F \\ & x & \longrightarrow & \alpha \\ & \lambda & \longrightarrow & \lambda, \text{ per a } \lambda \in K \end{array}$$

Amb $Ker(ev_\alpha) = 0$ o bé $Ker(ev_\alpha) = (p(x))$, amb $p(x)$ irreductible i mònic a $K[x]$.

- Diem que α és un element *algebraic* sobre K si $Ker(ev_\alpha) = (p(x))$, on $p(x) = Irr(\alpha, K)$.
- Diem que α és un element *transcendent* si $Ker(ev_\alpha) = 0$.

Definició iii. Donada una extensió de cossos $K \subseteq F$, tenim que F és un K-espai vectorial amb producte:

$$\begin{array}{ccc} K \times F & \longrightarrow & F \\ (\lambda, \alpha) & \longrightarrow & \lambda\alpha \end{array}$$

Definim el *grau* de l'extensió com $[F : K] = dim_K F$.

Definició iv. Sigui $K \subseteq F$ una extensió de cossos:

- Diem que l'extensió és *algebraica* si per a tot $\alpha \in F$ tenim que α és algebraic sobre K.
- Diem que l'extensió és *transcendent* si per a tot $\alpha \in F \backslash K$, α és transcendent sobre K.

Definició v. Sigui $K \subseteq F$ una extensió de cossos, definim el *grup de Galois* de l'extensió com:

$$Gal(F/K) = \{f : F \longrightarrow F \mid f \text{ és isomorfisme i } f|_K = id\}$$

Definició vi. Sigui $K \subseteq F$ una extensió de cossos. Diem que l'extensió és *normal* si:

- És algebraica.
- Si $p(x) \in K[x]$ és un polinomi irreductible amb una arrel a F llavors $p(x)$ descomposa en producte de factors lineals a $F[x]$.

Definició vii. Siguin K un cos i $p(x) \in K[x]$ un polinomi irreductible. Diem que $p(x)$ és *separable* si no té arrels múltiples al seu cos de descomposició. En general, $p(x) \in K[x]$ un polinomi no necessàriament irreductible és separable si tots els seus factors irreductibles ho són.

Proposició viiii. Sigui K un cos, $p(x) \in K[x] \setminus K$ i sigui L el cos de descomposició de $p(x)$. Llavors, $p(x)$ no té arrels múltiples a $L \iff (p(x), p'(x)) = 1$.

Definició ix. Sigui K un cos, una *extensió ciclotòmica* de K és una extensió de la forma $K \subseteq K(\zeta)$ amb $\zeta^n = 1$ per a algun n.

Lema x. Sigui K un cos finit, i $char(K)$ la característica de K, aleshores $char(K) = p > 0$ si i només si K té p^n elements per algun $n \geq 1$.

1 Introducció

L'anell $\mathbb{F}_p[T]$ té moltes analogies amb l'anell $\mathbb{Z}$, on $\mathbb{F}_p$ és un cos finit de p elements. Vegem-ne uns exemples:

- Sigui $m \in \mathbb{Z}$, $m \neq 0$, tenim que l'anell quocient $\mathbb{Z}/(m)$ és finit.

  Similarment, per a $M \in \mathbb{F}_p[T]$, $M \neq 0$, l'anell quocient $\mathbb{F}_p[T]/(M)$ també és finit.

- Els grups unitat $\mathbb{Z}^* = \{\pm 1\}$ i $\mathbb{F}_p[T]^* = \mathbb{F}_p{}^*$ són finits.

- A $\mathbb{Z}$, cada enter no nul pot esdevenir positiu en multiplicar-lo per la unitat adequada, de la mateixa manera que a $\mathbb{F}_p[T]$cada polinomi no nul pot fer-se mònic.

- Podem analitzar també una analogia més profunda: es pot interpretar el grup $(\mathbb{F}_p(T)/M)^*$ com el grup de Galois de l'extensió de $\mathbb{F}_p(T)$, tal com $(\mathbb{Z}/(m))^*$ és el grup de Galois de la m-èsima extensió ciclotòmica de $\mathbb{Q}(\mu_m)$ de $\mathbb{Q}$, on μ_m és el grup de les arrels m-èsimes de la unitat.

Per a cada $m \geq 1$, les arrels m-èsimes de la unitat són arrels de $X^m - 1 \in \mathbb{Z}[X]$ i formen un grup abelià per a la multiplicació. Per seguir amb l'analogia, construirem la família de polinomis $C_M(X) \in \mathbb{F}_p[T]\ [X]$, parametritzats per elements $M \in \mathbb{F}_p[T]$ i les arrels de cada $C_M(X)$ formaran un $\mathbb{F}_p[T]$-mòdul enlloc d'un grup abelià.

En particular, afegint les arrels de $C_M(X)$ a $\mathbb{F}_p(T)$, s'obté una extensió de Galois sobre $\mathbb{F}_p(T)$, el grup de Galois de la qual és isomorf a $(\mathbb{F}_p[T]/M)^*$.

Els polinomis $C_M(X)$ i les seves arrels van ser introduits per Carlitz cap al 1930, motiu pel qual s'anomenen polinomis de Carlitz.

2 Polinomis de Carlitz

Definició 2.1. *Per a cada $M \in \mathbb{F}_p[T]$, el **polinomi de Carlitz** $C_M(X)$ té coeficients a $\mathbb{F}_p[T]$ i es defineix recursivament de la forma següent:*

- $C_1(X) := X$
- $C_T(X) := X^p + TX$
- *Per $n \geq 2$, definim:*
  $C_{T^n}(X) := C_T(C_{T^{n-1}}(X)) := C_{T^{n-1}}(X)^p + TC_{T^{n-1}}(X)$.
- *Per a un polinomi general, M, amb $M = f_nT^n + \cdots + f_1T + f_o \in \mathbb{F}_p[T]$, definim $C_M(X)$ forçant la $\mathbb{F}_p$-linealitat de M:*

$$C_M(X) = f_nC_{T^n}(X) + \cdots + f_1C_T(X) + f_o \in \mathbb{F}_p[T][X].$$

Vegem alguns exemples sobre els polinomis de Carlitz:

Exemple 2.2. *Els polinomis de Carlitz de T^n per $n = 2$ i $n = 3$ i per a $M = T^2 - T$ són:*

- *Per $n = 2$:*
  $C_{T^2}(X) := C_T(X)^p + TC_T(X) = (X^p + TX)^p + T(X^p + TX) = [X^{p^2} + T^pX^p] + \cdots + [TX^p + T^2X] = X^{p^2} + (T^p + T)X^p + T^2X$.
- *Per $n = 3$:*
  $C_{T^3}(X) := C_{T^2}(X)^p + TC_{T^2}(X) = (X^{p^2} + (T^p + T)X^p + T^2X)^p + T[X^{p^2} + (T^p + \cdots + T)X^p + T^2X] =$
  $= [X^{p^3} + (T^p + T)^pX^{p^2} + T^{2p}X^p] + [TX^{p^2} + (T^{p+1} + T^2)X^p + T^3X]$
  $= X^{p^3} + (T^{p^2} + T^p + T)X^{p^2} + (T^{2p} + T^{p+1} + T^2)X^p + T^3X$.
- *Vegem-ho en $C_{T^2-T}(X)$:*

  $C_{T^2}(X) - C_T(X) = (X^{p^2} + (T^p + T)X^p + T^2X) - (X^p - TX)$
  $= X^{p^2} + (T^p + T - 1)X^p + (T^2 - T)X$.

Noti's que en desenvolupar $C_{T^n}(X)^p$, per a qualsevol n, tots els termes llevat dels de major grau s'anul·len, ja que els coeficients pertanyen a $\mathbb{F}_p[T] \backslash \mathbb{F}_p$.

Definició 2.3. *Sigui A un domini d'integritat de característica p, primer, un **p-polinomi sobre** A és un polinomi d'$A[X]$ format per una combinació lineal de $X, X^p, X^{p^2}, \ldots$ de la forma:*

$$f(X) = a_0X + a_1X^p + a_2X^{p^2} + \cdots + a_dX^{p^d}, \text{ per a alguns } a_j \in A.$$

Teorema 2.4. *Per a $M \in \mathbb{F}_p[T]$, $C_M(X)$ té grau $p^{grau\ M}$ sobre X i, a més, $C_M(X)$ és un p-polinomi en X:*

$$C_M(X) = \sum_{j=0}^{grau\ M} a_j(T)X^{p^j} = (leadM)X^{p^{grau\ M}} + \cdots + MX,$$

amb $a_j(T) \in \mathbb{F}_p[T]$, on $a_0(T) = M$ i $a_{grau\ M}(T) = leadM \in \mathbb{F}_p$ és el coeficient del terme de major grau de M.

Demostració. Tal com s'ha vist a l'Exemple 2.2, per $n = 2$ i $n = 3$ obtenim p-polinomis en X. Per tant, suposant-ho cert per inducció sobre T^n i aplicant $\mathbb{F}_p$-linealitat a $M = f_nT^n + \cdots + f_1T + f_o$, es demostra el teorema. □

Corol·lari 2.5. *Per a $M \in \mathbb{F}_p[T]$, $k \in \mathbb{F}_p$ i variables X i Y, tenim:*

- $C_M(X + Y) = C_M(X) + C_M(Y)$
- $C_M(kX) = kC_M(X)$

Per a $M_1, M_2 \in \mathbb{F}_p[T]$,

- $C_{M_1+M_2}(X) = C_{M_1}(X) + C_{M_2}(X)$
- $C_{M_1M_2}(X) = C_{M_1}(C_{M_2}(X))$

Demostració. $C_T(X)$ és un p-polinomi en X, perquè $C_T(X) = X^p + TX$. Per tant, un polinomi de Carlitz C_M també és un p-polinomi en X, ja que està definit mitjançant composició i $\mathbb{F}_p$-linealitat de $C_T(X)$. Per a qualsevol p-polinomi $f(X)$, tenim $f(X + Y) = f(X) + f(Y)$ i $f(kX) = kf(X)$, per a $k \in \mathbb{F}_p$.

Es pot provar que $M \mapsto C_M(X)$ és additiu en M i envia productes a composició per inducció sobre el grau de M. □

Del Corol·lari 2.5, podem extreure que els polinomis C_M commuten amb el producte donat per composició:

$$C_{M_1}(C_{M_2}(X)) = C_{M_1M_2}(X) = C_{M_2M_1}(X) = C_{M_2}(C_{M_1}(X))$$

Corol·lari 2.6. *Per a $M \in \mathbb{F}_p[T]$, la derivada en X de $C_M(X)$ és M.*

Demostració. La derivada de qualsevol $p-$polinomi $f(X) = a_0X + a_1X^p + a_2X^{p^2} + \cdots + a_dX^{p^d}$ és a_0, ja que qualsevol $(X^{p^j})' = 0$ en característica p, amb $j \geq 1$ i, pel Teorema 2.4, el coeficient de X de $C_M(X)$ és M. □

Cada $X^m - 1$ és separable sobre $\mathbb{Q}$, ja que no té arrels en comú amb la seva derivada mX^{m-1}. Per tant, hi ha m arrels m-èsimes diferents de la unitat en la característica 0. El polinomi $C_T(X) = X^p + TX$ és separable sobre $\mathbb{F}_p(T)$, ja que la seva derivada respecte

X és T, que és una constant no nul·la, si es considera com un polinomi en X, així que $(C_T(X), C'_T(X)) = 1$ a $\mathbb{F}_p(T)[X]$. Un càlcul similar mostra:

Teorema 2.7. *Per a $M \neq 0 \in \mathbb{F}_p[T]$, $C_M(X)$ és separable a $\mathbb{F}_p(T)[X]$.*

Demostració. Pel Corol·lari 2.6, sabem que la derivada en X de $C_M(X)$ és M. Com que M és una "constant" no nul·la respecte $\mathbb{F}_p(T)$[X], tenim que $(C_M(X), (C_M(X))') = M$ i, per tant, $C_M(X)$ i $(C_M(X))'$ són coprimers i, com s'ha vist als conceptes previs, $C_M(X)$ és separable. □

A continuació, estudiarem en detall $C_\pi(X)$, on π és un polinomi mònic i irreductible de $\mathbb{F}_p[T]$. Com es comporta $C_M(X) \mod \pi \in (\mathbb{F}_p[T]/\pi)[X]$? A $(\mathbb{Z}/(p))[X]$, amb p primer, el polinomi $X^m - 1$ és separable si $(m, p) = 1$, ja que $(X^m - 1)' = mX^{m-1}$, però $X^p - 1$ no és separable, ja que $X^p - 1 \equiv (X - 1)^p \mod p$, vegem l'analogia:

Teorema 2.8. *Sigui π un polinomi mònic i irreductible a $\mathbb{F}_p[T]$, definim $\mathbb{F}_\pi = \mathbb{F}_p[T]/\pi$. Per a $M \in \mathbb{F}_p[T]$, $\overline{C_M}(X) \in \mathbb{F}_\pi[X]$ és el resultat de reduir els coeficients de $C_M(X)$ a mòdul π.*

Si (M,π)=1, aleshores $\overline{C_M}(X)$ és separable a $\mathbb{F}_\pi[X]$, mentre que $\overline{C_\pi}(X) = X^{p^{grau\ \pi}}$.

Demostració. En el Corol·lari 2.6, hem vist que $C'_M(X) = M$ i $C'_\pi(X) = \pi$. Si $(M, \pi) = 1$, $\overline{C_M}'(X) = M \mod \pi$ és una constant no nul·la respecte X. Per tant, pel Teorema 2.7, $C_M(X)$ és separable a $\mathbb{F}_\pi[X]$.

D'altra banda, $\overline{C_\pi}'(X) = \pi \mod \pi = 0$ i així, $\overline{C_\pi}'(X)$ no és separable a $\mathbb{F}_\pi[X]$. Pel Teorema 2.4, sabem que el grau de $C_\pi(X)$ és $p^{\text{grau }\pi}$ i és mònic, perquè π ho és. Per tant, $\overline{C_\pi}(X)$ també és mònic i de grau $p^{\text{grau }\pi}$. Vegem que $\overline{C_\pi}(X) = X^{p^{\text{grau }\pi}}$, provant que l'única arrel de $\overline{C_\pi}(X)$ a la clausura algebraica $\overline{\mathbb{F}_\pi}$ és zero.

Suposem que hi ha una arrel $\alpha \neq 0 \in \overline{\mathbb{F}_\pi}$ tal que $C_\pi(\alpha) = 0$ i vegem que arribem a contradicció:

Per a qualsevol $M \in \mathbb{F}_p[T]$, $C_M(\alpha)$ és una arrel de $\overline{C_\pi}(X)$, perquè $C_\pi(C_M(\alpha)) = C_{\pi M}(\alpha) = C_M(C_\pi(\alpha)) = C_M(0) = 0$. Per tant, el número d'arrels de $\overline{C_\pi}(X) \in \overline{\mathbb{F}_\pi}$ és superior o igual als diferents valors de $M(\alpha)$, per a diferents M. Per comptar el número d'arrels, definim el morfisme $\mathbb{F}_p[T] \longrightarrow \overline{\mathbb{F}_\pi}$ donat per $M \longmapsto C_M(\alpha)$, que és additiu i té com a nucli:

$$\{M \in \mathbb{F}_p[T] : C_M(\alpha) = 0\}.$$

Aquest nucli no és només un subgrup de $\mathbb{F}_p[T]$, sinó que també és un ideal: si $C_M(\alpha) = 0$ i $N \in \mathbb{F}_p[T]$, aleshores $C_{NM}(\alpha) = C_N(C_M(\alpha)) = C_N(0) = 0$. Aquest ideal no és total, ja que conté π, però $C_1(\alpha) = \alpha \neq 0$. Com que (π) és un ideal maximal, el nucli és (π). Per tant, el número de $C_M(\alpha)$ per a diferents M és $\#(\mathbb{F}_p[T]/\pi) = p^{\text{grau }\pi} = \text{grau } \overline{C_\pi}(X)$, la qual cosa implica que $\overline{C_\pi}(X)$ té tantes arrels a $\overline{\mathbb{F}_\pi}$ com el seu grau i arribem a contradicció, ja que $\overline{C_\pi}(X)$ no és separable. Per tant, l'única arrel de $\overline{C_\pi}(X)$ a $\overline{\mathbb{F}_\pi}$ és 0. □

El següent corol·lari presenta una semblança amb $((1+X)^p-1)/X$, que compleix el criteri d'Eisenstein respecte p.

Corol·lari 2.9. *Per a cada polinomi irreductible $\pi \in \mathbb{F}_p[T]$, els coeficients de $C_\pi(X)$ són múltiples de π, exceptuant el terme de major grau. En particular, $C_\pi(X)/X$ compleix el criteri d'Eisenstein respecte π, on el terme constant és π.*

Demostració. Sigui $c \in \mathbb{F}_p{}^*$, tenim que $C_{c\pi}(X) = c \cdot C_\pi(X)$ per la linealitat dels polinomis de Carlitz; per tant, podem assumir que π és mònic. Aleshores, com hem vist al Teorema 2.4, $C_\pi(X) \in \mathbb{F}_p[T][\mathrm{X}]$ és $C_\pi(X) = X^{p^{grau\pi}} + \cdots + \pi X$. El primer terme de $C_\pi(X)$ és $X^{p^{\text{grau }\pi}}$. Pel Teorema 2.8, $\overline{C_\pi}(X) = X^{p^{\text{grau }\pi}} \in \mathbb{F}_\pi[X]$, amb la qual cosa tots els termes de menor grau de $C_\pi(X)$ són múltiples de π a $\mathbb{F}_p[T][X]$. Com que el terme de menor grau de $C_\pi(X)$ és πX, tenim que el terme independent de $C_\pi(X)/X$ és π i, per tant, el polinomi compleix el criteri d'Eisenstein. □

Noti's que $C_M(X) = (leadM)X^{p^{grau\ M}} + \cdots + MX$ presenta una estructura anàloga a $(1+X)^m - 1$, ja que $(1+X)^m - 1 = X^m + \cdots + mX$ i els termes de menor grau són MX i mX respectivament.

Corol·lari 2.10. *Per a qualsevol irreductible $\pi \in \mathbb{F}_p[T]$ i enter $k \geq 0$, els coeficients de $C_{\pi^k}(X)$ són múltiples de π, a excepció del coeficient principal.*

Demostració. El corol·lari és cert per a $k = 0$ i $k = 1$. Per a $k > 1$, usem la identitat $C_{\pi^k}(X) = C_\pi(C_{\pi^{k-1}}(X))$. □

A continuació, vegem l'analogia a $\mathbb{F}_p[T]$ de $a^p \equiv a \mod p$, amb p primer positiu i $a \in \mathbb{Z}$.

Teorema 2.11. *Per a qualsevol polinomi mònic irreductible $\pi \in \mathbb{F}_p[T]$, $C_\pi(A) \equiv A \mod \pi$ per a tot $A \in \mathbb{F}_p[T]$.*

Demostració. Pel Teorema 2.8, sabem que $\overline{C_\pi}(X) = X^{p^{\text{grau }\pi}} \in \mathbb{F}_\pi[X]$. Per tant, $\overline{C_\pi}(A) = A^{p^{\text{grau }\pi}} \mod \pi\ \forall A \in \mathbb{F}_p[T]$. Com que $\mathbb{F}_p[T]/\pi$ és un cos de $p^{\text{grau }\pi}$ elements, si l'elevem a aquesta potència, obtenim la identitat. Per tant, $C_\pi(A) \equiv A \mod \pi$. □

Si restem $A = C_1(A)$ a ambdós membres de l'equació, tenim l'anàleg del petit teorema de Fermat ($a^{p-1} \equiv 1 \mod p$, per a p primer positiu i $a \in (\mathbb{Z}/(p)^*)$.

Corol·lari 2.12. *Per a qualsevol mònic irreductible $\pi \in \mathbb{F}_p[T]$, $C \equiv 0 \mod \pi\ \forall A \in \mathbb{F}_p[T]$.*

Seguidament, mostrem un anàleg de $f(X^p) \equiv f(X)^p \mod p$, per a $f(X) \in \mathbb{Z}[X]$.

Teorema 2.13. *Sigui $\pi \in \mathbb{F}_p[T]$ un polinomi mònic irreductible i $f(X) \in \mathbb{F}_p[T][X]$, $f(C_\pi(X)) \equiv f(X)^{p^{grau\ \pi}} \mod \pi$, on la congruència significa que els coeficients dels dos membres de l'equació de la mateixa potència de X són iguals a $\mathbb{F}_p[T]/\pi$ per a tota potència en X.*

Demostració. Com hem vist al Teorema 2.8, $\overline{C_\pi}(X) = X^{p^{\text{grau }\pi}} \in \mathbb{F}_\pi[X]$. Per tant, $f(C_\pi(X)) \equiv f(X^{p^{\text{grau }\pi}}) \mod \pi$. A $\mathbb{F}_p[T]/\pi$, cada element és la seva potència $p^{\text{grau }\pi}$ i així tenim que $f(X)^{p^{\text{grau }\pi}} \equiv f(X^{p^{\text{grau }\pi}}) \mod \pi$. □

Per concloure la secció, recollim analogies vistes entre $\mathbb{Z}[X]$ i $\mathbb{F}_p[T][X]$, amb m i p positius i M i π mònics:

$\mathbb{Z}[X]$	$\mathbb{F}_p[T][X]$
$(1+X)^m - 1 = X^m + \cdots + mX$	$C_M(X) = X^{p^{\text{grau }M}} + \cdots + MX$
$(1+X)^p - 1 \equiv X^p \mod p$	$C_\pi(X) \equiv X^{p^{\text{grau }\pi}} \mod \pi$
$f(X^p) \equiv f(X)^p \mod p$	$f(C_\pi(X)) \equiv f(X)^{p^{\text{grau }\pi}} \mod \pi$

3 Mòdul de Carlitz i torsió de Carlitz

Sigui K una extensió de cossos de $\mathbb{F}_p(T)$, podem considerar K com un $\mathbb{F}_p(T)$-espai vectorial, de manera que també és un $\mathbb{F}_p[T]$-mòdul amb la multiplicació. A continuació, veurem com es pot definir una estructura diferent de $\mathbb{F}_p[T]$-mòduls mitjançant els polinomis de Carlitz. Per evitar ambigüitats, designarem $C(K)$ quan ens referim a K com a $\mathbb{F}_p[T]$-mòdul per l'acció de Carlitz.

Definició 3.1. *Sigui K una extensió de $\mathbb{F}_p(T)$, definim l'**acció de Carlitz de** $\mathbb{F}_p[T]$ **sobre** K fent que $\mathbb{F}_p[T]$ actui sobre K amb els polinomis de Carlitz:*

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

on $M \in \mathbb{F}_p[T]$ i $\alpha \in K$.

Exemple 3.2. *Vegem exemples d'accions de Carlitz:*

- $T \cdot \alpha = C_T(\alpha) = \alpha^p + T\alpha$.
- $c \cdot \alpha = C_c(\alpha) = c\alpha$, *amb* $c \in \mathbb{F}_p$.

Definició 3.3. *Anomenem **mòdul de Carlitz** al $\mathbb{F}_p[T]$-mòdul $C(\overline{\mathbb{F}_p(T)})$, on $\overline{\mathbb{F}_p(T)}$ és la clausura separable de $\mathbb{F}_p(T)$*[1]

El mòdul de Carlitz és anàleg al grup multiplicatiu $\mathbb{Q}^*$ com a $\mathbb{Z}$-mòdul:

- $m \in \mathbb{Z}$ actua sobre $\alpha \in \mathbb{Q}^*$, mitjançant $\alpha \longmapsto \alpha^m$

- $M \in \mathbb{F}_p[T]$ actua sobre $\alpha \in \overline{\mathbb{F}_p(T)}$, mitjançant $\alpha \longmapsto C_M(\alpha)$.

Els elements de torsió en el $\mathbb{Z}$-mòdul $\overline{\mathbb{Q}}^*$ són els $\alpha \in \overline{\mathbb{Q}}^*$ tals que $\alpha^m = 1$ per a algun $m > 0$. Per tant, α són les arrels m-èsimes de la unitat que generen extensions abelianes de $\mathbb{Q}$.

En el mòdul de Carlitz, $C(\overline{\mathbb{F}_p(T)})$, els elements de torsió són aquells $\alpha \in \overline{\mathbb{F}_p(T)}$ tals que $C_M(\alpha) = 0$.

Definició 3.4. *La M-**torsió del mòdul de Carlitz** és $\Lambda_M = \{\lambda \in \overline{\mathbb{F}_p(T)} : C_M(\lambda) = 0\}$.*

*Anomenem **torsió de Carlitz** a la unió de Λ_M per a tot $M \neq 0 \in \mathbb{F}_p[T]$.*

Exemple 3.5. *Vegem exemples de Torsió de Carlitz:*

- *Com que $C_T(X) = X^p + TX = X(X^{p-1} + T)$, tenim que la Torsió de Carlitz és:*

$$\Lambda_T = \{\lambda \in \overline{\mathbb{F}_p(T)} : \lambda^p + T\lambda = 0\} = \{0\} \cup \{\lambda : \lambda^{p-1} = -T\}.$$

  Anotem l'analogia amb $\mu_p = \{z \in \overline{\mathbb{Q}} : z^p = 1\}$.

[1] És a dir, els elements de la clausura algebraica de $\mathbb{F}_p(T)$ que són separables sobre $\mathbb{F}_p(T)$. Per exemple, $T^{1/p}$ és de la clausura algebraica de $\mathbb{F}_p(T)$, però no ho és de la separable.

- *De manera recursiva, descrivim C_{T^2} i la seva Torsió de Carlitz.*

  $C_{T^2}(X) = C_T(C_T(X)) = (X^p + TX)^p + T(X^p + TX)$ *i així:*

  $$\Lambda_{T^2} = \{\lambda \in \overline{\mathbb{F}_p(T)} : \lambda^p + T\lambda \in \Lambda_T\} = \Lambda_T \cup \{\lambda \in \overline{\mathbb{F}_p(T)} : (\lambda^p + T\lambda)^{p-1} = -T\}.$$

  Λ_{T^2} *presenta certa analogia amb* $\mu_{p^2} = \{z \in \overline{\mathbb{Q}} : z^p \in \mu_p\}$.

Pel Teorema 2.7, $C_M(X)$ és separable i, per tant, té $p^{grau\ M}$ arrels diferents a $\overline{\mathbb{F}_p(T)}$. Així, $\#\Lambda_M = p^{grau\ M}$. $C_M(X)$ és un p-polinomi i, per tant, les seves arrels Λ_M formen un $\mathbb{F}_p$-espai vectorial, a més d'altres propietats que ara veiem:

Teorema 3.6. *El subconjunt Λ_M és un submòdul de $C(\overline{\mathbb{F}_p(T)})$; és a dir, si $\lambda \in \Lambda_M$ i $A \in \mathbb{F}_p[T]$; aleshores, $C_A(\lambda) \in \Lambda_M$.*

Demostració. Per a $A \in \mathbb{F}_p[T]$ i $\lambda \in \Lambda_M$, es té que $C_A(\lambda) \in \Lambda_M$, ja que si usem l'última identitat del Corol·lari 2.5, tenim:

$$C_M(C_A(\lambda)) = C_{MA}(\lambda) = C_A(C_M(\lambda)) = C_A(0) = 0.$$

Per tant, Λ_M és un submòdul de $C(\overline{\mathbb{F}_p(T)})$. □

Exemple 3.7. *L'acció de Carlitz de $A \in \mathbb{F}_p[T]$ sobre $\lambda \in \Lambda_T$ es fa mitjançant la multiplicació del terme constant d'A. Escrivim $A = TQ + A(0)$ i realitzem l'acció de Carlitz:*

$$C_A(\lambda) = C_{TQ+A(0)}(\lambda) = C_Q(C_T(\lambda)) + C_{A(0)}(\lambda) = 0 + A(0)\lambda.$$

L'estructura de grup de les arrels m-èsimes μ_m no és només un $\mathbb{Z}$-mòdul, sinó que també és un $(\mathbb{Z}/(m))$-mòdul, ja que si $\zeta \in \mu_m$, tenim que $\zeta^a = \zeta^b$ si $a \equiv b \mod m$.

El grup μ_m és cíclic i si ζ genera μ_m, aleshores ζ^a genera μ_m si i només si $(a, m) = 1$. Vegem com Λ_M té propietats anàlogues.

Teorema 3.8. *Per $A, B \in \mathbb{F}_p[T]$ i $\lambda \in \Lambda_M$, tenim que $A \equiv B \mod M \iff C_A(\lambda) = C_B(\lambda)$.*

A més, l'acció de Carlitz sobre Λ_M crea un $\mathbb{F}_p[T]/M$-mòdul i hi ha un $\lambda_0 \in \Lambda_M$ que és un generador de Carlitz, amb $\Lambda_M = \{C_A(\lambda_0) : A \in \mathbb{F}_p[T]/M\}$ i els generadors de Λ_M són els $C_A(\lambda_0)$ tals que $(A, M) = 1$.

Demostració. $\Rightarrow$ Com que $A \equiv B \mod M$, escrivim $A = B + MN$, realitzem l'acció de Carlitz a A, amb λ tal que $C_M(\lambda) = 0$, i tenim:

$$C_A(\lambda) = C_{B+MN}(\lambda) = C_B(\lambda) + C_N(C_M(\lambda)) = C_B(\lambda) + C_N(0) = C_B(\lambda).$$

Per tant, $C_A(\lambda) = C_B(\lambda)$, tal com volíem provar.

$\Leftarrow$ Per veure que $A \equiv B \mod M$ si $C_A(\lambda) = C_B(\lambda)\ \forall \lambda \in \Lambda_M$, podem simplificar-ho restant $C_B(\lambda)$ a ambdós cantons de la igualtat i així caldrà provar:

Si $C_A(\lambda) = 0\ \forall \lambda \in \Lambda_M$, aleshores $A \equiv 0 \mod M$.

Escrivim $A = MQ + R$, on $R = 0$ o grau $R <$ grau M. Aleshores, per a tot $\lambda \in \Lambda_M$, tenim:

$$0 = C_A(\lambda) = C_{MQ+R}(\lambda) = C_Q(C_M(\lambda)) + C_R(\lambda) = C_Q(0) + C_R(\lambda) = C_R(\lambda).$$

Si $R \neq 0$, el polinomi de Carlitz $C_R(\lambda)$ té grau $p^{grau\ R} < p^{grau\ M} = \#\Lambda_M$. Per tant, C_R té més arrels que el seu grau, cosa que és impossible i, així, $M|A$ i $A \equiv 0 \mod M$, tal com volíem provar.

Per provar que Λ_M té un generador com a $\mathbb{F}_p[T]$-mòdul, realitzarem una prova anàloga a la demostració que μ_m és un grup cíclic.

Λ_M és un $\mathbb{F}_p[T]$-mòdul de torsió finitament generat. A qualsevol $\mathbb{F}_p[T]$-mòdul de torsió finitament generat, podem associar-li, a cada element $\lambda \in \Lambda$, el seu ordre a $\mathbb{F}_p[T]$, que és l'únic generador mònic de l'ideal "Aniquilador":

$$Ann_\Lambda(\lambda) = \{A \in \mathbb{F}_p[T] : A \cdot \lambda = 0\}$$

Tal com ocorre amb grups abelians finits, si N_1 i N_2 són els ordres a $\mathbb{F}_p[T]$ d'elements de Λ, aleshores hi ha un element de Λ que el seu ordre és el mínim comú múltiple de N_1 i N_2 a $\mathbb{F}_p[T]$.

L'ordre amb major grau a $\mathbb{F}_p[T]$ és divisible per l'ordre de cada element de Λ. Per tant, en el cas de Λ_M, si N denota l'ordre de major grau en Λ_M, llavors cada $\lambda \in \Lambda_M$ satisfà $C_N(\lambda) = 0$, així que $\#\Lambda_M \leq grau(C_N(X)) = p^{grau\ N}$ o, de manera equivalent: $p^{grau\ M} \leq p^{grau\ N}$ i també $N|M$, fet anàleg amb què tots els ordres del grup, divideixen la mida del grup.

Així, N és l'escalar mònic múltiple de M. Sigui $\lambda_0 \in \Lambda_M$ l'element que té ordre màxim a $\mathbb{F}_p[T]$ (i.e. ordre N), $Ann_{\Lambda_M}(\lambda_0) = (N) = (M)$, de manera que el submòdul de $\mathbb{F}_p[T]$ que λ_0 genera a Λ_M té mida:

$$\#\{C_A(\lambda_0) : A \in \mathbb{F}_p[T]\} = \#(\mathbb{F}_p[T]/M) = p^{grau\ M} = \#\Lambda_M,$$

que mostra que λ_0 és un generador de Λ_M i hi ha un isomorfisme com a $\mathbb{F}_p[T]$-mòduls: $\mathbb{F}_p[T]/\ M \cong \Lambda_M$, definit per $A \mod M \mapsto C_A(\lambda_0)$. En particular, $C_A(\lambda_0)$ genera Λ_M emprant l'acció de Carlitz si i només si $A \mod M$ genera $\mathbb{F}_p[T]/\ M$ com un $\mathbb{F}_p[T]$-mòdul de la manera habitual, i això passa si i només si $(A, M) = 1$. □

Per a mostrar de nou les similituds amb $\mathbb{Z}/(m)$, si s'escull un generador ζ de μ_m, s'obté l'isomorfisme $\mathbb{Z}/(m) \cong \mu_m$ amb $a \mod m \mapsto \zeta^a$. De la mateixa manera, si triem un generador $\lambda_0 \in \Lambda_M$ condueix a l' isomorfisme $\mathbb{F}_p[T]/M \cong \Lambda_M$, descrit per $A \mod M \mapsto C_A(\lambda_0)$, on $\mathbb{F}_p[T]/M$ és un $\mathbb{F}_p[T]$-mòdul amb la multiplicació estàndard.

Corol·lari 3.9. *Els $\mathbb{F}_p[T]$-submòduls de Λ_M són Λ_D tals que $D|M$.*

Demostració. Fixem un generador $\lambda_0 \in \Lambda_M$, aleshores $\mathbb{F}_p[T]/M \cong \Lambda_M$ com a $\mathbb{F}_p[T]$-mòduls, amb $A \mod M \mapsto C_A(\lambda_0)$. Per tant, el resultat és conseqüència que els submòduls de $\mathbb{F}_p[T]/M$ són $D\mathbb{F}_p[T]/M$ si $D|M$ i $D\mathbb{F}_p[T]/M$ correspon a $\Lambda_{M/D}$. □

L'anàleg de Carlitz del grup cíclic $\mathbb{Z}/(m)$ és el $\mathbb{F}_p[T]$-mòdul Λ_M (també cíclic), que és isomorf a $\mathbb{F}_p[T]/M$. Un anàleg de Carlitz de $(\mathbb{Z}/(m))^*$ és el grup additiu $\mathbb{F}_p[T]/M$ amb una nova estructura de $\mathbb{F}_p[T]$-mòdul: $N \cdot (A \mod M) = C_N(A) \mod M$ per a $N \in \mathbb{F}_p[T]$. Denotem $\mathbb{F}_p[T]/M$ amb l'acció de Carlitz per $\mathbb{F}_p[T]$ com $C(\mathbb{F}_p[T]/M)$. Vegem-ne un exemple:

Exemple 3.10. *Considerem $p = 3$ i $M = T^2 + 1$, aleshores el $\mathbb{F}_3[T]$-mòdul $C(\mathbb{F}_3[T]/(T^2 + 1))$ està generat per 1, vegem-ho:*

A	$C_A(X) \mod (T^2+1)$	$C_A(1) \mod (T^2+1)$
0	0	0
1	$1X$	$1 \cdot 1 = 1$
2	$2X$	$1 \cdot 2 = 2$
T	$X^3 + TX$	$1^3 + T \cdot 1 = T + 1$
$T+1$	$C_T(X) + C_1(X) = (X^3 + TX) + X$	$(1^3 + T \cdot 1) + 1 = T + 2$
$T+2$	$C_T(X) + C_2(X) = (X^3 + TX) + 2X$	$1 + T + 2 = T$
$2T$	$2C_T(X) = 2(X^3 + TX)$	$2(1 + T) = 2 + 2T$
$2T+1$	$2(X^3 + TX) + X$	$(2 + 2T) + 1 = 2T$
$2T+2$	$2(X^3 + TX) + 2X$	$(2 + 2T) + 2 = 2T + 1$

4 Les extensions de Carlitz de $\mathbb{F}_p(T)$

En aquesta secció, afegirem Λ_M a $\mathbb{F}_p(T)$ per tal de produir una extensió abeliana, així com $\mathbb{Q}(\mu_m)$ és una extensió abeliana de $\mathbb{Q}$. Per facilitar la notació, d'ara endavant escriurem F enlloc de $\mathbb{F}_p(T)$ i $F(\Lambda_M)$ per a denotar $\mathbb{F}_p(T, \Lambda_M)$.

Com que $C_M(X)$ és separable a $\mathbb{F}_p(T)[X]$, si afegim les arrels corresponents Λ_M a F, obtenim una extensió de Galois de $\mathbb{F}_p(T)$. Cada element de $\mathrm{Gal}(F(\Lambda_M)/F)$ permuta les arrels de $C_M(X)$ (i.e. permuta Λ_M).

Recordem que cada element de $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ ve determinat per un únic exponent de $(\mathbb{Z}/(\mathrm{m}))^*$ pel qual actuen sobre totes les arrels m-èsimes de la unitat. Així, anticipem que cada element de $\mathrm{Gal}(F(\Lambda_M)/F)$ actua sobre Λ_M per un polinomi Carlitz. Per fer-ho explícit, s'utilitza un generador de Λ_M.

Escollim $\sigma \in \mathrm{Gal}(F(\Lambda_M)/F)$ i prenem λ_0 un generador de Λ_M,

$$\Lambda_M = \sigma(\Lambda_M) = \sigma(\{C_N(\lambda_0) : N \in \mathbb{F}_p[T]\}) = \{C_N(\lambda_0) : N \in \mathbb{F}_p[T]\},$$

i així, $\sigma(\lambda_0)$ també és un generador de Λ_M: podem escriure $\sigma(\lambda_0) = C_A(\lambda_0)$ per a algun $A \in \mathbb{F}_p[T]$, que està ben definit a mòdul M, si $(A, M) = 1$ (Teorema 3.8). σ actua com A sobre λ_0 propagant per tot Λ_M: qualsevol $\lambda \in \Lambda_M$ és de la forma $C_N(\lambda_0)$ per a algun $N \in \mathbb{F}_p[T]$, per tant:

$$\sigma(\lambda) = \sigma(C_N(\lambda_0)) = C_N(\sigma(\lambda_0)) = C_N(C_A(\lambda_0)) = C_A(C_N(\lambda_0)) = C_A(\lambda).$$

D'aquesta manera, σ té el mateix efecte que l'acció de Carlitz sobre tots els elements de Λ_M. Escriurem A com A_σ per deixar palesa la seva dependència amb σ: per a cada $\sigma \in \mathrm{Gal}(F(\Lambda_M)/F)$, obtenim una unitat $A_\sigma \in (\mathbb{F}_p[T]/\mathrm{M})^*$ que descriu mitjançant els seus polinomis de Carlitz com σ permuta els elements de Λ_M.

Teorema 4.1. *El morfisme $\sigma \mapsto A_\sigma$ és un homomorfisme de grups injectiu*

$$\mathit{Gal}(F(\Lambda_M)/F) \hookrightarrow (\mathbb{F}_p[T]/M)^*.$$

Demostració. Per a σ i $\tau \in \mathrm{Gal}(F(\Lambda_M)/F)$ i algun $\lambda \in \Lambda_M$,

$$(\sigma\tau)(\lambda) = \sigma(\tau(\lambda)) = \sigma(C_{A_\tau}(\lambda)) = C_{A_\tau}(\sigma(\lambda)) = C_{A_\tau}(C_{A_\sigma}(\lambda)) = C_{A_\tau A_\sigma}(\lambda).$$

També tenim que $(\sigma\tau)(\lambda) = C_{A_{\tau\sigma}}(\lambda)$. Per tant, $A_{\sigma\tau}$ i $A_\tau A_\sigma = A_\sigma A_\tau$ tenen la mateixa acció de Carlitz sobre Λ_M. Per tant, $A_{\tau\sigma} \equiv A_\tau A_\sigma \mod M$ (Teorema 3.8), que prova que hi ha homomorfisme entre $\mathrm{Gal}(F(\Lambda_M)/F)$ i $(\mathbb{F}_p[T]/M)^*$.

Quan σ pertany al nucli de l'aplicació, $A_\sigma \equiv 1 \mod M$, i així, per a tot $\lambda \in \Lambda_M$, tenim $\sigma(\lambda) = C_{A_\sigma}(\lambda) = C_1(\lambda) = \lambda$. Per tant, σ és la identitat sobre Λ_M, així que també ho és a $\mathrm{Gal}(F(\Lambda_M)/F)$. □

Com que $(\mathbb{F}_p[T]/\mathrm{M})^*$ és abelià, $\mathrm{Gal}(F(\Lambda_M)/F)$ és abelià; per tant, les extensions de Carlitz $\mathbb{F}_p(T, \Lambda_M)$ sobre $\mathbb{F}_p(T)$ són abelianes. El següent resultat és anàleg a la isomorfia de $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ amb $(\mathbb{Z}/(\mathrm{m}))^*$:

Teorema 4.2. *$Gal(F(\Lambda_M)/F) \hookrightarrow (\mathbb{F}_p[T]/M)^*$ és un isomorfisme.*

Demostració. els ciclo □

Vegem-ne un exemple per a $M = T$:

Exemple 4.3. *Apliquem el teorema anterior a $M = T$ i, per tant, hi ha un isomorfisme entre $Gal(F(\Lambda_T)/F) \cong (\mathbb{F}_p[T]/T)^*$, que associa a cada σ un únic $A \mod T \in (\mathbb{F}_p[T]/T)^*$ tal que $\sigma(\lambda) = C_A(\lambda)\ \forall \lambda \in \Lambda_T$. A l'Exemple 3.7, hem vist que $C_A(\lambda) = A(0)\lambda$, i així, $(\mathbb{F}_p[T]/T)^* \cong \mathbb{F}_p^*$ si identifiquem cada congruència mòdul T amb la constant de la seva classe de congruència. Així, hi ha un isomorfisme entre $Gal(F(\Lambda_T)/F) \cong \mathbb{F}_p^*$, definit per $\sigma_f(\lambda) = f\lambda\ \forall \lambda \in \Lambda_T$, per a diferents $f \in \mathbb{F}_p^*$.*

La construcció de Carlitz ens dona extensions abelianes no només a $\mathbb{F}_p(T)$, sinó que també ho és sobre qualsevol cos K de característica p que no sigui algebraic sobre $\mathbb{F}_p$: denotant T com qualsevol element transcendent de K sobre $\mathbb{F}_p$, així $\mathbb{F}_p(T) \subset K$. Usant T, obtenim els polinomis $C_M(X) \in \mathbb{F}_p(T)[X] \subset K[X]$.

Aleshores, $C_M(X)$ és separable a $K[X]$ i $K(\Lambda_M)/K$ és una extensió de Galois amb efecte del grup de Galois sobre Λ_M, que ens porta a $Gal(K(\Lambda_M)/K) \hookrightarrow (\mathbb{F}_p[T]/M)^*$, per tant, el grup de Galois és abelià.

5 Més analogies entre els ciclotòmics i Carlitz

Les arrels dels polinomis $X^m - 1$ i $C_M(X)$ tenen característiques similars (per exemple, les arrels formen un grup cíclic de mida m i $C_M(X)$ és un $\mathbb{F}_p[T]$-mòdul de mida $p^{\text{grau } M}$), però són de major rellevància les analogies entre els isomorfismes dels grups Galois, $Gal(\mathbb{Q}(\mu_m)/\mathbb{Q}) \cong (\mathbb{Z}/(m))^*$ i $Gal(F(\Lambda_M)/F) \cong (\mathbb{F}_p[T]/M)^*$. Explorem analogies entre aquestes extensions en aquesta secció.

Pel Teorema 4.2 $[F(\Lambda_M) : F] = \#(\mathbb{F}_p[T]/M)^*$ per a qualsevol $M \neq 0$, així com $[\mathbb{Q}(\mu_m) : \mathbb{Q}] = \#(\mathbb{Z}/(m))^*$ per a $m \in \mathbb{Z}^+$. La mida de $(\mathbb{Z}/(m))^*$ es denota $\varphi(m)$ i, de manera similar, la mida de $(\mathbb{F}_p[T]/M)^*$ es denota $\varphi(M)$. Els seus valors són enters positius i estan descrits per les següents fórmules:

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right), \qquad \varphi(M) = p^{\text{grau } M} \prod_{\pi|M} \left(1 - \frac{1}{p^{\text{grau } \pi}}\right),$$

amb el producte dels factors primers (positius) divisors de m i de factors irreductibles (mònics) de M, respectivament. En particular, a partir d'aquestes fórmules es pot comprovar que:

$$\varphi(ab) = \frac{\varphi(a)\varphi(b)(a,b)}{\varphi((a,b))}, \qquad \varphi(AB) = \frac{\varphi(AB)p^{\text{grau } (A,B)}}{\varphi((A,B))}.$$

Vegem si hi ha analogies amb aquestes fórmules, també. Dos cossos ciclotòmics $\mathbb{Q}(\mu_m)$ i $\mathbb{Q}(\mu_n)$ amb $m \leq n$ són iguals si i només si $m = n$ o m és senar i $n = 2m$, com per exemple $\mathbb{Q}(\mu_3) = \mathbb{Q}(\mu_6)$. Podem plantejar-nos si el resultat és anàleg amb $F(\Lambda_M) = F(\Lambda_N)$.

Fem la prova del resultat del ciclotòmic extensions de $\mathbb{Q}$ i, a continuació, enunciem el teorema anàleg sobre les extensions de Carlitz de F.

Teorema 5.1. *Siguin m i n enters positius,*

1. *El nombre d'arrels de la unitat a $\mathbb{Q}(\mu_m)$ és mcm(2,m).*
2. $\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_n) \iff mcm(2,m) = mcm(2,n)$.
   Si $m \neq n$, és el mateix que $min(m,n) = k$ i $max(m,n) = 2k$, per a algun k senar.

Demostració. 1. L'arrel de la unitat $-\zeta_m$ pertany a $\mathbb{Q}(\mu_m)$ i té ordre $2m$, si m és senar i té ordre m, si m és parell; en general, l'ordre és $\text{mcm}(2,m)$. Per tant, $\mu_{mcm(2,m)} \subset \mathbb{Q}(\mu_m)$.

Si $\mathbb{Q}(\mu_m)$ conté una arrel r-èsima de la unitat, aleshores $\mathbb{Q}(\mu_r) \subset \mathbb{Q}(\mu_m)$ i prenent graus sobre $\mathbb{Q}$ es veu que $\varphi(r) \leq \varphi(m)$. Si $r \to \infty$, $\varphi(r) \to \infty$; per tant, hi ha un r que és el màxim que satisfà $\mu_r \subset \mathbb{Q}(\mu_m)$. Com que $\mu_m \mu_r = \mu_{mcm(m,r)} \in \mathbb{Q}(\mu_m)$,

tenim que $\text{mcm}(m,r) \leq r$; per tant, $\text{mcm}(m,r) = r$. Si escrivim $r = ms$ i apliquem la fórmula del producte de φ, tenim:

$$\varphi(r) = \varphi(ms) = \varphi(m)\varphi(s)\frac{(m,s)}{\varphi((m,s))} \geq \varphi(m)\varphi(s).$$

Com que $\mathbb{Q}(\mu_m)$=$\mathbb{Q}(\mu_r)$ per a r màxim, comptant graus sobre $\mathbb{Q}$ es veu que $\varphi(m) = \varphi(r) \geq \varphi(m)\varphi(s)$, aleshores $\varphi(s) \leq 1$, amb la qual cosa $s = 1$ o $s = 2$ i així $r = m$ o $r = 2m$, cosa que prova que les arrels de la unitat de $\mathbb{Q}(\mu_m)$ és m o bé $2m$.

Si m és parell $\varphi(2m) = 2\varphi(m) > \varphi(m)$ i així $r \neq 2m$. Per tant, per a m parell, el número d'arrels de la unitat a $\mathbb{Q}(\mu_m)$ és m.

Si m és senar, $-\zeta_m$ té ordre $2m$ i el número d'arrels de la unitat a $\mathbb{Q}(\mu_m)$ és $2m$.

En general, diem que el número d'arrels de la unitat a $\mathbb{Q}(\mu_m)$ és $\text{mcm}(2,m)$.

2. $\Longrightarrow$ Si $\mathbb{Q}(\mu_m) = \mathbb{Q}(\mu_n)$; aleshores, si es compten les arrels de la unitat de cada cos, es té que $\text{mcm}(2,m)$=$\text{mcm}(2,n)$.

   $\Longleftarrow$ Com que $\mu_{mcm(2,m)}$ és μ_m per a m parell i és $\pm\mu_m$ per a m senar, $\mathbb{Q}(\mu_m)$ =$\mathbb{Q}(\mu_{mcm(2,m)})$ per a tot m.

   Així, si $\text{mcm}(2,m)$=$\text{mcm}(2,n)$, tenim que $\mathbb{Q}(\mu_m)$ =$\mathbb{Q}(\mu_n)$.
   Si $m \neq n$, $\text{mcm}(2,m)$=$\text{mcm}(2,n)$ vol dir que m =$\text{mcm}(2,n)$ per a m parell, així que n és senar i $m = 2n$ i $2m$ =$\text{mcm}(2,n)$ si m és senar, i així n és parell i $n = 2m$.

□

Teorema 5.2. *Siguin M i N elements no nuls de $\mathbb{F}_p[T]$,*

1. *La torsió de Carlitz de $F(\Lambda_M)$ és Λ_M si $p \neq 2$ i és $\Lambda_{mcm(T(T+1),M)}$ si $p = 2$.*
2. *(a) Si $p \neq 2$, $F(\Lambda_M) = F(\Lambda_N) \iff N = fM$, amb $f \in \mathbb{F}_p{}^*$.*

   (b) Si $p = 2$, $F(\Lambda_M) = F(\Lambda_N) \iff mcm(M, T(T+1)) = mcm(N, T(T+1))$, amb el mínim comú múltiple definit com a mònic.

Per a $m \in \mathbb{Z}^+$, les arrels de la unitat a $\mathbb{C}$ d'ordre exactament m comparteixen el mateix polinomi mínim que $\mathbb{Q}$, el m-èsim polinomi ciclotòmic:

$$\Phi_m(X) = \prod_{\substack{1\leq a\leq m \\ (a,m)=1}} (X - \zeta^a) = \prod_{\substack{\zeta^m=1 \\ \text{ordre } m}} (X - \zeta),$$

on ζ és una arrel de la unitat d'ordre m en el primer producte i en el segon producte, ζ varia per totes les arrels de la unitat d'ordre m.

Per exemple, per a p primer, es té que:

- $\Phi_p(X) = (X^p - 1)/(X - 1)$, on cada arrel p-èsima té ordre p, excepte 1.

- $\Phi_p(X+1) = ((X+1)^p + 1)/X$ compleix el criteri d'Eisenstein respecte p.

Comparant els graus, les arrels i els coeficients principals de cada polinomi, es veu que $\Phi_{p^k}(X) = \Phi_p(X^{k-1})$ i també es veu que cada $\Phi_{p^k}(X+1)$ és Eisenstein respecte p.

Per a M mònic a $\mathbb{F}_p[T]$, tots els generadors de Λ_M tenen el mateix polinomi mínim sobre $\mathbb{F}_p(T)$, fet que és anàleg als polinomis ciclotòmics:

$$\Phi_M(X) = \prod_{\substack{\text{grau } A<\text{grau } M \\ (A,M)=1}} (X - C_A(\lambda_0)) = \prod_{\substack{C_M(\lambda)=0 \\ \mathbb{F}_p[T]\text{-ordre } M}} (X-\lambda),$$

on λ_0 és un generador escollit de Λ_M i en el segon producte, λ varia per totes les arrels de $C_M(X)$ que tenen $\mathbb{F}_p[T]$-ordre M: $C_D(\lambda) \neq 0$ per a qualsevol polinomi mònic D divisor de M. (Noti's que λ són els generadors de Λ_M, així com les arrels de la unitat d'ordre m són els generadors de μ_m, i per tant $\Phi_M(X) \in \mathbb{F}_p[T][X]$ resta invariant per l'acció del grup de Galois).

Exemple 5.3. *Si π és un polinomi irreductible a $\mathbb{F}_p[T]$, aleshores $\Phi_\pi(X) = C_\pi(X)/X$, ja que $C_\pi(X)/X$ compleix el criteri d'Eisenstein respecte π, com s'ha vist al Corol·lari 2.9 i, per tant, és irreductible a $\mathbb{F}_p(T) = F$.*

Si comparem graus, arrels i el coeficient principal, per a qualsevol $k \geq 1$, tenim que $\Phi_{\pi^k}(X) = \Phi_\pi(C_{\pi^{k-1}}(X))$; per tant, el terme constant de $\Phi_{\pi^k}(X)$ es calcula com $\Phi_\pi(C_{\pi^{k-1}}(0)) = \Phi_\pi(0) = \pi$.

Com que $\Phi_\pi(X)$ té tots els coeficients de X divisibles per π, exceptuant el coeficient principal, i $C_{\pi^{k-1}}(X)$ també té tots els coeficients divisibles per π, exceptuant del principal (Corol·lari 2.10), $\Phi_{\pi^k}(X)$ també té tots els coeficients divisibles per π exceptuant del principal i així tenim que $\Phi_{\pi^k}(X)$ compleix el criteri d'Eisenstein per π per a tot k.

Anteriorment, s'ha vist que $C_M(X)$ presenta una major similitud a $(1+X)^m - 1$ que a $X^m - 1$. Com que $C_M(X) = \prod_{D|M} \Phi_D(X)$, amb el producte dels divisors mònics D de M. Així, es podria anticipar que $\Phi_M(X)$ és més semblant a $\Phi_m(X+1)$ que $\Phi_m(X)$ i això sembla ser cert. Per exemple, $\Phi_{\pi^k}(X)$ compleix el criteri d'Eisenstein respecte π, mentre que $\Phi_{p^k}(X+1)$ també el compleix respecte p ($\Phi_{p^k}(X)$ no compleix el criteri d'Eisenstein). També tenim que si m no és la potència d'un primer $\Phi_m(1) = 1$ i, anàlogament, si M és mònic i no és la potència d'un irreductible, $\Phi_M(0) = 1$.

El teorema de Kronecker-Weber diu que cada extensió finita i abeliana finita de $\mathbb{Q}$ es troba en una extensió ciclotòmica $\mathbb{Q}(\mu_m)$ per a cert natural m. Hi ha un anàleg del teorema de Kronecker-Weber per $\mathbb{F}_p(T)$, fet per Carlitz [2].

[2] Vladimir Drinfeld i David Hayes van desenvolupar de forma independent el teorema anàleg quan $K/\mathbb{F}_p(T)$ és finita, amb $K \cap \overline{\mathbb{F}_p} = \mathbb{F}_p$.
En les extensions que treballem, remarquem que $\mathbb{F}_p(T)(\Lambda_M) \cap \overline{\mathbb{F}_p} = \mathbb{F}_p$

Teorema 5.4. (Kroenecker-Weber) *Sigui $K/\mathbb{Q}$ una extensió abeliana, aleshores existeix una arrel m-èsima de la unitat, ζ tal que $K \subseteq \mathbb{Q}(\zeta)$.*

El teorema anàleg a Kroenecker-Weber diu que cada extensió abeliana finita de $\mathbb{F}_p(T)$ es troba en algun $\mathbb{F}_{p^d}(T, \Lambda_M, \Lambda_{1/T^n})$ per a alguns $d \geq 1$, $n \geq 1$ i $M \in \mathbb{F}_p[T]$, on Λ_{1/T^n} és el conjunt d'arrels del polinomi Carlitz $C_{1/T^n}(X)$ construït amb $1/T$ enlloc de T:

- $C_{1/T}(X) = X^p + (1/T)X$.
- $C_{1/T^k}(X) = C_{1/T}(C_{1/T^{k-1}}(X))$.

Noti's que la família de polinomis $C_{1/T^n}(X)$ no interactua bé amb $C_M(X)$, per a $M \in \mathbb{F}_p[T]$, per exemple $C_{1/T}(C_T(X)) \neq X$ i $C_T(C_{1/T}(X)) \neq X$.

Exemple 5.5. *Utilitzant $1/T$ com a generador sobre $\mathbb{F}_p$ per $\mathbb{F}_p(T) = \mathbb{F}_p(1/T)$, el polinomi $C_{1/T}(X) = X^p + (1/T)X = X(X^{p-1} + 1/T)$ té arrels que generen la mateixa extensió de $\mathbb{F}_p(T)$ com $C_T(X)$. Però per $C_{1/T^2}(X)$ obtenim quelcom nou:*

$$C_{1/T^2}(X) = C_{1/T}(C_{1/T}(X)) = X^{p^2} + ((1/T)^p + (1/T))X^p + (1/T^2)X$$

i l'extensió $\mathbb{F}_p(T, \Lambda_{1/T^2})/\ \mathbb{F}_p(T)$ resulta tenir una propietat que no satisfan els subcossos de $\mathbb{F}_{p^d}(T, \Lambda_M)$ (i.e. extensions totalment ramificades a a ∞, on p divideix el grau de l'extensió), de manera que l'extensió no està dins d'aquest cos.

La següent taula mostra una analogia de característiques entre μ_m i Λ_M:

Ciclotòmic	Carlitz
$\#\mu_m = m$	$\#\Lambda_M = p^{grauM}$
Subgrups: μ_d, $d \mid m$	$D \mid M \iff \Lambda_D \subset \Lambda_M$
$\zeta \in \mu_m, a \in \mathbb{Z} \Rightarrow \zeta^a \in \mu_m$	$\lambda \in \Lambda_M, A \in \mathbb{F}_p[T] \Rightarrow C_A(\lambda) \in \Lambda_M$
$a \equiv b \mod m \Rightarrow \zeta^a = \zeta^b$	$A \equiv B \mod M \Rightarrow C_A(\lambda) = C_B(\lambda)$
$\zeta^a = \zeta^b\ (\zeta \in \mu_m) \Rightarrow a \equiv b \mod m$	$C_A(\lambda) = C_B(\lambda)\ (\lambda \in \Lambda_M) \Rightarrow A \equiv B \mod M$
$\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \cong (\mathbb{Z}/(m))^*$	$\mathrm{Gal}(\mathbb{F}_p(T, \Lambda_M)/\mathbb{F}_p(T)) \cong (\mathbb{F}_p[T]/M)^*$
$X^m - 1 = \prod_{d\mid m} \Phi_d(X)$	$C_M(X) = \prod_{D\mid M} \Phi_D(X)$
Teorema de Kroenecker-Weber	Teorema de Carlitz-Hayes

6 Bibliografia

[1] Goss, D., *Basic Structures of Function Field Arithmetic*, NY: Springer-Verlag (1991).

[2] Lorenzini, *D. An Invitation to Arithmetic Geometry*, NY: American Mathematical Society (1996).

[3] Neukirch, J. *Class Field Theory - The Bonn lectures-* (2015). https://www.mathi.uni-heidelberg.de/ schmidt/Neukirch-en/Neukirch_cft_02_may15.pdf

[4] Conrad, K. *Carlitz extensions.* Pot consultar-se a:
http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/carlitz.pdf

[5] Travesa, A. *Teoria de Nombres. Apunts del curs 1991-1992*

A Annex I: Ramificació dels ideals primers

Aquest annex pretén donar una visió més profunda del comportament dels ideals primers en les extensions que descrivim a continuació. S'enuncien alguns resultats de ramificació sense demostrar-los amb la finalitat de comprendre el procediment de ramificació:

Proposició A.1. *Es diu que un domini A és un domini de Dedekind factoritza de manera única per ideals primers.*

Sigui A un domini de Dedekind, K el seu cos de fraccions, L/K una extensió finita i $B := \{\alpha \in L,\ on\ Irr(\alpha, K)[X] \in A[X]\}$ un anell que compleix:

$$\begin{array}{ccc} B & \subseteq & L \\ | & & | \\ A & \subseteq & K \end{array}$$

Aleshores B és un domini de Dedekind si i només si tot ideal de A factoritza en producte d'ideals primers de forma única llevat ordre.

Pel treball, pensarem que $A = \mathbb{F}_p[T]$ i $K = \mathbb{F}_p(T)$.

Definició A.2. *B s'anomena la clausura entera de A en L, on tot ideal de B factoritza de forma única llevat d'ordre per ideals primers de B*[3]*.*

Tant A com B són anells de Dedekind. En particular, si $\mathfrak{p} \subseteq A$ és un ideal primer no nul de A, la seva extensió a B, $\mathfrak{p}B$, és un ideal no nul que descompon en producte d'ideals primers de B de manera única.

Sigui $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ aquesta descomposició en factors primers; on $\mathfrak{P}_i$ són ideals primers de B no nuls i diferents, , amb $1 \leq i \leq g$ i $e_i \geq 1$ enters.

Definició A.3. *S'anomena **índex de ramificació** d'un primer $\mathfrak{P}_i$ sobre $\mathfrak{p}$ l'exponent e_i i se sol designar per $e_{\mathfrak{P}_i/\mathfrak{p}}$.*

Observem que podem partir d'un ideal primer $\mathfrak{P} \subseteq B$, considerar la seva contracció $\mathfrak{p} := \mathfrak{P} \cap A$ en A i després mirar quin és l'exponent de $\mathfrak{P}$ en la descomposició de $\mathfrak{p}B$ en ideals primers de B; això sempre dona un exponent $e_{\mathfrak{P}/\mathfrak{p}} \geq 1$, ja que $\mathfrak{P} \supseteq \mathfrak{p}B$ i, per tant, $\mathfrak{P}$ és un ideal primer que divideix l'ideal $\mathfrak{p}B$ i es té que $B/\mathfrak{P} \Big/ A/\mathfrak{p}$ és una extensió finita de cossos.

Definició A.4. *Sigui $\mathfrak{p}$ un ideal primer no nul d'un domini de Dedekind A. L'anell quocient, $A/\mathfrak{p}$, és un cos, ja que $\mathfrak{p}$ és un ideal maximal de A. $A/\mathfrak{p}$ s'anomena el cos residual de A en $\mathfrak{p}$.*

Quan $A = \mathbb{Z}$ o $A = \mathbb{F}_p(T)$aquest cos residual és un cos finit.

[3]En un domini de Dedekind, tot ideal primer no nul és maximal. Per a més informació, consulteu Dino Lorenzini, "An invitation to Arithmetic Geometry".

Definició A.5. *El grau $[B/\mathfrak{P} : A/\mathfrak{p}]$ s'anomena* ***grau residual*** *en $\mathfrak{P}$ de l'extensió L/K amb A domini de Dedekind i es designa com $f_{\mathfrak{P}/\mathfrak{p}}$.*

Vegem com es relacionen e_i i f_i en extensions separables amb la següent proposició:

Proposició A.6. *Siguin A un anell de Dedekind, K el cos de fraccions de A, L/K una extensió finita i separable, B la clausura entera de A en L, $n := [L : K]$ el grau i $\mathfrak{p}$ un ideal primer no nul de A. Sigui $\mathfrak{p}B = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$ la descomposició de $\mathfrak{p}B$ en factors primers en B. Aleshores, se satisfà la igualtat:*

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

A més, si L/K és una extensió de Galois, es té que $e_1 = \cdots = e_g$ i llavors, si algun $e_i > 1$ diem que p ramifica en L/K.

Si $[L : K] = g$ diem que $\mathfrak{p}$ descomposa totalment en L.

Definició A.7. *Es diu que l'extensió L/K és* ***ramificada*** *en $\mathfrak{P}$ quan l'extensió residual en $\mathfrak{P}$ no és separable o bé $e(\mathfrak{P}/\mathfrak{p}) > 1$. Si $e(\mathfrak{P}/\mathfrak{p}) = [L : K]$ es diu que l'extensió està totalment ramificada. Si $e(\mathfrak{P}/\mathfrak{p}) = 1$, es diu que l'extensió L/K* ***no és ramificada****.*

Uns exemples bàsics són $A = \mathbb{Z}$ amb $K = \mathbb{Q}$ i també $A = \mathbb{F}_p[T]$ amb $K = \mathbb{F}_p(T)$. Ambdues A tenen DFU via identificació de primers i, per tant, són Dominis de Dedekind.

A.1 Ramificació a l'extensió $\mathbb{Q}(i)/\mathbb{Q}$

Prenem $A = \mathbb{Z}$ i considerem la següent extensió:

$$\begin{array}{ccc} B & \subseteq & \mathbb{Q}(i) \\ | & & | \\ \mathbb{Z} & \subseteq & \mathbb{Q} \end{array}$$

Es pot demostrar que $B = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$, d'on $\mathbb{Z}[i]$ és domini de Dedekind.

Estudiem algunes propietats de ramificació en l'extensió $\mathbb{Q}(i)/\mathbb{Q}$ amb $A = \mathbb{Z}$:

Exemple A.8. *Sabem que l'ideal generat per $\mathfrak{p} = 2$ és un ideal primer a $A = \mathbb{Z}$, però ho és a $\mathbb{Z}[i]$? Vegem-ho:*

$$2\,\mathbb{Z}[i] = ((1 + i)(1 - i)) = (1^2 - i^2) = (1 - (-1)) = (2)$$

Així doncs, (2) no és un ideal primer a $\mathbb{Z}[i]$, ja que és producte de dos ideals primers diferents de la unitat (i.e. diferents de $\pm 1, \pm i$).

Com que podem reescriure $(1 - i)$ de la manera següent: $1 - i = -i(1 + i)$; a $\mathbb{Z}[i]$, $2 = (1 + i)(1 - i) = -i(1 + i)^2$.

Per tant, a $\mathbb{Z}[i]$, 2 *no és primer i factoritza de forma única llevat d'unitats, de tal manera que pertany a l'ideal* $(1+i)$.

En aquest cas, l'índex de ramificació de 2 *sobre l'ideal* $(1+i)$ *és 2, ja que* $2 = k(1+i)^{e_{(1+i)/2}} = -i(1+i)^2$, *on* k *són les unitats de* $\mathbb{Z}[i]$ *i* $e_{(1+i)/2} = 2$.

Analitzem com es relacionen el grau de l'extensió i l'índex de ramificació per la Proposició A.6 amb $\mathfrak{p} = 2$ *i* $\mathfrak{P} = 1+i$:

$$e_{(1+i)/2}\left[\mathbb{Z}[i]\Big/(1+i) : \mathbb{Z}\Big/(2)\right] = [\mathbb{Q}(i) : \mathbb{Q}]$$

- *Hem vist que* $e_{(1+i)/2} = 2$.
- *L'extensió* $\mathbb{Q}/\mathbb{Q}(i)$ *és de grau 2 i és de Galois, així que* $[\mathbb{Q}\colon \mathbb{Q}(i)] = 2$.
- *Tenim que:*
$$\mathbb{Z}[x]\Big/((x^2+1),(x+1)) \cong \mathbb{Z}[i]\Big/(1+i)$$

Per tant, el grau residual en $(1+i)$ *de* $\mathbb{Z}[i]/\mathbb{Z}$ *és* $f_{(1+i)/2} = \left[\mathbb{Z}[i]\Big/(1+i) : \mathbb{Z}\Big/(2)\right] = 1$.

Vegem altres ideals de $\mathbb{Z}[i]$:

Exemple A.9. *Estudiarem si l'ideal generat per* $\mathfrak{p} = 3$ *a* $\mathbb{Z}$, *també és un ideal primer a l'anell* $\mathbb{Z}[i]$:

Suposem que 3 *no és un ideal primer a* $\mathbb{Z}[i]$, *aleshores el podem escriure com a producte de dos primers* $\mathfrak{p} \in \mathbb{Z}[i]$ *de la forma* $a+bi$, $c+di$, *amb* $a,b,c,d \in \mathbb{Z}$, *de manera que:*

$3 = (a+bi)(c+di) = (ac-bd) + i(ad+bc)$

Per tant, s'ha de complir que $ac - bd = 3$ *i* $ad + bc = 0$.
Resolem el sistema d'equacions per conèixer com factoritza 3 a $\mathbb{Z}[i]$.

- *Aïllem a a ambdues equacions i otenim:* $a = \dfrac{3+bd}{c}$ *i* $a = -\dfrac{bc}{d}$

  Igualem les dues expressions i escrivim b en funció dels paràmetres c i d:

  $$\frac{3+bd}{c} = -\frac{bc}{d} \longrightarrow 3d + bd^2 = -bc^2 \longrightarrow 3d = -b(c^2+d^2) \longrightarrow b = \frac{-3d}{c^2+d^2}$$

- *Similarment, aïllem b a les dues equacions inicials:* $b = \dfrac{ac-3}{d}$ *i* $b = -\dfrac{ad}{c}$.

  Igualem les dues equacions per a conèixer a:

  $$-\frac{3-ac}{d} = -\frac{ad}{c} \longrightarrow 3c - ac^2 = ad^2 \longrightarrow 3c = a(c^2+d^2) \longrightarrow a = \frac{3c}{c^2+d^2}$$

Per tant, 3 *no és ideal primer, ja que és producte de dos ideals primers diferents:* $(c+di)$ *i* $(a+bi) = \dfrac{3}{c^2+d^2}(c-id)$, *tals que* $a,b,c,d \in \mathbb{Z}$.

En aquest cas, $3 = \mathfrak{P}_1^1\mathfrak{P}_2^1$ *i es releciona el grau de l'extensió i l'índex de ramificació de la següent manera, per la Proposició A.6:*

$$e_{\mathfrak{p}_1}\left[\mathbb{Z}[i]\Big/\mathfrak{P}_1 : \mathbb{Z}\Big/(3)\right] + e_{\mathfrak{p}_2}\left[\mathbb{Z}[i]\Big/\mathfrak{P}_2 : \mathbb{Z}\Big/(3)\right] = [\mathbb{Q}(i) : \mathbb{Q}]$$

- *Hem vist que* $e_{\mathfrak{P}_i} = 1$ *per* $i = 1, 2$.
- *L'extensió* $\mathbb{Q}/\mathbb{Q}(i)$ *és de grau 2 i és de Galois, així que* $[\mathbb{Q}\colon \mathbb{Q}(i)] = 2$.
- *Tenim que:*
$$\mathbb{Z}[i]\Big/(3) \cong \mathbb{Z}[x]\Big/((x^2+1), 3) \cong {}^{\mathbb{Z}}\!/_{(3)}[x]\Big/(x^2+1)$$

Per tant, el grau residual en $(1+i)$ *de* $\mathbb{Z}[i]/\mathbb{Z}$ *és* $f_{(1+i)/2} = \left[\mathbb{Z}[i]\Big/(1+i) : \mathbb{Z}\Big/(2)\right] = 1$.

D'aquesta manera, $\mathfrak{p} = 3$ *a* $\mathbb{Z}[i]$ *és producte de dos ideals primers diferents i l'índex de ramificació és 1 en els dos ideals primers (i.e.* $e_{\mathfrak{P}_i} = 1$*). Per tant, el grau residual en* $\mathfrak{P}_i$ *de* $\mathbb{Z}[i]/\mathbb{Z}$ *és* $f_{\mathfrak{P}_i} = 1$ *per a* $i = 1, 2$.

Acabem de veure, doncs, com dos primers diferents de $\mathbb{Z}$ ramifiquen de manera diferent a $\mathbb{Z}[i]$: $\mathfrak{p} = 2$ ramifica, ja que $e_i = 2$; en canvi, $\mathfrak{p} = 3$, no ho fa ($e_i = 1$).

L'estudi dels ideals primers que ramifiquen en una extensió finita i separable L/K de dominis fixant A un domini de Dedekind en K es pot fer amb l'ajuda d'un invariant associat a l'extensió de manera natural i que serveix per a determinar el conjunt dels ideals primers de A que ramifiquen en l'extensió L/K: el discriminant.

Definició A.10. *Sigui* $\theta \in L$ *un element primitiu de l'extensió finita i separable* L/K[4] *i sigui* $f(X) := Irr(\theta, K)$ *el polinomi mònic irreductible de* $K[X]$ *que té per arrel* θ*, aleshores definim el* ***discriminant de l'extensió*** L/K *com:*

$$D(1, \theta, \theta^2, \ldots, \theta^{n-1}) := (-1)^{n(n-1)/2} N_{L/K}(f'(\theta)),$$

on n *és el grau de l'extensió* L/K*,* $f'(X)$ *denota el polinomi derivat de* $f(X)$ *i la norma* $N_{L/K}$ *es pot calcular com, si* L/K *és una extensió de Galois:*

$N_{L/K} = \prod_{i=1}^{n} f'(\theta_i)$*, on* $\theta_i = \sigma_i(\theta)$ *amb* $\sigma_i \in Gal(L/K)$.

Com que $\mathbb{Q}(i)/\mathbb{Q}$ té de polinomi mònic irreductible $f(X) = X^2 + 1$, amb $f'(X) = 2X$, el seu grau és $n = [\mathbb{Q}\colon \mathbb{Q}(i)] = 2$ i, per tant, el seu discriminant és:

$D(1, i) := (-1)^{2(2-1)/2} N_{\mathbb{Q}(i)/\mathbb{Q}}(f'(i)) = -N_{\mathbb{Q}(i)/\mathbb{Q}}(f'(i)) = -(-2i) \cdot \sigma(-2i) = -(-2i) \cdot (2i) = 4i^2 = -4 = -2^2$.

Usabt el discriminant, es troba que els primers ramifiquen a $\mathbb{Q}(i)/\mathbb{Q}$, fixant $A \subseteq \mathbb{Q}$. En aquest cas, ramifica $\mathfrak{p} = 2$.

[4] L'element primitiu existeix pel Teorema de Steinitz i prt la correspondència bijectiva de Galois.

Per exemple, si prenem dos ideals primers diferents de $\mathbb{Z}[i]$, $\mathfrak{P}_1 = (2+i)$ i $\mathfrak{P}_2 = (2-i)$, tenim que:

$$\begin{array}{ccc} (2+i)(2-i) & \subset & \mathbb{Z}[i] \\ | & & | \\ (5) & \subset & \mathbb{Z} \end{array}$$

Per tant, $\mathfrak{p} = 5$ descomposa totalment a $\mathbb{Z}[i]$, amb $e_i = f_i = 1$, però no ramifica.

A.2 Ramificació a l'extensió $\mathbb{F}_p(T, \Lambda_M)/\mathbb{F}_p(T)$

Prenem $A = \mathbb{F}_p[T]$ i considerem la següent extensió per i analitzar els ideals que generen polinomis de Carlitz:

$$\begin{array}{ccc} \mathbb{F}_p[T](\Lambda_M) & \subseteq & \mathbb{F}_p(T)(\Lambda_M) \\ | & & | \\ \mathbb{F}_p[T] & \subseteq & \mathbb{F}_p(T) \end{array}$$

En aquest cas, els ideals primers de $A = \mathbb{F}_p[T]$ són els polinomis irreductibles de $\mathbb{F}_p[T]$i λ és una arrel d'un polinomi de Carlitz (i.e. $C_M(X)$) que genera Λ_M. Per començar, analitzem els ideals que generen les arrels de $C_T(X)$:

Exemple A.11. *El polinomi de Carlitz bàsic per a la variable T és:*

$C_T(X) = TX + X^p = X(T + X^{p-1})$

$C_T(X)$ no és irreductible, però $f(X) = T + X^{p-1}$, sí.

Calculem, doncs, el discriminant de l'extensió $\mathbb{F}_p(T, \Lambda_T)/\mathbb{F}_p(T)$:

$f'(X) = (p-1)X^{p-2} \mod p \equiv -X^{p-2}$

Avaluem $f'(X)$ amb una arrel de $C_T(X)$, $\lambda = \sqrt[q-1]{-T}$:

$f'(\sqrt[q-1]{-T}) = -(\sqrt[q-1]{-T})^{q-2}$

Aleshores, tenim que:

$$N_{\mathbb{F}_q(T,\Lambda_T)}\big/_{\mathbb{F}_q(T)} = \prod_{\sigma \in Gal(\mathbb{F}_q(T,\Lambda_T)\big/_{\mathbb{F}_q(T)})} \sigma(\sqrt[q-1]{-T})^{q-2} = T^{q-2}$$

L'únic primer que ramifica a $A = \mathbb{F}_p[T]$ és T i ho fa totalment.

Hi ha altres dominis de Dedekind A' dins de $\mathbb{F}_p(T)$, amb $\mathrm{Quot}(A) = \mathbb{F}_p(T)$, on no necessàriament succeeix que $A \subseteq A'$.

A $\mathbb{F}_p(T)$ tenim també $A = \mathbb{F}_p[1/T] \subseteq \mathbb{F}_p(T)$, on $\mathbb{F}_p[1/T]$ és un domini de Dedekind i $\mathbb{F}_p(T)$=Quot($\mathbb{F}_p[1/T]$).

Per tant, a l'exemple anterior hem vist que únicament ramifica T a l'extensió $\mathbb{F}_p(T)(\Lambda_T)/\mathbb{F}_p(T)$ via $A = \mathbb{F}_p[T]$, però l'extensió pot tenir altres ramificacions si $A = \mathbb{F}_p[1/T]$. De fet, també ramifica en $1/T = \infty$.

Aquest fenomen no ocorre a $\mathbb{Q}$, on $\mathbb{Z}$ és un domini de Dedekind via inclusió .

A.3 Primers d'un cos L

Sigui $L/\mathbb{F}_p(X)$ una extensió finita, una valoració o primer de L on $L \cap \overline{\mathbb{F}_p} = \mathbb{F}_p$ és:

$$\nu : \qquad L^* \longrightarrow \mathbb{Z}$$

ν no és trivial i compleix:

- $\nu(x \times y) = \nu(x) + \nu(y)$
- $\nu(x + y) \geq min(\nu(x), \nu(y))$
- $\nu(1) = 0$
- $\nu^{-1}(\mathbb{N}_{\geq}1) \cup 0 = \mathfrak{p}$, ideal primer de l'anell.
  $\nu^{-1}(\mathbb{N})$ és un domini B de L, on Quot(B)=L, amb un únic ideal maximal $\mathfrak{p}$.

Per exemple, definim una valoració o primer de $\mathbb{Q}$:

$$\begin{array}{rccc} \nu_p : & \mathbb{Q}^* & \longrightarrow & \mathbb{Z} \\ & \frac{a}{b} = p^i \frac{a'}{b'} & \longmapsto & i \end{array}$$

on $(a, b) = 1$, $(a', b') = 1$, (b', p) i $(a', p) = 1$.

- $\nu^{-1}(\mathbb{N}) \cup 0 = \mathbb{Z}_{(p)}$, on $\mathbb{Z} \subseteq \mathbb{Z}_{(p)} \subseteq \mathbb{Q}$.

  $\mathbb{Z}_{(p)} = \{\frac{a}{b} | a, b \in \mathbb{Z}, (a, b) = 1 \ i \ p \nmid b\}$

  $\mathbb{Z}_{(p)}$ és localitzar $\mathbb{Z}$ en l'ideal (p).
- $\nu^{-1}(\mathbb{N}_{\geq 1}) = p\mathbb{Z}_{(p)}$

Exemple:

$$\begin{array}{ccc} \mathcal{O}_K & \subseteq & K \\ | & & | \\ \mathbb{F}_p[X] & \subseteq & \mathbb{F}_p(X) \end{array}$$

$\mathcal{O}_K$ és la clausura entera de K i $K/\mathbb{F}_p(X)$ és una extensió finita.

$\mathfrak{p}$ és un ideal de $\mathcal{O}_K$ i $\mathcal{O}_{K,\mathfrak{p}} = (\mathcal{O}_K \setminus \{\mathfrak{p}\})^{-1}\mathcal{O}_K$ (localitzar l'ideal $\mathfrak{p}$ en el domini $\mathcal{O}_K$).

Tot ideal primer de $\mathcal{O}_K$ dona una valoració d'un ideal primer de K i $\mathcal{O}_K, \mathfrak{p}$ Dedekind amb un únic ideal maximal. Llavors, un Domini de Dedekind és DIP (Lorenzini, 1996) i, per tant, aquest ideal és maximal $\mathfrak{p}\mathcal{O}_{K,\mathfrak{p}} = (\pi)$ i definim:

$$\begin{array}{rccc} \nu: & \mathcal{O}^*_{K,\mathfrak{p}} & \longrightarrow & \mathbb{N} \\ & \pi^i \cdot a & \longrightarrow & i \end{array}$$

amb $(a, \pi) = 1$

Similarment, tenim:

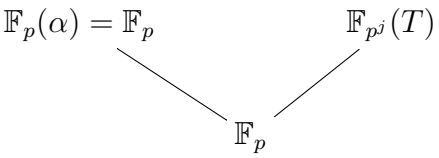
$$\begin{array}{ccc} \widetilde{\mathcal{O}_K} & \subset & K \\ | & & | \\ \mathbb{F}_p[1/X] & \subseteq & \mathbb{F}_p(X) \end{array}$$

$\widetilde{\mathcal{O}_K}$ és la clausura entera de $\mathbb{F}_p[1/X]$ dins K (domini de Dedekind) i donem valoracions diferents a les anteriors solucions, si i només si la valoració en $1/X$ és positiva, i.e. els primers de $\widetilde{\mathcal{O}_K}$ que estan sobre $\left(\frac{1}{X}\right)$ = "∞".

Tot ideal primer de K és d'un ideal primer de $\mathcal{O}_K$ o bé l'ideal orimer prové d'extendre "∞" = $\left(\frac{1}{X}\right)$. (Lorenzini, "An invitations to Arithmetic Geometry").

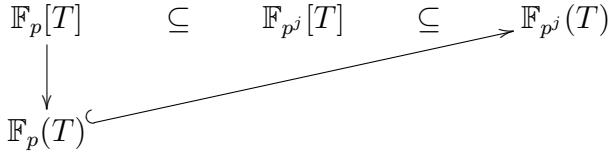
B Annex II: Extensió abeliana $\mathbb{F}_p(T)$ afegint-hi arrels de la unitat

L'extensió $\mathbb{F}_{p^j}/\mathbb{F}_p$ és finita, simple i algebraica. Pel curs d'Estructures Algebraiques, sabem que $\mathbb{F}_{p^j} = \mathbb{F}_p(\alpha) = \{w \in \overline{\mathbb{F}_p} : w^{p^j} - w\} = \{w(w^{p^j-1} - 1)\} =< \zeta_{p^j-1} >$, on $\zeta \in \overline{\mathbb{F}_p}$ és l'arrel de 1 en un cos de característica p i forma un grup cíclic.



L'extensió $\mathbb{F}_{p^j}/\mathbb{F}_p$ és Galois i, per tant, algebraica; en canvi, $\mathbb{F}_{p^j}(T)/\mathbb{F}_p$ és transcendent.

Per la propietat universal del cos de fraccions, tenim:



i volem estudiar $\mathbb{F}_{p^j}(T)/\mathbb{F}_p(T)$, on T és una variable sobre $\mathbb{F}_p$.

L'extensió $\mathbb{F}_p(T)/\mathbb{F}_p$ té grau de transcendència 1 i l'extensió de Galois $\mathbb{F}_{p^j}/\mathbb{F}_p$ té grau j i és cíclica, generada pel grup d'automorfismes de Frobenius $Frob$, definit per:

$$\begin{array}{rccc} Frob\colon & \mathbb{F}_{p^j} & \longrightarrow & \mathbb{F}_{p^j} \\ & a_0 & \longrightarrow & a_0^p \end{array}$$

$Frob$ és un automorfisme, ja que $\mathbb{F}_{p^j}$ és un cos finit amb característica positiva. En aplicar j vegades el morfisme de Frobenius, tenim $Frob^j(a_0) = a_0^{p^j} = a_0$, ja que $a_0^{p^j} = a_0$ per definició de $\mathbb{F}_{p^j}$ i, per tant, $Frob^j = id$ a $\mathbb{F}_{p^j}$.

A partir d'ara, suposem $j > 1$ i definim un nou morfisme d'anells:

$$\begin{array}{rccc} \widetilde{Frob}\colon & \mathbb{F}_{p^j}[T] & \longrightarrow & \mathbb{F}_{p^j}[T] \\ & a_0 + \cdots + a_n T^n & \longrightarrow & Frob(a_0) + \cdots + Frob(a_n)T^n \end{array}$$

$\widetilde{Frob}$ és un morfisme bijectiu que podem extendre al cos de fraccions de la següent manera:

$$\begin{array}{rccc} \widetilde{Frob}\colon & \mathbb{F}_{p^j}(T) & \longrightarrow & \mathbb{F}_{p^j}(T) \\ & \frac{p(T)}{q(T)} & \longrightarrow & \widetilde{Frob}\left(\frac{p(T)}{q(T)}\right) \end{array}$$

D'on tenim: $\widetilde{Frob}\left(\frac{p(T)}{q(T)}\right) = \frac{\widetilde{Frob}(p(T))}{\widetilde{Frob}(q(T))} = \frac{\widetilde{Frob}(a_nT^n+\cdots+a_0)}{\widetilde{Frob}(b_nT^n+\cdots+b_0)} = \frac{Frob(a_n)T^n+\cdots+Frob(a_0)}{Frob(b_n)T^n+\cdots+Frob(b_0)}$.

Hem vist que $Frob^j = id$; per tant, $\widetilde{Frob}^j = id$.

Volem veure que $\widetilde{Frob} \in Gal(\mathbb{F}_{p^j}(T)/\mathbb{F}_p(T))$ i, a més, $< \widetilde{Frob} >= Gal(\mathbb{F}_{p^j}(T)/\mathbb{F}_p(T))$.

Lema B.1. *L'extensió de cossos $\mathbb{F}_{p^j}(T)/\mathbb{F}_p(T)$ és Galois i abeliana.*

Demostració. Sabem que $\mathbb{F}_{p^j} = \mathbb{F}_p(\alpha)$, com que α és algebraic sobre $\mathbb{F}_p$, també ho és sobre $\mathbb{F}_p(T)$.

Així, volem veure que $Irr(\alpha, \mathbb{F}_p(T))[x] = Irr(\alpha, \mathbb{F}_p)[x]$ (clarament $Irr(\alpha, \mathbb{F}_p(T))[x] | Irr(\alpha, \mathbb{F}_p)[x]$, perquè $\mathbb{F}_p \subseteq \mathbb{F}_p(T)$). Suposem que són diferents; és a dir:

$Irr(\alpha, \mathbb{F}_p(T))[x] \cdot \pi(x) = Irr(\alpha, \mathbb{F}_p)[x]$, on $\pi(x) \in \mathbb{F}_p(T)[x]$

Noti's que el primer membre de l'equació depèn de T, mentre que el segon, no:

$(x^l + b_{l-1}x^{l-1} + \cdots + b_0)(x^{j-l} + \cdots) = x^j + a_{j-1}x^{j-1} + \cdots a_0$, on els coeficients $a_i \in \mathbb{F}_p$ i $b_i = \frac{c_i}{d_i} \in \mathbb{F}_p(T)$.

- Les arrels de $Irr(\alpha, \mathbb{F}_p)[x]$ pertanyen a $\mathbb{F}_{p^j}$=$\mathbb{F}_p(\alpha)$.
- Totes les arrels de $Irr(\alpha, \mathbb{F}_p(x))[T]$ estan a $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_p(\alpha)[T]$.

Així, les arrels d'ambdós polinomis pertanyen a $\mathbb{F}_{p^j} \subseteq \overline{\mathbb{F}_p}$.

Així doncs, en el cos de descomposició de $p(x) = Irr(\alpha, \mathbb{F}_p(T))[x]$, tenim:

$$Irr(\alpha, \mathbb{F}_p(T))[x] = \prod_{\beta \ tq. \ p(\beta)=0} (x - \beta) = x^i - b_{i-1}x^{j-1} + \cdots + b_0,$$

Amb $p(x) \in \ \mathbb{F}_{p^j}[x] \cap \mathbb{F}_p(T)[x]$ i $b_k \in \ \mathbb{F}_{p^j} \cap \mathbb{F}_p(T) = \mathbb{F}_p \ \forall k$.

Per tant, $Irr(\alpha, \mathbb{F}_p(T))[x] \ \in \mathbb{F}_p[T]$ i com que és no trivial i divideix $Irr(\alpha, \mathbb{F}_p)[x]$ són el mateix polinomi.

$\widetilde{Frob}$ és el generador del grup de Galois, ja que $(\widetilde{Frob})^j = id$ i cap $i < j$ fa que $(\widetilde{Frob})^i = id$.

El grau de l'extensió és $[\mathbb{F}_{p^j}(T) : \mathbb{F}_p(T)] = j$ i és Galois perquè és el cos de descomposició de $X^{p^j} - X$ sobre $\mathbb{F}_p(T)$. □

Definició B.2. *L'extensió $\mathbb{F}_{p^j}(T)/\mathbb{F}_p(T)$ s'anomena extensió constant de $\mathbb{F}_p(T)$.*