Universitat Autònoma de Barcelona

Anàlegs de l'equació de Fermat en l'aritmètica del cos de les funcions racionals sobre un cos finit

Autor
Habib Ullah Abdul Parveen

Supervisor
Francesc Bars Cortina

Juliol 2022

Índex

1 Introducció

L'objectiu d'aquest treball és estudiar l'equació de Fermat,

$$X^n + Y^n = Z^n. \tag{1.1}$$

en característica positiva, com poden ser els cossos finits $\mathbb{F}_q$ amb q potència d'un primer; cossos de funcions, i.e. extensions finites de $\mathbb{F}_q(T)$ i per acabar una analogia de l'equació de Fermat.

Per aquest propòsit el treball està dividit en tres parts, en la primera s'estudia l'equació (1.1) en cossos finits i cossos de funcions, segona i tercera secció respectivament.

La segona part comença amb la tercera secció, on s'observa que (1.1) es pot factoritzar,

$$(X - \xi_n^i Y) = Z^n, \tag{1.2}$$

en l'anell $\mathbb{Z}[\xi_n] \subset \mathbb{Q}(\xi_n)$ amb ξ_n arrel primitiva n-èssima de la unitat. Les extensions ciclotòmiques $\mathbb{Q}(\xi_n)/\mathbb{Q}$ són un cos de descomposició del polinomi $x^n - 1$. El propòsit de la secció 5 és introduir i justificar perquè l'acció de Carlitz $\mathbb{F}_q[T] \to \mathbb{F}_q[T][X]$, $a \mapsto [a](X)$ proporciona extensions i polinomis que són un anàleg de les extensions ciclotòmiques i els polinomis $x^n - 1$, però en $\mathbb{F}_q[T]$.

Un cop realitzada la justificació, en la tercera part s'introdueixen les equacions de Goss-Fermat, donat $a \in \mathbb{F}_q[T]$ considerarem

$$Z^{q^{\deg a}} = \prod_{\xi_i \in \Lambda_a} (X - \xi_i Y)$$

on $\Lambda_a \subset \overline{\mathbb{F}_q(T)}$ és el conjunt de totes les arrels de $[a](X)$ en la clausura separable de $\mathbb{F}_q(T)$ i $X, Y, Z \in \mathbb{F}_q[T]$. Veurem el teorema de Goss-Fermat entre altres coses afirma que no hi ha solucions si $q > 2$ i $\deg a > 1$.

2 L'equació de Fermat en cossos finits

En aquest apartat busquem $X, Y, Z \in \mathbb{F}_q$ amb q una potència d'un primer p, que compleixen la igualtat

$$X^n + Y^n = Z^n. \tag{2.1}$$

Proposició 2.2. *Fixats un primer p i $n \geq 1$, l'equació de Fermat $X^n + Y^n = Z^n$ sempre té solucions amb $XYZ \neq 0$ en $\mathbb{F}_q$ on $q = p^m$ per cert $m \in \mathbb{N}$.*

Demostració. Siguin $\alpha, \beta \in \mathbb{F}_{p^r}$ dos elements del cos finit de p^r elements. Si $\alpha^n + \beta^n = Z^n$ té alguna solució en $\mathbb{F}_{q^r}$ ja estem; en cas contrari, considerem el polinomi mònic $f(T) = T^n - (\alpha^n + \beta^n) \in \mathbb{F}_{p^r}[T]$; sigui $\mathbb{F}_{p^m}/\mathbb{F}_{p^r}$ una extensió on hi ha una arrel de $f(t)$ diguem-ne γ, llavors (α, β, γ) és solució de l'equació de Fermat en $\mathbb{F}_{p^m}$.

□

Exemple 2.3. *Fixem $n = q$ una potència d'un primer, llavors*

$$X^q + Y^q = Z^q \Leftrightarrow X + Y = Z$$

ja que $\alpha^q = \alpha$ per tot $\alpha \in \mathbb{F}_q$.

Exemple 2.4. *Considerem $n = 3$ i $p = 5$. Volem resoldre,*

$$X^3 + Y^3 = Z^3, \qquad amb\ X, Y, Z \in \mathbb{F}_5.$$

Pel petit teorema de Fermat, $a^4 = 1$ per tot $a \in \mathbb{F}_5^\times$; per tant $a^9 = a^5 = a$ per tot $a \in \mathbb{F}_5$. Considerem l'equació

$$A + B = C,$$

llavors (A^3, B^3, C^3) és solució de l'equació de Fermat; ja que $X^3 = A^9 = A$, $Y^3 = B$, $Z^3 = C$. Recíprocament, si (X, Y, Z) és una solució de l'equació de Fermat llavors (X^3, Y^3, Z^3) és solució de $A + B = C$.

El següent resultat generalitza els dos exemples anteriors.

Proposició 2.5. *Fixem q una potència d'un primer, i $n \in \mathbb{N}$ tal que $\gcd(n, q-1) = 1$. Hi ha una bijecció entre les solucions de $X^n + Y^n = Z^n$ i les de $A + B = C$ en $\mathbb{F}_q$.*

Demostració. Donat que $\mathbb{F}_q^\times$ és un grup cíclic de $q - 1$ elements, podem considerar α un generador qualsevol. Llavors α^n també és un generador donat que $\gcd(n, q-1) = 1$, per tant tot element de $\mathbb{F}_q$ és una potència n-èssima d'un únic element.

Per veure la unicitat, denotem per $\mu = \alpha^n$ i siguin $\beta, \gamma \in \mathbb{F}_q^\times$ tal que $\beta^n = \gamma^n$. Existeixen enters i, j tal que $\mu^i = \beta$ i $\mu^j = \gamma$ llavors $\mu^{in} = \mu^{jn}$ per tant $(q-1)|(i-j)n$ o sigui $(q-1)|(i-j)$ i així $\beta = \mu^i = \mu^j = \gamma$.

La correspondència ve donada per

$$(X, Y, Z) \mapsto (A, B, C) = (X^n, Y^n, Z^n)$$

La inversa està ben definida degut la unicitat. □

Recordem el següent teorema de Dirichlet, per una demostració mireu [9, pàg. 1].

Teorema 2.6. ***(Dirichlet)*** *Siguin $n, r \in \mathbb{Z}$ tals que $mcd(n, r) = 1$ llavors la successió $x_a = an + r$ conté infinits nombres primers.*

Corol·lari 2.7. *Fixem $n > 2$ senar. L'equació $X^n + Y^n = Z^n$ té solucions no trivials en $\mathbb{F}_p$ per cert primer p.*

Demostració. Per la proposició anterior serà suficient trobar un primer tal que $mcd(n, p-1) = 1$. Com n és senar llavors $\gcd(n, 2) = 1$ i pel Teorema (2.6) hi ha un primer p congruent amb 2 mòdul n. Aleshores $p - 1 \equiv 1 \mod n$ i per tant $\gcd(p-1, n) = 1$.

□

Exemple 2.8. *Considerem $p = 3$ i $n = 2$. L'equació $X^2 + Y^2 = Z^2$ només té solucions trivials. Pel petit teorema de Fermat $a^2 = 1$ per tot $a \in \mathbb{F}_3^\times$ i clarament $1 + 1 \neq 1$ en $\mathbb{F}_3$.*

Proposició 2.9. *Considerem $p \geq 5$ i $n = 2$. L'equació de Fermat sempre té solucions no trivials en $\mathbb{F}_p$.*

Demostració. Si dividem per Y^2 en l'equació obtenim una nova equació

$$X^2 + 1 = Z^2, \tag{2.10}$$

per veure l'existència d'una solució, serà suficient comprovar que hi ha dos quadrats no nuls $a, b \in \mathbb{F}_p$ tal que $a - b = 1$. Escollim els representants $\{\overline{0}, ..., \overline{p-1}\}$ de les classes mòdul p.

Raonem per reducció a l'absurd, suposem que (2.10) no té cap solucó, per tant no hi ha dos quadrats que els seus representats difereixen en 1. Però com en $\mathbb{F}_p^\times$ la meitat dels elements són quadrats i l'altre

no llavors el representant dels quadrats han de tenir la mateixa paritat. Com 1 és un quadrat llavors tots els representants dels quadrats han de ser senars. Però $\overline{4}$ és un quadrat i el seu representant no és senar (ja que $4 < 5 \leq p$)

□

Proposició 2.11. *Considerem l'equació*

$$A^n + B^n = C^n + D^n \tag{2.12}$$

en $\mathbb{F}_q$. Suposem $n|q-1$ i $4n^2+n+1 < q$, llavors hi ha solucions no trivials.

Demostració. Sigui $\lambda \in \mathbb{F}_q^\times$ un generador del grup cíclic de les unitats, denotem $\mu = \lambda^n$ i sigui el subgrup $G = \langle \mu \rangle$ i considerem $H_\alpha = G + \alpha$, amb $\alpha \in G$. Es compleix $|H_\alpha| = |G| = \frac{q-1}{n}$.

Remarquem que G conté tots, i només, els elements de $\mathbb{F}_q^\times$ que són una potència n-èssima. Observem, (2.12) té solucions no trivials si $H_\alpha \cap H_\beta \neq \{\alpha + \beta\}$ per algun $\alpha, \beta \in G$.

Per reducció a l'absurd suposem $H_\alpha \cap H_\beta = \{\alpha+\beta\}$ sempre i quan $\alpha \neq \beta$. Es segueix, $H_\alpha \cap H_\beta \cap H_\gamma = (H_\alpha \cap H_\beta) \cap (H_\beta \cap H_\gamma) = \{\alpha+\beta\} \cap \{\beta+\gamma\} = \emptyset$ si α, β, γ diferents dos a dos. Llavors

$$\begin{aligned} |\cup_{\alpha \in G} H_\alpha| &= \sum_{\alpha \in G} |H_\alpha| - \frac{1}{2} \sum_{\alpha \neq \beta \in G} |H_\alpha \cap H_\beta| \\ &= \Big(\frac{q-1}{n}\Big)^2 - \frac{1}{2}\Big(\frac{q-1}{n}\frac{q+n-1}{n}\Big) \\ &= \frac{q-1}{n^2}\Big(\frac{q-1}{2} - \frac{n}{2}\Big) \end{aligned}$$

En la segona igualtat hem usat $|G| = |H_\alpha| = \frac{q-1}{n}$ i que el segon sumant, equival a comptar parelles ordenades de $G \times G$, ja que $|H_\alpha \cap H_\beta| = 1$. Per construcció, el resultat no pot ser més gran que $|\mathbb{F}_q| = q$,

$$\frac{q-1}{n^2}\Big(\frac{q-1}{2} - \frac{n}{2}\Big) - 1 \leq q - 1 \tag{2.13}$$

$$\frac{q-1}{2} - \frac{n^2}{q-1} \leq n^2 + \frac{n}{2} \tag{2.14}$$

$$q - 1 \leq (2 + \frac{2}{q-1})n^2 + n \tag{2.15}$$

arribem a contradicció, per tant hi ha $\gamma \in H_\alpha \cap H_\beta$ diferent de $\alpha + \beta$, o sigui $\gamma = \alpha + \delta_1 = \beta + \delta_2$ amb $\delta_1, \delta_2 \in G$. Per tant hi ha solucions no trivials.

□

Observació 2.16. *Si $mcd(n, q-1) = 1$ llavors és immediat que l'equació de la proposició anterior té solucions no trivials, donat que tot element és una potència n-èssima.*

3 L'equació de Fermat en cossos de funcions

En aquest resoldrem l'equació de Fermat,

$$X^n + Y^n = Z^n$$

amb solucions en cossos de funcions. És a dir, extensions finites de $F(T)$, on F és un cos i T un element trascendent.

El següent Teorema, i la demostració, es poden trobar en [1, pàg. 94]. Els conceptes que s'utilitzen, com és el gènere g_K; el teorema ABC; l'altura; divisors, s'expliquen l'Apèndix IV : Global Fields.

Es diu que un cos F és perfecte si tot polinomi irreductible amb coeficients en F no té arrels repetides. En concret, tots els cossos finits $\mathbb{F}_q$ són exemple de cossos perfectes.

Teorema 3.1. *Sigui K un cos de funcions amb cos de constants perfecte F. Considerem l'equació $X^n + Y^n = 1$. Suposarem que n no és divisible per la característica p de F. Si $g_K = 0$ i $n \geq 3$, llavors no hi ha solucions no constants d'aquesta equació en K. Si $g_K \geq 1$ i $n > 6g_K - 3$, llavors no hi ha solucions no constants en K.*

Per solucions no constants ens referim a solucions $(X, Y, Z) \in K^\times \setminus F^\times$.

Demostració. Suposem que $(u, v) \in K^2$ és una solució no constant. Pel teorema ABC es compleix

$$\max(\deg_s u^n, \deg_s v^n) \leq 2g_K - 2 + \sum_{P \in \mathrm{Supp}(A+B+C)} \deg_K P, \tag{3.2}$$

on A és el zero divisor de u, B és el zero divisor de v, i C és el divisor polar comú.

Sigui M l'extensió maximal separable de $F(u)$ en K. Per la torre de cossos $F(u^n) \subset F(u) \subset M \subset K$ i $\mathrm{mcd}(p, n) = 1$ es concloeix: $F(u)/F(u^n)$ és una extensió separable de grau n i $\deg_s u^n = n \deg_s u$ de manera similar $\deg_s v^n = n \deg_s v$.

Comparant els zero divisors de u en M amb els zero divisors de u en K, es pot veure, $\sum_{P \in \mathrm{Supp}(A)} \deg_K P \leq \deg_s u$, pel mateix raonament $\sum_{P \in \mathrm{Supp}(B)} \deg_K P \leq \deg_s v$. Com C és el divisor polar en comú de u i v hi ha una desigualtat similar amb C.

Usant les desigualtats de l'anterior paràgraf, substituint en (3.2) arribem

$$n \sum_{P \in \mathrm{Supp}(A)} \deg_K P \leq 2g_K - 2 + \sum_{P \in \mathrm{Supp}(A+B+C)} \deg_K P.$$

Fem el mateix amb B i C; sumant les tres desigualtats i manipulant s'obté

$$(n-3) \sum_{P \in \mathrm{supp}(A+B+C)} \deg_K P \leq 6g_K - 6$$

Si $g_K = 0$ i $n \geq 3$, la part esquerrana de la desigualtat és no negativa, i la part dreata és -6. Arribem a una contradicció.

Si $g_K \geq 1$ i $n > 6g_K - 3$, clarament $n \geq 4$ per tant $n - 3$ és positiu. Dividint a les dues bandes de la desgualtat per $n - 3$ veiem que $(6g_K - 6)/(n - 3)$ ha de ser major que 1. Com $(6g_K - 6)/(n - 3) < 1$ és equivalent a $n > 6g_K - 3$ la proposició queda demostrada.

□

Observació 3.3. *Aquesta darrera proposiciò ens garanteix que l'equació $X^n + Y^n = Z^n$ no té solucions per a n suficienment gran en un cos de funcions K.*

En concret, $\mathbb{F}_q(T)$ té gènere 0, per tant l'eqüació (2.1) només té solucions constants. Recordem que el cas $\mathbb{F}_q(T)$ va ser estudiat influenciat per l'equació de Fermat en $\mathbb{Q}$ i finalment resolt per Wiles i altres matemàtics, veieu [10]

Teorema 3.4. ***(Últim Teorema de Fermat)*** *La igualtat*

$$X^n + Y^n = Z^n$$

amb $X, Y, Z \in \mathbb{Q}$ només té solucions trivials, i.e. $XYZ = 0$, quan $n > 2$.

4 Cap a un altre anàleg de l'equació de Fermat per $\mathbb{F}_q[T]$

Considerem l'equació de Fermat

$$X^n + Y^n = Z^n \tag{4.1}$$

amb $X, Y, Z \in \mathbb{Q}$. L'equació (4.1) es pot factoritzar usant les arrels del polinomi $X^n - 1$. Denotem per $\mu_n = \{\alpha \in \mathbb{C} : \alpha^n = 1\}$ i per $\xi_n = e^{\frac{2\pi i}{n}}$ una arrel primitiva n-èssima de la unitat, llavors

$$\prod_{i=1}^{n} \left(\frac{X}{Y} - \xi_n^i \right) = \left(\frac{X}{Y} \right)^n - 1;$$

d'on es segueix

$$X^n + Y^n = \prod_{i=1}^{n} \left(X - \xi_n^i Y \right) = Z^n. \tag{4.2}$$

Aquesta factorització ocòrre en $\mathbb{Z}[\mu_n] \subset \mathbb{Q}(\mu_n)$. A les extensions $\mathbb{Q}(\mu_n)/\mathbb{Q}$ es coneixen com extensions ciclotòmiques, algunes de les propietats que es coneixen: el grau, $[\mathbb{Q}(\mu_n) : \mathbb{Q}] = \varphi(n)$ (on φ denota la funció d'Euler); el grup de Galoi $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ és isomorf a $\left(\mathbb{Z}/n\right)^\times$; la clausura entera de $\mathbb{Z}$ en $\mathbb{Q}(\mu_n)$ (conegut com l'anell d'enters) és $\mathbb{Z}[\mu_n]$. L'anell $\mathbb{Z}[\mu_n]$ és un domini de Dedekind, i.e. tot ideal no nul de $\mathbb{Z}[\mu_n]$ factoritza de forma única en producte d'ideals primers. Si n és senar, llavors només ramifiquen els primers tal que $p|n$.

Un cop realitzat aquest anàlisi d'introduir arrels de la unitat, pensem en buscar un anàleg de les extensions ciclotòmiques en característica positiva.

Donat $\mathbb{F}_q(T)$, amb $\mathbb{F}_q$ un cos finit, podríem considerar el polinomi $X^n - 1$, i afegir les arrels d'aquesta (i.e. arrels de la unitat) en $\mathbb{F}_q(T)$. El resultat seria l'extensió $\mathbb{F}_{q'}(T)/\mathbb{F}_q(T)$ on $\mathbb{F}_q \subset \mathbb{F}_{q'}$ amb $q' = q^r$. La clausura entera de $\mathbb{F}_q[T]$ en $\mathbb{F}_{q'}(T)$ és $\mathbb{F}_{q'}[T]$. El grup de Galois és isomorf al grup de Galois de $\mathbb{F}_{q'}/\mathbb{F}_q$ que està generat per $F : x \mapsto x^q$ i té r elements. Veiem doncs, aquesta analogia no captura el grup de Galois de les extensions ciclotòmiques. A més, les equacions de Fermat sobre $\mathbb{F}_q(T)$ ja les hem resolt.

Per un altre analogia, comencem reinterpretant un dels fets més elementals, la funció exponencial. Ens centrem en el món complex, si $\alpha, \beta \in \mathbb{C}$ es ben conegut que $e^{\alpha\beta} = (e^\alpha)^\beta$, amb e^x la funció exponencial; és a dir el següent diagrama és commutatiu:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{e^x} & \mathbb{C} \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle x^\beta} \\ \mathbb{C} & \xrightarrow{e^x} & \mathbb{C} \end{array} \tag{4.3}$$

Observem que $\mathbb{C}$ adquireix una estructura de $\mathbb{Z}$ mòdul amb l'operació: $[n](\alpha) = \alpha^n$ amb $n \in \mathbb{Z}$ i $\alpha \in \mathbb{C}$. Els punts de torsió fixat n, corresponen a trobar els $\alpha \in \mathbb{C}$ tal que $[n](\alpha) = \alpha^n = 1$, i.e. les arrels n-èssimes de la unitat.

La idea és, substituir el paper dels enters $\mathbb{Z}$ per $\mathbb{F}_q[T]$, per tant $\mathbb{Q}$ per $\mathbb{F}_q(T)$ i finalment $\mathbb{C}$ per $\mathbf{C}_\infty$ la completació d'una clausura separable de $\mathbb{F}_q((1/T))$, que és un cos separablement tancat i complet respecte la valoració associada a "$\infty = \frac{1}{T}$".

Carlitz va introduir l'exponencial en característca positiva. Existeix una funció $e_C(x) : \mathbf{C}_\infty \to \mathbf{C}_\infty$ que satisfà la igualtat:

$$e_C(Tx) = Te_C(x) + \big(e_C(x)\big)^q,$$

el diagrama (4.3) es converteix en

$$\begin{array}{ccc} \mathbf{C}_\infty & \xrightarrow{e_C(x)} & \mathbf{C}_\infty \\ {\scriptstyle \pi(T)}\downarrow & & \downarrow{\scriptstyle [\pi](x)} \\ \mathbf{C}_\infty & \xrightarrow{e_C(x)} & \mathbf{C}_\infty \end{array} \tag{4.4}$$

on $\pi(T) \in \mathbb{F}_q[T]$ i a l'aplicació $\pi \to [\pi](x)$ s'anomena el mòdul de Carlitz i ho denotarem per $[\pi](x) \in (\mathbb{F}_q[T])[x]$. Com abans, si tenim $\pi(T) \in \mathbb{F}_q[T]$ i $\alpha \in \overline{\mathbb{F}_q(T)}$ llavors l'operació $\pi \cdot \alpha = [\pi](\alpha)$ dota a $\overline{\mathbb{F}_q(T)}^{\text{sep}}$ d'una estructura de $\mathbb{F}_q[T]$-mòdul.

Donat $\pi \in \mathbb{F}_q[T]$ podem considerar els punts de torsió, és a dir el conjunt $\alpha \in \Lambda_\pi \subset \overline{\mathbb{F}_q(T)}^{\text{sep}}$ tal que $[\pi](\alpha) = 0$. El conjunt Λ_π està generat per cert element $\lambda \in \Lambda_\pi$ com $\mathbb{F}_q[T]$-mòdul; és un anàleg de les arrels n-èssimes de la unitat.

Si denotem $K = \mathbb{F}_q(T)(\Lambda_\pi)$: l'extensió $K/\mathbb{F}_q(T)$ és abeliana (cíclica si π és una potència d'un irreductible i $q > 2$). La clausura entera de $\mathbb{F}_q[T]$ en K és $\mathbb{F}_q[T][\Lambda_\pi]$ que és un domini de Dedekind; només ramifiquen els primers $p|\pi$ ramifiquen completament i moderadament.

L'anàleg de (4.1) mitjançant el mòdul de Carlitz es realitza mitjançant (4.2), si $\pi \in \mathbb{F}_q[T]$ llavors considerarem

$$Z^{q^{\deg \pi}} = \prod_{\xi_i \in \Lambda_\pi} (X - \xi_i Y) \tag{4.5}$$

amb $Z, X, Y \in \mathbb{F}_q[T]$.

5 Mòdul de Carlitz

5.1 Polinomis de Carlitz

En aquestes seccions seguim [8]. En aquesta secciò ens centrem en l'anell $A := \mathbb{F}_q[T]$ i $A[X] := \mathbb{F}_q[T][X]$, veurem els seus elements com polinomis en X amb coeficients en $\mathbb{F}_q[T]$.

Donat $T \in \mathbb{F}_q[T]$ definim $[T](X) = X^q + TX$, i $T^n = [T^{n-1}]([T](X))$, finalment si $M(T) = \sum_{i=0}^{n} c_i T^i \in \mathbb{F}_q[T]$ llavors $[M(T)](X) = \sum_{i=0}^{n} c_i [T^n](X)$. Als polinomis $[M(T)](X)$ es diuen polinomis de Carlitz, i a l'aplicació $M(T) \to [M(T)](X)$ **mòdul de Carlitz**.

Exemple 5.1.

1. *Considerem T^2, llavors el polinomi de Carlitz és*

$$[T^2](X) = (X^q + TX)^q + T(X^q + TX) = X^{q^2} + (T^q + T)X^q + T^2X$$

2. *El cas T^3,*

$$[T^3](X) = X^{q^3} + (T^{q^2} + T^q + T)X^{q^2} + (T^{2q} + T^{q+1} + T^2)X^q + T^3X$$

Observació 5.2. *El mòdul de Carlitz proporciona polinomis $\mathbb{F}_q$-lineals, ja que s'obtenen de combinacions $\mathbb{F}_q$-lineals de composicions de $[T](X)$ i pel corol·lari (11.5) aquests són també $\mathbb{F}_q$-lineals.*

Observem també que si $f \in A$ llavors $\deg_X([f](X)) = q^{\deg f}$.

Proposició 5.3. *Siguin $f, g \in A$ llavors:*

1. $[g \cdot f](X) = [g]([f](X))$
2. *$f|g$ si i només si $[f](X)|[g](X)$.*
3. $[g]([f](X)) = [f]([g](X))$

Demostració. Les demostracions són bastant inmediates:

1. Usant $[T^n](X) = [T^{n-1}]([T](X))$ s'obté $[T^n](X) = [T^{n-m}]([T^m](X))$, llavors

$$\begin{aligned}
[g \cdot f](x) &= [\sum_{i=0}^{n}\sum_{j=0}^{m} g_i f_j T^{i+j}](X) \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} [g_i f_j T^{i+j}](X) \\
&= \sum_{i=0}^{n}\sum_{j=0}^{m} [g_i T^i]([f_j T^j](X)) \\
&= [g]([f](X))
\end{aligned}$$

   En la penúltima igualtat hem usat que els polinomis de Carlitz són $\mathbb{F}_q$-lineals.

2. Si $f|g$ llavors existeix $h \in A$ tal que $g = fh$, llavors $[g](X) = [hf](X) = [h]([f](X))$ i pel corol·lari (11.5) deduim $[f](X)|[g](X)$.

   Suposem ara $[f](X)|[g](X)$, per l'observació anterior $\deg f \leq \deg g$ i per tant $g = fh + r$ per certs $h, r \in A$ i $\deg r < \deg f$. D'on es segueix $[f](X)$ divideix $[h]([f](X)) + [r](X)$ però llavors $[f](X)$ divideix $[r](X)$ d'on concloem $\deg f \leq \deg r$, absurd.

3. Pel punt 1, i el fet que $fg = gf$.

□

Observació 5.4. *En l'exemple (5.1) al calcular $[T^2](X)$ i $[T^3](X)$, es veu que el coeficient de X és T^2 i T^3 respectivament. En general, el coeficient de X en $[T^i](X)$ és T^i i més en general, si $f = \sum_{i=0}^{n} f_i T^i \in A$ llavors*

$$[f](X) = \sum_{i=0}^{n} f_i [T^i](X) = \sum_{i=2}^{q^{\deg f}} c_i X^i + fX$$

amb $c_i \in A$.

Lema 5.5. *Sigui $f \in A$ llavors la derivada de $[f](X)$, respecte X, és f. Per tant, $[f](X)$ és separable si $f \neq 0$.*

Demostració. Per l'observació anterior. □

Tenint en compte el punt 3 de la Proposició (5.3) i el corol·lari (11.6) donat $\gamma \in \overline{\mathbb{F}_q(T)}$ (la clausura separable de $\mathbb{F}_q(T)$) una arrel no nula de $[f](X)$ amb $f \in A$ definim

$$\begin{aligned} v_\gamma : \mathbb{F}_q[T] &\to \mathbb{F}_q(T)[\gamma] \\ g(T) &\mapsto [g](\gamma) \end{aligned}$$

Aquesta aplicació és $\mathbb{F}_q$-lineal, però a més a més $\ker(v_\gamma)$ és un ideal de $\mathbb{F}_q[T]$ i $\mathrm{Im}(v_\gamma)$ conté arrels de $[f](X)$.

Lema 5.6. *Considerem f irreductible en A, v_γ el morfisme descrit, amb $\gamma \neq 0$ arrel de $[f](X)$. Llavors $|Im(v_\gamma)| = q^{\deg f}$*

Demostració. Pel teorema de l'isomorfisme $\mathrm{Im}(v_\gamma) \cong \mathbb{F}_q[T]/\ker(v_\gamma)$. Afirmem que $\ker(v_\gamma) = (f)$. Està clar que $(f) \subset \ker(v_\gamma)$ i com el nucli d'aquesta aplicació és propi, ja que $v_\gamma(1) = \gamma \neq 0$. I (f) maximal, ja que f és irreductible; llavors $\ker(v_\gamma) = (f)$.

$$|\mathrm{Im}(v_\gamma)| = |\mathbb{F}_q[T]/(f)| = q^{\deg f}$$

□

Lema 5.7. *Sigui $f, g \in A$, llavors $mcd(f, g) = 1$ si i només si $mcd([f](X), [g](X)) = X$, vists com apolinomis en la variable X.*

Demostració. Demostrem el contrarecíproc, $\gcd(f, g) > 1$ si i només si $\deg_X(\mathrm{mcd}([f](X), [g](X)) > 1$.

La implicació $\Rightarrow$) és evident per la proposició (5.3). Per l'altre, considerem $\gamma \in \overline{\mathbb{F}_q(T)}$ no nul tal que $[g](\gamma) = [f](\gamma) = 0$. Factoritzem $f = f_1 \cdot \ldots f_n$ en irreductibles (no necessàriament diferents), considerem $\gamma_i = [f_i \cdot \ldots f_n](\gamma)$.

Tenim dues possibilitats: $\gamma_i = 0$ per tot $i \leq n$ i per tant $[f_n](\gamma) = 0$, i.e. γ és una arrel no nula de $[f_n](X)$. Per la proposició anterior totes les arrels de $[f_n](\gamma)$ estan en $\mathrm{Im}(v_\gamma)$ i així $[f_n](X)|[g](X)$, llavors $f_n|g$.

En l'altre cas, considerem i minimal tal que $\gamma_i \neq 0$. Obsevem que $i > 1$, ja que γ és arrel de f per hipòtesis, aleshores $\gamma_{i-1} = [f_{i-1}](\gamma_i) = 0$, per tant $\gamma_i = [f_i \cdot \ldots \cdot f_n](\gamma)$ és una arrel de $[f_{i-1}](X)$. Observant que $\gamma_i \in \mathrm{Im}(v_\gamma)$ i per tant γ_i també és una arrel comuna de f i g. Considerem el morfisme v_{γ_i}, repetim l'argument de d'adalt i obtindrem $[f_{i-1}](X)|[g](X)$ o sigui $f_{i-1}|g$. □

Teorema 5.8. *Suposem $\pi \in A$ és un mònic irreductible i denotem $\boldsymbol{F}_\pi = \mathbb{F}_q[T]/\pi$. Per $f \in A$, sigui $\overline{[f]}(X)$ el resultat de reduir els coeficients de $[f](X)$ mòdul π. Si $\gcd(f, \pi) = 1$ llavors $\overline{[f]}(X)$ és separable en $\boldsymbol{F}_\pi[X]$, mentres que $\overline{[\pi]}(X) = X^{q^{\deg \pi}}$*

Demostració. Com $[f]'(X) = f$ i $[\pi]'(X) = \pi$. Si $\mathrm{mcd}(f, \pi) = 1$ llavors $\overline{[f]}'(X) = f \mod \pi$ és una constant no nula com a polinomi en X, per tant $\overline{[f]}(X)$ és separable sobre $\mathbf{F}_\pi$. Per altre banda, $\overline{[\pi]}'(X) = \pi \mod \pi$ i per tant zero, així $\overline{[\pi]}(X)$ és inseparable en $\mathbf{F}_\pi[X]$. Com $[\pi](X)$ és mònic i de grau $q^{\deg \pi}$, ja que π és mònic, la reducció $\overline{[\pi]}(X)$ en $\mathbf{F}_\pi[X]$ és mònic de grau $q^{\deg \pi}$. Per veure $\overline{[\pi]}(X) = X^{q^{\deg \pi}}$ comprovarem que la única arrel de $\overline{[\pi]}(X)$ en la clausura algebraica $\overline{\mathbf{F}_\pi}$ és 0.

Per reducció a l'absurd, suposem que hi ha una arrel γ de $\overline{[\pi]}(X)$ no nula. Per $M \in A$, $[M](\gamma)$ és una arrel de $\overline{[\pi]}(X)$ ja que $[\pi](M[\gamma]) = [\pi M](\gamma) = [M]([\pi](\gamma)) = 0 \mod \pi$. Per això considerem l'aplicació $A \to \overline{\mathbf{F}_\pi}$ donada per $M \to [M](\gamma)$, aquesta és una aplicació lineal amb nucli

$$\{M \in A : [M](\gamma) = 0\}.$$

El nucli no és només un subgrup de $\mathbb{F}_q[T]$ sino un ideal: si $[M](\gamma) = 0$ i $N \in \mathbb{F}_q[T]$ llavors $[NM](\gamma) = [N]([M](\gamma)) = [N](0) = 0$. El nucli és propi i a més conté π. Com (π) és un ideal maximal, llavors el nucli és (π), així pel teorema d'isomorfisme podem deduir que $|A/\pi| = q^{\deg \pi} = \deg \overline{[\pi]}(X)$. Per tant, $\overline{[\pi]}(X)$ té tantes arrels diferents com el seu grau, però el polinomi no és separable, per tant $\overline{[\pi]}(X) = X^{q^{\deg \pi}}$. □

Corol·lari 5.9. *Per tot $\pi \in A$ irreductible, els coeficients de $[\pi](X)$, menys el més gran, són múltiples de π. En particular, $[\pi](X)/X$ és un polinomi Eisenstein respecte π amb terme independent π.*

Demostració. Per $c \in \mathbb{F}_q^\times$ es compleix $[c\pi](X) = c[\pi](X)$, per tant podem assumir que π és mònic. Llavors el terme més gran de $[\pi](X)$ en $A[X]$ és $X^{q^{\deg \pi}}$ i pel teorema anterior, $\overline{\pi}(X) = X^{q^{\deg \pi}}$ en $(\mathbb{F}_q[T]/\pi)[X]$. Així tots els termes de grau menor a $q^{\deg \pi}$ són múltiples de π. Per l'observació (5.4) el terme independent de $[\pi](X)/X$ ha de ser π. □

Corol·lari 5.10. *Per tot irreductible $\pi \in A$ i enter $k \geq 1$, els coeficients de $[\pi^k](X)$, exceptuant el més gran, són múltiples de π.*

Demostració. És cert per $k = 1$. Per $k > 1$ fem servir la identitat $[\pi^k](X) = [\pi]([\pi^{k-1}](X))$. □

Teorema 5.11. *Per tot irreductible $\pi \in A$, $[\pi](f) \equiv f \mod \pi$ per tot $f \in A$.*

Demostració. Pel Teorema (5.8) $\overline{[\pi]}(X) = X^{q^{\deg \pi}}$ en $(A/\pi)(X)$. Per tant $[\pi](f) \equiv f^{q^{\deg \pi}} \mod \pi$ per tot $f \in A$. Com A/π és un cos de $q^{\deg \pi}$ elements per tant s'obté $[\pi](f) \equiv f \mod \pi$. □

Corol·lari 5.12. *Per tot mònic irreductible $\pi \in \mathbb{F}_q[T]$, $[\pi - 1](f) \equiv 0 \mod \pi$ per tot $f \in \mathbb{F}_q[T]$.*

Teorema 5.13. *Per mònic irreductible $\pi \in \mathbb{F}_q[T]$ i $f(X) \in \mathbb{F}_q[T][X]$, $f([\pi](X)) \equiv f(X)^{q^{\deg \pi}} \mod \pi$.*

Demostració. En $(\mathbb{F}_q[T]/\pi)[X]$, $\overline{[\pi]}(X) = X^{q^{\deg \pi}}$ pel teorema (5.8). Per tant $f([\pi](X)) \equiv f(X^{q^{\deg \pi}}) \mod \pi$. Com en $\mathbb{F}_q/\pi$ tot element és la seva potència $q^{\deg \pi}$, per tant $f(X)^{q^{\deg \pi}} \equiv f(X^{q^{\deg \pi}}) \mod \pi$. □

5.2 Mòdul de Carlitz

Com s'ha comentat abans, hi ha dues maneres, com a mínim, per convertir $\overline{\mathbb{F}_q(T)}$ (la clausura separable de $\mathbb{F}_q(T)$) en un $\mathbb{F}_q[T]$-mòdul. Per distingir els possibles cassos, denotarem per $C(\overline{\mathbb{F}_q(T)})$ el mòdul de Carlitz actuant sobre $\overline{\mathbb{F}_q(T)}$, és a dir $f \cdot \alpha = [f](\alpha)$ amb $f \in \mathbb{F}_q[T]$ i $\alpha \in \overline{F_q(T)}$.

Definició 5.14. *Donat $M \in \mathbb{F}_q[T]$ definim els punts de torsió del polinomi $M(T)$ al conjunt $\Lambda_M = \{\lambda \in \overline{\mathbb{F}_q(T)} : [M](\lambda) = 0\}$. La torsió de Carlitz és: $\Lambda = \bigcup_{M \in \mathbb{F}_q[T]} \Lambda_M$*

Els punts de torsió Λ_M són un anàleg en característica positiva de les arrels de la unitat $\mu_m = \{\alpha \in \overline{\mathbb{Q}} : \alpha^m - 1 = 0\}$.

Exemple 5.15. *Considerem l'irreductible $T \in \mathbb{F}_q[T]$, llavors*

$$[T](X) = X^q + TX = X(X^{q-1} + T)$$

així $\Lambda_T = \{0\} \cup \{\lambda \in \overline{\mathbb{F}_q(T)} : \lambda^{q-1} = -T\}$. Similarment, en característica zero $x^p - 1 = (x-1)\Phi_p(x)$ per tant $\mu_p = \{1\} \cup \{\alpha \in \mathbb{C} : \Phi_p(a) = 1\}$.

A més a més, totes les arrels de l'irreductible $X^{q-1} + T$ són $\{c\lambda : c \in \mathbb{F}_q^\times\}$. Per tant $\mathbb{F}_q(T, \Lambda_T) = \mathbb{F}_q(T, \lambda)$. L'extensió $\mathbb{F}_q(T, \lambda)/\mathbb{F}_q(T)$ és cíclica de grau $q-1$, els elements del grup de Galois són les aplicacions $\sigma_c : \lambda \mapsto c\lambda$ per $c \in \mathbb{F}_q^\times$.

Aquest últim càlcul és anàleg a l'extensió p-ciclotòmica $\mathbb{Q}(\xi_p)/\mathbb{Q}$, on ξ_p és una arrel primitiva p-èssima de la unitat.

Exemple 5.16. *Calculem els punts de torsió de T^2*

$$[T^2](X) = (X^q + TX)^q + T(X^q + TX) = X\big(X^{q-1} + T\big)\big((X^q + TX\big)^{q-1} + T\big)$$

Llavors $\Lambda_{T^2} = \Lambda_T \cup \{\lambda \in \overline{\mathbb{F}_q(t)} : (\lambda^q + T\lambda)^{q-1} = -T\}$. Aquesta part es l'anàleg de $\mu_{p^2} = \mu_p \cup \{\alpha \in \mathbb{C} : \Phi_p(\alpha^p) = 1\}$. Així, si $\alpha \in \Lambda_T$ i $\beta \in \Lambda_{T^2} \setminus \Lambda_T$ llavors Λ_{T^2} està generat per α, β com $\mathbb{F}_q$-espai vectorial. Així $\mathbb{F}_q(T, \Lambda_{T^2}) = \mathbb{F}_q(T, \alpha, \beta)$.

Pel lema (5.5) sabem que $[M](X)$ és separable, per tant $|\Lambda_M| = q^{\deg M}$. Al ser $[M](X)$ un polinomi $\mathbb{F}_q$-lineal el conjunt Λ_M és un $\mathbb{F}_q$-espai vectorial, de fet és més que això:

Teorema 5.17. *El conjunt Λ_M és un submòdul de $C(\overline{\mathbb{F}_q(T)})$. És a dir, si $\lambda \in \Lambda_M$ i $f \in \mathbb{F}_q[T]$ llavors $[f](\lambda) \in \Lambda_M$.*

Demostració. Es segueix de la proposició (5.3) i el corol·lari (11.6). □

L'anterior teorema és un anàleg que μ_m no és només un grup amb la multiplicació, sino també un $\mathbb{Z}$-submòdul de $\mathbb{C}$: si $\xi \in \mu_m$ llavors $[n](\xi) = \xi^n \in \mu_m$ donat que $\xi^m = 1$ per tant $(\xi^n)^m = (\xi^m)^n = 1$. A més, tots els submòdul de μ_m són μ_k on k és un divisor de m.

Teorema 5.18. *Siguin $M, N \in \mathbb{F}_q[T]$ coprimers, llavors $\Lambda_{MN} \cong \Lambda_M \oplus \Lambda_N$ com $\mathbb{F}_q[T]$-mòduls.*

Demostració. Considerem l'aplicació $\Lambda_M \oplus \Lambda_N \to \Lambda_{MN}$ donat per $(\lambda, \lambda') \mapsto \lambda + \lambda'$, aquesta suma té sentit donat que $\lambda, \lambda' \in \Lambda_{MN}$, i clarament l'aplicació és un morfisme. Ara bé, $|\Lambda_{MN}| = q^{\deg MN}$ i $|\Lambda_M \oplus \Lambda_N| = q^{\deg N} \cdot q^{\deg M}$ tenen el mateix nombre d'elements. Per tal de demostar que és un isomorfisme, serà suficient comprovar la injectivitat. Si $\lambda + \lambda' = 0$ llavors $\lambda = -\lambda'$ estan en la interseció $\Lambda_M \cap \Lambda_N = \{0\}$, però aquesta és nul·la al ser M, N coprimers pel lema (5.7) i per tant $(\lambda, \lambda') = (0, 0)$. □

Definició 5.19. *Donat $\lambda \in \Lambda$ definim l'annihilador de λ*

$$Ann_\Lambda(\lambda) = \{f \in \mathbb{F}_q[T] : [f](\lambda) = 0\}$$

Al ser un ideal de $\mathbb{F}_q[T]$ es segueix que és un ideal principal, a l'únic generador mónic $f \in \mathbb{F}_q[T]$ de $Ann_\Lambda(\lambda)$ l'anomenem l'ordre-$\mathbb{F}_q[T]$ de λ.

Teorema 5.20. *Siguin $C, D \in \mathbb{F}_q[T]$ i $\lambda \in \Lambda_M$, si $C \equiv D \bmod M$ llavors $[C](\lambda) = [D](\lambda)$. Per tant l'acció de Carlitz en Λ_M el converteix també en un $(\mathbb{F}_q[T]/M)$-mòdul. Recíprocament, si $[C](\lambda) = [D](\lambda)$ per tot $\lambda \in \Lambda_M$ llavors $C \equiv D \bmod M$. A més, existeix un generador $\lambda_0 \in \Lambda_M$ com $\mathbb{F}_q[T]$-mòdul, és a dir*

$$\Lambda_M = \{[P](\lambda_0) : P \in \mathbb{F}_q[T]\}$$

i els generadors de Λ_M són aquells tal que $\gcd(P, M) = 1$

Demostració. Si $C \equiv D \bmod M$ podem escriure $C = D + MN$,

$$[C](\lambda) = [D + MN](\lambda) = [D](\lambda) + [N]([M](\lambda)) = [D](\lambda) + [N](0) = [D](\lambda).$$

Per demostrar $[C](\lambda) = [D](\lambda)$ per tot $\lambda \in \Lambda_M$ llavors $C \equiv D \bmod M$ serà suficient veure que si $[C](\lambda) = 0$ per tot $\lambda \in \Lambda_M$ llavors $M|C$. Escrivim $C = MN + R$ on $R = 0$ o bé $\deg R < \deg M$. Llavors per tot $\lambda \in \Lambda_M$

$$0 = [C](\lambda) = [N]([M](\lambda)) + [R](\lambda) = [N](0) + [R](\lambda) = [R](\lambda)$$

Si $R \neq 0$ llavors $M|R$ però per construcció $\deg R < \deg M$ llavors R té més arrels que el seu grau.

Per demostrar que Λ_M té un generador com a $\mathbb{F}_q[T]$-mòdul. Considerem l'annihilador $\mathrm{Ann}_\Lambda(\lambda)$, per $\lambda \in \Lambda$.

Sigui N_1 i N_2 són dos polinomis que són $\mathbb{F}_q[T]$-ordres llavors hi ha un element de Λ que el seu ordre és $\mathrm{mcm}(N_1, N_2)$. Això significa que si N és el $\mathbb{F}_q[T]$-ordre més gran de Λ_M, llavors aquest és un múltiple de qualsevol $\mathbb{F}_q[T]$-ordre de Λ_M. Conseqüenment $[N](\lambda) = 0$ per tot $\lambda \in \Lambda_M$, per tant $|\Lambda_M| \leq \deg([N](X)) \leq q^{\deg N}$. D'altra banda, $N|M$, per tant M s'obté al multiplicar N per una constant. Considerem λ_0 amb l'ordre $\mathbb{F}_q[T]$ maximal N, $\mathrm{Ann}_\Lambda(\lambda_0) = (N) = (M)$, llavors el $\mathbb{F}_q[T]$-submòdul que genera λ_0 té mida:

$$|\{[C](\lambda_0) : C \in \mathbb{F}_q[T]\}| = |\mathbb{F}_q[T]/M| = q^{\deg M} = |\Lambda_M|$$

per tant λ_0 és un generador de Λ_M com $\mathbb{F}_q[T]$-mòdul, i a més hi ha un $\mathbb{F}_q[T]$-submòdul isomorfisme $\mathbb{F}_q[T]/M \cong \Lambda_M$ donat per $P \bmod M \mapsto [P](\lambda_0)$. En particular, $[P](\lambda_0)$ genera Λ_M si i només si $P \bmod M$ genera $\mathbb{F}_q[T]/M$ com $\mathbb{F}_q[T]$-mòdul amb estructura usual de multiplicació, i això passa quan $\mathrm{mcd}(P, M) = 1$. per □

Per veure l'anologia amb car=0, escollint un generador ξ_m de μ_m tenim un isomorfisme de grups no canònic $\mathbb{Z}/(m) \cong \mu_m$ via $a \bmod m \to \xi_m^a$, i de la mateixa manera escollint un generador λ de Λ_M proporciona un morfisme no canònic de $\mathbb{F}_q[T]$-mòduls via $P \bmod M \to [P](\lambda_0)$, on $\mathbb{F}_q[T]/M$ és un $\mathbb{F}_q[T]$-mòdul amb la multiplicació estàndar i Λ_M un $\mathbb{F}_q[T]$-mòdul via el mòdul de Carlitz.

Corol·lari 5.21. *Els $(\mathbb{F}_q[T])$-submòduls de Λ_M són tots isomorfs a Λ_D on $D|M$.*

Demostració. Fixem un generador λ_0 de Λ_M. Llavors $\mathbb{F}_q[T]/M \cong \Lambda_M$ com $\mathbb{F}_q[T]$-mòduls per l'aplicació $P \bmod M \mapsto [P](\lambda_0)$. El resultat és una conseqüència de que els submòduls de $\mathbb{F}_q[T]/M$ són de la manera $d\mathbb{F}_q[T]/M$ amb $D|M$ i que el submòdul $D\mathbb{F}_q[T]/M$ es correspon a un $\mathbb{F}_q[T]$-isomorfisme amb $\Lambda_{M/D}$ de l'algorisme de Bezout en $\mathbb{F}_q[T]$. □

5.3 L'estructura de $\mathbb{F}_q[T]/M$ i l'acció de Carlitz

En l'apartat anterior hem vist que un anàleg del grup cíclic $\mathbb{Z}/(m)$ és Λ_M com un $\mathbb{F}_q[T]$-mòdul (donat per l'acció de Carlitz); a més Λ_M és isomorf (no canònicament) a $\mathbb{F}_q[T]/M$. L'anàleg del grup multiplicatiu $(\mathbb{Z}/(m))^\times$ és el grup additiu $\mathbb{F}_q[T]/M$, però amb l'estructura de $\mathbb{F}_q[T]$-mòdul, és a dir

$$N \cdot (C \mod M) = [N](C) \mod M \text{ amb } C, N \in \mathbb{F}_q[T].$$

Denotarem per $C(\mathbb{F}_q[T]/M)$ a $\mathbb{F}_q[T]/M$ com a $\mathbb{F}_q[T]$-mòdul donat per l'acció de Carlitz.

Exemple 5.22. *El $\mathbb{F}_3[T]$-mòdul $C(\mathbb{F}_3[T]/(T^2+1))$ està generat per $\lambda_0 = 1$.*

El grup additiu $\mathbb{F}_3[T]/(T^2+1)$ té $3^{\deg T^2+1} = 3^2 = 9$ elements, en concret

$$\mathbb{F}_3/(T^2+1) = \{Ti + j : 0 \leq i, j \leq 2\}.$$

Per veure que $\lambda_0 = 1$ és generador computem $[Ti+j](X) = (X^q + TX)i + j$, per tant $[Ti+j](1) = Ti + (i+j)$. La taula següent resumeix els càlculs anteriors:

$A \in \mathbb{F}_3/(T^2+1)$	0	1	2	T	$T+1$	$T+2$	$2T$	$2T+1$	$2T+2$
$[A](1) \mod T^2+1$	0	1	2	$T+1$	$T+2$	T	$2T+2$	$2T$	$2T+1$

Teorema 5.23. *Per un irreductible $\pi \in \mathbb{F}_q[T]$, el $\mathbb{F}_q[T]$-mòdul $C(\mathbb{F}_q[T]/\pi)$ és cíclic i isomorf a $\mathbb{F}_q[T]/(\pi - 1)$.*

Demostració. El conjunt $C(\mathbb{F}_q[T]/\pi)$ és un $\mathbb{F}_q[T]/(\pi-1)$-mòdul donat que $[\pi-1](a) \equiv 0 \mod \pi$ per tot $a \in \mathbb{F}_q[T]$, corol·lari (5.12). Busquem $a_0 \mod \pi \in C(\mathbb{F}_q[T]/M)$ amb l'anihilador $(\pi-1)$, per tal que $\mathbb{F}_q[T]/(\pi-1) \cong C(\mathbb{F}_q[T]/\pi)$ com $\mathbb{F}_q[T]$-mòduls per $m \mod \pi - 1 \mapsto [m](a_0) \mod \pi$.

Descomposem $\pi - 1 = \pi_1^{2_1} ... \pi_k^{e_k}$ en $\mathbb{F}_q[T]$ amb π_i diferents irreductibles mònics i $e_i \geq 1$. Per $i = 1, ..., k$ trobarem un $a_i \mod \pi \in C(\mathbb{F}_q[T]/\pi)$ amb anihilador $(\pi_i^{e_i})$. Llavors la suma $a_1 + a_2 + \ldots + a_k \mod \pi$ té anihilador $\pi - 1$.

Com $\pi_i^{e_i} | (\pi - 1)$ llavors $[\pi_i^{e_i}](X) | [\pi - 1](X)$. El polinomi $[\pi-1](X)$ té grau, com polinomi en X, $q^{\deg(\pi-1)} = q^{\deg \pi} = |\mathbb{F}_q(T)/\pi|$ i a més anula tot element de $\mathbb{F}_q[T]/\pi$, per tant $[\pi-1](X)$ descomposa completament amb diferents arrels en $\mathbb{F}_q[T]/\pi$. Per tant $[\pi_i^{e_i}](X)$ també descomposa totalment sobre $\mathbb{F}_q[T]/\pi$ amb diferents factors de grau 1. Donat que $[\pi_i^{e_i}](X)$ té una arrel en $\mathbb{F}_q[T]/\pi$ que no és arrel de $[\pi_i^{e_i - 1}](X)$, llavors totes aquestes arrels tenen anihilador $(\pi_i^{e_i})$ en $\mathbb{F}_q[T]/\pi$. Sumant cada una d'aquestes arrels per i ens dona un generador de $C(\mathbb{F}_q[T]/\pi)$.

□

Per veure encara més la similitud entre $\mathbb{Z}/(m)^\times$ i $C(\mathbb{F}_q[T]/M)$ tenim aquests resultats, en [8, Structure of $\mathbb{F}_p/M$ with Carlitz Action] podeu trobar-ne una demostració.

Lema 5.24. *Sigui $k \geq 2$.*

1. $(\mathbb{Z}/(2^k))^\times = \langle -1 \mod 2^k \rangle \times \langle 5 \mod 2^k \rangle \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2^{k-2})$, *que no és cíclic.*
2. *Per primer senar p és cíclic i, $(\mathbb{Z}/(p^k))^\times = C_{p-1} \times \langle 1 + p \mod p^k \rangle \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/(p^{k-1})$, on C_{p-1} és el grup cíclic d'ordre $p-1$.*

Teorema 5.25. *Sigui π un irreductible mònic en $\mathbb{F}_q[T]$ i $k \geq 2$-*

1. *Per $\pi = T$ or $T+1$ en $\mathbb{F}_2[T]$, $C(\mathbb{F}_2[T]/\pi^k) = C_1 \times C_2$ on $C_1 \cong \mathbb{F}_2[T]/(T^2+T)$ està generat per 1 i $C_2 \cong \mathbb{F}_2[T]/(\pi^{k-2})$ està generat per π^2.*
2. *Si $(p, \deg \pi) \neq (2, 1)$ llavors $C(\mathbb{F}_p/\pi^k) = C_1 \times C_2$, on $C_1 \cong \mathbb{F}_p[T]/(\pi - 1)$ i C està generat per $\pi \mod \pi^k$.*

Si parlem del grup multiplicatiu $(\mathbb{Z}/(m))^\times$ llavors és natual pensar en la φ d'Euler, que recordem, $\varphi(m) = |(\mathbb{Z}/(m))^\times|$. A més, aquesta es pot expressar com

$$\varphi(m) = m\prod_{p|m}\left(1-\frac{1}{p}\right) = \sum_{d|m} m\frac{\mu(d)}{d},$$

on μ és la funció de Möbius.

Definició 5.26. *Per mònic $M \in \mathbb{F}_q[T]$, definim $\varphi_C(M) \in \mathbb{F}_q[T]$ com el polinomi:*

$$\varphi_C(M) = M\prod_{\pi|M}\left(1-\frac{1}{\pi}\right) = \sum_{D|M} M\frac{\mu(D)}{D},$$

on $\mu(D) \in \{0,1,-1\}$ està definit de la mateixa manera com en els enters: $\mu(D)$ és $(-1)^r$ si D és lliure de quadrats amb r factors irreductibles mònics, i $\mu(D)$ és 0 en cas contrari.

Exemple 5.27. *Si $\pi \in \mathbb{F}_q[T]$ és mònic irreductible llavors*

$$\varphi_C(\pi^k) = \pi^k(1-\frac{1}{\pi}) = \pi^k - \pi^{k-1}.$$

Teorema 5.28. *la funció φ_C té les següents propietats:*

1. *per mónic coprimers B i C, $\varphi_C(BC) = \varphi_C(B)\varphi_C(C)$.*
2. *per mónic M, $\sum_{D|M}\varphi_C(D) = M$, on D recorrer tots els factor mònics de M.*
3. *Per mònic M i per tot B en $\mathbb{F}_q[T]$, $[\varphi_C(M)](B) \cong 0 \mod M$.*
4. *Per mònic M i mònic B en $\mathbb{F}_q[T]$, $[M](B)$ és mònic i $M|\varphi_C([M](B))$ quan $q \neq 2$ i també quan $q = 2$ i $\deg B \geq 2$.*

Totes aquestes propietats de $\varphi_C(M)$ són anlogies de les propietats de $\varphi(m)$:

1. Per enters coprimers positius a i b $\varphi(ab) = \varphi(a)\varphi(b)$,
2. per $m \geq 1$, $\sum_{d|m}\varphi(d) = m$, on d recorre els factors positius de m,
3. per $a \mod m \in (\mathbb{Z}/m)^\times$, $a^{\varphi(m)} \cong 1 \mod m$,
4. per $k \geq 1$ i $a > 1$, $k|\varphi(a^k-1)$. Per tant l'ordre de $a \mod a^k-1$ és k.

5.4 El Group de Galois

En aquesta secció denotarem per $F = \mathbb{F}_q(T)$, llavors $\mathbb{F}_q(T,\Lambda_M) = F(\Lambda_M)$. Els cossos $F(\Lambda_M)$ són anomenats 'cossos ciclotòmics' degut que comparteixen moltes propietats similars amb les extensions $\mathbb{Q}(\mu_m)/\mathbb{Q}$, conegudes com extensions ciclotòmiques.

Com $[M](X)$ és separable en $F[X]$ llavors adjuntant totes les arrels Λ_M obtenim una extensió de Galois. De fet, només necessitem adjuntar un generador λ_0 de Λ_M a F degut que tots els altres elements de Λ_M són polinomis en λ_0 amb coeficients en $\mathbb{F}_q[T]$. Els elements de $\mathrm{Gal}(F(\Lambda_m)/F)$ permuten les arrels de $[M](X)$ és a dir a Λ_M i estan determinats com un automorfisme de cossos per la seva acció en les arrels. Tenint en compte que els elements de $\mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q})$ estan determinats per l'únic exponent en $(\mathbb{Z}/(m))^\times$ on actuen en totes les m-èssimes arrels de la unitat. Veurem que cada element de $\mathrm{Gal}(F(\Lambda_M)/F)$ actua sobre Λ_M via un polinomi de Carlitz.

Més concretament, escollim λ_0 un generador de Λ_M i donat $\sigma \in \mathrm{Gal}(F(\Lambda_M)/F)$,

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

per tant $\sigma(\lambda_0)$ també és un generador de Λ_M. Podem escriure $\sigma(\lambda_0) = [B_\sigma](\lambda_0)$ per un cert $B_\sigma \in \mathbb{F}_q[T]$, ben definit mòdul M amb $\mathrm{mcd}(B_\sigma, M) = 1$. Tot $\lambda \in \Lambda_M$ té la forma $[N](\lambda_0)$ per algun $N \in \mathbb{F}_q[T]$, per tant

$$\sigma(\lambda) = \sigma([N](\lambda_0)) = [N](\sigma(\lambda_0)) = [N]([B_\sigma](\lambda_0)) = [B_\sigma]([N](\lambda_0)) = [B_\sigma](\lambda).$$

Per tant σ té el mateix efecte per l'acció de Carlitz en tots els elements de Λ_M.

Teorema 5.29. *L'aplicació $\sigma \to B_\sigma$ és un morfisme de groups injectiu $Gal(F(\Lambda_M)/F) \hookrightarrow (\mathbb{F}_q[T]/M)^\times$.*

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

$$(\sigma\tau)(\lambda) = \sigma(\tau(\lambda)) = \sigma([B_\tau](\lambda)) = [B_\tau](\sigma(\lambda)) = [B_\tau]([B_\sigma](\lambda)) = [B_\tau B_\sigma](\lambda).$$

També $(\sigma\tau)(\lambda) = [B_{\sigma\tau}](\lambda)$ per tant $B_{\sigma\tau}$ i $B_\sigma B_\tau = B_\tau B_\sigma$ tenen la mateixa acció en Λ_M per tant $B_{\sigma\tau} = B_\sigma B_\tau \mod M$ pel teorema (5.20) El que mostra que tenim un morfisme de $\mathrm{Gal}(F(\Lambda_M)/F)$ a $(\mathbb{F}_q(T)/M)^\times$.

Quan σ pertany al nucli, $B_\sigma \equiv 1 \mod M$, per tant per tot $\lambda \in \Lambda_M$ tenim $\sigma(\lambda) = [B_\sigma](\lambda) = [1](\lambda) = \lambda$. Per tant σ és la identitat en Λ_M, i per tant σ és la identitat en $\mathrm{Gal}(F(\Lambda_M)/F)$.

□

Com $(\mathbb{F}_q[T]/M)^\times$ és abelià, $\mathrm{Gal}(F(\Lambda_M)/F)$ és abelià, per tant l'extensió de Carlitz de $F = \mathbb{F}_q(T)$ són extensions abelianes.

Teorema 5.30. *L'aplicació $Gal(F(\Lambda_M)/F) \hookrightarrow (\mathbb{F}_q[T]/M)^\times$ és un isomorfisme.*

Demostració. Tant Λ_M com $(\mathbb{F}_q[T]/M)^\times$ no es veuen afectats quan escalem M per un element de $\mathbb{F}_q^\times$, suposarem que M és mònic.

Escollim un generador λ_0 de Λ_M. La imatge de $\mathrm{Gal}(F(\Lambda_M)/F) \hookrightarrow (\mathbb{F}_q(T)/M)^\times$ és tot $B \mod M$ tal que $[B](\lambda_0)$ és una F-conjugació de λ_0 via $\mathrm{Gal}(F(\Lambda_M)/F)$. Per tant l'aplicació $\mathrm{Gal}(F(\Lambda_M)/F) \to (\mathbb{F}_q(T)/M)^\times$ és exhaustiva quan $[B](\lambda_0)$ és una F-conjugació de λ_0 per tot B coprimer amb M. Denotem per $f(X) \in F[X]$ a $\mathrm{Irr}(\lambda_0, F)[x]$ de λ_0. Els F-conjugats de λ_0 són les arrels de $f(X)$, així volem demostrar

$$\mathrm{mcd}(B, M) = 1 \Rightarrow f([B](\lambda_0)) = 0.$$

Com $[B](\lambda_0)$ només depèn de $B \mod m$, podem escollir B mònic i per tant B és producte de mònics irreductibles, cada un d'ells no divisors de M. Donat que $B \to [B](X)$ converteix multiplicacions en composicions, és suficient demostrar $f([\pi](\lambda_0)) = 0$ per tot irreductible mònic $\pi \in \mathbb{F}_q[T]$ no dividint M.

Sigui $\pi \in \mathbb{F}_q[T]$ un mònic irreductible que no divideix M, i $g(X)$ el polinomi mònic minimal de $[\pi](\lambda_0)$ en $F[X]$. Volem demostrar $g(X) = f(X)$. Com λ_0 i $[\pi](\lambda_0)$ estan en Λ_M, els dos $f(X)$ i $g(X)$ divideixen $[M](X)$ en $F[X] = \mathbb{F}_q(T)[X]$. Com M és mònic en $\mathbb{F}_q(T)$, $[M](X)$ és mònic en X i tot factor mònic de $[M](X)$ en $F[X]$ està en $\mathbb{F}_q[T][X]$. (Aquest resultat és anàleg a una conseqüència del Lemma de Gauss, tots els factor mònics en $\mathbb{Q}[X]$ d'un mònic en $\mathbb{Z}[X]$ han d'estar en $\mathbb{Z}[X]$). Per tant $f(X), g(X) \in \mathbb{F}_q[T][X]$.

Com $g([\pi](X)) = 0$, $g([\pi](X))$ té λ_0 com a arrel, per tant $f(X) | g([\pi](X))$ en $F[X]$. Els dos $f(X), g([\pi](X))$ són mònics en la variable X en $\mathbb{F}_q[T][X]$. Per tant la divisó en $F[X]$ de fet passa en $\mathbb{F}_q[T][X]$. És a dir, $g([\pi](X)) = f(X)h(X)$ per algun $h(X) \in \mathbb{F}_q[T][X]$. Ara reduïm mòdul π i usem el Teorema (5.13) per obtenir

$$\overline{g}(X)^{q^{\deg \pi}} = \overline{f}(X)\overline{h}(X)$$

.

Llavors $\overline{f}(X)$ i $\overline{g}(X)$ tenen un factor en comú en $(\mathbb{F}_q[T]/\pi)[\mathrm{X}]$, diguem, un factor irreductible de $\overline{f}(X)$.

Raonem per reducció a l'absurd, i suposem $f(X) \neq g(X)$. Són per tant diferents factors mònics irreductibles de $[M](X)$, per tant $[M](X) = f(X)g(X)k(X)$ per $k(X) \in \mathbb{F}_q(T)[X]$. Reduint de nou a mòdul π,

$$\overline{[M]}(X) = \overline{f}(X)\overline{g}(X)\overline{k}(X)$$

en $(\mathbb{F}_q[T]/\pi)[X]$. Això és impossible: la part dretana té múltiples factors en irreductibles, mentres que l'altre part és separable en $(\mathbb{F}_q[T]/\pi)[X]$ pel Teorema (5.8) □

5.5 Extensions ciclotòmiques

Denotem per $\mathcal{O}_M$ la clausura entera de $A = \mathbb{F}_q[T]$ en $\mathbb{F}_q(T)(\Lambda_M)$, amb $M \in A$.

Proposició 5.31. *Sigui $\lambda_1, \lambda_2 \in \Lambda_m$ dos generadors. Llavors $\lambda_1/\lambda_2 \in \mathcal{O}_m$ i és una unitat.*

Demostració. Com λ_1, λ_2 són generadors, llavors hi ha $B \in (\mathbb{F}_q[T]/m)^\times$ tal que $[B](\lambda_1) = \lambda_2$ o sigui, si $d = \deg B$ llavors

$$[B](\lambda_1) = a_d(\lambda_1)^{q^d} + \ldots + a_1(\lambda_1)^q + a_0\lambda_1 = \lambda_2$$

llavors dividint per λ_1, obtenim

$$a_d(\lambda_1)^{q^d-1} + \ldots + a_1(\lambda_1)^{q-1} + a_0 = \frac{\lambda_2}{\lambda_1}$$

i per tant $\lambda_2/\lambda_1 \in \mathcal{O}_M$, fent el matex raonament però cambiant el paper de λ_1 pel de λ_2 s'onbté $\lambda_1/\lambda_2 \in \mathcal{O}_M$. □

Proposició 5.32. *Sigui $P \in A$ un primer i $e \geq 1$. Considerem $M = P^e$ llavors $K = F(\Lambda_{P^e})/F$ on $F = \mathbb{F}_q(T)$, no ramifica en cap ideal QA amb $PA \neq QA$. El primer PA ramifica completament amb índex de ramificació igual a $[K : F]$.*

A més, l'únic ideal sobre PA és $(\lambda) = \lambda\mathcal{O}p^e$, on λ és un generador.

Per una demostració completa veure [1, pàg. 204].

Demostració. (*de la proposició 5.32*)

Farem el cas $e = 1$. Recordem que $[P](X)/X$ és un polinomi Eisenstein en P, llavors el producte de les seves arrels és P. Per tant,

$$P \cdot \mathcal{O}_P = \prod_{\xi_i \in \Lambda_p, \xi_i \neq 0} (\xi_i)$$

Recordem que tot $\xi_i \neq 0$ és una arrel primitiva en Λ_P. Fixem un generador λ; per la proposició (5.31) ξ_i/λ és una unitat per tant $\xi_i = \frac{\xi_i}{\lambda}\lambda$ d'on s'obté

$$P \cdot \mathcal{O}_P = (\lambda)^{q^{\deg P}-1}$$

□

Proposició 5.33. *Sigui $\mathcal{O}_M$ la clausura entera de $\mathbb{F}_q[T]$ en $F(\lambda)$, amb λ un generador de Λ_M. Llavors $\mathcal{O}_M = A[\lambda]$.*

Per una demostració veure [1, pàg. 207-208].

Tots aquest resultats són anàlegs de les extensions ciclotòmiques, però ara en característica positiva. Acabem aquest apartat amb una última analogia.

Sigui $m \in \mathbb{Z}$ i considerem l'extensió ciclotòmica $\mathbb{Q}(\mu_m)$, amb ξ_m una arrel m-èssima primitiva de la unitat. Denotem $K_m = \mathbb{Q}(\mu_m)$, totes les seves inmersions en $\mathbb{C}$ són complexes donat que $\mathbb{R}$ només té dos arrels de la unitat ± 1. Considerem $K_m^+ = \mathbb{Q}(\xi_m + \xi_m^{-1})$, aquest cos és real i totes les seves inmersions en $\mathbb{C}$ són reals. A més K_m/K_m^+ té grau 2, ja que ξ_m satisfà l'equació quadràtica $x^2 - x(\xi_m + \xi_m^{-1}) + 1 = 0$. Es conclou que el primer a l'infinit en $\mathbb{Q}$ (que correspon al valor absolut arquimidià usual), descomposa en $\varphi(m)/2$ valors absoluts arquimedians en K_m^+ donat per les diferents inmersions, i cada un d'aquests ramifica a un valor absolut en K_m. A més, el grup de Galois de K_m/K_m^+ està generat per la conjugació complexa.

Es té el següent resultat en característica positiva. Sigui $M \in A$, denotem per $K_M = F(\Lambda_M)$. Com $\mathrm{Gal}(K_M/F) \cong (A/M)^\times$ llavors $\mathbb{F}_q \hookrightarrow \mathrm{Gal}(K_M/F)$. Clarament, si $\lambda \in \Lambda_M$ és un generador, llavors $c\lambda$ és de nou un generador, amb $c \in \mathbb{F}_q^\times$.

Denotem el subgrup $J = \{\sigma_c : c \in \mathbb{F}_q^\times\} \subset \mathrm{Gal}(K_m/F)$. Denotem per $K_M^+ \subset K_M$ el cos fixat per J. Per construcció $[K_M : K_M^+] = q - 1$, a més es té el següent resultat.

Teorema 5.34. *El primer a l'infinit en F descomposa completament en K_M^+. I cada ideal primer sobre ∞ en K_M^+ està completament i moderadament ramificat en K_M. A més, $K_M = K_M^+(\lambda^{q-1})$ amb λ un generador de Λ_M.*

Corol·lari 5.35. *Per tot $M \in A$ no nul el cos de les constants de K_M és $\mathbb{F}_q$. És a dir la extensió K_M/F és geomètrica.*

Proposició 5.36. *Denotem per $\mathcal{O}_M^+$ la clausura entera de $\mathbb{F}_q[T]$ en K_M^+. Denotem $Q_0 = [\mathcal{O}_m^\times : \mathcal{O}_m^{+\times}]$. Llavors $Q_0 = 1$ si m és una potència d'un primer, i $Q_0 = q - 1$ si m no és una potència d'un primer.*

Per una demostració mireu [1, pàg. 217].

5.6 Coeficients del mòdul de Carlitz

5.6.1 Valoracions

Sigui R un anell commutatiu amb unitat $1 \neq 0$. Una valoració discreta és una funció $v : R \to \mathbb{N} \cup \{\infty\}$ que compleix:

1. $v(a) = \infty$ si i només si $a = 0$.
2. $v(ab) = v(a) + v(b), \forall a, b \in R$.
3. $v(a + b) \geq \min\{v(a), v(b)\}, \forall a, b \in R$

Exemple 5.37. *Considerem l'anell dels enters $\mathbb{Z}$. Fixat un primer p definim l'aplicació $v_p(n) = k$ de manera que $n = p^k m$ amb $\gcd(p, m) = 1$.*

Aques exemple admet una generalització en qualsevol DFU.

Proposició 5.38. *Sigui R un anell DFU, fixem un element $p \in R$ primer. Donat $a \in R$ escrivim $a = p^e b$, tal que $p \nmid b$: definim $v_p(a) = e$. Es diu que v_p és la valoració en p.*

Corol·lari 5.39. *Sigui v una valoració discreta en un anell R, si $v(a) \neq v(b)$ llavors es compleix la igualtat $v(a + b) = \min\{v(a), v(b)\}$.*

Demostració. Sense pèrdua de generalitat suposem $v(a) < v(b)$. Per definició $v(a + b) \geq v(a)$, per veure l'altre igualtat considerem

$$v(a) = v((a + b) - b) \geq \min\{v(a + b), v(b)\} = v(a + b),$$

la última igualtat es degut que $v(a) < v(b)$.

□

Corol·lari 5.40. *Considerem $r \in R$ un anell i v una valoració discreta. Si $r = \sum_{i=0}^{n} s_i$ amb $s_i \in R$ i existeix i_0 tal que $v(s_{i_0}) < v(s_i)$ per tot $i \neq i_0$ llavors $v(r) = v(s_{i_0})$*

5.6.2 Coeficients del mòdul de Carlitz

Els següents dos lemes discutiexen com es poden trobar els coeficients del mòdul de Carlitz. Donat $f(T) \in A$ denotarem per $[f(T)](X)$ el mòdul de Carlitz, on $A = \mathbb{F}_q[T]$

Lema 5.41. *Sigui $f(T) \in A$, denotem per $[f](X) = \sum_{i=0}^{n} c_i X^{q^i}$ llavors per $i \geq 1$ es compleix:*

$$c_m = \frac{c_{m-1}^q - c_{m-1}}{T^{q^m} - T} \tag{5.42}$$

Demostració. Calculem de dues maneres diferents $[Tf(T)](X)$, així és $[T]([f](X)) = [f]([T](X))$

$$[T]([f](X)) = (\sum_{i=0}^{n} c_i X^{q^i})^q + T \sum_{i=0}^{n} c_i X^{q^i} = \sum_{i=0}^{n} c_i^q X^{q^{i+1}} + T \sum_{i=0}^{n} c_i X^{q^i}$$

$$[f]([T](X)) = \sum_{i=0}^{n} c_i (X^q + TX)^{q^i} = \sum_{i=0}^{n} c_i (X^{q^{i+1}} + T^{q^i} X^{q^i})$$

Comparant els coeficients corresponents a X^{q^m} en aquestes dues expression s'obté

$$c_{m-1}^q + T c_m = c_{m-1} + T^{q^m} c_m$$

D'on es segueix l'expressió (5.42) □

Observació 5.43. *Aquesta fórmula també demostra que cap coeficient c_i és nul.*

Proposició 5.44. *Sigui $s(T)$ un polinomi mònic irreductible de A i escrivim $[s^n](X) = \sum_{i=0}^{n \deg s} c_i X^{q^i}$. Sigui v_s la valoració en $s(T)$. Llavors la successió $v_s(c_0), ..., v_s(c_{n \deg s})$ és decreixent.*

Demostració. Sabem pel corol·lari (5.10) que $v_s(c_m) > 0$ per $m < n \deg s$ i $v_s(c_{n \deg s}) = 0$. Ara observem, que per la fòrmula (5.42),

$$c_m = \frac{c_{m-1}^q - c_{m-1}}{T^{q^m} - T} = \frac{c_{m-1}(c_{m-1}^{q-1} - 1)}{T^{q^m} - T}$$

com $s(T)|c_{m-1}$ a més $\gcd(c_{m-1}, c_{m-1}^{q-1} - 1) = 1$ i $s(T)$ irreductible llavors,

$$v_s(c_m) = v_s\Big(\frac{c_{m-1}^q - c_{m-1}}{T^{q^m} - T}\Big) \leq v_s(c_{m-1}(c_{m-1}^{q-1} - 1)) \leq v_s(c_{m-1})$$

El que demostra que la successió és decreixent.

□

Observació 5.45. *Com $T^{q^m} - T$ són polinomis separables sobre $\mathbb{F}_q$ llavors de la demostració de la proposició anterior $0 \leq v_s(c_{m-1}) - v_s(c_m) \leq 1$. Ja que $v_s(c_m) = v_s(c_{m-1}^q - c_{m-1}) - v_s(T^{q^m} - T) \geq v_s(c_{m-1}) - 1$.*

Corol·lari 5.46. *Sigui $s(T)$ un irreductible mónic $[s^n](X) = \sum_{i=0}^{\deg(s)n} c_i X^{q^i}$. Sigui v_s la valoració en $s(T)$, Llavors $v_s(c_{\deg(s)i+j}) = n - i$ per $0 \leq j < \deg(s)$*

Demostració. El cas $n = 1$ és immediat, donat que $c_0 = s(T)$ i $s(T)|v_i$ per $i < \deg s$ i $c_{\deg s} = 1$.

Pal cas general, denotem per $m = \deg([s^n](X))$, és ben conegut que $s(T)|T^{q^{\deg s}} - T$ i a més de $T^{q^{\deg(s)}} - T | T^{q^{i \deg s}} - T$ es conclou $s(T)|T^{q^{i \deg s}} - T$. Deduïm que $v_s(c_{i \deg s - 1}) - v_s(c_{i \deg s}) = 1$ i la successió $v_s(c_0), ..., v_s(c_{n \deg s})$ decau justament n cops. Com que $v(c_0) = n$ i $v(c_{n \deg s}) = 0$ i és una successió decreixent es segueix l'enunciat. □

6 Les equacions de Goss-Fermat

6.1 Una analogia amb l'equació de Fermat

Sigui $\pi(T) \in A = \mathbb{F}_q[T]$ definim $\Psi_\pi(X,Y)$ com l'homogenització de $[\pi](X)$ i l'objectiu serà la resolució de l'equació del tipus:

$$Z^{q^{\deg(\pi)}} = \Psi_\pi(X,Y) = \prod_{\xi_i \in \Lambda_\pi} (X - \xi_i Y) \tag{6.1}$$

Amb solucions en $X, Y, Z \in A$. Quan $\pi(T)$ és irreductible, usant el corol·lari (5.10) i reduint en mòdul $\pi(T)$

$$\begin{aligned} Z^{q^{\deg \pi}} &\equiv \Psi_\pi(X,Y) \mod \pi(T) \\ &\equiv X^{q^{\deg \pi}} \mod \pi(T) \end{aligned}$$

per tant $\pi(T)|(Z-X)$, fent un canvi de variable $U\pi = Z - X$ l'equació (6.1) es transforma en, per π potència d'un irreductible,

$$(\pi U)^{q^{\deg \pi}} = \Psi_\pi(X,Y) - X^{q^{\deg \pi}}, \tag{6.2}$$

si escrivim $Z = X + U\pi$.

Exemple 6.3. *Per construcció* $[T](X) = X^q + TX$ *llavors* $\Psi_T(X,Y) = X^q + TXY^{q-1}$ *i tenim l'equació*

$$Z^q = X^q + TXY^{q-1} \tag{6.4}$$

Fixem-nos que ens podem restringir només al cas mcd$(X,Y) = 1$. *A més usant (6.2) obtenim* $T^q U^q = TXY^{q-1}$ *per tant* $T^{q-1}U^q = XY^{q-1}$ *així trobem infinites solucions* $(U^q, T, U^q + TU) \in A^3$, *per qualsevol* $U \in A$.

6.2 Primeres consideracions

En aquest apartat usarem la teoria de les valoracions per a donar algún tipus d'informació sobre l'equació plantejada. Recordem que $A = \mathbb{F}_q[T]$ a més $\pi(T) \in A$ sempre denotarà un irreductible mònic en A i l'equació en consideració és $Z^{q^{\deg \pi}} = \Psi_\pi(X, Y)$, i.e.

$$Z^{q^{\deg \pi}} = X^{q^{\deg \pi}} + \sum_{i=1}^{\deg \pi - 1} c_i X^{q^i} Y^{q^{\deg \pi} - q^i} + S(T) X Y^{q^{\deg \pi} - 1} \tag{6.5}$$

Observació 6.6. *Com l'anterior equació està homogenitzada podem suposar sense pèrdua de generalitat que mcd$(X, Y) = 1$. Aquest fet implica que mcd$(Y, Z) = 1$, es segueix immediatament de (6.5).*

De (6.5) també es seguex que $X | Z^{q^{\deg S}}$.

Proposició 6.7. *Sigui $a \in A$ primer tal que $a|X$. Denotem per v_a la valoració en a, llavors:*

1. *si $a \neq \pi$ aleshores $v_a(X) = v_a(Z) q^{\deg S}$.*
2. *si $a = \pi$ aleshores $v_a(X) + 1 = v_a(Z) q^{\deg S}$.*

Demostració. Denotem $n = \deg S$

1. Calculem, $v_a(c_i X^{q^i} Y^{q^n - q^i}) \geq v_a(X) q^i$ però $v_a(\pi X Y^{n-1}) = v_a(X)$, ja que $a \neq \pi$ i hem suposat X, Y coprimers. Llavors, $v_a(c_i X^{q^i} Y^{q^n - q^i}) > v_a(\pi X Y^{q^n - 1})$ per $i > 0$; aplicant el coroal·lari (5.40) obtenim $v_a(X) = v_a(Z^{q^{\deg \pi}}) = v_a(Z) q^{\deg \pi}$
2. Ara, $v_\pi(X^{q^n}) = v_\pi(X) q^n$, per $i < n$ es té $v_\pi(c_i X^{q^i} Y^{q^n - q^i}) > v_\pi(X) q^i + 1$ com el mínim és $v_\pi(\pi X Y^{q^n - 1}) = v_\pi(X) + 1$ aplicant de nou el coroalari (5.40)‘ s'obté l'enunciat.

□

Proposició 6.8. *Sigui $\pi \in A$ un irreductible. Considerem l'equació de $Z^{q^{n \deg \pi}} = \Psi_{\pi^n}(X, Y)$. Si* $\gcd(X, Y) = 1$ *i es compleix $\pi | Y$ llavors* $\deg(\pi^n) = 1$.

Demostració. Podem reescriure l'equació $Z^{q^{n \deg \pi}} = \Psi_{\pi^n}(X, Y)$ com

$$(Z - X)^{q^{n \deg \pi}} = \pi Y^{q^{n \deg \pi} - q^{n \deg \pi - 1}} \cdot \sum_{i=0}^{n \deg \pi - 1} \frac{c_i}{\pi} X^{q^i} Y^{q^{n \deg \pi - 1} - q^i}, \tag{6.9}$$

pel corol·lari (5.10) $\pi | c_i$ per $i < q^{n \deg \pi}$, així que dividir per π té sentit. A més $\pi | Y$ llavors $\pi | Z - X$. En altres paraules, si v_π és la valoració en π llavors $v_\pi(Y) > 0$ i $v_\pi(Z - X) = k > 0$. Evaluant banda i banda de la igualtat (6.9) obtenim

$$\begin{aligned} k q^{n \deg \pi} &= v_\pi\Big(\pi(T) Y^{q^{n \deg \pi} - q^{n \deg \pi - 1}} \cdot \sum_{i=0}^{n \deg \pi - 1} \frac{c_i}{\pi(T)} X^{q^i} Y^{q^{n \deg \pi - 1} - q^i}\Big) \\ &= 1 + v_\pi(Y)(q^{n \deg \pi} - q^{n \deg \pi - 1}) + v_\pi\Big(\sum_{i=0}^{n \deg \pi - 1} \frac{c_i}{\pi(T)} X^{q^i} Y^{q^{n \deg \pi - 1} - q^i}\Big) \\ &= 1 + v_\pi(Y)(q^{n \deg \pi} - q^{n \deg \pi - 1}) \end{aligned}$$

La última igualtat és degut,

$$v_\pi\left(\frac{c_i}{\pi}X^{q^i}Y^{q^{n\deg\pi-1}-q^i}\right)=v_\pi\left(\frac{c_i}{\pi}\right)+v_\pi\left(Y^{q^{n\deg\pi-1}-q^i}\right)=v_\pi\left(\frac{c_i}{\pi}\right)+\left(q^{n\deg\pi-1}-q^i\right)v_\pi(Y)$$

per $i=n\deg\pi-1$ es compleix $v_\pi(c_i)=1$ per (5.46) i per tant l'anterior expressió val zero. En canvi, per $i<n\deg\pi-1$ clarament l'anterior expressió és positiva, així la valoració de la suma original és zero.

De la igualtat $kq^{n\deg\pi}=1+v_\pi(Y)(q^{n\deg\pi}-q^{n\deg\pi-1})$, deduim que si $\deg\pi^n>1$ llavors $q|1$ absurd. Resta només l'opció $\deg\pi^n=1$. □

Exemple 6.10. *Considerem el polinomi $\pi=T+a$ amb $a\in\mathbb{F}_q$. Llavors l'equació*

$$Z^q=X^q+(T+a)XY^{q-1}$$

té infinites solucions inspirades per l'exemple (6.3): $(U^q,T+a,U^q+(T+a)U)$.

Proposició 6.11. *Considerem T^n amb $n>1$, l'equacó $Z^{q^n}=\Psi_{T^n}(X,Y)$ si X,Y són coprimers llavors $T|X$ i en concret $v_T(X)=q^n-n$.*

Demostració. Escrivim l'equació $Z^{q^n}-X^{q^n}=\Psi_{T^n}(X,Y)$, renombrant $Z-X=UT$

$$U^{q^n}T^{q^n}=\sum_{i=1}^{n-1}c_iX^{q^i}Y^{q^n-q^i}+T^nXY^{q^n-1}\tag{6.12}$$

degut que $\deg T=1$, pel coroalari (5.46) es conclou $v_T(c_k)=n-k$. Com T^2 divideix la part esquerrana de la igualtat, també divideix la dretana. A més, com $v_T(c_k)=n-k$ llavors T^2 divideix els nomomis $c_iX^{q^i}Y^{q^n-q}$ amb $i<n-1$ necessàriament $T^2|c_{n-1}X^{q^{n-1}}Y^{q^n-q^{n-1}}$ com $v_T(c_{n-1})=1$ es conclou $T|XY$ però només és possible $T|X$ per la proposició (6.8).

□

6.3 Idees de Kummer

En aquest apartat s'obté un resultat anàleg al de Kummer per l'equació de Fermat i primers p regulars.

Teorema 6.13. ***(Kummer)*** *Sigui $p > 3$ un primer regular, és a dir $p \nmid h_p$, llavors l'Últim Teorema de Fermat és cert per a p; és a dir no hi ha solucions de*

$$X^p + Y^p = Z^p$$

amb $X, Y, Z \in \mathbb{Z}$ i $XYZ \neq 0$.

Es denota per h_p el nombre de classe de $\mathbb{Q}(\mu_p)$. En cossos de funcions és possible definir també el nombre de classe, veure Apèndix IV : Globals Fields.

Si $\pi \in A = \mathbb{F}_q[T]$ un primer, denotem per $K = F(\lambda)$, on $F = \mathbb{F}_q(T)$ i λ és un generador de Λ_π. Denotem per B la clausura entera de A en K, i h_π el nombre de classe.

Teorema 6.14. *Sigui $\pi \in A$ un primer, amb $d = \deg \pi > 1$. Suposem $q^{\deg \pi} \nmid h_\pi$ i $q > 2$. Llavors l'equació de Fermat-Gauss només te solucions trivials.*

Necessitarem uns resultats preliminars per la prova del teorema.

Teorema 6.15. *Considerem $M \in A$, i l'extensió K_M/F, on $K_M = F(\Lambda_M)$. Denotem per S el conjunt de les places sobre ∞, per $E(S)$ el grup de les unitats de $\mathcal{O}_M$. Llavors $E(S)/\mathbb{F}_q^\times$ és un grup lliure, de com a molt, rang $|S| - 1$.*

Veure [1, pàg. 243]. Aquest resultat és un anàleg del teorema de les unitats de Dirichlet per extensions finites de $\mathbb{Q}$.

Denotem per K^+ el cos fixat per $\{\sigma_c : c \in \mathbb{F}_q^\times\}$, veure teorema (5.34). Per aquest mateix teorema, el número de places sobre ∞ en K^+ és $\frac{q^{\deg \pi}-1}{q-1}$. A més, per (5.36) $[B^\times : B^{+\times}] = 1$. Per tant totes les unitats de B són iguals a les unitats de B^+.

Lema 6.16. ***(Goss)*** *Sigui $M \in A$, suposem que l'ideal $\mathfrak{B} = M \cdot B$ és una potència p-èssima, amb p primer, llavors $M = M_1^p$ per $M_1 \in A$.*

Demostració. Serà suficient demostrar quan M és una potència d'un primer. Escrivim $(M) = \mathfrak{p}^r$ la factorització en A. Sigui $\mathfrak{P}_1^{e_1} \cdot \ldots \mathfrak{P}_s^{e_s} = \mathfrak{p}$ la factorització en B.

Si $\mathfrak{p}^r$ és una potència p-èssima, llavors $p | r e_i$ per tot i. Veguem que $p \nmid e_i$ per algun i. En cas contrari, $p | e_i$ per tot i i per la proposició (9.6) s'obté

$$\sum_{i=1}^{s} e_i f_i = q^n - 1$$

on $n = \deg \pi$. Llavors $p | q^n - 1$, absurd. Així $p \nmid e_i$ per algun i i llavors $p | r$.

Així $(M) = (M_1)^p$ per cert $M_1 \in A$ i aleshores $M = c M_1^p$ amb $c \in \mathbb{F}_q^\times$ i és obvi que podem considerar $c = 1$, ja que tot element en $\mathbb{F}_q^\times$ és una potència p-èssima. □

Lema 6.17. *Sigui $\pi \in A$ un primer de grau major que 1, fixem λ un generador de Λ_π i considerem*

$$u = \prod_{\xi_i \in \Lambda_\pi^*} \frac{\xi_i}{\lambda},$$

llavors u no és una potència p-èssima.

Aquests dos resultats es poden trobar en l'article de Goss, en concret el lema (6.16) és pot trobar en [6, pàg. 280], el lema (6.17) en [6, pàg. 274].

Recordem que l'equació $Z^{q^{\deg \pi}} = \Psi_\pi(X,Y)$ es pot reescriure com

$$Z^{q^{\deg \pi}} = \prod_{i=1}^{q^{\deg \pi}} (X - \xi_i Y) \tag{6.18}$$

amb $\xi_i \in \Lambda_\pi$. Com en característica zero, dividim la prova en dos cassos.

6.3.1 Cas I : $\pi \nmid XYZ$

Sense pèrdua de generalitat, suposem que X, Y són coprimers. En (6.18) prenem ideals,

$$(Z)^{q^{\deg \pi}} = \prod_{i=1}^{q^{\deg \pi}} (X - \xi_i Y) \tag{6.19}$$

L'objectiu és demostrar que els ideals $(X - \xi_i Y)$ són coprimers entre si. Sigui $\mathfrak{d}$ un factor en comú de $(X - \xi_i Y)$ i $(X - \xi_j Y)$ amb $i \neq j$. Com

$$(X - \xi_i Y) - (X - \xi_j Y) = Y(\xi_j - \xi),$$

llavors $\mathfrak{d}|(Y)(\xi_i - \xi_j)$; com $i \neq j$ i $[\pi](X)$ és un polinomi additiu ,llavors $\xi_k = \xi_j - \xi_i$ és una altre arrel de $[\pi](X)$. Per tant, $\mathfrak{d}|(Y\pi)$, com també es compleix $\mathfrak{d}|(Z)^{q^{\deg \pi}}$, però $\pi \nmid Z$ i Y, Z són coprimers (al ser X, Y coprimers) llavors $\mathfrak{d}$ és l'ideal unitat.

Un cop hem garantit que $(X - \xi_i Y)$ són ideals coprimers, la factorització única d'ideals implica $(X - \xi_i Y) = \mathfrak{a}_i^{q^{\deg \pi}}$.

Com $\mathfrak{a}_i^{q^{\deg \pi}}$ és principal, llavors l'ordre de $\mathfrak{a}_i$ és una potència de p diguem-ne p^m. Sabem, $p^m | h_\pi$ per tant $p^m < q^{\deg \pi}$; escrivim $q^{\deg \pi} = p^n$, llavors $\mathfrak{a}_i^{p^n} = (\mathfrak{a}_i^{p^m})^{p^{n-m}} = (w_i)^{p^{n-m}}$ per cert $w_i \in B$, però com $1 \leq n - m$ llavors sempre podem reescriure $(w_i)^{p^{n-m}} = (t_i)^p$ amb $t_i = w_i^{p^{n-m-1}}$.

Per tant,

$$X - \xi_i Y = u_i t_i^p \tag{6.20}$$

amb $u_i \in B$ unitat. Una unitat de B s'escriu com

$$u_i = c \cdot a_1^{e_1} \cdot \ldots \cdot a_r^{e_r} \tag{6.21}$$

amb $c \in \mathbb{F}_q^\times$ i $a_i \in B$ unitat i $r = \frac{q^{\deg \pi} - 1}{q-1} - 1$. Com $\mathrm{mcd}(p, q-1) = 1$ llavors $c = c_2^p$ per cert $c_2 \in \mathbb{F}_q$, llavors podem suposar $c = 1$ en (6.21) fent un canvi de variable $t_i \mapsto c_2 t_i$ en (6.20). De manera similar, suposarem $1 \leq e_i \leq p - 1$, ja que si $e_i = pb_i + e_i'$ podem fer el canvi $t_i \mapsto b_i t_i$.

En total hi ha $q^{\deg \pi}$ termes del tipus $X - \xi_i Y$. Suposant que les unitats u_i s'escriuen de la forma descrita en l'anterior paràgraf. Llavors hi ha com a molt

$$(p-1)r = (p-1)\left(\frac{q^{\deg \pi} - 1}{q-1} - 1\right) \leq q^{\deg \pi} - p$$

diferents u_i. Donat que $q^{\deg \pi} - p < q^{\deg \pi}$ llavors hi ha $i \neq j$ tal que $u_i = u_j$, es segueix

$$(\xi_j - \xi_i)Y = u_i(t_i - t_j)^p \tag{6.22}$$

on $\xi_k = \xi_j - \xi_i$ és no nul, agafant ideals

$$(\xi_k)(Y) = (t_i - t_j)^p \tag{6.23}$$

es segueix $(\xi_k)|(t_i - t_j)$ donat que $(\xi_k) = (\lambda)$ és un ideal irreductible. Llavors $(\lambda)|(Y)$, però havíem suposat $v_\pi(Y) = 0$ (veure Apèndix II o III) i acabem d'obtenir $v_\pi(Y) > 0$.

6.3.2 Cas II: $\pi|XYZ$

Si suposem X, Y coprimers, llavors hi ha tres possibilitats: π divideix X, Y o bé a Z. Si π divideix Y per la proposició (6.8) $\deg \pi = 1$. A més, els cassos π divideix X o Z es donen simultànement com ja hem comentat.

Suposarem, $\pi|X$ i X, Y corpimers, per tant Y, Z també són coprimers. De nou, prenem ideals en (6.18)

$$(Z)^{q^{\deg \pi}} = (X)\prod_{i=2}^{q^{\deg \pi}}(X - \xi_i Y), \tag{6.24}$$

en aquest cas suposem $\xi_1 = 0$. Afirmem que els ideals $(\frac{X-\xi_i Y}{\xi_i})$ són coprimers entre si i amb (X). Cal remarcar que $\frac{X-\xi_i Y}{\xi_i} \in B$.

Sigui $\mathfrak{d}$ el factor en comú de $(X - \xi_i Y)$ i $(X - \xi_j Y)$, amb $i \neq j$, com en el cas anterior

$$\mathfrak{d}|(\xi_j - \xi_i)(Y)$$

també es compleix $\mathfrak{d}|(Z)^{q^{\deg \pi}}$, per coprimalitat entre Y, Z es segueix $\mathfrak{d}|(\xi_j - \xi_i) = (\lambda)$. Com (λ) és primer, llavors $\mathfrak{d}$ és l'ideal unitat o bé (λ), clarament $(\lambda)|(X - \xi_k Y)$ per tot $0 \leq k \leq q^{\deg \pi}$. Es segueix que $(\frac{X-\xi_i Y}{\xi_i})$ són coprimers entre ells i amb (X).

Llavors $(X - \xi_i Y) = (\lambda)\mathfrak{a}_i^{q^{\deg \pi}}$ per cert ideal $\mathfrak{a}_i$. De la suposició $q^{\deg \pi} \nmid h_\pi$ tenim

$$X - \xi_i Y = \lambda u_i t_i^p. \tag{6.25}$$

De nou, si escrivim

$$u_i = c \cdot a_1^{e_1} \cdot \ldots \cdot a_r^{e_r} \tag{6.26}$$

i fent el mateix argument que en el primer cas, podem suposar $c = 1$ i $1 \leq e_i \leq p-1$. Hi ha com a molt $q^{\deg \pi} - p$ diferentes unitats u_i, i $q^{\deg \pi} - 1$ termes del tipus $X - \xi_i Y$ amb $\xi_i \neq 0$. Com $q^{\deg \pi} - p < q^{\deg \pi} - 1$, llavors hi ha $i \neq j$ tal que $u_i = u_j$. Restant,

$$(\xi_j - \xi_i)Y = \lambda u_i (t_i - t_j)^p,$$

prenent ideals

$$(\lambda)(Y) = (\lambda)(t_i - t_j)^p \to (Y) = (t_i - t_j)^p$$

Del lema (6.16) obtenim que $Y = Y_1^p$ per cert $Y_1 \in A$. En comptes de considerar (6.25) dividem per ξ_i

$$\frac{X}{\xi_i} - Y_1^P = \left(\frac{\lambda}{\xi_i}\right) u_i t_i^p \tag{6.27}$$

fent serveri λ/ξ_i és unitat, reescrivim

$$\frac{X}{\xi_i} - Y_1^p = u\delta_1^p \qquad \text{on } t_i = \delta_1 \tag{6.28}$$

El que segueix de demostració és degut a David Goss en l'article [6].

Considerem σ_τ, on $\tau \in \mathbb{F}_q^\times$ amb $\tau \neq 1$ (remarquem que hem suposat $q > 2$). Recordem, $[B^* : B^{+*}] = 1$ llavors $u \in B^+$ i per tant $\sigma_\tau(u) = u$. Aplicant σ_τ en (6.28),

$$\frac{X}{\tau\xi_i} - Y_1^p = u\delta_2^p, \quad \text{on } \delta_2 = \sigma_\tau(\delta_1) \tag{6.29}$$

Restant (6.28) i (6.29), s'obté

$$(1 - \tau^{-1})\frac{X}{\xi_i} = u\delta_3^p \quad \text{on } \delta_3 = \delta_1 - \delta_2 \tag{6.30}$$

.

Per la proposició (6.7) πX és una potència p-èssima. Llavors,

$$\frac{X}{\xi_i} = \frac{X_1^p}{\pi\xi_i} = u\delta_4^p \quad \text{on } \delta_3^p = (1 - \tau^{-1})^{-1}\delta_4^p \tag{6.31}$$

on $X\pi = X_1^p$ per cert $X_1 \in A$, com

$$\pi\xi_i = \xi_i^{q^{\deg \pi}} \prod_{\xi_j \neq 0} \frac{\xi_j}{\xi_i}$$

per tant podem suposar $u = \prod_{\xi_j \neq 0} \frac{\xi_i}{\xi_j}$. Restant (6.28) i (6.31) obtenim

$$Y_1^p = \prod_{\xi_j} \frac{\xi_j}{\xi_i}\delta_5^p$$

però llavors estem contradient (6.17). Remarquem que en l'article [6] Goss suposa que $p \nmid h_\pi$ en comptes de $q^{\deg \pi} \nmid h_\pi$. A més a més Goss aprofundeix molt més en el tema; en el Teorema 2.4 [6, pàg. 273] dona una condició necessària i suficient de quan p divideix h_π.

6.4 El Teorema de Fermat-Gauss

L'any 1994 el matemàtic Laurent Denis, en l'article Le Théoreme de Fermat-Goss [3] va resoldre l'equació anàloga a la Fermat pel mòdul de Carlitz. En concret, podem trobar el següent resultat

Teorema 6.32. ***(Denis)*** *Sigui $f \in A = \mathbb{F}_q[T]$ un polinomi de grau d. Considerem les equacions*

$$\Psi_a(X,Y) = Z^{q^d}, \tag{6.33}$$

$$\Psi_a(X,Y) = Z^{p}, \tag{6.34}$$

llavors,

1. *Si $q \geq 3$ i $d \geq 2$, o bé $q = 2$ i $d > 2$, tant (6.33) com (6.34) tenen un nombre finit de solucions amb X, Y coprimers.*
2. *si $q \geq 3$ i $d \geq 2$. Aleshores (6.33) no té solucions en A amb $XYZ \neq 0$.*
3. *si $q \geq 3$, $p \neq 2$ i $d \geq 2$. Aleshores (6.34) no té solucions en A amb $XYZ \neq 0$*
4. *si $q \geq 4$, $p = 2$, $d \geq 2$. Aleshores (6.34) té una solució únicament quan $a = (T^2 + T + \beta)$, on β és un quadrat de $\mathbb{F}_q$. A més, les solucions són múltiples de $(1, 1, T + T^{q/2} + \alpha)$, on $\alpha^2 = \beta$.*
5. *si $q = 2$, $d \geq 4$. Aleshores (6.33) i (6.34) només hi ha solució si a és de la forma $(T^2 + T)b(T) + 1$ i aquesta solució és $(1, 1, 1, 1)$*

Observació 6.35. *El cas $d = 1$ el vam discutir en l'exemple (6.10)*

6.4.1 Lemes Preliminars

Recordem, si $a \in A$ i $d = \deg a$ llavors

$$[a](X) = c_d X^{q^d} + \sum_{i=1}^{d} c_i X^{q^i} + aX$$

amb $a_i \in A$. Denotarem per a_i' la derivada respecte T de a_i.

Lema 6.36. *Si $d \geq 1$ llavors $c'_{d-1} \in \mathbb{F}_q^\times$ i si a és mònic llavors $c'_{d-1} = 1$.*

Demostració. Fem primer el cas $a = T^i$ amb $i \geq 1$. Per inducció, el cas $i = 1$ és obvi. Del fet $[T^i](X) = [T^{i-1}]([T](X))$ per tant $c_{i-1} = d_{i-1}T + d_{i-2}^q$ si d_i són els coeficients de $[T^{i-1}](X)$. Recordant $d_{i-1} = 1$ llavors és obvi $c'_{i-1} = 1$.

En el cas general, $a = \sum_{i=0}^{d} a_i T^i$. De la igualtat $[a](X) = \sum_{i=0}^{d} a_i [T^i](X)$ i de la discussió anterior es veu $c'_{i-1} = a_d$.

□

Lema 6.37. *Sigui $a \in A$ amb $d \geq 1$; llavors $\deg(c_i) = q^i \deg a - iq^i$, $\deg(c_i') \leq q^i(\deg(a) - 1) - 1$ i $\deg(c'_{d-1}) = 0$.*

Demostració. Recordem el Lema (5.42)

$$c_m = \frac{c_{m-1}^q - c_{m-1}}{T^{q^m} - T}$$

on c_i són els coeficients de $[a](X)$. Aplicant aquesta fòrmula reiteradament es dedueix $\deg(c_i) = q^i \deg a - iq^i$. D'on $\deg c_i' \leq q^i \deg a - iq^i - 1$ i $\deg c'_{d-1} = 0$ del lema anterior. □

Lema 6.38. *Sigui $a \in A$ amb $d \geq 3$, o bé $q = 2$ i $p \neq 2$. El coeficient c_{d-2} no és una potència p-èssima. A més, c_{d-2} conté un terme amb la potència estrictament més gran de T, dels que no són potència p-èssima, entre els termes dels coeficients c_i amb $i \leq i \leq r$.*

Demostració. Per inducció sobre el grau $s = \deg b \geq 1$ es fàcil veure que la potència de T més gran de $[b](X)$ és $T^{q^{s-1}}$.

Per $d = \deg a \geq 2$, podem escriure $a = Tb + c$, per la divisó Euclidiana. De $[a](X) = [T]([b](X)) + c$ i de l'argument anterior, la potència més gran de T (sense ser potència p-èssima) és $T^{q^{d-1}} + 1$.

Llavors l'enunciat és cert si $d \geq 3$ o bé $d = 2$ i $p \neq 2$.

□

Aquests tres lemes són suficients per entendre la demostració del cas $q > 2$. El cas $q = 2$ requereix més lemes, i l'ús de les altures.

Definició 6.39. *L'altura de Weil per $x/y \in F = \mathbb{F}_q(T)$, amb $x, y \in A$ coprimers, està definit per $h(x/y) = \max(\deg x, \deg y)$.*

Lema 6.40. *Siguin $b_0, \ldots, b_d$ elements de F. Escrivim $\Psi(T) = b_0X + b_1X^q + \ldots b_rX^{q^r}$. Amb $r \geq 1$ i $b_r \neq 0$, llavors es compleix*

1. *Existeix una funció $\hat{h}_\Psi : \boldsymbol{G_a}(F) \to \mathbb{R}$, verifiviant, per tot $a \in A$ i tot $\alpha \in F$*

$$\hat{h}_\Psi(\Psi(a)(\alpha)) = q^{r \deg a} \hat{h}_\Psi(\alpha)$$

2. *Existeix un real $C_\Psi > 0$, que no depén dels coeficients $b_0, \ldots, b_r$ ni de q tal que si h és l'altura de Weil, llavors per tot $\alpha \in F$ es compleix,*

$$|\hat{h}_\Psi(\alpha) - h(\alpha)| \leq C_\Psi$$

3. *$\hat{h}_\Psi(x) = \lim_{n\to\infty} q^{-nr} h(\Psi(T^n)(x))$.*

Per una prova vegueu el Teorema 1 de [4]. Es coneix com a mòdul de Drinfeld de rang r a Ψ, que és un morfisme de l'anell A a l'anell dels polinomis additius. Un exemple de mòdul de Drinfeld és el mòdul de Carlitz, que té rang 1.

Lema 6.41. *Sigui $\Psi(T) = \frac{1}{a}[c_0X + c_1X^q + \ldots + c_dX^{q^d}]$ amb*

1. *$a, c_0, \ldots, c_d \in A$,*
2. *$c_d \in A^\times$,*
3. *$\deg c_i + q^i < q^d$, $0 \leq i \leq d-1$*

Denotem per $\bar{h}_\Psi$ l'altura que ens assegura el lema (6.40). Per tot $x \in F$, es compleix:

$$|\hat{h}_\Psi(x) - h(x)| \leq \frac{\max_{0\leq i\leq d-1}(\deg c_i, \deg a)}{q^d - 1}$$

Demostració. La idea és estimar $h(\Psi(T)(\frac{P}{Q})x)$ en funció de $h(x)$. Sigui $P, Q \in A$ coprimers. Llavors

$$\Psi(T)\left(\frac{P}{Q}\right) = \frac{c_0PQ^{q^d-1} + c_1P^qQ^{q^d-q} + \ldots + c_dP^d}{aQ^{q^d}}$$

Com P, Q són coprimers i $c_d \in \mathbb{F}_q^\times$ llavors el numerador és coprimer amb Q, aleshores

$$\begin{aligned} q^d \deg Q &\leq h(\Psi(T)(P/Q)) \\ &\leq \max(\deg a + q^d \deg Q, \max_{0\leq i\leq d}(\deg c_i) + (q^d - q^i)\deg Q + q^i \deg P) \end{aligned}$$

Si $\deg Q \geq \deg P$, es segueix

$$\begin{aligned} q^d \deg Q &\leq h(\Psi(T)(P/Q)) \\ &\leq \max(\deg a + q^d \deg Q, \max_{0\leq i\leq d}(\deg c_i) + q^d \deg Q); \end{aligned}$$

equivalenment,

$$0 \leq \frac{h(\Psi(T)(P/Q))}{q^d} - h\left(\frac{P}{Q}\right) \leq \frac{\max_{0\leq i\leq d-1}(\deg c_i, \deg a)}{q^d}.$$

En cas contrari, $\deg Q < \deg P$, usem la estimació $h(\Psi(T)(P/Q)) \geq M - \deg a$, on M és el grau del numerador de $\Psi(T)(P/Q)$. Demostrem $M = q^d \deg P$. Serà suficient veure

$$q^d \deg P > \max_{0\leq i\leq d-1}(\deg c_i) + (q^d - q^i)\deg Q + q^i \deg P.$$

Com $\deg Q \leq \deg P - 1$ serà suficient verificar

$$q^d \deg P > \max_{0\leq i\leq d-1}(\deg c_i) + (q^d - q^i)(\deg P - 1) + q^i \deg P,$$

però usant la hipòtesis (iii) es dedueix

$$q^d > \max_{0\leq i\leq d-1}(\deg c_i + q^i)$$

Llavors s'obté

$$-\deg a \leq h(\Psi(T)(P/Q)) - q^d h(P/Q).$$

De d'aquest punt es procedeix de manera similar a l'altre cas, doncs es compleix

$$\left|\frac{h(\Psi(T)(P/Q))}{q^d} - h\left(\frac{P}{Q}\right)\right| \leq \frac{\max_{0\leq i\leq d-1}(\deg c_i, \deg a)}{q^d}.$$

L'enuncat s'obté sumant en n i al usar $\hat{h}_\Psi(x) = \lim_{n\to\infty} q^{-nd}$, resultat del lema (6.41)

□

Corol·lari 6.42. *Donat $a \in A$ de grau $d \geq 1$ i $\Phi(a) = aX + c_1X^q + \ldots + a_dX^{q^d}$. Llavors, $\Psi(T) = (1/a)[a'X + c_1X^q + \ldots + c'_{d-1}X^{q^{d-1}}]$, definiex un mòdul de Drinfeld de rang $d-1$ i la altura associada $\hat{h}_\Psi$ verifica la següent propitat, si $d \geq 2$, per tot $x \in F$:*

$$\left|\hat{h}_\Psi(x) - h(x)\right| \leq 2\frac{q^{d-2}}{q^{d-1}-1}$$

Demostració. Usant la cota proporcionada pel lema (6.41), les cotes del lema (6.37) pels polinomis a'_i s'obté la desigualtat de l'enunciat.

□

6.4.2 Demostració quan $q > 2$

Considerem $a \in A$ amb $d = \deg a \geq 2$, sense pèrdua de generalitat suposem a mònic, escriurem

$$[a](X) = X^{q^d} + c_{d-1}X^{q^{d-1}} + \ldots + c_0 X$$

Reescrivim les equacions (6.33) i (6.34) com

$$[a](X/Y) = Z^e/Y^{q^d} \tag{6.43}$$

és a dir,

$$(X/Y)^{q^d} + c_{d-1}(X/Y)^{q^{d-1}} + \ldots + aX/Y = Z^e/Y^{q^d} \tag{6.44}$$

amb $e = q^d$ o bé $e = p$. També suposarem que X, Y són coprimers i que són mònics. Derivant (6.44) respecte T

$$c'_{d-1}(X/Y)^{q^{d-1}} + \ldots + a'X/Y + a(X/Y)' = 0 \tag{6.45}$$

multiplicant per $Y^{q^{d-1}}$

$$c'_{d-1}X^{q^{d-1}} + \ldots + a'XY^{q^{d-1}-1} + a(X/Y)'Y^{q^{d-1}} = 0, \tag{6.46}$$

com $Y^{q^{d-1}}(X/Y)' = (X'Y - XY')Y^{q^{d-1}-2}$ i $c'_{d-1} \in \mathbb{F}_q^\times$ (lema 6.36) i $q^{d-1} > 2$ (ja que $q > 2$ i $d \geq 2$), es dedueix Y divideix X, d'on $Y = 1$.

L'equació (6.44) es converteix en

$$X^{q^d} + c_{d-1}X^{q^{d-1}} + \ldots + aX = Z^e \tag{6.47}$$

Ara ens fixem que la part dretana és una potència de p: pel lema (6.36) a_{d-1} és suma de dels T^{q^i} amb $i \geq 0$, el que implica

$$TX^{q^{d-1}} + c_{d-2}X^{q^{d-2}} + \ldots + aX \tag{6.48}$$

és una potència p-èssima. Pel lema (6.37), $\deg c_i X^{q^i} = q^i \deg X + q^i(d-i)$. Afirmem, el grau de (6.48) és el de $TX^{q^{d-1}}$. Per això comprovem $q^{d-1}\deg X + 1 > q^i \deg X + q^i(d-i)$, per tot $0 \leq i \leq r-2$, per això serà suficient veure

$$q^{d-1}\deg X + 1 > q^{d-2}\deg X + 2q^{d-2}$$

equivalenment,

$$(q-1)\deg X > 2 - \frac{1}{q^{r-2}}$$

com $q > 2$ la desigualtat es satisfà per $\deg X \geq 1$. Però llavors (6.48) té grau $q^{r-1}\deg X + 1$ i no pot ser una potència p-éssima. Per tant $X = 1$. L'equació (6.45) es transforma

$$a' + c'_1 + \ldots + c'_{d-1} = 0$$

llavors el lema (6.38) dona una contradicció si $d \geq 3$ o $d = 2$ i $p \neq 2$.

Falta examinar el cas $\deg a = 2$ i $p = 2$. Com $q > 2$ es segueix complint $X = 1$ i $Y = 1$, si a és mònic obtenim

$$a + c_1 + 1 = Z^e.$$

Escrivim $a = T^2 + \alpha T + \beta$, llavors $c_1 = T^q + T + \alpha$. L'equació es converteix

$$T^2 + \alpha T + \beta + T^q + T + \alpha + 1 = Z^e$$

Si $e = q^2$ està clar que no hi ha solucions. Si $e = 2$ llavors és necessari $\alpha = 1$, per tal que la part dretana sigui un quadrat. L'equació es redueix

$$T^q + T^2 + \beta = Z^2$$

És obvi que hi ha solucions només quan β és un quadrat. Això demostra el segon, tercer i quart punt del teorema.

6.4.3 Demostració quan $q = 2$

Suposem que $(X, Y, Z) \in A^3$ és solució de (6.44) tal que $d = \deg a > 1$, $XYZ \neq 0$, $\mathrm{mcd}(X, Y) = \mathrm{mcd}(Z, Y) = 1$.

Recordem que la derivada de (6.44) dona

$$c'_{d-1}(X/Y)^{q^{d-1}} + \ldots + a'X/Y + a(X/Y)' = 0. \tag{6.49}$$

Considerem $\Psi(T) = (\frac{1}{a})[a'X + c'_1X^q + \ldots + c'_{d-1}X^{q^{d-1}}]$, que pel corol·lari (6.42) és un mòdul de Drinfeld de rang $d-1$. Denotem per $\hat{h}_\Psi$ la seva altura associada, que garanateix el lema (6.40).

L'apartat 1) de (6.36) i (6.49) es segueix

$$q^{d-1}\hat{h}_\Psi(X/Y) \leq \hat{h}_\Psi((X'Y - XY')/Y^2).$$

L'apartat 2) de (6.40) implica

$$\hat{h}_\Psi((X'Y - XY')/Y^2) \leq h((X'Y - XY')/Y^2) + C_\Psi$$

Usant $\mathrm{mcd}(X, Y) = 1$ es dedueix

$$q^{d-1}\hat{h}_\Psi(X/Y) \leq 2h(X/Y) + C_\Psi \leq 2\hat{h}_\Psi + 3C_\Psi;$$

per tant

$$(q^{d-1} - 2)\hat{h}_\Psi(X/Y) \leq 3C_\Psi. \tag{6.50}$$

Com $q^{d-1} - 2 > 0$ llavors hi ha un nombre pinits de solucions, és a dir hem provar l'apartat 1) del teorema.

A continuació discutim en conret el cas $q = 2$. De la desigualtat $h(X/Y) \leq \hat{h}_\Psi(X/Y) + C_\Psi$ i de la desigualtat (6.50) s'obté

$$\max(\deg X, \deg Y) \leq C_\Psi + \frac{3C_\Psi}{q^{d-1} - 2} := f(q, d).$$

El corol·lari (6.42) justifica que l'apartat dretana de la desigualtat només depèn de q, d. Pel mateix corol·lari es comprova que $f(q, d)$ és decreixent en q, d. Fixem $q = 2$. Obtenim el valors, $f(3, 2) \leq 3.4$; $f(4, 2) \leq 1.8$; $f(d, 2) \leq 1.8$ per $d \geq 4$. Implica, $\deg X \leq 1$.

Tractem primer el cas $d > 3$ i $q = 2$. Es segueix complint $Y = 1$ i $\deg X \leq 1$. Calculant $[a](1)$. Cal remcarcar $[T^2 + T](1) = 0$. Escrivint $a = f(T)(T^2 + T) + eT + f$, es veu

$$[a](1) = [f]([T^2 + T](1)) + [eT + f](1) = e(T + 1) + f$$

Per tal que la aquesta quantitat sigui un quadrat no nul, és necessari i suficient que $e = 0$ i $f = 1$.

Com $[T](T) = 0$, $[a](T + g) = a(0)T + ge(T + 1) + gf$. Si $a(0) = 1$, trobem la mateixa condiciño que abans. Si T divideix a, $f = 0$ i no hi ha solucions no trivials. Resument, si $d <\geq 4$, hi ha solucions no trivials si i només si $a = f(T^2 + T) + 1$ per tota $f \in A$.

Discutim ara el cas $\deg a = 3$. Només discutim l'equació (6.34) l'altre (6.33) es raona de manera anàloga. L'equació és

$$aXY^7 + c_1X^2Y^6 + c_2X^4Y^4 + X^8 = Z^2,$$

la qüestiò és si el terme de l'esquerre pot ser un quadrat. Es veu que és equivalent si $aXY^3 + c_1X^2Y^2 + c_2X^4$ és un quadrat. Com $c_2' = 1$ la condició és equivalent demanr $aXY^3 + c_1X^2Y^2 + TX^4$ és un qadrat. Derivant,

$$a'XY^3 + aX'Y^2 + aXY^2Y' + c_1'X^2Y^2X^4 = 0$$

Es dedueix que tot factor primer de Y divideix X, llavors $Y = 1$ (recordem que hem suposat $\mathrm{mcd}(X, Y) = 1$). Així, la pregunta es redueix en si $aX + c_1X^2 + TX^4$ és un quadrat. El grau de a és 3, es verifica que $\deg a_1 = 4$. Es dedueix que si $\deg X > 1$, llavors el grau de l'expressió és $4 \deg X + 1$ i per tant no pot ser quadrat. Llavors $\deg X \leq 1$. Es poden donar noméstres cassos, $X = 1, T, T + 1$. Un càlcul mostra que les solucions per X, amb $Y = 1$:

$$\begin{aligned}
&T^3 + T^2 + T + 1 && :X = 1, X = T + 1;\\
&T^3 + T^2 + T && :X = 1, X = T, X = T + 1;\\
&T^3 + T^2 + 1 && :X = 1;\\
&T^3 + T^2 && :X = 1, X = T + 1;\\
&T^3 + T + 1 && :X = 1;\\
&T^3 + T && :X = 1, X = T, X = T + 1;\\
&T^3 + 1 && :X = T + 1;\\
&T^3 && :X = T;
\end{aligned}$$

El cas $\deg a = 2$ es fa cas a cas, pels polinomis $a = T^2, T^2 + T, T^2 + 1, T^2 + T + 1$. Es resolen de manera similar, es discuteix si $[a](X/Y)Y^{q^{\deg a}}$ pot ser un quadrat, i usant la mateixa técnica, si és un qaudrat llavors la derivada és zero, i fer servir que el coeficieint c_{d-1} és una constant no nula i si es necessari, discutir els graus dels coeficients. No té més misteri. Resumim les solucions per a cada cas

$$\begin{aligned}
&T^2 && :(X, Y, Z) = (T^2, T^2 + 1, T);\\
&T^2 + 1 && :(X, Y, Z) = (T^2 + 1, T, T + 1);\\
&T^2 + T && :(X, Y, Z) = (T^3 + T^2 + T + 1, T^2 + T), (T^3 + 1, T^2 + T + 1, T^+T),\\
& && \ (1, T^2 + T + 1, T^2 + T);\\
&T^2 + T + 1 && :(X, Y, Z) = (1, 1, 1);
\end{aligned}$$

7 Apèndix I: Anells de Valoració discreta i Dominis de Dedekind

En aquesta secció seguim el nové capítol de [2]. En el que segueix tots els anells seran commutatius amb unitat.

Definició 7.1. *Un ideal $\mathfrak{a} \subset R$ d'un anell, és irreductible si*

$$\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow \mathfrak{a} = \mathfrak{b} \text{ o bé } \mathfrak{a} = \mathfrak{c}$$

Lema 7.2. *En un anell Noetherià A tot ideal és intersecció finita d'ideals irreductibles.*

Demostració. Per reducció a l'asburd suopsem que no; llavors el conjunt dels ideals que no són interesecció finita d'irreductibles és no buit, per tant té un element maximal $\mathfrak{a}$. Com $\mathfrak{a}$ és reductible (i.e. no és irreductible), llavors $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c}$ amb $\mathfrak{a} \subset \mathfrak{b}$ i $\mathfrak{a} \subset \mathfrak{c}$. Per maximilitat $\mathfrak{b}$, $\mathfrak{c}$ són intersecció d'irreductibles i conseqüenment $\mathfrak{a}$.

□

Definició 7.3. *Direm que un ideal $\mathfrak{a} \subset R$ d'un anell és primari si $xy \in \mathfrak{a}$ llavors $x^n \in \mathfrak{a}$ o bé $y^n \in \mathfrak{a}$ per $n \geq 0$ i tot $x, y \in R$.*

Lema 7.4. *En un anell Noetherià tot ideal irreductible és primari.*

Demostració. Sigui $\mathfrak{a}$ un ideal irreductible, serà suficient comprovar que en l'anell $R/\mathfrak{a}$ l'ideal zero és primari. Sigui $xy = 0$ amb $y \neq 0$ i la cadena $\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \ldots$. Per la c.c.a. aquesta cadena ha de ser estacionària i.e. $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \ldots$ per cert n. Es segueix que $(x^n) \cap (y) = 0$; ja que si $a \in (y)$ llavors $ax = 0$, i si a més $a \in (x^n)$ llavors $a = bx^n$ però llavors $ax = bx^{n+1} = 0$, per tant $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$ i per tant $a = bx^n = 0$. Com (0) és irreductible i $(y) \neq 0$ llavors $x^n = 0$ el que demostra que (0) és primari. □

Corol·lari 7.5. *En un anell Noetherià tot ideal $\mathfrak{a}$ té una descomposició en ideals primaris.*

Definició 7.6. *Diem que la cadena d'ideals primers $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$ té longitud n. Definim la dimensió de Krull d'un anell R, $\dim_K(R)$, com el suprem de les longitud de cadenes d'ideals primers.*

Definició 7.7. *Donat un ideal $\mathfrak{a} \subset R$ d'un anell, definim el seu redical*

$$\sqrt{\mathfrak{a}} = \{x \in R : x^n \in \mathfrak{a}, \text{ per cert } n\}$$

Si $\mathfrak{p}$ és un ideal primer, llavors $\mathfrak{q} = \sqrt{\mathfrak{p}}$ és primari. Diem que $\mathfrak{q}$ és $\mathfrak{p}$-primari.

Definició 7.8. *Dos ideal $\mathfrak{a}, \mathfrak{b} \subset R$ són coprimers si $\mathfrak{a} + \mathfrak{b} = R$*

Proposició 7.9. *Sigui $\mathfrak{a}, \mathfrak{b} \subset R$ un ideal d'un anell amb unitat, llavors*

- $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$
- $\sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} = \sqrt{\mathfrak{a} + \mathfrak{b}}$
- $\sqrt{\mathfrak{a}} = R$ *si i només si* $\mathfrak{a} = R$

Demostració.

- Si $x \in \sqrt{\sqrt{\mathfrak{a}}}$ llavors $x^n \in \sqrt{\mathfrak{a}}$ per cert n, llavors $x^{nm} \in \mathfrak{a}$ per cert m i deduim $x \in \sqrt{\mathfrak{a}}$. La implicació contrària és evident.
- Si $x \in \sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}}$ llavors $x^n \in \sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}$ per tant $x^n = v + u$ amb $v \in \sqrt{\mathfrak{a}}$ i $u \in \sqrt{\mathfrak{b}}$, hi ha a, b enters tal que $v^a \in \mathfrak{a}$ i $u^b \in \mathfrak{b}$ considerem $m = 2\max(a, b)$ per tant $x^{nm} = \sum_{i=0}^{m} \binom{n}{i} u^i v^{n-i}$ i per construcció $i \geq \max(a, b)$ o bé $n - i \geq \max(a, b)$ i per tant $u^i \in \mathfrak{a}$ o bé $v^{n-1} \in \mathfrak{b}$ per tant $x^{nm} \in \mathfrak{a} + \mathfrak{b}$ o sigui $x \in \sqrt{\mathfrak{a} + \mathfrak{b}}$.

Si $x \in \sqrt{\mathfrak{a}+\mathfrak{b}}$ llavors $x^n \in \mathfrak{a}+\mathfrak{b}$ o sigui $x^n = u+v$ amb $u \in \mathfrak{a}$ i $v \in \mathfrak{b}$ i clarament $u \in \sqrt{\mathfrak{a}}$ i $v \in \sqrt{\mathfrak{b}}$ per tant $x^n \in \sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}$ i $x \in \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}}$.

- Clarament $1 \in \sqrt{\mathfrak{a}}$ si i només si $1 \in \mathfrak{a}$

□

Lema 7.10. *Sigui $\mathfrak{a}, \mathfrak{b}$ ideals d'un anell A de manera que $\sqrt{\mathfrak{a}}$ i $\sqrt{\mathfrak{b}}$ siguin coprimers. Llavors $\mathfrak{a}$ i $\mathfrak{b}$ són coprimers.*

Demostració. Usant la proprosició anterior

$$\sqrt{\mathfrak{a}+\mathfrak{b}} = \sqrt{\sqrt{\mathfrak{a}}+\sqrt{\mathfrak{b}}} = \sqrt{(1)} = (1)$$

per l'ultim punt, $\mathfrak{a}+\mathfrak{b} = (1)$ i per tant són coprimers.

□

Lema 7.11. *Si els ideals $\mathfrak{a}_i$ són coprimers dos a dos, llavors $\prod \mathfrak{a}_i = \cap \mathfrak{a}_i$.*

Demostració. Per inducció sobre n, el cas base $n = 2$,

$$(\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$$

que $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ està clar.

Suposem ara $n > 2$ i el resultat és cert per $\mathfrak{a}_1, \dots \mathfrak{a}_{n-1}$ sigui $\mathfrak{b} = \prod_{i=1}^{n-1} \mathfrak{a}_i = \cap_{i=1}^{n-1} \mathfrak{a}_i$. Com es compleix $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ per $i \leq n-1$ llavors $x_i + y_i = 1$, per $x_i \in \mathfrak{a}_i$ i $y_i \in \mathfrak{a}_n$ llavors

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1-y_i) \equiv 1 \mod \mathfrak{a}_n$$

Per tant $\mathfrak{a}_n + \mathfrak{b} = (1)$ i

$$\prod_{i=1}^{n} \mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_\mathfrak{n} = \cap_{i=0}^{n} \mathfrak{a}_n$$

□

Proposició 7.12. *Siguo A un domini Noetherià de dimensió 1. Llavors tot ideal no nul $\mathfrak{a} \subset A$ es pot expressar unívocament com producte producte d'ideals primeris que tenen el radical diferent.*

En aquesta demostració no vaurem la unicitat, només l'existència.

Demostració. Com A es Noetherà, llavors $\mathfrak{a}$ té una descomposició primari minimal, $a = \cap_{i=1}^{n} \mathfrak{q}_i$ on $\mathfrak{q}_i$ són $\mathfrak{p}_i$-primaris. Com $\dim_K(A) = 1$ i A és un domini d'integritat, tots els ideals primers no nuls són maximals, per tant $\mathfrak{p}_i$ són ideals maximals diferents i per tant coprimers dos a dos. Llavors els $\mathfrak{q}_i$ són també coprimers dos a dos per tant $\prod \mathfrak{q}_i = \cap \mathfrak{q}_i$ i per tant $\mathfrak{a} = \prod \mathfrak{q}_i$.

□

7.1 Valoracions discretes

Definició 7.13. *Sigui K un cos. Una valoració és una aplicació $v : K \to \mathbb{R} \cup \{\infty\}$, que compleix*

- $v(xy) = v(x) + v(y)$,
- $(x + y) \geq \min(v(x), v(y))$
- $v(a) = \infty$ *sii* $a = 0$.

Direm que una valoració és discreta, si la imatde de v està contingut en $\frac{1}{n}\mathbb{Z}$ per algún $n \in \mathbb{R}$.

Definim l'anell de valoració R_v i el seu únic ideal maximal. Una plaça de K és l'ideal maximal d'un anell de valoració discreta en K.

$$R_v = \{x \in K : v(x) \geq 0\}$$
$$M_v = \{x \in K : v(x) > 0\}$$

Denotem per $k_v = R_v/M_v$ el cos residual de la valoració v.

Observació 7.14. *De la identitat $1 = 1^2$ obtenim $v(1) = 2v(1)$ i per tant $v(1) = 0$. Si $u \in K^\times$ llavors $0 = v(1) = v(uu^{-1}) = v(u) + v(u^{-1})$ i per tant $v(u^{-1}) = -v(u)$.*

D'aquestes observacions es segueix que $R_v^\times = \{x \in K : v(x) = 0\}$ per tant: 1) El cos de fraccions de R_v és v. 2) $M_v = R_v \setminus R_v^\times$ i per això és l'únic ideal maximal.

Exemple 7.15. *Si $K = \mathbb{Q}$. Fixem $p \in \mathbb{Z}$ llavors tot $x \in \mathbb{Q}$ no nul s'expressa de manera única com $p^a y$ amb $a \in \mathbb{Z}$ amb el numerador i denominador de y coprimers amb p. Definim $ord_p(x) = a$.*

Exemple 7.16. *Considerem $K = k(x)$ amb k cos. Per polinomis $f(x), g(x) \in K[x]$, escrivim*

$$ord_\infty(f/g) = -\deg(f) + \deg(g),$$

llavors ord_∞ és una valoració en $k(x)$

Proposició 7.17. *Sigui A un domini noetherià local de dimensió 1, $\mathfrak{m}$ el seu ideal maximal, $k = A/m$ el seu cos de residual. Llavors és equivalent:*

- *A és una anell de valoració discreta;*
- *A és íntegrament tancat;*
- *$\mathfrak{m}$ és un ideal principal;*
- $\dim_K(\mathfrak{m}/\mathfrak{m}^2) = 1$
- *Tot ideal no nul és una potència de $\mathfrak{m}$.*

Per una prova veure [2] pàgines 94-95.

7.2 Dominis de Dedekind

Teorema 7.18. *Sigui A un domini Noetherià de dimensió 1. Llavors és equivalent:*

1. *A és íntegrament tancat.*
2. *Tot ideal primari de A és una potència d'un primer*
3. *Tot anell local $A_\mathfrak{p}$ ($\mathfrak{p} \neq 0$) és un anell de valoració discreta.*

Per una demostració, veure [2].

Definició 7.19. *Un anell R direm que és un domini de Dedekin si satisfà una de les condicions del teorema anterior.*

Corol·lari 7.20. *Tot ideal no nul en un domini de Dedekin té una descomposició única producte d'ideals primers.*

Demostració. Per 7.12 i pel segon punt del teorema anterior.

□

Corol·lari 7.21. *Sigui k un cos cos, llavors $k[x]$ l'anell de polinomis és un domini de Dedekind.*

Demostració. Com k és cos, llavors $k[x]$ és domini d'ideals principals. Per ser DIP, té dimensió 1; ja que tot ideal primer és maximal, és Noetherià; tot ideal és finitament generat. A més, tot anell local $A_{\mathfrak{p}}$, $\mathfrak{p} \neq 0$, és un domini d'ideals principals i pel teorema (7.18) es dedueix que $K[x]$ és un domini de Dedekind. □

Proposició 7.22. *Sigui $F = \mathbb{F}_q(T)$ i K/F una extensió finita. Denotem per B la clausura entera de $A = \mathbb{F}_q[T]$ en K. Llavors B és un domini de Dedekind.*

Demostració. (**Sketch**)

Per transitivitat B és íntegrament tancat. Per tant, per l'apartat 1) del teorema (7.18) només falta demostrar que B és Noetherià de dimensió 1.

Per veure que és Noetherià, primer es comprova que B és un A-mòdul finitament generat. Un resultat d'àlgebra commutativa ens asegura que B és Noetherià (donat que és un A-mòdul finitament generat i A és noethrià).

Hi ha un resultat d'àlgebra commutativa que ens asegura, si $A \subset B$ amb B entera sobre A. Si $\mathfrak{P} \subset B$ primer, i $\mathfrak{p} = \mathfrak{P} \cap A$. Llavors $\mathfrak{P}$ és maximal si i només $\mathfrak{p}$ es maximal. Això ens permet afirmar que B té dimensió 1.

□

8 Apèndix II : Valoracions i valors absoluts en característica positiva

8.1 Valoracions

En aquesta secció seguim el llibre [7]. Diem que dos valoracions v_1, v_2 són són equivalents si hi ha una constant $c \in \mathbb{R}$ tal que $v_1 = cv_2$. Una valoració no trivial, si hi ha un element x tal que $v(x) \neq 0$.

Teorema 8.1. *Sigui v una valoració no trivial en $k(x)$. Si v és no negativa en l'anell de polinomis $K[x]$ llavors hi ha un polinomi $P(x)$ tal que v és equivalent a la valoració ord_p. En canvi, si hi ha algun valor negatiu llavors v és equivalent a ord_∞.*

Demostració. Primer suposem que v és no negativa en $k[x]$. Llavors hi ha un polinomi mònic $P(x)$ amb grau minimal tal que $v(P) > 0$. Afirmem que P és irreductible, en cas contrari $P = f \cdot g$, llavors $v(P) = v(f) + v(g)$ i necessàraiment $v(f) > 0$ o bé $v(g) > 0$, en qualsevol dels dos cassos això contradiu l'elecció de P. Rescalant v podem suposar $v(P) = 1$. Suposem que $f(x) \in k[x]$ no és divisible per $P(x)$ llavors $f = Pg + r$ i $0 \leq \deg r < \deg P$, per maximilitat de $P(x)$ tenim $v(r) = 0$, llavors

$$0 = v(r) = v(f - Pg) \geq \min(v(f), v(P) + v(g)) \geq \min(v(f), v(P)).$$

Com $v(f) \geq 0$ i $v(P) > 0$ deduim $v(f) = \mathrm{ord}_P(f)$. Si $f = P^n g$ amb g coprimer amb P llavors, $v(P^n g) = v(P^n) + v(g) = nv(P)$. Llavors $v = \mathrm{ord}_P$.

Ara suposem v pren algún valor negatiu en $k[x]$. Llavors existeix un polinomi de grau minimal tal que $v(P) < 0$. Escrivim $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_0 = x^n + f(x)$, amb $n \geq 1$ i $v(f) \geq 0$. Com $0 > v(P) \geq \min(v(x^n), v(f))$ hem de tenir $v(x^n) = nv(x) < 0$ i per tant $v(x) < 0$. Rescalant podem suposar $v(x) = -1$. Escrivim $y = x^{-1}$ i considerem l'anell $k[y] \subset K$. Com $k[y]$ és un anell de polinomis i la valoració és no negativa, per l'argument previ tenim $v = \mathrm{ord}_y$ en $k[y]$. Llavors, $v = \mathrm{ord}_y$ també en $k(y) = K$. Per acabar, escrivim $f(x) \in k[x]$ de grau n com

$$f(x) = y^{-n}(a_n + a_{n-1}y + \ldots + a_0 y^n)$$

Com $a_n \neq 0$, tenim

$$v(f) = v_y(f) = -nv_+ v_y(a_n + a_{n-1}y + \ldots + a_0 y^n) = -n + 0 = -\mathrm{ord}_\infty(f)$$

□

Proposició 8.2. *Dos valoracions no trivials v_1, v_2 en un cos K són equivalent si i només si $M_{v_1} = M_{v_2}$.*

Demostració. És obvi que si v_1, v_2 són equivalents llavors $M_{v_1} = M_{v_2}$.

Suposem ara $M_{v_1} = M_{v_2}$. Sigui $0 \neq a \in M_{v_1}$. Llavors $c = v_1(a)/v_2(a)$ és un real positiu. Afirmem que $v_1(b) = c \cdot v_2(b)$ per tot $b \in K^\times$. Si no fos així, llavors hi ha b tal que $c \cdot v_2(b) < v_1(b)$ (possiblement canviant b per b^{-1}). Considerem un racional n/m, $m > 0$ tal que

$$c \cdot v_2(b) < \frac{n}{m} c \cdot v_2(a) = \frac{n}{m} v_1(a) < v_1(b).$$

Llavors

$$c \cdot v_2(b^m) < c \cdot v_2(a^n) = v_1(a^n) < v_1(b^m),$$

per tant

$$c \cdot v_2(b^m) - c \cdot v_2(a^n) < 0 < v_1(b^m) - v_1(a^n),$$

llavors

$$v_2(b^m/a^n) < 0, \quad \text{i} \quad 0 < v_1(b^m/a^n)$$

el que contradiu $M_{v_1} = M_{v_2}$. □

Observació 8.3. *Com a conseqüència, hi ha una relació bijectiva entre les classes de valoracions i els maximals M_v.*

8.2 Valors absoluts

Definició 8.4. *Un valor absolut no arquimedià en un cos K és una funció $|\cdot| : K \to \mathbb{R}_{\geq 0}$ que satisfà les següents condicions:*

- $|a| = 0$ *si i només si* $a = 0$.
- $|ab| = |a| \cdot |b|$ *per tot* $a, b \in K$
- $|a + b| \leq \max(|a|, |b|)$ *amb igualtat si* $|a| \neq |b|$.

Direm que dos valors absoluts $|\cdot|, |\cdot|'$ són equivalents si $|a|^s = |a|'$ per tot $a \in K$ per una constant positiva s.

Observació 8.5. *Observem que si $|\cdot|$ és un valor absolut i c una constant positiva llavors $v = -\log_c |a|$ és una valoració en K. Recíprocament, si v és una valoració llavors $|a| := c^{-v(a)}$ és un valor absolut en K.*

Definició 8.6. *Sigui L un cos que conté K, un altre cos. Diem que un valor absolut $\|\cdot\|$ en L exten un valor absolut $|\cdot|$ en K si $\|a\| = |a|$ per tot $a \in K$.*

Definició 8.7. *Si L/K és una extensió de cossos de grau n. Considerant L com un K-espai vectorial, definim la K-transformació $T_\alpha : \beta \to \alpha\beta$ amb $\alpha \in L$. Fixat una base de n elements podem definir $Nr_{L/K} : L \to K$ tal que $\alpha \mapsto det(T_\alpha)$.*

Proposició 8.8. *Sigui L/K una extensió de cossos de grau n. L'aplicació $\|\cdot\| : L \to \mathbb{R}_{\geq 0}$ definida per*

$$\|a\| = |Nr_{L/K}(a)|^{1/n}$$

és un valor absolut en L que exten el valor absolut en K.

La demostració requereix un corol·lari d'un resultat que es coneix com el Lema de Hensel, i un altre resultat.

Teorema 8.9. ***(Lema de Hensel)*** *Considerem un cos K complet respecte una valoració no trivial. Denotem per R l'anell dels enters i M l'ideal maximal de R i considerem el cos $k = R/M$. Sigui $f(x) \in R[x]$ tal que $\bar{f}(x) \in k[x]$ (la reducció dels coeficients de f mòdul M) sigui no nula. Suposem que es compleix*

1. $\bar{f}(x) = g_0(x) \cdot h_0(x)$ *amb* $g_0(x), h_0(x) \in k[x]$,
2. g_0 *és mònic,*
3. g_0 *i* h_0 *són coprimers en* $k[x]$.

Llavors $f(x)$ factoritza com

$$f(x) = g(x) \cdot h(x)$$

amb únic $g(x), h(x) \in R[x]$ tal que $\bar{g}(x) = g_0(x)$ i $\bar{h}(x) = h_0(x)$ i $g(x)$ és mònic.

Que K sigui complet respecte una valoració no trivial, significa que la completació de K respecte la mètrica induida per aquesta valoració es K mateix.

Corol·lari 8.10. *Sigui* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$ *un irreductible, llavors*

$$\max\{|a_n|, |a_{n-1}|, \ldots, |a_0|\} = \max\{|a_n|, |a_0|\},$$

Demostració. L'enunciat és trivial per $n \leq 1$. Suposem $n \geq 2$, en cas contrari, existeix un natural $1 \leq m \leq n-1$ tal que

$$|a_m| > \max\{|a_n|, |a_0|\}.$$

Considerem que m és el més gran amb aquesta propietat. El polinomi $a_m^{-1} f(x)$ té coeficients en $R[x]$, i la seva reducció g_0 en $k[x]$ és mònic de grau m. Considerem $h_0(x) = 1$. Pel Lema de Hensel $a_m^{-1} f(x)$ factoritza en $R[x]$ com $a_m^{-1} f(x) = g(x)h(x)$ amb $\deg(g) = m$. Això contradiu el fet que $f(c)$ és irreductible. □

9 Apèndix III : Ramificacions

9.1 Ramificacions

Sigui L/K una extensió de cossos finita, per (8.8) sabem que podem estendre una valoració v de K en L per

$$v(\alpha) = \frac{1}{n} v(\mathrm{Nr}_{L/K}(\alpha)), \quad \alpha \in L$$

Si suposem que v és una valoració discreta en K, és a dir $v(K^\times) = \mathbb{Z}$, llavors $v(L^\times) \subset \frac{1}{n}\mathbb{Z}$, més en concret

$$v(L^\times) = \frac{1}{e}\mathbb{Z}, \quad \text{tal que } e|n$$

Definició 9.1. *El número $e = e(L/K) \geq 1$ s'anomenra l'índex de ramificació de L/K. L'extensió L/K es diu que ramifica totalment si $e = n$, i no ramifica quan $e = 1$. Si la caracterísitca $p \nmid e$ es parta d'una ramificació moderada, en cas constrari, $p|e$, ramificació salvatje.*

Denotem per R_K, R_L l'anell d'enters de K, L respectivament, M_K, M_L els seus respectius ideals maximals. Escriurem $k = R_K/M_K$ i $l = R_L/M_L$.

Està clar que $M_K = R_K \cap M_L$, per tant l/k és una extensió de cossos.

Definició 9.2. *Denotem per grau residual per*

$$f(L/K) = [l : k]$$

Teorema 9.3. *Amb la notació introduida en aquesta secció, tenim*

1. *R_L és la clausura entera de R_K*
2. *$M_K R_L = M_L^e$*
3. *$[L : K] = e(L/K)f(L/K)$*

Demostrem 1 i 2

Demostració.

1. Suposem $\alpha \in L$ és enter sobre R_K. Llavors $\mathrm{Nr}_{L/K}(\alpha) \in R_K$, per tant $\frac{1}{n} v(\mathrm{Nr}_{L/K}(\alpha)) \geq 0$ el que siginifica $\alpha \in R_L$. Recíprocament, suposem $\alpha \in R_L$, i.e. $v_L(\alpha) \geq 0$. Sigui $m(x) \in K[X]$ el polinomi mínim de α en K. Per definició de l'extensió de la valoració v en L el terme independent de $m(x)$ està en R_K. Llavors, pel corol·lari (8.8) $m(x) \in R_K[x]$, per tant α és enter sobre R_K.
2. Per definició $v(\pi_L) > 0$ genera $v(L^\times)$, llavors $v_L(\pi_L) = \frac{1}{e}$. Per altra banda $v(\pi_L) = 1$. Llavors $u = (\pi_L)^e/\pi_K$ és una unitat (la seva valoració és zero) per tant $(\pi_L)^e$ i (π_K) generen el mateix ideal en R_L, per tant $M_L^e = (\pi_L)^e = \pi_K R_L = M_K R_L$.

□

Teorema 9.4. *Sigui L/K una extensió finita de grau n. Llavors L/K ramifica totalment si i només si $L = k(\alpha)$ on $\alpha \in L$ és una arrel d'un polinomi Eisenstein de grau n.*

Observació 9.5. *Una conseqüència d'aquest teorema, és que si $K/\mathbb{F}_q(x)$ és una extensió finita, llavors R_L, R_K són dominis de Dedekind per la proposició (7.22) i la transitivitat de ser enter.*

Per aquesta demostració necessitem saber que si $f(x) = x^n + a_{n-1}x^{n-1} + \ldots a_1 x + a_0$ és polinomi Eisenstein, tal que $v(a_0) = 1$ llavors $v(\alpha) = \frac{1}{n}$ per les seves arrels. Aquest és un resultat que s'obté d'aplicar el Polígon de Newton al polinomi f.

Demostració. Sigui $f(x) \in K[x]$ un polinomi Eisenstein de grau n. Sigui α una arrel de $f(x)$, sabem que compleix $v(\alpha) = \frac{1}{n}$. Per tant $[K(\alpha) : K] = n$ i $n|e(K(\alpha)/K)$, llavors $e(K(\alpha)/K) = n$ i $K(\alpha)/K$ ramifica completament.

L'altre implicació requereix el polígon de Newton i no en fem la demostració.

□

9.2 Ramificacions

Considerem $\mathbb{F}_q$ un cos de $q = p^n$ elements, denotem per $A = \mathbb{F}_q[T]$ l'anell de polinomis i per $F = \mathbb{F}_q(T)$ el cos de fraccions de A. Considerem K/F una extensió finita, i B la clausura entera de A en K.

Recordem que en un domini de Dedekind R tot ideal no nul descompon de manera única en productes d'ideals primers. Donat un ideal primer $\mathfrak{p} \subset R$ podem definit una valoració, $\mathrm{ord}_\mathfrak{p}$: donat $a \in R$ descomposem (a) en ideals primers i definim $\mathrm{ord}_\mathfrak{p}(a)$ com l'exponent de $\mathfrak{p}$ en aquesta descomposició.

Per la proposició (7.22) l'anell B és un domini de Dedekind. Per tant, donat un primer $\mathfrak{q} \subset B$ podem considerar $\mathrm{ord}_\mathfrak{q}$, s'esten a K mitjançant $\mathrm{ord}_\mathfrak{q}(a/b) = \mathrm{ord}_\mathfrak{q}(a) - \mathrm{ord}_\mathfrak{q}(b)$

Ara bé, sigui $\mathfrak{p} = (P) \subset A$ un ideal primer, considerem $\mathfrak{P} = \mathfrak{p}B$ i la seva descomposició en ideals primers, en B

$$\mathfrak{P} = \mathfrak{q}_1^{e_1} \cdot \ldots \cdot \mathfrak{q}_r^{e_r}.$$

Diem que els primers $\mathfrak{q}_i$ viuen adalt de $\mathfrak{p}$ i que $\mathfrak{p}$ viu abaix dels primers $\mathfrak{q}_i$. A més, $\mathrm{ord}_\mathfrak{q}$ esten ord_P si i només si $\mathfrak{P}$ viu sobre $\mathfrak{p}$. De fet, tota extensió de ord_P és d'aquesta forma, mòdul equivalència.

Proposició 9.6. *Tot primer $\mathfrak{P}$ de B viu a sobre un únic primer $\mathfrak{p}$ de A. Tot ideal primer $\mathfrak{P}$ viu sota un nombre finit d'ideals primers de B. Per acabar, $\sum_{i=1}^{r} e_i f_i = n$, on n és el grau de l'extensió K/F; e_i és l'índex de ramificació i f_i el grau relatiu de $\mathfrak{q}_i$ sobre $\mathfrak{p}$. Aquest últim es defineix com la deminsió de $B_{\mathfrak{P}_i}/\mathfrak{P}_i$ sobre $A_\mathfrak{p}/\mathfrak{p}$.*

Veugeu [1], secció 7 o [7] sobre ramificacions.

10 Apèndix IV : Global Fields

Considerem $K = F(T)$ un cos de funcions, denotem per $A = F[T]$ l'anell de polinomis. Considerem L/K una extensió finita.

Definició 10.1. *Un primer P en K és un anell de valoració discreta R amb ideal maximal P de manera que $F \subset R$.*

Denotem per ord_P la valoració associada al primer P, en K. El grau de P serà $\deg(P) = [R/P : F]$.

Exemple 10.2. *Considerem $K = \mathbb{F}_q(T)$. Sabem que totes les valoracions són equivalents a ord_P per un irreductible mònic $P \in A$ o bé v_∞.*

Llavors tots els anells de valoracions són A_P o bé $\mathbb{F}_q(\frac{1}{T})$. Per tant, tots els primers són de la forma

$$\{P^l(x)\frac{f(x)}{g(x)} : l \geq 1 \ i \ P \nmid fg\}$$

o bé

$$\{f(1/T) : f \in A, \deg f \geq 1\}$$

Observació 10.3. *La valoració ord_P està beh definida en K. Ja que està ben definida en R, i com el cos de fraccions de R és K llavors, $\alpha \in K$ s'escriu $\alpha = \frac{f}{g}$ per $f, g \in R$. Aleshores $ord_P(\alpha) = ord_P(f) - ord_P(g)$.*

Observació 10.4. *El grau* $\deg(P)$ *és un nombre finit. Sigui $y \in P \setminus F$, llavors $[R/P : F] \leq [K : F(y)]$. Considerem $u_1, ..., u_m \in R$ de manera que $\overline{u}_1, ..., \overline{u}_n \in R/P$ siguin linealment independents sobre F. Afirmem que $u_1, \dots u_n$ són linealment indepents sobre $F(y)$. Per reducció a l'absurd suposem que existeixen $f_1(y), \dots, f_n(y) \in \mathbb{F}_q(y)$ de manera que*

$$f_1(y)u_1 + \ldots + f_n(y)u_n = 0$$

podem suposar, sense pèrdua de generalitat, que no tots els $f_i(y)$ són múltplies de y. Reduint mòdul P obtenim que no tots els $\overline{f_i}$ són zero, i per tant $\overline{u_1}, \dots, \overline{u_m}$ no són linealment independents.

Exemple 10.5. *Si $K = \mathbb{F}_q(T)$, com hem vist els primers de K corresponen a un irreductible $P \in A$ o bé ∞. Llavors el grau d'aquests primers és* $\deg(P)$ *i* $\deg(\infty) = 1$.

Efectivament, tots els anells de valoració discreta són: A_P o $\mathbb{F}_q(1/T)$, llavors $\mathfrak{p} = P \cdot A_P$ és l'ideal maximal. Llavors $[A_\mathfrak{p} : \mathbb{F}_q] = \deg P$ i en cas de l'infinit és 1.

Definició 10.6. *Denotem per $\mathcal{D}_L$ al grup abelià lliure generat pels primers de K. Per tant, un element $D \in \mathcal{D}_K$ l'escreiurem com*

$$D = \sum_P a(P)P$$

on la suma recorre als primers P de K i tots els $a(P) \in \mathbb{Z}$ són zero, exceptuant un nombre finit. Considerem el morfisme grau $\mathcal{D}_K \to \mathbb{Z}$

$$\deg(D) = \sum_P a(P)\deg(P)$$

Al nucli d'aquest morfisme, el grup de divisors de grau zero, es denota per $\mathcal{D}_K^0$.

Donat $a \in K^\times$ definim el divisor de a, (a), per $\sum_P v_P(a)P$. També s'anomena divisor principal. A més,

$$(a)_0 = \sum_{P, v_P(a)>0} v_P(a)P, \qquad (a)_\infty = -\sum_{P, v_P(a)<0} v_P(a)P$$

s'anomenen els zeros de a, i els pols de a, respectivament.

Proposició 10.7. *Sigui $a \in K^\times$. Llavors $ord_P(a) = 0$ casi per tot P. Segonament, $(a) = 0$ si i només si $a \in F^\times$. Finalment $\deg(a)_0 = \deg(a)_\infty = [K : F(a)]$. Es segueix que $\deg(a) = 0$.*

Demostració. **(Sketch)**

Es veu fàcil que $a \in F^\times$ si i només si $(a) = 0$. Per tant, sigui $a \in K^\times \setminus \mathbb{F}_q^\times$. Com hem vist, $[K : F(a)]$ és finit. Considerem R la clausura entera de $F[a]$ en K.

Es pot veure que R és un domini de Dedekind, veure [1] secció 5 per una demostració; llavors $aR = \mathfrak{P}_1^{e_1} \cdot \ldots \cdot \mathfrak{P}_g^{e_g}$ per la descomposició única en ideals primers. Considerem els anells local $R_{\mathfrak{P}_i}$ i denotem per P_i els seus ideals maximals. Aleshores $\text{ord}_{P_i}(a) = e_i$.

Es demostra que $\{P_1, \ldots, P_g\}$ és el conjunt de tots els zeros de a. Aplicant el mateix raonament a a^{-1} obtindrem tots els pols de a.

Aplicant la proposició (9.6) obtenim $[K : F(a)] = \deg(a)_0 = \deg(a)_\infty$.

□

Definició 10.8. *Dos divisors D_1, D_2 són linealment equivalents, $D_1 \sim D_2$ si $D_1 - D_2 = (a)$, per $a \in K^\times$. Definim la classe de divisors $Cl_K = \mathcal{D}_K/\mathcal{P}_K$.*

Observació 10.9. *Per la proposició (10.7) concloem que dos divisors d'una mateixa classe tenen el mateix grau. Per tant el morfisme grau $Cl_K \to \mathbb{Z}$ està ben definit. Denotarem el seu nucli per Cl_K^0. Es pot comprovar, veure [1, pàg. 51] que $|Cl_K^0| = h_K$ és finit, i es diu el nombre de classe.*

Definició 10.10. *Diem que un divisor $D = \sum_P a(P)P$ és efectiu si $a(P) \geq 0$, ho denotarem per $D \geq 0$. També escriurem $D_1 \geq D_2$ si $D_1 - D_2$ és efectiu. Definim*

$$L(D) = \{x \in K^\times : (x) + D \geq 0\} \cup \{0\}$$

Lema 10.11. *El conjunt $L(D)$ té estructura d'e.v. sobre $\mathbb{F}_q$ i té dimensió finita. Denotem per $l(D)$ a la seva dimensió.*

Teorema 10.12. ***(Riemann-Roch)*** *Existeix un enter $g \geq 0$ i una classe de divisor $\mathcal{C}$ de manera que per $C \in \mathcal{C}$ i $A \in \mathcal{D}_K$ es compleix*

$$l(A) = \deg(A) - g + 1 + l(C - A)$$

Definició 10.13. *Aquest natural g, també escrit g_K, s'anomena el gènere de K i està unívocament determinat per K.*

Per una demostració d'aquests resultats vegueu [1] secció 5.

Teorema 10.14. ***(Teorema Reimann-Hurwitz)***

Sigui L/K una extensió separable, finita, geomètrica de cossos de funcions. Llavors

$$2g_L - 2 = [L : K](2g_K - 2) + \deg D_{L/K}$$

en particular,

$$2g_L - 2 \geq [L : K](2g_K - 2) + \sum_{\mathfrak{P}} (e(\mathfrak{B}/P) - 1) \deg_L \mathfrak{P}$$

S'anomena divisor de ramificació al divisor $D_{L/K}$; resulta que un primer $\mathfrak{P}$ de L està remificat sobre K si i només si apareix en el suport de $D_{L/K}$ (el suport d'un divisor són tots els primers amb coeficient no nul). A més, es compleix que

$$D_{L/K} \geq \sum_{\mathfrak{B}} (e(\mathfrak{P}/P) - 1)\mathfrak{P}$$

on $\mathfrak{P}$ recòrrer tots els primers de L i P indica l'únic primer de K que està sota $\mathfrak{P}$. I l'anterior desigualtat és una igualtat, quan la característica del cos és zero o bé tot primer ramifica moderadament en L.

La conjectura ABC afirma: doants $a, b, c \in \mathbb{N}$ coprimers dos a dos i es compleix $a + b = c$. Llavors per tot $\epsilon > 0$ hi ha una constant M_ϵ tal que

$$\max(|a|, |b|, |c|) \leq M_\epsilon \Big(\prod_{p|abc} p \Big)^{1+\epsilon}.$$

Es pot donar un enunciat equivalent però en $\mathbb{Q}$. Considerem $u, v \in \mathbb{Q}^\times$ amb $u + v = 1$. Llavors per tot ϵ existeix una constant m_ϵ tal que

$$\max(\mathrm{ht}(u), \mathrm{ht}(v)) \leq m_\epsilon + (1 + \epsilon) \sum_{p|ABC} \ln(p)$$

on hem denotat per $\mathrm{ht}(u) = \max(\ln n, \ln m)$ amb $u = \frac{m}{n}$ i m, n coprimers.

Volem definir una altura en cossos de funcions. Sigui $u \in K^\times$, amb K un cos de funcions; si denotem per A, B el zero divisor de u i el divisor polar de u, respectivament, llavors es compleix

$$\deg A = \deg B = [K : F(u)]$$

Definició 10.15. *Donat $u \in K^\times$ definim $\deg u = [K : F(u)]$. Si M és la extensió separable maximal de $F(u)$ en K, denotem per $\deg_s u = [M : F(u)]$.*

Teorema 10.16. ***(Teorema - ABC)***

Sigui K un cos de funcions amb F cos de constants perfecte. Si $u, v \in K^\times$ i $u + v = 1$. Llavors,

$$\deg_s u = \deg_s v \leq 2g_K - 2 + \sum_{P \in Supp(A+B+C)} \deg_K P$$

On A, B són els zero divisors de u i v en K respectivament, C és el divisor en comú dels divisors polars en K.

Abans de provar el teorema necessitem un resultat. Sigui K/L una extensió finita de cossos de funcions. Denotem per $\mathcal{D}_K$ i $\mathcal{D}_L$ el grup dels divisors. Definim,

- $i_{L/K} : \mathcal{D}_K \to \mathcal{D}_L$ definit per $i_{L/K}(P) = \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)\mathfrak{P}$ per tot primer P de L, i extenem per linealitat. On la suma és sobre els primers $\mathfrak{P}$ de K que estan sobre P.

Es compleix $\deg_L(i_{L/K}(A)) = \frac{[L:K]}{[E:F]} \deg_K A$ per tot divisor de K, on F és el cos de les constants de K i E el cos de les constants de L.

Demostració. Escrivim $k = F(u)$. Considerem primer el cas K/k una extensió separable, per una demostració en el cas complet veure [2] pàgina 105-106. Si $n = \deg u = [K : k]$, llavors el teorema de Reimann-Hurwitz implica

$$2g_K - 2 \geq -2n + \sum_{\mathfrak{P}} (e(P/\mathfrak{P} - 1) \deg_K P,$$

a més hem usat que el gènere de k és zero, al ser u trascendet sobre F. Una propietat dels cossos perfecte, llavors un primer ramifica si i només si el seu índex ramificació és major que 1. Si el seu índex de ramificació fos 1 no constribueix en la suma.

En $k = F(u)$ considerem tres primers, $\mathfrak{P}_0$, $\mathfrak{P}_1$ i $\mathfrak{P}_\infty$ que són els zero divisors en k de $u, v = 1 - u$ i $1/u$, respectivament. Llavors $A = i_{K/k}(\mathfrak{P}_0)$, $B = i_{K/k}(\mathfrak{P}_1)$ i $C = i_{K/k}(\mathfrak{P}_\infty)$. Aleshores,

$$\sum_{P \in \mathrm{sepp}(A)} (e(P/\mathfrak{P}_0) - 1) \deg_K P = \deg_K(i_{K/k}) - \sum_{P \in \mathrm{Supp}(A)} \deg_K P.$$

Pel que hem comentat abans i per la proposició (9.6), $\deg_K(i_{K/k}\mathfrak{P}_0) = [K : k] \deg_k \mathfrak{P}_0 = n$. Per tant la suma d'adalt simplement és n menys la suma dels graus dels primers del suport de A. S'obté les mateixes desigualtats per B, C i per tant es conclou

$$2g_K - 2 \geq n - \sum_{P \in \mathrm{supp}(A+B+C)} \deg_K P$$

□

Per una prova en el cas general veure [1] secció 7.

11 Apèndix V : Polinomis additius i $\mathbb{F}_q$-lineals

Com és usual $\mathbb{F}_q(T)$ denotarà el cos finit de $q = p^n$ elements i K denotarà un cos de característica $p > 0$.

Definició 11.1. *Sigui K un cos, es diu que un cert polinomi $P(X) \in K[X]$ és additiu si compleix $P(X+Y) = P(X) + P(Y)$ en $K[X,Y]$. Si a més, $\mathbb{F}_q \subset K$ i es compleix $P(cX) = cP(X)$ diem que és $\mathbb{F}_q$-lineal.*

Exemple 11.2. *En $\mathbb{F}_q[T][X]$ considerem el polinomi $P(X) = X^q + TX$, llavors*

$$P(X+Y) = (X+Y)^q + T(X+Y) = X^q + Y^q + TX + TY = P(X) + P(Y)$$

$$P(cX) = (cX)^q + T(cX) = c(X^q + TX) = cP(X),$$

és un polinomi $\mathbb{F}_q$ lineal.

Els següents dos resultats caracteritzen els polinomis $\mathbb{F}_q$-lineals.

Teorema 11.3. *Sigui K un cos, llavors $P(X) \in K[X]$ és un polinomi $\mathbb{F}_q$-lineal si i només si les seves arrels $W \subset \overline{K}$ formen un $\mathbb{F}_q$-subespai vectorial.*

Demostració. Si $a, b \in W$ i $\lambda \in \mathbb{F}_q$ llavors $P(a + \lambda b) = P(a) + \lambda P(b) = 0 + 0 = 0$, a més $0 \in W$ ja que $P(0) = P(0) + P(0) = 2P(0)$. Així W és un subespai vectorial.

Ara suposem que W és un $\mathbb{F}_q$-subespai vectorial de $\overline{K}$. Veguem primer que $P(X)$ és additiu, per això demostrarem que $H(Y) = P(X+Y) - P(X) - P(Y) \in K[X][Y]$ és el polinomi zero. Fixem-nos que $\deg_Y(H(X,Y)) < \deg_Y(P(Y))$, vists com a polinomis en Y amb coeficients en $K[X]$

Sigui $a \in W$ qualsevol element, llavors $H(X,a) = P(X+a) - P(X) - P(a)$ el podem veure com un polinomi en $K[X]$, de nou es compleix la desigualtat $\deg_X(H(X,a)) < \deg_X(P(X))$. Eevaluant en $b \in W$ obtenim $P(b+a) - P(b) - P(b) = 0$; és a dir $H(X,a)$ té $|W| = \deg_X(P(X))$ arrels i necessàriament $H(X,a) = 0$ per tot $a \in W$, de nou $H(X,Y)$ té $|W|$ arrels, però ara vist com un polinomi en la variable Y, i per tant $H(X,Y) = 0$.

Ens falta per veure que és $\mathbb{F}_q$-lineal. Que $F(0 \cdot X) = 0 \cdot F(0) = 0$ és obvi, considerem $\lambda \in \mathbb{F}_q$ diferent de zero, com hem suposat que W és $\mathbb{F}_q$-e.v. llavors l'acció de multiplicar $\lambda \cdot w$, amb $w \in W$, permuta els elements de W, aleshores

$$P(\lambda X) = \prod_{w \in W} (\lambda X - w) = \prod_{w \in W} (\lambda X - \lambda w) = \lambda^{|W|} \prod_{w \in W} (X - w) = \lambda P(X)$$

En la última igualtat s'ha fet servir que $|W|$ és una potència de q, per tant $\lambda^{|W|} = \lambda$. □

Teorema 11.4. *Sigui K un cos, llavors $P(X) \in K[X]$ és un $\mathbb{F}_q$-lineal si i només si és de la forma $P(X) = \sum_{i=0}^{n} c_i X^{q^i}$ amb $c_i \in K$.*

Demostració. Està clar que si $P(X) = \sum_{i=0}^{n} c_i X^{q^i}$ llavors és $\mathbb{F}_q$-lineal.

Per la implicació contrària, derivant $P(X+Y) = P(X) + P(Y)$ respecte Y i imposant $Y = 0$ s'obté $P'(X) = P'(0)$, és a dir $P'(X)$ és una constant que només passa si $P(X) = \sum_{i=0}^{n} c_i X^{p^i}$. Llavors falta que en l'anterior suma només hi apareixen potències de q. Si $\lambda \in \mathbb{F}_q$ llavors $0 = P(\lambda X) - \lambda P(X) = \sum_{i=0}^{\deg P} c_i(\lambda^{p^i} - \lambda) X^{p^i}$ així per cada $i \leq \deg P$ amb $c_i \neq 0$ tenim $\lambda^{p^i} = \lambda$ i necessàriament p^i ha de ser una potència de q. □

Corol·lari 11.5. *Si $P(X), Q(X) \in K[X]$ són $\mathbb{F}_q$-lineals llavors $P(X) + Q(X)$ i $P(Q(X))$ són $\mathbb{F}_q$-lineals i a més $Q(X) | P(Q(X))$.*

Corol·lari 11.6. *Siguin $P(X), Q(X) \in K[X]$ tal que $P(Q(X)) = Q(P(X))$ llavors si $\gamma \in \overline{K}$ és una arrel de $P(X)$ llavors $Q(\gamma) \in \overline{K}$ és també arrel de $P(X)$.*

Demostració. Com $P(\gamma) = 0$ llavors $0 = Q(0) = Q(P(\gamma)) = P(Q(\gamma))$ □

Referències

[1] Michael Rosen (2000) Llibre, Number Theory in Function Fields.

[2] Michael Atiyah (1994) Llibre, Introductions to Commutative Algebra.

[3] Laurent Denis (1994) Article, Le théorème de Fermat-Goss.

[4] Laurent Denis (1994) Article, Altures.

[5] David Goss Llibre, Basic Structures of Function Field Arithmeitc.

[6] David Goss (1982) Article, On a Fermat Equation Arising in the Arithmetic Theory of Function Fields.

[7] Mihram Papikian Llibre, Drinfield Modules.

[8] Keith Conrad Article, Carlitz Module

[9] Anthony Várilly, Article, Dirichlet's Theorem on Arithmetic Progressions

[10] Nigel Boston, Article, The Proof of Fermat's Last Theorem