UAB
Universitat Autònoma de Barcelona

Sobre punts de torsió de mòduls de Drinfeld de rang 2

Autor:
David Olivar Lacambra

Tutor:
Francesc Bars Cortina

Treball Final de Grau
Departament de Matemàtiques
Facultat de Ciències

Bellaterra, 12 de juliol de 2022

Índex

Notació **1**

1 Introducció **2**

2 Propietats bàsiques dels mòduls de Drinfeld **3**

2.1 Polinomis $\mathbb{F}_q$-lineals 3

2.2 Mòduls de Drinfeld 4

2.3 Morfismes de mòduls de Drinfeld 5

2.4 Punts de torsió 7

2.5 Emparellament de Weil 9

2.6 Isomorfismes 9

2.7 Reduccions de mòduls de Drinfeld 10

3 Mòduls de Drinfeld finits **13**

3.1 L'endomorfisme de Frobenius 13

3.2 Polinomi característic 13

4 El grup $\mathrm{GL}_2(\mathbb{F}_q)$ **16**

4.1 Classes de conjugació 16

4.2 Subgrups 16

5 Mòduls de Drinfeld sobre cossos globals **20**

5.1 El tipus de conjugació de $\mathrm{Frob}_{\mathfrak{P}}$ 20

5.2 El mòdul de Carlitz 21

5.3 Exemples de cossos de divisió de mòduls de Drinfeld 22

5.4 Multiplicació complexa 28

Bibliografia **31**

Notació

Presentem les notacions bàsiques que farem servir al llarg del treball:

- n sempre és un enter.
- p sempre és un primer positiu de $\mathbb{Z}$ fixat.
- $\mathbb{F}_q$ és el cos finit de q elements on q és una potència de p.
- $A = \mathbb{F}_q[T]$ és l'anell de polinomis amb indeterminada T i coeficients a $\mathbb{F}_q$.
- $F = \mathbb{F}_q(T)$ és el cos de fraccions de A.
- $\mathfrak{p}$ és un ideal primer arbitrari de A. Per norma general, $\mathfrak{p}$ és mònic.
- $\mathbb{F}_\mathfrak{p}$ és l'anell quocient $A/(\mathfrak{p})$. Notem que $\mathbb{F}_\mathfrak{p} \cong \mathbb{F}_{q^{\deg(\mathfrak{p})}}$ és un cos ja que $(\mathfrak{p})$ és un ideal maximal de A.
- $v_\mathfrak{p}$ és la valoració $\mathfrak{p}$-àdica normalitzada sobre F.
- $|\cdot|_\mathfrak{p}$ és el valor absolut associat a $v_\mathfrak{p}$.
- $F_\mathfrak{p}$ és la completació de F respecte $|\cdot|_\mathfrak{p}$.
- $A_\mathfrak{p}$ és l'anell d'enters de $F_\mathfrak{p}$, o alternativament, $A_\mathfrak{p} = \varprojlim_{n\geq 1} A/(\mathfrak{p}^n)$.

1 Introducció

L'anell de polinomis sobre un cos finit $\mathbb{F}_q[T]$ comparteix moltes propietats amb $\mathbb{Z}$, per exemple ambdós són dominis euclidians, tenen una quantitat d'unitats finita i de primers infinita, l'anell quocient respecte d'un ideal diferent de zero és finit, etc. A partir d'aquest fet sorgeixen conceptes anàlegs entre la teoria de nombres clàssica i la de cossos funcionals, dels quals destaquem els mòduls de Drinfeld que es poden veure com una analogia de les corbes el·líptiques. De fet, Vladimir Drinfeld en l'influent article [**Dri74**] que els introdueix els va anomenar mòduls el·líptics. Concretament, els mòduls de Drinfeld de rang 2 són els que tenen una major similitud amb les corbes el·líptiques, i per això, ens centrarem en el seu estudi.

Una diferència important entre les corbes el·líptiques i els mòduls de Drinfeld és que els últims essencialment són objectes d'àlgebra lineal, i per tant, en aquest treball els presentarem sense cap menció de geometria algebraica. L'objectiu d'aquest treball serà introduir el concepte de mòdul de Drinfeld i fer una recopilació de les propietats més rellevants d'aquests per després poder explicar el comportament dels punts de torsió i les extensions associades a aquests.

En el Capítol 2 començarem amb una discussió de l'anell de polinomis twistats i la seva relació amb els polinomis $\mathbb{F}_q$-lineals, que és fundamental en la teoria de mòduls de Drinfeld. Després definirem la noció de mòdul de Drinfeld i estudiarem els seus morfismes, submòduls de torsió i propietats de reducció. Tot això es farà amb mòduls de Drinfeld de rang arbitrari i sobre un cos vàlid qualsevol.

En el Capítol 3 estudiarem els mòduls de Drinfeld sobre cossos finits i ens centrarem en el càlcul del polinomi característic d'un mòdul de Drinfeld de rang 2.

En el Capítol 4 parlarem del grup $\mathrm{GL}_2(\mathbb{F}_q)$, les seves classes de conjugació i els seus subgrups més importants.

Un cop vist tot això, en el Capítol 5 estudiarem els mòduls de Drinfeld sobre cossos globals. Començarem parlant de mòduls de Drinfeld de rang 1 i, en particular, del mòdul de Carlitz el qual precedeix als mòduls de Drinfeld per quaranta anys i va ser introduït per Leonard Carlitz a [**Car35**]. A continuació construirem diversos exemples explícits de cossos de divisió associats a torsions de mòduls de Drinfeld i, per últim, discutirem el fenomen de multiplicació complexa.

2 Propietats bàsiques dels mòduls de Drinfeld

2.1 Polinomis $\mathbb{F}_q$-lineals

Definició 2.1.1. Sigui K una extensió de cossos de $\mathbb{F}_q$, diem que un polinomi $f(x) \in K[x]$ és $\mathbb{F}_q$-lineal si és additiu, és a dir $f(x+y) = f(x) + f(y)$ a $K[x,y]$, i si $f(\alpha x) = \alpha f(x)$ per tot $\alpha \in \mathbb{F}_q$.

Lema 2.1.2 ([Pap23], Lema 3.1.4)**.** *Un polinomi $f(x) \in K[x]$ és $\mathbb{F}_q$-lineal si i només si és de la forma*

$$f(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

per algun $n \geq 0$ i $a_0, \ldots, a_n \in K$.

Per una banda, si $f(x) \in K[x]$ és un polinomi $\mathbb{F}_q$-lineal, és obvi que 0 sempre és una arrel de $f(x)$. A més, si λ_1 i λ_2 són arrels de $f(x)$, és fàcil comprovar que $\alpha_1\lambda_1 + \alpha_2\lambda_2$ també ho és per tot $\alpha_1, \alpha_2 \in \mathbb{F}_q$. Com a conseqüència, $\ker(f)$ forma un $\mathbb{F}_q$-subespai vectorial de dimensió finita de $\overline{K}$. Per altra banda, tenim el següent:

Lema 2.1.3 ([Pap23], Lema 3.1.5)**.** *Sigui W un $\mathbb{F}_q$-subespai vectorial de K, llavors*

$$f(x) = \prod_{w \in W} (x - w) \in K[x]$$

és $\mathbb{F}_q$-linear i separable.

Aleshores com la composició de polinomis $\mathbb{F}_q$-lineals és $\mathbb{F}_q$-lineal, denotant $+$ i $\circ$ com la suma i la composició habituals respectivament, tenim el següent anell amb unitat no commutatiu:

$$(K\langle x\rangle, +, \circ) = \Big\{ \sum_{i=0}^{n} a_i x^{q^i} \mid n \geq 0 \text{ i } a_0, \ldots, a_n \in K \Big\}.$$

Exemple 2.1.4. Siguin $f(x) = x + ax^q + bx^{q^2} \in K\langle x\rangle$ i $g(x) = x^q \in K\langle x\rangle$, observem que

$$\begin{aligned}
(f \cdot g)(x) &= x^{q+1} + ax^{2q} + bx^{q^2+q} \notin K\langle x\rangle, \\
(f \circ g)(x) &= x^q + ax^{q^2} + bx^{q^3} \in K\langle x\rangle, \\
(g \circ f)(x) &= x^q + a^q x^{q^2} + b^q x^{q^3} \in K\langle x\rangle.
\end{aligned}$$

A més, $f \circ g \neq g \circ f$ a no ser que $a, b \in \mathbb{F}_q$.

Definició 2.1.5. L'anell de polinomis twistats de K amb indeterminada τ és

$$(K\{\tau\}, +, \cdot) = \Big\{ \sum_{i=0}^{n} b_i \tau^i \mid n \geq 0 \text{ i } b_0, \ldots, b_n \in K \Big\}$$

on $+$ és la suma ordinària i definim el producte $\cdot$ de manera que $(a\tau^i) \cdot (b\tau^j) = ab^{q^i}\tau^{i+j}$.

Lema 2.1.6. *L'aplicació $\iota : K\{\tau\} \to K\langle x\rangle$ donada per*

$$\iota\Big(\sum_{i=0}^{n} a_i \tau^i\Big) = \sum_{i=0}^{n} a_i x^{q^i}$$

és un isomorfisme de $\mathbb{F}_q$-àlgebres.

Com ι és un isomorfisme natural, per abús de notació lleuger, normalment escriurem $f(x)$ com $\iota(f(\tau))$.

Demostració. Clarament ι és una aplicació bijectiva. Ara siguin $f(\tau), g(\tau) \in K\{\tau\}$ i $\alpha \in \mathbb{F}_q$, $\iota(f(\tau)+g(\tau)) = f(x)+g(x) = \iota(f(\tau))+\iota(g(\tau))$ i $\iota(\alpha f(\tau)) = f(\alpha x) = \alpha f(x) = \alpha \cdot \iota(f(\tau))$. Per últim, només cal veure que ι satisfà la propietat multiplicativa per monomis de $K\{\tau\}$ per trobar que ι és un morfisme de $\mathbb{F}_q$-àlgebres. Siguin $a\tau^i, b\tau^j \in K\{\tau\}$ amb $a, b \in K$ i $i, j \geq 0$ enters, aleshores $\iota(a\tau^i) \circ \iota(b\tau^j) = a(bx^{q^j})^{q^i} = ab^{q^i}x^{q^{i+j}} = \iota(ab^{q^i}\tau^{i+j}) = \iota((a\tau^i)\cdot(b\tau^j))$. □

Definició 2.1.7. Sigui $f(\tau) = \sum_{i=h}^{n} a_i\tau^i$ amb $n \geq h \geq 0$ tals que $a_h \neq 0$ i $a_n \neq 0$, llavors l'altura de f és $\mathrm{ht}(f) = h$ i el grau és $\deg(f) = n$. Posem formalment que $\mathrm{ht}(0) = +\infty$ i $\deg(0) = -\infty$. Diem que f és separable si $\mathrm{ht}(f) = 0$ i inseparable en cas contrari. Això últim és equivalent a dir que $f(x)$ és separable en el sentit polinomial perquè $f'(x) = a_0$.

Siguin $f, g \in K\{\tau\}$ no nuls, veiem que l'altura i el grau compleixen les següents propietats:

$$\begin{aligned} \mathrm{ht}(fg) &= \mathrm{ht}(f) + \mathrm{ht}(g). \\ \mathrm{ht}(f+g) &\geq \min(\mathrm{ht}(f), \mathrm{ht}(g)). \\ \deg(fg) &= \deg(f) + \deg(g). \\ \deg(f+g) &\leq \max(\deg(f), \deg(g)). \end{aligned}$$

Definició 2.1.8. Definim el morfisme $\partial : K\{\tau\} \to K$ donat per

$$\partial(\sum_{i=0}^{n} a_i\tau^i) = a_0$$

com la *derivada*. Notem que $\partial(f) = f'(x)$ per qualsevol $f \in K\{\tau\}$, i per això, f és separable si i només si $\partial(f) \neq 0$.

2.2 Mòduls de Drinfeld

Definició 2.2.1. Un A-cos (K, γ) és una extensió de cossos K sobre $\mathbb{F}_q$ equipat amb un morfisme de $\mathbb{F}_q$-àlgebres $\gamma : A \to K$.

Definim la A-característica de (K, γ) com $\mathrm{car}_A(K, \gamma) = \ker(\gamma)$. Com K és un cos, observem que $\mathrm{car}_A(K, \gamma) = 0$ si γ és injectiva, i si no ho és, $\mathrm{car}_A(K, \gamma) = \mathfrak{p}$ és un primer de A.

Definició 2.2.2. Sigui (K, γ) un A-cos, un mòdul de Drinfeld de rang r sobre K és un morfisme de $\mathbb{F}_q$-àlgebres

$$\begin{aligned} \phi : A &\longrightarrow K\{\tau\} \\ a &\longmapsto \phi_a(\tau) = \gamma(a) + g_1(a)\tau + \cdots + g_n(a)\tau^n \end{aligned}$$

tal que per $a \neq 0$ tenim que $n = r \cdot \deg(a)$ i $g_n(a) \neq 0$.

Observació 2.2.3. Com T genera A com a $\mathbb{F}_q$-àlgebra, ϕ_T determina unívocament a ϕ, i per tant, per definir un mòdul de Drinfeld, només s'han d'escollir $g_1, \ldots, g_r \in K$ amb $g_r \neq 0$ i posar

$$\phi_T(\tau) = \gamma(T) + g_1\tau + \cdots + g_r\tau^r.$$

A més, si $a = \sum_{i=0}^{n} a_i T^i$, llavors

$$\phi_a = \sum_{i=0}^{n} a_i \phi_{T^i} = \sum_{i=0}^{n} a_i \phi_T^i.$$

Exemple 2.2.4. El mòdul de Drinfeld de rang 1 definit per $C_T(\tau) = \gamma(T) + \tau$ és el mòdul de Carlitz. Aquest és el mòdul de Drinfeld més simple. Així, si volem computar $C_{T^2+T+1}(\tau)$, trobem que

$$\begin{aligned} C_{T^2+T+1}(\tau) &= C_{T^2}(\tau) + C_T(\tau) + 1 \\ &= (\gamma(T) + \tau)(\gamma(T) + \tau) + (\gamma(T) + \tau) + 1 \\ &= (\gamma(T)^2 + (\gamma(T)^q + \gamma(T))\tau + \tau^2) + (\gamma(T) + \tau) + 1 \\ &= \gamma(T^2 + T + 1) + \gamma(T^q + T + 1)\tau + \tau^2. \end{aligned}$$

Exemple 2.2.5. Sigui ϕ el mòdul de Drinfeld de rang 2 sobre F donat per $\phi_T(\tau) = T + T\tau + \tau^2$, computem que

$$\begin{aligned} \phi_{2T^2+3}(\tau) &= 2\phi_{T^2}(\tau) + 3 \\ &= 2(T + T\tau + \tau^2)(T + T\tau + \tau^2) + 3 \\ &= (2T^2 + 3) + (2T^{q+1} + 2T^2)\tau + (2T^{q^2} + 2T^{q+1} + 2T)\tau^2 + (2T^{q^2} + 2T)\tau^3 + 2\tau^4. \end{aligned}$$

Observació 2.2.6. Veiem que un mòdul de Drinfeld $\phi : A \to K\{\tau\}$ indueix a K una estructura de A-mòdul via $a * \beta = \phi_a(\beta)$, on $\phi_a(\beta)$ és el polinomi $\mathbb{F}_q$-linear $\phi_a(x)$ avaluat a β. Denotarem aquest A-mòdul com ${}^{\phi}K$.

Lema 2.2.7 ([Pap23], Lema 3.2.11)**.** *Si* $\operatorname{car}_A(K, \gamma) = \mathfrak{p} \neq 0$ *i* ϕ *és un mòdul de Drinfeld de rang* r *sobre* K*, aleshores existeix un enter* $1 \leq H(\phi) \leq r$*, anomenat l'altura de* ϕ*, tal que*

$$\operatorname{ht}(\phi_a) = H(\phi) \cdot \operatorname{ord}_{\mathfrak{p}}(a) \cdot \deg(\mathfrak{p}).$$

Exemple 2.2.8. Siguin $q = 3$ i $K = \mathbb{F}_{\mathfrak{p}} = A/(\mathfrak{p})$ on $\mathfrak{p} = T^2 + 1$ i $\gamma : A \to K$ és la projecció canònica i sigui ϕ el mòdul de Drinfeld de rang 2 definit per $\phi_T(\tau) = \gamma(T) + \tau^2$, calculem que

$$\begin{aligned} \phi_{\mathfrak{p}}(\tau) &= \phi_{T^2}(\tau) + 1 \\ &= (\gamma(T) + \tau^2)(\gamma(T) + \tau^2) + \gamma(1) \\ &= \gamma(T)^2 + \gamma(1) + (\gamma(T)^{3^2} + \gamma(T))\tau^2 + \tau^4 \\ &= -\gamma(T)\tau^2 + \tau^4. \end{aligned}$$

Per tant, $H(\phi) = 1$.

Definició 2.2.9. Sigui ϕ un mòdul de Drinfeld de rang 2 sobre K amb $\operatorname{car}_A(K, \gamma) = \mathfrak{p}$, l'invariant de Hasse de ϕ, que denotarem $I(\phi)$, és el coeficient de grau $\deg(\mathfrak{p})$ en variable τ de $\phi_{\mathfrak{p}}(\tau)$.

Lema 2.2.10. *Usant aquesta notació, tenim que* $I(\phi) = 0$ *si i només si* $H(\phi) = 2$.

Demostració. Pel Lema 2.2.7, sabem que $1 \leq H(\phi) \leq 2$. Aleshores si $I(\phi) \neq 0$ és clar que $H(\phi) = 1$, i si $I(\phi) = 0$, $H(\phi) > 1$, és a dir, $H(\phi) = 2$. □

2.3 Morfismes de mòduls de Drinfeld

Definició 2.3.1. Un morfisme $u : \phi \to \psi$ de mòduls de Drinfeld sobre K és un polinomi $u \in K\langle x \rangle$ tal que $u\phi_a = \psi_a u$ per tot $a \in A$. En particular, $u : {}^{\phi}K \to {}^{\psi}K$ és un morfisme de A-mòduls, és a dir, el diagrama

$$\begin{array}{ccc} K & \xrightarrow{u} & K \\ {\scriptstyle \phi_a}\downarrow & & \downarrow{\scriptstyle \psi_a} \\ K & \xrightarrow{u} & K \end{array}$$

commuta per tot $a \in A$. Un morfisme $u : \phi \to \psi$ diferent del zero és una isogènia.

Definició 2.3.2. El grup de tots els morfismes de ϕ a ψ sobre K el denotem per $\mathrm{Hom}_K(\phi, \psi)$. L'anell d'endomorfismes de ϕ és $\mathrm{End}_K(\phi) = \mathrm{Hom}_K(\phi, \phi)$ i és un subanell de $K\{\tau\}$ amb la suma i la composició. Els elements invertibles de $\mathrm{End}_K(\phi)$ formen el grup d'automorfismes de ϕ i l'escrivim com $\mathrm{Aut}_K(\phi)$.

Proposició 2.3.3 ([Pap23], Teorema 3.3.4)**.** *Suposem que $u : \phi \to \psi$ és una isogènia, llavors ocorre que:*

(1) El rang de ϕ és igual al rang de ψ.

(2) $H(\phi) = H(\psi)$.

(3) Si $\mathrm{car}_A(K, \gamma) = 0$, u és separable.

(4) Si $\mathrm{car}_A(K, \gamma) = \mathfrak{p} \neq 0$, aleshores $\deg(\mathfrak{p})$ divideix a $\mathrm{ht}(u)$.

(5) Si $\mathrm{car}_A(K, \gamma) = 0$, el morfisme

$$\begin{aligned} \mathrm{Hom}_K(\phi, \psi) &\longrightarrow K \\ u &\longmapsto \partial(u). \end{aligned}$$

és injectiu. En particular, en aquest cas, $\mathrm{End}_K(\phi)$ és un anell commutatiu.

Teorema 2.3.4 ([Pap23], Teorema 3.3.9)**.** *Siguin ϕ i ψ mòduls de Drinfeld definits sobre K, per qualsevol cos L que contingui K^{sep} la clausura separable de K tenim que*

$$\mathrm{Hom}_L(\phi, \psi) = \mathrm{Hom}_{K^{\mathrm{sep}}}(\phi, \psi).$$

Com a conseqüència, per simplificar la notació escriurem

$$\begin{aligned} \mathrm{Hom}(\phi, \psi) &:= \mathrm{Hom}_{K^{\mathrm{sep}}}(\phi, \psi) = \mathrm{Hom}_{\overline{K}}(\phi, \psi), \\ \mathrm{End}(\phi) &:= \mathrm{End}_{K^{\mathrm{sep}}}(\phi) = \mathrm{End}_{\overline{K}}(\phi), \\ \mathrm{Aut}(\phi) &:= \mathrm{Aut}_{K^{\mathrm{sep}}}(\phi) = \mathrm{Aut}_{\overline{K}}(\phi). \end{aligned}$$

Teorema 2.3.5 ([Pap23], Teorema 3.4.1)**.** *$\mathrm{Hom}_K(\phi, \psi)$ és un A-mòdul lliure de rang $\leq r^2$. En particular, $\mathrm{Hom}(\phi, \psi)$ també ho és.*

Teorema 2.3.6 ([Pap23], Corol·lari 3.4.15)**.** *Sigui ϕ un mòdul de Drinfeld de rang r sobre un cos K amb $\mathrm{car}_A(K, \gamma) = 0$, llavors $F \otimes_A \mathrm{End}_K(\phi)$ és una extensió de cossos de F de grau divisor de r. Concretament, $\mathrm{End}_K(\phi)$ és A-mòdul lliure de rang divisor de r.*

Aquest teorema implica que $\mathrm{End}(\phi)$ és un A-mòdul lliure de rang $\leq r$, cosa que motiva la definició següent:

Definició 2.3.7. Sigui ϕ un mòdul de Drinfeld de rang r sobre un cos K amb $\mathrm{car}_A(K, \gamma) = 0$, diem que ϕ té *multiplicació complexa*, o CM en curt, si $\mathrm{rang}_A(\mathrm{End}(\phi)) = r$.

Observació 2.3.8. Utilitzant la notació anterior, com $A \cong \phi(A) \subseteq \mathrm{End}(\phi)$ ja que $\phi_a\phi_b = \phi_{ab} = \phi_{ba} = \phi_b\phi_a$ per tot $a, b \in A$, $\mathrm{rang}_A(\mathrm{End}(\phi)) \geq 1$. Per això, si r és primer, o bé $\mathrm{End}(\phi) = \phi(A)$ o bé ϕ té multiplicació complexa pel Teorema 2.3.6.

Si $\mathrm{car}_A(K, \gamma) = 0$, usualment $\mathrm{End}(\phi) = \phi(A)$. Donem dos exemples per entendre millor aquest fenomen.

Exemple 2.3.9. Sigui $\phi_T(\tau) = T^2 + (T^q + T)\tau + \tau^2 = (T + \tau)^2$ sobre F, està clar que $\mathrm{car}_A(F, \gamma) = 0$. Observem que $T + \tau \in \mathrm{End}_F(\phi)$ perquè $(T + \tau)\phi_T = (T + \tau)^3 = \phi_T(T + \tau)$. Això implica que $\phi(A) \subsetneq \mathrm{End}_K(\phi)$, és a dir, ϕ té multiplicació complexa perquè és de rang 2.

Exemple 2.3.10. Considerem $\phi_T(\tau) = T + \tau + \tau^2$ sobre F. Segons la Definició 2.6.3, aquest té j-invariant 1. Així, la llista completa de mòduls de Drinfeld de rang 2 amb multiplicació complexa està donada a ([Sch97], Teorema 6) i com el 1 no hi és, deduïm que $\mathrm{End}(\phi) = \phi(A)$.

2.4 Punts de torsió

Definició 2.4.1. Si ϕ és un mòdul de Drinfeld de rang r sobre K i $a \in A \setminus \{0\}$, anomenarem $\phi[a]$ com els *punts de a-torsió* de ϕ, és a dir

$$\phi[a] = \ker(\phi_a) = \{\lambda \in \overline{K} \mid \phi_a(\lambda) = 0\}.$$

Veiem que $\phi[a]$ és un A-mòdul de manera natural via

$$b \circ \lambda = \phi_b(\lambda) \text{ on } b \in A \text{ i } \lambda \in \phi[a].$$

Això es deu a que $b \circ \lambda \in \phi[a]$ perquè

$$\phi_a(b \circ \lambda) = \phi_a(\phi_b(\lambda)) = \phi_b(\phi_a(\lambda)) = \phi_b(0) = 0.$$

Definició 2.4.2. Diem que el polinomi $\mathbb{F}_q$-linear $\phi_a(x) \in K[x]$ és el *polinomi de a-divisió de* ϕ i $K(\phi[a])$, el cos de descomposició de $\phi_a(x)$, serà el *cos de a-divisió de* ϕ. A més, si $\mathrm{car}_A(K,\gamma) \nmid a$, $\phi_a(x)$ és separable, i per tant, l'extensió $K(\phi[a])/K$ és de Galois.

Lema 2.4.3 ([Pap23], Lema 3.5.1)**.** *Siguin $a, b \in A$ no nuls coprimers, llavors, com a A-mòduls, tenim que*

$$\phi[ab] \cong \phi[a] \times \phi[b].$$

Si $\alpha \in \mathbb{F}_q^*$, $\phi_{\alpha a}(x) = \alpha\phi_a(x)$, i per tant, $\phi[\alpha a] = \phi[a]$. Això implica que sigui $\mathfrak{n}$ un ideal de A, un pot definir $\phi[\mathfrak{n}]$ com els punts de torsió de qualsevol generador de $\mathfrak{n}$ i, en general, assumirem que $\mathfrak{n}$ és mònic.

Teorema 2.4.4 ([Pap23], Teorema 3.5.2)**.** *Siguin $\mathfrak{p}$ un primer de A i $n \geq 1$ enter, aleshores*

(1) Si $\mathrm{car}_A(K,\gamma) \neq \mathfrak{p}$,
$$\phi[\mathfrak{p}^n] \cong (A/(\mathfrak{p}^n))^r.$$

(2) Si $\mathrm{car}_A(K,\gamma) = \mathfrak{p}$,
$$\phi[\mathfrak{p}^n] \cong (A/(\mathfrak{p}^n))^{r-H(\phi)}.$$

Corol·lari 2.4.5. *Sigui $a \in A$ no nul tal que* $\mathrm{car}_A(K,\gamma) \nmid a$*, llavors*

$$\phi[a] \cong (A/(a))^r.$$

Demostració. Com $a \neq 0$, existeixen $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ primers de A i $\alpha \in \mathbb{F}_q^*$ tals que $a = \alpha\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_s^{n_s}$ on $n_i \geq 1$ per tot $1 \leq i \leq s$. Pel Lema 2.4.3, $\phi[a] \cong \phi[\mathfrak{p}_1^{n_1}] \times \cdots \times \phi[\mathfrak{p}_s^{n_s}]$. Ara pel Teorema 2.4.4 i pel teorema xinés de les restes,

$$\phi[\mathfrak{p}_1^{n_1}] \times \cdots \times \phi[\mathfrak{p}_s^{n_s}] \cong (A/(\mathfrak{p}_1^{n_1}))^r \times \cdots \times (A/(\mathfrak{p}_s^{n_s}))^r \cong (A/(a))^r. \qquad \square$$

Ara assumim que $\mathrm{car}_A(K,\gamma) \nmid a$. Recordem que en aquest cas el polinomi $\phi_a(x) \in K[x]$ és separable, i per això, $\phi[a]$ està equipat amb una acció del grup de Galois absolut $G_K := \mathrm{Gal}(K^{\mathrm{sep}}/K)$ ja que cada element d'aquest permuta les arrels de $\phi_a(x)$. Aquesta acció de G_K commuta amb l'acció de A, ja que per $\sigma \in G_K$, $b \in A$ i $\lambda \in \phi[a]$ tenim que $\phi_b(\sigma\lambda) = \sigma\phi_b(\lambda)$, i per tant, obtenim la representació

$$\rho_{\phi,a} : G_K \to \mathrm{Aut}_A(\phi[a]) \cong \mathrm{GL}_r(A/(a)). \tag{2.4.1}$$

El grup de Galois de $K(\phi[a])/K$ és isomorf a la imatge de $\rho_{\phi,a}$.

Exemple 2.4.6. Considerem $\phi_T(\tau) = T + (T^3+1)\tau + \tau^2$ sobre F i calculem $|\mathrm{Gal}(F(\phi[T])/F)|$ usant el següent codi de `Magma`:

```
> F<T> := FunctionField(GF(5));
> R<x> := PolynomialRing(F);
> f := x^25 + (T^3+1)*x^5 + T*x;
> G := GaloisGroup(f);
> #G;
```

Trobem que $|\mathrm{Gal}(F(\phi[T])/F)| = 480$. Així, com $\mathrm{Gal}(F(\phi[T])/F)$ és isomorf a un subgrup de $\mathrm{GL}_2(\mathbb{F}_5)$ i $|\mathrm{GL}_2(\mathbb{F}_5)| = 480$, deduïm que $\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{GL}_2(\mathbb{F}_5)$.

Sigui ϕ un mòdul de Drinfeld de rang r sobre K i sigui $\mathfrak{p}$ un primer de A, $\phi[\mathfrak{p}^n] \subseteq \phi[\mathfrak{p}^{n+1}]$ per tot $n \geq 1$ i observem que l'acció de $\phi_\mathfrak{p}$ resulta en morfismes exhaustius naturals via

$$\begin{aligned} \phi_\mathfrak{p} : \phi[\mathfrak{p}^{n+1}] &\longrightarrow \phi[\mathfrak{p}^n] \\ \alpha &\longmapsto \phi_\mathfrak{p}(\alpha). \end{aligned}$$

Com a conseqüència, obtenim el sistema invers de A-mòduls $(\phi[\mathfrak{p}^n], \phi_\mathfrak{p})_{n\geq 1}$ i definim el *mòdul de Tate $\mathfrak{p}$-àdic* com el seu límit invers, és a dir

$$T_\mathfrak{p}(\phi) := \varprojlim_{n\geq 1} \phi[\mathfrak{p}^n] \cong \begin{cases} \varprojlim_{n\geq 1} (A/(\mathfrak{p}^n))^r \cong A_\mathfrak{p}^r & \text{si } \mathrm{car}_A(K,\gamma) \neq \mathfrak{p}, \\ \varprojlim_{n\geq 1} (A/(\mathfrak{p}^n))^{r-H(\phi)} \cong A_\mathfrak{p}^{r-H(\phi)} & \text{si } \mathrm{car}_A(K,\gamma) = \mathfrak{p}. \end{cases}$$

Ara suposem que $\mathrm{car}_A(K,\gamma) \neq \mathfrak{p}$. L'acció de G_K en cada $\phi[\mathfrak{p}^n]$ commuta amb l'acció de $\phi_\mathfrak{p}$ usada per definir el mòdul de Tate $\mathfrak{p}$-àdic, i per tant, G_K actua en $T_\mathfrak{p}(\phi)$. Per aquesta raó, tenim la representació

$$\hat{\rho}_{\phi,\mathfrak{p}} : G_K \to \mathrm{Aut}_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi)) \cong \mathrm{GL}_r(A_\mathfrak{p}). \tag{2.4.2}$$

Aleshores siguin ϕ i ψ dos mòduls de Drinfeld de rang r sobre K i sigui $u : \phi \to \psi$ una isogènia, llavors u indueix morfismes $\phi[\mathfrak{p}^n] \to \psi[\mathfrak{p}^n]$ per tot $n \geq 1$, i per això, indueix una aplicació $A_\mathfrak{p}$-lineal $u_\mathfrak{p} : T_\mathfrak{p}(\phi) \to T_\mathfrak{p}(\psi)$.

Així, obtenim el morfisme natural

$$\mathrm{Hom}_K(\phi,\psi) \longrightarrow \mathrm{Hom}_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi), T_\mathfrak{p}(\psi)). \tag{2.4.3}$$

A més, si $\phi = \psi$, l'aplicació

$$\mathrm{End}_K(\phi) \longrightarrow \mathrm{End}_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi))$$

és un morfisme d'anells.

Si $\mathfrak{p} \neq \mathrm{car}_A(K,\gamma)$, el morfisme (2.4.3) és injectiu perquè si $u_\mathfrak{p} : T_\mathfrak{p}(\phi) \to T_\mathfrak{p}(\psi)$ és l'aplicació zero, llavors $\phi[\mathfrak{p}^n]$ és un subconjunt de $\ker(u)$ per tot $n \geq 1$, cosa que és falsa una vegada $|\phi[\mathfrak{p}^n]|$ és més gran que $\deg(u(x))$. El següent teorema diu que aquest morfisme segueix sent injectiu fins i tot després d'estendre'l linealment a $A_\mathfrak{p}$.

Teorema 2.4.7 ([Pap23], Teorema 3.5.4)**.** *Siguin ϕ i ψ mòduls de Drinfeld definits sobre K i sigui $\mathfrak{p} \neq \mathrm{car}_A(K,\gamma)$ un primer de A, aleshores el morfisme natural*

$$\begin{aligned} \mathrm{Hom}_K(\phi,\psi) \otimes_A A_\mathfrak{p} &\longrightarrow \mathrm{Hom}_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi), T_\mathfrak{p}(\psi)) \\ u &\longmapsto u_\mathfrak{p} \end{aligned}$$

és injectiu.

2.5 Emparellament de Weil

Definició 2.5.1. Sigui ϕ un mòdul de Drinfeld de rang r sobre K donat per

$$\phi_T(\tau) = \gamma(T) + g_1\tau + \cdots + g_r\tau^r,$$

diem que el mòdul de Drinfeld ψ de rang 1 sobre K associat per l'emparellament de Weil és aquell definit per

$$\psi_T(\tau) = \gamma(T) + (-1)^{r-1}g_r\tau.$$

Teorema 2.5.2 ([Pap23], Teorema 3.7.1)**.** *Usant la mateixa notació, obtenim que:*

(1) Si assumim que $a \in A$ no és divisible per $\mathrm{car}_A(K,\gamma)$, sigui

$$\rho_{\phi,a} : G_K \to \mathrm{Aut}_A(\phi[a]) \cong \mathrm{GL}_r(A/(a))$$

la representació (2.4.1) i sigui $\rho_{\psi,a} : G_K \to \mathrm{Aut}_A(\psi[a]) \cong (A/(a))^*$ la representació corresponent per ψ, llavors

$$\det(\rho_{\phi,a}(\sigma)) = \rho_{\psi,a}(\sigma) \text{ per tot } \sigma \in G_K.$$

(2) $K(\psi[a]) \subseteq K(\phi[a])$ per tot $a \in A \setminus \{0\}$.

(3) Si $\mathfrak{p}$ és un primer de A tal que $\mathrm{car}_A(K,\gamma) \neq \mathfrak{p}$, sigui

$$\hat{\rho}_{\phi,\mathfrak{p}} : G_K \to \mathrm{Aut}_{A_\mathfrak{p}}(T_\mathfrak{p}(\phi)) \cong \mathrm{GL}_r(A_\mathfrak{p})$$

la representació (2.4.2) i sigui $\hat{\rho}_{\psi,\mathfrak{p}} : G_K \to \mathrm{Aut}_{A_\mathfrak{p}}(T_\mathfrak{p}(\psi)) \cong (A_\mathfrak{p})^*$ la representació corresponent per ψ, aleshores

$$\det(\hat{\rho}_{\phi,\mathfrak{p}}(\sigma)) = \hat{\rho}_{\psi,\mathfrak{p}}(\sigma) \text{ per tot } \sigma \in G_K.$$

2.6 Isomorfismes

Siguin ϕ i ψ dos mòduls de Drinfeld de rang r sobre K, una isogènia $u : \phi \to \psi$ sobre K és un isomorfisme si té inversa en $K\{\tau\}$, és a dir, si existeix $v \in K\{\tau\}$ tal que $uv = vu = 1$. Computant els graus veiem que $\deg_\tau(u) + \deg_\tau(v) = \deg_\tau(uv) = 0$. Per això, $v = c \in K^*$ és una constant no nul·la tal que $c\phi_T c^{-1} = \psi_T$.

Si $\phi_T(\tau) = \gamma(T) + g_1\tau + \cdots + g_r\tau^r$ i $\psi_T(\tau) = \gamma(T) + h_1\tau + \cdots + h_r\tau^r$, això és equivalent a que

$$g_i = h_i c^{q^i-1} \text{ per tot } 1 \leq i \leq r.$$

Diem que ϕ i ψ són isomorfs sobre L una extensió de K, si existeix $c \in L^*$ tal que $c\phi_T c^{-1} = \psi_T$.

Exemple 2.6.1. Suposem que ϕ i ψ tenen rang 1. Sigui c una arrel de $x^{q-1} = g_1/h_1$, llavors $c\phi_T c^{-1} = \psi_T$, i per tant, ϕ i ψ són isomorfs sobre $K(\sqrt[q-1]{g_1/h_1})$. Com $x^{q-1} = g_1/h_1$ sempre és un polinomi separable, això implica que el mòdul de Carlitz $C_T(\tau) = \gamma(T) + \tau$ és l'únic mòdul de Drinfeld sobre K^{sep} llevat d'isomorfisme. Notem que $x^{q-1} = g_1/h_1$ pot no tenir arrels a K, i en aquest cas, ϕ i ψ no són isomorfs sobre K.

Lema 2.6.2. *Sigui $\phi_T(\tau) = \gamma(T) + g_1\tau + \cdots + g_r\tau^r$ un mòdul de Drinfeld de rang r sobre K i sigui*

$$m = \mathrm{mcd}\{1 \leq i \leq r \mid g_i \neq 0\},$$

aleshores $\mathrm{Aut}(\phi) \cong \mathbb{F}_{q^m}^*$.

Demostració. Per una banda, sigui $0 \neq c \in \mathrm{Aut}(\phi) \subseteq K^{\mathrm{sep}}$, sabem que $g_i = g_i c^{q^i-1}$ per tot $1 \leq i \leq r$. Per això, $c^{q^i-1} = 1$ si $g_i \neq 0$. Així, $c \in \mathbb{F}_{q^i}^*$ si $g_i \neq 0$. Com $\mathbb{F}_{q^i} \cap \mathbb{F}_{q^j} = \mathbb{F}_{q^{\mathrm{mcd}(i,j)}}$, necessàriament $c \in \mathbb{F}_{q^m}^*$. Per altra banda, és clar que tot $c \in \mathbb{F}_{q^m}^*$ és satisfà $c\phi_T c^{-1} = \phi_T$. En conclusió, $\mathrm{Aut}(\phi) \cong \mathbb{F}_{q^m}^*$. □

Definició 2.6.3. Sigui $\phi_T(\tau) = \gamma(T) + g\tau + \Delta\tau^2$ un mòdul de Drinfeld de rang 2 sobre K, aleshores el *j-invariant* és

$$j(\phi) := \frac{g^{q+1}}{\Delta}.$$

Lema 2.6.4 ([Pap23], Lema 3.8.4)**.** *Dos mòduls de Drinfeld ϕ i ψ de rang 2 sobre K són isomorfs sobre K^{sep} si i només si $j(\phi) = j(\psi)$.*

Observació 2.6.5. Per un argument similar al de l'Exemple 2.6.1, dos mòduls de Drinfeld ϕ i ψ de rang 2 amb $j(\phi) = j(\psi)$ poden no ser isomorfs sobre K. Per exemple, $\phi_T(\tau) = \gamma(T) + \tau^2$ i $\psi_T(\tau) = \gamma(T) + (\gamma(T)+1)\tau^2$ tenen j-invariant 0, però són isomorfs si i només si $\gamma(T)+1$ és una potència (q^2-1)-èssima en K.

Corol·lari 2.6.6. *Sigui ϕ un mòdul de Drinfeld de rang 2 sobre K, llavors*

$$\mathrm{Aut}(\phi) = \begin{cases} \mathbb{F}_{q^2}^* & \text{si } j(\phi) = 0, \\ \mathbb{F}_q^* & \text{si } j(\phi) \neq 0. \end{cases}$$

Demostració. Pel Lema 2.6.2, sabem que $\mathrm{Aut}(\phi) = \mathbb{F}_{q^2}^* \iff g = 0 \iff j(\phi) = 0$. És obvi que $\mathrm{Aut}(\phi) = \mathbb{F}_q^*$ en la resta dels casos. □

Observació 2.6.7. Per cada $j \in K$ sempre hi ha un mòdul de Drinfeld ϕ de rang 2 sobre K amb $j(\phi) = j$, ja que si $j = 0$

$$\phi_T(\tau) = \gamma(T) + \tau^2 \text{ té } j(\phi) = 0,$$

i si $j \in K^*$,

$$\phi_T(\tau) = \gamma(T) + \tau + j^{-1}\tau^2 \text{ té } j(\phi) = j.$$

Per això i pel Lema 2.6.4, les classes d'isomorfisme de mòduls de Drinfeld de rang 2 sobre K^{sep} estan en bijecció amb els elements de K.

2.7 Reduccions de mòduls de Drinfeld

Sigui (K, γ) un A-cos i sigui v una valoració discreta no trivial en K, assumirem que

$$v(\gamma(a)) \geq 0 \text{ per tot } a \in A.$$

A més, definim $R_v = \{\alpha \in K \mid v(\alpha) \geq 0\}$, $M_v = \{\alpha \in K \mid v(\alpha) > 0\}$ i $R_v^* = R_v \setminus M_v = \{\alpha \in K \mid v(\alpha) = 0\}$. Notem que R_v és un anell i M_v un ideal maximal d'aquest, i per això, $k_v := R_v/M_v$ és un cos.

Definició 2.7.1. Sigui ϕ un mòdul de Drinfeld de rang r sobre K donat per

$$\phi_T(\tau) = \gamma(T) + g_1\tau + \cdots + g_r\tau^r,$$

diem que ϕ està definit a R_v si $\phi_a \in R_v\{\tau\}$ per tot $a \in A$.

Lema 2.7.2. *Són equivalents:*

(1) ϕ està definit a R_v.

(2) $\phi_T \in R_v\{\tau\}$.

(3) $\phi_a \in R_v\{\tau\}$ *per algun* $a \in A$ *amb* $\deg(a) \geq 1$.

Demostració. Les implicacions (1) $\iff$ (2) $\implies$ (3) són òbvies. Ara escollim $a \in A$ amb $\deg(a) \geq 1$ mínim tal que $\phi_a \in R_v\{\tau\}$. Si $\deg(a) = 1$, aleshores $a = \alpha T + \beta$ per algun $\alpha \in \mathbb{F}_q^*$ i $\beta \in \mathbb{F}_q$, i per tant, $\phi_T = \alpha^{-1}(\phi_a - \beta) \in R_v\{\tau\}$. Si $\deg(a) > 1$, agafem $\delta \in \mathbb{F}_q$ tal que T divideix a $a + \delta$, i per tant, $a + \delta = T \cdot b$ per algun $b \in A$. Així, sabem que $\phi_T \cdot \phi_b = \phi_{a+\delta} = \phi_a + \delta \in R_v\{\tau\}$, però com $\deg(T) = 1 < \deg(a)$ i $1 \leq \deg(a) - 1 = \deg(b) < \deg(a)$, tenim que $\phi_T, \phi_b \notin R_v\{\tau\}$. Això últim implica que $\phi_T \cdot \phi_b \notin R_v\{\tau\}$ que és una contradicció i deduïm que $\deg(a) = 1$. En conclusió, (3) $\implies$ (2). □

Sempre podem trobar un mòdul de Drinfeld ψ isomorf a ϕ que està definit a R_v. Si triem $c \in K^*$ de manera que $(q^i - 1)v(c) + v(g_i) \geq 0$ per tot $1 \leq i \leq r$, observem que

$$\psi_T(\tau) := c\phi_T(\tau)c^{-1} = \gamma(T) + \sum_{i=1}^{r} c^{q^i - 1} g_i \tau^i$$

és isomorf a ϕ i està definit a R_v. Reduint els coeficients de ψ mòdul M_v obtenim un morfisme $\mathrm{Red}(\psi, v) : A \to k_v\{\tau\}$. El problema és que $\mathrm{Red}(\psi, v)$ pot ser un mòdul de Drinfeld de rang estrictament inferior o fins i tot no ser un mòdul de Drinfeld si $\mathrm{Red}(\psi, v)(A) \subset k_v$.

Exemple 2.7.3. Considerem $\phi_T(\tau) = T + \frac{1}{T}\tau + \tau^2$ sobre F i $v = v_T$. Per fer que $\psi = c\phi c^{-1}$ estigui definida a R_v, hem d'agafar $c \in F$ amb $v(c) \geq 1$. En aquest cas,

$$\psi_T(\tau) = T + \frac{c^{q-1}}{T}\tau + c^{q^2-1}\tau^2.$$

Com a conseqüència, $\mathrm{Red}(\psi, v)$ és un mòdul de Drinfeld de rang 1 si $q = 2$ i $v(c) = 1$ i no és un mòdul de Drinfeld si $q \neq 2$ o si $v(c) > 1$.

Definició 2.7.4. Sigui ϕ un mòdul de Drinfeld de rang r sobre K, diem que ϕ té *reducció estable* respecte v si existeix $c \in K^*$ tal que $\psi = c\phi c^{-1}$ està definit a R_v i $\mathrm{Red}(\psi, v)$ és un mòdul de Drinfeld. Si existeix $c' \in K^*$ de manera que $\psi' = c'\phi(c')^{-1}$ està definit a R_v i $\mathrm{Red}(\psi', v)$ és un mòdul de Drinfeld de rang r, diem que ϕ té *bona reducció* respecte v. Notem que les nocions de reducció bona i estable coincideixen a $r = 1$. Si ϕ no té bona reducció, diem que té *mala reducció*.

A partir d'ara suposem que ϕ és un mòdul de Drinfeld de rang r sobre F i $\gamma(a) = a$ per tot $a \in A$.

Definició 2.7.5. Si $\phi_T(\tau) = T + g_1\tau + \cdots + g_r\tau^r$, diem que ϕ és minimal si $g_1, \ldots, g_r \in A$ i si no existeix $\mathfrak{p} \in A$ primer tal que $v_\mathfrak{p}(g_i) \geq q^i - 1$ per tot $1 \leq i \leq r$.

Teorema 2.7.6 ([Geb03], Teorema 1.9.4)**.** *Existeix un únic* ψ *mòdul de Drinfeld de rang* r *minimal que és isomorf a* ϕ *sobre* F*. Denotarem* $\psi = \min(\phi)$.

Lema 2.7.7. *Si* $\phi_T(\tau) = T + g_1\tau + \cdots + g_r\tau^r$, $\mathfrak{p} \in A$ *és un primer,* $v = v_\mathfrak{p}$, $\psi = \min(\phi)$ *i* $\psi_T(\tau) = T + h_1\tau + \cdots + h_r\tau^r$*, llavors ocorre que:*

(1) ϕ *té reducció estable respecte* $v \iff v(h_j) = 0$ *per algun* $1 \leq j \leq r$.

(2) ϕ *té bona reducció respecte* $v \iff v(h_r) = 0$.

(3) ϕ *té mala reducció respecte* $v \iff v(h_i) > 0$ *per tot* $1 \leq i \leq r$.

Demostració. És conseqüència directa de les Definicions 2.7.4 i 2.7.5 i del Teorema 2.7.6. □

Exemple 2.7.8. Siguin $\mathfrak{p}, \mathfrak{q}, \mathfrak{l} \in A$ primers diferents, considerem

$$\phi_T(\tau) = T + \mathfrak{p}\mathfrak{l}^{q-1}\mathfrak{q}^{q-1}\tau + \mathfrak{p}\mathfrak{l}^{q^2-1}\mathfrak{q}^{q^2}\tau^2.$$

Aleshores $\min(\phi)_T(\tau) = T + \mathfrak{p}\tau + \mathfrak{p}\mathfrak{q}\tau^2$. Per això, ϕ té reducció estable per tot primer de A excepte $\mathfrak{p}$, té bona reducció per tot primer de A excepte $\mathfrak{p}$ i $\mathfrak{q}$ i té mala reducció per $\mathfrak{p}$.

Per concloure l'apartat introduïm el següent teorema que ens serà útil més endavant. En aquest assumim que K és una extensió finita de $F_{\mathfrak{p}}$ per $\mathfrak{p} \in A$ un cert primer i $\gamma(a) = a$ per tot $a \in A$.

Teorema 2.7.9 ([Pap23], Teorema 6.3.1)**.** *Sigui ϕ un mòdul de Drinfeld sobre K i sigui $\mathfrak{l} \in A$ un primer diferent de $\mathfrak{p}$, llavors les següents propietats són equivalents:*

(1) ϕ té bona reducció respecte $v_{\mathfrak{p}}$.

(2) $\phi[a]$ és no-ramificat[1] per tot $a \in A$ coprimer amb $\mathfrak{p}$.

(3) Hi ha infinits $a \in A$ coprimers amb $\mathfrak{p}$ pels quals $\phi[a]$ és no-ramificat.

(4) $T_{\mathfrak{l}}(\phi)$ és no-ramificat.

[1] La definició d'aquesta noció de no-ramificació la podem trobar al mateix Teorema 6.3.1 de [Pap23].

3 Mòduls de Drinfeld finits

En aquesta secció, suposarem que (K,γ) és un A-cos finit. Més precisament, assumirem que $\mathrm{car}_A(K,\gamma)=\mathfrak{p}$ és un primer de A, K és una extensió de $\mathbb{F}_\mathfrak{p}=A/(\mathfrak{p})$ i $\gamma:A\longrightarrow\mathbb{F}_\mathfrak{p}\hookrightarrow K$ és la projecció mòdul $\mathfrak{p}$. Si definim $d=\deg(\mathfrak{p})$ i escollim $K\cong\mathbb{F}_{q^m}$, notem que m és divisible per d ja que K és una extensió de $\mathbb{F}_\mathfrak{p}\cong\mathbb{F}_{q^d}$.

3.1 L'endomorfisme de Frobenius

Considerem l'endomorfisme de Frobenius de K

$$\begin{aligned}\mathrm{Frob}_K : K &\longrightarrow K\\ x &\longmapsto x^{|K|}=x^{q^m}.\end{aligned}$$

Així, si identifiquem τ amb l'endomorfisme de Frobenius de $\mathbb{F}_q$ perquè $\tau x=x^q\tau$, obtenim que $\mathrm{Frob}_K=\tau^m\in K\{\tau\}$. Observem que τ^m commuta amb tot element de $K\{\tau\}$ ja que $\tau^m\cdot(a\tau^i)=$ $=(a^{q^m}\tau^i)\cdot\tau^m=(a\tau^i)\cdot\tau^m$ per tot $a\in K$ i $i\geq 0$. També tenim els següents resultats:

Lema 3.1.1. *Sigui $Z(K\{\tau\})=\{\alpha\in K\{\tau\}\mid\alpha\beta=\beta\alpha\ \forall\beta\in K\{\tau\}\}$ el centre de $K\{\tau\}$, tenim que $Z(K\{\tau\})=\mathbb{F}_q[\tau^m]$.*

Demostració. Siguin $\alpha\in\mathbb{F}_q$ i $\beta\in K$, $\beta\alpha=\alpha\beta$ i $\tau\alpha=\alpha^q\tau=\alpha\tau$, cosa que implica que $\alpha\in Z(K\{\tau\})$. Per això, $\mathbb{F}_q[\tau^m]\subseteq Z(K\{\tau\})$ ja que ja hem vist que $\tau^m\in Z(K\{\tau\})$.

Suposem que $f=a_0+a_1\tau+\cdots+a_s\tau^s$ commuta amb τ, aleshores

$$\tau f=a_0^q\tau+a_1^q\tau^2+\cdots+a_s^q\tau^{q+1}=a_0\tau+a_1\tau^2+\cdots+a_s\tau^{s+1}=f\tau.$$

Això implica que $a_i^q=a_i$, és a dir $a_i\in\mathbb{F}_q$, per tot $1\leq i\leq s$. Si a més f commuta amb tot $\beta\in K$, comparant els coeficients de $\beta f=\sum_{i=0}^s\beta a_i\tau^i$ i $f\beta=\sum_{i=0}^s\beta^{q^i}a_i\tau^i$, trobem que $a_i=0$ o $\beta=\beta^{q^i}$. Com $\beta=\beta^{q^i}$ per tot $\beta\in K$ si i només si i és divisible per m, $a_i=0$ si $m\nmid i$. En conclusió, $f\in\mathbb{F}_q[\tau^m]$. Això vol dir que $\mathbb{F}_q[\tau^m]=Z(K\{\tau\})$. □

Proposició 3.1.2 ([Pap23], Proposició 4.1.1)**.** *Sigui $\mathbb{F}_q(\tau^m)$ el cos de fraccions de $\mathbb{F}_q[\tau^m]$, llavors $K(\tau)=K\{\tau\}\otimes_{\mathbb{F}_q[\tau^m]}\mathbb{F}_q(\tau^m)$ és una àlgebra de divisió sobre $\mathbb{F}_q(\tau^m)$.*

Ara sigui ϕ un mòdul de Drinfeld de rang r sobre K, sabem que és un morfisme injectiu perquè $\deg(\phi_a)=r\cdot\deg(a)$ per tot $a\in A$, i per tant, $\phi(a)=\phi_a=0\iff a=0$. Per aquesta raó, obtenim que $A\xhookrightarrow{\phi}K\{\tau\}\hookrightarrow K(\tau)$ i com tot element no nul de $K(\tau)$ té inversa per la Proposició 3.1.2, la inclusió $A\hookrightarrow K(\tau)$ s'estén a $\iota:F\hookrightarrow K(\tau)$. Així, identificant A i F amb $\iota(A)$ i $\iota(F)$ dins de $K(\tau)$, podem considerar $\widetilde{F}:=F(\tau^m)$ com una extensió de F dins de $K(\tau)$.

Proposició 3.1.3 ([Pap23], Teorema 4.1.3)**.** *Utilitzant la mateixa notació, tenim que $[\widetilde{F}:F]$ divideix a r.*

Definim el polinomi mínim de ϕ com $m_\phi(x):=\mathrm{Irr}(\tau^m,F)(x)$ i com τ^m és enter sobre A, sabem que $m_\phi(x)\in A[x]$.

3.2 Polinomi característic

Sigui ϕ un mòdul de Drinfeld de rang r sobre K, com $\mathrm{Frob}_K=\tau^m$ commuta amb ϕ_T, Frob_K és un element de $\mathrm{End}_K(\phi)$. Sigui $\mathfrak{l}\neq\mathfrak{p}=\mathrm{car}_A(K,\gamma)$ un primer de A, $T_\mathfrak{l}(\phi)\cong A_\mathfrak{l}^r$ és el mòdul de Tate $\mathfrak{l}$-àdic, i pel Teorema 2.4.7, obtenim el morfisme d'anells injectiu

$$i_\mathfrak{l}:\mathrm{End}_K(\phi)\otimes_A A_\mathfrak{l}\longrightarrow\mathrm{End}_{A_\mathfrak{l}}(T_\mathfrak{l}(\phi)). \tag{3.2.1}$$

Considerem $i_\mathfrak{l}(\text{Frob}_K \otimes 1)$ la imatge de l'endomorfisme de Frobenius sota el morfisme (3.2.1). Com $\text{Frob}_K \in G_K$, sigui $\hat{\rho}_{\phi,\mathfrak{l}}$ la representació (2.4.2), veiem que $\hat{\rho}_{\phi,\mathfrak{l}}(\text{Frob}_K)$ és igual per construcció a $i_\mathfrak{l}(\text{Frob}_K \otimes 1)$. Com a conseqüència, definim el polinomi característic de $i_\mathfrak{l}(\text{Frob}_K \otimes 1)$ com $P_{\phi,\mathfrak{l}}(x) = \det(x - i_\mathfrak{l}(\text{Frob}_K \otimes 1)) = \det(x - \hat{\rho}_{\phi,\mathfrak{l}}(\text{Frob}_K)) \in A_\mathfrak{l}[x]$.

Teorema 3.2.1 ([Gek91], Lema 3.3). *Sigui $\mathfrak{l}$ un primer de A diferent $\mathfrak{p}$, si $\widetilde{F} = F(\tau^m)$, llavors*

$$P_{\phi,\mathfrak{l}}(x) = m_\phi(x)^{r/[\widetilde{F}:F]}.$$

En particular, $P_{\phi,\mathfrak{l}}(x)$ té coeficients en A que no depenen de $\mathfrak{l}$ i té grau r.

Per això, podem definir el polinomi característic de ϕ com $P_\phi := P_{\phi,\mathfrak{l}}$.

Ara sigui $\mathfrak{n} \in A$ coprimer amb $\mathfrak{p}$, considerem $\phi[\mathfrak{n}] \cong (A/(\mathfrak{n}))^r$ i si considerem Frob_K com un automorfisme A-lineal, aquest es pot representar com un element de $\text{GL}_r(A/(\mathfrak{n}))$ ben definit llevat de conjugació. Com a conseqüència, $P_\mathfrak{n} \in (A/(\mathfrak{n}))[x]$ el polinomi característic d'aquesta matriu està ben definit i tenim el següent resultat:

Proposició 3.2.2. *La reducció mòdul $\mathfrak{n}$ de P_ϕ és igual a $P_\mathfrak{n}$.*

Demostració. Pel Lema 2.4.3, podem reduir-nos al cas on $\mathfrak{n} = \mathfrak{l}^n$ és una potència d'un primer diferent de $\mathfrak{p}$, i en aquest cas, pel Teorema 3.2.1 sabem que $P_{\mathfrak{l}^n}$ és igual a la reducció mòdul $\mathfrak{l}^n$ de $\det(x - i_\mathfrak{l}(\text{Frob}_K \otimes 1)) = P_{\phi,\mathfrak{l}} = P_\phi$. □

Teorema 3.2.3 ([Gek91], Teorema 5.1). *Per ϕ i ψ dos mòduls de Drinfeld de rang r sobre K, els següents enunciats són equivalents:*

(1) Existeix una isogènia sobre K entre ϕ i ψ.

(2) $m_\phi = m_\psi$.

(3) $P_\phi = P_\psi$.

Teorema 3.2.4 ([Pap23], Teorema 4.2.7). *Sigui $P_\phi(x) = x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0 \in A[x]$, aleshores ocorre que:*

(1) Per qualsevol $0 \leq i \leq r-1$ obtenim que

$$\deg(a_i) \leq \frac{(r-i)m}{r}.$$

(2) Si $\phi_T(\tau) = \gamma(T) + g_1\tau + \cdots + g_r\tau^r \in K\{\tau\}$, llavors $a_0 = (-1)^{rm-r-m} \cdot \text{Nr}_{\mathbb{F}_q}^K(g_r)^{-1} \cdot \mathfrak{p}^{m/d}$.[1]

Observació 3.2.5. Si ϕ té rang 2, el primer enunciat d'aquest teorema diu que

$$\deg(a_1) \leq \frac{m}{2} = \frac{\deg(\mathfrak{p})}{2} \cdot [K : \mathbb{F}_\mathfrak{p}]$$

que és un anàleg per mòduls de Drinfeld del teorema de Hasse per corbes el·líptiques.

Recordem que ${}^\phi K$ és un A-mòdul amb la suma habitual i l'operació $a * \beta = \phi_a(\beta)$ per $a \in A$ i $\beta \in K$. Com ${}^\phi K$ és un A-mòdul finit i A és un domini d'ideals principals, pel teorema d'estructura per mòduls finitament generats sobre un domini d'ideals principals, sabem que

$${}^\phi K \cong A/(b_1) \times \cdots \times A/(b_s)$$

per uns certs $b_1, \ldots, b_s \in A$ mònics de manera $b_1 \mid b_2 \mid \cdots \mid b_s$. Notem que b_s aniquila a ${}^\phi K$, i per tant, ${}^\phi K \subseteq \phi[b_s] \subseteq (A/(b_s))^r$ pel Teorema 2.4.4, cosa que implica que $s \leq r$.

[1] La definició de $\text{Nr}_{\mathbb{F}_q}^K$ la podem trobar a la Definició 2.5 de [Neu99].

Definició 3.2.6. Usant aquesta notació, la característica d'Euler-Poincaré de ϕ és

$$\chi({}^{\phi}K) = \prod_{i=1}^{s} a_i.$$

Teorema 3.2.7 ([Gek91], Lema 3.10)**.** *Tenim la igualtat d'ideals* $(\chi({}^{\phi}K)) = (P_{\phi}(1))$.

Si ϕ és un mòdul de Drinfeld de rang 2 sobre K donat per $\phi_T(\tau) = \gamma(T) + g\tau + \Delta\tau^2$, llavors el polinomi característic de ϕ és de la forma

$$x^2 + \widetilde{a}x + (-1)^m \cdot \mathrm{Nr}_{\mathbb{F}_q}^{K}(\Delta)^{-1} \cdot \mathfrak{p}^{m/d}$$

on $\widetilde{a} \in A$ pels Teoremes 3.2.1 i 3.2.4.

Proposició 3.2.8 ([Jun00], Proposició 4.2.9)**.** *Utilitzant la mateixa notació, es compleix que*

$$\gamma(\widetilde{a}) = (-1)^{m-1} \cdot \mathrm{Nr}_{\mathbb{F}_q}^{K}(\Delta)^{-1} \cdot \mathrm{Nr}_{\mathbb{F}_{\mathfrak{p}}}^{K}(I(\phi)) \in \mathbb{F}_{\mathfrak{p}}$$

on $I(\phi)$ és l'invariant de Hasse de ϕ com a la Definició 2.2.9.

Si considerem el cas on $K = \mathbb{F}_{\mathfrak{p}}$, $\mathrm{Nr}_{\mathbb{F}_q}^{\mathbb{F}_{\mathfrak{p}}}(\Delta) = \Delta^{\frac{q^d-1}{q-1}}$ i pel Teorema 3.2.4 i la Proposició 3.2.8, obtenim que

$$\deg(\widetilde{a}) \leq \frac{\deg(\mathfrak{p})}{2} \text{ i } \gamma(\widetilde{a}) = (-1)^{m-1} \cdot (\Delta^{\frac{q^d-1}{q-1}})^{-1} \cdot I(\phi).$$

Observem que existeix exactament un element $\widetilde{b} \in A$ tal que $\deg(\widetilde{b}) < \deg(\mathfrak{p})$ i $\gamma(\widetilde{b}) = I(\phi)$, i per tant, $\widetilde{a} = (-1)^{m-1} \cdot \mathrm{Nr}_{\mathbb{F}_q}^{\mathbb{F}_{\mathfrak{p}}}(\Delta)^{-1} \cdot \widetilde{b}$. Així, per trobar $I(\phi)$ tenim el següent resultat:

Lema 3.2.9 ([Gek88], Corol·lari 12.3)**.** *Sigui ϕ un mòdul de Drinfeld de rang 2 sobre $\mathbb{F}_{\mathfrak{p}}$ donat per $\phi_T(\tau) = \gamma(T) + g\tau + \Delta\tau^2$ on $\gamma : A \to \mathbb{F}_{\mathfrak{p}}$ és la projecció mòdul $\mathfrak{p}$, si $c_0 = 1$, $c_1 = g$ i $c_k = c_{k-1} \cdot g^{q^{k-1}} - (\gamma(T)^{q^{k-1}} - \gamma(T)) \cdot c_{k-2} \cdot \Delta^{q^{k-2}}$, llavors $c_d = I(\phi)$.*

Aquest cas en particular es important perquè el podem obtenir reduint $\min(\phi)$ on ϕ és un mòdul de Drinfeld de rang 2 sobre F de reducció estable respecte $v_{\mathfrak{p}}$. Si ϕ té bona reducció, $\mathrm{Red}(\min(\phi), v_{\mathfrak{p}})$ és un mòdul de Drinfeld de rang 2, i si no la té, $\mathrm{Red}(\min(\phi), v_{\mathfrak{p}})$ té rang 1. En qualssevol de les dues situacions és fàcil implementar un algoritme en un ordinador per computar el polinomi característic de $\mathrm{Red}(\min(\phi), v_{\mathfrak{p}})$ utilitzant els resultats vists en aquest apartat.

Exemple 3.2.10. Considerem $A = \mathbb{F}_5[T]$ i $\mathfrak{p} = T^2 + 2$. Sigui ϕ el mòdul de Drinfeld sobre F definit per $\phi_T(\tau) = T + T\tau + (T^2+2)\tau^2$, aquest té reducció estable no bona respecte $v_{\mathfrak{p}}$. Trobem que

$$\overline{\phi}_T(\tau) = \mathrm{Red}(\phi, v_{\mathfrak{p}})_T(\tau) = \overline{T} + \overline{T}\tau.$$

Pel Teorema 3.2.4, tenim que $P_{\bar{\phi}}(x) = x + 3\mathfrak{p}$. Ara pel Teorema 3.2.7 sabem que $(\chi({}^{\bar{\phi}}K)) = (P_{\bar{\phi}}(1)) = (3T^2 + 2)$, és a dir, $\chi({}^{\bar{\phi}}K) = T^2 + 4 = (T+1)(T+4)$. Això implica que

$${}^{\bar{\phi}}K \cong A/(T+1) \times A/(T+4).$$

Exemple 3.2.11. Siguin $A = \mathbb{F}_3[T]$ i $\mathfrak{p} = T^2 + T + 2$, si ϕ és el mòdul de Drinfeld sobre F donat per $\phi_T(\tau) = T - T^2\tau + (T^5 + T + 2)\tau^2$, aquest té bona reducció respecte $v_{\mathfrak{p}}$ i calculem que

$$\overline{\phi}_T(\tau) = \mathrm{Red}(\phi, v_{\mathfrak{p}})_T(\tau) = \overline{T} + (\overline{T+2})\tau + \overline{2}\tau^2.$$

Pel Teorema 3.2.4, la Proposició 3.2.8 i el Lema 3.2.9, trobem que $P_{\bar{\phi}}(x) = x^2 + 2Tx + \mathfrak{p}$. Aleshores pel Teorema 3.2.7, $(\chi({}^{\bar{\phi}}K)) = (P_{\bar{\phi}}(1)) = (T^2)$, és a dir, $\chi({}^{\bar{\phi}}K) = T^2$. Això vol dir que o bé ${}^{\bar{\phi}}K \cong A/(T) \times A/(T)$ o bé ${}^{\bar{\phi}}K \cong A/(T^2)$. Ara bé, com $\overline{\phi}_T(\overline{1}) = \overline{2T+1} \neq 0$, ${}^{\bar{\phi}}K \not\subseteq \overline{\phi}[T]$ i ${}^{\bar{\phi}}K \not\cong \overline{\phi}[T] \cong A/(T) \times A/(T)$, cosa que implica que

$${}^{\bar{\phi}}K \cong A/(T^2).$$

4 El grup $\mathrm{GL}_2(\mathbb{F}_q)$

Sigui ϕ un mòdul de Drinfeld de rang 2 sobre un A-cos (K,γ) i sigui $\mathfrak{p}$ un primer de A, l'existència de la representació (2.4.1) implica que $\mathrm{Gal}(K(\phi[\mathfrak{p}])/K)$ és isomorf a un subgrup de $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$.

Per aquesta raó, en aquesta secció parlarem del grup lineal general $\mathrm{GL}_2(\mathbb{F}_q)$ i ho farem des d'un punt de vista purament de teoria de grups sense referir-nos a resultats de mòduls de Drinfeld. La connexió entre aquests dos temes s'establirà més endavant.

4.1 Classes de conjugació

Proposició 4.1.1 ([Pia83], Proposició 5.1)**.** *Les classes de conjugació de* $\mathrm{GL}_2(\mathbb{F}_q)$ *estan classificades en les següents quatre famílies:*

Tipus	Quantitat	Mida	Ordre
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^*$	$q-1$	1	$\mathrm{ord}(a)$
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^*$	$q-1$	$(q-1)(q+1)$	$p \cdot \mathrm{ord}(a)$
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a,b \in \mathbb{F}_q^*$ *i* $a \neq b$	$\frac{1}{2}(q-1)(q-2)$	$q+1$	$\mathrm{mcm}(\mathrm{ord}(a),\mathrm{ord}(b))$
$\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix} \mid x^2+ax+b$ *és irreductible a* $\mathbb{F}_q[x]$	$\frac{1}{2}q(q-1)$	$q-1$	$\mathrm{ord}(\alpha)$ *on* $\alpha \in \mathbb{F}_{q^2}^*$ *és tal que* $\alpha^2+a\alpha+b=0$

En l'últim cas, notem que $\alpha^q = \mathrm{Frob}_q(\alpha)$ és l'altra arrel de polinomi característic perquè es irreductible. Aleshores com q i $|\mathbb{F}_{q^2}^*| = q^2-1$ són coprimers, $\mathrm{ord}(\alpha^q) = \mathrm{ord}(\alpha)$.

Observació 4.1.2. Dues matrius $M, N \in \mathrm{GL}_2(\mathbb{F}_q)$ pertanyen a la mateixa classe de conjugació si i només si existeix $P \in \mathrm{GL}_2(\mathbb{F}_q)$ tal que $N = P^{-1}MP$, és a dir, si i només si M i N són similars i P és una matriu de canvi de base que les associa.

Lema 4.1.3. *Sigui* $M \in \mathrm{GL}_2(\mathbb{F}_q)$*, llavors* M *és del tipus de conjugació:*

(1) $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ *o* $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ *si i només si* $\mathrm{ord}(M) \mid (q-1)$.

(2) $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ *si i només si* $p \mid \mathrm{ord}(M)$.

(3) $\left(\begin{smallmatrix} 0 & -b \\ 1 & -a \end{smallmatrix}\right)$ *si i només si* $\mathrm{ord}(M) \nmid (q-1)$ *i* $p \nmid \mathrm{ord}(M)$.

Demostració. Veiem que tot $a \in \mathbb{F}_q^*$ té ordre divisor de $q-1$ perquè $|\mathbb{F}_q^*| = q-1$ i que tot $\alpha \in \mathbb{F}_{q^2}^* \setminus \mathbb{F}_q^*$ compleix que $(q-1) \nmid \mathrm{ord}(\alpha)$ ja que $\mathbb{F}_{q^2}^*$ és cíclic, i per tant, $\mathbb{F}_q^*$ és l'únic subgrup d'ordre $q-1$ de $\mathbb{F}_{q^2}^*$. Aleshores com $\mathrm{mcd}(p, |\mathbb{F}_q^*|) = \mathrm{mcd}(p, |\mathbb{F}_{q^2}^*|) = 1$, per la Proposició 4.1.1 ja tenim el resultat que buscàvem. □

4.2 Subgrups

Ara introduïm els subgrups de $\mathrm{GL}_2(\mathbb{F}_q)$ següents:

(1) El grup $\mathrm{SL}_2(\mathbb{F}_q) = \{M \in \mathrm{GL}_2(\mathbb{F}_q) \mid \det(M) = 1\}$ és el grup lineal especial.

(2) El grup $B := \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)\}$ s'anomena subgrup de Borel estàndard. Diem que un subgrup de $\mathrm{GL}_2(\mathbb{F}_q)$ és de Borel si és conjugat amb B.

(3) El grup $\mathfrak{S} := \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)\}$ és el subgrup escalar i també és el centre de $\mathrm{GL}_2(\mathbb{F}_q)$.

(4) El grup $\mathfrak{D} := \{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)\}$ s'anomena subgrup diagonal.

(5) Diem que un subgrup de $\mathrm{GL}_2(\mathbb{F}_q)$ és de Cartan escindit si és isomorf a $\mathbb{F}_q^* \times \mathbb{F}_q^*$.

(6) Un subgrup de $\mathrm{GL}_2(\mathbb{F}_q)$ isomorf a $\mathbb{F}_{q^2}^*$ és un subgrup de Cartan no escindit.

Denotem els subgrups de Borel, de Cartan escindits i de Cartan no escindits com $\mathfrak{B}$,$\mathfrak{Z}$ i $\mathfrak{T}$ respectivament.

Definició 4.2.1. Sigui S un subconjunt d'un grup G, definim el normalitzador de S en G com

$$\mathcal{N}(S) = \{g \in G \,|\, gSg^{-1} = S\}.$$

Proposició 4.2.2. *Sigui $\mathfrak{Z}$ un subgrup de Cartan escindit, $\mathfrak{Z}$ és conjugat amb $\mathfrak{D}$. Per això, sigui $\mathfrak{Z} = M\mathfrak{D}M^{-1}$ per un $M \in \mathrm{GL}_2(\mathbb{F}_q)$, llavors*

$$\mathcal{N}(\mathfrak{Z}) = \begin{cases} \mathrm{GL}_2(\mathbb{F}_2) & \text{si } q = 2, \\ \langle \mathfrak{Z}, M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)M^{-1} \rangle & \text{si } q \neq 2. \end{cases}$$

En particular, $\mathcal{N}(\mathfrak{Z})$ és no abelià i $[\mathcal{N}(\mathfrak{Z}) : \mathfrak{Z}] = \begin{cases} 6 & \text{si } q = 2, \\ 2 & \text{si } q \neq 2. \end{cases}$

Demostració. Si $q = 2$, $\mathfrak{Z} = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\} = \mathfrak{D}$, i per tant, $\mathcal{N}(\mathfrak{Z}) = \mathrm{GL}_2(\mathbb{F}_2)$.

Si $q \neq 2$, sigui $\mathfrak{Z} = \langle \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \rangle \cong \mathbb{F}_q^* \times \mathbb{F}_q^*$, pel Lema 4.1.3 sabem que existeix $M' \in \mathrm{GL}_2(\mathbb{F}_q)$ tal que $M'\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(M')^{-1} = \left(\begin{smallmatrix} a' & 0 \\ 0 & d' \end{smallmatrix}\right) \in \mathfrak{D}$. Ara sigui $\left(\begin{smallmatrix} e' & f' \\ g' & h' \end{smallmatrix}\right) = M'\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)(M')^{-1}$, aquesta commuta amb $\left(\begin{smallmatrix} a' & 0 \\ 0 & d' \end{smallmatrix}\right)$, cosa que implica que $f' = g' = 0$ o $a' = d'$. En el primer cas, ja tenim que $M'\mathfrak{Z}(M')^{-1} = \mathfrak{D}$, i en el segon, $\langle \left(\begin{smallmatrix} a' & 0 \\ 0 & d' \end{smallmatrix}\right) \rangle = \mathfrak{S}$ és el centre de $\mathrm{GL}_2(\mathbb{F}_q)$ i és invariant per conjugacions, així que podem calcular $M'' \in \mathrm{GL}_2(\mathbb{F}_q)$ de manera que $M''\left(\begin{smallmatrix} e' & f' \\ g' & h' \end{smallmatrix}\right)(M'')^{-1} \in \mathfrak{D}$ i obtenim que $(M''M')\mathfrak{Z}(M''M')^{-1} = \mathfrak{D}$. A partir d'ara denotem M com la matriu de $\mathrm{GL}_2(\mathbb{F}_q)$ que conjuga $\mathfrak{Z}$ amb $\mathfrak{D}$.

Sigui $N = \left(\begin{smallmatrix} x & y \\ z & t \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)$, llavors calculem que

$$N\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)N^{-1} \in \mathfrak{D} \text{ per tot } a, b \in \mathbb{F}_q^* \iff x = t = 0 \text{ o } y = z = 0.$$

Com a conseqüència, $\mathcal{N}(\mathfrak{D}) = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) \,|\, a, b \in \mathbb{F}_q^*\} = \langle \mathfrak{D}, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle$ i deduïm que $\mathcal{N}(\mathfrak{Z}) = \langle \mathfrak{Z}, M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)M^{-1} \rangle = M\langle \mathfrak{D}, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \rangle M^{-1} = M\mathcal{N}(\mathfrak{D})M^{-1}$ perquè

$$\begin{aligned} M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)M^{-1}\mathfrak{Z}(M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)M^{-1})^{-1} &= M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)M^{-1}M\mathfrak{D}M^{-1}M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1}M^{-1} \\ &= M\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\mathfrak{D}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1}M^{-1} \\ &= M\mathfrak{D}M^{-1} = \mathfrak{Z}. \end{aligned}$$

Per últim, com $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$ i, si $q \neq 2$, $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & a \\ b & 0 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & b \\ a & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ per $a, b \in \mathbb{F}_q^*$ diferents, tenim que $\mathcal{N}(\mathfrak{Z}) = M\mathcal{N}(\mathfrak{D})M^{-1}$ sempre és no abelià. □

Lema 4.2.3. *Suposant que q és parell, si $\delta, \delta' \in \mathbb{F}_q^*$ són tals que $x^2 + x + \delta$ i $x^2 + x + \delta'$ són irreductibles a $\mathbb{F}_q[x]$, aleshores $x^2 + x + \delta + \delta'$ no ho és.*

Demostració. Sigui $\varphi : (\mathbb{F}_q, +) \to (\mathbb{F}_q, +)$ l'aplicació donada per $\varphi(x) = x^2 + x$, aquesta és un morfisme de grups perquè

$$\varphi(x+y) = (x+y)^2 + x + y = x^2 + x + y^2 + y = \varphi(x) + \varphi(y).$$

Així, com $\varphi(x) = 0$ si i només si $x = 0$ o $x = 1$, tenim que $\ker(\varphi) = (\mathbb{F}_2, +)$ i també que $(\varphi(\mathbb{F}_q), +) \cong (\mathbb{F}_q, +)/(\mathbb{F}_2, +)$. Notem que $\alpha \in \varphi(\mathbb{F}_q)$ si i només si $x^2 + x + \alpha \in \mathbb{F}_q[x]$ no és irreductible.

Ara sigui $\delta \in \mathbb{F}_q^*$ tal que $x^2 + x + \delta \in \mathbb{F}_q[x]$ és irreductible, definim $\varphi_\delta : \mathbb{F}_q \to \mathbb{F}_q$ de manera que $\varphi_\delta(x) = x^2 + x + \delta$. Si suposem que existeix $\beta \in \varphi(\mathbb{F}_q) \cap \varphi_\delta(\mathbb{F}_q)$, siguin $\alpha_1, \alpha_2 \in \mathbb{F}_q$ tals que $\alpha_1^2 + \alpha_1 = \beta$ i $\alpha_2^2 + \alpha_2 + \delta = \beta$, llavors $(\alpha_1 + \alpha_2)^2 + \alpha_1 + \alpha_2 + \delta = \alpha_1^2 + \alpha_1 + \alpha_2^2 + \alpha_2 + \delta = 0$ i arribem a una contradicció. Deduïm que $\varphi(\mathbb{F}_q) \cap \varphi_\delta(\mathbb{F}_q) = \varnothing$ i com $|\varphi(\mathbb{F}_q)| + |\varphi_\delta(\mathbb{F}_q)| = 2|\varphi(\mathbb{F}_q)| = 2|\mathbb{F}_q|/|\mathbb{F}_2| = q = |\mathbb{F}_q|$, $\varphi(\mathbb{F}_q) \cup \varphi_\delta(\mathbb{F}_q) = \mathbb{F}_q$. Per últim, sigui $\delta' \in \mathbb{F}_q^*$ de manera que $x^2 + x + \delta' \in \mathbb{F}_q[x]$ és irreductible, $\delta' \in \varphi_\delta(\mathbb{F}_q)$ ja que $\delta' \notin \varphi(\mathbb{F}_q)$, i per tant, $\delta + \delta' \in \varphi(\mathbb{F}_q)$, és a dir, $x^2 + x + \delta + \delta'$ no és irreductible. □

Proposició 4.2.4. *Sigui $\mathfrak{T}$ un subgrup de Cartan no escindit, aleshores ocorre que:*

(1) Si q és parell, $\mathfrak{T}$ és conjugat amb

$$\mathfrak{E} = \{ \left(\begin{smallmatrix} a+b & b\delta \\ b & a \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_q \text{ tal que } (a,b) \neq (0,0) \}$$

on es fixa $\delta \in \mathbb{F}_q^*$ de manera que $x^2 + x + \delta \in \mathbb{F}_q[x]$ és un polinomi irreductible. Així, sigui $\mathfrak{T} = M\mathfrak{E}M^{-1}$ per un cert $M \in \mathrm{GL}_2(\mathbb{F}_q)$, $\mathcal{N}(\mathfrak{T}) = \langle \mathfrak{T}, M \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) M^{-1} \rangle$.

(2) Si q és senar, $\mathfrak{T}$ és conjugat amb

$$\mathfrak{F} = \{ \left(\begin{smallmatrix} a & b\varepsilon \\ b & a \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_q \text{ tal que } (a,b) \neq (0,0) \}$$

on $\varepsilon \in \mathbb{F}_q^*$ és un no quadrat fixat. Per això, sigui $\mathfrak{T} = N\mathfrak{F}N^{-1}$ per un $N \in \mathrm{GL}_2(\mathbb{F}_q)$, llavors $\mathcal{N}(\mathfrak{T}) = \langle \mathfrak{T}, N \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) N^{-1} \rangle$.

En qualsevol cas, $\mathcal{N}(\mathfrak{T})$ és no abelià i $[\mathcal{N}(\mathfrak{T}) : \mathfrak{T}] = 2$.

Demostració. (1) Sigui $\alpha \in \mathbb{F}_{q^2}$ una arrel de $x^2 + x + \delta$, veiem que $\mathfrak{E} \cong \mathbb{F}_q(\alpha)^* \cong \mathbb{F}_{q^2}^*$ via $\left(\begin{smallmatrix} a+b & b\delta \\ b & a \end{smallmatrix}\right) \mapsto a + b\alpha$ ja que

$$\left(\begin{smallmatrix} a+b & b\delta \\ b & a \end{smallmatrix}\right) \left(\begin{smallmatrix} c+d & d\delta \\ d & c \end{smallmatrix}\right) = \left(\begin{smallmatrix} ac+bd\delta+ad+bc+bd & (ad+bc+bd)\delta \\ ad+bc+bd & ac+bd\delta \end{smallmatrix}\right) \mapsto ac + bd\delta + (ad+bc+bd)\alpha = (a+b\alpha)(c+d\alpha).$$

Sigui $\delta' \in \mathbb{F}_q^*$ tal que $x^2 + x + \delta' \in \mathbb{F}_q[x]$ és irreductible, aleshores $x^2 + x + \delta + \delta'$ no és irreductible pel Lema 4.2.3. Per això, sigui $\alpha \in \mathbb{F}_q$ tal que $\alpha^2 + \alpha + \delta + \delta' = 0$, la classe de conjugació de $\mathfrak{E}$ no depèn de la tria de δ perquè $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} a+b & b\delta \\ b & a \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} a+b\alpha+b & b\delta' \\ b & a+b\alpha \end{smallmatrix}\right)$.

Així, sigui $\mathfrak{T} = \langle \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \rangle$, pel Lema 4.1.3 sabem que hi ha una matriu $M' \in \mathrm{GL}_2(\mathbb{F}_q)$ de manera que $M' \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) (M')^{-1} = \left(\begin{smallmatrix} 0 & f' \\ 1 & h' \end{smallmatrix}\right)$ amb $x^2 + h'x + f' \in \mathbb{F}_q[x]$ irreductible. Com $\mathrm{car}(\mathbb{F}_q) = 2$, $h' \neq 0$ i podem prendre $\delta = f'/(h')^2$ ja que

$$\frac{x^2 + h'x + f'}{(h')^2} = \left(\frac{x}{h'}\right)^2 + \frac{x}{h'} + \frac{f'}{(h')^2}.$$

Com $\left(\begin{smallmatrix} 1/h' & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & f' \\ 1 & h' \end{smallmatrix}\right) \left(\begin{smallmatrix} 1/h' & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} 0 & h'\delta \\ h' & h' \end{smallmatrix}\right) \in \mathfrak{E}$, escollim $M = M' \left(\begin{smallmatrix} 1/h' & 0 \\ 0 & 1 \end{smallmatrix}\right)$ i com $\mathfrak{E}$ és cíclic, obtenim que $\mathfrak{E} = \langle M \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) M^{-1} \rangle = M\mathfrak{T}M^{-1}$. A partir d'aquest punt, la demostració és la mateixa que la de la Proposició 4.2.2 excepte que calculem que

$$\mathcal{N}(\mathfrak{E}) = \{ \left(\begin{smallmatrix} a+b & b\delta \\ b & a \end{smallmatrix}\right), \left(\begin{smallmatrix} a & a+b\delta \\ b & a \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_q^* \} = \langle \mathfrak{E}, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle.$$

(2) Primer, observem que $\mathfrak{F} \cong \mathbb{F}_q(\sqrt{\varepsilon})^* \cong \mathbb{F}_{q^2}^*$ via $\left(\begin{smallmatrix} a & b\varepsilon \\ b & a \end{smallmatrix}\right) \mapsto a + b\sqrt{\varepsilon}$ ja que

$$\left(\begin{smallmatrix} a & b\varepsilon \\ b & a \end{smallmatrix}\right)\left(\begin{smallmatrix} c & d\varepsilon \\ d & c \end{smallmatrix}\right) = \left(\begin{smallmatrix} ac+bd\varepsilon & (ad+bc)\varepsilon \\ ad+bc & ac+bd\varepsilon \end{smallmatrix}\right) \mapsto ac + bd\varepsilon + (ad+bc)\sqrt{\varepsilon} = (a+b\sqrt{\varepsilon})(c+d\sqrt{\varepsilon}).$$

A continuació, sigui $\varepsilon' \in \mathbb{F}_q^*$ un no quadrat, coneixem que ε'/ε és un quadrat, és a dir existeix $\alpha \in \mathbb{F}_q^*$ tal que $\alpha^2 = \varepsilon'/\varepsilon$ i com $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b\varepsilon \\ b & a \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} a\alpha & (b/\alpha)\varepsilon' \\ b/\alpha & a\alpha \end{smallmatrix}\right)$, la tria de ε és independent de la classe de conjugació de $\mathfrak{F}$.

Ara sigui $\mathfrak{T} = \langle \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \rangle$, pel Lema 4.1.3 sabem que hi ha una matriu $N' \in \mathrm{GL}_2(\mathbb{F}_q)$ de manera que $N'\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)(N')^{-1} = \left(\begin{smallmatrix} 0 & -f' \\ 1 & -h' \end{smallmatrix}\right)$ amb $x^2 + h'x + f' \in \mathbb{F}_q[x]$ irreductible, i per tant, $f' \neq 0$. Ara podem escollir $\varepsilon = a^2/4 - b$ perquè

$$x^2 + h'x + f = \left(x + \frac{h'}{2}\right)^2 - \left(\frac{a^2}{4} - b\right).$$

Com $\left(\begin{smallmatrix} -1 & h'/2 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -f' \\ 1 & -h' \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & h'/2 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} -h'/2 & -\varepsilon \\ -1 & -h'/2 \end{smallmatrix}\right) \in \mathfrak{F}$, prenem $N = N'\left(\begin{smallmatrix} -1 & h'/2 \\ 0 & 1 \end{smallmatrix}\right)$ i com $\mathfrak{F}$ és cíclic, trobem que $\mathfrak{F} = \langle N\left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right)N^{-1} \rangle = N\mathfrak{T}N^{-1}$. A partir d'aquí, la demostració és igual a la de la Proposició 4.2.2 excepte que

$$\mathcal{N}(\mathfrak{F}) = \left\{ \left(\begin{smallmatrix} a & b\varepsilon \\ b & a \end{smallmatrix}\right), \left(\begin{smallmatrix} a & b\varepsilon \\ -b & -a \end{smallmatrix}\right) \mid a, b \in \mathbb{F}_q^* \right\} = \langle \mathfrak{F}, \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \rangle. \qquad \square$$

Com $\mathfrak{S}$ és el centre de $\mathrm{GL}_2(\mathbb{F}_q)$, és un subgrup normal i podem definir $\mathrm{PGL}_2(\mathbb{F}_q) = \mathrm{GL}_2(\mathbb{F}_q)/\mathfrak{S}$ el grup lineal projectiu. Sigui $\pi : \mathrm{GL}_2(\mathbb{F}_q) \to \mathrm{PGL}_2(\mathbb{F}_q)$ la projecció usual i sigui G un subgrup de $\mathrm{GL}_2(\mathbb{F}_q)$, aleshores diem que $\pi(G)$ és la imatge de G en $\mathrm{PGL}_2(\mathbb{F}_q)$.

Teorema 4.2.5 ([Lan76], Teoremes 2.2 i 2.3 del Capítol XI)**.** *Sigui G un subgrup de $\mathrm{GL}_2(\mathbb{F}_q)$ i sigui H la imatge de G en $\mathrm{PGL}_2(\mathbb{F}_q)$, si l'ordre de G és divisible per p llavors:*

(1) O bé G està contingut en un subgrup de Borel.

(2) O bé G conté a $\mathrm{SL}_2(\mathbb{F}_q)$.

Si l'ordre de G és coprimer amb p, aleshores ocorre una de les següents:

(1) H és cíclic i G està contingut en un subgrup de Cartan.

(2) H és dièdric i G està contingut en el normalitzador d'un subgrup de Cartan, però no en un subgrup de Cartan.

(3) H és isomorf a A_4, S_4 o A_5.

5 Mòduls de Drinfeld sobre cossos globals

En aquesta secció assumirem que K és una extensió finita de F i (K,γ) és un A-cos via el morfisme injectiu natural $\gamma : A \hookrightarrow F \hookrightarrow K$. Escriurem $\gamma(a) = a$ per simplificar la notació i denotarem B com la clausura entera de A en K.

5.1 El tipus de conjugació de $\mathrm{Frob}_{\mathfrak{P}}$

Sigui ϕ un mòdul de Drinfeld sobre F de rang r i sigui $\mathfrak{p} \in A$ un primer de bona reducció de ϕ, en aquest apartat suposarem que $\mathfrak{n} \in A$ és coprimer amb $\mathfrak{p}$ primer i que $K_{\mathfrak{n}} = F(\phi[\mathfrak{n}])$ és el cos de $\mathfrak{n}$-divisió de ϕ. Sabem que l'extensió $K_{\mathfrak{n}}/F$ és de Galois. Així, sigui $B_{\mathfrak{n}}$ la clausura entera de A en $K_{\mathfrak{n}}$, si $\mathfrak{P} \in B_{\mathfrak{n}}$ és un primer que divideix a $\mathfrak{p}$, obtenim el següent diagrama:

$$\begin{array}{ccccc} \mathfrak{P} & \hookrightarrow & B_{\mathfrak{n}} & \hookrightarrow & K_{\mathfrak{n}} \\ & & | & & | \\ \mathfrak{p} & \hookrightarrow & A & \hookrightarrow & F \end{array}$$

Aleshores com $\mathfrak{p}$ és no-ramificat[1] a $K_{\mathfrak{n}}$ pel Teorema 2.7.9, tenim un element de Frobenius ben definit $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(K_{\mathfrak{n}}/F)$[2] que està unívocament per la següent condició:

$$\mathrm{Frob}_{\mathfrak{P}}(\alpha) \equiv \alpha^{|\mathbb{F}_{\mathfrak{p}}|} \pmod{\mathfrak{P}} \text{ per tot } \alpha \in \phi[\mathfrak{n}].$$

Així, podem definir el polinomi característic de $\mathrm{Frob}_{\mathfrak{P}}$ vist com a element de $\mathrm{GL}_r(A/(\mathfrak{n}))$ i el denotem $P_{\phi,\mathfrak{p},\mathfrak{n}}(x) \in (A/(\mathfrak{n}))[x]$. Observem que com $\mathrm{Frob}_{\mathfrak{P}}$ i $\mathrm{Frob}_{\mathfrak{P}'}$ estan conjugats si $\mathfrak{P}' \in B_{\mathfrak{n}}$ és un altre primer que divideix $\mathfrak{p}$, $P_{\phi,\mathfrak{p},\mathfrak{n}}$ no depèn de l'elecció de $\mathfrak{P}$ o de la tria d'una base de $\phi[\mathfrak{n}]$.

La reducció mòdul $\mathfrak{P}$ indueix un isomorfisme canònic de A-mòduls

$$\iota : \phi[\mathfrak{n}] \xrightarrow{\cong} \mathrm{Red}(\phi,\mathfrak{p})[\mathfrak{n}].$$

Aquest és compatible amb l'acció de $\mathrm{Frob}_{\mathfrak{P}}$ sobre $\phi[\mathfrak{n}]$ i la de $\mathrm{Frob}_{\mathbb{F}_{\mathfrak{p}}}$ sobre $\mathrm{Red}(\phi,\mathfrak{p})[\mathfrak{n}]$ ja que

$$\overline{\mathrm{Frob}_{\mathfrak{P}}(\alpha)} = \overline{\alpha}^{|\mathbb{F}_{\mathfrak{p}}|} = \mathrm{Frob}_{\mathbb{F}_{\mathfrak{p}}}(\overline{\alpha}) \text{ per tot } \alpha \in \phi[\mathfrak{n}]$$

on $\overline{*}$ és la reducció mòdul $\mathfrak{P}$. Això implica que $P_{\phi,\mathfrak{p},\mathfrak{n}}$ és igual al polinomi característic de $\mathrm{Frob}_{\mathbb{F}_{\mathfrak{p}}}$ actuant sobre $\mathrm{Red}(\phi,\mathfrak{p})[\mathfrak{n}]$. Per altra banda, per la Proposició 3.2.2 aquest últim és igual a la reducció mòdul $\mathfrak{n}$ de $P_{\mathrm{Red}(\phi,\mathfrak{p})}$ el qual hem estudiat a l'apartat 3.2, és a dir

$$P_{\phi,\mathfrak{p},\mathfrak{n}} \equiv P_{\mathrm{Red}(\phi,\mathfrak{p})} \pmod{\mathfrak{n}}.$$

La utilitat d'aquesta congruència és que calcular $P_{\mathrm{Red}(\phi,\mathfrak{p})}$ és relativament fàcil, i una vegada fet això, només s'ha de reduir mòdul $\mathfrak{n}$ per obtenir $P_{\phi,\mathfrak{p},\mathfrak{n}}$.

Si suposem que ϕ té rang 2 i que $\mathfrak{n} = \mathfrak{l}$ és primer, la classe de conjugació de $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{GL}_2(A/(\mathfrak{l}))$ està determinada pel polinomi característic per la Proposició 4.1.1 a no ser que $P_{\phi,\mathfrak{p},\mathfrak{l}}$ tingui una arrel doble. En aquest cas, si $P_{\phi,\mathfrak{p},\mathfrak{l}}(x) = (x-a)^2$, la classe de conjugació és del tipus $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ si $p \mid \mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}})$ i si no, és del tipus $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ pel Lema 4.1.3.

Per calcular l'ordre de $\mathrm{Frob}_{\mathfrak{P}}$ tenim el següent resultat:

[1] En aquest cas ens referim a la noció clàssica de no-ramificació. Les definicions d'aquest concepte, d'escissió i d'inèrcia d'un ideal primer les podem trobar a la pàgina 49 de [Neu99].

[2] Les propietats de $\mathrm{Frob}_{\mathfrak{P}}$ usades en aquest apartat estan explicades a les pàgines 69-70 de [MIT21].

Teorema 5.1.1 ([Geb03], Teorema 4.1.7). *Siguin ϕ un mòdul de Drinfeld sobre F de rang r, $\mathfrak{p} \in A$ un primer de bona reducció de ϕ i $\mathfrak{l} \in A$ un primer diferent de $\mathfrak{p}$, si $g(x) = \mathrm{Red}(\phi, \mathfrak{p})_{\mathfrak{l}}(x) = a_0 x + a_1 x^q + \cdots + a_{q^{r\cdot\deg(\mathfrak{p})}} x^{q^{r\cdot\deg(\mathfrak{p})}}$ i $f(x) = a_{q^{r\cdot\deg(\mathfrak{p})}}^{-1} g(x)$, llavors*

$$\mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}}) = \min\{n \in \mathbb{N} \mid x^{|\mathbb{F}_{\mathfrak{p}}|^n} \equiv x \pmod{f(x)}\} = |\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}(\mathrm{Red}(\phi, \mathfrak{p})[\mathfrak{l}])/\mathbb{F}_{\mathfrak{p}})|.$$

Corol·lari 5.1.2. *Sigui ϕ un mòdul de Drinfeld sobre F de rang 2 i siguin $\mathfrak{p}, \mathfrak{l}$ i $f(x)$ com al Teorema 5.1.1, si $P_{\phi,\mathfrak{p},\mathfrak{l}}(x) = (x-a)^2$ per algun $a \in \mathbb{F}_{\mathfrak{p}}$, aleshores són equivalents:*

(1) $\mathrm{Frob}_{\mathfrak{P}}$ *és conjugat amb* $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$.

(2) $x^{|\mathbb{F}_{\mathfrak{p}}|^{\mathrm{ord}(a)}} \equiv x \pmod{f(x)}$.

(3) $x^{|\mathbb{F}_{\mathfrak{p}}|^{(|\mathbb{F}_{\mathfrak{l}}|-1)}} \equiv x \pmod{f(x)}$.

Demostració. És conseqüència directa del Lema 4.1.3 i del Teorema 5.1.1. □

5.2 El mòdul de Carlitz

Ara assumim que $\Delta \in F \setminus \{0\}$ i que ϕ és un mòdul de Drinfeld de rang 1 sobre F donat per $\phi_T\{\tau\} = T + \Delta\tau$ el qual denotarem $C^{(\Delta)}$. Recordem que el mòdul de Carlitz és $C = C^{(1)}$ i diem que $C^{(\Delta)}$ és el twist de C per Δ. Sigui $\mathfrak{n} \in A$, també escriurem $K_{\mathfrak{n}}^{(\Delta)} = F(C^{(\Delta)}[\mathfrak{n}])$, i així, com $C^{(\Delta)}$ és separable, $K_{\mathfrak{n}}^{(\Delta)}/F$ és una extensió de Galois i tenim el següent teorema:

Teorema 5.2.1 ([Geb03], Teorema 4.4.10). *Usant aquesta notació, sigui $\mathfrak{n} \in A$ de manera que $C^{(\Delta)}$ té bona reducció respecte tot primer divisor de $\mathfrak{n}$, llavors ocorre que:*

(1) $\mathrm{Gal}(K_{\mathfrak{n}}^{(\Delta)}/F) \cong (A/(\mathfrak{n}))^*$.

(2) El cos de constants de $K_{\mathfrak{n}}^{(\Delta)}$ *és* $\mathbb{F}_q$.

Observació 5.2.2. Si denotem $K_{\mathfrak{n}} = F(C[\mathfrak{n}])$, aleshores $\mathrm{Gal}(K_{\mathfrak{n}}/F) \cong (A/(\mathfrak{n}))^*$ ja que C té bona reducció respecte tot primer de A.

Com $C^{(\Delta)}[\mathfrak{n}] \cong A/(\mathfrak{n})$ vist com un A-mòdul amb l'acció de $C^{(\Delta)}$ pel Corol·lari 2.4.5, sabem que existeix $\zeta_{\mathfrak{n}} \in C^{(\Delta)}[\mathfrak{n}]$ de manera que

$$C^{(\Delta)}[\mathfrak{n}] = \{C_a^{(\Delta)}(\zeta_{\mathfrak{n}}) \mid a \in A \text{ i } \deg(a) < \deg(\mathfrak{n})\}.$$

Això es deu a que $C_{\mathfrak{n}}^{(\Delta)}(C_a^{(\Delta)}(\zeta_{\mathfrak{n}})) = C_a^{(\Delta)}(C_{\mathfrak{n}}^{(\Delta)}(\zeta_{\mathfrak{n}})) = C_a^{(\Delta)}(0) = 0$ i a que $\mathfrak{n}$ és l'element de menor grau llevat de múltiples constants complint que $\zeta_{\mathfrak{n}} \in C^{(\Delta)}[\mathfrak{n}]$ per la tria de $\zeta_{\mathfrak{n}}$. Per tant, si existeixen $a, b \in A$ tals que $\deg(a), \deg(b) < \deg(\mathfrak{n})$ i que $C_a^{(\Delta)}(\zeta_{\mathfrak{n}}) = C_b^{(\Delta)}(\zeta_{\mathfrak{n}})$, llavors $C_{a-b}^{(\Delta)}(\zeta_{\mathfrak{n}}) = 0 \iff a = b$.

Definició 5.2.3. Diem que tota $\zeta \in C^{(\Delta)}[\mathfrak{n}]$ amb aquesta propietat és una *arrel primitiva $\mathfrak{n}$-èssima* de $C^{(\Delta)}$. Notem que això passa si i només si ζ és de la forma $C_a^{(\Delta)}(\zeta_{\mathfrak{n}})$ per algun $a \in A$ coprimer amb $\mathfrak{n}$.

Així, $K_{\mathfrak{n}}^{(\Delta)} = F(\zeta_{\mathfrak{n}})$, i per tant, tot $\sigma \in \mathrm{Gal}(K_{\mathfrak{n}}^{(\Delta)}/F)$ ve unívocament determinat per $\sigma(\zeta_{\mathfrak{n}})$ que ha de ser una arrel primitiva $\mathfrak{n}$-èssima de $C^{(\Delta)}$. Això implica que existeix $a \in A$ coprimer amb $\mathfrak{n}$ tal que $\sigma(\zeta_{\mathfrak{n}}) = C_a^{(\Delta)}(\zeta_{\mathfrak{n}})$ i obtenim que si ζ és una altra arrel primitiva $\mathfrak{n}$-èssima, llavors existeix $b \in A$ coprimer amb $\mathfrak{n}$ tal que $\sigma(\zeta_{\mathfrak{n}}) = C_b^{(\Delta)}(\zeta_{\mathfrak{n}})$ i

$$\sigma(\zeta) = \sigma(C_b^{(\Delta)}(\zeta_{\mathfrak{n}})) = C_b^{(\Delta)}(\sigma(\zeta_{\mathfrak{n}})) = C_b^{(\Delta)}(C_a^{(\Delta)}(\zeta_{\mathfrak{n}})) = C_a^{(\Delta)}(C_b^{(\Delta)}(\zeta_{\mathfrak{n}})) = C_a^{(\Delta)}(\zeta).$$

En aquest cas, escriurem que σ és σ_a, i si prenem les hipòtesis del Teorema 5.2.1, l'isomorfisme ve donat per l'aplicació

$$\begin{aligned} \mathrm{Gal}(K_{\mathfrak{n}}^{(\Delta)}/F) &\longrightarrow (A/(\mathfrak{n}))^* \\ \sigma_a &\longmapsto a \pmod{\mathfrak{n}}. \end{aligned}$$

En general, $[K_{\mathfrak{n}}^{(\Delta)} : F]$ pot ser més petit que $|(A/(\mathfrak{n}))^*|$ i l'estudi complet d'aquest esdeveniment està fet a [Gek16] d'on trobem el següent:

Teorema 5.2.4 ([Gek16], Teorema 3.13)**.** *Usant la mateixa notació,* $|(A/(\mathfrak{n}))^*|/[K_{\mathfrak{n}}^{(\Delta)} : F]$ *és un enter que divideix a* $q-1$.

Exemple 5.2.5. Si considerem C el mòdul de Carlitz sobre F i $\mathfrak{n} = T^2+T+1$, pel Teorema 5.2.1 coneixem que

$$G = \mathrm{Gal}(K_{T^2+T+1}/F) \cong (A/(T^2+T+1))^*.$$

Ara volem saber per quins valors de $q = p^n$, existeix $a \in \mathbb{F}_q$ tal que $T^2+T+1 = (T-a)^2 = = T^2 - 2aT + a^2$ i això ocorre si i només si $-2a = 1$ i $a^2 = 1$. Concloem que $p = \mathrm{car}(\mathbb{F}_q) = 3$ i $a = 1$. Aleshores com en aquest cas $|G| = q(q-1)$ i $\mathrm{mcd}(q-1, q) = 1$, existeixen H_1 i H_2 subgrups de G amb ordre $q-1$ i q respectivament de manera que $G \cong H_1 \times H_2$ pel teorema xinès de les restes. Veiem fàcilment que $H_1 = \mathbb{F}_q^*$. Així, sigui $\lambda = \alpha(T-\beta) \in (A/(T^2+T+1))^*$, $\alpha \in \mathbb{F}_q^*$, $\beta \in \mathbb{F}_q \setminus \{1\}$ i $\lambda^3 = \alpha^3(T-\beta)^3 = \alpha^3(T^3-\beta^3) = \alpha^3(1-\beta^3) \in \mathbb{F}_q^* = H_1$, i per tant, tot element de H_2 té ordre 3. Com $q = 3^n$ i $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z}$, això implica que

$$G \cong H_1 \times H_2 \cong \mathbb{Z}/(q-1)\mathbb{Z} \times (\mathbb{Z}/3\mathbb{Z})^n.$$

Si suposem que $p \neq 3$, llavors T^2+T+1 o bé és irreductible o bé té dues arrels diferents. En el primer cas, $G \cong \mathbb{F}_{q^2}^* \cong \mathbb{Z}/(q^2-1)\mathbb{Z}$, i en el segon, $G \cong \mathbb{F}_q^* \times \mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z}$ pel teorema xinès de les restes. Per distingir cada cas usarem el següent lema:

Lema 5.2.6. *Sigui* $p \in \mathbb{N}$ *un primer diferent de* 3*,* x^2+x+1 *és irreductible a* $\mathbb{F}_p[x]$ *si i només si* $p = 2$ *o* $p \equiv 5 \pmod 6$.

Demostració. Primer observem que o bé $p = 2$, o bé $p \equiv 1 \pmod 6$ o bé $p \equiv 5 \pmod 6$ i que quan $p = 2$, x^2+x+1 no té arrels, és a dir, és irreductible.

Com $p \neq 3$ i $x^3-1 = (x-1)(x^2+x+1)$, x^2+x+1 no és irreductible a $\mathbb{F}_p[x]$ si i només si existeix $\lambda \in \mathbb{F}_p \setminus \{1\}$ tal que $\lambda^3 = 1$ i això ocorre si i només si $3 \mid (p-1)$, és a dir, $p \equiv 1 \pmod 6$. □

Per últim, sabem que si $q = p^n$ amb n senar el comportament de T^2+T+1 a $\mathbb{F}_q[T]$ és el mateix que a $\mathbb{F}_p[T]$ i si n és parell, T^2+T+1 no és irreductible. Com a conseqüència, suposant que $p \neq 3$, obtenim que

$$G \cong \begin{cases} \mathbb{F}_{q^2}^* \cong \mathbb{Z}/(q^2-1)\mathbb{Z} & \text{si } p = 2 \text{ o } p \equiv 5 \pmod 6 \text{ i } n \text{ és senar,} \\ \mathbb{F}_q^* \times \mathbb{F}_q^* \cong \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} & \text{si } p \equiv 1 \pmod 6 \text{ o } n \text{ és parell.} \end{cases}$$

5.3 Exemples de cossos de divisió de mòduls de Drinfeld

En aquest apartat construirem mòduls de Drinfeld ϕ de rang 2 sobre F explícits de manera que $F(\phi[T])$ el cos de T-divisió de ϕ compleix que $\mathrm{Gal}(F(\phi[T])/F)$ és isomorf a un dels següents subgrups de $\mathrm{GL}_2(\mathbb{F}_q)$:

- $\mathrm{GL}_2(\mathbb{F}_p)$ el grup lineal general per p primer,

- $\mathrm{SL}_2(\mathbb{F}_p)$ el grup lineal especial per p primer,
- $\mathfrak{B}$ un subgrup de Borel,
- $\mathfrak{Z}$ un subgrup de Cartan escindit,
- $\mathfrak{T}$ un subgrup de Cartan no escindit,
- $\mathcal{N}(\mathfrak{Z})$ el normalitzador d'un subgrup de Cartan escindit,
- $\mathcal{N}(\mathfrak{T})$ el normalitzador d'un subgrup de Cartan no escindit.

Recordem que tots aquests grups han estat estudiats a l'apartat 4.2. Aleshores pels dos primers casos ens serà útil el següent:

Proposició 5.3.1 ([Ser72], Proposició 19)**.** *Sigui V un espai vectorial de dimensió 2 sobre $\mathbb{F}_p$ on $p \in \mathbb{N}$ és un nombre primer i sigui $G \subseteq \mathrm{GL}(V)$ un subgrup d'automorfismes lineals de V, si assumim que $p \geq 5$ i que es verifiquen les següents hipòtesis:*

(1) G conté un element s tal que $\mathrm{Tr}(s) \neq 0$ i $\mathrm{Tr}(s)^2 - 4\det(s)$ és un quadrat de $\mathbb{F}_p$ diferent de 0.

(2) G conté un element s' tal que $\mathrm{Tr}(s') \neq 0$ i $\mathrm{Tr}(s')^2 - 4\det(s')$ no és un quadrat de $\mathbb{F}_p$.

(3) G conté un element s'' tal que $u = \mathrm{Tr}(s'')^2/\det(s'')$ és diferent de $0, 1, 2$ i 4 i $u^2 - 3u + 1 \neq 0$.

Llavors G conté $\mathrm{SL}(V)$. En particular, si $\det : G \to \mathbb{F}_p^*$ és exhaustiu, $G = \mathrm{GL}(V)$.

Prèviament a procedir amb els exemples farem un petit càlcul preliminar. Sigui ϕ un mòdul de Drinfeld de rang 2 sobre F definit per

$$\phi_T(x) = Tx + g(T)x^q + \Delta(T)x^{q^2} \text{ amb } g(T), \Delta(T) \in A,$$

si suposem que $g_2(c) \neq 0$ per algun $c \in \mathbb{F}_q^*$, aleshores $\mathfrak{p} := T - c$ és un primer de bona reducció de ϕ. La reducció està donada per $\overline{\phi}_T(x) = \mathrm{Red}(\phi, \mathfrak{p})(x) = cx + g(c)x^q + \Delta(c)x^{q^2}$ i utilitzant el Teorema 3.2.4 i la Proposició 3.2.8 obtenim que

$$P_{\bar{\phi}}(x) = x^2 + \frac{g(c)}{\Delta(c)}x + \frac{c - T}{\Delta(c)} \in A[x].$$

Ara sigui $\mathfrak{P}$ un primer de $F(\phi[T])$ que divideix a $\mathfrak{p}$, per la Proposició 3.2.2, coneixem que $P_{\phi,\mathfrak{p},T}$ és la reducció de $P_{\bar{\phi}}$ mòdul T, o equivalentment

$$\begin{aligned} \mathrm{Tr}(\rho_{\phi,T}(\mathrm{Frob}_{\mathfrak{P}})) &= -g(c)/\Delta(c), \\ \det(\rho_{\phi,T}(\mathrm{Frob}_{\mathfrak{P}})) &= c/\Delta(c). \end{aligned}$$

Per simplificar la notació en els exemples a continuació escriurem $\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}})$ i $\det(\mathrm{Frob}_{\mathfrak{P}})$ enlloc de $\mathrm{Tr}(\rho_{\phi,T}(\mathrm{Frob}_{\mathfrak{P}}))$ i $\det(\rho_{\phi,T}(\mathrm{Frob}_{\mathfrak{P}}))$.

Exemple 5.3.2 (Grup lineal general)**.** Usant la mateixa notació, escollim $g = \Delta = 1$, és a dir, considerem el mòdul de Drinfeld determinat per

$$\phi_T(x) = Tx + x^q + x^{q^2}.$$

Així, tenim que $\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}}) = -1$ i $\det(\mathrm{Frob}_{\mathfrak{P}}) = c$, i per tant,

$$\begin{aligned} \mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}})^2 - 4\det(\mathrm{Frob}_{\mathfrak{P}}) &= 1 - 4c \text{ i} \\ \mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}})^2/\det(\mathrm{Frob}_{\mathfrak{P}}) &= 1/c. \end{aligned}$$

Aleshores com c pot ser un element arbitrari de $\mathbb{F}_q^*$, les hipòtesis de la Proposició 5.3.1 es compleixen si $q = p \geq 5$ és primer. A més, com det : $\mathrm{Gal}(F(\phi[T])/F) \to \mathbb{F}_q^*$ és exhaustiva ja que $\det(\mathrm{Frob}_{\mathfrak{P}}) = c$, obtenim que

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{GL}_2(\mathbb{F}_p) \text{ per } p \geq 5.$$

Podem estendre aquest fet a $p = 2$ i $p = 3$ computant directament amb `Magma` utilitzant un programa semblant al de l'Exemple 2.4.6. Calculem que $|\mathrm{Gal}(F(\phi[T])/F)| = 6 = |\mathrm{GL}_2(\mathbb{F}_2)|$ si $p = 2$ i que $|\mathrm{Gal}(F(\phi[T])/F)| = 48 = |\mathrm{GL}_2(\mathbb{F}_3)|$ si $p = 3$. Com $\mathrm{Gal}(F(\phi[T])/F)$ sempre és isomorf a un subgrup de $\mathrm{GL}_2(\mathbb{F}_p)$, això implica que

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{GL}_2(\mathbb{F}_p) \text{ per } p \text{ primer.}$$

Exemple 5.3.3 (Grup lineal especial)**.** Ara assumim que $g = 1$ i $\Delta = T$ que és equivalent a triar el mòdul de Drinfeld definit per

$$\phi_T(x) = Tx + x^q + Tx^{q^2}.$$

En aquest cas, $\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}}) = -1/c$ i $\det(\mathrm{Frob}_{\mathfrak{P}}) = 1$, i per això,

$$\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}})^2 - 4\det(\mathrm{Frob}_{\mathfrak{P}}) = 1/c^2 - 4 \text{ i}$$
$$\mathrm{Tr}(\mathrm{Frob}_{\mathfrak{P}})^2/\det(\mathrm{Frob}_{\mathfrak{P}}) = 1/c^2.$$

Per comprovar que es verifiquen les hipòtesis de la Proposició 5.3.1 per $c \in \mathbb{F}_q^*$ qualsevol, usem el següent resultat:

Lema 5.3.4. *Siguin $q \in \mathbb{N}$ una potència primera senar i $a \in \mathbb{F}_q^*$ fixat, llavors el nombre de solucions de $x^2 - y^2 = a$ en $\mathbb{F}_q$ és igual a $q - 1$.*

Demostració. Si denotem $u = x + y$ i $v = x - y$, resoldre $x^2 - y^2 = a$ és equivalent a resoldre $uv = a$ amb $u, v \in \mathbb{F}_q$. Clarament les solucions d'aquesta última equació són $\{(u, a/u) \mid u \in \mathbb{F}_q^*\}$, cosa que implica que n'hi ha exactament $|\mathbb{F}_q^*| = q - 1$. □

Per una banda, per cada $d \in \mathbb{F}_q$ el nombre de solucions de $(1/c)^2 - 4 = d^2$ és 0 o 2 assumint que q és senar. Per altra banda, pel Lema 5.3.4, com $(1/c)^2 - 4 = d^2$ si i només si $(1/c)^2 - d^2 = 4$,

$$\sum_{d \in \mathbb{F}_q} |\{c \in \mathbb{F}_q^* \mid (1/c)^2 - 4 = d^2\}| = \begin{cases} q - 1 & \text{si } -1 \text{ no és un quadrat en } \mathbb{F}_q, \\ q - 3 & \text{si } -1 \text{ és un quadrat en } \mathbb{F}_q. \end{cases}$$

Això es deu a que si existeix $\alpha \in \mathbb{F}_q$ tal que $\alpha^2 = -1$, dues de les solucions comptabilitzades en el Lema 5.3.4 són $(0, 2\alpha)$ i $(0, -2\alpha)$, però $1/c \neq 0$. També notem que -4 és un quadrat en $\mathbb{F}_q$ si i només si -1 ho és ja que 4 sempre és igual a 2^2.

Per aquesta raó, mentre c varia en $\mathbb{F}_q^*$, $1/c^2 - 4$ és un quadrat diferent de 0 entre $(q-3)/2 - 1 = (q-5)/2$ i $(q-1)/2$ vegades. Com a conseqüència, les dues primeres hipòtesis de la Proposició 5.3.1 es compleixen si $q = p \geq 7$.

Així, per $c \in \mathbb{F}_q^*$, $1/c^2$ pren $(q-1)/2$ valors ja que q és senar i com $x^2 - 3x + 1$ té com a molt dues solucions en $\mathbb{F}_q$, es verifica la tercera hipòtesi de la Proposició 5.3.1 si $q = p \geq 13$ ja que $(q-1)/2 - 5 \geq 1$. En el cas de $q = 11$, podem prendre $c = 2$ i llavors $1/c^2 = 3$ que és diferent de $0, 1, 2$ i 4 i $3^2 - 3 \cdot 3 + 1 = 1 \neq 0$, és a dir, aquesta hipòtesi també és certa si $q = 11$. Per tant, $\mathrm{SL}_2(\mathbb{F}_p)$ és isomorf a un subgrup de $\mathrm{Gal}(F(\phi[T])/F)$ per $p \geq 11$ primer.

Ara sigui q una potència primera arbitrària i sigui ψ el mòdul de Drinfeld associat per l'emparellament de Weil a ϕ, aquest últim ve donat per

$$\psi_T(x) = Tx - Tx^q = T(x - x^q).$$

Per això, $\psi[T] = \mathbb{F}_q$, cosa que implica que pel Teorema 2.5.2 que

$$\{\det(M) \mid M \in \mathrm{Gal}(F(\phi[T])/F)\} = \mathrm{Gal}(F(\psi[T])/F) = \{1\}.$$

Com a conseqüència, $\mathrm{Gal}(F(\phi[T])/F)$ sempre és isomorf a un subgrup de $\mathrm{SL}_2(\mathbb{F}_q)$, i per tant,

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{SL}_2(\mathbb{F}_p) \text{ per } p \geq 11 \text{ primer.}$$

Com a l'Exemple 5.3.2 podem trobar per força bruta usant `Magma` que $|\mathrm{Gal}(F(\phi[T])/F)| = 6 = |\mathrm{SL}_2(\mathbb{F}_2)|$ si $p = 2$, $|\mathrm{Gal}(F(\phi[T])/F)| = 24 = |\mathrm{SL}_2(\mathbb{F}_3)|$ si $p = 3$, $|\mathrm{Gal}(F(\phi[T])/F)| = 120 = |\mathrm{SL}_2(\mathbb{F}_5)|$ si $p = 5$ i $|\mathrm{Gal}(F(\phi[T])/F)| = 336 = |\mathrm{SL}_2(\mathbb{F}_7)|$ si $p = 7$. En conclusió,

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{SL}_2(\mathbb{F}_p) \text{ per } p \text{ primer.}$$

Exemple 5.3.5 (Subgrup de Borel)**.** Sigui a un generador de $\mathbb{F}_q^*$ i sigui α una arrel de $x^{q-1} - a$, la resta d'arrels d'aquest polinomi són $\mathbb{F}_q^*$-múltiples de α. Aleshores com $F(\alpha)/F$ és una extensió de cossos de constants, aquesta és cíclica i tot primer és no-ramificat. A més, per un primer $\mathfrak{p}$ de A amb $\deg(\mathfrak{p}) = d$ tenim que

$$\mathrm{Frob}_{\mathfrak{p}}(\alpha) = \alpha^{|\mathbb{F}_{\mathfrak{p}}|} = b \cdot \alpha \text{ per algun } b \in \mathbb{F}_q^*.$$

Clarament $b = \alpha^{|\mathbb{F}_{\mathfrak{p}}|-1} = a^{|\mathbb{F}_{(\mathfrak{p}}|-1)/(q-1)} = a^{1+q+q^2\cdots+q^{d-1}} = a^d$ ja que $a^q = a$. Per això, b no depèn de l'elecció de α. A més, G_F el grup de Galois absolut de F permuta transitivament les arrels de $x^{q-1} - a$, i per tant, aquest és un polinomi irreductible i $[F(\alpha) : F] = q - 1$.

Considerem ϕ el mòdul de Drinfeld sobre F determinat per

$$\phi_T(x) = Tx + x^q - \frac{T+a}{a^2}x^{q^2}.$$

Notem que

$$\phi_T(\alpha) = \alpha\left(T + \alpha^{q-1} - \frac{T+a}{a^2}(\alpha^{q-1})^{q+1}\right) = \alpha\left(T + a - (T+a)a^{q-1}\right) = 0.$$

Com a conseqüència, $\mathbb{F}_q\alpha \subseteq \phi[T]$ és un subespai 1-dimensional que és Galois invariant. Escollint α com un dels elements de la base del $\mathbb{F}_q$-espai vectorial 2-dimensional $\phi[T]$, obtenim que $G := \mathrm{Gal}(F(\phi[T])/F)$ és isomorf a un subgrup de B el subgrup de Borel estàndard.

Per demostrar que $G \cong B$ basta amb provar que $q(q-1)^2 = |B|$ divideix a $|G|$. Sigui $\mathfrak{p} = T + a$, el polígon de Newton[1] de $\phi_T(x)/x$ respecte $v_{\mathfrak{p}}$ té dos segments amb pendents 0 i $1/(q(q-1))$ respectivament. Per això, l'índex de ramificació $e_{\mathfrak{p}}$ de $\mathfrak{p}$ és divisible per $q(q-1)$. Ara bé, com $F(\alpha) \subseteq F(\phi[T])$ i $F(\alpha)/F$ és una extensió de cossos de constants de grau $q-1$, l'índex residual $f_{\mathfrak{p}}$ de $\mathfrak{p}$ és divisible per $q-1$. Així, com $q(q-1)^2$ divideix a $e_{\mathfrak{p}}f_{\mathfrak{p}}$ que divideix a $|G|$, ja tenim el resultat que buscàvem i sabem que

$$\mathrm{Gal}(F(\phi[T])/F) \cong B = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_q)\}.$$

Observació 5.3.6. En aquest exemple hem vist que si $\phi[T]$ té un subespai 1-dimensional Galois invariant, llavors $\mathrm{Gal}(F(\phi[T])/F)$ ha de ser isomorf a un subgrup de B. En el següent, trobarem un mòdul de Drinfeld ϕ de manera que $\phi[T]$ tindrà dos subespais 1-dimensionals Galois invariants i podríem usar aquesta mateixa idea per determinar que $\mathrm{Gal}(F(\phi[T])/F)$ és isomorf a un subgrup de $\mathfrak{D}$ el subgrup diagonal.

[1] La noció de polígon de Newton i les propietats utilitzades d'aquest estan explicades a les pàgines 144-151 de [Neu99]

Exemple 5.3.7 (Subgrup de Cartan escindit)**.** Siguin a una arrel del polinomi $f(x) = x^{q-1} - T$ i b una arrel de $g(x) = x^{q-1} - (T+1)$, aquest dos polinomis són irreductibles pel criteri d'Eisenstein aplicat als primers T i $T+1$ respectivament. A més, com $\ker(f) = \mathbb{F}_q^* a$ i $\ker(g) = \mathbb{F}_q^* b$, $F(a)/F$ i $F(b)/F$ són extensions de Galois de grau $\geq q-1$. També tenim el següent:

Proposició 5.3.8 ([DF04], Proposició 36 de la Part IV)**.** *Sigui K un cos de característica que no que no divideix a n i que conté les arrels n-èssimes de la unitat, llavors l'extensió $K(\sqrt[n]{a})/K$ per $a \in K$ és cíclica de grau divisor de n.*

Així, pel que ja hem vist i per la Proposició 5.3.8, $\mathrm{Gal}(F(a)/F) \cong \mathrm{Gal}(F(b)/F) \cong \mathbb{F}_q^*$.

Ara sigui $W = \mathbb{F}_q a + \mathbb{F}_q b$, aquest és un $\mathbb{F}_q$-subespai vectorial 2-dimensional de F^{sep} i com W és estable respecte de l'acció de $\mathrm{Gal}(F^{\mathrm{sep}}/F)$,

$$h(x) = x \prod_{0 \neq w \in W} \left(1 - \frac{x}{w}\right) \in F[x].$$

A més, pel Lema 2.1.3, $h(x)$ és $\mathbb{F}_q$-lineal i si definim $\phi_T(x) = Th(x)$, ϕ és un mòdul de Drinfeld de rang 2 sobre F ja que $\deg(\phi_T) = |W| = q^2$.

Veiem que $F(a) \cap F(b) = F$ perquè T ramifica totalment en $F(a)$, però no ramifica en $F(b)$. Aleshores tenim el següent resultat de teoria de Galois que diu que:

Proposició 5.3.9 ([DF04], Corol·lari 22 de la Part IV)**.** *Siguin E_1 i E_2 dos extensions de Galois d'un cos K amb $E_1 \cap E_2 = K$, llavors*

$$\mathrm{Gal}(E_1E_2/K) \cong \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K).$$

Per això, com $F(\phi[T]) = F(a,b) = F(a)F(b)$, per la Proposició 5.3.9 obtenim que

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{Gal}(F(a)/F) \times \mathrm{Gal}(F(b)/F) \cong \mathbb{F}_q^* \times \mathbb{F}_q^*.$$

Exemple 5.3.10 (Subgrup de Cartan no escindit)**.** Sigui $\mathfrak{p} \in A$ un primer amb $\deg(\mathfrak{p}) = 2$, definim

$$\phi_T(x) = \frac{T}{\mathfrak{p}} C_{\mathfrak{p}}(x)$$

on $C_T(x) = Tx + x^q$ és el mòdul de Carlitz. Òbviament $F(\phi[T]) = F(C[\mathfrak{p}])$, i pel Teorema 5.2.1,

$$\mathrm{Gal}(F(\phi[T])/F) \cong (A/(\mathfrak{p}))^* \cong \mathbb{F}_{q^2}^*.$$

Exemple 5.3.11 (Normalitzador d'un subgrup de Cartan escindit)**.** Si $q = 2$, el normalitzador d'un subgrup de Cartan escindit és $\mathrm{GL}_2(\mathbb{F}_2)$ per la Proposició 4.2.2 i això ja ho hem vist a l'Exemple 5.3.2.

Suposem que $q \neq 2$ i llavors sigui $K = F(\alpha)$ on α és una arrel de x^2+x+T, K/F és una extensió de Galois de grau 2 ja que x^2+x+T és irreductible a F. Això es deu a que si $\deg(\alpha) \leq 0$, tenim que $\deg(\alpha^2+\alpha) \leq 0 < 1 = \deg(T)$ i si $\deg(\alpha) \geq 1$, $\deg(\alpha^2+\alpha) \geq 2 > 1 = \deg(T)$ que no pot ser. Observem que això implica que el ∞[1] ramifica totalment a K i denotem β a l'altra arrel de x^2+x+T.

Notem que si q és parell, $\beta = \alpha + 1$ i si q és senar, les arrels de x^2+x+T són

$$\frac{-1+\sqrt{1-4T}}{2} \quad \text{i} \quad \frac{-1-\sqrt{1-4T}}{2}.$$

[1] Per ∞ ens referim a la valoració $v_\infty = -\deg$, la qual clarament ramifica perquè a K hi ha elements de grau no enter com α ja que $\deg(\alpha) = 1/2$.

Així, siguin a una arrel de $x^{q-1}+\alpha$ i b una arrel de $x^{q-1}+\beta$, aquests dos polinomis són irreductibles pel criteri d'Eisenstein aplicat a $\widetilde{\infty}$, que és l'infinit de K i és únic perquè ∞ ramifica totalment a K. Per això, seguint el mateix argument que a l'Exemple 5.3.7 tenim que $\mathrm{Gal}(K(a)/K) \cong \mathrm{Gal}(K(b)/K) \cong \mathbb{F}_q^*$ per la Proposició 5.3.8. Veiem que $K(a) \cap K(b) = K$ ja que T escindeix completament en dos primers diferents α i β perquè $T = \alpha\beta$ i α ramifica totalment en $K(a)$, però no ramifica en $K(b)$. Aleshores com $K(a,b) = K(a)K(b)$, per la Proposició 5.3.9 obtenim que

$$\mathrm{Gal}(K(a,b)/K) \cong \mathrm{Gal}(K(a)/K) \times \mathrm{Gal}(K(b)/K) \cong \mathbb{F}_q^* \times \mathbb{F}_q^*.$$

Sigui σ l'element no trivial de $\mathrm{Gal}(F/K)$, llavors $\sigma(\alpha) = \beta$, i per tant, $\sigma(a)^{q-1} = \sigma(a^{q-1}) = = \sigma(\alpha) = \beta$. Això implica que $\sigma(a)$ és una arrel de $x^{q-1}+\beta$, és a dir, és un $\mathbb{F}_q$-múltiple de b. Com a conseqüència, $W = \mathbb{F}_q a + \mathbb{F}_q b$ és un $\mathbb{F}_q$-subespai vectorial 2-dimensional de $K(a,b)$ estable respecte l'acció de $\mathrm{Gal}(K(a,b)/F)$ i si definim

$$\phi_T(x) = Tx \prod_{0 \neq w \in W} \Big(1 - \frac{x}{w}\Big),$$

ϕ és un mòdul de Drinfeld de rang 2 sobre F pel Lema 2.1.3 i $F(\phi[T]) = K(a,b)$. Si prenem $\{a, \sigma(a)\}$ com la base de W, podem identificar $\mathrm{Gal}(F(\phi[T])/K)$ amb $\mathfrak{D}$ i σ amb $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, i per això, per la Proposició 4.2.2,

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathcal{N}(\mathfrak{D}).$$

Exemple 5.3.12 (Normalitzador d'un subgrup de Cartan no escindit)**.** Considerem ϕ el mòdul de Drinfeld sobre F donat per

$$\phi_T(x) = Tx - x^{q^2}.$$

Pel Corol·lari 2.6.6 sabem que $\mathbb{F}_{q^2} \subseteq F(\phi[T])$, i per tant, $F(\phi[T])/\mathbb{F}_{q^2}(T)$ és una extensió de Galois. També veiem que $C_T^{(-1)}(x) = Tx - x^{q^2}$ determina un mòdul de Drinfeld de rang 1 sobre $\mathbb{F}_{q^2}(T)$. Com a conseqüència, pel Teorema 5.2.1, tenim que

$$\mathrm{Gal}(F(\phi[T])/\mathbb{F}_{q^2}(T)) = \mathrm{Gal}(\mathbb{F}_{q^2}(T, C^{(-1)}[T])/\mathbb{F}_{q^2}(T)) \cong \mathbb{F}_{q^2}^*.$$

Ara siguin $a = \sqrt[q^2-1]{T}$ i $\alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $\phi[T] = \mathbb{F}_{q^2} a = \mathbb{F}_q a + \mathbb{F}_q \alpha a$ és un $\mathbb{F}_q$-subespai vectorial 2-dimensional de $F(\phi[T])$ pel qual triem la base $\{a, \alpha a\}$. En cas que q sigui parell, es pot escollir $\delta \in \mathbb{F}_q$ de manera que $x^2 + x + \delta$ sigui irreductible i si escollim α com una de les arrels d'aquest polinomi, l'altra és $\alpha + 1$. Així, sigui σ l'element no trivial de $\mathrm{Gal}(\mathbb{F}_{q^2}(T)/F)$, $\sigma(a) = a$ i $\sigma(\alpha a) = (\alpha+1)a$ i el podem identificar amb $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Si q és senar, sempre existeix $\varepsilon \in \mathbb{F}_q$ tal que $x^2 - \varepsilon$ és irreductible i si α és una de les seves arrels, $-\alpha$ és l'altra. Per això, $\sigma(a) = a$ $\sigma(\alpha a) = -\alpha a$ i podem identificar σ amb $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. En tot cas, per la Proposició 4.2.4 obtenim que

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathfrak{T}$$

on $\mathfrak{T}$ denota un subgrup de Cartan no escindit de $\mathrm{GL}_2(\mathbb{F}_q)$ qualsevol.

Observació 5.3.13. Sigui K una extensió finita de F, llavors tota extensió L/K de Galois finita és de la forma $L = K(\phi[T])$. Això es deu a que L ha de ser el cos de descomposició d'un polinomi separable $f(x) \in K[x]$ i siguin $\alpha_1, \ldots, \alpha_n \in K^{\mathrm{sep}}$ les arrels d'aquest, llavors $W = \mathbb{F}_q\alpha_1 + \cdots + \mathbb{F}_q\alpha_n$ és un $\mathbb{F}_q$-subespai vectorial de K^{sep} estable respecte l'acció de $\mathrm{Gal}(K^{\mathrm{sep}}/K)$. Aleshores definim

$$\phi_T(x) = Tx \prod_{0 \neq w \in W} \Big(1 - \frac{x}{w}\Big),$$

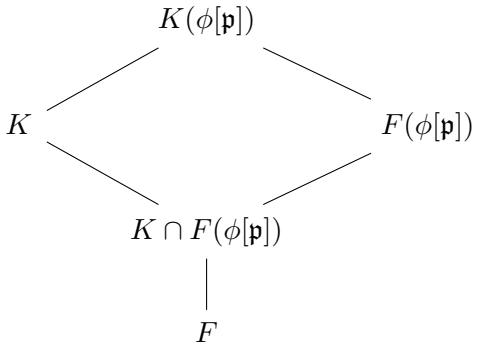
i pel Lema 2.1.3, ϕ és un mòdul de Drinfeld de rang n sobre K que compleix que $L = K(\phi[T])$.

5.4 Multiplicació complexa

Recordem que un mòdul de Drinfeld ϕ de rang 2 sobre F té multiplicació complexa si ocorre que $\text{rang}_A(\text{End}(\phi)) = 2$. Com ϕ és injectiu ja que $\deg(\phi_a) = -\infty$ si i només si $a = 0$, identifiquem $\phi(A)$ amb A i com $\phi(A) \subseteq \text{End}(\phi)$, podem pensar que $A \subseteq \text{End}(\phi)$. Així, com $\text{End}(\phi)$ és un domini commutatiu per la Proposició 2.3.3, si definim $K = Q(\text{End}(\phi))$ el cos de fraccions de $\text{End}(\phi)$, obtenim una extensió de cossos K/F de grau 2. Sigui B la clausura entera de $\text{End}(\phi)$ en K, tenim el següent diagrama:

$$\begin{array}{ccccc} \text{End}(\phi) & \hookrightarrow & B & \hookrightarrow & K \\ & & \downarrow & & \downarrow \\ & & A & \hookrightarrow & F \end{array}$$

Aleshores sigui $\mathfrak{p}$ un primer de A, obtenim el següent diagrama de cossos:



Com K/F és una extensió de grau 2, o bé $\mathfrak{p}$ ramifica totalment, o bé escindeix completament o bé és inert. No obstant, pel primer cas tenim el següent resultat:

Lema 5.4.1 ([Bae95], Teorema 1.5)**.** *Usant aquesta notació, si $\mathfrak{p}$ ramifica en K, llavors ϕ té mala reducció respecte $\mathfrak{p}$.*

A partir d'ara suposem que $\mathfrak{p}$ és un primer de bona reducció de ϕ i ens restringim als dos últims casos.

Teorema 5.4.2 ([Geb03], Teorema 4.3.3)**.** *Usant la mateixa notació, si $G = \text{Gal}(F(\phi[\mathfrak{p}])/F)$, $\mathfrak{Z}$ és un subgrup de Cartan escindit i $\mathfrak{T}$ és un subgrup de Cartan no escindit de $\text{GL}_2(\mathbb{F}_\mathfrak{p})$, llavors si $\mathbb{F}_\mathfrak{p} \neq \mathbb{F}_2$, ocorre que:*

(1) $\begin{cases} \mathfrak{p} \text{ escindeix en } K/F \text{ i} \\ K \cap F(\phi[\mathfrak{p}]) = F \end{cases} \Rightarrow$ *G és isomorf a un subgrup de $\mathfrak{Z}$,*

(2) $\begin{cases} \mathfrak{p} \text{ escindeix en } K/F \text{ i} \\ K \cap F(\phi[\mathfrak{p}]) = K \end{cases} \Rightarrow$ *G no és isomorf a un subgrup de $\mathfrak{Z}$, però sí a un de $\mathcal{N}(\mathfrak{Z})$,*

(3) $\begin{cases} \mathfrak{p} \text{ és inert en } K/F \text{ i} \\ K \cap F(\phi[\mathfrak{p}]) = F \end{cases} \Rightarrow$ *G és isomorf a un subgrup de $\mathfrak{T}$,*

(4) $\begin{cases} \mathfrak{p} \text{ és inert en } K/F \text{ i} \\ K \cap F(\phi[\mathfrak{p}]) = K \end{cases} \Rightarrow$ *G no és isomorf a un subgrup de $\mathfrak{T}$, però sí a un de $\mathcal{N}(\mathfrak{T})$.*

Si $\mathbb{F}_\mathfrak{p} = \mathbb{F}_2$, aleshores tenim que:

$$\textit{(1)} \begin{cases} \mathfrak{p} \textit{ escindeix en } K/F \textit{ i} \\ K \cap F(\phi[\mathfrak{p}]) = F \end{cases} \Rightarrow \ G \cong \{1\},$$

$$\textit{(2)} \begin{cases} \mathfrak{p} \textit{ escindeix en } K/F \textit{ i} \\ K \cap F(\phi[\mathfrak{p}]) = K \end{cases} \Rightarrow \ G \cong \mathbb{Z}/2\mathbb{Z},$$

$$\textit{(3)} \begin{cases} \mathfrak{p} \textit{ és inert en } K/F \textit{ i} \\ K \cap F(\phi[\mathfrak{p}]) = F \end{cases} \Rightarrow \ G \cong \{1\} \textit{ o } G \cong \mathbb{Z}/3\mathbb{Z},$$

$$\textit{(4)} \begin{cases} \mathfrak{p} \textit{ és inert en } K/F \textit{ i} \\ K \cap F(\phi[\mathfrak{p}]) = K \end{cases} \Rightarrow \ G \cong \mathbb{Z}/2\mathbb{Z} \textit{ o } G \cong \mathrm{GL}_2(\mathbb{F}_2).$$

Observem que si ϕ té multiplicació complexa i $\mathrm{Gal}(F(\phi[\mathfrak{p}])/F) \cong \mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$, aleshores $q = 2$, $\deg(\mathfrak{p}) = 1$, $\mathfrak{p}$ és inert en K/F i $K \subseteq F(\phi[\mathfrak{p}])$. Aquesta situació pot ocórrer com veurem en el següent exemple:

Exemple 5.4.3. Considerem ϕ el mòdul de Drinfeld de rang 2 sobre F determinat per

$$\phi_T(x) = Tx - x^{q^2}.$$

Aquest té multiplicació complexa perquè $\mathrm{End}(\phi) = \mathbb{F}_{q^2}\phi(A) \cong \mathbb{F}_{q^2}[T]$ pel Corol·lari 2.6.6. A més, com hem vist a l'Exemple 5.3.12, $\mathrm{Gal}(F(\phi[T])/F) \cong \mathcal{N}(\mathfrak{T})$ i si $q = 2$, això vol dir que

$$\mathrm{Gal}(F(\phi[T])/F) \cong \mathrm{GL}_2(\mathbb{F}_2).$$

També veiem que sigui $\mathfrak{p}$ un primer de A amb $d = \deg(\mathfrak{p})$, és obvi que $\mathbb{F}_{q^2} \subseteq F(\phi[\mathfrak{p}])$ i com $K = \mathbb{F}_{q^2}(T)$, $\mathfrak{p}$ és inert en K/F si d és senar i escindeix si d és parell. Així, com ϕ no té primers de mala reducció, pel Teorema 5.4.2 sabem que si d és senar, $\mathrm{Gal}(F(\phi[\mathfrak{p}])/F)$ no és isomorf a un subgrup de $\mathfrak{T}$, però sí a un de $\mathcal{N}(\mathfrak{T})$, i si d és parell, no és isomorf a un subgrup de $\mathfrak{Z}$, però sí a un de $\mathcal{N}(\mathfrak{Z})$.

Notem que sempre ens referim a $\mathfrak{Z}$ i $\mathfrak{T}$ com a subgrups de Cartan de $\mathrm{GL}_2(\mathbb{F}_\mathfrak{p})$, així que poden variar en funció de d.

Ara suposem que d és senar. Si pensem en $\overline{\phi} = \mathrm{Red}(\phi, \mathfrak{p})$ la reducció de ϕ mòdul $\mathfrak{p}$ i ens posem en el context del Lema 3.2.9, $g = 0$ i $\Delta = -1$, i per tant, $c_0 = 1$, $c_1 = 0$ i $c_k = (-1)^{q^{k-2}}(\overline{T} - \overline{T}^{q^{k-1}})$, cosa que implica que $c_n = 0$ per tot n senar positiu. En particular, $I(\overline{\phi}) = c_d = 0$, i pel Lema 2.2.10, $H(\overline{\phi}) = 2$. Com el coeficient de grau 1 de $\phi_\mathfrak{p}$ és $\mathfrak{p}$ i el de grau q^{2d} és -1, això és equivalent a dir que $\phi_\mathfrak{p}(x)/x$ compleix les hipòtesis del criteri d'Eisenstein aplicat a $\mathfrak{p}$, i per tant, és irreductible. A més, com $\mathfrak{p}$ és inert en K, $\phi_\mathfrak{p}(x)/x$ segueix sent irreductible en K, i per això, $[F(\phi[\mathfrak{p}]) : F] = [F(\phi[\mathfrak{p}]) : K] \cdot [K : F] \geq 2(q^{2d} - 1)$. Com a conseqüència,

$$\mathrm{Gal}(F(\phi[\mathfrak{p}])/F) \cong \mathcal{N}(\mathfrak{T}).$$

Concretament, $\mathrm{Gal}(F(\phi[T])/F) \cong \mathcal{N}(\mathfrak{T})$ com ja havíem vist a l'Exemple 5.3.12.

Si d és parell, com $B = \mathbb{F}_{q^2}[T]$ és un domini d'ideals principals, sabem que existeixen dos primers diferents $\mathfrak{P}_1$ i $\mathfrak{P}_2$ de grau $d' = d/2$ de B tals que $\mathfrak{p} = \mathfrak{P}_1\mathfrak{P}_2$. Aleshores com $C_T^{(-1)}(x) = Tx - x^{q^2}$ defineix un mòdul de Drinfeld sobre K i és clar que $F(\phi[\mathfrak{p}]) = K(C^{(-1)}[\mathfrak{p}])$, pel Teorema 5.1.1 i pel teorema xinès del residus tenim que

$$\mathrm{Gal}(F(\phi[\mathfrak{p}])/K) = \mathrm{Gal}(K(C^{(-1)}[\mathfrak{p}])/K) \cong (B/(\mathfrak{p}))^* \cong (B/(\mathfrak{P}_1))^* \times (B/(\mathfrak{P}_2))^* \cong \mathbb{F}_{q^{2d'}}^* \times \mathbb{F}_{q^{2d'}}^*.$$

Per tant, $[F(\phi[\mathfrak{p}]) : F] = [F(\phi[\mathfrak{p}]) : K] \cdot [K : F] = 2(q^{2d'} - 1)^2 = 2(q^d - 1)^2$ i obtenim que

$$\mathrm{Gal}(F(\phi[\mathfrak{p}])/F) \cong \mathcal{N}(\mathfrak{Z}).$$

Observem que una variació d'aquest últim argument també funciona per al cas on d és senar.

Bibliografia

[Bae95] Sunghan Bae. *Hecke characters of singular Drinfeld modules*. Pacific J. Math. **167**, no. 2, 215-230, 1995.

[Car35] Leonard Carlitz. *Elliptic Modules*. Duke Math. J. **1**, no. 2, 137-168, 1935.

[DF04] David Steven Dummit i Richard Martin Foote. *Abstract Algebra*. 3rd Edition. John Wiley & Sons Inc., Hoboken, New Jersey, 2004. ISBN: 978-0-471-43334-7.

[Dri74] Vladimir Drinfeld. *Elliptic Modules*. Mat. Sb. (N.S.) **94(136)**, 594-627, 1974.

[Geb03] Maximilian Gebhardt. *Galoisdarstellungen auf den Torsionspunkten von Drinfeld-Moduln des Rangs zwei*. Dissertation, Universität des Saarlandes. 2003. DOI: `http://dx.doi.org/10.22028/D291-26020`.

[Gek16] Ernst-Ulrich Gekeler. *The Galois image of twisted Carlitz modules*. J. Number Theory **163**, 316-330, 2016.

[Gek88] Ernst-Ulrich Gekeler. *On the coefficients of Drinfeld modular forms*. Invent. Math. **93**, no. 3, 667-700, 1988.

[Gek91] Ernst-Ulrich Gekeler. *On finite Drinfeld modules*. J. Algebra **141**, no. 1, 187-203, 1991.

[Jun00] Florian Jung. *Charakteristische Polynome von Drinfeld-Moduln*. Diplomarbeit, Universität des Saarlandes. 2000.

[Lan76] Serge Lang. *Introduction to Modular Forms*. Grundlehren der mathematischen Wissenschaften, Vol. 222, 1st Edition. Springer-Verlag, Berlin-Heidelberg, 1976. ISBN: 978-3-540-07833-3.

[MIT21] Massachusetts Institute of Technology. *Lecture Notes in Number Theory I Fall 2021*. Apunts online accedits el 26/06/2023. 2021. URL: `https://ocw.mit.edu/courses/18-785-number-theory-i-fall-2021/mit18_785f21_full_lec.pdf`.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften, Vol. 322, 1st Edition. Springer-Verlag, Berlin-Heidelberg, 1999. ISBN: 978-3-540-65399-8.

[Pap23] Mihran Papikian. *Drinfeld modules*. Graduate Texts in Mathematics, Vol. 296, 1st Edition. Springer, Cham, 2023. ISBN: 978-3-031-19706-2.

[Pia83] Ilya Piatetski-Shapiro. *Complex Representations of GL(2,K) for finite fields K*. Contemporary Mathematics, Vol. 16. American Mathematical Society, 1983. ISBN: 0-8218-5019-9.

[Sch97] Andreas Schweizer. *On singular and supersingular invariants of Drinfeld modules*. Ann. Fac. Sci. Toulouse Math. (6) **6**, no. 2, 319-334, 1997.

[Ser72] Jean-Pierre Serre. *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15**, no. 4, 259-331, 1972.